ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"ASEGURAMIENTO DE SISTEMA OPERATIVO RED HAT 6.6 ENTERPRISE PARA CUMPLIMIENTO DE NORMATIVA PCI DSS 3.0"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del Título de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por

PEDRO JOSÉ ROBLES TOMALÁ

Guayaquil – Ecuador

2015

AGRADECIMIENTO

Mi agradecimiento a Dios por permitirme llegar hasta este momento tan importante de mi carrera, María por su guía de toda una vida, a mis padres, hermanos, mi sobrino, mi niña, familia y amigos que estuvieron pendientes en todo momento del resultado de este proyecto.

Al Ing. Lenin Freire por el apoyo y la invitación a formar parte de este grupo.

Y muy particularmente a aquellos que creyeron posible el que pueda llegar hasta aquí y me siguen apoyando en cada paso y decisión de mi vida, a todos ellos mi cariño y lo que con este proyecto pueda lograr. Va por cada uno de ellos. G.I, E.R, F.G. P.R, C.T y S.G.

QCD? YDDD? YDDM?

DEDICATORIA

A Dios en primer lugar y a María por su compañía incondicional.

Dedico este regalo de Dios a tres personas muy importantes que siempre estuvieron conmigo y estarán sobre todo en mi corazón, Gustavo Robles, Raúl Tomalá y Carmen Ruiz, mi motivación para seguir adelante cada día buscando honrarlos con cada acción por todo lo que me han enseñado.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenín Freire
DIRECTOR DEL MSIA

Mgs. Laura Ureta
PROFESOR DELEGADO
POR LA UNIDAD ACADÉMICA

Mgs. Albert Espinal
PROFESOR DELEGADO
POR LA UNIDAD ACADÉMICA

RESUMEN

Como objetivo de este trabajo, se desea realizar el aseguramiento del sistema operativo LINUX en su distribución Red Hat versión 6.6 Enterprise a ser utilizado para un servidor que cumple con la función de switch transaccional en una empresa que presta servicios de interconexión de instituciones financieras.

Como antecedentes al proyecto, tenemos que la normativa PCI DSS dentro de su versión 3.0 incluyó el aseguramiento de la plataforma operativa como un requerimiento primario dentro de su auditoria tanto de certificación como de cumplimiento para la renovación anual.

Con este proyecto, la empresa podrá contar con una plataforma operativa aprobada por el ente certificador y sus QSA’s (Asesores de calidad autorizados) responsables de realizar la validación.

Con ello lograremos que la empresa cuente con el nivel requerido de seguridad, que permitirá que su credibilidad tanto a nivel nacional como internacional crezca

y permanezca siendo considerada una de las más fuertes en el mercado de switches transaccionales.

ÍNDICE GENERAL

ABREVIATURAS

PCI DSS	Estándar de Seguridad de Datos para Industria de Tarjetas de Crédito
QSA	Consultor de Calidad de Seguridad
SSH	**I**ntérprete de Órdenes Seguro
PAM	Mecanismo de Autenticación Flexible
NFS	Sistema de Archivos de Red
RPC	Llamada a Procedimiento Remoto
TELNET	Red de Telecomunicaciones
RSH	Intérprete de Órdenes Remoto
TFTP	Protocolo de Transferencia de Archivos Trivial
UDP	Protocolo de Intercambio de Datagramas
TCP	Protocolo de Control de Transmisión
NIS	Servicio de Información de Red
DHCP	Protocolo de Configuración Dinámica de Host
LDAP	Protocolo Ligero de Acceso a Directorios

NTP	Protocolo de Tiempo de la Red
DNS	Sistema de Nombres de Dominio
FTP	Protocolo de Transferencia de Archivos
HTTP	Protocolo de Transferencia de Hipertexto
SMNP	Protocolo Simple de Administración de Red
IP	Protocolo de Internet
ICMP	Protocolo de Mensajes de Control de Internet
SYN	Bit de Control del Segmento TCP

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Se adquirió un servidor HP con una solución que requiere una plataforma operativa LINUX, por lo que se solicitó la evaluación de los sistemas operativos que aplican para soportar operativamente dicha aplicación, por lo que la recomendación fue de utilizar un sistema operativo REDHAT LINUX en su versión aprobada más actualizada para empresas que es la 6.6 [1].

Dentro del proceso de preparación del servidor, se procedió con la instalación de la aplicación previo al versionamiento con la finalidad de validar la correcta transaccionalidad del mismo, se verificó que se cumplió con el funcionamiento correcto según fue indicado por el proveedor externo responsable de la preparación de los ambientes.

Con los resultados obtenidos, se solicitó el aseguramiento del sistema operativo del servidor luego de la ejecución del demo de pruebas, motivo por el cual se inició este proyecto y del cual se espera obtener el mejor resultado con respecto al cumplimiento de la normativa.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

En el campo financiero, la seguridad de la información se ha convertido en el punto más crítico para todas las instituciones que lo integran, tanto instituciones privadas como públicas en la actualidad se encuentran realizando arduos trabajos para garantizar la seguridad de sus clientes y por medio de esto atraer la atención del mercado.

Basándonos en las estadísticas, los índices de fraude se han visto incrementados, por lo que la mayoría de instituciones financieras están optando por implementar mecanismos que les permitan minimizar el riesgo sobre las transacciones que en ellas se realiza, de ahí la concepción de este proyecto.

1.2 Objetivo General.

Realizar el aseguramiento del sistema operativo Red Hat 6.6 Enterprise de un servidor transaccional orientado al cumplir requerimientos propuestos dentro de la normativa PCI/DSS 3.0. [2].

1.3 Objetivo Específico

Detallar los pasos para la efectiva implementación del aseguramiento del sistema operativo para que se cumpla con los requerimientos indicados en la normativa

PCI/DSS 3.0, confirmando que no se afecte la transaccionalidad soportada por sus aplicativos.

1.4 Descripción del Problema

Actualmente, en nuestro medio existen un sinnúmero de casos en los que hemos podido evidenciar fraudes realizados tanto por personal interno como externo a las instituciones financieras. Por ello la Superintendencia de Bancos y Seguros del Ecuador (SBS) se vio en la necesidad de incluir dentro de sus resoluciones una normativa que detalla que las instituciones financieras sujetas a ella, deben cumplir con un conjunto de consideraciones de seguridad básicas, las cuales están incluidas en la normativa PCI DSS, brindando mayor seguridad y confianza a todos los usuarios de la banca ecuatoriana. Esta normativa se extiende hasta el desarrollo de soluciones que cuenten con los estándares de seguridad implementados en muchas instituciones financieras de nivel mundial.

Los sistemas operativos que se encuentran en el mercado cuentan con un nivel de seguridad mediano, el cual se encuentra en riesgo de ser atacado si no se encuentra debidamente asegurado.

Las normativas internacionales, siendo en este caso particular la PCI/DSS en su versión 3.0, han presentado a sus acreditados un nivel mínimo recomendado de seguridad dentro de sus plataformas tecnológicas para mantener dicha certificación, por lo que la empresa se ve en la necesidad de realizar este aseguramiento ya que el equipo en mención se considera dentro del dominio de la norma dado que por el fluye información sensible.

1.5 Solución Propuesta

Se recomienda el aseguramiento del sistema operativo indicado, siendo en este caso RED HAT LINUX en su versión 6.6 Enterprise [4].

Este aseguramiento permitirá que tanto archivos de configuración como la información contenida en el mismo, al igual que la comunicación con los equipos a los que por medio de este se accede, cuenten con la configuración de seguridad idónea que nos permita el bloqueo de comunicación, enmascaramiento de datos y control de acceso restringido sin que este afecte a la transaccionalidad que se soporta.

Dentro de las opciones a utilizarse tomamos en consideración los siguientes puntos:

- Análisis del sistema operativo previo a la implementación.
- Ubicación de los archivos de configuración.
- Reconfiguración de accesos de usuarios.
- Control de acceso y de sesiones.
- Configuración de redes y enlaces de comunicación.
- Configuración de puertos y red.
- Deshabilitación de servicios.

1.6 Términos y Acuerdos

El proyecto se limita a la realización del aseguramiento del sistema operativo Red Hat en su versión 6.6 Enterprise instalado para el servidor transaccional, cubriendo con los requerimientos básicos solicitados por la entidad certificadora de la normativa PCI DSS v. 3.0 sobre los sistemas operativos Linux.

.

CAPÍTULO 2

Levantamiento de información del equipo

Este capítulo contiene el detalle de los procedimientos realizados mostrando sus respectivos resultados sobre la auditoría realizada al equipo sobre el que se está trabajando.

La información aquí obtenida es de suma importancia, ya que en base a ella se definirá el plan de acción al igual que el cronograma de trabajo que se presentará al cliente para completar con el requerimiento.

