



ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

**“APLICACIÓN DE CONTROLES Y SEGURIDADES DE
SERVICIOS EN SERVIDORES LINUX”**

TESINA DE SEMINARIO

Previa a la obtención del Título de:

“LICENCIATURA EN REDES Y SISTEMAS OPERATIVOS”

Presentada por:

SANDRA VÁSQUEZ MITE

EDUARDO LOOR ALCÍVAR

GUAYAQUIL – ECUADOR

AÑO

2014

AGRADECIMIENTO

Agradezco a Dios por haber permitido que culminaran mis estudios con éxito y me supo mantener en pie para seguir adelante durante todo este tiempo

A mis padres que con todo su sacrificio y esfuerzo a lo largo de mi camino estuvieron siempre apoyándome para cumplir con una de mis metas.

A Miguel Paladines quien gracias a su apoyo incondicional no dejo que me rinda fácilmente.

A mis compañeros de Credimatic por brindarme todo su apoyo y conocimientos para lograr esta meta.

A mis profesores que fueron la parte fundamental para poder crecer profesionalmente

A la Escuela Superior Politécnica del Litoral por su exigencia y brindarme la oportunidad de poder crecer profesionalmente y desarrollarme en el mundo de la tecnología.

Sandra Vásquez Mite

A Dios, que me ha dado fuerzas cada día para llegar a esta meta tan ansiada.

A mí dedicada y muy amada madre Ana Teresa Alcívar Ostaíza, quien con su apoyo, su valor y su amor me enseñó a salir siempre adelante en todos los aspectos de mi vida.

De manera especial y primordial a mi padre Vicente Eduardo Loor Jácome porque no dejó de creer en mí y es mi mejor amigo porque con sus sabios consejos me canalizo hacia la terminación de esta profesión.

A mi hermana Anita Cristina Loor Alcívar que siempre me incentivo para este logro. Gracias por su paciencia y por compartir esta etapa tan importante.

Este triunfo es dedicado a ustedes mi familia.

Eduardo Javier Loor Alcívar

DEDICATORIA

A Dios, mis padres, hermanos, Miguel y Perry que siempre estuvieron presentes a lo largo de mi carrera profesional.

Sandra Vásquez Mite

A mi Tutor de tesis Ing. Fabián Barboza Gilces por sus buenos conocimientos, experiencia y dedicación por dirigirme en el presente trabajo, a mi director de carrera el Ing. Albert Giovanny Espinal Santana quien como buen líder supo apoyarme durante toda mi carrera universitaria.

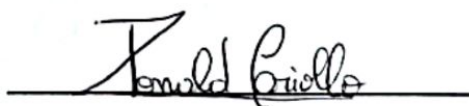
Eduardo Loor Alcívar

TRIBUNAL DE SUSTENTACIÓN

A handwritten signature in black ink, consisting of several overlapping loops and a horizontal line at the bottom, positioned above the printed name.

Ing. Fabián Barboza

PROFESOR DEL SEMINARIO DE GRADUACION

A handwritten signature in black ink, written in a cursive style, positioned above the printed name.

Ing. Ronald Criollo.

PROFESOR DELEGADO POR LA UNIDAD ACADEMICA


DECLARACIÓN EXPRESA

“La responsabilidad del contenido de esta Tesina de Seminario, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral”.

(Reglamento de Graduación de la ESPOL)



Sandra Vásquez Mite



Eduardo Llor Alcívar

RESUMEN

El principal objetivo de este proyecto es implementar la metodología aprendida en nuestro desarrollo académico y en el seminario asistido con respecto a “LINUX NETWORKING Y SEGURIDADES”, para fortalecer la seguridad informática en servidores para instituciones financieras aplicado a la empresa “DROFMAN S.A.” la cual ha solicitado un estudio de su infraestructura TI, detectando vulnerabilidades, aplicando soluciones e implementar un plan de prevención a futuro para mitigar los riesgos de seguridad y cumplir con los requerimientos del Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS).

ÍNDICE GENERAL

AGRADECIMIENTO	II
DEDICATORIA	IV
TRIBUNAL DE SUSTENTACIÓN	V
DECLARACIÓN EXPRESA	VI
RESUMEN	VII
ÍNDICE GENERAL	VIII
ÍNDICE DE FIGURAS	XIII
ÍNDICE DE TABLAS	XXI
INTRODUCCIÓN	XXII
CAPÍTULO 1	1
ESTÁNDAR PCI-DSS	1
1.1 INTRODUCCIÓN	1
1.1.1 Qué es PCI DSS	2
1.2 REQUERIMIENTOS DE PCI DSS	2
1.3 POR QUÉ SE DEBE CUMPLIR PCI DSS:	5
1.3.1 Como cumplir PCI DSS.....	5
1.3.2 Selección de un Asesor de Seguridad Calificado:	7
1.3.3 Ámbito de la evaluación del cumplimiento	9
CAPÍTULO 2	11
ANÁLISIS DE LA INFRAESTRUCTURA TI	11
2.1 INFRAESTRUCTURA TECNOLÓGICA TI	11
2.1.1 DataCenter Guayaquil.....	11

2.1.1.1	Red de Producción	12
2.1.1.2	Red de Preproducción.....	14
2.1.1.3	Red de Protección de equipos críticos.	14
2.1.1.4	Red DMZ	15
2.1.1.5	Red Datacard /Chip	16
2.1.1.6	Red LAN.....	18
2.1.2	DataCenter Quito	19
2.1.2.1	Red LAN UIO.....	20
2.1.2.2	Red DMZ UIO.....	20
2.1.2.3	Red de Protección de quipos críticos UIO.	20
2.1.3	LAN.....	22
2.1.4	WAN	22
2.1.5	Seguridades	22
CAPÍTULO 3.....		24
IDENTIFICACIÓN DE VULNERABILIDADES		24
3.1	IDENTIFICACIÓN DE VULNERABILIDADES	24
3.2	DETERMINACIÓN DE VULNERABILIDADES EN LA INFRAESTRUCTURA TI	27
3.3	CLASIFICACIÓN DE VULNERABILIDADES	33
3.3.1	Infraestructura	34
3.3.2	Operacional	34
3.3.3	Personal	35
3.4	MATRIZ DE IMPACTO DE VULNERABILIDADES EN LA EMPRESA.....	35
CAPITULO 4.....		39
IMPLEMENTACIÓN DE SOLUCIONES A LAS VULNERABILIDADES IDENTIFICADAS		39

4.1	APLICACIÓN DE SOLUCIONES EN SERVIDORES DE PRUEBA.....	39
4.2	ANÁLISIS DE RESULTADOS DE IMPACTOS EN SERVIDORES DE PRUEBA.	41
4.3	IMPLEMENTACIÓN DE LAS SOLUCIONES EN PRODUCCIÓN.....	42
4.3.1	Menú Principal de Aplicación de Hardening basado en la norma PCI DSS	42
4.3.1.1	Opción 1 – Servicios habilitados en el servidor.....	43
4.3.1.2	Opción 2 – Hardening a los servicios instalados en el servidor.....	46
4.3.1.2.1	Hardening a SAMBA	48
4.3.1.2.1.1	Definir host permitidos para transferencia de información	50
4.3.1.2.1.2	Definir los host denegados para la transferencia de información	53
4.3.1.2.1.3	Denegar permisos a usuarios del sistema	55
4.3.1.2.1.4	Reversa de hardening SAMBA.....	57
4.3.1.2.2	Hardening a HTTP	58
4.3.1.2.2.1	Deshabilitar módulos innecesarios.....	60
4.3.1.2.2.2	Ocultar versión de Apache y OS de errores.....	61
4.3.1.2.2.3	Configuración de puerto de conexión	62
4.3.1.2.2.4	Reversa de Hardening HTTP.....	64
4.3.1.2.3	Hardening a POSTFIX.....	65
4.3.1.2.3.1	Cambios de permisos en los archivos de configuración	66
4.3.1.2.3.2	Configurar banner de Bienvenida.....	68
4.3.1.2.3.3	Proteger el servicio de ataques de DOS	69
4.3.1.2.3.4	Reversar Hardening POSTFIX	70
4.3.1.2.4	Hardening a SQUID	71
4.3.1.2.4.1	Opción 1 - Apagar la función PIC y HTCP.....	72
4.3.1.2.4.2	Opción 2 - Activar SNMP	73
4.3.1.2.4.3	Opción 3.- Restringir acceso a Proxy Squid	74
4.3.1.2.4.4	Opción 4.- Reversar Hardening SQUID	76

4.3.1.2.5	Hardening SSH	77
4.3.1.2.5.1	Opción 1 - Desactivar usuario Root para que no pueda realizar conexión remota.	78
4.3.1.2.5.2	Opción 2 - Configurar intervalo de espera entre conexión con el usuario	79
4.3.1.2.5.3	Opción 3 - Establecer permisos de usuarios a archivos de configuración de SSH	80
4.3.1.2.5.4	Opción 4 - Número máximo de intentos fallidos durante el login del usuario.	81
4.3.1.2.5.5	Opción 5 - Configuración de usuarios para acceso mediante SSH	83
4.3.1.2.5.6	Opción 6 - Personalización de Banner de Bienvenida	84
4.3.1.2.5.7	Opción 7 - Configuración de tiempo de sesiones inactivas	85
4.3.1.2.5.8	Opción 8 - Configuración de puerto de conexión de SSH	87
4.3.1.2.5.9	Opción 9 - Reversa de hardening SSH	88
4.3.1.2.6	Hardening a NTP	89
4.3.1.2.6.1	Sincronización automática	90
4.3.1.2.6.2	Sincronización manual	91
4.3.1.2.6.3	Reversa de Hardening NTP	92
4.3.1.3	Opción 3 – Reportes de servicios en el servidor	93
4.3.1.3.1	Opción 1 - Hardening aplicado en la sesión actual.	94
4.3.1.3.2	Opción 2 - Hardening no aplicado en sesión actual	95
4.3.1.3.3	Opción 3 - Histórico de servicios que cumplen hardening	96
4.3.1.3.4	Opción 4 - Histórico de servicios que no cumplen hardening	97
4.3.1.3.5	Opción 5 - Auditoria a los servicios instalados.	98
4.3.1.3.5.1	Opción B – Auditoria SAMBA	99
4.3.1.3.5.2	Opción H – Auditoria HTTP	100
4.3.1.3.5.3	Opción Q – Auditoria SQUID	102

4.3.1.3.5.4	Opción S – Auditoria SSH.....	103
4.3.1.3.5.5	Opción T – Auditoria NTP.....	104
4.4	IMPLEMENTACIÓN DE UN PLAN DE PREVENCIÓN CONTRA VULNERABILIDADES	105
	CONCLUSIONES	108
	BIBLIOGRAFÍA	110
	ANEXOS	112
	GLOSARIO	157

ÍNDICE DE FIGURAS

Figura 2. 1 Infraestructura TI de DROFMAN	12
Figura 2. 2 Red de Producción Guayaquil	13
Figura 2. 3 Red de PRE-Producción Guayaquil.....	14
Figura 2. 4 Red de Protección Guayaquil	15
Figura 2. 5 Red de DMZ Guayaquil	16
Figura 2. 6 Red Datacard / Chip Guayaquil	17
Figura 2. 7 Red de Mantenimiento & Producción Guayaquil	17
Figura 2. 8 Red LAN Guayaquil	18
Figura 2. 9 Enlace con Bancos Asociados.....	19
Figura 2. 10 Red de Infraestructura Quito DROFMAN.....	21
Figura 3. 1 Metodología para la detección de vulnerabilidades	26
Figura 3. 2 Ejecución de nmap -v localhost	28
Figura 3. 3 Ejecución de nmap -v localhost	29
Figura 3. 4 Ejecución de nmap -sv localhost.....	29
Figura 3. 5 Ejecución de nmap -A localhost.....	30
Figura 3. 6 Ejecución de nmap -v localhost	31

Figura 3. 7 Ejecución de nmap –iflist	31
Figura 3. 8 Ejecución de nmap –v –A 192.168.0.10	32
Figura 3. 9 Grafico estadísticos de vulnerabilidades e impacto	38
Figura 4. 1 Menú principal de Hardening	43
Figura 4. 2 Opción de Hardening de Servicios	44
Figura 4. 3 Servicios instalados en el servidor.....	44
Figura 4. 4 Servicios instalados por default	45
Figura 4. 5 Servicios instalados por default	45
Figura 4. 6 Servicios por default en el servidor.....	46
Figura 4. 7 Opción 2 de Menú Hardening	47
Figura 4. 8 Servicios instalados en el servidor.....	48
Figura 4. 9 Opción B ingresando S para realizar el hardening a SAMBA	49
Figura 4. 10 Opción B ingresando N para NO realizar el hardening a SAMBA .	49
Figura 4. 11 Menú de Hardening SAMBA	50
Figura 4. 12 Opción 1 – Definir host permitidos para transferencia de información.	51
Figura 4. 13 Ingreso de direcciones IP para aplicar permiso	52
Figura 4. 14 Opción 1 SAMBA aplicada.....	52
Figura 4. 15 Opción 1 Samba Ya aplicada.....	53

Figura 4. 16 Opción 2 - Definir host denegados para transferencia de información	54
Figura 4. 17 Host denegados SAMBA	54
Figura 4. 18 Opción 2 SAMBA aplicado.....	55
Figura 4. 19 Opción 3 - Denegar permisos a usuarios del sistema	56
Figura 4. 20 Configuración realizada	56
Figura 4. 21 Opción 4 Reversa de Hardening SAMBA	57
Figura 4. 22 Mensaje de acción realizada	57
Figura 4. 23 Menú listo para ser nuevamente aplicado	58
Figura 4. 24 Menú de Servicios Habilitados.....	59
Figura 4. 25 Menú Hardening HTTP	59
Figura 4. 26 Opción 1 – Deshabilitar módulos innecesarios.....	60
Figura 4. 27 Opción 1 Resultado	61
Figura 4. 28 Opción 2 – Ocultar versión de Apache y OS de errores	61
Figura 4. 29 Reinicio de servicios para aplicar cambios	62
Figura 4. 30 Opción 3 – Configuración de puerto de conexión	63
Figura 4. 31 Ingreso de nuevo puerto HTTP.....	63
Figura 4. 32 Reinicio de Servicio	64
Figura 4. 33 Opción 4 – Reversa de hardening HTTP	64
Figura 4. 34 Opción 4 - Mensaje de acción realizada	65

Figura 4. 35 Opción P ingresando S para realizar hardening POSTFIX.....	65
Figura 4. 36 Menú Hardening de POSTFIX.....	66
Figura 4. 37 Opción 1 Cambios de permisos en los archivos de configuración .	67
Figura 4. 38 Resultado de cambios de permisos en los archivos de configuración	68
Figura 4. 39 Resultado de cambios de permisos en los archivos de configuración	68
Figura 4. 40 Opción 2 Configuración Banner de Bienvenida	69
Figura 4. 41 Resultados de Configuración de Banner	69
Figura 4. 42 Opcion3 Proteger servicio de ataques de DOS	70
Figura 4. 43 Resultado de Límite de Ataques DOS	70
Figura 4. 44 Opción 4 – Reverso de hardening POSTFIX.....	71
Figura 4. 45 Opción 4 - Mensaje de acción realizada.....	71
Figura 4. 46 Opción P ingresando S para realizar hardening SQUID.....	72
Figura 4. 47 Opción 1 - Apagar la función PIC y HTCP	72
Figura 4. 48 Opción 1 - Resultado de Apagar PIC y HTCP	73
Figura 4. 49 Opción 2 - Activar SNMP	73
Figura 4. 50 Opción 2 - Resultado de Activar SNMP	74
Figura 4. 51 Opción 3 - Restringir acceso por medio de SQUID	74
Figura 4. 52 Opción 3 - Creación de ACL	74

Figura 4. 53 Opción 3 - Parámetro antes de Hardening SQUID	75
Figura 4. 54 Opción 3 - Parámetro antes de Hardening SQUID	75
Figura 4. 55 Opción 3 - Parámetro antes de Hardening SQUID	75
Figura 4. 56 Opción 3 - Parámetro después de Hardening SQUID	76
Figura 4. 57 Opción 4 – Reversa de hardening SQUID	76
Figura 4. 58 Opción S ingresando S para realizar hardening SSH	77
Figura 4. 59 Opción 1 – Desactivar usuario Root	78
Figura 4. 60 Opción 1 – Resultado obtenido.....	79
Figura 4. 61 Opción 2 - Intervalo de espera de conexión remota	79
Figura 4. 62 Opción 2 – Ingreso de número de mensajes	80
Figura 4. 63 Opción 2 – Resultado de Hardening Aplicado	80
Figura 4. 64 Opción 3 – Establecer permisos a usuarios en archivos de configuración	81
Figura 4. 65 Opción 3 – Resultado obtenido.....	81
Figura 4. 66 Opción 4 – Número máximo de intentos fallidos de login	82
Figura 4. 67 Opción 4 - Ingreso de valor máximo de intentos.....	82
Figura 4. 68 Opción 4 – Resultado obtenido.....	82
Figura 4. 69 Opción 5 – Configuración de usuarios para acceso SSH	83
Figura 4. 70 Opción 5 - Ingreso de usuarios y grupos	83
Figura 4. 71 Opción 5 - Resultado de Hardening Aplicado	84

Figura 4. 72 Opción 6 – Personalización de Banner.....	84
Figura 4. 73 Opción 6 – Ingreso de texto para banner	85
Figura 4. 74 Opción 6 - Resultado obtenido	85
Figura 4. 75 Opción 7 – Configuración de tiempo de sesiones inactivas.....	86
Figura 4. 76 Opción 7- Ingrese valor de intervalo de tiempo	86
Figura 4. 77 Opción 7 – Resultado obtenido.....	86
Figura 4. 78 Opción 8 - Configuración de puerto de conexión.....	87
Figura 4. 79 Opción 8 – Ingrese valor del puerto.....	87
Figura 4. 80 Opción 8 – Resultado obtenido de Hardening Aplicado.....	88
Figura 4. 81 Opción 9 - Reversa de hardening SSH.....	88
Figura 4. 82 Opción 10 - Mensaje de acción realizada	89
Figura 4. 83 Opción T ingresando S para realizar hardening NTP	89
Figura 4. 84 Menú Hardening de NTP	90
Figura 4. 85 Opción 1 – Sincronización automática.....	91
Figura 4. 86 Opción 1 – Resultado obtenido.....	91
Figura 4. 87 Opción 2 – Sincronización manual	91
Figura 4. 88 Opción 2 – Ingreso de servidor para la sincronización	92
Figura 4. 89 Opción 2 – Resultado obtenido.....	92
Figura 4. 90 Opción 3 – Reversa de hardening NTP	93
Figura 4. 91 Opción 3 - Mensaje de acción realizada	93

Figura 4. 92 Menú principal de Hardening	94
Figura 4. 93 Submenú de Reportes	94
Figura 4. 94 Opción 1 – Hardening aplicado en la sesión actual	95
Figura 4. 95 Reporte de hardening aplicado en sesión actual	95
Figura 4. 96 Opción 2 – Hardening no aplicado en sesión actual.....	96
Figura 4. 97 Reporte de Hardening no aplicado en sesión actual	96
Figura 4. 98 Opcion 3 – Historico de servicios que cumplen Hardening.....	96
Figura 4. 99 Reporte de Hardening Aplicados (Histórico)	97
Figura 4. 100 Opción 4 – Histórico de servicios que no cumplen Hardening.....	97
Figura 4. 101 Reporte de Hardening Aplicados (Histórico)	98
Figura 4. 102 Opción 5 – Auditoria a los servicios instalados	98
Figura 4. 103 Opción B – Auditoria SAMBA.....	99
Figura 4. 104 Reporte de Auditoria Samba.....	99
Figura 4. 105 Opción H – Auditoria HTTP.....	100
Figura 4. 106 Menú de Auditoria HTTP.....	100
Figura 4. 107 Opcion 1 - Auditoria de acceso a nuestro Website	101
Figura 4. 108 Resultado de Accesos a nuestra Website.....	101
Figura 4. 109 Opción 2 - Auditoria de errores en nuestro WebSite.....	102
Figura 4. 110 Resultado de Errores en nuestro WebSite	102
Figura 4. 111 Opción Q – Auditoria SQUID	103

Figura 4. 112 Resultado de Auditoria SQUID.....	103
Figura 4. 113 Opción S – Auditoria SSH.....	104
Figura 4. 114 Resultado de Auditoria SSH.....	104
Figura 4. 115 Opción T – Auditoria NTP.....	105
Figura 4. 116 Resultado de Auditoria NTP.....	105
Figura ANEXO 2-Prueba de Aplicativo. 1 Ingreso por SSH con puerto asignado	151
Figura ANEXO 2-Prueba de Aplicativo. 2 Banner de Bienvenida asignado	152
Figura ANEXO 2-Prueba de Aplicativo. 3 Usuario Root Denegado	152
Figura ANEXO 2-Prueba de Aplicativo. 4 Ingreso de clave de usuario permitido	153
Figura ANEXO 2-Prueba de Aplicativo. 5 Ingreso de sesión con usuario asignado	153
Figura ANEXO 2-Prueba de Aplicativo. 6 Ingreso de clave de usuario negado	154
Figura ANEXO 2-Prueba de Aplicativo. 7 Indica que el usuario no puede ingresar	154
Figura ANEXO 2-Prueba de Aplicativo. 8 Mensaje de intentos fallidos llegados al máximo	155

ÍNDICE DE TABLAS

Tabla 1 Los 12 requerimientos de las PCI DSS	4
Tabla 2 Matriz de impacto de vulnerabilidades	37

INTRODUCCIÓN

El objetivo del proyecto es fortalecer la seguridad informática en servidores para instituciones financieras aplicando nuestros conocimientos y demás temas aprendidos durante el trascurso de la materia de graduación.

En el primer capítulo, haremos una descripción detallada de conceptos sobre el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS) para una mejor comprensión de lo que debe cumplir la empresa.

En el segundo capítulo se menciona el análisis de la infraestructura TI de la empresa, detallando su distribución y la tecnología aplicada en el manejo de información de tarjetas de crédito a la cual le aplicaremos nuestro proyecto.

En el tercer capítulo, se da un detalle sobre la identificación de las vulnerabilidades existentes tras el análisis de la Infraestructura TI de la empresa, su clasificación y la matriz de impacto en el negocio.

El cuarto y último capítulo se muestra la implementación de las soluciones en servidores de desarrollo, el análisis de resultados de las pruebas para luego implementarlas en servidores de Producción para al final implementar un plan de prevención contra vulnerabilidades.

CAPÍTULO 1

ESTÁNDAR PCI-DSS

1.1 Introducción

El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS), fue desarrollado por un comité conformado por la compañías más importantes de tarjetas denominado Payment Card Industry Security Standards Council (PCI SSC), como una guía para organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes, asegurando su infraestructura de TI para garantizar que la información de sus clientes este totalmente protegida y cifrada.

1.1.1 Qué es PCI DSS

El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS), es un conjunto de directrices de prácticas de seguridad de red y empresariales que deben ser observados y aplicados con la finalidad de garantizar la seguridad de la información, disminuyendo el riesgo de compromiso de esta información mediante un manejo adecuado de los datos de las tarjetas de pago.

El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS), es además un acuerdo contractual que describe en detalle cómo deben ser manejados los datos sensibles de las tarjetas de pago. La norma describe claramente lo que debe hacer en forma de “Cumplimiento de Requisitos” y la forma de demostrarlo en forma de “Requerimientos de validación”.

1.2 Requerimientos de PCI DSS

Los 12 requerimientos del Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS) son un conjunto de controles de seguridad que las empresas están obligadas a implementar para proteger los datos de las tarjetas de crédito y cumplir con el Estándar de Seguridad de Datos para la Industria de

Tarjetas de Pago (PCI DSS). Los requerimientos han sido desarrollados y mantenidos por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI).

Cualquier organización que reciba tarjetas de pago, incluyendo tarjetas de débito y crédito, deberá cumplir con los 12 requerimientos de forma directa o bien a través de un control de compensación. No obstante, los controles de compensación no siempre se admiten y deben ser aprobados bajo un criterio de caso, por parte de un asesor de seguridad cualificado de la PCI (QSA PCI).

Principios	Requerimientos
Construir y mantener una red segura	<p>Requerimiento 1: Instalar y mantener un cortafuego y su configuración para proteger la información de tarjetas.</p> <p>Requerimiento 2: No emplear parámetros de seguridad y usuarios del sistema por defecto.</p>
Proteger los datos de tarjetas	<p>Requerimiento 3: Proteger los datos almacenados de tarjetas.</p> <p>Requerimiento 4: Cifrar las transmisiones de datos de tarjetas en redes abiertas o públicas.</p>
Mantener un programa de gestión de Vulnerabilidades	<p>Requerimiento 5: Usar y actualizar regularmente software antivirus.</p> <p>Requerimiento 6: Desarrollar y mantener de forma segura sistemas y aplicaciones.</p>
Implementar medidas de control de acceso	<p>Requerimiento 7: Restringir acceso a la información de tarjetas según "need-to-know".</p> <p>Requerimiento 8: Asignar un único ID a cada persona con acceso a computadoras.</p> <p>Requerimiento 9: Restringir acceso físico a la información de tarjetas.</p>
Monitorizar y testear regularmente las Redes	<p>Requerimiento 10: Auditar y monitorizar todos los accesos a los recursos de red y datos de tarjetas.</p> <p>Requerimiento 11: Testear de forma regular la seguridad de los sistemas y procesos.</p>
Mantener una política de seguridad de la Información	<p>Requerimiento 12: Mantener una política que gestione la seguridad de la información.</p>

Tabla 1 Los 12 requerimientos de las PCI DSS

1.3 Por qué se debe cumplir PCI DSS:

Una organización puede buscar cumplir con el Estándar de seguridad de datos de la Industria de Tarjetas de Pago por varias razones.

Frecuentemente, dicho requerimiento se origina de una fuente externa; el volumen de transacciones que procesa o bien debido a un incidente de seguridad.

Algunas organizaciones y/o compañías financieras progresistas buscan cumplir con el estándar porque desde el punto de vista de sus negocios no desean estar asociadas a ningún hurto virtual, que no es otra cosa que el fraude electrónico a través de tarjetas de crédito. El cumplimiento con la norma PCI DSS permite a una organización y/o compañía financiera reducir considerablemente su exposición a los riesgos.

1.3.1 Como cumplir PCI DSS

Los comerciantes y otras entidades que almacenan, procesan y/o transmiten datos de tarjetahabientes deben cumplir con PCI DSS. Si bien el Consejo es responsable de la gestión de las normas de seguridad de datos, cada marca de tarjetas de pago mantiene sus propios programas independientes de aplicación

de conformidad.

Cada marca de tarjetas de pago ha definido los requisitos específicos para la validación de cumplimiento y presentación de informes, tales como las disposiciones para la realización de autoevaluaciones y el momento de contratar a un QSA. Dependiendo de la clasificación de la entidad o el nivel (determinado por las distintas marcas de tarjetas de pago) riesgo, los procesos de validación de cumplimiento y presentación de informes a la adquisición de instituciones financieras suelen seguir esta pista:

1. **Definición del alcance de PCI DSS.-** Determinar qué componentes del sistema se rigen por PCI DSS.
2. **Evaluación.-** Examinar la conformidad de los componentes del sistema de alcance.
3. **Controles de compensación.-** Asesorar alternativas de control de tecnología y/o procesos válidos.
4. **Informes.-** Presentar la documentación requerida por el asesor y/o entidad.
5. **Justificaciones.-** Aclarar o actualizar reportes de informes si aplican a petición de la entidad adquiriente o la marca de tarjetas de pagos.

Las preguntas específicas sobre niveles de validación de cumplimiento deben dirigirse a su entidad financiera, la adquisición o la marca de tarjetas de pago. Sólo la entidad financiera adquirente puede asignar un nivel de validación para los comerciantes.

1.3.2 Selección de un Asesor de Seguridad Calificado:

Un asesor de seguridad cualificado (QSA) es una empresa de seguridad de datos que se ha formado y está certificado por el Consejo de Estándares de Seguridad (PCI) para llevar a cabo evaluaciones de la seguridad en el lugar, para verificar el cumplimiento con PCI DSS. El QSA hará lo siguiente:

- Verificar toda la información técnica proporcionada por comercio o proveedor de servicios.
- Utilizar un juicio independiente para confirmar que el estándar se ha cumplido.
- Proporcionar apoyo y orientación durante el proceso de cumplimiento.
- Estar en el lugar para la validación de la evaluación o la duración según sea necesario.
- Revisar el producto de trabajo que soporte los requisitos de PCI DSS y su evaluación de los procedimientos de seguridad.

- Asegurarse de que la adhesión a los Procedimientos de Evaluación de Seguridad (PCI DSS)
- Validar el alcance de la evaluación.
- Selección de los sistemas y componentes del sistema que se emplean en el muestreo.
- Evaluar los controles de compensación.
- Elaborar el informe final.

El QSA seleccionado debe tener conocimientos sólidos del negocio y tener experiencia en la evaluación de la seguridad de las organizaciones similares. Ese conocimiento ayuda al QSA a entender los matices de negocio específicos por sector de seguridad de los datos de tarjetahabientes bajo PCI DSS. Por otra parte, buscar un buen ajuste con la cultura de su empresa. La evaluación concluirá si se cumplen o no, pero el QSA también trabajará con su organización para ayudar a entender cómo lograr y mantener el cumplimiento de la misma. Muchos QSA también pueden proporcionar servicios adicionales relacionados con la seguridad, tales como la evaluación de las vulnerabilidades actuales y remediación de las mismas.

1.3.3 Ámbito de la evaluación del cumplimiento

El proceso de determinación del alcance incluye la identificación de todos los componentes del sistema que se encuentran dentro o conectados al entorno de datos de titulares de tarjetas. El entorno del titular se compone de personas, procesos y tecnología que manejan datos de los tarjetahabientes o datos confidenciales de autenticación. Los componentes del sistema incluyen dispositivos de red (cable e inalámbricas), servidores y aplicaciones. Componentes de virtualización, tales como máquinas virtuales, switches, routers, dispositivos virtuales, aplicaciones virtuales, desktops, e HyperV, también se consideran los componentes del sistema dentro de PCI DSS.

Las entidades deben confirmar la exactitud e idoneidad del alcance PCI DSS mediante la realización de los siguientes pasos:

- La entidad evaluada identifica y documenta la existencia de todos los datos de los titulares de su entorno, para comprobar que no existen datos de los tarjetahabientes fuera del entorno del titular actualmente definido (CDE).
- Una vez que todas las ubicaciones de los datos de los tarjetahabientes son identificados y documentados, la entidad utiliza los resultados para comprobar que el alcance de PCI DSS es apropiado (por

ejemplo, los resultados pueden ser un diagrama o un inventario de ubicaciones de datos de titulares de tarjetas).

- La entidad considera los datos de titulares de tarjetas que se encuentren en el ámbito de la evaluación de PCI DSS y parte de la CDE a menos que tales datos se eliminan o migraron/consolidaron en el CDE definida actualmente.
- La entidad retiene la documentación que muestra cómo se confirmó el alcance de PCI DSS y los resultados, para su examen evaluador y/o de referencia durante la próxima actividad confirmación alcance SCC PCI anual.

CAPÍTULO 2

ANÁLISIS DE LA INFRAESTRUCTURA TI

2.1 Infraestructura tecnológica TI

2.1.1 DataCenter Guayaquil

DROFMAN cuenta con su sede principal en Guayaquil el cual está conformado de la siguiente manera (Figura 2):

Dos equipos de las franquicias (con las debidas certificaciones) de Visa (VEA1 y VEA2), MasterCard (MIP).

Enlace proporcionado por Level 3 y CLARO en router CISCO más un enlace directo con telefónica a Internet con lo cual se obtiene el factor de doble redundancia de enlace con la sede en Quito.

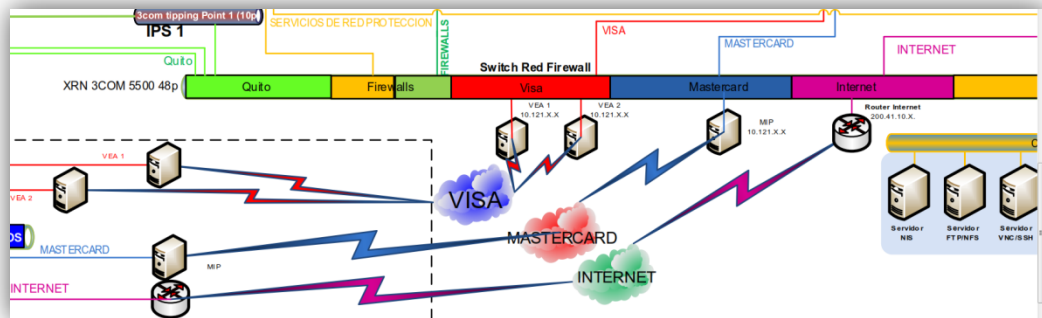


Figura 2. 1 Infraestructura TI de DROFMAN

Arquitectura de la Red (GYE):

- Red de Producción.
- Red de PRE-Producción.
- Red de Protección.
- Red DMZ.
- Red Datacard/Chip.
- Red LAN.

2.1.1.1 Red de Producción

Es la red principal dentro de la compañía, la cual cuenta con los servidores que interactúan con los aplicativos creados por la entidad y otros servidores que se encuentran en la red de protección para el manejo de las autorizaciones automáticas de tarjetas de crédito.

Comprende un Switch 3COM 5500 al cual se conectan equipos HPUX que

comprenden los servidores de: Bases de datos de los Switch Autorizaciones y Servicios, Bases de datos del servidor de Sentinel (monitoreo de fraudes), Servidor de componentes principales, File Server, Bases de Datos, Brightstor (respaldos de bases de datos en tape), Atalla de Producción (manejo de llaves encriptadoras para tarjetas de crédito), Replicador de Sentinel, Active Directory, Servidores SQUID (Proxy) y Servidor NTP.

Además se tiene un CISCO 3560 48P en el cual se encuentran las PCS que son utilizadas en el Dpto. del Centro de Cómputo las cuales son utilizadas para monitorear servicios, ejecución de procesos y demás actividades del área.

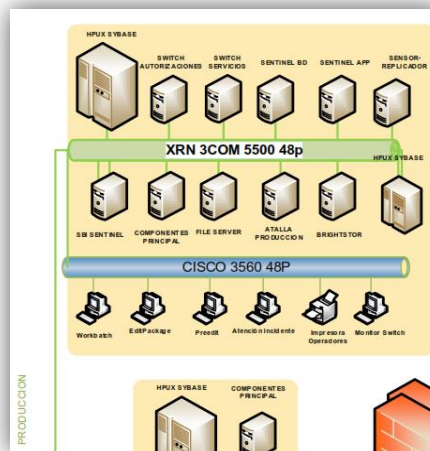


Figura 2. 2 Red de Producción Guayaquil

2.1.1.2 Red de Preproducción

Es la red que maneja la información de la base de datos antes de llegar a la red de producción manejando una interacción con el servidor de componentes y almacenando su información en un ambiente Sybase.

Consta de un Switch 3COM a la cual se conecta un Servidor de componentes principal y un Servidor HPUX Sybase protegidos por el Firewall Interno.

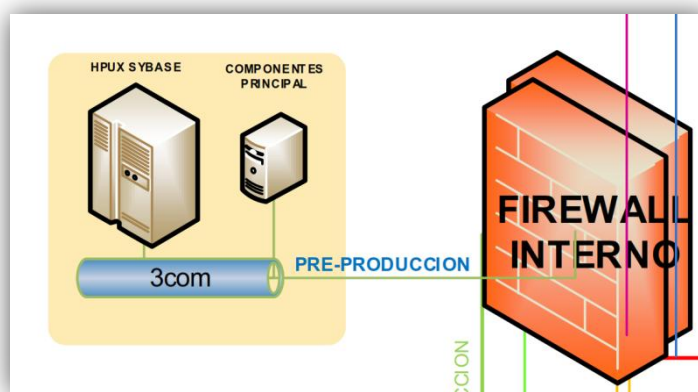


Figura 2. 3 Red de PRE-Producción Guayaquil

2.1.1.3 Red de Protección de equipos críticos.

Como su nombre lo indica esta red protege los equipos que contienen información sensible, la cual de no estar en esta red sería vulnerable a cualquier desvío de información.

Comprende un CISCO 3560G 24P a la cual se conectan un Servidor NIS, Servidor SFTP/NFS, Servidor VNC, Servidor SAMBA, Servidor SSH, Servidor de Correo electrónico y Smart Center.

