ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"ASEGURAMIENTO A INFRAESTRUCTURA DE INFORMACIÓN DE DATAWAREHOUSE DE EMPRESA DE TELECOMUNICACIONES"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentada por:

GONZALO ARTURO ARGUDO ALDAS

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTO

A Dios por llenarme de vida y permitirme terminar con esta etapa profesional. A mi familia por el apoyo brindado, de manera especial a mi esposa por su empuje y aliento a seguir. A mis padres por ser ejemplo a seguir con su constancia y a todos aquellos amigos y docentes que hicieron posible finalizar este reto profesional.

DEDICATORIA

El presente proyecto lo dedico a Clarisse, mi hija por darme su sonrisa, cariño que me ayudó mucho en todo este tiempo.

TRIBUNAL DE SUSTENTACIÓN

_____

MGS. LENIN FREIRE

PROFESOR DELEGADO POR LA UNIDAD ACADEMICA

_____

MGS JUAN CARLOS GARCÍA

PROFESOR DELEGADO POR LA UNIDAD ACADEMICA

RESUMEN

El presente documento nos brinda los pasos a seguir en la elaboración de un aseguramiento (“hardening”) a un equipo con Sistema Operativo Linux, puntualmente trabajaremos con la distribución, CentOS 6.

Este esquema para proteger los equipos que conforman la infraestructura donde se aloja la información que es administrada y generada por el Área de Datawarehouse, nos permitirá minimizar el riesgo de ser vulnerados ante un ataque a la infraestructura tecnológica, con esto tener la tranquilidad que la confidencialidad de los datos se cumplirá.

En el primer capítulo se describe el problema que hizo posible este trabajo, teniendo en cuenta que es un equipo nuevo que formará parte de la infraestructura del Área.

Siguiendo con el segundo capítulo se realiza el análisis de riesgos y el impacto en el negocio, que podría generar un ataque a nuestra infraestructura y las consecuencias en no brindar los servicios respectivos y el incumplimiento de tareas programadas.

Finalmente en el tercer capítulo se detalla los pasos recomendados por el Institute SANS, con el cual se llega a dejar nuestro equipo con los permisos necesarios, para los usuarios correspondientes dando cumplimiento al objetivo descrito en la solución del problema planteado en este trabajo.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

DNS	Domain Name System
IP	Internet Protocol
NFS	Network File System
SO	Sistema Operativo
TCP	Transmission control Protocol

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad un alto porcentaje de empresas han sido infectadas por algún malware o han sufrido algún ataque que podrían provocar situaciones que ponga en riesgo los activos de las mismas.

La mayoría de empresas grandes tienen muy claro la ventaja y la importancia de tener las seguridades debidas a los equipos físicos de los centros de cómputo, de una manera especial si en estos equipos, mantenemos el activo más importante y neurológico en el giro del negocio como es la información.

Por tal motivo, el hardware donde se aloje debe tener las seguridades recomendadas para estar lo menos expuesto posible, con esto evitar algún ataque que impida el buen uso de dicho equipo, o alguna situación tal como la pérdida, alteración de datos importantes, o la perdida de la confidencialidad, la cual pueda provocar algún impacto en la toma de decisiones y con esto algún retraso o pérdida del mercado.

CAPÍTULO 1

GENERALIDADES

1.1. Descripción del problema

El área de Datawarehouse, en la empresa, es un área relativamente nueva, en la cual se maneja, administra y almacena todos los datos de los sistemas transaccionales, información de clientes, facturación, tráfico y demás información del giro del negocio, la cual es vital precautelar la confidencialidad e integridad.

Desde esta área se genera reportes, cubos, Datamart los cuales sirven para el análisis y toma de decisiones para promociones y diversos reportes solicitados por el ente regulador, ya que se

maneja información como detalles de llamadas, celdas, duración, costos, nuevas activaciones, inactivaciones, etc.

Al ser la información el activo más importante de la empresa y la infraestructura en la cual reposa dicha información, no tiene mayor control por lo tanto está expuesta a cualquier evento que puede poner en riesgo la disponibilidad de la información, representando problemas legales y más aún el daño en la imagen de esta empresa.

1.2. Solución propuesta

Dada la situación presentada, se requieren la gestión de seguridad de la información basados en la confidencialidad de la información almacenada, es necesario realizar un aseguramiento (hardening) adecuado para precautelar dicho activo de la empresa y el uso de aplicaciones necesarias para la operación normal de la infraestructura.

El aseguramiento propuesto se basará en un análisis de riesgos de los servicios de dicha infraestructura para garantizar la seguridad de la información y minimizar los posibles riesgos.

Con este proyecto en cualquier empresa se puede realizar la implementación de un aseguramiento de su infraestructura a nivel

de sistema operativo, para garantizar múltiples servicios y obtención de información fidedigna para la toma de decisiones del giro del negocio y cumplimiento con requerimientos del ente regulador.

CAPÍTULO 2

GESTIÓN DEL RIESGO

2.1 Identificación de aplicaciones y servicios

En este equipo se almacena información muy sensible tanto para el cliente como para la empresa, con la cual se realizan Datamart, Cubos, Reportes para las diferentes áreas, con los cuales el área de Datawarehouse mantiene acuerdos de servicios donde se garantiza la confidencialidad de la información que se pueda generar.

Como aplicaciones tenemos los Datamart, entre los cuales y entre los más importantes podremos nombrar:

Facturación de Equipos,

Facturación de servicio

Cantidad de Abonados por Tecnología, Región, Subproductos.

Detalles de servicios usados llamadas, sms, internet y demás.

Activaciones nuevas.