2.1. Auditoria de Seguridad Recomendada PCI/DSS 3.0

Dentro de la última actualización (versión 3.0), PCI DSS establece una serie de mejoras que deben ser consideradas para cada sistema operativo sobre el cual se recibirá transacciones que lleven números de tarjetas tanto de débito como de crédito.

Para poder determinar que configuraciones deben aplicarse en el sistema operativo, es conveniente en primer lugar, realizar una auditoría del mismo, la cual nos permita evaluar cada una de las vulnerabilidades y su mecanismo de remediación.

Las consideraciones que se deben tener en cuenta para el proceso de auditoria cubren los siguientes campos detallados a continuación:

- Actualizaciones y parches instalados
- Servicios del sistema operativo
- Servicios de propósitos especiales
- Configuración de red y firewall
- Logs y Auditoría
- Acceso a sistema, autenticación y autorización
- Cuentas de usuario y ambiente

- Banners de advertencia
- Mantenimiento del sistema

De las validaciones previas realizadas sobre el servidor, se pudo acordar, con el QSA asignado a la cuenta, los siguientes dominios, que contendrían todos los puntos requeridos para el cumplimiento de la norma según sus especificaciones, sin afectar el funcionamiento correcto de la herramienta:

1. Remover servicios por defecto
2. Servicios de propósitos especiales
3. Configuración de red y firewall
4. Protocolos de red poco comunes
5. Logs del sistema
6. Configuración SSH
7. Configuración PAM [3]
8. Cuentas de usuario y ambientes
9. Banners de advertencia

2.2. Recopilación detalle de vulnerabilidades encontradas

Se procedió con la revisión de los puntos indicados previamente, de los cuales obtuvimos los siguientes resultados:

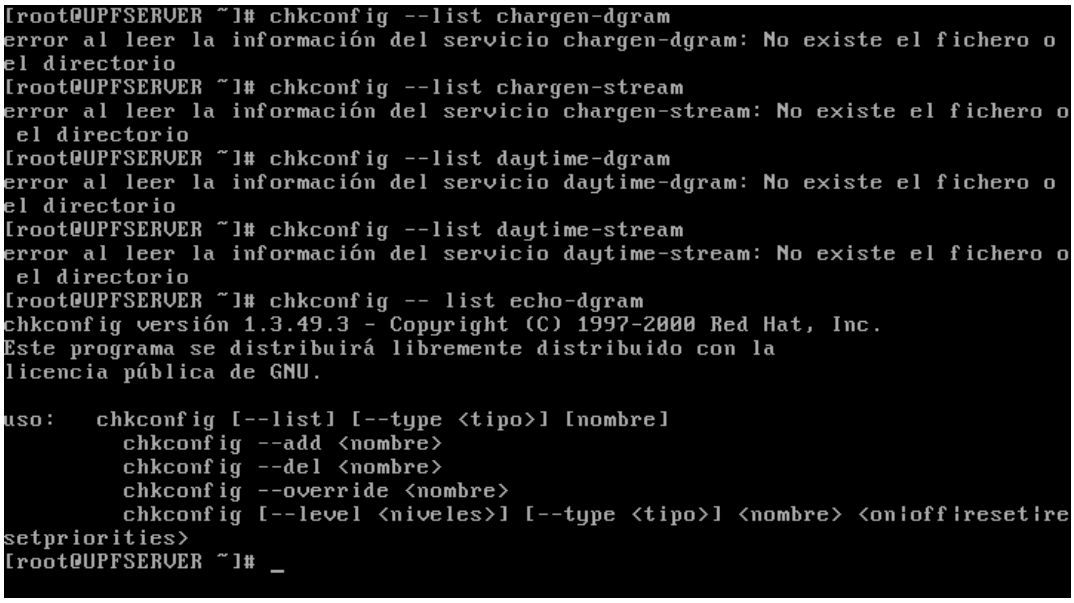

Figura 2.1: Verificación de configuraciones datagram por defecto.

```
[root@UPFSERVER ~]# chkconfig -- list echo-stream
chkconfig versión 1.3.49.3 - Copyright (C) 1997-2000 Red Hat, Inc.
Este programa se distribuirá libremente distribuido con la
licencia pública de GNU.

uso:   chkconfig [--list] [--type <tipo>] [nombre]
         chkconfig --add <nombre>
         chkconfig --del <nombre>
         chkconfig --override <nombre>
         chkconfig [--level <niveles>] [--type <tipo>] <nombre> <on|off|reset|re
setpriorities>
[root@UPFSERVER ~]# chkconfig --list tcpmux-server
error al leer la información del servicio tcpmux-server: No existe el fichero o
el directorio
[root@UPFSERVER ~]# _
```

Figura 2.2: Verificación de configuración echo-stream

```
[root@UPFSERVER ~]# grep umask/etc/sysconfig/init
^C
[root@UPFSERVER ~]# rpm -q xorg-x11-server-common
el paquete xorg-x11-server-common no está instalado
[root@UPFSERVER ~]# chkconfig --list avahi-daemon
error al leer la información del servicio avahi-daemon: No existe el fichero o e
l directorio
[root@UPFSERVER ~]# chkconfig --list cups
cups            0:desactivado   1:desactivado   2:activo        3:activo        4
:activo 5:activo        6:desactivado
[root@UPFSERVER ~]# rpm -q dhcp
el paquete dhcp no está instalado
[root@UPFSERVER ~]# grep "restrict default" /etc/ntp.conf
restrict default kod nomodify notrap nopeer noquery
[root@UPFSERVER ~]# grep "restrict-6 default" /etc/ntp.conf
[root@UPFSERVER ~]# grep "restrict-6 default" /etc/ntp.conf
[root@UPFSERVER ~]# grep "ntp:ntp" /etc/sysconfig/ntpd
# Drop root to id 'ntp:ntp' by default.
OPTIONS="-u ntp:ntp -p /var/run/ntpd.pid -g"
[root@UPFSERVER ~]# rpm -q openldap-servers
el paquete openldap-servers no está instalado
[root@UPFSERVER ~]# rpm -q openldap-clients
el paquete openldap-clients no está instalado
[root@UPFSERVER ~]# _
```

