ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD PERIMETRAL EN LA RED DE DATOS DE UNA EMPRESA DE SERVICIOS FINANCIEROS"

TRABAJO DE TITULACIÓN

Previo a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

ALLAN OMAR GALLEGOS VINCES

VÍCTOR MANUEL CONTRERAS ARCOS

GUAYAQUIL – ECUADOR

AÑO: 2017

AGRADECIMIENTOS

A Dios por llenarme de voluntad, paciencia y sobre todo no rendirme aun en los momentos difíciles.

A mis padres, hermano y esposa que fueron el motor desde fuera de las aulas para motivarme a luchar en el continuo mejoramiento de mi formación académica.

A todo el personal docente que forma parte de la carrera del MSIA para poder elaborar esta tesis y en especial a nuestro tutor el Ing. Fabián Barboza por su valioso aporte en el desarrollo de nuestra tesis.

Allan Gallegos Vinces

A Dios por darme la fuerza de seguir siempre adelante. A mi esposa Jessenia y a mis hijas María Belén & Daniela Sofía por su apoyo incondicional y por ser el pilar que sustenta mi vida. A mi madre Romelia Victoria por su apoyo permanente. A nuestro Director de Tesis Fabián Barboza por guiarnos tan acertadamente durante el proyecto de titulación. A Luis Ángel Ushca y Gabriel Valencia por compartir su conocimiento y experiencia profesional; y, finalmente un agradecimiento especial a mis compañeros, personal Docente y Administrativo de la MSIA-ESPOL que a través de su colaboración, gestión y enseñanza han permitido fortalecer mi formación profesional.

Víctor Contreras Arcos

DEDICATORIA

A mi esposa, mi madre, mi padre y hermano.

Allan Gallegos Vinces

A mi esposa Jessenia y a mis hijas María Belén & Daniela Sofía.

Víctor Contreras Arcos

TRIBUNAL DE SUSTENTACIÓN

MSIG. LENIN FREIRE

DIRECTOR MSIA

MGS. FABIÁN BARBOZA

DIRECTOR DEL PROYECTO DE GRADUACIÓN

MGS. LAURA URETA

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de esta Tesis de Grado, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Ing. Allan Gallegos Vinces

Ing. Víctor Contreras Arcos

RESUMEN

Las empresas e instituciones que basan su línea de negocios en la prestación de servicios financieros, deben considerar a la información como parte integral de sus principales activos y establecer las medidas de seguridad necesarias para proteger a todos los elementos que interactúan con ella permitiendo su acceso, edición y almacenamiento. Es de suma importancia la protección de estos elementos llamados activos de información, ya que representan valor para la institución y en caso de ser atacados, pondrían en riesgo su integridad, disponibilidad y confidencialidad.

En la actualidad, las empresas e instituciones de servicios financieros, están conectadas a redes externas (internet) para facilitar la oferta y prestación de servicios a través de aplicaciones web; lo cual crea una ventana, que de no ser protegida adecuadamente, podría permitir la materialización efectiva de ataques de intrusión, desencadenando graves consecuencias y afectaciones en el desempeño normal del giro de negocios.

En el presente proyecto de titulación, se realiza la implementación de un esquema de seguridad perimetral en la red de datos de una institución financiera ecuatoriana, a través de la identificación y valoración de sus activos de información, definición de políticas apegadas a las normas ISO 27001 e ISO 27002, análisis de

vulnerabilidades y mitigación de riesgos en el servidor web; y finalmente, la implementación de un sistema de detección y prevención de intrusos.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

ACL Access Control List (Lista de control de acceso)

BDD Base de Datos

BGP Border Gateway Protocol (Protocolo de puerta de enlace de borde)

CFOS Chief Financial Officer (Gerente Financiero)

DDR3 Double Data Rate Type Three (Velocidad de datos doble tipo tres)

DHCP Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de host)

DMZ Demilitarized Zone (Zona desmilitarizada)

DoS Denial of Service (Denegación de servicio)

DDoS Distributed Denial of Service (Denegación de servicio distribuido)

DPS Data Protection Systems (Sistemas de protección de datos)

EIGRP Enhanced Interior Gateway Routing Protocol (Protocolo de enrutamiento de puerta de enlace interior mejorado)

ERP Enterprise Resource Planning (Planificación de Recursos Empresariales)

GB Gigabyte

GNU GNU's Not Unix - (GNU No es Unix - Acrónimo recursivo)

GPON Gigabit-capable Passive Optical Network (Red óptica pasiva con capacidad Gigabit)

HSRP Hot Standby Router Protocol (Protocolo de despliegue de ruteadores redundantes)

HTTPS Hypertext Transfer Protocol Secure (Protocolo seguro de transferencia de hipertexto)

ICMP Internet Control Message Protocol (Protocolo de mensajes de control de internet)

IDS Intrusion Detection System (Sistema de detección de intrusos)

IP Internet Protocol (Protocolo de Internet)

IPS Intrusion Prevention System (Sistema de prevención de intrusos)

ISO International Organization for Standardization (Organización Internacional de Normalización)

ISP	Internet service provider (Proveedor de servicios de internet)
LAN	Local Area Network (Red de área local)
MB	Megabyte
Mbps	Megabit por segundo
NAT	Network Address Translation (Traducción de direcciones de red)
OSI	Open Systems Interconnection (Modelo de interconexión de sistemas abiertos)
OSPF	Open Shortest Path First (Primer camino más corto)
PHVA	Planificar, Hacer, Verificar, Actuar
RADIUS	Remote Authentication Dial-In User Service (Protocolo de servicio de usuario de acceso telefónico de autenticación remota)
RDIMM	Registered Dual In-Line Memory Modules (Módulos de memoria con contactos duales registrados)
RIP	Routing Information Protocol (Protocolo de información de encaminamiento)
SD HC	Secure Digital High Capacity (Tarjeta de memoria de alta capacidad)

SSH	Secure Shell (Intérprete de órdenes seguro)
SSL/TLS	Secure Sockets Layer/Transport Layer Security (Capa de puertos seguros/Seguridad de la capa de transporte)
TACACS	Terminal Access Controller Access Control System (Sistema de control de acceso mediante control del acceso desde terminales)
TB	Terabyte
TCP	Transmission Control Protocol (Protocolo de control de transmisión)
TI	Tecnologías de la Información
UDP	User Datagram Protocol (Protocolo de datagrama de usuario)
USB	Universal Serial Bus (Bus universal en serie)
VPN	Virtual Private Network (red privada virtual)
WAN	Wide Area Network (Red de área extensa)

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad, las medidas de seguridad aplicadas adecuadamente al perímetro de una red de datos, constituyen una fortaleza de protección empresarial, especialmente si se tratan de instituciones cuyo giro del negocio radica en la prestación de servicios financieros.

En el presente proyecto de titulación, se realiza la implementación de un esquema de seguridad perimetral en una empresa ecuatoriana que brinda servicios financieros y que complementa su giro de negocios a través de la prestación de servicios mediante una aplicación web.

En el capítulo uno, se realiza un análisis del entorno empresarial y su infraestructura tecnológica, se identifican los problemas inherentes a la seguridad perimetral y se realiza el planteamiento de una propuesta de solución.

El capítulo dos establece el marco teórico que sirve de guía para la implementación del esquema de seguridad perimetral utilizado durante el presente proyecto de titulación.

En el capítulo tres, se realiza un análisis de riesgos, vulnerabilidades y amenazas a la red perimetral de datos, tomando como punto de partida la identificación y valoración de los activos de información de la empresa.

El análisis y diseño del esquema de seguridad perimetral se plantea en el capítulo cuatro, aquí se definen las políticas de seguridad perimetral apegadas a las normas ISO 27001 e ISO 27002, se analizan el servidor web y el cortafuegos perimetral como activos de información críticos y el diseño de las medidas de protección requeridas para mitigar sus riesgos; y finalmente, se diseña un esquema de detección y protección contra intrusos en la red de datos perimetral.

En el capítulo cinco, se realizan las pruebas e implementación del esquema de seguridad, validando la eficacia de protección en los diferentes escenarios establecidos.

Finalmente en el capítulo seis, se realiza un análisis de los resultados obtenidos posterior a la implementación del esquema de seguridad perimetral, los mismos que sirven de base para el planteamiento de las respectivas conclusiones y recomendaciones.

CAPÍTULO 1

GENERALIDADES

1.1. Antecedentes

La empresa Financiera Lago Azul (nombre protegido por razones de confidencialidad), es una institución ecuatoriana dedicada a la prestación de servicios financieros enfocada en brindar de manera ágil y oportuna a sus clientes los siguientes servicios: préstamos, seguro de vida, pago de pensiones y jubilaciones.

Como parte de su planificación estratégica global, Financiera Lago Azul ha definido el contexto de su organización (misión, visión y objetivo) de la siguiente manera:

1.1.1. Visión

Ampliar los beneficios sociales a favor de nuestros afiliados activos y su entorno familiar, como también el personal de servicios pasivos y estar como ente solidario de apoyo.

1.1.2. Misión

Organizar, administrar las prestaciones y servicios sociales para propiciar el desarrollo integral de los afiliados activos y pasivos, impulsando su participación activa, organizada a través de una gestión promotora de consensos que, respetando y haciendo respetar el marco legal establecido, proyecte el crecimiento ordenado de la institución.

1.1.3. Objetivo

El objetivo fundamental de la institución es garantizar y fortalecer la estabilidad financiera del sistema de prestaciones y servicios sociales, sin menoscabar el objetivo social, a través de una eficiente organización y administración de las prestaciones y servicios sociales establecida en la ley.

1.1.4. Organigrama

Financiera Lago Azul, mantiene una adecuada organización y segregación de funciones, la misma que permite mantener un correcto flujo tanto comunicacional como operativo. A continuación, se muestra el organigrama funcional de la empresa:

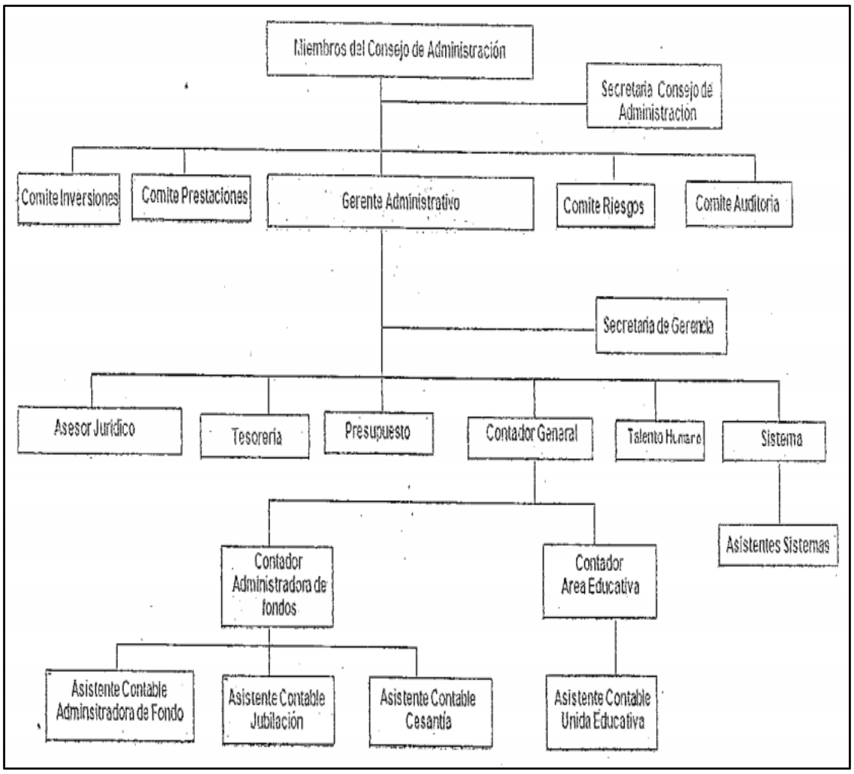


Figura 1.1 Organigrama Financiera Lago Azul

1.1.5. Localización

Financiera Lago Azul tiene su ubicación en el norte de la ciudad de Guayaquil; brindando así una adecuada cobertura de servicios financieros a sus clientes, ya que posee una sólida infraestructura tecnológica capaz de soportar efectivamente todos los procesos inherentes a su línea de negocios.

1.1.6. Infraestructura tecnológica

La infraestructura tecnológica empresarial está soportada por equipos y elementos de red, servidores de procesamiento de datos, equipos de seguridad y dispositivos de usuario final.

1.1.6.1. Conectividad WAN

El servicio de conectividad exterior WAN (Red de área extensa), permite a los usuarios internos acceder a internet y a todos los servicios relacionados al giro del negocio (correo electrónico corporativo, Cash Management, etc.); y a la vez, permite el acceso de los clientes externos a los servicios web institucionales (portal de servicios).

El servicio de acceso a internet lo provee un ISP (Proveedor de Servicios de Internet) a través de un enlace dedicado de fibra óptica GPON (Red óptica pasiva con capacidad Gigabit) con un ancho de banda de 3Mpbs.

El principal equipo de conectividad de borde es un ruteador de marca Cisco, el cual permite conectar la red de datos local con la red externa (internet).

Tabla 1. Características del ruteador de borde.

CARACTERÍSTICA	DESCRIPCIÓN
Identificación	R1
Servicio	Ruteador de borde
Dispositivo	Ruteador
Marca	Cisco
Modelo	881 (800 Series)
Puertos WAN	1 Ethernet (RJ-45)
Puertos LAN	4 puertos
Puertos USB	1 puerto
Protocolos de ruteo	BGP, EIGRP, HSRP, OSPF, RIP-1, RIP-2
DHCP	Cliente / Servidor
Velocidad Ethernet LAN	10/100BASE-T(X)
Memoria interna	256 MB
Memoria Flash	128 MB

1.1.6.2. LAN

La red de área local (LAN) está conformada por equipos de red (conmutadores) y cableado blindado categoría 6, los cuales permiten establecer conectividad de alto rendimiento entre los distintos dispositivos de usuario final, así como también acceder a servicios tanto locales como externos.

Tabla 2. Características del conmutador principal.

CARACTERÍSTICA	DESCRIPCIÓN
Identificación	S1
Servicio	Conmutador principal
Dispositivo	Conmutador administrable
Marca	Cisco
Modelo	SF-300
Interfaces 10Base-T/100Base-TX	48 (RJ-45 - PoE)
Interfaces de consola	1 - 9 pin D-Sub (DB-9)
Interfaces 10Base-T/100Base-TX/1000Base-T	4 (RJ-45)
Interfaces SFP	2 (mini-GBIC)
Desempeño	17.6 Gbps
Método de autenticación	Secure Shell (SSH), RADIUS, TACACS+

Memoria Flash	16 MB
Memoria RAM	128 MB

1.1.6.3. Servidores

Para brindar atención a los clientes internos, se cuenta con un servidor que soporta los servicios de aplicaciones (ERP – Planeamiento de Recursos Empresariales), base de datos y protección de datos. La prestación de servicios a usuarios externos se lo realiza a través de un servidor web.

Tabla 3. Características del servidor de aplicaciones y base de datos.

CARACTERÍSTICA	DESCRIPCIÓN
Identificación	SRV1
Servicios	Aplicaciones (ERP) / Base de Datos (BDD) / DPS (Data Protection Systems)
Dispositivo	Servidor
Marca	IBM
Modelo	X3530 M4
Plataforma	Microsoft Windows

Procesador	Intel Xeon E5-2407 (2.20GHz/4-core/10MB/80W)
Memoria RAM	32 GB DDR3-1333MHz ECC RDIMM
Sistema Operativo	Windows Server 2012 Standard 64 bits
Puertos de red	2 puertos Gigabit Ethernet
Espacio en disco	2TB
Nivel de Raid	Raid 1

Tabla 4. Características del servidor Web.

CARACTERÍSTICA	DESCRIPCIÓN
Identificación	SRV
Servicios	Aplicación Web
Dispositivo	Servidor
Marca	HP
Modelo	3130 MT
Plataforma	Microsoft Windows
Procesador	Intel® Core™ i3 (3.2Ghz/2-core)
Memoria RAM	2 GB
Sistema Operativo	Windows Server 2008 Enterprise 64 bits
Puertos de red	2 LAN Ethernet
Espacio en disco	1TB

1.1.6.4. Estaciones de trabajo

Las estaciones de trabajo o centros de atención al usuario, están soportados por computadores personales de escritorio, éstos son de altas prestaciones, lo que permite rapidez de procesamiento e incremento en la productividad.

Tabla 5. Características de las estaciones de trabajo.

CARACTERÍSTICA	DESCRIPCIÓN
Identificación	PC (n)
Servicio	Estación de trabajo
Dispositivo	Computador de
Marca	HP
Modelo	HP Compaq Elite 8300
Plataforma	Microsoft Windows
Procesador	Intel® Core™ i7
Memoria RAM	4 GB
Sistema Operativo	Windows 7 Professional
Puertos de red	1 LAN Ethernet
Espacio en disco	1TB

1.1.6.5. Infraestructura de seguridad

A fin de precautelar de forma física los elementos activos de la red de datos de la institución, se cuenta con un Centro de Datos climatizado con acceso biométrico, cámaras de video vigilancia y sistema automático contra incendios.

Todo acceso físico, ya sea por parte del personal de TI (Tecnologías de la Información) como por parte de proveedores externos, se lo realiza mediante autorización expresa, manteniendo un registro permanente de actividades en bitácoras de gestión.

1.1.6.6. Seguridad lógica

La seguridad lógica se encuentra establecida en políticas y reglas implementadas tanto en el equipo cortafuegos perimetral como en la Suite de Protección de Datos.

En el cortafuego perimetral se definen los accesos, servicios y aplicaciones a los que pueden acceder los usuarios, basados en políticas previamente establecidas en el Esquema de Seguridad Informática.

La Suite de Protección de Datos es un servicio que permite controlar y evitar que se presenten fugas de información confidencial e institucional a través de cualquier medio electrónico, ya sea a través de dispositivos USB, discos duros externos, discos ópticos, discos magnéticos, correos electrónicos, e incluso medios impresos.

Tabla 6. Características del cortafuegos perimetral.

CARACTERÍSTICA	DESCRIPCIÓN
Identificación	F1
Servicio	Protección del perímetro
Dispositivo	Cortafuegos
Marca	Fortinet
Modelo	Fortigate 60C
Puertos WAN	2 Gigabit Ethernet (RJ-45)
Puertos DMZ	1 conexión (opcional a una red/dispositivo DMZ o a otras unidades
Puertos LAN	5 Gigabit Ethernet (RJ-45)
Rendimiento	- (512 / 1518 bytes paquetes UDP) de 1
Sesiones concurrentes	80000
IPSec VPN (AES-256 + SHA-1)	70 Mbps

Antivirus	Rendimiento de 20 Mbps
IPS	Rendimiento de 60 Mbps
Características adicionales	Incluye 4 GB de almacenamiento en tarjeta SD HC Clase 6 (soporta hasta 32 GB, a partir de 4GB se pueden almacenar logs y hacer reportes; a partir de 16 GB además Web Cache y optimización WAN)

1.1.6.7. Sistemas Antivirus

Para proteger los equipos de ataques a través de software malicioso (malware) como virus, troyanos, etc., la empresa dispone del sistema Kaspersky Endpoint Security 10 para Windows, el mismo que protege tanto las estaciones de trabajo como los servidores transaccionales.

1.1.6.8. Esquema de red

El esquema de la red de datos de Financiera Lago Azul, se muestra a continuación:

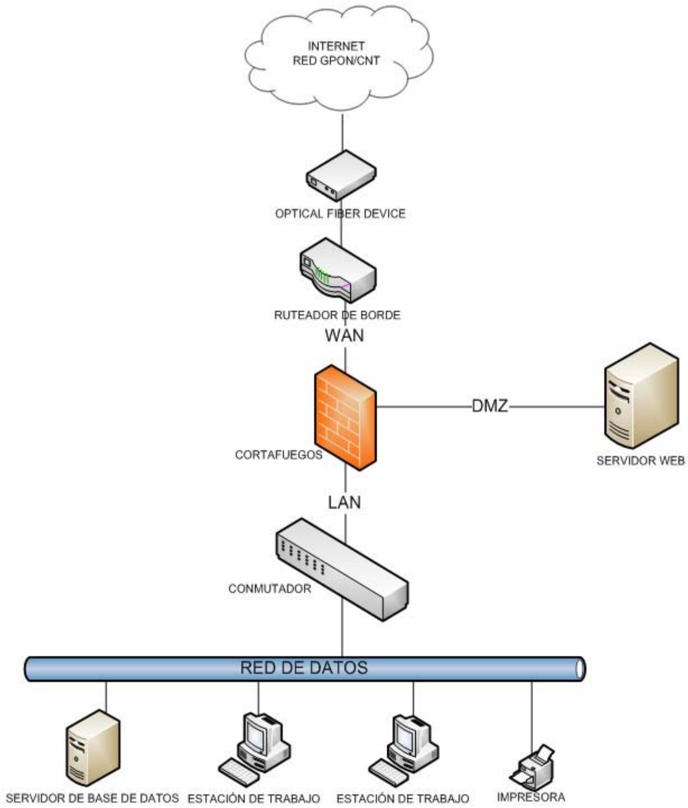


Figura 1.2 Esquema de red de datos de Financiera Lago Azul

1.1.7. Esquema de seguridad informática

Dentro de sus políticas de control para la mitigación de riesgos, Financiera Lago Azul posee un esquema de seguridad informática, cuya finalidad es establecer un marco para la implantación de seguridad y control, la misma que cubre los siguientes aspectos:

- Seguridad física y del entorno.

- Seguridad lógica.
- Seguridad Outsourcing.
- Planificación de seguridad informática.
- Planificación de contingencia y recuperación de desastres.

1.1.8. Implementaciones

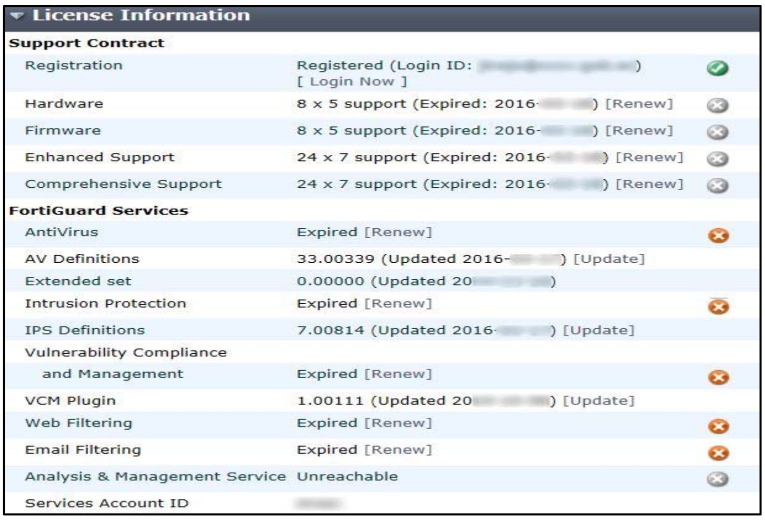
Como parte de sus operaciones de negocios, Financiera Lago Azul ha adquirido e implementado un nuevo aplicativo web, el mismo que se encuentra alojado en el servidor de aplicaciones web, el cual permite tanto a sus afiliados como al público en general consultar el catálogo de nuevos servicios, utilizar un simulador de créditos y a la vez acceder a un módulo de operaciones transaccionales (consulta de estados de cuenta, solicitudes en línea y transferencias).

