Hardenización Integral del Servidor DELL PowerEdge R7515 en Software y Hardware para reforzar la seguridad de la información en la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre (DTIC) en Quito

Cando Santo, Alexis Paul y Moyano Álvarez, Darwin Darío

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Trabajo de Unidad de Integración Curricular, previo a la obtención del título de Tecnólogo Superior en Redes y Telecomunicaciones

Ing. Caicedo Altamirano, Fernando Sebastián

27 de febrero de 2024

Latacunga

Scan details

Scan time	Total Pages	Total Words
March 2th, 2024 at 1:46 UTC	53	13095

Plagiarism Detection

9.3%

Types of plagiarism		Words
Identical	4.5%	591
Minor Changes	1.5%	195
Paraphrased	3.3%	437
Omitted Words	0%	0

AI Content Detection

N/A

Text coverage
AI text
Human text

Plagiarism Results: (15)

Microsoft Word - TESIS_AnaCaiza.docx — 5.2%

https://repositorio.unach.edu.ec/bitstream/123456789/3340/1/tesis_anacaiza.pdf

acaiza001

FACULTAD DE ARQUITECTURA E INGENIERÍAS Trabajo de Investigación de fin de carrera titulado: DISEÑO DE UN PROCESO DE HARDENING DE SERVIDO...

Pinduisaca G, Karina P.(2022) MANUAL DE IMPLEMENTACIÓN DE UN PROC... — 4.7%

http://dspace.unach.edu.ec/bitstream/51000/10128/1/pinduisaca%20g%20karina%20p.(2022)%20manual%2...

Microsoft Office User

UNIVERSIDAD NACIONAL DE CHIMBORAZO FACULTAD DE INGENIERÍA CARRERA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN Proyecto de investigación previ...

Administración de servicios, hacking etico y soporte en Linux: Hardening... — 0.4%

https://kimberling146.blogspot.com/2018/06/hardening-actividades-deberes.html

Administración de servicios, hacking etic...

Servidor - Glosario de términos para el periodismo en la era digital — 0.3%

http://ufv-digital.wikidot.com/servidor

Wikidot.com .wikidot.com Compartir en ...

Ing. Caicedo Altamirano, Fernando Sebastián

Director

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnologia Superior en Redes y Telecomunicaciones

Certificación

Certifico que el Trabajo de Unidad de Integración Curricular "**Hardenización Integral del Servidor DELL PowerEdge R7515 en Software y Hardware para reforzar la seguridad de la información en la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre (DTIC) en Quito.**" fue realizado por los señores **Cando Santo, Alexis Paul y Moyano Álvarez, Darwin Darío;** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizada en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Latacunga, 05 de marzo del 2024

Ing. Caicedo Altamirano, Fernando Sebastián

C.C.: 1803935020

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Responsabilidad de Autoría

Nosotros, **Cando Santo, Alexis Paul, y Moyano Álvarez, Darwin Dario,** con cédulas de ciudadanía n° **0550123087** y n° **1804203303**, declaramos que el contenido, ideas y criterios del Trabajo de Unidad de Integración Curricular: **"Hardenización Integral del Servidor DELL PowerEdge R7515 en Software y Hardware para reforzar la seguridad de la información en la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre (DTIC) en Quito."**, es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y refiriendo las citas bibliográficas.

Latacunga, 05 de marzo del 2024

Cando Santo, Alexis Paul

C.C.: 0550123087

Moyano Álvarez, Darwin Dario

C.C.: 1804203303

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Autorización de Publicación

Nosotros, **Cando Santo, Alexis Paul, y Moyano Álvarez, Darwin Dario,** con cédulas de ciudadanía n° **0550123087** y n° **1804203303**, autorizamos a la Universidad de las Fuerzas Armadas ESPE, publicar el Trabajo de Unidad de Integración Curricular **"Hardenización Integral del Servidor DELL PowerEdge R7515 en Software y Hardware para reforzar la seguridad de la información en la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre (DTIC) en Quito."**, en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi/nuestra responsabilidad.

Latacunga, 05 de marzo del 2024

Cando Santo, Alexis Paul

C.C.: 0550123087

Moyano Álvarez, Darwin Dario

C.C.: 1804203303

Dedicatoria

Con profunda gratitud, dedico primeramente el presente trabajo de investigación a Dios todopoderoso, fuente de mi fortaleza y guía en cada paso de mi camino.

Expreso mi más sincero agradecimiento a mi amada familia y seres queridos cercanos, cuyo apoyo incondicional y generosa colaboración han sido fundamentales para llevar a cabo esta investigación. A través de su constante aliento y sacrificio, han sido mi inspiración para perseverar y alcanzar este logro.

A cada uno de ustedes, mi más profundo reconocimiento y afecto.

Cando Santo, Alexis Paul

Con profundo agradecimiento, dedico este trabajo de investigación a mis padres, cuyo amor, sacrificio y apoyo incondicional han sido el faro que ha guiado cada paso de mi camino académico. A mi familia, por su comprensión, ánimo y aliento constante en los momentos más desafiantes. A mis amigos, por su amistad, compañerismo y motivación a lo largo de esta travesía. A mis profesores y mentores, por su sabiduría, guía y enseñanzas que han enriquecido mi formación académica. A todos aquellos que de una u otra forma han contribuido en este proceso, mi más sincero agradecimiento. Este logro es también de ustedes.

Moyano Álvarez, Darwin Darío

Agradecimiento

En primer lugar, deseo expresar mi profunda gratitud a Dios por brindarme la oportunidad de continuar con mis estudios y por otorgarme la fuerza necesaria para concluir este proyecto con éxito. También quiero agradecer a todas las personas que me han apoyado a lo largo de este camino, con un reconocimiento especial a mi familia, cuyo amor y apoyo han sido mi principal motor para avanzar en esta investigación.

Asimismo, quiero extender mi sincero agradecimiento a mi tutor de tesis, quien ha sido una guía invaluable en este proceso. Sus ideas, correcciones y orientación han sido fundamentales para desarrollar un trabajo viable y cumplir con los objetivos establecidos. Su dedicación y compromiso han sido una fuente constante de inspiración y aprendizaje.

Cando Santo, Alexis Paul

Me gustaría expresar mi profundo agradecimiento a todas las personas que contribuyeron de alguna manera a la realización de este proyecto.

En primer lugar, quisiera agradecer a mi familia por su constante apoyo, comprensión y amor incondicional durante todo este proceso.

También me gustaría agradecer a mis amigos y compañeros de estudios por su amistad, cooperación y aliento en cada etapa de este proyecto. Sus palabras de aliento y apoyo han hecho más llevadero este viaje académico.

Me gustaría expresar mi agradecimiento a mis profesores y tutores, cuya guía, conocimiento y sabios consejos han sido fundamentales para el desarrollo de este trabajo. Su dedicación y compromiso con mi educación académica fueron invaluables.

Moyano Álvarez, Darwin Darío

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Resumen

El presente proyecto de titulación se enfoca en la "Hardenización Integral de un Servidor en Software y Hardware", con el objetivo principal de fortalecer la seguridad y la estabilidad de un servidor mediante medidas específicas tanto a nivel de software como de hardware. En primer lugar, se realiza un análisis exhaustivo de las posibles vulnerabilidades del servidor, tanto a nivel de software como de hardware. Este análisis incluye una evaluación detallada de los sistemas operativos, aplicaciones y componentes de hardware utilizados en el servidor. A continuación, se diseñará e implementará un plan de Hardening integral que aborda las vulnerabilidades identificadas. Esto incluye configurar y optimizar los ajustes de seguridad en el sistema operativo, así como implementar medidas de seguridad físicas en el hardware del servidor. Finalmente, se llevarán a cabo pruebas exhaustivas para validar la eficacia de las medidas de endurecimiento implementadas. Esto incluye pruebas de penetración, pruebas de vulnerabilidad y evaluaciones de rendimiento para garantizar que el servidor pueda resistir ataques y mantener altos niveles de disponibilidad y confiabilidad. El proyecto proporcionara una solución integral y robusta para mejorar la seguridad y estabilidad de un servidor, ayudando a proteger los datos y recursos críticos de la DTIC de posibles amenazas y vulnerabilidades.