Figura 2.3: Verificación de configuraciones para máscara por defecto

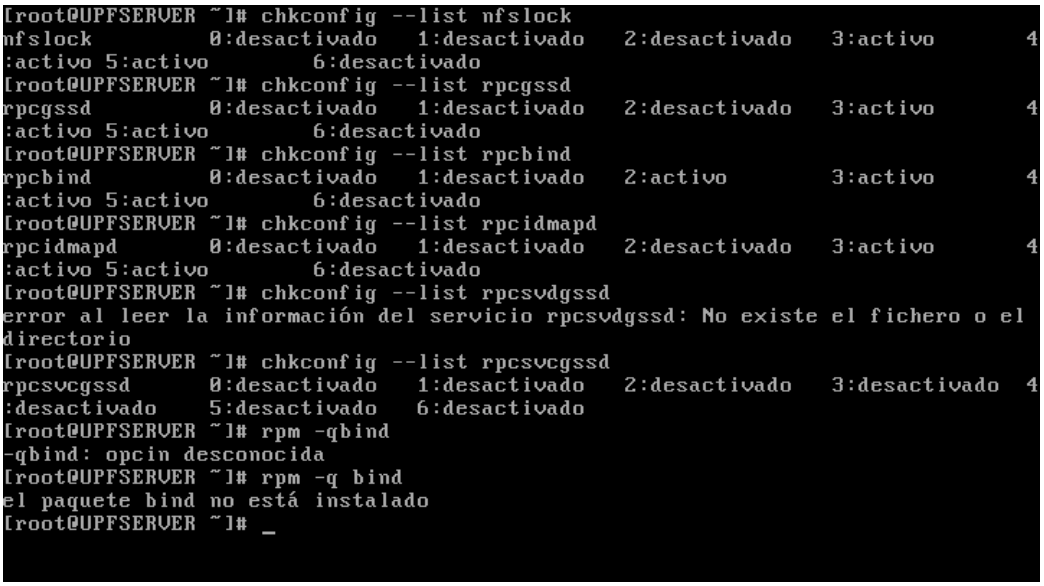

Figura 2.4: Verificación de configuraciones NFS y RPC

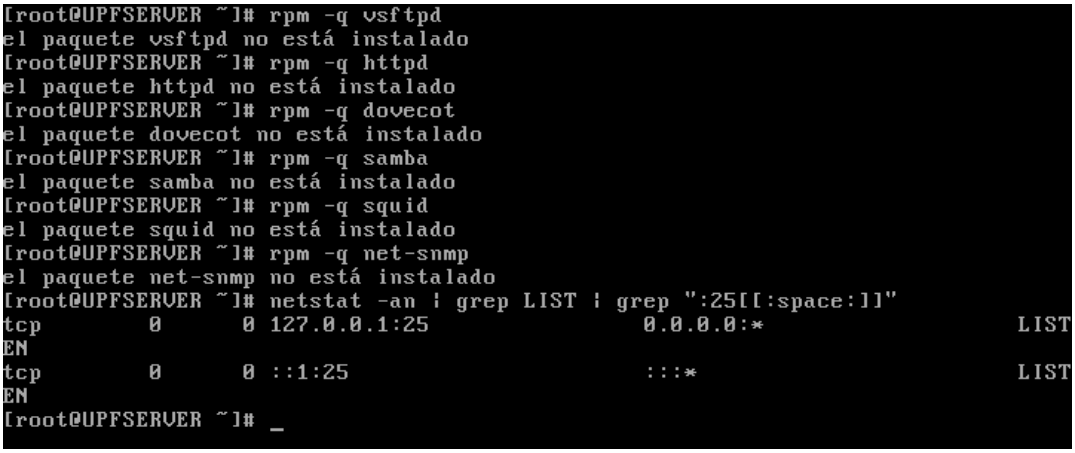

Figura 2.5: Verificación de servicios de propósitos especiales

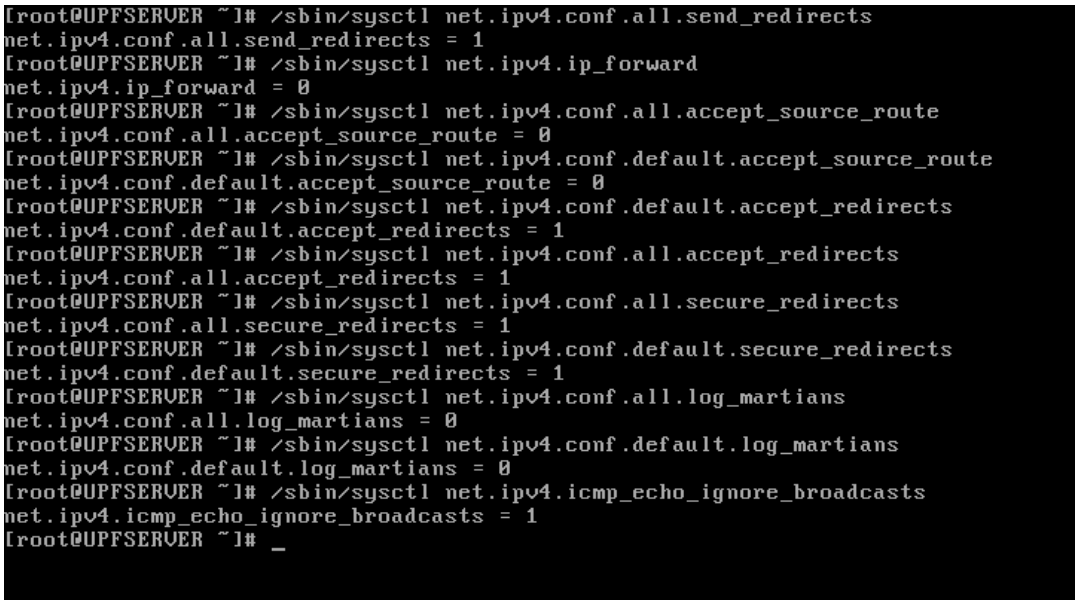

Figura 2.6: Verificación de configuraciones de red y firewall

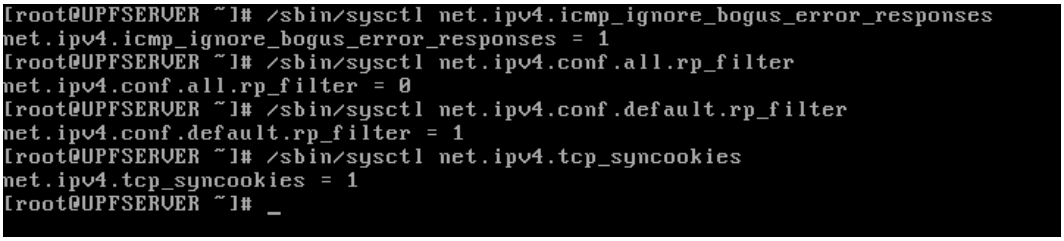

Figura 2.7: Verificación de configuraciones redirección y enrutamiento de paquetes

```
[root@UPFSERVER ~]# grep "install dccp/bin/true"
^C
[root@UPFSERVER ~]# grep "install sctp/bin/true"
^C
[root@UPFSERVER ~]# grep "install rds/bin/true"
^C
[root@UPFSERVER ~]# grep "install tipc/bin/true"
^C
[root@UPFSERVER ~]# chkconfig --list iptables
iptables        0:desactivado   1:desactivado   2:activo        3:activo        4
:activo 5:activo        6:desactivado
[root@UPFSERVER ~]# _
```

Figura 2.8: Verificación de protocolos de red poco comunes

```
[root@UPFSERVER ~]# rpm -q rsyslog
rsyslog-5.8.10-6.el6.x86_64
[root@UPFSERVER ~]# chkconfig --list syslog
error al leer la información del servicio syslog: No existe el fichero o el dire
ctorio
[root@UPFSERVER ~]# chkconfig --list rsyslog
rsyslog         0:desactivado   1:desactivado   2:activo        3:activo        4
:activo 5:activo        6:desactivado
[root@UPFSERVER ~]# _
```

Figura 2.9: Verificación de configuraciones Rsyslog

```
-rw-------. 1 root root  57040 jul 28 18:11 anaconda.xlog
-rw-------. 1 root root  64821 jul 28 18:11 anaconda.yum.log
drwxr-x---. 2 root root   4096 jul 31 23:12 audit
-rw-r--r--. 2 root root   2861 jul 31 23:12 boot.log
-rw-------. 1 root utmp   1536 jul 31 23:13 btmp
drwxr-xr-x. 2 root root   4096 jul 31 23:13 ConsoleKit
-rw-------. 1 root root   1981 ago  1 01:20 cron
drwxr-xr-x. 2 lp   sys    4096 nov  6  2012 cups
-rw-r--r--. 1 root root  21569 jul 31 23:12 dmesg
-rw-r--r--. 1 root root 161260 jul 28 18:11 dracut.log
-rw-r--r--. 1 root root 146000 jul 31 23:13 lastlog
-rw-------. 1 root root    197 jul 31 23:12 maillog
-rw-r--r--. 1 root root      0 jul 31 23:12 mcelog
-rw-------. 1 root root  30998 jul 31 23:13 messages
drwxr-xr-x. 2 ntp  ntp    4096 ene 10  2013 ntpstats
drwxr-xr-x. 2 root root   4096 oct 20  2011 prelink
drwxr-xr-x. 2 root root   4096 jul 31 23:14 rhsm
drwxr-xr-x. 2 root root   4096 ago  1 00:00 sa
drwx------. 3 root root   4096 jul 28 18:08 samba
-rw-------. 1 root root   1360 jul 31 23:13 secure
-rw-------. 1 root root      0 jul 28 18:08 spooler
drwxr-x---. 2 root root   4096 ene 23  2013 sssd
-rw-------. 1 root root      0 jul 28 18:06 tallylog
-rw-rw-r--. 1 root utmp   4224 jul 31 23:13 wtmp
[root@UPFSERVER ~]# _
```

Figura 2.10: Verificación de parámetros en archivo rsyslog.conf

```
[root@UPFSERVER ~]# grep '$ModLOAD imtcp.so' /etc/rsyslog.conf
[root@UPFSERVER ~]# grep '$InputTCPServerRun' /etc/rsyslog.conf
#$InputTCPServerRun 514
[root@UPFSERVER ~]# _
```

Figura 2.11: Verificación de parámetros por defecto en rsyslog.conf

```
[root@UPFSERVER ~]# grep "Protocol" /etc/ssh/sshd_config
Protocol 2
[root@UPFSERVER ~]# grep "LogLevel" /etc/ssh/sshd_config
#LogLevel INFO
[root@UPFSERVER ~]# grep "X11Forwarding"
^C
[root@UPFSERVER ~]# grep "MaxAuthTries"
^C
[root@UPFSERVER ~]# grep "IgnoreRhosts"
^C
[root@UPFSERVER ~]# grep "HostbasedAuthentication"
^C
[root@UPFSERVER ~]# grep "PermitRootLogin"
^C
[root@UPFSERVER ~]# grep "PermitEmptyPasswords"
^C
[root@UPFSERVER ~]# grep "PermitUserEnviroments"
^C
[root@UPFSERVER ~]# grep PermitUserEnviroments
^C
[root@UPFSERVER ~]# grep "Ciphers" /etc/ssh/sshd_config
[root@UPFSERVER ~]# grep "ClentAliveCountMax" /etc/ssh/sshd_config
[root@UPFSERVER ~]# _
```