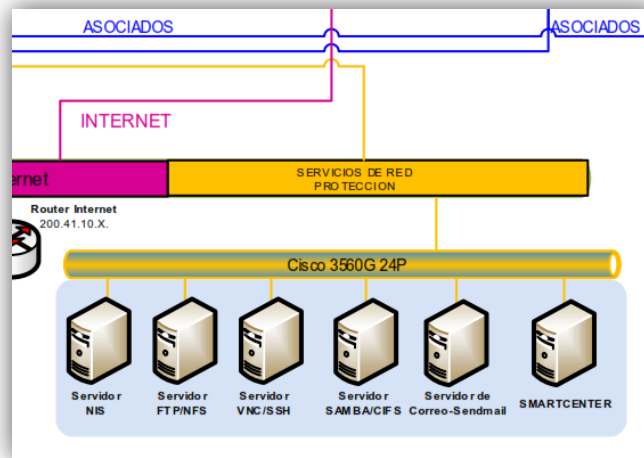


Figura 2. 4 Red de Protección Guayaquil

2.1.1.4 Red DMZ

Es la red que se conecta a través de un 3COM TIPPING POINT 1(10p) pasando por el Firewall Externo; siendo los enlaces principales con las entidades, a quienes se brinda el servicio del Portal Transaccional.

Además comprende de un Switch 3 COM 4226t a la cual se conectan al Servidor del Switch de Alignet, Portal transaccional, Active Directory, SFTP Server (por el cual se envían y reciben archivos de los establecimientos), Service Desk (mesa de ayuda con los bancos) y el servidor de correo electrónico.

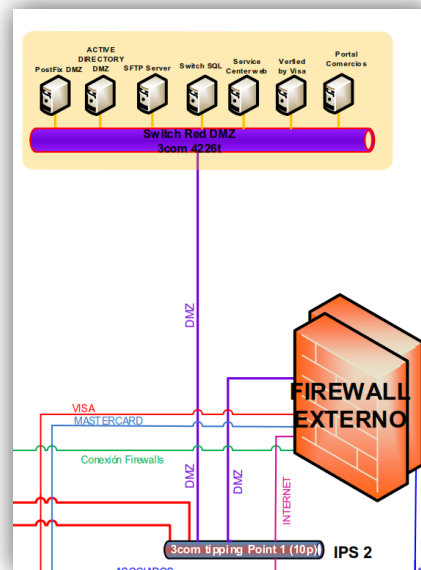


Figura 2. 5 Red de DMZ Guayaquil

2.1.1.5 Red Datacard /Chip

La red de Datacard maneja los servidores encargados de generar información de tarjeta de crédito para la creación de las mismas.

Comprende de un Switch 3COM 4226t las cuales se conectan Servidores de Chip tanto para impresiones de tarjetas con banda magnética, HSM e impresión de tarjetas con chip inteligente, adicional sus PC's de personalización y zonificación, las cuales son encargadas de la creación de las tarjetas y sus respectivos sobres para su entrega.

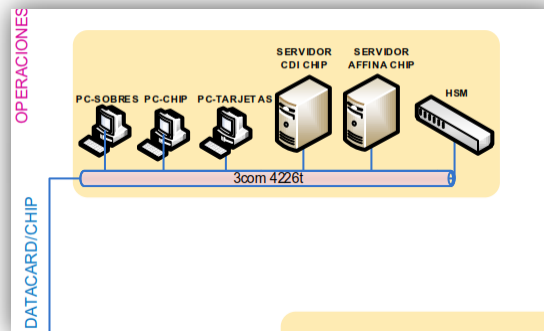


Figura 2. 6 Red Datacard / Chip Guayaquil

Posee además un Switch 4226t que incluye las PC's de Mantenimiento & Producción, Operaciones, Analistas de riesgo y Autorizaciones manuales de tarjetas de crédito.

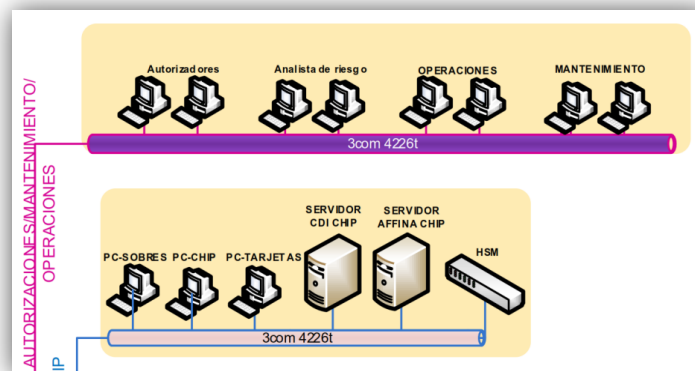


Figura 2. 7 Red de Mantenimiento & Producción Guayaquil

2.1.1.6 Red LAN

Esta red es la encargada de interactuar con todos los equipos de la empresa tanto para su autenticación por medio del Domain Controller y la sincronización del tiempo.

Comprende servidores de Active Directory, Servidor NTP, Servidor Proxy y el Servidor de la Intranet para uso interno de la empresa.

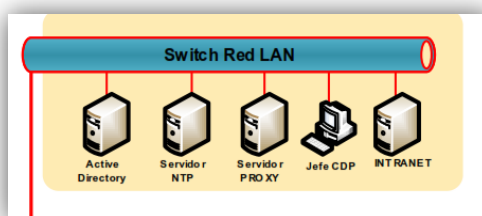


Figura 2. 8 Red LAN Guayaquil

La conexión hacia los bancos asociados se realiza por un Firewall Externo direccionado a un XRN 3COM 5500 24P los cuales van a los ROUTERS (Router Motorola Produbanco y Router CISCO Telconet) los que van a los enlaces principales de cada establecimiento pasando por sus Router y Firewall respectivos, dichos Equipos cuenta con las seguridades respectivas a las cuales se les aplicó el tema de enlace VPN; la comunicación entre la sede de Guayaquil y lo Bancos Socios se tiene configurado que el canal de enlace se encuentra encriptado.

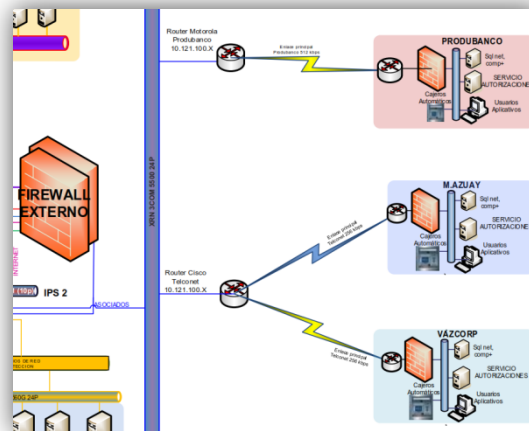


Figura 2. 9 Enlace con Bancos Asociados

2.1.2 DataCenter Quito

DROFMAN S.A. como empresa certificada de generación de tarjetas de crédito tiene un sitio alternativo o contingencia ubicado en la ciudad de Quito la cual tiene infraestructura de igual características a la que se tiene en su matriz, la misma entra en funcionamiento cuando los enlaces de Guayaquil están fuera de línea y como plan de acción todos los servicios son direccionados al sitio de contingencia.

Está constituida de la siguiente manera:

Red LAN (UIO)

Red DMZ (UIO)

Red de Protección de equipos críticos (UIO)

2.1.2.1 Red LAN UIO

Esta red como sitio alternativo se encargada de interactuar sólo con equipos críticos de la empresa así también tanto para su autenticación por medio del Domain Controller y la sincronización del tiempo.

Comprende el Servidor Active Directory, equipos de Sentinel (monitoreo de fraude), Switch de Autorizadores y Servicios, una Base de Datos HP/UX Sybase, Atalla Alterno y 2 PCS para procesos y monitoreo en el centro de cómputo.

2.1.2.2 Red DMZ UIO

Es la red que se conecta a través de un 3COM TIPPING POINT 1(10p) pasando por el Firewall Quito; siendo también enlaces principales con las entidades .

Comprende de Servidores NTP y SFTP conectados a nuestros establecimientos asociados.

2.1.2.3 Red de Protección de equipos críticos UIO.

Comprende el Servidor de componentes, Chip, HSM, PCS de personalización y zonificación (tarjetas de crédito).

Todo tipo de información transmitida a Quito pasa por el Firewall respectivo el

cual permite el paso de la misma a los establecimientos o franquicias respectivamente.

De la misma manera que Guayaquil, el sitio alterno en Quito posee equipos de las franquicias de Visa (VEA1 y VEA2) y MasterCard (MIP) las cuales entran a operar en cuanto se haga el cambio o direccionamiento respectivo y así poder trabajar Quito como centro principal de transmisión y proceso de información a franquicias y establecimientos.

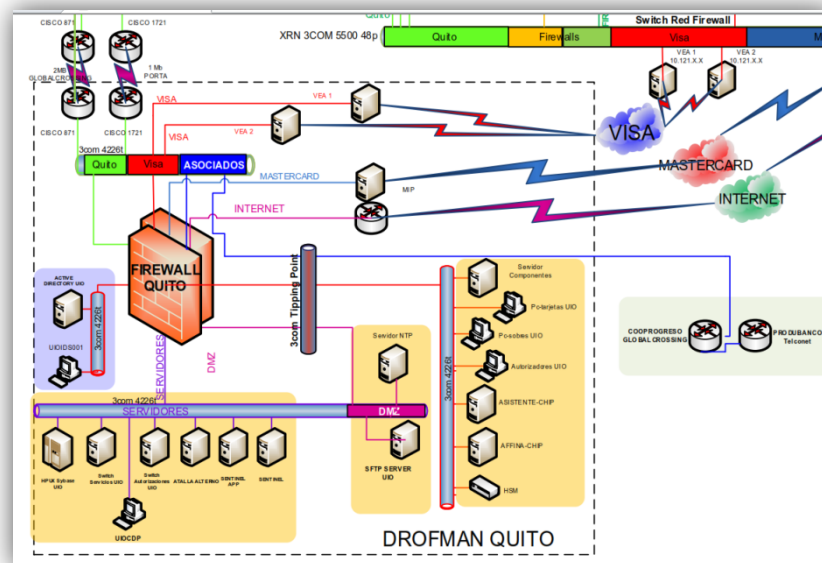


Figura 2. 10 Red de Infraestructura Quito DROFMAN

2.1.3 LAN

A nivel LAN se tiene segmentada la red, esta arquitectura se la tiene para precautelar la información que se maneja entre los equipos, a la vez toda la red LAN se encuentra protegido por los Firewalls Externos e Internos y controlando el tráfico que llega desde los perímetros fuera de la red LAN por los Equipo Tipping Point, con esto se mitiga el impacto que se tenga de vulnerabilidad de la red LAN y asegurando el funcionamiento de la red LAN.

2.1.4 WAN

La conexión WAN es suministrada por los proveedores para la comunicación entre la sede de Guayaquil y los Bancos, dicho enlace que provee la empresa que se contrata es la responsable de la Seguridad que se maneje sobre estos equipos, de igual manera se solicita que toda conectividad WAN entre la Sedes y los cliente sea segura, cifrada. De esta manera se garantiza la confiabilidad del enlace WAN para la conexión de datos entre las entidades.

2.1.5 Seguridades

A nivel perimetral de la red se consideró todas las normas de Seguridad, que son solicitadas por PCI y la norma ISO 27001 con las cuales se asegura el nivel

de Seguridad a nivel de la red, las cuales implican la instalación de un Firewall Perimetral con todas las normas de seguridad, también se tiene colocado un IPS para el control del tráfico que viene desde los clientes a la Empresa DROFMAN, todo paquete que llega hasta el IPS es analizado de acuerdo al comportamiento que tiene si se lo detecta este será bloqueado, caso contrario los paquetes serán permitidos.

En el Firewall Externo e Interno se tiene configurado reglas en las cuales se permite o deniega el acceso según las IP's que los clientes determinen para la conexión, el resto será denegado.

CAPÍTULO 3

Identificación de vulnerabilidades

3.1 Identificación de Vulnerabilidades

La metodología para la detección de vulnerabilidades que se propone consta de tres fases, la **primera fase** consiste en obtener tanta información como sea posible de la red objetivo, para esto se implementan técnicas que se basan en diferentes tipos de consultas a servidores DNS y técnicas que se basan en el análisis de los mensajes de enrutamiento. Se resalta que esta fase no busca obtener vulnerabilidad alguna, lo que se pretende con ella es obtener una lista lo más amplia posible sobre los equipos con presencia en Internet de la red objetivo. Dicha lista de equipos de red es utilizada en la **segunda fase** llamada

escaneo de puertos y enumeración de servicios, en esta fase se evalúan los equipos obtenidos para determinar los puertos y servicios que están activos en cada uno de ellos. Dependiendo del tipo de puerto y servicio que este activo en cada equipo se puede inferir el rol que este juega dentro de la organización. Una vez obtenida la lista de los equipos de la red objetivo y habiendo determinado cuáles de ellos juegan un rol crítico, se procede con la **tercera fase** o **fase final** de la metodología propuesta, la cual evaluará a los equipos críticos en busca de vulnerabilidades. Es en esta última fase en la que se realiza la evaluación de todos los servicios y puertos activos de cada uno de los equipos encontrados como críticos para la red objetivo.

El esquema de la metodología para detección de vulnerabilidades se presenta en la Figura 3. 1 en la cual puede verse la metodología propuesta consta de tres fases, las cuales se detallan a continuación:

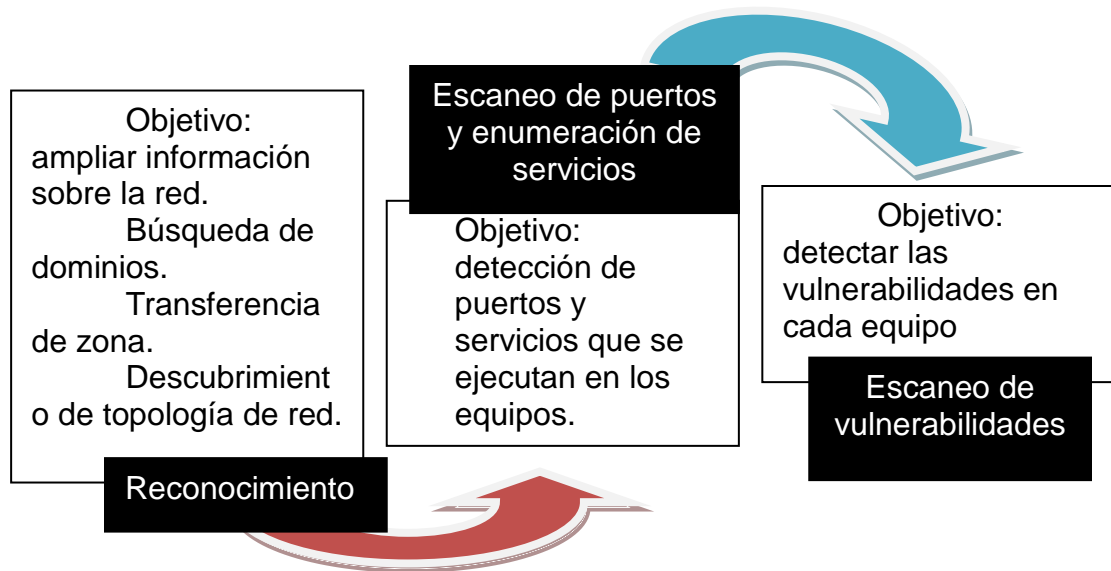


Figura 3. 1 Metodología para la detección de vulnerabilidades

La figura anterior muestra cada una de las fases que deben llevarse a cabo. Después de realizar la ejecución y al obtener el reporte se logra evidenciar los riesgos que afectan a la empresa poniendo en peligro su infraestructura tecnológica TI, llegando a causar daños no sólo en la información sino; traer consecuencias económicas y afectando el prestigio de la empresa.

De igual manera se sugieren las posibles soluciones que permitan mitigar, aceptar o delegar estos riesgos, a la vez fortaleciendo la seguridad de la misma. Estas sugerencias tienen como fin encaminar a la empresa a la aplicación de buenas prácticas.

3.2 Determinación de vulnerabilidades en la infraestructura TI

Para determinar las vulnerabilidades en la infraestructura se utilizó el comando **NMAP** la cual es una herramienta de red para administrar sistemas al momento de monitorizar redes, equipos y detectar vulnerabilidades antes que sean aprovechadas para entrar a nuestro equipo o red empresarial. Tiene funciones integradas que permiten analizar cualquier red y equipo sin importar si los objetos de escaneo están en una red local o en un servidor remoto de Internet.

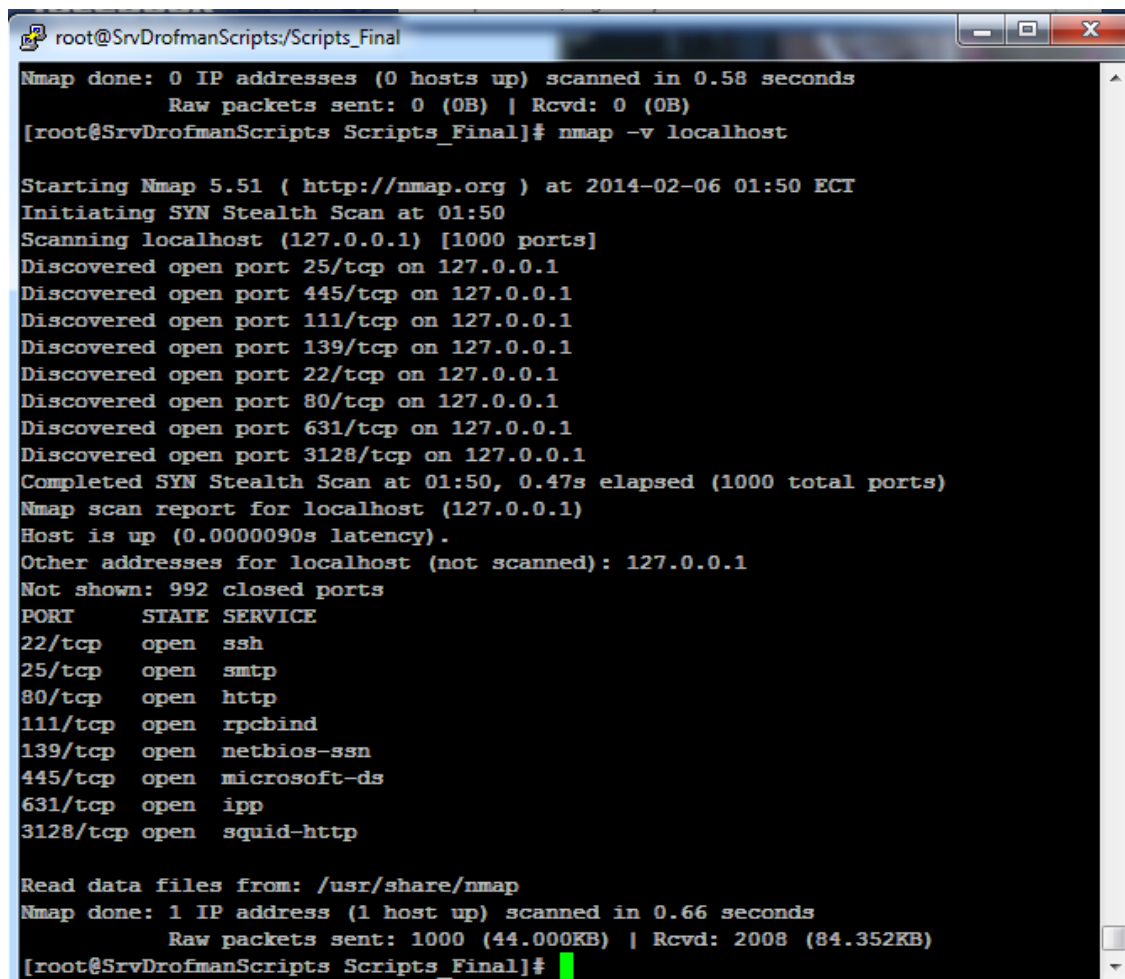
El estudio de los riesgos con esta herramienta se realiza abarcando varios planos tales como personal, a nivel de proceso y con la tecnología permitiendo de esta manera el mejoramiento de la seguridad en todos los aspectos

Tal como se mencionó en el punto anterior se realizó el reconocimiento de la red donde se obtuvo la información necesaria, luego el escaneo de los puertos donde se mostraron los servicios con sus estados y al final se somete a evaluación de los resultados para determinar los potenciales riesgos a los que están expuestos los equipos.

En base a lo indicado y con la ejecución de la herramienta mencionada se obtuvo los siguientes resultados:

- `nmap -v localhost`: muestra la información de los puertos TCP habilitados, su estado y a qué servicio se refiere. Se pueden observar los

puertos de servicios tales como SSH, HTTP y otros en los cuales existen riesgos por ser puertos inseguros.



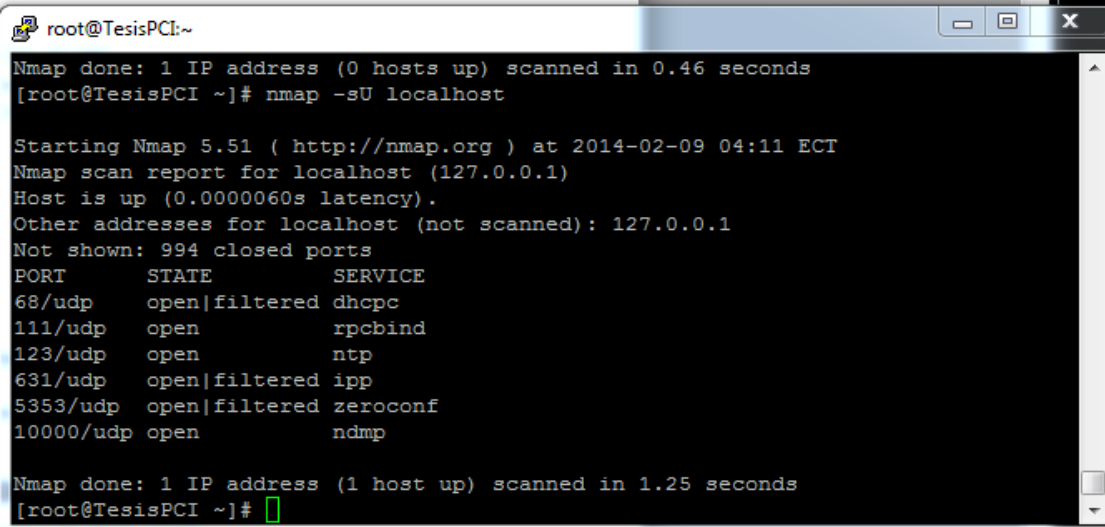
```
root@SrvDrofmanScripts:/Scripts_Final
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.58 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
[root@SrvDrofmanScripts Scripts_Final]# nmap -v localhost

Starting Nmap 5.51 ( http://nmap.org ) at 2014-02-06 01:50 ECT
Initiating SYN Stealth Scan at 01:50
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 25/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 111/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Discovered open port 3128/tcp on 127.0.0.1
Completed SYN Stealth Scan at 01:50, 0.47s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000090s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3128/tcp  open  squid-http

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
Raw packets sent: 1000 (44.000KB) | Rcvd: 2008 (84.352KB)
[root@SrvDrofmanScripts Scripts_Final]#
```

Figura 3. 2 Ejecución de nmap -v localhost

- nmap -sU localhost: muestra la información de los puertos UDP habilitados, su estado y a qué servicio se refiere.



```

root@TesisPCI:~
Nmap done: 1 IP address (0 hosts up) scanned in 0.46 seconds
[root@TesisPCI ~]# nmap -sU localhost

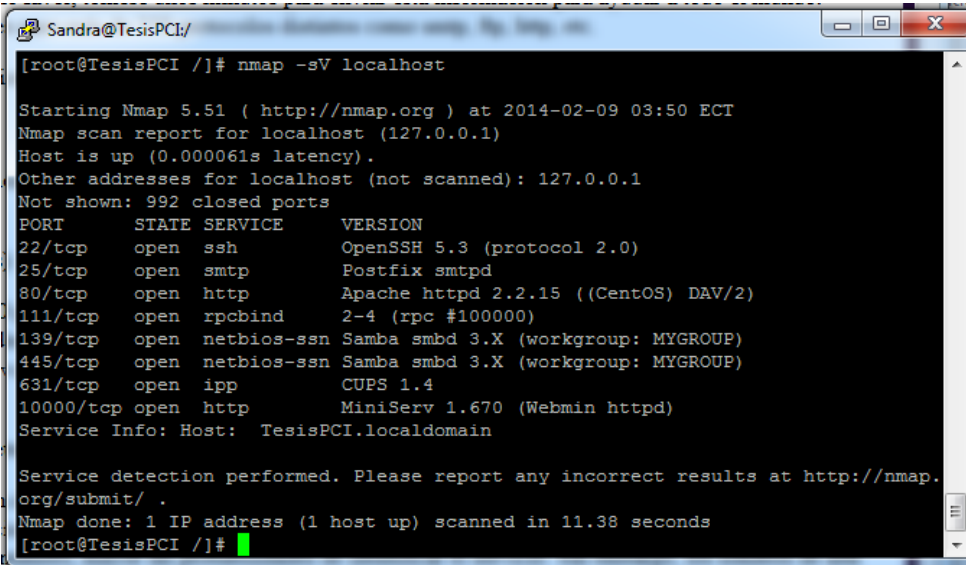
Starting Nmap 5.51 ( http://nmap.org ) at 2014-02-09 04:11 ECT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 994 closed ports
PORT      STATE      SERVICE
68/udp    open|filtered dhcpc
111/udp   open       rpcbind
123/udp   open       ntp
631/udp   open|filtered ipp
5353/udp  open|filtered zeroconf
10000/udp open       ndmp

Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds
[root@TesisPCI ~]#

```

Figura 3. 3 Ejecución de nmap -v localhost

- nmap -sV localhost: muestra los puertos, sus estados con los servicios y las versiones de cada servicio.



```

Sandra@TesisPCI:/
[root@TesisPCI /]# nmap -sV localhost

Starting Nmap 5.51 ( http://nmap.org ) at 2014-02-09 03:50 ECT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000061s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3 (protocol 2.0)
25/tcp    open  smtp         Postfix smtpd
80/tcp    open  http         Apache httpd 2.2.15 ((CentOS) DAV/2)
111/tcp   open  rpcbind     2-4 (rpc #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: MYGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: MYGROUP)
631/tcp   open  ipp          CUPS 1.4
10000/tcp open  http         MiniServ 1.670 (Webmin httpd)
Service Info: Host: TesisPCI.localdomain

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.38 seconds
[root@TesisPCI /]#

```

Figura 3. 4 Ejecución de nmap -sv localhost

En la figura 3.4 se muestra el servicio http con la versión 2.2.15.

- `nmap -A localhost | more`: muestra un análisis agresivo donde se muestra información antes mencionada adicional muestra seriales los cuales deben estar cifrados y rastros de métodos de riesgos potenciales.

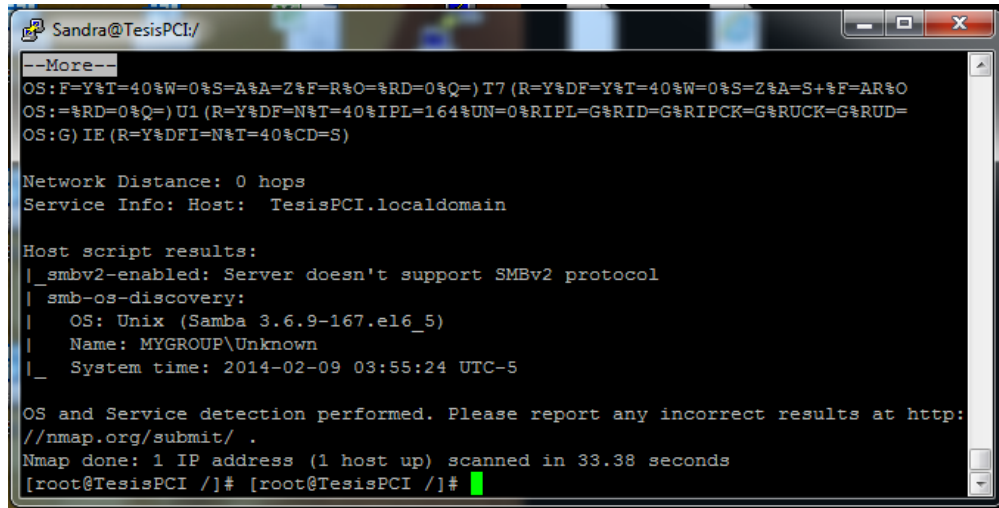
```

Sandra@TesisPCI:/
Nmap done: 1 IP address (1 host up) scanned in 33.77 seconds
[root@TesisPCI /]# nmap -A localhost | more

Starting Nmap 5.51 ( http://nmap.org ) at 2014-02-09 03:55 ECT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000027s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey: 1024 68:33:2b:c0:d7:02:0d:1e:25:1a:cc:11:3e:10:0d:62 (DSA)
|_ 2048 d9:2a:14:d9:32:53:d1:d5:8b:13:c1:fc:c9:fa:d2:55 (RSA)
25/tcp    open  smtp         Postfix smtpd
80/tcp    open  http         Apache httpd 2.2.15 ((CentOS) DAV/2)
|_ http-methods: Potentially risky methods: TRACE
|_ See http://nmap.org/nse/doc/scripts/http-methods.html
|_ http-title: Inicio
111/tcp   open  rpcbind     2-4 (rpc #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: MYGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: MYGROUP)
631/tcp   open  ipp         CUPS 1.4
|_ http-robots.txt: 1 disallowed entry
|_/
|_ http-methods: Potentially risky methods: PUT
|_ See http://nmap.org/nse/doc/scripts/http-methods.html
10000/tcp open  http        MiniServ 1.670 (Webmin httpd)
|_ http-robots.txt: 1 disallowed entry
|_/
|_ http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_ http-title: Login to Webmin
|_ http-favicon:
No exact OS matches for host (If you know what OS is running on it, see http://n
map.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.51%D=2/9%OT=22%CT=1%CU=38769%PV=N%DS=0%DC=L%G=Y%TM=52F74286%P=i
OS:386-redhat-linux-gnu)SEQ(SP=105%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)SEQ(SP
OS:=105%GCD=2%ISR=10C%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=105%GCD=1%ISR=10B%TI=Z%CI=
OS:Z%II=I%TS=A)OPS(O1=M400CST11NW6%O2=M400CST11NW6%O3=M400CNNT11NW6%O4=M400
OS:CST11NW6%O5=M400CST11NW6%O6=M400CST11)WIN(W1=8000%W2=8000%W3=8000%W4=800
OS:0%W5=8000%W6=8000)ECN(R=Y%DF=Y%T=40%W=8018%O=M400CNNSNW6%CC=Y%Q=)T1(R=Y%
OS:DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A
OS:=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%D
--More--

```

Figura 3. 5 Ejecución de nmap -A localhost



```

Sandra@TesisPCI:/
--More--
OS: F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=) T7 (R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=) U1 (R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=
OS:G) IE (R=Y%DFI=N%T=40%CD=S)

Network Distance: 0 hops
Service Info: Host: TesisPCI.localdomain

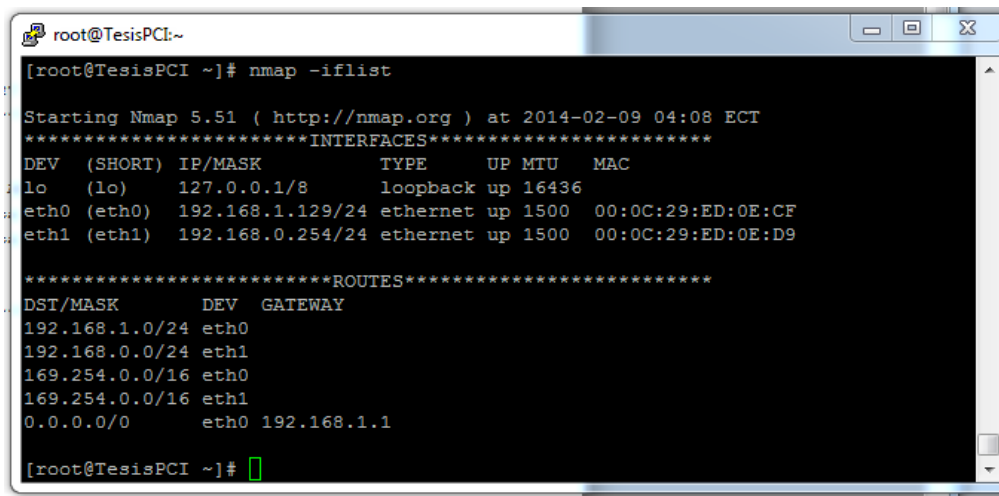
Host script results:
|_ smbv2-enabled: Server doesn't support SMBv2 protocol
|_ smb-os-discovery:
|   OS: Unix (Samba 3.6.9-167.e16_5)
|   Name: MYGROUP\Unknown
|_   System time: 2014-02-09 03:55:24 UTC-5

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.38 seconds
[root@TesisPCI /]# [root@TesisPCI /]#

```

Figura 3. 6 Ejecución de nmap -v localhost

- nmap -iflist: muestra información que por norma PCI es considerada sensible y debe estar oculta a cualquier tipo de análisis.



```

root@TesisPCI:~
[root@TesisPCI ~]# nmap -iflist

Starting Nmap 5.51 ( http://nmap.org ) at 2014-02-09 04:08 ECT
*****INTERFACES*****
DEV (SHORT) IP/MASK      TYPE      UP MTU  MAC
lo (lo)      127.0.0.1/8      loopback up 16436
eth0 (eth0)  192.168.1.129/24 ethernet up 1500 00:0C:29:ED:0E:CF
eth1 (eth1)  192.168.0.254/24 ethernet up 1500 00:0C:29:ED:0E:D9

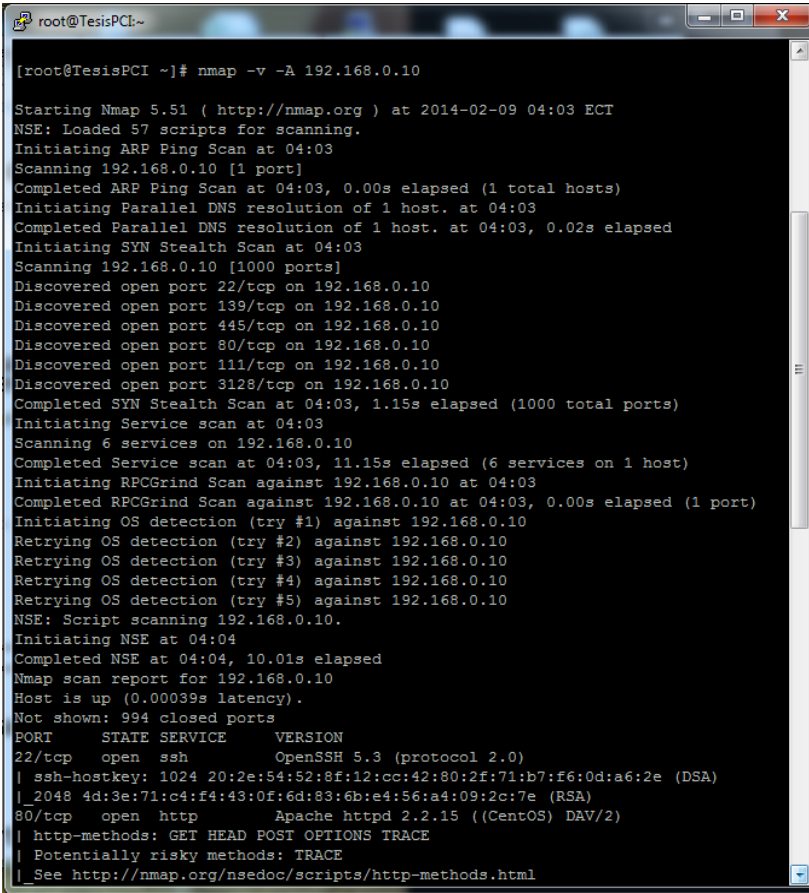
*****ROUTES*****
DST/MASK      DEV  GATEWAY
192.168.1.0/24 eth0
192.168.0.0/24 eth1
169.254.0.0/16 eth0
169.254.0.0/16 eth1
0.0.0.0/0     eth0 192.168.1.1
[root@TesisPCI ~]#

```

Figura 3. 7 Ejecución de nmap -iflist

Las bases de datos son un elemento fundamental para la mayoría de las empresas. Prácticamente cualquier aplicación empresarial está construida alrededor de una base de datos donde se almacena información altamente sensible y vital para el funcionamiento del negocio.