Churn, Fidelización de clientes

2.2 Análisis de riesgos

El equipo al ser relativamente nuevo, no dispone de una protección adecuada y/o recomendada en lo que se refiere a su Sistema Operativo y por tal motivo es un riesgo latente el poder ser vulnerado o sufrir algún ataque que pueda imposibilitar su uso.

Se detalla la tabla de riesgos encontrados.

Tabla 1. Análisis Actual de Riesgo

#	Punto de revisión	Riesgo	Observación
1	Cd de boteo o rescate	SI	Tener cd de arranque
2	Sistema de Parches	SI	Actualización parches
3	Deshabilitar servicios no necesarios	SI	Todos los servicios activos
4	Verificar archivos críticos	SI	Estado de archivos críticos
5	Políticas de password	SI	Configuración de password
6	Limitar uso usando comando SUDO	SI	Configurar acceso vía sudo
7	Permitir solo al root acceso al Cron	SI	Configuración de ejecución cron
8	Banners de advertencia	SI	No hay banner de advertencia
9	Configuración de acceso remote ssh	SI	No hay reglas para ssh
10	Firewall basado en iptable	SI	No configurado firewall

#	Punto de revisión	Riesgo	Observación
11	Xinetd and inetdconf	NO	No se usa estos servicios
12	Tcpwrappers	NO	No se usa estos servicios
13	Sistemas de Logs	SI	Configurar sistema de log
14	Backups - Respaldos	SI	Configurar Shell de respaldos
15	Verificación de integridad de archivos	SI	No se cuenta con AIDE
16	Apache Security (all *nix)	NO	El equipo no será webserver
17	Apache Mod_security module	NO	El equipo no será webserver
18	Xwindow	NO	No hay interfaz gráfica
19	LIDS (Linux Intrusion Detection System)	NO	LIDS proyecto cerrado
20	Selinux (Security Enhanced Linux)	SI	Habilitar servicio
21	Seguridad en el mail	SI	Protección de servicio de email
22	Compartir Archivos	NO	No se comparte archivos
23	Encryption	SI	Para cifrar carpetas sensibles
24	Anti-Virus Protection	NO	No hay compartición de archivos
25	Bastille Linux	NO	Se usó instalación Minimal CentOS

CAPÍTULO 3

ASEGURAMIENTO DE LA INFRAESTRUCTURA

3.1 Arquitectura y características del Equipo

Las características del equipo sobre el cual vamos a trabajar es:

Tabla 2. Características del servidor.

Fabricante	HP
Tipo de Hardware	Server (Blade)
Modelo	ProLiat BL460c GenB
Procesador	Intel Xenon
Modelo	Core 2 Duo Procesor E8400 3 Ghz (10 cores)
Arquitectura de Procesador	x86_64
Memoria	66 GB

3.2 Evidencias del Aseguramiento realizado

Para realizar este Aseguramiento de la infraestructura del área de Datawarehouse, se siguieron las indicaciones del checklist de SANS Institute[1], con los cuales lograremos minimizar las vulnerabilidades de nuestros equipos.

A continuación se detallara punto a punto el checklist mencionado.

Punto 1. Boot and Rescue Disk

Se procede a sacar un cd de respaldo del sistema operativo CentOs 6.6, el cual nos servirá para arrancar el sistema operativo en caso de que un ataque origine la imposibilidad de acceder al equipo con el Sistema operativo instalado localmente. Con esto reducimos el riesgo atado a este vector.

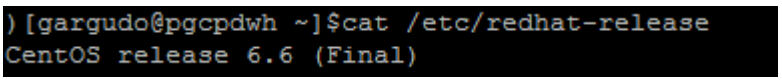


Figura 3.1 Sistema Operativo

Punto 2. System Patches

Utilizando el comando YUM (Yellowdog Linux Manager), con la opción update

```
[gargudo@pgcpdwh ~]$ yum update
```

Figura 3.1. Ejecución del comando yum

```
Resumen de la transacciÃ³n
================================================
=
Instalar       4 Paquete(s)
Actualizar     128 Paquete(s)
```

Figura 3.2. Resultado del comando yum

Mediante esta revisión se evidenció la necesidad de actualizar 128 paquetes, lo cual fue ejecutado, minimizando el riesgo de ataques por “bugs” de paquetes del sistema operativo.

Se recomienda actualizar los parches al menos 4 veces al año para mantener nuestro servidor seguro.

Como sugerencia del cheklist nos subscribimos a listas de noticias de seguridades

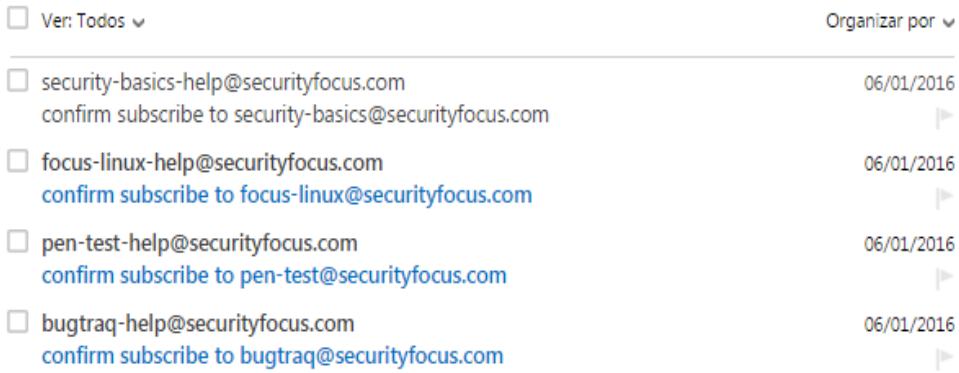
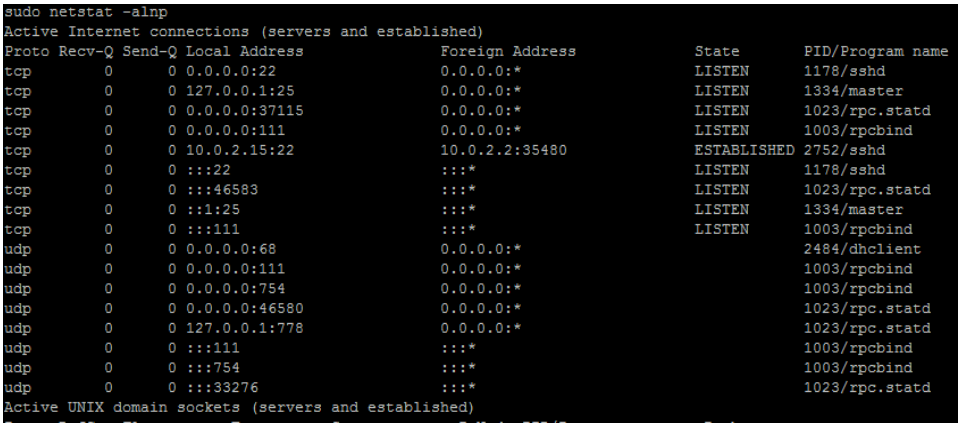


