UNIVERSIDAD LASALLISTA BENAVENTE

INGENIERÍA EN COMPUTACIÓN

Con Estudios Incorporados a la Universidad Nacional Autónoma de México

CLAVE: 8793-16

"FIREWALL EN WINDOWS Y LINUX"

TESIS

Que para obtener el título de

INGENIERO EN COMPUTACIÓN

Presenta:

JUAN ANTONIO NAVARRETE MACÍAS

Asesor:

ING. ANSELMO RAMÍREZ GONZÁLEZ

Celaya, Gto. Enero 2010.

AGRADECIMIENTOS

A mis padres que me han otorgado la vida y que desde que me la dieron me han apoyado incondicionalmente en el transcurso de ella, gracias por el apoyo, he logrado un paso importante mas en mi vida, como es la de haber terminado mis estudios profesionales con los cuales a partir de ahora me ayudaran a tener un mejor trabajo y por consiguiente un estilo de vida mejor.

A mi esposa que me ha apoyado desde el momento en que la conocí, así mismo me ha dado palabras de aliento, ánimos y ganas de seguir superándome.

A mis compañeros y amigos de clase que durante el transcurso de la carrera me apoyaron en la realización de trabajos y proyectos que se me dificultaron y que había que sacar adelante para no quedar a deber materias.

A la UNIVERSIDAD LASALLISTA BENAVENTE que me abrió las puertas para poder realizar mis estudios y me albergo durante 5 años cumpliendo con los planes de estudio para mi educación profesional.

CONTENIDO

PÁGINA

INTRODUCIÓN

El desarrolló de este tema se realiza con el propósito de llevar acabo el estudio de los Firewall en Windows y Linux para proporcionar elementos y conocimientos de los mismos con el fin de proporcionar al alumno de ingeniería desarrollos que puedan servir para su formación académica como ingeniero en sistemas.

La siguiente tesis desarrolla temas referentes a los Firewall desde la parte de los sistemas de Windows y Linux, estos son los sistemas operativos qua han buscado un desarrollo de nuevos programas que mantengan la seguridad de nuestra información, recordando así que la información es lo mas importante dentro de las organizaciones; así mismo se pretende realizar un estudio de algunos métodos y programas que se han realizado en estos sistemas operativos. En esta tesis también se exponen los peligros que se pueden correr al navegar en Internet, también se busca que una vez comprendidos estos peligros se tenga el conocimiento para poder defenderse de aquellos ataques que se pudieran tener al navegar en Internet.

Una vez realizado este estudio podremos formar un amplio criterio acerca de los métodos y programas que nos permiten tener a salvo nuestra información.

CAPÍTULO 1

SEGURIDAD EN INTERNET

OBJETIVO: Conocer lo que es Internet y saber como funciona, con el fin de entender cuales son los riesgos que se corren al navegar, enviar correos y manejar información dentro de esta red, además de saber quienes pueden robar información, para que en los capítulos posteriores se comprenda mejor el manejo de los FIREWALL (corta fuegos).

1.1 INTERNET: PASADO, PRESENTE Y FUTURO

Internet en un principio

"En 1969 el Departamento de Defensa de los Estados Unidos creó la ARPA (Agencia para Proyectos Avanzados de Investigación). El Departamento de Defensa aspiraba crear una red de comunicación de tal manera que si una parte de la misma sufría un colapso total, los mensajes pudieran encontrar el camino hasta su destino de cualquier manera. El resultado fue ARPAnet. En 1983, más que nada debido a razones pragmáticas, ARPAnet se dividió en dos sistemas diferentes llamados ARPAnet y MILENET. La primera fue puesta a disposición de los ciudadanos para uso civiles, y MILENET fue reservado para uso militar. Las redes se conectaron de tal manera que los usuarios pudieran intercambiar información; esto acabó por conocerse como Internet. Con el paso del tiempo comenzaron a surgir otras redes como BITNET Y CSNET. Al principio se trabajaba con redes totalmente independientes, usadas con propósitos educativos o de investigación, pero más adelante se conectaron con Internet para poder compartir información fácilmente entre organizaciones.

Uno de los avances más importantes de Internet tuvo lugar en 1986, cuando NFS (Fundación Nacional de la Ciencia) de los Estados Unidos creo NSFNET con el propósito de conectar varias supercomputadoras de gran velocidad a lo largo del país, principalmente con fines de investigación. ARPAnet fue desmantelada y NSFNET se convirtió en el principal conducto de Internet."[1]

[1] Internet Paso A Paso Segunda Edición (Jerry Honeycutt) www.monografias.com

Internet hoy en día

Internet es una gran red. ¿Por qué es una gran red? Porque Internet no es más que una red de grandes servidores en configuración de cliente-servidor, quiero decir con esto que nosotros le mandamos una petición al servidor que es respondida por éste y son vistos e interpretados en nuestra propia computadora. Por ello, Internet es una red WAN[2].

Ya a estas alturas casi todo el mundo ha oído o sabe navegar en Internet, como comúnmente se le dice. Este es tan variado y ofrece tantos servicios que la comunicación no es ni será la misma jamás gracias a este servicio. Uno de los ejemplos mas comunes es el del E-MAIL o correo electrónico.

Una de las redes más grandes del mundo es la Microsoft. La razón es simple, las mayorías de computadoras personales utilizan su sistema operativo Windows aunque en el mercado existan otros sistemas operativos como LINUX.

Internet en el futuro

Aunque ya en el presente el comercio por internet es algo común, se esperará más de éste en el futuro al igual que las videoconferencias, música, juegos, educación, televisión, imágenes, radio y muchas cosas mas que se volverán cada día más que cotidianas, se harán necesarias y a este medio se le sacara el mayor provecho posible.

[2] WAN (world area network) Red de Area Mundial

1.2 ¿CÓMO FUNCIONA INTERNET?

Casi todas las computadoras ya poseen un módem y en todos los países hay servicio de Internet; por lo tanto, no hay que ser un experto para tener acceso a Internet sino recursos, que es lamentable aunque justo, ya que todo servicio se debe de pagar.

Cada computadora que ingresa o se conecta a Internet recibe el nombre de host. Algunos host ofrecen el contenido o aplicaciones que poseen, por lo que se les denomina servidores.

Otras computadoras como las que utilizan todos los usuarios de Internet (clientes) consumen el contenido o la información ofrecida por los servidores. A esta relación se le denomina cliente-servidor.

En la figura 1.1 se muestra gráficamente la relación cliente-servidor, del lado izquierdo de nuestra figura se muestra a un usuario común en Internet solicitando información, si algún servidor dentro de la red contiene la información relacionada con la que el usuario solicitó, éste otorga la información al cliente siempre y cuando el cliente tenga permisos para utilizar la información.

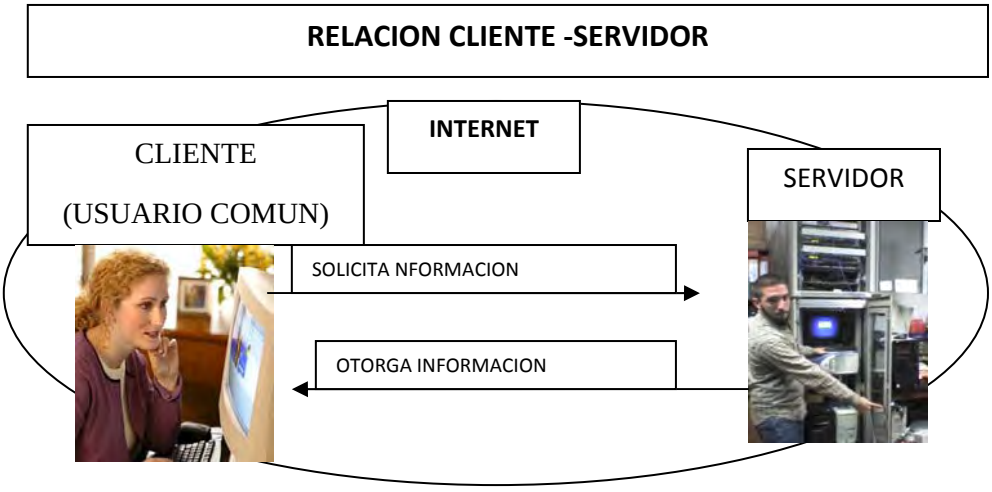


Fig. 1.1 Relación cliente -servidor[3]

[3] imagen realizada por el autor de esta tesis

Cada computadora necesita una configuración correcta para conectarse a Internet, esto es un protocolo, un cliente y un adaptador. En nuestro caso, el cliente seríamos los que utilizamos alguna computadora, el adaptador del dispositivo que esté utilizando en su computadora (donde ya viene instalado un MODEN o Tarjeta de red) y un protocolo que será el TCP/IP (lo trae instalado el sistema operativo de nuestra máquina cuando trae tarjeta de red o MODEM).

El protocolo TCP/IP no es más que un protocolo para poder comunicarse con otras computadoras. Este protocolo norma la manera en que el host se comunica, empaqueta los datos y encuentra el camino hasta la computadora remota. Este protocolo está formado por dos protocolos diferentes, unidos y acoplados. Cada persona tiene una contraseña dada por el proveedor de Internet que es única también para poder tener acceso a este servicio.

1.3 DIRECCIONES IP

Una dirección IP (Protocolo de Internet) es un número de identificación único de la computadora tal como es reconocida por las demás computadoras en Internet. Las direcciones IP constan de cuatro números separados por puntos como muestra, Ej. 99.90.40.187.

El protocolo de IP usa direcciones de IP para identificar los host y encaminar los datos hacia ellos. Todos los host deben tener una dirección de IP única para las comunicaciones.

1.3.1 Formatos de direcciones

Una dirección de IP tiene un formato de dos partes que son la dirección de red y la dirección local.

- La dirección de red: identifica la red a la que está conectado el nodo.
- La dirección local: identifica a un nodo particular dentro de la red de una organización

Todas las computadoras deben tener una dirección de IP única en el rango de sistemas con los que se comunican, ejemplo: no puede haber dos IP 99.90.40.187.

1.3.2 Clases de Direcciones

Toda organización que planee conectarse a Internet debe conseguir un bloque de direcciones IP únicas. Las direcciones se consiguen de la autoridad de riesgo apropiada (InterNIC) y aquí en México es NIC.mx.

Las direcciones de IP son números de 32 bits habitualmente en formato decimal (la representación decimal de cuatro valores binarios 8 bits concatenados por puntos).

Por ejemplo, el formato binario para la dirección IP 128.2.7.9 es: 10000000.00000010.00000111.00001001

Existen 5 clases de dirección IP

- Clase A: el rango de IP es 0.1.0.0 a 126.0.0.0
- Clase B: el rango de IP es 128.0.0.0 a 191.255.0.0
- Clase C: el rango de IP es 192.0.1.0 a 223.255.255.0
- Clase D: el rango de IP es 224.0.0.0 a 239.255.255.255
- Clase E: Las direcciones de esta clase se reservan para usos futuros.

1.4 TCP

El TCP (Protocolo de Control de Transmisión) define la manera en que la información será separada en paquetes y enviada a través de Internet, se asegura también de que estos paquetes se reordenen y también los revisa para localizar errores. Como en cada computadora que participa en Internet se le asigna una dirección IP, una persona ordinaria no podría recordar tantos números de cada computadora, por lo que hay una manera más fácil de hacerlo, por el DOMINIO.

1.4.1 Dominio

Es el nombre para un host determinado. Por ejemplo, la dirección IP de HOTMAIL (64.4.44.7), pero su nombre dominio es www.hotmail.com. Los tres primeros números indican la red a la que pertenece nuestra computadora, y el último sirve para diferenciar nuestra computadora de los otros que utilizan la misma red.

Los nombres de dominio consisten en dos o más palabras separadas por puntos, por ejemplo: www.yahooo.com.mx, www.esmas.com, www.google.com, etc.

Los dominios del primer nivel son más específicos como COM, NET, EDU, lo cual indica el tipo de organización que es, incluso el país donde se encuentra.

Mostraremos algunos ejemplos

Nombre	Descripción
Com	Organizaciones comerciales y con fines de lucro
Net	Organizaciones Diversas y sin fines de lucro
Edu	Agencias de Educación
Gob	Agencias del gobierno federal
Es	España

Mx	México
Ar	Argentina
Uk	Reino unido

WWW (World Wide Web) es una recopilación masiva de documentos estáticos e interactivos vinculados entre sí. Se utiliza un navegador web, para visualizar esas páginas web, las cuales se encuentran en cientos de miles de servidores alrededor del mundo.

1.4.2 DNS

Los servidores de nombre de dominio (DNS) traducen estos nombres en direcciones IP.

1.4.3 IPS

El concepto de proveedor de servicios de Internet (IPS) refiere a una empresa que proporciona conectividad con Internet. La labor de estas empresas es de mantener una gran red que se conecta directamente con Internet. La computadora que utiliza la gente común como usted y yo, establece una conexión de red con el proveedor de servicios a través de un protocolo de conexión y de un módem. A esto se le llama conexión PPP (protocolo punto a punto). La diferencia entre una conexión directa con una PPP es que la PPP es más lenta que la directa y también que es temporal o hasta que el cliente siga pagando el servicio. Todas las páginas de Internet tienen un formato, este es el HTML[4] que es un lenguaje que especifica como se ve un documento de Internet. Es conocido como lenguaje de etiquetas o de marcado de hipertexto.

[4] HTML (lenguaje de hipertexto de marcas) herramienta que permite desarrollar aplicaciones 'WWW'

1.5 HACKER´s

Los piratas ya no tienen un parche en su ojo ni un garfio en reemplazo de la mano. Tampoco existen los barcos ni los tesoros escondidos debajo del mar. Los piratas se presentan con un cerebro desarrollado, curioso y con muy pocas armas: una simple computadora y una línea telefónica.

HACKER`s: Una palabra que aún no se encuentra en los diccionarios pero que ya suena en todas las personas que alguna vez se interesaron por la informática o leyeron algún diario. Proviene de "hack", el sonido que hacían los técnicos de las empresas telefónicas al golpear los aparatos para que funcionen. Hoy es una palabra temida por empresarios, legisladores y autoridades que deseen controlar a quienes se divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información que es exclusiva o privada.

Los HACKER's se definen como aquellos que, con ayuda de sus conocimientos informáticos, consiguen acceder a los servidores de los bancos y de las instituciones del gobierno. Navegan por información que no les pertenece, roban software caro y realizan transacciones de una cuenta bancaria a otra.

1.5.1 El área de los HACKER's

El HACKER puede realizar dos tipos de actividades:

- *Acceder a un sistema informático*: El término lleva asociados las herramientas y trucos para obtener cuentas de usuarios válidos de un sistema informático, que de otra forma serian inaccesibles para los HACKER's. Se podría pensar que esta palabra está íntimamente relacionada con la naturaleza repetitiva de los intentos de acceso. Además, una vez que se ha conseguido acceder, las cuentas ilícitas a veces compartidas con otros asociados se denominan frescas.

Los medios de comunicación conceptualizan a los HACKER‘s como un joven de menos de veinte años, con conocimientos de informática, pegado al teclado de su computadora, siempre en busca de una cuenta no usada o un punto débil en el sistema de seguridad. Aunque esta visión no es muy precisa, representa bastante bien el aspecto del término.

- *Explorar y aprender a utilizar un sistema informático*: se ocupa de lo que sucede una vez que se ha conseguido acceder al sistema cuando se ha conseguido una clave de acceso. Como el sistema está siendo utilizado sin autorización, el HACKER no suele tener, acceso a los manuales de operación y otros recursos disponibles para los usuarios legítimos del sistema. Por tanto, el usuario experimenta con estructuras de comandos y explora ficheros para conocer el uso que se da al sistema. En oposición con el primer aspecto del término, aquí no se trata sólo de acceder al sistema (aunque alguno podría estar buscando niveles de acceso más restringidos), sino de aprender más sobre la operación general del sistema.

Contrariamente a lo que piensan los medios de comunicación, la mayoría de los HACKER’s no destruyen y no dañan deliberadamente los datos. El hacerlo iría en contra de su intención de mezclarse con el usuario normal y atraería la atención sobre su presencia, haciendo que la cuenta usada sea borrada. Después de gastar un tiempo sustancioso en conseguir la cuenta, el HACKER pone una alta prioridad para que su uso no sea descubierto. Además de la obvia relación entre las dos acepciones, la palabra “HACKER” se reserva generalmente a aquellos que se dedican al segundo tipo. En otras palabras, un HACKER es una persona que tiene el conocimiento, habilidad y deseo de explorar completamente un sistema informático. El mero hecho de conseguir el acceso

(adivinando la clave del acceso) no es suficiente para conseguir la denominación. Debe haber un deseo de liderar, explotar y usar el sistema después de haber accedido a él. Esta distinción parece lógica, ya que no todos los intrusos mantienen el interés un vez que han logrado acceder al sistema.

1.6 SEGURIDAD EN EL INTERNET

Seguridad en el internet tiene distintos significados dependiendo del punto de vista que se tome.

- Para algunos significa poder observar Internet en paz, sabiendo que nadie está husmeando lo que se está viendo. Además de proteger la privacidad del usuario y la integridad de su computadora. Soluciones tecnológicas incluyen antivirus que protegen a la computadora de los virus, programas maliciosos, y limitan la transmisión de información desde el browser sin la autorización del usuario.
- Para otros significa ejecutar en forma segura transacciones financieras. Además de la confidencialidad de documentos, proteger información privada para que no sea divulgada por terceras personas. La principal solución es la criptografía, y otras como el uso de Passwords.
- Para los ISP, servidores y proveedores de servicios, proteger al servidor de entradas sin autorización, vandalismo y ataques que lo dejen fuera de servicio. Las soluciones tecnológicas abarcan desde sistemas de FIREWALL' s (cortafuegos) hasta sistemas de seguridad de sistema operativo.
- Para los operadores del internet significa la confianza de que sus sitios no serán invadidos por delincuentes (HACKER's) o usados como una entrada para colapsar una red de área local.

En la actualidad, la seguridad en Internet es muy simple y muy compleja a la vez.

- Simple por que es muy fácil quebrar la internet en partes y descubrir donde residen los problemas.
- Difícil porque no existen soluciones simples o mágicas que hagan a la internet segura.

La seguridad considera los siguientes puntos de vista:

- *Desde el punto de vista del usuario*: El servidor es administrado por una organización que se supone que es la dueña de éste. El documento que retorna al servidor se encuentra libre de virus maliciosos. El servidor remoto no grabará y distribuirá información del usuario que éste considere privada.

- *Desde el punto de vista del administrador del servidor*: El usuario no irrumpirá el servidor y alterará su contenido. El usuario no ganará acceso a documentos no permitidos a él. El usuario no acaparará el servidor inhabilitado al resto de las personas. Debe haber autentificación de usuarios.

- *Desde el punto de vista de ambos*: La conexión de red se encuentra libre de terceras personas que están espiando la comunicación. La información que se envía entre el usuario y el servidor se mantiene intacta, libre de la corrupción que le puedan hacer terceras personas. El propósito de la seguridad en Internet es asegurar que estas suposiciones sean válidas.

1.6.1 Formas de entrada, de ataques en un sitio

Existen diversos riesgos, algunos afectan al usuario, otros al administrador del sitio y muchas veces a ambos al mismo tiempo.

Esto es debido a que los intrusos dañan a cualquiera, por lo tanto la encriptación le interesa tanto al usuario como al administrador.

