OFICINA DE POSGRADOS

Tema:

IMPLEMENTACIÓN DE SEGURIDAD DE VOIP ELASTIX EN LA EMPRESA LÁCTEOS GUSTALAC LA POLACA

Proyecto de Investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de investigación:

SEGURIDAD DE LA INFORMACIÓN

Autor:

Wiliam David Lam Cheang

Director:

Ing. Alberto Leopoldo Arellano Aucancela, Mg.

Ambato – Ecuador

Julio 2023

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

IMPLEMENTACIÓN DE SEGURIDAD DE VOIP ELASTIX EN LA EMPRESA LÁCTEOS GUSTALAC LA POLACA

Línea de investigación:

Seguridad de la información

Autor: Wiliam David Lam Cheang

Alberto Leopoldo Arellano Aucancela, Ing. Mg. f. _____
CALIFICADOR

Verónica Maribel Pailiacho Mena, Ing. Mg. f. _____
CALIFICADOR

Galo Mauricio López Sevilla, Ing. Mg. f. _____
CALIFICADOR

Juan Carlos Acosta Teneda, P. PhD. f. _____
COORDINADOR DE POSGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f. _____
SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
DIRECCIÓN CENTRO DE POSGRADOS
Sede Ambato
Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL PROCURADURÍA

Ambato – Ecuador

Junio 2023

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **WILIAM DAVID LAM CHEANG** con cédula de ciudadanía 1203014350, autor del trabajo de graduación intitulado: **"IMPLEMENTACIÓN DE SEGURIDAD DE VOIP ELASTIX EN LA EMPRESA LÁCTEOS GUSTALAC LA POLACA",** previa a la obtención del título profesional de **MAGÍSTER EN CIBERSEGURIDAD**, en la escuela de POSGRADOS.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, julio 2023

Wiliam David Lam Cheang

CC. 1203014350

DEDICATORIA

Dedicó a Dios por darme la vida, su gracia y su misericordia cada día de mi vida. A mi esposa y compañera de vida Mercedes, por su apoyo incondicional que me impulsa a ser una mejor persona, ser un mejor profesional y animarme para alcanzar las metas trazadas.

A mis hijas Sunney y Mei Ling que son los tesoros de mi vida que Dios me regaló, ellas son la razón de seguir esta maestría, mostrarles que no importa la edad y obstáculo que nos impida alcanzar nuestras metas.

AGRADECIMIENTOS

Agradezco a Dios por darme la oportunidad de volver a estudiar, El conoce los deseos de mi corazón, por la sabiduría y capacidad para entender las enseñanzas impartidas por cada profesor.

De manera especial quiero agradecer a cada profesor que aportó sus conocimientos para mi desarrollo académico y profesional, por ello, tengo buenos recuerdos y experiencias adquiridos en cada clase.

Sobre todos quiero agradecer a mi esposa Mercedes y mis hijas Sunney y Mei Ling por su apoyo incondicional, por sacrificar sus tiempos y darme las fuerzas para culminar esta meta.

RESUMEN

En este proyecto de investigación tiene como principal objetivo de desarrollar una guía en la implementación de seguridad VoIP Elastix en la empresa Lácteos Gustalac La Polaca, el cual garantice una mayor seguridad frente a los ataques informáticos, que ocasiona la perdida de la información o daños en la infraestructura, lo cual afecta económicamente y también a la imagen de la empresa frente a sus clientes. En el proyecto, se hallaron algunas vulnerabilidades que pone en riesgo la información privada de la empresa como: puertos abiertos, no tener contraseñas seguras para cada usuario, no tener habilitado una encriptación que garantice un seguro envió y recepción de datos entre el servidor y el cliente, todas estas brechas que pone en riesgo la confidencialidad fueron mitigadas en gran parte. En el capítulo 1, se verá las problemáticas que surgen en la seguridad de las redes relacionados a los servidores VoIP Elastix, así como también las posibles soluciones, que se dan en estos casos. En el siguiente capítulo 2, se verá el diseño metodológico donde, se abordará como va implementar la solución, en la metodología, se basará el proyecto de investigación para lograr resultados confiables y por último en el capítulo 3, se mostraran los resultados obtenidos de las mejoras que realizaron sobre la infraestructura VoIP de posibles vulnerabilidades y las soluciones propuestas para mitigarlas, las cuales están afecta a la seguridad: disponibilidad, integridad y confidencialidad de la comunicación en la empresa de Lácteos Gustalac la Polaca.

Palabras claves: VoIP, Elastix, seguridad de la comunicación, vulnerabilidad

ABSTRACT

The main objective of this research project is to develop a guide in the implementation of VoIP Elastix security in the company Lácteos Gustalac La Polaca, which ensures greater security against computer attacks, which could cause the loss of information or damage to the infrastructure, which would affect economically and also the image of the company in front of its customers. Some vulnerabilities were found in the project that put the company's confidential information at risk, such as open ports, not having passwords for each user, not having encryption enabled that guarantees secure data exchange between the server and the client, all of these breaches that put confidentiality at risk were largely mitigated. In chapter 1 you will see the problems that arise in network security related to Elastix VoIP servers, as well as the possible solutions that can be given in these cases. In the next chapter 2 you will see the methodological design where it will be addressed how the solution will be implemented, on which methodology the research project will be based to achieve reliable results, finally in chapter 3, the results that we have obtained, the improvements that were made, on the VoIP infrastructure of possible vulnerabilities will be shown. and the proposed solutions to mitigate them, which are affecting security: availability, integrity, and confidentiality of communication in the Lácteos Gustalac la Polaca company.

Keywords: VoIP, Elastix communication security, vulnerability.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La tecnología VOIP, se desarrolló a mediados del año 1980, esta tecnología de comunicación conocida como Protocolo de Voz sobre Internet, realiza la transmisión de señales de voz en tiempo real. Los servicios de VOIP convierten el paquete de voz del teléfono en un paquete de voz digital que viaja a través de la red LAN o por vía del Internet.

Debido a la gran utilidad de VOIP, muchas de las empresas a nivel global han visto la necesidad de implementar este tipo de servicio para la comunicación entre sus localidades remotos y móviles. Pero también han ignorado las vulnerabilidades que presentan en estos servicios, los problemas de seguridad son muy similares a la seguridad de la red LAN.

La tecnología VoIP al igual que las demás, se encuentra expuesta a muchas amenazas de seguridad, con la creciente implementación de este servicio también ha aumentado las preocupaciones por la seguridad de las comunicaciones. VoIP es una tecnología que, se apoya en las diferentes capas y protocolos que ya están en las redes de datos. Es por esta razón que VoIP va a heredar algunos de los problemas de las capas y además los protocolos ya existentes tienen las amenazas más conocidas de VoIP y son problemas clásicos de seguridad, porque existen algunos ataques específicos de VoIP.

La metodología utilizada es OSSTM (Metodología Abierta de Testeo de Seguridad), esta permite la búsqueda de vulnerabilidades, donde procede a hacer comprobaciones en un sistema de red, además plantea un test de pruebas para comprobar la seguridad del servidor Elastix, para esto, se usan buenas prácticas de hacking ético, las cuales mediante comandos realizan ataques para detectar deficiencias en el sistema, para posteriormente mitigarlas.

Antecedentes

La Empresa Gustalac Lácteos La Polaca, se dedica a producir y distribuir avena de la propia marca a nivel nacional que está situada en la ciudad de Santo

Domingo de los Tsáchilas con varias agencias localiza en las ciudades de Guayaquil, Quito, Manta y Quevedo. En los años anteriores uno de los servidores sufrió un ataque informático, como consecuencia toda la información fue encriptada por un atacante, quien utiliza técnicas de ataques sofisticadas como Ransomware, encontró una vulnerabilidad en el protocolo RPC (Remote Procedure Call) a través del puerto 3389. Como efecto del ataque, se perdió toda la información dentro del servidor y la denegación de accesos remotos de los usuarios localizado en las diferentes agencias.

La empresa cuenta con un servidor en Elastix que es un software open source que integra la funcionalidad de PBX (“Private Branch Exchange”) en IP, mensajería y funciones corporativas. Este servidor tiene la función de Central telefónica de comunicación en los diferentes departamentos administrativos, operativos, las agencias y para sus clientes. En la actualidad este servidor no cuenta con la seguridad implementada, es vulnerable para la confidencialidad y disponibilidad de la comunicación de los medios VoIP.

Con fundamento de lo expuesto, se evidencia la necesidad de proteger la comunicación establecida por el servicio de VOIP entre las agencias, es de vital importancia mantener dicha comunicación, en el servidor está instalado el PBX Elastix. El problema radica en la inseguridad, debido al ataque que la empresa recibió en uno de sus servidores, generan preocupación de seguridad en su plataforma implementado de VOIP sobre Elastix, se ignoran las vulnerabilidades que existen o que un atacante logra infiltrar a la red de la empresa a través de estos protocolos que usa VOIP, provocan daños a los servicios existentes, denegación de servicios de comunicación, robo de credenciales para escuchar las conversaciones en línea y robo de identidad.

Planteamiento Del Problema

Un buen Servicio de Voz, se ha dado con el Protocolo de Internet (VoIP) que ha sido ampliamente implementado en algunas partes del mundo en los últimos años. Muchas de las organizaciones que implementaron los servicios VoIP no son conscientes o ignoran los problemas de seguridad y vulnerabilidades con

VoIP. Una red de VoIP también es susceptible de abuso, por la facilidad de explotar sus vulnerabilidades.

En la empresa Lácteos Gustalac La Polaca, VOIP es una de las aplicaciones más importantes. Que sirve para la comunicación de las agencias a nivel nacional. Sin embargo, presenta en el ámbito de la seguridad varios riesgos y vulnerabilidades, que exponen fallos en la integridad de los datos que los crackers consiguen para usar diferentes propósitos maliciosos. Tal es el caso que en el año anterior la empresa sufrió un ataque de Ransomware en uno de los 3 servidores institucionales.

Entonces el problema científico de investigación redactado como pregunta es:

¿Se presenta una opción de seguridad frente a los riesgos en el servidor PBX VOIP en la empresa Lácteos Gustalac La Polaca?

Objetivos

Objetivo General

Proponer la implementación de una guía de seguridad en la plataforma de VOIP Elastix en la empresa Lácteos Gustalac La Polaca.

Objetivos Específicos

1. Determinación del estado del arte en los riesgos de seguridad para la disponibilidad VOIP.
2. Revisión de metodología para el análisis de riegos de seguridad en redes VOIP.
3. Selección de una metodología de análisis de riegos de disponibilidad en redes VOIP.
4. Identificación de las vulnerabilidades encontrada para el desarrollo de una guía de seguridad en redes VOIP.

Justificación

El desarrollo del presente proyecto de investigación es importante porque elabora una guía de implementación en la seguridad de la plataforma VOIP en Elastix, para prevenir ataques sobre las vulnerabilidades en esta plataforma, mantiene la integridad, disponibilidad y confidencialidad de la comunicación. La mejor manera de lograrlo es utilizar técnicas de descubrimiento, detecciones de amenazas y mitigar estas vulnerabilidades. Con este proyecto no solamente beneficia la empresa en la que, se realiza la implementación, sino también, cualquier institución pública y privada que desee implementar seguridad sobre su plataforma VOIP con Elastix.

CAPÍTULO I. ESTADO DEL ARTE Y TEÓRICO

1.1. Origen y evolución de la Tecnología VoIP

Los primeros inicios de la comunicación de voz a través del protocolo IP, se diseñó en los años 70 para la red ARPANET, utilizó experimentalmente para emitir una comunicación mediante voz a las personas que integraban la red. Por el año de 1995, se logra realizar la primera llamada por teléfono de PC a PC por medio del internet, cuando la compañía VocalTec lanzo uno de sus primeros Softphone. Al año siguiente logra hacer la primera llamada de teléfono a PC y de teléfono a teléfono IP (Romero, 2019).

La tecnología VoIP evoluciona con el pasar de los tiempos, en un principio, se inicia con llamadas telefónicas a través del protocolo IP, el cual en un comienzo tenía interferencias, pero mejora con la implementación de una nueva infraestructura que permitió que tome de otra forma, en la actualidad una comunicación VoIP logra hacer llamadas de voz por medio de la red, esto manejan las empresas pequeñas, medias y grandes para la comunicación tanto a nivel interno como externo, ofrece un servicio eficaz y de óptima calidad para los usuarios finales.

1.2. Antecedentes de estudio

Según el artículo académico realizado por Sotomayor, Romero & Sáenz (2014) del tema “Análisis de vulnerabilidades de seguridad en centrales VoIP Elastix a través del hacking ético” el objetivo de este trabajo es analizar las vulnerabilidades del servidor Elastix, utiliza el sistema operativo Kali Linux mediante técnica de Hacking Ético, se logra realizar la penetración al sistema Elastix, con el uso de las herramientas, NMAP, HYDRA, SVMAP y SVCRACK, una vez aplicado esto, se logra determinar que existían puertos abiertos, para lo cual concluye que el sistema tiene vulnerabilidades que ponen en peligro la confidencialidad de los usuarios.

El trabajo titulado “Esquema de seguridad para una central VoIP, en software libre en su implementación Elastix” del autor Maldonado (2016), tiene como objetivo la implementación de un plan para la seguridad en un laboratorio, que permita la mayor mitigación de ataque por parte de los crackers informáticos, que se encuentran vulnerables las centrales VoIP, para esto utiliza Kali Linux, para realizar las pruebas de vulnerabilidades, específicamente usa la herramienta HYDRA para realizar ataques de fuerza bruta, con la utilización de diccionarios donde determina que existían puertos abiertos, los cuales fueron mitigados para de esta manera garantizar la integridad de la información para los usuarios.

En la investigación que con el tema “Implementación De Un Esquema De Seguridad Para Configurar Centrales VoIP” realizada por el autor (Jaramillo, 2015) tiene como objetivo mitigar las brechas de seguridad existentes en las centrales VOIP, para dar una solución propone algunos aspectos como el cambio cada cierto tiempo de contraseñas, un monitoreo constante por parte del departamento de seguridad de la información, además tener un Firewall, para reducir los posibles ataques hacia las centrales VoIP y evitar poner en riesgo la confidencialidad por parte de los clientes que usan esta tecnología para la comunicación.

En el “Estudio y elaboración de un sistema de comunicaciones unificadas VoIP basado en Elastix con seguridad perimetral” elaborado por Espinoza (2021), se tiene por objetivo la implementación de un plan de seguridad en un entorno, que se alcanza medir las vulnerabilidades para posteriormente mitigar los ataques informáticos que amenazan a la central VoIP, para esto utiliza controles de BLOX como SBC (Session Border Controller) en open source, se consigue garantizar la mitigación de ataques informáticos que generan peligro para las redes VoIP, donde concluye que con políticas y un plan de seguridad de protección perimetral preventivas y reactivas, se consigue resguardar la información, en este caso la central Elastix, reduce así al mínimo riesgo de ataques exitosos.

Se ha hecho el análisis de los diferentes trabajos de investigación, de los diferentes autores, en donde logra analizar que la mayoría de ellos, se concluye

con éxito, la metodología que aplicaron junto con las herramientas estuvieron a la par, con la parte práctica para así lograr el éxito en la investigación, las herramientas que emplearon en la mayoría de trabajos fue Kali Linux, es un sistema de software libre y no tiene restricciones para el uso de los diferentes programas que ya vienen por defecto en una instalación normal, fue este uno de los puntos por lo que la mayoría de autores lo utiliza, también cabe destacar que tiene un gran número de paquetes para realizar pruebas de vulnerabilidades, como por ejemplo Nmap, que se encarga de buscar todos los puertos que están abiertos, otra seria Hydra que es una potente herramienta para realizar ataques de fuerza bruta con la utilización de diccionarios los cuales, se consiguen encontrar en internet desde el más básico hasta el más avanzado.

Hoy en la actualidad donde, se produce miles de ataques cibernéticos por minuto en el mundo, las empresas necesitan tener un plan de seguridad en caso de existir un ataque masivo a los servidores donde almacenan información, se tiene que haber un monitoreo o una persona que esté a cargo de esta acción, de esta manera evitar que intrusos logre tener acceso a la información crítica de la empresa. Los ataques con mayor frecuencia, que se efectúan son por fuerza bruta, a través de técnicas donde utilizan diccionarios muy completos, con gran cantidad de caracteres, que con una buena máquina de computación logra el objetivo de acceder al sistema.

1.3. Marco Teórico

Elastix

La EOS (2014) establece, que Elastix es un software de código abierto el cual, se usa para comunicaciones unificadas, el objetivo principal es lograr una comunicación buena de calidad, estable y óptima para las empresas que implementen este sistema, para lo cual necesita tener conocimientos previos para la configuración de los medios de comunicación existentes en la empresa.

La central Elastix IP-PBX está a un paso en telefonía empresarial. En la actualidad la tecnología telefónica abarca un campo importante en la informática esto es una realidad, ha avanzado a pasos gigante ser así hoy en día muy

importante para la comunicación, porque todo el mundo está en constante interacción que comunica con las demás personas. La central IP compone por un equipo de funcionalidades similares a una central tradicional y le suma la tecnología de Voz sobre IP, esto con el pasar del tiempo va innovando hasta hoy en día tener una comunicación eficaz y de calidad.

Está diseñada para hacer gran número de llamadas simultáneas por medio de la infraestructura de red actual existente, esta tecnología ofrece una red de telefonía que permite una comunicación VoIP interna y externa en la empresa o lugar donde se haya implementado, a través del servidor configurado, se logra acceder desde distintas ubicaciones remotamente y con esto, se evitan costos extras. Ver Figura 1.

Figura 1. Elastix IP-PBX

Fuente: (EOS, 2014)

Ventajas de telefonía IP según EOS

1. Reportes de consumo de recursos.
2. Recepcionista automática de llamadas multi empresa.
3. Transferencia de llamadas en caso de no recibir respuesta del receptor.
4. Paso de llamadas con la red pública.
5. Conferencias.
6. Grabación de llamadas.
7. Colas de llamadas.
8. Tono o música en espera.
9. Implementar extensiones remotas.

10. Interfaz gráfica con administración vía web.
11. Interconexión entre oficinas remotas.
12. Soporte de usuario remotos.
13. Registro con la información de llamadas.
14. Transferencia de llamadas si el usuario no está disponible.
15. Correo de voz que es enviado en forma audio a casilla de correo electrónico.
16. Claves de acceso por usuario (EOS, 2014).

Distribuciones De GNU/Linux

Como Tanenbaum (2013) dice, una distribución de GNU/Linux es la unión de varios paquetes que están listos para instalarse en un sistema operativo funcional en un disco duro en blanco. El núcleo que emplea Linux está basado en GNU el cual posea una gran biblioteca con programas del sistema los cuales permiten un óptimo funcionamiento.

Las funcionalidades más destacadas de una distribución son:

1. El sistema que gestiona los paquetes.
2. La cantidad y calidad que actualizan los paquetes que tienen.
3. En esto es de importancia saber si, se dispone un sistema de control de calidad.
4. Sistema de instalación inicial.
5. La frecuencia que tienen las actualizaciones de la distribución de las nuevas versiones.
6. Se tiene un soporte para los usuarios para dar un seguimiento del tipo de sistema de la documentación, existen foros en los que logra encontrar ayuda, de soporte de pago.
7. Compatibilidad existen una gran cantidad de distribuciones de Linux, las más populares en la actualidad son:
8. Gentoo es creada por voluntarios, utiliza un sistema de paquetes basado en código fuente que son compilados antes de instalar. Contiene más de 4000 paquetes de software.

9. Fedora es un proyecto que fue implementado por la compañía Red Hat en sustitución de la distribución denominada Red Hat Linux. Este es un proyecto público que es fácil de usar, está disponible para portátiles y de escritorio.
10. Debían GNU/Linux fue diseñada por más de 100 voluntarios de todo el mundo, usa el formato de paquete .deb y los paquetes oficiales son redistribuibles totalmente. Cuenta con más de 44000 paquetes de software listo para su uso.
11. Mandrake, distribución comercial, emplea el formato rpm.
12. SuSE Linux, distribución comercial que fue comprada recientemente por Novell, emplea el formato rpm.
13. Red Hat Enterprise Linux, es una distribución que está basada en Fedora.

Voz sobre Protocolo IP (VoIP)

El protocolo de internet sobre voz, se dice que es la reunión de recursos el cual transmite una señal de voz por medio del internet, a través de paquetes digitales, por IP diferente a la tecnología analógica que usaban los teléfonos antiguos para la transmisión de voz (Robalino, 2012).

La tecnología de VoIP es muy usada por parte de las empresas para la comunicación tanto internamente como externamente, al ser un medio muy utilizado existen terceras personas que intenta vulnerar la seguridad para tener acceso a esta comunicación, que se usan técnicas de hackeo para encontrar vulnerabilidad que les permitan ingresar a la información que intercambia en cada momento, la cual consigue ser usada con fines de espionaje por parte de la competencia, o para robar la información de los clientes.

Elementos que componen a una red VoIP

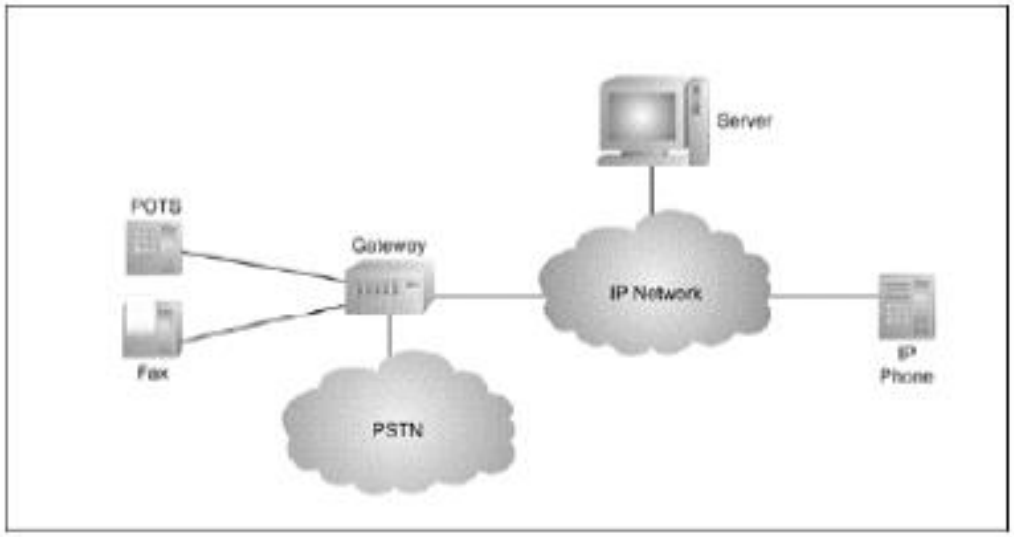
En una infraestructura de red VoIP existen tres elementos básicos que es necesario diferenciar que son:

Gateway: En un aparato que permite la comunicación el cual comparte recursos entre uno o más dispositivos de telefonía, permite una red conmutada o digital, por lo que brinda una señal optima y de calidad (Matango, 2016).

Terminales: Son dispositivos en hardware o software el cual tienen la función de permitir la comunicación con los usuarios.

Servidor/Gatekeeper: Este tiene la función de administrar el enrutamiento de llamadas, la autentificación de usuarios al igual que el manejo. Ver Figura 2.

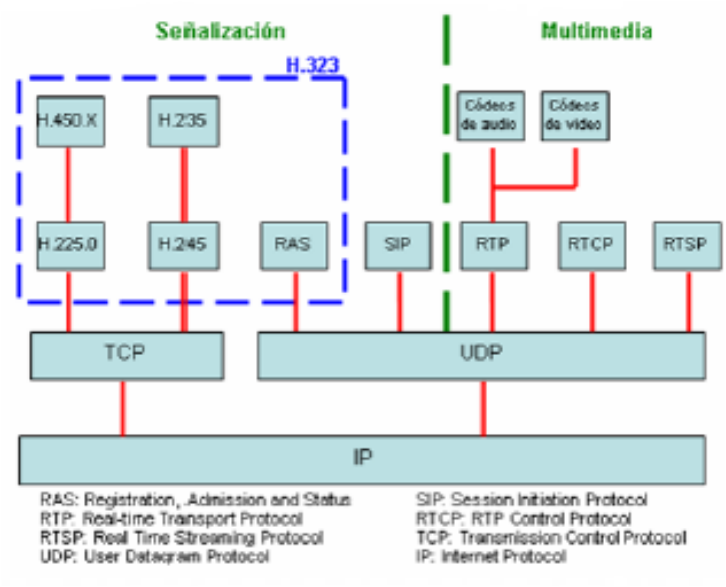
Figura 2. Elemento de una red VoIP



Fuente: (Matango, 2016)

Protocolos VoIP

Figura 3. Estructura del protocolo VoIP



Fuente: Servervoip.com

Protocolos de transporte y control

RTP (Protocolo de Transporte en Tiempo Real)

El RTP es un medio uniforme, que se utiliza para la transmisión de datos el cual está definido a las limitaciones de tiempo real, además es el encargado de añadir los paquetes UDP la marca de tiempo, identificación de carga y número de secuencia por lo cual es muy importante para la comunicación (Arroba & Salazar, 2011).

