UNIVERSIDAD DEL AZUAY

Facultad de Ciencia y Tecnología

Escuela de Ingeniería Electrónica

Análisis y diseño de la seguridad informática del servidor de archivos Linux Centos aplicado a una Entidad Bancaria.

Trabajo de graduación previo a la obtención del título de Ingeniero Electrónico

Autor:

Stalin Rodrigo Godoy Sánchez

Director:

Leopoldo Vázquez Rodríguez

Cuenca, Ecuador

2012

Agradecimiento

En primer lugar agradezco a Dios por darme la fuerza perseverancia y la vida para poder realizar este trabajo de graduación, a mis padres por su apoyo incondicional, a Rosmary Franco por su ayuda durante mi carrera, al ingeniero Leopoldo Vázquez, mi director, al ingeniero Leonel Pérez quien me supo dar sabios concejos.

Dedicatoria

Este trabajo está dedicado a mis padres quienes en todo momento han sido un pilar fundamental, a través de su apoyo y aliento, para llegar a esta nueva etapa de mi vida.

De igual forma dedico este trabajo de grado a todas aquellas personas que han estado junto a mí, brindándome su apoyo, concejos y enseñanzas a lo largo de mi carrera.

RESUMEN

Para esta investigación se realizó un diagnostico de seguridad al servidor de archivos de una entidad bancaria. Una vez detectadas las vulnerabilidades que causan perdidas de dinero y errores a los empleados, se proponen varias soluciones: Cambiar el sistema operativo del servidor a Linux Centos, crear un nuevo árbol de niveles de acceso con permisos específicos a la información, implementar un dispositivo de respaldo de información, crear políticas de seguridad para proteger hardware e información contra intrusos.

Como resultado de esta investigación se alcanzo mejoras significativas de seguridad permitiendo al personal del banco, propietarios y clientes operar en un entorno confiable minimizando pérdidas e incrementando la eficiencia.

PALABRAS CLAVES: Políticas de seguridad, servidor de archivos, sistema operativo Linux Centos, seguridad de la información, Entidad Bancaria.

Stalin Godoy

Lcdo. Leopoldo Vázquez.

ABSTRACT

This research is based on a former security diagnostic in a Bank File Server. Once detected the vulnerabilities that caused money losses and employees operation mistakes a group of solutions are proposed. Within those solutions are: Server Operating System was changed to Linux Centos, a new Access Level Tree was design in order to settle specific access permissions to information, an information backup device was implemented and physical security policies referred to protect hardware and information from intrudes.

As a result of this research a significant security improvement was reached allowing Bank Staff, Owners and Clients to operate in very reliable environment minimizing losses and increasing efficiency.

KEY WORDS: Security Policies, file server, Linux Centos operating system, information security, bank entity.

Lcdo. Leopoldo Vázquez.

Ing. Leonel Pérez.

Stalin Godoy

ÍNDICE DE CONTENIDOS

CAPITULO 3: ANÁLISIS DE LAS VULNERABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN DE UN SERVIDOR DE ARCHIVOS DE UNA INSTITUCIÓN FINANCIERA

CAPITULO 4: DISEÑO DE LA SOLUCIÓN AL PROBLEMA DE VULNERABILIDAD EN EL SERVIDOR DE ARCHIVOS DE UNA ENTIDAD BANCARIA

Stalin Rodrigo Godoy Sánchez
Trabajo de graduación
Lcdo. Leopoldo Vázquez
Marzo del 2012

Análisis y diseño de la seguridad informática del servidor de archivos Linux Centos aplicado a una Entidad Bancaria

INTRODUCCIÓN

Desde que una entidad bancaria fue inaugurada con una infraestructura, capital humano y económico se comprometió, gracias a la confianza de sus socios, a ofrecer servicios de calidad tales como aperturas de cuentas de ahorros, depósitos a plazo fijo, créditos, etc.; por lo tanto la misma debe de retribuir esa confianza a través del uso eficiente y seguro de la información confidencial que en la entidad bancaria dejan los socios tales como el saldo en dólares que poseen, los datos personales (direcciones, teléfonos, etc.); una de las formas para lograrlo es adoptar una tecnología que esté a la vanguardia en las políticas de la seguridad de información, dejando atrás tecnologías arcaicas que dejan vulnerable la información que se almacena en el servidor de archivos.

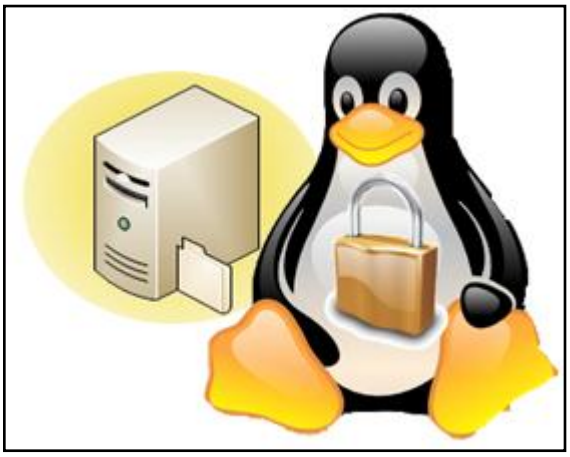
Una de las políticas de seguridad adoptadas en la entidad bancaria, es que se comparte las carpetas dentro de Windows tan solo con hacer clic con el botón derecho del mouse sobre la carpeta y escogiendo la opción compartir, sin darse cuenta que en cualquier otro computador, dentro de la entidad bancaria, se puede ingresar a esa carpeta compartida y por tanto con el riesgo de modificar o incluso eliminar las información contenida ya sea accidentalmente o mal intencionalmente; por lo cual se sugiere utilizar políticas modernas en la cual la seguridad de los archivos del usuario es

encargada a un servidor de archivos con Linux Centos, con herramientas de antivirus, firewall, cortafuegos, etc., los cuales van a permitir que solo personas autorizadas sean las únicas que pueda modificar el mismo.

En las entidades bancarias, no se están realizando el debido procedimiento para informar sobre un incidente de daño o pérdida parcial o total de cualquier archivo confidencial dentro de la cooperativa, por lo que se va a analizar políticas que permitan informar, de parte del asesor, en forma sistemática la ocurrencia de cualquier evento que afecte la seguridad de la información, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades, evitando la pérdida de información y la interrupción de los servicios.