- `nmap -v -A`: Habilita la detección de SO y de versión de la IP asignada.



```
[root@TesisPCI ~]# nmap -v -A 192.168.0.10

Starting Nmap 5.51 ( http://nmap.org ) at 2014-02-09 04:03 ECT
NSE: Loaded 57 scripts for scanning.
Initiating ARP Ping Scan at 04:03
Scanning 192.168.0.10 [1 port]
Completed ARP Ping Scan at 04:03, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:03
Completed Parallel DNS resolution of 1 host. at 04:03, 0.02s elapsed
Initiating SYN Stealth Scan at 04:03
Scanning 192.168.0.10 [1000 ports]
Discovered open port 22/tcp on 192.168.0.10
Discovered open port 139/tcp on 192.168.0.10
Discovered open port 445/tcp on 192.168.0.10
Discovered open port 80/tcp on 192.168.0.10
Discovered open port 111/tcp on 192.168.0.10
Discovered open port 3128/tcp on 192.168.0.10
Completed SYN Stealth Scan at 04:03, 1.15s elapsed (1000 total ports)
Initiating Service scan at 04:03
Scanning 6 services on 192.168.0.10
Completed Service scan at 04:03, 11.15s elapsed (6 services on 1 host)
Initiating RPCGrind Scan against 192.168.0.10 at 04:03
Completed RPCGrind Scan against 192.168.0.10 at 04:03, 0.00s elapsed (1 port)
Initiating OS detection (try #1) against 192.168.0.10
Retrying OS detection (try #2) against 192.168.0.10
Retrying OS detection (try #3) against 192.168.0.10
Retrying OS detection (try #4) against 192.168.0.10
Retrying OS detection (try #5) against 192.168.0.10
NSE: Script scanning 192.168.0.10.
Initiating NSE at 04:04
Completed NSE at 04:04, 10.01s elapsed
Nmap scan report for 192.168.0.10
Host is up (0.00039s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey: 1024 20:2e:54:52:8f:12:cc:42:80:2f:71:b7:f6:0d:a6:2e (DSA)
|_ 2048 4d:3e:71:c4:f4:43:0f:6d:83:6b:e4:56:a4:09:2c:7e (RSA)
80/tcp    open  http         Apache httpd 2.2.15 ((CentOS) DAV/2)
|_ http-methods: GET HEAD POST OPTIONS TRACE
|_ Potentially risky methods: TRACE
|_ See http://nmap.org/nse/doc/scripts/http-methods.html
```

Figura 3. 8 Ejecución de `nmap -v -A 192.168.0.10`

- El núcleo del sistema operativo realiza las funciones básicas como la interacción con el hardware, la gestión de la memoria, la comunicación entre procesos y la asignación de tareas. La existencia de vulnerabilidades en el núcleo puede provocar problemas de seguridad que afecten a todos los componentes del sistema. Es muy importante la correcta configuración del núcleo, para evitar o reducir el alcance de las posibles vulnerabilidades.
- Configuración incorrecta de servicios de compartición de recursos e información.
- Los equipos Unix tiene deficiencias en sus mecanismos de autenticación.
- Existe una mala gestión en la administración de las redes.

3.3 Clasificación de vulnerabilidades

Después de haber ejecutado el comando nmap se puede ver el estado en que se haya la seguridad de los servicios en DROFMAN S.A., siendo esta analizada y clasificada en tres aspectos generando un resultado severo en las áreas analizadas, siendo estos:

- Infraestructura.
- Operaciones.
- Personal.

3.3.1 Infraestructura

Se logró evidenciar que existen punto críticos los cuales están relacionados con:

- **Defensa del perímetro.-** siendo la principal protección contra intrusos se encontraron dos puntos críticos los cuales ponen en riesgo la seguridad de la infraestructura informática de la empresa. Los cuales fueron el acceso remoto ya que cuenta con una forma de conexión insegura y adicional tiene un puerto de conexión por default la cual es vulnerable.

- **Autenticación.-** no se encontraron procedimientos de autenticación de usuarios administradores y remotos lo cual ayuda a que los intrusos accedan sin autorización a la red mediante ataques locales o remotos.

No se utilizan directivas de contraseñas (cuenta administrador y cuenta de usuario) y los usuarios tienen habilitados accesos administrativos en sus estaciones de trabajo.

3.3.2 Operacional

Se visualizan puntos críticos los que corresponden a directivas de seguridad, gestión de actualizaciones/revisiones y a las copias de seguridad/recuperación ya que no existen pautas para regular el uso adecuado y seguro de tecnologías

al igual que los procesos de la empresa. Esta área incluye directivas para los aspectos de seguridad como los usuarios, los sistemas y los datos. Adicional se evidenció que no existe un proceso de gestión de cambios y configuraciones.

3.3.3 Personal

La empresa no cuenta con evaluaciones de seguridad al personal interno, tampoco cuenta con algún programa de capacitación específica para la seguridad de la empresa mostrando como punto crítico este aspecto en el área del personal.

3.4 Matriz de impacto de vulnerabilidades en la empresa.

Después del análisis realizado a las áreas mencionadas se muestra un cuadro de clasificación donde se muestra su nivel de impacto para ser considerados para fortalecer la infraestructura de la empresa.

Clasificación	Vulnerabilidad	% Probabilidad	Nivel de impacto
Infraestructura	Configuración incorrecta de servicios de compartición de recursos e información.	20	Alta
Infraestructura	Los equipos Unix tiene deficiencias en sus mecanismos de autenticación	10	Alta
Infraestructura	Existe una mala gestión en la administración de las redes	5	Alta
Infraestructura	Gestionar un proceso de creación de informes de incidentes y repuesta documentado para garantizar que todos los problemas e incidentes se revisan y se evalúan de forma coherente, permitiendo llevar un indicativo de los incidentes presentados al igual que las soluciones dadas en su momento, para que sirva de referencia a futuros incidentes.	20	Alta
Infraestructura	Resultados no esperados como el caso de que los recursos del sistemas estén siendo agotados fácilmente (Memoria RAM, Procesador)	10	Medio
Infraestructura	Contar con un adecuado sistema de copias de seguridad y recuperación en caso de desastres para reanudar el negocio sin afectar funcionamiento.	5	Alta
Operaciones	Considere implantar otro factor de autenticación para disminuir el riesgo de accesos no autorizados.	20	Medio
Infraestructura	La existencia de vulnerabilidades en el núcleo puede provocar problemas de seguridad que afecten a todos	5	Alta

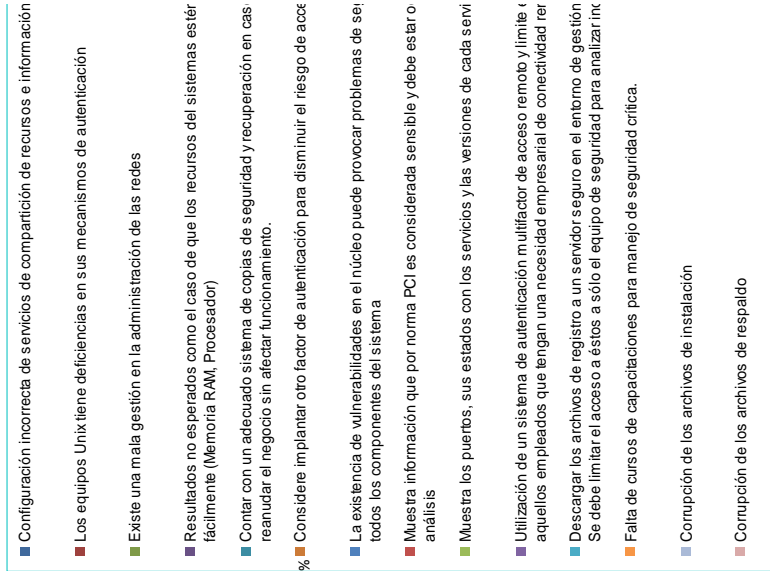
	los componentes del sistema		
Infraestructura	Muestra información que por norma PCI es considerada sensible y debe estar oculta a cualquier tipo de análisis	10	Medio
Infraestructura	Muestra los puertos, sus estados con los servicios y las versiones de cada servicio	20	Medio
Operaciones	Utilización de un sistema de autenticación multifactor de acceso remoto y limite el acceso únicamente a aquellos empleados que tengan una necesidad empresarial de conectividad remota.	10	Medio
Operaciones	Descargar los archivos de registro a un servidor seguro en el entorno de gestión para fines de almacén. Se debe limitar el acceso a éstos a sólo el equipo de seguridad para analizar incidentes.	5	Medio
Personal	Falta de cursos de capacitaciones para manejo de seguridad crítica.	20	Medio
Infraestructura	Corrupción de los archivos de instalación	5	Bajo
Infraestructura	Corrupción de los archivos de respaldo	5	Bajo

Tabla 2 Matriz de impacto de vulnerabilidades

En base al un programa de gestión de vulnerabilidades el cual fue alimentado en base a la información de los reportes obtenidos de los análisis realizados, pruebas y demás acciones tomadas se obtuvo la información que se detalla en la tabla anterior donde se clasifican las vulnerabilidades mostrando el nivel de riesgo de impacto y el porcentaje de probabilidad que se presente en la empresa. Esta información también se detalla el siguiente gráfico:

Vulnerabilidades, estadísticas e impacto

Vulnerabilidades existentes



Lista de probabilidades que suceda

- Configuración incorrecta de servicios de compartición de recursos e información
- Los equipos Unix tiene deficiencias en sus mecanismos de autenticación
- Existe una mala gestión en la administración de las redes
- Resultados no esperados como el caso de que los recursos del sistemas estén fácilmente (Memoria RAM, Procesador)
- Contar con un adecuado sistema de copias de seguridad y recuperación en caso de reanudar el negocio sin afectar funcionamiento.
- Considerare implantar otro factor de autenticación para disminuir el riesgo de acceso
- La existencia de vulnerabilidades en el núcleo puede provocar problemas de seguridad en todos los componentes del sistema
- Muestra información que por norma PCI es considerada sensible y debe estar protegida
- Muestra los puertos, sus estados con los servicios y las versiones de cada servicio
- Utilización de un sistema de autenticación multifactor de acceso remoto y limitar el acceso a aquellos empleados que tengan una necesidad empresarial de conectividad remota
- Descargar los archivos de registro a un servidor seguro en el entorno de gestión de seguridad. Se debe limitar el acceso a éstos a sólo el equipo de seguridad para analizar los logs
- Falta de cursos de capacitaciones para manejo de seguridad crítica.
- Corrupción de los archivos de instalación
- Corrupción de los archivos de respaldo

Figura 3. 9 Grafico estadísticos de vulnerabilidades e impacto

CAPITULO 4

IMPLEMENTACIÓN DE SOLUCIONES A LAS VULNERABILIDADES IDENTIFICADAS

4.1 Aplicación de soluciones en servidores de prueba.

En base al análisis realizado mediante el cual fueron obtenidas las vulnerabilidades antes mencionadas y su matriz de impacto se plantea aplicar un plan de acción en servidores de prueba para así tratar de mitigar las vulnerabilidades halladas.

- En los servicios con puertos inadecuados se cambian los puertos que se encuentran por default a puertos seguros

- Implementar las cláusulas para el cumplimiento del Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS).
- Llevar un control de perfiles de usuarios y permisos asignados de los mismos para mitigar los accesos innecesarios a la infraestructura TI.
- Implementar Hardening de servicios críticos de infraestructura TI expuestos a Internet.
- Aplicar soluciones a las vulnerabilidades identificadas, a fin de evitar exponer servicios críticos de la infraestructura TI.
- Mantener un programa de gestión de vulnerabilidades, para minimizar las consecuencias por ataques de seguridad informática.
- Definir nombres de equipos para transferir y denegar información.
- Deshabilitar módulos innecesarios.
- Ocultar versión de servicios y demás información sensible para así evitar que sea utilizada para ocasionar perjuicios en aplicaciones y servicios.
- Desactivar usuarios administradores para así no realizar conexiones remotas.
- Configurar parámetros de conexiones remotas (tiempos de espera, números máximo de intentos fallidos, etc). (Anexo 2)

4.2 Análisis de resultados de impactos en servidores de prueba.

Luego de aplicar el plan de acción detallado en el punto anterior se procede a realizar pruebas obteniendo los siguientes resultados:

- Habiendo aplicado cambios de puertos que vienen por default, se obtuvo mayor seguridad evitando filtraciones de información.
- Habiendo implementado normas de seguridad, se obtuvo mayor control de seguridad a cualquier tipo de vulnerabilidad existente.
- Aplicado políticas de usuario se obtiene un mayor control con respecto a los accesos a la infraestructura TI.
- Aplicando programas de gestión de vulnerabilidades se obtiene información importante de cómo actuar en caso de recaer en incidentes.
- Habiendo deshabilitados módulos innecesarios en las aplicaciones se gana mayor rendimiento a nivel de procesos en los servidores.
- No mostrando información sensible ya sea de versiones u otro tipo se gana confidencialidad en los servicios instalados.
- Por normas de PCI el usuario administrador Root debe estar deshabilitado, para evitar daños involuntarios en los mismos.

4.3 Implementación de las soluciones en Producción

En base a la análisis realizado en base a las vulnerabilidades encontradas se implementará un sistema el cual se solucionará y permitirá que las vulnerabilidades encontradas sean mitigadas para de esta manera tener mejor segura la información de la empresa y proveer un servicio seguro para nuestros clientes, mediante el siguiente sistema se realizará el Hardening de servidores en base a las normas PCI donde a continuación se detalla cada menú con sus submenús y opciones que lo componen.

4.3.1 Menú Principal de Aplicación de Hardening basado en la norma PCI DSS

Corresponde la ventana principal interactiva mediante la cual se llevará el control de los servicios habilitados, se realizará el hardening de los servicios y se presentarán reportes en base a los realizado, desde luego tiene su opción respectiva de salir ingresando el 0.

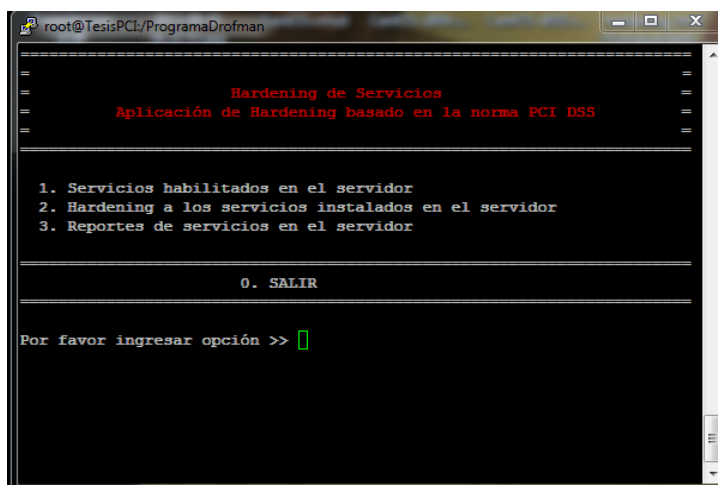
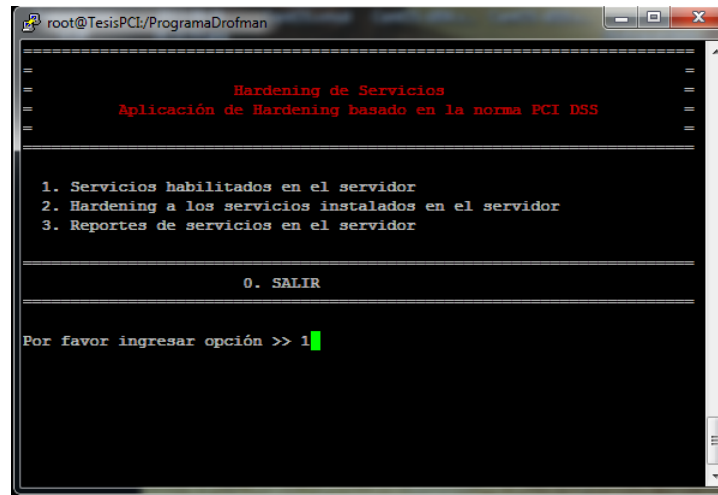


Figura 4. 1 Menú principal de Hardening

Como se observa en la figura anterior (figura 4.1) se ingresa una opción del menu indicado (opciones del 1 al 3) luego del texto “Por favor ingrese una opción >> ” para según la selección pasar a otro menú en el cual se interactúa con el usuario en base a lo indicado y selección a realizar. Para salir del sistema se ingresa 0.

4.3.1.1 Opción 1 – Servicios habilitados en el servidor

Al ingresar la opción 1 del menú principal se mostrará en otra ventana la información correspondiente a los servicios habilitados en el servidor.



```
root@TesisPCI/ProgramaDrofman
-----
                        Hardening de Servicios
                Aplicación de Hardening basado en la norma PCI DSS
-----

1. Servicios habilitados en el servidor
2. Hardening a los servicios instalados en el servidor
3. Reportes de servicios en el servidor

-----

0. SALIR

-----

Por favor ingresar opción >> 1 █
```

Figura 4. 2 Opción de Hardening de Servicios

En la siguiente figura (figura 4.3) se muestra la información donde se detallan los servicios instalados en el servidor, su estado (siendo estos RUNNING o STOPPED) y el respectivo puerto por el cual se encuentra escuchando.



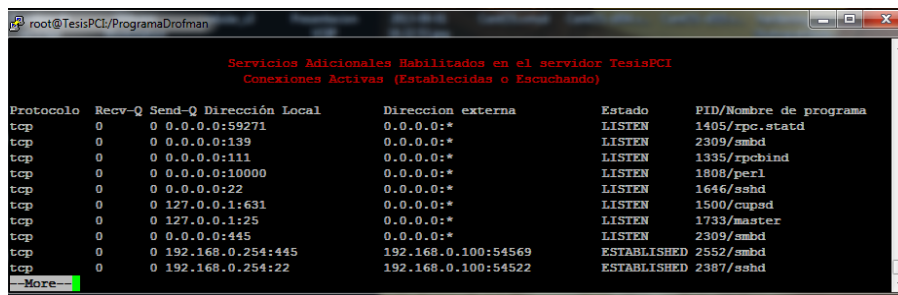
```
root@TesisPCI/ProgramaDrofman
-----
SERVICIOS INSTALADOS EN EL SERVIDOR
-----
SERVICIOS          ESTADO          PUERTO
-----
POSTFIX            RUNNING         25/TCP
SQUID              STOPPED
SSH                RUNNING         22/TCP
NTPD               RUNNING         123/TCP - 123/UDP
SAMBA              RUNNING         135:139/TCP
HTTP               RUNNING         80/TCP
-----

* * * Presione una tecla para mostrar todos los servicios... █
```

Figura 4. 3 Servicios instalados en el servidor

En la figura se puede ver POSTFIX el cual está RUNNING teniendo el puerto 25/TCP como medio de conexión así como de igual manera los demás servicios sus respectivos estados y puertos.

Se presiona una tecla para mostrar una nueva ventana (figura 4.4) la cual muestra servicios adicionales habilitados en el servidor. Dicha ventana detalla el protocolo, su dirección local, dirección externa, estado y el nombre del programa habilitado.



```

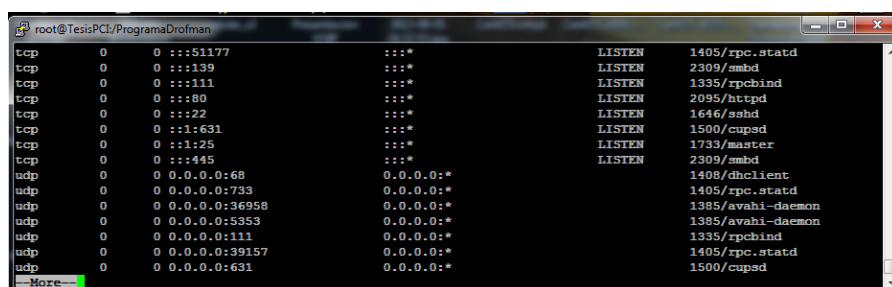
root@TesisPCI:/ProgramaDrofman
Servicios Adicionales Habilitados en el servidor TesisPCI
Conexiones Activas (Establecidas o Escuchando)

Protocolo Recv-Q Send-Q Dirección Local Dirección externa Estado PID/Nombre de programa
tcp 0 0 0.0.0.0:59271 0.0.0.0:* LISTEN 1405/rpc.statd
tcp 0 0 0.0.0.0:139 0.0.0.0:* LISTEN 2309/smbd
tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN 1335/rpcbind
tcp 0 0 0.0.0.0:10000 0.0.0.0:* LISTEN 1808/perl
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 1646/sshd
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN 1500/cupsd
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN 1733/master
tcp 0 0 0.0.0.0:445 0.0.0.0:* LISTEN 2309/smbd
tcp 0 0 192.168.0.254:445 192.168.0.100:54569 ESTABLISHED 2552/smbd
tcp 0 0 192.168.0.254:22 192.168.0.100:54522 ESTABLISHED 2387/sshd
--More--

```

Figura 4. 4 Servicios instalados por default

Para puede ver más información se presionando una tecla correspondiente a lo detallado en la ventana anterior (figura 4.5).



```

root@TesisPCI:/ProgramaDrofman

tcp 0 0 :::51177 :::* LISTEN 1405/rpc.statd
tcp 0 0 :::139 :::* LISTEN 2309/smbd
tcp 0 0 :::111 :::* LISTEN 1335/rpcbind
tcp 0 0 :::80 :::* LISTEN 2095/htpd
tcp 0 0 :::22 :::* LISTEN 1646/sshd
tcp 0 0 :::1:631 :::* LISTEN 1500/cupsd
tcp 0 0 :::1:25 :::* LISTEN 1733/master
tcp 0 0 :::445 :::* LISTEN 2309/smbd
udp 0 0 0.0.0.0:68 0.0.0.0:* 1408/dhclient
udp 0 0 0.0.0.0:733 0.0.0.0:* 1405/rpc.statd
udp 0 0 0.0.0.0:36958 0.0.0.0:* 1385/avahi-daemon
udp 0 0 0.0.0.0:5353 0.0.0.0:* 1385/avahi-daemon
udp 0 0 0.0.0.0:111 0.0.0.0:* 1335/rpcbind
udp 0 0 0.0.0.0:39157 0.0.0.0:* 1405/rpc.statd
udp 0 0 0.0.0.0:631 0.0.0.0:* 1500/cupsd
--More--

```

Figura 4. 5 Servicios instalados por default

Así hasta llegar al final habiendo mostrado toda la información y se muestra un mensaje “Presione una tecla para continuar” (figura 4.6 para salir al menú principal del sistema.

```

root@TesisPCL/ProgramaDrofman
udp 0 0 0.0.0.0:39157 0.0.0.0:* 1405/rpc.statd
udp 0 0 0.0.0.0:631 0.0.0.0:* 1500/cupsd
udp 0 0 192.168.0.254:123 0.0.0.0:* 2523/ntpd
udp 0 0 192.168.1.129:123 0.0.0.0:* 2523/ntpd
udp 0 0 127.0.0.1:123 0.0.0.0:* 2523/ntpd
udp 0 0 0.0.0.0:123 0.0.0.0:* 2523/ntpd
udp 0 0 0.0.0.0:10000 0.0.0.0:* 1808/xpcr1
udp 0 0 0.0.0.0:662 0.0.0.0:* 1335/rpcbind
udp 0 0 ::111 :::* 1335/rpcbind
udp 0 0 fe80::20c:29ff:feed:ed9:123 :::* 2523/ntpd
udp 0 0 fe80::20c:29ff:feed:ecf:123 :::* 2523/ntpd
udp 0 0 ::1:123 :::* 2523/ntpd
udp 0 0 ::123 :::* 2523/ntpd
udp 0 0 ::662 :::* 1335/rpcbind
udp 0 0 ::36282 :::* 1405/rpc.statd
Presione una tecla para continuar...

```

Figura 4. 6 Servicios por default en el servidor

4.3.1.2 Opción 2 – Hardening a los servicios instalados en el servidor

Ingresando 2 se mostrará una siguiente ventana la cual permitirá realizar el respectivo hardening en cada servicio instalado y mostrado en la opción anterior. Se ingresa la opción 2 del menú principal junto al texto “Por favor ingresar opción >>”

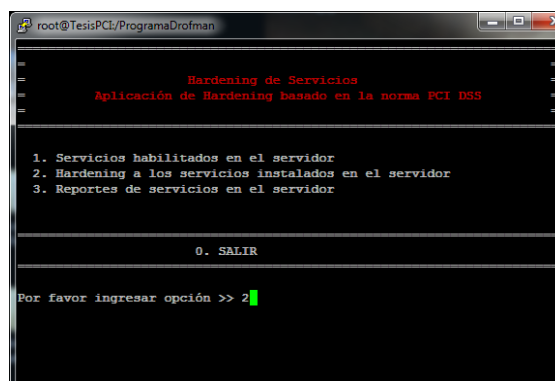


Figura 4. 7 Opción 2 de Menú Hardening

Inmediatamente se despliega el menú HARDENING A LOS SERVICIOS INSTALADOS EN EL SERVIDOR (figura 4.8 en el cual se muestra cada servicio instalado en el equipo identificado por una letra la cual deberá ser ingresada para proceder a realizar el hardening luego del texto “Por favor ingrese opción” para así pasar a la ventana en la cual según la selección se mostrará un menú de hardening correspondiente al servicio elegido. Si se ingresa 0 se vuelve al menú principal.

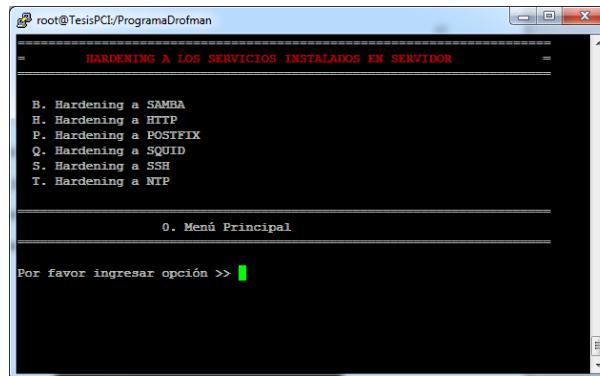


Figura 4. 8 Servicios instalados en el servidor

4.3.1.2.1 Hardening a SAMBA

Como primera opción se tiene B. Hardening a SAMBA por lo que para realizar el hardening a este servicio se ingresa la letra B y se muestra un mensaje “Desea aplicar hardening a servicio SAMBA (S/N)” (figura 4.9) para lo cual al ingresar S (si) se muestra una ventana donde se ven las opciones de hardening que se aplicarán al servicio SAMBA, si se ingresa N (no) (figura 4.10) no realiza acción y nuevamente se muestra el menú indicado.

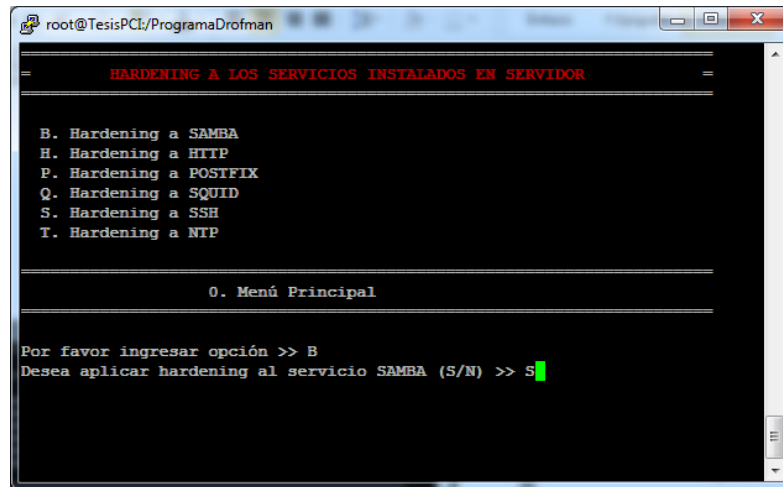


Figura 4. 9 Opción B ingresando S para realizar el hardening a SAMBA

Si es NO, vuelve a desplegar el menú de Hardening inicial.

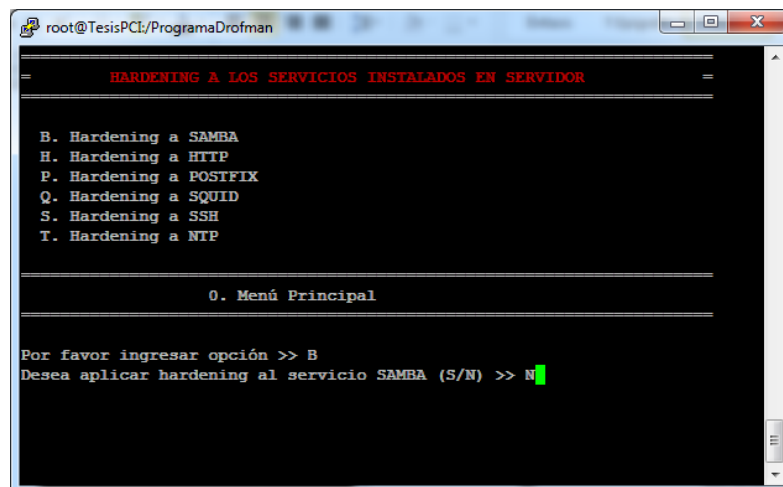
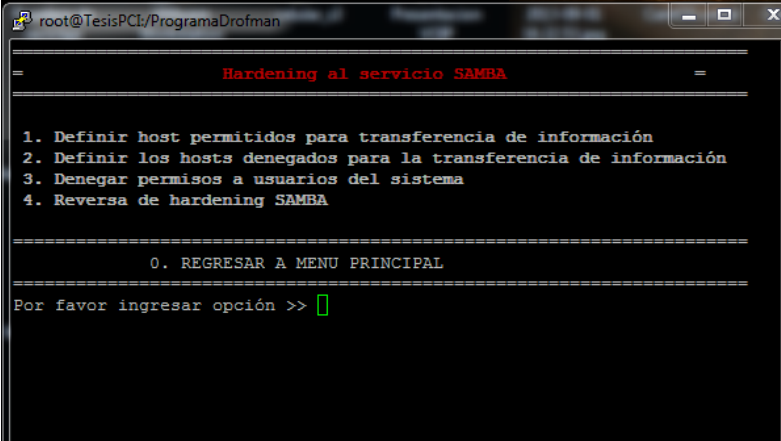


Figura 4. 10 Opción B ingresando N para NO realizar el hardening a SAMBA

Habiendo seleccionado la opción B y S al momento de la pregunta “Desea aplicar hardening a SAMBA” se muestra el menú en el cual se detalla las opciones de hardening a aplicar al servicio (figura 4.11). Se ingresará un número por hardening a aplicar siendo estas del 1 al 4 y al ingresar 0 se regresa al menú principal HARDENING A LOS SERVICIOS INSTALADOS EN EL SERVIDOR.



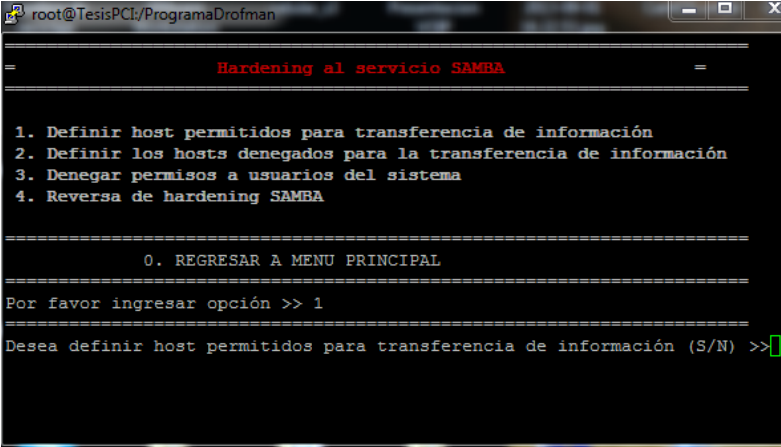
```
root@TesisPCI:/ProgramaDrofman
=====
Hardening al servicio SAMBA
=====
1. Definir host permitidos para transferencia de información
2. Definir los hosts denegados para la transferencia de información
3. Denegar permisos a usuarios del sistema
4. Reversa de hardening SAMBA
-----
0. REGRESAR A MENU PRINCIPAL
-----
Por favor ingresar opción >> █
```

Figura 4. 11 Menú de Hardening SAMBA

4.3.1.2.1.1 Definir host permitidos para transferencia de información

En esta opción se definen los host con las cuales se permitirá realizar transferencia de información (figura 4.12). Se ingresa 1 y se muestra un mensaje donde consulta si se desea definir los host permitidos con los cuales se realizará la transferencia de información a la cual se pondrá S (si) y se pasa a

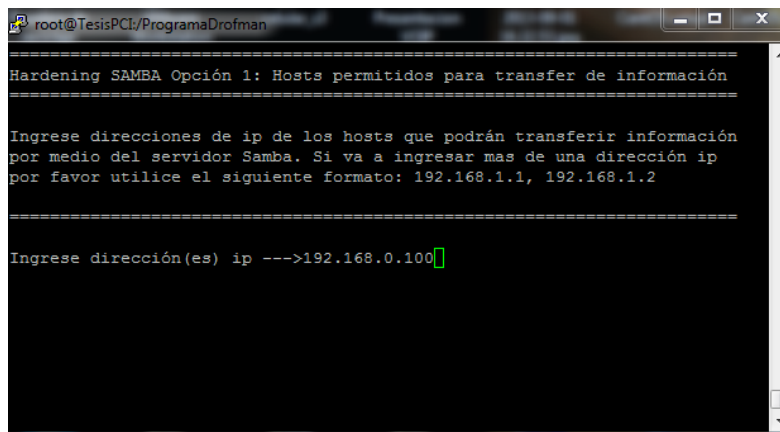
una siguiente ventana en la cual se ingresará las direcciones IP admitidas. En caso de ingresar N no se realizará acción alguna quedando en mismo menú.



```
root@TesisPCI:/ProgramaDrofman
=====
Hardening al servicio SAMBA
=====
1. Definir host permitidos para transferencia de información
2. Definir los hosts denegados para la transferencia de información
3. Denegar permisos a usuarios del sistema
4. Reversa de hardening SAMBA
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 1
=====
Desea definir host permitidos para transferencia de información (S/N) >> 
```

Figura 4. 12 Opción 1 – Definir host permitidos para transferencia de información.