RTCP (Protocolo de Control Transporte en Tiempo Real)

Este protocolo que controla mediante el RTCP permite hacer llamada para lograr intercambiar los paquetes de control con los terminales, también permite la medición de desempeño, lo que no ofrece son las garantías. Estos protocolos son las que hacen que exista la comunicación, que además administre de una mejor manera los recursos para así evitar posibles conflictos al momento de intercambiar los datos por la red (Arroba & Salazar, 2011).

Los protocolos son los que facilitan la comunicación, para que sea segura,

óptima y lo más importante exista confidencialidad, para esto depende de factores de como esta implementado la comunicación, prácticas de seguridad que ayuden a encontrar brechas para posteriormente mitigarlas, para que exista una comunicación segura.

TCP (Protocolo de Control de Transmisión)

El protocolo TCP es utilizado para conexión, permite la transferencia de datos entre dos dispositivos. Además, permite el control de datos en niveles menores de aplicación, y asegura que estos lleguen a su destino de la orden que fueron enviados.

UDP (Protocolo de Datagrama de Usuario)

El protocolo de datagrama de usuario (UDP) es ligero para el transporte de datos que funciona sobre protocolo IP, no está orientado a conexión, es decir que tiene un método para detectar errores que son corruptos en los paquetes, cuando se da la conexión, pero existen errores, este no intenta resolverlos simplemente la información queda ahí, lo cual no permite el intercambio datagramas por lo que habría perdida de los datos que hayan sido corruptos.

Por medio de este protocolo producen el intercambio de datos, pero en el instante de entrega del paquete no existe un mensaje de aviso por lo que no consigue garantizar que los paquetes sean correctamente entregados en su destino, si producen errores esta capa no ofreces servicios de recuperación de los datos.

Tipos de Servicio

La comunicación VoIP es una tecnología donde da a conocer algunos servicios que logra tener con este medio de comunicación, es decir que son los más generales, hasta la actualidad no se conoce un estándar definido para los servicios básico en VoIP y, pero conocen los siguientes:

1. Buzón de Voz

2. Transferencia de llamada
3. Marcación Rápida estos son los numero de servicio público como policía, emergencia y bomberos.
4. Follow – me: son números que redirecciona a una llamada en caso de que la extensión tenga respuesta.
5. Desvío de llamada
6. Llamada en espera
7. Operadora Automática / Virtual
8. Música en espera: cuando no tiene una respuesta.
9. DirectDialling-In: bloqueo de una llamada mediante la extensión directa.
10. Envío y recepción automática de faxes
11. Mensajería SMS
12. Listas Negras: son los números que han sido bloqueados
13. CallerID
14. Registro y listado de llamadas entrantes y salientes
15. Grabar y reproduce llamadas
16. Salas conferencia
17. Visualización de llamadas en curso

Seguridad en las redes VoIP

A escala que aumenta la popularidad también, se incrementan las preocupaciones por la seguridad de la telefonía IP y comunicaciones. VoIP es una tecnología que necesita de muchas otras capas y protocolos ya existente en las redes de datos. Por todo esto la telefonía IP, se heredan problemas que tienen las capas y protocolos, donde las amenazas principales son de VoIP la cual presenta problemas comunes de seguridad que afectan en todas las redes de datos a nivel mundial, donde es cierto también que existen muchos ataques a VoIP (Gutiérrez, 2017). Ver Figura 4.

Figura 4. Seguridad VoIP

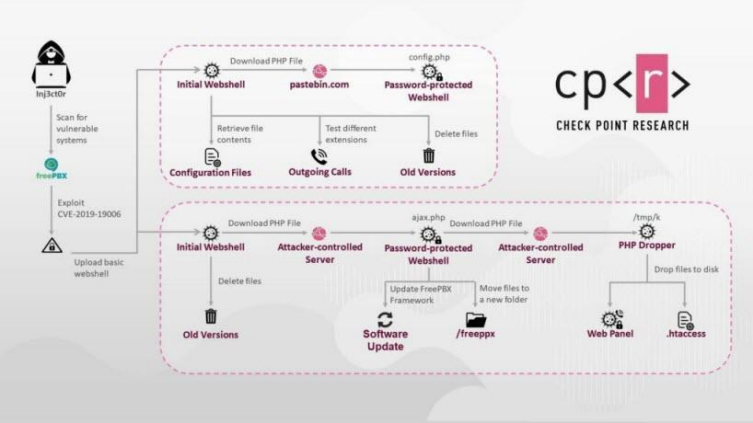
Fuente: (Gutiérrez, 2017)

Un informe elaborado por los expertos en ciberseguridad de *Check Point*, se ha observado que un grupo de piratería a atacado las redes de VoIP de al menos 1.200 instituciones en al menos 20 pises. De este modo, Reino Unido tiene más de la mitad de los ataques, es el país más amenazadas, se dice que han sido atacados varios departamentos de gobiernos, sectores de finanzas y seguros, los fabricantes y el ejército.

Además, se halló un patrón de explotación de los servidores SIP de algunos de los fabricantes. El romper vulnerabilidades de los servidores SIP, es importante para tener el control y manejo. Los métodos más importantes para la explotación es hacer llamadas telefónicas mediante el cual, se utiliza para la generación de varios beneficios, el hacer llamadas es una función legal y común, lo difícil es hallar cuando, se ha explotado un servidor.

En este diagrama, se ve el método de ataque por Inyección:

Figura 5. Tipo de Ataque



Fuente: (Lorenzo, 2020)

Lo que alcanza a ver la seguridad VoIP, se elabora en base a otras capas convencionales de seguridad de la información. En la tabla, que se muestra a continuación detallan varios puntos vulnerables y ataque que afecta a las diferentes capas. Que posteriormente van a analizar más a profundidad algunos de los ataques que logran afectar directa o indirectamente a la telefonía VoIP, hoy en día existe gran cantidad de métodos para ataques.

Tabla 1. Ataques y vulnerabilidades

Capa	Ataques y vulnerabilidades
Procedimientos y políticas	Contraseñas menores de 8 caracteres. Ejemplo: Contraseña del VoiceMail no tener una buena política establecida.
Seguridad Física	Acceso físico a dispositivos principales. Ejemplo: Acceso físico a un Gateway.
Seguridad de Red	DDoS ICMP, SYN floods, gran variedad de floods.
Seguridad en los Servicios	SQL Injection, denegación en DHCP DoS.
Seguridad en el S.O.	Buffer overflows, gusanos y malware.
Seguridad en las Aplicaciones y protocolos de VoIP	SPAM, Phishing, Fuzzing Floods. Secuestro de sesiones. Interceptación, Redirección de llamadas, Reproducción de llamadas.

Fuente: (Carrillo, 2017)

Se logra ver ciertos ataques que tiene como principal prioridad el robo de información crítica para la empresa y otros impedir la conexiones salientes y entrantes (DoS). Para los atacantes no es solamente estar interesado por la conversación, sino también por la información y los datos de una llamada, los cuales si utilizan de forma irresponsable facilita al atacante a realizar registro de llamadas salientes o entrantes, redirige las llamadas, grabador de datos, bombardear SPAM, todo es lo que quiere lograr es interceptar y secuestrar llamadas. Todos los dispositivos de red, sistemas operativos, servidores, protocolos con los que trabajen y tengan una infraestructura VoIP esta expuestos a sufrir ataques.

Clasificación de los ataques

Existen algunas amenazas importantes que ponen en peligro la confidencialidad de la telefonía IP. Se han encontrado gran cantidad de riesgos en las capas en las que utiliza la tecnología VoIP, algunos de los ataques, se efectúan con técnicas comunes. A continuación, se muestra una clasificación de las amenazas de redes de telefonía IP**:**

1. Accesos sin autorización y estafas.
2. Denegación de servicios
3. Ataques a los dispositivos informáticos
4. Intromisión de la red subyacente.
5. Enumeración y descubrimiento de vulnerabilidades.
6. Ataques, que se realizan a nivel de aplicación.

Amenazas a la Seguridad De Un Sistema VoIP

Amenaza está escrita por la norma ISO 27001, (2012) como: “Una causa potencial de un incidente indeseado, que consigue daños a un sistema o a una organización”. Como se observa, las amenazas de seguridad dañan los archivos que están alojados, además generan inseguridad por parte de los ciudadanos que prefieren no confiar en un sistema VoIP, se menciona a continuación las amenaza amenazas de seguridad (VoIP):

Fuzzing

Este se lo conoce como testeo funcional, usa paquetes alterados el cual ocasiona que el funcionamiento afecte la integridad de los mensajes y el funcionamiento del sistema, también ocasiona desbordamiento de buffer, se reinicia los dispositivos y finaliza las llamadas.

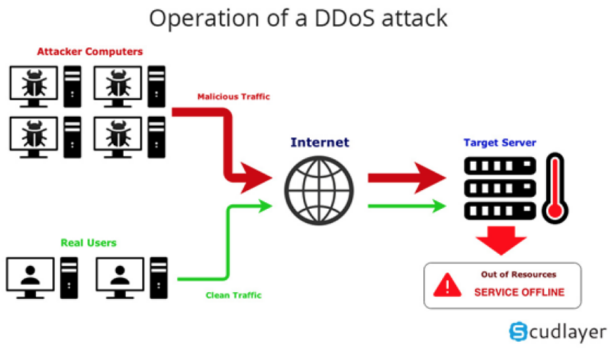
Denegación de Servicio (DoS)

Son ataques maliciosos para deshabilitar el funcionamiento del sistema, afecta al objetivo, que se quiere dejar inactivo, esto envían grandes paquetes para así explotar el software. Lo que quiere hacer esto es denegar el servicio VoIP para de esta manera colapsar por medio de llamadas falsas que generan tráfico enorme, las llamadas legales no logra ser realizada, quedan interrumpidas (Krasheninnikova, 2013).

Denegación de Servicio Distribuido (DDoS)

Estos ataques son realizados, la mayoría están programados para deshabilitar un sistema VoIP lo que afecta su confidencialidad**.** En la tecnología VoIP estos ataques distribuidos tienen como objetivo lograr DoS en varios nodos de una red, de forma concurrente, interrumpe el sistema totalmente. Además, se logra generar un enorme tráfico que ningún dispositivo logra soportar (Liberona, 2010). Ver Figura 6.

Figura 6. Operación ataque DOS



Fuente: (Gutiérrez, 2017)

Interceptación (Eavesdropping)

Este ataque es conocido como Eavesdropping, tiene como objetivo realizar la toma de datos mediante un tercero al que no estaba direccionado los datos. En modo de telefonía VoIP, trata de la vulnerar de las llamadas telefónicas entre dos personas, existen hackers que quieren interceptar las llamadas, para lograr obtener información, la cual intercambia cada instante que utiliza la tecnología VoIP. Ver Figura 7.

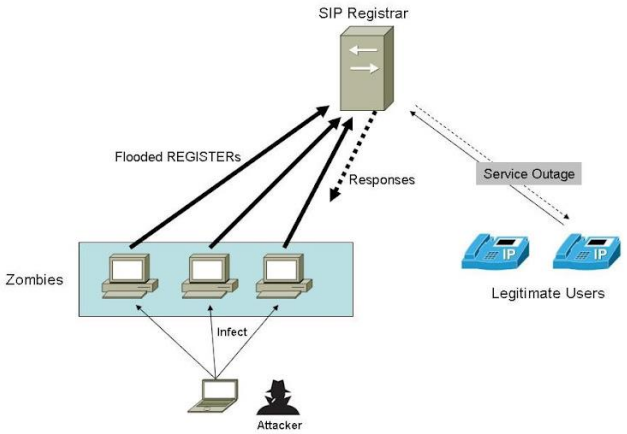
Figura 7**.** Intercepción

Fuente: (Espinoza, 2021)

Inundaciones (Flooders)

Una inundación, consiste en enviar gran cantidad de datos en corto tiempo a una aplicación para lograr que este colapse. Afecta principalmente a la integridad y disponibilidad. En VoIP los flooders atacan hacia los puertos de telefonía IP, logra de esta manera bloquear los puertos para de esta manera impedir el servicio a todos los usuarios (Liberona, 2010). Ver Figura 8.

Figura 8. Inundación

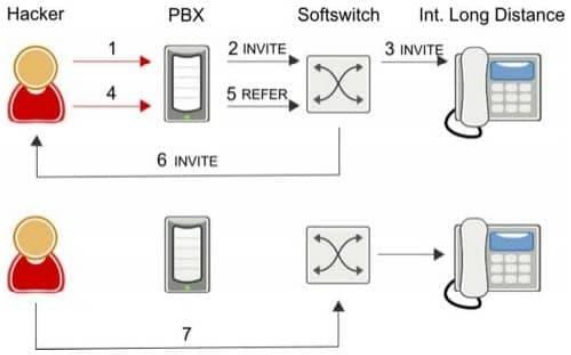


Fuente: (Gutiérrez, 2017)

Fraude telefónico (Toll Fraud)

Son ataques que tienen como objetivo de reunir dinero en beneficio del servicio telefónico, realiza llamadas internacionales o robo de minutos de llamadas telefónicas. Ver figura a continuación.

Figura 9. Fraude Telefónico



Fuente: (Gutiérrez, 2017)

Herramientas

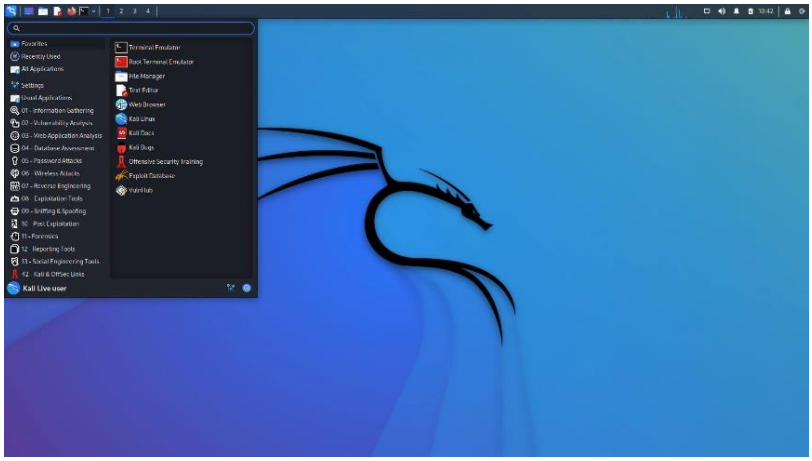
Kali Linux

Para la ejecución de pruebas de detección de brechas de las redes VOIP, se utiliza Kali Linux que es la actualización de Linux Backtrack, esta es una

distribución gratuita que normalmente, se utilizan para realizar auditorías informáticas y pruebas de penetración, cuentan con una gran variedad de herramientas que ayudan a controlar, buscar y explotar las vulnerabilidades de los sistemas informáticos. Kali Linux tiene más de 350 herramientas para realizar pruebas de penetración, está basado en GNU/Linux Debian, dentro de esto las herramientas que más van a utilizar están relacionadas con descubrimiento de red, ataques de fuerza bruta, y ataques dispositivos SIP.

Es una distribución basada en GNU, principalmente utiliza en la protección y optimización de ordenadores, también para descifrar contraseñas. Es un software que además, se consigue utilizar con fines ilegales, hay ciertas personas que la usan para realizar ataques a otros ordenadores, como también es considerada una de las mejores herramientas para la seguridad de la información y la auditoria de redes, por ejemplo, se consigue realizar pruebas de vulnerabilidades, penetración y ataques de fuerza bruta, para todo esto Kali Linux cuenta con un paquete extenso de herramientas donde muchas de ellas ya vienen instaladas por defecto en una instalación normal. Ver figura a continuación.

Figura 10. Kali Linux



Fuente: (Cruz, 2016)

Nmap (Network Mapper)

Esta es una de las mejores herramientas de comandos que tiene Linux, para realizar auditoria y seguridad de redes, además de rastreo para encontrar

vulnerabilidades en el sistema. Con los siguientes comandos más utilizados:

1. Escanea todos los puertos de un host. - #nmap -v host
2. Escanea un único puerto existente. - #nmap -p host
3. Busca puerto TCP abierto en la máquina. - #nmap -sT host
4. Escanea un rango de puertos. - #nmap -p host
5. Sirve para hacer un escaneo de rango de puertos y puertos específicos, como TCP y UDP.
6. #Nmap -p U:53, T:1000, 8080 host
7. **Escaneo de hosts detrás de un firewall**

   # Nmap -PS host

   # Nmap -PA host
8. Se logra indagar con nmap si el host, se encuentra oculto detrás de un firewall.

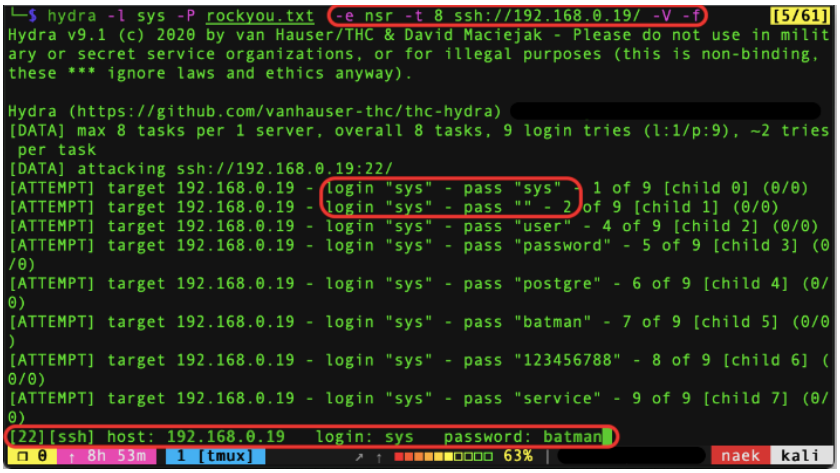
   # Nmap -SA host

Ataque SSH

Para realizar ataques por diccionarios a protocolos comunes, se usa la siguiente sintaxis.

Hydra comando. - -l o -L <usuario, lista> -p, -P <contraseña o diccionario> <dirección IP> <protocolo>

Figura 11**.** Obtiene el usuario y contraseña con ataque SSH



Fuente: (Romero, 2019)

Otras herramientas que utilizaron son los siguientes:

RSMANGLER

Genera diccionarios para realizar ataques de fuerza bruta.

HYDRA

Es una herramienta, que se utiliza para realizar auditorías que trabaja con múltiples tareas que funcionan en paralelo, soporte y gran variedad de protocolos, además permite a los investigadores y consultores de seguridad, mostrar de una forma más fácil lo que sería lograr acceso a un sistema no autorizado de manera remota.

SVMAP

Escanea dispositivos SIP.

SVCRACK

Ataque de fuerza bruta a un usuario principal.

SVWAR

Escanea usuarios y extensiones de centrales IP.

VMware Workstation

Este es un software el cual ayuda a instalar máquinas virtuales dentro de un sistema operativo, el cual va a ser de mucha ayuda para las respectivas pruebas de penetración.

NESSUS

Es un software que permite realizar un escaneo de vulnerabilidades a un host, se ejecuta en cualquier tipo de sistema operativo y presenta los resultados encontrados en un informe para sus análisis. Todas están herramientas ayudan para hacer las respectivas pruebas de vulnerabilidades en este proyecto de investigación, aplica buenas técnicas con la metodología OSSTMM, que facilitara la implementación de pruebas de penetración para de esta manera determinar, las inseguridades que tiene los sistemas VOIP con el fin de mitigar los riegos, de esta forma, tener un sistema más seguro contra posibles ataques externos, que se dan así como sucedió hace algún tiempo cuando por medio de Ransomware hicieron ataques a uno de los servidores, donde lo dejaron inactivo, la información quedo encriptada, lo que ocasionó la perdida de la información.

1.4. Protocolos de Señalización.

Es un protocolo que cumple unas reglas y acuerdos, para que los dispositivos y computadores logren establecer comunicación entre ellos, los protocolos más empleados en las redes de voz sobre IP son, MGCP, H.323 y SIP los cuales son los más importantes, todos estos están regulados con normas de control como la ITU T, la IETF, el ETSI o el EIA TIA. La mayoría de estos medios de comunicación con interfaces estandarizadas y abiertas con una buena infraestructura de paquetes (Carmona, 2015).

Protocolo SIP

Este protocolo establece una comunicación entre el cliente y servidor, para una transmisión de video y voz, usa una sintaxis similar a la HTTP y la SMTP, que son las usadas en sitios web y servicios de correo electrónico, el cual permite una conexión estable (Carmona, 2015).

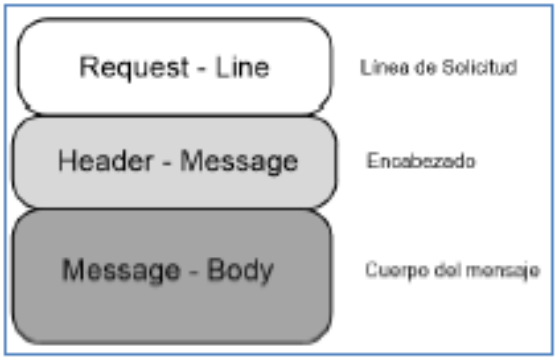
Como se observa estos protocolos facilitan la comunicación entre dos o más sesiones con los usuarios, existen llamadas por internet, conferencia y la

distribución de datos multimedia, pero estos protocolos ayudan a dirigir las peticiones, hasta el destinatario final, cuenta también que permiten autentificación y autorización a los usuarios, para que logren ingresar a los servidores, donde consigue tener control y administrar las comunicaciones, dan permisos y deniegan accesos.

Mensajes SIP

Los mensajes SIP, es la identidad digital de los usuarios cuando realiza una llamada, y como los usuarios logran interactuar en una red, para esto hay códecs que están disponibles que consigue comunicarse uno con otros en la red de tecnología IP. Ver figura a continuación.

Figura 12. Mensaje SIP



Fuente: (Carmona, 2015)

1. El cuerpo del mensaje es el que lleva la información.
2. El encabezado tiene información correspondiente a las llamadas.
3. La línea de solicitud es la que contiene las direcciones y la versión de protocolo.

Método Sip

Existen las peticiones SIP, que se basan en un mensaje donde tienen Request-Line, que es el que describe el método, también existe el destino de la solicitud que es el Request-URI y además la versión de protocolo SIP que utiliza, pero SIP destaca los siguientes: (Carmona, 2015).

1. SIP Option: Solicita información sobre el envío y recepción de teléfonos SIP.
2. SIP Bye: Finaliza una sesión
3. SIP Cancel: Permite cancelar una invitación pendiente
4. SIP prack: Mensaje de confirmación que ha establecido una llamada.
5. SIP Register: Registra una ubicación en un servidor
6. SIP re-invite: Permite un cambio en una sesión actual
7. SIP invite: Es para iniciar o modificar las sesiones.

Hardware

En la actualidad existen muchos equipos disponibles que transmiten Voz sobre IP, con esto de abren a nuevas oportunidades para la mejora de los procesos comerciales, mejor así en gran medida los costos de operación de la infraestructura informática y de telecomunicaciones. Algunos de estos son:

- Teléfonos IP.
- Cisco IP Phone 7902G.- Teléfono IP.

Figura 13. Cisco IP Phone 7902G

Producto: Cisco Teléfono IP.

Modelo: 7902G

Fabricante: Cisco.

Fuente: (Carrillo, 2017)

Es un teléfono con muchos detalles y funcionalidades, gran cantidad de ventajas en conexión y disponibilidad de las comunicaciones IP, como se observar es de marca Cisco muy reconocida en el mercado de las telecomunicaciones, este teléfono se usa en pequeñas, medianas y grandes empresas, menciona también sitios empresariales.