Figura 2.12: Verificación de configuraciones SSH

```
[root@UPFSERVER ~]# grep "AllowUsers" /etc/ssh/sshd_config
[root@UPFSERVER ~]# grep "AllowGroups" /etc/ssh/sshd_config
[root@UPFSERVER ~]# grep "DenyUsers" /etc/ssh/sshd_config
[root@UPFSERVER ~]# grep "DenyGroups" /etc/ssh/sshd_config
[root@UPFSERVER ~]# grep "Banner" /etc/ssh/sshd_config
#Banner none
[root@UPFSERVER ~]# _
```

Figura 2.13: Verificación de parámetros y configuraciones SSH

```
[root@UPFSERVER ~]# authconfig --test | grep hashing | grep sha512
 password hashing algorithm is sha512
[root@UPFSERVER ~]# grep pam_cracklib.so /etc/pam.d/system-auth
password    requisite     pam_cracklib.so try_first_pass retry=3 type=
[root@UPFSERVER ~]# grep "pam_faillock" /etc/pam.d/password-auth !grep success_1
[root@UPFSERVER ~]# grep "pam_faillock" /etc/pam.d/password-auth !grep success=1

[root@UPFSERVER ~]# grep "pam_faillock" /etc/pam.d/password-auth !grep success=1
[root@UPFSERVER ~]# grep "pam_faillock" /etc/pam.d/system-auth
[root@UPFSERVER ~]# grep "pam_unix.so" /etc/pam.d/system-auth !grep success=1
[root@UPFSERVER ~]# grep "remember" /etc/pam.d/system-auth
[root@UPFSERVER ~]# cat/etc/securetty
-bash: cat/etc/securetty: No existe el fichero o el directorio
[root@UPFSERVER ~]# grep pam_wheel.so /etc/pam.d/su
#auth           sufficient      pam_wheel.so trust use_uid
#auth           required        pam_wheel.so use_uid
[root@UPFSERVER ~]# grep wheel /etc/group
wheel:x:10:
[root@UPFSERVER ~]# _
```

Figura 2.14: Verificación de configuraciones PAM

```
[root@UPFSERVER ~]# grep PASS_MAX_DAYS /etc/login.defs
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
PASS_MAX_DAYS   99999
[root@UPFSERVER ~]# chage --list root
Last password change                                    : Jul 28, 2015
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
[root@UPFSERVER ~]# chage --list qauser
Last password change                                    : Aug 01, 2015
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
[root@UPFSERVER ~]# grep "root" /etc/passwd | cut -f4 -d:
0
0
[root@UPFSERVER ~]# _
```

Figura 2.15: Verificación de configuraciones de usuarios.

Figura 2.16: Verificación de configuración de máscara por defecto.

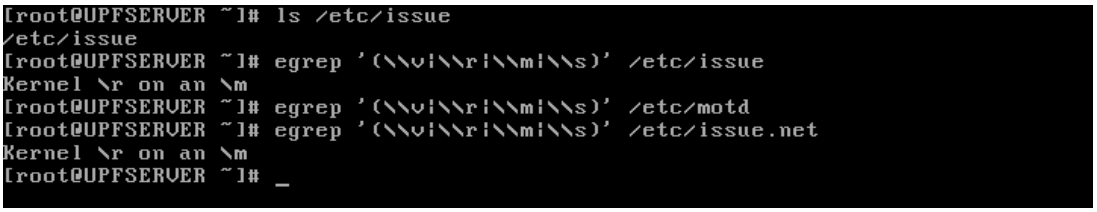

Figura 2.17: Verificación de configuraciones banners de advertencia

De la revisión realizada sobre los resultados obtenidos como parte de la auditoria llevada a cabo sobre la configuración del sistema operativo encontramos las siguientes novedades:

- Existen paquetes que no están instalados debido a que no se incluyen dentro de la instalación original del sistema operativo.
- Existen directorios que no fueron encontrados, por lo que se procede al registro de dichas novedades.
- El usuario root se encuentra habilitado y con el se realizará el proceso de aseguramiento, luego de ello se procederá con su inhabilitación.

- Se procedió a crear un usuario de prueba, el mismo que demostró contener permisos de administración, excluyendo la caducidad de la clave, posibilidad de inhabilitación e inhabilitación posterior de cuenta por expiración.
- El syslog se encuentra deshabilitado, sin embargo el rsyslog permanece activo y está registrando actividad que podría realizarse en el syslog.

2.3. Elaboración del plan de ejecución para el aseguramiento del sistema operativo.

Para poder ejecutar el aseguramiento del servidor indicado, se estableció un plan de acción por medio del cual se remediarán las inconformidades registradas durante la auditoría preliminar, mismo que se ejecutará tomando en consideración lo siguiente:

- Se validará la funcionalidad del equipo antes de iniciar con el proceso de aseguramiento.
- Se verificará en conjunto con el QSA los resultados obtenidos con la ejecución de cada uno de los comandos indicados.
- Aunque el usuario root sea el que realice las configuraciones, este quedará deshabilitado, por lo que las validaciones de acceso se realizarán con el usuario administrador creado.

- Se deberá documentar los pasos a realizar con la finalidad de evidenciar cualquier novedad que pudiera presentarse.
- Previo a la ejecución de cada configuración se debe contar con su respectiva opción de reverso para que en caso de reportarse una novedad, la misma pueda ser solucionada inmediatamente.
- Se realizará una validación final de los resultados, con la que se dará por cerrado el proceso de aseguramiento, y el mismo deberá ser aprobado por el cliente.

Con las consideraciones mencionadas, los dominios que se procederá a verificar cubren los siguientes puntos:

- Servicios propios del sistema operativo que se encuentran en ejecución
- Servicios especiales requeridos por el aplicativo
- Configuraciones de entrada y salida de red
- Firewall interno del servidor
- Protocolos de red
- Logs del sistema
- Configuración SSH para acceso al sistema de forma remota
- Mecanismos de autenticación

- Cuentas de usuario
- Configuración de ambientes separados por etapa del ciclo de vida de los sistemas
- Alertas

CAPÍTULO 3

Ejecución del aseguramiento del equipo.

Finalmente, en este capítulo se detalla paso a paso como realizar el aseguramiento del servidor siguiendo tanto las recomendaciones de la norma PCI DSS como lo indicado por el asesor del ente certificador.

En base a lo indicado, dentro de esta etapa del proyecto, se presentará el resultado obtenido, mismo que nos brindará las evidencias suficientes para determinar el beneficio logrado para la institución.

3.1. Remover servicios por defecto

Figura 3.1: Remover servicio de servidor Telnet

Figura 3.2: Remover paquete de Telnet

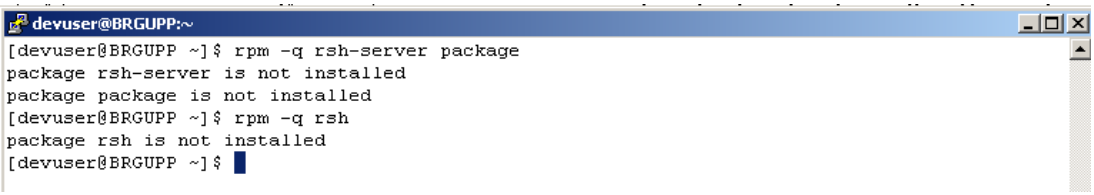

Figura 3.3: Remover servicio de servidor RSH

Figura 3.4: Remover servicio de información de red.

Figura 3.5: Remover paquete de servicio TFTP

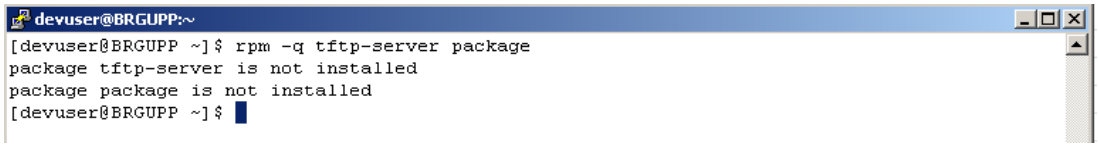

Figura 3.6: Remover servicio de servidor TFTP

Figura 3.7: Remover controlador de servicios extendidos de internet.