CAPÍTULO I

Seguridad de archivos en Linux



1.1. Introducción

Para potenciar la seguridad de archivos hoy en día se implementan servidores de archivos sobre sistemas operativos que den la confianza necesaria de que la información almacenada en los mismos van a permanecer con restricciones de acceso. Es por eso que las instituciones financieras y de otras índoles optan por instalar servidores de archivos sobre el sistema operativo Linux Centos el cual además de ofrecer seguridad es una opción bastante económica al ser un software de libre distribución en el mercado.

En este capítulo se va a describir las principales características y políticas que utiliza el sistema operativo Linux Centos para mantener la información de un servidor de archivos en un estado fiable, confidencial, integro y disponible. Así como también las posibles vulnerabilidades a las que Linux se encuentra expuesta al no usar de una manera responsable y adecuada las configuraciones que se haga a los servicios de seguridad que Linux posee.

1.2. Concepto de seguridad

El término seguridad informática en una institución financiera significa tener un sistema libre de todo peligro, daño o riesgo en donde a cada empleado se le asigne permisos sobre los archivos que es propietario y así se pueda desempeñar en sus labores diarias sin poner en riesgo el trabajo de los demás.

1.3. Tipos de seguridad

En Linux para poder definir una determinada política de seguridad que requiere un sistema de archivos se debe de definir si se va a utilizar una seguridad física o lógica.

1.3.1. Seguridad Física

La seguridad física que proporciona Linux a un servidor de archivos significa tener en cuenta aspectos sobre el entorno en donde se encuentra ubicado el servidor de archivos. Para establecer una seguridad física adecuada primeramente se debe de ver que personas van a tener acceso físico al equipo de cómputo, tales como los administradores del centro de datos o DataCenter. Uno de los requerimientos más importantes de seguridad física es tener un servidor LINUX que al arrancar solicite un usuario y password.

A continuación se enumera las seguridades que debe de tener el DataCenter que alberga a un servidor de Archivos:

- Guardias de Seguridad las 24 Horas del Día, los 365 Días del Año.
- Sistemas de Vigilancia por circuito cerrado de televisión.
- Control de Acceso inicial en recepción.
- Control de Acceso a todas las salas, con acceso exclusivo mediante tarjetas de acceso.
- Y seguros eléctricos.

1.3.2. Seguridad Lógica

La seguridad lógica que proporciona Linux en un servidor de archivos hace referencia a la configuración adecuada del sistema que evitaría que personas no autorizadas tengan acceso a los recursos y a la propia configuración.

Entre los aspectos a tomar en cuenta para configurar el sistema se mencionara:

- Elección de buenos passwords que combinen letras, números y símbolos.
- Habilitar el protector de pantalla con password al momento que el servidor queda desatendido.
- Escoger un buen firewall (Cortafuegos).
- Escoger un buen antivirus que detecte troyanos.
- Utilización de dispositivos biométricos como lectores de huellas digitales.

1.4. Características de un sistema de archivos seguro

Para que un sistema de archivos bajo Linux se encuentre seguro debe poseer las siguientes características:

- **Integridad.-** Esta característica establece que la información almacenada en el servidor de archivos no puede ser modificada por quien no está autorizado.
- **Confidencialidad.-** Característica que establece que la información almacenada en el servidor de archivos solo debe de ser legible para personas autorizadas.
- **Disponibilidad.-** Característica que establece que la información almacenada en el servidor de archivos va a estar disponible en cualquier momento que su propietario lo requiera.

1.5. Seguridad Local

La seguridad local hace referencia a que Linux adopta medidas de seguridad adiciones para proteger a un servidor de archivos cuando accedan simultáneamente múltiples usuarios locales en tiempo real con el riesgo de que se viole el sistema intencionalmente o accidentalmente por ignorancia.

Los usuarios para vulnerar el sistema primeramente obtienen un nivel de privilegios de usuario para posteriormente ir aumento este nivel hasta llegar a los de un usuario administrador root. Además se utiliza la técnica de la "ingeniería social" que consiste en convencer a usuarios ingenuos para que entreguen su nombre de usuario y clave.

1.5.1. Cuentas y grupos de Usuarios

La organización jerárquica que utiliza Linux para los recursos de los usuarios y grupos es:

1. Cada recurso (archivo y directorios) pertenece a un usuario.
2. Cada cuenta de usuario está definida por una línea en el archivo /etc/passwd.
3. Cada grupo de usuarios por una línea en el archivos /etc/group.
4. Un permiso para un recurso se puede asignar a un usuario, un grupo u otro usuario.

Ejemplo:

```
chmod 766 file.txt   # brinda acceso total al dueño (7)

                     # y lectura y escritura a los demás (66)
```

Es por eso que un administrador de un servidor de archivos debe de dar los mínimos privilegios a un usuario para que pueda realizar su trabajo sin poner en riesgo a otros usuarios o al sistema.

1.5.2. Seguridad de Claves

Para mantener una cuenta de usuario segura Linux le obliga al usuario a claves con los siguientes requerimientos:

- No utilizar palabras conocidas como nombres u otros.
- Realizar una combinación entre letras, números y símbolos.
- Deben de ser fáciles de recordar pero a la vez difíciles de adivinar.
- No anotar la clave en un papel menos aun pegarla en el monitor.

Como se sabe las claves de los usuarios están guardadas en el archivo /etc/passwd el cual posee permisos solo de lectura para todos los usuarios en general a diferencia del usuario administrador root que posee permisos de lectura y escritura; un hacker por lo general lo que hace es tener acceso a este archivo a fin de obtener las claves de los usuarios, lo cual resulta una vulnerabilidad para el sistema, que puede ser solucionada al utilizar el archivo de sombra /etc/passwd en donde se guarde los nombres de los usuarios con sus claves cifradas y cuyo acceso sea dado solo al administrador root.

El formato del archivo /etc/passwd es el siguiente:

Usuario : clave : ultimo : puede : debe : aviso : expira : desactiva : reservado

Donde:

- **Usuario:** El nombre del usuario.
- **Clave:** La clave cifrada
- **Ultimo:** Días transcurridos del último cambio de clave desde el día 1/1/70
- **Puede:** Días transcurridos antes de que la clave se pueda modificar.
- **Tiene:** Días transcurridos antes de que la clave tenga que ser modificada.
- **Aviso:** Días de aviso al usuario antes de que expire la clave.
- **Expira:** Días que se desactiva la cuenta tras expirar la clave.
- **Desactiva:** Días de duración de la cuenta desde el 1/1/70.
- **Reservado:** Reservado complementos para el sistema.