Palabras clave: servidor DELL PowerEdge, servidores hardening, ciberseguridad.

Abstract

This graduation project focuses on the "Comprehensive Hardening of a Server in Software and Hardware", aiming to enhance the security and stability of a server through specific measures at both software and hardware levels. Initially, a thorough analysis of potential vulnerabilities of the server is conducted, encompassing evaluations of operating systems, applications, and hardware components. Subsequently, a comprehensive Hardening plan addressing identified vulnerabilities will be designed and implemented. This includes configuring and optimizing security settings in the operating system, along with implementing physical security measures in the server's hardware. Finally, extensive testing will be carried out to validate the effectiveness of the implemented hardening measures. This involves penetration tests, vulnerability assessments, and performance evaluations to ensure the server can withstand attacks and maintain high levels of availability and reliability. The project will provide an integrated and robust solution to enhance the security and stability of a server, thereby safeguarding critical data and resources from potential threats and vulnerabilities.

Keywords: DELL PowerEdge server, hardening servers, cybersecurity.

Capítulo I

Introducción

Antecedentes

En el escenario actual, la ciberseguridad representa un desafío global que impacta a instituciones gubernamentales, corporativas y militares en todo el mundo. La interconexión global y la dependencia de sistemas informáticos avanzados exponen a las organizaciones a amenazas cibernéticas sofisticadas, aumentando la frecuencia y magnitud de ciberataques, poniendo en riesgo información sensible y sistemas críticos de infraestructura (Ciberseguridad, 2024)

En América Latina, la región enfrenta desafíos particulares en ciberseguridad, con un aumento de incidentes que destaca la necesidad de fortalecer las defensas digitales. La falta de conciencia, recursos limitados y la rápida adopción tecnológica sin debida seguridad contribuyen a la vulnerabilidad de instituciones (Oas.org, 2024).

Ecuador, inmerso en la creciente amenaza cibernética global, experimenta riesgos de seguridad informática debido a la rápida transformación digital. La preservación de la integridad, confidencialidad y disponibilidad de información se erige como prioridad nacional (Org.ec, 2024).

En el ámbito de la Fuerza Terrestre Ecuatoriana, la DTIC juega un rol crucial en la gestión de información y operaciones militares. La utilización del servidor DELL PowerEdge R7515, conectado mediante IP pública, añade complejidad y exposición a amenazas cibernéticas. La DTIC al manejar información confidencial necesita incrementar la seguridad de sus servidores ya que la seguridad informática implica la protección de información sensible.

De acuerdo a un estudio realizado en una empresa de telecomunicaciones revela la identificación de 52 vulnerabilidades en los servidores evaluados. Es destacable que el 50% de

estas vulnerabilidades estaba asociado al software, mientras que el 30% afectaba al hardware. Con la implementación de hardenización de servidores pertenecientes a la empresa se consiguió una reducción significativa del 50% en el número de vulnerabilidades, demostrando su eficacia en este contexto. (Edu.ec., 2024).

En un estudio llevado a cabo en una institución financiera, se encontraron 65 vulnerabilidades en sus servidores. Se determinó que el 60% de estas vulnerabilidades estaban relacionadas con el software, mientras que el 40% afectaba al hardware. Estos hallazgos resaltan la importancia de la hardenización de servidores para proteger información confidencial no solo en instituciones financieras sino que también en otras entidades del estado que manejan información sensible del personal (Caiza, 2019).

Planteamiento del problema

Desde su creación en el año 2001, la Dirección de Tecnologías de la Información y Comunicaciones (DTIC) ha sido un pilar fundamental en la modernización de las operaciones militares de la Fuerza Terrestre Ecuatoriana. Su función principal se centra en optimizar la utilización de tecnologías de la información y comunicaciones mediante el desarrollo, administración y mantenimiento de servicios y sistemas a fin de entregar información oportuna y segura para la toma de decisiones (DTIC, 2024)

A lo largo de los años, la DTIC ha sido la responsable de la elaboración de programas y proyectos para mejorar los sistemas de Tecnologías de la Información y Comunicaciones para mitigar las amenazas cibernéticas. La interconexión global y la dependencia de sistemas informáticos avanzados han expuesto a la institución a riesgos significativos, particularmente en la seguridad de los servidores (DTIC, 2024).

En el contexto latinoamericano, la región se enfrenta a desafíos específicos en términos de ciberseguridad. Las organizaciones en América Latina han experimentado un aumento en

los incidentes de ciberseguridad, destacando la necesidad de fortalecer las defensas digitales. Ecuador no es ajeno a esta realidad, ya que la rápida transformación digital en el país ha expuesto a las organizaciones, incluida la Fuerza Terrestre, a riesgos significativos en seguridad informática (Ciberseguridad, 2024).

La preservación de la integridad, confidencialidad y disponibilidad de la información se ha convertido en una prioridad nacional para Ecuador. La creciente amenaza cibernética no solo representa un riesgo para las instituciones militares, sino también para la seguridad nacional en su conjunto (Martínez Ramírez, 2020).

En el ámbito específico de la Fuerza Terrestre Ecuatoriana, la DTIC es la encargada de diriguir la operación, mantenimiento y actualización de servidores, redes, interconexiones, almacenamiento, respaldo/recuperación y centralización/virtualización para proporcionar servicios óptimos de Tecnologías de la Información y Comunicaciones, por lo que con la utilización del servidor DELL PowerEdge R7515 hardenizado, conectado a través de una IP pública, agrega una capa adicional de complejidad y exposición a potenciales amenazas cibernéticas (DTIC, 2024).

La vulnerabilidad de los servidores en la DTIC es una problemática compleja y dinámica. Las consecuencias de estas vulnerabilidades, como el robo de información sensible, la interrupción de servicios críticos y los daños a la reputación institucional, ponen en riesgo la integridad de los datos almacenados y la continuidad de las operaciones de la Fuerza Terrestre.

Para la solucionar este problema se propone mediante el desarrollo de un plan de hardening integral para el servidor DELL PowerEdge R7515. Esta solución busca no solo preservar la confidencialidad y la integridad de la información almacenada sino también fortalecer las capacidades de la DTIC en el manejo seguro de la información. La

implementación de medidas proactivas no solo protegerá los activos digitales de la institución, sino que también contribuirá al fortalecimiento general de las capacidades tecnológicas de la Fuerza Terrestre.

Justificación

En la actualidad, la Hardenización Integral de servidores es importante a nivel global debido a la creciente amenaza de ataques cibernéticos en todos los sectores de la sociedad. En un mundo interconectado, los servidores desempeñan un papel central al gestionar datos críticos para entidades gubernamentales, militares y empresariales. A nivel nacional, este proceso no solo aborda desafíos específicos de seguridad, sino que también se alinea con los objetivos de modernización y digitalización, contribuyendo significativamente a la protección de datos (Martínez Ramírez, 2020).

En respuesta a la creciente amenaza de ataques cibernéticos, la Dirección de Tecnologías de la Información y Comunicaciones (DTIC) requiere de un sistema que garantice la seguridad de la información que maneja, debido a que en el mismo existen los datos críticos tanto del personal de la Fuerza Terrestre como de las operaciones militares que diariamente se realizan a nivel nacional por parte del personal militar, para lo cual existe un servidor en el cual se aloja en la base de datos de la DTIC, por lo que se busca fortalecer la seguridad de la información de manera que se pueda garantizar la integridad, confidencialidad y disponibilidad de la información crítica que administra dicho servidor.

Con la Hardenización del servidor no solo impactará directamente en la seguridad de la información de la DTIC, sino que también establecerá un estándar elevado para las prácticas de seguridad en el manejo de servidores en otras áreas de la Fuerza Terrestre. La creación de un entorno informático más seguro y resistente fortalecerá la postura de esta unidad militar frente a los desafíos contemporáneos en ciberseguridad.

Objetivos

Objetivo General

Desarrollar e implementar políticas integrales de seguridad para la hardenización de servidores, abarcando tanto aspectos de software como de hardware, con el propósito de garantizar la protección de la información en la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre (DTIC).