- *Riesgos que afectan al cliente y al servidor*: si dos computadoras se encuentran en lugares físicos distintos, la información viaja a través de muchos sitios intermedios antes de llegar a su destino final. Un mensaje desde el browser puede viajar a través de la línea telefónica hasta el proveedor de servicios de Internet ISP, luego a través de una línea dedicada hasta el proveedor regional de ISP o RSP, y desde ahí transferido rápidamente al servidor de destino en alguna otra parte del mundo. En cualquier parte de este camino el mensaje puede ser interceptado por algún intruso. Pequeños programas llamados "rastreadores de paquetes" (packet sniffers) son enviados para escuchar o husmear el tráfico en la red, mirando ciertos elementos interesantes como passwords o números de tarjetas de créditos. Este programa puede ser instalado en cualquier nodo perteneciente al camino que recorre el mensaje. Para ello, el individuo debe irrumpir algún ISP o alguna computadora de la LAN o el mismo servidor Internet. Los pequeños ISP son más vulnerables y por lo tanto son un objetivo común para los delincuentes.

Los "rastreadores de paquetes" pueden escuchar cualquier tráfico que esté circulando:

- URL requerido
- Documento retornado por el servidor
- Passwords
- Formularios llenados por el usuario
- Más aún, un individuo puede alterar el contenido escuchando. Estos dañinos programas pueden residir en un servidor por varios días sin que se dé cuenta el administrador. La nueva generación de cable módem incrementa el riesgo del "rastreador de paquetes".

- *La defensa contra estos programas es la criptografía*: Esto es encriptar o codificar todo lo que se transmite entre el browser y el servidor. Cuando un usuario se conecta al sitio de Internet de su banco, ¿Cómo puede saber que el sitio al cual se conecto pertenece efectivamente al banco? En sentido contrario, ¿Cómo puede saber el banco que el cliente que se conecto responde efectivamente a un cliente legítimo?.

  Para ello, debe existir un mecanismo de autentificación de individuos y organizaciones. Las mismas técnicas de encriptación son utilizadas para resolver este problema. Se crean firmas digitales y certificados para autentificar usuarios y servidores, respectivamente.

- *Riesgos que afectan sólo a clientes*: Actualmente las páginas de Internet contienen una colección de tecnología que las hacen más interesantes e interactivas. Los Java Applets, controles de ActiveX, plugs-in, Java scripts, etc. Son programas que vienen incrustados en páginas de Internet que pueden poner en riesgo al cliente si están programados para esto y son ejemplos de estas tecnologías.

  Pero estos contenidos activos pueden contener problemas de seguridad que comprometen la privacidad del usuario y la integridad de los datos almacenados en su computadora. Este problema es más bien potencial que real. Una variedad de Applets maliciosos se han demostrado, pero muy pocos ataques se han denunciado. Por ejemplo, existen Applets molestosos que hacen congelar y caer al browser.

- *Infringir la privacidad*: Cada vez que se trae una página de un sitio remoto, se libera en el servidor una tarjeta de llamado, que puede ser la dirección de Internet del usuario, o información personal.

- *Los sitios de Internet pueden extraer información del usuario de diversas maneras*: la más básica es el log del servidor, el cual corresponde a la hora y fecha de conexión; otra es la dirección del usuario, la identidad del documento requerido, y el URL del documento solicitado previamente. Otra información está disponible en los ISP donde los servidores proxy guardan cada servidor visitado por sus clientes. Otra manera en que los sitios de Internet recolectan información es a través de los "cookies". Los "cookies" son diseñados para mejorar la navegación por la Internet, ya sea entrando a bases de datos, recorriendo mapas complejos y otras operaciones que requieren mantener continuidad a lo largo de la navegación. Lo que debe preocupar mas es cuando el usuario entrega información voluntariamente, e-mails, news, formularios etc.

- *Riesgos que afectan solo a servidores*: Existe la posibilidad de que un sitio de una organización sea irrumpido y modificado por delincuentes, los cuales explotan alguna debilidad tal como un sistema operativo o un servidor de Internet mal configurado. Otra fuente de problemas de seguridad son los Scripts de CGI. Los CGI corresponden a interfaces de motores de búsqueda y base de datos. Estos programas son muy usados y muy simples de construir, y por lo tanto son hechos por programadores sin experiencia en temas de seguridad. Muchos delincuentes irrumpen servidores de Internet con diversos objetivos: atacar las bases de datos, sistemas de archivos, y otros sistemas de misión crítica. Siempre el servidor provee una puerta para los intrusos. El problema de los servidores de Internet es que son sistemas complejos con una presión constante al crecimiento, y cualquier error que se cometa es una puerta para intrusos. La tecnología que hace un servidor protegido es el uso de cortafuegos (FIREWALL's).

- *Inhabilitación del Servidor*: Los intrusos pueden dejar el servidor fuera de servicio. Estos ataques se hacen al sistema operativo, software de Internet y CGI's. No existe una fórmula para evitar este riesgo, simplemente se puede disminuir el daño poniendo límites a los recursos del servidor y de otros programas, cerrando las vulnerabilidades conocidas del sistema operativo y otro software.

- *Seguridad en el Servidor*: Si el servidor está conectado a Internet o si está restringido a una intranet[5] tendrá un incremento de visibilidad que puede tener un efecto: ser un objetivo natural para atacar.

1.6.2 Problemas que abren hoyos en la seguridad de los sitios de Internet.

A continuación se muestran algunas fallas mortales de seguridad en los sitios de Internet:

Un software seguro es aquel que hace lo que se supone que hace y nada más. Sin embargo, casi todos los software tienen Bugs; la mayoría son errores de programación inadvertidos, pero algunos son "back doors" (código deliberadamente ubicado en el programa por el desarrollador del software para ayudar al debugging, que luego olvidan quitar). Los Bugs son más frecuentes mientras más grandes y complejo es el programa. Cuando ocurre un bug en un programa de aplicación, las consecuencias son molestas: el programa se cae, los documentos quedan corruptos, etc. Cuando un bug ocurre en un programa que actúa en un servidor de red, puede llegar a comprometer al servidor. Bugs típicos de software de servidor aparecen cuando el servidor se expone a una situación no anticipada por los desarrolladores, o cuando subsistemas del software

[5] Intranet es una red privada

interactúan inesperadamente. Los HACKERS están constantemente buscando Bugs en el software de servidor, ya que cada bug representa un potencial portal de entrada. Ya sea alimentando el input del servidor o manipulando el ambiente del servidor en una manera controlada, el HACKER puede engañarlo para que desempeñe una acción determinada o conseguir acceso a alguna parte del sistema. Los software contienen Bugs relacionados con la seguridad debido a la complejidad de los servidores modernos y la competencia entre los vendedores, que sacan rápidamente nuevas versiones, grandes, complejas y poco gestadas. Además, los Bugs en cualquier sistema que interactúe con el servidor (base de datos, Scripts de CGI, módulos API de servidor) pueden abrir hoyos en la seguridad.

Configuración incorrecta del software de sistema. Un sitio de Internet no será seguro al menos que el servidor y el sistema operativo estén configurados correctamente. La mayoría de los sistemas transportan datos en modo permisivo; servicios de red populares se activan por defecto, se habilitan facilidades de configuración remota, y la política de acceso a los archivos del sistema es muy liberal. Ejecutar un servidor de red sin saber sobre él es la mayor vulnerabilidad.

Otra vulnerabilidad son las cuentas de usuario creadas por defecto que algunos sistemas operativos crean como una conveniencia de instalación, pero que no las borran cuando ya no las necesitan.

La configuración por defecto de Windows NT Workstation es particularmente promiscua, aunque la versión de servidor no lo es tanto. Muchos dialectos de UNIX vienen con todo activado, y cuesta lograr un sistema que haga solo lo que necesita y nada más.

Los permisos de archivo desconfigurado son un gran problema. Sistemas operativos multiusuario (UNIX y Windows NT incluidos) usan privilegios de cuenta como su mecanismos de seguridad fundamental. Cada usuario tiene registrada una cuenta y cada cuenta

es asociada a un diferente set de privilegios. Estos mecanismos dan a usuarios confiables, tales como administradores de sistemas, la habilidad de hacer los ajustes necesarios en la configuración del sistema mientras previene que otros hagan cambios no autorizados. Si un usuario malicioso ve que un archivo de configuración puede ser manipulado, podría modificar el sistema y posiblemente expandir su acceso a éste.

Como los usuarios, servidores de red y otros programas también tienen distintos privilegios. En teoría un servidor debería tener sólo los privilegios que necesita para hacer su trabajo; en la práctica, muchos sitios dan a sus servidores mucho más amplio acceso al sistema que el que necesitan. Cuando este es el caso, el servidor se vuelve un tentador objetivo para atacar. Los HACKER's de sistemas buscarán explotar hoyos en la seguridad del software del servidor para ejecutar comandos de su elección. Cuando son exitosos, los comandos se ejecutarán con privilegios de servidor, permitiendo acceso a información confidencial.

No tener una política de seguridad. Sin una política de seguridad no se puede saber si un sitio es seguro. Esta política debería estar escrita, con una lista de lo que es o no permitido; debe reflejar la realidad política de la organización y cualquier riesgo y conveniencia que se podría aceptar. Su importancia radica en que da algo concreto para diseñar y evaluar las medidas de seguridad. También sirve para evaluar cambios propuestos al sistema.

Por último, la experiencia de la gente que ejecuta el host y los software de los servidores es el aspecto más importante en la seguridad del sistema. El sistema más seguro es con el que se sienten más confortables y con el cual tiene mayor experiencia.

1.6.3 ¿Son los servidores realmente seguros?

Servidores seguros simplemente son aquellos que pueden proteger documentos en tránsito con encriptación. Desde un punto de

vista más amplio, los servidores seguros son tan vulnerables a los HACKER's como cualquier otro. El servidor más seguro es el más simple. Servidores Web que sólo recuperan páginas HTML estáticas tienen menos Bugs que aquellos más elegantes.

1.6.4 Pasos para asegurar un sitio Web

- Asegurar el sistema operativo y el servidor Web. Hacer el sistema operativo tan seguro como sea posible, instalando los parches de los vendedores relacionados con seguridad, remover servicios innecesarios, y fijar las configuraciones por defecto para hacerlas menos permisivas. Cuando el sistema operativo es seguro, se puede instalar el software del servidor.
- Monitorear el servidor por actividad sospechosa. No todos los ataques son obvios, por ellos se debe monitorear la actividad sospechosa del servidor.
- Controlar el acceso a documentos confidenciales. No todas las partes del servidor Web son públicas. Muchos sitios tienen áreas privadas que sólo los usuarios registrados pueden visitar.

  En Intranet es deseable que el sitio entero sea accesible sólo por invitación. Servidores con SSL protegen información confidencial, encriptando documentos Web que pasan por la red, y usando certificados de clientes para autentificación de usuario confiable.

- Escribir scripts de CGI seguros. Aún si el servidor, el sistema operativo y todos los programas que soportan son seguros, los scripts de CGI o módulos de servidor que se instalen pueden dejar al sitio abierto a un ataque.
- Proteger la LAN contra el servidor Web. Antes de conectar el servidor Web a Internet, debe asegurarse que no puede ser usado como trampolín para atacar otras máquinas de misión critica dentro de la organización. Lo mismo se aplica para organizaciones grandes donde un departamento no confía en

otro. A menudo esto se logra endureciendo cuidadosamente el servidor y removiendo relaciones confiables entre unos y otros miembros de la LAN. A veces es necesario ir más allá y levantar un muro entre al LAN y el servidor.

- Mantenerse al día en problemas de seguridad. Hoyos en la seguridad se descubren todos los días. Se debe checar periódicamente los sitios Web de los vendedores y fabricantes del sistema operativo y de software third-party que se han instalado. Si hay un parche de seguridad, se debe usar tan pronto como sea posible.

En conclusión se puede afirmar que, hoy en día, en casi las partes del mundo existe el servicio de Internet, la mayoría de la gente la sabe utilizar ya sea por pasatiempo o por necesidad, pero existen grandes problemas que se pueden presentar una vez navegando en ella, como es la de poner en peligro la información que se guarda en su computadora, ya que existen muchos HACKER'S esperando y buscando errores o entradas(hoyos) para poder manipular o robar aquella información que les parezca importante y si se puede para beneficio de ellos, pero no debemos de olvidar que puede haber personas trabajando dentro de organizaciones muy grandes y pueden robarse información en dispositivos de almacenamiento tal vez por interés propio o porque son espías, así que no debemos olvidar que se deben de crear políticas de seguridad para tener, lo mas que se pueda, a salvo de información.

CAPÍTULO 2

FIREWALL

OBJETIVO: Conocer que es un cortafuegos (firewall) y algunos aspectos importantes de este sistema, con el fin de tener los conocimientos para poder implementarlos en Windows y Linux.

2.1 INTRODUCCION

La seguridad ha sido el tema principal a tratar cuando una organización desea conectar su red privada a Internet. Sin tomar en cuenta el tipo de negocios, se ha incrementado el número de usuarios de redes privadas por la demanda del acceso a los servicios de Internet. También, al igual las organizaciones, buscan las ventajas que ofrecen las paginas en el WWW y los servidores FTP de acceso público en el Internet.

Los administradores de la red tienen que incrementar todo lo relacionado con la seguridad de sus sistemas, debido a que exponen a la organización privada de su información, así como la infraestructura de su red a los Expertos de Internet (Internet HACKER's). Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no autorizado de usuarios a los recursos mismos de la red privada, y protegerse contra la exportación privada de información. Aun así, si una organización no está conectada a Internet, ésta debería establecer una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger eficazmente la información que es exclusiva y solamente para uso de la empresa.

La política de seguridad deberá de ser un documento que esté firmado por la alta gerencia de la empresa y mediante el cual se especifican varios aspectos referentes a la seguridad de la información de la empresa. Estos aspectos pueden ser desde cuantas letras han de tener las contraseñas de los usuarios corporativos y cada cuanto tiempo han de cambiarlas, que protocolos (Telnet, http, smtp, ftp, etc.) van a permitir utilizar en las máquinas internas con las externas y en su caso quien va a poder iniciar la conexión, y hasta la política que se va a seguir para permitir el acceso restringido a recursos internos.

Un cortafuegos (FIREWALL) nunca protegerá al cien por ciento a estos recursos internos de acceso no autorizados, ya que las técnicas de violar los sistemas avanzan día a día y todos los días se descubren nuevos fallos en sistemas operativos y software de servidores. Pero también es cierto que un cortafuegos bien configurado junto con servidores bien configurados y protegidos pueden poner las cosas muy difíciles a estos potenciales intrusos, por no decir imposibles (siempre teniendo en cuenta la política de seguridad de la empresa y a la correcta configuración de cortafuegos y servidores).

Los sistemas cortafuegos son uno de los dos enfoques básicos que se han dado al aspecto de la seguridad en redes informáticas.

Estos dos enfoques han sido tradicionalmente:

1. La defensa en profundidad que se caracterizaba para proteger cada una de las máquinas disponibles a ser accedidas por personas no autorizadas.
2. La defensa perimetral consistente en llevar toda la carga correspondiente a la seguridad en la red corporativa al elemento de conexión de esta red corporativa con el exterior, o con las redes en las que potencialmente se encuentren las personas que puedan querer acceder a nuestra información de forma no autorizada, ya que está demostrado que un tanto por ciento elevado de los fraudes informáticos proceden del interior de las propias organizaciones.

Existen muchos tipos de cortafuegos, no obstante la clasificación más clara quizás sería la que los diferencia según la forma de implementar la política de seguridad de la empresa atendiendo al nivel de la capa OSI[6] en la que se implementa dicha política de seguridad.

[6] CAPA OSI (Open Systems Interconnect) interactua con los programas de aplicacion o con ususario.

Internet es una red accesible a todo el mundo, sin ningún requisito de entrada, bastando con tener la conexión a algún proveedor de acceso, por lo que puede ser considerada como insegura.

Disposición de router como frontera (FIREWALL) entre redes

Sus protocolos y modo de funcionamiento son conocidos y la manera de acceder a ella es muy sencilla.

Una red corporativa, diseñada para ser usada en una empresa o grupo de empresas, es muy diferente aunque emplee los mismos protocolos o técnicas de acceso; en este caso, la información que se maneja es un bien inapreciable para la empresa y deben ponerse todos los medios necesarios para garantizar que se utilizan correctamente.

Por tanto, en todos aquellos casos que exista una conexión entre la red de la empresa e Internet, se ha de ser muy cuidadoso para evitar cualquier ataque, activo o pasivo, que pueda venir del exterior, en este caso de Internet. Ello se puede hacer de muy diversas maneras, y una de ella es poniendo una barrera de entrada/salida entre ambas redes, que controle la información en uno u otro sentido, barrera que suele estar en el router que sirve para la interconexión.

Los routers operan en el nivel 3 (red) de OSI, que incluye una dirección de red y una del dispositivo; ello proporciona innumerables ventajas, ya que permite la interconexión entre redes diferentes, como puede ser una Token Ring, o una red WAN, y permite dividir una red en varias subredes, eligiendo el mejor camino para enviar un paquete IP sin la necesidad de mantener extensas tablas que contengan la dirección de todos y cada uno de los dispositivos.

Una aplicación adicional de los routers es actuar como pasarela de seguridad (FIREWALL o cortafuegos) entre la red del cliente y otra red exterior, como pueda ser Internet. Con ello se pretende proteger las redes corporativas frente a entradas o salidas no autorizadas. La posición en la que se coloque el FIREWALL es

crítica, ya que debe ser en la zona de separación entre lo que se considera de la red interna segura y la red externa insegura.

En las aplicaciones de acceso a Internet el FIREWALL se coloca entre la red local o intranet e Internet. La regla básica de un FIREWALL es asegurar que todas las comunicaciones entre la red propia e Internet se realicen conforme a las políticas de seguridad de la organización o corporación, para lo que evalúan cada paquete que circula por la red (paquetes que atraviesan la frontera entre el interior y el exterior de la red). Además estos sistemas conllevan características de privacidad y autenticación, etc.

2.2 ¿QUÉ ES UN FIREWALL?

Es un sistema o grupo de sistemas básicos de seguridad, que se encarga de otorgar permisos a los usuarios externos de una red privada para tener acceso a la información y a ciertos servicios que pueden ser ejecutados por los usuarios; estos permisos deben cumplir con las reglas y políticas que tienen definidas las empresas para el manejo de la información y aplicaciones que están en red.

Un FIREWALL tiene como función ser el guardia de una red al igual funciona como una barrera entre la computadora y el entorno de red por la cual circula toda la información y protege a toda la red de ataques provenientes del exterior.

Desafortunadamente, cuando el agresor ha logrado ingresar a nuestro sistema, este ya no puede proteger la información mientras el agresor se encuentre adentro.

Un FIREWALL funciona, en principio, denegando cualquier tráfico que se produzca cerrando todos los puertos de nuestra computadora. En el momento que un determinado servicio o programa intente acceder a Internet o a nuestra computadora nos lo hará saber. Podremos en ese momento aceptar o denegar dicho tráfico, pudiendo

así mismo hacer (para no tener que repetir la operación cada vez) permanente la respuesta hasta que no cambiemos nuestra política de aceptación.

El FIREWALL es parte de una política de seguridad completa que crea una defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, reglas de encriptación de datos y discos, normas de protección de virus y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad.

