Implementación de Herramientas open source para mejorar la seguridad en pequeños callcenter

Diego Alejandro Rodríguez, Diego Ferney Paramo, James Orlando Patiño, Luis Carlos Ruiz

Especialización seguridad informática, Fundación Universitaria Compensar

Proyecto fin de grado (Seguridad informática basada en sistemas open source)

Jaime Andrés Chaparro Sánchez

Marzo de 2024

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

Implementación de Herramientas open source para mejorar la seguridad en pequeños callcenter

Diego Alejandro Rodriguez, Diego Ferney Paramo, James Orlando Patiño, Luis Carlos Ruiz

Trabajo de grado presentado como requisito parcial para optar al título de:

Especialista En Seguridad Informática

Director (a):

Ingeniero(a), Jaime Andres Chaparro Sanchez

Codirector (a):

Línea de Investigación:

Ingeniería de Sistemas

Grupo de Investigación:

Seguridad Informática

Fundación Universitaria Compensar

Facultad de Ingeniería, Ingeniería de (Especialización en Seguridad Informática)

Bogotá, Colombia

2024

Internal

Resumen

El presente proyecto tiene como objetivo fortalecer la seguridad de las comunicaciones telefónicas las cuales son fundamentales para tener un entorno seguro y efectivo en pequeñas empresas que no cuentan con un presupuesto suficiente para adquirir grandes implementaciones (dispositivos de seguridad perimetral).

Con el aumento de las amenazas cibernéticas es fundamental implementar medidas de seguridad adecuadas, es por ello por lo que se plantea mejorar la seguridad de una planta telefónica Issabel que comúnmente son utilizadas en pequeñas empresas al estar basadas en sistemas de código abierto especialmente para empresas dedicadas a call center.

El proyecto se llevó a cabo utilizando un enfoque práctico en un ambiente virtualizado y controlado que incluirá el análisis de la infraestructura actual de la planta telefónica Issabel y el hardering de la misma, la instalación y configuración de un Firewall (Pfsense) Open Source junto con los servicios open vpn e IDS/IPS de acuerdo con lo requerido, para posteriormente llevar a cabo las pruebas necesarias con las cuales se pretende evaluar su rendimiento y efectividad teniendo como resultado la documentación de todo el proceso en el cual se dan a conocer las recomendaciones y conclusiones obtenidos en el desarrollo de los laboratorios.

Se espera que este proyecto proporcione las mejoras necesarias que en los dispositivos propuestos y poder aumentar la seguridad del servidor de telefonía ip, garantizando la confidencialidad, integridad y disponibilidad de las comunicaciones telefónicas.

Palabras clave:
Open source, firewall, hardering, IDS/IPS.

Abstract

The present project aims to strengthen the security of telephone communications, which are essential for maintaining a secure and effective environment in small businesses that do not have a sufficient budget to acquire large-scale security implementations (perimeter security devices).

With the increasing cyber threats, it is crucial to implement adequate security measures. Therefore, the objective is to enhance the security of an Issabel phone system, which is commonly used in small businesses and is based on open-source systems, especially for companies dedicated to call centers.

The project was carried out using a practical approach in a virtualized and controlled environment. This involved analyzing the current infrastructure of the Issabel phone system and hardening it, as well as installing and configuring an Open-Source Firewall (Pfsense) along with the open VPN and IDS/IPS services as required. Subsequently, necessary tests were conducted to evaluate its performance and effectiveness, resulting in the documentation of the entire process, including the recommendations and conclusions drawn from the development of the laboratories.

It is expected that this project will provide necessary improvements in the proposed devices and increase the security of the IP telephony server, ensuring the confidentiality, integrity, and availability of telephone communications.

Keywords:
Open source, firewall, hardening, IDS/IPS.

Contenido

PÁG.