Figura 14. Cisco IP Phone 7902G

Descripción del producto	**Cisco IP Phone 7902G - teléfono IP**
Tipo de producto	Teléfono IP
Capacidad de correo de voz	Sí
Teléfono con altavoz	Sí
Líneas soportadas	Una sola línea
Cantidad de puertos de red	1 x Ethernet 10/100Base-TX
Características principales	Soporte de Power over Ethernet
Codecs de voz	G.711, G.729
Protocolos VoIP	SCCP
Software compatible	Cisco Call Manager 3.3(3) ó posterior

Fuente: (Carrillo, 2017)

Figura 15. Budge 100.- Telephone IP SIP

Producto: GrandStream Teléfono IP SIP 1 RJ45

Modelo: BudgeTone 100

Fabricante: GrandStream

Fuente: (Carrillo, 2017)

El BudgeTone 100 es un dispositivo que tiene una toma a la red Rj45, además tiene compatibilidad con la tecnología SIP, y logra comunicarse con la mayoría de los dispositivos que existen en el mercado. Se concentra una central telefónica digital (PBX) como Asterisk que es el más usado para este tipo de comunicaciones, la telefonía IP permite ingresar automáticamente el formulario del usuario en la pantalla en una llamada telefónica, para de esta forma conservar los datos de historial de llamadas (Carrillo, 2017).

Software

En cuanto a software tiene algunos, mediante los cuales logra establecer una comunicación entre dos dispositivos, es decir que uno de ellos es:

Sutil

Es un sistema utilizado para la comunicación automatizado y desarrollado que facilita la comunicación a través de VoIP. Se utiliza como central telefónica y tiene algunas ventajas las extensiones VoIP que son las siguientes:

1. No requiere cableado telefónico, solo de datos, se logra hacer todo con el cableado de datos.
2. Se logra utilizar IP para una comunicación más estable, optima y eficaz, también se conecta un teléfono IP a cualquier toma de la red que esté disponible.
3. Además, se utiliza un software Softphone en el ordenador que atiende y realiza las llamadas telefónicas.
4. Se consigue tener extensiones de teléfono remotas, es decir son operadores que trabajan desde casa.
5. Permite conectar varios equipos a la vez, para realizar varias llamadas entre algunos departamentos que van a por medio de la red IP.

Sutil consigue usar configuraciones IP más personalizadas:

1. Se modificar con uno o más dispositivos Sutil, que logra transferir llamadas a la extensión del operador.
2. Se utiliza dos o más equipos Sutil interconectados en caso de que uno falle funcionaria el otro, actúa como operador telefónico a escala.

Software FastCall

FastCall es una empresa internacional que tiene por objetivo brindar soluciones de VoIP a nivel de pequeñas y grandes empresas, con una gran variedad de

productos que permiten una facilitar y economizar la comunicación con el resto

Características:

1. Soporta NAT, esto significa que alcanza a realizar llamadas por detrás de un NAT (en una IP privada).
2. Forma segura de autenticación del usuario.
3. g723 códec (compresión de audio que permite realizar llamadas con poco consumo de recursos del ancho de banda).
4. Llamar directamente a IP
5. Función en espera (HOLD).

Figura 16. Funcionamiento FastCall

Fuente: (Espinoza, 2021)

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la organización

La empresa Lácteo Gustalac La Polaca está situada en la ciudad de Santo Domingo de los Tsáchilas y cuenta con varias agencias a nivel nacional como Guayaquil, Quito, Manta y Quevedo. Cuenta con más de 20 años de trayectoria, comprometido con el país y con el incremento de sus clientes. La empresa Lácteo Gustalac La Polaca, se considera una de las mejores empresas en la creación y comercialización de productos lácteos que son naturales y de excelente calidad (Polaca, 2021).

Desde los inicios de esta empresa este ha sido el valor principal y el principal objetivo para todos los que conformamos la empresa creando todas nuestras tareas bajas estos parámetros, de estar siempre predispuestos a ofrecer productos de muy buena calidad que sean frescos, naturales y con un gran contenido nutricional para los consumidores finales, es por esto, que se ha convertido en una empresa reconocida ampliamente en el mercado, y es elegida por millones de familias ecuatorianas.

Avena POLACA con el paso de los años, se ha esforzado para conseguir estar siempre entre las mejores empresas con los más altos estándares de calidad en los procesos productivos, para de esta manera cumplir este objetivo que es contar una certificación de Buenas Prácticas de Manufactura B.P.M, sistemas de gestión de calidad y personal capacitado (Polaca, 2021).

El centro de operaciones está ubicado en la ciudad de Santo Domingo, por este motivo, comercialmente está presente en 15 provincias y se espera llegar a más lugares del Ecuador, cuenta con 4 agencias en las ciudades de (Guayaquil, Quito, Manta y Quevedo). Trabajo, que se realiza arduamente para estar más cerca de los hogares y brindar la más deliciosa y saludable experiencia de tomar un vaso de Avena POLACA (Polaca, 2021).

MISIÓN

Ser la empresa líder en la industria alimenticia, aplicación de tecnología, innovación, buenas prácticas de manufactura e incorporan personas altamente calificado. Cumplir los estándares de calidad e higiene, respeta el medio ambiente para brindar productos sanos, nutritivos, que garanticen la completa satisfacción del consumidor (Polaca, 2021).

VISIÓN

Lograr ser una organización industrial y comercial con cobertura nacional y desarrollo tecnológico para ampliar el portafolio de productos, establecer franquicias, abrir mercados internacionales y desarrollar nuevos socios estratégicos (Polaca, 2021) .

VALORES CORPORATIVOS

- Responsabilidad
- Lealtad
- Solidaridad
- Sentido de pertenencia
- Honestidad
- Compromiso

La empresa cuenta con un servidor en Elastix que es un software open source que integra la funcionalidad de PBX (“Private Branch Exchange”) en IP, mensajería y funciones corporativas. Este servidor tiene la función de Central telefónica de comunicación en los diferentes departamentos administrativos, operativos, las agencias y para sus clientes. En la actualidad no cuenta con la seguridad implementada, es vulnerable para la integridad y disponibilidad de la comunicación.

2.2. Metodología de la Investigación

Tipo de investigación

El tipo de investigación para desarrollo del presente proyecto es cuasiexperimental. Para ello, se implementa un laboratorio en vivo para simular la comunicación entre el PBX Elastix y las extensiones, se realiza diagnóstico de vulnerabilidad utiliza herramientas de escaneos en estado activo, se alcanza a mitigar las brechas de seguridad e implementar una buena práctica para la seguridad en esta plataforma.

Enfoque de investigación

En la presente investigación, se va a usar un tipo de enfoque mixto, porque se usarán datos cualitativos y cuantitativos.

Población y muestra

La población que será tomada en la presente investigación es de 18 personas, son los que conforman el personal administrativo de la empresa. Ver Tabla 2.

Tabla 2. Población

Departamento	No Empleados	%
Sistemas	2	11,11
Contabilidad	2	11,11
Cobranza	2	11,11
Centro de atención telefónica	3	16,6
Talento Humano	2	11,11
Ventas	3	16,66
Logística	4	22,22
TOTAL	18	100

Fuente: Elaborado por el autor

2.3. Herramientas y técnicas recolección de información

La entrevista, se la realiza con el objetivo de recopilar información del departamento de sistemas de la empresa, de esta manera obtener datos reales de como ha venido con el tema de la seguridad, de esta forma tener una idea general de las deficiencias que existen y posteriormente realizar un análisis más avanzado de las vulnerabilidades.

Para esta entrevista, se ha realizado mediante un dialogo con la persona

encargada del departamento de sistemas, donde se le formulan unas preguntas que el entrevistado va a responder con la mayor veracidad del caso, se escoge a esa persona que está más involucrado en el área de sistemas de la empresa que conoce el manejo y el funcionamiento interno de las redes y los servidores. Entrevista dirigida al personal del Departamento de Sistemas, Anexo 2.

2.4. Metodología de desarrollo OSSTMM

Para este proyecto, se utiliza la metodología OSSTMM “Open Source Security Testing Metodología y Manual” creada por el instituto de Seguridad y Metodologías abiertas (ISECOM) (Herzog, 2010), esta metodología propone una serie de procesos de evaluación de vulnerabilidades, que se refleja de manera eficaz los niveles de seguridad en la infraestructura que va a ser evaluada, así se consigue ver que está formada por 4 ítems los cuales son los siguientes:

1. Seguridad de la Información
2. Seguridad de los Procesos
3. Seguridad de las Tecnologías de Internet
4. Seguridad de Comunicación

Seguridad de la Información.

En esta sección, se procede a evaluar la privacidad de las personas que son miembros de la empresa, para eso recopila información de internet, de fuentes confiables esta información tiene que ser procesada para determinar qué datos son privados y no estar expuestos al exterior.

Seguridad de los Procesos.

Esta esta sección, se efectúan pruebas, de esta manera consigue determinar que vulnerabilidades tienen en los dispositivos de comunicación y además analizar la información que está expuesta.

Seguridad en las Tecnologías de Internet.

Esta parte determina los servicios que tienen los servidores en cuestión y aplicaciones de internet, en busca de vulnerabilidades para posteriormente detectarlas, explotarla y dar una solución. Se realiza también pruebas referentes a peticiones de internet y sistemas de detección de terceras (intrusos que quieren vulnerar el sistema).

Seguridad en las Comunicaciones.

Esta sección, se efectúan pruebas en los dispositivos de comunicación como son VoIP, FAX, Correo de voz y PBX.

- **Seguridad Inalámbrica.**
  Se busca evalúan dispositivos que ofrecen comunicación no cableada mediante wifi, el objetivo es buscar configuraciones por defecto, para posteriormente dar una solución a la vulnerabilidad, que se encuentre en el proceso de pruebas.

- **Seguridad Física.**
  Esta parte evalúa la seguridad física de la empresa como son los controles de administración para acceso, donde se realiza por monitoreo mediante cámaras de seguridad, donde además existen alarmas que indican en caso de amenazas o catástrofes.

Esta propuesta de seguridad en el servidor VOIP Elastix, se va a realizar en la empresa LÁCTEO GUSTALAC LA POLACA, para prevenir ataques que amenacen la integridad, disponibilidad y la confidencialidad de la empresa, existen antecedentes de ataques realizados a los servidores principales de la empresa que pusieron en riesgo la información.

Esquema de la metodología OSSTMM

La metodología OSSTMM está dividida en cinco secciones, mediante las cuales permitirán identificar las vulnerabilidades, que posteriormente mitiga esos riesgos que compromete la información de la empresa, ante posibles ataques masivos en contra de los servidores. Además, al ser una metodología abierta de testeo de seguridad ayuda a la identificación de errores. Ver figura a continuación.

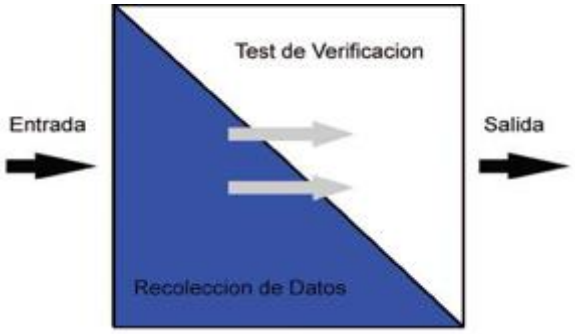
Figura 17. Esquema de la metodología OSSTMM.

Fuente: (Cruz, 2016)

Propósito

Tiene como propósito realizar la inspección de la seguridad de una empresa, dar técnicas para el auditor y además dar a conocer e interpretar los módulos, que se logra aplicar en cualquier tipo de prueba de seguridad. Ver figura a continuación.

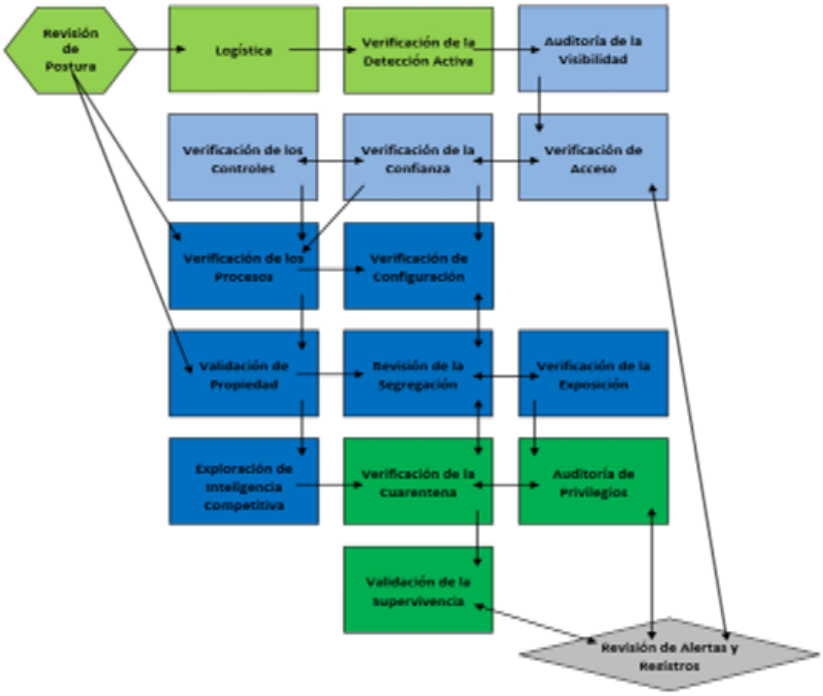
Figura 18. Propósito de OSSTMM



Fuente: (Cruz, 2016)

En la figura 19, se alcanza a observar cada uno de los procesos que van a ser adoptados por parte de los miembros del personal, que tenga que realizar la identificación de vulnerabilidades de cualquier ámbito informático que presentan las empresas tanto públicas como privadas que utilizan esta metodología OSSTMM, están clasificadas por secciones para su mejor comprensión.

Figura 19. Diagrama de secciones de metodología OSSTMM



Fuente: (Herzog, 2010)

Secciones de prueba

El modelo OSSTMM, se dividen en 3 módulos y cinco secciones como muestra la figura a continuación:

Figura 20. Secciones de prueba

MODULO	SECCIÓN OSSTMM	DESCRIPCIÓN
Seguridad Física	Humano	Todo el elemento humano comprometido en la organización
	Físico	Todo lo referente a hardware de la organización
Seguridad de las comunicaciones	Redes de datos	Son los sistemas electrónicos y redes de datos de la organización
	Telecomunicaciones	Comunicaciones analógicas y digitales de la comunicación
Seguridad del espectro electromagnética	Inalámbricas	Señales electromagnéticas en las comunicaciones o cualquier emanación de espectro

Fuente: (Herzog, 2010)

Para el caso de este proyecto de investigación, se analizarán las secciones que intervienen para determinar brechas que tiene el servidor Elastix PBX.

Ámbito y limitaciones de OSSTMM

La metodología de testeo de seguridad, se define como la reunión de reglas y lineamientos para QUÉ, CUÁLES, y CUÁNDO eventos son testeados, esta metodología es la que realiza las pruebas de seguridad externas, es decir la prueba de seguridad desde un entorno de privilegio, para así eludir los componentes, alarmas, procesos y ganar acceso privilegiado. Estas limitaciones de testeo tienen diferencias considerables para testeo externo e interno, esto radica fundamentalmente en que los objetivos, privilegios y los resultados que tengan relación con testeo interno a interno. Ver figura a continuación.

Figura 21. Etapa de pruebas de penetración

Fuente: (Pinzón, Talero, & Jhon, 2014)

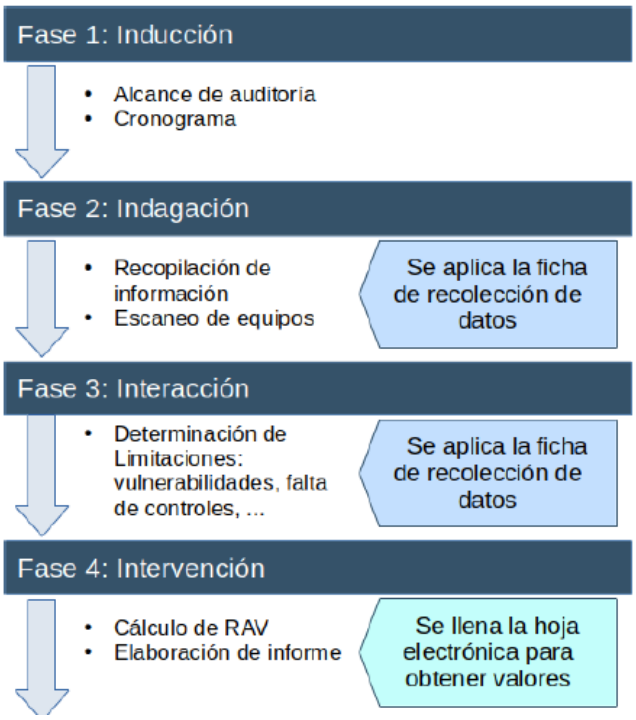
Fases de la metodología OSSTMM

La metodología de OSSTMM tiene cuatro fases que es necesario seguir cada una, para tener una prueba de seguridad eficaz, de los sistemas información de esta manera es como se tiene lo siguiente:

A. Fase de inducción
B. Fase de indagación
C. Fase interacción
D. Fase de intervención

Ver figura a continuación.

Figura 22. Fases Metodologia OSSTMM



Fuente: (Navia & Zambrano, 2021)

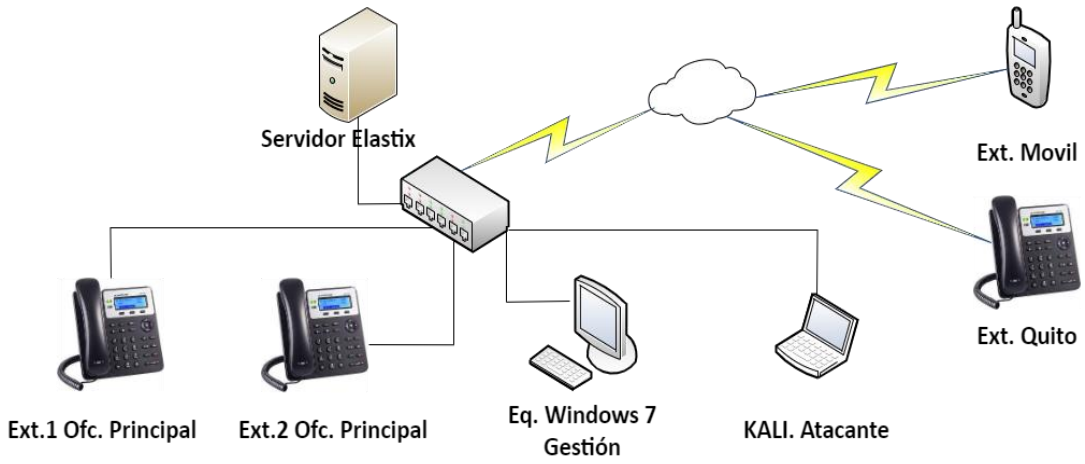
A. Fase de Inducción

En esta fase de inducción el encargado de la auditoria comienza con una evaluación de los alcances y las limitaciones que va a tener la auditoria, con frecuencia este tipo de test, se determina mejor después de esta fase (Ortega, Pupiales, & Suárez, 2017). El primer paso consiste en determinar el lugar físico donde se llevará a cabo la implementación. Esto puede ser un laboratorio de la empresa u otro entorno adecuado para realizar pruebas y análisis de seguridad. El siguiente paso es realizar un análisis exhaustivo para identificar las posibles brechas de seguridad. Esto implica revisar el sistema, la red, los dispositivos y cualquier otro componente relevante en busca de vulnerabilidades o debilidades que puedan ser explotadas por posibles amenazas. Una vez que se ha establecido el entorno de laboratorio y se han definido los equipos y dispositivos disponibles, se llevan a cabo prácticas de seguridad para identificar y detectar vulnerabilidades

Estado actual del laboratorio

Como alcanza ver en la figura 23, en el laboratorio, que se implementa cuenta con un servidor Elastix 2.4 que permite las comunicaciones VoIP, también tiene un switch el cual tiene acceso a internet, a este dispositivo, se conectan los teléfonos alámbricos e inalámbrico, se agrega un computador con sistema operativo Windows 7 para realizar la gestión de configuración del servidor Elastix y las extensiones, y por último en una computadora más que tiene instalado Kali Linux el cual va ayudar a realizar ataques, de esta manera comprobar las vulnerabilidades existentes que posteriormente ir solucionado cada uno de ellos. De esta forma crear un ambiente seguro que garantiza a la empresa confidencialidad y privacidad respecto a las comunicaciones entre las sucursales, dispositivos móviles y los clientes. Se comprueba la criticidad de la información de la empresa.

Figura 23. Laboratorio implementado



Fuente: Elaborado por el autor

En la tabla 3, se logra ver la cantidad de equipos, que se tienen en el laboratorio, también la descripción de cada equipo que sea implementado y las características de cada modelo que tiene, esto además logra servir para llevar un control de inventario de los activos que tiene la empresa. En el equipo de gestión, se logra acceder web a la configuración del Servidor Elastix.

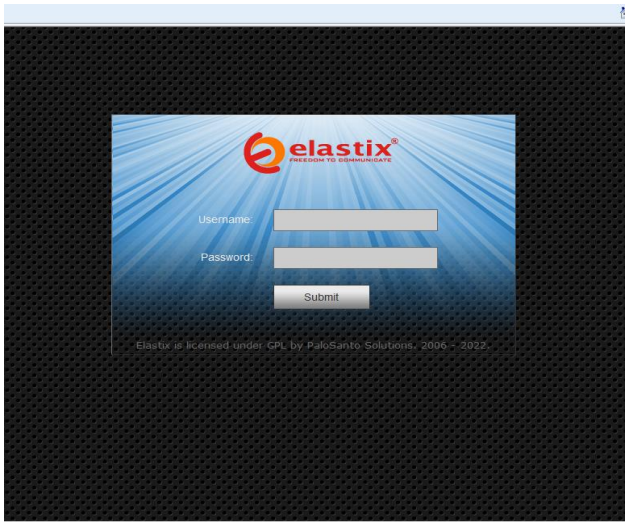
Tabla 3. Equipos de implementación en laboratorio

Equipos para la implementación del laboratorio			
Nro.	**Cant.**	**Descripción**	**Característica o Modelo**
1	1	Servidor con Elastix	AMD E-350D, Mem de 4Gb y HD 500 Gbs
2	3	Teléfono IP Grandstream	GRP2601
3	1	teléfono Samsung	A03
4	1	Switch TP-link 10/100/1000	TL-SG105

Fuente: Elaborado por el autor

En la figura 24, logra ver que es la pantalla de inicio de sesión del servidor Elastix, donde ingresa un usuario y contraseña, para lograr acceder al sistema de configuraciones.

Figura 24. Inicio sesión Elastix



Fuente: Elaborado por el autor

En la tabla 4, se va a especificar el número de dispositivo y además las extensiones, de esta manera realizar la conectividad y posteriormente proceder a realizar el análisis de vulnerabilidades, se planteó 4 dispositivos para la realización de las pruebas.