El administrador solo debe de ejecutar el comando pwconv como root; para crear el fichero /etc/shadow.

1.5.3. El bit SUID y el SGID

El bit SUID permite a un usuario cualquiera adquirir los privilegios de un usuario propietario de un recurso.

Por ejemplo:

chmod 4355 /usr/bin/passwd

Se estará activando el permiso SUID y estableciendo los permisos 355 al archivo /usr/bin/passwd que originalmente solo tiene el usuario administrador root.

El bit SGID permite a un usuario cualquiera adquirir los privilegios de un usuario propietario de un grupo de usuarios.

Por ejemplo:

chmod 2355 /usr/bin/passwd

Se estará activando el permiso SGID y estableciendo los permisos 355 al archivo /usr/bin/passwd, que es necesario cuando el grupo de usuario normales necesitan cambiar su password.

Hay que tener en cuenta que al activar el bit SUID y SGID se está corriendo el riesgo de que algún intruso trate de ejecutar otro código distinto con los privilegios de este proceso.

1.5.4. Manejo del usuario ROOT

En ocasiones, en un sistema de archivos, las seguridades de los recursos de los usuarios son vulneradas por el propio administrador root provocando la caída del servidor de archivos; y para evitar esto se recomienda que el administrador del servidor de archivos:

- No utilice la cuenta de usuario root, en lugar de ello debe utilizar una cuenta de usuario diferente en la cual se maneje el comando SU para ejecutar cualquier proceso que requiera de privilegios de administrador root.
- Se cerciore bien antes de ejecutar un comando como los que borran archivos.
- Utilice SSH o cualquier otra conexión remota.
- Piense bien antes de realizar cualquier acción.

1.6. Seguridad en el Sistema de archivos

El sistema de archivos de Linux se refiere a la forma de escribir los datos en el disco duro, lo que lleva a utilizar normas de seguridad en el disco. La estructura de del sistema de archivos de Linux se basa en directorios, permisos y enlaces.

1.6.1. El árbol de directorios

La seguridad de los directorios está en función del de que el administrador del servidor de archivos realice una correcta distribución del espacio en disco ya que si es que se pierde una partición no va a afectar a todo el sistema.
Aunque se debe de seguir las siguientes normas:

- Crear una única partición para el directorio /home ya que existirán múltiples usuarios que ingresarán al servidor de archivos.
- Crear una única partición para el directorio /var e incluso para /var/spool.
- Crear una única partición para el directorio /var e incluso para /var/spool.
- Mantener los directorios /dev, /etc, /bin, /sbin, /lib, /boot en el directorio raíz ya que se utilizan durante el arranque del sistema.

1.6.2. Permisos de ficheros y directorios.

Un permiso es un conjunto de bits individuales que definen el acceso a un fichero o directorio. En general Linux para asegurar el acceso de un usuario, clasifica el control de acceso en propietario, grupo y otros. El propietario y el grupo son únicos para cada fichero o directorio. A un grupo pueden pertenecer múltiples usuarios; y otros usuarios no pueden acceder a un archivo que no es propietario.

Los permisos para directorio tienen un sentido diferente a los permisos para ficheros entre los cuales se tiene:

- **Lectura (r)**:

  - **Fichero**: Poder acceder a los contenidos de un fichero
  - **Directorio**: Poder leer un directorio, ver qué ficheros contiene

- **Escritura (w)**:

  - **Fichero**: Poder modificar o añadir contenido a un fichero
  - **Directorio**: Poder borrar o mover ficheros en un directorio

- **Ejecución(x)**:

  - **Fichero**: Poder ejecutar un programa binario o guion de shell
  - **Directorio**: Poder entrar en un directorio

1.6.3. Enlaces

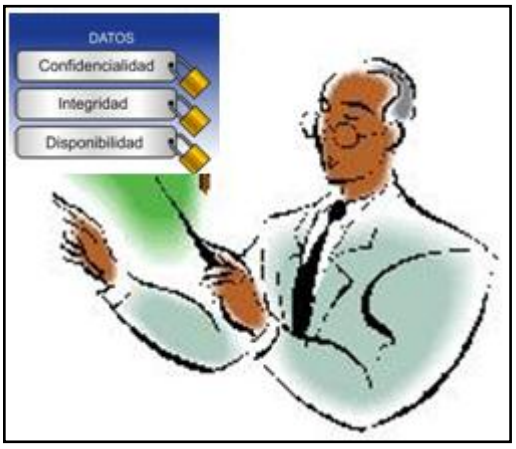
Los enlaces se refieren a que un fichero se puede conectar con otro de una manera dura o solo simbólica; siendo el enlace duro el que asigna más de un nombre a un mismo archivo y el simbólico el que contiene la dirección de otro archivo.

Hay que tener especial cuidado con los enlaces ya que puede ser causa de

vulnerabilidad en el sistema de archivos ya que se está enlazando múltiples archivos.

CAPÍTULO II

Políticas de seguridad de información usadas en una entidad bancaria.



2.1. Introducción

Una entidad financiera preocupada por la seguridad de sus consumidores financieros con una posición importante y creciente en el sistema financiero requiere dentro del alcance de sus proyectos de mejoramiento continuo, implementar las mejores políticas de seguridad de la información que le permitan mantener una posición primordial en el sector de negocios, es por ello que se deben de tomar las acciones tecnológicas más apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje, extorsión, etc. que serán vistos en el siguiente capítulo.

Una entidad financiera adopta medidas de seguridad para proteger la información que es propietaria de acuerdo a su importancia y valor; medidas que se adoptarán sin importar si la información se guarda en papel o en forma electrónica, ó si se procesa en una computadora personal, un servidor, correo de voz, etc. o la manera en la que se

trasmite bien sea correo electrónico o vía telefónica. Y para lograr a su fin de estas medidas se debe de restringir el acceso a la información a los usuarios de acuerdo a su cargo (Asesor de crédito, cajeros, asesores de servicio al cliente, promotores de venta, jefe de agencia, etc.).