Objetivos Específicos

- Realizar un análisis de los diferentes mecanismos, herramientas y protocolos para brindar seguridad a los servidores de datos.
- Aplicar los mecanismos de seguridad para la hardenización, identificados a través de la investigación bibliográfica, con el propósito de garantizar la protección de la información almacenada en el servidor.
- Realizar pruebas de funcionamiento y elaborar un manual de usuario de los mecanismos de seguridad implementados en el proceso de hardenización, con el propósito de asegurar su correcto funcionamiento y facilitar su utilización por parte del personal.

Alcance

La Dirección de Tecnologías de la Información y Comunicaciones (DTIC), al manejar información crítica del todo el personal del Ejército, requiere de un fortalecimiento de sus sistemas informáticos, es aquí donde cobra gran importancia la hardenización del servidor para lo cual se configurarán los puertos para utilizar protocolos seguros como HTTPS en lugar de HTTP, para proteger la transmisión de datos. Además, se realizará la actualización completa del sistema operativo.

Se realizarán pruebas de funcionamiento en el servidor para comprobar que no existan puertos abiertos que puedan ser vulnerados para atacar nuestra información, conjuntamente se aplicarán mecanismos de detección de vulnerabilidades para posteriormente aplicar herramientas que permitan fortalecer el servidor en software y hardware. Se entregará un manual de usuario de manera que los encargados de los sistemas de la DTIC puedan realizar el respectivo mantenimiento, actualización y fortalecimiento de los sistemas informáticos que alberga el servidor. Se crearán y almacenarán copias de seguridad en ubicaciones seguras y fuera del servidor principal

.

Capítulo II

Marco teórico

Generalidades

En este capítulo se detallan todos los contenidos teóricos relacionados a ciberseguridad, hardenización y a su vez los requerimientos técnicos esenciales a tener en cuenta durante la hardenización de un servidor, conceptos que ayudan a una comprensión general del tema de investigación.

Infraestructura Tecnológica

Es un conjunto de hardware y software que ayuda a las organizaciones a prestar servicios, es donde están instaladas las aplicaciones requeridas por la organización, su administración y gestión interna.

Hardware es cualquier dispositivo físico que soporta la comunicación y el procesamiento y almacenamiento de información como: enrutadores, conmutadores, firewalls, repetidores, cámaras, estaciones de trabajo, impresoras, teléfonos, servidores. Los paquetes de software son todos los programas y sistemas diseñados para ayudar o facilitar servicios, comunicaciones, operación, procesamiento y almacenamiento de información, Por ejemplo: sistema operativo, motor de base de datos, aplicación, software de red, plataforma de trámites, administración y operación de oficina (Caiza, 2019).

Servidor

Un servidor es un ordenador o una partición de este muy potente que se encarga de almacenar archivos y distribuirlos en internet para que sean accesibles a los usuarios, en el mundo de la informática se le llama servidor al programa que ofrece una serie de servicios a esto se suele acceder por medio de programas especiales que se denomina clientes el caso es que por extensión se suele denominar servidor al ordenador en el que funciona estos

programas técnicamente un servidor es un equipo que tiene instalado un software que sirve recursos útiles o información que necesitamos (Cruz, 2017).

Tipos de servidor

Los servidores pueden clasificarse de diferentes maneras tomando en cuenta sus características como por ejemplo por su capacidad de procesamiento como expone en su texto Sandra Jara (Caiza, 2019)

- Supercomputadoras
- Macro computadoras
- Minicomputadoras
- Microcomputadoras

Los servidores dependiendo del servicio que brinden, de su función a desempeñar en la red puede clasificarse en:

- Servidor Web
- Servidor Proxy
- Servidor de Acceso Remoto
- Servidor de Correo
- Servidores de base de Datos
- Servidores de Archivos

A continuación, se resume cada uno de los tipos de servidor de acuerdo a su funcionalidad.

- **Servidor Web:** Es un servidor que recibe datos de múltiples hosts locales o desde Internet para guardar texto visible, imágenes, vídeos y otros archivos de red usando el navegador, el servidor permanece conectado para ejecutar el servicio www "World World Wide Web" (Neira, 2017)

- **Servidor Proxy**: Es una computadora diseñada para realizar tareas de filtrado de paquetes es el intermediario entre las solicitudes del cliente y el servidor web, es decir, realiza comprobaciones para acceder a servidores web (Caiza, 2019).
- **Servidor de base de datos:** sistema para almacenamiento y archivo de datos, realizar cualquier tarea requerida por el usuario en base a la arquitectura cliente/servidor.
- **Servidor de Acceso Remoto (RAS):** es el sistema que recibe las solicitudes de conexiónes remotas a dispositivos en una red local
- **Servidor de correo:** una computadora que le permite enviar y recibir correo por correo electrónico por internet facilitando la comunicación ágil entre usuarios internos y externos de una organización (Caiza, 2019).
- **Servidor de Archivos:** es un sistema que permite transferir archivos entre clientes y servidores que utilizan los protocolos FTP o SFTP.

Instalación de servidores

La instalación del servidor se refiere a una serie de pasos o actividades que garantizan la calidad de la entrega del servidor. Los pasos que se deberían considerar son los siguientes:

- Identificación el hardware en el cual se realizará la instalación.
- Seleccionar el sistema Operativo que va ser instalado.
- Validar compatibilidad.
- Configuración.
- Definir variables de entornos.
- Realizar pruebas de conectividad.

Seguridad de la información

Es un conjunto de estándares de seguridad desarrollados por una empresa u organización para proteger información sensible y proteger su privacidad, es decir, proteger los activos de información. (Silva, 2021).

Objetivos de la seguridad de la información

La finalidad de la seguridad de la información es mantener la integridad, disponibilidad y confidencialidad de la información.

- **Integridad:** los recursos y la información no se modifica permanece intacta, solo personal autorizado puede realizar cambios.
- **Disponibilidad:** la información y los medios están disponibles en cualquier momento.
- **Confidencialidad:** garantiza que los datos están protegidos y solo personal habilitado tienen acceso. (Silva, 2021).

Figura 1

Principios de la seguridad de la información

Nota. En la figura se observa los principios básicos de la seguridad de la información. Recuperado de (Martínez Ramírez, 2020)

- **Autenticidad:** este objetivo se relaciona con el usuario, se obtiene el seguimiento de

quien tiene acceso, permisos, quien puede modificar y quién no.

- **No repudio:** permite visualizar quien tuvo acceso a un archivo y si realizó alguna modificación (ISO, 2018)

Ciberseguridad

La ciberseguridad es la protección de computadoras, servidores, dispositivos móviles, sistemas electrónicos, dispositivos y datos contra ataques maliciosos. También se le llama seguridad informática o seguridad de la información electrónica. El término se utiliza en una variedad de contextos, desde tiendas hasta este tipo de tecnología de la información, y se puede dividir en algunas categorías comunes. (Silva, 2021).

Dominios de ciberseguridad

Una estrategia sólida de ciberseguridad incluye múltiples capas de defensa contra el cibercrimen, incluidos los ciberataques diseñados para acceder, alterar o destruir datos, extorsionar a usuarios u organizaciones, o interrumpir las operaciones comerciales normales. (IBM, 2020). Las contramedidas deben estar dirigidas a:

- **Seguridad de la red:** Las conexiones Wi-Fi y por cable son una de las medidas de seguridad utilizadas para proteger las redes del sistema de personas no autorizadas. Según la Universidad Católica de San Pablo, hay varios niveles a considerar cuando se trata de ciberseguridad en las organizaciones. Los ataques pueden ocurrir en cualquier capa del modelo de capa de seguridad de la red, por lo que se deben desarrollar políticas de seguridad de red, hardware y software para cada área. (UCSP., 2022)

- **Seguridad de las aplicaciones:** Estas son precauciones para evitar el robo de datos o códigos; Las políticas de seguridad también se consideran al desarrollar aplicaciones.

- **Seguridad de cloud:** Es el respaldo a la privacidad del cliente específicamente encripta los datos en la nube mientras está en reposo, en movimiento y en uso (Karina P, 2020).