RESUMEN ..... **V**

INTRODUCCIÓN **9**

ANTECEDENTES Y JUSTIFICACIÓN 10
FORMULACIÓN DEL PROBLEMA 11
OBJETIVO GENERAL 11
Objetivos Específicos *11*
ALCANCES Y LIMITACIONES 12

1. MARCO TEÓRICO **14**

1.1 VIRTUALIZACIÓN MEDIANTE LA HERRAMIENTA VIRTUALBOX 14
1.2 FIREWALL PFSENSE 15
1.3 ISSABEL PBX 16

2. DISEÑO METODOLÓGICO **18**

2.1 PLANIFICAR 18
2.2 HACER 19
2.3 COMPROBAR 19
2.3.1 Servicios En Issabel *20*
2.3.2 Servicios En Firewall (Pfsense) *21*
2.4 HACER / AJUSTAR 21

3. CONCLUSIONES Y RECOMENDACIONES **22**

3.1 CONCLUSIONES 22
3.2 RECOMENDACIONES 23
3.3 BIBLIOGRAFÍA 24

Introducción

El auge de internet de la mano de la relevancia actual de la información, abren una brecha de vulnerabilidades, creando una gran tendencia a romper las barreras de seguridad implementadas en los sistemas de información, las soluciones de seguridad deben tener como premisa los siclos de mejora continua, los cuales garanticen la protección de la información y sistemas.

En el contexto actual de las comunicaciones empresariales, la seguridad de la red y la protección de los datos son prioridades fundamentales para cualquier organización, es esencial contar con soluciones robustas y confiables para salvaguardar la integridad de la infraestructura tecnológica.

En este sentido, la combinación de un firewall potente y una plataforma telefónica eficiente se convierte en un enfoque integral para garantizar la seguridad y la estabilidad de las comunicaciones de pequeños call center. En este proyecto, se propone implementar el firewall Open Source pfsense en conjunto con la plataforma telefónica Issabel, brindando una solución completa y escalable que cumpla con los más altos estándares de seguridad.

A lo largo de este proyecto, se explorarán los pasos necesarios para integrar los servicios del firewall pfSense con la planta telefónica issabel, optimizando la configuración para maximizar la protección mientras se mantiene la funcionalidad y el rendimiento de la plataforma telefónica.

Antecedentes y Justificación

El auge de los pequeños call center impulsados en su crecimiento del 30 por ciento a partir de la pandemia según estudio realizado por ZENDESK en Colombia, (Zendesk, 2022). estos centros telefónicos están divididos en tres grupos, inbound que se centra en la recepción de llamadas, outbound se encarga de la salida de llamadas y blended el cual combina la entrada y salida de llamadas, los cuales se caracterizan por implementación con bajos recursos convirtiendo a Colombia en el cuarto país en el mercado latinoamericano en servicios tercerizados de callcenter según la asociación colombiana de BPO (Asociación colombiana de BPO, 2022), para el año 2023 el sector represento un 2.8 por ciento del PIB colombiano según portafolio, caracterizándose por la mano de obra económica, esto implica a su vez el incremente exponencial de los riesgos a nivel de seguridad que se pueden presentar en el ámbito de las comunicaciones empresariales, la protección de los sistemas de telefonía IP es de suma importancia, plataformas telefónicas modernas como Issabel ofrecen una amplia gama de servicios y funcionalidades, pero al estar conectadas a redes públicas e Internet, se vuelven vulnerables a ataques maliciosos que podrían comprometer la confidencialidad, integridad y disponibilidad de las comunicaciones empresariales.

Es evidente la necesidad de brindar una solución que garantice la seguridad y la estabilidad de las comunicaciones en los pequeños call center. Factores como los bajos recursos para su implementación impiden blindarse con seguridad en sus sistemas de información, al realizar la implementación de sistemas open source enfocado en la infraestructura de la planta telefónica Issabel, se adquiere una protección robusta garantizando la operabilidad y continuidad del negocio al mitigar los riesgos de ataques cibernéticos.

Formulación del Problema

¿De qué manera se puede implementar una infraestructura segura basada en sistemas open source que permita detectar, prevenir intrusiones y ataques a una planta telefónica issabel?

Objetivo General

- Implementar una infraestructura segura para la planta telefónica issabel.

Objetivos Específicos

- Implementar un dispositivo de seguridad perimetral (pfsense) enfocando en la infraestructura de una planta telefónica, que se garantice la accesibilidad de manera remota para los empleados y/o propietarios de pequeñas empresas con recursos limitados.

- Configurar políticas de seguridad en el firewall pfsense para detectar y prevenir intrusiones y ataques (IDS/IPS).

- Realizar un correcto hardering en el servidor issabel para prevenir ataques de fuerza bruta.

Alcances y Limitaciones

El presente proyecto se basa en una prueba de concepto por medio del cual se pretende demostrar como a través de sistemas open source es posible mitigar posibles ataques que pongan en peligro los pilares de la seguridad de la información.