Figura 3.3. Subscripción a listas de noticias de securityfocus.com

Punto 3. Disabling Unnecessary Services

Deshabilitar los servicios innecesarios de tal manera que no existan medios posibles de ingreso al equipo, que no sean los estrictamente necesarios.

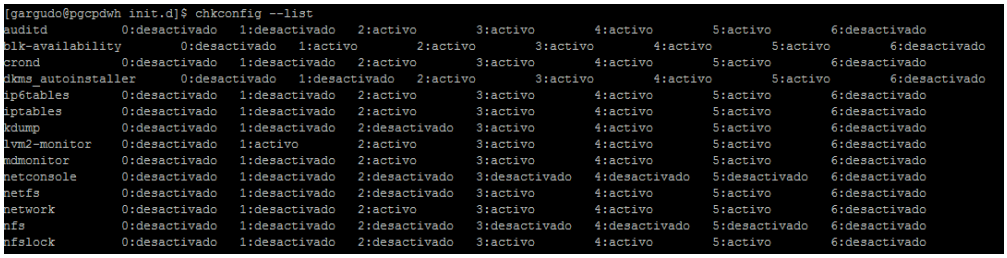
Con el comando netstat podemos ver los servicios que está escuchando nuestro equipo, se empieza el análisis de cual debe o no debe estar habilitado.



```
sudo netstat -alnp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      1178/sshd
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      1334/master
tcp        0      0 0.0.0.0:37115               0.0.0.0:*                   LISTEN      1023/rpc.statd
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN      1003/rpcbind
tcp        0      0 10.0.2.15:22                10.0.2.2:35480              ESTABLISHED 2752/sshd
tcp        0      0 :::22                       :::*                        LISTEN      1178/sshd
tcp        0      0 :::46583                    :::*                        LISTEN      1023/rpc.statd
tcp        0      0 ::1:25                      :::*                        LISTEN      1334/master
tcp        0      0 :::111                      :::*                        LISTEN      1003/rpcbind
udp        0      0 0.0.0.0:68                  0.0.0.0:*                               2484/dhclient
udp        0      0 0.0.0.0:111                 0.0.0.0:*                               1003/rpcbind
udp        0      0 0.0.0.0:754                 0.0.0.0:*                               1003/rpcbind
udp        0      0 0.0.0.0:46580               0.0.0.0:*                               1023/rpc.statd
udp        0      0 127.0.0.1:778               0.0.0.0:*                               1023/rpc.statd
udp        0      0 :::111                      :::*                                    1003/rpcbind
udp        0      0 :::754                      :::*                                    1003/rpcbind
udp        0      0 :::33276                    :::*                                    1023/rpc.statd
Active UNIX domain sockets (servers and established)
```

Figura 3.4. Ejecución del comando netstat

En este caso deshabilitaremos el que se está ejecutando en el puerto 37115, que es el proceso 1023, para este caso llegamos a la conclusión que es nfslock



```
[gargudo@pgcpdwh init.d]$ chkconfig --list
auditd          0:desactivado   1:desactivado   2:activo        3:activo        4:activo        5:activo        6:desactivado
blk-availability        0:desactivado   1:activo        2:activo        3:activo        4:activo        5:activo        6:desactivado
crond           0:desactivado   1:desactivado   2:activo        3:activo        4:activo        5:activo        6:desactivado
dkms_autoinstaller      0:desactivado   1:desactivado   2:activo        3:activo        4:activo        5:activo        6:desactivado
ip6tables       0:desactivado   1:desactivado   2:activo        3:activo        4:activo        5:activo        6:desactivado
iptables        0:desactivado   1:desactivado   2:activo        3:activo        4:activo        5:activo        6:desactivado
kdump           0:desactivado   1:desactivado   2:desactivado   3:activo        4:activo        5:activo        6:desactivado
lvm2-monitor    0:desactivado   1:activo        2:activo        3:activo        4:activo        5:activo        6:desactivado
mdmonitor       0:desactivado   1:desactivado   2:activo        3:activo        4:activo        5:activo        6:desactivado
netconsole      0:desactivado   1:desactivado   2:desactivado   3:desactivado   4:desactivado   5:desactivado   6:desactivado
netfs           0:desactivado   1:desactivado   2:desactivado   3:activo        4:activo        5:activo        6:desactivado
network         0:desactivado   1:desactivado   2:activo        3:activo        4:activo        5:activo        6:desactivado
nfs             0:desactivado   1:desactivado   2:desactivado   3:desactivado   4:desactivado   5:desactivado   6:desactivado
nfslock         0:desactivado   1:desactivado   2:desactivado   3:activo        4:activo        5:activo        6:desactivado
```

Figura 3.5.Verificación del comando chconfig -list

Vemos activo el programa nfslock en nivel 3 – 4- 5.