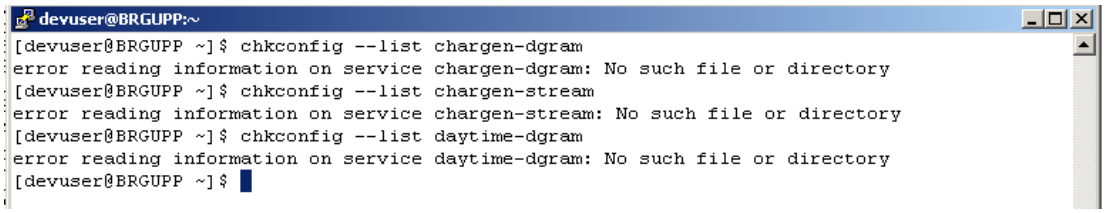

Figura 3.8: Remover servicio de generación de caracteres

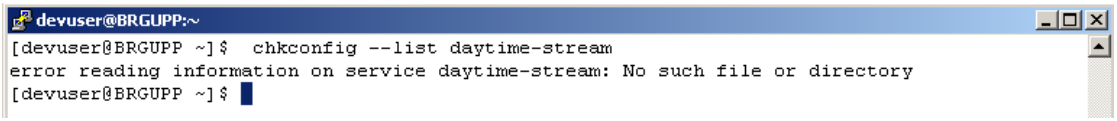

Figura 3.9: Remover servicio de envío de fecha actual

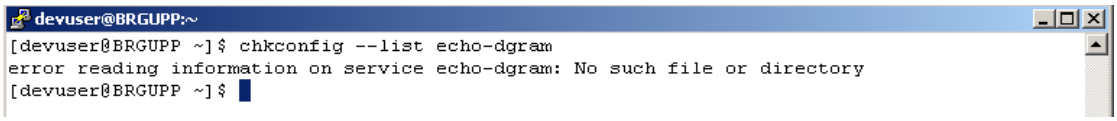

Figura 3.10: Remover servicio de generación de mensajería de control por protocolo UDP

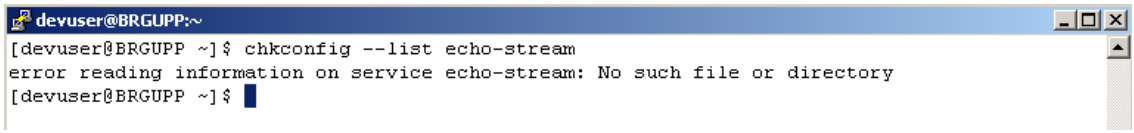

Figura 3.11: Remover servicio de generación de mensajería de control por flujos

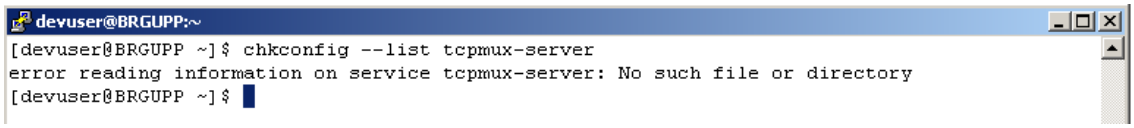

Figura 3.12: Remover servicio de multiplexado de protocolo TCP.

Como parte del proceso de aseguramiento se procedió a realizar las siguientes actividades:

- Remover servidor y cliente Telnet
- Remover servidor y cliente RSH

- Remover cliente y servidor NIS
- Remover tftp
- Remover tftp-server
- Remover xinetd
- Deshabilitar chargen-dgram
- Deshabitliarchargen-stream
- Deshabilitar daytime-dgram
- Deshabilitar daytime-stream
- Deshabilitar echo-dgram
- Deshabilitar echo-stream
- Deshabilitar tcpmux-server

3.2. Servicios de propósitos especiales

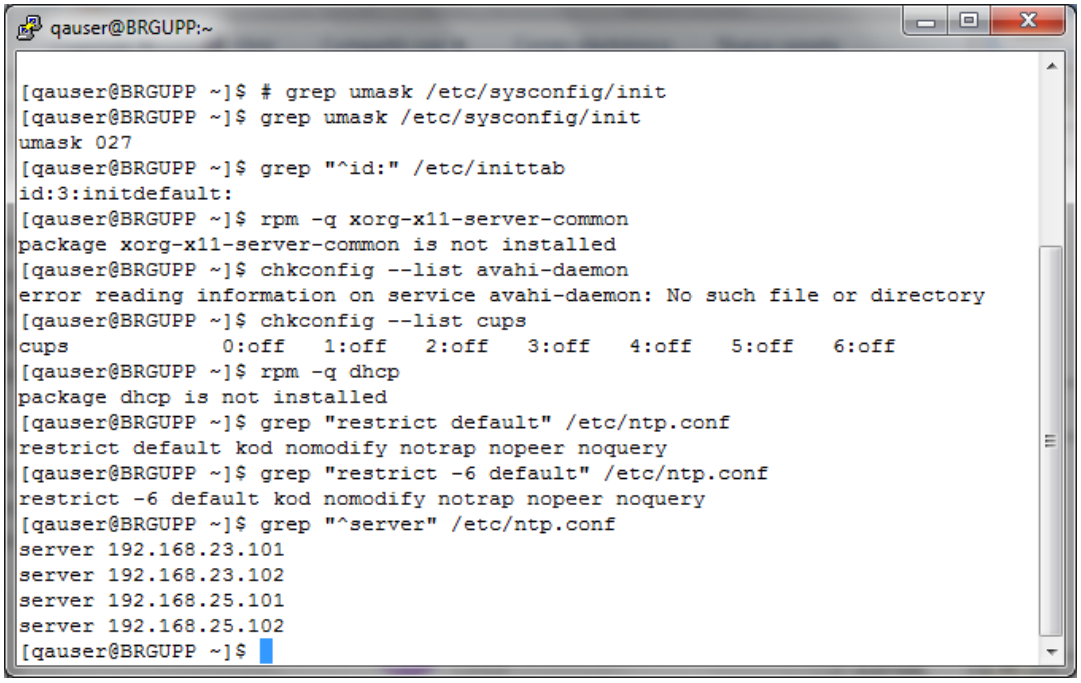

Figura 3.13: Remover servicios de propósito especiales.

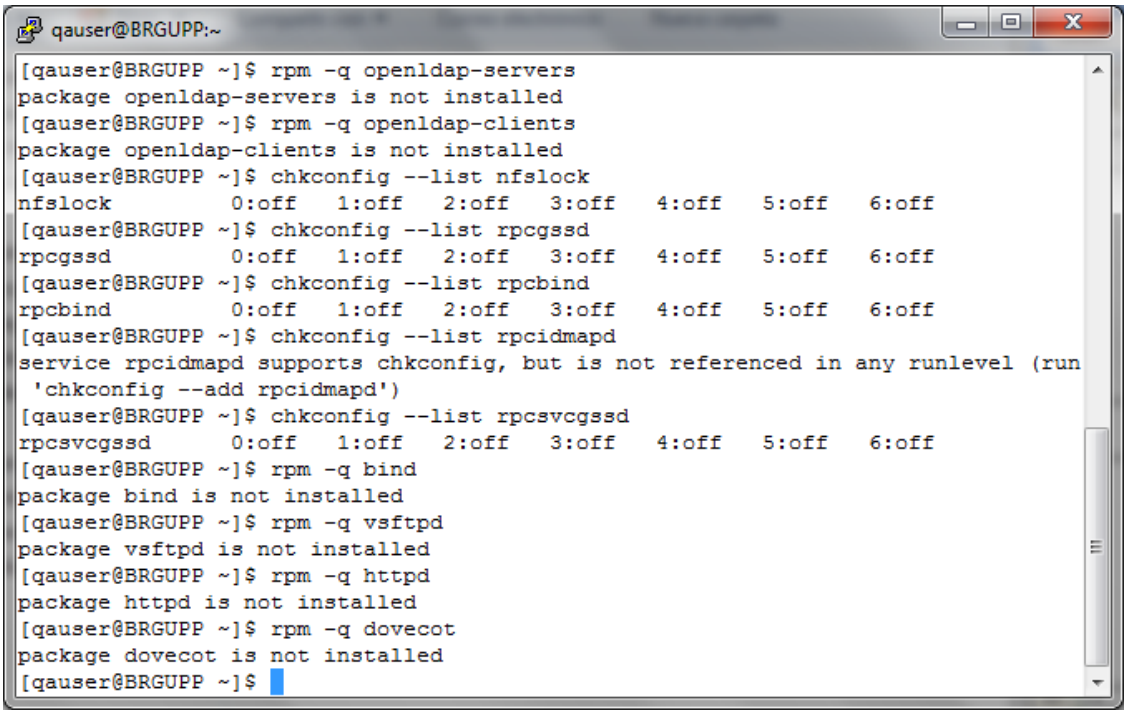

Figura 3.14: Ajustar parámetros de servicios de propósito especiales.