Una buena política debería ser, ante la duda, no aceptar nunca cualquier acceso hasta comprobar que es necesario para un correcto funcionamiento del servicio que pretendamos usar y no es potencialmente peligroso para el sistema. Si denegamos el acceso y nuestro sistema sigue funcionando bien, no es necesario, así que lo debemos denegar.

Con la instalación de un FIREWALL conseguiremos hacer nuestro sistema mucho menos vulnerable a intrusos. Como ejemplo podemos poner el correo electrónico. Si autorizamos en nuestro FIREWALL a que determinado programa de correo acceda a Internet, y al recibir nuestro correo, en un mensaje recibido viene un archivo adjunto con un virus, por ejemplo tipo gusano, el FIREWALL no nos va defender de ello, ya que le hemos autorizado a que este programa acceda a la Red. Lo que si va a hacer es que, si al ejecutar el archivo adjunto, el gusano intenta acceder a la Red por algún puerto que no esté previamente aceptado por nosotros, no lo va a dejar propagarse. Ahora bien, si se hace uso por ejemplo del mismo cliente de correo, si va a propagarse. La misión del FIREWALL es la de aceptar o denegar el trafico, pero no el contenido del mismo. En este caso, la

misión de protegernos es (además del sentido común no ejecutar sin mas de un archivo adjunto) de un programa Antivirus.

El siguiente diagrama muestra en forma grafica la función que realiza un FIREWALL, la cual es rechazar al HACKER, no permitiéndole el acceso a nuestra red; por consiguiente, se muestra una red de computadoras protegida y segura para el fácil manejo de nuestra información.

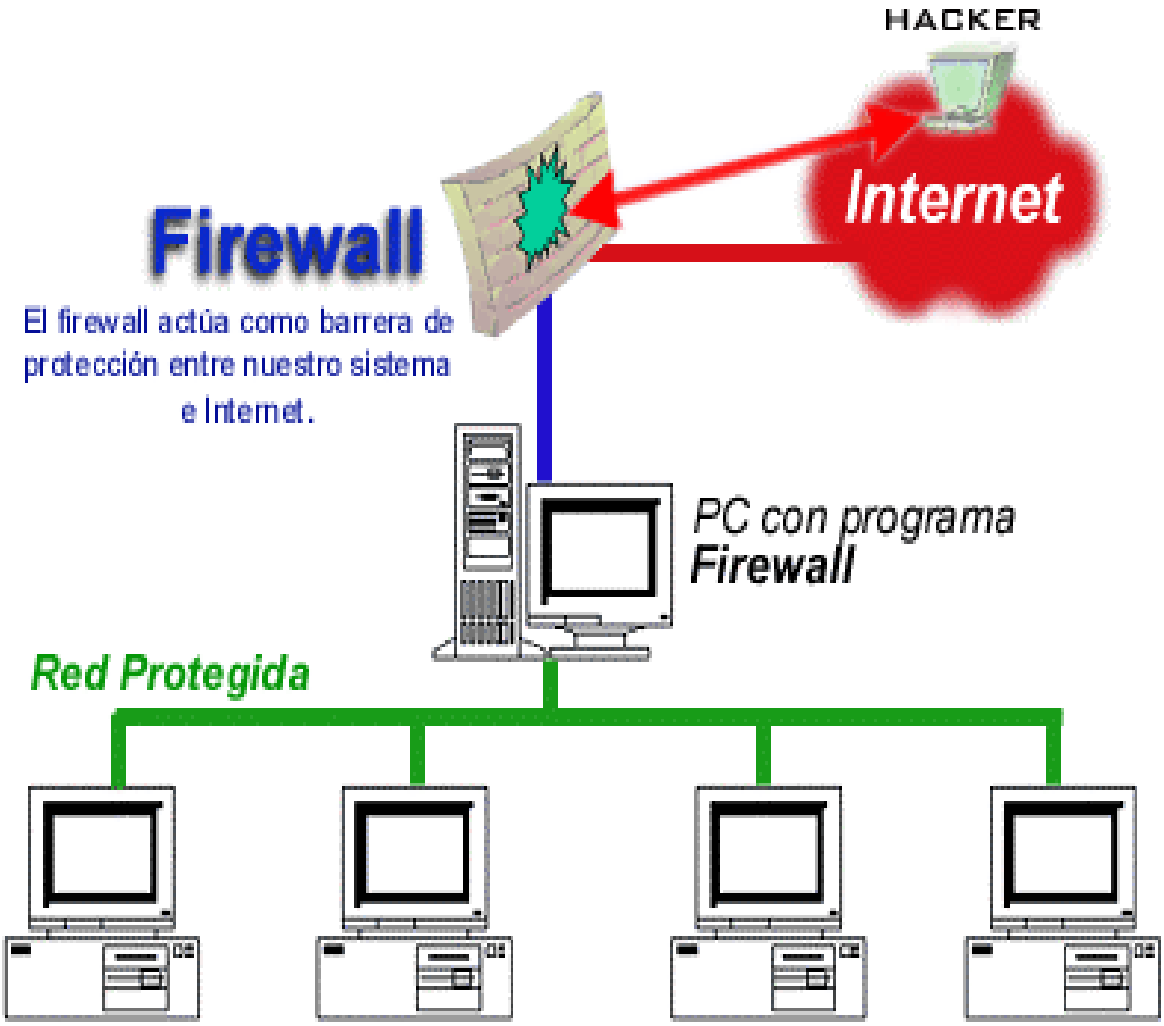


Figura 2.1 [7]

[7] El diagrama fue bajado de www.zonealarm.com

2.3 LIMITACIONES DE UN FIREWALL

Un FIREWALL no puede proteger contra aquellos ataques que se efectúen fuera de su punto de operación.

El FIREWALL no puede proteger de las amenazas a que está sometido por traidores o usuarios inconscientes. El FIREWALL no pude prohibir que los traidores o espías corporativos copien información privada en discos o cualquier otro dispositivo de almacenamiento y substraigan estas de la empresa.

El FIREWALL no puede proteger contra los ataques de la ingeniería social, por ejemplo, un HACKER que pretenda ser un supervisor o un nuevo empleado despistado, persuade al menos sofisticado de los usuarios a que le permita usar su contraseña al servidor de la empresa o que le permita el acceso temporal a la red. Para controlar estas situaciones, los empleados deberían ser educados acerca de los varios tipos de ataque social que pueden suceder, y a cambiar sus contraseñas si es necesario periódicamente.

El FIREWALL no puede proteger contra los ataques posibles a la red interna por virus informativos a través de archivos y software obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios, el FIREWALL de Internet no puede contar con un sistema preciso de SCAN[8] para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él.

La solución real está en que la organización debe ser consciente en instalar software antivirus en cada computadora para protegerse de los virus que llegan por medio de discos o cualquier otra fuente.

Por último, el FIREWALL de Internet no puede proteger contra los ataques posibles en la transferencia de datos; éstos ocurren

[8] SCAN se refiere a los antivirus

cuando aparentemente los datos son enviados o copiados a un servidor interno y son ejecutados provocando un ataque.

Por ejemplo, una transferencia de datos podría causar que un servidor modificara los archivos relacionados a la seguridad haciendo más fácil el acceso de un intruso al sistema.

2.4 BASES PARA EL DISEÑO DICISIVO DEL FIREWALL

Cuando se diseña un FIREWALL de Internet, se tiene que tomar algunas decisiones que pueden ser asignadas por el administrador de red:

⇒ Políticas del FIREWALL
⇒ Política interna de seguridad
⇒ Costo del FIREWALL

2.4.1 Políticas del FIREWALL

Las posturas del sistema FIREWALL describen la seguridad en la organización. Estas son dos posturas opuestas que la política de un FIREWALL de Internet puede tomar:

⇒ La primera postura asume que un FIREWALL puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas.

Esta postura se recomienda únicamente a un limitado número de servicios que pueden ser soportados y seleccionados en un servidor. La desventaja es que el punto de vista de seguridad es más importante que facilitar el uso de los servicios y estas limitantes numeran las opciones disponibles para los usuarios de la comunidad.

⇒ La segunda postura asume que el FIREWALL puede desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso.

Esta postura crea ambientes más flexibles al disponer más servicios para los usuarios de la comunidad. La desventaja de esta postura se basa en la importancia de facilitar el uso que la propia seguridad del sistema. También, el administrador de la red está en su lugar de incrementar la seguridad en el sistema conforme crece la red. Diferente a la primera propuesta, esta postura está basada en conocer las causas acerca de los que tienen la habilidad para conocerlas.

2.4.2 Política interna de seguridad

Tan discutidamente escuchado, un FIREWALL de Internet no está solo, es parte de la política de seguridad total en una empresa, la cual define todos los aspectos en lo que se refiere al perímetro de defensa. Para que ésta sea exitosa, la organización debe conocer qué es lo se está protegiendo. La política de seguridad se basará en una dirección cuidadosa, analizando la seguridad, la asesoría en caso de riesgo y la situación del negocio. Si no se posee la información detallada de la política a seguir, aunque sea un FIREWALL cuidadosamente desarrollado y armado, estará exponiendo la red privada a un posible ataque de un HACKER.

2.4.3 Costo del FIREWALL

¿Cuánto puede ofrecer una organización por su seguridad?

Un simple paquete de filtrado FIREWALL puede tener un costo mínimo, ya que la organización necesita un ruteador conectado al Internet, y dicho paquete ya está incluido como estándar del equipo.

Un sistema comercial de FIREWALL provee un incremento más a la seguridad, pero su costo aumenta dependiendo de la complejidad y el número de sistemas protegidos. Si la empresa posee al experto con ella, un FIREWALL casero pude ser construido con software de domino público, pero este ahorro de recursos repercute en términos del tiempo de desarrollo y el despliegue del sistema FIREWALL. Por último, requiere de soporte continuo para la administración, mantenimiento general, actualización de software, reparación de seguridad e incidentes de manejo. Un sistema comercial Firewall puede puede tener un costo de $32,000.00 hasta $ 240,000.00 pesos dependiendo de la complejidad del mismo.

2.5 COMPONENTES DEL SISTEMA FIREWALL

Después de las decisiones acerca de los ejemplos previos, la empresa puede determinar específicamente los componentes del sistema. Un FIREWALL típico se compone de uno, o una combinación, de los siguientes obstáculos.

- Filtrado de aplicaciones
- Filtrado a Nivel-circuito
- Filtra-paquetes
- Servidor Proxy

2.5.1 Filtrado de Aplicaciones (Applications filtering)

Los FIREWALL que son aplicaciones cliente-servidor y que trabajan al nivel 7 de OSI simulan procesos de aplicación, contraseñas y verificación. Estos dispositivos no tratan los paquetes entre las interfaces a nivel 3, sino que disponen de programas específicos para cada protocolo, por lo que, debido a su complejidad, son poco eficientes, pero muy seguros.

Examinan el contenido de nivel de aplicación de todos los paquetes y ofrecen servicios Proxy. Es el extremo opuesto al filtrado de paquetes. En lugar de basarse en el filtrado del flujo de paquetes, tratan los servidores por separado, utilizando el código adecuado para cada uno.

Es probablemente el sistema más seguro, ya que no necesita tratar complicadas listas de acceso, y centraliza en un solo punto de gestión los servicios. Las pasarelas a nivel de aplicación son prácticamente la única solución efectiva para el tratamiento seguro de aquellos servicios que requieren permitir conexiones iniciadas desde el exterior (servicios como FTP, Telnet, Correo Electrónico).

En realidad, lo que utiliza es una puerta de acceso para cualquier servicio. Al ser esta puerta de uso obligatorio, podemos establecer en ella los criterios de control que queramos. Atravesada la puerta, puede ocurrir que la propia pasarela de nivel de aplicación ofrezca el servicio de forma segura o que establezca una conexión con la computadora interna que realmente ofrece el servicio, teniendo en cuenta que este último deberá estar configurado para aceptar conexiones tan sólo desde nuestra pasarela de nivel de aplicación para este servicio.

2.5.2 Filtrado a nivel de circuito (Circuit-level Firewall)

Trabajan a nivel de la capa de transporte creando un sistema cliente-servidor de pasarelas (proxy’s) que actúan filtrando paquetes por protocolos; establecen un control sobre el tráfico de cada protocolo y son específicos para cada uno de ellos, por lo que su eficacia queda disminuida.

Se basan en el control de las conexiones TCP y actúan como si fueran un cable de red: por un lado, reciben las peticiones de conexión a un puerto TCP, y por otro, establecen la conexión con el destinatario deseado, si se han cumplido las restricciones establecidas, copiando los octetos de un puesto al otro.

Este tipo de FIREWALL suele trabajar conjuntamente con los servidores proxy, utilizados para la acreditación, es decir, comprobaciones sobre máquina fuente, máquina destino, puerto a utilizar.

2.5.3 Software filtra-paquetes

Toma las decisiones de rehusar o permitir el paso de cada uno de los paquetes que son recibidos. El programa examina cada data grama para determinar si éste corresponde a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes un su encabezado, lo que hace posible su desplazamiento en un proceso de IP. Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado (TCP, UDP, ICMP, O IP) el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interfaz de entrada del paquete, y la interfaz de salida del paquete. Si se encuentra la correspondencia y las reglas permiten el paso del paquete, éste será desplazado de acuerdo a la información de la tabla de filtrado, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado si éstos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete.

Este software ofrece algunos servicios y beneficios, y tiene además unas limitaciones que se deben considerar.

Servicio dependiente del filtrado

Las reglas acerca del filtrado de paquetes a través de un programa para rehusar o permitir el tráfico están basadas en un servicio específico; por ello, muchos servicios vierten su información en numerosos puertos TCP/UDP conocidos.

Por ejemplo, un servidor Telnet está a la espera para conexiones remotas en el puerto 23 TCP y un servidor SMPT espera las conexiones de entrada en el puerto 25 TCP. Para bloquear todas las entradas de conexión Telnet, el filtro simplemente descarta todos los paquetes que contengan el valor del puerto destino TCP igual a 23. Para restringir las conexiones Telnet a un limitado número de servidores internos, el filtro podrá rehusar el paso a todos aquellos paquetes que contengan el puerto destino TCP igual a 23 y que no contengan la dirección destino IP de uno de los servidores permitidos.

Algunas características típicas de filtrado que un administrador de redes podría solicitar en un filtra-paquetes para perfeccionar su funcionamiento serian:

- Permite la entrada de sesiones Telnet únicamente a una lista específica de servidores internos.
- Permite la entrada de sesiones FTP únicamente a los servidores internos especificados.
- Permite todas las salidas para sesiones Telnet.
- Permite todas las salidas para sesiones FTP.
- Rehusar todo el tráfico UDP.

Servicio independiente del filtrado

Este tipo de ataques ciertamente es difícil de identificar usando la información básica de los encabezados debido a que éstos son independientes al tipo se servicio. Los filtros pueden ser configurados para protegerse de este tipo de ataques pero son más difíciles de especificar; por lo tanto, las reglas para el filtrado requieren de información adicional que pueda ser estudiada y examinada por la tabla de filtrado, inspeccionando las opciones especificas IP, revisando fragmentos especiales de edición, etc.

Algunos ejemplos de este tipo de ataques incluyen:

- *Agresiones originadas por el direccionamiento IP*: para este tipo de ataque, el intruso trasmite paquetes desde afuera, pretendiendo pasar como servidor interno, los paquetes poseen una dirección fuente IP falsa de un servidor interno del sistema. El agresor espera que usando este impostor se pueda penetrar al sistema para emplearlo seguramente como dirección fuente donde los paquetes que trasmita sean autentificados y los del otro servidor sean descartados dentro del sistema. Los ataques por seudofuentes pueden ser frustrados si descartamos la dirección fuente de cada paquete con una dirección fuente "interna" si el paquete llega a una de las interfaces del filtro "externo".
- *Agresiones originadas en el filtro*: En un ataque de filtro, la estación de origen especifica la ruta que un paquete deberá tomar cuando cruce a través del Internet. Este tipo de ataques es diseñado para cuantificar las derivaciones de seguridad y encauzan al paquete por un inesperado camino a su destino.

  Los ataques originados en el filtro pueden ser frustrados simplemente descartando todos los paquetes que contengan fuentes de filtrado opcionales.
- *Agresiones por fragmentación*: Por este tipo de ataques, los intrusos utilizan las características de fragmentación para crear fragmentos extremadamente pequeños y obligan a la información del encabezado TCP a separarse en paquetes. Estos pequeños fragmentos son diseñados para evitar las reglas definidas por el filtrado, examinando los primeros fragmentos y el resto pasa sin ser visto. Aunque si bien únicamente es explotado por sencillos decodificadores, una agresión pequeñísima puede ser frustrada si se descartan todos los

paquetes donde el tipo de protocolo es TCP y la fragmentación de compensación IP es igual a 1.

Beneficios del software filtra-paquetes

La mayoría de sistemas FIREWALL son desplegados usando únicamente filtra-paquetes. Otros, planean los filtros y configuran el ruteador, sea éste pequeño o no. El costo para implementar la filtración de paquetes no es alto, desde que los componentes básicos de los ruteadores incluyen revisiones estándar de software para dicho efecto. Desde entonces, el acceso a Internet es generalmente provisto a través de interfaces WAN, optimizando la operación del filtro, moderando el tráfico y definiendo menos filtros. Finalmente, el filtra-paquetes es por lo general transparente a los usuarios finales y a las aplicaciones, por lo que no se requiere de entrenamiento especializado o software específico que tenga que ser instalado en cada uno de los servidores.

Limitaciones del filtra-paquetes

Definir el filtrado de paquetes puede ser una tarea compleja porque el administrador de redes necesita tener un estudio detallado de varios servicios de Internet, como los formatos del encabezado de los paquetes, y los valores específicos esperados a encontrarse en cada campo. Si las necesidades de filtrado son muy complejas, se necesitará soporte adicional, con la cual el conjunto de reglas de filtrado puede empezar a complicarse y alargar el sistema, haciendo más difícil su administración y compresión. Finalmente, éstas serán menos fáciles de verificar para las correcciones de las reglas de filtrado después de ser configuradas. Potencialmente se puede dejar una localidad abierta sin probar su vulnerabilidad.

Cualquier paquete que pasa directamente a través de un filtra-paquetes puede ser posiblemente usado como parte inicial de un ataque dirigido de datos. Haciendo memoria, este tipo de ataques ocurren cuando los datos se desplazan por el filtro a un servidor

interno. Los datos contienen instrucciones ocultas que puedan causar que el servidor modifique su control de acceso y seguridad relacionando sus archivos y facilitando al intruso el acceso al sistema.

Generalmente, los paquetes entorno al filtro disminuyen conforme el número de filtros utilizados se incrementa. Los filtra – paquetes son optimizados para extraer la dirección destino IP de cada paquete, haciendo relativamente simple la consulta a la tabla de reglas de filtrado, y el desplazamiento de paquetes para la interfaz apropiada de la transmisión. Esto puede consumir ciclos de CPU e impactar al perfecto funcionamiento del sistema. El filtrado de paquetes IP no puede ser capaz de proveer el suficiente control sobre el tráfico. Un filtra-paquetes puede permitir o negar un servicio en particular, pero no es capaz de comprender el contexto y dato del servicio.

Por ejemplo, un administrador de red necesita filtrar el tráfico de la capa de aplicación limitando el acceso a un subconjunto de comandos disponibles por FTP o Telnet, bloquear la importación de Mail o Newsgroups concerniente a tópicos específicos. Este tipo de control es muy perfeccionado a las capas altas por los servicios de un servidor Proxy y en Gateway a Nivel-aplicación.