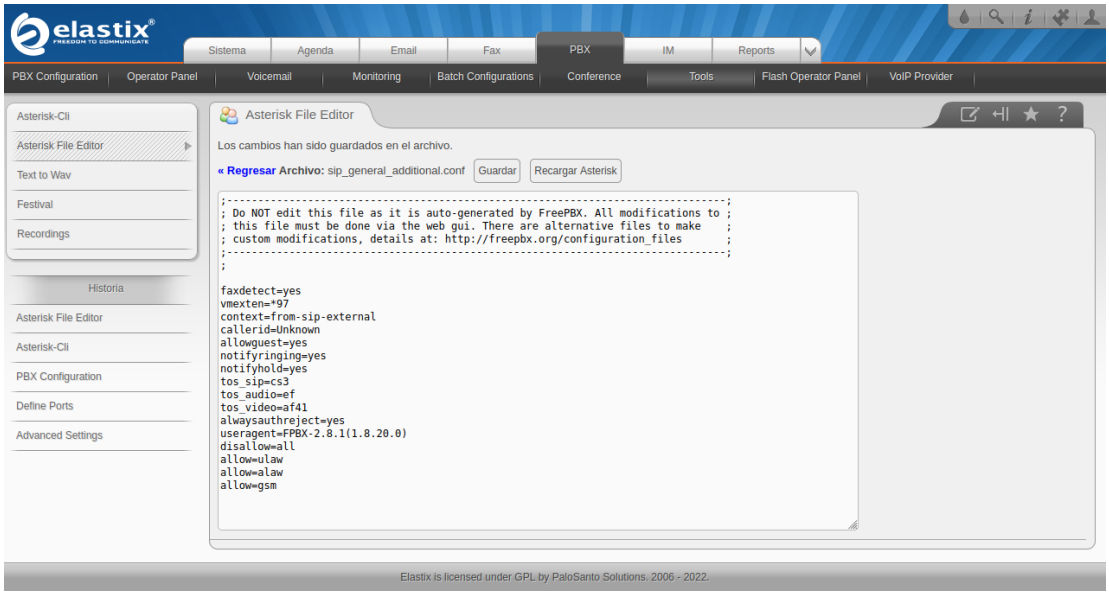
Tabla 4. Extensiones creadas por el laboratorio

Extensiones Creado en Laboratorio		
Nro.	**Ext.**	**descripción**
1	101	Ventas1
2	102	Contabilidad
3	103	Quito
4	104	Vendedor1

Fuente: Elaborado por el autor

En la figura 25, se evidencia el estado de la configuración default del servidor Elastix con la opción de allowguest en YES. Esta función permite llamada INVITE.

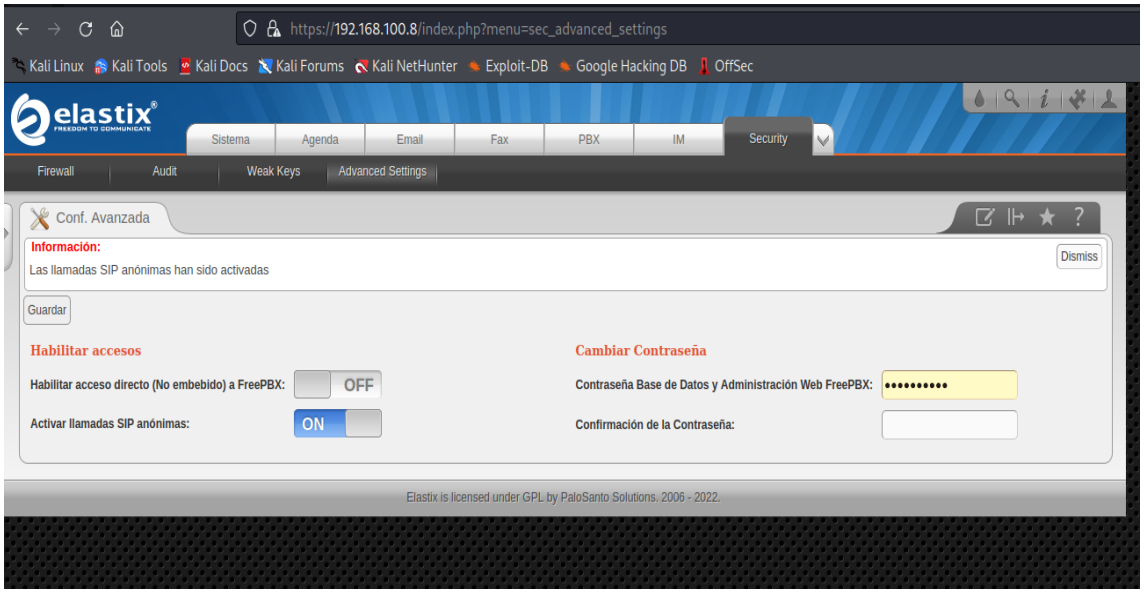
Figura 25. opción allowguest = YES



Fuente: Elaborado por el autor

En la figura 26, se evidencia el estado de la configuración default del servidor Elastix con la opción Permitir llamada SIP Anónima. Esta función permite llamadas anónimas.

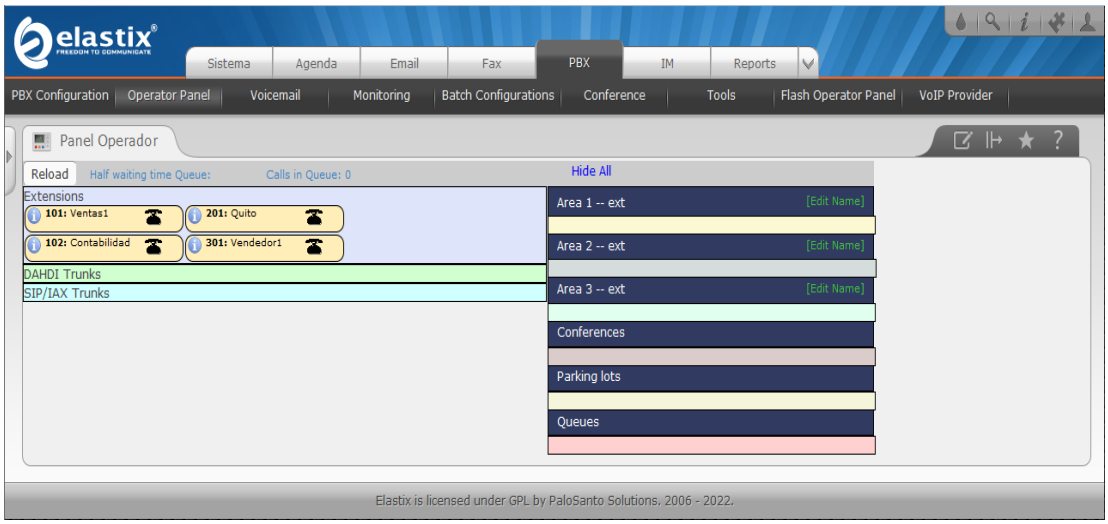
Figura 26. Llamadas SIP



Fuente: Elaborado por el autor

En la figura 27, se logra ver la configuración del PBX, que son las extensiones creadas en los diferentes departamentos de la empresa y una extensión móvil.

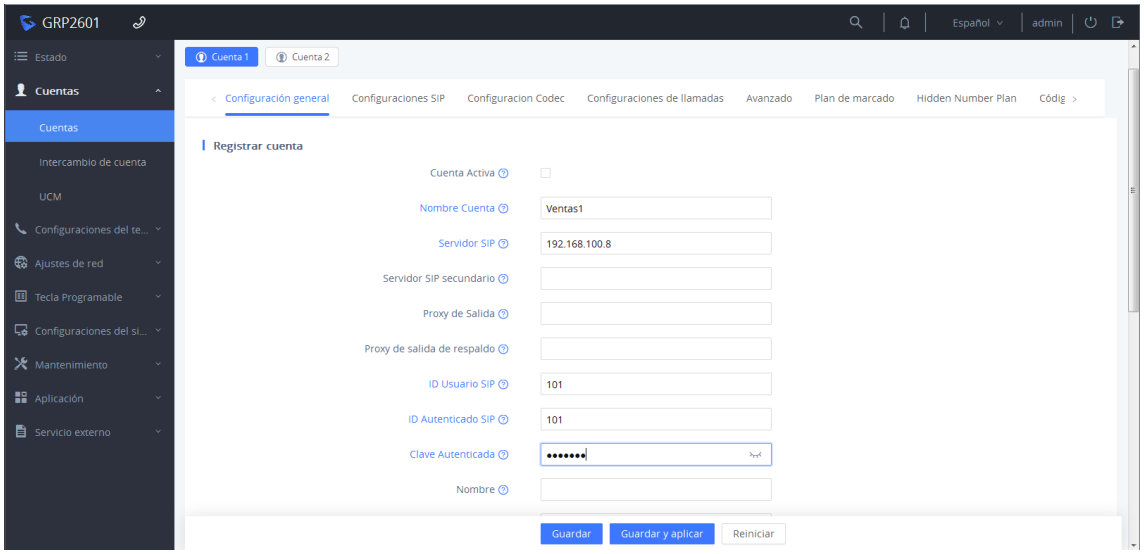
Figura 27. Configuraciones los teléfonos IP con el servidor PBX



Fuente: Elaborado por el autor

En la figura 28, se alcanza a ver que está realizada las configuraciones para la extensión del departamento de ventas.

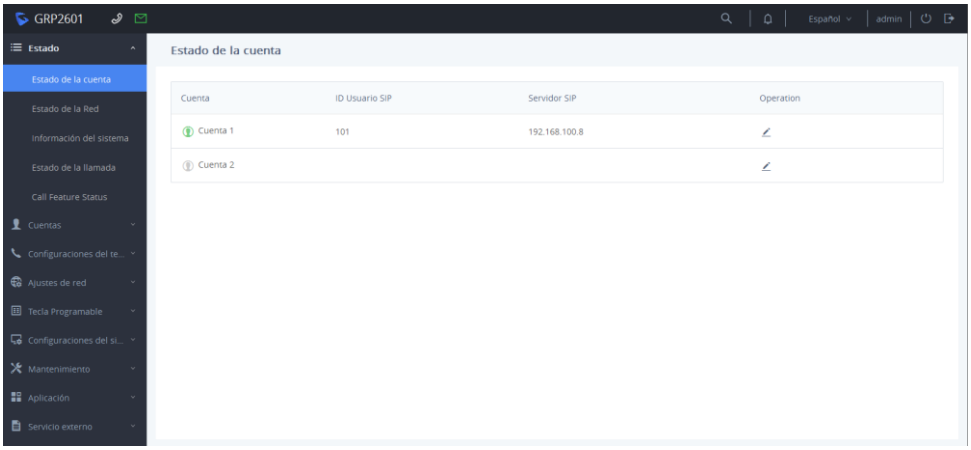
Figura 28. Extensión Ventas 1



Fuente: Elaborado por el autor

En la figura 29, se logra ver que establece la conexión de la extensión 101 al servidor Elastix.

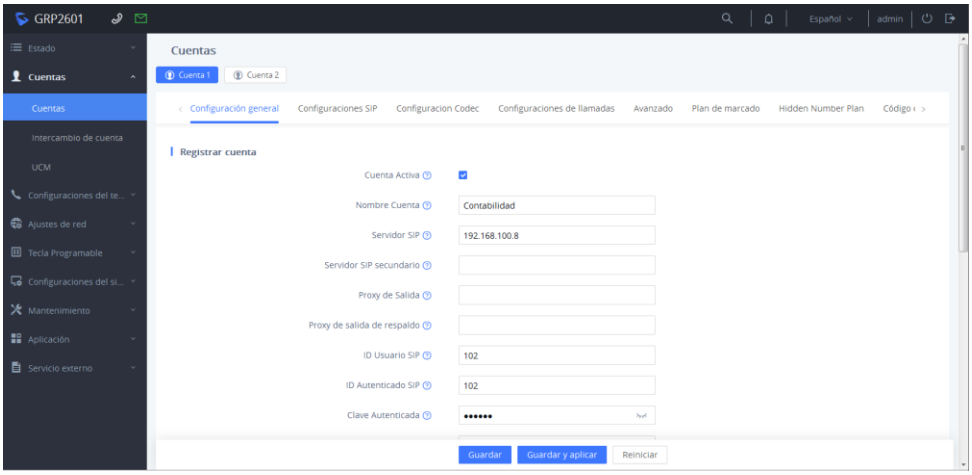
Figura 29. Panel de configuraciones



Fuente: Elaborado por el autor

En la figura 30, se logra ver que está realizada las configuraciones para la extensión del departamento de contabilidad.

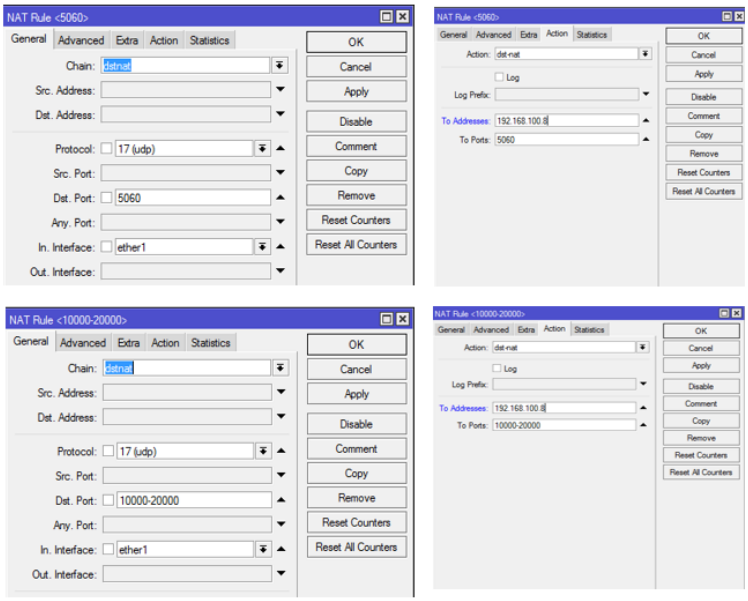
Figura 30. Extensión Contabilidad



Fuente: Elaborado por el autor

En la configuración del router principal matriz, se alcanza a observar que la comunicación de las extensiones de las sucursales y extensiones móviles está configurada en NAT para su redireccionamiento de los puertos requeridos para la interconexión. Figura 31, configuración de puertos abiertos para la conexión de las extensiones de los otros sucursales o móviles.

Figura 31. NAT



Fuente: Elaborado por el autor

B. Fase de indagación

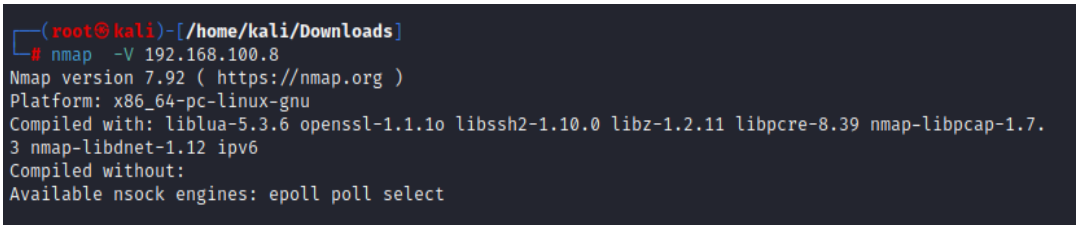
En esta fase, se requiere conocer las pruebas de seguridad, en base a los objetivos trasmitidos a las interacciones con los activos, aquí es donde se definirá los alcances. En este punto, se escoge las técnicas para el análisis de las vulnerabilidades, después va a detallar cada evento, que se va a realizar y como se van a elaborar, para tener un respaldo de lo que vendría siendo la documentación. Se va a usar las siguientes herramientas y técnicas para encontrar las vulnerabilidades que tiene el servidor Elastix.

1. **Nmap**
2. **NESSUS**
3. **CVE (Common Vulnerabilities and Exposures)**
4. **SIPVICIOUS**

NMAP

En la figura 32, se procede a ejecutar el comando NMAP para saber que puertos están abiertos, lo correcto sería que estén cerrados, evitar que intrusos logre ingresar, de esta manera corrigen las brechas de seguridad para posteriormente mitigarla.

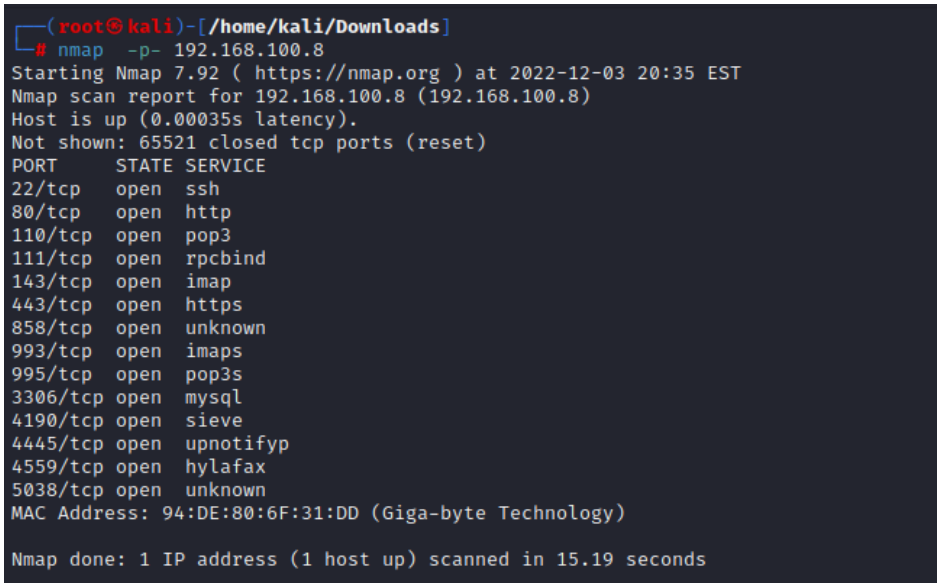
Figura 32. Versión de Elastix 2.4



Fuente: Elaborado por el autor

En la figura 33, con el comando **nmap -p- 192.168.100.8**, el cual permite realizar un escaneo, para finalmente mostrar los puertos abiertos y los servicios que tiene el servidor.

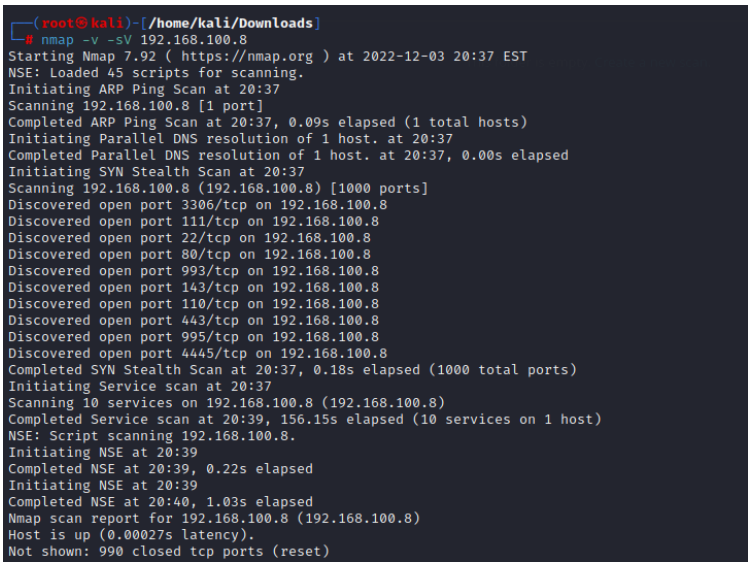
Figura 33. Nmap



Fuente: Elaborado por el autor

En la figura 34, se observa cómo están los servicios y los puestos disponible que tiene el servidor Elastix. Esta fase permite realizar un reconocimiento del estado del servidor, aprovechar alguno tipo debilidad en el equipo para un posible ataque.

Figura 34. Puertos abiertos búsqueda más avanzada



Fuente: Elaborado por el autor

En la tabla 5, se detalla los puertos y servicios disponibles en el servidor Elastix versión 2.4:

Tabla 5. Puertos y Servicios descubierto por NMAP

N°	PUERTO ABIERTO	SERVICION DISPONIBLES
1	22	SSH
2	80	HTTP
3	110	POP3
4	111	RPCBIND
5	143	IMAP
6	443	HTTPS
7	858	UNKNOWN
8	993	IMPAS
9	995	POSP3
10	3306	MYSQL
11	4190	SIEVE
12	4445	UPNOTIFYP
13	4559	HYLAFAS
14	5038	UNKNOWN

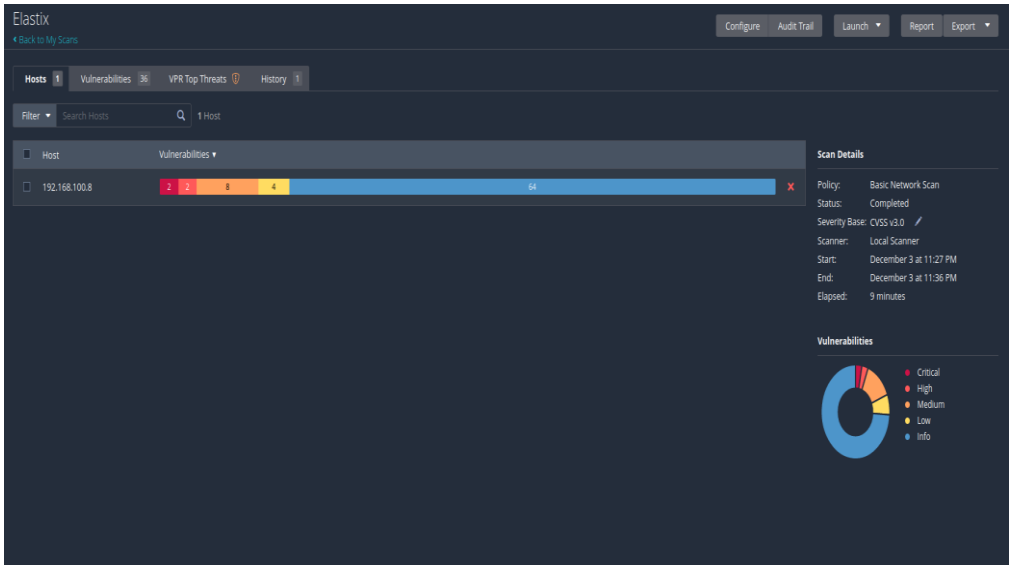
Fuente: Elaborado por el autor

NESSUS

En la figura 35, se realizó un análisis de las vulnerabilidades al servidor Elastix 2.4 con la herramienta NESSUS, se hallaron las siguientes vulnerabilidades:

- 80% corresponde a datos informativo.
- 5% corresponde al nivel bajo que representa 4 vulnerabilidades.
- 10% corresponde al nivel medio que representa 8 vulnerabilidades.
- 2.5% corresponde al nivel alto que representa 2 vulnerabilidad.
- 2.5% corresponde al nivel crítico que representa 2 vulnerabilidad.