Es por ello por lo que se plantea un escenario de pruebas controlado y virtualizado en la herramienta virtual box escenario que contempla:

Firewall perimetral del fabricante pfsense en el cual se configura servicios básicos y reglas necesarias para un funcionamiento inicial, a nivel de detenciones se utiliza el servicio snort para realizar el filtrado a nivel IDS/IPS dicho servicio queda a nivel de detención mas no de bloqueo puesto que los requerimientos dependen de las necesidades de cada empresa y el nivel de agresividad va a variar con el pasar del tiempo post implementación, las reglas de filtrado se obtienen de la comunidad de snort y se ajustan al presente proyecto.

Se realiza la configuración del servicio openvpn el cual incluye la creación del ente certificador y los certificados necesarios para establecer los túneles, se crean las reglas del firewall para permitir el acceso al servidor issabel de manera segura por medio del túnel creado con anterioridad, este túnel se establece a nivel de pruebas puesto que al ser un laboratorio no se cuenta con un peer público y al tratarse de una red LAN no es posible establecer conectividades a nivel de red WAN, las reglas de acceso a los distintos segmentos y/o rutas se pueden definir de acuerdo a los evolutivos o requerimientos de cada empresa.

En la planta telefónica issabel al estar basada en una distribución de Linux se realizará la construcción de un script el cual realizara la creación y configuración a nivel de certificados auto firmados para consumos por el puerto seguro 443 en la interfaz web, se implementan las configuraciones básicas con unas extensiones tipo SIP y un

hardering inicial el cual incluye contraseñas seguras asignadas de acuerdo con roles y perfiles.

La configuración del servicio fail2ban se establece de acuerdo con la documentación del fabricante dejando el bloqueo de ip por un periodo de 12 horas para evitar posibles ataques de denegación de servicio y/o instrucciones la configuración queda sujeta a cambios post implementación y comportamiento del servidor no se establecen listas negras o blancas ya que se deben definir en concordancia a la empresa y los servicios.

Las configuraciones definidas con anterioridad se dan por un grupo de 4 ingenieros con arduo conocimiento en infraestructura, seguridad e implementación de sistemas open source y toma un tiempo de 27 días calendario con un esfuerzo diario de 8 horas.

Al tratarse de un laboratorio virtualizado se tiene como limitación el estar atados al performance reducido de las maquinas host en el cual se desplego el virtualizador y las maquinas alojadas.

Las pruebas de funcionabilidad son limitadas puesto que no se cuenta con una ip publica para poder levantar los túneles de la vpn en un escenario real.

Los certificados auto firmados son funcionales porque encriptan la conexión y se ajusta a la prueba de concepto dada, pero no son expedidos por un ente certificador pago ni va a contar con saltos de validación.

1. Marco teórico

Para la elaboración de la presente prueba de concepto, se realizó una investigación acerca de la manera de simular ataques y analizar vulnerabilidades sin que resulte complicado de manera para el usuario, además de las herramientas que deben contener para que sea un complemento al conocimiento teórico empresarial como call center de planta telefónica Issabel.

Durante la investigación se trabajaron como temas los componentes de un sistema de información tales como: Software, Virtualización, Sistemas Operativos, datos y métodos.

La seguridad informática se basa principalmente en tres puntos fundamentales: integridad, disponibilidad y confidencialidad. Actualmente la información sobre la variedad de ataques informáticos a diferentes sistemas muy extensa. Puesto que se puede encontrar información acerca de todo tipo de ataques y a su vez, las posibles soluciones o recomendaciones para mitigar las vulnerabilidades ante un tipo de ataque de hombre en el medio (C. L. Coloma Almeida, 2018).

1.1 Virtualización mediante la herramienta VirtualBox

La virtualización de sistemas operativos toma fuerza desde los años 90, el objetivo principal de esto trata de que por medio de un software en este caso VirtualBox sea capaz de crear varias máquinas virtuales.

Al utilizar entornos virtuales en las pruebas de pentesting, facilita el trabajo para un hacker ético ya que de esta forma se tiene control de las vulnerabilidades que se encuentran en todo su proceso. En la actualidad, las herramientas de seguridad son muy versátiles en distintas versiones, como aplicaciones de escritorio, aplicaciones web y sistemas operativos completos como es el caso de Kali Linux.