En la siguiente figura se muestra el ingreso de direcciones IP perteneciente a las máquinas con las cuales se podrá realizar transferencia de información (figura 4.13)



```
root@TesisPCI:/ProgramaDrofman
=====
Hardening SAMBA Opción 1: Hosts permitidos para transfer de información
=====

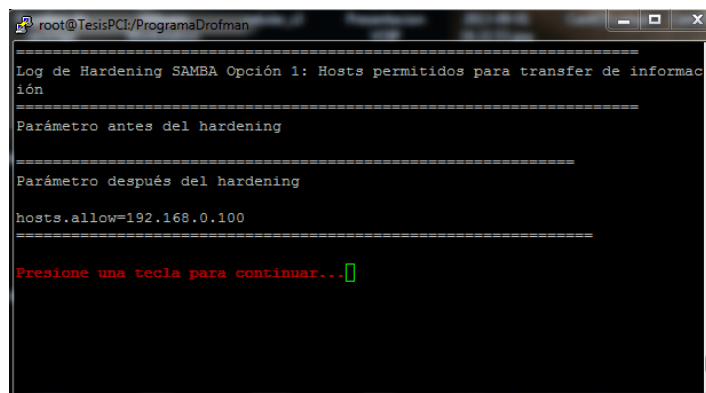
Ingrese direcciones de ip de los hosts que podrán transferir información
por medio del servidor Samba. Si va a ingresar mas de una dirección ip
por favor utilice el siguiente formato: 192.168.1.1, 192.168.1.2

=====

Ingrese dirección(es) ip --->192.168.0.100
```

Figura 4. 13 Ingreso de direcciones IP para aplicar permiso

Luego de haber sido ingresada la dirección IP necesaria, se mostrará por pantalla los parámetros aplicados en la sesión activa (antes de hardening y luego de haber aplicado hardening).



```
root@TesisPCI:/ProgramaDrofman
=====
Log de Hardening SAMBA Opción 1: Hosts permitidos para transfer de informac
ión
=====

Parámetro antes del hardening

=====

Parámetro después del hardening

hosts.allow=192.168.0.100

=====

Presione una tecla para continuar...
```

Figura 4. 14 Opción 1 SAMBA aplicada

Luego de ser aplicada cualquier opción, al ser seleccionada nuevamente mostrará un mensaje en el que indica que dicha opción ya fue aplicada adicional tomará un color turquesa lo cual la diferenciará de las demás para tener en

consideración lo mencionado, pero de igual manera da la opción al usuario de permitir tomarla nuevamente por si debe ingresar cualquier parámetro adicional.

```

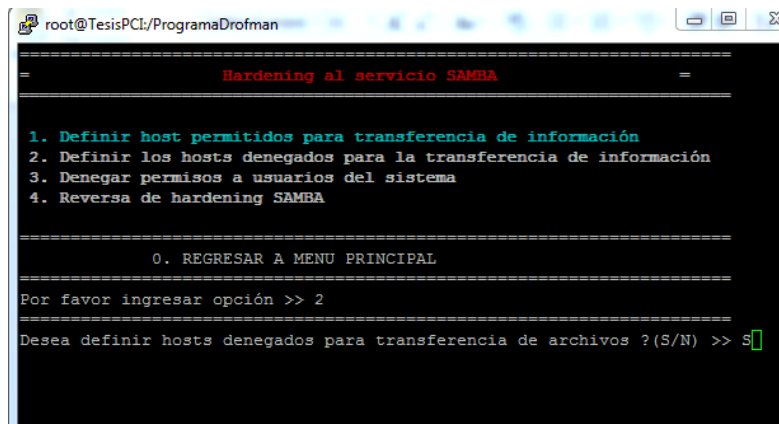
root@TesisPCL/ProgramaDrofman
=====
Hardening al servicio SAMBA
=====
1. Definir host permitidos para transferencia de información
2. Definir los hosts denegados para la transferencia de información
3. Denegar permisos a usuarios del sistema
4. Reversa de hardening SAMBA
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 1
=====
* * * * * OPCION DE HARDENING YA APLICADA * * * * *
Desea definir host permitidos para transferencia de información (S/N) >>

```

Figura 4. 15 Opción 1 Samba Ya aplicada

4.3.1.2.1.2 Definir los host denegados para la transferencia de información

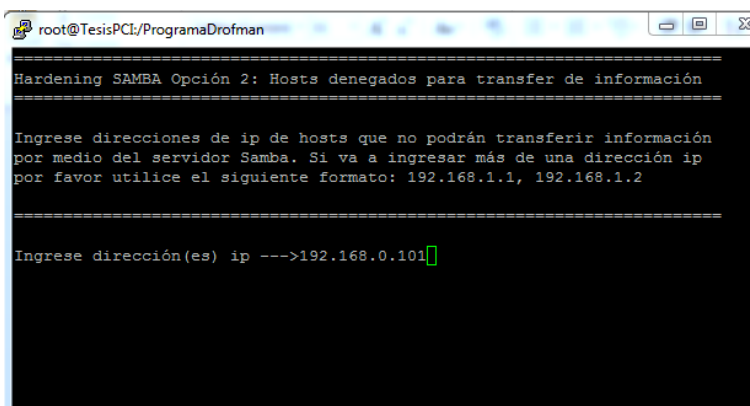
En esta opción se definen los host con las cuales no se permitirá realizar transferencia de información (figura 4.16). Se ingresa 2 y se muestra un mensaje donde consulta si se desea definir los host denegados con los cuales no se realizará la transferencia de información a la cual se pondrá S (si) y se pasa a una siguiente ventana en la cual se ingresará las direcciones IP denegadas. En caso de ingresar N no se realizará acción alguna quedando en mismo menú.



```
root@TesisPCI:/ProgramaDrofman
=====
Hardening al servicio SAMBA
=====
1. Definir host permitidos para transferencia de información
2. Definir los hosts denegados para la transferencia de información
3. Denegar permisos a usuarios del sistema
4. Reversa de hardening SAMBA
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 2
=====
Desea definir hosts denegados para transferencia de archivos ?(S/N) >> s
```

Figura 4. 16 Opción 2 - Definir host denegados para transferencia de información

En la siguiente figura se muestra el ingreso de direcciones IP perteneciente a las máquinas con las cuales no se podrá realizar transferencia de información (figura 4.17).

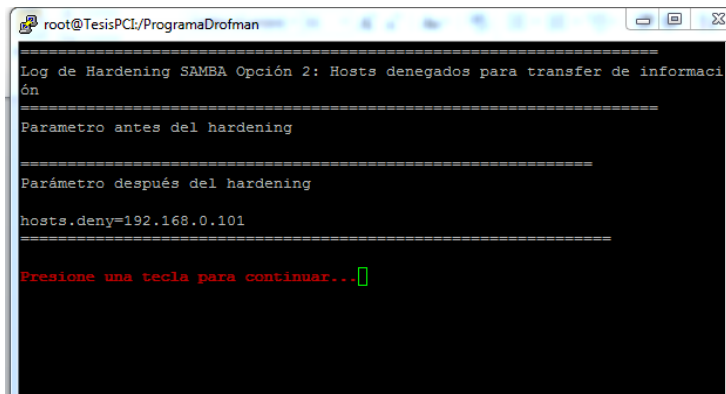


```
root@TesisPCI:/ProgramaDrofman
=====
Hardening SAMBA Opción 2: Hosts denegados para transfer de información
=====
Ingrese direcciones de ip de hosts que no podrán transferir información
por medio del servidor Samba. Si va a ingresar más de una dirección ip
por favor utilice el siguiente formato: 192.168.1.1, 192.168.1.2
=====
Ingrese dirección(es) ip --->192.168.0.101
```

Figura 4. 17 Host denegados SAMBA

Luego de haber sido ingresada la dirección IP necesaria, se mostrará por pantalla los parámetros aplicados en la sesión activa (antes de hardening y

luego de haber aplicado hardening).

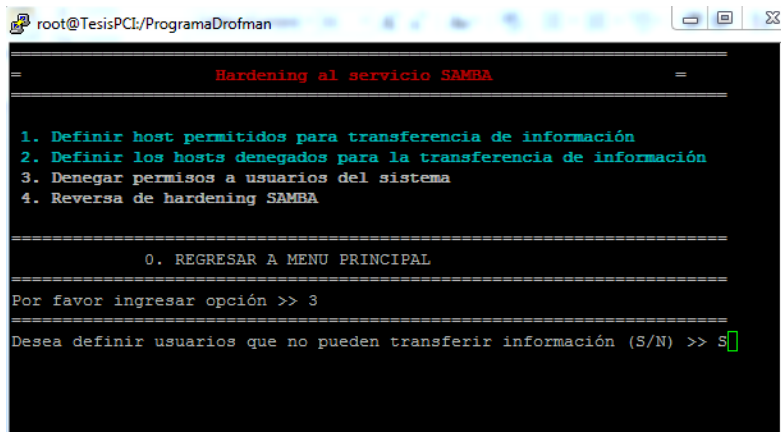


```
root@TesisPCI/ProgramaDrofman
=====
Log de Hardening SAMBA Opción 2: Hosts denegados para transferencia de información
=====
Parametro antes del hardening
=====
Parámetro después del hardening
hosts.deny=192.168.0.101
=====
Presione una tecla para continuar... █
```

Figura 4. 18 Opción 2 SAMBA aplicado

4.3.1.2.1.3 Denegar permisos a usuarios del sistema

En esta opción se definen los (Root, Bin y Daemon) usuarios los cuales por norma PCI deben ser denegados para poder realizar transferencia de información. Se ingresa 3 y se muestra un mensaje donde consulta si se desea definir los usuarios que no pueden realizar transferencia de información (figura 4.19) a la cual se pondrá S (si) y se pasa a una siguiente ventana donde se verá aplicada dicha hardening. En caso de ingresar N no se realizará acción alguna quedando en mismo menú.



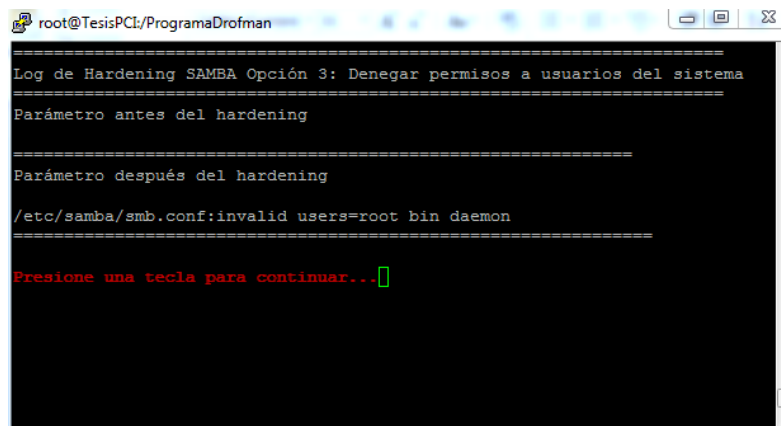
```
root@TesisPCI:/ProgramaDrofman
Hardening al servicio SAMBA

1. Definir host permitidos para transferencia de información
2. Definir los hosts denegados para la transferencia de información
3. Denegar permisos a usuarios del sistema
4. Reversa de hardening SAMBA

=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 3
=====
Desea definir usuarios que no pueden transferir información (S/N) >> S
```

Figura 4. 19 Opción 3 - Denegar permisos a usuarios del sistema

Esta opción realiza la acción en el archivo de configuración del servicio smb.conf tal como se ve en la figura siguiente (figura 4.20). Luego se presiona una tecla para continuar y volver al menú de aplicación de hardening de SAMBA.

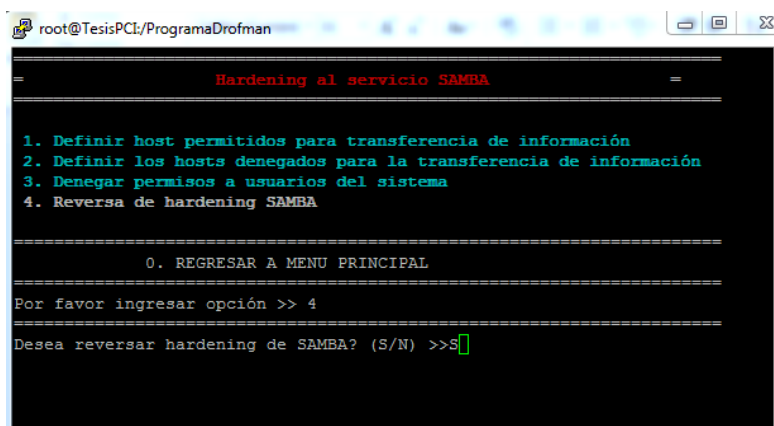


```
root@TesisPCI:/ProgramaDrofman
=====
Log de Hardening SAMBA Opción 3: Denegar permisos a usuarios del sistema
=====
Parámetro antes del hardening
=====
Parámetro después del hardening
/etc/samba/smb.conf:invalid users=root bin daemon
=====
Presione una tecla para continuar... 
```

Figura 4. 20 Configuración realizada

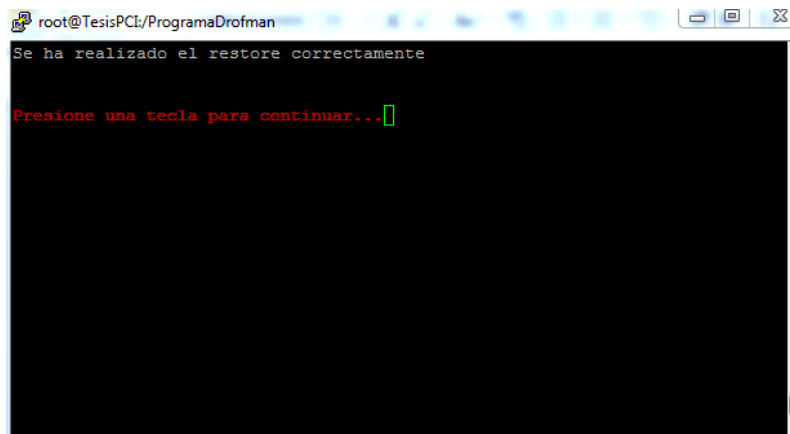
4.3.1.2.1.4 Reversa de hardening SAMBA

Esta opción permite realizar una reversa de todo el Hardening aplicado en el servicio mencionado. Este a su vez vuelve a activar todas las opciones del menú de SAMBA para poder ser aplicados nuevamente (figuras 4.21 – 4.22 – 4.23)



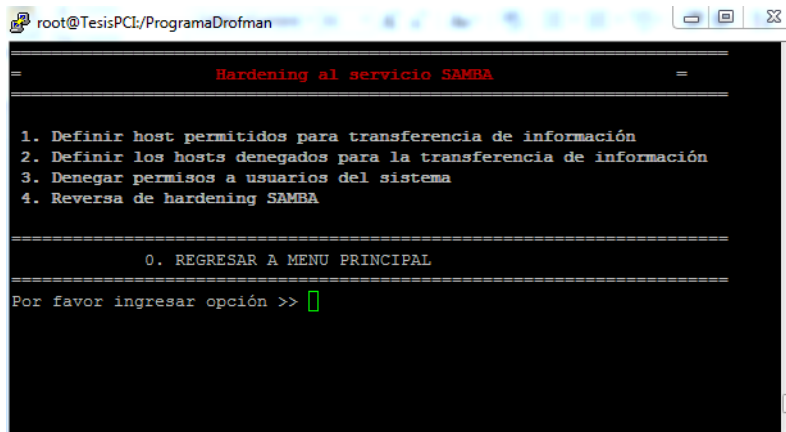
```
root@TesisPCI:/ProgramaDrofman
Hardening al servicio SAMBA
-----
1. Definir host permitidos para transferencia de información
2. Definir los hosts denegados para la transferencia de información
3. Denegar permisos a usuarios del sistema
4. Reversa de hardening SAMBA
-----
0. REGRESAR A MENU PRINCIPAL
-----
Por favor ingresar opción >> 4
-----
Desea reversar hardening de SAMBA? (S/N) >>S
```

Figura 4. 21 Opción 4 Reversa de Hardening SAMBA



```
root@TesisPCI:/ProgramaDrofman
Se ha realizado el restore correctamente
Presione una tecla para continuar...
```

Figura 4. 22 Mensaje de acción realizada



```
root@TesisPCI:/ProgramaDrofman
=====
Hardening al servicio SAMBA
=====
1. Definir host permitidos para transferencia de información
2. Definir los hosts denegados para la transferencia de información
3. Denegar permisos a usuarios del sistema
4. Reversa de hardening SAMBA
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> █
```

Figura 4. 23 Menú listo para ser nuevamente aplicado

4.3.1.2.2 Hardening a HTTP

La siguiente opción que se muestra es H. Hardening a HTTP por lo que para realizar el hardening a este servicio se ingresa la letra H y se muestra un mensaje “Desea aplicar hardening al servicio HTTP (S/N)” (figura 4.24) para lo cual al ingresar S (si) se muestra una ventana donde se ven las opciones de hardening que se aplicarán al servicio, si se ingresa N (no) no realiza acción y nuevamente se muestra el menú indicado.

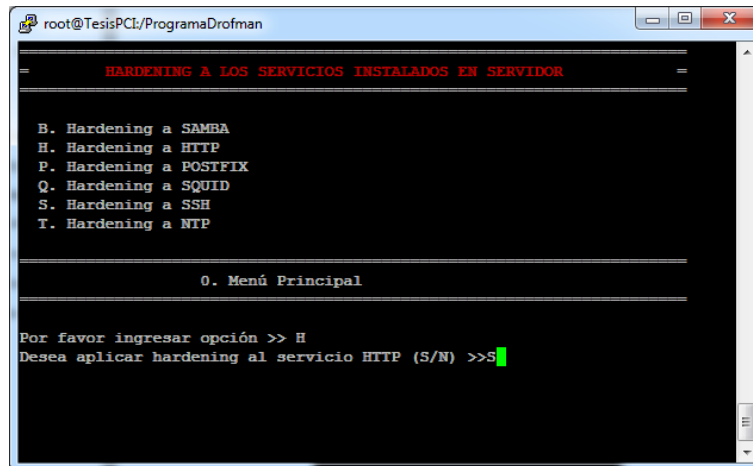


Figura 4. 24 Menú de Servicios Habilitados

Habiendo seleccionado la opción H y S (si) al momento de la pregunta “Desea aplicar hardening al servicio HHTTP (S/N)” se muestra un menú en una siguiente ventana en la cual se detalla las opciones de hardening a aplicar al servicio (figura 4.25). Se ingresará un número por hardening a aplicar siendo estas del 1 al 4, al ingresar 0 se regresa al menú principal HARDENING A LOS SERVICIOS INSTALADOS EN EL SERVIDOR.

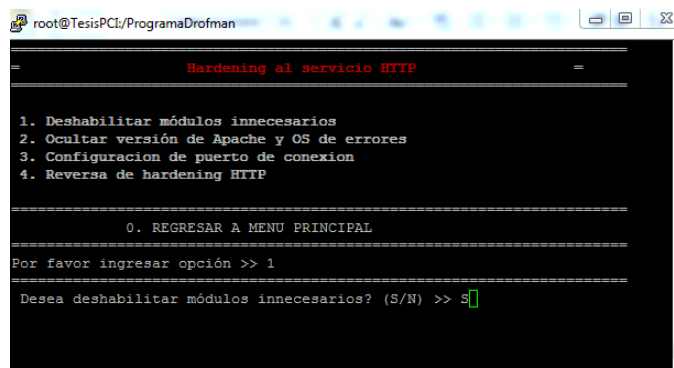
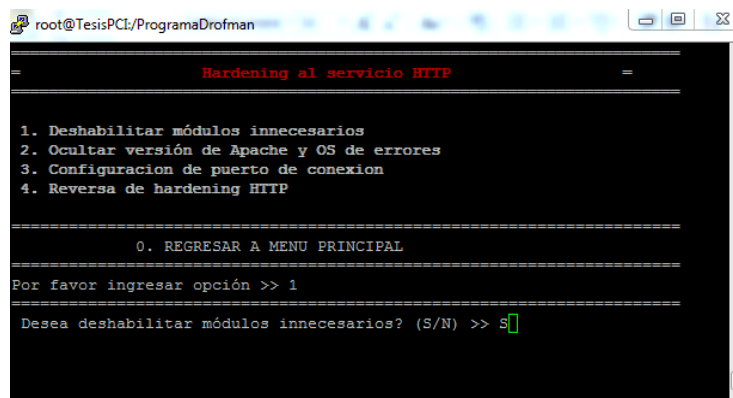


Figura 4. 25 Menú Hardening HTTP

4.3.1.2.2.1 Deshabilitar módulos innecesarios

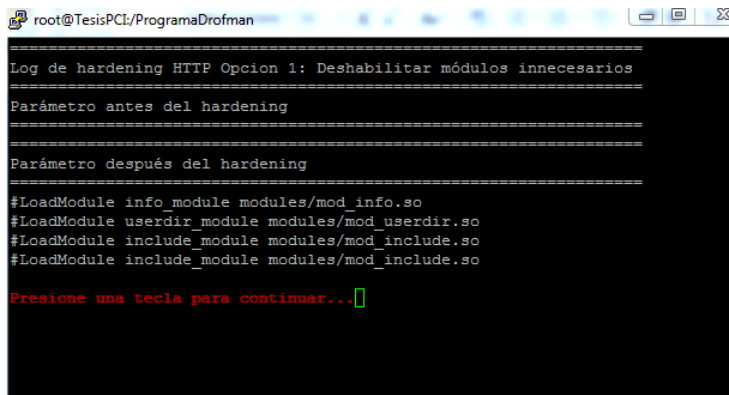
En esta opción se aplica una deshabilitación de módulos de http los cuales son innecesarios para su funcionamiento (figura 4.26). Se ingresa 1 y se muestra un mensaje donde consulta si se desea deshabilitar módulos innecesarios a la cual se pondrá S (si) y se pasa a una siguiente ventana en la cual se mostrará la opción aplicada. En caso de ingresar N no se realizará acción alguna quedando en mismo menú.



```
root@TesisPCI:/ProgramaDrofman
=====
Hardening al servicio HTTP
=====
1. Deshabilitar módulos innecesarios
2. Ocultar versión de Apache y OS de errores
3. Configuración de puerto de conexión
4. Reversa de hardening HTTP
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 1
=====
Desea deshabilitar módulos innecesarios? (S/N) >> S
```

Figura 4. 26 Opción 1 – Deshabilitar módulos innecesarios

En la siguiente figura (figura 4.27) se muestra la acción realizada indicando los módulos que han sido deshabilitados del servicio.



```

root@TesisPCI:/ProgramaDrofman
=====
Log de hardening HTTP Opcion 1: Deshabilitar módulos innecesarios
=====
Parámetro antes del hardening
=====
Parámetro después del hardening
=====
#LoadModule info_module modules/mod_info.so
#LoadModule userdir_module modules/mod_userdir.so
#LoadModule include_module modules/mod_include.so
#LoadModule include_module modules/mod_include.so

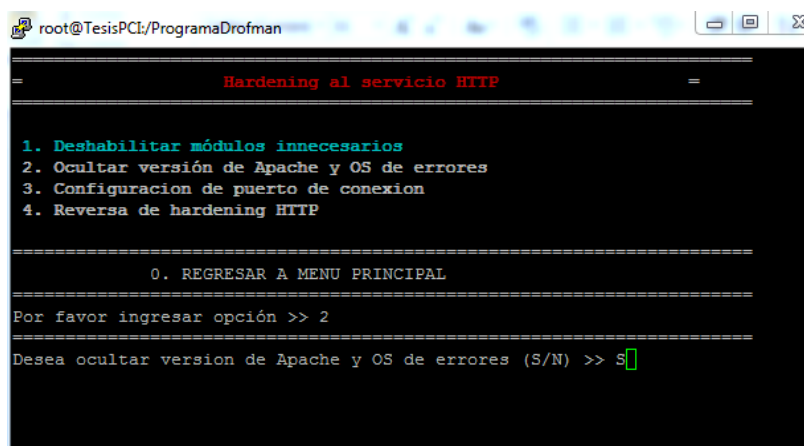
Presione una tecla para continuar...

```

Figura 4. 27 Opción 1 Resultado

4.3.1.2.2 Ocultar versión de Apache y OS de errores

En esta opción se oculta la versión de Apache para que de esta manera no sea fácil ver sus debilidades y así poder ser víctima de un intento de violación de información así como también los errores del sistema operativos del servidor web (figura 4.28).



```

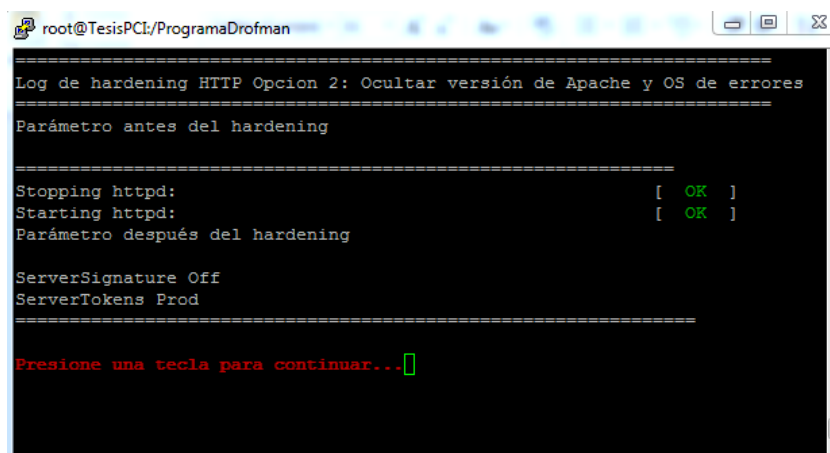
root@TesisPCI:/ProgramaDrofman
=====
Hardening al servicio HTTP
=====
1. Deshabilitar módulos innecesarios
2. Ocultar versión de Apache y OS de errores
3. Configuración de puerto de conexión
4. Reversa de hardening HTTP

=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 2
=====
Desea ocultar version de Apache y OS de errores (S/N) >> S

```

Figura 4. 28 Opción 2 – Ocultar versión de Apache y OS de errores

Adicional este luego de aplicar el hardening se realiza un reinicio del servicio para así sean aplicados los cambios aplicados (figura 4.29).



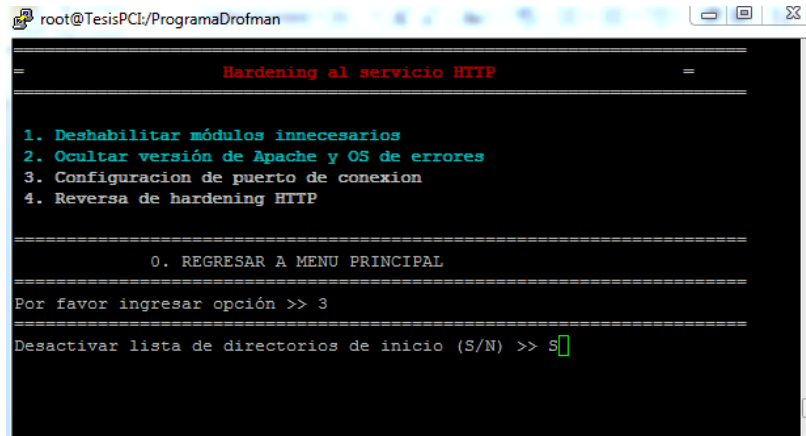
```
root@TesisPCI:/ProgramaDrofman
=====
Log de hardening HTTP Opcion 2: Ocultar versión de Apache y OS de errores
=====
Parámetro antes del hardening
=====
Stopping httpd:           [ OK ]
Starting httpd:          [ OK ]
Parámetro después del hardening

ServerSignature Off
ServerTokens Prod
=====
Presione una tecla para continuar... [ ]
```

Figura 4. 29 Reinicio de servicios para aplicar cambios

4.3.1.2.2.3 Configuración de puerto de conexión

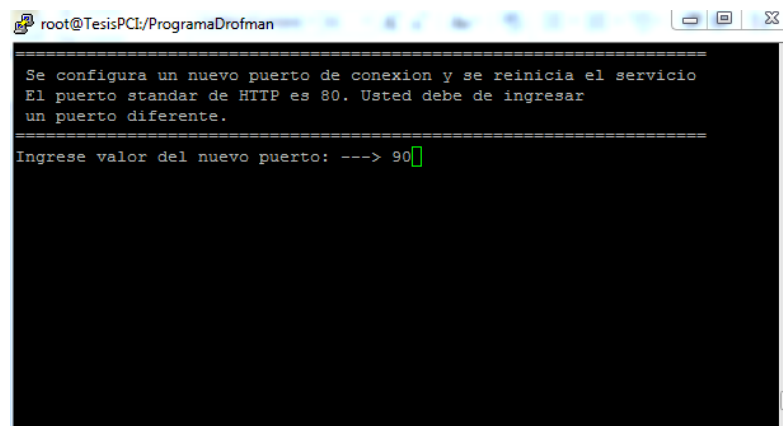
En esta se le puede asignar a nuestro servicio de HTTP un nuevo puerto ya que comunmente todas las aplicaciones Web tienen puerto 80 como default se procede a cambiar para así evitar cualquier filtro de información a travez de el mismo (figura 4.30). Se ingresa 3 y se muestra un mensaje donde consulta si se desea desactivar la lista de directorios de inicio a la cual se pondrá S (si) y se pasa a una siguiente ventana en la cual se ingresa el nuevo puerto de conexión (figura 4.31). En caso de ingresar N no se realizará acción alguna quedando en mismo menú.



```
root@TesisPCI/ProgramaDrofman
=====
Hardening al servicio HTTP
=====
1. Deshabilitar módulos innecesarios
2. Ocultar versión de Apache y OS de errores
3. Configuración de puerto de conexión
4. Reversa de hardening HTTP

-----
0. REGRESAR A MENU PRINCIPAL
-----
Por favor ingresar opción >> 3
-----
Desactivar lista de directorios de inicio (S/N) >> S
```

Figura 4. 30 Opción 3 – Configuración de puerto de conexión



```
root@TesisPCI/ProgramaDrofman
=====
Se configura un nuevo puerto de conexión y se reinicia el servicio
El puerto standar de HTTP es 80. Usted debe de ingresar
un puerto diferente.
=====
Ingrese valor del nuevo puerto: ---> 90
```

Figura 4. 31 Ingreso de nuevo puerto HTTP

Luego de haber realizado el cambio del puerto reiniciará el servicio para poder ingresar a nuestro WebSite con el nuevo puerto asignado tal como se muestra en la siguiente figura (figura 4.32).

```

root@TesisPCI/ProgramaDrofman
=====
Log de hardening HTTP Opcion 3: Configurar nuevo puerto de conexion
=====
Parametro antes del hardening
=====
Listen 80
=====
Stopping httpd:          [ OK ]
Starting httpd:         [ OK ]
=====
Parametro después del hardening
Listen 90
=====
Presione una tecla para continuar...

```

Figura 4. 32 Reinicio de Servicio

4.3.1.2.2.4 Reversa de Hardening HTTP

Esta opción permite realizar una reversa de todo el Hardening aplicado en el servicio mencionado. Este a su vez vuelve a activar todas las opciones del menú de HTTP para poder ser aplicados nuevamente (figuras 4.33 – 4.34)

```

root@TesisPCI/ProgramaDrofman
=====
Hardening al servicio HTTP
=====
1. Deshabilitar módulos innecesarios
2. Ocultar versión de Apache y OS de errores
3. Configuración de puerto de conexión
4. Reversa de hardening HTTP
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 4
=====
Desea revertir hardening de HTTP? (S/N) >>S

```

Figura 4. 33 Opción 4 – Reversa de hardening HTTP

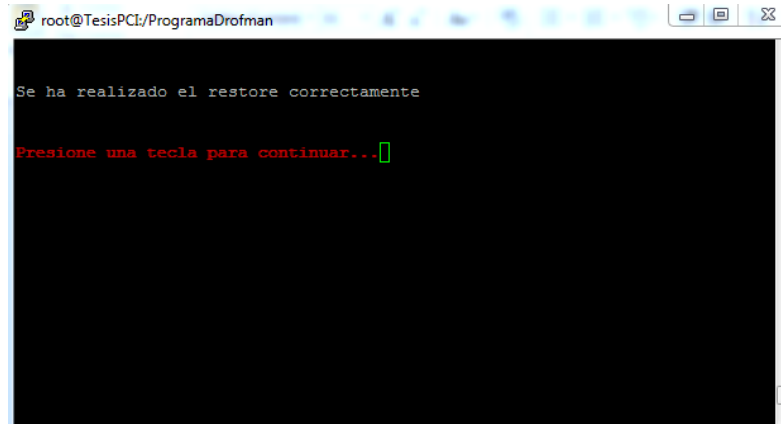


Figura 4. 34 Opción 4 - Mensaje de acción realizada

4.3.1.2.3 Hardening a POSTFIX

Para aplicar Hardening del servicio POSTFIX escogemos la opción P, luego muestra un mensaje “Desea aplicar hardening al servicio POSTFIX (S/N)” (figura 4.35) para lo cual al ingresar S (si) se muestra una ventana donde se ven las opciones de hardening que se aplicarán al servicio POSTFIX, si se ingresa N (no) no realiza acción y nuevamente se muestra el menú.

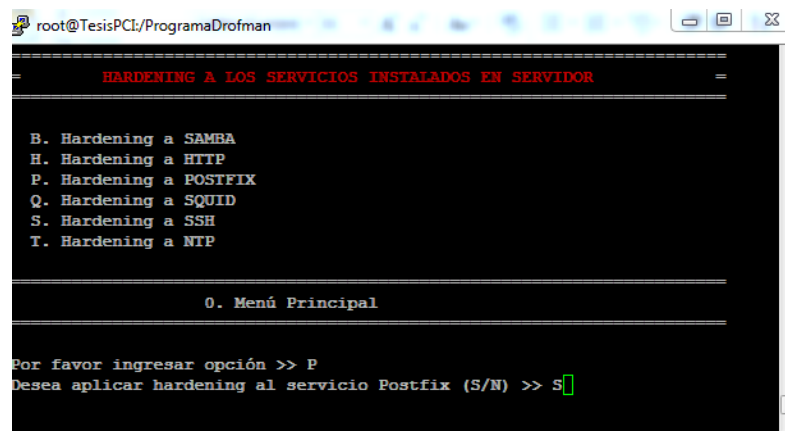
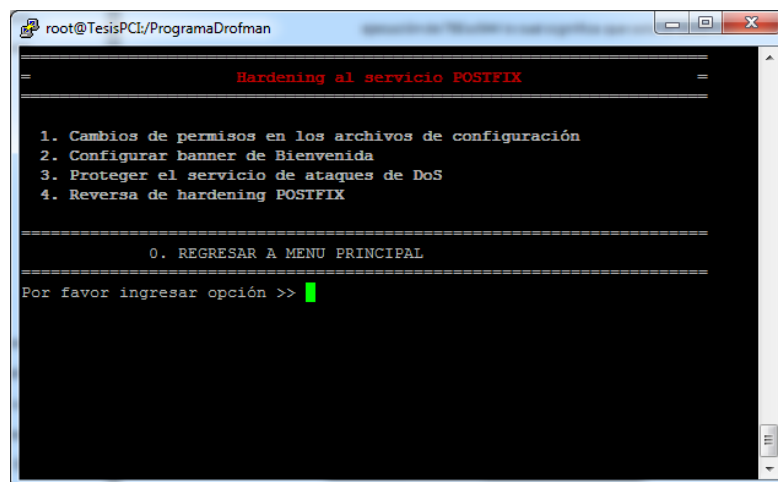


Figura 4. 35 Opción P ingresando S para realizar hardening POSTFIX

Habiendo seleccionado la opción P y S al momento de la pregunta “Desea aplicar hardening al servicio POSTFIX” se muestra el menú en el cual se detalla las opciones de hardening a aplicar al servicio (figura 4.36). Se ingresará un número por hardening a aplicar siendo estas del 1 al 4 y al ingresar 0 se regresa al menú principal HARDENING A LOS SERVICIOS INSTALADOS EN EL SERVIDOR.



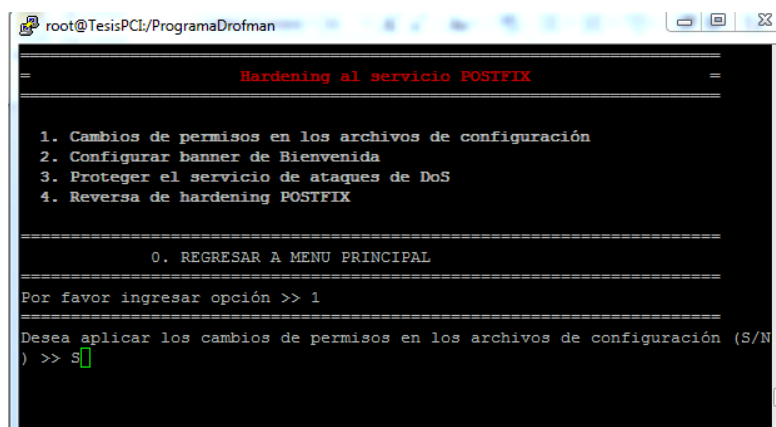
```
root@TesisPCI:/ProgramaDrofman
=
Hardening al servicio POSTFIX
=
1. Cambios de permisos en los archivos de configuración
2. Configurar banner de Bienvenida
3. Proteger el servicio de ataques de DoS
4. Reversa de hardening POSTFIX
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> █
```

Figura 4. 36 Menú Hardening de POSTFIX

4.3.1.2.3.1 Cambios de permisos en los archivos de configuración

Esta opción realiza cambios de permisos en los archivos de configuración automáticamente de lectura, escritura y ejecución de 755 a 644 lo cual significa que solo el usuario Root tiene permisos de lectura y escritura pero no de ejecución.