1.2. Descripción del problema

Los servicios de antivirus, sistema de prevención de intrusos (IPS), gestión y cumplimiento de vulnerabilidades; y, filtrado de paquetes del cortafuegos de la empresa Financiera Lago Azul, en ocasiones se han encontrado deshabilitados debido a la expiración de sus licencias de uso

(Figura 3), debido principalmente a la ausencia de procedimientos de control en el proceso de renovación oportuna de licencias de software, lo que ha conllevado a la empresa a generar tiempos de espera sin servicio y soporte hasta completar la gestión de renovación y activación de licencias.

Este escenario hace que el Cortafuegos no cuente con todas sus funcionalidades operativas y a la vez no permita realizar las actualizaciones correspondientes, lo que representa un riesgo en la seguridad perimetral de la red de datos, ya que durante el tiempo que dura el proceso de renovación, pueden aparecer nuevas amenazas o vulnerabilidades, las mismas que pueden ser aprovechadas por terceras personas para perpetrar ataques externos y cometer diferentes tipos de delitos informáticos [1] comprometiendo los activos de información la empresa.



License Information	
Support Contract	
Registration	Registered (Login ID:) [Login Now]
Hardware	8 x 5 support (Expired: 2016-) [Renew]
Firmware	8 x 5 support (Expired: 2016-) [Renew]
Enhanced Support	24 x 7 support (Expired: 2016-) [Renew]
Comprehensive Support	24 x 7 support (Expired: 2016-) [Renew]
FortiGuard Services	
AntiVirus	Expired [Renew]
AV Definitions	33.00339 (Updated 2016-) [Update]
Extended set	0.00000 (Updated 20)
Intrusion Protection	Expired [Renew]
IPS Definitions	7.00814 (Updated 2016) [Update]
Vulnerability Compliance and Management	Expired [Renew]
VCM Plugin	1.00111 (Updated 20) [Update]
Web Filtering	Expired [Renew]
Email Filtering	Expired [Renew]
Analysis & Management Service	Unreachable
Services Account ID	

Figura 1.3 Información de licencia del cortafuegos de Financiera Lago Azul.

El esquema de seguridad informática de Financiera Lago Azul, no incluye políticas de control relacionadas a la seguridad perimetral de la red de datos, lo que implica que no existen procedimientos normativos que guíen y obliguen a realizar acciones que precautelen la seguridad de los activos de información ante amenazas externas a la red de datos.

Financiera Lago Azul no contempla políticas de alta disponibilidad que permitan mantener la prestación de servicios financieros aun cuando se presenten fallos o exista la ausencia de alguno de sus componentes críticos (cortafuegos perimetral, base de datos, ISP). Asimismo, no se han definido políticas de continuidad del negocio en caso de que el centro de datos entre en un estado de inoperatividad.

Dentro del plan operativo anual, el área de Tecnologías de la Información y Comunicaciones de la empresa Financiera Lago Azul, no ha contemplado ni ha realizado análisis de vulnerabilidades en su servidor web publicado, lo que ocasiona que no se cuente con información actualizada sobre los riesgos existentes y la eficacia del funcionamiento de las reglas implementadas para proteger los activos de información de la empresa; situación que genera incertidumbre, ya que no se tiene una visibilidad integral del tráfico entrante desde internet hacia la red de la empresa y sus afectaciones una vez que ha entrado en operaciones el nuevo aplicativo web.

El cortafuegos perimetral carece de robustez tanto en su configuración como en la aplicación de reglas de filtrado.

No se dispone de protección contra intentos de intrusión.

A continuación se resumen los principales problemas relacionados a la seguridad perimetral de la empresa Financiera Lago Azul:

- Como parte de la gestión de activos, no se han definido políticas integrales de control del inventario de licenciamiento de software.

- Las políticas de seguridad de la información de la empresa no incluyen controles relacionados a la seguridad perimetral de la red de datos de la empresa.

- No existen implementadas políticas de alta disponibilidad que garanticen la prestación ininterrumpida de servicios cuando se presenten incidentes en los equipos de la red de datos.

- No se cuenta con políticas de continuidad del negocio que permitan que los tiempos de restauración de servicios y continuidad de operaciones sean óptimos en caso de que el centro de datos falle.

- No se ha realizado análisis de vulnerabilidades al servidor web publicado.

- El cortafuegos perimetral carece de robustez en la configuración de reglas de filtrado.

- No se dispone de protección contra intentos de intrusión.

1.3. Solución propuesta

Con la finalidad de proteger los activos de información de la empresa Financiera Lago Azul, se propone implementar un esquema de seguridad perimetral que permita mitigar el riesgo de ataques externos a través de la red. De la misma forma, se plantea establecer políticas alineadas a la norma ISO 27001, las cuales al ser implementadas permitan reducir los tiempos de interrupción de servicios cuando se presenten incidentes. Para ello, a continuación se indican las acciones de solución a llevarse a cabo:

- Definir y otorgar a Financiera Lago Azul, los lineamientos y políticas generales relacionadas a la seguridad perimetral que incluyan gestión de activos y administración de licencias de software, así como también políticas de alta disponibilidad y continuidad del negocio, alineadas a la norma ISO 27001 e ISO 27002 para que sean incorporadas en su esquema de seguridad informática.

- Realizar un análisis de vulnerabilidades en el servidor web publicado ya que el mismo puede constituirse en un punto crítico para la seguridad de la red de datos perimetral.

- Implementación de configuración y reglas de filtrado robustas en el cortafuegos perimetral que permita reducir el riesgo de ataques externos a la red de datos.

- Implementar un esquema de seguridad perimetral que permita proteger la red de datos de ataques de intrusión.

Los beneficios de la solución propuesta son:

- Incorporar políticas de seguridad perimetral, al esquema de seguridad informática de la empresa Financiera Lago azul, apegadas a las normativas ISO 27001 e ISO 27002

- Reforzar la seguridad perimetral de la empresa Financiera Lago Azul de la siguiente manera:

    - Conocer las vulnerabilidades existentes en el servidor web y mitigar los riesgos de materialización de ataques externos.

    - Aumentar el nivel de protección perimetral contra ataques de intrusión.

    - Reforzar las políticas/configuraciones en el cortafuego perimetral para el filtrado.

- Incorporar la capacidad de monitorear y controlar la seguridad perimetral de la red de datos.

1.4. Objetivo general

Definir los lineamientos y políticas generales relacionadas a la seguridad perimetral apegadas a las normas ISO 27001 e ISO 27002 e implementar un esquema de seguridad perimetral en la red de datos de la empresa Financiera Lago Azul, a fin de proteger los activos de información de ataques externos que se realicen a través de la red de datos perimetral.

1.5. Objetivos específicos

- Establecer y otorgar los lineamientos y políticas de seguridad perimetral apegadas a las normas ISO 27001 e ISO 27002 que puedan ser incorporadas en el actual esquema de seguridad informática de la empresa Financiera Lago Azul.

- Identificar riesgos, amenazas y vulnerabilidades de la red de datos perimetral de la empresa Financiera Lago Azul.

- Robustecer la configuración y reglas de filtrado del cortafuegos perimetral.

- Mitigar el riesgo de ataques de intrusión a través de la implementación de un esquema de seguridad perimetral en la red de datos de la empresa Financiera Lago Azul.

- Probar la eficacia de la implementación del esquema de seguridad perimetral en la red de datos de la empresa Financiera Lago Azul.

1.6. Metodología

A fin de cumplir satisfactoriamente con los objetivos planteados, se ha definido el siguiente esquema metodológico:

- Identificar los activos de información de la empresa Financiera Lago Azul, que deben ser protegidos de amenazas y ataques externos a través de la red de datos.
- Elaborar una matriz de riesgos de seguridad perimetral en la red de datos de la empresa Financiera Lago Azul.
- Definir las políticas y controles que deben ser incorporadas en el actual esquema de seguridad perimetral, apegados a las normas ISO 27001 e ISO 27002.
- Realizar análisis de vulnerabilidades en el servidor web publicado, bajo la supervisión del área de Tecnologías de la Información de la empresa Financiera Lago Azul
- Configurar el equipo cortafuegos perimetral de la empresa Financiera Lago Azul, en apego a los controles de seguridad

definidos en el esquema de seguridad informática, manteniendo un equilibrio razonable entre accesos y restricciones.

- Implementar un esquema de protección de ataques de intrusión y las herramientas de monitoreo y control asociadas en la empresa Financiera Lago Azul.

- Analizar los resultados obtenidos luego de implementación del esquema de seguridad perimetral en la empresa Financiera Lago Azul y proponer mejoras.

CAPÍTULO 2

MARCO TEÓRICO

El presente trabajo de titulación es desarrollado en base a la norma ISO 27001 y 27002 con enfoque en los controles requeridos en la red perimetral.

2.1. Seguridad del Perímetro en la red de datos

2.1.1. Perímetro de la red de datos

La red de área local (LAN) de cualquier empresa, sea esta pública o privada, generalmente requiere de conectividad hacia otras redes de área local o redes de área amplia (WAN-Internet) a fin de sostener adecuadamente su línea de negocios.

Para conectar dos o más redes se requiere la utilización de dispositivos de borde tales como ruteadores, cortafuegos, sistemas de detección y/o prevención de intrusos, entre otros.

Cuando se realiza la conectividad entre dos o más redes, se puede considerar como el perímetro físico de la red de datos, a todos aquellos dispositivos de borde que permiten y hacen posible esta conectividad [2], tal como se muestra en el figura 4.

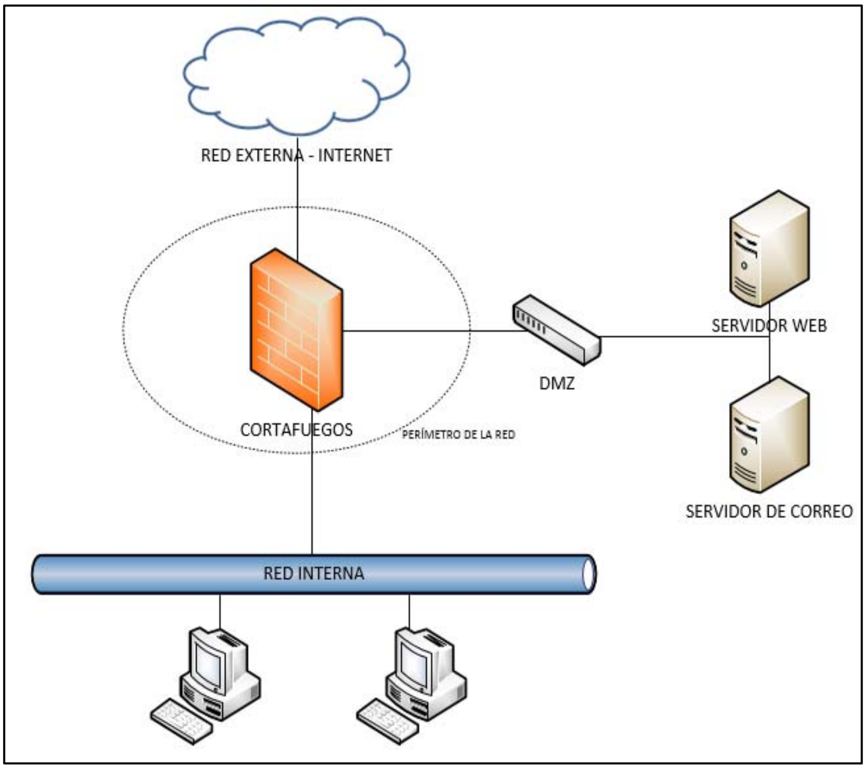


Figura 2.1 Perímetro de la red de datos

2.1.2. Elementos de seguridad de la información

Para proteger y asegurar los activos de información de la red de datos, se deben cumplir con los siguientes elementos de seguridad de la información [3]:

- Confidencialidad y Autenticidad: La información debe provenir de fuentes originales y debe ser a accedida únicamente por entes autorizados (usuarios, aplicaciones, servicios, etc.).

- Integridad: La información no debe permitir cambios no autorizados.

- Disponibilidad: La información debe estar accesible en el momento en el que se la necesita.

2.1.3. Importancia de asegurar el perímetro de la red de datos

En el instante en que una red de datos interna de una empresa, se conecta a una red externa (WAN, Internet), se abre un canal comunicacional por el cual puede circular diferente tipo de tráfico (voz, datos, etc.), lo que hace que la red de datos interna quede expuesta; es por esta razón, que se deben implementar las medidas de seguridad necesarias a fin de mitigar riesgos y garantizar que el tráfico entrante sea confiable y seguro.

La ausencia de implementación de medidas y políticas de seguridad perimetral en la red de datos, podría permitir accesos no autorizados provenientes de redes externas, los cuales pueden comprometer los elementos de seguridad de los activos de información de la empresa y verse perjudicada por el cometimiento de algún acto ilícito.

Resume de gran importancia la implementación de medidas de seguridad en la red perimetral de datos, a fin de protegerla de accesos no autorizados, cumpliendo así con el propósito principal de la seguridad en las redes de datos [3].

2.1.4. Riesgos que amenazan la seguridad en el perímetro de la red de datos

Considerando que un riesgo es la posibilidad de ocurrencia de un suceso que pudiera afectar de forma negativa la seguridad perimetral en una red de datos, a continuación se describen aquellos que revisten mayor importancia; y por lo tanto, deberán ser tratados a fin de mitigar la materialización de los mismos.

2.1.4.1. Escaneo y Enumeración de vulnerabilidades

El escaneo y enumeración de vulnerabilidades es un proceso en el cual un atacante a través de herramientas informáticas, obtiene información de los elementos activos de la red de datos, la misma que le servirá de base para posteriormente materializar un ataque aprovechándose de las vulnerabilidades encontradas. Los resultados que se pueden obtener luego de realizar un proceso de escaneo y enumeración van desde identificar los hosts activos, hasta conocer información sensible de la red de datos como versiones de sistemas operativos (servidores, ruteadores, cortafuegos), direcciones ip internas, aplicaciones, servicios activos (puertos TPC/UDP) y hasta nombres de cuenta de usuarios [4].

2.1.4.2. Denegación de servicios

La denegación de servicios consiste en la materialización de un ataque aprovechado por la explotación de una o más vulnerabilidades existentes en la red de datos y cuyo objetivo principal es impedir la prestación de servicios de red; como por ejemplo, sitios y aplicaciones web, servicios web, nombres de dominio, correo electrónico, acceso a redes privadas virtuales (VPN), etc.

Entre los ataques de denegación de servicios más conocidos están: Inundación SYN, Smurf IP, Inundación UDP, Inundación ICMP y Ping de la muerte [5].

2.1.4.3. Apropiación ilegal de recursos e información

Las vulnerabilidades existentes y que no han sido mitigadas en el perímetro de la red de datos, pueden desencadenar en la materialización de ataques y llevar al atacante incluso a tomar el control total de uno o más equipos de la red, por lo que tanto los recursos como la información contenida en los mismos son expuestos a la apropiación no autorizada.

2.1.4.4. Fraude electrónico

Una de las motivaciones que tienen los delincuentes para realizar ataques externos a la red de datos de una empresa, es obtener provecho personal o para terceros de los privilegios no autorizados conseguidos producto de la materialización efectiva de un ataque.

Entre los hechos más peligrosos que por ejemplo un atacante podría cometer, se tienen los siguientes: obtención de información confidencial no autorizada, alteración de calificaciones de alumnos en sistemas académicos, movimientos no autorizados de dinero de cuentas bancarias, apropiación y utilización no autorizadas de credenciales financieras para realización de compras o pagos, alteración de datos personales, etc.

2.1.4.5. Afectación de imagen institucional

El solo hecho de que se conozca públicamente que una institución especialmente de índole financiera ha sido víctima de ataques externos efectivos a su red de datos, genera una alta afectación en su imagen institucional y a la vez desconfianza en sus clientes, los cuales podrían decidir abandonar la institución financiera y elegir otra que le garantice mayor seguridad a la hora de proteger valores monetarios. Es por esto, que no se debe escatimar esfuerzos en tomar todas las medidas de seguridad necesarias para mitigar toda clase de riesgos.

2.1.5. Factores que incrementan el riesgo de ataques en el perímetro de la red de datos

Existen factores que de una u otra manera inciden en el incremento del riesgo de ataques a través del perímetro de la red de datos. Entre los factores que se deben tomar en consideración se tienen:

2.1.5.1. Humano

El ser humano es uno de los factores más importantes y al que se debe poner mayor énfasis en la implementación de medidas de seguridad perimetral de datos. Un descuido, equivocación o negligencia por parte de la persona encargada de implementar una política o medida de seguridad, podría exponer considerablemente a una empresa a que ésta sea víctima de un ataque.

2.1.5.2. Organizacional

Una empresa correctamente organizada, con lineamientos y segregación de funciones adecuadas, en apego al cumplimiento de normas, políticas y controles establecidos como por ejemplo las normas ISO 27001 e ISO 27002, podrá estar mejor preparada para entender y mitigar los riesgos que una empresa que no se encuentre bien organizada.

2.1.5.3. Tecnológico

Debido a que constantemente se descubren y aparecen nuevas vulnerabilidades relacionadas al hardware y software de los equipos de borde de las redes de datos, el aspecto tecnológico es muy importante, ya que si los equipos o aplicaciones de borde se encuentran descontinuados o desactualizados, se abren puertas de seguridad que podrían ser aprovechados por terceras personas para realizar la materialización efectiva de ataques perimetrales.

2.1.6. Medidas que protegen la seguridad en el perímetro de la red de datos

A fin de mitigar los riesgos de ataques externos a través del perímetro de la red de datos, se puede considerar la realización de las siguientes acciones:

- Segregación y documentación adecuada de funciones y responsabilidades del personal de la empresa.

- Definición e implementación de políticas, procedimientos y controles de seguridad en apego a normas como la ISO 27001 e ISO 27002.

- Capacitación técnica y actualización de conocimientos al personal responsable de la seguridad perimetral de la red de datos.

- Socialización de los riesgos y toma de conciencia del cumplimiento de las normas básicas de seguridad a todo el personal de la empresa.
- Mantener una actualización permanente de respaldos de las configuraciones de seguridad de los equipos de borde.
- Mantener actualizado el software de los equipos de borde.
- Realizar un proceso de depuración (hardening) en los equipos de borde y servidores, a fin de desactivar puertos de aplicaciones que no se encuentren utilizados [4].
- Implementar conexiones seguras en las aplicaciones o sitios web mediante cifrado SSL/TLS y uso de certificados digitales; así como también, implementar cifrado de la data aplicando algoritmos de cifrado.
- Realizar auditorías y pruebas de evaluación de seguridad perimetral periódicas a fin de verificar su correcto funcionamiento.

2.2. Dispositivos y aplicaciones de seguridad perimetral

2.2.1. Dispositivos de seguridad perimetral

En la actualidad existen diferentes dispositivos que brindan seguridad en la red perimetral de datos. Entre los más destacados tenemos:

- Ruteadores
- Cortafuegos
- Cortafuegos de próxima generación
- Detección de Intrusos (IDS)
- Prevención de Intrusos (IPS)

Estos dispositivos ubicados en el borde de la red de datos, ayudan a proteger la infraestructura de la red de ataques externos [6] y se los puede conseguir en el mercado en diferentes marcas, modelos y fabricantes.

2.2.1.1. Ruteadores

Los ruteadores son dispositivos físicos que permiten conectar dos o más redes. Cuando son empleados para conectar la red interna de una empresa con una red externa, estos dispositivos proveen seguridad permitiendo configurar reglas de inspección y filtrado de paquetes o listas de acceso (ACL) [7] para denegar accesos no autorizados a equipos y/o servicios de red y a la vez permitir el tráfico de red deseado.

2.2.1.2. Cortafuegos

Los cortafuegos son dispositivos especializados en brindar seguridad y protección a la red de datos, bloqueando el tráfico no autorizado y aceptando el tráfico permitido, estos dispositivos pueden realizar el filtrado de paquetes a nivel de la capa 3 (red) y capa 4 (transporte) del modelo OSI [8].

Se puede utilizar un cortafuegos como medida de protección contra la exposición de equipos y aplicaciones sensibles a usuarios no autorizados, limitar el ámbito de posibles ataques por explotación efectiva de fallas en los protocolos; y, detectar y bloquear los datos maliciosos destinados a afectar equipos y servidores de la red interna [9].

2.2.1.3. Cortafuegos de próxima generación

Los cortafuegos de próxima generación son dispositivos de seguridad perimetral que cambian el concepto de seguridad de los cortafuegos tradicionales (filtrado por dirección ip - puerto), los cuales no permiten realizar un control basado en aplicaciones.

Considerando que en la actualidad existe un alto incremento, aceptación y uso de diversas aplicaciones y servicios web, los cortafuegos de próxima generación permiten fortalecer la seguridad perimetral y mantener un control basado en políticas flexibles sobre segmentos de red, aplicaciones, usuarios y contenido [10].

2.2.1.4. Sistemas de detección de intrusos (IDS)

Los sistemas de detección de intrusos (IDS) son herramientas que complementan la seguridad que brindan los cortafuegos. Los sistemas de detección de intrusos identifican si alguien con la finalidad de acceder a la red interna intenta romper las políticas de seguridad de un cortafuegos, y emite una alerta al administrador en caso de existir un evento malicioso de seguridad. Analógicamente, se puede comparar un sistema de detección de intrusos como una alarma antirrobo instalada en un domicilio. Un sistema de detección de intrusos, monitorea el tráfico de la red, analizándolo en búsqueda de posibles ataques originados desde la red externa, así como de la red interna de la organización [11].

2.2.1.5. Sistemas de prevención de intrusos (IPS)

Los sistemas de prevención de intrusos (IPS) permiten bloquear ataques proactivamente, a diferencia de los sistemas de detección de intrusos que únicamente evalúan el tráfico que pasa a través de los puertos abiertos, pero sin detenerlo [12].

2.2.2. Seguridad perimetral con GNU/Linux

La seguridad perimetral de una red de datos, también puede ser implementada utilizando un computador con sistema operativo GNU/Linux, ya que este incluye una herramienta (marco de trabajo) de procesamiento de paquetes de red llamada Netfilter, la cual puede ser configurada utilizando el comando iptables [13].

Iptables opera en la capa 3 (red) del modelo OSI a través de la aplicación de reglas de procesamiento para el filtrado de paquetes. Estas reglas son definidas en tablas por función (filtrado de paquetes, traducción de direcciones de red, y otro tipo de modificación de paquetes), cada uno de los cuales tiene cadenas (secuencias) de procesamiento. Las reglas básicamente consisten en combinaciones que especifican a qué paquetes se deben aplicar las políticas y cuál es su destino (acción a realizar con los paquetes) [13].