VirtualBox es un software de virtualización elaborado por la empresa alemana (innotek GmbH). Actualmente es desarrollado por la empresa Oracle, este software permite instalar sistemas operativos adicionales, cada uno independiente del otro. (Oracle, 2020)

Uno de los principales aspectos considerados para el desarrollo del presente proyecto, fue el uso de un sistema operativo totalmente distinto a las plataformas más comunes como Windows o de herramientas licenciadas, como es el caso de las herramientas utilizadas para la virtualización de los servidores y la administración de estos, en lugar de aquello, se utilizó herramientas de código abierto.

1.2 Firewall Pfsense

Es una distribución de firewall de red gratuita, basada en el sistema operativo FreeBSD con un kernel personalizado e incluye paquetes de software gratuitos de terceros para una funcionalidad adicional. El software pfsense, con la ayuda del sistema de paquetes, puede proporcionar la misma funcionalidad o más de los firewalls comerciales comunes, sin ninguna de las limitaciones artificiales. (FreeBSD, 2013).

Pfsense incluye características similares a la mayoría de los firewalls comerciales. También características adicionales que no están disponibles en soluciones de código cerrado comerciales, tales como: Check Point, Cisco PIX, Palo Alto, SonicWall entre otros.

La consultoría es de tipo descriptiva, ya que se analizaron y describieron las características y ventajas del Firewall Pfsense como opción gratuita para la seguridad en call centers. Además, se hizo un diagnóstico de las percepciones relativas a la seguridad informática de parte de los encargados de los centros de cómputo, de los directores y de las medidas o políticas utilizadas. (kali by offensive security, 2019)

1.3 Issabel PBX

Desde el momento en que Elastix fue adquirida por 3CX surgió Issabel, el cual seguiría con la tranquilidad, continuidad y soportes necesarios para seguir con el desarrollo de PBX con el apoyo de la comunidad la cual estaría compuesta por expertos, empresas, colaboradores y público en general diseñada para brindar gran capacidad de llamadas simultáneas usando la infraestructura de red actual, la central IP se integra con la red de telefonía pública ofreciendo comunicación VoIP dentro y fuera de la oficina.

Usted puede mantener anexos remotos en otra ciudad o país conectándolos por internet, o interconectar sucursales en ubicaciones remotas por medio de un acceso a internet, reduciendo significativamente los costos de comunicación entre las mismas. Esta tecnología también permite el uso de los computadores como teléfonos por medio de Softphone instalado en los mismos, o teléfonos tradicionales por medio de adaptadores especiales, todo sobre la red LAN que usted posea. (Murillo, R., 2015).

Según Jesús Armando Yépez Jiménez Issabel tiene las siguientes características "Soporte para protocolos SIP, IVR configurable y flexible, soporte para sinterización de voz, herramienta para la creación de extensiones por lote, Identificación de llamadas (Caller ID), Cancelador de eco integrado, troncalización, soporte para grupos de timbrado, Panel de Operador basado en Web". (E. Tanya and P. Mancilla, 2019), (Defaz Parra Kevin Andrés, Salazar Barrionuevo Darwin Stalin, 2020).

- OpenSSL

Es una implementación de código libre de protocolo SSL (secure sockets layer) utilizada para establecer comunicaciones seguras en la red, fue creado por la necesidad de realizar envió de datos brindando confidencialidad y seguridad a través de la red para esto era necesario autenticar al destinatario. La información puede ser capturada en su trayecto es por ello por lo que se necesita que las comunicaciones viajen protegidas,

como alternativa, para esto actualmente se cuenta con el protocolo SSL cuyo funcionamiento se describe a continuación:

El protocolo SSL es un protocolo en base a la comunicación que se encuentra en el conjunto de protocolos sobre TCP/IP, este protocolo concede a los usuarios servicios de comunicaciones seguras entre cliente y servidor a través de certificados, mediante firmas digitales y mediante encriptación usando una variedad de algoritmos para el cifrado y firmas. (T. Diaz, 2006).

Una de las principales funciones de esta herramienta es ofrecer certificados para el uso con aplicaciones. Los certificados garantizan que las credenciales de una entidad o individuo son válidas proveyendo autenticación. Estos certificados digitales deben ser verificados por una de las diversas autoridades certificadoras "CA" (T. Rhodes, 2020).

- Openvpn

Según (Bucsa, R, 2020) definió en su investigación a las conexiones de tipo VPN de acceso remoto a aquellas conexiones que utilizan la tecnología de tunelización para las conexiones de usuarios en puntos geográficos distintos, para ello se crea un túnel a través del servicio público de internet que conecta el servidor VPN y los usuarios remotos, los demás usuarios que lo intentan solo conectados mediante internet, no obtendrán acceso al túnel.