Se ingresa 1 y se muestra un mensaje donde consulta si se desea realizar cambio en los archivos de configuración a la cual se pondrá S (si) y se pasa a una siguiente ventana donde se muestra el resultado de la aplicación de este hardening (figura 4.37). En caso de ingresar N no se realizará acción alguna quedando en mismo menú.



```
root@TesisPCI:/ProgramaDrofman
=
Hardening al servicio POSTFIX
=
1. Cambios de permisos en los archivos de configuración
2. Configurar banner de Bienvenida
3. Proteger el servicio de ataques de DoS
4. Reversa de hardening POSTFIX
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 1
=====
Desea aplicar los cambios de permisos en los archivos de configuración (S/N
) >> S
```

Figura 4. 37 Opción 1 Cambios de permisos en los archivos de configuración

En las figuras siguientes (figuras 4.38 y 4.39) se muestra el resultado de la aplicación de este hardening la cual es realizada directamente al archivo de configuración.

```

root@TesisPCI/ProgramaDrofman
=====
Log Hardening de Postfix Opcion 1: Cambio de permisos en archivos de Cfg
=====
Directorio antes del cambio de permisos a 755
drwxr-xr-x.  2 root root  4096 Feb  8 19:07 postfix
Directorio después de cambiar permisos a 755
drwxr-xr-x.  2 root root  4096 Feb  8 19:07 postfix
Archivos antes de cambiar permisos a 644
-rw-r--r--.  1 root root 27014 Dec  2 2011 main.cf
-rw-r--r--.  1 root root  5113 Dec  2 2011 master.cf
Archivos después de cambiar permisos a 644
/etc/postfix/:
total 140
-rw-r--r--.  1 root root 19579 Dec  2 2011 access
-rw-r--r--.  1 root root 11681 Dec  2 2011 canonical
-rw-r--r--.  1 root root  9904 Dec  2 2011 generic
-rw-r--r--.  1 root root 18287 Dec  2 2011 header_checks
-rw-r--r--.  1 root root 27014 Dec  2 2011 main.cf
--More--

```

Figura 4. 38 Resultado de cambios de permisos en los archivos de configuración

```

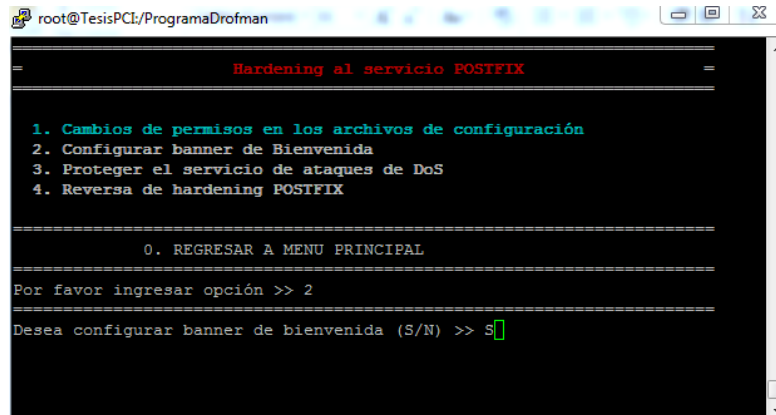
root@TesisPCI/ProgramaDrofman
-rw-r--r--.  1 root root  9904 Dec  2 2011 generic
-rw-r--r--.  1 root root 18287 Dec  2 2011 header_checks
-rw-r--r--.  1 root root 27014 Dec  2 2011 main.cf
-rw-r--r--.  1 root root  5113 Dec  2 2011 master.cf
-rw-r--r--.  1 root root  6816 Dec  2 2011 relocated
-rw-r--r--.  1 root root 12500 Dec  2 2011 transport
-rw-r--r--.  1 root root 12494 Dec  2 2011 virtual
=====
Directorio antes del cambio de permisos a 755
drwxr-xr-x. 16 root  root  4096 Feb  8 19:07 postfix
Directorio después de cambiar permisos a 755
drwxr-xr-x. 16 root  root  4096 Feb  8 19:07 postfix
Archivos antes de cambiar permisos a 600 y propietario Root:Root
-rw-----.  1 root root 1144 Feb  8 19:53 /var/log/maillog
Archivos después de cambiar permisos a 600 y propietario a Root:Root
-rw-----.  1 root root 1144 Feb  8 19:53 /var/log/maillog
=====
Presione una tecla para continuar..

```

Figura 4. 39 Resultado de cambios de permisos en los archivos de configuración

4.3.1.2.3.2 Configurar banner de Bienvenida

En la opción 2, se configura un banner de smtp, el cual muestra el nombre del servidor.



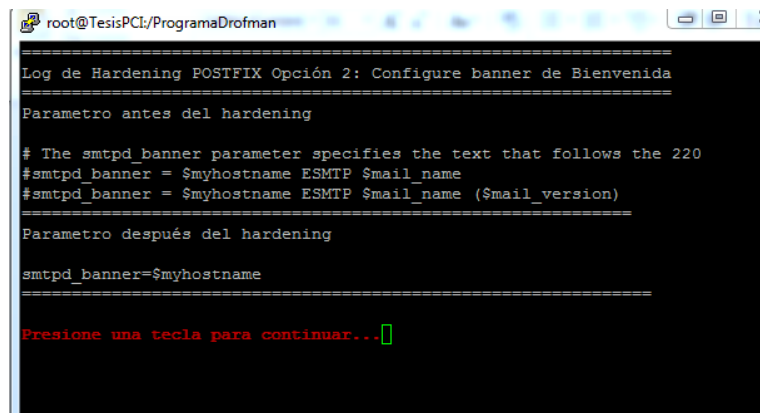
```

root@TesisPCI:/ProgramaDrofman
=====
Hardening al servicio POSTFIX
=====
1. Cambios de permisos en los archivos de configuración
2. Configurar banner de Bienvenida
3. Proteger el servicio de ataques de DoS
4. Reversa de hardening POSTFIX

-----
0. REGRESAR A MENU PRINCIPAL
-----
Por favor ingresar opción >> 2
-----
Desea configurar banner de bienvenida (S/N) >> S

```

Figura 4. 40 Opción 2 Configuración Banner de Bienvenida



```

=====
Log de Hardening POSTFIX Opción 2: Configure banner de Bienvenida
=====
Parametro antes del hardening

# The smtpd_banner parameter specifies the text that follows the 220
#smtpd_banner = $myhostname ESMTP $mail_name
#smtpd_banner = $myhostname ESMTP $mail_name ($mail_version)
-----
Parametro después del hardening

smtpd_banner=$myhostname
=====
Presione una tecla para continuar...

```

Figura 4. 41 Resultados de Configuración de Banner

4.3.1.2.3.3 Proteger el servicio de ataques de DOS

EN la opción 3, proteger el servicio de ataque de DOS, incluye al archivo de configuración main.cf, las opciones de límite de número de usuarios que pueden ingresar a la vez.

```

root@TesisPCI/ProgramaDrofman
=====
Hardening al servicio postfix
=====
1. Cambios de permisos en los archivos de configuración
2. Configurar banner de Bienvenida
3. Proteger el servicio de ataques de DoS
4. Reversa de hardening postfix

-----
0. REGRESAR A MENU PRINCIPAL
-----
Por favor ingresar opción >> 3
-----
Desea proteger el servicio de ataques DoS (S/N) >> S

```

Figura 4. 42 Opcion3 Proteger servicio de ataques de DOS

```

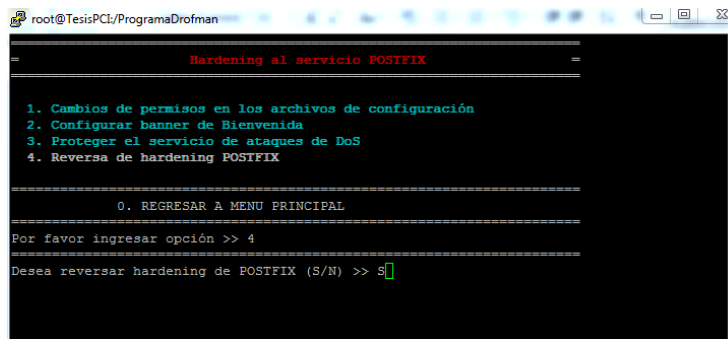
root@TesisPCI/ProgramaDrofman
=====
Log de Hardening postfix Opción 3: Limite de Ataques de Denegación de Servicio
=====
Parámetros antes del Hardening
-----
Parámetro después del Hardening
-----
default_process_limit=100
smtpd_client_connection_count_limit=10
smtpd_client_connection_rate_limit=30
queue_minfree=20971520
header_size_limit=51200
message_size_limit=10485760
smtpd_recipient_limit=100
-----
Presione una tecla para continuar...

```

Figura 4. 43 Resultado de Límite de Ataques DOS

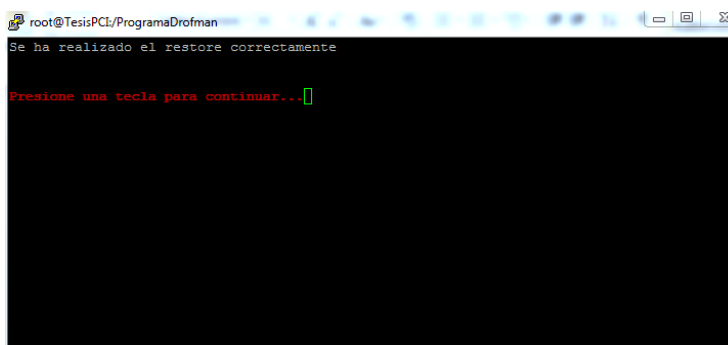
4.3.1.2.3.4 Reversar Hardening postfix

Esta opción permite realizar una reversa de todo el Hardening aplicado en el servicio mencionado. Este a su vez vuelve a activar todas las opciones del menú de postfix para poder ser aplicados nuevamente (figura 4.44).



```
root@TesisPCI/ProgramaDrofman
=====
Hardening al servicio POSTFIX
=====
1. Cambios de permisos en los archivos de configuración
2. Configurar banner de Bienvenida
3. Proteger el servicio de ataques de DoS
4. Reversa de hardening POSTFIX
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 4
Desea revertir hardening de POSTFIX (S/N) >> s
```

Figura 4. 44 Opción 4 – Reverso de hardening POSTFIX



```
root@TesisPCI/ProgramaDrofman
Se ha realizado el restore correctamente
Presione una tecla para continuar...
```

Figura 4. 45 Opción 4 - Mensaje de acción realizada

4.3.1.2.4 Hardening a SQUID

Para aplicar Hardening del servicio SQUID escogemos la opción (Q), la cual nos enviara a un submenu de varias opciones que nos ayudara a cumplir con el estandar de PCI.

El submenú de Squid incluye los siguientes puntos:

```

root@TesisPC1:/ProgramaDrofman
=====
HARDENING A LOS SERVICIOS INSTALADOS EN SERVIDOR
=====
B. Hardening a SAMBA
H. Hardening a HTTP
P. Hardening a POSTFIX
Q. Hardening a SQUID
S. Hardening a SSH
T. Hardening a NTP

-----
0. Menú Principal
-----

Por favor ingresar opción >> Q
Desea aplicar hardening al servicio SQUID (S/N) >> S

```

Figura 4. 46 Opción P ingresando S para realizar hardening SQUID

4.3.1.2.4.1 Opción 1 - Apagar la función PIC y HTCP

En la opción 1; Apagar la función PIC y HTCP, agrega al archivo de configuración squid.conf las opciones que desactivan el PIC y HTCP.

```

root@TesisPC1:/ProgramaDrofman
=====
Hardening al servicio SQUID
=====
1. Apagar la función PIC y HTCP
2. Activar SNMP
3. Restringir accesos a Proxy Squid
4. Reversa de hardening SQUID

-----
0. REGRESAR A MENU PRINCIPAL
-----

Por favor ingresar opción >> 1
Desea apagar las funciones PIC y HTCP? (S/N) >> S

```

Figura 4. 47 Opción 1 - Apagar la función PIC y HTCP

```

root@TesisPCI:/ProgramaDrofman
=====
Log de Hardening SQUID Opción 1: Deshabilitar funcion PIC y HTCP
=====
Parámetro antes del hardening
=====
Parámetro después del hardening
icp_port 0
htcp_port 0
icp_access 0
htcp_access 0
=====
Presione una tecla para continuar... █

```

Figura 4. 48 Opción 1 - Resultado de Apagar PIC y HTCP

4.3.1.2.4.2 Opción 2 - Activar SNMP

En la opción 2, Se activa la opción de SNMP para servicios de proxy

```

root@TesisPCI:/ProgramaDrofman
=====
Hardening al servicio SQUID
=====
1. Apagar la función PIC y HTCP
2. Activar SNMP
3. Restringir accesos a Proxy Squid
4. Reversa de hardening SQUID
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 2
Desea activar uso de SNMP (S/N) >> s █

```

Figura 4. 49 Opción 2 - Activar SNMP


```

root@TesisPCL/ProgramaDrofman
=====
Log de Hardening SQUID Opción 2: Activación de SNMP
=====
Parametro antes del hardening
=====
Parámetro después del hardening
snmp_port 0
snmp_access deny all
=====
Presione una tecla para continuar... █

```

Figura 4. 50 Opción 2 - Resultado de Activar SNMP

4.3.1.2.4.3 Opción 3.- Restringir acceso a Proxy Squid

En la opción 3, se agregan las ACL que no tendrán acceso a INTERNET por medio del proxy.

```

root@TesisPCL/ProgramaDrofman
=====
Hardening al servicio SQUID
=====
1. Apagar la función PIC y HTCP
2. Activar SNMP
3. Restringir accesos a Proxy Squid
4. Reversa de hardening SQUID
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 3
=====
Desea restringir acceso a su ProxySquid (S/N) >> S █

```

Figura 4. 51 Opción 3 - Restringir acceso por medio de SQUID

```

root@TesisPCL/ProgramaDrofman
=====
Hardening SQUID Opción 3: Restringir acceso a Proxy Squid
=====
Con esta función se procederá a crear una ACL para controlar acceso
por medio de Squid. El formato del segmento debe de ser:
172.16.0.0/24
Ingrese nombre de acl: ---->INTERNET
Ingrese segmento de red: ---->192.168.0.0/24
Ingrese nombre de port: ---->PRUEBA
Ingrese número de puerto: ---->8080 █

```

Figura 4. 52 Opción 3 - Creación de ACL

```

root@TesisPCI:/ProgramaDrofman
=====
Log de hardening SQUID Opción 3: Restringir acceso a Proxy Squid
=====
Parámetro antes del hardening

# include /path/to/included/file/squid.acl.config
#   challenged for authentication on the first such acl encountered
#   type acl.
#   If you use an authenticator, make sure you have 1 acl of type
#   If you use an NTLM authenticator, make sure you have 1 acl
#   one acl of type proxy_auth active. By default, the negotiate
#   This option defines external acl classes using a helper program
#   children=n      Number of acl helper processes spawn to service
#                   external acl lookups of this type. (default 5)
#   protocol=2.5   Compatibility mode for Squid-2.5 external acl helpers
#   %EXT_USER      Username from external acl
#   acl will also be included in the helper request line, after the
#   specified formats (see the "acl external" directive)
# TAG: acl
--More--

```

Figura 4. 53 Opción 3 - Parámetro antes de Hardening SQUID

```

root@TesisPCI:/ProgramaDrofman
#
# acl aclname acltype argument ...
# acl aclname acltype "file" ...
#
# Some acl types require suspending the current request in order
#
# acl aclname src ip-address/netmask ... # clients IP address [fast]
# acl aclname src addr1-addr2/netmask ... # range of addresses [fast]
# acl aclname dst ip-address/netmask ... # URL host's IP address [slow]
# acl aclname myip ip-address/netmask ... # local socket IP address [fast]
# acl aclname arp mac-address ... (xx:xx:xx:xx:xx:xx notation)
#
# # The arp ACL requires the special configure option --enable-arp-acl.
#
# acl aclname srcdomain .foo.com ...
# acl aclname dstdomain .foo.com ...
#
# acl aclname srcdom regex [-i] \.foo\.com ...
# acl aclname dstdom regex [-i] \.foo\.com ...
#
# acl aclname src as number ...
#
# acl aclname dst as number ...
#
# # acl asexample dst_as 1241
#
# acl aclname peername myPeer ...
#
# acl aclname time [day-abbrevs] [h1:m1-h2:m2]
#
# acl aclname url_regex [-i] ^http:// ...
#
--More--

```

Figura 4. 54 Opción 3 - Parámetro antes de Hardening SQUID

```

root@TesisPCI:/ProgramaDrofman
#
# ALL the acl's specified (which must be defined in acl clauses).
# If no acl is specified, all requests will be logged to this file.
# icap_log <filepath> [klogformat name] [acl acl ...]
# icap_log none [acl acl ...]
#
# TAG: log_access allow/deny acl acl...
#
# This clause only supports fast acl types.
# This clause supports both fast and slow acl types.
# This clause supports both fast and slow acl types.
# This clause only supports fast acl types.
#
# acl buggy_server url_regex ^http://...
# This clause only supports fast acl types.
# Usage: deny_info err_page_name acl
# or deny_info http://... acl
# or deny_info TCP_RESET acl
#
# acl it evaluated in http_access, and if a 'deny_info' line exists
# the first authentication related acl encountered
#
# acl processed on the last http_access line.
#
# acl local-servers dstdomain my.domain.net
#
--More--

```

Figura 4. 55 Opción 3 - Parámetro antes de Hardening SQUID

```

root@TesisPCI/ProgramaDrofman
# This clause supports both fast and slow acl types.
# This clause only supports fast acl types.
# acl buggy_server url_regex ^http://....
# This clause only supports fast acl types.
# Usage: deny_info err_page_name acl
# or deny_info http://... acl
# or deny_info TCP RESET acl
# acl it evaluated in http access, and if a 'deny_info' line exists
# The acl is typically the last acl on the http_access deny line which
# the first authentication related acl encountered
# acl processed on the last http_access line.
# acl local-servers dstdomain my.domain.net
# acl FTP proto FTP
# acl local-external dstdomain external.foo.net
# acl local-servers dstdomain .foo.net
# This clause supports both fast and slow acl types.
# acl local-servers dstdomain .foo.net
# acl local-intranet dstdomain .foo.net
# acl local-external dstdomain external.foo.net
# This clause supports both fast and slow acl types.
=====
Parámetro después del hardening
acl INTERNET src 192.168.0.0/24
http_access allow INTERNET PRUEBA
acl PRUEBA myport 8080
=====
Presione una tecla para continuar...

```

Figura 4. 56 Opción 3 - Parámetro después de Hardening SQUID

4.3.1.2.4.4 Opción 4.- Reversar Hardening SQUID

Esta opción permite realizar una reversa de todo el Hardening aplicado en el servicio mencionado. Este a su vez vuelve a activar todas las opciones del menú de SQUID para poder ser aplicados nuevamente (figura 4.57)

```

root@TesisPCI/ProgramaDrofman
=====
Hardening al servicio SQUID
=====
1. Apagar la función PIC y HTCP
2. Activar SNMP
3. Restringir accesos a Proxy Squid
4. Reversa de hardening SQUID
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 4
=====
Desea reversar hardening de SQUID? (S/N) >>S

```

Figura 4. 57 Opción 4 – Reversa de hardening SQUID

4.3.1.2.5 Hardening SSH

Para aplicar Hardening del servicio SSH escogemos la opción (S), la cual nos enviara a un submenu de varias opciones que nos ayudara a cumplir con el estandar de PCI.

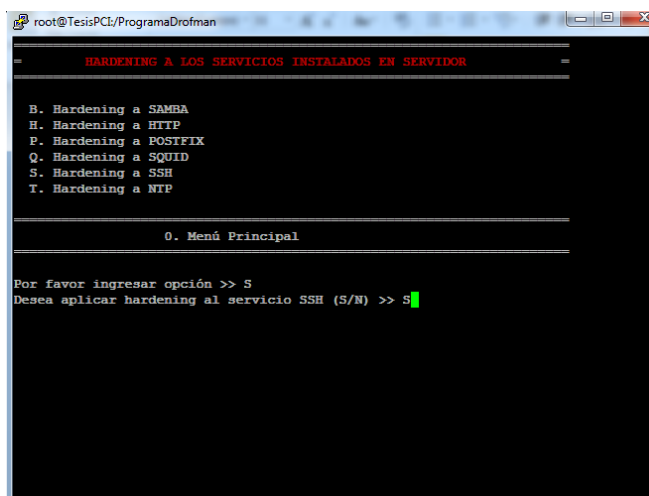


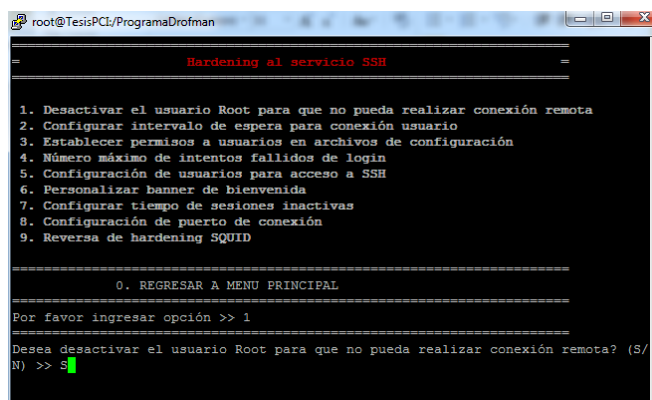
Figura 4. 58 Opción S ingresando S para realizar hardening SSH

Habiendo seleccionado la opción S y S al momento de la pregunta “Desea aplicar hardening al servicio SSH” se muestra el menú en el cual se detalla las opciones de hardening a aplicar al servicio (figura 4.58). Se ingresará un número por hardening a aplicar siendo estas del 1 al 9 y al ingresar 0 se regresa al menú principal HARDENING A LOS SERVICIOS INSTALADOS EN EL SERVIDOR

El submenú de SSH incluye los siguientes puntos:

4.3.1.2.5.1 Opción 1 - Desactivar usuario Root para que no pueda realizar conexión remota.

Esta opción deshabilita el usuario Root para realizar el primer login en conexiones remotas



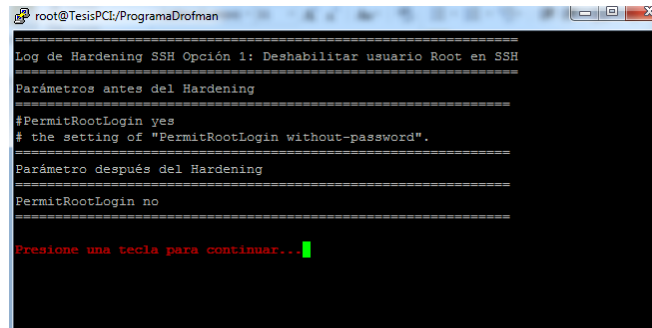
```
root@TesisPCI/ProgramaDrofman
=
Hardening al servicio SSH
=
1. Desactivar el usuario Root para que no pueda realizar conexión remota
2. Configurar intervalo de espera para conexión usuario
3. Establecer permisos a usuarios en archivos de configuración
4. Número máximo de intentos fallidos de login
5. Configuración de usuarios para acceso a SSH
6. Personalizar banner de bienvenida
7. Configurar tiempo de sesiones inactivas
8. Configuración de puerto de conexión
9. Reversa de hardening SQUID

=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 1
Desea desactivar el usuario Root para que no pueda realizar conexión remota? (S/
N) >> S
```

Figura 4. 59 Opción 1 – Desactivar usuario Root

Se ingresa 1 y se muestra un mensaje donde consulta si se desea realizar cambio en los archivos de configuración a la cual se pondrá S (si) y se pasa a una siguiente ventana donde se muestra el resultado de la aplicación de este hardening (figura 4.59). En caso de ingresar N no se realizará acción alguna quedando en mismo menú.

En la figura siguiente (figuras 4.60) se muestra el resultado de la aplicación de este hardening la cual es realizada directamente al archivo de configuración.



```

root@TesisPCL/ProgramaDrofman
Log de Hardening SSH Opción 1: Deshabilitar usuario Root en SSH
=====
Parámetros antes del Hardening
=====
#PermitRootLogin yes
# the setting of "PermitRootLogin without-password".
=====
Parámetro después del Hardening
=====
PermitRootLogin no

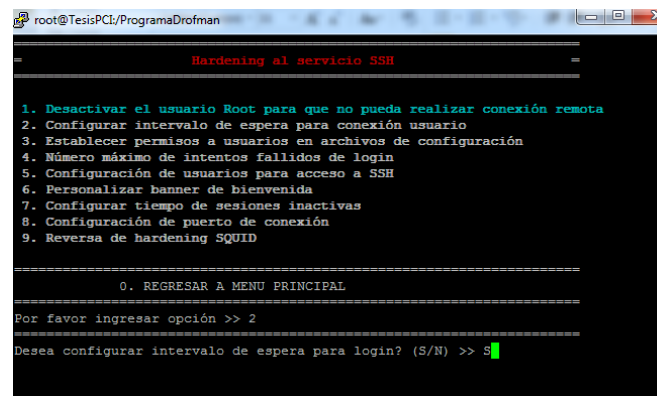
Presione una tecla para continuar... █

```

Figura 4. 60 Opción 1 – Resultado obtenido

4.3.1.2.5.2 Opción 2 - Configurar intervalo de espera entre conexión con el usuario

En la opción 2, se configura el intervalo de espera entre conexión con el usuario, es decir el tiempo que el usuario tiene para ingresar la clave correctamente; caso contrario deberá realizar una nueva conexión SSH (figura 4.61 – 4.62).

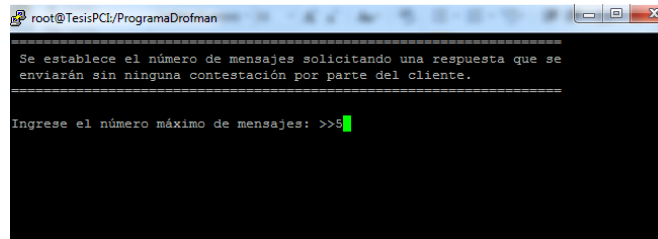


```

root@TesisPCL/ProgramaDrofman
=====
Hardening al servicio SSH
=====
1. Desactivar el usuario Root para que no pueda realizar conexión remota
2. Configurar intervalo de espera para conexión usuario
3. Establecer permisos a usuarios en archivos de configuración
4. Número máximo de intentos fallidos de login
5. Configuración de usuarios para acceso a SSH
6. Personalizar banner de bienvenida
7. Configurar tiempo de sesiones inactivas
8. Configuración de puerto de conexión
9. Reversa de hardening SQUID
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 2
=====
Desea configurar intervalo de espera para login? (S/N) >> S █

```

Figura 4. 61 Opción 2 - Intervalo de espera de conexión remota

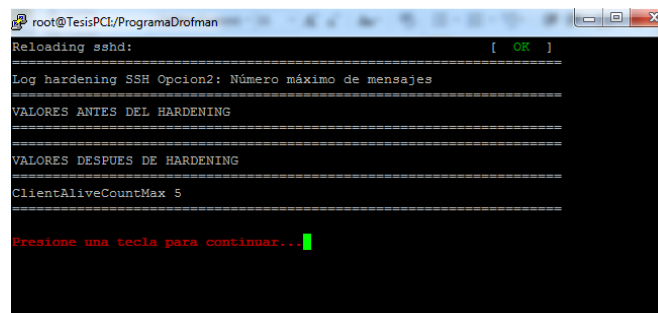


```

root@TesisPCl/ProgramaDrofman
=====
Se establece el número de mensajes solicitando una respuesta que se
enviarán sin ninguna contestación por parte del cliente.
=====
Ingrese el número máximo de mensajes: >>5

```

Figura 4. 62 Opción 2 – Ingreso de número de mensajes



```

root@TesisPCl/ProgramaDrofman
Reloading sshd: [ OK ]
Log hardening SSH Opcion2: Número máximo de mensajes
=====
VALORES ANTES DEL HARDENING
=====
VALORES DESPUES DE HARDENING
ClientAliveCountMax 5
=====
Presione una tecla para continuar...

```

Figura 4. 63 Opción 2 – Resultado de Hardening Aplicado

4.3.1.2.5.3 Opción 3 - Establecer permisos de usuarios a archivos de configuración de SSH

En la opción 3, se establece los permisos de usuarios a archivos de configuraciones en un nivel 600; que significa que el usuario pueda leer y escribir (figura 4.64 - 4.65).

```

root@TesisPCI/ProgramaDrofman
-----
Hardening al servicio SSH
-----
1. Desactivar el usuario Root para que no pueda realizar conexión remota
2. Configurar intervalo de espera para conexión usuario
3. Establecer permisos a usuarios en archivos de configuración
4. Número máximo de intentos fallidos de login
5. Configuración de usuarios para acceso a SSH
6. Personalizar banner de bienvenida
7. Configurar tiempo de sesiones inactivas
8. Configuración de puerto de conexión
9. Reversa de hardening SQUID
-----
0. REGRESAR A MENU PRINCIPAL
-----
Por favor ingresar opción >> 3
-----
Desea asignar permisos a archivos de configuración (S/N) >> S

```

Figura 4. 64 Opción 3 – Establecer permisos a usuarios en archivos de configuración

```

root@TesisPCI/ProgramaDrofman
Log Hardening SSH Opcion 3: Establece permisos en el Archivo de Configuración
-----
El archivo tiene asignado grupo y propietario correcto
-FW----- 1 root root 3816 Feb  9 02:40 /etc/ssh/sshd_config
El archivo tiene el permiso correcto 600
-FW----- 1 root root 3816 Feb  9 02:40 /etc/ssh/sshd_config
-----
Presione una tecla para continuar...

```

Figura 4. 65 Opción 3 – Resultado obtenido

4.3.1.2.5.4 Opción 4 - Número máximo de intentos fallidos durante el login del usuario.

En la opción 4, número máximo de intentos fallidos durante el login de usuario, indica hasta cuantas veces el usuario puede equivocarse al ingresar el usuario (figura 4.66 – 4.67 - 4.68).


```

root@TesisPCL/ProgramaDrofman
=====
Hardening al servicio SSH
=====
1. Desactivar el usuario Root para que no pueda realizar conexión remota
2. Configurar intervalo de espera para conexión usuario
3. Establecer permisos a usuarios en archivos de configuración
4. Número máximo de intentos fallidos de login
5. Configuración de usuarios para acceso a SSH
6. Personalizar banner de bienvenida
7. Configurar tiempo de sesiones inactivas
8. Configuración de puerto de conexión
9. Reversa de hardening SQUID

-----
0. REGRESAR A MENU PRINCIPAL
-----
Por favor ingresar opción >> 4
-----
Desea configurar el no. máximo de intentos fallidos de login? (S/N) >> S

```

Figura 4. 66 Opción 4 – Número máximo de intentos fallidos de login

```

root@TesisPCL/ProgramaDrofman
=====
Hardening SSH OP 4: Número máximo de Intento fallidos de login
=====
Este parámetro indica la cantidad de veces que podemos equivocarnos
en ingresar el usuario y/o contraseña. Luego de que se cumpla el no.
máximo de intentos se cierra la conexión ssh y evitaremos ataques
basados en la persistencia de la conexión.
=====
Ingrese valor máximo de intentos fallidos -->7

```

Figura 4. 67 Opción 4 - Ingreso de valor máximo de intentos

```

root@TesisPCL/ProgramaDrofman
=====
Log hardening SSH OP 4: No. máx. de Intentos fallidos de login
=====
VALOR ANTES DEL HARDENING
#MaxAuthTries 6
=====
VALORES DESPUES DEL HARDENING
MaxAuthTries 7
=====
Presione una tecla para continuar...

```

Figura 4. 68 Opción 4 – Resultado obtenido

4.3.1.2.5.5 Opción 5 - Configuración de usuarios para acceso mediante SSH

En la opción 5, configuración de usuarios para acceso mediante SSH, se establece los usuarios con sus respectivos grupos que tengan acceso permitido y denegado para realizar conexiones entrantes vía SSH (figuras 4.69 – 4.70 - 4.71).

```

root@TesisPC1/ProgramaDrofman
Hardening al servicio SSH

1. Desactivar el usuario Root para que no pueda realizar conexión remota
2. Configurar intervalo de espera para conexión usuario
3. Establecer permisos a usuarios en archivos de configuración
4. Número máximo de intentos fallidos de login
5. Configuración de usuarios para acceso a SSH
6. Personalizar banner de bienvenida
7. Configurar tiempo de sesiones inactivas
8. Configuración de puerto de conexión
9. Reversa de hardening SQUID

=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 5
=====
Desea configurar usuarios o grupos para acceso a SSH (S/N) >> S

```

Figura 4. 69 Opción 5 – Configuración de usuarios para acceso SSH

```

root@TesisPC1/ProgramaDrofman
Agregar lista de usuarios/grupos que pueden hacer login en el servidor
por medio del servicio SSH, también se especificará los usuarios/grupos
que no pueden ingresar. Ingrese cada usuario o grupo en el formato:
usuario1, usuario2 o grupo1, grupo2
=====
LISTADO DE USUARIOS CONFIGURADOS EN EL SERVIDOR
=====
nfsnobody
Sandra
=====
LISTADO DE GRUPOS CONFIGURADOS EN EL SERVIDOR
=====
nfsnobody
Sandra
=====
Usuarios Permitidos: >> Sandra
Grupos Permitidos: >> Sandra
Usuarios Denegados: >>
Grupos Denegados: >>

```

Figura 4. 70 Opción 5 - Ingreso de usuarios y grupos

```

root@TesisPCI/ProgramaDrofman
Log hardening OP 5: Limitar acceso via SSH
=====
VALORES ANTES DEL HARDENING
=====
No se ingreso listado de usuarios no permitidos
No se ingreso listado de grupos no permitidos
=====
VALORES DESPUES DEL HARDENING
AllowUsers Sandra
AllowGroups Sandra
=====
Presione una tecla para continuar... █

```

Figura 4. 71 Opción 5 - Resultado de Hardening Aplicado

4.3.1.2.5.6 Opción 6 - Personalización de Banner de Bienvenida

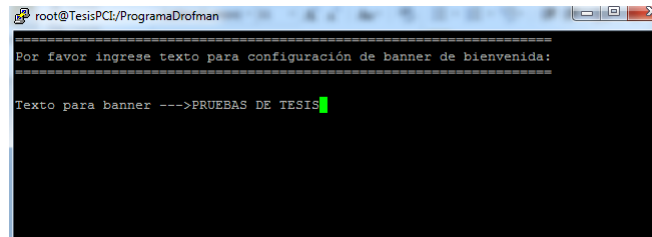
En la opción 6, Personalización de Banner de Bienvenida, se ingresa el texto que el usuario vera al inicio de cada conexión remota (figuras 4.72 – 4.73 - 4.74).

```

root@TesisPCI/ProgramaDrofman
=====
Hardening al servicio SSH
=====
1. Desactivar el usuario Root para que no pueda realizar conexión remota
2. Configurar intervalo de espera para conexión usuario
3. Establecer permisos a usuarios en archivos de configuración
4. Número máximo de intentos fallidos de login
5. Configuración de usuarios para acceso a SSH
6. Personalizar banner de bienvenida
7. Configurar tiempo de sesiones inactivas
8. Configuración de puerto de conexión
9. Reversa de hardening SQUID
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 6
=====
Desea configurar banner de bienvenida? (S/N) >> S █

```

Figura 4. 72 Opción 6 – Personalización de Banner

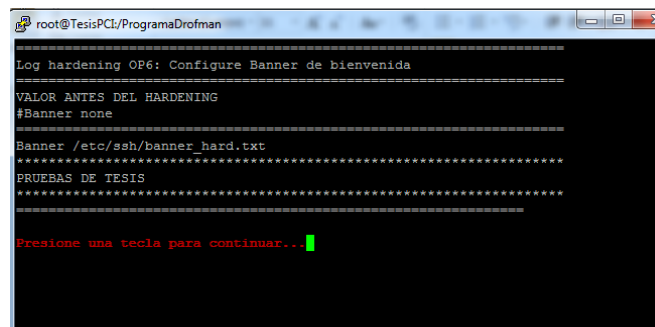


```

root@TesisPC1/ProgramaDroFman
=====
Por favor ingrese texto para configuración de banner de bienvenida:
=====
Texto para banner --->PRUEBAS DE TESIS

```

Figura 4. 73 Opción 6 – Ingreso de texto para banner



```

root@TesisPC1/ProgramaDroFman
=====
Log hardening OP6: Configure Banner de bienvenida
=====
VALOR ANTES DEL HARDENING
#Banner none
=====
Banner /etc/ssh/banner_hard.txt
*****
PRUEBAS DE TESIS
*****
Presione una tecla para continuar...

```

Figura 4. 74 Opción 6 - Resultado obtenido

4.3.1.2.5.7 Opción 7 - Configuración de tiempo de sesiones inactivas

En la opción 7, configuración de tiempo de sesiones inactivas la cual indica el tiempo permitido en el que el usuario puede estar sin hacer uso de la conexión remota, caso contrario habiendo llegado al límite fijado la conexión se inactiva teniendo que reiniciar la sesión figuras (4.75 – 4.76 - 4.77).

```

root@TesisPCI/ProgramaDrofman
=====
Hardening al servicio SSH
=====
1. Desactivar el usuario Root para que no pueda realizar conexión remota
2. Configurar intervalo de espera para conexión usuario
3. Establecer permisos a usuarios en archivos de configuración
4. Número máximo de intentos fallidos de login
5. Configuración de usuarios para acceso a SSH
6. Personalizar banner de bienvenida
7. Configurar tiempo de sesiones inactivas
8. Configuración de puerto de conexión
9. Reversa de hardening SQUID

-----
0. REGRESAR A MENU PRINCIPAL
-----
Por favor ingresar opción >> 7
Desea configurar tiempo de espera de inactividad de sesión (S/N) >> S

```

Figura 4. 75 Opción 7 – Configuración de tiempo de sesiones inactivas

```

root@TesisPCI/ProgramaDrofman
=====
Se configura la opcion ClientAliveInterval
Al configurar esta opción se establecerá un intervalo de tiempo
de espera en SEGUNDOS después del cual, si no hay datos recibidos
por parte del cliente SSH enviará un mensaje cifrado. En caso de
no recibir respuesta el usuario se desconectará.
Se recomienda valores mayores a 0
-----
Ingrese valor del Intervalo de tiempo en Segundos: >>5

```

Figura 4. 76 Opción 7- Ingrese valor de intervalo de tiempo

```

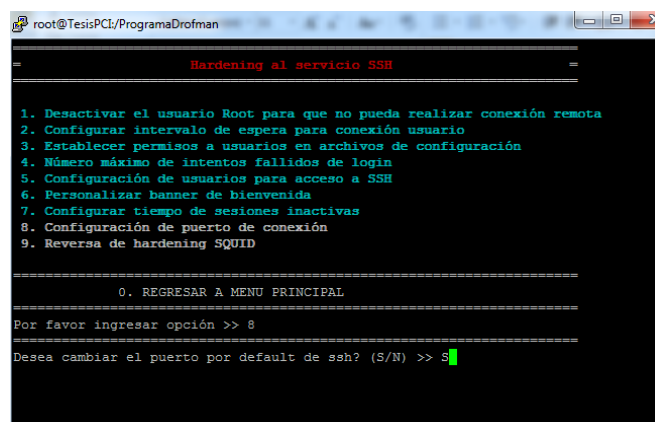
root@TesisPCI/ProgramaDrofman
=====
LOG HARDENING SSH_7: Tiempo de espera de sesiones sin actividad
=====
VALORES ANTES DEL HARDENING
=====
VALORES DESPUES DE HARDENING
=====
ClientAliveInterval 5
=====
Presione una tecla para continuar...