Amenaza

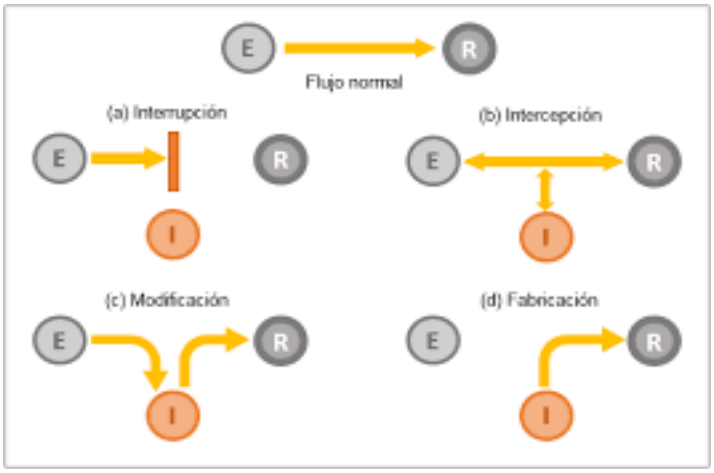
Un Es un ente que puede explotar una vulnerabilidad, también es algo o alguien que identifica una vulnerabilidad específica para explotarla y usarla en contra (Incibe., 2020).

En general, se pueden utilizar cuatro categorías para clasificar las amenazas según el factor de seguridad.

- **Interrupción:** en este ataque de disponibilidad, los recursos del sistema se destruyen o dejan de estar disponibles.
- **Intercepción:** Una violación de la confidencialidad por parte de personas no autorizadas que acceden a los recursos.
- **Modificación:** Implica la manipulación no autorizada de recursos, lo que supone un ataque a la integridad

Figura 2

Tipos de amenaza



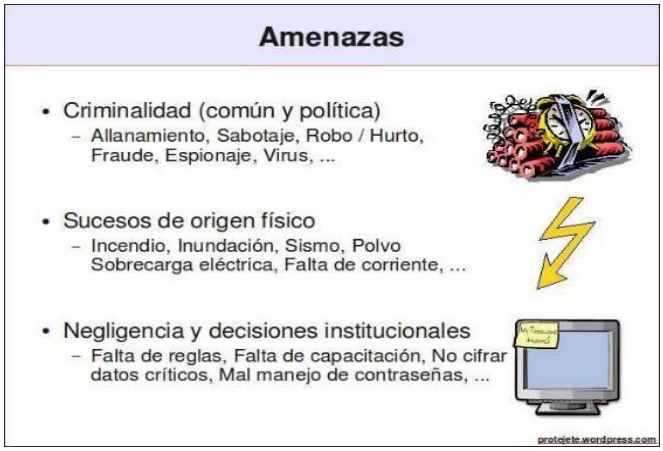
Nota. En la figura se muestra los tipos de amenazas. Recuperado de (Solano, 2017).

Amenaza Física

Es cualquier acto de la naturaleza o daño causado por el hombre de forma directa o indirecta en el hardware del computador (Jurado, 2019).

Figura 3

Amenaza Física



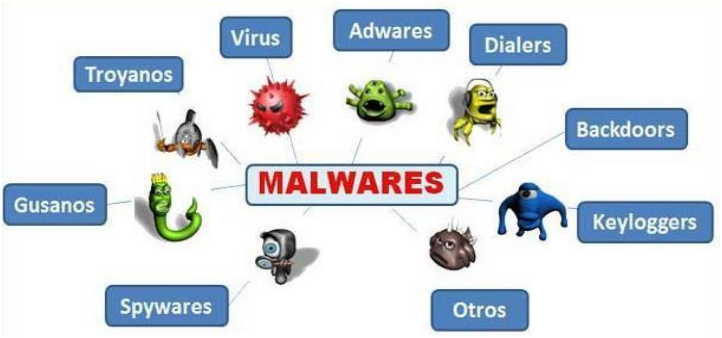
Nota. En la figura se puede observar las causas de las amenazas físicas. Recuperado de (Maribel., 2017).

Amenaza Lógica

Están asociadas con el software que daña los sistemas informáticos, ya sea a propósito o no (Maribel., 2017).

Figura 4

Amenaza Lógica.



Nota. En la figura se observa los tipos de amenazas lógicas. Recuperado de (UNAD., 2022)

Los siguientes grupos serían las amenazas lógicas más significativas.

- **Malware:** es un software malicioso que se encuentra en los archivos adjuntos de los correos electrónicos y que roba información o elimina datos en secreto. El software espía, el ransomware, los virus y los gusanos son ejemplos de malware. (Tokio., 2022).

- **Ransomware:** se trata de la confiscación de datos o equipos que requieren el pago de una determinada cantidad para recuperarlos. Una de las formas más comunes en que los delincuentes extorsionan a clientes y empresas es mediante este ataque. Pueden penetrar en las computadoras de varias maneras, principalmente utilizando estrategias de manipulación o errores de software para instalarse en la máquina del usuario (CISCO., 2022).

- **Gusano:** Este tipo de malware se reproduce sin cesar y se propaga por el ordenador sin causar ningún daño, pero la cantidad de clones ocupa espacio y recursos. (Fernández, 2020)

- **Virus:** este tipo de malware es todo lo contario a los gusanos, el virus afecta el rendimiento del equipo siempre y cuando el usuario autorice (Fernández, 2020).

- **Troyano:** Es lo contrario a un gusano, es decir que no se reproduce por sí solo, debe ser activado por el usuario para propagarse como un virus, con la diferencia de que se oculta como si fuera una aplicación legítima, con la particularidad de que se oculta como si fuera una aplicación legítima. de ingresar al sistema a través de una puerta trasera o también conocida como puerta trasera. (Digicert.).

Ingeniería social

Se refiere a varias estrategias y tácticas utilizadas por los piratas informáticos para engañar a las personas para que, sin saberlo, revelen información privada o hagan clic en enlaces a sitios web maliciosos a cambio. Estos piratas informáticos engañan a sus víctimas para que eludan las medidas típicas de ciberseguridad y obtengan acceso a sus computadoras o información personal (Softwarelab, 2021).

- **Phishing:** también conocido como robo de identidad, es el acto de robar información confidencial, como nombres de usuario y contraseñas, de personas a través del correo electrónico (IBM, 2020).

- **Spyware:** es un programa espía cuya función principal es recopilar en secreto la mayor cantidad de información posible del usuario. Cabe señalar que se instala sin el consentimiento del usuario (G4s, 2020)

- **Adware:** también conocida como publicidad no solicitada. Su objetivo es mostrar anuncios a través de ventanas emergentes mientras navegas por Internet (Aleph, 2021)

- **Rootkit:** utilizado por los hackers para robar información sin ser detectados a través de un acceso remoto (ICA, 2022)

- **Ataques DoS:** el propósito de esto es sobrecargar al servidor con tráfico hasta el punto de que no pueda responder a las solicitudes de servicio de los usuarios (Cámara Valencia, 2018)

Vulnerabilidad

Los errores o fallas en los sistemas de información amenazan los activos más importantes de una empresa, organización o individuo, permitiendo a los atacantes comprometer la integridad, disponibilidad o confidencialidad de la información. Es importante poder encontrar estas vulnerabilidades y solucionarlas. Deshazte de ellos lo antes posible. Estos fallos pueden ocurrir por diversas razones, como un diseño deficiente, una mala configuración o la falta de procedimientos (Silva, 2021).

Riesgo

Es la probabilidad que una amenaza explote una vulnerabilidad y el impacto se refleja en la empresa sea fuga o perdida de información (ISO 27001, 2018)

Ciberguerra

Estos son los ataques digitales que los países reciben todos los días. El objetivo de las agencias militares es identificar agujeros de seguridad en las redes o sistemas informáticos del adversario para penetrar, atacar y robar información y datos confidenciales. En este escenario, el campo de batalla es el ciberespacio y las armas son programas o aplicaciones informáticas (Sain, 2016)

Ciberataques

Este es un intento de atacar los sistemas informáticos de una organización específica para robar información. Las personas que realizan estas actividades se denominan ciberatacantes, hackers o hackers (González, 2018). Los ataques informáticos se pueden dividir en:

- **Ataques pasivos:** En este tipo de ataque, el atacante simplemente observa la comunicación y recopila datos sobre lo que se envía, en lugar de modificarlo. Los ataques pasivos son muy difíciles de detectar porque no se modifican datos, este ataque identifica remitentes y receptores de comunicaciones y comprueba los tiempos de los principales movimientos e intercambios de datos, sin embargo, es posible que cifrar los datos o utilizar otros métodos no tenga éxito.