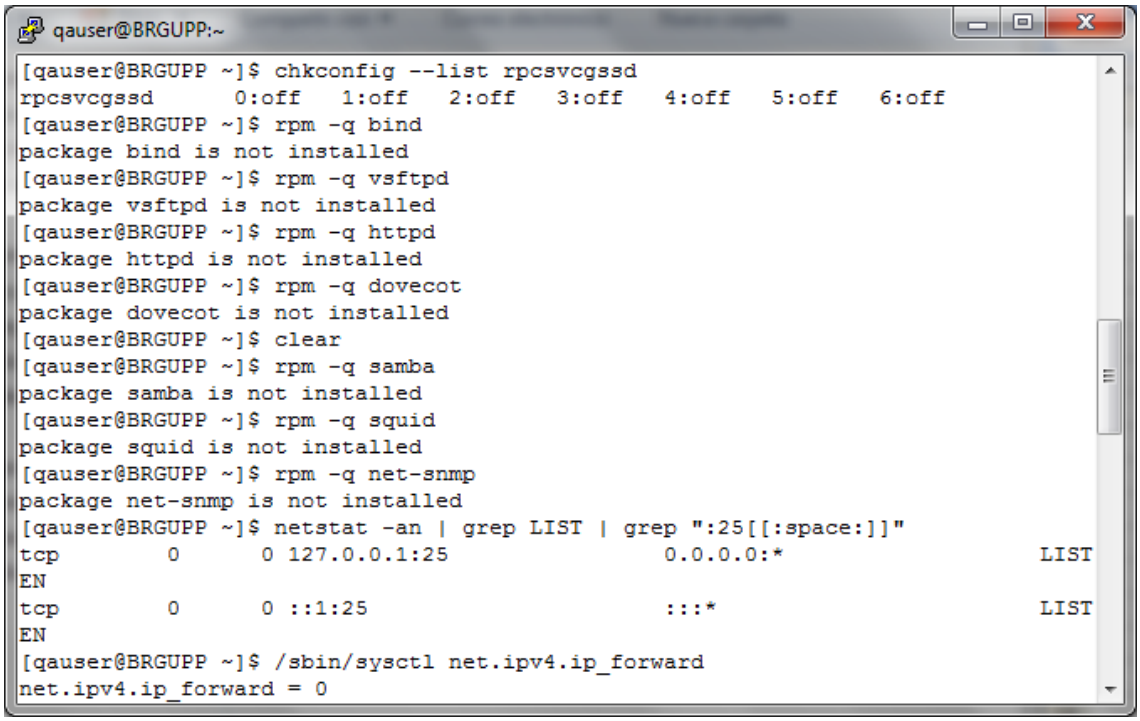

Figura 3.15: Desinstalar y Remover servicios de propósito especiales.

Para solventar las novedades evidenciadas en este punto, se procedió a:

- Configurar Daemon umask
- Remover X Window System
- DeshabilitarAvahi Server
- Deshabilitar Print Server - CUPS
- Remover DHCP Server
- Configurar NTP
- Remover LDAP
- Deshabilitar NFS Y RPC

- Remover DNS Server
- Remover FTP Server
- Remvoer HTTP Server
- Remover Dovecot (IMAP Y POP3 Services)
- Remover Samba
- Remover HTTP Server
- Remover SNMP Server
- Configurar Mail Transfer Agent para Modo Local - Only

3.3. Configuración de red y firewall

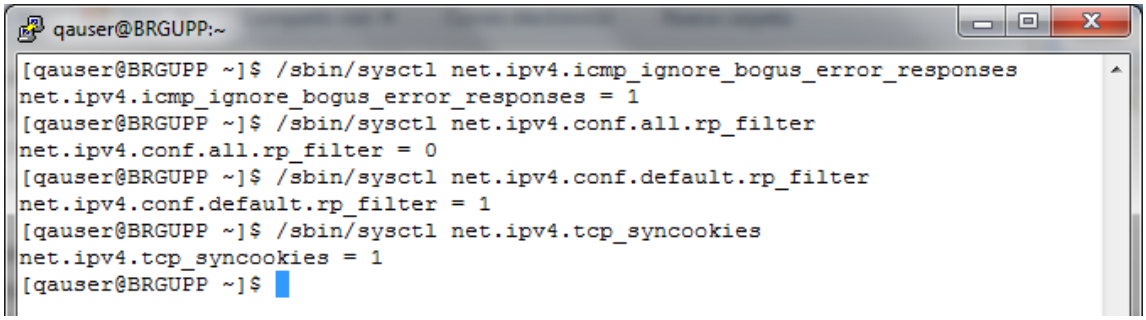

Figura 3.16: Parámetros para servicios de red y firewalls.

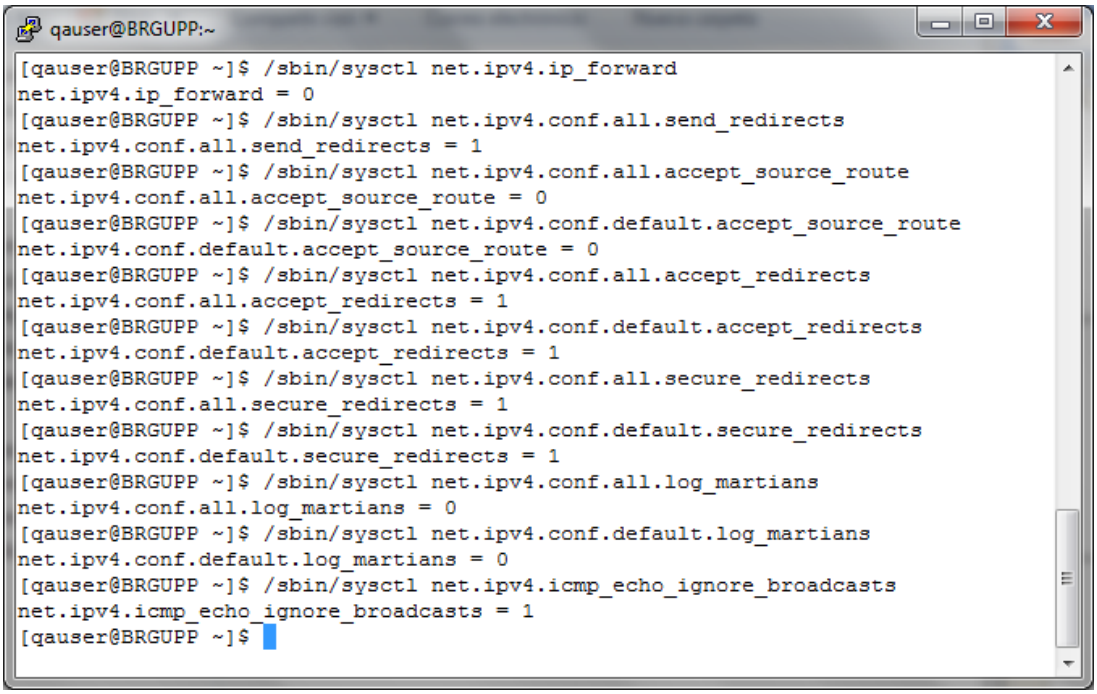

Figura 3.17: Remover configuraciones para redireccionamiento de paquetes.

Para solventar las novedades en este punto, se realizaron las siguientes actividades:

- Deshabilitar IP Forwarding
- Deshabilitar Redirección de envío de paquetes
- Deshabilitar aceptación de paquetes de enrutación de fuentes
- Deshabilitar aceptación de paquetes ICMP redirigidos
- Deshabilitar aceptación de paquetes ICMP seguros
- Logs de Paquetes Sospechosos

- Habilitar "Ignorar peticiones de broadcast"
- Habilitar Protección contra "Bad Error Message"
- Habilitar "RFC-recommende Source Route Validation"
- Habilitar TCP SYN Cookies

3.4. Protocolos de redes poco comunes

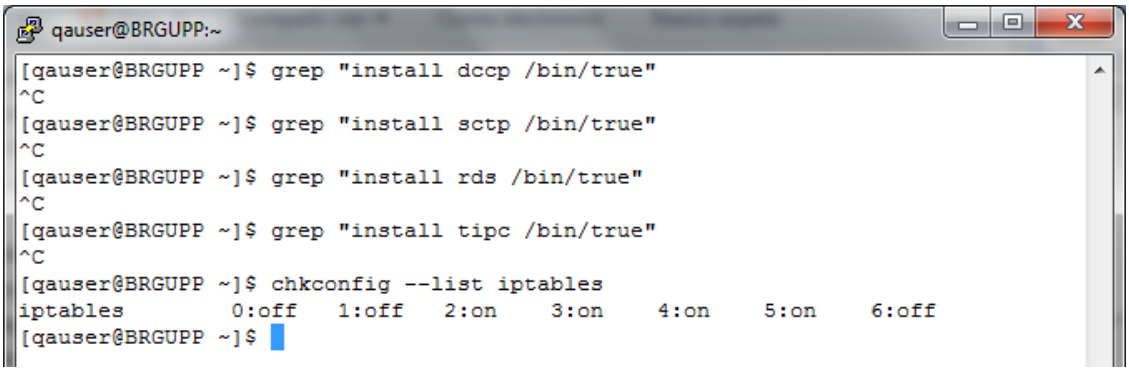

Figura 3.18: Parámetros para servicios de red poco comunes.

Como solución a las novedades reportadas, se ejecutaron las siguientes tareas:

- Con la configuración de iptables para la denegación de acceso a direcciones IP no permitidas por el administrador del servicio.

- al cierre de puertos y monitoreo de los mismos por medio del uso de iptables.
- al levantamiento de firewall local.