```

Figura 4. 77 Opción 7 – Resultado obtenido

4.3.1.2.5.8 Opción 8 - Configuración de puerto de conexión de SSH

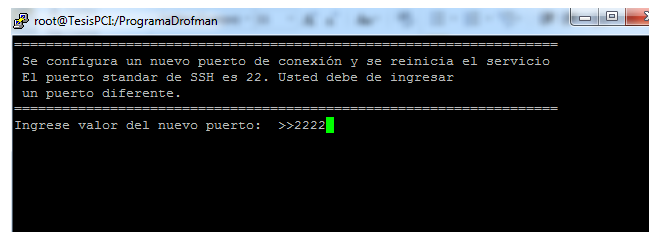
En la opción 8, configuración de puerto de conexión de SSH: se cambia el puerto por default que tiene SSH, cabe recalcar que los puertos asignados no deben ser los mismos que para otros servicios de Linux figura (4.78 – 4.79 - 4.80).



```
root@TesisPCL/ProgramaDrofman
=====
Hardening al servicio SSH
=====
1. Desactivar el usuario Root para que no pueda realizar conexión remota
2. Configurar intervalo de espera para conexión usuario
3. Establecer permisos a usuarios en archivos de configuración
4. Número máximo de intentos fallidos de login
5. Configuración de usuarios para acceso a SSH
6. Personalizar banner de bienvenida
7. Configurar tiempo de sesiones inactivas
8. Configuración de puerto de conexión
9. Reversa de hardening SQUID

=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 8
=====
Desea cambiar el puerto por default de ssh? (S/N) >> S
```

Figura 4. 78 Opción 8 - Configuración de puerto de conexión



```
root@TesisPCL/ProgramaDrofman
=====
Se configura un nuevo puerto de conexión y se reinicia el servicio
El puerto standar de SSH es 22. Usted debe de ingresar
un puerto diferente.
=====
Ingrese valor del nuevo puerto: >>2222
```

Figura 4. 79 Opción 8 – Ingrese valor del puerto

```

root@TesisPCL/ProgramaDrofman
=====
LOG HARDENING SSH_8: Configuración de puerto de conexión
=====
VALORES ANTES DEL HARDENING
=====
VALORES DESPUES DE HARDENING
=====
Port 2222
=====
Presione una tecla para continuar.. █

```

Figura 4. 80 Opción 8 – Resultado obtenido de Hardening Aplicado

4.3.1.2.5.9 Opción 9 - Reversa de hardening SSH

Esta opción permite realizar una reversa de todo el Hardening aplicado en el servicio mencionado. Este a su vez vuelve a activar todas las opciones del menú de SSH para poder ser aplicados nuevamente (figura 4.81 - 4.82).

```

root@TesisPCL/ProgramaDrofman
=====
HARDENING al servicio SSH
=====
1. Desactivar el usuario Root para que no pueda realizar conexión remota
2. Configurar intervalo de espera para conexión usuario
3. Establecer permisos a usuarios en archivos de configuración
4. Número máximo de intentos fallidos de login
5. Configuración de usuarios para acceso a SSH
6. Personalizar banner de bienvenida
7. Configurar tiempo de sesiones inactivas
8. Configuración de puerto de conexión
9. Reversa de hardening SQUID
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 9
=====
Desea revertir hardening de SSH? (S/N) >>S █

```

Figura 4. 81 Opción 9 - Reversa de hardening SSH

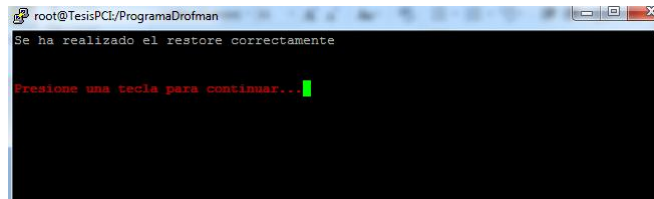


Figura 4. 82 Opción 10 - Mensaje de acción realizada

4.3.1.2.6 Hardening a NTP

Siendo la última opción tenemos en el menú por lo que se ingresa T y se muestra un mensaje “Desea aplicar hardening a servicio NTP (S/N)” (figura 4.83) para lo cual al ingresar S (si) se muestra una ventana donde se ven las opciones de hardening que se aplicarán al servicio NTP, si se ingresa N (no) no realiza acción y nuevamente se muestra el menú indicado.

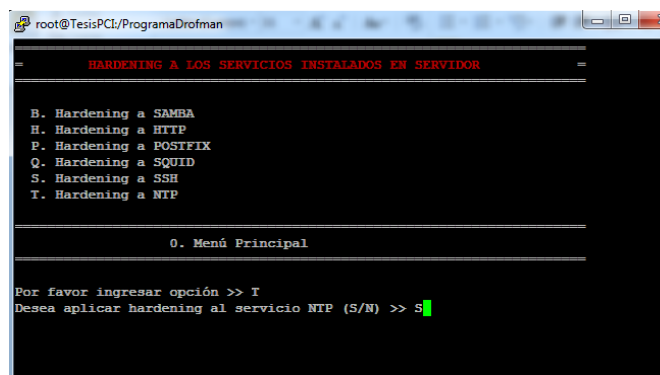
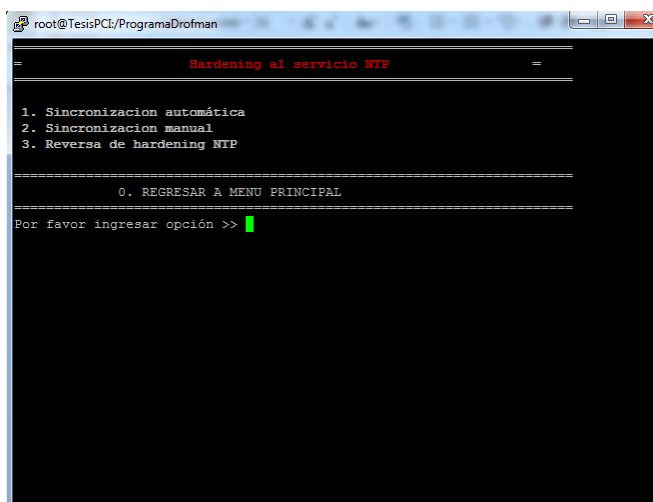


Figura 4. 83 Opción T ingresando S para realizar hardening NTP

Habiendo seleccionado la opción T y S al momento de la pregunta “Desea aplicar hardening al servicio NTP” se muestra el menú en el cual se detalla las

opciones de hardening a aplicar al servicio (figura 4.84). Se ingresará un número por hardening a aplicar siendo estas del 1 al 3 y al ingresar 0 se regresa al menú principal HARDENING A LOS SERVICIOS INSTALADOS EN EL SERVIDOR.



```
root@TesisPCI:/ProgramaDrofrman
=
Hardening al servicio NTP
=
1. Sincronización automática
2. Sincronización manual
3. Reversa de hardening NTP
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> █
```

Figura 4. 84 Menú Hardening de NTP

4.3.1.2.6.1 Sincronización automática

En esta opción como su nombre lo indica realiza la sincronización de la hora de manera automática con un servidor externo (figura 4.85 - 4.86).

Se ingresa 1 y se muestra un mensaje donde consulta si se desea aplicar la sincronización automática a la cual se pondrá S (si) y se pasa a una siguiente ventana en la cual se el resultado de la aplicación de este hardening. En caso de ingresar N no se realizará acción alguna quedando en mismo menú.

```

root@TesisPCL/ProgramaDrofman
=====
Hardening al servicio NTP
=====
1. Sincronizacion automática
2. Sincronizacion manual
3. Reversa de hardening NTP
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 1
=====
Desea aplicar sincronización automática? (S/N) >> S

```

Figura 4. 85 Opción 1 – Sincronización automática

```

root@TesisPCL/ProgramaDrofman
=====
Log hardening NTP Opción 1: Sincronización automática
=====
Se aplicó comando nptdate -u 2.pool.ntp.org
Presione una tecla para continuar...

```

Figura 4. 86 Opción 1 – Resultado obtenido

4.3.1.2.6.2 Sincronización manual

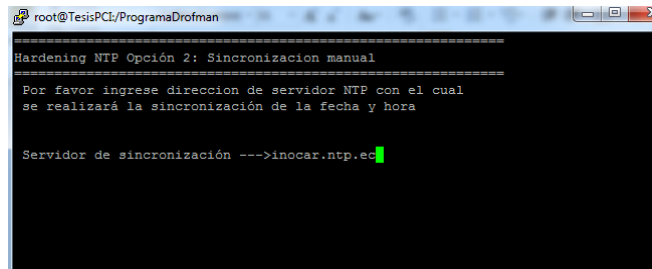
En la opción 2, le pide al usuario ingresar con que servidor de sincronización desea conectarse para tomar la fecha y hora, luego mostrara un reporte que indica cuales son los servidores NTP asignados a ese servidor.

```

root@TesisPCL/ProgramaDrofman
=====
Hardening al servicio NTP
=====
1. Sincronizacion automática
2. Sincronizacion manual
3. Reversa de hardening NTP
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 2
=====
Desea configurar sincronización manual (S/N) >> S

```

Figura 4. 87 Opción 2 – Sincronización manual



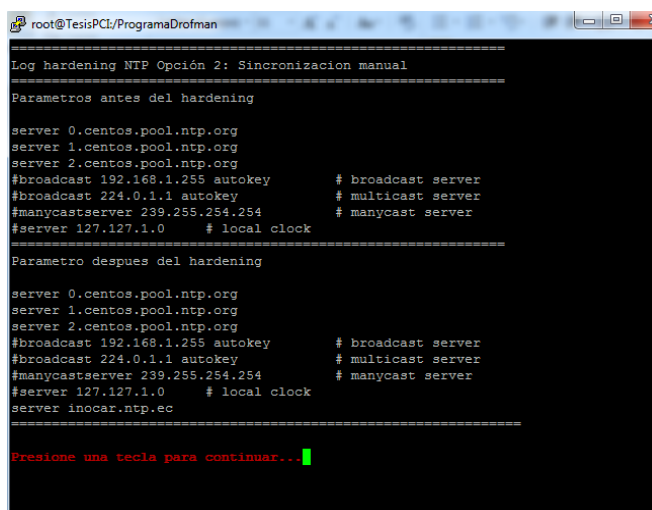
```

root@TesisPCL/ProgramaDrofman
=====
Hardening NTP Opción 2: Sincronizacion manual
=====
Por favor ingrese direccion de servidor NTP con el cual
se realizará la sincronización de la fecha y hora

Servidor de sincronización --->inocar.ntp.ec

```

Figura 4. 88 Opción 2 – Ingreso de servidor para la sincronización



```

root@TesisPCL/ProgramaDrofman
=====
Log hardening NTP Opción 2: Sincronizacion manual
=====
Parametros antes del hardening

server 0.centos.pool.ntp.org
server 1.centos.pool.ntp.org
server 2.centos.pool.ntp.org
#broadcast 192.168.1.255 autokey      # broadcast server
#broadcast 224.0.1.1 autokey        # multicast server
#manycastserver 239.255.254.254     # manycast server
#server 127.127.1.0                # local clock

Parametro despues del hardening

server 0.centos.pool.ntp.org
server 1.centos.pool.ntp.org
server 2.centos.pool.ntp.org
#broadcast 192.168.1.255 autokey      # broadcast server
#broadcast 224.0.1.1 autokey        # multicast server
#manycastserver 239.255.254.254     # manycast server
#server 127.127.1.0                # local clock
server inocar.ntp.ec

Presione una tecla para continuar...

```

Figura 4. 89 Opción 2 – Resultado obtenido

4.3.1.2.6.3 Reversa de Hardening NTP

Esta opción permite realizar una reversa de todo el Hardening aplicado en el servicio mencionado. Este a su vez vuelve a activar todas las opciones del menú de NTP ingresando el número 3 para poder ser aplicados nuevamente (figura 4.90)

```

root@TesisPCI/ProgramaDrofman
=====
Hardening al servicio NTP
=====
1. Sincronización automática
2. Sincronización manual
3. Reversa de hardening NTP
=====
0. REGRESAR A MENU PRINCIPAL
=====
Por favor ingresar opción >> 3
=====
Desea revertir hardening de NTP (S/N) >> s

```

Figura 4. 90 Opción 3 – Reversa de hardening NTP

```

root@TesisPCI/ProgramaDrofman
Se ha realizado el restore correctamente

Presione una tecla para continuar..

```

Figura 4. 91 Opción 3 - Mensaje de acción realizada

4.3.1.3 Opción 3 – Reportes de servicios en el servidor

En la opción 3, se mostraran todos los reportes ya sea a nivel de sesión, histórico y reportes de auditoria. Se ingresa a la opción 3 del menú principal junto al texto “Por favor ingresar opción >>”. (Figura 4.92)



Figura 4. 92 Menú principal de Hardening

Habiendo ingresado la opción 3, se muestra una ventana la cual tiene otro menú de reportes detallados de la siguiente manera: (figura 4.93)

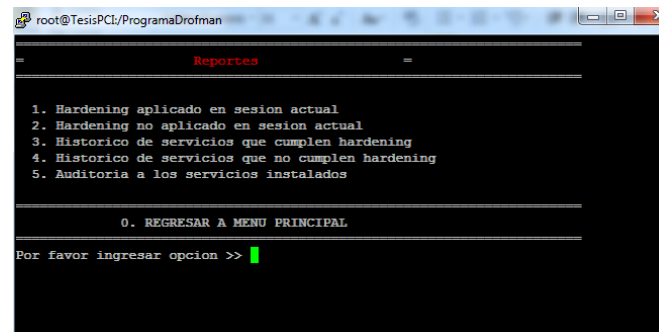


Figura 4. 93 Submenú de Reportes

4.3.1.3.1 Opción 1 - Hardening aplicado en la sesión actual.

Habiendo ingresado la opción 1 (figura 4.94), se genera el reporte de las opciones de hardening que fueron aplicadas durante la sesión actual del aplicativo realizado para el proyecto (figura 4.95).

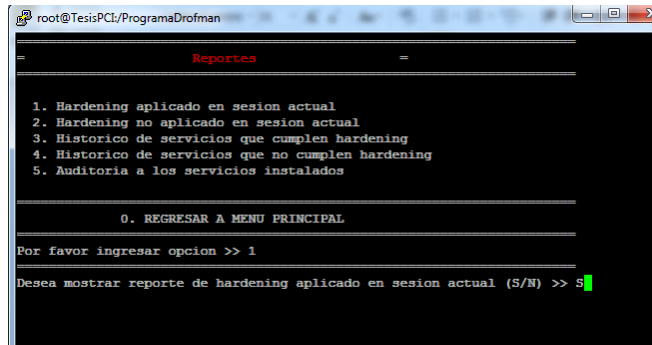


Figura 4. 94 Opción 1 – Hardening aplicado en la sesión actual

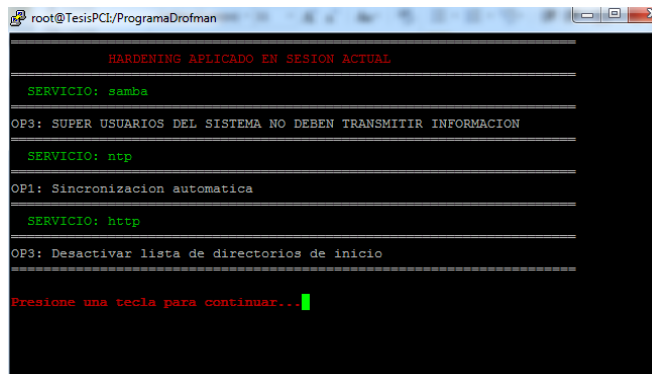


Figura 4. 95 Reporte de hardening aplicado en sesión actual

4.3.1.3.2 Opción 2 - Hardening no aplicado en sesión actual

Habiendo ingresado la opción 2 (figura 4.96), se genera el reporte de las opciones de hardening que no fueron aplicadas durante la sesión actual del aplicativo realizado para el proyecto (figura 4.97).

```

root@TesisPCL/ProgramaDrofman
Reportes
-----
1. Hardening aplicado en sesion actual
2. Hardening no aplicado en sesion actual
3. Historico de servicios que cumplen hardening
4. Historico de servicios que no cumplen hardening
5. Auditoria a los servicios instalados
-----
0. REGRESAR A MENU PRINCIPAL
-----
Por favor ingresar opcion >> 2
Desea mostrar reporte del hardening no aplicado en sesion actual (S/N) >> S

```

Figura 4. 96 Opción 2 – Hardening no aplicado en sesión actual

```

root@TesisPCL/ProgramaDrofman
HARDENING NO APLICADO EN SESION ACTUAL
-----
SERVICIO: ssmtp
-----
OP1: Definir host permitidos para transferencia de informacion
-----
Presione una tecla para continuar...

```

Figura 4. 97 Reporte de Hardening no aplicado en sesión actual

4.3.1.3.3 Opción 3 - Histórico de servicios que cumplen hardening

Habiendo ingresado la opción 3 (figura 4.98), se genera el reporte histórico de las opciones de hardening que fueron aplicadas en el proyecto (figura 4.99).

```

root@TesisPCL/ProgramaDrofman
Reportes
-----
1. Hardening aplicado en sesion actual
2. Hardening no aplicado en sesion actual
3. Historico de servicios que cumplen hardening
4. Historico de servicios que no cumplen hardening
5. Auditoria a los servicios instalados
-----
0. REGRESAR A MENU PRINCIPAL
-----
Por favor ingresar opcion >> 3
Desea mostrar reporte historico de servicios que cumplen hardening? (S/N) >> S

```

Figura 4. 98 Opción 3 – Histórico de servicios que cumplen Hardening

```

root@TesisPC1/ProgramaDrofman
LISTADO HISTORICO DE SERVICIOS QUE CUMPLEN CON PCI
POR APLICACION DE HARDENING

SERVICIO: samba
OP3: SUPER USUARIOS DEL SISTEMA NO DEBEN TRANSMITIR INFORMACION

SERVICIO: squid
OP1: Apagar funcion PIC y HTCP
OP2: Activar SNMP
OP3: Restringir accesos a Proxy Squid

SERVICIO: ntp
OP1: Sincronizacion automatica

SERVICIO: http
OP3: Desactivar lista de directorios de inicio

Presione una tecla para continuar... █

```

Figura 4. 99 Reporte de Hardening Aplicados (Histórico)

4.3.1.3.4 Opción 4 - Histórico de servicios que no cumplen hardening.

Habiendo ingresado la opción 4 (figura 4.100), se genera el reporte histórico de las opciones de hardening que fueron rechazadas por el usuario en el proyecto (figura 4.101).

```

root@TesisPC1/ProgramaDrofman
Reportes
-----
1. Hardening aplicado en sesion actual
2. Hardening no aplicado en sesion actual
3. Historico de servicios que cumplen hardening
4. Historico de servicios que no cumplen hardening
5. Auditoria a los servicios instalados

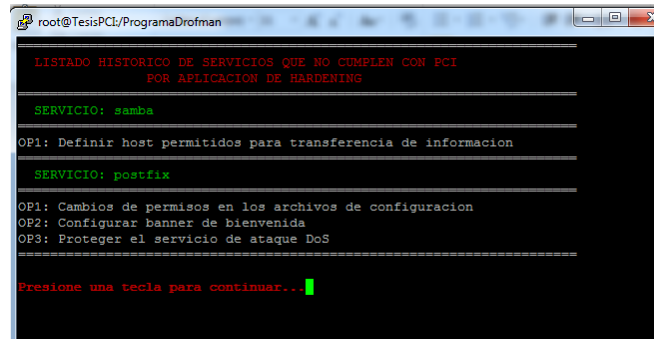
0. REGRESAR A MENU PRINCIPAL

Por favor ingresar opcion >> 4

Desea mostrar reporte historico de servicios que no cumplen hardening? (S/N)
>> S █

```

Figura 4. 100 Opción 4 – Histórico de servicios que no cumplen Hardening



```

root@TesisPCI/ProgramaDrofman
LISTADO HISTORICO DE SERVICIOS QUE NO CUMPLEN CON PCI
POR APLICACION DE HARDENING
-----
SERVICIO: samba
OP1: Definir host permitidos para transferencia de informacion
-----
SERVICIO: postfix
OP1: Cambios de permisos en los archivos de configuracion
OP2: Configurar banner de bienvenida
OP3: Proteger el servicio de ataque DoS
=====
Presione una tecla para continuar... █

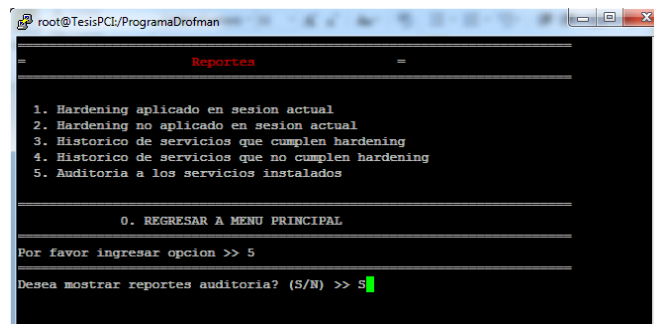
```

Figura 4. 101 Reporte de Hardening Aplicados (Histórico)

NOTA: El hecho de mostrar información en este reporte indica que la empresa como tal no está cumpliendo con el estándar PCI y generaría que la empresa pierda sus certificaciones.

4.3.1.3.5 Opción 5 - Auditoria a los servicios instalados.

Habiendo ingresado la opción 5 (figura 4.102), muestra otro menú en el que se detallan reportes por servicio instalado los cuales ayudan al usuario a tener una mejor administración de lo que se realiza en los servidores.



```

root@TesisPCI/ProgramaDrofman
-----
Reportes
-----
1. Hardening aplicado en sesion actual
2. Hardening no aplicado en sesion actual
3. Historico de servicios que cumplen hardening
4. Historico de servicios que no cumplen hardening
5. Auditoria a los servicios instalados
-----
0. REGRESAR A MENU PRINCIPAL
-----
Por favor ingresar opcion >> 5
Desea mostrar reportes auditoria? (S/N) >> S █

```

Figura 4. 102 Opción 5 – Auditoria a los servicios instalados

4.3.1.3.5.1 Opción B – Auditoria SAMBA

Habiendo ingresado la opción B (figura 4.103), se genera el reporte de auditoria de Samba donde muestra las conexiones y desconexiones que ha tenido el usuario, creación y eliminación de archivos/carpetas. (Figura 4.104).



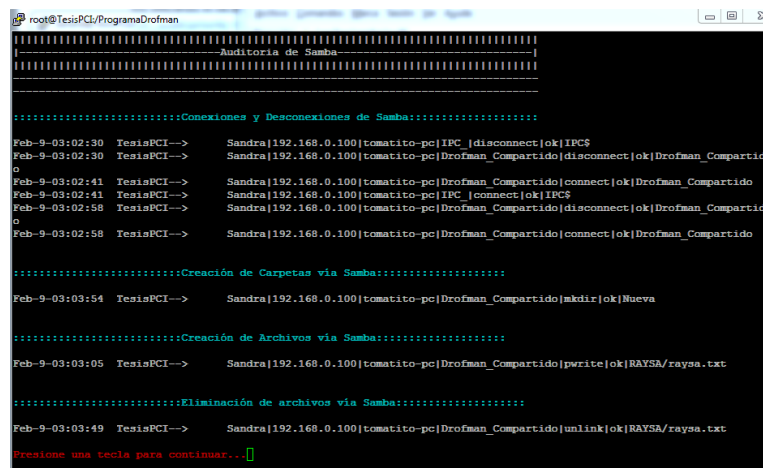
```

root@TesisPCI/ProgramaDrofman
=====
          AUDITORIA A LOS SERVICIOS INSTALADOS EN SERVIDOR
=====
B. Auditoria a SAMBA
H. Auditoria a HTTP
P. Auditoria a POSTFIX
Q. Auditoria a SQUID
S. Auditoria a SSH
T. Auditoria a NTP

-----
0. Menú Principal
-----

Por favor ingresar opción >> B
Desea aplicar auditoria al servicio SAMBA (S/N) >> S
  
```

Figura 4. 103 Opción B – Auditoria SAMBA



```

root@TesisPCI/ProgramaDrofman
=====
          Auditoria de Samba
=====
-----
.....:Conexiones y Desconexiones de Samba:.....
-----
Feb-9-03:02:30 TesisPCI--> Sandra|192.168.0.100|tomatito-pc|IPC |disconnect|ok|IPC$
Feb-9-03:02:30 TesisPCI--> Sandra|192.168.0.100|tomatito-pc|Drofman_Compartido|disconnect|ok|Drofman_Compartido
0
Feb-9-03:02:41 TesisPCI--> Sandra|192.168.0.100|tomatito-pc|Drofman_Compartido|connect|ok|Drofman_Compartido
Feb-9-03:02:41 TesisPCI--> Sandra|192.168.0.100|tomatito-pc|IPC |connect|ok|IPC$
Feb-9-03:02:58 TesisPCI--> Sandra|192.168.0.100|tomatito-pc|Drofman_Compartido|disconnect|ok|Drofman_Compartido
0
Feb-9-03:02:58 TesisPCI--> Sandra|192.168.0.100|tomatito-pc|Drofman_Compartido|connect|ok|Drofman_Compartido

.....:Creación de Carpetas via Samba:.....
-----
Feb-9-03:03:54 TesisPCI--> Sandra|192.168.0.100|tomatito-pc|Drofman_Compartido|mkdir|ok|Nueva

.....:Creación de Archivos via Samba:.....
-----
Feb-9-03:03:05 TesisPCI--> Sandra|192.168.0.100|tomatito-pc|Drofman_Compartido|write|ok|RAYSA/raysa.txt

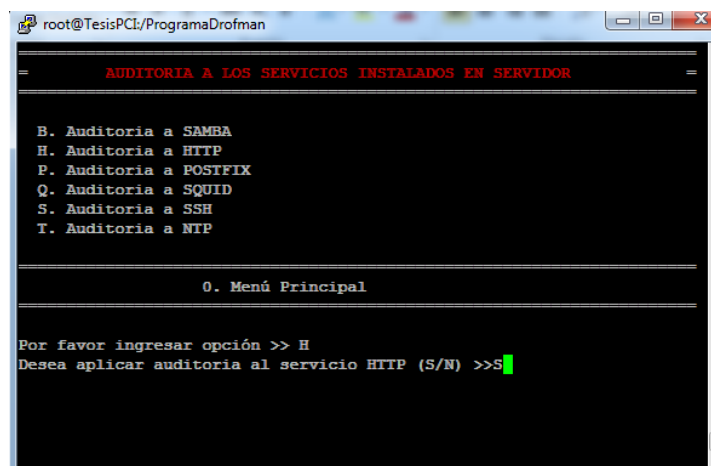
.....:Eliminación de archivos via Samba:.....
-----
Feb-9-03:03:49 TesisPCI--> Sandra|192.168.0.100|tomatito-pc|Drofman_Compartido|unlink|ok|RAYSA/raysa.txt

Presione una tecla para continuar...
  
```

Figura 4. 104 Reporte de Auditoria Samba

4.3.1.3.5.2 Opción H – Auditoria HTTP

Habiendo ingresado la opción H (figura 4.105), se muestra un menú (figura 4.106) en el cual nos da las opciones de revisar desde que IP han ingresado a nuestros servidores Web (figura 4.107 - 4.108) y la revisión de los errores ocurridos en nuestra WebSite (figura 4.109 - 4.110).

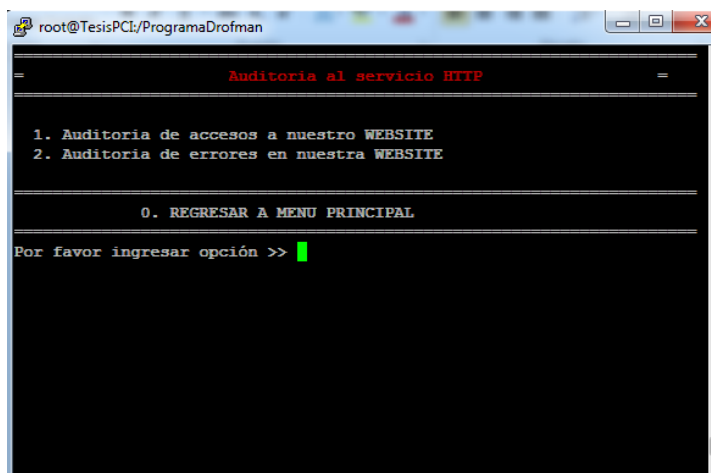


```
root@TesisPCI:/ProgramaDrofman
=
  AUDITORIA A LOS SERVICIOS INSTALADOS EN SERVIDOR
=
B. Auditoria a SAMBA
H. Auditoria a HTTP
P. Auditoria a POSTFIX
Q. Auditoria a SQUID
S. Auditoria a SSH
T. Auditoria a NTP

0. Menú Principal

Por favor ingresar opción >> H
Desea aplicar auditoria al servicio HTTP (S/N) >>S
```

Figura 4. 105 Opción H – Auditoria HTTP

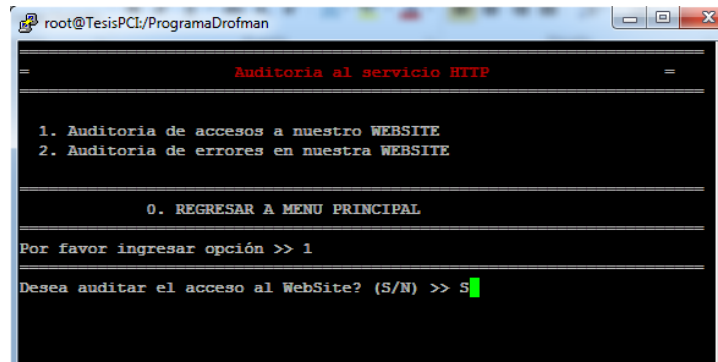


```
root@TesisPCI:/ProgramaDrofman
=
  Auditoria al servicio HTTP
=
1. Auditoria de accesos a nuestro WEBSITE
2. Auditoria de errores en nuestra WEBSITE

0. REGRESAR A MENU PRINCIPAL

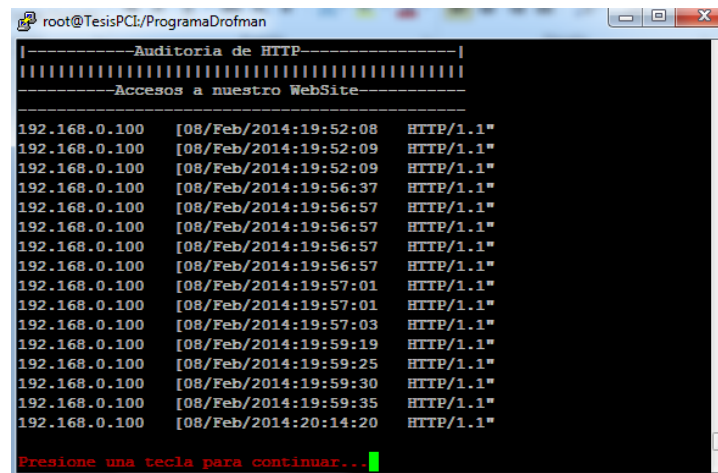
Por favor ingresar opción >>
```

Figura 4. 106 Menú de Auditoria HTTP



```
root@TesisPCI/ProgramaDrofman
-----
Auditoria al servicio HTTP
-----
1. Auditoria de accesos a nuestro WEBSITE
2. Auditoria de errores en nuestra WEBSITE
-----
0. REGRESAR A MENU PRINCIPAL
-----
Por favor ingresar opción >> 1
-----
Desea auditar el acceso al WebSite? (S/N) >> S
```

Figura 4. 107 Opción 1 - Auditoria de acceso a nuestro WebSite



```
root@TesisPCI/ProgramaDrofman
|-----Auditoria de HTTP-----|
|=====|
|-----Accesos a nuestro WebSite-----|
|=====|
192.168.0.100 [08/Feb/2014:19:52:08 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:52:09 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:52:09 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:56:37 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:56:57 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:56:57 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:56:57 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:56:57 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:56:57 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:57:01 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:57:01 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:57:03 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:59:19 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:59:25 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:59:30 HTTP/1.1"
192.168.0.100 [08/Feb/2014:19:59:35 HTTP/1.1"
192.168.0.100 [08/Feb/2014:20:14:20 HTTP/1.1"
Presione una tecla para continuar...
```

Figura 4. 108 Resultado de Accesos a nuestra WebSite

```

root@TesisPCI:/ProgramaDrofman
=====
                        Auditoria al servicio HTTP
=====

1. Auditoria de accesos a nuestro WEBSITE
2. Auditoria de errores en nuestra WEBSITE

=====

0. REGRESAR A MENU PRINCIPAL

=====

Por favor ingresar opción >> 2

=====

Desea auditar los errores del WebSite (S/N) >> S

```

Figura 4. 109 Opción 2 - Auditoria de errores en nuestro WebSite

```

root@TesisPCI:/ProgramaDrofman
-----Auditoria de HTTP-----
|||||
-----Errores en nuestra WebSite-----
-----

[Sat Feb 08 19:52:09 192.168.0.100] /var/www/html/drofmansite/favico
n.ico
[Sat Feb 08 19:52:09 192.168.0.100] /var/www/html/drofmansite/favico
n.ico
[Sat Feb 08 19:56:57 192.168.0.100] /var/www/html/drofmansite/logo1
.jpg,
[Sat Feb 08 19:56:57 192.168.0.100] /var/www/html/drofmansite/icono
.ico
[Sat Feb 08 19:56:57 192.168.0.100] /var/www/html/drofmansite/icono
.ico
[Sat Feb 08 19:57:01 192.168.0.100] /var/www/html/drofmansite/logo1
.jpg,
[Sat Feb 08 19:57:03 192.168.0.100] /var/www/html/drofmansite/diagr
ama.html,
[Sat Feb 08 20:14:20 192.168.0.100] /var/www/html/drofmansite/logo1
.jpg,

Presione una tecla para continuar...

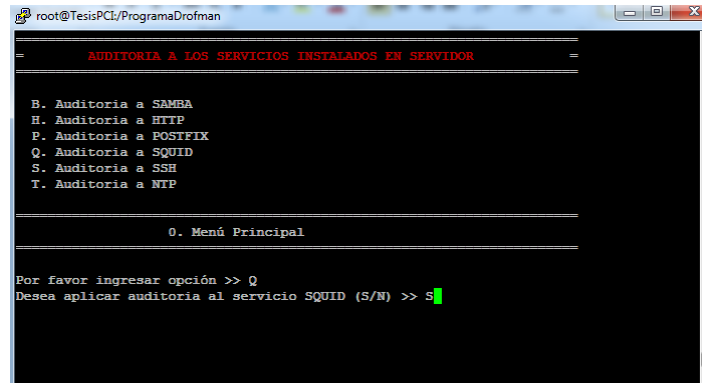
```

Figura 4. 110 Resultado de Errores en nuestro WebSite

4.3.1.3.5.3 Opción Q – Auditoria SQUID

Habiendo ingresado la opción Q (figura 4.111), se genera el reporte de proxy Squid el cual nos muestra un informe de las 10 últimas páginas visitadas a través de nuestro servidor proxy, así se podrá tener un mayor control con los

usuarios referente al uso de acceso a Internet.(figura 4.112)



```

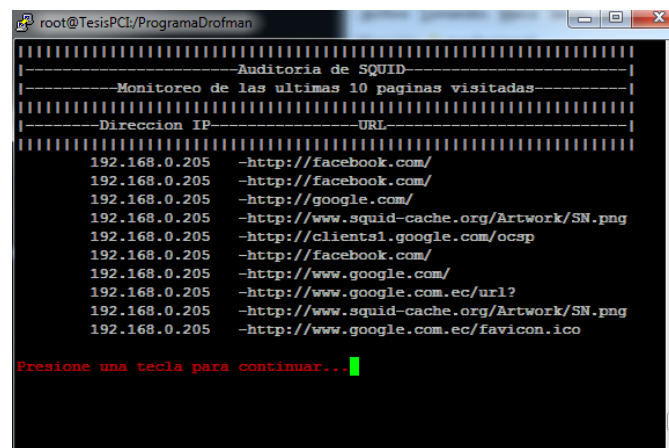
root@TesisPCI:/ProgramaDrofman
=====
          AUDITORIA A LOS SERVICIOS INSTALADOS EN SERVIDOR
=====
B. Auditoria a SAMBA
H. Auditoria a HTTP
P. Auditoria a POSTFIX
Q. Auditoria a SQUID
S. Auditoria a SSH
T. Auditoria a NTP

0. Menú Principal

Por favor ingresar opción >> Q
Desea aplicar auditoria al servicio SQUID (S/M) >> S

```

Figura 4. 111 Opción Q – Auditoria SQUID



```

root@TesisPCI:/ProgramaDrofman
=====
          Auditoria de SQUID
=====
|-----Monitoreo de las ultimas 10 paginas visitadas-----|
|-----Direccion IP-----URL-----|
|-----|-----|-----|-----|-----|-----|-----|-----|-----|
192.168.0.205 -http://facebook.com/
192.168.0.205 -http://facebook.com/
192.168.0.205 -http://google.com/
192.168.0.205 -http://www.squid-cache.org/Artwork/SN.png
192.168.0.205 -http://clients1.google.com/ocsp
192.168.0.205 -http://facebook.com/
192.168.0.205 -http://www.google.com/
192.168.0.205 -http://www.google.com.ec/url?
192.168.0.205 -http://www.squid-cache.org/Artwork/SN.png
192.168.0.205 -http://www.google.com.ec/favicon.ico

Presione una tecla para continuar...