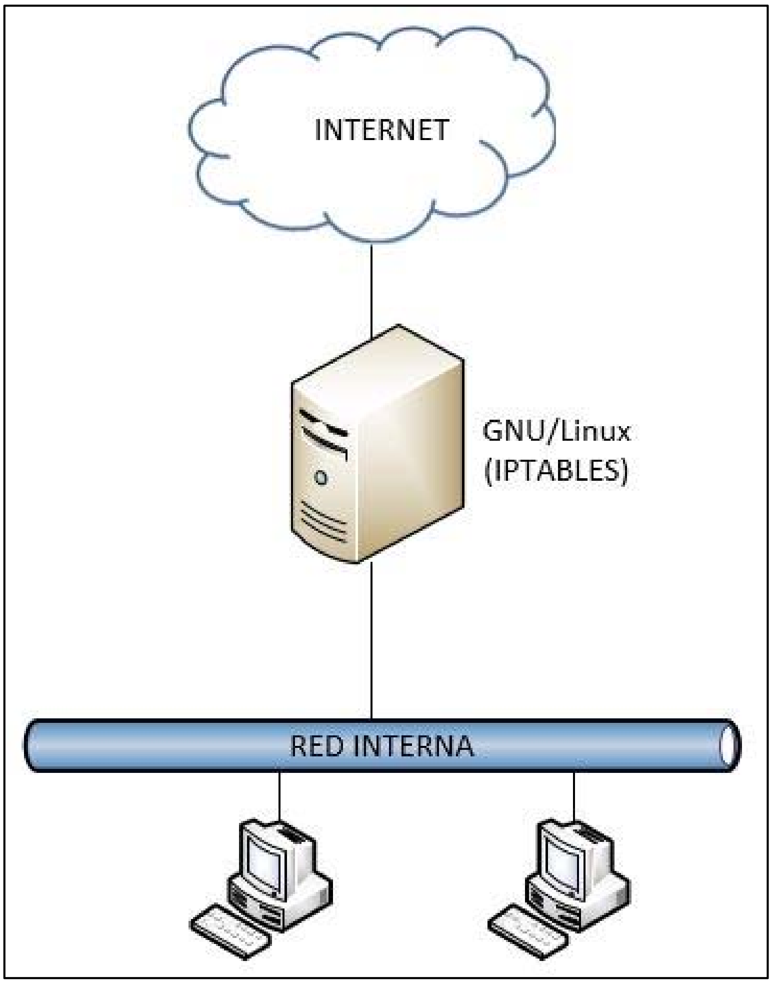


Figura 2.2 Seguridad perimetral con GNU/Linux

A continuación se especifican las tablas y cadenas que se pueden utilizar para configurar iptables [13]:

Tabla 7. Cadenas de iptables.

CADENA	INSTANCIA DE PROCESO DE PAQUETES
FORWARD	REENVIO. El flujo de tráfico pasa a través del equipo, ingresando por una interfaz de entrada con destino a una interfaz de salida.

INPUT	ENTRADA. Antes de ser entregados a un proceso local.
OUTPUT	SALIDA. Después de que se generan por un proceso local.
POSTROUTING	POST ENRUTAMIENTO. Antes de salir a una interfaz de red.
PREROUTING	PRE ENRUTAMIENTO. Antes de ingresar a una interfaz de red.

Tabla 8. Tablas que incorpora iptables.

TABLA	DESCRIPCIÓN
Nat	Se utiliza para redirigir conexiones hacia Nat (Network Address Translation - Traducción de direcciones de red). Se basa en direcciones de origen y destino. Incorpora las cadenas: OUTPUT, POSTROUTING y
Filter	Se utiliza para definir políticas para el tipo de tráfico permitido (entrada, salida, reenvío). Incorpora las cadenas FORWARD, INPUT y OUTPUT
Mangle	Se utiliza para modificar paquetes especializados. Incorpora las siguientes cadenas: FORWARD, INPUT, OUTPUT, POSTROUTING y PREROUTING.

Un ejemplo de filtrado de paquetes al puerto 443 (HTTPS) utilizando iptables, se indica a continuación:

iptables -t filter -I INPUT -p tcp --dport 443 –j DROP

El comando anterior, se puede interpretar como: Utilizando la tabla filter (-t filter), agregue una regla de filtrado de paquetes con cadena de entrada (-I INPUT) aplicada al protocolo tcp (-p tcp) con puerto de destino HTTPS 443 (--dport 443) y que ejecute la acción de eliminar los paquetes que cumplan la regla (-j DROP). Es decir que todo tráfico de entrada destinado al puerto 443, será descartado.

2.3. Gestión de riesgos de TI

2.3.1. Definición de riesgos

Cuando se presentan uno o varios eventos, éstos pueden generar impacto positivo, negativo o ambos. Los eventos con un impacto negativo representan riesgos, que pueden evitar la creación de valor o disminuir el valor existente. Los eventos con impacto positivo pueden compensar los impactos negativos o representar oportunidades [14].

Al riesgo, se lo puede definir también como el grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente [15].

2.3.2. Partes interesadas en la gestión de riesgos de TI

La gestión de riesgos, es responsabilidad de todas las personas que componen la organización, desde los altos ejecutivos hasta el último colaborador definido en los niveles jerárquicos de la institución. Sin embargo, pueden ser consideradas como partes interesadas para la gestión de riesgos de TI los siguientes grupos [16]:

- Junta y Dirección Ejecutiva
- Gestores de Riesgos
- Administrador de los riesgos Operacionales
- Dirección de TI
- Directores de servicios de TI
- Administrador de la continuidad de negocio
- Administrador de seguridad de TI
- CFOs (Chief Financial Officer – Gerente Financiero)
- Oficiales del gobierno organizacional
- Directores ejecutivos
- Auditores de TI
- Reguladores

- Auditores externos
- Aseguradores
- Agencias de calificación

2.3.3. Tareas relacionadas a la gestión de riesgos

La adecuada ejecución de la gestión de riesgos (aplicada también a la seguridad perimetral), conlleva la realización básica de las siguientes tareas [17]:

- Identificación y clasificación de los activos de información.
- Identificación y evaluación de los riesgos de información.
- Evaluación de impacto al negocio.
- Evaluación de amenazas y vulnerabilidades.
- Identificar y evaluar los controles y contramedidas para mitigar el riesgo a niveles aceptables.
- Integrar la identificación y gestión de riesgos, amenazas y vulnerabilidades dentro del ciclo de vida de los procesos.
- Reportar los cambios significativos en los riesgos a niveles de gestión apropiados para su aceptación.

2.3.4. Metodología para la gestión de riesgos tecnológicos

A fin de cumplir adecuadamente las tareas relacionadas a la gestión de riesgos, se deben utilizar metodologías basadas estándares como la ISO 31000 [18] e ISO/IEC 27005 [19].

Alexandra Ramirez y Zulima Ortiz [20], proponen una metodología para la gestión de riesgos tecnológicos basado en el modelo PHVA (Planificar, Hacer, Verificar, Actuar), la cual contempla las siguientes etapas:

- Establecimiento de un plan de comunicación interno y externo
- Definición del contexto organizacional interno y externo
- Valoración de riesgos tecnológicos
- Tratamiento de riesgos tecnológicos
- Monitoreo y mejora continua del proceso de gestión

2.3.4.1. Establecimiento de un plan de comunicación interno y externo

Consiste en establecer los conceptos y definiciones de los riesgos tecnológicos y sus consecuencias a fin de crear conciencia en seguridad; y a la vez, permite establecer e implementar los canales de comunicación adecuados para trasmitirlos a todas las partes interesadas tanto a nivel interno como externo.

2.3.4.2. Definición del contexto organizacional interno y externo

Permite conocer la organización y su contexto tanto interno (misión, visión, políticas, objetivos, estrategias, metas, etc.) como externo (competencia, regulaciones legales, economía, política, etc.) a fin de determinar los aspectos que la pudieran afectar, los elementos que se deben proteger, los recursos a utilizar para brindar protección y el nivel de aceptación del riesgo.

2.3.4.3. Valoración de riesgos tecnológicos

Consiste en la identificación de los activos de información que se deben proteger, las amenazas a las que están expuestos y el impacto que pudieran causar en caso de materializarse. En esta etapa también se identifican los controles (preventivos, correctivos, detectivos) que se deben aplicar para mitigar el riesgo.

2.3.4.4. Tratamiento de riesgos tecnológicos

Permite definir e implementar las acciones que minimicen los riesgos encontrados y valorados. Estas acciones pueden ser reducir (implementar controles), aceptar (reconocer el riesgo y monitorearlo), eliminar (evitar el riesgo) o transferir el riesgo (compartir el riesgo).

2.3.4.5. Monitoreo y mejora continua del proceso de gestión

Consiste en el control de cambios a través del monitoreo permanente sobre los activos, procesos, vulnerabilidades, amenazas, controles, políticas y procedimientos a fin de definir acciones frente a cambios como aumento de activos, aparición de nuevos riesgos y amenazas, actualizando contantemente la documentación relacionada a la gestión de riesgos y comunicarlos adecuadamente entre las partes interesadas.

2.4. Normativas utilizadas para la valoración y tratamiento de riesgos de seguridad perimetral

La implementación del esquema de seguridad perimetral en la red de datos de Financiera Lago Azul, está basada en los estándares ISO/IEC 27001:2013 [21], ISO ISO/IEC 27002:2013 [22] e ISO/IEC 27005:2008 [19].

La norma ISO/IEC 27001:2013 [21], establece los lineamientos adecuados para la correcta gestión de un sistema de gestión de seguridad de la información a través de la valoración y tratamiento de los riesgos (Numerales 8.2 y 8.3) relacionados a la seguridad perimetral.

El estándar ISO/IEC 27002:2013 [22]; a su vez, establece un conjunto de controles que permiten dar tratamiento a los riesgos una vez que estos hayan sido identificados y valorados por las organizaciones.

La norma que guía la administración de riesgos de seguridad de la información es la ISO/IEC 27005 [19], la cual establece el lineamiento a seguir para la evaluación y tratamiento de los riesgos que en este caso se aplica a la seguridad perimetral de la red de datos.

Los controles a ser implementados, dependen de los riesgos que la organización decida tratar o reducir luego de obtenidos los resultados de la valoración de riesgos.

CAPÍTULO 3

ANÁLISIS DE RIESGOS, VULNERABILIDADES Y AMENAZAS DE RED

3.1. Generalidades

De acuerdo a lo que establece la norma ISO/IEC 27001:2013 [21] en su numeral 6.1.1.; para el tratamiento de riesgos, se debe realizar un proceso de valoración de riesgos de seguridad de la información enfocados en mitigar aquellos relacionados a la pérdida de confidencialidad, integridad y disponibilidad de la información, identificando los dueños de los riesgos y estimando el impacto en caso de materializarse. La normativa ISO

27005:2008 [19], a su vez, establece una guía para la adecuada administración de los riesgos de seguridad de la información, la cual se toma de base para la presente valoración de riesgos.

3.2. Identificación de los activos de información

El numeral 8.2.1.2 de la normativa ISO 27005:2008 [19] establece la identificación de activos como el primer paso dentro del proceso de valoración de riesgos.

Para determinar los principales activos de información que deberán ser considerados para su protección ante posibles eventos o incidentes de seguridad perimetral, el Jefe de TI, realiza el levantamiento inicial de activos de información, el mismo que en base a una encuesta realizada a personal de rango jerárquico superior, complementa el proceso de identificación y establece la valoración de los mismos:

En la siguiente tabla, se muestra la clasificación inicial de los activos de información levantados por TI (Anexo A), que deben ser considerados para su protección ante posibles eventos o incidentes de seguridad perimetral:

Tabla 9. Activos de información asociados a la seguridad perimetral.

NRO	ACTIVO	DESCRIPCIÓN	TIPO	REPOSITORIO DE INFORMACION	RESPONSABLE	AREA
1	Base de datos	Motor de base de datos	Intangible	Servidor principal-pruebas	Jefe de TI	TI
2	Aplicaciones ERP – Web	Aplicaciones de Gestión de la institución	Intangible	Servidor principal	Jefe de TI	TI
3	Fuentes y ejecutables de los sistemas de gestión (ERP - Web)	Código fuente, archivos ejecutables e instaladores de aplicaciones.	Intangible	Servidor principal	Jefe de Desarrollo	TI
4	Respaldos	Archivos digitales que contienen copias de seguridad de información relevante (base de datos, aplicaciones, etc.)	Tangible	Cintas magnéticas	Jefe de TI	TI
5	Correos electrónicos	Correos institucionales del personal.	Intangible	Proveedor externo	Jefe de Infraestructura y redes	TI
6	Cortafuegos	Dispositivo físico de seguridad perimetral.	Tangible	Cortafuegos	Jefe de Infraestructura y redes	TI

7	Reglas de configuración perimetral	Reglas de filtrado que restringen o permiten el acceso a redes e internet	Intangible	Cortafuegos	Jefe de Infraestructura y redes	TI
8	Configuración de equipos de red	Archivos que contienen información de configuración de dispositivos de red.	Intangible	Equipos de red	Jefe de Infraestructura y redes	TI
9	Archivos digitales	Documentos de usuario.	Intangible	Equipos de usuario	Oficial de Riesgos	Riesgos
10	Servidores	Equipos especializados en brindar servicios: Base de datos, aplicaciones, internet, correo electrónico, respaldos, etc.	Tangible	Centro de datos	Jefe de Infraestructura y redes	TI

11	Instaladores (Software base)	Software y licenciamiento de: Sistemas operativos (servidores y clientes), controladores (equipos, impresoras, escáneres, etc.), bases de datos, herramientas de desarrollo, seguridad informática (antivirus, antispam, antimalware, etc.), ofimática (editores de texto, hojas de cálculo), editores gráficos y utilitarios.	Tangible	Caja de seguridad / Servidor de respaldos	Jefe de Infraestructura y redes	TI
12	Manuales técnicos de software y aplicaciones	Manuales y guías de instalación y/o configuración del software de la institución.	Tangible	Servidor principal	Jefe de Desarrollo	TI
13	Manuales de usuario	Manuales de usuario de las principales aplicaciones de la institución.	Tangible	Servidor principal	Jefe de Desarrollo	TI
14	Discos duros	Dispositivos de almacenamiento interno.	Tangible	Chasis de servidores	Jefe de Infraestructura y redes	TI

15	Cintas magnéticas de respaldo	Medios de almacenamiento externo de respaldos de información	Tangible	Caja de seguridad	Jefe de TI	TI
16	Bitácoras de TI	Registro de accesos, eventos y actividades del área de TI.	Tangible	Archivador metálico del área de Operaciones de TI	Jefe de TI	TI
17	Central telefónica IP	Equipos y aplicaciones de telefonía IP	Tangible	Centro de datos	Jefe de Infraestructura y redes	TI
18	Cableado estructurado	Medio físico de transmisión de datos	Tangible	Ductos y canaletas de cableado estructurado	Jefe de Infraestructura y redes	TI
19	UPS	Dispositivo de suministro eléctrico contingente	Tangible	Centro de datos	Jefe de Infraestructura y redes	TI

3.3. Valoración de los activos de información

El numeral 8.2.1.3 de la normativa ISO 27005:2008 [19] establece la identificación de potenciales amenazas que pudieran comprometer o dañar los principales activos de información. Los criterios utilizados para valorar los activos de información, se muestra en la siguiente tabla:

Tabla 10. Criterios de valoración de activos de información.

ELEMENTO	NRO	CRITERIO	ESPECIFICACIÓN
INTEGRIDAD	1	Nulo	Los objetivos de la empresa no se ven afectados en caso de que el activo sea comprometido en su integridad.
	2	Bajo	Es probable que los objetivos de la empresa se vean afectados en caso de que el activo sea comprometido en su integridad.
	3	Medio	Si se compromete la integridad del activo, se retrasará el cumplimiento de los objetivos de la empresa.
	4	Alto	Si se compromete la integridad del activo no se cumplirá con los objetivos de la empresa.
	5	Catastrófico	Si se compromete la integridad del activo, se perderá la confianza de los inversionistas, proveedores y/o clientes.
CONFIDENCIALIDAD	1	Nulo	Los objetivos de la empresa no se ven afectados en caso de que el activo de información esté extremadamente expuesto para su acceso a personal externo e interno.

	2	Bajo	Los objetivos de la empresa no se ven afectados en caso de que el activo de información esté expuesto a personal externo (clientes, proveedores o personal de la empresa).
	3	Medio	Los objetivos de la empresa no se ven afectados en caso de que el activo de información esté expuesto a todo el personal interno.
	4	Alto	Los objetivos de la empresa no se ven afectados en caso de que el activo de información esté expuesto solo a personal involucrado en el proceso.
	5	Catastrófico	Los objetivos de la empresa no se ven afectados en caso de que el activo de información esté expuesto al personal estrictamente necesario.
DISPONIBILIDAD	1	Nulo	Los objetivos de la empresa no se ven afectados en caso de que el activo sea comprometido o no se encuentre disponible.
	2	Bajo	Es probable que los objetivos de la empresa se vean afectados en caso de que el activo sea comprometido o no se encuentre disponible.

	3	Medio	Si se compromete el activo o no se encuentra disponible, se retrasará el cumplimiento de los objetivos de la empresa.
	4	Alto	Si se compromete el activo o no se encuentra disponible no se cumplirá con los objetivos de la empresa.
	5	Catastrófico	Si se compromete el activo o no se encuentra disponible, no se cumplirá con los objetivos de la Empresa, se perderá la confianza de los inversionistas, proveedores y/o clientes.

Para definir el valor del activo de información respecto de las potenciales amenazas, se han establecido los siguientes rangos:

Tabla 11. Rangos de valoración de activos de información.

RANGO	VALOR DEL ACTIVO
1 – 5	BAJO
6 – 10	MEDIO
11 – 15	ALTO

El análisis de potenciales amenazas sobre los activos de información, se realiza tomando una muestra de nueve personas que participaron en la encuesta de valoración de activos de información (ANEXO B). Los resultados se indican en la tabla siguiente:

Tabla 12. Valoración de los activos de información.

NRO	ACTIVO	AMENAZAS	INTEGRIDAD	CONFIDENCIALIDAD	DISPONIBILIDAD	TOTAL	VALOR
1	Base de datos	1. Accesos no autorizados. 2. Modificación/Eliminación no autorizada de datos. 3. Denegación de servicio de base de datos. 4. Errores operativos de gestión de base de datos. 5. Generación de respaldos corruptos. 6. Catástrofe natural. 7. Catástrofe provocada por terceros	4	5	5	14	ALTO
2	Aplicaciones ERP - Web	1. Accesos no autorizados. 2. Modificación/Eliminación no autorizada de datos. 3. Denegación de servicio de base de datos. 4. Filtración de información confidencial. 5. Catástrofe natural. 6. Catástrofe provocada por terceros	3	3	3	9	MEDIO

3	Fuentes y ejecutables de los sistemas de gestión (ERP - Web)	1. Código programado con brechas de seguridad. 2. Modificación/Eliminación no autorizada de líneas de código. 3. Catástrofe natural. 4. Catástrofe provocada.	1	2	1	4	BAJO
4	Respaldos	1. Accesos no autorizados. 2. Daño intencional en los archivos de respaldo. 3. Modificación/Eliminación no autorizados. 4. Respaldos desactualizados. 5. Catástrofe natural. 6. Catástrofe provocada.	1	1	1	3	BAJO
5	Correos electrónicos	1. Accesos no autorizados. 2. Suplantación de identidad. 3. Modificación/Eliminación no autorizados.	1	2	1	4	BAJO
6	Cortafuegos	1. Accesos no autorizados. 2. Modificación/Eliminación no autorizado de configuración. 3. Ataques de día cero. 4. Desactivación de reglas de filtrado y protección antimalware. 5. Ataques externos. 6. Ataques de denegación de servicios. 7. Ausencia de dispositivo de protección perimetral (daño total o parcial).	4	4	4	12	ALTO
7	Reglas de configuración perimetral	1. Accesos no autorizados. 2. Modificación/Eliminación no autorizados.	3	3	3	9	MEDIO

8	Configuración de equipos de red	1. Accesos no autorizados. 2. Modificación/Eliminación no autorizado. 3. Errores operativos de configuración. 4. Daño físico. 5. Catástrofe natural. 6. Catástrofe provocada.	2	2	3	7	MEDIO
9	Archivos digitales	1. Accesos no autorizados. 2. Modificación/Eliminación no autorizados. 3. Catástrofe natural. 4. Catástrofe provocada.	5	5	5	15	ALTO
10	Servidores	1. Accesos no autorizados. 2. Daño físico de partes y componentes. 3. Catástrofe natural. 4. Catástrofe provocada.	4	4	4	12	ALTO
11	Instaladores (Software base)	1. Accesos no autorizados. 2. Sustracción de medios. 3. Daño físico medios. 4. Caducidad de licencias sin renovación. 5. Catástrofe natural. 6. Catástrofe provocada.	1	1	1	3	BAJO
12	Manuales técnicos de software y aplicaciones	1. Accesos no autorizados. 2. Sustracción de documentos. 3. Daño físico. 4. Catástrofe natural. 5. Catástrofe provocada.	1	1	1	3	BAJO
13	Manuales de usuario	1. Accesos no autorizados. 2. Sustracción de documentos. 3. Daño físico. 4. Catástrofe natural. 5. Catástrofe provocada.	1	1	1	3	BAJO
14	Discos duros	1. Daño físico. 2. Espacio insuficiente. 3. Bajo rendimiento.	2	3	2	7	MEDIO

15	Cintas magnéticas de respaldo	1. Accesos no autorizados. 2. Daño físico.	1	1	1	3	BAJO
16	Bitácoras de TI	1. Accesos no autorizados. 2. Daño físico.	1	1	1	3	BAJO
17	Central telefónica IP	1. Accesos no autorizados. 2. Daño físico.	1	1	1	3	BAJO
18	Cableado estructurado	1. Accesos no autorizados. 2. Daño físico.	1	1	1	3	BAJO
19	UPS	1. Accesos no autorizados. 2. Daño físico.	1	1	1	3	BAJO
20	Impresoras	1. Accesos no autorizados. 2. Daño físico.	1	1	1	3	BAJO

3.4. Valoración de riesgos del cortafuegos perimetral

Las amenazas de afectación a los activos de información pueden materializarse cuando las vulnerabilidades presentes no han sido tratadas para mitigar el riesgo inherente. El numeral 8.2.1.5 de la normativa ISO 27005:2008 [19] establece que se debe realizar la identificación de vulnerabilidades que de ser explotadas y materializadas podrían comprometer o dañar los principales activos de información.

El cortafuegos institucional comprende el activo más importante dentro de la seguridad perimetral de la red de datos, ya que al ser víctima de un ataque de seguridad y materializarse efectivamente, podría comprometer todos los demás activos de información que componen la red interna de la organización.

La valoración de riesgos del cortafuegos perimetral, se realiza en base a una encuesta tomando una muestra de diez personas (ANEXO C). Los criterios de valoración y resultados, se indican en las siguientes tablas:

Tabla 13. Criterios de valoración de probabilidades

NRO	CRITERIO	ESPECIFICACIÓN
1	Muy baja	Mínima o ninguna probabilidad de ocurrencia
2	Baja	Poca probabilidad de ocurrencia
3	Medio	Aceptable probabilidad de ocurrencia
4	Alta	Alta probabilidad de ocurrencia
5	Muy alta	Máxima o segura probabilidad de ocurrencia

Tabla 14. Criterios de valoración de impacto

NRO	CRITERIO	ESPECIFICACIÓN
1	Nulo	Los objetivos de la empresa no se ven afectados en caso de que el activo sea comprometido o no se encuentre disponible.

2	Bajo	Es probable que los objetivos de la empresa se vean afectados en caso de que el activo sea comprometido o no se encuentre disponible.
3	Medio	Si se compromete el activo o no se encuentra disponible, se retrasará el cumplimiento de los objetivos de la empresa.
4	Alto	Si se compromete el activo o no se encuentra disponible no se cumplirá con los objetivos de la empresa.
5	Catastrófico	Si se compromete el activo o no se encuentra disponible, no se cumplirá con los objetivos de la empresa, se perderá la confianza de los inversionistas, proveedores y/o clientes.