- Fail2Ban

Es una herramienta (aplicación) de código abierto que permite bloquear a aquellos que intenten vulnerar servicios como SSH, protocolo para transferencia simple de correo (SMTP, del inglés Simple Mail Transfer Protocol), protocolo de transferencia de hipertextos (HTTP, del inglés Hypertext Transfer Protocol), etcétera, mediante el intento de fuerza bruta. Cuando Fail2ban encuentra reiterados intentos de sesión fallidos desde una misma IP rechaza estos intentos de conexión y los bloquea con reglas de Iptables, es decir, cuando alguien intenta conectarse muchas veces Fail2ban lo bloquea y lo pone en su tabla entonces no deja que vuelva a intentar conectarse. (Fail2Ban, 2015).

2. Diseño Metodológico

Partiendo del análisis de los posibles riesgos más latentes junto con la manera de solventarlos se implementa el presente laboratorio por medio del ciclo PDCA o Deming siguiendo los pasos establecidos de la siguiente manera Identificar, planificar, implementar y Resultados.



Figura 1Ciclo PDCA: https://www.researchgate.net/figure/Figura-3-Metodologia-de-los-7-pasos-Ciclo-PDCA-Fuente-Elaboracion-Propia-Por-otra_fig1_316911482

2.1 Planificar

En el transcurso de esta fase se realizó un análisis de las múltiples vulnerabilidades con el fin de identificar las soluciones a los mismos, la mayoría de estos riesgos posiblemente se materializaron en la pandemia del COVID y la transición que se tuvo en las empresas al modelo de trabajo.

Con la finalidad de solventar los posibles riesgos identificados y utilizar sistemas de bajos costos se formula la presente prueba de concepto la cual al momento de presentarla se encuentra de manera funcional en el laboratorio la cual es aplicable a cualquier tipo de empresa.

2.2 Hacer

En esta fase se realizaron las implementaciones de servicios en el firewall y en el servidor issabel, teniendo como base el siguiente diagrama de infraestructura a alto nivel se logra comprender el funcionamiento de las soluciones propuestas en cada uno de los sistemas que intervienen y la manera en la que se llevó a cabo la configuración de cada uno.

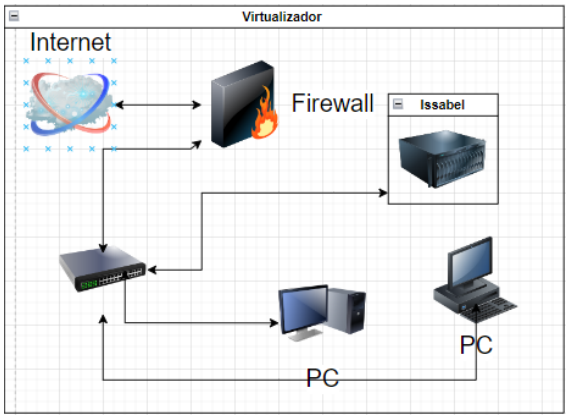


Figura 2 Diagrama de infraestructura: Elaboración propia

2.3 Comprobar

En esta fase se busca destacar los resultados obtenidos en los dispositivos propuestos, esto implica la presentación de los servicios y sus respectivos funcionamientos en los dispositivos con los que se pretende fortalecer los controles de seguridad de cada equipo.

2.3.1 Servicios En Issabel

En issabel se realiza validación de que cuente con las actualizaciones necesarias para poder instalar los servicios fail2ban, el cual es un servicio que funciona para distintas distribuciones de Linux siendo un potente detector de ataques de fuerza bruta.

Fail2ban cumple con la función de supervisar las entradas de los archivos de registro de los distintitos protocolos como son SSH o FTP, los cuales son utilizados muy frecuentemente para la administración del servidor al detectar demasiados intentos fallidos que se hacen desde una o más ip procede a bloquearla durante cierto periodo de tiempo impidiendo que se establezcan conexiones.