2.5.4 Servidor Proxy (Proxy Server)

Normalmente, un servidor proxy es un programa que trabaja con servidores externos en nombre de clientes internos. Los clientes proxy se comunican con los servidores proxy, los cuales, a su vez, transmiten solicitudes aprobadas de clientes a servidores auténticos y luego transmiten de nuevo las respuestas a los clientes.

Una de las principales ventajas de utilizar un servidor proxy es la capacidad de ocultar la red interna a proteger desde el exterior, debido a que todos los paquetes que atraviesan el proxy, aparecen en el exterior con la dirección de origen del proxy. La ocultación de las

direcciones IP internas es una técnica que pueda aplicarse sin un servidor proxy, utilizando un Gateway o pasarela de traducción de direcciones. Cuando se utiliza un proxy se establecen conexiones separadas desde el servidor hacia cada punto terminal, lo que permite conexiones más seguras con el uso de la red ya que permite ocultar los detalles del direccionamiento IP interno. En situaciones de tráfico pesado este tipo de FIREWALL's puede convertirse en un cuello de botella en la red, debido a la cantidad de procesos que realiza.

Una función que también realizan los servidores proxy es el "caching" local de contenidos web y la de permitir trabajar en la red de empresa con direcciones ilegales (no permitidas) de Internet y evitar la necesidad de declarar éstas al registro NIC de Internet.

Por todo lo expuesto en este capítulo, se puede señalar que los FIREWALL's son parte esencial de cualquier solución de seguridad en redes y para proporcionar la máxima protección contra ataques, a la vez que permiten soportar aplicaciones innovadoras, es importante que estos equipos actúen como parte de una plataforma integral de seguridad. En definitiva, un FIREWALL es un complemento al resto de medidas corporativas que se han de tomar para garantizar la protección de la información y que han de contemplar no solo los ataques externos, sino también los internos, que puede realizar el propio personal, así como todas aquellas aplicaciones que están instaladas y que pueden tener hoyos por los que se puedan entrar intrusos.

En seguridad, toda medida es poca y hay que estar innovando continuamente para no dejar huecos por donde puedan colarse los intrusos; pero, como esto no siempre es evitable, se empiezan a utilizar técnicas más sofisticadas e ingeniosas, como es facilitar la entrada a la red pero por caminos falsos que no conducen a nada y que permiten detectar los intentos de intrusión, con lo que se está sobre aviso y es más fácil protegerse.

CAPÍTULO 3

FIREWALL EN LINUX

OBJETIVO: Conocer el desarrollo de algunos ejemplos de un cortafuegos en LINUX y algunos aspectos importantes de este sistema.

3.1 INTRODUCCION

LINUX ha tenido capacidad de cortafuegos desde hace ya un tiempo, en forma de Ipfwadm, que era un filtro a nivel de paquetes muy sencillo. De un tiempo a la fecha, se ha visto reemplazado por Ipchains, que es un poco más sofisticado. Este a su vez se ve reemplazado en el Kernel[9] 2.4, con un filtrado de paquetes todavía más avanzado, que es más independiente. Sin embargo, ambos todavía siguen siendo filtros de paquetes, y no permiten características más avanzadas como la inspección de estados o algunos tipos de conexiones proxy. Sin embargo, LINUX soporta IPMASQ, una forma de NAT (Traducción de Direcciones de Red, Network Address Translation). El IPMASQ permite enlazar una red de computadoras a internet, pero haciendo un proxy de sus conexiones a nivel de IP. De tal forma que todo el tráfico parezca provenir y dirigirse a una máquina (la máquina LINUX con IPMASQ) lo cual proporciona un alto grado de protección a la red interna. Como algo mas añadido, los clientes de la red interna no necesitan configurar su proxy; mientras el servidor IPMASQ del LINUX este bien configurado y los clientes lo utilicen como su puerta de enlace por defecto, todo irá bien.

Ipchains e Ipfwadm proporcionan las siguientes funcionalidades:

- ✓ Bloqueo / permiso del paso de datos basado en IP/puerto/interface origen/destino
- ✓ Enmascaramiento de conexiones, basado en IP/puerto/interface origen/destino

[9] KERNEL es el núcleo del sistema

Además, Ipchains soporta:

- ✓ Redireccionamiento de puertos
- ✓ Creación de cadenas, para reglas y condiciones mas complejas, más fácil de mantener
- ✓ Rutado de calidad de servicio, útil en conexiones de baja velocidad o saturadas
- ✓ Especificaciones de IP/puerto/interface además de especificación inversa (utilizando el !)

El HOWTO del cortafuegos y las páginas de “man <command>” (Ipchains o Ipfwadm) se ocupan en gran detalle de la mecánica para la configuración de las reglas, pero en realidad no se ocupan de la estrategia para hacer un filtrado de forma segura. La primera elección que se debe de hacer es si se va a seguir una política de negación o de permisión por defecto, seguido de qué servicios y host se requiere permitir y bloquear.

Cuando se vaya a decidir la política, se debería escoger aquella que deniega todo por defecto, a menos de que esté específicamente permitido o una política que permita todo y bloquee ciertos servicios/host. Generalmente se utiliza una política de negación por defecto, pues de esta forma puede arreglar errores y cambios de forma más segura que una política que permita el flujo de datos por defectos.

Pongamos por ejemplo, se tiene un servidor asegurado vía filtrado con cortafuegos, ejecutando Apache y se le olvida cambiar las reglas del cortafuegos. Si se ha escogido una política permisiva por defecto, cualquiera puede acceder al servidor FTP desde internet, y además, permitiría a cualquiera a comprometer la máquina. Si, por otra parte, se sigue una política de negación por defecto, no habrían accedido al servidor de FTP, ni lo habrían hecho sus usuarios, pero

se daría cuenta más rápidamente. Los usuarios molestos son algo más sencillo de tratar que una red que haya sido comprometida.

A continuación veremos ejemplos para cada servicio de red, ya que para filtrar adecuadamente un protocolo primero hay que entender como se comporta.

3.2 PROGRAMA CON IPFWADM

El Ipfwadm es un sólido paquete de filtrado para LINUX, aunque carece de muchas características disponibles de Ipchains.

Ipfwadm solo soporta 3 objetivos para cada paquete: aceptar, denegar o rechazar, mientras que las reglas del Ipchains se pueden dirigir a 6 objetos, o a un objetivo definido por el usuario. En realidad, el Ipfwadm solo es apropiado para un cortafuegos sencillo a nivel IP y enmascaramiento de IP.

Las opciones básicas son; especificar una dirección, reglas de entrada, reglas de salida, reglas de redireccionamiento (supongamos que se tienen múltiples interfaces, también se ocupan de las reglas de enmascaramiento) y reglas de enmascaramiento que controlan el comportamiento del enmascaramiento (timeouts, etc.) se pueden insertar, añadir y borrar reglas, configurar políticas por defecto y listar todas las reglas.

Aparte de eso es muy parecido a Ipchains, con pequeñas variaciones.

El script que se muestra a continuación es apropiada para un servidor que está haciendo un enlace entre 2 redes (10.0.0.x en eth0, 10.0.0.1 y 192.168.0.x en eth1, 192.168.0.1) ejecutando un servidor de correo.

```
#!/bin/bash
#
# Primero limpiar todas las reglas
#
ipfwadm -f -I
ipfwadm -f -O
ipfwadm -f -F
#
# Permitir el redireccionamiento entre las dos redes y si no es entre # ellas, denegarlo
#
ipfwadm -F -a accept -P all -S 10.0.0.0/24 -i eth0 -D 192.168.0.0/24
ipfwadm -F -a accept -P all -S 192.168.0.0/24 -i eth1 -D 10.0.0.0/24
ipfwadm -F -p deny
#
# Y por supuesto hay que dejar que entren los paquetes
#
ipfwadm -I -a accept -P tcp -S 10.0.0.0/24 -i eth0 -D 192.168.0.0/24
ipfwadm -I -a accept -P tcp -S 192.168.0.0/24 -i eth1 -D 10.0.0.0/24
#
# Dejarles acceder al servidor de correo pero a nada más
#
ipfwadm -I -a accept -P tcp -S 10.0.0.0/24 -i eth0 -D 10.0.0.1 25
ipfwadm -I -a accept -P tcp -S 192.168.0.0/24 -i eth0 -D 192.168.0.1 25
ipfwadm -I -p deny
```

Nunca se debería escoger Ipfwadm sobre Ipchains, ya que Ipchains ofrece un grado de control mucho más afinado y es mucho más flexible que Ipfwadm.

3.3 PROGRAMA IPCHAINS

A través del programa Ipchains se puede filtrar el tráfico por una gran variedad de criterios, mediante reglas (algo así como sentencias, si condición entonces acción).

Las reglas se integran es tres grupos diferenciados:

- ✓ Reglas de entrada (para paquetes que llegan al router).
- ✓ Reglas de encaminamiento (decisión sobre encaminar paquetes o no).
- ✓ Reglas de salida (paquetes que salen del router por algún interfaz).

Este programa es tan versátil que nos permite indicar, en cada, regla la cadena (entrada, encaminamiento, salida); el protocolo interfaz, direcciones de origen y destino, y el puerto utilizado en la conexión, así como la acción a tomar (denegar, rechazar, aceptar o enmascarar) caso que determinado paquete cumpla la regla.

Es muy necesario denegar el acceso desde el exterior a todos los servicios. El siguiente script (se muestra en la siguiente hoja) se encarga de cerrar el acceso exterior a todos los servicios, manteniendo abierto el acceso desde la red local y realizando el trabajo de encaminador hacia Internet.

Para ejecutar las reglas del script correctamente se deben tener dos datos:

- ✓ La dirección IP del interfaz por el que nos conectamos a Internet.
- ✓ El nombre de la interfaz.

En caso de que la conexión sea mediante PPP con asignación dinámica de IP por lo que recibimos la IP y el nombre del interfaz del programa PPP que al establecer la conexión nos pasa esa información en dos variables de entorno que son $IFNAME e $IPLOCAL.

La ejecución del script se invoca en /etc/ppp/ip-up.local[10]

/etc/ppp/ip-up.local

Este fichero se encarga de realizar las acciones que podamos necesitar una vez que se establezca la conexión PPP. Por ejemplo, registrar conexiones, o establecer las reglas del cortafuegos. En este caso invocaremos en el la llamada a un script */etc/rc.d/rc.firewall* en el que incluiremos las reglas de filtrado de paquetes.

#!/bin/sh

/etc/rc.d/rc.firewall

#!/bin/sh

#----------

CONFIGURACIÓN DEL CORTAFUEGOS

#----------

[10] En caso de tener conexión directa o IP fija, la llamada a rc. Firewall debe realizarse en otro sitio(por *ejemplo /etc/rc.d/rc.local*) y estos datos, asignarse a mano.

```
# Incluir la llamada a este script en /etc/ppp/ip-up.local
#--------------------------------------------------------------------
# Variables de entorno activadas por pppd al establecerá la comunicación
#--------------------------------------------------------------------
# IPLOCAL <- dirección IP del interfase ppp
# IFNAME  <- nombre del interfase local


# Asignaciones locales

LOCALNET="192.168.0.0/24"
IPADDR=$IPLOCAL
TODAS="0.0.0.0/0"

# Nombres de Interfaz

PPP=$IFNAME
ETH="eth0"
LO="lo"

# Direcciones

LOOPBACK="127.0.0.1/32"
CLASE_A="10.0.0.0/8"
CLASE_B="172.16.0.0/16"
CLASE_C="192.168.0.0/16"
MULTICAST="240.0.0.0/3"
BROADCAST_0="0.0.0.0"
BROADCAST_1="255.255.255.255"

# Puertos conocidos

ROOT="0:1023"          # Puertos reservados a root
NO_ROOT="1024:65535"    # puertos no root
NFS="2049"             # (TCP/UDP) NFS
OPENWINDOWS="2000"      # (TCP) OpenWindows
```

```
XWINDOWS="6000:6001"    # (TCP) X Window
PORTS="1020:1023"       # Rango de puertos de SSH
PORTS="6667"            # Puertos del servidor IRC

#--------------------------------
# Limpiamos las reglas anteriores
#--------------------------------
/sbin/ipchains -F

#-------------------------------------------
# Establecer la política por defecto
#      Permitir entrada
#      Permitir salida
#      Denegar IP Forward
#-------------------------------------------
/sbin/ipchains -P input   ACCEPT
/sbin/ipchains -P forward DENY
/sbin/ipchains -P output  ACCEPT

#-----------------------------------------------------------------------
#               Spoofing y direcciones ilegales
#-----------------------------------------------------------------------
# Evitar que entren paquetes de fuera indicando como dirección de origen
# nuestra IP

/sbin/ipchains -A input -i $PPP -s $IPADDR -j DENY

# Evitar que lleguen de fuera paquetes con origen o destino 127.0.0.1

/sbin/ipchains -A input -i $PPP -s $LOOPBACK -j DENY
/sbin/ipchains -A input -i $PPP -d $LOOPBACK -j DENY

# Evitar que lleguen de fuera paquetes con origen o destino de direcciones
# reservadas para redes privadas
```

```
/sbin/ipchains -A input -i $PPP -s $CLASE_A -j DENY
/sbin/ipchains -A input -i $PPP -d $CLASE_A -j DENY
/sbin/ipchains -A input -i $PPP -s $CLASE_B -j DENY
/sbin/ipchains -A input -i $PPP -d $CLASE_B -j DENY
/sbin/ipchains -A input -i $PPP -s $CLASE_C -j DENY
/sbin/ipchains -A input -i $PPP -d $CLASE_C -j DENY

# Evitar que salgan hacia el exterior paquetes cuyo destino sea nuestra
# propia IP

/sbin/ipchains -A output -i $PPP -d $IPADDR -j REJECT

# Evitar que salgan paquetes con origen o destino 127.0.0.1

/sbin/ipchains -A output -i $PPP -s $LOOPBACK -j REJECT
/sbin/ipchains -A output -i $PPP -d $LOOPBACK -j REJECT

# Evitar que salgan paquetes con origen o destino a direcciones reservadas
# para redes privadas

/sbin/ipchains -A output -i $PPP -s $CLASE_A -j REJECT
/sbin/ipchains -A output -i $PPP -d $CLASE_A -j REJECT
/sbin/ipchains -A output -i $PPP -s $CLASE_B -j REJECT
/sbin/ipchains -A output -i $PPP -d $CLASE_B -j REJECT
/sbin/ipchains -A output -i $PPP -s $CLASE_C -j REJECT
/sbin/ipchains -A output -i $PPP -d $CLASE_C -j REJECT

# Denegar paquetes de broadcast de fuera

/sbin/ipchains -A input -i $PPP -s $BROADCAST_1 -j DENY
/sbin/ipchains -A input -i $PPP -d $BROADCAST_0 -j DENY

#------------------------------------------------------------------------
# Poner aquí los servicios explícitamente permitidos
# auth (identd) 113, ctcp (irc) (59)
#------------------------------------------------------------------------
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR  59 -j
```

```
ACCEPT
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 113 -j
ACCEPT

#------------------------------------------------------------------------
# Rechazar acceso del exterior a servicios de nuestra máquina
# Echa un vistazo con "netstat -a" para ver qué puertos tienes abiertos por encima
# del 1023 y por tanto deberíass cerrar
#------------------------------------------------------------------------
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR $ROOT -l -j
DENY
/sbin/ipchains -A input -p udp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR $ROOT -l -j
DENY

/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR $NFS -j
DENY
/sbin/ipchains -A input -p udp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR $NFS -j
DENY

/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR
$OPENWINDOWS -j DENY
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR
$XWINDOWS -j DENY
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR $SSH -j
DENY
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR $IRCD -j
DENY

/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 3128 -j
DENY
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 3130 -j
DENY
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 8080 -j
DENY
```

```
/sbin/ipchains -A input -p tcp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 1024 -j
DENY
/sbin/ipchains -A input -p udp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 1024 -j
DENY
/sbin/ipchains -A input -p udp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 1026 -j
DENY
/sbin/ipchains -A input -p udp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 1119 -j
DENY
/sbin/ipchains -A input -p udp -i $PPP -s $TODAS $NO_ROOT -d $IPADDR 3401 -j
DENY

#---------------------------------------------
# Forward con enmascaramiento para la red local
#---------------------------------------------
/sbin/ipchains -A forward -s $LOCALNET  -j MASQ
```
[11]

3.4 CONFIGURANDO EL SOFWARE

Así que ahora tenemos un LINUX conectado a internet por una línea PPP. Además tenemos una red Ethernet que conecta el LINUX y el resto de las computadoras. Lo primero, debemos recopilar el núcleo con la opciones apropiadas.

Las opciones requeridas son:

- ✓ Habilitar el soporte de red
- ✓ Habilitar la opción de red TCP/IP (TCP/IP Networking)
- ✓ Deshabilitar el reenvió de paquetes IP (CONFI_IP_FORWARD)
- ✓ Habilitar la opción de cortafuegos IP (IP firewalling)
- ✓ Probablemente, habilitar las cuentas IP (IP Accounting)

[11] Scrip realizado por Santiago González Herrero, http://roble.pntic.mec.es/~sgonzale/linux/cortafuegos.html

- ✓ Parece razonable, dado que estamos configurando un dispositivo de seguridad
- ✓ Habilitar el soporte de dispositivos de red (Networking Decive Support)
- ✓ Habilitar el soporte de PPP y Ethernet, aun que esto depende del tipo de interfaces que se tenga en cada caso.

Ahora, recopilamos y reinstalamos el núcleo y reiniciamos la máquina. Las interfaces deberían ser reconocidas en la secuencia de arranque para que todo estuviera bien.

3.4.1 Las direcciones de red

Esta es la parte interesante. Dado que no queremos que la Internet tenga acceso a nuestras máquinas, no necesitamos usar direcciones reales. Una buena elección es el rango de direcciones de clase C 192.168.2.xxx, que está designado como rango para pruebas. Es decir, nadie lo usa, y no entrará en conflicto con ninguna petición al exterior. De modo que, en esta configuración, sólo se necesita una dirección IP real. Las otras se pueden elegir libremente y de ninguna manera afectara a la red.

Asignamos la dirección IP real al puerto serie de los cortafuegos que usamos para la conexión PPP. Asignamos 192.168.2.1 a la tarjeta Ethernet del cortafuegos. Asignamos a las otras máquinas de la red protegida cualquier dirección del rango anterior.

3.5 SEGURIDAD PARA EL CORTAFUEGOS

El cortafuegos no sirve si lo dejamos vulnerable a los ataques. Primero se debe revisar el fichero /etc/inetd.conf. Este es el fichero de configuración del así llamado superservidor, que arranca en buen número de demonios servidores cuando les llega una petición.

Entre ellos:

- ✓ Telnet
- ✓ Talk
- ✓ FTP
- ✓ Daytime

Se debe desactivar todo lo que no se necesite. No dudaremos en desactivar netstat, systat, FTP, bootp, y finger. Seguramente querremos desactivar telnet, y dejar sólo rlogin o viceversa.

Para desactivar un servicio basta con poner un # al comienzo de la línea que se refería a él. Después hay que mandar una señal SIG-HUP al proceso inetd tecleando “kill –HUP <pid>”, donde <pid> es el número de proceso de inetd. Esto hará que inetd relea su fichero de configuración (inetd.conf) y se reinicie. Lo comprobaremos haciendo un telnet al puerto 15 del cortafuego, el puerto de netstat. Si aparece la respuesta de netstatd, no hemos reiniciado inetd correctamente.