Figura 35. Nessus

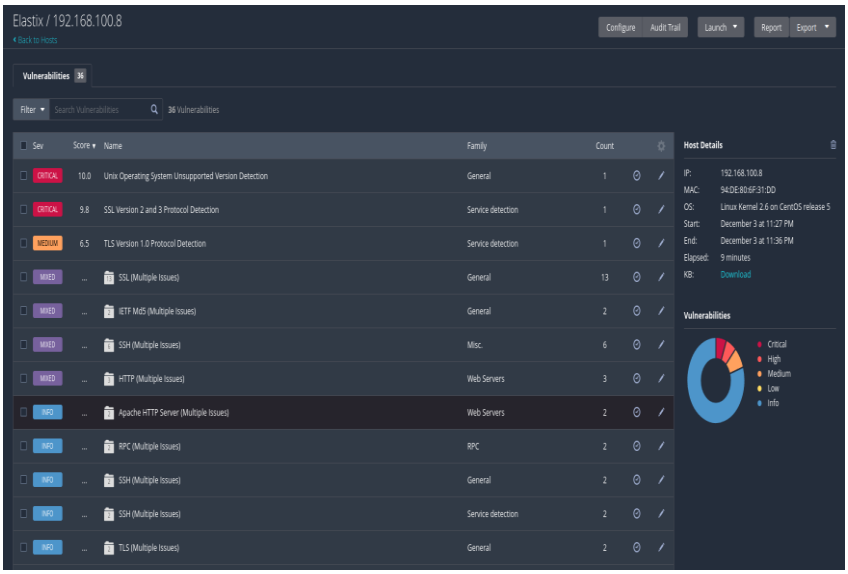


Fuente: Elaborado por el autor

En las figuras 36, 37 y 38, se logra observar las vulnerabilidades critica del servidor que detallo a continuación:

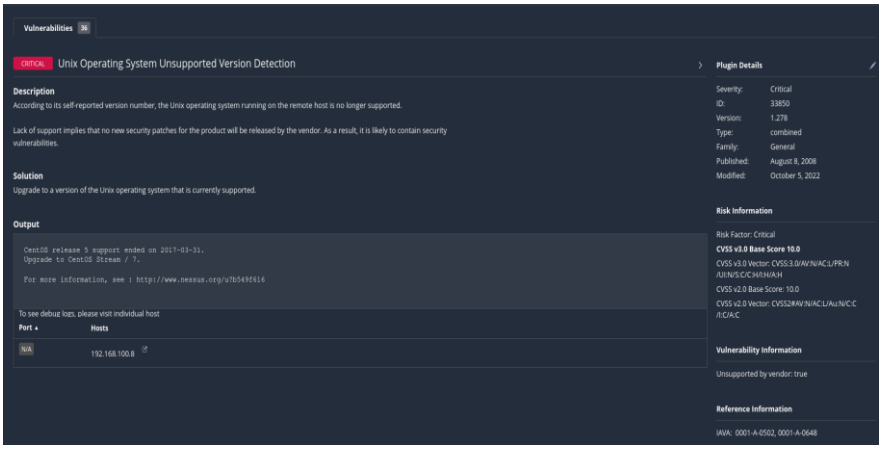
- Unix Operating System Unsupported Version Detection
- SSL Version 2 and 3 Protocol Detection

Figura 36. Nessus



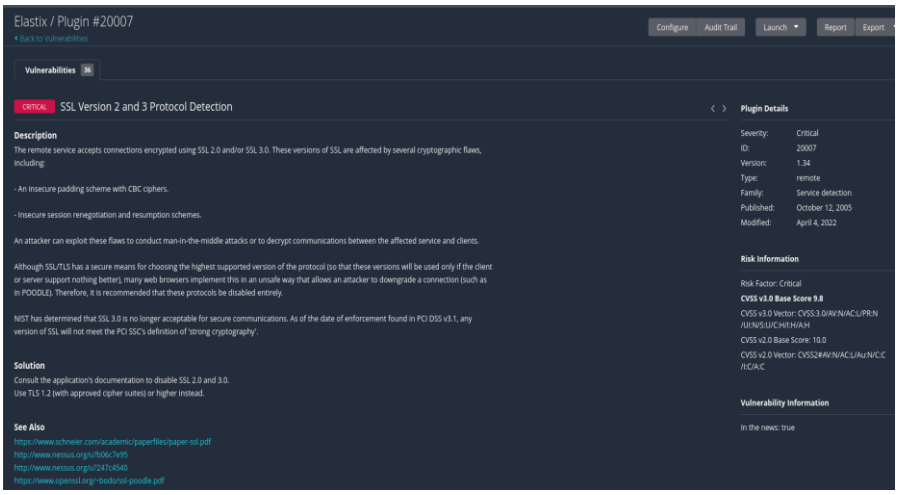
Fuente: Elaborado por el autor

Figura 37. Nessus



Fuente: Elaborado por el autor

Figura 38. Nessus

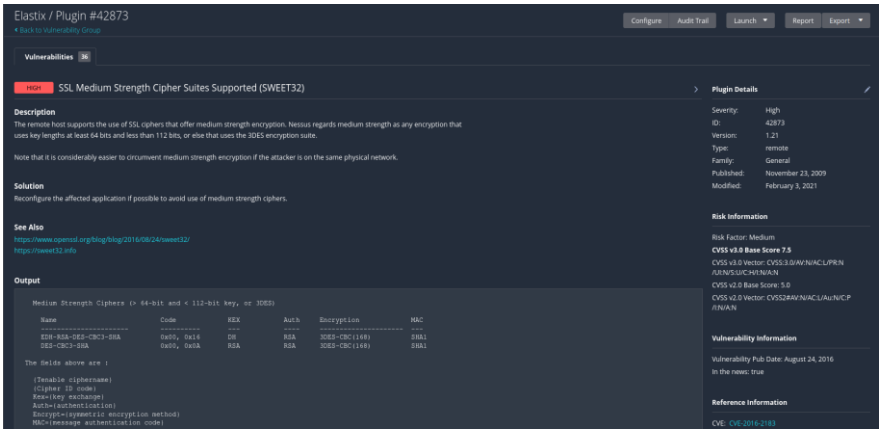


Fuente: Elaborado por el autor

En la figura 39, se observa la vulnerabilidad alta del servidor que detallo a continuación:

- SSL Medium Stengthc Cipher Suite Supported (SWEET32)

Figura 39. Nessus

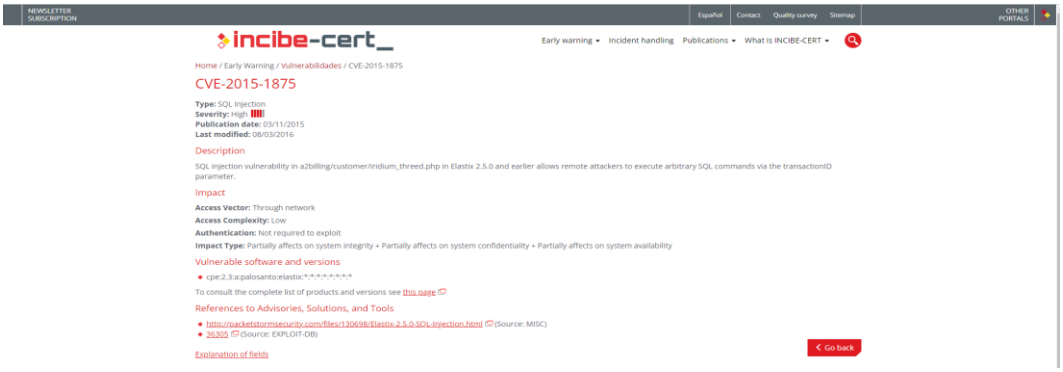


Fuente: Elaborado por el autor

CVE (Common Vulnerabilities and Exposures)

CVE es un proyecto de seguridad centralizado en software para el público general, financiado por los Estados Unidos con el departamento División de Seguridad Nacional y MITRE Corporation es el encargo de mantener los registros actualizados. El glosario CVE utiliza el Protocolo de automatización de contenido de seguridad (SCAP) para recopilar información sobre vulnerabilidades y exposiciones de seguridad, catalogarlas de acuerdo con varios identificadores y proporcionarles ID únicos. Ver figuras a continuación.

Figura 40. Vulnerabilidad Registra con CVE-2015-1875



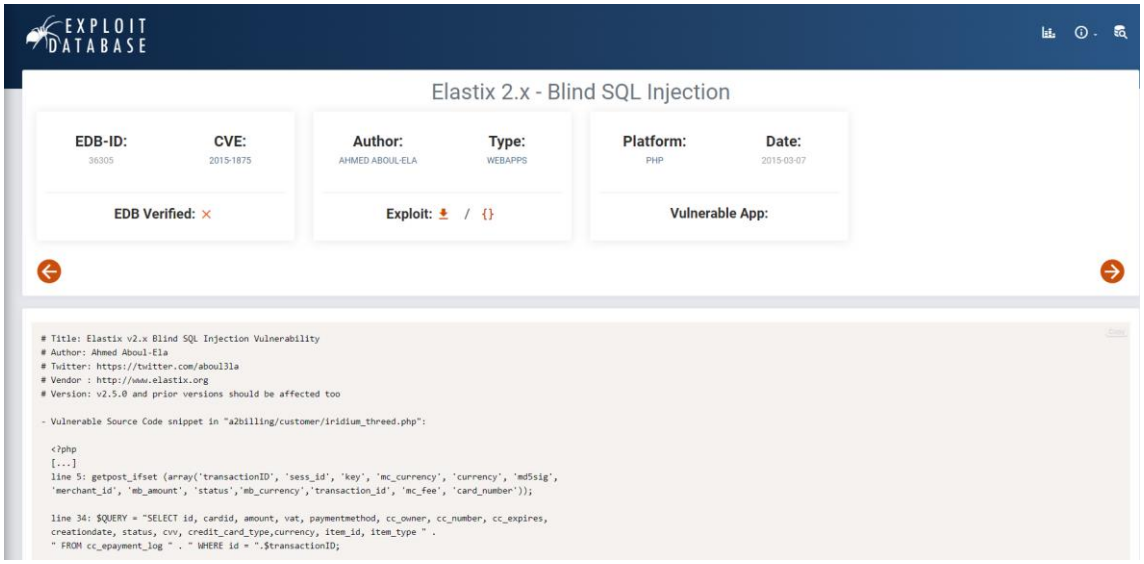
Fuente: Incibe-Cert

Existen varias plataformas donde encontraron información de vital importancia sobre los CVE (Common Vulnerabilities and Exposures), en las figuras 41, 42 y 43, se alcanza a observar la criticidad de esta plataforma PBX Elastix 2.4

Figura 41. Vulnerabilidad Registran NIST

Fuente: NIST

Figura 42. Vulnerabilidad Registrado en Exploit database



Fuente: Exploit Database

Figura 43. Exploit para la explotación

```
# Title: Elastix v2.x Blind SQL Injection Vulnerability
# Author: Ahmed Aboul-Ela
# Twitter: https://twitter.com/aboul3la
# Vendor : http://www.elastix.org
# Version: v2.5.0 and prior versions should be affected too

- Vulnerable Source Code snippet in "a2billing/customer/iridium_threed.php":

 <?php
```

```
[...]
line 5: getpost_ifset (array('transactionID', 'sess_id', 'key', 'mc_currency', 'currency', 'md5sig',
'merchant_id', 'mb_amount', 'status','mb_currency','transaction_id', 'mc_fee', 'card_number'));

line 34: $QUERY = "SELECT id, cardid, amount, vat, paymentmethod, cc_owner, cc_number,
cc_expires,
creationdate, status, cvv, credit_card_type,currency, item_id, item_type " .
" FROM cc_epayment_log " . " WHERE id = ".$transactionID;

line 37: $transaction_data = $paymentTable->SQLExec ($DBHandle_max, $QUERY);
[...]
?>

 The GET parameter transactionID was used directly in the SQL query
 without any sanitization which lead directly to SQL Injection vulnerability.

- Proof of Concept:

http://[host]/a2billing/customer/iridium_threed.php?transactionID=-1 and
1=benchmark(2000000,md5(1))

The backend response will delay for few seconds, which means the benchmark() function was
executed successfully

- Mitigation:

 The vendor has released a fix for the vulnerability. It is strongly recommended to update your
elastix server now

 [~] yum update elastix-a2billing
```

Fuente: Exploit Database

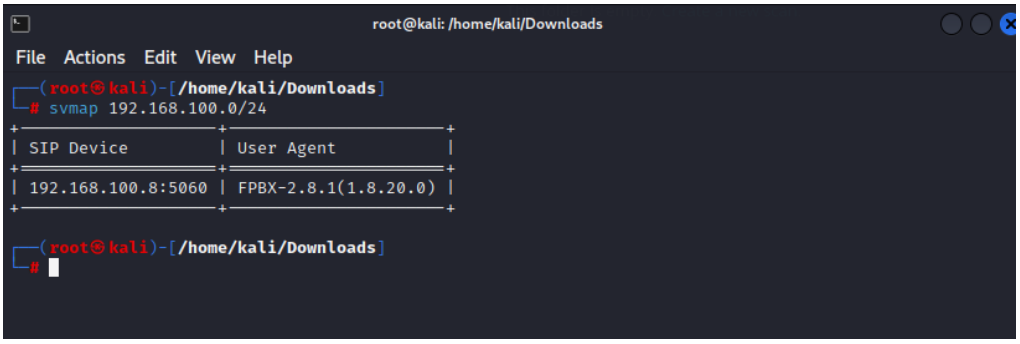
SIPVICIOUS

La herramienta para realizar esta fase indagación es SIPVICIOUS con los siguientes comandos como:

- svmap
- svwar

En la figura 44, se procede hacer el reconocimiento del servidor Elastix para lo cual para el ingreso el comando svmap.

Figura 44. Reconocimiento del servidor Elastix

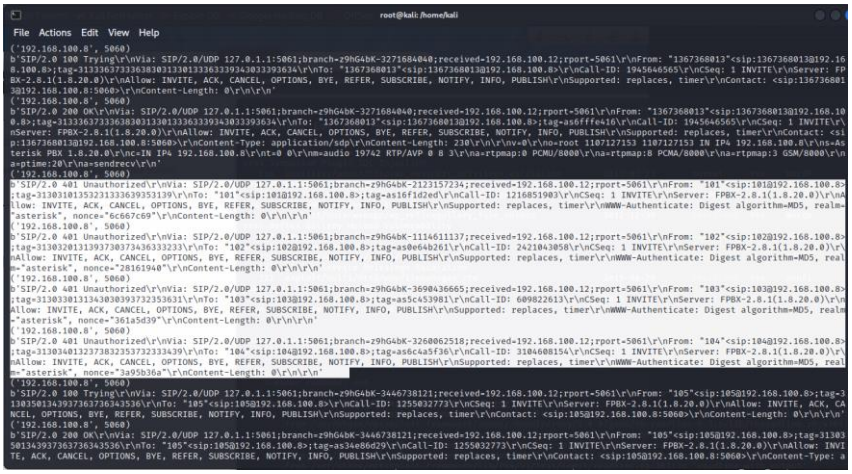


Fuente: Elaborado por el autor

En la figura 45, se procede a realizar el descubrimiento de las extensiones existentes en el servidor Elastix, utiliza el siguiente comando:

svwar -m INVITE 192.168.100.8 -e 101-104 –debug –force.

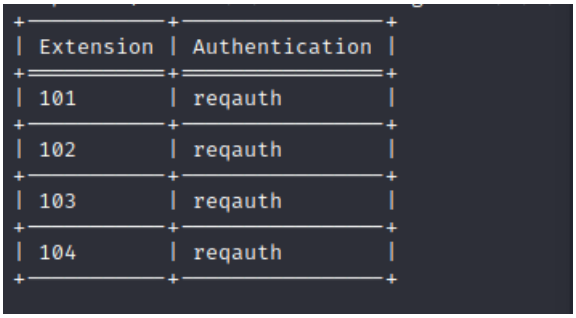
Figura 45. Reconocimiento de las extensiones



Fuente: Elaborado por el autor

En la figura 46, se logra ver las extensiones, que se tiene cada departamento de la empresa.

Figura 46. Resultado del reconocimiento de las extensiones



Fuente: Elaborado por el autor

C. Fase interacción

Esta fase es importante para la auditoria de la información, el auditor descubre una vez hecho el análisis como son las fortalezas y debilidades que tienen el sistema, también se dan a conocer distintos tipos de valores e información fuera de lugar y mal administrada como un activo que descubre (Ortega et al.,(2017).

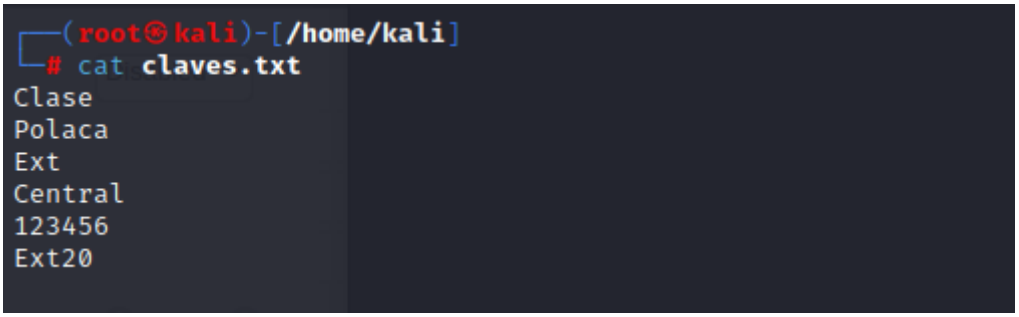
En esta fase se procede a realizar los posibles ataques mediante técnicas de Hacking Ético para encontrar posibles vulnerabilidades, identificar correctamente las brechas de seguridad en sus configuraciones. Con estos se alcanza a verificar cuales son los riesgos que presenta este servidor y los pasos a realizar son las siguientes, que se detallan a continuación.

- Robo de contraseña

Para realizar esta fase, se necesita contar con un diccionario, y el uso de la herramienta SVCRACK, que se encuentra en la suite de SIPVICIOUS. Como primer paso para la creación del diccionario, para crear un archivo con el siguiente comando vi claves.txt y dentro del archivo, se especifican palabras claves que permitirá crear un diccionario.

En la figura 47, se muestra el texto plano con las palabras claves para generar un diccionario.

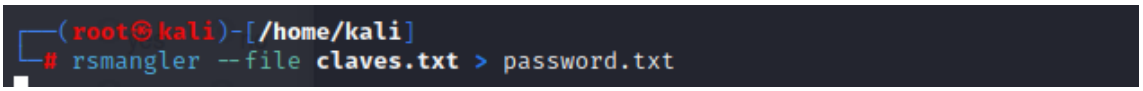
Figura 47. Directorio Kali Linux



Fuente: Elaborado por el autor

En la figura 48, se usa el siguiente comando para generar un diccionario como los muestra la figura a continuación.

Figura 48. Comando generar diccionario

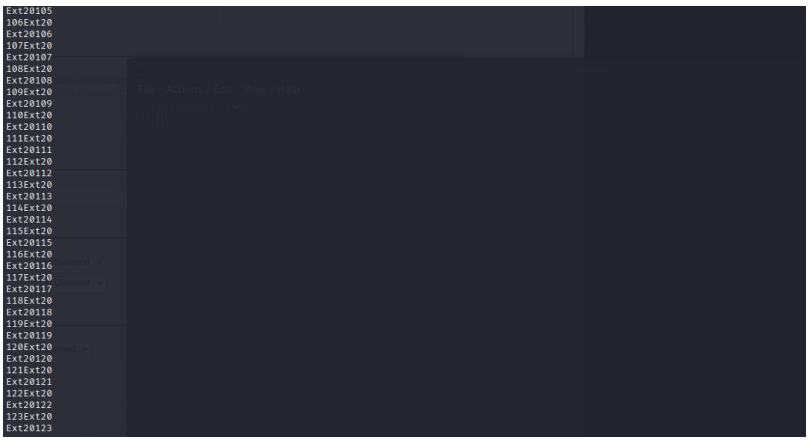


Fuente: Elaborado por el autor

En la figura 49, se generó un diccionario para realizar el ataque de fuerza bruta a las extensiones, para realizar esta acción, se usa la herramienta Svcrack con el siguiente comando.

svcrack -u101 192.168.100.8 -d password.txt

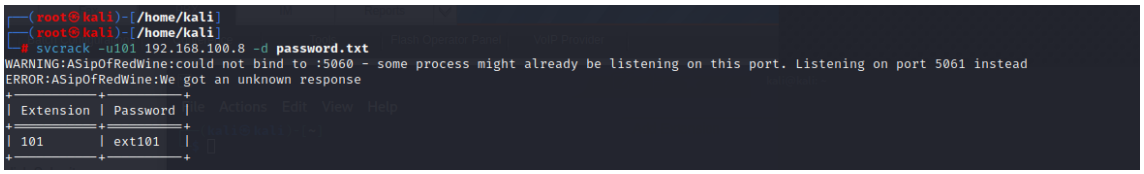
Figura 49. Explotación servidor



Fuente: Elaborado por el autor

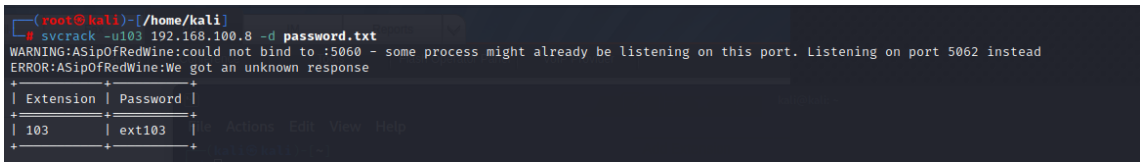
En la figura 50, 51 y 52, se realizó los descubrimientos de las contraseñas de las extensiones.

Figura 50**.** Svcrack ext101



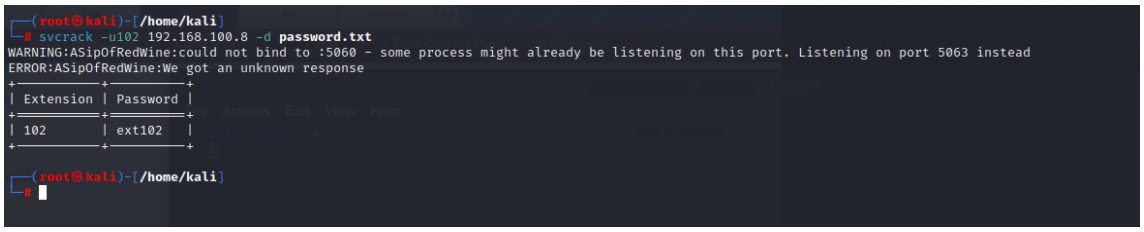
Fuente: Elaborado por el autor

Figura 51**.** Svcrack ext103



Fuente: Elaborado por el autor

Figura 52**.** Svcrack ext102

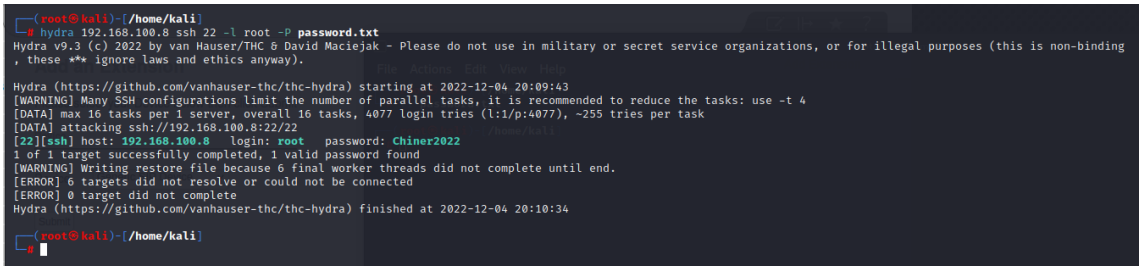


Fuente: Elaborado por el autor

En la figura 53, se aprecia que obtuvo la coincidencia con la contraseña por medio del diccionario. Con este ataque de fuerza bruta al usuario root, por medio de esta herramienta de HYDRA, se logra tener acceso total a central VoIP por medio del servicio SSH en el puerto 22. Para realizar este ataque, se ejecuta la siguiente línea de comando:

hydra 192.168.100.8 ssh 22 -l root -P password.txt.

Figura 53**.** Ataque SSH



Fuente: Elaborado por el autor

- **Interceptación (Eavesdropping)**

En la figura 54, se logra ver el comando para ejecutar esta herramienta ETTERCAP para la captura de tráfico de la red.

Figura 54. Sniifer tráfico de las llamadas

Fuente: Elaborado por el autor

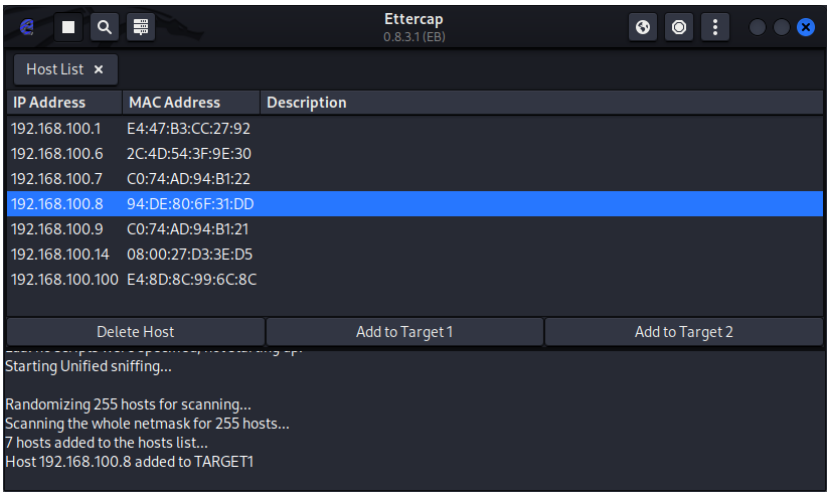
En la figura 55, se logra ver la pantalla principal del Ettercap para LAN con switch.

Figura 55**.** Ettercap

Fuente: Elaborado por el autor

En la figura 56, se logran visualizar los dispositivos que están en la red, se consigue ver las direcciones IP y además la dirección MAC de los dispositivo.