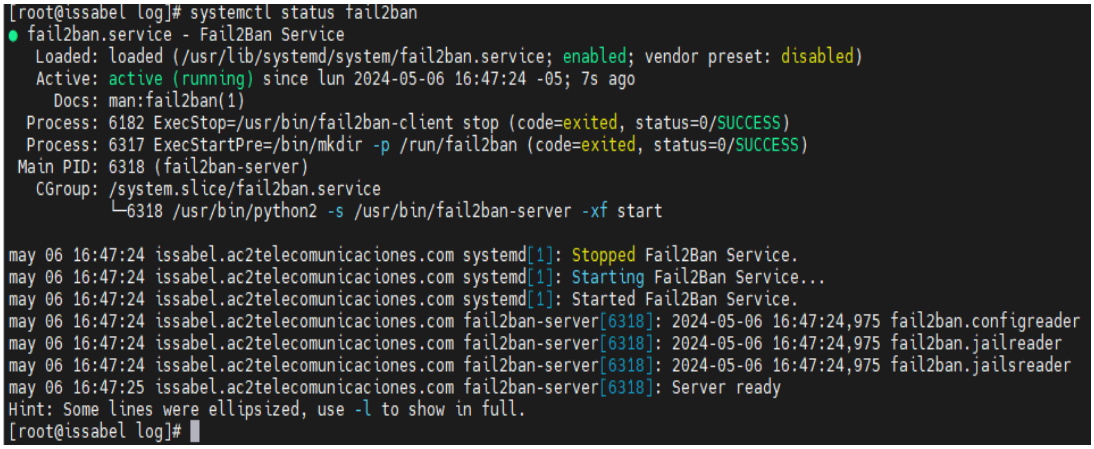


Figura 3 Servicio Habilitado en issabel: Elaboración propia

El periodo de bloqueo de las ip es definido de acuerdo con los requerimientos de las empresas pudiendo dejar bloqueados los orígenes por periodos de tiempo o definitivamente.

Como otra medida de seguridad se realiza la implementación de certificados de seguridad auto firmados para cifrar las conexiones por el puerto 443 y así asegurar una conectividad segura con la cual se puede acceder a la administración grafica del servidor.

2.3.2 Servicios En Firewall (Pfsense)

En el firewall perimetral pfsense se realiza las configuraciones iniciales y se ajusta al funcionamiento básico que comprenden direccionamiento ip (DHCP), servicios de redireccionamiento DNS, logs de eventos para el firewall y adicional se realiza la instalación y configuración de los servicios Snort y Openvpn.

Snort es un servicio que se desarrolla para realizar los filtrados IDS/IPS en el firewall se puede realizar la configuración de las reglas que tiene la comunidad y son de manera gratuita, como también se pueden implementar reglas pagas mucho más robustas y específicas las cuales permiten realizar el filtrado a las interfaces WAN y LAN en modo bloqueo o detención.

Con el fin de contribuir o apoyar el modelo de trabajo hibrido o trabajo en casa se configuran vpn sitio a sitio (s2s) en el firewall dando acceso a los usuarios al servidor issabel para que así se pueda atender de manera remota el call center o la operación.

2.4 Hacer / Ajustar

En esta fase se establecen las implementaciones que se deberían de ajustar a la necesidad de cada empresa que decida llevar la presente prueba de concepto sus premisas u operaciones.

De acuerdo con los resultados obtenidos en el ítem que antecede se debe de ajustar los servicios de snort, fail2ban y openvpn a la necesitad de la empresa.

El script utilizado en el laboratorio con el fin de generar los certificados auto firmados es ajustable y se debe de definir de acuerdo con las políticas de seguridad de la empresa.

3. Conclusiones y recomendaciones

3.1 Conclusiones

- Implementación del Dispositivo de Seguridad Perimetral (pfsense): Se logró con éxito la implementación del firewall pfsense, teniendo como foco la protección de la planta telefónica issabel. la implementación garantiza una sólida protección garantizando así la accesibilidad remota para empleados y propietarios de pequeñas empresas con recursos limitados.

- Configuración de Políticas de Seguridad: Se establecieron y configuraron políticas de seguridad detalladas en el firewall pfsense, para detectar y prevenir intrusiones y ataques. la seguridad establecida ha demostrado ser efectivo para mitigar riesgos y proteger la planta telefónica issabel contra amenazas.

- Hardering del Servidor Issabel: Se implementaron medidas de hardering exitosas en el servidor Issabel, dirigidas a prevenir ataques de fuerza bruta, Generando así acciones que contribuyen significativamente a la integridad de la planta y a su funcionamiento.