Tabla 15. Valoración de riesgos del cortafuegos perimetral

ACTIVO	TIPIFICACION RIESGO	RIESGO EVALUADO	PROBABILIDAD	IMPACTO
CORTFUEGOS PERIMETRAL	R1	Accesos no autorizados	3	4
	R2	Modificación / Eliminación no	2	4
	R3	Ataques de día cero	2	4
	R4	Desactivación de reglas de filtrado y	3	4
	R5	Ataques externos	3	5
	R6	Ataques de denegación de	2	4
	R7	Ausencia de dispositivo de protección	2	4

3.5. Mapa de calor de riesgos

A continuación se muestra gráficamente el mapa de calor de riesgos del cortafuegos perimetral:

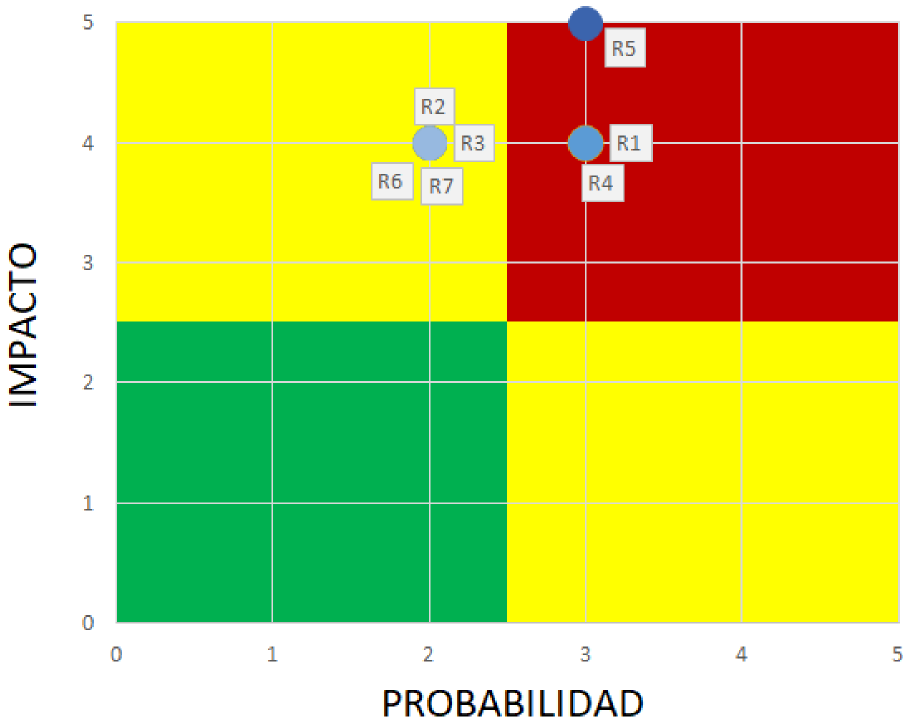


Figura 3.1 Mapa de calor de riesgos del cortafuegos perimetral

Como se puede apreciar en la matriz de calor, el principal riesgo que requiere ser tratado es el relacionado a ataques externos.

CAPÍTULO 4

ANÁLISIS Y DISEÑO DE UN ESQUEMA DE SEGURIDAD PERIMETRAL

4.1. Políticas de seguridad perimetral

4.1.1. Definición de políticas

A fin de reducir las incidencias de seguridad y solucionar los problemas detectados, se definen políticas apegadas a las normas ISO 27001 e ISO 27002, que constituyen los lineamientos de seguridad perimetral que Financiera Lago

Azul debe considerar incluir en su actual esquema de seguridad informática.

Una vez que las políticas, procedimientos y controles de seguridad perimetral sean incluidos en el esquema de seguridad informática de Financiera Lago Azul, se deberán aplicar los controles establecidos y difundirlos a todo el personal involucrado, para que puedan ser cumplidos.

4.1.2. Selección y definición de dominios, controles y políticas de seguridad perimetral

Para el tratamiento de los riesgos relacionados a la seguridad perimetral de la red, tomando como referencia la norma ISO/IEC 27002:2013 [21], dentro del análisis realizado se considera que Financiera Lago Azul necesita la implementación de los siguientes controles y políticas:

Tabla 16. Controles aplicables a la seguridad perimetral de la red.

DOMINIO	OBJETIVO	CONTROL
8. GESTION DE ACTIVOS (Red perimetral de datos y equipos internos a proteger)	8.1. Responsabilidad sobre los activos	8.1.1. Inventario de activos

9. CONTROL DE ACCESOS (red perimetral de datos)	9.1. Requisitos de negocio para el control de accesos.	9.1.1. Política de control de accesos
	9.2. Gestión de acceso de usuario.	9.2.2. Gestión de los derechos de
		9.2.3. Gestión de los derechos de
		9.2.4. Gestión de información confidencial de
	9.4. Control de acceso a sistemas y aplicaciones.	9.4.1. Restricción del acceso a la
		9.4.2 Procedimientos
		9.4.3. Gestión de contraseñas de
10. CIFRADO. (Red perimetral de datos)	10.1. Controles criptográficos	10.1.1. Política de uso de los
12. SEGURIDAD OPERATIVA. (Red perimetral de datos)	12.3. Copias de seguridad.	12.3.1. Copias de seguridad de
	12.4. Registro de actividad y supervisión	12.4.4. Sincronización de relojes.
13. SEGURIDAD EN LAS TELECOMUNICACIONES (Red perimetral de datos)	13.1. Gestión de la seguridad en las redes.	13.1.1. Controles de red.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	17.2. Redundancias.	17.2.1. Disponibilidad de instalaciones para el procesamiento de la información.

4.1.3. Inventario de activos

Con el objetivo de proteger los activos de información de la institución, estos deben ser adecuadamente identificados y asignados a sus respectivos responsables. Las siguientes políticas permitirán mantener una gestión razonable de los activos de información relacionados a la seguridad perimetral:

a) El Jefe de TI es el responsable de inventariar los activos de información relacionados a la seguridad perimetral y asignar a la persona encargada de su administración y custodia.

b) El responsable asignado se encargará de clasificar, etiquetar y documentar los activos de información, estableciendo y monitoreando periódicamente el cumplimiento de la contratación tanto de renovación de licencias como de soporte técnico.

c) El responsable se encargará de realizar la evaluación periódica del estado de los activos de información, comunicando al Jefe de TI acerca de las observaciones encontradas.

d) El Jefe de TI autorizará la ejecución de mantenimientos, cambios o actualización de componentes, reclasificación y baja de activos.

e) El responsable se encargará de obtener y guardar de forma segura los respaldos de la información sensible contenida en los activos de información y a la vez eliminarlos del activo cuando este deba ser trasladado a terceros o requiera ser dado de baja.

4.1.4. Política de control de accesos

El acceso a los activos de información constituye un elemento crítico de seguridad; en tal virtud, se han definido las siguientes políticas que debe contemplar la empresa financiera Lago Azul:

a) El acceso a los activos de información perimetral debe ser realizado utilizando medios de transmisión o canales seguros.

b) Se debe implementar la creación de contraseñas seguras de mínimo 8 caracteres que incluyan números, letras en mayúsculas y minúsculas; así como también caracteres especiales.

c) Todos los dispositivos, servidores y aplicaciones de seguridad perimetral deben solicitar credenciales de autenticación seguras para su acceso.

d) Se debe establecer y definir una adecuada segregación de funciones y roles de tal manera que los usuarios puedan acceder únicamente a los recursos a los cuales tienen autorización.

e) Todo acceso a los activos de información perimetral, debe contar con el registro de auditorías o logs que permita identificar a los usuarios registrados y las acciones realizadas.

f) Se debe implementar el bloqueo automático de sesiones inactivas abiertas por un lapso superior a 30 minutos en todo activo de información perimetral que permita esta funcionalidad.

g) Se debe implementar un control de vídeo vigilancia que registre el acceso físico al centro de datos.

h) El acceso físico al centro de datos debe contar con la autorización del Jefe de TI, registrando una bitácora de identificación y actividades realizadas en el interior del centro de datos.

4.1.5. Gestión de los derechos de acceso asignados a usuarios

a) La Jefatura de TI conjuntamente con Infraestructura y Redes definirán los roles de acceso a los diferentes equipos y dispositivos, los cuales delimitarán las acciones a realizar a los usuarios dependiendo de sus perfiles de acceso.

b) Cuando ingresa un nuevo recurso a la institución y se defina que debe tener un perfil que requiera acceso a los sistemas, equipos y dispositivos de la red perimetral, se deberá llenar un formulario de solicitud de accesos, el mismo que deberá ser aprobado y autorizado por la Jefatura de TI y por Infraestructura y Redes previo a su asignación.

c) Talento Humano deberá notificar a TI formalmente la salida de cada recurso de la institución, quienes a su vez procederán a deshabilitar todos los permisos al funcionario saliente.

4.1.6. Gestión de los derechos de acceso con privilegios especiales

a) Las contraseñas de súper usuario o también conocido como usuario de máximos privilegios, la deberán administrar únicamente el Jefe de TI y el Jefe de Infraestructura y Redes siendo responsables de su adecuada utilización.

b) Las contraseñas asignadas a los proveedores de servicios de tecnología, deberán ser cambiadas una vez que los mismos hayan culminado sus actividades de instalación, soporte y mantenimiento.

c) TI conjuntamente con Riesgos, se encargarán de que las contraseñas de súper usuario se almacenen en sobre cerrado y en la caja de seguridad de la institución.

d) Para la apertura del sobre cerrado en caso de que se requiera la actualización de contraseñas o su utilización, se deberá contar con la autorización expresa del Gerente General y participarán en el proceso de apertura conjuntamente las áreas de TI y Riesgos.

4.1.7. Gestión de información confidencial de autenticación de usuarios

a) Tanto el personal interno de la institución como el personal externo (proveedores) deberán firmar un acuerdo de confidencialidad de la información reservada y sensible, incluidos los privilegios y contraseñas encomendadas.

b) Cuando las contraseñas de acceso a los sistemas sean provistos por un administrador de aplicaciones, los sistemas deberán obligar al usuario a cambiar la contraseña luego del primer inicio de sesión.

4.1.8. Restricción del acceso a la información

Implementar reglas de navegación web en el proxy perimetral de acuerdo a la segregación de funciones establecida en la institución.

4.1.9. Procedimientos seguros de inicio de sesión

a) Implementar la definición de tres oportunidades de acceso a los sistemas y dispositivos perimetrales. Al tercer intento fallido bloquear al usuario por un lapso de dos horas y remitir por correo electrónico la alerta de intentos fallidos a los usuarios administradores

b) En los dispositivos y equipos perimetrales, definir la visualización de la fecha y hora del último acceso correcto y la fecha y hora del último intento de acceso fallido.

4.1.10. Gestión de contraseñas de usuarios

a) Permitir a los usuarios realizar los cambios únicamente de sus contraseñas.

b) Implementar en los dispositivos y equipos perimetrales el uso de contraseñas seguras.

c) No desplegar las contraseñas en la pantalla de registro de claves.

4.1.11. Política de uso de los controles criptográficos

Definir una política de uso de cifrado basado en llaves pública y privada para proteger los documentos sensibles (contratos, calendarios de mantenimiento, entre otros) durante su intercambio y transporte.

4.1.12. Copias de seguridad de la información

El Jefe de TI debe:

a) Definir los elementos de la red perimetral que requieran la obtención de copias de seguridad (archivos de configuración, guías de instalación y mantenimiento, logs, bases de datos, etc.) que permitan soportar procesos contingentes.

b) Establecer la periodicidad de la obtención de las copias de seguridad.

c) En conjunto con Riesgos definir el tiempo de custodia de los respaldos y la ubicación externa a la institución en la que almacenarán los respaldos.

d) Definir un calendario de anual de pruebas de calidad de respaldos para verificar que los mismos se estén obteniendo y almacenando adecuadamente.

4.1.13. Sincronización de relojes

Los equipos y dispositivos de la red perimetral deberán contar con sus relojes sincronizados con una fuente que proporcione la hora exacta, a fin de garantizar la exactitud tanto de registro de operaciones como de bitácoras (logs) de auditoría.

4.1.14. Controles de red

Para proteger la información que se transmite a través de las redes de comunicación, se han definido las siguientes políticas:

a) El Jefe de TI designará un responsable de administrar las redes y comunicaciones de la institución.

b) El administrador de redes y comunicaciones elaborará e implementará procedimientos de administración y manejo de los equipos de red y comunicaciones.

c) El administrador de redes deberá registrar una bitácora de los procesos y observaciones encontradas durante la ejecución de mantenimientos (preventivo/correctivo) de los elementos de red y comunicaciones.

d) El administrador de redes, periódicamente evaluará el rendimiento de los elementos de red y comunicaciones a fin de realizar proyecciones de incremento de capacidad futura.

4.1.15. Disponibilidad de instalaciones para el procesamiento de la información

a) Se debe realizar la gestión necesaria para disponer de un Centro de Datos alterno con enlaces redundantes al Centro de Datos principal y hacia internet para garantizar la continuidad de operaciones en caso de que el Centro de Datos principal no se encuentre operativo.

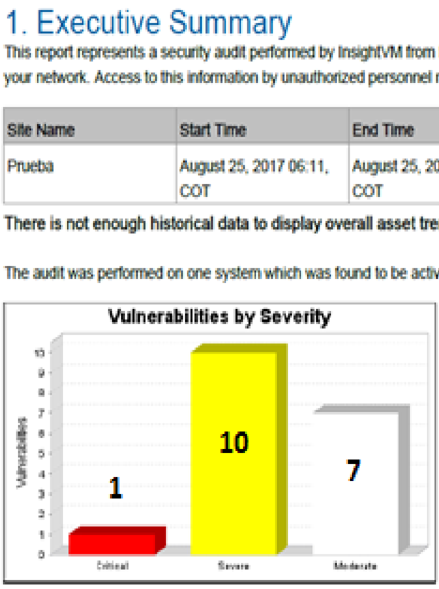
b) El Centro de Datos alterno deberá contar con la infraestructura y configuraciones similares a las del Centro de Datos principal con el objetivo de reducir los tiempos de puesta en operación del sitio alterno.

4.2. Servidor web

4.2.1. Análisis de vulnerabilidades

Con la finalidad de definir los controles a implementar en el esquema de seguridad perimetral, se realiza un análisis de vulnerabilidades en el servidor web publicado, el mismo que permite visualizar las falencias de seguridad perimetral que podrían ser aprovechados para la materialización de ataques externos.

Para la realización del análisis de vulnerabilidades (ANEXO D), se utiliza el software InsightVM de Rapid7 LLC, cuya versión de evaluación limita la generación de un reporte impreso con todas las vulnerabilidades que se muestran en pantalla.



1. Executive Summary

This report represents a security audit performed by InsightVM from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
Prueba	August 25, 2017 06:11, COT	August 25, 2017 06:23, COT	12 minutes	Success

There is not enough historical data to display overall asset trend.

The audit was performed on one system which was found to be active and was scanned.

Figura 4.1 Reporte inicial de vulnerabilidades en el servidor web

La vulnerabilidad que se debe priorizar en atender es la que se encuentra en nivel crítico y está relacionada a la base de datos, la misma que se encuentra obsoleta y sin soporte por parte del fabricante.

3.1. Critical Vulnerabilities

3.1.1. Microsoft SQL Server Obsolete Version (mssql-obsolete-version)

Description:

An obsolete version of the Microsoft SQL database server is running. Note: When the support period ends for a Microsoft SQL Server product, no further patches will be provided even for serious security problems.

Affected Nodes:

Affected Nodes:	Additional Information:
186[redacted]12:1433	Running TDS serviceProduct SQL Server 2008 found in fingerprint is not SQL Server 2000Product SQL Server 2008 found in fingerprint is not SQL Server 2005Product SQL Server 2008 exists -- Microsoft SQL Server 2008 10.0.1600 Vulnerable version of product SQL Server 2008 found -- Microsoft SQL Server 2008 10.0.1600

References:

Source	Reference
URL	https://support.microsoft.com/en-us/lifecycle/search?alpha=SQL%20Server

Figura 4.2 Vulnerabilidad crítica en el servidor web

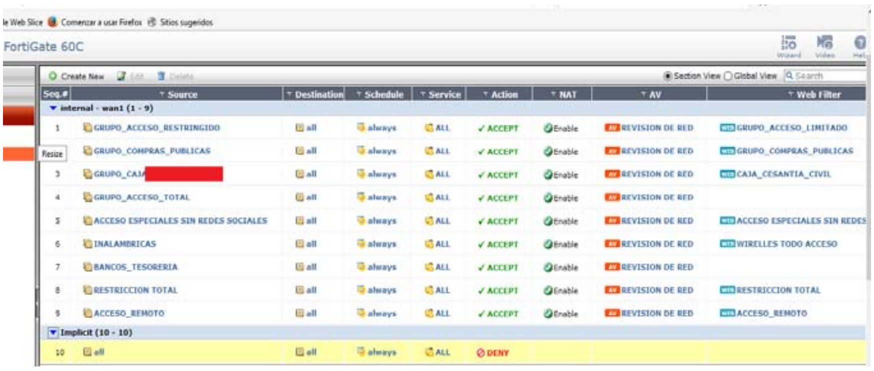
4.2.2. Diseño de mitigación de vulnerabilidades

Como parte de la mitigación de la vulnerabilidad crítica encontrada, se plantea la apertura de una ventana de mantenimiento programada para la realización de la actualización de la base de datos a una versión con soporte por parte del fabricante.

4.3. Cortafuegos perimetral

4.3.1. Análisis de configuración y reglas de filtrado

Se realiza un análisis de la configuración de reglas de filtrado definidas en el cortafuegos perimetral, a fin de establecer recomendaciones que podrán ser implementadas por la empresa, para fortalecer las capacidades de protección ante eventuales accesos no autorizados y ataques externos.



Seq.#	Source	Destination	Schedule	Service	Action	NAT	AV	Web Filter
internal - wan1 (1 - 9)								
1	GRUPO_ACCESO_RESTRINGIDO	all	always	ALL	ACCEPT	Enable	REVISION DE RED	GRUPO_ACCESO_LIMITADO
2	GRUPO_COMPRAS_PUBLICAS	all	always	ALL	ACCEPT	Enable	REVISION DE RED	GRUPO_COMPRAS_PUBLICAS
3	GRUPO_CAJ[redacted]	all	always	ALL	ACCEPT	Enable	REVISION DE RED	CAJA_CESANTIA_CIVIL
4	GRUPO_ACCESO_TOTAL	all	always	ALL	ACCEPT	Enable	REVISION DE RED	
5	ACCESO ESPECIALES SIN REDES SOCIALES	all	always	ALL	ACCEPT	Enable	REVISION DE RED	ACCESO ESPECIALES SIN REDES
6	INALAMBRICAS	all	always	ALL	ACCEPT	Enable	REVISION DE RED	WIRELLES TODO ACCESO
7	BANCOS_TESORERIA	all	always	ALL	ACCEPT	Enable	REVISION DE RED	
8	RESTRICCION TOTAL	all	always	ALL	ACCEPT	Enable	REVISION DE RED	RESTRICCION TOTAL
9	ACCESO_REMOTO	all	always	ALL	ACCEPT	Enable	REVISION DE RED	ACCESO_REMOTO
Implicit (10 - 10)								
10	all	all	always	ALL	DENY			

Figura 4.3 Reglas de filtrado del Cortafuegos perimetral

En la configuración revisada, se observa que las reglas han sido agrupadas en segmentos de acuerdo a grupos o áreas de trabajo comunes, con aplicación de reglas de filtrado de contenido web.

4.3.2. Diseño de configuración y reglas de filtrado

Considerando las reglas de filtrado existentes, se deberán incorporar al cortafuegos los siguientes elementos a fin de fortalecer el nivel de protección perimetral:

a) Establecer reglas de acceso entrante

b) Definir restricciones de acceso a la consola de administración del cortafuegos

c) Incorporar mecanismos de contraseñas seguras a los usuarios de administración del cortafuegos o en su defecto, integrar la autenticación con el Directorio Activo.

d) Implementar políticas de respaldo periódico de las reglas de filtrado configuradas.

e) Implementar el acceso a la consola de administración de manera segura (HTTPS)

f) Certificar los respaldos realizados para garantizar su aplicación.

4.4. Protección contra ataques de intrusión y denegación de servicios

4.4.1. Análisis de detección y protección contra intrusos

Luego de la revisión de las políticas de seguridad del cortafuegos perimetral de la empresa Financiera Lago Azul, se pudo evidenciar que uno de los puntos vulnerables es la ausencia de mecanismos de detección y protección contra intrusos en el servidor web.

El no contar con mecanismos oportunos de detección y protección de intrusos, podría ocasionar que se materialicen de manera efectiva tanto ataques de intrusión como de denegación de servicios, lo que podría generar consecuencias negativas para la empresa.

Dentro del esquema de detección y protección contra intrusos, se ha considerado la evaluación e implementación de reglas que permitan mitigar los riesgos de seguridad perimetral basados en los siguientes escenarios:

a) Ping de la muerte

b) Conectividad remota SSH

c) Ataque de inundación SYN

d) Escaneo de puertos

4.4.2. Diseño de esquema de detección y protección contra intrusos

Para mitigar el riesgo de ataques de intrusión y denegación de servicios en Financiera Lago Azul, se ha definido la implementación de un sistema IDS-IPS basado en Sistema Operativo Ubuntu, Software de detección de intrusos Snort y la implementación de reglas de protección basados en Iptables.

El IPS-IDS Ubuntu, será colocado entre el Cortafuegos perimetral y el servidor web, permitiendo fluir todo el tráfico entrante y saliente; y a la vez, bloqueando el tráfico considerado como malicioso (definido en reglas Iptables), manteniendo registros de intentos de ataques externos (IDS Snort) para su posterior análisis.