Luego procedemos a desactivar dicho programa.

```
[gargudo@pgcpdwh init.d]$ chkconfig --levels 345 nfslock off
```

Figura 3.6. Comando que nos permite deshabilitar el programa nfslock

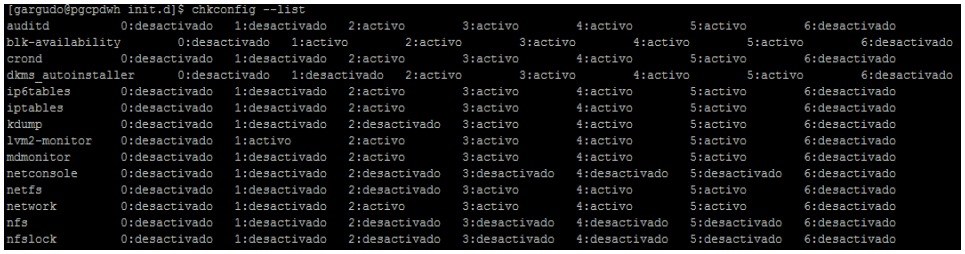


Figura 3.7. Programa nfslock Desactivado

Se detalla los servicios encontrados, el status encontrado y status final

Tabla 3. Servicios encontrados al iniciar y el estatus final que se dejará

				STATUS	STATUS FINAL
tcp	0.0.0.0:22	LISTEN	1178/sshd	Mantener	Se mantiene
tcp	127.0.0.1:25	LISTEN	1334/master	Mantener	Se mantiene
tcp	0.0.0.0:37115	LISTEN	1023/rpc.statd	Deshabilitar	Deshabilitado
tcp	0.0.0.0:111	LISTEN	1003/rpcbind	Deshabilitar	Deshabilitado
tcp	:::22	LISTEN	1178/sshd	Deshabilitar	Deshabilitado
tcp	:::46583	LISTEN	1023/rpc.statd	Deshabilitar	Deshabilitado
tcp	::1:25	LISTEN	1334/master	Deshabilitar	Deshabilitado
tcp	:::111	LISTEN	1003/rpcbind	Deshabilitar	Deshabilitado
udp	0.0.0.0:111		1003/rpcbind	Deshabilitar	Deshabilitado
udp	0.0.0.0:754		1003/rpcbind	Deshabilitar	Deshabilitado
udp	0.0.0.0:46580		1023/rpc.statd	Deshabilitar	Deshabilitado
udp	127.0.0.1:778		1023/rpc.statd	Deshabilitar	Deshabilitado
udp	:::111		1003/rpcbind	Deshabilitar	Deshabilitado
udp	:::754		1003/rpcbind	Deshabilitar	Deshabilitado
udp	:::33276		1023/rpc.statd	Deshabilitar	Deshabilitado

Punto 4. Check for Security on Key Files

Verificar que ciertos archivos importantes del sistema operativo tengan ciertos tipos de permisos y de usuario, para salvaguardar el mal uso que un intruso o usuario visitante pueda realizar sobre archivos críticos del sistema operativo.

Se detalla la verificación de los archivos indicados, se los encontró como lo sugiere este punto, no se realiza ningún cambio.

Tabla 4. Verificación de permisos de rutas indicadas

	Verificación
/etc/fstab: usuario root y permisos (-rw-r--r--) (644)	OK
/etc/passwd, /etc/shadow /etc/group usuario root	OK
/etc/passwd , /etc/group permisos (rw-r--r--) (644)	OK
/etc/shadow permisos (r--------) (400)	OK

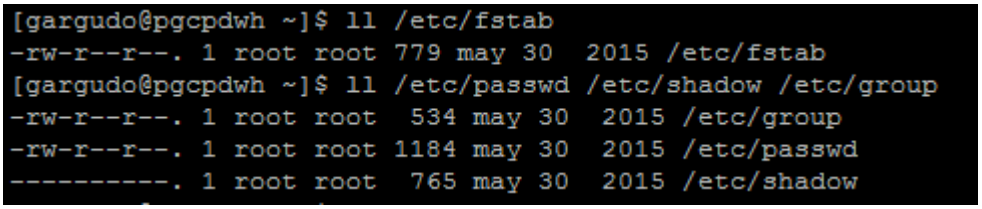


Figura 3.8.Permisos encontrados en el equipo

Punto 5. Default Password Policy

Se toma como referencia los tiempos recomendados en este punto y se procede a configurar las políticas mínimas necesarias para el manejo de claves a nivel de sistema operativo.

En este archivo se configura 4 tiempos.