3.5.1 Ejemplo de programas con ipchains

El siguiente Script es apropiado para una puerta de enlace ejecutándose con 2 interfaces, que es por lo que se ha utilizado el objetivo DENY en lugar de REJECT, de modo que se descarte el paquete y no se responda de ninguna manera, lo cual alenta los escaneos de red (puesto que esperan el time out en lugar de escribir una respuesta) y revela menos información. También no se aconseja guardar logs de los datos, a menos que se disponga de la suficiente cantidad de espacio en disco duro, puesto que cada paquete que se envía se utilizan muchos bytes de disco duro para crear la entrada del log, siendo fácil saturar el syslog y/o el disco duro en una conexión rápida.

```
#!/bin/bash
   #
   # Este script configura las reglas apropiadas de un cortafuegos para un
   # Servidor con 2 interfaces ejecutándose como puerta de enlace.
   #
   # Si se planea utilizarlo, es necesario editar este script.
   #
   # Se supone que las máquinas internas hacen todas una llamada a la puerta
   # de enlace, de modo que las reglas no bloquean el tráfico interno.
   #
   # Un par de variables
   #
   # ETH0IP es la dirección IP de ETH0 (el interfaz externo)
   # ETH0NET es la red
   # ETH0NETMASK es la máscara de red
   # HOSTFIABLE1 es un host fiable (para administración de web/ssh)
   # HOSTFIABLE2 es un host fiable (para administración de web/ssh)
   # ETH1IP es la dirección IP de ETH1 (el interfaz interno)
   # ETH1NET es la red
   # ETH1NETMASK es la máscara de red
   #
   ETH0IP=1.1.1.1
```

```
ETH0NET=1.1.1.0

ETH0NETMASK=24

HOSTFIABLE1=1.5.1.1

HOSTFIABLE2=1.5.1.2

ETH1IP=10.0.0.1

ETH1NET=10.0.0.0

ETH1NETMASK=24

#

PATH=/sbin

# LIMPIAR TODAS LAS REGLAS

ipchains -F input

ipchains -F output

ipchains -F forward

# ANTI-SPOOFING

ipchains -A input -p all -j DENY -s 10.0.0.0/8 -i eth0 -d 0.0.0.0/0

ipchains -A input -p all -j DENY -s 127.0.0.0/8 -i eth0 -d 0.0.0.0/0

ipchains -A input -p all -j DENY -s 192.168.0.0/16 -i eth0 -d 0.0.0.0/0

ipchains -A input -p all -j DENY -s 172.16.0.0/16 -i eth0 -d 0.0.0.0/0

ipchains -A input -p all -j DENY -s $ETH0IP -i eth0 -d 0.0.0.0/0

# PRIMERO ICMP

ipchains -A input -p icmp -j ACCEPT -s $ETH0NET/$ETH0NETMASK -i eth0 -d
0.0.0.0/0
```

```
ipchains -A input -p icmp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0

# SSH

ipchains -A input -p tcp -j ACCEPT -s $HOSTFIABLE1 -i eth0 -d 0.0.0.0/0 22

ipchains -A input -p tcp -j ACCEPT -s $HOSTFIABLE2 -i eth0 -d 0.0.0.0/0 22

# BLOQUEO 1:1023

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 1:1023

ipchains -A input -p udp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 1:1023

# BLOQUEO DE OTRAS COSAS

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 1109

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 1524

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 1600

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 2003

ipchains -A input -p udp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 2049

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 2105

ipchains -A input -p udp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 3001

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 3001

ipchains -A input -p udp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 3128:3130

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 3128:3130

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 3306

ipchains -A input -p udp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 3306

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 4444

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 6000:6100
```

```
ipchains -A input -p udp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 6000:6100

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 6667

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 7000

# ADMINISTRACIÓN DE WEB

ipchains -A input -p tcp -j ACCEPT -s $HOSTFIABLE1 -i eth0 -d 0.0.0.0/0 10000

ipchains -A input -p tcp -j ACCEPT -s $HOSTFIABLE2 -i eth0 -d 0.0.0.0/0 10000

ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 10000

# REGLAS DE REDIRECCIONAMIENTO

ipchains -P forward DENY

ipchains -A forward -p all -j MASQ -s $ETH1NET/$ETH1NETMASK -d 0.0.0.0/0
```
[12]

3.6 SOFTWARE PARA CORTAFUEGOS

3.6.1 Paquetes disponibles

Un cortafuegos en sentido estricto no necesita ningún software aparte del núcleo de LINUX y los programas básicos de red (inetd, telnetd y telnet, FTDP y FTP). Pero un cortafuegos así es extremadamente restrictivo y no muy útil.

Así que la gente ha hecho programas para aumentar la utilidad de los cortafuegos. El que examinaremos con mayor detalle es un paquete llamado “Socks”, que implementa un servidor proxy. Sin embargo, existe otro par de programas que hay que tomar en consideración.

---

[12] Script realizado por José Antonio Revilla http://gluv.univalle.edu.co/gsal/cortafuegos.htm

3.6.2 El juego de herramientas de TIS

TIS ha sacado una colección de programas para facilitar la realización de cortafuegos. Básicamente, los programas hacen lo mismo que el paquete Socks, pero tiene una estrategia de diseño diferente. Mientras que Socks tiene un único programa que cubre todas las operaciones del internet, TIS provee un programa para cada utilidad que quiera usar el cortafuegos.

Para compararlos mejor, veamos el ejemplo del acceso al web y por Telnet. Con socks, hay que hacer un fichero de configuración y poner en marcha un programa. Mediante ese fichero y ese programa se activan tanto el Telnet como el Web, así como cualquier otro servicio que no se haya desactivado.

Con las herramientas TIS, se arranca un programa para el Web y otro para el Telnet, y se escribe un fichero de configuración para cada uno. Después de haber hecho eso, el resto de formas de acceso a Internet siguen prohibidas hasta que se configuren. Si no existe un programa especial para una determinada utilidad (por ejemplo, para talk), hay un programa para todo pero no es ni tan flexible, ni tan fácil de configurar como las otras herramientas.

Esto puede parecer una diferencia menor, pero en realidad es una gran diferencia. Socks permite ser desidioso. Con un servidor de Socks mal configurado la gente de dentro tiene más acceso al Internet del que se quería. Con las herramientas TIS, la gente del interior tiene solamente el acceso que el administrador del sistema quiere que tengan.

- ✓ Socks es más fácil de configurar, más fácil de compilar, y permite una mayor flexibilidad.
- ✓ El juego de herramientas de TIS es más seguro si se quiere controlar a los usuarios de dentro

Los dos proporcionan una protección absoluta del exterior.

3.6.3 El Limitador de TCP (TCP Wrapper)

El Limitador de TCP no es una utilidad de cortafuegos, pero sirve para algo parecido. Usando el limitador de TCP podemos controlar quién tiene acceso a nuestra máquina y a qué servicios, así como registrar las conexiones. También ofrece detección de impostores.

El limitador de TCP no se cubre de manera más extensa aquí por un par de razones:

- ✓ No es un verdadero cortafuegos.
- ✓ Para utilizarlo se tiene que estar directamente conectado a la Internet, es decir, se tiene que tener una dirección IP.
- ✓ Sólo controla la máquina en la que está instalado, y por lo tanto no sirve para una red.
- ✓ Los cortafuegos pueden proteger todas las máquinas, cualquiera que sea su arquitectura.

3.6.4 Algunos paquetes cortafuegos que existen en el mercado:

Ipf

El IPF es un paquete de cortafuegos alternativo, disponible para LINUX (y la mayoría de sistemas operativos). Se puede conseguir en http://cheops.anu.edu.au/

Sinus FIREWALL

El SINUS FIREWALL es un cortafuegos alternativo para LINUX (Kernel 2.0.x and 2.2.x). se puede conseguir en: http://WWW.sinusfirewall.org/.

Phoenix Adaptive FIREWALL

Reemplaza Ipchains completamente y añade un montón de inteligencia al proceso de filtrado. Sin embargo, es un producto comercial (sobre los 3000 US), y es el primer cortafuegos para LINUX en estar certificados por la ICSA. Está disponible en: http://www.progresive-systems.com/produts/phoenix/

Creación de Reglas

Un simple Script que convierte las reglas de Ipfwadm a Ipchains, haciendo más fácil la migración.

El script se encuentra disponible en la siguiente dirección: http://users.dhp.com/ whisper/Ipfwadm2Ipchains/

Mason

Mason es un generador automático de reglas para Ipfwadm e Ipchains. Se encarga y monitoriza el flujo de paquetes a través de la máquina, y después, basándose en eso, crea un conjunto de reglas para permitir ese tipo de actividad (por ejemplo; si se hace un FTP al servidor desde un sitio remoto, permitirá ese tipo de acceso en las reglas que crea).

Es una buena herramienta para administradores de cortafuegos novatos, disponible en: http://devplanet.fastethernet.net/Utilities/

MkLINUXfw

MkLINUXfw es una herramienta dirigida a proporcionar una variedad de interfaces para la creación de reglas de cortafuegos. Actualmente soporta interfaz CGI y está en progreso el GTK.

Se puede descargar de:

http://www.madhouse.org.uk/red/framepage.phtml?/mkLINUXfw/index.html

kfirewall

kfirewall es una aplicación basada en GUI para la creación de reglas Ipfwadm o Ipchains. Se puede conseguir en: http://megaman.ypsilonia.net/kfirewall/

fwconfig

fwconfin es una herramienta interesante para configurar Ipfwadm e Ipachains, basada en WWW.

Se puede conseguir desde:

http://www.mindstorm.com/sparlin/fwconfig.shtml

XIpfwadm

XIpfwadm es una aplicación que simplifica la creación de reglas Ipfwadm. Se puede conseguir en:

http://www.x25.org/xIpfwadm.htlm

FIREWALL Manager

FIREWALL Manager es una aplicación orientada a ser ejecutada desde X-Window que proporciona un GUI para gestión de cortafuegos.

Se puede descargar desde: http://www.tectrip.net/arg/

LINUX FIREWALL Tools

Un sitio interesante, tiene un cgi online para crear Scripts de cortafuegos.

Se puede ver en: http://www.LINUX-firewall-tools.com

FCT - Firewall Configuration Tool

Una de las herramientas de configuración online mediante cgi más avanzadas.

Se puede probar en:

http://www.fen.baynet.de/ ft114/FCT/index.htm

DNi

DNi es un cgi online que te ayuda a crear reglas de cortafuegos para Ipfwadm.

Se puede probar en: http://members.tripod.com/robel/dni/

Finalmente, se puede decir que, al hablar de un FIREWALL en Linux, es hablar de un software gratuito, ya que para hacer funcionar un FIREWALL en Linux se deben desarrollar Script. Un script no es más que un programa desarrollado por los administradores de red o por especialistas en el desarrollo o por cualquier persona con conocimientos en este paquete; cada script se debe desarrollar de acuerdo a las necesidades del sistema con el que se cuenta y con los objetivos que se desean, ya que se deben declarar reglas y pasos que permiten denegar o permitir accesos a los usuarios de la red para un mejor manejo y seguridad de la información y cerrando aquellos puertos que permiten el tráfico de paquetes maliciosos que no sólo perjudican a una computadora sino a toda la red.

CAPÍTULO 4

FIREWALL EN WINDOWS

OBJETIVO: Conocer los cortafuegos (FIREWALL) que existen para el ambiente Windows, además de cómo funcionan en el propio Windows.

4.1 COMO ADMINISTRAR LA SEGURIDAD WINDOWS NT

Requiere la comprobación de usuario y contraseña para iniciar sesión.

Mediante la herramienta de Administrador de usuarios es posible:

- ✓ Crear, modificar y borrar grupos tanto locales como globales.
- ✓ Crear, modificar y borrar cuentas de usuarios.
- ✓ Definir política de cuentas.
- ✓ Establecer los derechos de acceso a los recursos de cada usuario o grupo.
- ✓ Definir los parámetros referidos a usuarios que se van a auditar.
- ✓ Definir relaciones de confianza entre dominios.

Grupo: Conjunto de usuarios con una serie de características comunes.

Windows NT distingue entre dos tipos de grupos:

- ✓ **Grupos Globales**: Contienen cuentas de usuario del dominio donde se creó dicho grupo. A un grupo global se le pueden dar derechos sobre su propio dominio, sobre las estaciones de trabajo del dominio, sobre servidores miembro o sobre dominios que confían. Los grupos globales se pueden agregar a grupos locales.
- ✓ **Grupos Locales**: Contienen cuentas de usuario y cuentas de grupo globales de uno o más dominios, agrupados bajo un nombre de la cuenta de grupo. Los usuarios y grupos globales de otro dominio se pueden incorporar aun grupo local siempre y cuando pertenezcan a un dominio que confía. Un grupo local no puede contener otros grupos locales.

Por defecto, Windows NT crea una serie de grupos locales cuando se instala.

Grupo de Administradores (para cualquier tipo de servidor): Posee la mayoría o todos los derechos, para crear parámetros en el servidor.

Operadores de Servicios (sólo controladores de dominio): Poseen derechos para administrar en servidor de dominio. Pueden arrancar copias de seguridad, administrar usuarios y grupos, y compartir y bloquear recursos del servidor.

Usuarios Avanzados (sólo para servidores que no sean controladores de dominio y estaciones de trabajo): Usuarios para administrar cuentas en la propia máquina.

Operadores de cuentas (sólo controladores de dominio): Son los encargados de administrar las cuentas de usuario, a excepción de las cuentas de administración, en las cuales no tienen permiso de gestión.

Operadores de impresión (sólo controladores de dominio): Responsables de todos los temas de impresión en el servidor, gestionan los trabajos de impresión y los derechos de acceso.

Operadores de seguridad (para cualquier tipo de servidor): Gestionan las copias de seguridad y la recuperación de archivos.

Replicadores (para cualquier tipo de servidor): Encargados de administrar y gestionar la replicación de directorios entre distintos servidores.

Usuarios (para cualquier tipo de servidor): Sólo tienen derecho a iniciar sesión en el servidor. En este grupo se incluyen por defecto todos los usuarios que se creen.

Invitados (para cualquier tipo de servidor): Se creó con la finalidad de permitir a cualquier usuario que se conecte al servidor. Como su nombre indica, invitados, y por lo tanto, su actividad está muy limitada.

Grupos especiales

Todos (para cualquier tipo de servidor): Están todos los usuarios que se pueden conectar al dominio, tanto locales como remotos.

Interactivos: Cualquiera que utilice el equipo localmente.

Red: Todos los usuarios conectados al equipo a través de la red.

Sistema: Sistema operativo

Creador Propietario: Transferencia de permisos a los creadores de subdirectorios, archivos y trabajos de impresión.

Usuarios Autentificados: Este grupo se crea una vez que se instala el service pack. Es un grupo similar al grupo “todos” pero con la diferencia que no incluye usuarios anónimos.

4.2 TIENE PROTECCIÓN DE LOS OBJETOS COMUNES EN EL SISTEMA

EN Windows NT existen varios tipos de objetos como por ejemplo: procesos, subprocesos, archivos, servicios. Todos los recursos del sistema operativo se muestran a las aplicaciones como objetos.

Para poder proteger dichos objetos, NT comprueba los privilegios que tiene cada usuario para acceder a dichos recursos. Dependiendo del objeto tendremos un tipo de permisos o privilegios. No son iguales los permisos para acceder a un archivo o directorio que para el acceso a un puerto de comunicaciones o a una impresora.

Los principales objetos que son susceptibles de establecer algún tipo de protección sobre ellos son los siguientes:

- ✓ Procesos y subprocesos
- ✓ Archivos y directorios
- ✓ Servicios
- ✓ Impresoras
- ✓ Particiones de disco
- ✓ Las claves del registro
- ✓ Los buzones de correo
- ✓ Escritorios
- ✓ Testigos de acceso
- ✓ Sockets y semáforos
- ✓ Temporizadores y dispositivos

4.3 ¿TIENE AUDITORIA DE SEGURIDAD?

El sistema de seguridad NT tiene la capacidad de generar una serie de sucesos de auditoría. Estos sucesos permiten controlar quién ha intentado un acceso a un objeto y el tipo de operaciones que se han llevado a cabo con dicho objeto.

El sistema de auditoría recoge todos esos sucesos para que el administrador pueda verlos y detecte algún fallo de seguridad, como por ejemplo:

- ✓ Un número excesivo de intentos de conexión fallidos sobre una cuenta.
- ✓ Intentos de utilización de servicios a los que no se tiene acceso.
- ✓ La conexión al sistema a horas inusuales.
- ✓ El acceso a determinados archivos confidenciales.

4.4 BUGS EN WINDOWS NT Y RECOMENDACIONES

La cuenta de Invitado

Siempre se debe bloquear la cuenta de invitados en servidores que deben un nivel de seguridad importante. Además es recomendable renombrar la cuenta de invitado a pesar de bloquearla.

La cuenta de Usuario Anónimo

En WINDOWS la cuenta de usuario Anónimo, por defecto, tiene acceso a algunas operaciones que pueden ser de mucha utilidad para un HACKER, ya que esta cuenta no requiere ningún tipo de identificación.

Para impedir el acceso anónimo a un servidor es necesario modificar el siguiente valor de Registro (observar la tabla 4.1).

Tabla 4.1 Valor de Registro

Árbol	HKEY_LOCAL_MACHINE
Situación	\system\CurrentControlSet\Control\LSA
Nombre	\RestrictAnonymous
Tipo	REG_DWORD
Acción	Poner a 1

El servidor Scheduler

Este servicio permite el arranque automático de procesos a través del comando at.exe. El problema esta que el servicio scheduler se ejecuta con la cuenta del sistema, luego, tiene poder ilimitado. Un usuario malicioso podría ponerse a ejecutar un programa que tendría acceso a cualquier recurso. Para evitar este problema hay dos soluciones: la primera consiste en dar permisos al comando at, de manera que sólo sea ejecutado por el servidor; la otra opción consiste en arrancar el servicio de scheduler con un usuario distinto.

El bug Getadmin

Circula por Internet una utilidad denominada GETADMIN.EXE que permite a un usuario sin privilegios, obtener derechos administrativos introduciéndolo en el grupo de administradores. Esta utilidad puede ser ejecutada desde el contexto de un usuario normal, excepto desde la cuenta de invitados.

Posterior al Service Pack 3 se ha diseñado un parche para fijar este problema.

Desencriptación de contraseñas

- ✓ PWDUMP.EXE: Utilidad que accede a la base de datos (contraseña LAN manager y contraseña NT) y desencripta su contenido.

- ✓ NTCRACK.EXE: Utilidad que permite realizar ataques de diccionario.
- ✓ LOPHTCRACK.EXE: Utilidad que permite realizar ataques de fuerza bruta y de diccionario.

Para impedir el acceso a la base de datos desde la red.

- ✓ Añadir el valor de la clave winreg(Ver tabla 4.2).

Tabla 4.2 Claves Winreg

Árbol	HKEY_LOCAL_MACHINE
Situación	\system\CurrentControlSet\Control\SecurePipeSer
Nombre	\winreg
Tipo	REG_DWORD
Acción	Poner a 1

- ✓ Instalar el match Im-fix de Microsoft
- ✓ Realizar la encriptación de la base de datos.