En este capítulo se va describir las políticas de seguridad de la información más recomendadas por su eficacia que permitan proteger la información en función de los criterios de la confidencialidad (acceso a la información solo por parte de las personas que estén autorizadas), disponibilidad (posibilidad de que la información esté disponible, encontrado o utilizado por personas autorizadas) e integridad (que la información está completa y podrá ser modificada con autorización) y que aseguren directa o indirectamente la información que origine o procese cada usuario que labora en una entidad financiera, tales como políticas para clasificar la información, asignar dueños de la información, contra software malicioso, para usar contraseñas, para usar equipos portátiles y medios removibles como memorias USB dentro de la entidad.

2.2. Clasificación de la Información

Uno de los activos más importantes dentro de una entidad financiera es la información ya sea esta un documento, programa, archivo, pantallas de consulta, reportes, impresiones o correos electrónicos o cualquier otro tipo de información generada, almacenada o procesada, y uno de los métodos para precautelarla es clasificarla aplicando medios y procesos informáticos.

El objetivo principal de estas políticas es la de proteger la información ante una posible pérdida, divulgación no autorizada, uso indebido, y difundir entre cada empleado directo, temporal o tercealizado que labora en la entidad financiera.

La clasificación de la información será:

- **Información Pública.-** Toda información categorizada en este grupo podrá ser utilizada y/o conocida por cualquier persona, incluso el público, es decir esta información podrá ser acezada por cualquier medio de difusión impresa o electrónica, como por ejemplo información promocional de los productos y servicios, tasas de interés, balances financieros de fin de año, etc.
- **Información de uso interno.-** Información que podrá ser utilizada y/o conocida solo por cualquier directivo o colaborador interno de la entidad financiera y cualquier consulta de información entre ellos se la realizará bajo autorización del dueño de la información. La posible pérdida de este tipo de información podría causar daños leves a la entidad financiera. Esta información incluye políticas internas, manuales, formularios con información de los clientes, reportes internos que se utilizan en la gestión interna de la entidad, etc.
- **Información confidencial.-** Información que podrá ser utilizada y/o conocida solo por un grupo reducido de directivos o colaboradores internos de la entidad financiera y cualquier consulta de información entre ellos se la realizará bajo autorización gerencial. La posible pérdida de este tipo de información causará daños graves a la entidad financiera. Esta información incluye análisis de mercado, análisis financiero, planificaciones estratégicas, contratos, acuerdos extrajudiciales, etc.

2.3. Dueños de la Información

Debido a que toda información tiene un origen y un destino entonces obligatoriamente va a tener un dueño quien va a ser el encargado de velar por el buen uso y finalidad que se le dé a la información, y así lograr el buen desempeño del sistema de Gestión de la seguridad de la información. Esta política tiene como finalidad principal normar las responsabilidades y funciones, directas o a través de sus subordinados, del manejo

de la información que es dueño cada empleado de una institución financiera.

Los empleados dueños de la información deben de cumplir las siguientes políticas:

- Clasificar la información al momento que se genera y durante todo el tiempo de vida que tenga la misma.
- Autorizar la reclasificación de la información en caso de reformas en las normas internas de la institución financiera.
- Autorizar por escrito el acceso a su información a cualquier otra persona o a terceros que solicite con autorización de su jefe inmediato.
- Autorizar la destrucción de la información que es dueño desde el lugar en donde se encuentre almacenada.
- Estar pendiente sobre el uso que se le dé a la información a la que haya autorizado usar a terceros con relación a respaldos, restauraciones, etc.
- Participar en la toma de decisiones para el encriptamiento que se le dé a la información que es dueño.
- No podrá autorizar acceso a información a la que no es dueño.

2.4. Software Malicioso

Esta política está orientada a proteger la información de los empleados de una institución financiera contra acciones ilegales o perjudiciales, debido a causas inseguridad informática, así como detectar oportunamente a través antivirus cualquier código malicioso contenido en archivos o correos electrónicos, entendiéndose como código malicioso cualquier clase de programa informático conocido como virus informático.

Entre las políticas para prevención de software malicioso se tiene:

- Cada equipo de cómputo interno tendrá instalado un antivirus.
- Cada archivo que ingrese al disco duro de un equipo de cómputo deberá ser escaneado por el antivirus.
- No ejecutar archivos sospechosos adjuntos a correos o de una fuente desconocida. Borrar inmediatamente esos archivos.
- Borrar cualquier archivo “Spam” y cualquier archivo chatarra sin reenviarlo.
- No utilizar recursos compartidos de archivos a menos que sea necesario.
- Realizar periódicamente una copia de seguridad de toda la información más crítica en cualquier clase de medio de almacenamiento.
- En caso de sospecha o certeza de que un computador esté con algún tipo de software malicioso se deberá contactar inmediatamente con el departamento de soporte para que examine y repare el inconveniente.
- En caso de que no se pueda eliminar el software malicioso se procederá a restaurar la instalación del sistema operativo de fábrica.
- Cualquier computadora infectada con alguna clase de software malicioso debe ser desconectada de la red para evitar que se propague el software malicioso.
- Todo equipo de cómputo deberá poseer instalado software con licencia o que sea software libre.

2.5. Manejo de contraseñas

Para controlar que solo el dueño de la información se autentifique y tenga acceso a la misma, se le asigna un usuario y una contraseña que son únicos y confidenciales. El

objetivo de estas políticas es la de lograr que los empleados dueños de la información usen planificada mente las contraseñas que maneja, además de dar los limites de seguridad de dichas claves para que se pueda realizar el trabajo asignado a cada usuario.

Las políticas de uso de contraseñas en una institución financiera serán:

- A cada empleado nuevo que ingrese a laborar en la institución se le asignará una contraseña para el acceso a una carpeta compartida de almacenamiento de información, la cual tendrá que ser cambiada inmediatamente por motivos de privacidad y confidencialidad en las claves.
- Igualmente todo empleado que no se acuerde alguna clave se le asignará una clave la cual tendrá que ser cambiada inmediatamente.
- Las características que tendrá las claves serán:

    - Cantidad de caracteres establecida para cada recurso.
    - Tener una combinación de caracteres alfanuméricos.
    - Que sean fáciles de recordar pero difíciles de descifrar.
    - No utilizar sus propios nombres, fechas de nacimiento, etc.