```

Figura 4. 112 Resultado de Auditoria SQUID

4.3.1.3.5.4 Opción S – Auditoria SSH

Habiendo ingresado la opción S (figura 4.113), se genera un informe de las conexiones entrantes hacia nuestro servidor por medio del puerto asignado en el aplicativo.

```

root@TesisPCI:/ProgramaDrofman
=====
          AUDITORIA A LOS SERVICIOS INSTALADOS EN SERVIDOR
=====
B. Auditoria a SAMBA
H. Auditoria a HTTP
P. Auditoria a POSTFIX
Q. Auditoria a SQUID
S. Auditoria a SSH
T. Auditoria a NTP

0. Menú Principal

Por favor ingresar opción >> S
Desea aplicar auditoria al servicio SSH (S/N) >> S

```

Figura 4. 113 Opción S – Auditoria SSH

```

root@TesisPCI:/ProgramaDrofman
-----Auditoria de SSH-----
-----Conexiones entrantes aceptadas-----
Feb 8 19:24:01      192.168.0.100    root
Feb 8 19:34:44      192.168.0.100    root
Feb 8 19:50:30      192.168.0.100    root
Feb 8 19:53:56      192.168.0.100    root
Feb 8 19:55:13      192.168.0.100    root
Feb 8 19:55:56      192.168.0.100    root
Feb 8 20:12:30      192.168.0.100    root
Feb 9 01:58:44      192.168.0.100    root
Feb 9 03:01:54      192.168.0.100    Sandra
-----Conexiones rechazadas o fallidas-----
Presione una tecla para continuar...

```

Figura 4. 114 Resultado de Auditoria SSH

4.3.1.3.5.5 Opción T – Auditoria NTP

Habiendo ingresado la opción T (figura 4.115), se genera un informe de todas las sincronizaciones de hora exitosas de nuestro servidor. (Figura 4.116)

```

root@TesisPCI:/ProgramaDrofman
=====
          AUDITORIA A LOS SERVICIOS INSTALADOS EN SERVIDOR
=====
B. Auditoria a SAMBA
H. Auditoria a HTTP
P. Auditoria a POSTFIX
Q. Auditoria a SQUID
S. Auditoria a SSH
T. Auditoria a NTP

0. Menú Principal

Por favor ingresar opción >> T
Desea aplicar auditoria al servicio NTP (S/N) >> S
  
```

Figura 4. 115 Opción T – Auditoria NTP

```

root@TesisPCI:/ProgramaDrofman
=====
          Auditoria de NTP
=====
          Registro de Sincronizaciones
=====
9 Feb  02:44:28      adjust time   server 192.188.53.26
9 Feb  02:45:07      adjust time   server 190.15.128.72
9 Feb  02:46:52      adjust time   server 192.188.53.26

Presione una tecla para continuar...
  
```

Figura 4. 116 Resultado de Auditoria NTP

4.4 Implementación de un plan de prevención contra vulnerabilidades

- Implementar las cláusulas para el cumplimiento del **Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago**, software que fue implementado puede ser aplicados en servidores Linux.

- Llevar un control de perfiles de usuarios y permisos asignados de los mismos para mitigar los accesos innecesarios a la infraestructura TI.
- Implementar hardening de servicios críticos de TI expuestos a Internet, es decir aplicar Hardening a servidores Web,
- Aplicar soluciones a las vulnerabilidades identificadas a fin de evitar exponer servicios vulnerables críticos de la infraestructura TI.
- Mantener un programa de gestión de vulnerabilidades, para minimizar las consecuencias por ataques de seguridad informática.

CONCLUSIONES

Las principales conclusiones alcanzadas son las siguientes:

1. Se realizó un proceso de identificaron de los riesgos y vulnerabilidades a los que estaba expuesto DROFMAN S.A., lo cual permitió generar un plan de acción para su mitigación y protección de la infraestructura TI de la empresa.

2. Se propuso un procedimiento que consistió en desarrollar un aplicativo que puede ser utilizado en cualquier institución financiera el cual que permite cumplir con el Estándar PCI.
3. Se aplicaron soluciones a las vulnerabilidades reportadas aplicando Hardening basado en PCI y se generaron reportes para entregar a las personas indicadas quienes velan por la seguridad integra de la empresa.
4. Se fijó un plan de implementación para de prevención contra vulnerabilidades en los servicios a futuro.
5. Es necesario ejecutar cada tres meses el plan de implementación propuesto para lograr llevar un índice de vulnerabilidades encontradas con sus respectivas soluciones y de esta manera tener indicativos que orienten el buen desarrollo de la práctica.

BIBLIOGRAFÍA

- [1] Wikipedia, Payment Card Industry Data Security Standard,
http://es.wikipedia.org/wiki/PCI_DSS, fecha de consulta noviembre 2013
- [2] Security Standards Council, Requirements and Security Assessment
Procedures, https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf,
fecha de consulta noviembre 2013
- [3] Puschitz Werner, A Practical Guide to Basic Linux Security in Production
Enterprise Environments, <http://www.puschitz.com/SecuringLinux.shtml>, fecha
de consulta noviembre 2013
- [4] Slideshare, Mejorando la seguridad del servicio ssh,
[http://www.slideshare.net/gnrfan/mejorando-la-seguridad-del-servicio-ssh-
hardening](http://www.slideshare.net/gnrfan/mejorando-la-seguridad-del-servicio-ssh-hardening), fecha de consulta noviembre 2013
- [5] Caballé Xavier, Top 10 de Vulnerabilidades Windows y Linux según el Sans,
<http://www.somoslibres.org/modules.php?name=News&file=article&sid=307>,
fecha de consulta noviembre 2013
- [6] Mifsud Elvira, Introducción a la seguridad informática - Vulnerabilidades de
un sistema informático,
[http://recursostic.educacion.es/observatorio/web/es/component/content/article/1
040-introduccion-a-la-seguridad-informatica?start=3](http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3), fecha de consulta
noviembre 2013

- [7] Internet Security Auditors, Implantación y Certificación en el Estándar PCI DSS, <http://www.isecauditors.com/implantacion-pci-dss>, fecha de consulta noviembre 2013
- [8] Saurio Dino, Fortalece Tu Servidor y Dificulta La Tarea del Atacante, <http://world-of-dino.blogspot.com/2012/04/hardening-fortalece-tu-servidor-y.html>, fecha de consulta noviembre 2013
- [9] Pichel Ferran, Hardening básico de Linux Permisos y Configuraciones, http://www.isecauditors.com/sites/default/files//files/iseclab13-hardening_basico_linux_permisos_y_configuraciones.pdf, fecha de consulta noviembre 2013
- [10] Norma PCI, Requerimientos para administrar la seguridad, las políticas, procedimientos, la arquitectura de redes, el diseño de software y otras medidas críticas de protección de la información, <http://www.normapci.com/>, fecha de consulta noviembre 2013

ANEXOS

ANEXO 1.- Scripts implementados.

Menú Principal De Hardening A Los Servicios Instalados En El Servidor

```

#menu.sh Versión 2 del menú principal para cumplir pedido de director de tesis
# donde se divide el proceso de hardening en 5 pasos
# Se invoca con un número entero según opciones del menú
cp logs/*.log logs/backup/
clear
echo
"=====
=====
echo "=
echo -e "=
=e[o"
echo -e "=
DSS\e[o \e[1;37m =\e[o"
echo "=
echo
"=====
=====
echo "
echo " 1. Servicios habilitados en el servidor "
echo " 2. Hardening a los servicios instalados en el servidor "
echo " 3. Reportes de servicios en el servidor "
echo "
echo
"=====
=====
echo " 0. SALIR "
echo
"=====
=====
echo "
read -p "Por favor ingresar opción >> " X

```

```

VALOR=$X
case $VALOR in
    1)
        sh seccion1.sh;;
    2)
        sh seccion2.sh;;
    3)
        sh seccion4.sh;;
    0)
        cp logs/*.log logs/backup> /dev/null;
        cp logs/*.rpt logs/backup> /dev/null;
        rm -f logs/*.log> /dev/null;
        rm -f logs/*.rpt> /dev/null;
        clear
        exit;;
    *)
        echo -e "\e[1;31m      ***** ENTRADA NO VÁLIDA *****\e[o \e[1;37m"
        read -p " "
        sh menu.sh;;
esac
#fin del menú

```

Sección # 1

```

#!/bin/bash
#Validación de servicios habilitados en el servidor
#Esta validación se realizara con 7 servicios previamente seleccionados
#Postfix - Samba - SSH - FTP - VNC - Squid - NTP
#Esta validación será; la base para la aplicación del hardening en la seccion2
#Para lo cual se creará; un archivo oculto dentro del directorio
#.config/.servicios.cfg
#Se define ruta de archivo de configuración de servicios
FILECFG=".config/.serviceON.cfg"
FILETMP=".config/.tmp1.cfg"
FILECFGNULL=".config/.serviceNULL.cfg"
#Cada vez que se ejecute este script procederá; a eliminar el archivo
# de configuración
rm $FILECFG
rm $FILECFGNULL

```

```

#Se empieza a armar archivo de configuración de servicios
echo
"=====
"
> $FILECFG
echo "          SERVICIOS INSTALADOS EN EL SERVIDOR          " >>
$FILECFG
echo
"=====
"
>> $FILECFG
echo "  SERVICIOS          ESTADO          PUERTO          " >> $FILECFG
echo "-----" >> $FILECFG
#Validamos postfix
SERVI1="postfix"
SERVI2="POSTFIX      "
service $SERVI1 status > $FILETMP
if grep -i running $FILETMP > /dev/null; then
#Si el servicio está en ejecución registra configuración
echo -e "  $SERVI2    \e[1;32m RUNNING \e[0m          25/TCP          "
>>$FILECFG
else
#Si servicio no está; running se valida si está detenido o no existe"
if grep -i stopped $FILETMP > /dev/null; then
#Si el servicio está; detenido registra configuración
echo -e "  $SERVI2    \e[0;31m STOPPED \e[0m          "
>>$FILECFG
else
echo "$SERVI2 NO INSTALADO" >> $FILECFGNULL
fi
fi
SERVI1="squid"
SERVI2="SQUID      "
service $SERVI1 status > $FILETMP
if grep -i running $FILETMP > /dev/null; then
#Si el servicio está en ejecución registra configuración
echo -e "  $SERVI2    \e[1;32m      RUNNING \e[0m          3128/TCP          "
>>$FILECFG
else
#Si servicio no está; running se valida si está detenido o no existe"
if grep -i stopped $FILETMP > /dev/null; then
#Si el servicio está; detenido registra configuración

```



```

echo -e "  $SERVI2 \e[0;31m  STOPPED \e[0m          " >>$FILECFG
else
echo "$SERVI2 NO INSTALADO" >> $FILECFGNULL
fi
fi
clear
#Validamos SSH
SERVI1="sshd"
SERVI2="SSHD          "
service $SERVI1 status > $FILETMP
if grep -i running $FILETMP> /dev/null; then
#Si el servicio está en ejecución registra configuración
if grep ^Port /etc/ssh/sshd_config> /dev/null; then
PUERTO=`grep "^Port" /etc/ssh/sshd_config | awk '{ print $2}'`
echo -e "  $SERVI2 \e[1;32m  RUNNING \e[0m          $PUERTO/TCP          "
>>$FILECFG
else
echo -e "  $SERVI2 \e[1;32m  RUNNING \e[0m          22/TCP          "
>>$FILECFG
fi
else
#Si servicio no está; running se valida si está detenido o no existe"
if grep -i stopped $FILETMP> /dev/null; then
#Si el servicio está; detenido registra configuración
echo -e "  $SERVI2 \e[0;31m  STOPPED          \e[0m          "
>>$FILECFG
else
echo "$SERVI2 NO INSTALADO" >> $FILECFGNULL
fi
fi
#Validamos NTP
SERVI1="ntpd"
SERVI2="NTPD          "
service $SERVI1 status > $FILETMP
if grep -i running $FILETMP> /dev/null; then
#Si el servicio está en ejecución registra configuración
echo -e "  $SERVI2 \e[1;32m  RUNNING \e[0m          123/TCP - 123/UDP          "
>>$FILECFG
else
#Si servicio no está; running se valida si está detenido o no existe"

```

```

if grep -i stopped $FILETMP > /dev/null; then
#Si el servicio está detenido registra configuración
echo -e "  $SERVI2 \e[0;31m      STOPPED      \e[0m          "
>>$FILECFG
else
echo "$SERVI2 NO INSTALADO" >> $FILECFGNULL
fi
fi
SERVI1="vsftpd"
SERVI2="FTP      "
service $SERVI1 status > $FILETMP
if grep -i running $FILETMP > /dev/null; then
#Si el servicio está en ejecución registra configuración
echo -e "  $SERVI2 \e[1;32m      RUNNING \e[0m          990/TCP          "
>>$FILECFG
else
#Si servicio no está; running se valida si está detenido o no existe"
if grep -i stopped $FILETMP > /dev/null; then
#Si el servicio está detenido registra configuración
echo -e "  $SERVI2 \e[0;31m      STOPPED      \e[0m          "
>>$FILECFG
else
echo "$SERVI2 NO INSTALADO" >> $FILECFGNULL
fi
fi
#Validamos SAMBA
SERVI1="smb"
SERVI2="SAMBA      "
service $SERVI1 status > $FILETMP
if grep -i running $FILETMP > /dev/null; then
#Si el servicio está en ejecución registra configuración
echo -e "  $SERVI2 \e[1;32m      RUNNING \e[0m          135:139/TCP          "
>>$FILECFG
else
#Si servicio no está; running se valida si está detenido o no existe"
if grep -i stopped $FILETMP > /dev/null; then
#Si el servicio está detenido registra configuración
echo -e "  $SERVI2 \e[0;31m      STOPPED      \e[0m          "
>>$FILECFG
else

```

```

echo "$SERVI2 NO INSTALADO" >> $FILECFGNULL
fi
fi
#Validamos VNC
SERVI1="vncserver"
SERVI2="VNC-SERVER  "
service $SERVI1 status > $FILETMP
if grep -i running $FILETMP> /dev/null; then
#Si el servicio está en ejecución registra configuración
echo -e " $SERVI2 \e[1;32m  RUNNING \e[0m  7609/TCP  "
>>$FILECFG
else
#Si servicio no está; running se valida si está detenido o no existe"
if grep -i stopped $FILETMP> /dev/null; then
#Si el servicio está; detenido registra configuración
echo -e " $SERVI2 \e[0;31m  STOPPED \e[0m  " >>$FILECFG
else
echo "$SERVI2 NO INSTALADO" >> $FILECFGNULL
fi
fi
#Validamos HTTP
SERVI1="httpd"
SERVI2="HTTP  "
service $SERVI1 status > $FILETMP
if grep -i running $FILETMP> /dev/null; then
#Si el servicio está en ejecución registra configuración
PUERTO=`grep "^Listen" /etc/httpd/conf/httpd.conf | awk '{ print $2}`
echo -e " $SERVI2 \e[1;32m  RUNNING \e[0m  $PUERTO/TCP  "
>>$FILECFG
else
#Si servicio no está; running se valida si está detenido o no existe"
if grep -i stopped $FILETMP> /dev/null; then
#Si el servicio está; detenido registra configuración
echo -e " $SERVI2 \e[0;31m  STOPPED \e[0m  "
>>$FILECFG
else
echo "$SERVI2 NO INSTALADO" >> $FILECFGNULL
fi
fi
clear

```

```

#SE MUESTRA ARCHIVO DE SERVICIOS INSTALADOS EN EL SERVIDOR
cat $FILECFG
#SE MUESTRA ARCHIVO DE SERVICIOS NO INSTALADOS EN EL
SERVIDOR
#echo
"=====
#echo "      SERVICIOS NO INSTALADOS EN EL SERVIDOR      "
#echo
"=====
#cat $FILECFGNULL
echo "-----"
#echo " "
echo " "
read -p " * * * Presione una tecla para mostrar todos los servicios..."
rm $FILETMP
clear
#ess .config/services.tmp
echo " " > srvhabilitados.txt
echo -e "          \e[1;31mServicios  Adicionales  Habilitados  en  el
servidor $HOSTNAME\e[o \e[1;37m          \e[o" >> srvhabilitados.txt
echo -e "          \e[1;31mConexiones  Activas  (Establecidas  o
Escuchando)\e[o \e[1;37m \e[o" >> srvhabilitados.txt
echo " " >> srvhabilitados.txt
echo "Protocolo  Recv-Q  Send-Q  DirecciÃ³n Local          Direcci3n externa
Estado  PID/Nombre de programa" >> srvhabilitados.txt
netstat -plan | grep tcp >> srvhabilitados.txt
netstat -plan | grep udp >> srvhabilitados.txt
cat srvhabilitados.txt | more
read -p "Presione una tecla para continuar..."
sh menu.sh

```

Sección # 2

```

#!/bin/bash
#Se arma menú de hardening solo para servicios instalados en el servidor
#Esta funci3n solo se ejecutará siempre y cuando se haya ejecutado la
#opción 1 del menú principal.
#Este menú se basa en el listado del archivo .config/.serviceON.cfg
clear
FILECFG=".config/.serviceON.cfg"

```

```

FILECFGON="serviceON"
OP=1
UNO=1
#SE VALIDA QUE ARCHIVO DE CONFIGURACION EXISTA
if ls -la $FILECFG | grep -i $FILECFGON> /dev/null; then
#SI EXISTE SE ARMA MENU
    echo
    "=====
    ====="
        echo -e "=      \e[1;31mHARDENING A LOS SERVICIOS INSTALADOS
EN SERVIDOR\e[o \e[1;37m      =\e[o"
        echo
    "=====
    ====="
        echo " "
        if grep -i SAMBA $FILECFG> /dev/null; then
            #SI SAMBA ESTA INSTALADO EN EL SERVIDOR SE AGREGA
AL MENU
            echo " B. Hardening a SAMBA"
        fi
        if grep -i FTP $FILECFG> /dev/null; then
            #SI FTP ESTA INSTALADO EN EL SERVIDOR SE AGREGA AL
MENU
            echo " F. Hardening a FTP"
        fi
        if grep -i HTTP $FILECFG> /dev/null; then
            #SI VNC ESTA INSTALADO EN EL SERVIDOR SE AGREGA AL
MENU
            echo " H. Hardening a HTTP"
        fi
        if grep -i POSTFIX $FILECFG> /dev/null; then
            #SI POSTFIX ESTA INSTALADO EN EL SERVIDOR SE AGREGA
AL MENU
            echo " P. Hardening a POSTFIX"
        fi
        if grep -i SQUID $FILECFG> /dev/null; then
            #SI SQUID ESTA INSTALADO EN EL SERVIDOR SE AGREGA AL
MENU
            echo " Q. Hardening a SQUID"
        fi

```

```

        if grep -i SSHD $FILECFG> /dev/null; then
            #SI SSHD ESTA INSTALADO EN EL SERVIDOR SE AGREGA AL
MENU
            echo " S. Hardening a SSH"
        fi
        if grep -i NTPD $FILECFG> /dev/null; then
            #SI NTPD ESTA INSTALADO EN EL SERVIDOR SE AGREGA AL
MENU
            echo " T. Hardening a NTP"
        fi
        if grep -i VNC-SERVER $FILECFG> /dev/null; then
            #SI VNC ESTA INSTALADO EN EL SERVIDOR SE AGREGA AL
MENU
            echo " V. Hardening a VNC-SERVER"
        fi
        echo " "
        echo
        "=====
=====
        echo "          0. Menú Principal"
        echo
        "=====
=====
        echo " "
        read -p "Por favor ingresar opción >> " X
        VALOR=$X
        case $VALOR in
            P)
                read -p "Desea aplicar hardening al servicio Postfix (S/N) >> " y
                if [ "$y" = "S" ]; then
                    sh menu_hard_postfix.sh
                else
                    clear
                    sh seccion2.sh
                fi;;
            S)
                read -p "Desea aplicar hardening al servicio SSH (S/N) >> " y
                if [ "$y" = "S" ]; then
                    sh menu_hard_ssh.sh
                else

```

```
        clear
        sh seccion2.sh
fi;;
T)
read -p "Desea aplicar hardening al servicio NTP (S/N) >> " y
if [ "$y" = "S" ]; then
    sh menu_hard_ntp.sh
else
    clear
    sh seccion2.sh
fi;;
F)
read -p "Desea aplicar hardening al servicio FTP (S/N) >> " y
if [ "$y" = "S" ]; then
    sh menu_hard_ftp.sh
else
    clear
    sh seccion2.sh
fi;;
Q)
read -p "Desea aplicar hardening al servicio SQUID (S/N) >> " y
if [ "$y" = "S" ]; then
    sh menu_hard_squid.sh
else
    clear
    sh seccion2.sh
fi;;
B)
read -p "Desea aplicar hardening al servicio SAMBA (S/N) >> " y
if [ "$y" = "S" ]; then
    sh menu_hard_samba.sh
else
    clear
    sh seccion2.sh
fi;;
V)
read -p "Desea aplicar hardening al servicio VNC (S/N) >>" y
if [ "$y" = "S" ]; then
    sh menu_hard_vnc.sh
else
```

```

        clear
        sh seccion2.sh
    fi;;
H)
read -p "Desea aplicar hardening al servicio HTTP (S/N) >>" y
if [ "$y" = "S" ]; then
    sh menu_hard_http.sh
else
    clear
    sh seccion2.sh
fi;;
0)
    sh menu.sh;;
*)
    echo -e "\e[1;31m          ***** ENTRADA NO VÁLIDA *****\e[0
\e[1;37m"
    read -p " "
        sh seccion2.sh;;
esac
else
    clear
    echo
"=====
=====
    echo -e "\e[1;31m!!! ERROR - POR FAVOR PRIMERO EJECUTE
OPCION 1 DEL MENU PRINCIPAL\e[0 \e[1;37m =\e[0"
    echo
"=====
=====
    read -p "PRESIONE UNA TECLA PARA CONTINUAR..."
    sh menu.sh
fi

```

Sección # 3

```

#!/bin/bash
#Se arma menú de auditoria solo para servicios instalados en el servidor
#Esta función solo se ejecutará siempre y cuando se haya ejecutado la
#opción 1 del menú principal.
#Este menú se basa en el listado del archivo .config/.serviceON.cfg

```



```

clear
FILECFG=".config/.serviceON.cfg"
FILECFGON="serviceON"
OP=1
UNO=1
#SE VALIDA QUE ARCHIVO DE CONFIGURACION EXISTA
if ls -la $FILECFG | grep -i $FILECFGON> /dev/null; then
#SI EXISTE SE ARMA MENU
    echo
    "=====
    ====="
    echo -e "=          \e[1;31mAUDITORIA A LOS SERVICIOS INSTALADOS
EN SERVIDOR\e[o \e[1;37m          =\e[o"
    echo
    "=====
    ====="
    echo " "
    if grep -i SAMBA $FILECFG> /dev/null; then
        #SI SAMBA ESTA INSTALADO EN EL SERVIDOR SE AGREGA
AL MENU
        echo " B. Auditoria a SAMBA"
        let OP=$OP+$UNO
    fi
    if grep -i FTP $FILECFG> /dev/null; then
        #SI FTP ESTA INSTALADO EN EL SERVIDOR SE AGREGA AL
MENU
        echo " F. Auditoria a FTP"
        let OP=$OP+$UNO
    fi
    if grep -i HTTP $FILECFG> /dev/null; then
        #SI HTTPD ESTA INSTALADO EN EL SERVIDOR SE AGREGA AL
MENU
        echo " H. Auditoria a HTTP"
        let OP=$OP+$UNO
    fi
    if grep -i POSTFIX $FILECFG> /dev/null; then
        #SI POSTFIX ESTA INSTALADO EN EL SERVIDOR SE AGREGA
AL MENU
        echo " P. Auditoria a POSTFIX"
        let OP=$OP+$UNO

```

```

fi
if grep -i SQUID $FILECFG> /dev/null; then
    #SI SQUID ESTA INSTALADO EN EL SERVIDOR SE AGREGA AL
MENU
    echo " Q. Auditoria a SQUID"
    let OP=$OP+$UNO
fi
if grep -i SSHD $FILECFG> /dev/null; then
    #SI SSHD ESTA INSTALADO EN EL SERVIDOR SE AGREGA AL
MENU
    echo " S. Auditoria a SSH"
    let OP=$OP+$UNO
fi
if grep -i NTPD $FILECFG> /dev/null; then
    #SI NTPD ESTA INSTALADO EN EL SERVIDOR SE AGREGA AL
MENU
    echo " T. Auditoria a NTP"
    let OP=$OP+$UNO
fi
if grep -i VNC-SERVER $FILECFG> /dev/null; then
    #SI VNC ESTA INSTALADO EN EL SERVIDOR SE AGREGA AL
MENU
    echo " V. Auditoria a VNC-SERVER"
    let OP=$OP+$UNO
fi
echo " "
echo
"=====
=====
echo "          0. Menú Principal "
echo
"=====
=====
echo " "
read -p "Por favor ingresar opción >> " X
VALOR=$X
case $VALOR in
    P)
        read -p "Desea aplicar auditoria al servicio Postfix (S/N) >> " y
        if [ "$y" = "S" ]; then

```

```
        sh Auditoria_postfix.sh
    else
        clear
        sh seccion3.sh
    fi;;
S)
read -p "Desea aplicar auditoria al servicio SSH (S/N) >> " y
if [ "$y" = "S" ]; then
    sh Auditoria_ssh.sh
else
    clear
    sh seccion3.sh
fi;;
T)
read -p "Desea aplicar auditoria al servicio NTP (S/N) >> " y
if [ "$y" = "S" ]; then
    sh Auditoria_ntp.sh
else
    clear
    sh seccion3.sh
fi;;
F)
read -p "Desea aplicar auditoria al servicio FTP (S/N) >> " y
if [ "$y" = "S" ]; then
    sh seccion3.sh
else
    clear
    sh seccion3.sh
fi;;
Q)
read -p "Desea aplicar auditoria al servicio SQUID (S/N) >> " y
if [ "$y" = "S" ]; then
    sh Auditoria_squid_2.sh
else
    clear
    sh seccion3.sh
fi;;
B)
read -p "Desea aplicar auditoria al servicio SAMBA (S/N) >> " y
if [ "$y" = "S" ]; then
```

```

        sh Auditoria_samba.sh
    else
        clear
        sh seccion3.sh
    fi;;
V)
read -p "Desea aplicar auditoria al servicio VNC (S/N) >>" y
if [ "$y" = "S" ]; then
    sh seccion3.sh
else
    clear
    sh seccion3.sh
fi;;
H)
read -p "Desea aplicar auditoria al servicio HTTP (S/N) >>" y
if [ "$y" = "S" ]; then
    sh menu_auditoria_http.sh
else
    clear
    sh seccion3.sh
fi;;
0)
    sh menu.sh;;
*)
    echo -e "\e[1;31m          ***** ENTRADA NO VÁLIDA *****\e[o
\e[1;37m"
    read -p " "
        sh seccion3.sh;;
esac
else
    clear
    echo
    "=====
    ====="
    echo -e "\e[1;31m!!! ERROR - POR FAVOR PRIMERO EJECUTE
OPCION 1 DEL MENU PRINCIPAL\e[o \e[1;37m =\e[o"
    echo
    "=====
    ====="
    read -p "PRESIONE UNA TECLA PARA CONTINUAR..."

```

```
sh menu.sh
fi
```

Sección # 4

```
#!/bin/bash

#Menú para reportes - sección 4 del menú principal
# Se invoca con un número entero según opciones del menú
clear
echo
"=====
=====
echo -e "          \e[1;31mReportes\e[o \e[1;37m          =\e[o"
echo
"=====
=====
echo "
echo " 1. Hardening aplicado en sesión actual
echo " 2. Hardening no aplicado en sesión actual
echo " 3. Histórico de servicios que cumplen hardening
echo " 4. Histórico de servicios que no cumplen hardening
echo " 5. Auditoria a los servicios instalados
echo " "
echo
"=====
=====
echo "          0. REGRESAR A MENU PRINCIPAL
echo
"=====
=====
read -p "Por favor ingresar opción >> " X
echo
"=====
=====
VALOR=$X
case $VALOR in
    1)
        read -p "Desea mostrar reporte de hardening aplicado en sesión actual
(S/N) >> " y
```

```

if [ "$y" = "S" ]; then
    sh reporte_1.sh
else
    clear
    sh seccion4.sh
fi;;
2)
read -p "Desea mostrar reporte del hardening no aplicado en sesión
actual (S/N) >> " y
if [ "$y" = "S" ]; then
    sh reporte_2.sh
else
    clear
    sh seccion4.sh
fi;;
3)
read -p "Desea mostrar reporte histórico de servicios que cumplen
hardening? (S/N) >> " y
if [ "$y" = "S" ]; then
    sh reporte_1b.sh
else
    clear
    sh seccion4.sh
fi;;
4)
read -p "Desea mostrar reporte histórico de servicios que no cumplen
hardening? (S/N) >> " y
if [ "$y" = "S" ]; then
    sh reporte_2b.sh
else
    clear
    sh seccion4.sh
fi;;
5)
read -p "Desea mostrar reportes auditoria? (S/N) >> " y
if [ "$y" = "S" ]; then
    sh seccion3.sh
else
    clear
    sh seccion4.sh

```

```

    fi;;
    0)
    clear
    sh menu.sh;;
    *)
    echo -e "\e[1;31m    ***** ENTRADA NO VÁLIDA *****\e[o \e[1;37m"
    read -p " "
    sh seccion4.sh;;
esac
#fin del menú de reportes

```

Sección #4b

```

#!/bin/bash

#Menú para reportes - sección 4 del menú principal
# Se invoca con un número entero según opciones del menú
clear
echo
"=====
=====
echo -e "=          \e[1;31mReportes de backup\e[o \e[1;37m          =\e[o"
echo
"=====
=====
echo "
echo " 1. Servicios que cumplen con hardening "
echo " 2. Servicios que no cumplen con hardening "
echo " "
echo
"=====
=====
echo "          0. REGRESAR A MENU PRINCIPAL          "
echo
"=====
=====
read -p "Por favor ingresar opción >> " X
echo
"=====
=====

```

```

VALOR=$X
case $VALOR in
    1)
        read -p "Desea mostrar reporte de los servicios que cumplen PCI? (S/N)
>> " y
        if [ "$y" = "S" ]; then
            sh reporte_1b.sh
        else
            clear
            sh seccion4b.sh
        fi;;
    2)
        read -p "Desea mostrar reporte de los servicios que no cumplen PCI (S/N)
>> " y
        if [ "$y" = "S" ]; then
            sh reporte_2b.sh
        else
            clear
            sh seccion4b.sh
        fi;;
    0)
        clear
        sh menu.sh;;
    *)
        echo -e "\e[1;31m      ***** ENTRADA NO VÃ• LIDA *****\e[o \e[1;37m"
        read -p " "
        sh seccion4b.sh;;
esac
#fin del men reportes

```

Men Hardening SSH

```

#!/bin/bash

#menu6.sh Men para la categora 6 de Sistemas, accesos, autenticaciones.
# Se invoca con un nmero entero segn opciones del men
BAN="wam0"
WHI=".config/.historico.cfg"

```



```

WVA="WSSH"
touch $WHI
clear
echo
"=====
=====
echo -e "=
                                \e[1;31mHardening al servicio SSH\e[o \e[1;37m
=\e[o"
echo
"=====
=====
echo "
                                "
if grep "$WVA"1 $WHI> /dev/null; then
echo -e "\e[1;36m 1. Desactivar el usuario Root para que no pueda realizar
conexión remota \e[0m "
else
echo -e "\e[1;37m 1. Desactivar el usuario Root para que no pueda realizar
conexión remota \e[0m "
fi
if grep "$WVA"2 $WHI> /dev/null; then
echo -e "\e[1;36m 2. Configurar intervalo de espera para conexión usuario
\e[0m "
else
echo -e "\e[1;37m 2. Configurar intervalo de espera para conexión usuario
\e[0m "
fi
if grep "$WVA"3 $WHI> /dev/null; then
echo -e "\e[1;36m 3. Establecer permisos a usuarios en archivos de
configuración \e[0m "
else
echo -e "\e[1;37m 3. Establecer permisos a usuarios en archivos de
configuración \e[0m "
fi
if grep "$WVA"4 $WHI> /dev/null; then
echo -e "\e[1;36m 4. Número máximo de intentos fallidos de login
\e[0m "
else
echo -e "\e[1;37m 4. Número máximo de intentos fallidos de login
\e[0m "
fi

```

```

if grep "$WVA"5 $WHI> /dev/null; then
echo -e "\e[1;36m 5. Configuraci3n de usuarios para acceso a SSH \e[0m "
else
echo -e "\e[1;37m 5. Configuraci3n de usuarios para acceso a SSH \e[0m "
fi
if grep "$WVA"6 $WHI> /dev/null; then
echo -e "\e[1;36m 6. Personalizar banner de bienvenida \e[0m "
else
echo -e "\e[1;37m 6. Personalizar banner de bienvenida \e[0m "
fi
if grep "$WVA"7 $WHI> /dev/null; then
echo -e "\e[1;36m 7. Configurar tiempo de sesiones inactivas \e[0m "
else
echo -e "\e[1;37m 7. Configurar tiempo de sesiones inactivas \e[0m "
fi
if grep "$WVA"8 $WHI> /dev/null; then
echo -e "\e[1;36m 8. Configuraci3n de puerto de conexi3n \e[0m "
else
echo -e "\e[1;37m 8. Configuraci3n de puerto de conexi3n \e[0m "
fi
echo -e "\e[1;37m 9. Reversa de hardening SSH \e[0m "
echo " "
echo
"=====
=====
echo " 0. REGRESAR A MENU PRINCIPAL "
echo
"=====
=====
read -p "Por favor ingresar opci3n >> " X
echo
"=====
=====
VALOR=$X
case $VALOR in
1)
if grep "$WVA"1 $WHI> /dev/null; then
echo -e "\e[0;31m \e[o"
read -p "***** OPCION DE HARDENING YA APLICADA *****"

```

```

        echo -e "\e[0;37m \e[o"
    fi
        read -p "Desea desactivar el usuario Root para que no pueda
realizar conexiÃ³n remota? (S/N) >> " y
        if [ "$y" = "S" ]; then
            sh hard_ssh_1.sh
        else
            clear
            echo "$BAN" > logs/hardening_ssh_1.log
            sh menu_hard_ssh.sh
        fi;;
    2)
if grep "$WVA"2 $WHI> /dev/null; then
    echo -e "\e[0;31m \e[o"
    read -p "***** OPCION DE HARDENING YA APLICADA *****"
    echo -e "\e[0;37m \e[o"
fi
" y
        read -p "Desea configurar intervalo de espera para login? (S/N) >>

        if [ "$y" = "S" ]; then
            sh hard_ssh_2.sh
        else
            clear
            echo "$BAN" > logs/hardening_ssh_2.log
            sh menu_hard_ssh.sh
        fi;;
    3)
if grep "$WVA"3 $WHI> /dev/null; then
    echo -e "\e[0;31m \e[o"
    read -p "***** OPCION DE HARDENING YA APLICADA *****"
    echo -e "\e[0;37m \e[o"
fi
        read -p "Desea asignar permisos a archivos de configuraciÃ³n
(S/N) >> " y
        if [ "$y" = "S" ]; then
            sh hard_ssh_3.sh
        else
            clear
            echo "$BAN" > logs/hardening_ssh_3.log
            sh menu_hard_ssh.sh