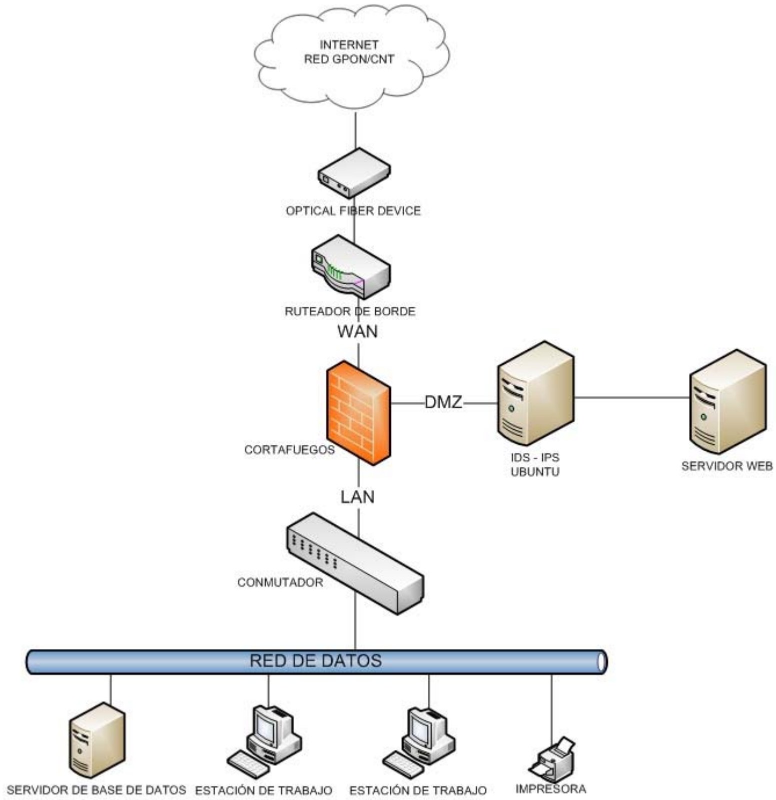


Figura 4.4 Diseño de solución de detección y protección contra intrusos

CAPÍTULO 5

PRUEBAS E IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD PERIMETRAL

5.1. Implementación de acciones mitigantes en servidor Web

Para mitigar la vulnerabilidad crítica encontrada durante la fase de análisis efectuado, se procedió a abrir una ventana de mantenimiento con el proveedor de base de datos, en la que se realizó la actualización de versión y aplicación de parches, con lo que la vulnerabilidad crítica fue mitigada, lo que se refleja en los resultados de un nuevo análisis de vulnerabilidades realizado (ANEXO E):

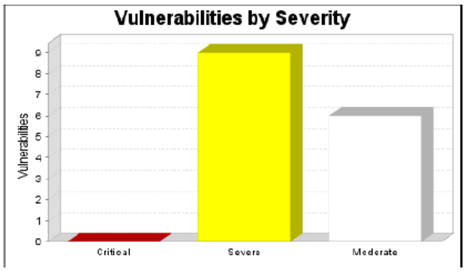
1. Executive Summary

This report represents a security audit performed by InsightVM from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
Prueba	September 02, 2017 03:15, COT	September 02, 2017 03:23, COT	7 minutes	Success

There is not enough historical data to display overall asset trend.

The audit was performed on one system which was found to be active and was scanned.



There were 15 vulnerabilities found during this scan. No critical vulnerabilities were found. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 9 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 6 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.

Figura 5.1 Reporte final de vulnerabilidades en el servidor web

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

No critical vulnerabilities were reported.

Figura 5.2 Vulnerabilidad crítica mitigada en el servidor web

5.2. Implementación y evaluación de IDS-IPS en ambiente de pruebas

5.2.1. Esquema de evaluación del IDS-IPS

A fin de probar la funcionalidad del IDS-IPS previo a su implementación en la empresa Financiera Lago Azul, se ha establecido el siguiente esquema de evaluación y pruebas:

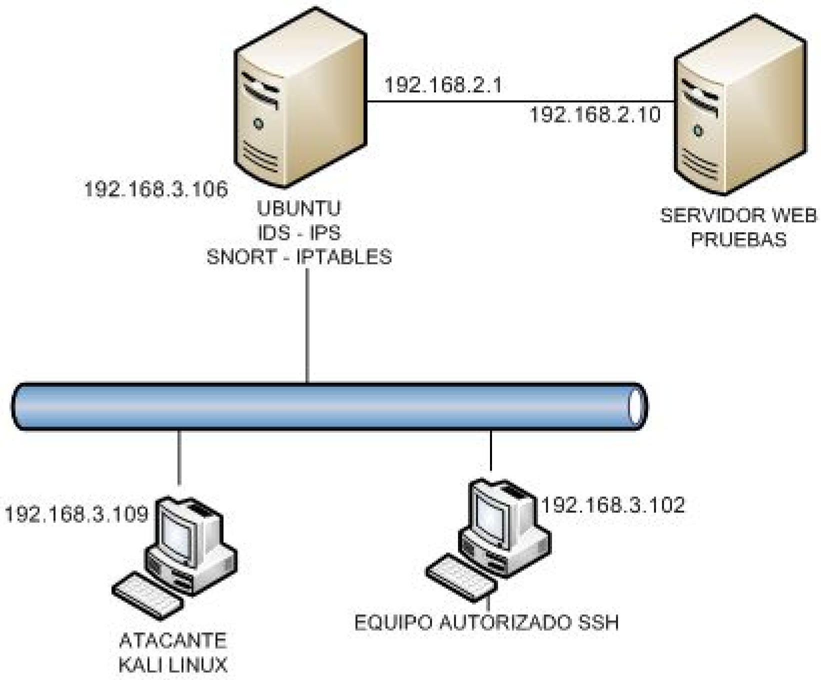


Figura 5.3 Esquema del ambiente de evaluación del IDS-IPS (Snort-Iptables)

En este esquema se define un servidor Ubuntu, en el cual se configurarán las herramientas necesarias a fin de que trabaje como un IDS-IPS, detectando escenarios de ataques externos y a la vez tomando las acciones de protección respectivas.

En este ambiente de evaluación, se han definido dos redes. La primera corresponde a la red interna de la empresa, la cual tiene un servidor web, brindando servicios de aplicaciones web. La segunda red corresponde a la red externa o internet, desde la cual se pueden realizar ataques ya sea al cortafuegos perimetral o al servidor web expuesto.

A continuación, se resume el esquema de direccionamiento del ambiente de evaluación descrito:

Tabla 17. Esquema de direccionamiento en ambiente de pruebas.

EQUIPO	INTERFAZ OBJETIVO	DIRECCIÓN IP OBJETIVO	MÁSCARA DE SUBRED
SERVIDOR IDS-IPS UBUNTU	wlan0	192.168.3.106	255.255.255.0
SERVIDOR IDS-IPS UBUNTU	p2p1	192.168.2.1	255.255.255.0
EQUIPO ATACANTE KALI - LINUX	eth0	192.168.3.109	255.255.255.0
EQUIPO AUTORIZADO SSH	eth0	192.168.3.102	255.255.255.0
SERVIDOR WEB PRUEBAS	eth0	192.168.2.10	255.255.255.0

5.2.2. Evaluación de afectación previa a la implementación protección IDS-IPS

Previo a la implementación de protección y configuración de reglas de protección en el IDS-IPS, se verifica que los escenarios de riesgo establecidos pueden ser materializados de forma efectiva:

5.2.2.1. Afectación por ataque ping de la muerte

Antes de proceder a configurar el IDS-IPS contra ataques ping de la muerte, se verifica que este tipo de ataque es susceptible de materializarse; para lo cual, previamente se procede a configurar su detección utilizando la herramienta SNORT:

Figura 5.4 Archivo de configuración de reglas de detección Snort

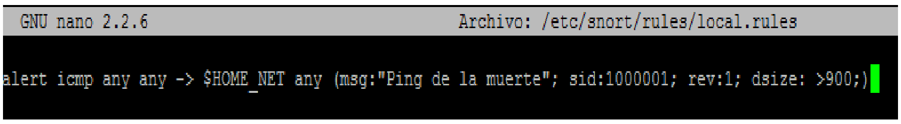


Figura 5.5 Configuración de regla de detección ping de la muerte

Se procede a levantar la detección por consola en el servidor IDS-IPS para visualizar ataques ping de la muerte

Figura 5.6 Comando de activación de detección de regla ping de la muerte

Se realiza la verificación de conectividad hacia la interfaz de red del servidor IDS-IPS Ubuntu:

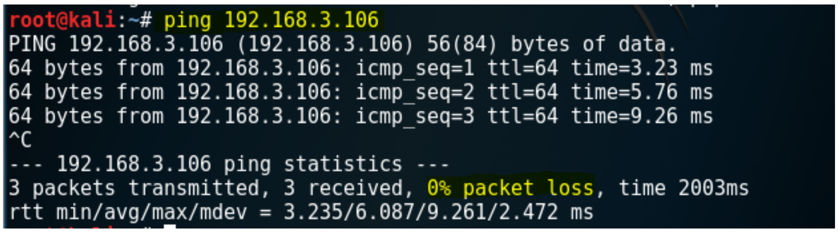


Figura 5.7 Verificación de conectividad hacia el servidor IDS-IPS Ubuntu

En la herramienta de captura de paquetes Wireshark se confirma la conectividad entre el equipo atacante y el servidor víctima:

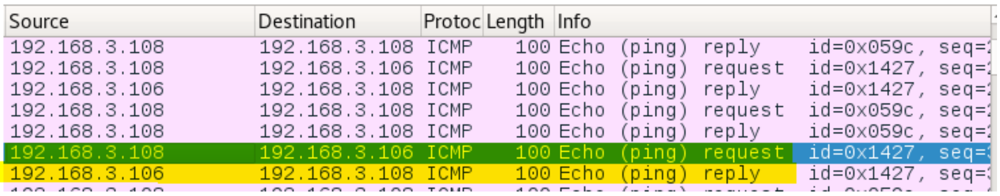


Figura 5.8 Verificación de conectividad mediante la herramienta Wireshark

Se procede a realizar la materialización del ataque (ping de la muerte):

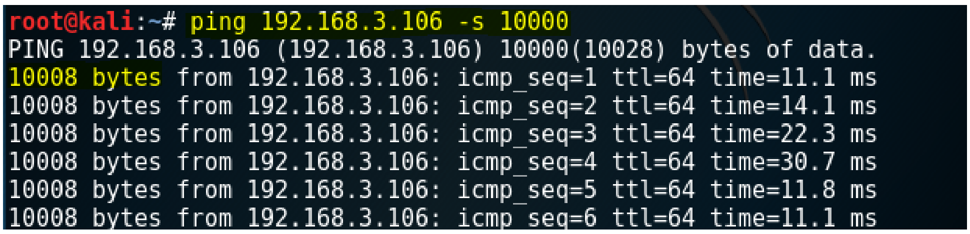
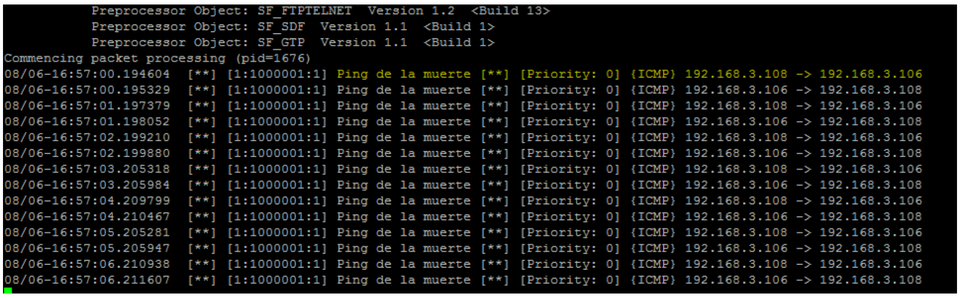


Figura 5.9 Materialización de ataque ping de la muerte (ambiente de pruebas)

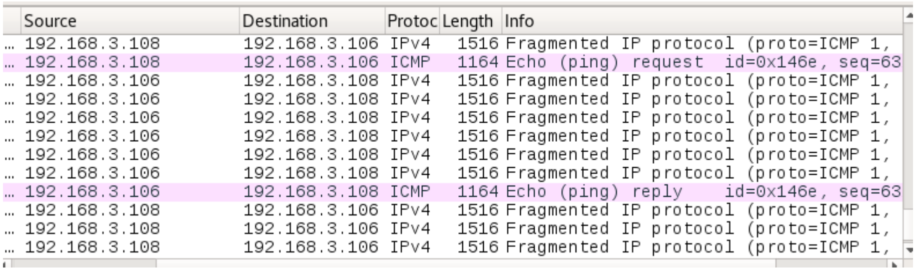
Se verifica la detección de ataque (Snort)



```
            Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
            Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
            Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
Commencing packet processing (pid=1676)
08/06-16:57:00.194604  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.108 -> 192.168.3.106
08/06-16:57:00.195329  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.106 -> 192.168.3.108
08/06-16:57:01.197379  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.108 -> 192.168.3.106
08/06-16:57:01.198052  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.106 -> 192.168.3.108
08/06-16:57:02.199210  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.108 -> 192.168.3.106
08/06-16:57:02.199880  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.106 -> 192.168.3.108
08/06-16:57:03.205318  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.108 -> 192.168.3.106
08/06-16:57:03.205984  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.106 -> 192.168.3.108
08/06-16:57:04.209799  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.108 -> 192.168.3.106
08/06-16:57:04.210467  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.106 -> 192.168.3.108
08/06-16:57:05.205281  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.108 -> 192.168.3.106
08/06-16:57:05.205947  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.106 -> 192.168.3.108
08/06-16:57:06.210938  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.108 -> 192.168.3.106
08/06-16:57:06.211607  [**] [1:1000001:1] Ping de la muerte [**] [Priority: 0] {ICMP} 192.168.3.106 -> 192.168.3.108
```

Figura 5.10 Detección de ataque ping de la muerte (ambiente de pruebas)

A través del analizador de paquetes se confirma el tráfico atacante



	Source	Destination	Protoc	Length	Info
…	192.168.3.108	192.168.3.106	IPv4	1516	Fragmented IP protocol (proto=ICMP 1,
…	192.168.3.108	192.168.3.106	ICMP	1164	Echo (ping) request id=0x146e, seq=63
…	192.168.3.106	192.168.3.108	IPv4	1516	Fragmented IP protocol (proto=ICMP 1,
…	192.168.3.106	192.168.3.108	IPv4	1516	Fragmented IP protocol (proto=ICMP 1,
…	192.168.3.106	192.168.3.108	IPv4	1516	Fragmented IP protocol (proto=ICMP 1,
…	192.168.3.106	192.168.3.108	IPv4	1516	Fragmented IP protocol (proto=ICMP 1,
…	192.168.3.106	192.168.3.108	IPv4	1516	Fragmented IP protocol (proto=ICMP 1,
…	192.168.3.106	192.168.3.108	IPv4	1516	Fragmented IP protocol (proto=ICMP 1,
…	192.168.3.106	192.168.3.108	ICMP	1164	Echo (ping) reply id=0x146e, seq=63
…	192.168.3.108	192.168.3.106	IPv4	1516	Fragmented IP protocol (proto=ICMP 1,
…	192.168.3.108	192.168.3.106	IPv4	1516	Fragmented IP protocol (proto=ICMP 1,
…	192.168.3.108	192.168.3.106	IPv4	1516	Fragmented IP protocol (proto=ICMP 1,

Figura 5.11 Tráfico atacante en Wireshark (ambiente de pruebas)

5.2.2.2. Afectación por acceso SSH

Una de las causas de materialización de ataques, se debe al aprovechamiento de la habilitación del servicio de acceso remoto SSH a todos los equipos de la red. Es por esto que es necesario restringir el acceso SSH únicamente a equipos que se establezcan como conocidos y seguros.

A continuación, se define la configuración de regla de detección de accesos SSH

```
GNU nano 2.2.6                          Archivo: /etc/snort/rules/local.rules

#alert icmp any any -> $HOME_NET any (msg:"Ping de la muerte"; sid:1000001; rev:1; dsize: >900;)
alert tcp any any -> $HOME_NET 22 (msg:"Conexión Puerto 22 SSH!"; sid:1000002;)
```

Figura 5.12 Configuración de regla de detección de accesos SSH

Se verifica la habilitación de accesos mediante SSH desde el equipo atacante Kali Linux:

```
root@kali:~# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.3.109  netmask 255.255.255.0  broadcast 192.168.3.255
        inet6 fe80::20c:29ff:fe72:5e3f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:72:5e:3f  txqueuelen 1000  (Ethernet)
        RX packets 72816  bytes 59273222 (56.5 MiB)
```

Figura 5.13 Dirección ip de equipo no autorizado a acceso SSH

```
root@kali:~# ssh netadmin@192.168.3.106
netadmin@192.168.3.106's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Mon Aug  7 05:38:13 ECT 2017

  System load:  0.02               Processes:           123
  Usage of /:   2.8% of 70.29GB    Users logged in:     1
  Memory usage: 4%                 IP address for p2p1:  192.168.2.1
  Swap usage:   0%                 IP address for wlan0: 192.168.3.106

  Graph this data and manage this system at:
    https://landscape.canonical.com/

59 packages can be updated.
50 updates are security updates.

New release '16.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Mon Aug  7 05:38:14 2017 from 192.168.3.102
netadmin@server100:~$
```

Figura 5.14 Acceso efectivo de equipo no autorizado mediante SSH

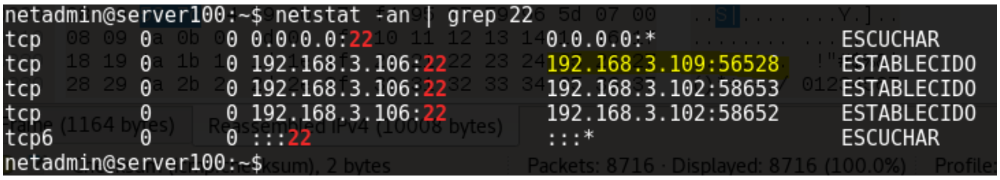


Figura 5.15 Ejecución de comandos desde equipo no autorizado mediante SSH

A continuación, se observa que las conexiones SSH son detectadas a través de la herramienta SNORT

Figura 5.16 Comando de activación de detección de regla SSH

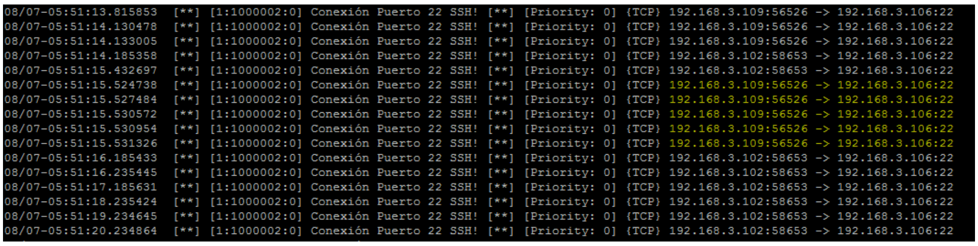


Figura 5.17 Detección de conexiones SSH (ambiente de pruebas)

5.2.2.3. Afectación inundación SYN

Un método efectivo de denegación de servicios se realiza a través de inundación SYN. En el esquema de pruebas, se verifica la materialización de este tipo de ataques hacia el servidor web, su detección y posterior protección.

Previamente, se realiza la validación de disponibilidad del servicio web en el servidor:

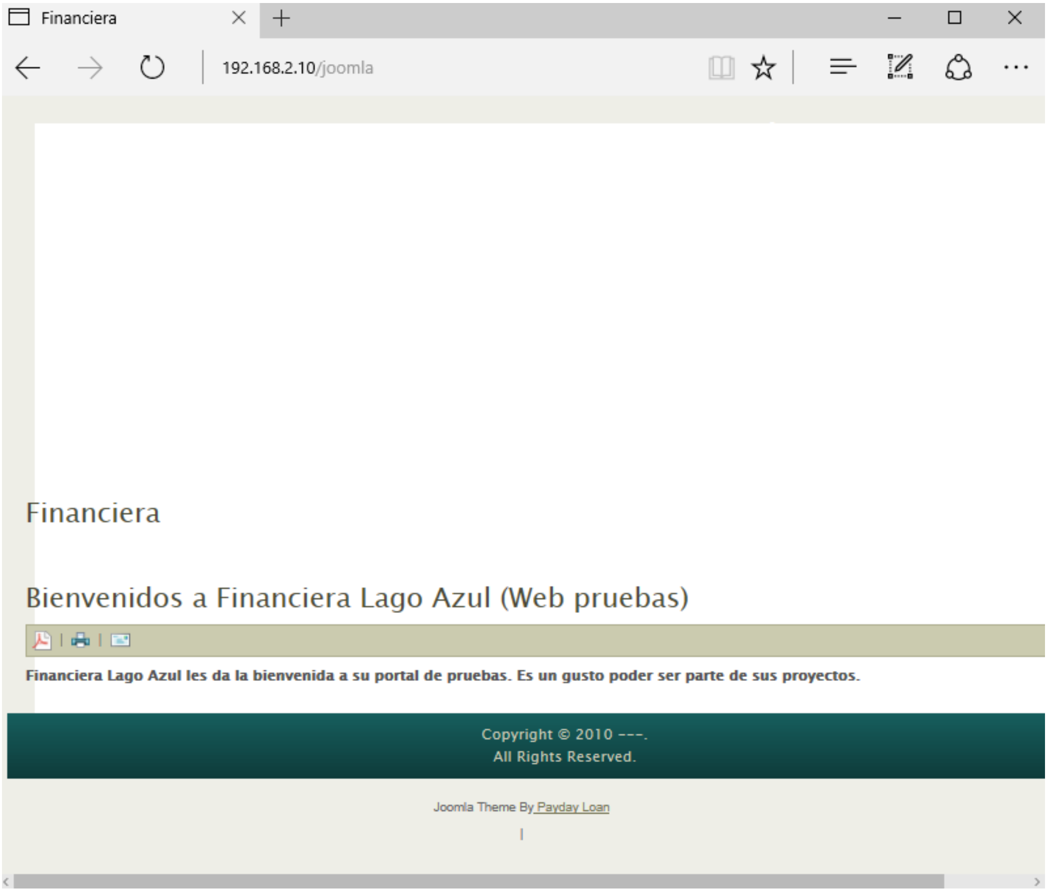
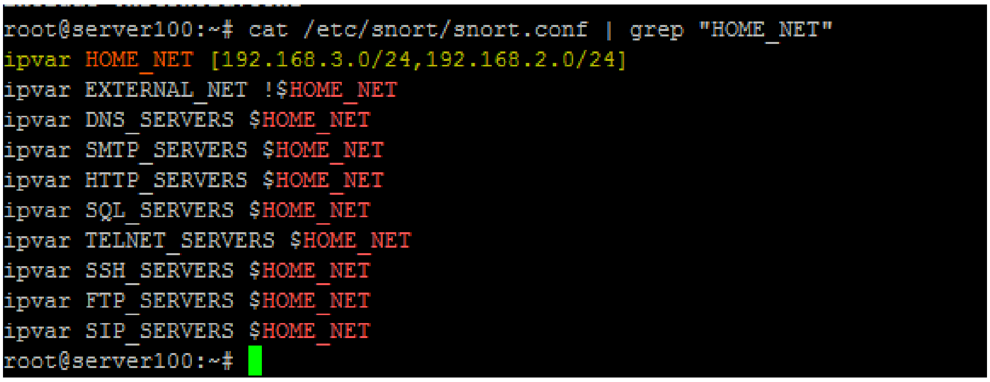


Figura 5.18 Validación de disponibilidad del servicio web (ambiente de pruebas)

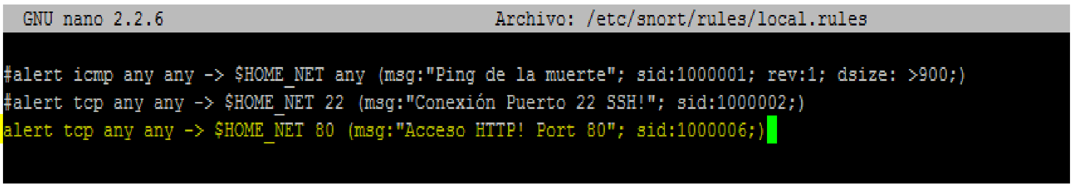
Se verifica que en la herramienta SNORT, estén configurados los segmentos de red que deberán ser monitoreados:



```
root@server100:~# cat /etc/snort/snort.conf | grep "HOME_NET"
ipvar HOME_NET [192.168.3.0/24,192.168.2.0/24]
ipvar EXTERNAL_NET !$HOME_NET
ipvar DNS_SERVERS $HOME_NET
ipvar SMTP_SERVERS $HOME_NET
ipvar HTTP_SERVERS $HOME_NET
ipvar SQL_SERVERS $HOME_NET
ipvar TELNET_SERVERS $HOME_NET
ipvar SSH_SERVERS $HOME_NET
ipvar FTP_SERVERS $HOME_NET
ipvar SIP_SERVERS $HOME_NET
root@server100:~#
```