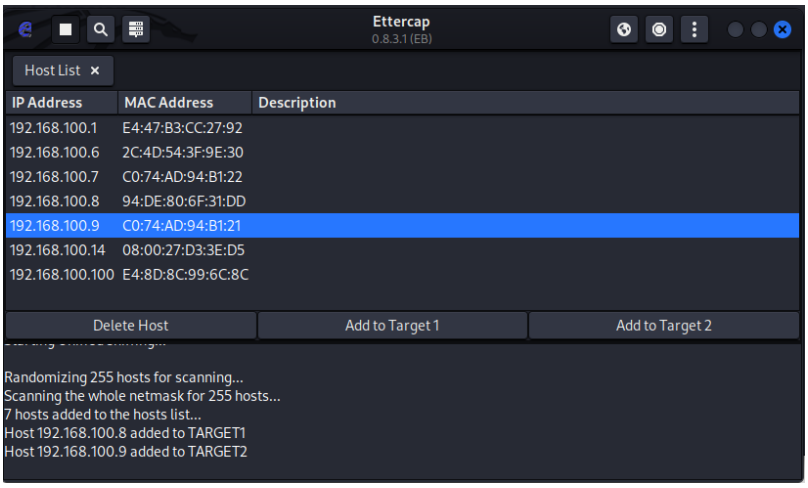
Figura 56**.** Direcciones IP y Mac



Fuente: Elaborado por el autor

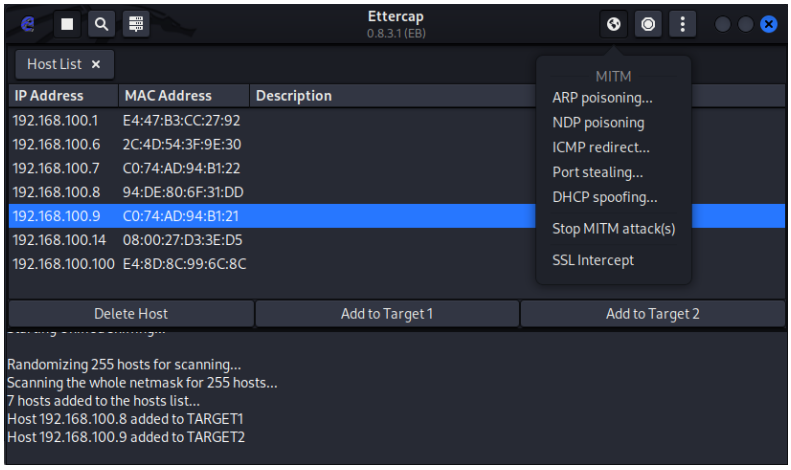
En la figura 57 y 58, se muestra los hosts que están en las listas y los que van a agregar al Target.

Figura 57. Hosts agregados a las listas



Fuente: Elaborado por el autor

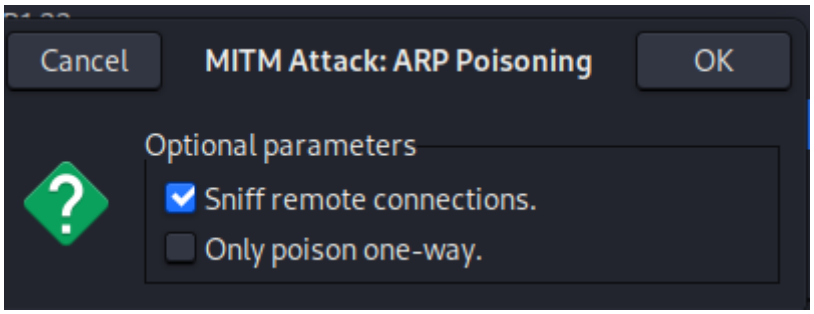
Figura 58. Hosts agregados a las listas



Fuente: Elaborado por el autor

En la figura 59, es esta opción que muestra los parámetros donde logra hacer el Sniffer conexiones remotas, para después realizar los ataques de interceptación.

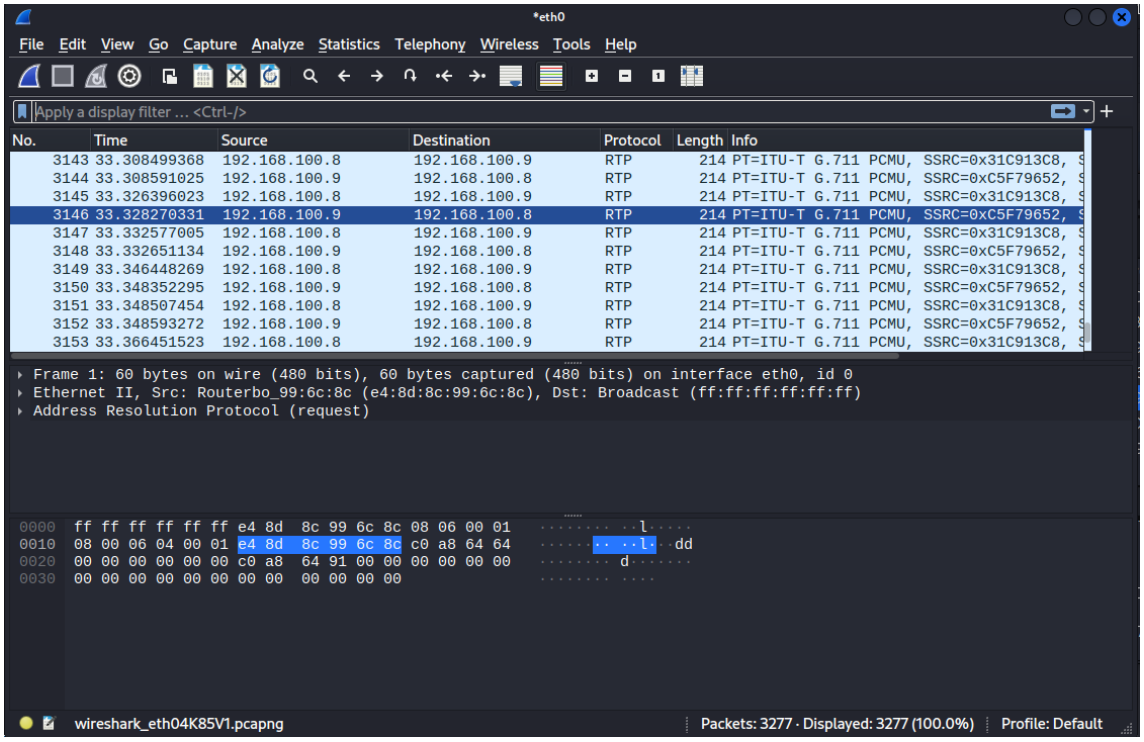
Figura 59. Conexiones remotas



Fuente: Elaborado por el autor

Se observa que la herramienta empieza a mostrar el tráfico que hay en la red, los recursos que consume en las sesiones el número de información, que se está intercambiado, como se observa en la figura 60.

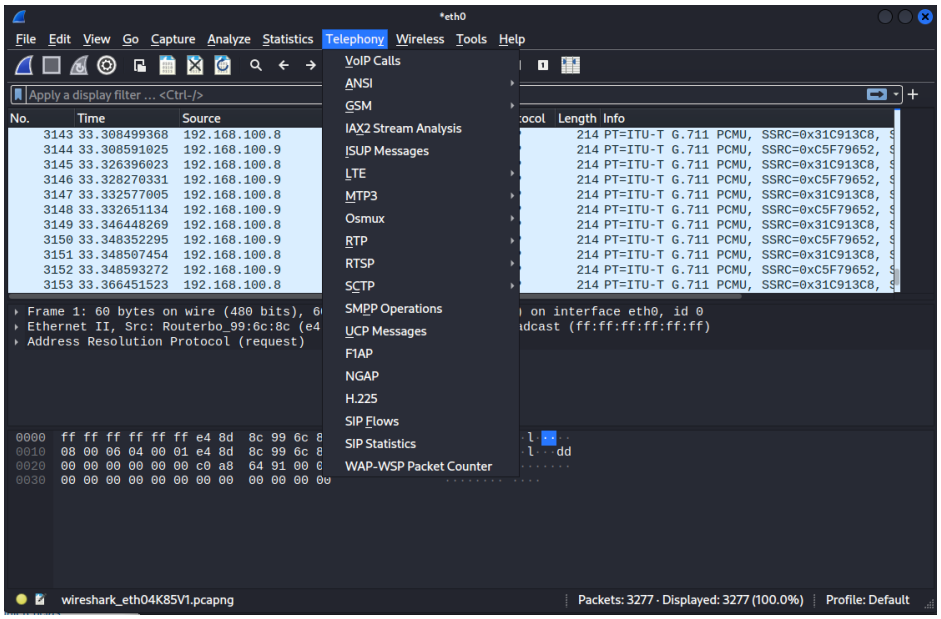
Figura 60. Herramienta Wireshack



Fuente: Elaborado por el autor

En la figura 61, se logra ver las capturas del tráfico para VoIP Calls, en donde a continuación, se muestra los resultados que logran obtener el escaneo.

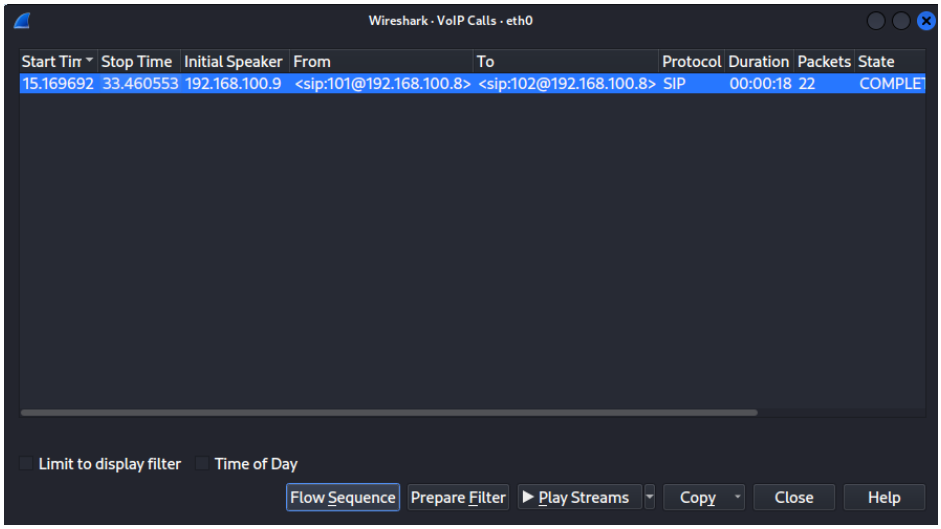
Figura 61. Captura el tráfico en la red



Fuente: Elaborado por el autor

En la figura 62, se observa que a través del VOIP Calls, se logra ensamblar los paquetes entre las comunicaciones de los 2 targets. Indica el tiempo de duración de la llamada efectuado.

Figura 62**.** Herramienta Eavesdropping



Fuente: Elaborado por el autor

En la figura 63, se consigue escuchar la conversación entre los targets, este ataque se ejecutó con normalidad y como resultado obtuvo la conversación confidencial sin ningún tipo de autorización.

Figura 63**.** Escucha De Llamadas Ilegales O Eavesdropping

Fuente: Elaborado por el autor

- **Ataque WEB**

Un ataque web, se refiere a cualquier intento malicioso de comprometer la seguridad de un sitio web o aplicación web. Estos ataques suelen tener como objetivo obtener acceso no autorizado, robar información confidencial, interrumpir o dañar el funcionamiento del sitio web, o llevar a cabo actividades ilegales.

Existen varios tipos de ataques web, entre los cuales se incluyen:

- Inyección de código: Se aprovechan de las vulnerabilidades en la entrada de datos para inyectar y ejecutar código malicioso en la aplicación web.

- Cross-Site Scripting (XSS): Consiste en la inserción de código malicioso en páginas web visitadas por otros usuarios, lo que permite robar información, realizar redireccionamientos no autorizados o ejecutar acciones no deseadas en el navegador del usuario.

- Cross-Site Request Forgery (CSRF): Implica el engaño de un usuario para que realice acciones no deseadas en una aplicación web en la que está autenticado, se aprovecha de su sesión activa.

- Ataques de fuerza bruta: Se intenta adivinar contraseñas o claves mediante la prueba sistemática de diferentes combinaciones hasta encontrar la correcta.

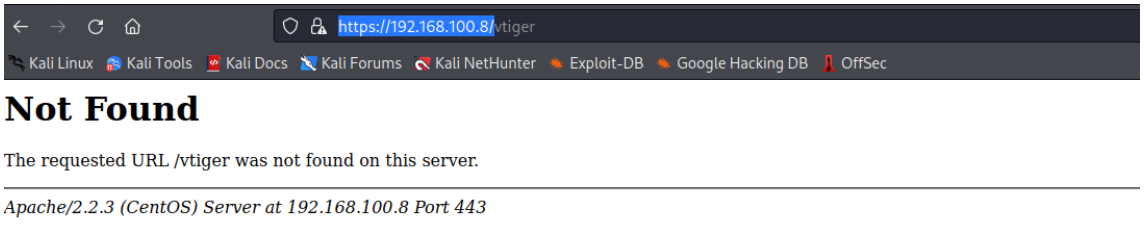
- DDoS (Distributed Denial of Service): Se realiza mediante la inundación del sitio web con una gran cantidad de solicitudes de tráfico falso o tráfico legítimo excesivo, lo que provoca la saturación de los recursos del servidor y la interrupción del servicio para los usuarios legítimos.

- Secuestro de sesión: El atacante roba o intercepta la sesión de un usuario legítimo para obtener acceso no autorizado a la aplicación o sitio web.

Es importante implementar medidas de seguridad adecuadas, como el uso de firewall, la validación de datos de entrada, el cifrado de información confidencial y la aplicación de buenas prácticas de desarrollo seguro, para protegerse contra estos ataques.

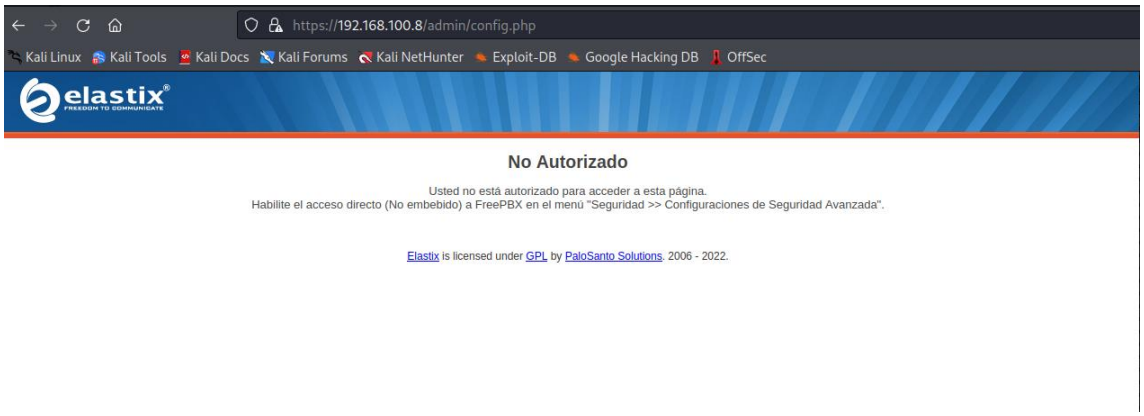
Los resultados no fueron de manera exitosa, sin embargo, se logra recopilar información como qué tipo de servidor web tiene instalado, la versión del servicio, el puerto a la escucha y sobre todo no utiliza un certificado SSL para una conexión segura a través del puerto 443, se detallan en las figuras 62, 63 y 64.

Figura 64. Descubrimiento de la información del servidor WEB



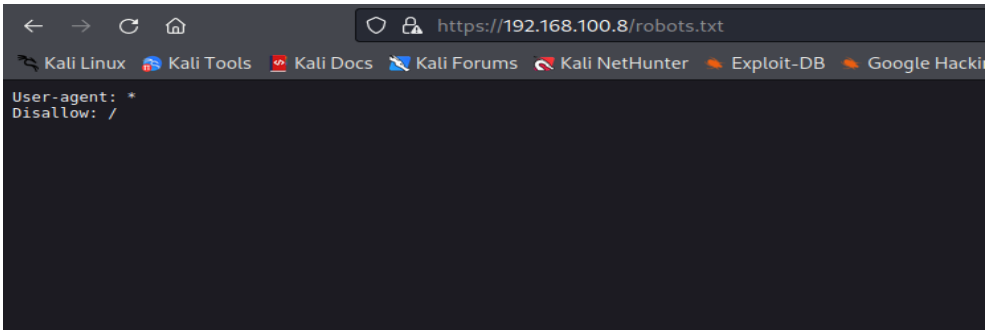
Fuente: Elaborado por el autor

Figura 65. Descubrimiento de la información del servidor WEB



Fuente: Elaborado por el autor

Figura 66. Descubrimiento de la información del servidor WEB



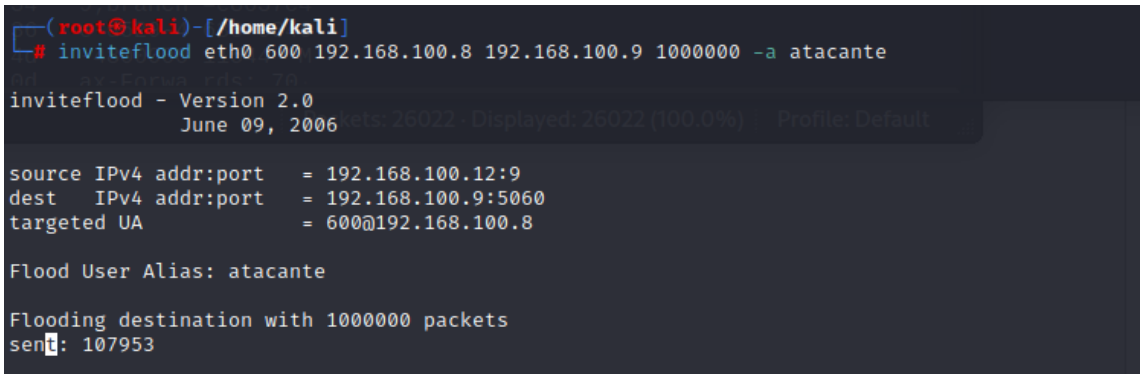
Fuente: Elaborado por el autor

- **Denegación de servicio**

Mediante este ataque de denegación de servicio son intentos de degradar los recursos del servidor para sus funcionamientos, esta técnica se basa en enviar paquetes especialmente construidos para explotar las vulnerabilidades tanto en la parte de software y hardware del sistema, saturan el flujo de datos en la red y sobrecarga los procesos del servidor.

En la figura 67, se muestra el procedimiento para enviar 1000000 de paquete al servidor para saturar el funcionamiento, así provocan una denegación de servicio.

Figura 67. Ataque de DDOS

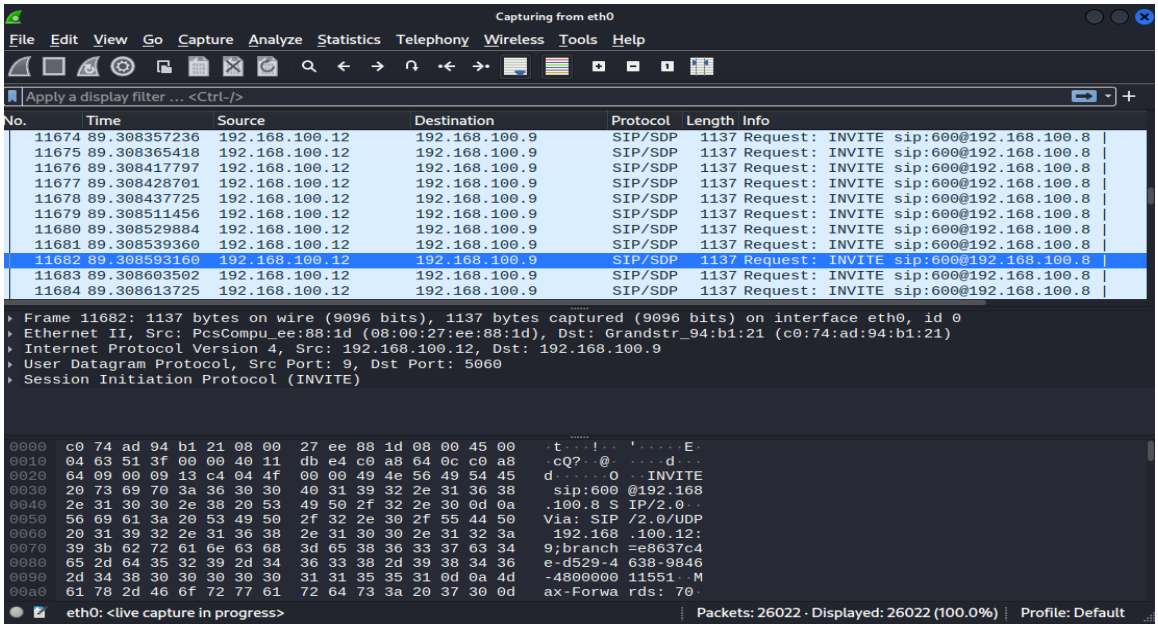


Fuente: Elaborado por el autor

Mediante Wireshack, se consigue ver el tráfico sobrecargan al servidor de Elastix, en la figura 68, se logra notar los paquetes enviado al servidor. Con la información recolectada mediante los análisis de resultados obtenidos sobre las

vulnerabilidades en el servidor Elastix 2.4, aplicado las fases de la metodología del OSSTMM, se resume que el servidor presenta riegos para la disponibilidad, confidencialidad e integridad de la comunicación e información.

Figura 68. Captura de tráfico del Ataque de DDOS



Fuente: Elaborado por el autor

En la siguiente tabla, se detallan las vulnerabilidades encontradas.

Tabla 6. Vulnerabilidades encontradas

N°	Vulnerabilidad Encontrado
1	Servicios no utilizados habilitados.
2	Permiso para llamada de INVITE
3	Contraseñas de Extensiones débiles
4	Contraseña de root débil
5	Firewall deshabilitado
6	SSH sin protección
7	Robo de contraseña
8	Nat del router principal no asegurado

Fuente: Elaborado por el autor

D. Fase de Intervención

En esta fase las pruebas, que se realizan son en base a los objetivos que habían planteado, esto es a menudo la fase final de una prueba de seguridad para de esta manera asegurar que las interrupciones no afecten a las respuestas de las pruebas menos invasivas, porque la información de estas pruebas no consigue ser conocidas hasta que otras fases se lleven a cabo, las pruebas de seguridad que no se incluyen en esta fase, todavía consigue ejecutar un último examen de perspectiva final de los objetivos (Ortega, Pupiales, & Suárez, 2017).

Para las implementaciones de seguridades sobre la plataforma instalado de Elastix en la empresa Lácteo Gustalac La Polaca, en esta sección, se procede a realizar las soluciones, en la siguiente tabla, se detalla las vulnerabilidades. Además, se ha planteado elaborar una guía de seguridad, la cual está dada en una secuencia de pasos, que se tienen que seguir para garantizar que el ambiente sea seguro en la plataforma de VOIP Elastix.

Guía de seguridad de la plataforma de VOIP Elastix, caso práctico en la empresa LACTEO GUSTALAC LA POLOCA

Paso 1.- Encontrar las vulnerabilidades que tiene el servidor Elastix, para posteriormente dar una solución, esto se realizó en la anterior sección en la Fase de C. Interacción, donde se describe cada uno de los ataques efectuados, el método utilizado y los resultados.

Paso 2. Identificación de las vulnerabilidades encontradas, se hallaron 8 vulnerabilidades, como se observa la tabla 7, para cada una se procedió a dar una solución técnica.

Tabla 7. Solución vulnerabilidades encontradas

No	Vulnerabilidad Encontrado	Solución
1	Servicios no utilizados habilitados.	Deshabilitar los servicios no usados
2	Permiso para llamada de INVITE	Restringir llamadas de INVITE
3	Contraseñas de Extensiones débiles	Cambiar por contraseñas Fuertes
4	Contraseña de root débil	Cambiar por contraseñas Fuertes
5	Firewall deshabilitado	Habilitar Firewall y configurar las reglas
6	SSH sin protección	Configurar herramienta FAIL2BAN
7	Robo de contraseña	Configurar herramienta FAIL2BAN
8	NAT del router principal no asegurado	Implementar VPN entre las sucursales y móviles

Fuente: Elaborado por el autor

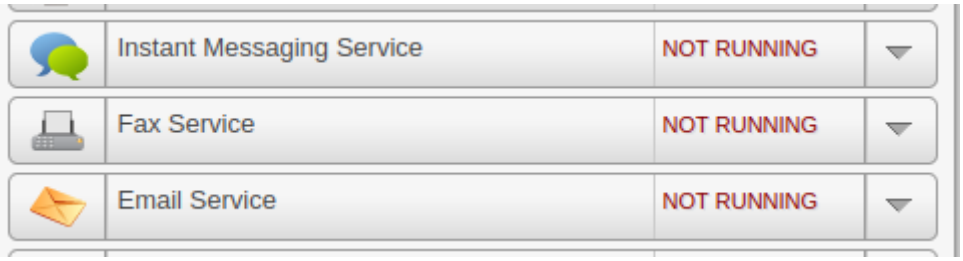
Paso 3. Se procede a ejecutar la solución, en cada vulnerabilidad encontrada en el servidor Elastix:

a) Deshabilitar los servicios no usados.