- Cada clave es personal, confidencial, intransferible y solo son designadas para desarrollar su trabajo.
- Existe la posibilidad de que un usuario comparta su clave con un colaborador siempre y cuando el dueño del usuario por seguridad, deberá solicitar el cambio de clave al administrador del sistema.
- Cada empleado será responsable absoluto por el uso que se le dé a su usuario y clave
- Procurar en lo posible evitar escribir las contraseñas en cualquier lugar como papeles de fácil acceso.
- El sistema no debe permitir que se utilice una contraseña anteriormente utilizada por el usuario.
- El usuario podrá solicitar el cambio de contraseña las veces que sean.
- Cuando el usuario se ausente de su puesto de trabajo debe de dejar protegida toda aplicación y activar el bloqueo del sistema operativo.

- El usuario podrá solicitar el aumento de roles a su cuenta previa autorización del jefe inmediato y comunicado al administrador del sistema para que los ponga en ejecución.
- Ningún empleado podrá tener simultáneamente dos usuarios con los mismos roles dentro del sistema informático.
- Si es que el empleado es separado de la institución financiera, entonces se le deberá de notificar al administrador del sistema a fin de que se le sea desactivado su cuenta.

2.6. Uso de Computadoras Portátiles

Estas políticas hacen referencia a que por lo general las altas gerencias, jefaturas y personal seleccionado realizan trabajo de campo y necesitan como herramienta de trabajo un equipo de cómputo portátil, en donde mantienen información importante para la institución financiera, por ende la misma tiene que ser tratada con toda la seguridad posible y así contribuir con la seguridad de toda la información y así evitar incurrir en las posibles amenazas en las que incurren las computadoras portátiles que provocarían un gran problema a la institución financiera.

Entre las políticas se tiene:

- Se debe de identificar a cada responsable de cada portátil de la Institución Financiera.

- Cada empleado que es responsable de la seguridad física de la portátil que se le asigne, tanto dentro como fuera de la institución financiera.
- El departamento de sistemas es el responsable de instalar un antivirus adecuado en cada portátil y software con licencia.
- Cada computador portátil es propiedad de la institución Financiera y se consideran como activos relevantes de información y como tal deben ser continuamente protegidos.
- Todos los computadores portátiles deben ser usados solo para propósitos de cumplimiento de funciones y/o actividades que sean debidamente autorizadas.
- Todos los computadores deben ser fijados con el cable de seguridad hacia el escritorio donde labora cada empleado.
- Cualquier computador que ingrese a las instalaciones de la institución financiera, deberá antes de ser registrada su MAC (Control de Acceso al Medio), marca, modelo, la fecha de ingreso y justificación de acceso a la institución y a su red de datos; y luego de haber culminado la visita, a la laptop se le retirará los permisos de acceso a la red que se le hayan dado.
- La restricción de instalar cualquier tipo de software sin licencia y sin autorización del jefe inmediato superior.
- Cualquier incidente que ocurra con el equipo debe de ser reportado a soporte técnico de sistemas de la institución.
- Al finalizar la jornada de trabajo el empleado de la institución financiera deberá de dejar apagando la misma y en un lugar seguro con llave.
- El computador portátil deberá de ser revisado periódicamente tanto en hardware como en software por parte del departamento de sistemas.
- En caso de que se comparta la computadora portátil entre varios empleados de la institución financiera, entonces se deberá de registrar tanto los datos del de empleado que vaya a usar como también para que va usar la misma.

2.7. Medios Removibles

Estas políticas tienen como objetivo principal la de controlar el acceso a los usuarios (empleados y terceros) al uso de medios informáticos removibles como flash memorys, teléfonos inteligentes, CD, DVDs , cámaras, etc., cuya función como se sabe es la de almacenar y ser un dispositivo de fácil transportabilidad de información, que utiliza el personal que labora en una institución financiera, con los riesgos de que alguna persona mal intencionada extraiga información de su computador o cualquier otro servidor de datos para usarlo con fines malévolos que provoquen daño a la institución.

En la institución financiera existirán grupos que no podrán utilizar medios extraíbles, por lo general el área operativa y otros que con autorización si los podrán utilizar, por lo general el área administrativa, los cuales en ocasiones transporten información desde una computadora de la institución a o su casa, con el riesgo de que si darse cuenta infecte de virus, gusanos y troyanos el dispositivo extraíble y a la vez al retornar a la institución ponga en riesgo toda la red de computadoras de la misma.

Entre estas políticas se tiene:

- Se puede categorizar como medio removible a los siguientes medios electrónicos: floppy disk, memory stick, PDAs, flash memory, ZIP drives, cámaras digitales, CDs, CD-Rs, DVDs, DVD-Rs, Discos duros removibles, etc., o cualquier otro medio de almacenamiento de información removible.
- Se podrá autorizar el uso de medios removibles únicamente a las gerencias y jefaturas, siempre y cuando se cumpla con las presentes políticas.

- No se permitirá bajo ninguna circunstancia el uso de medios removibles en el área de ventanillas, debido a las funciones que desempeña dicha área con manejo de dinero.
- Para que un empleado pueda usar un medio removible deberá de solicitar al jefe inmediato superior la respectiva autorización por escrito.
- Toda autorización debe de ser registrada en un historial por parte del personal encargado de administrar la seguridad de la información.
- Es recomendable y en lo posible evitar usar medios de almacenamiento removibles en áreas críticas como en servidores, procesamiento y transmisión de datos, etc.
- En caso de que se autorice el uso de un medio removible a un empleado, es recomendable que el mismo este formateado y solo sea designado para la función de almacenar información de la institución.

CAPÍTULO III

Análisis de las vulnerabilidades en la seguridad de la información de un servidor de archivos de una Entidad Bancaria

3.1. Introducción

Para implementar una buena estrategia de seguridad en un servidor de archivos, primeramente se debe de tomar en cuenta las vulnerabilidades a los que se encuentra inmerso el mismo, tales como la presencia de un atacante (hacker o una persona normal) motivado y determinado a comprometer la integridad de la información vital de la institución almacenada en dicho servidor.

Este capítulo descubre las potenciales vulnerabilidades de Linux que podrían poner en riesgo la seguridad de la información que se encuentra almacenada en el servidor de archivos de una institución financiera y que el administrador de sistema debe de tomar en cuenta para no caer en las mismas, sobre todo al saber que el código fuente de Linux es de acceso libre.

3.2. Vulnerabilidades en la instalación de Linux Centos

En ocasiones el administrador de un servidor de archivos al momento que comienza con el proceso de instalación del software, es decir el sistema operativo que en este caso es Linux Centos, no se toma en cuenta que dicho sistema operativo contiene un paquete con más de 1000 aplicaciones y bibliotecas de paquetes; esto puede causar la instalación de servicios innecesarios, configurados con sus valores por defecto y posiblemente activados por defecto tales como telnet, DHCP, DNS, etc.