3.5. Logs del sistema

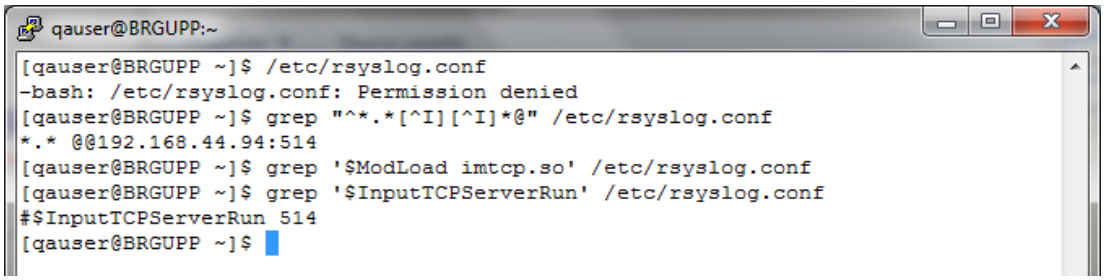

Figura 3.19: Aseguramiento de Log's del sistema.

El caso fue cubierto con las siguientes consideraciones:

- Instalar el paqutersyslog
- Activar el servicio rsyslog
- Configurar /etc/rsyslog.conf
- Crear y configurar permisos sobre archivos de rsyslog
- Configurar rsyslog para enviar logs a servidor remoto
- No aceptar mensajes remotos de rsyslog

3.6. Configuración SSH

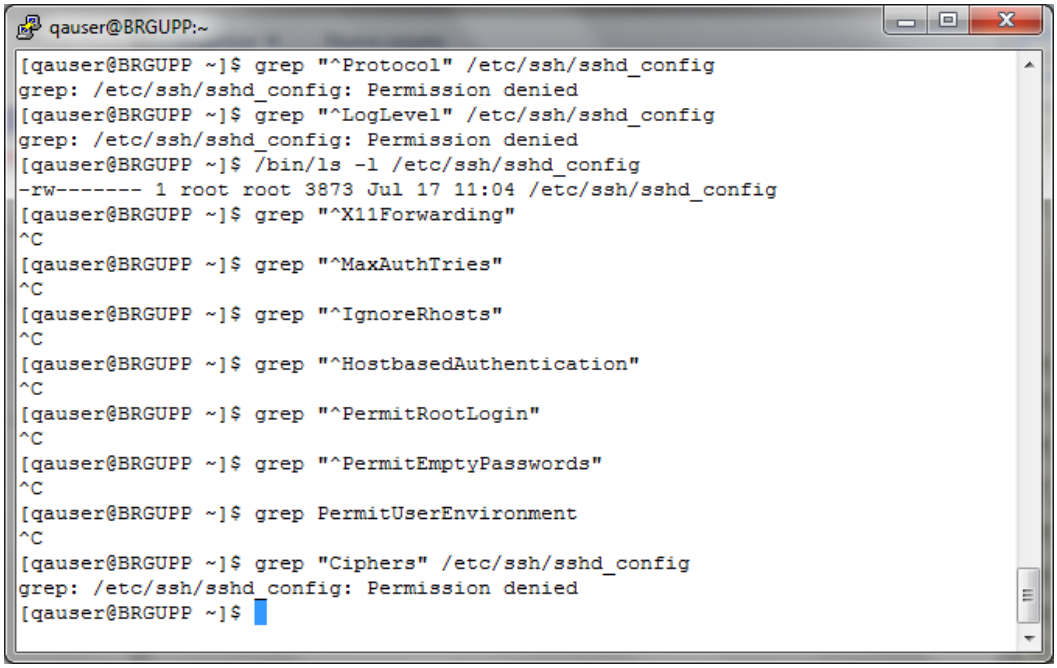

Figura 3.20: Ajuste en parámetros SSH.

Figura 3.21: Remover permisos de acceso a archivos de configuración en directorio/etc/ssh.

Para este punto, se consideró lo siguiente:

- Se procede con la configuración del algoritmo de cifrado de datos para contraseñas sha512
- Se procede a configurar el borrado automático del archivo cat/etc/pam.d/password-auth #%PAM-1.0 para cada oportunidad en que el authconfig se encuentre en ejecución.

3.7. Configuración PAM

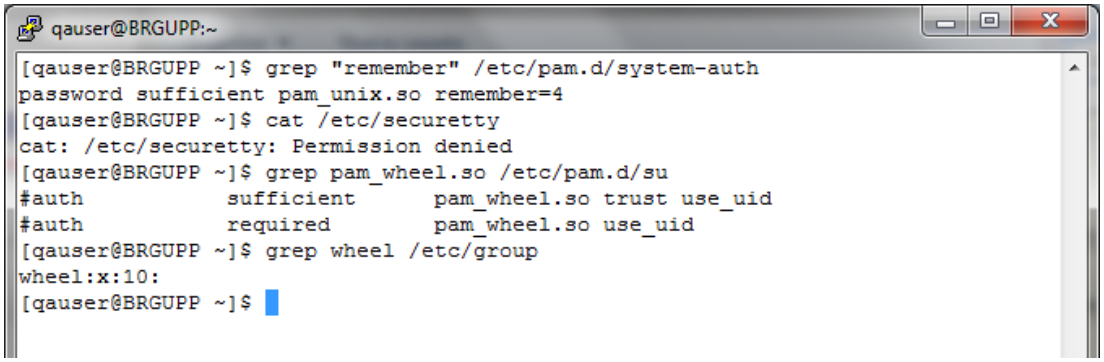

Figura 3.22: Ajuste en configuración PAM.

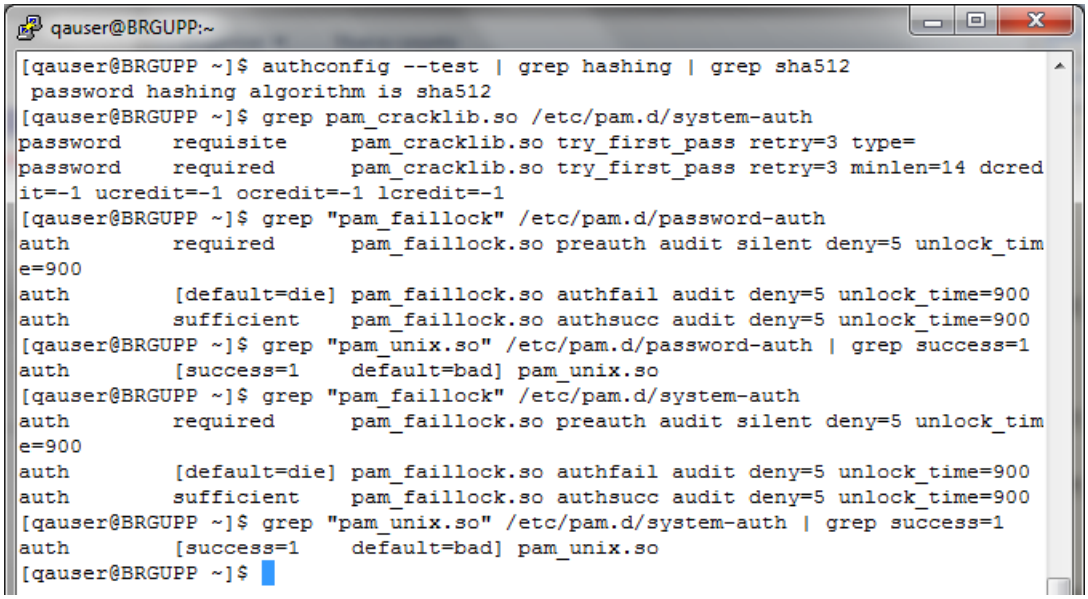

Figura 3.23: Confirmación de ejecución de aseguramiento para PAM.

Para este caso, se efectuaron las siguientes tareas:

- Se procede con la restricción el acceso a los archivos de sistema y de configuración de permisos de usuario.
- Se procede a configurar en /etc/pam.d/su el parámetro authrequiredpam_wheel_souse_uid.
- Se incluye la lista de los usuarios que pueden ejecutar el comando su en el archivo Wheel en el directorio /etc/groups.