- ✓ El máximo de días que sea válido el password
- ✓ El mínimo número de días permitidos entre cada cambio de password
- ✓ Longitud mínima aceptada para cada vez que se cambie el password
- ✓ Número de días de aviso antes que el password actual expire

El archivo que se configura es login.defs en la ruta /etc/

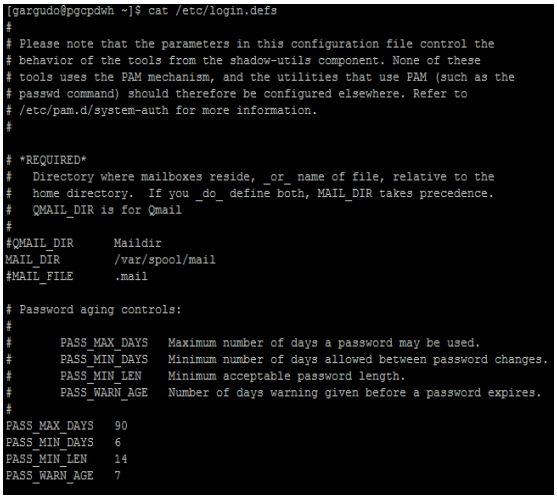


Figura 3.9. Archivo donde se configura las políticas de password sugeridas

Punto 6. Limit root access using SUDO

Limitar el acceso de root utilizando el comando SUDO[3], el uso de SUDO permite al administrador del sistema operativo en este caso CentOS, dar el acceso a usuarios o grupos a determinados programas o aplicaciones que de otra manera no podrían utilizar, para esto ya no sería necesario conocer la clave de root.

Para que un usuario normal pueda ejecutar debe constar en el archivo /etc/sudoers

Al usar la instalación minimal de centOS viene por default este acceso limitado.

```
[gargudo@pgcpdwh ~]$ sudo ls /etc/sudoers.d/
gargudo
```

Figura 3.10. En archivo sudoers.d se le da permiso de root al usuario gargudo

Punto 7. Only allow root to access CRON

El acceso al cron de nuestro equipo limitarlo para que solo pueda tener acceso el usuario root, de esta forma precautelamos que ningún usuario no autorizado ejecute tareas periódicas en el equipo, sin previa revisión y autorización del administrador del mismo.

Se procede con la edición del archivo cron.allow, dejando como único usuario al root, dando también los permisos indicados.

```
[gargudo@pgcpdwh etc]$ sudo vi cron.allow
[gargudo@pgcpdwh etc]$ cat cron.allow
root
[gargudo@pgcpdwh etc]$ ll cron.allow
-rw-r--r--. 1 root root 5 ene  6 22:53 cron.allow
[gargudo@pgcpdwh etc]$ sudo chmod 400 cron.allow
[gargudo@pgcpdwh etc]$
[gargudo@pgcpdwh etc]$
[gargudo@pgcpdwh etc]$
[gargudo@pgcpdwh etc]$ ll cron.allow
-r--------. 1 root root 5 ene  6 22:53 cron.allow
```

Figura 3.11. Configuración de archivo cron.allow para root único acceso permitido

Punto 8. Warning Banners

Nos sugiere que nuestro equipo debe contener unos banners de alerta a lo que algún usuario se conecte, de tal forma que el usuario sepa que política y procedimiento estará violentando al ingresar sin contar con las debidas autorizaciones.

Se verifica existan los siguientes archivos.

/etc/motd /etc/issue /etc/issue.net

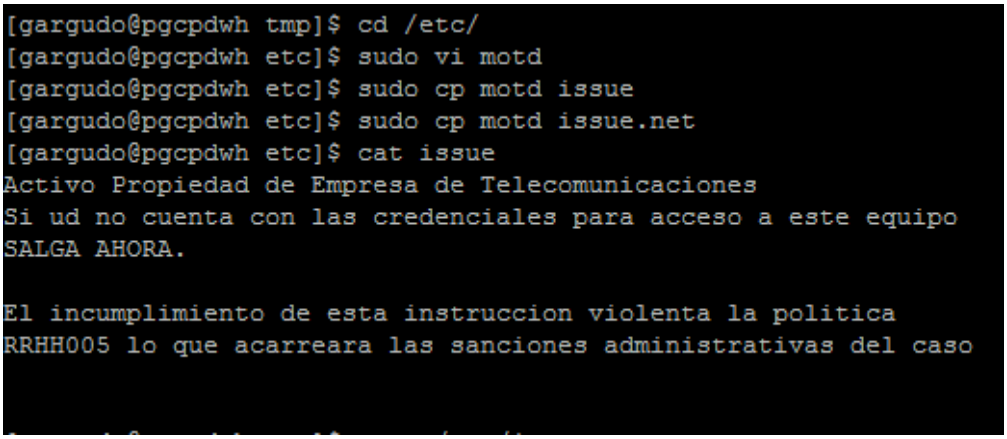


Figura 3.12.Verificación de archivos y creación del Banners de advertencia

Punto 9. Remote Access and SSH Basic Settings

Se procede a configurar el archivo sshd_config [5] para de acuerdo a esto permita la ejecución del ssh, bajo las sugerencias indicadas, mencionamos las siguientes

Tabla 5. Configuración archivo sshd_config

Protocol	2
PermitRootLogin	no
PermitEmptyPasswords	no
Banner	/etc/issue
IgnoreRhosts	yes
RhostsAuthentication	no
RhostsRSAAuthentication	no
HostbasedAuthentication	no
LoginGraceTime	1m
SyslogFacility	AUTH
AllowUser	gargudo, gsioper, lbeltran
DenyUser	monitor
MaxStartups	10

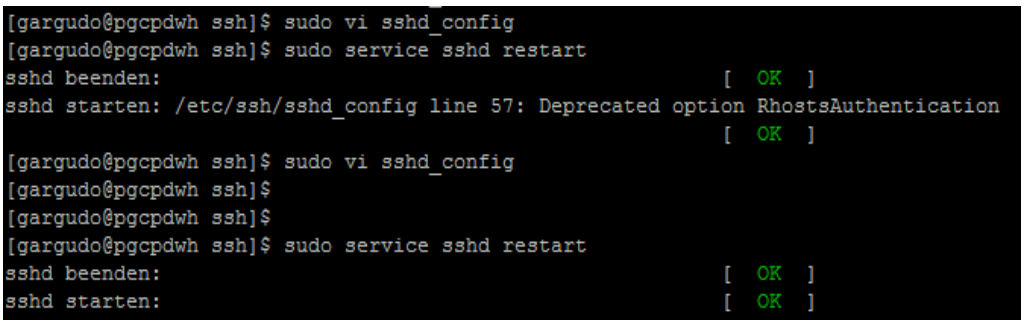


Figura 3.13. Se resetea el servicio de sshd para la actualización de configuración

Punto 10. Host-based Firewall Protection with iptables

Implementar un firewall en este equipo basado en iptables[4], con el cual proteger el equipo para accesos no autorizados a nivel de red. Con el comando iptables configuraremos las reglas de seguridad en entrada a este equipo (INPUT).