Además es necesario que se instale el paquete de software Linux Centos actualizado (kernel, aplicaciones y herramientas del sistema) a la penúltima versión ya que la última no se ha puesto a prueba en su fase de diseño ni ha sido suficientemente validada por los usuarios, y así mantenerse al día en la evolución de los productos, así como conocerlos a fondo para poder configúralo correctamente.

3.3. Los servicios instalados sin sus parches.

A pesar de que una versión de Linux implica que ha sido probado y reprobado en todas las posibles ámbitos de trabajo de un servidor de archivos sin encontrar un solo error de vulnerabilidad a la información almacenada, eso no del todo creíble ya que siempre queda una vulnerabilidad escondida que es necesario de corregirla utilizando los llamados parches, que son programas ejecutables que incluyen servicios en el sistema que redirigen el rumbo de un proceso.

Por lo general estos parches son publicados en las páginas del internet a fin de que los administradores del servidor de archivos los encuentren y los instale en el servidor, y así asegurar un ambiente computacional seguro. Pero estas fuentes de parches también constituyen una vulnerabilidad para la seguridad de la información ya que ciertos hackers se adelantan e investigan esta información y actúan en contra de la seguridad la información almacenada en los servidores de archivos.

3.4. La administración inadecuada del servidor de archivos

Una de las principales causas de la vulnerabilidad de un servidor de archivos es que no se tiene en la institución bancaria una persona capacitada, o poco motivada en el área de trabajo, ya que si es así tal persona va a descuidar la seguridad del servidor y por tal la información almacenada de gran importante para la institución bancaria.

El Administrador del sistema de archivos debe de mantener el servidor desde la instalación hasta la puesta en producción del sistema, ya sea actualizando contraseñas, parches o monitoreando cualquier alerta que se presente en el sistema.

3.5. Los servicios más vulnerables de Linux.

Linux es un sistema operativo que posee muchos servicios que se ejecutan en background, los mismos que son instalados por default, y que son desarrolladas para que funcionen en ambientes sin una conexión a internet, pero si es que se conecta el server a internet para alguna actualización, dicho servicio se convertirá en una vulnerabilidad más del sistema contra la información almacenada en el servidor de la institución financiera.

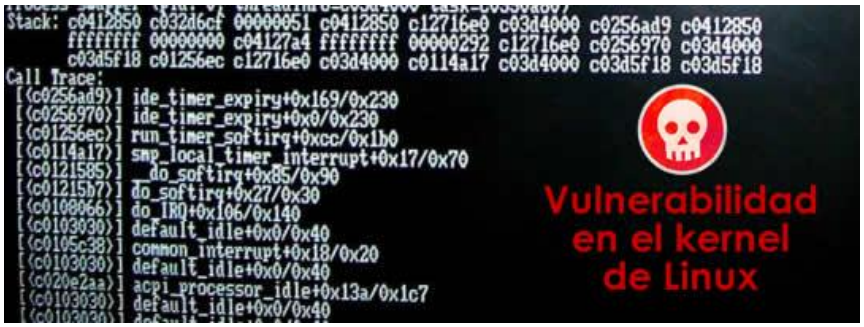
Entre los servicios más inseguros tenemos el de Telnet y FTP que son servicios de red que requieren nombre y contraseñas sin encriptar, los mismos que pueden ser monitoreados por software que husmean el tráfico de paquetes de la red. E incluso los hacker podrían utilizar estos servicios vulnerables para redirigir el tráfico de paquetes hacia su computadora sin que el servidor o el usuario se den cuenta. En otra categoría de servicios se encuentran los servicios del sistema de archivos de red (NFS) y servicios de información (NIS) ya que los mismos son servicios de red LAN, aplicándose incorrectamente en redes LAN donde un hacker utilizaría este error para accesar a permisos y las contraseñas y usuario que dichos servicios manejan.

Por lo general Linux Centos viene ya configurado con los servicios desactivados, pero también existe la posibilidad de que el administrador del servidor de archivos tenga la necesidad de activarlos por a o b razón, lo cual lo debe hace de una manera cuidadosa.

3.6. Uso de contraseñas y carpetas compartidas

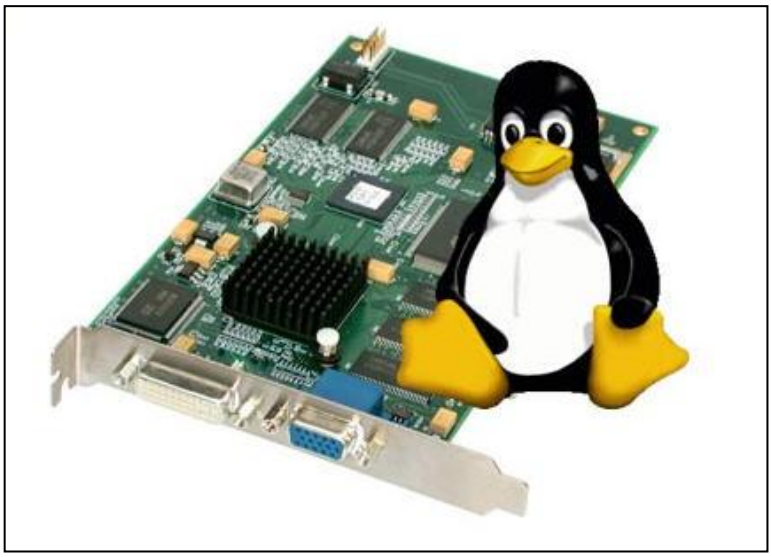
Uno de las primeras formas que un hacker utiliza para vulnerabilidad la seguridad de un servidor de archivos es la de probar posibles contraseñas que se refieran a la aplicación que está usando, obteniendo éxito en algunas ocasiones ya que los usuarios dueños de carpetas compartidas en el servidor de archivos, utilizan contraseñas muy fáciles de descubrir.

3.7. Permisos, privilegios y/o control de acceso



Esta vulnerabilidad se produce cuando se le asigna los privilegios de lectura, escritura o de ejecución a ciertos usuarios que no deberían de tenerlos para el acceso a archivos o carpetas, debido a que el administrador del servidor se equivocó al asignar privilegios.