En la fase de indagación en la tabla 7, se observa que hay servicios con sus puertos habilitados y muchos de estos servicios no utiliza y como por ejemplo el servicio de Email, Fax y Mensajería.

En la figura 69, se observar que estos servicios están deshabilitados

Figura 69. Deshabilitar servicios



Fuente: Elaborado por el autor

b) Para proteger las llamadas anónimas

Para realizar la solución a este problema e impedir el cracker de contraseña a las extensiones, se necesita deshabilitar llamadas SIP anónimas y llamadas invitado en la configuración allowguest no, como se muestra en la figura 70 y 71.

Figura 70. Deshabilitar llamadas anónimas

Fuente: Elaborado por el autor

Figura 71. Deshabilitar llamadas Invitado - ALLOWGUEST =NO

```
;------------------------------------------------------------------------------;
; Do NOT edit this file as it is auto-generated by FreePBX. All modifications to ;
; this file must be done via the web gui. There are alternative files to make    ;
; custom modifications, details at: http://freepbx.org/configuration_files       ;
;------------------------------------------------------------------------------;
;

faxdetect=yes
vmexten=*97
context=from-sip-external
callerid=Unknown
notifyringing=yes
notifyhold=yes
tos_sip=cs3
tos_audio=ef
tos_video=af41
alwaysauthreject=yes
useragent=FPBX-2.8.1(1.8.20.0)
disallow=all
allow=ulaw
allow=alaw
allow=gsm
```

Fuente: Elaborado por el autor

Establecer a nivel de señalización para el cifrado que utiliza TLS y para la media se utilizará SRTP. En cada extensión hay que escoger las siguientes opciones para habilitar el cifrado: Transport: TLS Only Encryption: Yes (SRTP only). Se generan certificados para el servidor y para las extensiones.

c) Cambiar las contraseñas fuertes para las extensiones

Para la seguridad de las contraseñas de las extensiones es necesario definir política de contraseñas basado en reglas de intensidad, especificar los

siguientes estándares:

1. Longitud mínima y máxima
2. Restricciones de caracteres
3. Frecuencia de reutilización de contraseñas
4. Nombres de usuario o ID de usuario prohibidos
5. Especifique una duración mínima de la contraseña

Tabla 8. Contraseñas sugeridas para las extensiones

Extensiones Creado en Laboratorio		
Nro	**Ext.**	**Contraseñas fuertes**
1	101	CuM$a?I9XvVsvb7b
2	102	BxsuL?oFgB@6#Y9K
3	103	R3qCpN&um3xTbUKy
4	104	a!85y?mDpdckP2HG

Fuente: Elaborado por el autor

d) Cambiar la contraseña del ROOT

Para una implementación seguro de contraseña para el usuario root, hay que considerar las siguientes recomendaciones, mínimo 14 caracteres, que contenga mayúscula, números y caracteres especiales y necesita ser administrado por una persona responsable del área del Sistemas. Para realizar el cambio de la contraseña como nuestra en la figura 72 en el terminal del Servidor con el comando **passwd**, se permite cambiar la contraseña.

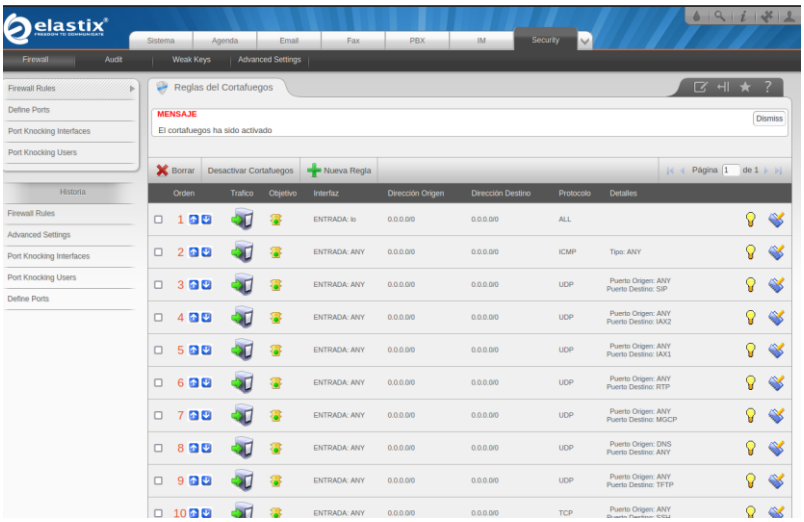
Figura 72. Cambio de contraseña al usuario root

Fuente: Elaborado por el autor

e) Activar Firewall en el Elastix

Para habilitar el Firewall, se consigue realizar desde el pc gestor por medio del web en la opción seguridad. En la figura 73, se observa que el firewall está habilitado.

Figura 73. Habilitar Firewall



Fuente: Elaborado por el autor

A continuación, se define en IPTABLES para las reglas del firewall:

Regla para aceptar todo el tráfico en entrada con destino a la interfaz local 192.168.100.0/24

iptables -A INPUT -s 192.168.100.0/24 -j ACCEPT

Acceso al protocolo SIP (tcp y upd)

iptables -A INPUT -p udp -m udp -i eth0 --dport 5060 -j ACCEPT

iptables -A INPUT -p udp -m tcp -i eth0 --dport 5060 -j ACCEPT

Acceso al protocolo IAX2

iptables -A INPUT -p udp -m udp -i eth0 --dport 4569 -j ACCEPT

Aceptar el tráfico RTP

iptables -A INPUT -p udp -m udp -i eth0 --dport 10000:20000 –j ACCEPT

Aceptar el tráfico WEB (HTTP Y HTTPS) para administración por interface web

```
iptables -A INPUT -p tcp -i eth0 --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -i eth0 --dport 443 -j ACCEPT
iptables -A INPUT -m conntrack --ctstate STABLISHED,RELATED -j ACCEPT
```

Finalmente Bloquear todos los demás puertos

```
iptables -A INPUT -p tcp -i eth0 --dport 39765 -j ACCEPT
```

Para finalizar deniegan el acceso a todo lo demás en la interfaz eth0:

```
iptables -A INPUT -p all -i eth0 -j DROP
```

Para guardar nuestras reglas y que estas sean aplicadas cada vez que reinicie el servidor, se usa siguiente el comando:

```
service iptables save
```

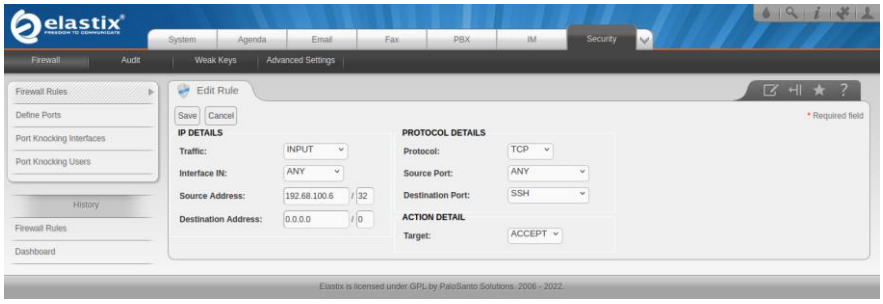
Cargan las nuevas configuraciones

```
service iptables restart
```

Con el firewall habilitado, se consigue configurar para el acceso de forma seguro permite que una sola dirección IP logra ingresar a través del http y ssh al servidor Elastix.

En la figura 74, se realiza la configuración permitir la dirección IP 192.168.100.6 accede por SSH al Servidor y de igual forma para el Servicio http y https con la dirección.

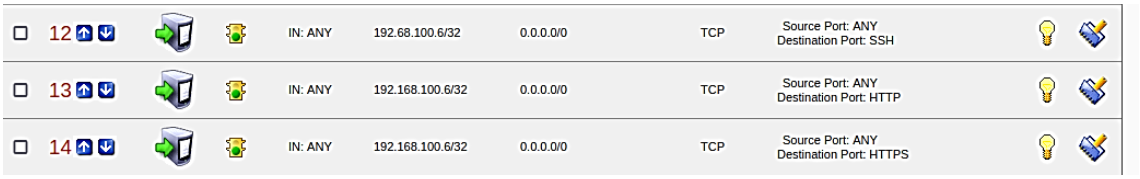
Figura 74. Firewall para acceso por IP



Fuente: Elaborado por el autor

Se realiza la configuración para el acceso al Servidor únicamente el IP 192.168.100.6 mediante los servicios de SSH, HTTP y HTTPS, como se muestra en la figura 75.

Figura 75. Firewall para acceso por IP

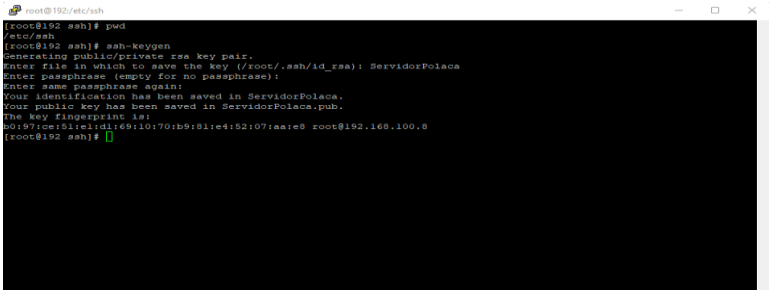


Fuente: Elaborado por el autor

f) Implementación conexión segura al SSH por medio llave privada

En la figura 76, con el comando ssh-keygen sirve para crear la llave privada

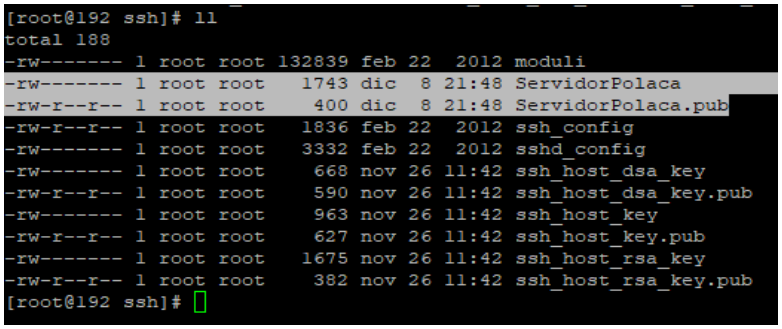
Figura 76. Creación de la llave privado



Fuente: Elaborado por el autor

En la figura 77, se evidencia que la llave ha sido creada con éxito.

Figura 77. La llave privada generadas



Fuente: Elaborado por el autor

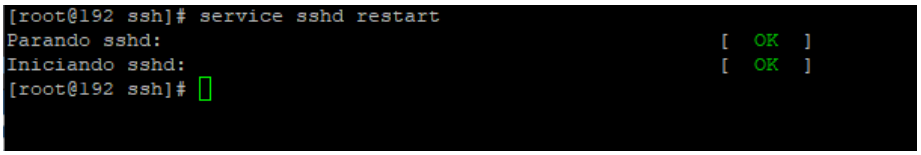
En la figura 78, en el archivo de configuración de ssh.conf, se parametriza la autenticación por llave privada.

Figura 78. Configuración en archivo ssh.conf

Fuente: Elaborado por el autor

En la figura 79, se reinicia el servicio de sshd para cargar la configuración implementado.

Figura 79. Reinicia el servicio de SSH



Fuente: Elaborado por el autor

En la figura 80, se logra observar, cómo se procede a deshabilitar el acceso al usuario root, con esto logra restringir el acceso.

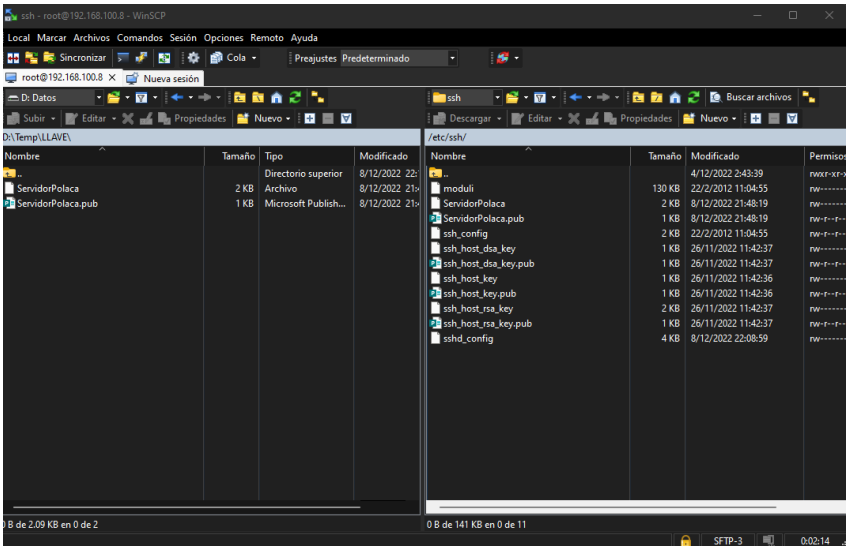
Figura 80. Deshabilitar el acceso al root

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6

#RSAAuthentication yes

PubkeyAuthentication yes
AuthorizedKeysFile      .ssh/authorized_keys

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
```

Fuente: Elaborado por el autor

En la figura 81, con el programa WINSCP, se copia los archivos que contiene la llave privada al host

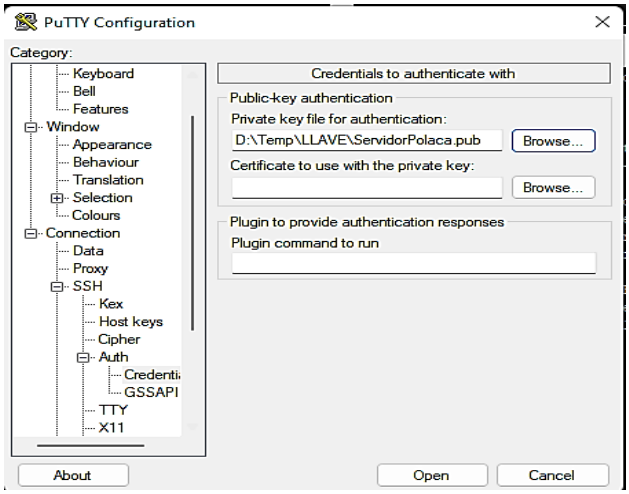
Figura 81. Copiar la llave privada a los PC



Fuente: Elaborado por el autor

En la figura 82, se realiza las configuraciones en PuTTY, donde se ingresan las credenciales del servidor para la autentificación.

Figura 82. Configuración de PuTTY para la conexión de la segura



Fuente: Elaborado por el autor

En la figura 83, se realiza el cambio del puerto 22 por el puerto 39765 para la conexión por medio de SSH, esta configuración se lo realiza en el archivo de ssh.conf.

Figura 83. Cambio del puerto default 22 al puerto 39765

```
Port 39765
#Protocol 2,1
Protocol 2
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

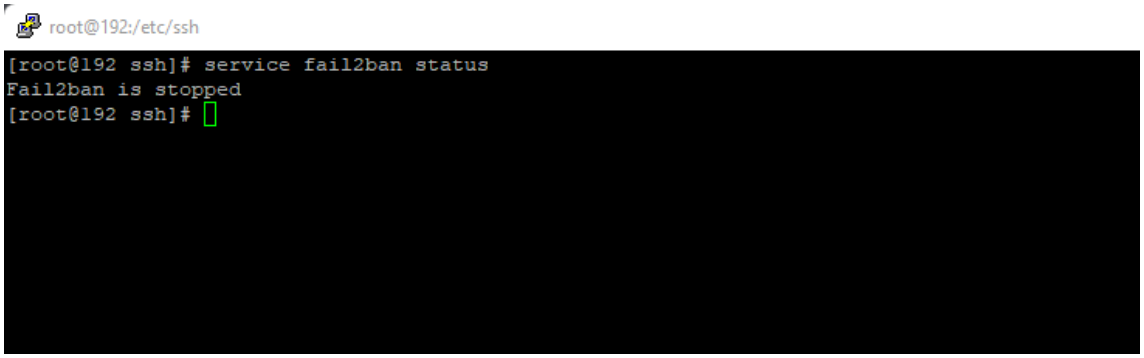
Fuente: Elaborado por el autor

g) Prevención de ataque contra fuerza bruta por medio Fail2ban

Fail2ban es una aplicación realizada en el lenguaje Python para la prevención de intrusiones a un sistema, bloqueado las conexiones remotas que intentan acceder por fuerza bruta. Esta herramienta ya está instalada en el servidor Elastix 2.4 pero, que se encuentra deshabilitado. Ver figura a continuación.

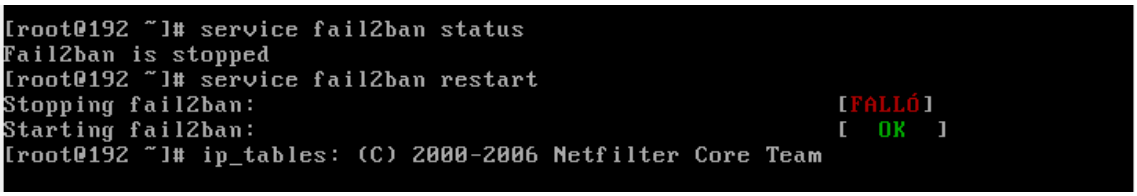
En la figura 84 y 85, se muestra cómo habilita el servicio y ejecutar la herramienta fail2ban.

Figura 84. Habilita fail2ban en el servidor



Fuente: Elaborado por el autor

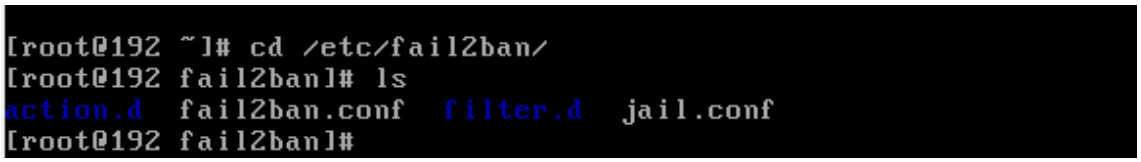
Figura 85. Se inicia el servicio de fail2ban



Fuente: Elaborado por el autor

En la figura 86, se hace la configuración para lo cual, se lo realiza con el siguiente comando vi /etc/fail2ban/jail.conf.

Figura 86. Configuración fail2ban



Fuente: Elaborado por el autor

En la figura 87, muestra la configuración que necesita realizar, va a permitir máximo 3 intento de conexión por medio de ssh y en un lapso de 36000 minutos, el host que trata de acceder más de 3 veces fallida, automáticamente logra bloquea el IP.

Figura 87. Configuración fail2ban

```
enabled  = true
filter   = sshd
action   = iptables[name=SSH, port=ssh, protocol=tcp]
           sendmail-whois[name=SSH, dest=root, sender=fail2ban@example.com]
logpath  = /var/log/secure
maxretry = 3
bantime = 36000_
```

Fuente: Elaborado por el autor

Figura 88. Se inicia el servicio de fail2ban

```
[root@192 fail2ban]# service fail2ban restart
Stopping fail2ban:                                         [  OK  ]
Starting fail2ban:                                         [  OK  ]
[root@192 fail2ban]#
```

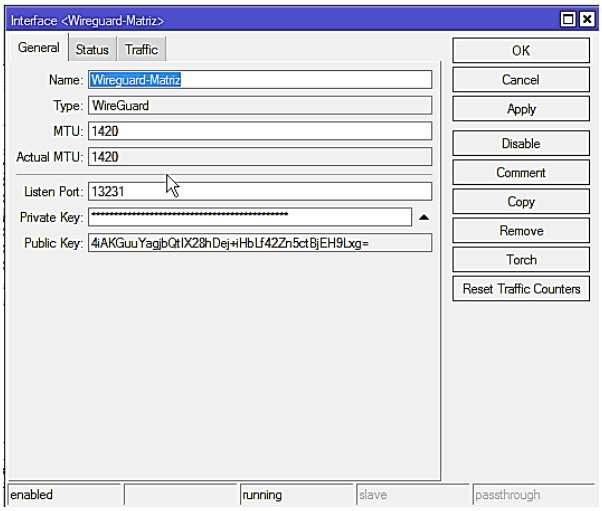
Fuente: Elaborado por el autor

h) Implementar conexión remotas y móviles mediante VPN

Establecer una red privada virtual (VPN) entre los sucursales, los dispositivos móviles con la matriz para tener una conexión segura y encriptado. Wireguard es un *software* libre que permite realizar esta implementación, en la empresa cuento con un Router Mikrotik que cuenta con esta herramienta integrada.

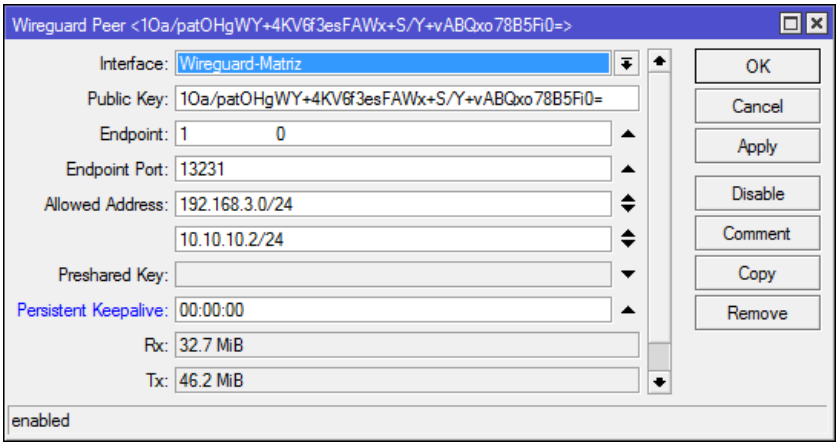
En las figuras 89, 90, 91 y 92, se muestra las configuraciones del VPN Wireguard en router Matriz y router sucursal.

Figura 89. Configuración de Wireguard en la Matriz



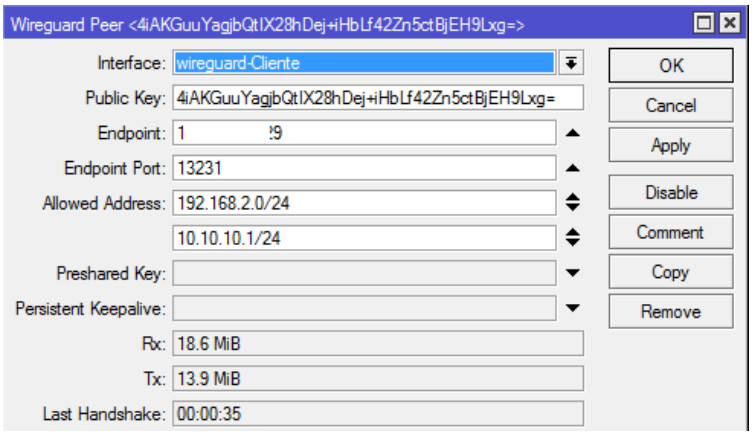
Fuente: Elaborado por el autor

Figura 90. Configuración de Wireguard en la Matriz en el peer



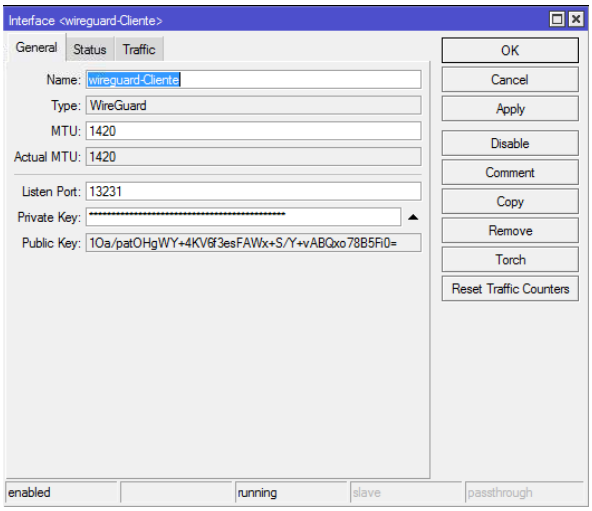
Fuente: Elaborado por el autor

Figura 91. Configuración de Wireguard en el cliente



Fuente: Elaborado por el autor

Figura 92. Configuración de Wireguard en el cliente peer



Fuente: Elaborado por el autor

i) Para corregir la vulnerabilidad CVE- 2015-1875

Para corregir esta vulnerabilidad desde el terminal, se necesita actualizar el repositorio Elastix a2billing con el siguiente comando:

update elastix-a2billing

Paso 4. Al seguir estos pasos, deberías poder determinar si cada una de las soluciones fue realizada correctamente. La tabla de control es una herramienta útil para registrar los avances, como se ve en la tabla 9.