Figura 5.19 Configuración de segmentos de red en SNORT

A continuación, se define la configuración de regla de detección de accesos web



```
GNU nano 2.2.6                    Archivo: /etc/snort/rules/local.rules

#alert icmp any any -> $HOME_NET any (msg:"Ping de la muerte"; sid:1000001; rev:1; dsize: >900;)
#alert tcp any any -> $HOME_NET 22 (msg:"Conexión Puerto 22 SSH!"; sid:1000002;)
alert tcp any any -> $HOME_NET 80 (msg:"Acceso HTTP! Port 80"; sid:1000006;)
```

Figura 5.20 Configuración de regla de detección de accesos web

Se puede observar que las conexiones web son detectadas a través de la herramienta SNORT

```
root@server100:~# snort -c /etc/snort/snort.conf -A console
```

Figura 5.21 Comando de activación de detección de regla de acceso web

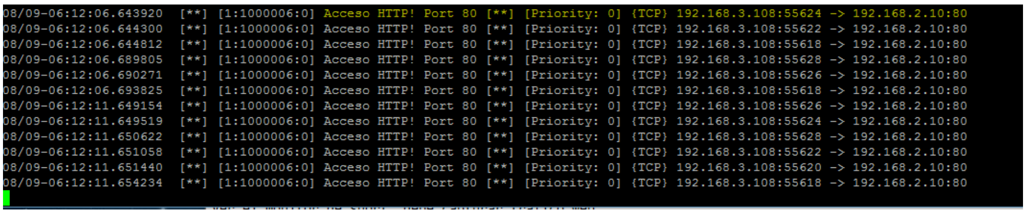


Figura 5.22 Detección de conexiones web en la herramienta SNORT

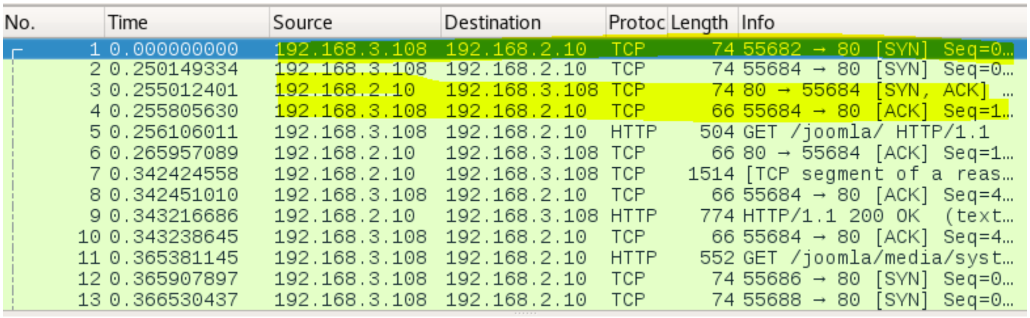


Figura 5.23 Detección de conexiones web en la herramienta Wireshark

En el servidor web, se verifica el tráfico entrante y saliente, utilizando la herramienta de monitoreo nload:

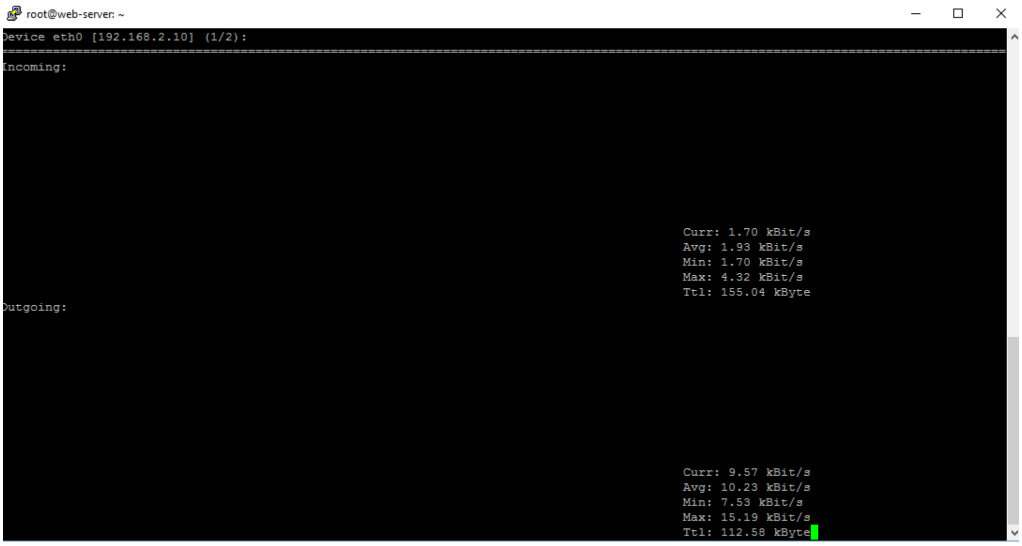


Figura 5.24 Monitoreo inicial de tráfico entrante y saliente en el servidor web

Una vez que se ha validado que el servicio web se encuentra disponible, se define la configuración de regla de detección de ataques SYN:

```
GNU nano 2.2.6                    Archivo: /etc/snort/rules/local.rules

#alert icmp any any -> $HOME_NET any (msg:"Ping de la muerte"; sid:1000001; rev:1; dsize: >900;)
#alert tcp any any -> $HOME_NET 22 (msg:"Conexión Puerto 22 SSH!"; sid:1000002;)
#alert tcp any any -> $HOME_NET 80 (msg:"Acceso HTTP! Port 80"; sid:1000006;)
alert tcp any any -> $HOME_NET any (flags:S; msg:"ATAQUE SYN FLOOD"; sid:1000007;)
```

Figura 5.25 Configuración de regla de detección de ataques SYN

Posterior a la configuración, se habilita la salida en pantalla la detección de ataques SYN

```
root@server100:~# snort -c /etc/snort/snort.conf -A console
```

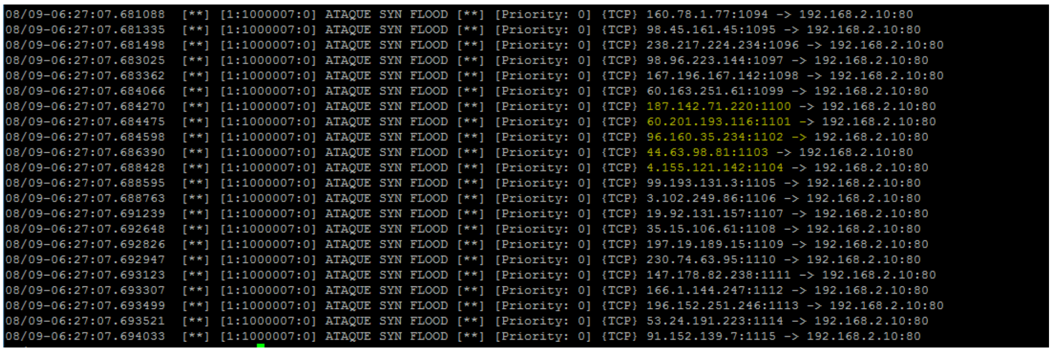
Figura 5.26 Comando de activación de detección de regla de ataque SYN

Para verificar que el servidor es susceptible de sufrir ataques de denegación de servicios, se ejecuta el comando que realiza la inundación SYN desde el equipo atacante

```
root@kali:~# hping3 192.168.2.10 -S -p 80 --rand-source --flood
HPING 192.168.2.10 (eth0 192.168.2.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

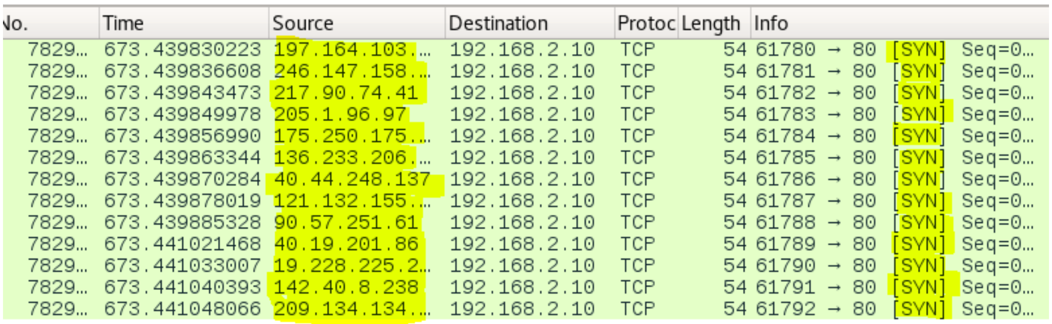
Figura 5.27 Comando que lanza el ataque inundación SYN al servidor web

Desde la herramienta SNORT, se verifica la detección del ataque SYN:



```
08/09-06:27:07.681088  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 160.78.1.77:1094 -> 192.168.2.10:80
08/09-06:27:07.681335  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 98.45.161.45:1095 -> 192.168.2.10:80
08/09-06:27:07.681498  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 238.217.224.234:1096 -> 192.168.2.10:80
08/09-06:27:07.683025  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 98.96.223.144:1097 -> 192.168.2.10:80
08/09-06:27:07.683362  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 167.196.167.142:1098 -> 192.168.2.10:80
08/09-06:27:07.684066  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 60.163.251.61:1099 -> 192.168.2.10:80
08/09-06:27:07.684270  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 187.142.71.220:1100 -> 192.168.2.10:80
08/09-06:27:07.684475  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 60.201.193.116:1101 -> 192.168.2.10:80
08/09-06:27:07.684598  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 96.160.35.234:1102 -> 192.168.2.10:80
08/09-06:27:07.686390  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 44.63.98.81:1103 -> 192.168.2.10:80
08/09-06:27:07.688428  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 4.155.121.142:1104 -> 192.168.2.10:80
08/09-06:27:07.688595  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 99.193.131.3:1105 -> 192.168.2.10:80
08/09-06:27:07.688763  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 3.102.249.86:1106 -> 192.168.2.10:80
08/09-06:27:07.691239  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 19.92.131.157:1107 -> 192.168.2.10:80
08/09-06:27:07.692648  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 35.15.106.61:1108 -> 192.168.2.10:80
08/09-06:27:07.692826  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 197.19.189.15:1109 -> 192.168.2.10:80
08/09-06:27:07.692947  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 230.74.63.95:1110 -> 192.168.2.10:80
08/09-06:27:07.693123  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 147.178.82.238:1111 -> 192.168.2.10:80
08/09-06:27:07.693307  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 166.1.144.247:1112 -> 192.168.2.10:80
08/09-06:27:07.693499  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 196.152.251.246:1113 -> 192.168.2.10:80
08/09-06:27:07.693521  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 53.24.191.223:1114 -> 192.168.2.10:80
08/09-06:27:07.694033  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 91.152.139.7:1115 -> 192.168.2.10:80
```

Figura 5.28 Detección de ataque SYN en la herramienta SNORT



No.	Time	Source	Destination	Protoc	Length	Info
7829…	673.439830223	197.164.103.…	192.168.2.10	TCP	54	61780 → 80 [SYN] Seq=0…
7829…	673.439836608	246.147.158.…	192.168.2.10	TCP	54	61781 → 80 [SYN] Seq=0…
7829…	673.439843473	217.90.74.41	192.168.2.10	TCP	54	61782 → 80 [SYN] Seq=0…
7829…	673.439849978	205.1.96.97	192.168.2.10	TCP	54	61783 → 80 [SYN] Seq=0…
7829…	673.439856990	175.250.175.…	192.168.2.10	TCP	54	61784 → 80 [SYN] Seq=0…
7829…	673.439863344	136.233.206.…	192.168.2.10	TCP	54	61785 → 80 [SYN] Seq=0…
7829…	673.439870284	40.44.248.137	192.168.2.10	TCP	54	61786 → 80 [SYN] Seq=0…
7829…	673.439878019	121.132.155.…	192.168.2.10	TCP	54	61787 → 80 [SYN] Seq=0…
7829…	673.439885328	90.57.251.61	192.168.2.10	TCP	54	61788 → 80 [SYN] Seq=0…
7829…	673.441021468	40.19.201.86	192.168.2.10	TCP	54	61789 → 80 [SYN] Seq=0…
7829…	673.441033007	19.228.225.2…	192.168.2.10	TCP	54	61790 → 80 [SYN] Seq=0…
7829…	673.441040393	142.40.8.238	192.168.2.10	TCP	54	61791 → 80 [SYN] Seq=0…
7829…	673.441048066	209.134.134.…	192.168.2.10	TCP	54	61792 → 80 [SYN] Seq=0…

Figura 5.29 Detección de ataque SYN en la herramienta Wireshark

A través de la herramienta nload, se puede apreciar el incremento del tráfico en el servidor web:

Figura 5.30 Monitoreo de tráfico entrante y saliente durante ataque SYN

Con la materialización efectiva del ataque SYN, se valida que el servicio web se ha caído:

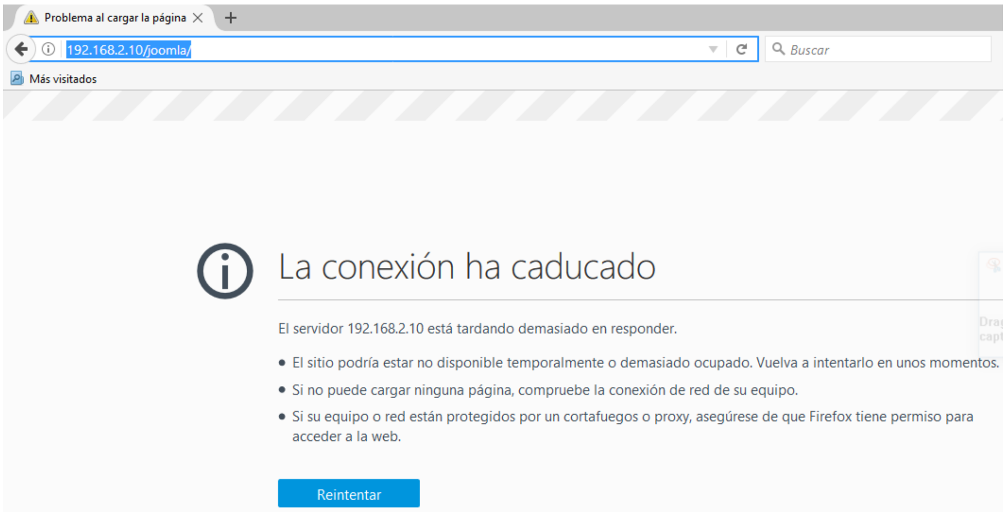


Figura 5.31 Caída de servicio web debido a ataque SYN

En la máquina atacante se puede observar la cantidad de paquetes transmitidos:

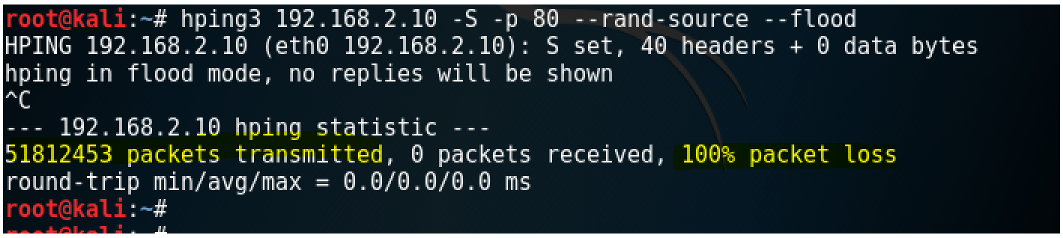


Figura 5.32 Cantidad de paquetes transmitidos durante ataque SYN

5.2.2.4. Afectación por escaneo de puertos

A través del escaneo de puertos, se puede obtener información acerca de la infraestructura y servicios activos de un servidor o dispositivo perimetral, con lo que esta información podría servir de base a un atacante para realizar diferentes tipos de intrusión, aprovechándose de vulnerabilidades que pueda detectar. Utilizando la herramienta SNORT, se pueden identificar actividades de escaneo de puertos, y con la aplicación de reglas IPTABLES, se lo puede restringir.

A continuación se verifica si desde el equipo atacante de pruebas se permite realizar escaneo de puertos al servidor IDS-IPS

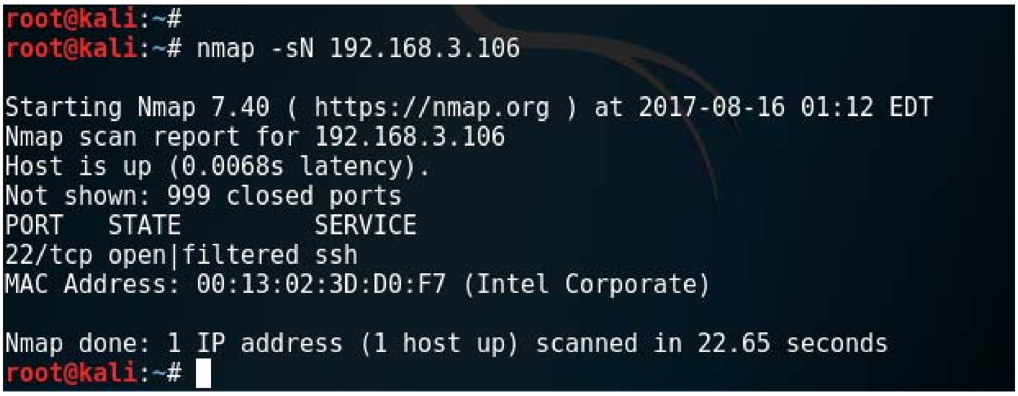


Figura 5.33 Exploración Null scan con bandera 0 en encabezado TCP

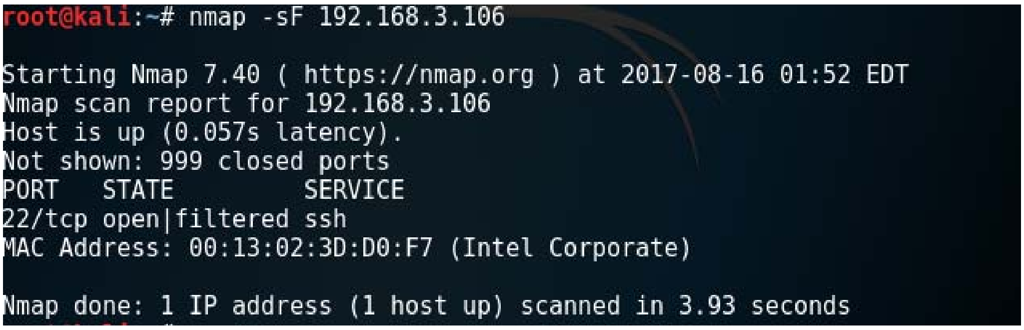


Figura 5.34 Exploración FIN scan estableciendo sólo el bit FIN TCP

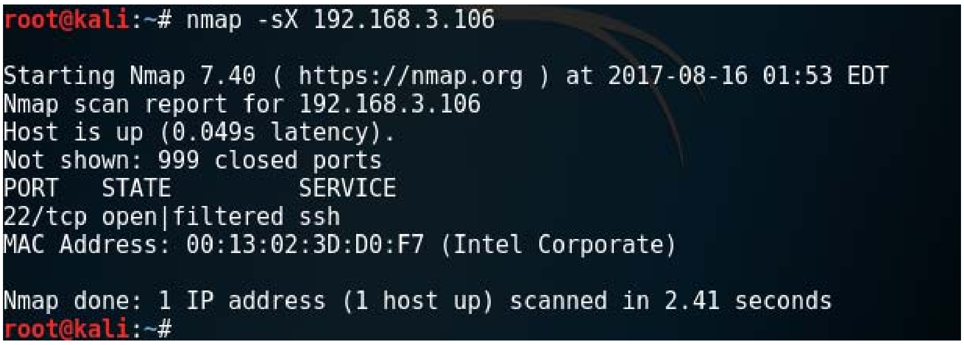


Figura 5.35 Exploración Xmas scan con bits de bandera FIN, PSH y URG

Una vez que se ha determinado que es posible realizar el escaneo de puertos en el servidor IDS-IPS, se procede a configurar SNORT para poder visualizar detectar este tipo de intrusión:

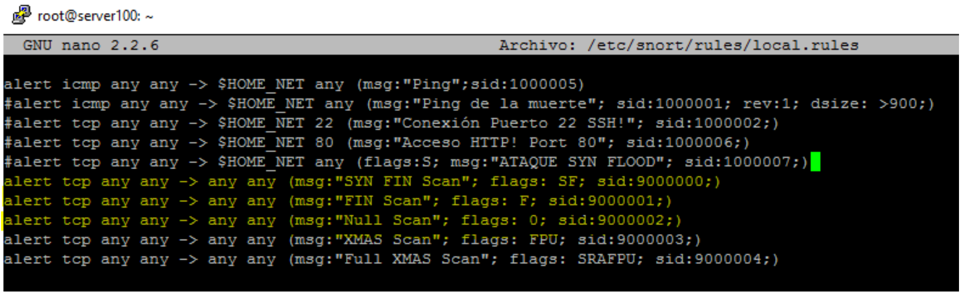


Figura 5.36 Configuración de reglas de detección de escaneo de puertos

Se valida la detección de escaneo de puertos a través de SNORT

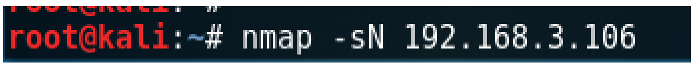


Figura 5.37 Ejecución de escaneo de puertos Null scan

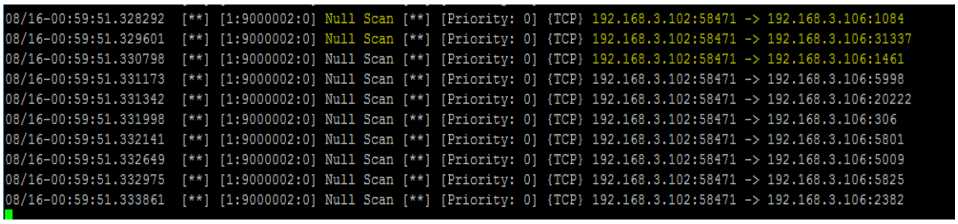


Figura 5.38 Validación de detección de escaneo de puertos Null scan en SNORT

Figura 5.39 Ejecución de escaneo de puertos FIN scan

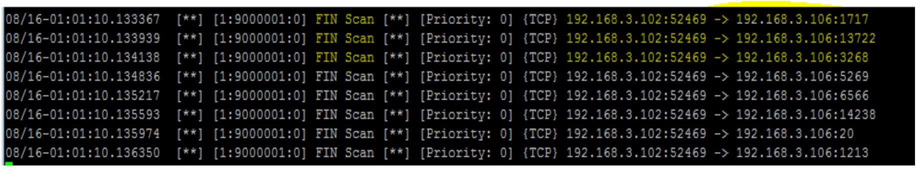


Figura 5.40 Validación de detección de escaneo de puertos FIN scan en SNORT

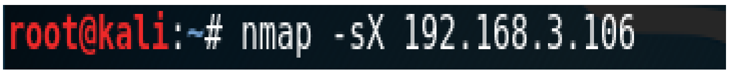


Figura 5.41 Ejecución de escaneo de puertos Xmas scan

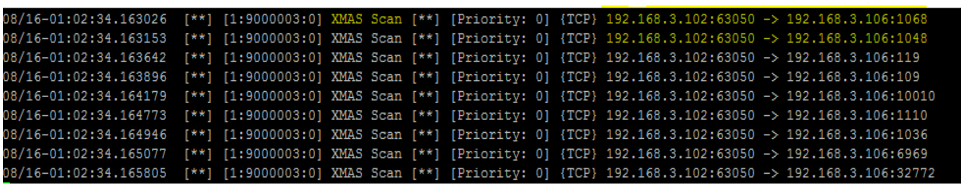


Figura 5.42 Detección de escaneo de puertos Xmas scan en SNORT

5.2.3. Configuración de reglas de protección IDS-IPS

5.2.3.1. Protección ping de la muerte

Una vez que se ha verificado el proceso de detección de ataques, se procede a configurar mediante IPTABLES, las reglas que permiten proteger el servidor de ataques ping de la muerte:

```
root@server100:~# iptables -N ping_muerte
root@server100:~# iptables -A ping_muerte -m limit --limit-burst 6 --limit 2/m -j RETURN
root@server100:~# iptables -A ping_muerte -j DROP
root@server100:~# iptables -A INPUT -s 0/0 -i wlan0 -p icmp --icmp-type echo-request -j ping_muerte
root@server100:~#
```

Figura 5.43 Configuración de reglas de protección ping de la muerte

5.2.3.2. Protección SSH

Una vez que se ha verificado que es posible acceder a través de SSH, se establecen las reglas que permiten únicamente acceder al equipo autorizado:

```
root@server100:~#
root@server100:~# # iptables -A INPUT -s 192.168.3.102 -p tcp --dport 22 -j ACCEPT
```

Figura 5.44 Configuración de reglas de autorización de conexión SSH

Se deniega el acceso de conexión SSH a los demás equipos:

```
root@server100:~# iptables -A INPUT -p tcp --dport 22 -j DROP
```

Figura 5.45 Configuración de reglas de bloqueo de conexión SSH no autorizada

5.2.3.3. Protección inundación SYN

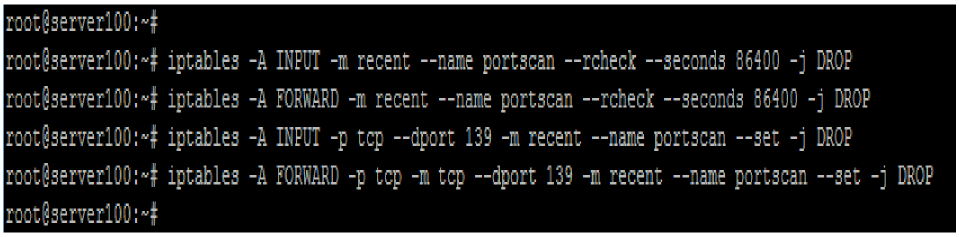
Una vez que se ha verificado que el servidor web es susceptible a ataques de denegación de servicios, se configuran las reglas que permiten evitar la materialización de un ataque por inundación SYN:

```
root@server100:~# iptables -A FORWARD -p tcp --syn -m limit --limit 1/s --limit-burst 3 -j RETURN
root@server100:~# iptables -N syn_flood
root@server100:~# iptables -A FORWARD -p tcp --syn -j syn_flood
root@server100:~# iptables -A syn_flood -m limit --limit 1/s --limit-burst 3 -j RETURN
root@server100:~# iptables -A syn_flood -j DROP
```

Figura 5.46 Configuración de reglas de protección contra ataques SYN

5.2.3.4. Protección contra escaneo de puertos

Luego de validar la detección de escaneo de puertos, se procede a configurar las reglas que impidan materializarlos:



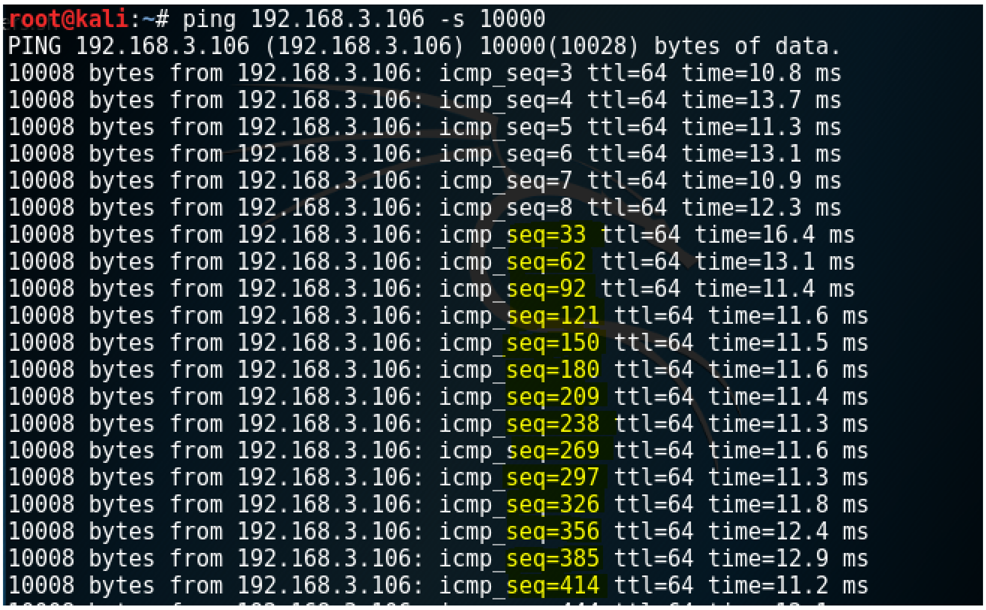
```
root@server100:~#
root@server100:~# iptables -A INPUT -m recent --name portscan --rcheck --seconds 86400 -j DROP
root@server100:~# iptables -A FORWARD -m recent --name portscan --rcheck --seconds 86400 -j DROP
root@server100:~# iptables -A INPUT -p tcp --dport 139 -m recent --name portscan --set -j DROP
root@server100:~# iptables -A FORWARD -p tcp -m tcp --dport 139 -m recent --name portscan --set -j DROP
root@server100:~#
```

Figura 5.47 Configuración de reglas de protección de escaneo de puertos

5.2.4. Validación de protección IDS-IPS

5.2.4.1. Validación de protección ping de la muerte

Una vez implementadas las reglas de protección, se realiza nuevamente el ataque ping de la muerte:



```
root@kali:~# ping 192.168.3.106 -s 10000
PING 192.168.3.106 (192.168.3.106) 10000(10028) bytes of data.
10008 bytes from 192.168.3.106: icmp_seq=3 ttl=64 time=10.8 ms
10008 bytes from 192.168.3.106: icmp_seq=4 ttl=64 time=13.7 ms
10008 bytes from 192.168.3.106: icmp_seq=5 ttl=64 time=11.3 ms
10008 bytes from 192.168.3.106: icmp_seq=6 ttl=64 time=13.1 ms
10008 bytes from 192.168.3.106: icmp_seq=7 ttl=64 time=10.9 ms
10008 bytes from 192.168.3.106: icmp_seq=8 ttl=64 time=12.3 ms
10008 bytes from 192.168.3.106: icmp_seq=33 ttl=64 time=16.4 ms
10008 bytes from 192.168.3.106: icmp_seq=62 ttl=64 time=13.1 ms
10008 bytes from 192.168.3.106: icmp_seq=92 ttl=64 time=11.4 ms
10008 bytes from 192.168.3.106: icmp_seq=121 ttl=64 time=11.6 ms
10008 bytes from 192.168.3.106: icmp_seq=150 ttl=64 time=11.5 ms
10008 bytes from 192.168.3.106: icmp_seq=180 ttl=64 time=11.6 ms
10008 bytes from 192.168.3.106: icmp_seq=209 ttl=64 time=11.4 ms
10008 bytes from 192.168.3.106: icmp_seq=238 ttl=64 time=11.3 ms
10008 bytes from 192.168.3.106: icmp_seq=269 ttl=64 time=11.6 ms
10008 bytes from 192.168.3.106: icmp_seq=297 ttl=64 time=11.3 ms
10008 bytes from 192.168.3.106: icmp_seq=326 ttl=64 time=11.8 ms
10008 bytes from 192.168.3.106: icmp_seq=356 ttl=64 time=12.4 ms
10008 bytes from 192.168.3.106: icmp_seq=385 ttl=64 time=12.9 ms
10008 bytes from 192.168.3.106: icmp_seq=414 ttl=64 time=11.2 ms
```

Figura 5.48 Segunda ejecución de ataque ping de la muerte

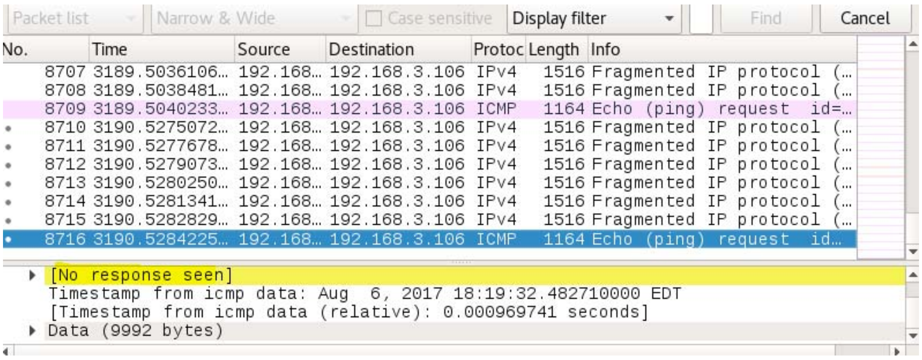


Figura 5.49 Verificación de ausencia de respuesta a solicitud de echo

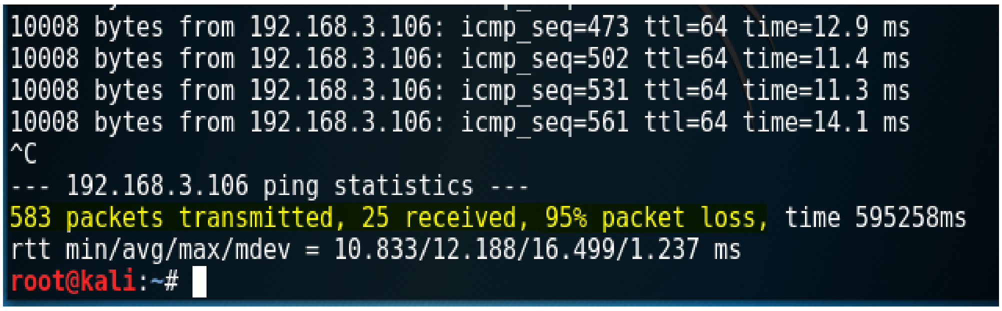


Figura 5.50 Verificación de pérdida de paquetes en ataque ping de la muerte

Al analizar los resultados de la ejecución del ataque, se observa que las reglas de protección implementadas, limitan la cantidad de solicitudes de paquetes, desechando la mayor cantidad de peticiones. Esto se lo puede comprobar al observar que existen grandes saltos de secuencia en las peticiones aceptadas y asimismo observando para este caso que el 95% de paquetes se pierden.

5.2.4.2. Validación de protección SSH

Se verifica que se encuentran configuradas las reglas de protección SSH:

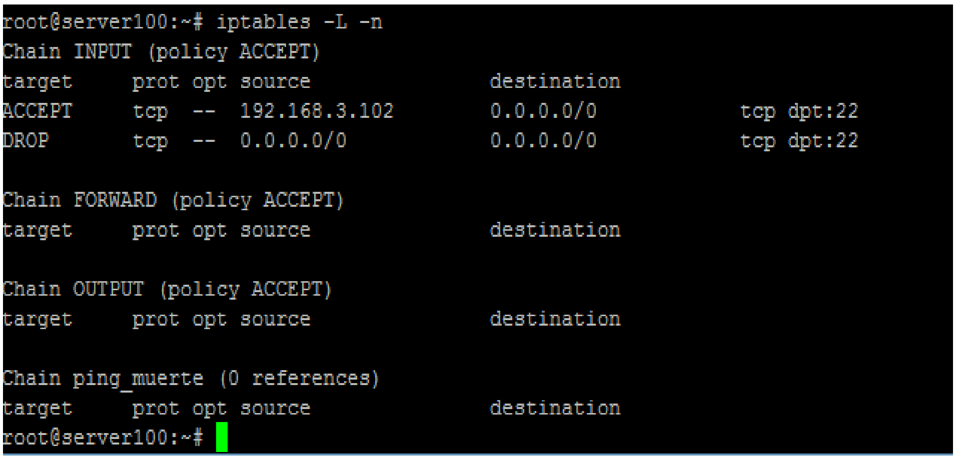


Figura 5.51 Validación de aplicación de reglas de protección SHH

Una vez realizada la configuración, se verifica la denegación de acceso no autorizado SSH al equipo atacante:

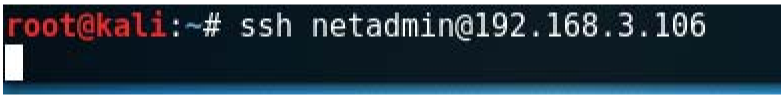


Figura 5.52 Intento fallido de conexión SSH en la maquina no autorizada

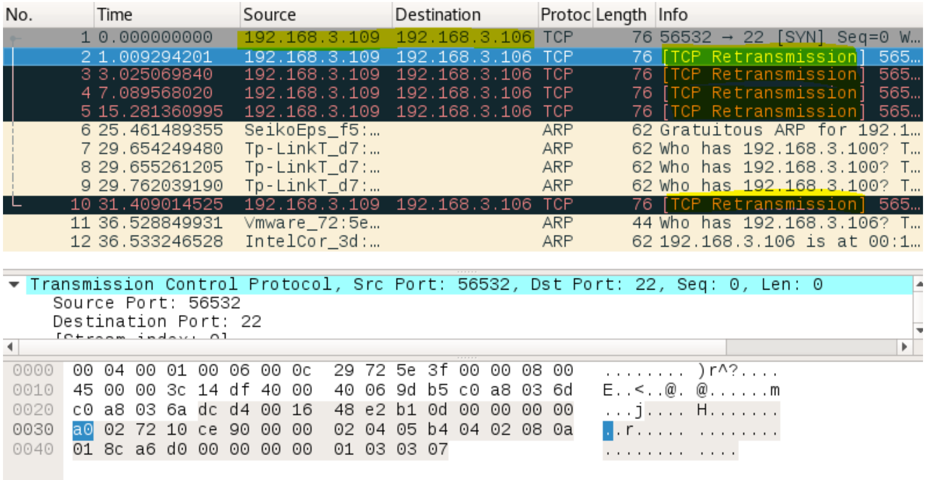


Figura 5.53 Verificación de flujo de tráfico SSH en la herramienta Wireshark

Se verifica que la detección de intentos de accesos SSH son registrados por la herramienta SNORT:

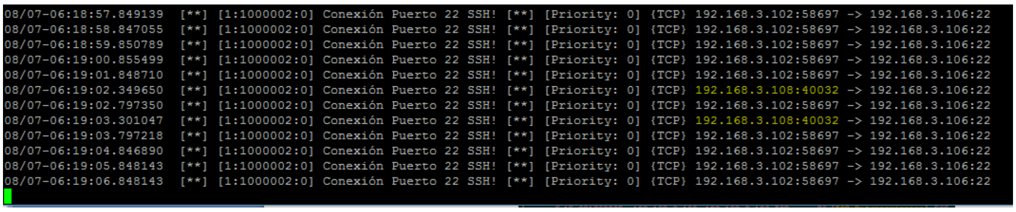


Figura 5.54 Detección de conexiones SSH (fallidas) en la herramienta SNORT

5.2.4.3. Validación de protección inundación SYN

Una vez configuradas las reglas de protección, se procede a realizar nuevamente el ataque de inundación SYN hacia el servidor web de pruebas:

```
root@kali:~# hping3 192.168.2.10 -S -p 80 --rand-source --flood
HPING 192.168.2.10 (eth0 192.168.2.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.2.10 hping statistic ---
7029068 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

Figura 5.55 Segunda ejecución de ataque inundación SYN al servidor web

Se verifica que el ataque es detectado por la herramienta SNORT:

```
08/10-00:02:27.313077  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 224.23.124.24:4179 -> 192.168.2.10:80
08/10-00:02:27.313923  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 153.219.30.253:4180 -> 192.168.2.10:80
08/10-00:02:27.315164  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 43.244.31.46:4186 -> 192.168.2.10:80
08/10-00:02:27.317147  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 230.228.41.231:4187 -> 192.168.2.10:80
08/10-00:02:27.355996  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 102.174.25.244:4193 -> 192.168.2.10:80
08/10-00:02:27.356432  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 166.155.31.70:4200 -> 192.168.2.10:80
08/10-00:02:27.357244  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 64.100.125.120:4209 -> 192.168.2.10:80
08/10-00:02:27.359010  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 214.123.244.165:4217 -> 192.168.2.10:80
08/10-00:02:27.359500  [**] [1:1000007:0] ATAQUE SYN FLOOD [**] [Priority: 0] {TCP} 64.224.97.136:4226 -> 192.168.2.10:80
```

Figura 5.56 Detección de ataques de inundación SYN en la herramienta SNORT

9053…	99.325625353	250.252.208.…	192.168.2.10	TCP	54	56911 → 80 [SYN] Seq=0…
9053…	99.325629327	177.6.200.143	192.168.2.10	TCP	54	56912 → 80 [SYN] Seq=0…
9053…	99.325633284	54.230.211.18	192.168.2.10	TCP	54	56913 → 80 [SYN] Seq=0…
9053…	99.325637237	235.227.151.…	192.168.2.10	TCP	54	56914 → 80 [SYN] Seq=0…
9053…	99.325641195	123.241.27.1…	192.168.2.10	TCP	54	56915 → 80 [SYN] Seq=0…
9053…	99.325645191	112.102.175.…	192.168.2.10	TCP	54	56916 → 80 [SYN] Seq=0…
9053…	99.325649170	33.212.22.73	192.168.2.10	TCP	54	56917 → 80 [SYN] Seq=0…
9053…	99.325653141	16.71.226.184	192.168.2.10	TCP	54	56918 → 80 [SYN] Seq=0…
9053…	99.325657086	151.90.24.168	192.168.2.10	TCP	54	56919 → 80 [SYN] Seq=0…

Figura 5.57 Detección de segundo ataque SYN en la herramienta Wireshark

Asimismo, se valida que el ataque está siendo mitigado con la aplicación de reglas IPTABLES, a través de la herramienta nload, que muestra que no se incrementa el tráfico en el servidor web:

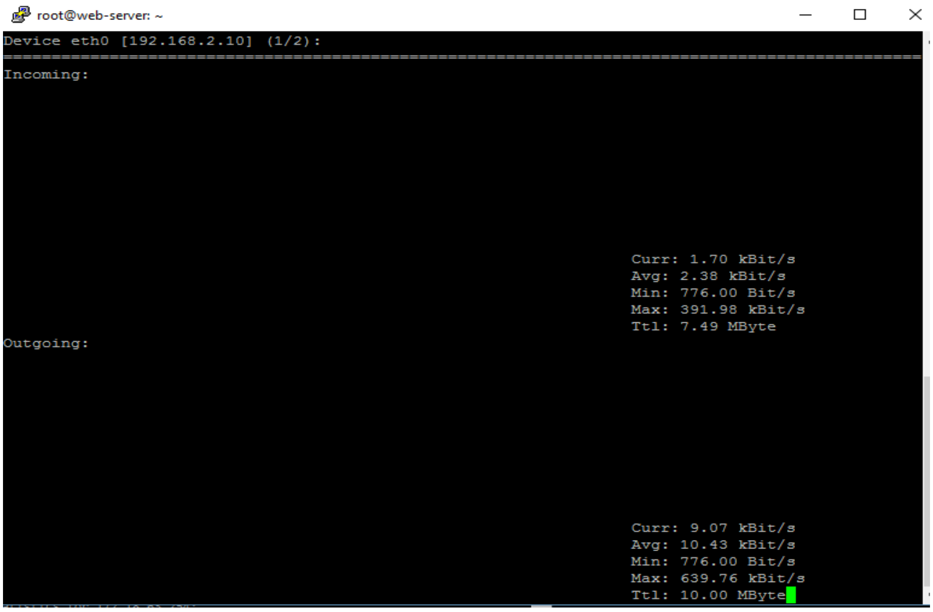


Figura 5.58 Baja afectación de tráfico entrante y saliente durante ataque SYN

Finalmente se valida que el servicio web esté disponible y no haya sido afectado por el ataque SYN:

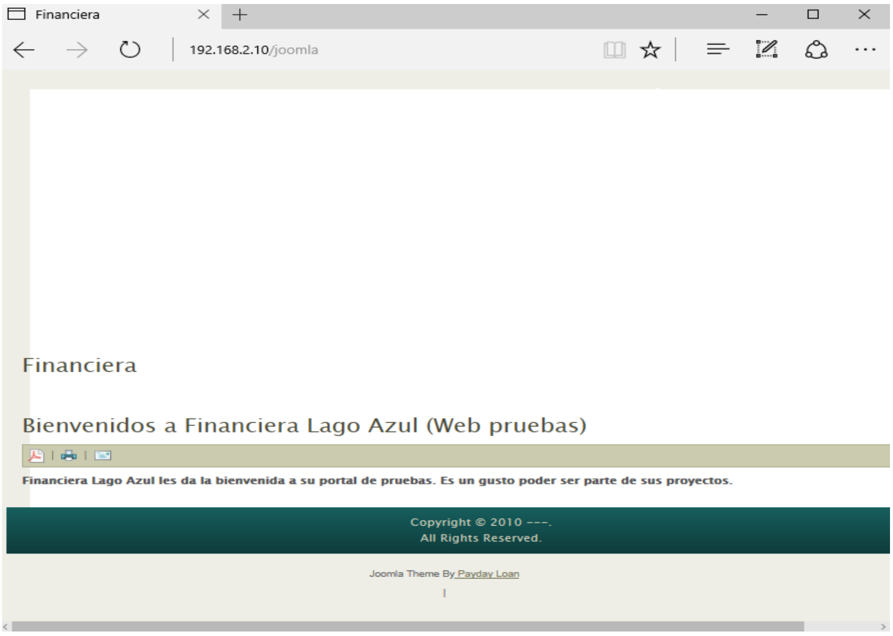


Figura 5.59 Estado de servicio web activo durante ataque SYN

5.2.4.4. Validación de protección de escaneo de puertos

Se procede a validar que el servidor IDS-IPS aplique efectivamente la restricción de escaneo de puertos:

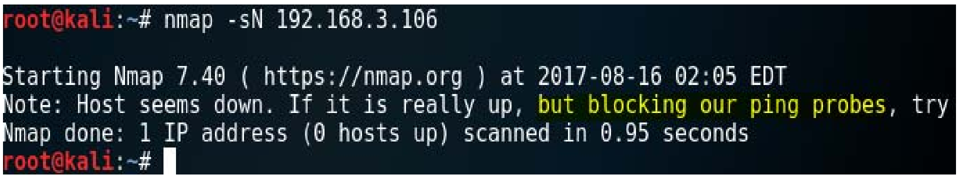


Figura 5.60 Validación de protección de escaneo de puertos Null scan

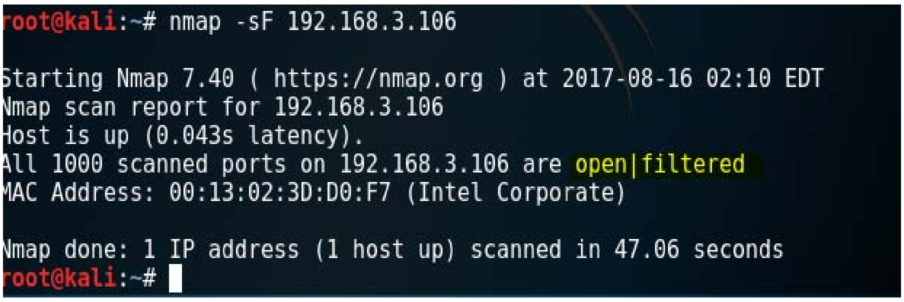


Figura 5.61 Validación de protección de escaneo de puertos FIN scan

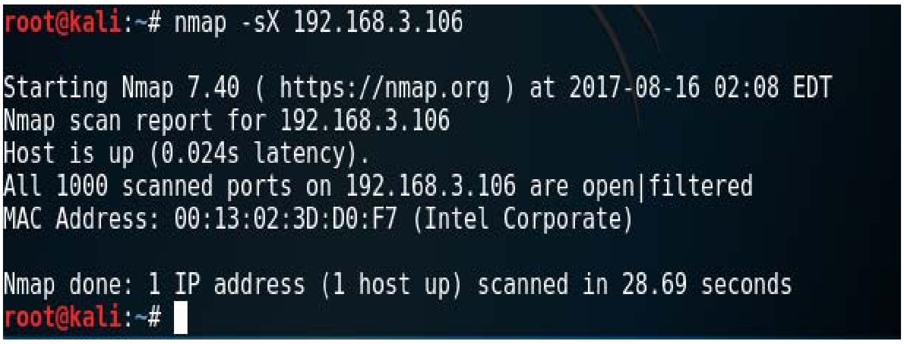


Figura 5.62 Validación de protección de escaneo de puertos Xmas scan

5.3. Implementación de IDS-IPS en producción

5.3.1. Instalación y configuración de IDS-IPS

Una vez que se ha validado el funcionamiento del servidor IDS-IPS Ubuntu en un ambiente de pruebas, se procede a realizar los cambios necesarios, acorde a la configuración de red de Financiera Lago Azul, a fin de que se empiecen a aplicar las reglas de filtrado de paquetes con IPTABLES. Las reglas de detección se mantienen igual a las definidas en el ambiente de desarrollo.