Anteriormente se configuro para que ssh, solo lo pueda ejecutar por ciertos usuarios, con esto tenemos la protección a nivel de protocolo, con iptables, aparte de filtrado por usuario también lo haremos a nivel de IP, con esto por ejemplo tendremos más filtros para realizar ssh, que sea versión 2, por los usuarios definidos y además por las IP configuradas en este punto, con esto cada vez es más seguro y menos probable algún ingreso no permitido.

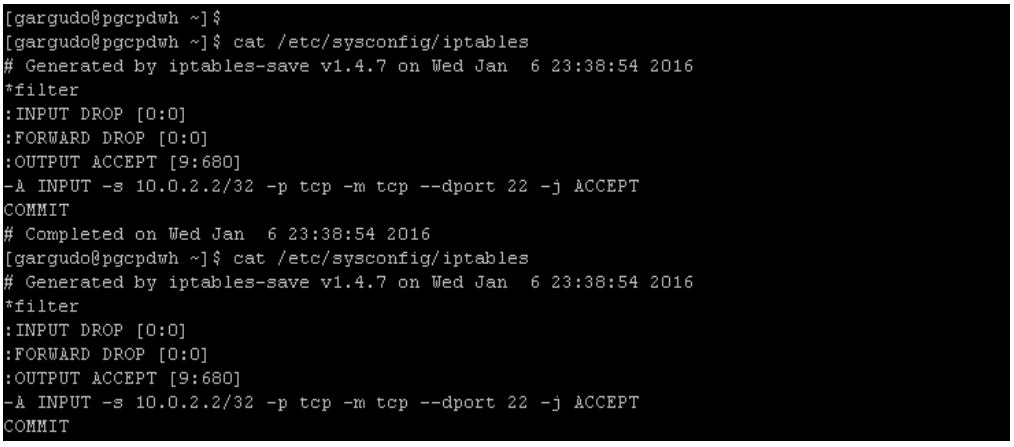


Figura 3.14. Configuración de iptables

Punto 11. Xinetd and inetd.conf

No aplicaría por que no se está utilizando estos servicios, ya que no hay servicios que publicar a excepción del ssh, que se configuro en el punto 9.

Punto 12. tcpwrappers

No aplicaría por que no se está utilizando Xinetd, ya que la protección se la realiza a nivel de iptables.

Punto 13. System Logging

Para cumplir este punto se procede a configurar logwatch en el servidor de logs que es donde direccionamos todos los logs importantes de este equipo.

En caso de algún ataque lo primero que será modificado o eliminado son los logs que es donde se registra todo lo ejecutado en nuestro equipo, por tal motivo la recomendación en este punto es replicar a otro servidor los logs importantes para tener como respaldo.