- **Ataques activos:** Esta operación ofensiva de alguna manera altera el orden de los datos transmitidos o crea un flujo de datos inexistente. El robo de identidad, el reenvío (es decir, pretender reenviar mensajes legítimos), la alteración de mensajes o la denegación de servicio (DoS) son algunos de los ataques activos (Itca, 2022).

Herramientas de seguridad informática

Capacitar a los empleados para manejar los datos de la empresa, los protocolos operativos y responder a las amenazas cibernéticas y, por supuesto, utilizar software y otras herramientas de seguridad digital de varios proveedores son formas de lograr la seguridad de los datos. En este estudio, analizamos algunas de las herramientas de ciberseguridad más interesantes disponibles, qué pueden hacer por nosotros y por qué deberíamos utilizarlas en el trabajo para proteger nuestros archivos (Castellnou, 2021).

Software Antivirus

Cada computadora empresarial conectada a la red debe tener instalado un buen programa antivirus. El software antivirus previene eficazmente la detección de malware u otros elementos maliciosos, que también pueden eliminar amenazas potenciales y poner en cuarentena el dispositivo para evitar que los problemas empeoren (Castellnou, 2021).

Firewall perimetral de red

Un firewall es uno de los dispositivos de seguridad de la información más importantes. Simplemente escanea los paquetes de red y decide si bloquearlos según las reglas predefinidas por el administrador. Los firewalls le permiten inspeccionar el tráfico de la red, identificar usuarios, evitar el acceso no autorizado y realizar muchas otras tareas (Castellnou, 2021).

Servidor proxy

Se trata de un dispositivo que se sitúa entre las conexiones a Internet del navegador y filtra los paquetes que viajan entre ellas. Los sitios web que se consideran peligrosos o prohibidos en el trabajo se bloquean gracias al servidor proxy. Un servidor proxy también ayuda a configurar un sistema de autenticación que restringe el acceso a la red externa (Castellnou, 2021).

End Point Disk Encryption

Este método de codificación de datos, también conocido como cifrado de punto final, evita que cualquier persona que no tenga la clave de descifrado los lea. Al prohibir los archivos almacenados en computadoras, servidores y otros puntos finales, protege los sistemas operativos de archivos de instalación corruptos (Castellnou, 2021).

Escáner de vulnerabilidades

Los escáneres de vulnerabilidades son una importante herramienta de ciberseguridad para todo tipo de empresas, independientemente de su tamaño o industria. Un escáner es un software que encuentra, evalúa y monitorea las vulnerabilidades del sistema. Reduzca drásticamente el tiempo que lleva resolver conflictos enviando alertas instantáneas cuando se detectan problemas (Castellnou, 2021).

Hardening

Un administrador puede realizar muchas actividades dentro del sistema operativo para maximizar los distintos niveles de seguridad de la computadora. El objetivo del endurecimiento es mejorar la seguridad de un sistema mediante la implementación de medidas que reduzcan las vulnerabilidades y el potencial de intrusión o compromiso. Este es un proceso de seguridad que consiste en tomar medidas para aumentar la protección de su sistema operativo o dispositivo.

Algunos puntos en los que un atacante puede acceder o corromper varios tipos de sistemas operativos incluyen el software instalado, los usuarios finales, las interfaces de red y otros puntos que ya no son necesarios dentro del sistema. Incluye brechas (Caiza, 2019).

Actividades del proceso de hardening

El proceso de hardening o endurecimiento de un servidor, se le conoce como “refuerzo del sistema operativo”. Entre las actividades que pueden considerarse dentro de este, de manera general, se encuentran: la eliminación de cuentas sin uso, el empleo de políticas de contraseñas, el cierre de puertos de red sin uso, la administración de privilegios de usuarios, la eliminación de servicios no deseados, y la administración de actualizaciones (Caiza, 2019).

- Procedimientos de administración de cuentas de usuario, grupos, TCBS (Truste Base Computing), módulos de autenticación agregables y relaciones de confianza.
- Administrar los paquetes Las actividades de hardening específicas a sistemas operativos Linux, según Maldonado, son las siguientes:
- Asegurar las herramientas de desarrollo y compiladores.
- Instalar y configurar Firewalls, Kits de Seguridad (antivirus, antispyware, antimalware, anti hackers, anti banners).
- Usar herramientas para Pen Testing y Monitoreo.

- Configurar protocolos, puertos y servicios (solo los necesarios).
- Implementar esquemas de seguridad, DMZ (Demilitarized Zone), Front End / Back End, Router apantallado, proxys, Firewalls (Caiza, 2019).

Aseguramiento de Servidores

Se trata de un conjunto de acciones realizadas para establecer un servidor o equipo con ajustes de seguridad específicos. Este proceso también puede denominarse fortalecimiento del sistema operativo.

Hardening de Servidores

Hardening (palabra en ingles que significa endurecimiento), En seguridad informática, es el proceso de proteger la seguridad del sistema reduciendo las vulnerabilidades del sistema. Esto se logra eliminando software, servicios, usuarios, etc. Puertos que el sistema no necesita, así como puertos que están cerrados y sin uso (Caiza, 2019).

El aseguramiento de servidores (conocido también como "Server Hardening") es responsable de inspeccionar y probar todos los componentes de su solución, que estén configurados adecuadamente para la seguridad y que no existan tales grietas. Dado que las aplicaciones web dependen del servidor web y del sistema operativo subyacente, hay muchas ventajas en no, tener una seguridad completa a nivel de aplicación cuando ocurren problemas (Caiza, 2019).

Los beneficios que nos aporta el hardening de servidores son reducir los riesgos asociados al fraude y error humano, facilitar el despliegue de configuraciones más limpias y seguras, garantizar que los recursos críticos tengan parches actualizados y sean capaces de defenderse de vulnerabilidades conocidas; se presenta ciertas consideraciones a tomar al momento de blindar los servidores:

- Para sus comunicaciones se deberá usar cifrado de datos.

- Evite utilizar protocolos inseguros de transmisión de información sensible.
- Desinstalar o desactivar software innecesario en los servidores
- Actualizar los sistemas a versiones vigentes y principalmente los parches de seguridad.
- Usar extensiones de seguridad
- Deshabilitar binarios no deseados de SUID, SGID
- Las credenciales de los administradores de los sistemas deben ser fuertes y de no fácil deducción.
- No permitir contraseñas en vacío.
- Bloquear la cuenta después de un número de intentos fallidos
- Establecer un periodo frecuente de cambio de contraseña
- Deshabilitar y no utilizar puestos por defecto
- Deshabilitar los servicios innecesarios.
- Deshabilitar los inicios de sesión directos a root
- Ocultar la versión del sistema Operativo y contenedor web
- Establecer controles perimetrales como firewall, sistema de detección de intrusos.
- Usar protocolo SSH para comunicación.

Herramientas utilizadas

Pentest Tools En un programa de scaneo que realiza evaluaciones de seguridad de red externa de caja negra, a su vez ofrece compromisos de pentesting exitosos con velocidad, consistencia y flexibilidad superiores. Cubre todas las etapas de un compromiso, desde la recopilación de información hasta el escaneo del sitio web, el escaneo de la red, la explotación y la generación de informes.

Centos Es una distribución de GNU/LINUX completamente gratuita, se deriva del código de fuente que lanza Red Hat, es un sistema operativo de código abierto conocida por su consistencia, estabilidad, administración fácil de usar.

OpenVas Sistema Abierto para la Evaluación de Vulnerabilidades, está compuesto por una serie de servicios y herramientas de escaneo y administración de vulnerabilidades; su arquitectura es robusta y completa, siendo su componente más importante el Escáner OpenVAS, el cual es altamente eficiencia en la ejecución de NVTs (pruebas de vulnerabilidad en redes), mismo que obtiene actualizaciones diarias a través de OpenVAS NVT Feed (Caiza, 2019).