3.8. Gestión inadecuada de los recursos hardware



Otra de las vulnerabilidades comprende el compartir recursos de hardware con demasiados privilegios a los usuarios del sistema, ya que si es que se asigna demasiada memoria, disco duro o procesador, se podría provocar que se tome el control del sistema o que vuelvan lento al mismo.

CAPÍTULO IV

Diseño de la solución al problema de vulnerabilidad en el servidor de archivos de una entidad bancaria

4.1. Introducción

Para constituir una entidad financiera sólida es necesario que a más de dar buenos servicios financieros, brinde a sus socios la confianza de que la información de su estado financiero se encuentra segura sin que otros puedan acceder a esa información sin su consentimiento, algo se logra principalmente con el respaldo de una infraestructura tecnológica robusta y estratégicamente planeada desde sus bases hasta sus puntos que están más al contacto con los socios de la entidad financiera.

Se va a diseñar una solución a una entidad financiera para que esta almacene la información de sus socios en un medio informático seguro, llamado servidor de archivos, eliminando las vulnerabilidades que amenazan hoy en día la seguridad de la información de una entidad bancaria.

Se va a diseñar un servidor de archivos bajo Linux Centos para una entidad financiera con el mayor número de controles tecnológicos de seguridad que erradiquen cualquier tipo de vulnerabilidad a la que por su naturaleza está expuesta la información que esta almacenada en este tipo de servidor. Controles tales como firmwares, permisos de acceso a los archivos de los usuarios, que serán descritas paso a paso desde la instalación del Sistema Operativo Linux hasta la creación de las diferentes carpetas de archivos de cada usuario en el disco del servidor.

4.2. Instalar y configurar un cortafuego (firewall)

Un cortafuego bien instalado y configurado es la defensa más importante en un servidor de archivos, ya que cualquier servicio que posea alguna potencial vulnerabilidad será solapada por la seguridad que proporcione el cortafuego que está en primera línea en contacto con los usuarios.
El cortafuegos debe ser lo primero que se debe de configurar antes de proceder a realizar las posteriores etapas sobre todo las que impliquen conexión a internet. El cortafuegos debe ser configurado para denegar cualquier paquete a excepción de los que se encuentran en estado establecido (ESTABLISHED) o relacionado (RELATED), proporcionando la máxima seguridad para llevar a cabo el resto de tareas de seguridad de la información.

4.3. Actualizar todos los paquetes instalados

Linux Centos posee más de 1000 paquetes que al momento de instalar, siempre habrá la probabilidad de que uno de ellos esté desactualizado, por lo que es necesario que se realice la tarea de actualizar por lo menos los paquetes que se van a utilizar ya que

estas actualizaciones van hacer a instalar nuevas características y correcciones de errores, tales como parches a ciertas vulnerabilidades que pueden atentar con la seguridad de la información del servidor de archivos.

La actualización de los parches es recomendable debido a que a cada momento están saliendo en internet nuevas mejoras. Este proceso de actualización de parches toma por lo general muchos minutos del tiempo del administrador, pero existen una aplicación que lo realiza por uno automáticamente, llamada APT (Advanced Package Tool), el mismo que es configurado. Una vez instalado lo único que hay que hacer es ejecutar los siguientes comandos en el terminal de Linux:

$ yum list update
$ yum upgrade

El primer comando descarga la información mas actual de los paquetes del repositorio y el segundo utiliza esta información para descargar e instalar nuevas versiones de paquetes ya instalados si estas están disponibles. Estos comandos deben de ser ejecutados periódicamente cuando se presienta alguna anormalidad en el servidor de archivos.

4.4. Parar y deshabilitar todos los servicios innecesarios

Al momento de instalar Linux Centos en el Servidor de archivos se instalan también múltiples servicio o también llamados demos los cuales deben de ser cuidadosamente parados y deshabilitados a fin de no dejar una puerta vulnerable a la información del servidor de archivos.

Servicios tales como:

- HTTP (Servidor WEB).

- POP3/IMAP (email).

- Servicios de Bases de Datos.

En Linux Centos se realiza la configuración mediante la utilidad de comandos chkconfig.

Para realizar un listado de todos los servicios activos se debe de ejecutar el comando en el terminal:

$ chkconfig –list

Y el resultado será el que se muestra a continuación:

```
iptables        0:off   1:off   2:on    3:on    4:on    5:on    6:off
sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
sendmail        0:off   1:off   2:on    3:on    4:on    5:on    6:off
httpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
 ...             ...     ...     ...     ...     ...     ...     ...
 ...             ...     ...     ...     ...     ...     ...     ...
smb             0:off   1:off   2:off   3:off   4:off   5:off   6:off
squid           0:off   1:off   2:off   3:off   4:off   5:off   6:off
xinetd based services:
        chargen-udp:    off
        rsync:          off
        chargen:        off
          ...           ...
          ...           ...
        sgi_fam:        on
```

Los números del 0 al 6 que preceden a los dos puntos representan el nivel de ejecución del sistema donde los dos más importantes son el 3 y 5; si el sistema arranca en consola (sin interfaz gráfica) entonces se ejecuta en nivel 3 y viceversa si arranca una interfaz gráfica corre en nivel 5.

Para activar un servicio (por ejemplo squid) en los niveles de ejecución 2,3,4 y 5 ejecutaríamos (como root):

$ chkconfig --level 2345 squid on

Y para deshabilitar un servicio (por ejemplo sshd) en los niveles 3 y 5 ejecutaríamos (como root);

$ chkconfig --level 35 sshd off

Si no se sabe qué hace alguno de los servicios que se tenga activado se debe buscar información en internet o usar el comando man con el nombre del servicio como palabra clave (man -k).

El comando chkconfig activará/desactivará los servicios la próxima vez que se arranque la pc pero no tendrá ningún efecto hasta que reinicies. Bajo Linux RedHat Centos, se utiliza el comando service de la siguiente forma:

$ service nombre_servicio start

$ service nombre_servicio stop

$ service nombre_servicio restart

$ service nombre_servicio status

Donde:

- nombre_servicio será el que nos indique chkconfig --list.

Puedes ejecutar netstat -l después de deshabilitar todos los servicios innecesarios para asegurarte de que se ha acabado con todos (este comando comprueba qué sockets están escuchando esperando conexiones). Para cada uno de los servicios que aún estén ejecutándose, se debe de asegurar de que estén configurados correctamente (y de la forma más restrictiva posible) y que el cortafuego los proteja.