3.8. Cuentas de Usuario y ambientes.

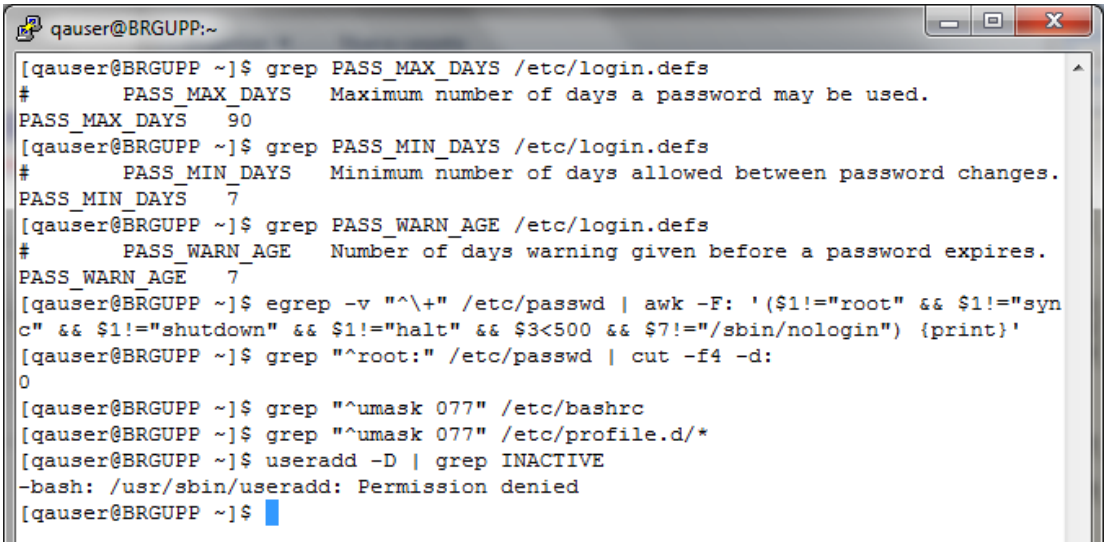

Figura 3.24: Ajuste en parámetros de usuarios.

Para el control de usuarios, las consideraciones fueron las siguientes:

- Se procede con el ajuste dentro del sistema para que la caducidad de las contraseñas sea de 90 días.
- Se procede con la inhabilitación del usuario root para hacer login en el sistema operativo directamente.
- Se procede con la reducción de privilegios para los usuarios no administradores aprobados por la empresa.
- Se procede con la configuración del mínimo de días para cambiar la contraseña, incluyendo el mensaje de advertencia de expiración del password.
- Se procede a deshabilitar las cuentas del sistema por medio del uso del siguiente comando:
    - egrep -v "^\+" /etc/passwd | awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $3<500 && $7!="/sbin/nologin") {print}'
- Se procede a configurar la máscara por defecto para los usuarios en las rutas:
    - /etc/bashrc
    - /etc/peodilw.s/cis.sh

3.9. Banners de advertencia.

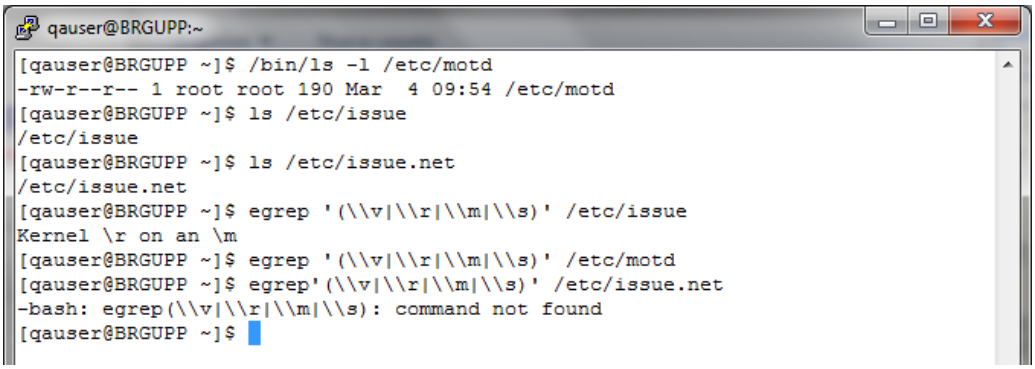

Figura 3.25: Ajuste en configuración de Banners de advertencia.

Finalmente, para solventar estas novedades, se realizó lo siguiente:

- Configurar Banner de Advertencia para servicios standard de login.
- Remover Información de Sistema Operativo para logeo de Banners de Advertencia.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

1. Con el desarrollo del proyecto se pudo completar exitosamente lo solicitado, lo cual consistía en el aseguramiento de la plataforma operativa del nuevo switch transaccional para producción, el cual fue ejecutado en conjunto entre el personal responsable por parte del proveedor del aplicativo, de Red Hat Inc., la entidad certificadora y los ingenieros de la empresa.

2. Dentro de la ejecución de las pruebas pudimos observar que existen mejoras que podrían realizarse a nivel de cada una de las instancias participantes por lo que

fue el inicio de un proyecto de mejoras en los que se participará de igual manera, generando así una gran ayuda para futuros proyectos con otros clientes.

Recomendaciones:

1. Se pudo evidenciar dentro del proceso del aseguramiento que existen opciones las cuales son consideradas por la entidad certificadora y ya fueron solventadas en las últimas actualizaciones del sistema operativo, por lo que se levantó la alerta para el ajuste de la documentación hacia nuestros auditores.

2. Una vez implementada la solución, se recomienda igualmente que como alcance al proyecto, se haga una evaluación sobre los permisos requeridos por el sistema para incrementar el nivel de seguridad, ya que la implementación realizada actualmente cubre con las necesidades básicas de PCI 3.0, sin embargo para inicios del año 2016 se espera que las auditorias de cumplimiento se realicen sobre su última actualización en la versión 3.1

3. Con la implementación se contempla un crecimiento transaccional del 50%, lo cual está proyectado para cubrir los próximos 3 años, sin embargo el tiempo puede verse reducido por lo que luego de su salida a producción se recomienda se haga un análisis de las transacciones por segundo que el mismo podrá soportar y así tener una proyección más real

4. Dentro del proceso de aseguramiento, el personal administrador de la infraestructura tecnológica nos indicó que cuentan con un servidor con sistema operativo Oracle LINUX 6 sobre el que se desea realizar el mismo trabajo; se procedió con la evaluación de la plantilla de aseguramiento y según pudimos evidenciar se mantienen las mismas consideraciones que en la plantilla utilizada para Red Hat 6, por lo que se recomienda aplicar las mismas configuraciones indicadas en el documento. [5]

GLOSARIO

Aseguramiento (hardening)

Consiste en el endurecimiento de la plataforma operativa, de manera que se puedan solventar las vulnerabilidades que han sido estudiadas y publicadas previamente por los organismos de seguridad competentes tanto a nivel nacional como internacional.

PCI DSS

P.C.I. D.S.S. son las siglas por las cuales reconocemos al PaymentCardIndustry Data security Standard, o en su traducción a nuestra lengua como el estándar de seguridad en los datos de la industria de pagos por tarjetas. Este estándar nos permite mantener un nivel de seguridad adecuado para el correcto uso de tarjetas de crédito y débito, reduciendo en gran porcentaje el número de fraudes y el impacto de estos tanto para los clientes como para las instituciones financieras.

QSA:

Siglas utilizadas para describir al Quality Security Advisor, o su traducción Consultor de Calidad de Seguridad. Es el oficial encargado de realizar la auditoría PCI DSS por parte

de la entidad certificadora. Se asigna regularmente un QSA por cada ejercicio, es decir por cada proceso de auditoría que se realice, ya sea de certificación inicial o de renovación.

Vulnerabilidad:

Es un punto débil que se descubre tanto a nivel de software como de hardware, el cual compromete la disponibilidad, confidencialidad o integridad de la información. Estas vulnerabilidades son catalogadas dependiendo el impacto que puede producir su explotación, siendo el caso de las más severas pueden permitir al atacante tener control absoluto del equipo y por ende de la información a la que este puede tener acceso.

Booteo:

Denominado se esta manera al proceso de arranque del sistema desde su estado de apagado.

PAM:

PluggableAuthentication Modules, es un mecanismo de acceso o autenticación que trabaja de manera flexible, este permite aislar a las aplicaciones y otro software existente del proceso de identificación. La identificación del usuario, implementa niveles de

seguridad mayores, tal sea el caso del uso de Biométricos, autenticaciones con claves temporales, entre otras, reemplazando a los mecanismos tradicionales o simplemente fortaleciendo dichos métodos de autenticación.

BIBLIOGRAFÍA

[1] Red Hat Inc., Red Hat Enterprise Linux 6 Guía de Seguridad, https://access.redhat.com/documentation/es-ES/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-es-ES.pdf

[2] PCI Security Standards Council, Requirements and Security Assessment ProceduresVersion 3.0, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf, fecha de consulta julio 2015.

[3] Gonzalez, Padrón, PluggableAuthentication Modules, http://sopa.dis.ulpgc.es/ii-aso/portal_aso/leclinux/seguridad/pam/pam_doc.pdf, fecha de consulta julio 2015.

[4] Capek, T., Petrová, A., Navrátil, M., Ballard, E., Red Hat Enterprise Linux 6 Identity Management Guide, https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Identity_Management_Guide/Red_Hat_Enterprise_Linux-6-Identity_Management_Guide-en-US.pdf, fecha de consulta julio 2015.

[5] ORACLE, Oracle Linux

Security GuideforRelease 6, http://docs.oracle.com/cd/E37670_01/E36387/E36387.pdf, fecha de consulta julio 2015.