Sistemas operativos orientados a la ciberseguridad

Todas las empresas necesitan contar con herramientas y sistemas operativos de ciberseguridad por varias razones. Aquí hay algunos parámetros a considerar. Debido a la acelerada digitalización provocada por la pandemia, la cantidad de datos gestionados por las empresas ha crecido exponencialmente. Es por eso que la seguridad organizacional se ha convertido en una parte importante no solo para cumplir con la ley, sino también para proteger su honor al proteger la información privada y confidencial. Sin embargo, lo más preocupante es que, según Eurostat, a una persona media le lleva 5,4 meses darse cuenta de que ha sido hackeada (Bello, 2022).

Kali Linux

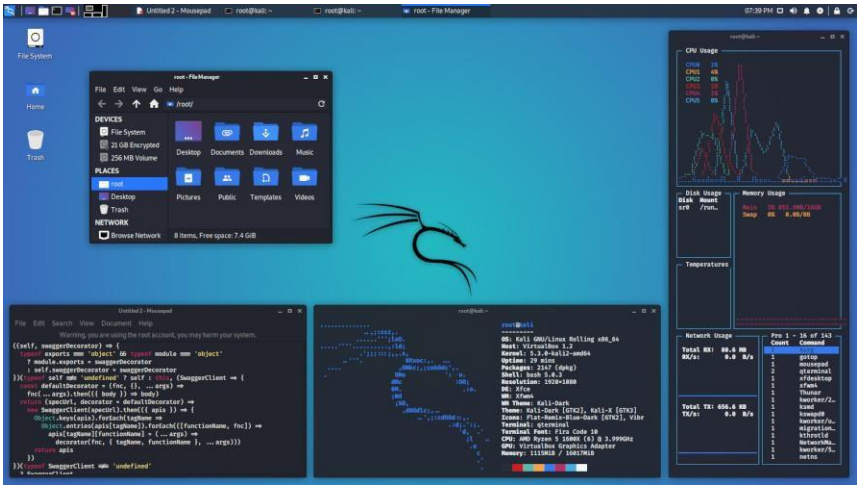
Para muchos temas de seguridad, incluidos análisis de redes, ataques inalámbricos, análisis forense y más, Kali Linux es la mejor opción, es una distribución de Linux basada en el sistema operativo Debian (Altube, 2021).

Kali Linux se utiliza con más de 600 herramientas de seguridad diferentes, principalmente para pruebas de penetración y análisis forense digital. La distribución de Linux escanea computadoras y redes en busca de posibles errores, descifra claves y cifra datos, y

evalúa el estado del sistema de seguridad. Una vez eliminados los datos o archivos, se pueden recuperar siempre que no se sobrescriban (IONOS, 2022).

Figura 5

Entorno de Kali Linux.



Nota. Para sistemas operativos tipo UNIX, Xfce es un entorno de escritorio liviano. Recuperado de (Kali, 2022)

Metasploit

Según la Universidad Complutense de Madrid, el proyecto de seguridad informática de código abierto Metasploit difunde conocimientos sobre fallos de seguridad, ayuda en las pruebas de penetración y ayuda en la creación de firmas de sistemas de detección de intrusiones. Es una herramienta GNU que utiliza varios lenguajes de programación diferentes, incluidos C, Python, ASM, etc., para crear, probar, desarrollar y penetrar en varios sistemas, incluido Windows (UCM, 2022).

Figura 6

Interfaz de Metasploit.

Nota. En la figura se visualiza la interfaz del sistema operativo Metasploit. Recuperado de (Xringarchery, 2019).

Red Informática

Es un conjunto de dispositivos informáticos que controlan o no controlan una conexión media que se pueda compartir. También son sistemas de comunicación. Más equipo que cambia transmisores alternativos y recibo de personajes (Implika, 2021). Estos son los componentes de las redes informáticas:

- **Servidores:** son los que concentran el control de la red y tratan el flujo de datos.
- **Clientes:** se refiere a dispositivos en la red que no son servidores pero que aún se usan para acceder a la red.
- **Medios de transmisión:** la transmisión de información es posible gracias al cableado.
- **Elementos de hardware:** son los componentes que hacen posible construir la red físicamente.
- **Elementos de software:** son las aplicaciones necesarias para controlar todo el sistema operativo (Implika, 2021).

Tipos de Redes Informáticas

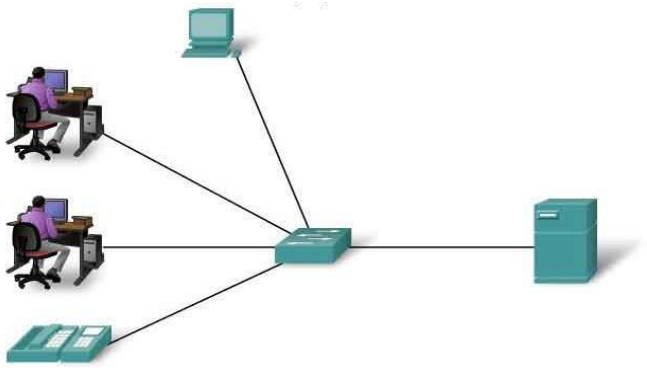
Las redes informáticas se clasifican por su tamaño y por su forma. Según su tamaño: LAN, MAN, WAN, y según la forma en que se conecten los equipos: bus, malla en estrella y en anillo (Áreatecnológica, 2022).

Redes de Área Local (LAN)

Una LAN es una red ubicada en un área pequeña, generalmente dentro del mismo edificio. Ejemplos de redes de área local son las redes Wi-Fi domésticas y las redes de pequeñas organizaciones. Un enrutador actúa como concentrador para la mayoría de las conexiones LAN a Internet. Las redes domésticas suelen utilizar un único enrutador, mientras que las LAN en áreas más amplias también pueden utilizar varios conmutadores de red para entregar paquetes más rápido (Hwang, 2021).

Figura 7

Red LAN.



Nota. En la figura se visualiza la comunicación que existe en una red LAN. Recuperado de (UAEH, 2022).

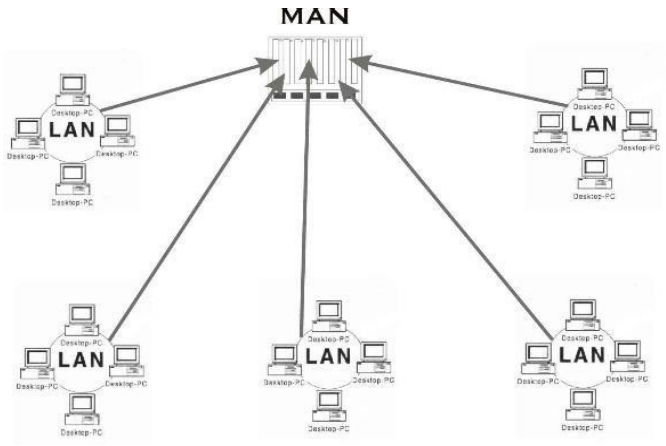
Redes de Área metropolitana (MAN)

Las redes de área metropolitana operan a altas velocidades, cubren grandes áreas y tienen la cualidad de combinar servicios de datos, voz y video a través de medios de transmisión

guiados. La definición de LAN se ha convertido en el concepto de red de área metropolitana que tiene una cobertura más amplia (Cisco, 2022).

Figura 8

Red MAN.



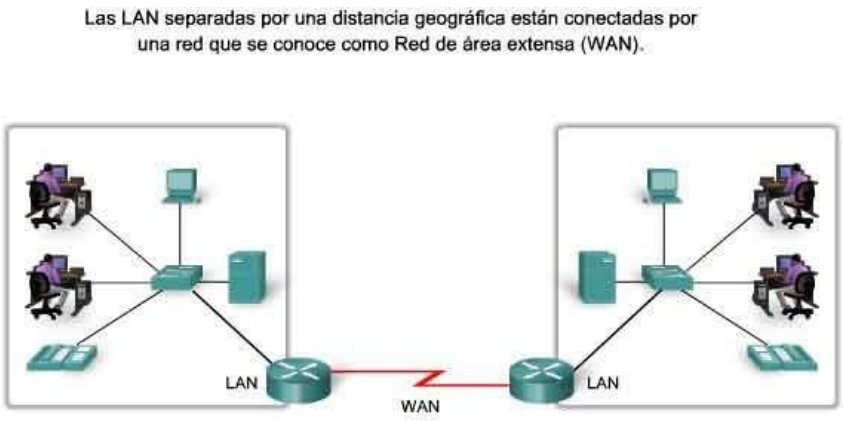
Nota. En la figura se puede observar la comunicación que existe en una red MAN. Recuperado de (Cisco, 2022).