Tabla 9. Control de seguridad

No	Vulnerabilidad Encontrado	Realizado/No realizado
1	Servicios no utilizados habilitados.	Realizado
2	Permiso para llamada de INVITE	Realizado
3	Contraseñas de Extensiones débiles	Realizado
4	Contraseña de root débil	Realizado
5	Firewall deshabilitado	Realizado
6	SSH sin protección	Realizado
7	Robo de contraseña	Realizado
8	NAT del router principal no asegurado	Realizado

Fuente: Elaborado por el autor

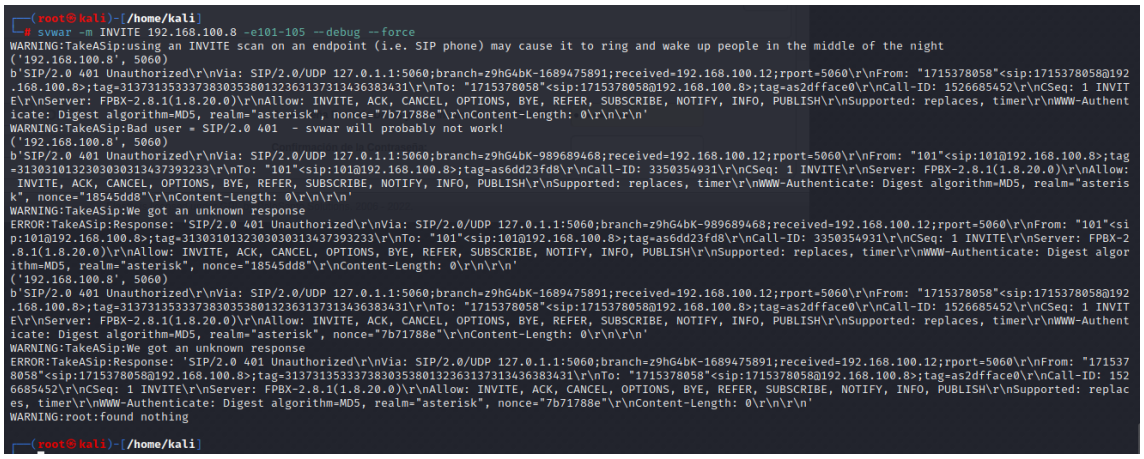
Como se consigue ver en la tabla 9, todas las vulnerabilidades, se solucionaron correctamente, con esto se implementa un servidor Elastix seguro, se ha seguido cada uno de los pasos que plantea esta guía de seguridad y conseguir ser de utilidad para configurar otro servidor con las características similares.

CAPÍTULO III. RESULTADOS DE LA INVESTIGACIÓN

3.1. Seguridad de llamadas de invitados y anónimas

En la figura 93, se realiza comprobación de los id de las extensiones del servidor 192.168.100.8, para encontrar las extensiones, que se encuentran activas en el PBX. Hace una comparativa con el trabajo realizado por el autor (Gutiérrez, 2017), se compara con el autor (Romero, 2019), ambos utilizan la herramienta svwar la cual ya no es posible ver las extensiones, que se encuentran activa en el servidor PBX.

Figura 93. Comprobación de descubrir los id de las extensiones

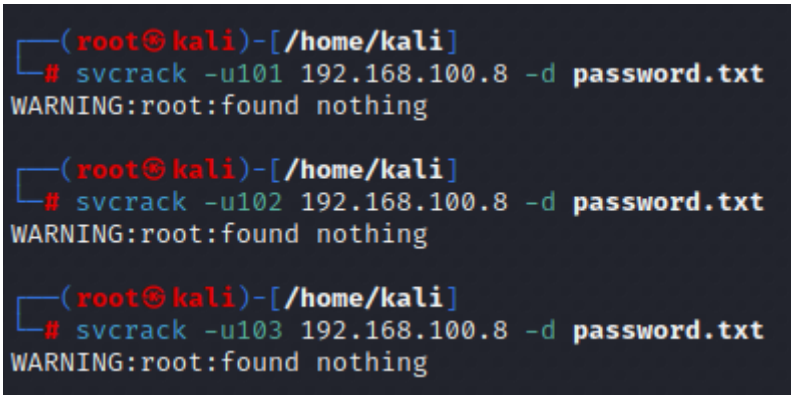


Fuente: Elaborado por el autor

3.2. Seguridad de contraseñas fuertes para cada extensión

En la figura 94, se realizan comprobaciones de las contraseñas, para de esta manera detectar que tan fuertes y seguras son, para lo cual, se ejecuta el comando svcrack -u101 192.168.100.8 -d password.txt, hace referencia al autor (Espinoza, 2021), donde se observó en el informe, que se utilizó la herramienta svcrack mediante cual se intentó robar las contraseñas, esto lo realizo por ataques por diccionario, de esta manera se demostró que tan fuerte era la encriptación que tenían las contraseñas del servido Elastix IP.

Figura 94. Comprobación del ataque para descubrir las contraseñas

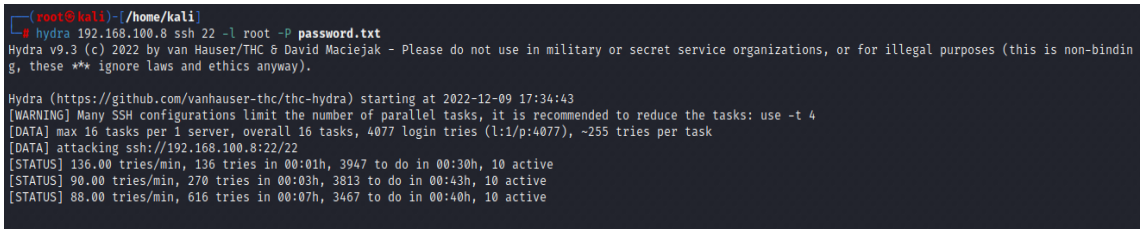


Fuente: Elaborado por el autor

Seguridad de contraseña fuertes al usuario root

En la figura 95, se procede a realizar un ataque de fuerza bruta a la dirección ip 192.168.100.8 por ssh al puerto 22, utiliza passwort.txt el cual sería el usuario root, lo que se quiere lograr es vulnerar la seguridad para de esta forma probar que tan seguro es la contraseña, que se tiene configurada en el servidor. El autor (Andrade, 2019) utilizo la herramienta hydra la cual permitió realizar ataques de fuerza bruta, donde se probó diferentes combinaciones, pero luego de un tiempo no se logró iniciar sesión, lo cual consigue determinar que era una contraseña fuerte que cumpla con las políticas de seguridad, pero esto no quiere decir que sea del todo segura, con un diccionario más completo y fuerte se logra cifrar la contraseña. Toma en cuenta también al autor (Romero, 2019), se observa que al utiliza y realizar el ataque, se logró iniciar sesión para lo cual se determinó que no tenía una contraseña que cumpla con las políticas de seguridad, para lo cual se procedió a implementarlas.

Figura 95. Comprobación del ataque para descubrir las contraseñas

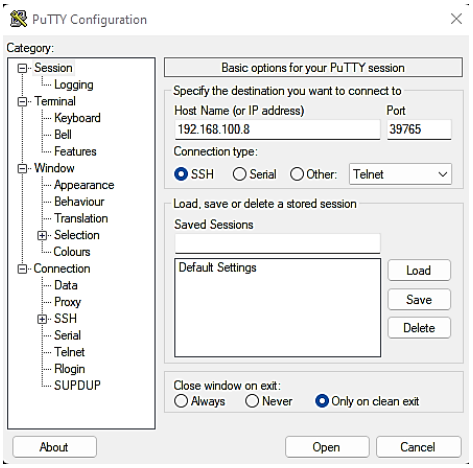


Fuente: Elaborado por el autor

3.3. Seguridad de Firewall

En la figura 96, se procede a configurar con la llave privado para acceso al servidor y donde se ingresa la dirección IP, el puerto de conexión, y se escoge el tipo de conexión. Se toma en cuenta el trabajo del autor (Andrade, 2019), se manejan un Firewall privado el cual está a cargo de una empresa que es quien gestiona la seguridad, para lo cual es más seguro, al depender de una tercera no sobrecarga todo el tema de seguridad en el personal del departamento de sistemas.

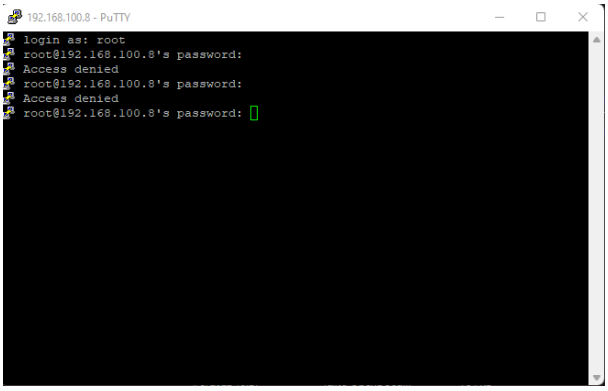
Figura 96. Prueba de acceso al root al puerto 39765



Fuente: Elaborado por el autor

Sobre la Figura 97, el acceso fue denegados con el usuario root, lo cual ayuda a proteger de terceras personas que intenten ingresar al servidor.

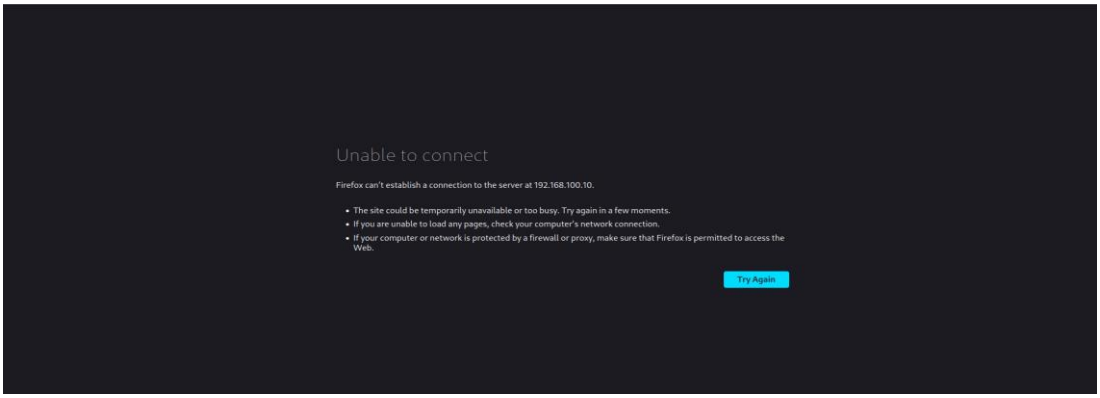
Figura 97. Prueba de acceso al root



Fuente: Elaborado por el autor

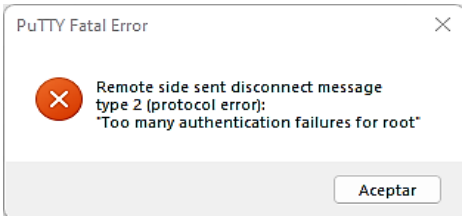
En la figura 98 y 99, se nuestra la restricción para acceder por web y ssh a una dirección ip diferente. Verifico el trabajo realizado por el autor (Romero, 2019), se realiza una comparación, donde se observa que realiza una configuración similar para denegar los accesos ssh, al momento de querer ingresar con una ip diferente salta un mensaje de error en el programa PuTTY, con esto protege los accesos por terceras personas al servidor.

Figura 98. Acceder por web con un ip diferente



Fuente: Elaborado por el autor

Figura 99. Acceder por ssh con un IP diferente



Fuente: Elaborado por el autor

CONCLUSIONES

- Una vez realizada la revisión del estado del arte, se encontraron varias vulnerabilidades, como Denegación de Servicios (DoS) y Fuzzing entra los más conocidos en ataques a servidores Elastix, los cuales ocasionan caídas en los servicios. Permite que intrusos sustraigan la información confidencial para la empresa, o hasta que logra ocasionar daños a gran parte de la infraestructura lo que representaría una pérdida económica para la empresa. Para mitigar estos riesgos, es importante que la empresa implemente medidas de seguridad adecuadas. Estas medidas logran tener una configuración adecuada de los firewalls y otros sistemas de seguridad. También es importante mantener actualizados los sistemas operativos y el software del servidor, y realizar pruebas regulares de penetración y evaluaciones de vulnerabilidades para detectar y corregir posibles problemas.

- En resumen, la metodología OSSTMM ha sido una herramienta eficaz para identificar las brechas de seguridad presentes en el departamento de sistemas y mejorar la seguridad de las comunicaciones en la plataforma del servidor Elastix. A través de la identificación y solución de las vulnerabilidades detectadas, se ha logrado aumentar la protección del servidor central de la empresa y reducir el riesgo de ataques por parte de terceros. La implementación de medidas de seguridad adecuadas ha demostrado ser fundamental para proteger la infraestructura de la red y garantizar la integridad y confidencialidad de la información. En general, se espera que los resultados de esta investigación sean de utilidad para otros profesionales y organizaciones que buscan mejorar la seguridad de sus sistemas de comunicaciones y reducir los riesgos asociados a los ataques cibernéticos.

- Una vez implementada las soluciones para solventar las vulnerabilidades, se logra concluir que, para garantizar la seguridad de los datos, es importante mantener un monitoreo constante del tráfico de red para detectar cualquier actividad inusual. Esto se logra mediante el uso de

herramientas de monitoreo de red, como IDS (Sistemas de Detección de Intrusos) y IPS (Sistemas de Prevención de Intrusos). Además, es importante tener contraseñas seguras para el ingreso al servidor Elastix y cualquier otro sistema o aplicación que utilice en la red. Las contraseñas tienen que ser lo suficientemente largas y complejas para evitar que sean adivinadas fácilmente. Otras medidas importantes que tomar para garantizar la seguridad de los datos incluyen la implementación de políticas de seguridad de la información, la capacitación del personal en cuanto a las buenas prácticas de seguridad y la realización regular de auditorías de seguridad para detectar y corregir posibles vulnerabilidades.

- La investigación llevada a cabo demostró que el servidor Elastix VOIP presentaba 8 vulnerabilidades que logra ser solucionadas mediante la implementación de medidas de seguridad adecuadas. Como resultado, se ha elaborado una guía detallada que describe los pasos necesarios para asegurar el servidor de comunicaciones y reducir el riesgo de ser vulnerado por terceras personas. Dado que los ataques cibernéticos son cada vez más frecuentes en todo el mundo, es importante destacar la importancia de contar con un servidor seguro y la necesidad de implementar medidas preventivas para proteger los sistemas de comunicaciones. En general, se espera que los hallazgos y recomendaciones de esta investigación contribuyan a la mejora de la seguridad en los sistemas de comunicaciones y sean útiles para profesionales y usuarios en el campo de las tecnologías de la información.

RECOMENDACIONES

- Es una buena práctica tener un respaldo de la información importante de la empresa en caso de un ataque por parte de intrusos o cualquier otra situación imprevista que logra causar la pérdida de datos. Si la empresa no tiene un plan de respaldo adecuado, corre el riesgo de perder datos críticos, consecuencias financieras y de reputación significativas. Para proteger la información de la empresa, es importante tener una estrategia de respaldo clara y bien definida, que incluya la frecuencia con la que se realizarán los respaldos y cómo se almacenarán y protegerán los datos de respaldo. También es importante hacer pruebas periódicas del proceso de respaldo para asegurarse de que los datos logre consigue recuperar de manera efectiva en caso de que ocurra una emergencia.

- Implementar un plan de seguridad de la información y continuidad de negocio, mitigar las amenazas, incluyen ataques de hackers, fallas en los servidores, desastres naturales y otros eventos imprevistos. Necesita incluir medidas para proteger la infraestructura de red, los sistemas y los datos, así como para garantizar la continuidad del negocio en caso de una interrupción.

- Registrar y controlar los activos de TI implica llevar un registro de los dispositivos y sistemas informáticos de la empresa, como servidores, computadoras, laptops, dispositivos móviles, entre otros, y monitorear su uso para garantizar su seguridad, el control de los activos de TI es esencial para la protección de la información crítica de la empresa y para garantizar una mejor administración y control sobre lo que tiene la empresa internamente. También de lo que se quiere proteger que, en este caso, lo más importante es la información crítica, para evitar que esta llegué a manos de terceras personas o incluso de la competencia.

BIBLIOGRAFÍA

Andrade, J. (2019). *Análisis de vulnerabilidades de seguridad en sistemas de VoIP con el uso de herramientas de hacking ético.* Universidad de Guayaquil, Guayaquil-Ecuador.

Arroba, M., & Salazar, M. (2011). *Propuesta de soluciones a las vulnerabilidades del protocolo de señalización SIP en voz sobre IP, caso práct.* Riobamba-Ecuador. Obtenido de http://dspace.espoch.edu.ec/handle/123456789/82

Carmona, D. (2015). *Implementación de una central IP –PBX basada en Asterisk para el sistema de telefonía de la Universidad Católica de Pereira.* Universidad Católica de Pereira, Pereira-Colombia. Obtenido de http://hdl.handle.net/10785/2882

Carrillo, L. (2017). *ESTUDIO DE MÉTODOS DE TRANSFERENCIA DE VOZ SOBRE IP.* Universidad Técnica de Ambato, Ambato-Ecuador.

Cruz, Y. (2016). *METODOLOGÍA OSSTMM PARA LA DETECCIÓN DE ERRORES DE SEGURIDAD Y VULNERABILIDAD EN SISTEMAS OPERATIVOS DE 64 BITS A NIVEL DE USUARIO FINAL.* Riobamba-Ecuador.

EOS. (2014). *Telefonia IP VoIP Elastix-Asterik*. Obtenido de https://www.eopen solutions.com/productos-y-servicios/voip-elastix-asterisk

Espinoza, P. (2021). *Estudio y diseño de un sistema de comunicaciones unificadas VoIP basado en Elastix con seguridad perimetral.* Universidad Católica Santiago de Guayaquil, Guayaquil-Ecuador.

Gutiérrez, R. (2017). *Seguridad en VoIP Ataques, Amenazas y Riesgo.* Valencia-España.

Herzog, P. (2010). *Manual de la Metodología Abierta de Testeo de Seguridad.* Barcelona-España.

Incide. (s.f.). *https://www.incibe-cert.es/en/early-warning/vulnerabilities/cve-2015-1875.*

Jaramillo, Y. (2015). *Implementación de un esquema de seguridad para configurar centrales VoIP.* Escuela Superior Politécnica del Litoral, Guayaquil-Ecuador.

Lorenzo, A. (15 de Noviembre de 2020). *redeszone*. Obtenido de https://www.redeszone.net/noticias/seguridad/ciberdelincuentes-vulnerabilidades-voip-empresas/

Maldonado, P. (2016). *Esquema de seguridad para una central VoIP, en software libre en su implementación Elastix".* PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR, Quito-Ecuador.

Matango, F. (2016). *Fundamentos en una Arquitectura VoIP.* Madrid-España. Obtenido de http://www.servervoip.com/blog/elementos-fundamentales-en-una-arquitectura-voip/

Navia, M., & Zambrano, W. (Diciembre de 2021). *Instrumento para la auditoría técnica de seguridad informática en pequeños proveedores de Internet. Revistas de Tecnologías de la Informática y las Telecomunicaciones*, 119-128. doi: https://doi.org/10.33936/isrtic.v5i2.3952

Ortega, C., Pupiales, C., & Suárez, L. (12 de Julio de 2017). *Auditoría de seguridad informática siguiendo la metodología OSSTMMv3:. MASKANA,* 1-13.

Pinzón, L., Talero, M., & Jhon, B. (2014). *Pruebas de intrusión y metodologías abiertas. Revista Ciencia, Innovación Y Tecnología.* Boyacá-Colombia. Obtenido de https://revista.jdc.edu.co/index.php/rciyt/article/view/120

Polaca. (2021). *Avena Polaca*. Obtenido de https://avenapolaca.com.ec/nosotros

Ponce, P. (2015). *DOCPLAYER.* Obtenido de https://docplayer.es/2001087-Capitulo-i-marco-teorico-conceptual.html

Robalino, C. (2012). *REALIZACIÓN DE UNA PROPUESTA DE MEJORA DEL SERVICIO DE VoIP EN LA FACULTAD DE LA INGENÍERIA ESCUELA DE SISTEMAS DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR.* Pontificia Universidad Católica del Ecuador, Quito-Ecuador.

Romero, G. (2019). *Análisis de vulnerabilidades de seguridad en sistemas de VoIP, con el uso de herramientas de hacking ético.* Guayaquil-Ecuador.

Salcedo, O., López, D., & Hernández, C. (2012). *Estudio comparativo de la utilización de ancho de banda con los protocolos SIP e IAX.* Bogotá-Colombia. Obtenido de http://www.scielo.org.co/scielo .php?script=sci_ arttext&pid=S0123-921X2012000400013

Sotomayor, J., Romero, C., & Saenz, F. (2014). *Análisis de vulnerabilidades de seguridad en centrales VoIP Elastix a través del hacking ético.* Quito-Ecuador. Obtenido de http://repositorio.espe.edu .ec/xmlui/handle/2 1000/9557

Tanenbaum, A. (2013). *Computer Networks.* Amsterdam-Netherlands.

ANEXOS

Anexo 1. Cuestionario

Fecha: 27/10/2022

Cargo: jefe de TIC

Lugar: Oficina de la empresa

1. ¿Se tiene un inventario de todos los activos TI de la empresa?

2. ¿Se tiene dispositivos dedicados exclusivamente al monitoreo del tráfico de actividades de la red?

3. ¿Se tiene un Firewall para la protección de entrada y salida de datos?

4. ¿Se tiene un plan de seguridad en caso de haber un ataque masivo a los ordenadores?

5. ¿Se realiza copias de seguridad de la información de la empresa en un tiempo aproximado entre 3, 6 o 12 meses?

6. ¿Se tiene contraseñas para cada equipo que funciona dentro de la empresa?

7. ¿Se tiene registro de un posible ataque malicioso, que haya tenido la empresa a sus servidores?

Anexo2. Entrevista dirigida al jefe del Departamento de Sistemas

Nombre de entrevistado:

Fecha: 27/10/2022

Cargo: jefe de TIC

Lugar: Oficina de la empresa

¿Se tiene un inventario de todos los activos TI de la empresa?

Si, cuenta con un inventario.

¿Se tiene dispositivos dedicados exclusivamente al monitoreo del tráfico de actividades de la red?

Sí, hay un monitoreo de los servidores que están en producción como los físicos y lo que están alojados en la nube.

¿Se tiene un Firewall para la protección de entrada y salida de datos?

Si, cuenta con uno, pero es gestionado por una empresa privada.

¿Se tiene un plan de seguridad en caso de haber un ataque masivo a los ordenadores?

No, no se ha implementado ninguno.

¿Se realiza copias de seguridad de la información de la empresa en un tiempo aproximado entre 3, 6 o 12 meses?

Si, se realizan los respectivos backups de los Servidores

¿Se tiene contraseñas para cada equipo que funciona dentro de la empresa?

Si, cada uno cuenta con su usuario y contraseña.

¿Se tiene registro de un posible ataque malicioso, que haya tenido la empresa a sus servidores?

Si, hace tiempo uno de los servidores sufrió un ataque informático, como consecuencia toda la información fue encriptada por un atacante, quien utilizan técnicas de ataques sofisticadas como Ransomware, encontró una vulnerabilidad en el protocolo RPC (Remote Procedure Call) a través del puerto 3389.

Análisis de entrevista aplicada

Se consigue ver que la empresa lleva un control del inventario de los activos TI, lo cual es bueno para la empresa.