```

```

fi;;
4)
if grep "$WVA"4 $WHI> /dev/null; then
    echo -e "\e[0;31m \e[o"
    read -p "***** OPCION DE HARDENING YA APLICADA *****"
    echo -e "\e[0;37m \e[o"
fi
    read -p "Desea configurar el no. máximo de intentos fallidos de
login? (S/N) >> " y
    if [ "$y" = "S" ]; then
        sh hard_ssh_4.sh
    else
        clear
        echo "$BAN" > logs/hardening_ssh_5.log
        sh menu_hard_ssh.sh
fi;;
5)
if grep "$WVA"5 $WHI> /dev/null; then
    echo -e "\e[0;31m \e[o"
    read -p "***** OPCION DE HARDENING YA APLICADA *****"
    echo -e "\e[0;37m \e[o"
fi
    read -p "Desea configurar usuarios o grupos para acceso a SSH
(S/N) >> " y
    if [ "$y" = "S" ]; then
        sh hard_ssh_5.sh
    else
        clear
        echo "$BAN" > logs/hardening_ssh_6.Log
        sh menu_hard_ssh.sh
fi;;
6)
if grep "$WVA"6 $WHI> /dev/null; then
    echo -e "\e[0;31m \e[o"
    read -p "***** OPCION DE HARDENING YA APLICADA *****"
    echo -e "\e[0;37m \e[o"
fi
    read -p "Desea configurar banner de bienvenida? (S/N) >> " y
    if [ "$y" = "S" ]; then
        sh hard_ssh_6.sh

```

```

else
    clear
    echo "$BAN" > logs/hardening_ssh_7.log
    sh menu_hard_ssh.sh
fi;;
7)
if grep "$WVA"7 $WHI> /dev/null; then
    echo -e "\e[0;31m \e[o"
    read -p "***** OPCION DE HARDENING YA APLICADA *****"
    echo -e "\e[0;37m \e[o"
fi
    read -p "Desea configurar tiempo de espera de inactividad de
sesiÃ³n (S/N) >> " y
    if [ "$y" = "S" ]; then
        sh hard_ssh_7.sh
    else
        clear
        echo "$BAN" > logs/hardening_ssh_8.log
        sh menu_hard_ssh.sh
fi;;
8)
if grep "$WVA"8 $WHI> /dev/null; then
    echo -e "\e[0;31m \e[o"
    read -p "***** OPCION DE HARDENING YA APLICADA *****"
    echo -e "\e[0;37m \e[o"
fi
    read -p "Desea cambiar el puerto por default de ssh? (S/N) >> " y
    if [ "$y" = "S" ]; then
        sh hard_ssh_8.sh
    else
        clear
        echo "$BAN" > logs/hardening_ssh_9.log
        sh_menu_hard_ssh.sh
fi;;
9)
read -p "Desea reversar hardening de SSH? (S/N) >>" y
if [ "$y" = "S" ]; then
    sh restore_ssh.sh
else
    clear

```

```

        echo "$BAN" > logs/hardening_http_3.log
        sh menu_hard_ssh.sh
    fi;;
    0)
    clear
    sh seccion2.sh;;
    *)
    echo -e "\e[1;31m    ***** ENTRADA NO VÁLIDA *****\e[0 \e[1;37m"
    read -p " "
    sh menu_hard_ssh.sh;;
esac
#fin del menú ssh

```

Opción 1 Menú SSH

```

#!/bin/bash
ARCHIVO="logs/hardening_ssh_1.log"
WHI=".config/historico.cfg"
WVA="WSSH1"
echo "$WVA" >> $WHI
echo
"=====
=== " > $ARCHIVO
echo "Log de Hardening SSH Opción 1: Deshabilitar usuario Root en SSH" >>
$ARCHIVO
echo
"=====
=== " >> $ARCHIVO
#SE ELIMINA VALOR ANTERIOR
echo "Parámetros antes del Hardening" >> $ARCHIVO
echo
"=====
=== " >> $ARCHIVO
grep "PermitRootLogin" /etc/ssh/sshd_config >> $ARCHIVO
echo
"=====
=== " >> $ARCHIVO
sed -i '/"PermitRootLogin"/d' /etc/ssh/sshd_config
#SE ADICIONA VALORES
echo "PermitRootLogin no" >> /etc/ssh/sshd_config

```

```

#SE SACA LOG CON LOS CAMBIOS
echo "Parámetro después del Hardening" >> $ARCHIVO
echo
"=====
==" >> $ARCHIVO
grep "PermitRootLogin" /etc/ssh/sshd_config >> $ARCHIVO
echo
"=====
==" >> $ARCHIVO
service sshd reload
clear
cat $ARCHIVO | more
echo -e "\e[1;31m \e[o"
read -p "Presione una tecla para continuar..."
echo -e "\e[1;37m \e[o"
sh menu_hard_ssh.sh

```

Opción # 2

```

#!/bin/bash
ARCHIVO="logs/hardening_ssh_2.log"
WHI=".config/.historico.cfg"
WVA="WSSH2"
echo "$WVA" >> $WHI
clear
echo
"=====
======"
echo " Se establece el número de mensajes solicitando una respuesta que se"
echo " enviarán sin ninguna contestación por parte del cliente."
echo
"=====
======"
echo " "
read -p "Ingrese el número máximo de mensajes: >>" b
echo
"=====
======" > $ARCHIVO
echo "Log hardening SSH Opcion2: Número máximo de mensajes" >>
$ARCHIVO

```

```

echo
"=====
===== " >> $ARCHIVO
#SE SACA LOG CON LOS VALORES ACTUALES
echo "VALORES ANTES DEL HARDENING" >> $ARCHIVO
echo
"=====
===== " >> $ARCHIVO
grep "^ClientAliveCountMax" /etc/ssh/sshd_config >> $ARCHIVO
echo
"=====
===== " >> $ARCHIVO
#SE ELIMINA VALOR ANTERIOR
sed -i '/'"ClientAliveCountMax"/d' /etc/ssh/sshd_config
#SE ADICIONAN VALORES
echo "ClientAliveCountMax $b" >> /etc/ssh/sshd_config
#SE SACA LOG CON LOS CAMBIOS
echo "VALORES DESPUES DE HARDENING" >> $ARCHIVO
echo
"=====
===== " >> $ARCHIVO
grep "^ClientAliveCountMax" /etc/ssh/sshd_config >> $ARCHIVO
echo
"=====
===== " >> $ARCHIVO
clear
service sshd reload
cat $ARCHIVO | more
echo -e "\e[1;31m \e[o"
read -p "Presione una tecla para continuar..."
echo -e "\e[1;37m \e[o"
sh menu_hard_ssh.sh

```

Opción # 3

```

#!/bin/bash
ARCHIVO="logs/hardening_ssh_3.log"
WHI=".config/.historico.cfg"
WVA="WSSH3"

```



```

echo "$WVA" >> $WHI
#Primero generamos log
echo
"=====
===== " > $ARCHIVO
echo "Log Hardening SHH Opción 3: Establece permisos en el Archivo de
ConfiguraciÃ³n" >> $ARCHIVO
echo
"=====
===== " >> $ARCHIVO
if ls -l /etc/ssh/sshd_config | grep "root root"> /dev/null; then
    echo "El archivo tiene asignado grupo y propietario correcto" >>
$ARCHIVO
    ls -l /etc/ssh/sshd_config >> $ARCHIVO
else
    echo "archivo antes de cambiar propietario y grupo" >> $ARCHIVO
    ls -l /etc/ssh/sshd_config >> $ARCHIVO
    /bin/chown root:root /etc/ssh/sshd_config >> $ARCHIVO
    echo "Archivo después de cambiar propietario y grupo" >> $ARCHIVO
    ls -l /etc/ssh/sshd_config >> $ARCHIVO
fi
if ls -l /etc/ssh/sshd_config | grep "rw-----"> /dev/null; then
    echo "El archivo tiene el permiso correcto 600" >> $ARCHIVO
    ls -l /etc/ssh/sshd_config >> $ARCHIVO
else
    echo "Archivo antes de cambiar permisos a 600" >> $ARCHIVO
    ls -l /etc/ssh/sshd_config >> $ARCHIVO
    /bin/chmod 600 /etc/ssh/sshd_config >> $ARCHIVO
    echo "Archivo después de cambiar permisos a 600" >> $ARCHIVO
    ls -l /etc/ssh/sshd_config >> $ARCHIVO
fi
echo
"=====
===== " >> $ARCHIVO
service sshd reload
clear
cat $ARCHIVO | more
echo -e "\e[1;31m \e[o"
read -p "Presione una tecla para continuar..."
echo -e "\e[1;37m \e[o"

```

```
sh menu_hard_ssh.sh
```

Opción # 4

```
#!/bin/bash
ARCHIVO="logs/hardening_ssh_4.log"
FICFG="/etc/ssh/sshd_config"
WHI=".config/.historico.cfg"
WVA="WSSH4"
echo "$WVA" >> $WHI
echo
"=====
==" > $ARCHIVO
echo "Log hardening SSH OP 4: No. Max. de Intentos fallidos de login" >>
$ARCHIVO
echo
"=====
==" >> $ARCHIVO
echo "VALOR ANTES DEL HARDENING" >> $ARCHIVO
echo
"=====
=" >> $ARCHIVO
grep "MaxAuthTries" $FICFG >> $ARCHIVO
echo
"=====
=" >> $ARCHIVO
#SE ELIMINA VALOR ANTERIOR
sed -i '/'"MaxAuthTries"/d' $FICFG
#SE ADICIONA VALORES
clear
echo
"=====
=====
"
echo "Hardening SSH OP 4: Número máximo de Intento fallidos de login  "
echo
"=====
=====
"
echo "Este parámetro indica la cantidad de veces que podemos equivocarnos"
echo "en ingresar el usuario y/o contraseña. Luego de que se cumpla el no."
```

```

echo "mximo de intentos se cierra la conexin ssh y evitaremos ataques"
echo "basados en la persistencia de la conexin."
echo
"=====
=====
echo " "
read -p "Ingrese valor mximo de intentos fallidos --->" M
echo MaxAuthTries $M >> $FICFG
#SE SACA LOG CON LOS CAMBIOS
echo "VALORES DESPUES DEL HARDENING" >> $ARCHIVO
echo
"=====
=" >> $ARCHIVO
grep "MaxAuthTries" $FICFG >> $ARCHIVO
echo
"=====
=== " >> $ARCHIVO
service sshd reload
clear
cat $ARCHIVO | more
echo -e "\e[1;31m \e[o"
read -p "Presione una tecla para continuar..."
echo -e "\e[1;37m \e[o"
sh menu_hard_ssh.sh

```

Opcin # 5

```

#!/bin/bash
ARCHIVO="logs/hardening_ssh_5.log"
FITMP=".config/usr.temp"
FICFG="/etc/ssh/sshd_config"
P1="AllowUsers"
P2="AllowGroups"
P3="DenyUsers"
P4="DenyGroups"
WHI=".config/.historico.cfg"
WVA="WSSH5"
echo "$WVA" >> $WHI
#Primero generamos log

```

```

echo
"=====
===== " > $ARCHIVO
echo "Log hardening OP 5: Limitar acceso vía SSH" >> $ARCHIVO
echo
"=====
===== " >> $ARCHIVO
#SE SACA ENVIDENCIA ANTES DEL HARDENING
echo "VALORES ANTES DEL HARDENING" >> $ARCHIVO
grep $P1 $FICFG >> $ARCHIVO
grep $P2 $FICFG >> $ARCHIVO
grep $P3 $FICFG >> $ARCHIVO
grep $P4 $FICFG >> $ARCHIVO
echo
"=====
===== " >> $ARCHIVO
clear
echo
"=====
===== "
echo "Agregar lista de usuarios/grupos que pueden hacer login en el servidor "
echo "por medio del servicio SSH, también se especificaráj los usuarios/grupos
"
echo "que no pueden ingresar. Ingrese cada usuario o grupo en el formato:  "
echo " usuario1, usuario2 o grupo1, grupo2                                "
echo
"=====
===== "
echo "LISTADO DE USUARIOS CONFIGURADOS EN EL SERVIDOR"
echo
"=====
===== "
#grep ":/home" /etc/passwd > $FITMP
#cat $FITMP
awk '$3 >499 {print $1}' FS=":" /etc/passwd | sort
echo
"=====
===== "
echo "LISTADO DE GRUPOS CONFIGURADOS EN EL SERVIDOR"
echo

```

```

"=====
=====
awk '$3 >499 {print $1}' FS=":" /etc/group | sort
echo
"=====
=====
read -p "Usuarios Permitidos: >> " UPERM
read -p "Grupos Permitidos: >> " GPERM
read -p "Usuarios Denegados: >> " UDENE
read -p "Grupos Denegados: >> " GDENE
if ["$UPERM" = ""]> /dev/null; then
    echo "No se ingresÃ³ listado de usuarios permitidos" >> $ARCHIVO
else
    sed -i /"$P1"/d' $FICFG
    echo "$P1 $UPERM" >> $FICFG
fi
if ["$GPERM" = ""]> /dev/null; then
    echo "No se ingresÃ³ listado de grupos permitidos" >> $ARCHIVO
else
    sed -i /"$P2"/d' $FICFG
    echo "$P2 $GPERM" >> $FICFG
fi
if ["$UDENE" = ""]> /dev/null; then
    echo "No se ingresó listado de usuarios no permitidos" >> $ARCHIVO
else
    sed -i /"$P3"/d' $FICFG
    echo "$P3 $UDENE" >> $FICFG
fi
if ["$GDENE" = ""]> /dev/null; then
    echo "No se ingresó listado de grupos no permitidos" >> $ARCHIVO
else
    sed -i /"$P4"/d' $FICFG
    echo "$P4 $GDENE" >> $FICFG
fi
echo
"=====
===== >> $ARCHIVO
#SE SACA ENVIDENCIA ANTES DEL HARDENING
echo "VALORES DESPUES DEL HARDENING" >> $ARCHIVO
grep $P1 $FICFG >> $ARCHIVO

```

```

grep $P2 $FICFG >> $ARCHIVO
grep $P3 $FICFG >> $ARCHIVO
grep $P4 $FICFG >> $ARCHIVO
echo
"=====
===== " >> $ARCHIVO
service sshd reload
clear
cat $ARCHIVO | more
echo -e "\e[1;31m \e[o"
read -p "Presione una tecla para continuar..."
echo -e "\e[1;37m \e[o"
sh menu_hard_ssh.sh

```

Opción # 6

```

#!/bin/bash
ARCHIVO="logs/hardening_ssh_6.log"
FICFG="/etc/ssh/sshd_config"
FIBAN="/etc/ssh/banner_hard.txt"
P1="Banner"
WHI=".config/.historico.cfg"
WVA="WSSH6"
echo "$WVA" >> $WHI
echo
"=====
===== " > $ARCHIVO
echo "Log hardening OP6: Configure Banner de bienvenida" >> $ARCHIVO
echo
"=====
===== " >> $ARCHIVO
#SE SACA EVIDENCIA ANTES DEL HARDENING
echo "VALOR ANTES DEL HARDENING" >> $ARCHIVO
grep $P1 $FICFG >> $ARCHIVO
echo
"=====
===== " >> $ARCHIVO
#SE ELIMINA VALOR ANTERIOR
sed -i '/'"Banner"/d' $FICFG

```

```

#SE ADICIONA VALORES
clear
echo
"=====
====="
echo "Por favor ingrese texto para configuraci3n de banner de bienvenida: "
echo
"=====
====="
echo " "
read -p "Texto para banner --->" B
echo "Banner /etc/ssh/banner_hard.txt" >> $FICFG
#SE CREA ARCHIVO BANNER
echo "*****" > $FIBAN
echo $B >> $FIBAN
echo "*****" >> $FIBAN
#SE SACA EVIDENCIA DESPUES DE HARDENING
grep "^Banner" $FICFG >> $ARCHIVO
cat $FIBAN >> $ARCHIVO
echo
"=====
=====" >> $ARCHIVO
service sshd reload
clear
cat $ARCHIVO | more
echo -e "\e[1;31m \e[o"
read -p "Presione una tecla para continuar..."
echo -e "\e[1;37m \e[o"
sh menu_hard_ssh.sh

```

Opción # 7

```

#!/bin/bash
ARCHIVO="logs/hardening_ssh_7.log"
WHI=".config/historico.cfg"
WVA="WSSH7"
echo "$WVA" >> $WHI
clear

```

```

echo
"=====
=====
echo " Se configura la opción ClientAliveInterval "
echo " Al configurar esta opción se establecerá un intervalo de tiempo "
echo " de espera en SEGUNDOS después del cual, si no hay datos recibidos "
echo " por parte del cliente SSH enviará un mensaje cifrado. En caso de "
echo " no recibir respuesta el usuario se desconectará. "
echo " Se recomienda valores mayores a 0"
echo
"=====
=====
read -p "Ingrese valor del Intervalo de tiempo en Segundos: >>" a
echo
"=====
===== > $ARCHIVO
echo " LOG HARDENING SSH_7: Tiempo de espera de sesiones sin actividad"
>> $ARCHIVO
echo
"=====
===== >> $ARCHIVO
#SE SACA LOG CON LOS VALORES ACTUALES
echo
"=====
=== >> $ARCHIVO
echo "VALORES ANTES DEL HARDENING" >> $ARCHIVO
echo
"=====
=== >> $ARCHIVO
grep "^ClientAliveInterval" /etc/ssh/sshd_config >> $ARCHIVO
echo
"=====
=== >> $ARCHIVO
#SE ELIMINA VALOR ANTERIOR
sed -i '/"ClientAliveInterval"/d' /etc/ssh/sshd_config
#SE ADICIONAN VALORES
echo "ClientAliveInterval $a" >> /etc/ssh/sshd_config
#SE SACA LOG CON LOS CAMBIOS
echo "VALORES DESPUES DE HARDENING" >> $ARCHIVO
echo

```



```

=====
=== >> $ARCHIVO
grep "^ClientAliveInterval" /etc/ssh/sshd_config >> $ARCHIVO
echo
=====
=== >> $ARCHIVO
service sshd reload
clear
cat $ARCHIVO | more
echo -e "\e[1;31m \e[o"
read -p "Presione una tecla para continuar..."
echo -e "\e[1;37m \e[o"
sh menu_hard_ssh.sh

```

Opción # 8

```

#!/bin/bash
ARCHIVO="logs/hardening_ssh_8.log"
WHI=".config/.historico.cfg"
WVA="WSSH8"
echo "$WVA" >> $WHI
clear
echo
=====
=====
echo " Se configura un nuevo puerto de conexión y se reinicia el servicio "
echo " El puerto standar de SSH es 22. Usted debe de ingresar      "
echo " un puerto diferente.                                     "
echo
=====
=====
read -p "Ingrese valor del nuevo puerto: >>" a
echo
=====
===== > $ARCHIVO
echo " LOG HARDENING SSH_8: Configuración de puerto de conexión" >>
$ARCHIVO
echo

```

```

"=====
===== " >> $ARCHIVO
#SE SACA LOG CON LOS VALORES ACTUALES
echo
"=====
=== " >> $ARCHIVO
echo "VALORES ANTES DEL HARDENING" >> $ARCHIVO
echo
"=====
=== " >> $ARCHIVO
grep "^Port" /etc/ssh/sshd_config >> $ARCHIVO
echo
"=====
=== " >> $ARCHIVO
#SE ELIMINA VALOR ANTERIOR
sed -i '/'"Port"/d' /etc/ssh/sshd_config
#SE ADICIONAN VALORES
echo "Port $a" >> /etc/ssh/sshd_config
echo "ssh $a/stcp          #SSH nuevo puerto cambiado por hardening" >>
/etc/services
service sshd restart
#SE SACA LOG CON LOS CAMBIOS
echo "VALORES DESPUES DE HARDENING" >> $ARCHIVO
echo
"=====
=== " >> $ARCHIVO
grep "^Port" /etc/ssh/sshd_config >> $ARCHIVO
echo
"=====
=== " >> $ARCHIVO
service sshd reload
clear
cat $ARCHIVO | more
echo -e "\e[1;31m \e[o"
read -p "Presione una tecla para continuar..."
echo -e "\e[1;37m \e[o"
sh menu_hard_ssh.sh

```

Restore de SSH


```
echo "|-----Auditoria de SSH-----|" >> ssh_auditoria.txt
echo "||||||||||||||||||||||||||||||||||||||||" >> ssh_auditoria.txt
echo "-----Conexiones entrantes aceptadas-----" >> ssh_auditoria.txt
echo "-----" >> ssh_auditoria.txt
cat log_Accepted.txt >> ssh_auditoria.txt
echo "-----" >> ssh_auditoria.txt
echo "-----Conexiones rechazadas o fallidas-----" >> ssh_auditoria.txt
echo "-----" >> ssh_auditoria.txt
cat log_failed.txt >> ssh_auditoria.txt
clear
cat ssh_auditoria.txt
echo -e "\e[1;31m \e[o"
read -p "Presione una tecla para continuar..."
echo -e "\e[1;37m \e[o"
sh seccion3.sh
```

ANEXO 2.- Pruebas del aplicativo

Pruebas de SSH

Los cambios aplicados fueron los siguientes donde se comprueba que el hardening funcionó correctamente y se han resuelto vulnerabilidades:

- Configuración de puerto de conexión de SSH (figura Anexo 2- Prueba de Aplicativo 1). En la siguiente imagen se muestra el ingreso con el cambio de puerto a uno seguro.

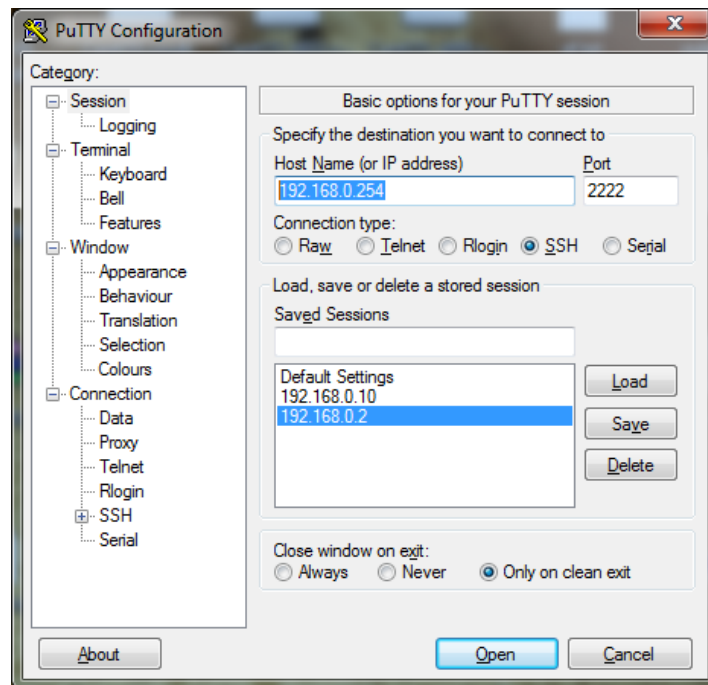



Figura ANEXO 2-Prueba de Aplicativo. 1 Ingreso por SSH con puerto asignado

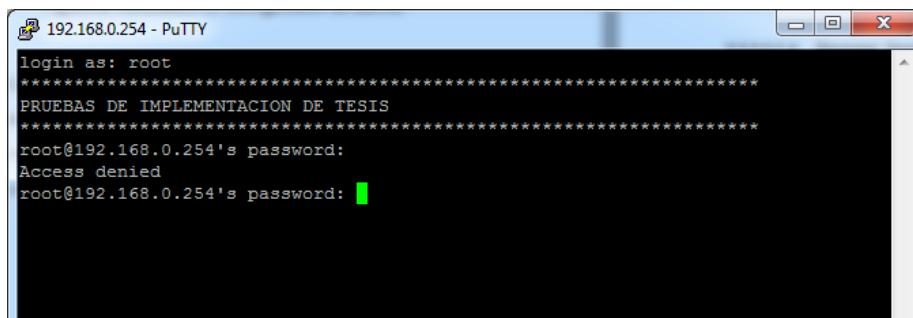
- Personalización de Banner de Bienvenida (Figura ANEXO 2-Prueba de Aplicativo. 2). Se puede observar el texto ingresado el cual se muestra al ingresar al servidor.



```
192.168.0.254 - PuTTY
login as: root
*****
PRUEBAS DE IMPLEMENTACION DE TESIS
*****
root@192.168.0.254's password: █
```

Figura ANEXO 2-Prueba de Aplicativo. 2 Banner de Bienvenida asignado

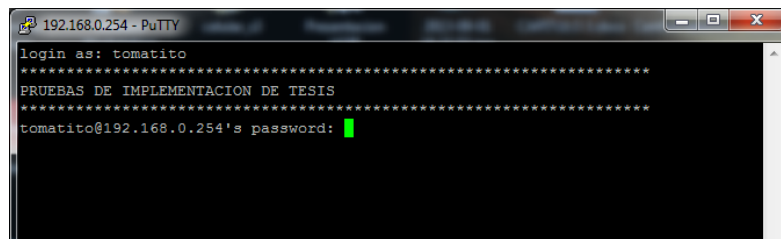
- Desactivar usuario Root (Figura ANEXO 2-Prueba de Aplicativo.3). El usuario Root por normas PCI debe ser deshabilitado lo cual se puede comprobar en la imagen siguiente:



```
192.168.0.254 - PuTTY
login as: root
*****
PRUEBAS DE IMPLEMENTACION DE TESIS
*****
root@192.168.0.254's password:
Access denied
root@192.168.0.254's password: █
```

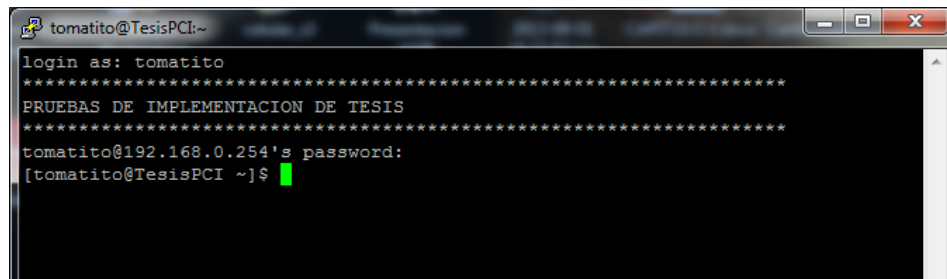
Figura ANEXO 2-Prueba de Aplicativo. 3 Usuario Root Denegado

- Configuración de usuarios para acceso mediante SSH. En las siguientes figuras (Figura ANEXO 2-Prueba de Aplicativo. 4 - 5- -6 -7) se puede apreciar los cambios realizados a nivel de ingresos a los usuarios donde se realizan el intento con los usuarios que tienen el acceso permitido así como los denegados.



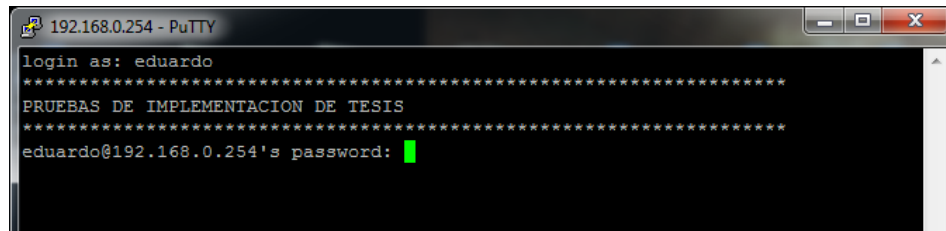
```
192.168.0.254 - PuTTY
login as: tomatito
*****
PRUEBAS DE IMPLEMENTACION DE TESIS
*****
tomatito@192.168.0.254's password: █
```

Figura ANEXO 2-Prueba de Aplicativo. 5 Ingreso de clave de usuario permitido



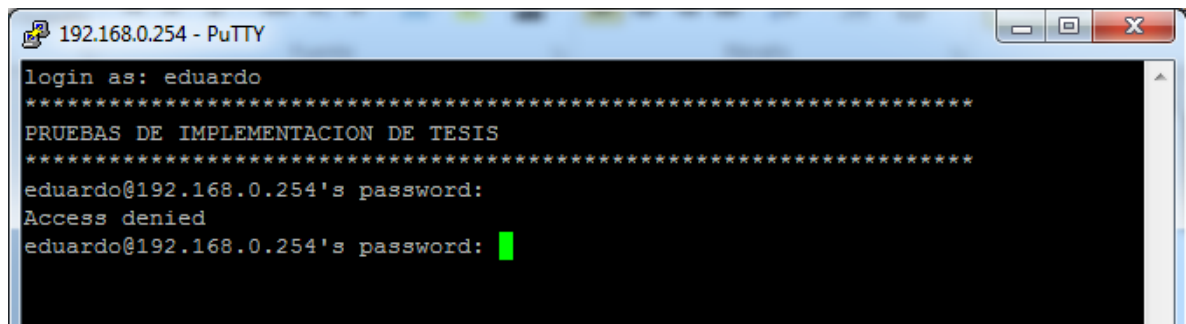
```
tomatito@TesisPCI:~
login as: tomatito
*****
PRUEBAS DE IMPLEMENTACION DE TESIS
*****
tomatito@192.168.0.254's password:
[tomatito@TesisPCI ~]$ █
```

Figura ANEXO 2-Prueba de Aplicativo. 6 Ingreso de sesión con usuario asignado



```
192.168.0.254 - PuTTY
login as: eduardo
*****
PRUEBAS DE IMPLEMENTACION DE TESIS
*****
eduardo@192.168.0.254's password: █
```

Figura ANEXO 2-Prueba de Aplicativo. 7 Ingreso de clave de usuario negado



```
192.168.0.254 - PuTTY
login as: eduardo
*****
PRUEBAS DE IMPLEMENTACION DE TESIS
*****
eduardo@192.168.0.254's password:
Access denied
eduardo@192.168.0.254's password: █
```

Figura ANEXO 2-Prueba de Aplicativo. 8 Indica que el usuario no puede ingresar

- Número máximo de intentos fallidos durante el login del usuario (Figura ANEXO 2-Prueba de Aplicativo.8). En caso del ingreso incorrecto del password se muestra el cambio aplicado luego de varios intentos fallidos.

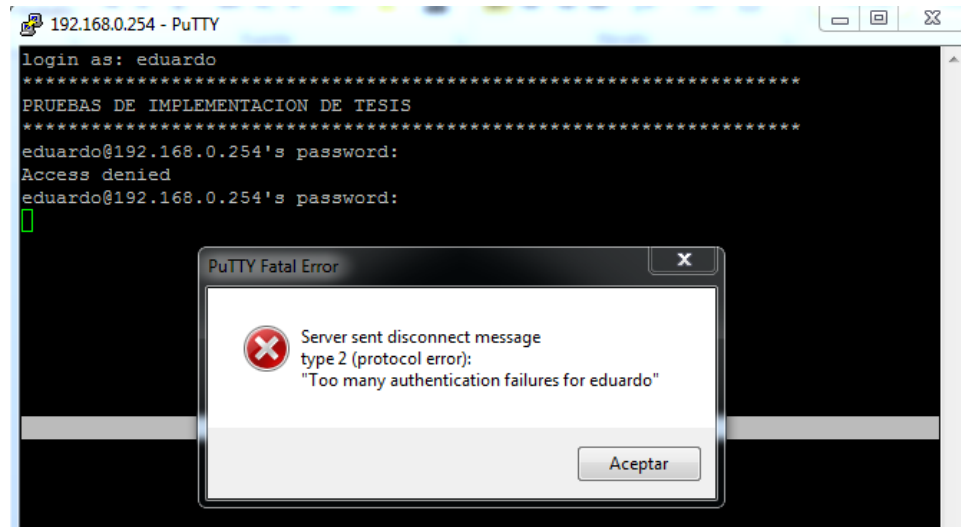
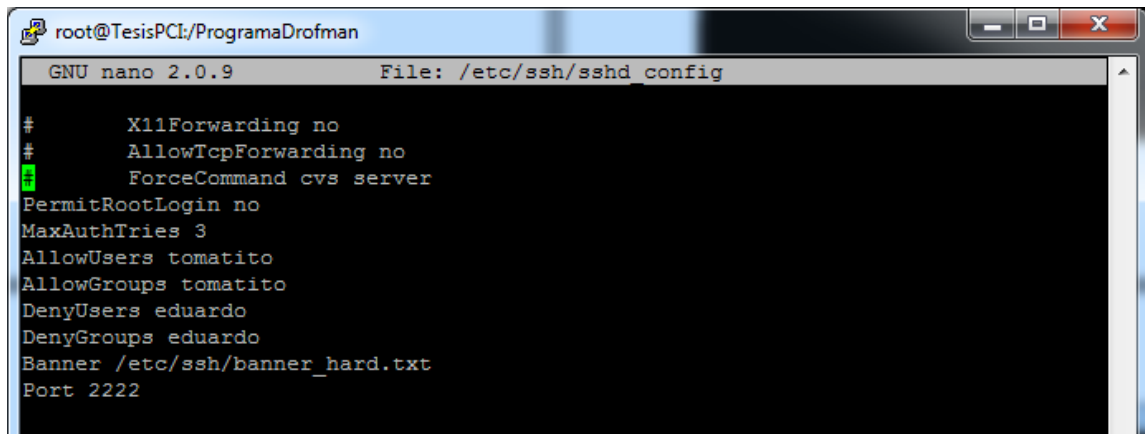


Figura ANEXO 2-Prueba de Aplicativo. 9 Mensaje de intentos fallidos llegados al máximo

- Cambios en archivos de configuración (Figura ANEXO 2- Cambios realizados bajo el aplicativo 9). Se muestra los cambios aplicados a nivel de configuración en archivos para poder cumplir las normas establecidas PCI.



```
root@TesisPCI:/ProgramaDrofman
GNU nano 2.0.9 File: /etc/ssh/sshd config
# X11Forwarding no
# AllowTcpForwarding no
# ForceCommand cvs server
PermitRootLogin no
MaxAuthTries 3
AllowUsers tomatito
AllowGroups tomatito
DenyUsers eduardo
DenyGroups eduardo
Banner /etc/ssh/banner_hard.txt
Port 2222
```

Figura ANEXO 2- Cambios realizados bajo el aplicativo 9

GLOSARIO

ACL: lista de control de acceso o *ACL* (del inglés, *Access control list*) es un concepto de seguridad informática usado para fomentar la separación de privilegios.

CDE: Cardholder data environment – datos de los tarjetahabientes.

DMZ: Demilitarized Zone - hace referencia a una zona aislada que posee aplicaciones disponibles para el público

DNS: Domain Name System (en español: **sistema de nombres de dominio**) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

DOS: Denial of Service - **ataque de denegación de servicios** es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

DSS: Decision Support System - sistema informático utilizado para servir de apoyo más que automatizar el proceso de toma de decisiones.

HSM: Hardware Security Module - dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas.

HTCP: Hyper Text Caching Protocol - protocolo para la consulta, administración y de servidores de caché HTTP.

HTTP: Hypertext Transfer Protocol - (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web.

IP: Internet Protocol - protocolo de comunicación de datos digitales clasificado funcionalmente en la Capa de Red según el modelo internacional OSI.

IPS: Intrusion prevention systems - software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

LAN: Local Area Network - Red de área local.

NFS: Network File System - protocolo de nivel de aplicación, según el Modelo

OSI utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local.

NIS: Network Information Service - (*Sistema de Información de Red*), es el nombre de un protocolo de servicios de directorios cliente-servidor desarrollado por Sun Microsystems para el envío de datos de configuración en sistemas distribuidos tales como nombres de usuarios y hosts entre computadoras sobre una red.

NTP: Network Time Protocol - protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123.

OS: Operating System - colección de software que maneja el hardware del ordenador y proporciona los recursos comunes de servicios de los programas de ordenador.

PCI DSS: Payment Card Industry Data Security Standard - consiste en una serie de estándares de seguridad que incluyen: Requerimientos para administrar la

seguridad, las políticas, procedimientos, la arquitectura de redes, el diseño de software y otras medidas críticas de protección de la información.

PCI SSC: Payment Card Industry Security Standards Council - foro mundial abierto destinado a la formulación, la mejora, el almacenamiento, la difusión y la aplicación permanentes de las normas de seguridad para la protección de datos de cuentas.

RAM: Random-access memory - memoria de acceso aleatorio.

SFTP: SSH File Transfer Protocol - protocolo del nivel de aplicación que proporciona la funcionalidad necesaria para la transferencia y manipulación de archivos sobre un flujo de datos fiable.

SNMP: Simple Network Management Protocol - un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

SSH: Secure Shell - nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

VNC: Virtual Network Computing - programa de software libre basado en una estructura cliente-servidor el cual permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente.

VPN: Virtual Private Network - esquema se utiliza para conectar oficinas remotas con la sede central de la organización.

WAN: Wide Area Network - es la unión de dos o más redes LAN.