Redes de Área Amplia (WAN)

Es una conexión entre dos o más redes de área local (LAN) que están físicamente separadas entre sí pero crean una sensación de conexión local. Para que una gran cantidad de computadoras funcionen en dicha red, deben estar conectadas entre sí mediante alguna forma de transmisión (generalmente cables o fibra óptica) para comunicarse con una estación central a cientos de kilómetros de distancia (Higo, 2022).

Figura 9

Red WAN.



Nota. En la figura se visualiza la comunicación de una red WAN. Recuperado de (Higo, 2022).

Topología de Red

Según la Universidad Internacional de La Rioja, este es el método mediante el cual instalamos el cable que se conecta al dispositivo que conforma la red. Al diseñar redes de computadoras, es importante considerar la topología de la red. Debido a que estos tipos de topologías de red determinan cómo se conectan las computadoras entre sí, es importante conocerlas. Algunos ejemplos incluyen malla, estrella, árbol, bus y anillo (UNIR, 2022). Básicamente, hay dos niveles en una topología de red:

- **Físico:** Determina las conexiones físicas entre terminales y dispositivos, incluido el uso de cables y antenas.
- **Lógico:** Es el diagrama más completo de cómo se mueven los datos dentro de una red.

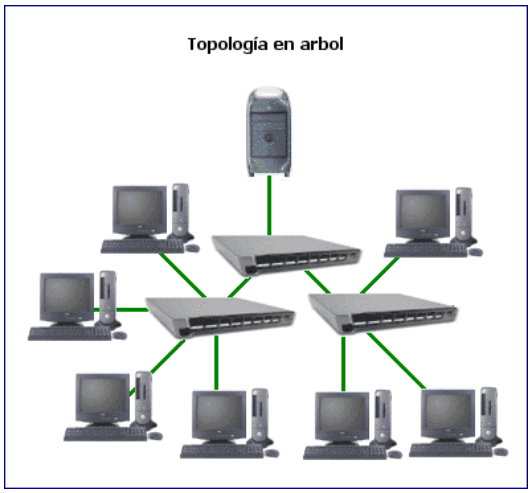
Disponer de una red bien estructurada tanto física como lógicamente es fundamental para garantizar el correcto desempeño de todos los dispositivos conectados (UNIR, 2022).

Topología en Árbol

Dado que cuenta con un dispositivo central al que se conectan los nodos, en este caso compartiendo el mismo canal de comunicación, este tipo de topología con modelo jerárquico se puede describir como una combinación de topologías en estrella y bus. Todos los nodos reciben información, pero se propaga desde la raíz (Limones, 2021).

Figura 10

Topología en Árbol.



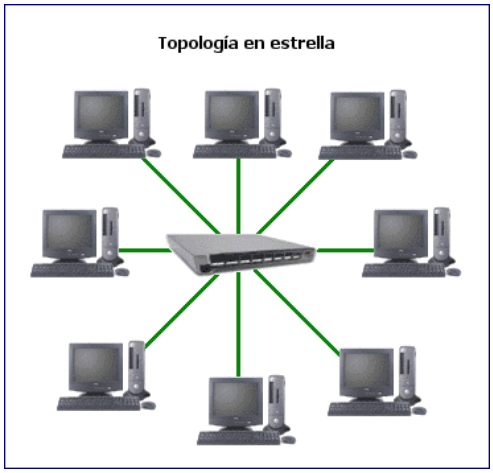
Nota. En la figura se observa el diseño físico de la red en árbol. Recuperado de (Tinet, 2022).

Topología en Estrella

A diferencia de una topología de bus donde todos los dispositivos comparten un único canal de comunicación, en esta topología cada dispositivo de red tiene un canal separado. A diferencia de las topologías anteriores (bus y anillo), si un nodo falla o falla no afecta a los demás nodos, pero si falla un switch toda la red se cae. La organización de la red mejora a medida que resulta más fácil agregar nuevos nodos, ya que todo lo que hay que hacer es conectarlos a un conmutador (Limones, 2021).

Figura 11

Topología en Estrella.



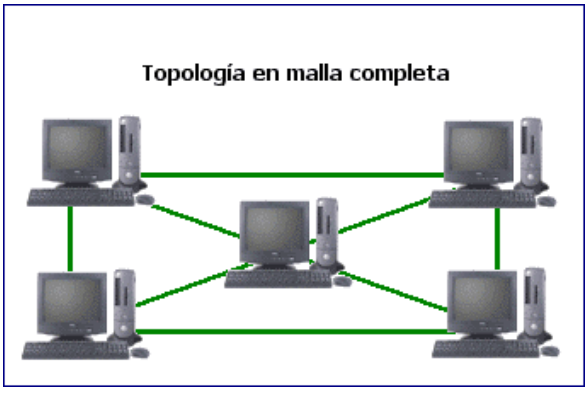
Nota. En la figura se observa el diseño físico de la red en estrella. Recuperado de (Tinet, 2022).

Topología en Malla

Cada nodo está conectado entre sí, son responsables de enviar mensajes por el camino más corto y cada uno tiene conexiones en todas las direcciones. Hacer llegar el mensaje al destinatario es su máxima prioridad, pero si algo falla, buscan en otra parte (Limones, 2021).

Figura 12

Topología en Malla.



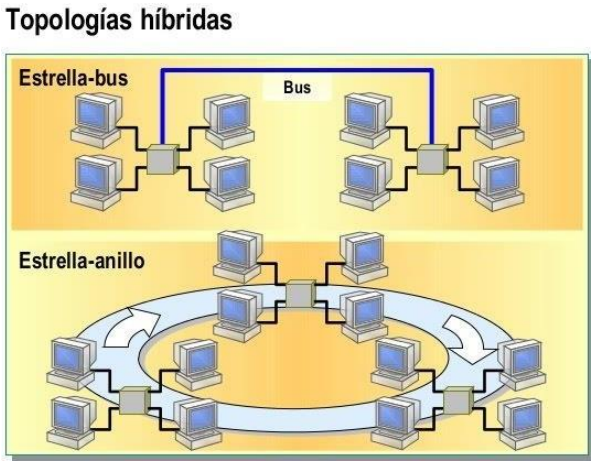
Nota. En la figura se visualiza el diseño físico de la red en malla. Recuperado de (Tinet, 2022).

Topología Híbrida

Se refiere al uso de dos o más topologías combinadas por una red empresarial con necesidades específicas. Como resultado, acepta las ventajas y desventajas de la topología incluida (Limones, 2021).

Figura 13

Topología Híbrida.



Nota. En la figura se observa el diseño físico de la red híbrida. Recuperado de (Google, 2022).

Protocolos de red

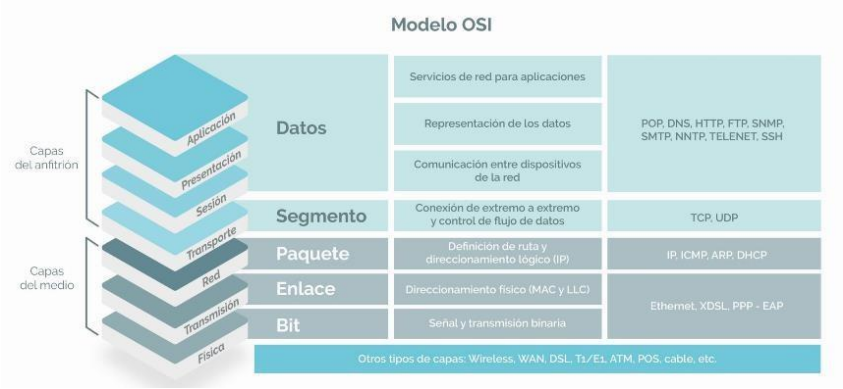
Los protocolos de Internet definen un formato estándar y un conjunto de pautas para el intercambio de mensajes entre dispositivos. Hay que entender cómo se comunican las computadoras. El Protocolo de transferencia de hipertexto (HTTP), el Protocolo de control de transmisión (TCP) y el Protocolo de Internet (IP) son algunos de los protocolos de Internet más populares (CISCO, 2019).