4.5 SERVICIO NETBIOS EN ENTORNOS DE RED NO SEGUROS

El sistema de comparación de impresoras, archivos, carpetas y unidades se basa en los protocolos:

- ✓ NETBIOS (Network Basic Input/Output System) desarrollado por IBM
- ✓ NETBEUI (NetBIOS Extended User Interface) desarrollado por Microsoft
- ✓ SMB (Server Message Block) Protocolo que se utiliza para acceder a recursos compartidos, desarrollado por Pathworks de DEC.

Compartir recursos en Windows, sobre todo unidades o directorios es un tema delicado en temas de seguridad, ya que suministra a usuarios remotos la posibilidad de acceder al servidor, es decir, si ese servidor está conectado a Internet, da la posibilidad de acceso a un hacker desde Internet a los recursos internos.

Para evitar el acceso a recursos compartidos desde Internet habría que deshabilitar los servicios de Workstation, Server y el protocolo NETBIOS del servidor. El problema es que desactivando estos servicios nadie tendría acceso a esos recursos, ni desde Internet ni desde la red interna.

La recomendación es evitar en todo lo posible la utilización de recursos compartidos en computadoras que tengan acceso desde Internet. De esta manera se evita cualquier tipo de filtración desde Internet.

La compartición de recursos es útil y más recomendable en redes internas, donde el acceso siempre esté más controlado y sea por usuarios de la propia empresa.

4.6 SOLUCIÓN MEDIANTE UN FIREWALL

El protocolo NETBIOS utiliza tres puertos para comunicarse: 137,138 y 139(ver tabla 4.3).

Tabla 4.3 Puertos

Nombre Asociado	Puerto	protocolo	Descripción
Netbios-ns	137	TCP	NETBIOS name service
Netbios-ns	137	UDP	NETBIOS name service
Netbios-dgm	138	TCP	NETBIOS datagram service
Netbios-dgm	138	UDP	NETBIOS datagram service
Netbios-ssn	139	TCP	NETBIOS sessión service

Netbios-ssn	139	UDP	NETBIOS sesión service

Para impedir el acceso a través de Internet a esos puertos del servidor, lo mejor es tener instalado un FIREWALL que compruebe cada paquete TCP/IP de entrada y deshabilite todos aquellos cuyo puerto de origen estén en ese rango.

4.7 ALGUNOS PAQUETES FIREWALL'S QUE EXISTEN EN EL MERCADO

A continuación se muestran algunos paquetes de FIREWALL que existen en el mercado para manejar la seguridad y cerrar los puertos que tenemos abiertos.

KERIO WIN ROUTE FIREWALL

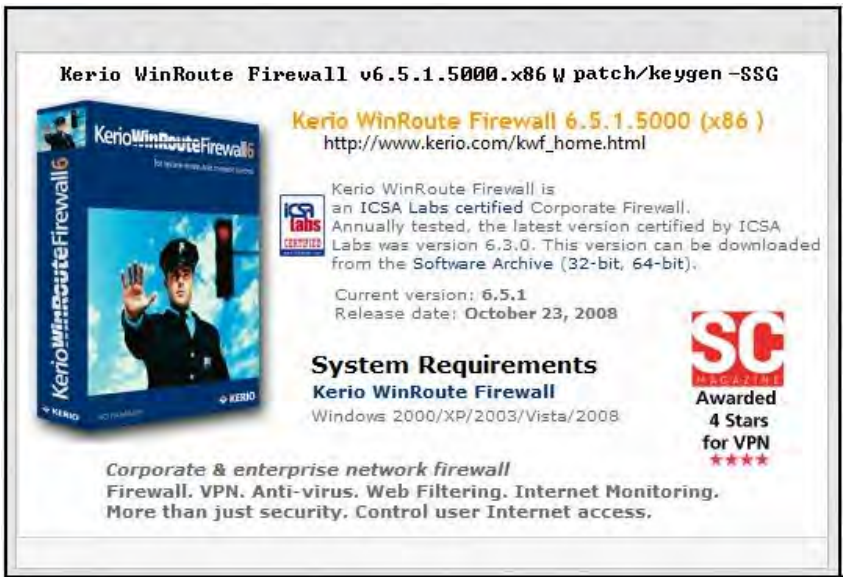


Figura 4.7.1

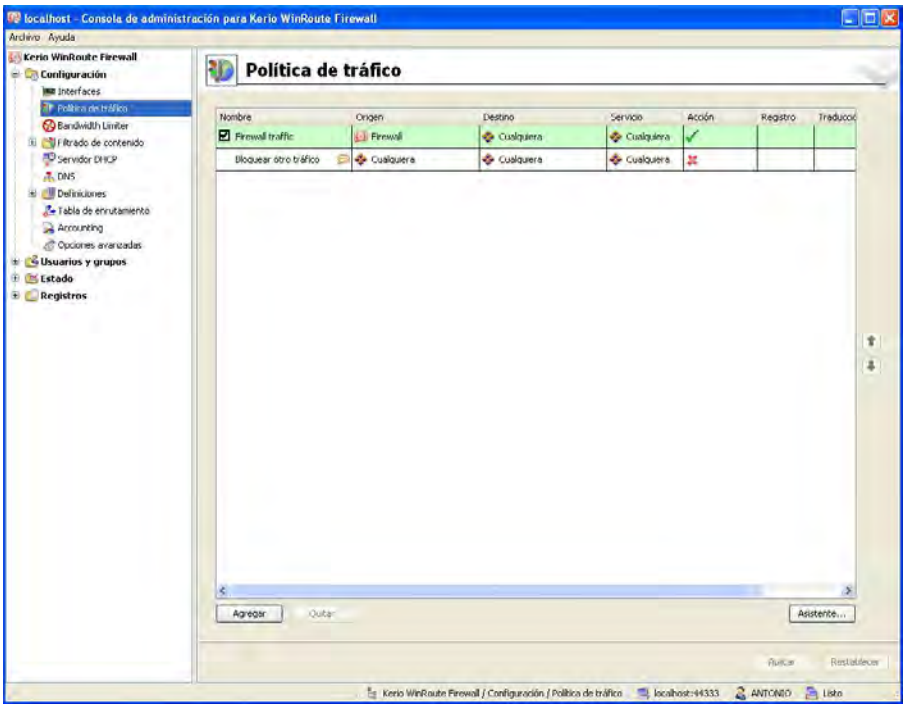


Figura 4.7.2 [13]

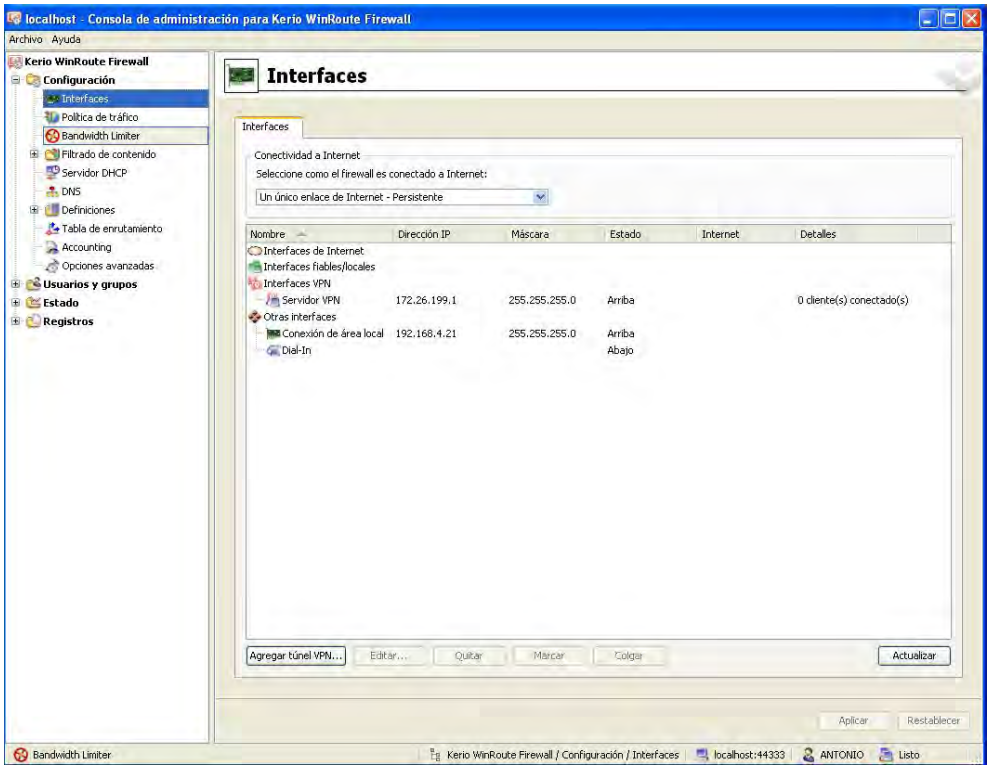


Figura 4.7.3 [14]

[13] Imagen del programa Kerio Win Route

[14] Imagen del programa Kerio Win Route

Si bien estrictamente no es un cortafuego, sino un servidor proxy que permite que otras computadoras se conecten a INTERNET a través de un host, incluye indirectamente un cortafuegos que cierra todos los puertos a Internet (a menos que se le diga lo contrario), y permite conexiones de la red interna, pudiendo filtrar las conexiones de origen y de destino, tanto entrantes como salientes.

Por supuesto, se le puede y se debe proteger con contraseña, permite administración remota, y se le puede y se debe cambiarle el puerto por defecto, por las mismas razones de seguridad.

No consume muchos recursos del sistema, y como proxy, no es necesaria la instalación de software alguno en las computadoras que accederán a Internet a través del nuestro.

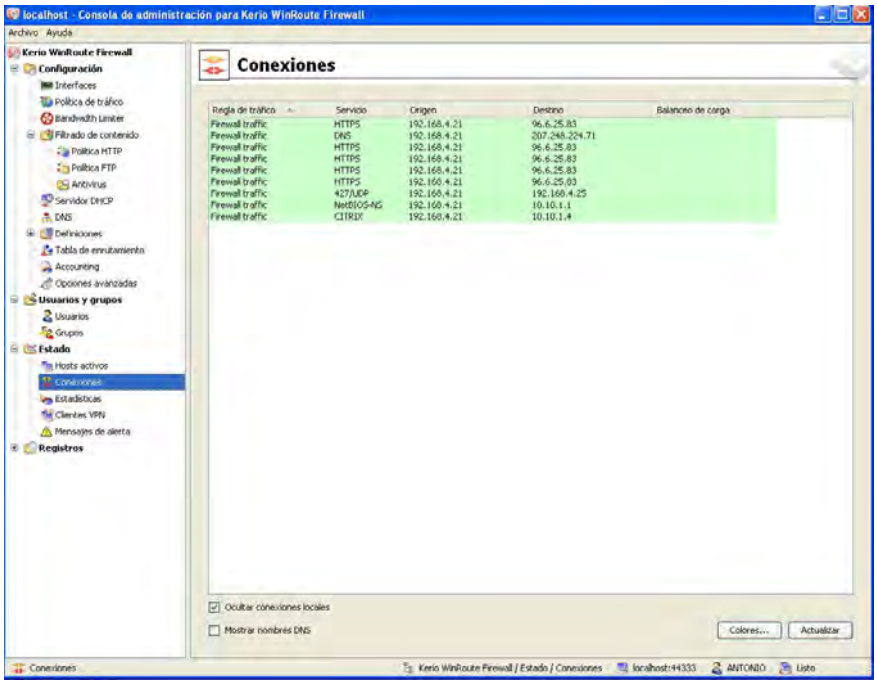


Figura 4.7.4 [15]

Tal y como se instala, no hace falta hacer nada para tener la computadora inmediatamente protegida y todos los puertos en modo

[15] Imagen del programa Kerio Win Route

invisible salvo que se le llegara a realizar un ataque con otro WinRouter, pero no esté diseñado ni preparado para ello.

Este programa FIREWALL se puede conseguir en

http://www.Kerio.com/Kwf_download.html.

Recomendado

TINY FIREWALL

Figura 4.7.5

Al reiniciar la computadora después de instalarlo, se mete él solito en el registro, como si fuera un servicio. Ideal, porque con eso carga incluso antes de que acceda al sistema. No obstante, permite la ejecución de forma manual.

La configuración por defecto, es un nivel medio de seguridad, con lo que pone todos los puertos en modo invisible, y resiste todos los ataques que le hacen desde Internet y desde la red local. Además permite seguir trabajando con la red local.

Puede ser configurado mediante contraseña, y permite la administración remota, incluso para los logs y estadísticas. Consume poco recursos del sistema.

Parece muy simple en comparación con otros, y lo es. Lo que se le tiene que pedir a un cortafuegos es precisamente eso: facilidad de uso y efectividad ocultándonos en la red. Este producto lo cumple muy bien.

Este programa FIREWALL se puede conseguir en

http://www.tinysoftware.com/home/tiny2?s=5107951253794215827A3&pg=solo_download

Recomendado

TERMINET FIREWALL

Al instalarlo, realiza una pregunta de que si queremos que los puertos pasen a modo invisible. Un buen detalle. Después de reiniciar el equipo, además muestra un recordatorio durante 30 días para registrarlo o comprar el paquete.

Según las herramientas de ataque, con unas aparecen todos los puertos en modo invisible, y con otras, aparecen todos los puertos cerrados, excepto el 139-NETBIOS, que aparece abierto.

Atacando desde la red local, sucede lo mismo, todo en modo invisible, pero permite continuar trabajando normalmente.

Sin embargo, cualquier troyano que se tenga o contagie, podría conectarse tranquilamente con su autor para pedir instrucciones.

Durante los ataques, el cortafuegos no molesta. Se puede continuar trabajando, jugando o chateando, sin recibir los molestos informes de otros cortafuegos advirtiendo de tal o cual amenaza, salvo que vía web por el puerto 80, se encontrara con páginas maliciosas que intenten hacer otra cosa, en cuyo caso se informa de los motivos por los que no se muestra la página.

La primera vez que se ingresa al cortafuegos, se le proporciona una contraseña de al menos 6 caracteres, y a partir de aquí, siempre se le habrá de indicar.

Respecto a la configuración por defecto, no es necesario modificarla para estar protegidos, pero si se desea se le pueden definir reglas normalmente o avanzadas por URL, direcciones IP, puertos, horas, días, visualizar el tráfico, crear listas negras y listas blancas de direcciones web, y perfiles individuales o de grupos.

La ayuda es muy completa, e incluso se dispone de un manual en formato pdf. Desinstalarlo ya es otra cosa, pues no aparece en “agregar o quitar programas” del panel de control, ni tiene ningún desinstalador en su directorio, por lo que se deberá de usar el mismo archivo de instalación para desinstalarlo.

Este programa FIREWALL se puede conseguir en http://www.danu.ie/main.htm

Es un cortafuego muy bueno y muy fácil de utilizar

SYGATE FIREWALL

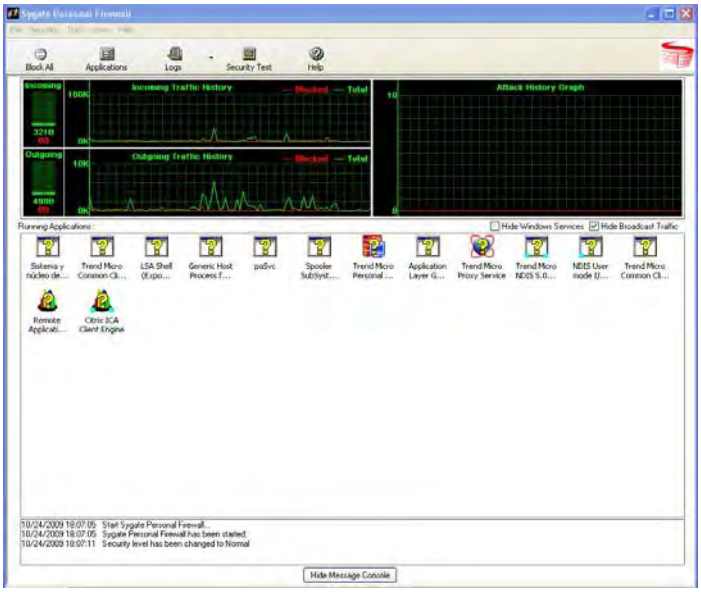


Figura 4.7.6 [16]

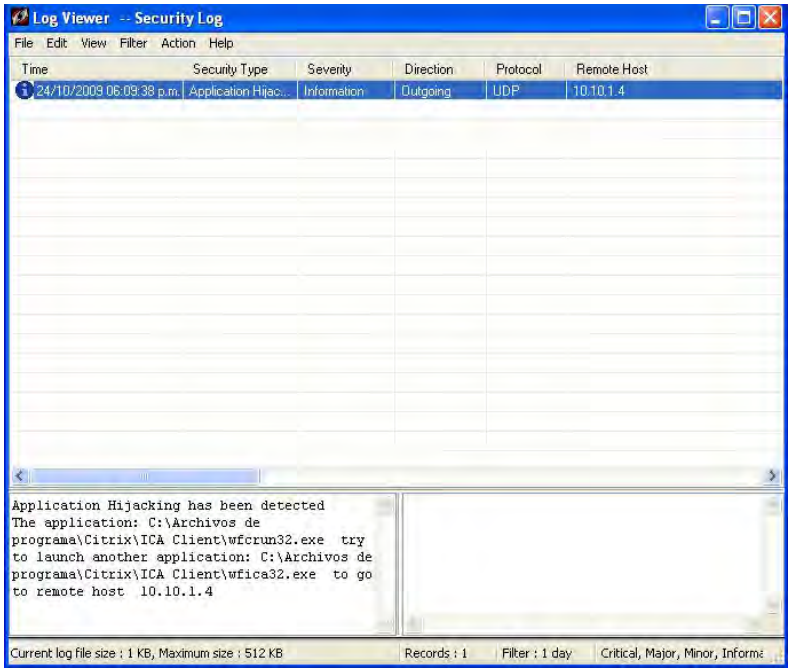


Figura 4.7.7

[16] Imagen del programa Sygate

Este cortafuegos por defecto viene configurando con un nivel de seguridad alto. En este nivel, tanto en ataques a través de Internet como en ataques en red local, el cortafuegos no es gran cosa. No se recomienda poner en nivel medio, o en nivel bajo.

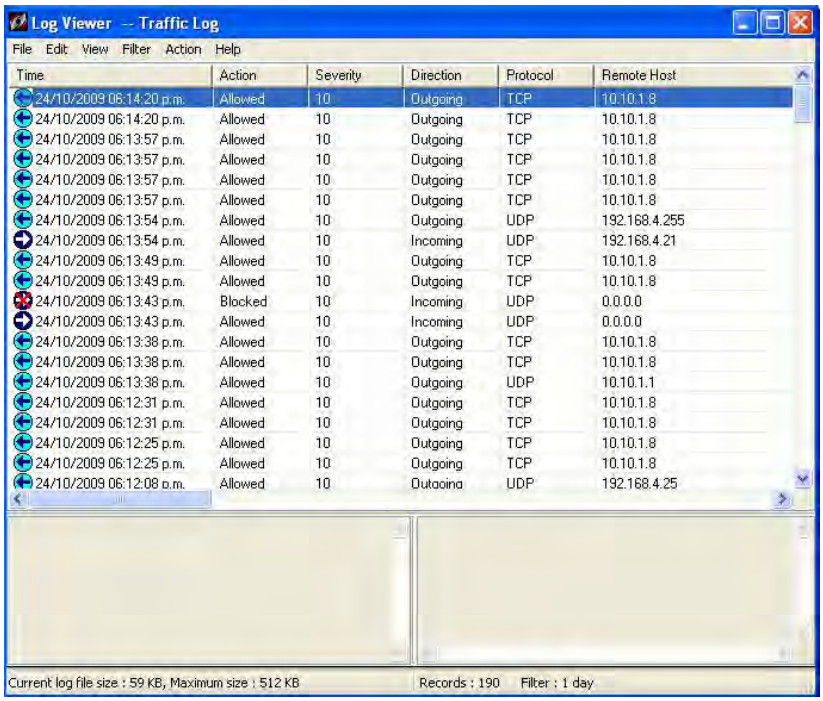


Figura 4.7.8 [17]

Se recomienda poner en nivel ULTRA y se consigue únicamente que pase el puerto 80 de cerrado a invisible.