Para aplicar las reglas de validación, se procede a aplicar las conexiones físicas de acuerdo al diseño anteriormente propuesto, cambiar la dirección ip pública del servidor web por una dirección privada, configurar la dirección ip pública en una de las interfaces del servidor IDS-IPS, e implementar NAT para que las peticiones de servicio web que llegan al servidor IDS-IPS sean traducidas y redireccionadas al servidor web:

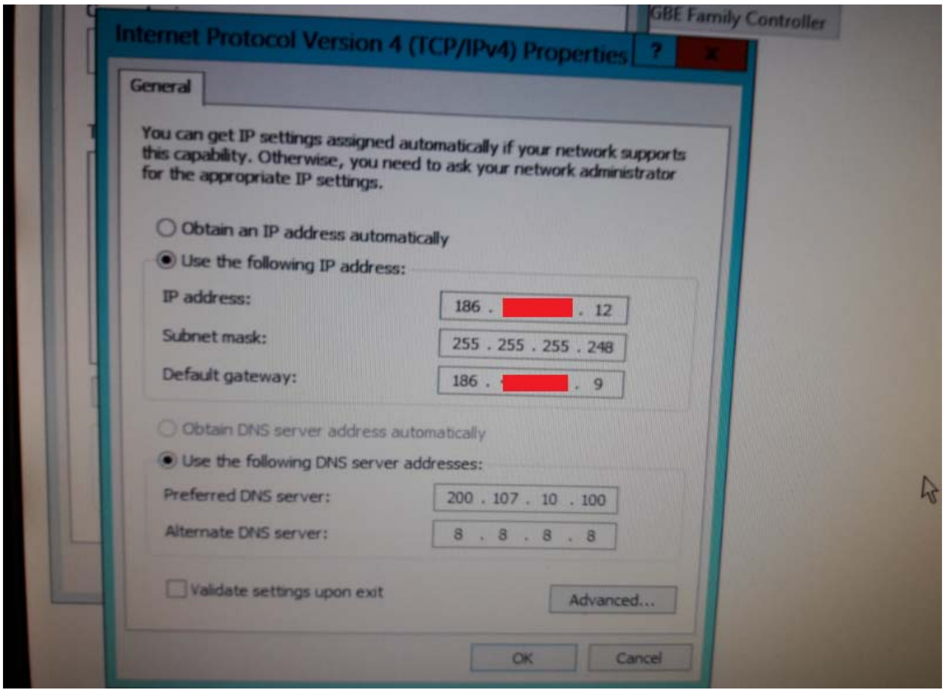


Figura 5.63 Cambio de dirección ip del servidor web

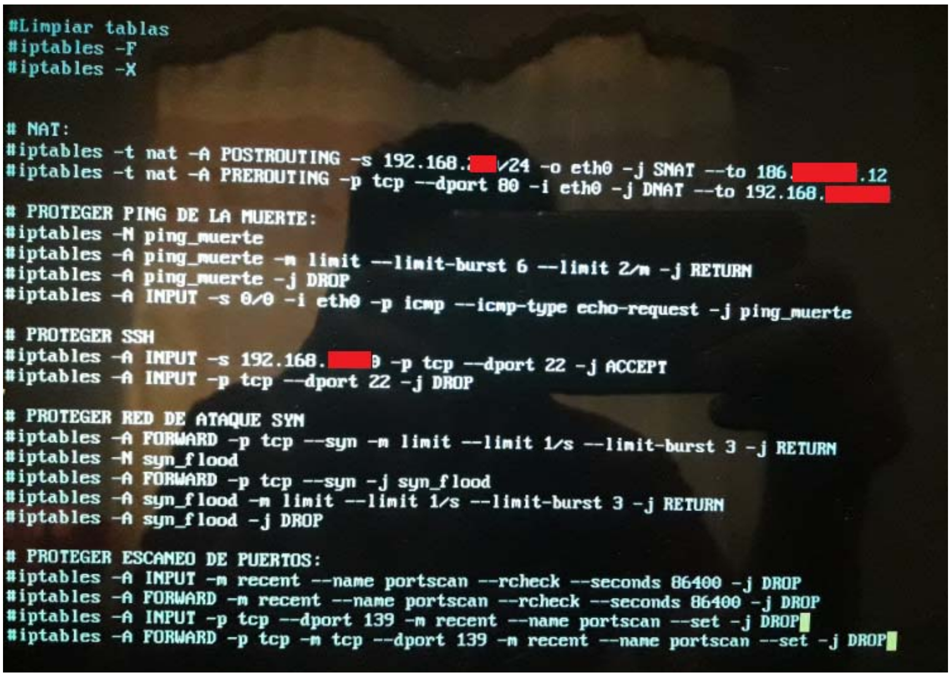


Figura 5.64 Aplicación de reglas de filtrado de paquetes en producción

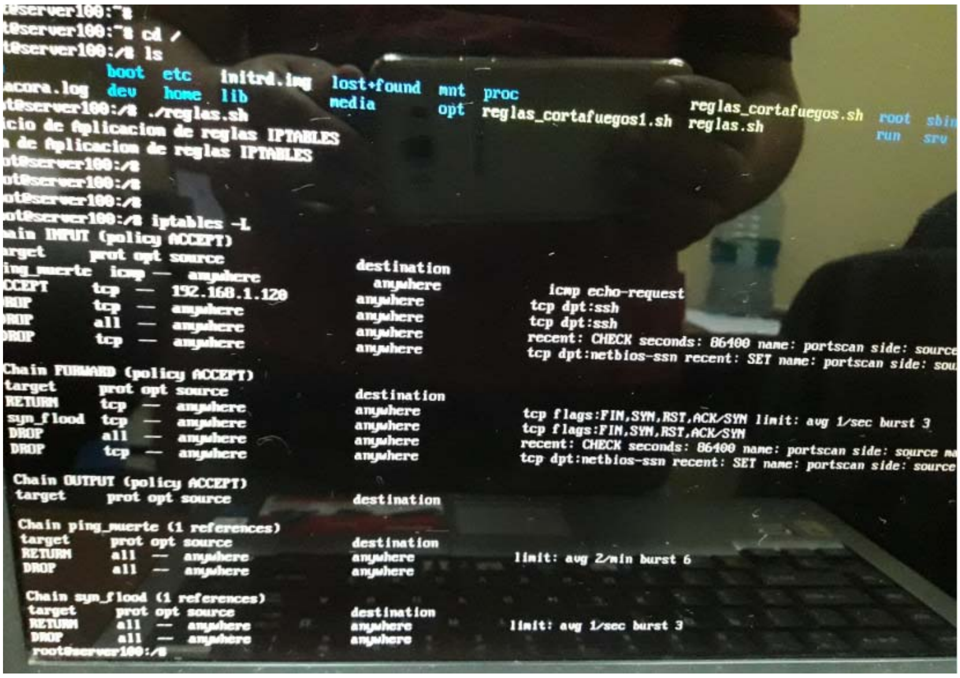


Figura 5.65 Validación de aplicación de reglas en producción

5.3.2. Pruebas de efectividad en ambiente de producción

5.3.2.1. Validación de Ping de la muerte

A continuación se indica el funcionamiento de la aplicación de reglas de filtrado ante la ejecución un ataque de ping de la muerte en producción:

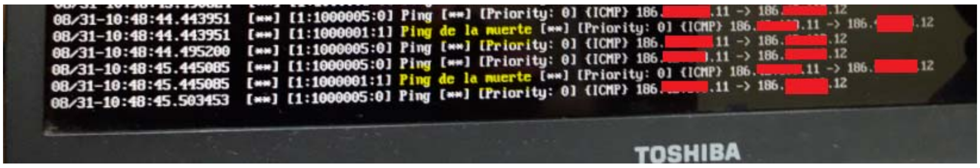


Figura 5.66 Detección de ataque ping de la muerte en producción

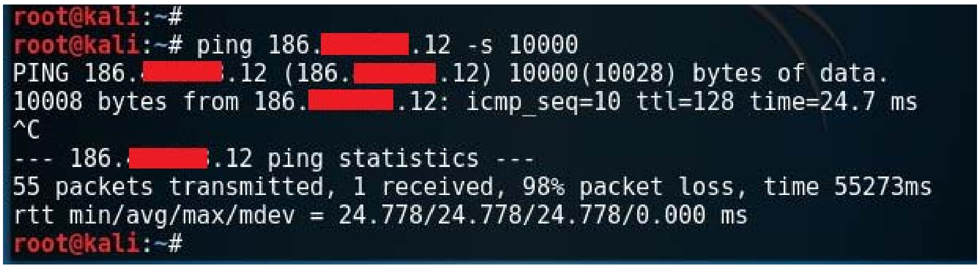


Figura 5.67 Protección de ataque ping de la muerte en producción

5.3.2.2. Validación SSH

Se verifica la detección y bloqueo de solicitudes SSH de equipos no autorizados

Figura 5.68 Detección de solicitud de acceso SSH no autorizado en producción

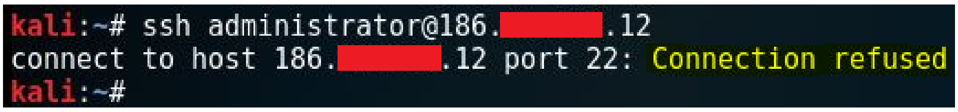


Figura 5.69 Validación de protección de acceso SSH en producción

5.3.2.3. Validación inundación SYN

Se procede con la verificación de la aplicación de reglas de detección y protección de inundación SYN

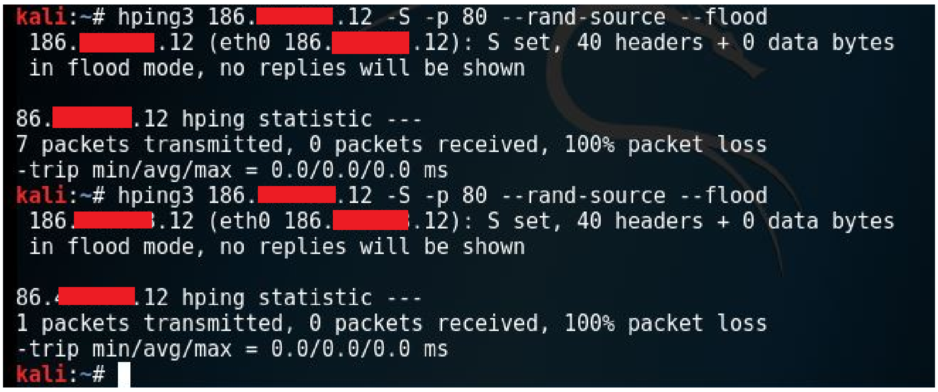


Figura 5.70 Ejecución de ataque de inundación SYN en producción

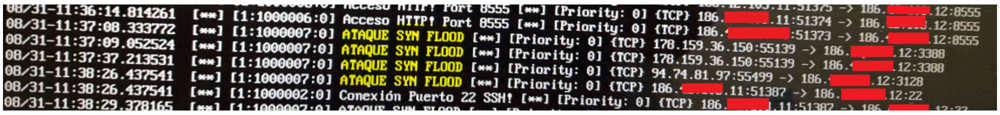


Figura 5.71 Detección de ataque de inundación SYN en producción

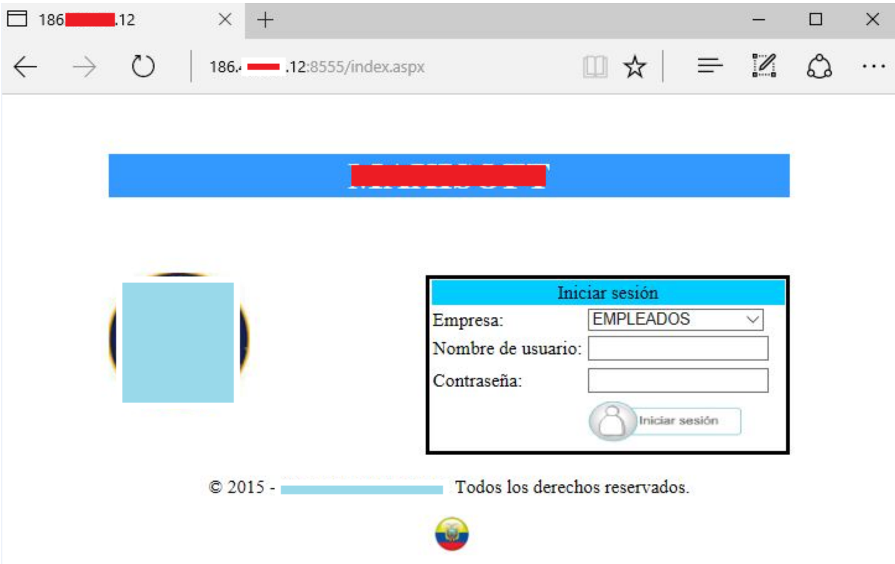


Figura 5.72 Validación de servicio web disponible durante ataque de inundación SYN en producción

5.3.2.4. Validación escaneo de puertos

La validación de configuración de escaneo de puertos no es posible reproducir en producción debido a que el proveedor de la dirección ip pública, realiza esta protección y filtrado a través de su cortafuegos:

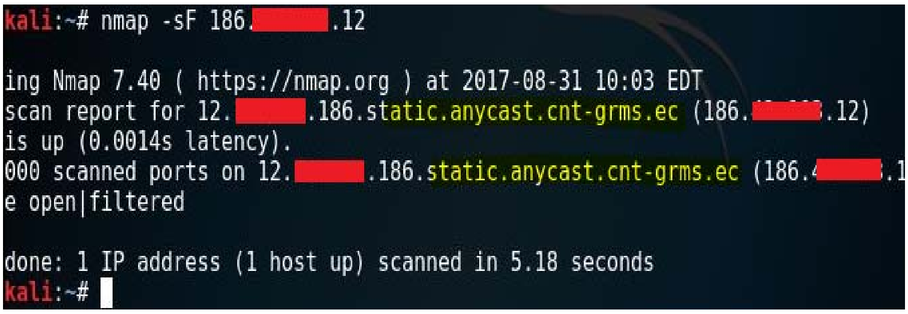


Figura 5.73 Validación de protección de escaneo de puertos por el proveedor

5.3.3. Logs de detección de ataques

La herramienta utilizada para la detección de intrusiones SNORT cuenta con un registro histórico de archivos, los cuales se encuentran en el directorio /var/log/snort y permite realizar una consulta detallada de los eventos de seguridad suscitados:

```
08/31-11:49:49.892926 186.42.103.11 -> 186.42.103.12
ICMP TTL:62 TOS:0x0 ID:7381 IpLen:20 DgmLen:84
Type:8  Code:0  ID:62464   Seq:52  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+=+=+=+

08/31-11:49:50.923428 186.42.103.11 -> 186.42.103.12
ICMP TTL:62 TOS:0x0 ID:7382 IpLen:20 DgmLen:84
Type:8  Code:0  ID:62464   Seq:53  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+=+=+=+

08/31-11:49:51.939553 186.42.103.11 -> 186.42.103.12
ICMP TTL:62 TOS:0x0 ID:7383 IpLen:20 DgmLen:84
Type:8  Code:0  ID:62464   Seq:54  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+=+=+=+

08/31-11:49:52.970674 186.42.103.11 -> 186.42.103.12
ICMP TTL:62 TOS:0x0 ID:7384 IpLen:20 DgmLen:84
Type:8  Code:0  ID:62464   Seq:55  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+=+=+=+
```

Figura 5.74 Log de detección de ataques de intrusión en la herramienta SNORT

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

Los resultados obtenidos luego de la implementación del esquema de seguridad perimetral en Financiera Lago Azul han sido satisfactorios ya que han permitido contar con una herramienta que a través de diferentes configuraciones permite detectar los eventos de seguridad que se requieren monitorear y a la vez permite realizar el filtrado de paquetes a fin de restringir aquellos considerados maliciosos o no deseados, lo que optimiza la prestación de servicios, y permite mantener activa la continuidad del negocio.

Asimismo, luego de realizado el análisis de vulnerabilidades se ha podido aplicar las medidas necesarias a fin de eliminar especialmente aquella considerada como crítica y que podría ser aprovechada para la materialización de posibles ataques.

Finalmente, las mejoras aplicadas en las reglas de filtrado web en el firewall brindarán un mayor control en los accesos a los usuarios y evitar accesos innecesarios y que además de generar improductividad ponen en riesgo la seguridad de la información.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Se desarrolló el levantamiento de los activos de información de la empresa clasificados por su criticidad.

2. Se realizó la definición de políticas de seguridad perimetral alineadas a la ISO 27001.

3. Se implementó un IPS que ayudó a dar visibilidad en los intentos de intrusión a la empresa.

4. Se identificaron las vulnerabilidades del servidor web expuesto donde se aloja el portal transaccional de la organización y se realizó la remediación de la vulnerabilidad crítica dejando como pendiente al Jefe de TI la remediación de las vulnerabilidades de nivel medio y bajo.

5. Se definieron procedimientos de revisión periódica de las reglas de filtrado en el firewall con la finalidad de depurar reglas según las necesidades del negocio y dejar sin efecto accesos no necesarios.

Recomendaciones

1. Actualizar el inventario de activos de empresa conforme la empresa vaya adquiriendo nuevos servicios.

2. Incluir las políticas y controles establecidos en el presente proyecto de titulación en el esquema de seguridad informática de Financiera Lago Azul.

3. Afinar las políticas del IPS debido a nuevas amenazas que puedan aparecer así como también monitorear a través de alertas los intentos de intrusión.

4. Utilizar una versión licenciada del software de análisis de vulnerabilidades que permita generar reportes de resultados impresos completos.

5. Elaborar un cronograma de trabajo para resolver las vulnerabilidades de nivel medio y bajo encontradas en el análisis efectuado y de igual manera establecer análisis periódicos para mitigar nuevas vulnerabilidades

6. Programar ventanas de mantenimiento para lo siguiente:

    - Actualizar el cortafuegos perimetral de su software base

    - Implementar las reglas de filtrado establecidas en el presente proyecto de titulación.

    - Resolver las vulnerabilidades encontradas en el análisis efectuado.

BIBLIOGRAFÍA

[1] Código Orgánico Integral Penal. Sección Tercera. Delitos contra la seguridad de los activos de los sistemas de información y comunicación. Art. [329-234]. Vigente desde Agosto 2014.

[2] Northcutt, S., Zeltser, L., Winters, S., Kent, K., & Ritchey, R. W. (2005). Inside Network Perimeter Security (Inside). Sams.

[3] EC-Council (2011). Network Defense: Security Policy and Threats. Cengage Learning, 2-3.

[4] Astudillo B. Karina (2013). Hacking Ético 101. Cómo hackear profesionalmente en 21 días o menos!, 63,96,93-94.

[5] Easttom Chuck (2012). Computer Security Fundamentals. Second Edition, 72-84.

[6] Wallace Kevin (2015). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide,701,705-707.

[7] Americas Headquarters Cisco Systems, Inc. Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S, 1-2.

[8] Cisco Systems, Inc. (2012). Cisco ASA Series Firewall CLI. Configuration Guide, 12-16.

[9] Cisco Systems, Inc. (2003). Designing Perimeter Security. Student Guide.

[10] Lawrence C. Miller, CISSP (2011). Next-Generation Firewalls For Dummies, 27, 59-62.

[11] SANS Institute (2001). Intrusion Detection Systems: Definition, Need and Challenges, 3-4.

[12] Sequeira Dinesh (2002). Intrusion Prevention Systems – Security's Silver Bullet?. SANS Institute, 7.

[13] Purdy Gregor N. (2004). Linux iptables pocket reference, 1-6.

[14] COSO (2004). Entrerprise Risk Management – Integrated Framework. Executive Summary, 2.

[15] Ministerio de Hacienda y Administraciones Públicas (2012). MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método, 9.

[16] Isaca. (2009). Marco de Riesgos de TI. ISACA, 12

[17] Isaca. (2008). Definición de Gerencia de la seguridad de la información. Requerimientos de la posición. Orientación para ejecutivos y gerentes. ISACA, 11.

[18] ISO (International Standard Organization). (2009). Gestión de Riesgos – Principios y guías. NORMA INTERNACIONAL ISO 31000.

[19] ISO (International Standard Organization). (2008). Tecnología de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información. Estándar de Seguridad ISO/IEC 27005:2008

[20] Ramírez, A., Ortiz, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. En: Ingeniería, Vol. 16, No. 2, pág. 56-66.

[21] ISO (International Standard Organization). (2013). Information Technology – Security techniques – Information security management systems - Requirements. International Standar ISO/IEC 27001:2013

[22] ISO (International Standard Organization). (2013). Information Technology – Security techniques – Code of practice for information security controls. International Standard ISO/IEC 27002:2013