Hacemos uso del comando yum para realizar la búsqueda de logwatch

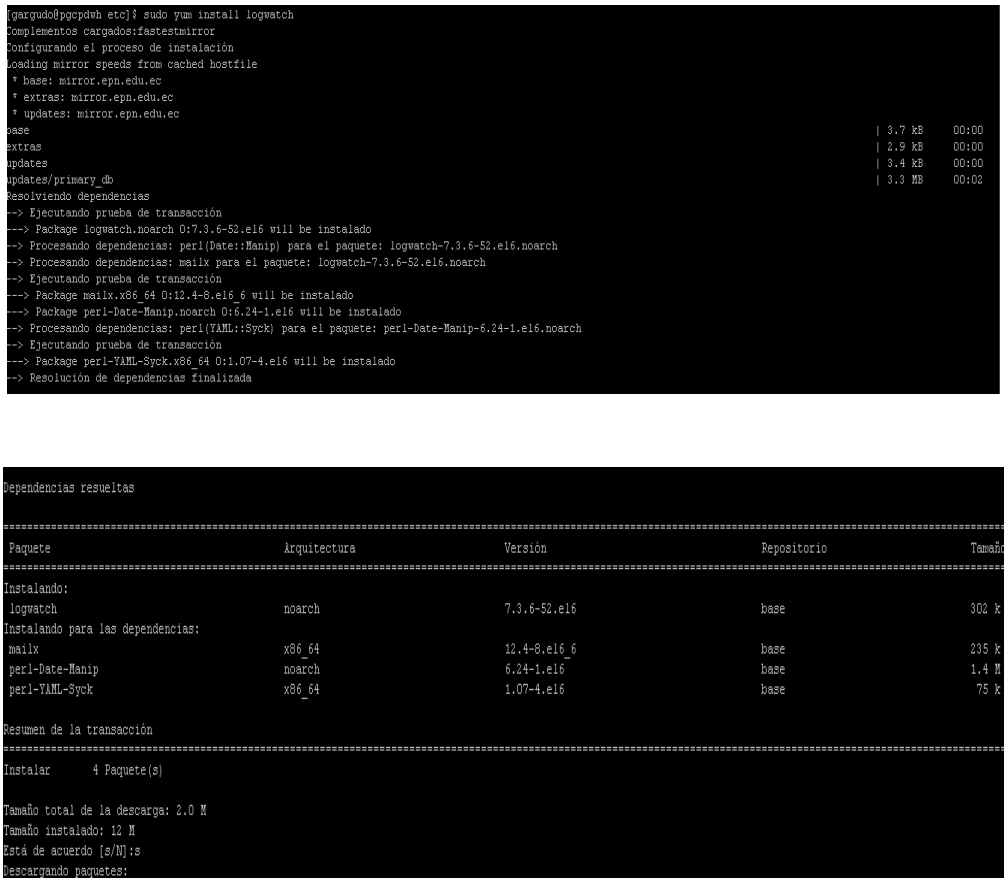


Figura 3.15.Uso del comando yum para la búsqueda de programa logwatch

Procedemos a instalarlo y configurar con el siguiente comando

sudo logwatch --detail Low --mailto root --service all --range today

Punto 14. Backups

Dado que en este equipo se aloja la información en bases de datos, se deja una política de respaldo para la misma

Lo cual seguirá el mismo estándar de los otros equipos, que los respaldos de base y sistema operativo, serán diarios, ya que en caso de vulneración de la información del equipo, el único punto de recuperación será desde los respaldos los cuales se los garantiza en este punto.

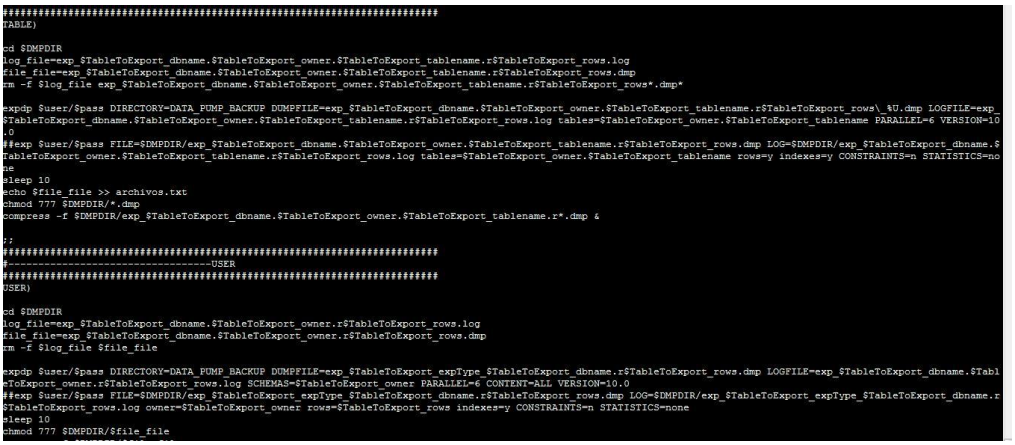


Figura 3.16. Shell para respaldo de base de datos

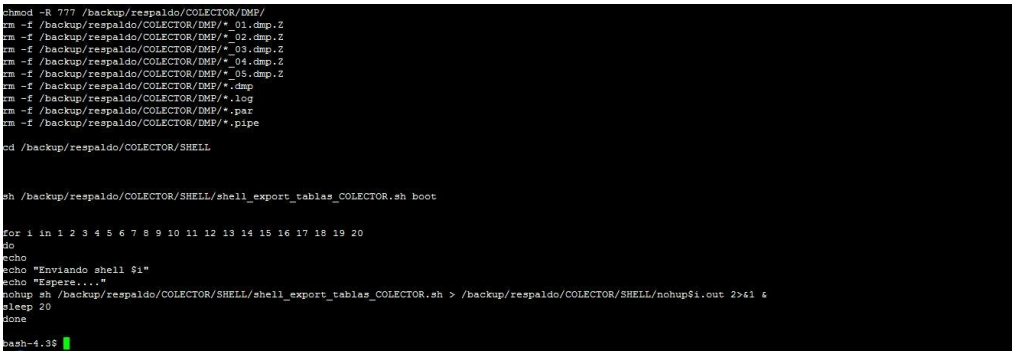


Figura 3.17. Shell para respaldos diarios

Punto 15. Integrity-checking Software

Se utilizara el producto AIDE[2] con el cual podremos monitorear el estado de los archivos críticos del sistema, realizando comparaciones periódicas, que certifiquen que los archivos críticos del sistema operativo no han sido modificados.

Utilizamos el comando yum para la búsqueda de AIDE.