Sin embargo, si se cuenta con un poquito de experiencia, se pueden hacer un montón de cosas con este producto, como permitir acceso a alguna PC, a redes privadas virtuales, a determinadas IP, enviar un correo electrónico en caso de ataque, 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 salva pantallas.

Los logs de actividad brillan por su ausencia y la ayuda remite a su web, donde se recomienda su producto.

Este cortafuegos no es muy seguro.

[17] Imagen del programa Sygate

AT GUARD

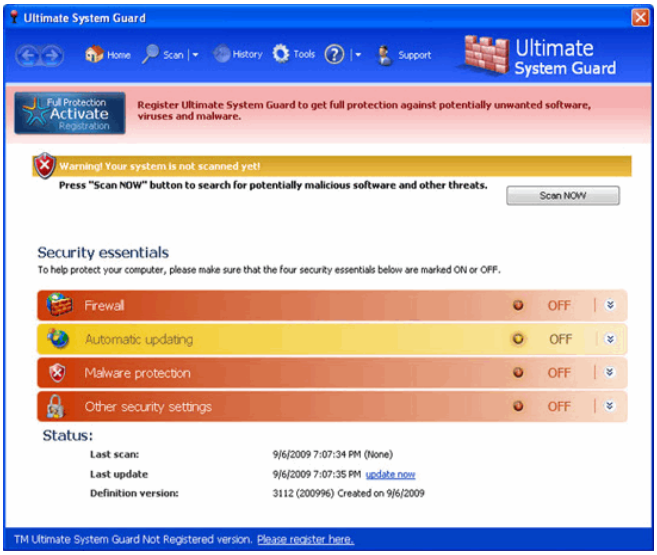


Figura 4.7.9

Lo primero que llama la atención es la rapidez y la sensación de que se tiene el control de cuanto esta sucediendo.

Bloquea la publicidad no deseada, con un especial énfasis en toda la que comienza por http://ad, lleva un log de fecha, hora, URL, IP, bytes enviados y recibidos, y tiempo de todas las conexiones web y de red local, así como la 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.

Junto a Norton Personal FIREWALL, Sygate, Tyny y ZoneAlarm, es de los pocos consistentes en la simulación de lo que haría un troyano o en programa espía, al conectarse saltándose el cortafuegos, a un servidor FTP. No obstante, no supera los ataques simulados vía web ni red local, y consume demasiados recursos del sistema, en comparación con otros cortafuegos. Tampoco llega a la facilidad de uso de ZoneAlarm.

La definición de reglas de seguridad es bastante compleja, aun usando el asistente, y no se llega a tener claro que es lo que está autorizando o bloqueando, lo cual, para alguien que se inicia en este mundo de la seguridad, no es la opción más 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 muy buena cualquier pregunta que pudiera surgir, ellos ya han pensado en ella.

Para un acceso rápido a todas las funciones del cortafuegos, está la función “dasboard”, que muestra una barra de acceso directo a las más importantes funciones del mismo. Esta barra, por defecto aparece en la parte superior de la pantalla, pero basta con arrastrarla para ponerla donde menos estorbe, o incluso ocultarla.

BLACK ICE

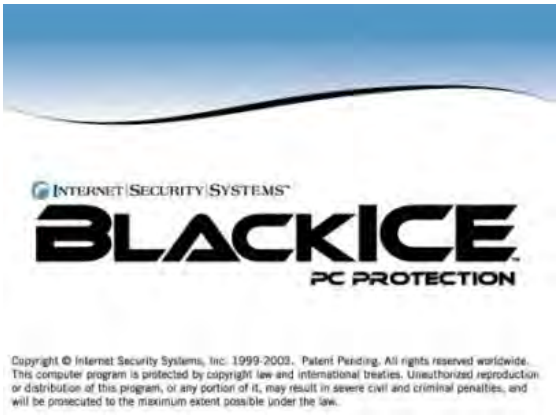


Figura 4.7.10

Es muy bueno, y él único defecto que puede tener es que deja el puerto 113 abierto, cuando lo correcto sería que estuviese invisible.

Tiene, como casi todos, la posibilidad de varios niveles de protección y cuando es escaneado, avisa mediante un sonido y un icono parpadeante.

Ofrece una gran cantidad de información sobre los atacantes, casi tanta como HackTracer, y unas estadísticas muy conseguidas de los ataques, detalladas por horas, días y meses.

Ventajas sobre algunos programas: Detecta ataques fragmentados, escaneos, y se accede ON LINE a páginas actualizadas

donde se informa de los ataques recibidos. Además de proteger nuestra computadora de ataques externos, protege a las demás computadoras de ataques desde el que se tiene, para lo cual canaliza todo tipo de actividad en la computadora.

Al igual que HackTracer, analiza a los atacantes tratando de conseguir el máximo de información de ellos, tales como su IP, grupo de trabajo, y guarda pruebas de los ataques por si fuera necesario demostrar su ocurrencia.

El consumo de recursos del sistema es prácticamente despreciables, es muy fácil de configurar tanto los permisos como las restricciones de acceso.

Permite trabajar con recursos compartidos, y es recomendable configurarlo en modo recomendado por el fabricante, pues hace tiempo se reporto un fallo de seguridad que decían que lo hace vulnerable al Back orífice.

En cualquier caso, lo recomendable es hacerle caso al fabricante y configurarlo en modo paranoico.

CONSEAL PC

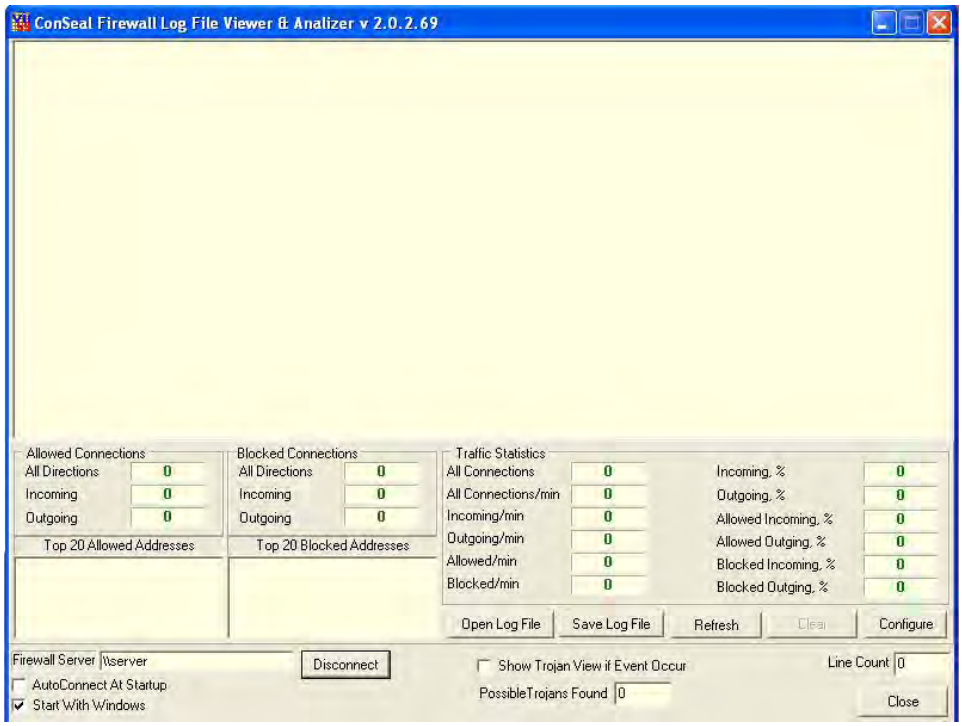


Figura 4.7.11 [18]

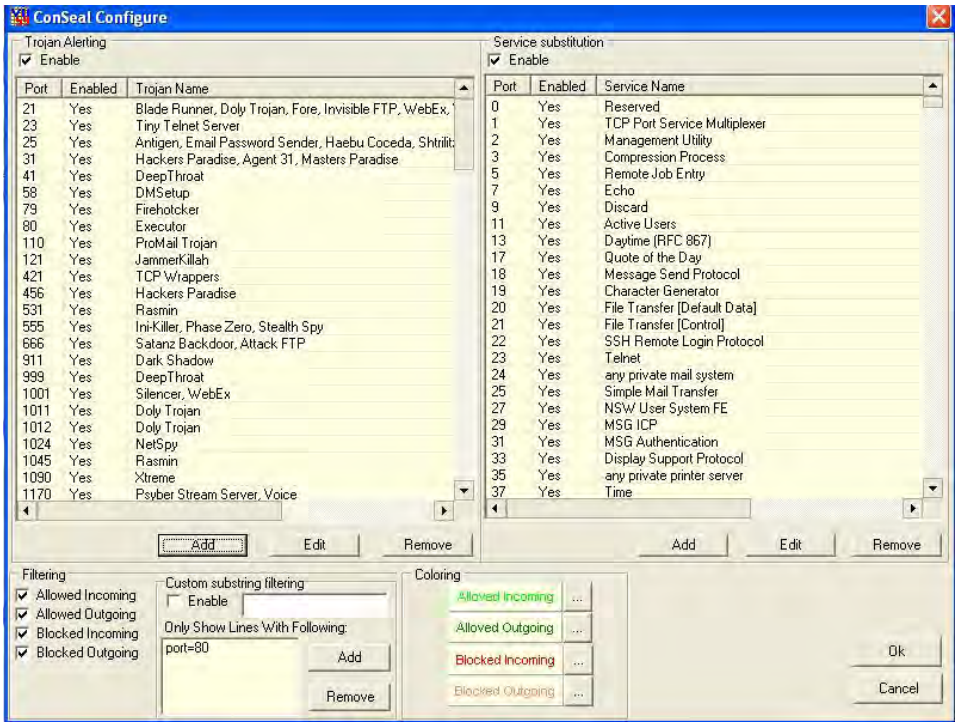


Figura 4.7.12

[18] Imagen del programa Conseal

Al instalarse, copia varios ficheros antiguos, pero Windows advierte, y se restauran las versiones antiguas que ha copiado Conseal, por las más recientes que se tengan instaladas en la computadora.

Atacado desde Internet, todos los puertos aparecen por defecto en modo invisible, a excepción del puerto 113. Mismos resultados para un ataque desde red local. En cada uno de los ataques, un cuadro de diálogo informa de la IP del atacante o computadora que quiere conectar con la computadora que se está utilizando, con indicación del puerto y el nombre del servicio, dando la opción de permitirlo, bloquearlo, ignorarlo, permitirlo o bloquearlo solo durante esta sesión (por si se quisiera que alguien más con IP dinámica se conecte a la computadora), mostrar los detalles del ataque y explicar los riesgos. Todo esto lo hace por defecto, sin que se tenga que preocupar en configurar nada.

Si se le hace clic con el botón derecho sobre cualquiera de los ataques, dice a qué dominio pertenece el atacante, intruso o servicio que quiera conectarse a la computadora que se utiliza.

Recomendado

ESAFE DESKTOP

Este cortafuegos incluye un antivirus, por lo que no se tiene que complementar al sistema defensivo con otro producto, todo ello en una perfecta construcción teórica que no sirve para nada.

No reconoce bastantes virus y además, como casi todos los antivirus, impide que tenga otro instalado, por lo que la solución que se puede tomar es la instalación de otro antivirus en otra

computadora de la red, que escanee toda la red, ya que si no se tiene instalado otro antivirus se corre el riego de recibir muchos virus, no solicitados, pasando todos tranquilamente por el antivirus de Esafe, sin que éste diga lo que está ocurriendo.

Otro inconveniente es si se instala sin haber desinstalado previamente el antivirus, la computadora se reiniciará continuamente, hasta que se decida arrancar en modo a prueba de fallos, y se desinstale el anterior antivirus.

Ventajas del cortafuegos: detecta ataques desde webs maliciosas por el puerto 80

Por otra parte, desde la instalación, se autoconfigura en modo aprendizaje, por lo que prácticamente se olvida de el, salvo por el excesivo consumo de recursos del sistema.

Se tiene que dedicarle mucho tiempo a aprender su funcionamiento, pero luego será recompensado, puesto que incluso se puede prohibir el acceso total o parcial a la computadora o a determinados directorios, entre otras muchas cosas.

FREEDOM

FREEDOM
Internet Security & Privacy

Encontrarlo en la red es muy difícil, como todo lo que rodea a su creador Zero Knowledge. Esta empresa ofrece entre otras cosas, navegación anónima a través de cuatro servidores proxy anónimos, ubicados en distintos países, y viajando la información encriptada entre ellos.

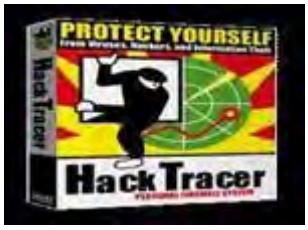
Su instalación es muy fácil, pero por defecto viene como casi todos los cortafuegos, con los puertos cerrados y el NETBIOS abierto, pero basta con hacer click en la “llama de personal

FIREWALL" y desmarcar un par de casillas en "personal FIREWALL behavior", para que todos nuestros puertos pasen a modo invisible.

Entre otras muchas opciones, permite rellenar los formularios, con datos reales o inventados o aleatoriamente, evita las ventanas de publicidad de unos 300 anunciantes habituales tipo "Doubleclick", pudiendo añadir lo que se desee, posee un filtro de cookies, puede escanear el correo saliente buscando texto sensible que se quiera enviar, como el verdadero e- mail, nombre, teléfono, se puede proteger con contraseña para que nadie salvo el administrador lo utilice, permite el uso de servidores proxy, lleva un registro de conexiones, puede usar múltiples identidades, y en la versión comercial del producto, se puede enviar y recibir correo electrónico encriptado de imposible rastreo (ni siquiera por el proveedor de acceso a Internet), navegación anónima, telnet anónimo y chateo anónimo.

Se dice que este cortafuegos lo utilizan habitualmente: los terroristas, los espías, los delincuentes organizados, los servidores secretos, algunos HACKER's y la mafia.

HACKTRACER



Un espectacular cortafuegos. Cuando se recibe un ataque, se tiene la opción de tracear al atacante pues el cortafuegos incorpora el programa neotrace, que muestra un mapamundi con la ruta que la computadora del atacante ha seguido hasta llegar a la computadora, resolviendo también los nombres de los servidores por los que ha pasado.

En algunos casos, es posible obtener del atacante y de su proveedor de acceso a Internet: su nombre, domicilio, teléfono, fax.

Su instalación, desinstalación y uso son de lo más fácil e intuitivo, e incluso dispone de una base de datos mundial donde se puede enviar información del atacante. Con la instalación por defecto todos los puertos pasan a modo invisible, por lo que no se debe de preocupar de nada, no siendo excesivo en consumo de recursos del sistema.

INTERNET FIREWALL

Al instalarse, avisa que no funciona en red local. De entrada, por defecto acepta conexiones de la red, no avisa de los escaneos desde el, y deshabilitar el NETBIOS es poco menos que una idea. Al escanear desde la web, responde que los puertos están cerrados, en lugar de invisibles, que seria lo deseable en un cortafuegos.

Tiene una opción muy buena, que es la de escaneo gratuito de virus por PC-CILLIN, mientras se esta conectado a Internet. Esto mismo puede hacerse visitado la página de PC-CILLIN, de McAFEE o de PANDA , e incluso agregando estas páginas a favoritos.

En la ayuda. Lo primero que dicen es que no garantiza ningún nivel de seguridad.

Dice que se pueden ver las conexiones activas, pero es mentira. Incluyen opciones que no funcionan.

Lo que si funciona es el bloqueo del escritorio mediante contraseña. De hecho, junto al desinstalador (que deja un par de carpetas en el directorio raíz), es lo único funciona.

INVATION

Es una copia de VIRUS MD (hasta el icono), y al igual que éste, no es muy recomendado. No recomiendo instalarlo, salvo que se quiera para pasar un rato agradable viendo como atacan a nuestra computadora, porque es para lo único que sirve.

MCAFEE FIREWALL

Antes de instalarlo, se debe tener a la mano el parche e instalarlo también. Cuando se desee descargar, se debe descargar el cortafuegos y el parche, que por cierto están en paginas distintas de su sitio web.

En la instalación inicial, aparentemente queda todo instalado y bien configurado. Si se le hace una prueba con un ataque simulado, resulta que dice que los puertos están cerrados, y el 139 abierto.

Por consiguiente, tras una configuración ya en condiciones, los pone en modo invisible. Respecto a la red local, es imposible configurarlo para un no iniciado. No avisa quien esta atacando para que se haga lo que se crea que se deba hacer.

Por defecto, permite que otros equipos entren a la computadora que se esta utilizando con NETBIOS sobre TCP/IP desde Internet, pero no desde la red local. Debería estar configurado por defecto, justo al revés.

También permite que otros equipos puedan conocer nuestra identidad. Puede que sea para evitar problemas con sus clientes, ya que algunos sistemas necesitan que uno se identifique antes de permitir el acceso a sus servicios.

En la documentación dice que se puede descargar una actualización en los 90 días siguientes a la fecha de compra del producto, y que transcurrido este plazo, no se tiene ningún derecho a nada (articulo 3 de la licencia). La desinstalación no es adecuada. Dado que carece de desinstalador, y se debe usar la opción de "agregar o quitar programas" del panel de control. Como al instalarlo crea ficheros en el directorio temporal de Windows, y al desinstalarlo no los encuentre, no se desinstala, pero tampoco funciona. Es decir: consume recursos gratuitamente, sin ofrecer nada a cambio.

McAfee FIREWALL ofrece una falsa sensación de seguridad, lo que hace entender que es mucho peor que saber que se está totalmente desprotegido, máximo cuando encima, bloquea la red local. Es decir, se comparten los recursos de la computadora con las demás computadoras y con los desconocidos.

Desde otro punto de vista este cortafuegos es el mejor para nuestros enemigos, pues les permite pasearse por nuestras computadoras como tal.

NORTON PERSONAL FIREWALL

Al instalarlo, es un detalle el que permita imprimir la hoja de registro. Luego queda a criterio que ellos sepan o no, que se está evaluando su software. Lo primero que se tiene que preparar con este cortafuegos, es mucha RAM.

Por defecto, viene configurado con un nivel de seguridad medio, y explica que es el adecuado para una navegación normal en Internet. Atacando la computadora vía Internet, muestra cerrados los puertos 113 y 139, dejando el resto en modo invisible. No obstante, muestra el nombre de la máquina.

Si se pone en modo de seguridad alta, y al atacar la computadora desde Internet, los puertos siguen como antes, pero la velocidad de navegación es muy lenta. Lo que se a cambiado en el modo seguridad alta son los applets de Java y los controles ActiveX, algo que se podrá haber hecho tranquilamente desde las opciones de seguridad del navegador.