3.2 Recomendaciones

- Muchas industrias, incluida la de telecomunicaciones, están sujetas a regulaciones estrictas en materia de seguridad y protección de datos. Se recomienda hacer revisión del uso de los controles y regulaciones para la configuración de políticas de seguridad que también demuestra un compromiso con la protección de la información sensible y la privacidad de los usuarios.

- Pese a que los certificados autofirmados son muy funcionales y cumplen con los requerimientos de uso interno, se recomienda que estos sean firmados por entidades certificadoras si se quiere llevar a cabo la publicación de los servidores.

- orientados en la seguridad de las comunicaciones telefónicas de pequeñas empresas con recursos limitados, se recomienda demostrar el compromiso de la empresa con estándares de seguridad elevados, lo cual es esencial al momento de ganar y mantener la confianza de los clientes. Además, esta práctica asegura que, incluso con soluciones de bajo costo, la empresa cumple con las normativas vigentes y minimiza los riesgos asociados a las amenazas cibernéticas.

3.3 Bibliografía

Zendesk (2022) Call center creció un 30% durante la pandemia, impulsado por el comercio en línea.https://www.zendesk.com.mx/blog/estructura-call-center/

Asociación colombiana de BPO (2022) colombia es el cuarto mayor mercado en Latinoamérica en servicios tercerizados después de Brasil, México y Costa Rica https://www.bpro.org/

Cámara Colombiana de ciberseguridad (2023) Informe anual de ciberseguridad chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ccit.org.co/wp-content/uploads/estudio-anual-de-ciberseguridad.pdf

Kaspersky Daily (2023) Nueva epidemia: el phishing se sextuplicó en América Latina con el reinicio de la actividad económica y el apoyo de la IA https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/

Infobae (2023) Panorama cibernético https://www.infobae.com/tecno/2023/08/24/panorama-cibernetico-2023-america-latina-bajo-asedio-de-los-criminales-por-aumento-de-ataques/

C. L. Coloma Almeida, «repositorio.ug.edu.ec,» 2018. [En línea]. Available: http://repositorio.ug.edu.ec/bitstream/redug/35450/1/B-CINT-PTGN.378%20Almeida%20Coloma%20Cesar%20Leonardo%20.%20Pincay%20P% c3%a1rraga%20Jasson%20Alfredo.pdf. [Último acceso: diciembre 2020].

Oracle, «VirtualBox,» [En línea]. Available: https://www.virtualbox.org/. [Último acceso: diciembre 2020].

kali by offensive security, «kali linux,» 25 noviembre 2019. [En línea]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/. [Último acceso: agosto 2020].

T. Diaz, «blyx.com,» 06 Julio 2006. [En línea]. Available: https://blyx.com/public/docs/security/Usando_OpenSSL_en_el_mundo_real.pdf. [Último acceso: diciembre 2020].

T. Rhodes, «www.freebsd.org,» [En línea]. Available: https://www.freebsd.org/doc/es_ES.ISO8859-1/books/handbook/openssl.html. [Último acceso: diciembre 2020].

FreeBSD (13 de noviembre de 2013). ¿Qué es FreeBSD? Recuperado de https://www.freebsd. org/es/about.html.

Murillo, R. (21 de agosto de 2015). PfSense: Instalación y Configuración del Firewall, NAT, DHCP y DNS [Video]. Recuperado de https://www.youtube.com/watch?v=HR1aTQP6oO8

E. Tanya and P. Mancilla, "Universidad De Guayaquil Tutor:," p. 83, 2019.

Defaz Parra Kevin Andrés, Salazar Barrionuevo Darwin Stalin (2020), "Implementación de una central telefónica voz IP utilizando software libre Issabel PBX y comunicaciones unificadas basado en Asterisk en la constructora MA Construcciones". http://repositorio.utc.edu.ec/handle/27000/8609

BUCŞĂ, R., 2020. Teleworking and Securing Data with VPN Technology. [en línea], vol. 23, no. 1/2020, pp. 78-86. Disponible en: http://web.b.ebscohost.com/ehost/detail/detail?vid=8&sid=c3470a3d-edc0-4bb6-8bd4-dcad6f97ec4d%40pdc-vsessmgr03&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=144538821&db=bth

Fail2Ban para protección contra intentos de conexión. 2015. Recuperado de https://soporte.itlinux.cl/hc/es/articles/200121798-Fail2Ban-para-protecciónn-contra-intentos-de-conexión.