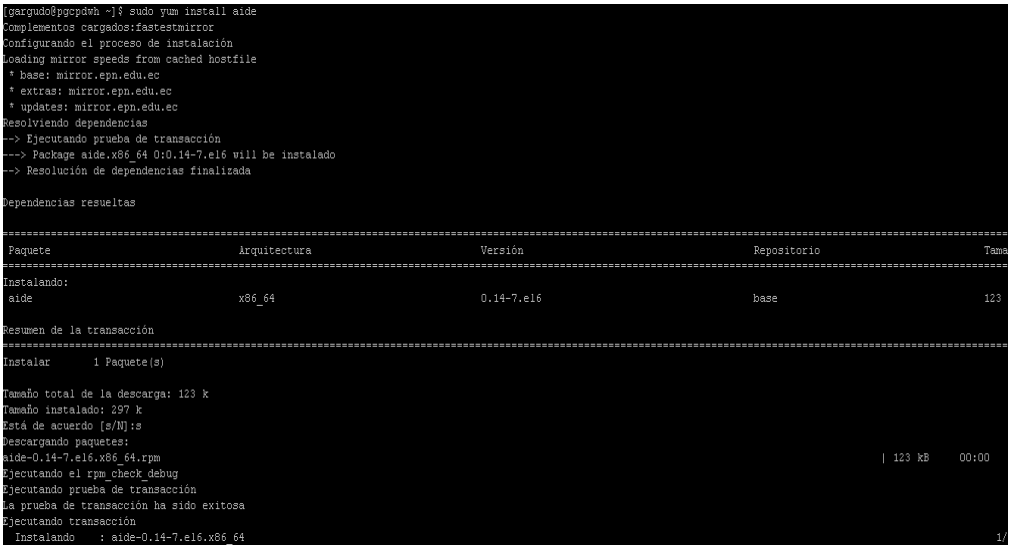


Figura 3.18. Uso del comando yum para la búsqueda de programa AIDE

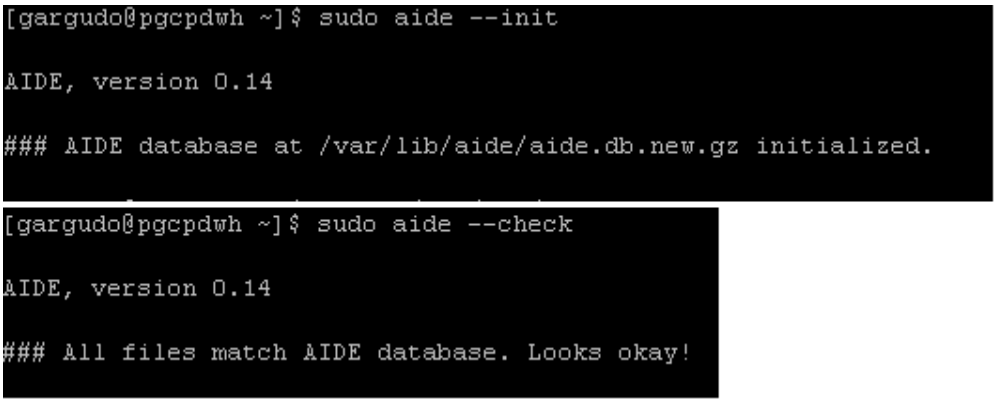


Figura 3.19. Inicialización de AIDE

Punto 16. Apache Security (all *nix)

Este punto que nos indica seguridad sobre el producto apache, en este caso no aplicaría para este equipo, pues no se utilizará como webserver.

Punto 17. Apache Mod_security module

Este punto que nos indica seguridad sobre el producto apache, en este caso no aplicaría para este equipo, pues no se utilizará como webserver.

Punto 18. Xwindow

Este punto no aplica en este equipo pues no tendrá interfaz gráfica, por políticas de seguridad

Punto 19. LIDS (Linux Intrusion Detection System)

No aplica, LIDS proyecto cerrado en 2013. SELinux del punto 20 cubre todo lo de LIDS y mas

Punto 20. Selinux (Security Enhanced Linux)

Al momento del aseguramiento de este equipo no se pudo habilitar por incompatibilidad con la base que se maneja, Oracle 11g

Punto 21. Email Security

En la parte de seguridad sobre el email, está seguro pues solo escucha en localhost /127.0.0.1 , evitando el uso mal intencionado del servicio de correo por otros usuarios de la red.

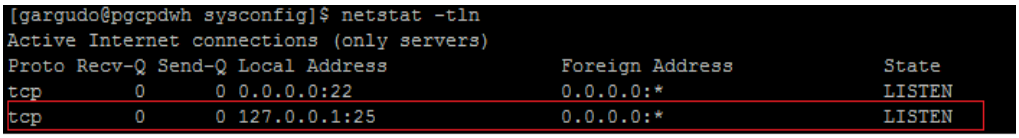


Figura 3.20. El equipo solo escucha los mail internos

Punto 22. File Sharing

Este equipo no servirá para compartir archivos, por lo tanto no se instalara samba, ni NFS Server (NFS client se lo deshabilitó)

Punto 23. Encryption

Cifrar los directorios que contengan información sensible, para esto usamos el producto encfs.

Punto 24. Anti-Virus Protection

Esta recomendación, no aplicaría pues, ya que no hay compartición de archivos, como se mencionó anteriormente no se instalará samba para comparticiones con equipos Windows que son los potenciales transmisores de virus.

Punto 25. Bastille Linux

Para la instalación de este servidor se utilizó CentOS Minimal para el sistema Operativo base y por lo tanto muchas no aplican como DNS, printing, entre otras.

CONCLUSIONES Y RECOMENDACIONES

1. La seguridad de la información, es algo muy serio a considerar dentro de una empresa, requiere darle la importancia necesaria, sea contratando expertos o a una empresa dedicada a ello, con esto se evitarán baja de productividad, mayores costos operativos, pérdida de información y de dinero y se conseguirá continuidad en el negocio con una máxima seguridad.

2. Con el “Hardnenig” realizado en este servidor se ha ganado la tranquilidad que en nuestro equipo se podrán realizar los procesos necesarios, por los usuarios adecuados, manteniendo un historial de log de todos los eventos que se registren.

3. El aseguramiento o también conocido como hardening debería ser una práctica dentro de las políticas de seguridad informática.

BIBLIOGRAFÍA

[1] Institute SANS, Security Consensus Operational Readiness Evaluation

http://www.sans.org/media/score/checklists/linuxchecklist.pdf

[2] AIDE

http://www.jsitech.com/linux/aide-y-como-instalarlo-en-linux-centosrhelfedora/

[3] SUDO

http://www.cloverte.com/news/21/83/Como-permitir-a-un-usuario-el-acceso-a-sudo-en-CentOS-6.html

[4] IPTABLES

https://wiki.archlinux.org/index.php/Iptables_(Espa%C3%B1ol)

[5] CONFIGURACION SSH

http://www.comoinstalarlinux.com/centos-ssh-para-acceder-a-tu-servidor-linux/