En red, permite trabajar normalmente, sin necesidad de estar configurando reglas especiales.

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

El parecido con las estadísticas que reporta AT GUARD, es sospechoso. De hecho, están las mismas, en el mismo orden, con las mismas opciones y las mismas casillas de verificación.

Respecto a la privacidad, tiene un filtro tipo FREEDOM para la información confidencial (que no funciona si se envía por correo electrónico), y una opción para poner a prueba los nervios aceptando o denegando cookies (para luego tenerlas que aceptar porque caso contrario la web no permitiría continuar).

ZONE ALARM

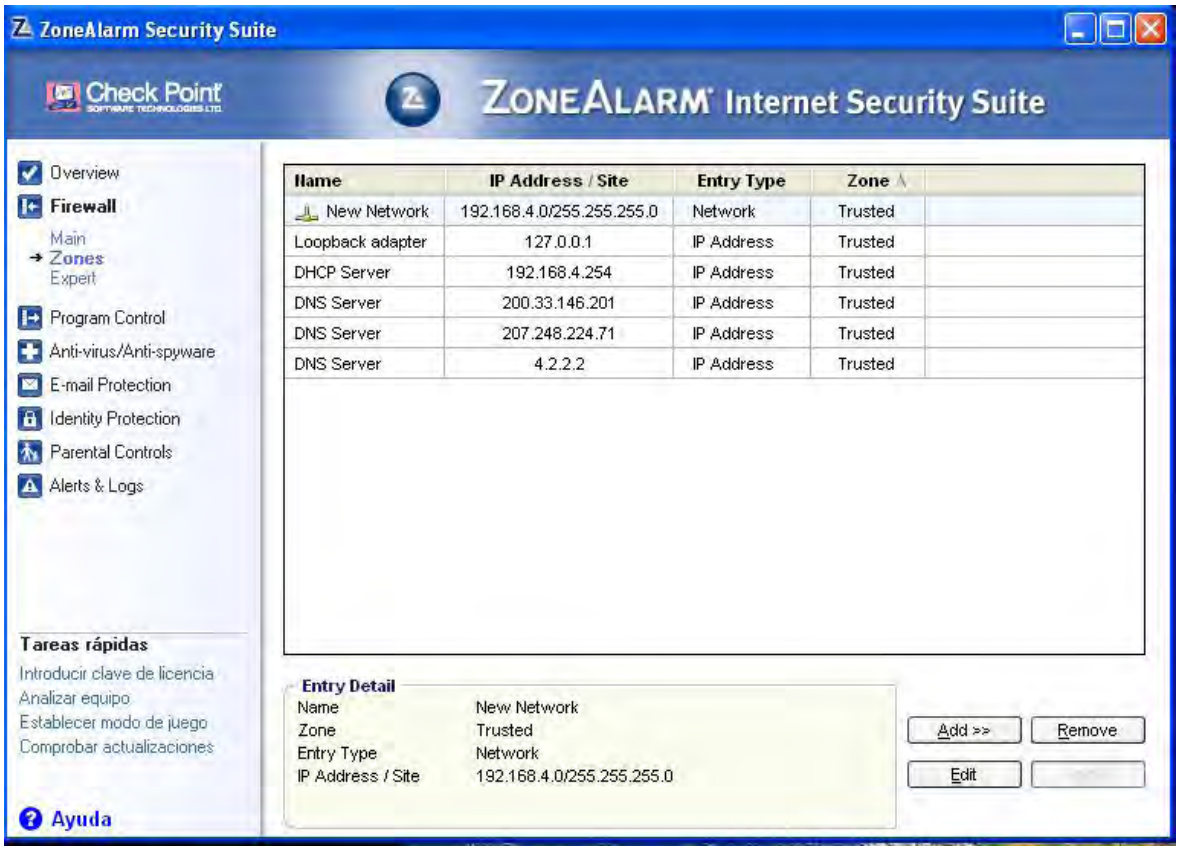


Figura 4.7.13 [19]

Todo un clásico en el mundo de los cortafuegos, que no sólo permite detectar todos los accesos desde Internet permitiendo solo el tráfico que se haya iniciado o se esté esperando, sino que además permite tener el control de los programas que intentan acceder a Internet, como por ejemplo un programa tipo Spyware que bien podría ser un visor de imágenes, y lo que hace para enviar información de nuestra computadora, y la vez mostrar publicidad adecuada a los gustos o preferencias de navegación por Internet.

[19] Imagen del programa Zone Alarm

Figura 4.7.14 [20]

Es un gran producto totalmente personalizable: se pueden seleccionar los niveles de protección tanto en red local como para Internet, bloquear o permitir acceso a Internet a las aplicaciones, bloquear el acceso a Internet tras un determinado tiempo con o sin actividad en la computadora.

Es fabuloso contra los troyanos, pues impide su acceso a Internet, aun cuando no intenten conectarse por sus puertos habituales.

Inconvenientes: Muestra a todos los que intentan conectarse a tu computadora. Por otra parte, no dice lo que hacen los programas que intentan conectarse a Internet.

[20] Imagen del programa Sygate

AGNITUM OUTPOST FIREWALL

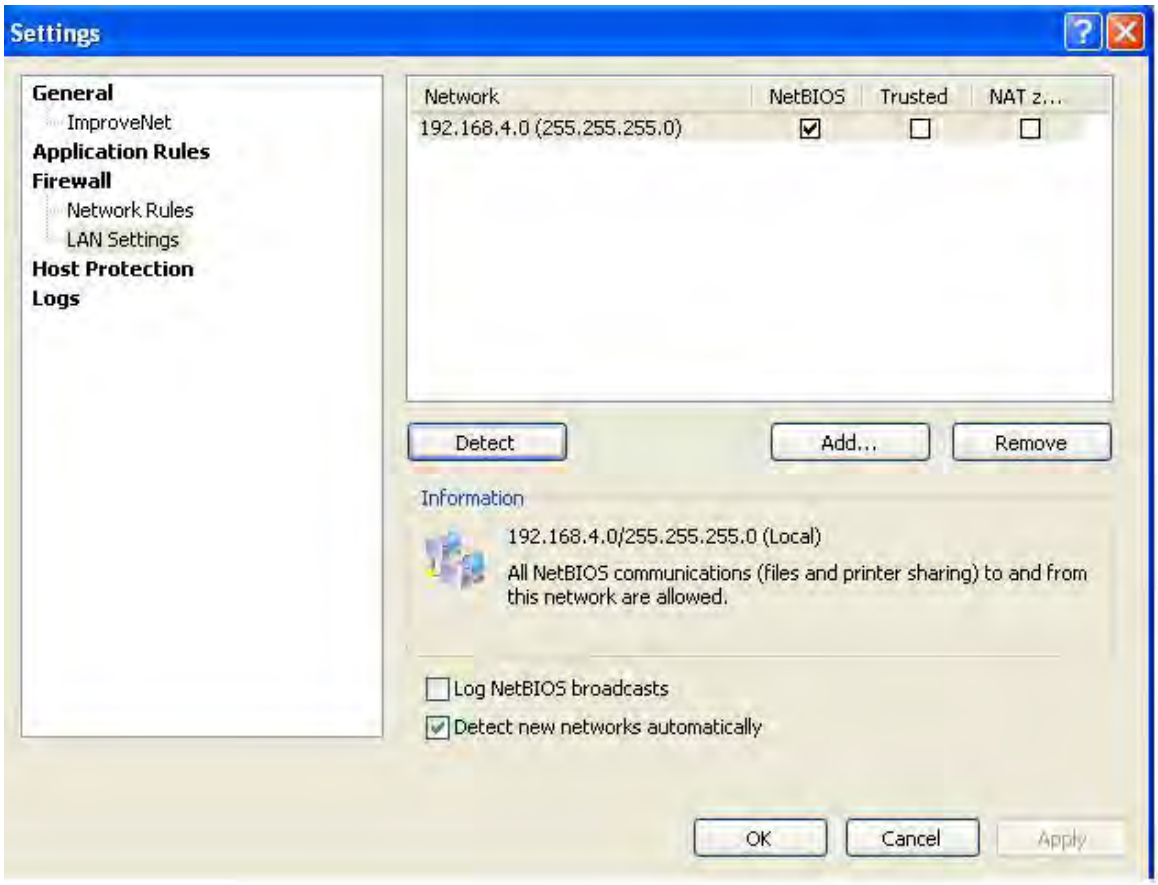


Figura 4.7.15 [21]

Este cortafuegos ya viene con las reglas preconfiguradas (navegadores, clientes de correo y aplicaciones), además elimina la publicidad y tiene un asistente muy cómodo y fácil de entender, se puede poner en modo invisible y se puede filtrar el contenido web, consume pocos recursos del sistema.

[21] Imagen del programa Agnitum Outpost

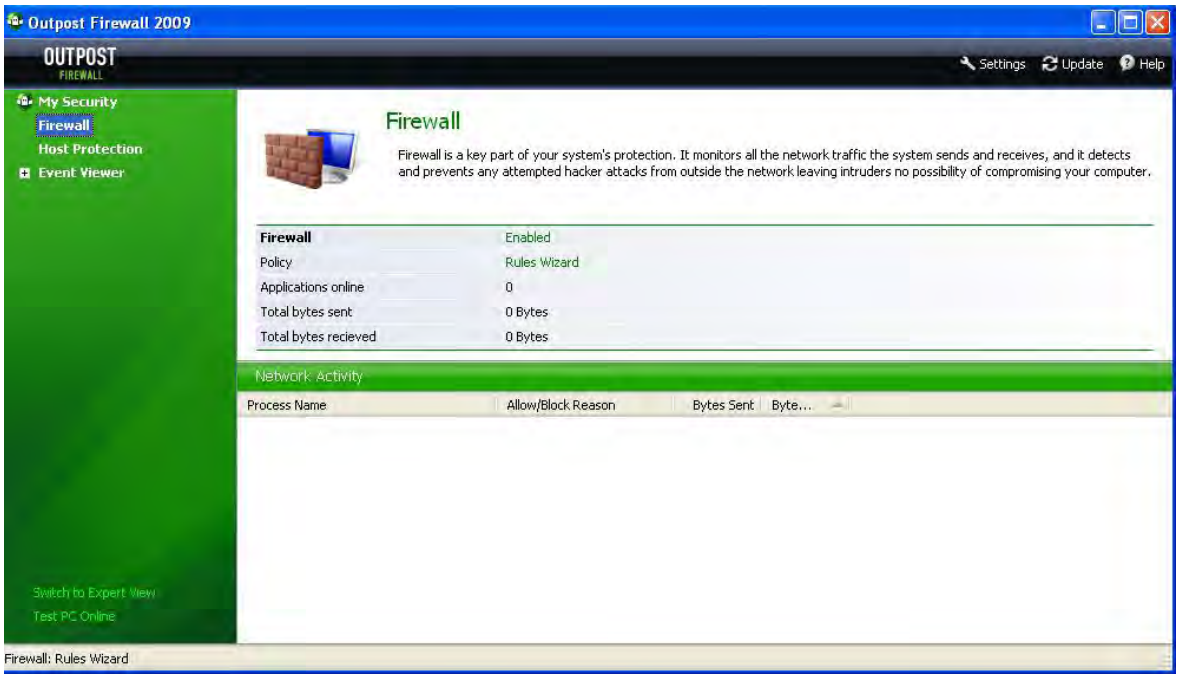


Figura 4.7.16 [22]

Deja el puerto 135 abierto, pero es imposible para un atacante aprovecharse de las dos únicas vulnerabilidades reportadas.

Recomendado

CISCO ASA

El Cisco ASA permite a las organizaciones obtener los beneficios de la conectividad y el costo de Internet de transporte sin comprometer la integridad de las

[22] Imagen del programa Agnitum Outpost

políticas de seguridad corporativas. Mediante la convergencia de seguro Sockets Layer (SSL) y Seguridad IP (IPsec), VPN con los servicios de defensa integral de la amenaza tecnológicas.

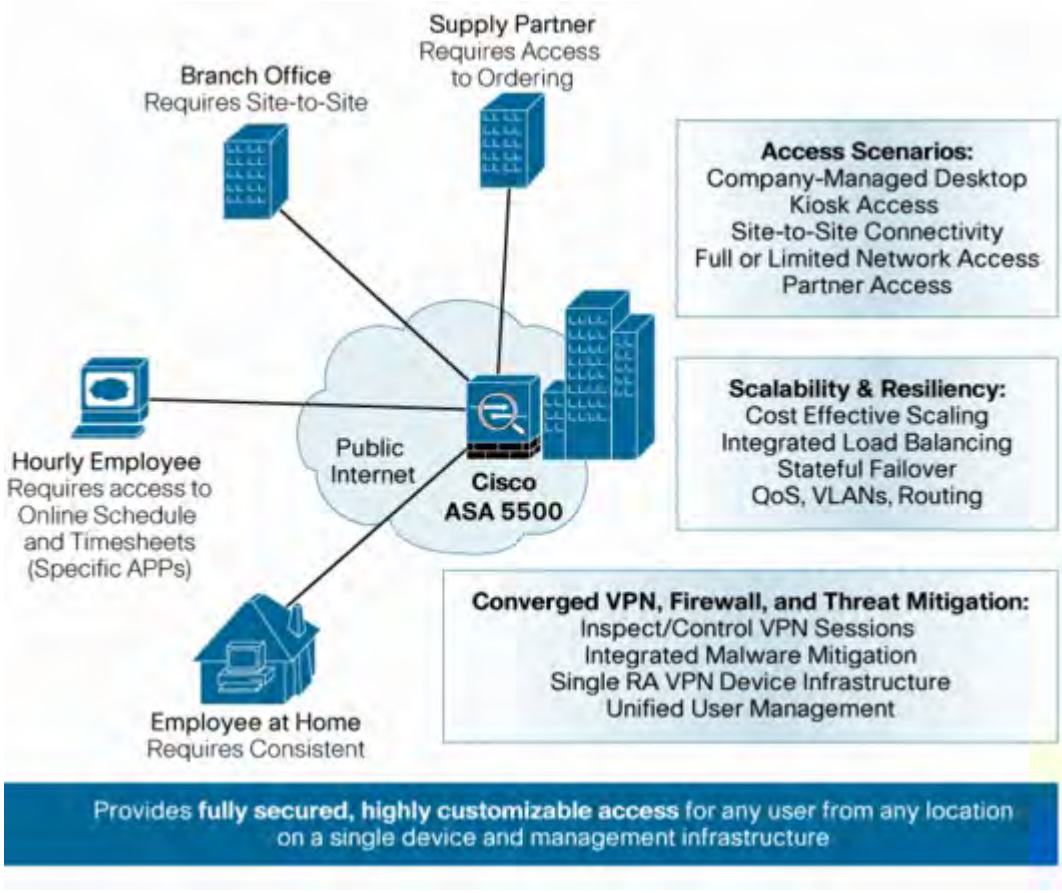


Figura 4.7.17 [23]

Integra numerosas funciones, tales como la seguridad y el equilibrio de carga que pueden reducir el número de dispositivos necesarios para la escala y asegurar la VPN, lo que disminuye costos de los equipos, la complejidad arquitectónica, y los gastos operacionales.

OFFICE SCAN

[23] Imagen descargada de la Pagina de Cisco

Figura 4.7.18 [24]

Por su parte, bloquea el acceso a sitios Web maliciosos. La flexible arquitectura de complementos, el nuevo control de dispositivos, la funcionalidad HIPS, la virtualización y la ampliación de las plataformas

Principales ventajas

- *Protección inmediata***.** Rompe la cadena de infección mediante el bloqueo del acceso a archivos y sitios Web maliciosos.

[24] Imagen del programa Office Scan

- *Reducción de los riesgos para empresas.* Evita las infecciones, el robo de identidades, la pérdida de datos, los tiempos de inactividad, la merma de productividad y las infracciones de cumplimiento de normativas.
- *Seguridad exhaustiva***.** Protege todos los tipos de puntos finales con una completa suite de seguridad específica para ellos.
- *Reducción de los costes informáticos***.** Reduce la carga de trabajo de TI mediante la reputación de archivos, la integración con Active Directory y la posibilidad de virtualización.
- *Arquitectura ampliable***.** Es posible agregar nuevas funciones de seguridad sin necesidad de volver a implementar toda una solución.

Como conclusión a este capítulo se puede señalar que para poder manejar la seguridad en Windows, se requiere de un FIREWALL que proteja la red. El FIREWALL en Windows puede ser un programa de muchos que hay en el mercado, la elección de FIREWALL que se realice debe cumplir con los requisitos de la política de seguridad y debe ser muy bueno no permitiendo la entrada de HACKER's y tráfico malicioso, además de no dejar ningún puerto abierto; se podría sugerir que cuando se tenga la intención de comprar un FIREWALL, se consiga primero la evaluación del programa y se tenga a prueba por el tiempo que permita el software o el tiempo que sea necesario y de aquí basarse para comprarlo una vez que se haya probado no sólo uno sino algunos, además el costo del software debe de ser uno que se adapte al presupuesto con el que se cuente. Recordemos que la seguridad de la información no es un juego y que es importante tenerla segura y respaldada

CONCLUSIONES

El desarrollo de software para garantizar el buen uso de la información, se ha vuelto indispensable para todas las organizaciones, existen muchas personas ajenas a esta información que buscan incansablemente nuevos métodos para apoderarse de ella, y utilizarla con fines de lucro. Por lo que el realizar esta tesis me ha llenado de satisfacciones propias, debido a que su desarrollo me permitió conocer más acerca de los métodos que podemos utilizar para resguardar toda nuestra información, con el objetivo de defendernos de aquellos ataques maliciosos.

Como experiencia puedo comentar que lo más importante para una empresa, es la responsabilidad y honestidad de las personas que ahí laboran; la información en movimiento dentro de la empresa puede ser sustraída por los mismos empleados, ya sea en memorias USB, por correo, discos u otros dispositivos de almacenamiento. Ej. De sustracción son; Nomina de los trabajadores, presupuestos de ventas, costos de elaboración, formulas para elaborar productos, programas, listas de precios, etc.

Una de las muchas satisfacciones que me deja el haber elaborado este trabajo es el de darme cuenta de que las empresas desarrolladoras de software se preocupan por mantener la integridad de la información, buscando siempre aquellos errores que pudieran tener los sistemas actuales para poder elaborar los parches necesarios para la corrección del mismo.

Bibliografía

A Simon y Schuster Company, ***Firewalls y la Seguridad en Internet,*** Editorial Prentice Hall, USA, 1996, pp 357.

Morant Ramos José Luis y Riba gorda Arturo, ***Seguridad y Protección de la Información***, Editorial Ramón Areces, España,1994, pp 392.

Strassberg, Keith E. y Gondek, Richard J. y Rollie, Gary ***Firewalls (Manual de Referencia)*** Editorial Mcgraw-Hill / Interamericana de España, Barcelona, 2003, pp 260.

Otras fuentes

www.danu.ie/

www.tinysoftware.com/

www.kerio.com

www.pablin.com.ar/computer/info/varios/firewall.htm

www.download.com

www.haygentepato.8k.com

http://gluv.univalle.edu.co/gsal/cortafuegos.htm

http://roble.pntic.mec.es/~sgonzale/linux/cortafuegos.html

http://es.wikipedia.org/wiki/Ipchains

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

www.zonealarm.com