4.5. Buscar y borrar/modificar los ejecutables SUID/SGID innecesarios

El ejecutable SUID (set user ID, establecer identificador de usuario) o el SGID (set group ID, establecer identificador de grupo) es aquel que permite a un usuario ordinario ejecutarlo con privilegios mayores de los que tiene por defecto; por ejemplo el binario

passwd el cual, entre otras cosas, permite a un usuario normal cambiar su contraseña. Estas contraseñas están almacenadas en un archivo que solo puede ser alterado (y algunas veces leído) por el usuario root y, por lo tanto, los usuarios que no sean root no deberían ser capaces de cambiar sus contraseñas. Los permisos de acceso para este ejecutable son:

-r-s--x--x 1 root root 18992 Jun 6 2003 /usr/bin/passwd

Como puedes ver, el bit de dueño está establecido a 's' en lugar del 'x' normal, haciendo que el binario sea SUID; es decir, cuando un usuario ordinario ejecuta passwd, se ejecutará con los privilegios del dueño del archivo - en este caso el usuario root.

Muchos de los ejecutables SUID/SGID son necesarios, como el ejecutable passwd ya comentado. Sin embargo muchos otros no lo son. Los programas SUID/SGID pueden ser aprovechados por usuarios locales maliciosos para ganar privilegios en tu sistema. En el servidor de archivos se debe de ejecuta los siguientes comandos como root para encontrar todos estos ejecutables:

find / \(-perm -4000 -o -perm -2000 \)

o si se desea una lista más detallada:

find / \(-perm -4000 -o -perm -2000 \) -exec ls -ldb {} \;

Ahora se debe de recorrer cada uno de los elementos de la lista intentado reducir el número de los archivos cuyo dueño sea el usuario root o que estén en el grupo root a lo mínimo imprescindible bien borrando los binarios SUID/SGID innecesarios y/o borrando el bit SUID/SGID.

Los paquetes que contengan ejecutables SUID/SGID y que no vayas a usar pueden eliminarse buscando primero el paquete con, por ejemplo, rpm -q --whatprovides /usr/sbin/kppp y después desinstalándolo con rpm -e package-name.

El bit SUID/SGID puede eliminarse con chmod -s /usr/sbin/kppp. El ejecutable podrá iniciarse entonces por el usuario root cuando lo necesitemos.

4.6. Uso de las aplicaciones Logwatch Tripwire

A pesar de que el administrador del sistema haga todo lo que pueda para asegurar el sistema del servidor de archivos, en realidad por mucho que se empeñe nunca estará completamente seguro. Una mejor estrategia es cerciorarse de que el sistema ha sido comprometido y en el caso de que lo sea, cuándo.

Uno de los programa de detección de intrusos es Tripwire (http://www.tripwire.org/), el mismo comprueba los archivos del sistema de manera periódica para ver si alguno de ellos ha sido modificado. Si alguno se ha modificado y no debería haberlo sido, Tripwire generará un informe para que tomar decisiones según esta información. Tripwire requiere de un poco de tiempo para ser configurado de manera apropiada pero los resultados son muy satisfactorios.

CONCLUSIONES

Durante la realización del presente trabajo de grado se realizo diversos estudios y análisis a una entidad bancaria para diseñar una solución de vulnerabilidad en el servidor de archivos y basándose en los resultados del estudio se pueden hacer las siguientes aseveraciones:

Se han alcanzado con éxito todos los objetivos planteados al inicio del trabajo de grado, por lo cual se puede asegurar que el sistema de seguridad en el servidor de archivos Linux es igual a servidores que se asemejan en sus funciones y características, usan significativamente mayores recursos tecnológicos, económicos y humanos.

A partir de este análisis e investigación se pueden detectar errores y vulnerabilidades que pueden existir en entidades bancarias similares.

Para el correcto desempeño que se quiere obtener del servidor de archivos se debe cumplir las políticas de seguridad de la información que asegurarán que que no se vulnere la integridad de la información almacenada en el servidor de archivos para lograr una solida confianza, de parte de los socios o clientes, sobre la institución financiera.

BIBLIOGRAFÍA

Referencias bibliográficas

1. COLINA, Carlos. ISLAS C., OCTAVIO; COORD. ISLAS C., OCTAVIO; COORD.; (2005) Protección de datos personales en la sociedad de la información/ Internet y la sociedad de la información; v 2. CONFERENCIA. CIESPAL Quipus. Quito. 290 p. pp. 165-210. Es. Encuentros.

2. GONZÁLEZ ZUBIETA, José María. PIATTINI, Mario Gerardo; PESO NAVARRO, Emilio Del; COORD. (2001) Metodologías de control interno, seguridad y auditoría informática/ Auditoría informática: un enfoque práctico. México. 2 ed. 660 p. pp. 45-92. ilus., grafs., tabs. Es. Alfa omega.

3. NOVOA BERMEJO, Julio A. PIATTINI, Mario GERARDO; PESO NAVARRO, EMILIO DEL; COORD. (2001)Auditoría de técnica de sistemas/ Auditoría informática: un enfoque práctico. México. 2 ed. 660 p. pp. 335 - 360. ilus., grafs., tabs. Es. Alfa omega.

4. RAMOS GONZÁLEZ, Miguel Angel. PIATTINI, Mario Gerardo; PESO NAVARRO, Emilio Del; COORD. (2001)Auditoría de la seguridad/ Auditoría informática: un enfoque práctico. México. 2 ed. 660 p. pp. 389 - 422. ilus., grafs., tabs. Es. Alfa omega.

5. TACKETT, Jack; BURNETT, Steven; PAREDES, Beatriz. (2000). Linux 4 ed. 1069 p. Es.

6. TANENBAUM, Andrew S.; ESCALONA GARCÍA, Roberto; TRAD.; LEVINE GUTIÉRREZ, Guillermo; REV. TEC. (2003) Sistemas operativos modernos. México. 2 ed. 951 p. Ilus. gráf. Es. Pearson Educación.

Referencias electrónicas:

7. Linux firewall and security site, consultado: 25/04/2001, Disponible: http://www.linux-firewall-tools.com/linux/

8. Linux security, Consultado: 27/04/2011, Disponible: http//www.linuxsecurity.com

9. Security Focus, consultado: 27/04/2011, Disponible: http://www.securityfocus.com

10. RevistaLinux.net, Consultado 07/06/2011, Disponible: http://revistalinux.net/articulos/seguridad-basica-en-servidores-linux/