Modelo OSI

La Organización Internacional de Normalización ISO creó el modelo OSI (Open Systems Interconnection), que es una referencia a las redes de computadoras que utilizan protocolos para conectar diferentes sistemas de comunicación (Cloudflare, 2022). El modelo OSI consta de siete niveles que se representa en la figura 23.

Figura 14

Modelo OSI.



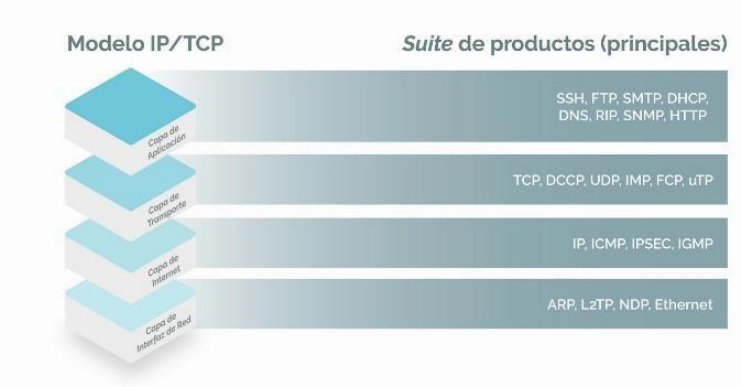
Nota. En la figura se muestra las 7 capas del modelo OSI. Recuperado de (Process, 2022).

Modelo TCP/IP

Actualmente es el modelo que se usa para las comunicaciones informáticas, está constituido por protocolos que permiten la comunicación entre equipos informáticos (Robledano, 2019). En la figura 24 se plasma las cuatro capas del modelo TCP/IP que deben tenerse en cuenta.

Figura 15

Modelo IP/TCP.



Nota. En la figura se muestra las 4 capas del modelo IP/TCP. Recuperado de (Process, 2022).

Una ilustración de cómo interactúan los diferentes protocolos es la comunicación entre un servidor web y un cliente web.

- **HTTP:** protocolo de aplicación que controla la comunicación entre un servidor web y un

cliente web.

- **TCP:** gestionar conversaciones individuales a través de un protocolo de transporte.
- **IP:** crea paquetes a partir de segmentos TCP, asigna direcciones y los envía al host de destino.
- **Ethernet:** hace posible la transmisión física de datos a través de medios de red (CISCO, 2019).

Figura 16

Interacción de Protocolos.

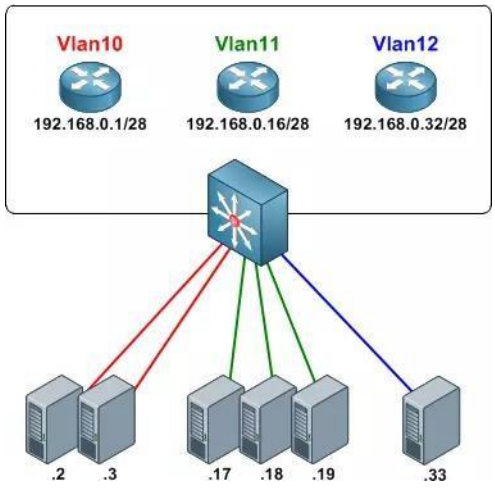
Nota. En la figura se observa la interacción entre los protocolos. Recuperado de (Educa Sistemas, 2018).

VLAN

Es una tecnología que permite dividir o segmentar redes independientes de diferentes grupos de usuarios de red que conforman la red física, es decir, un usuario puede tener múltiples VLAN en un solo switch (TokioSchool, 2021).

Figura 17

Ejemplo de una Red con VLAN.



Nota. En la figura se observa un ejemplo de VLAN. Recuperado de (De Luz, 2022).

Tipos de VLAN

- **VLAN de datos o de usuario:** para transmitir únicamente el tráfico de datos creado por los usuarios.
- **VLAN Predeterminada:** La VLAN estándar en Cisco es la VLAN 1 la cual no se puedo borrar, se transporta tráfico de control de capa 2 y al encender el conmutador esta VLAN es la VLAN predeterminada para todos los dispositivos.
- **VLAN nativa:** conectado a un puerto de tipo troncal 802.1Q. Todo el tráfico que se coloca en esta VLAN no se etiqueta con otra VLAN.
- **VLAN de administración**: Está configurado para tener acceso a la gestión de los conmutadores.
- **VLAN de Voz:** Permite mantener el nivel de servicio de telefonía VoIP. Este tráfico con etiquetas de VLAN tiene prioridad sobre otros tipos de tráfico, como los datos de Internet (De Luz, 2022).

Capítulo III

Desarrollo y resultados

Análisis técnico del entorno físico del servidor

Verificación del entorno físico en donde se encuentra ubicado el servidor

El propósito de la revisión del data center, donde se encuentran los servidores de la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre (DTIC), es verificar las condiciones en las que se encuentra la instalación física del servidor en un rack. Esta revisión es importante para mantener los estándares establecidos por el Uptime Institute en su certificación Tier III, especialmente en lo que respecta a la seguridad física. Durante la revisión, se verifica varias vulnerabilidades de acuerdo con los estándares del Uptime Institute, y se crea una tabla de cumplimiento para evaluar el grado de cumplimiento con dichos estándares.

Tabla 1

Verificación de estándares Tier III seguridad física del data center en DTICS de la Fuerza Terrestre

	REQUISITO	DESCRIPCIÓN	CUMPLIMIENTO
1	Valla perimetral segura	La valla debe ser de al menos 2 metros de altura y estar coronada con alambre de púas o concertina.	NO APLICA El centro de datos está ubicado dentro de un edificio con seguridad perimetral propia.
2	Control de acceso a las instalaciones	Se debe controlar el acceso a las instalaciones mediante tarjetas de identificación, lectores biométricos o sistemas de seguridad similares.	SI CUMPLE
3	Monitoreo de	Se debe realizar un monitoreo de videovigilancia de las	SI CUMPLE

	REQUISITO	DESCRIPCIÓN	CUMPLIMIENTO
	videovigilancia	instalaciones las 24 horas del día, los 7 días de la semana.	
4	Sistemas de detección de intrusos	Se deben instalar sistemas de detección de intrusos en las instalaciones.	NO CUMPLE
5	Puertas y ventanas seguras	Las puertas y ventanas deben ser seguras y estar cerradas con llave cuando no estén en uso.	NO CUMPLE
6	Control de acceso a las áreas restringidas	Se debe controlar el acceso a las áreas restringidas mediante tarjetas de identificación, lectores biométricos o sistemas de seguridad similares.	NO CUMPLE
7	Sistemas de detección de incendios y de extinción de incendios	Se deben instalar sistemas de detección de incendios y de extinción de incendios en las instalaciones.	NO CUMPLE
8	Sistemas de control ambiental	Se deben instalar sistemas de control ambiental para mantener la temperatura y la humedad dentro de los rangos especificados.	SI CUMPLE
9	Control de acceso a las salas de servidores	Se debe controlar el acceso a las salas de servidores mediante tarjetas de identificación, lectores biométricos o sistemas de seguridad similares.	NO CUMPLE
10	Racks de servidores seguros	Los racks de servidores deben estar cerrados con llave y tener acceso restringido.	NO CUMPLE
11	Sistemas de detección de fugas de agua	Se deben instalar sistemas de detección de fugas de agua en las salas de servidores.	NO CUMPLE
12	Sistemas de detección de humo y de extinción de incendios	Se deben instalar sistemas de detección de humo y de extinción de incendios en las salas de servidores.	NO CUMPLE

Nota. Estándares técnicos de un data center.

Una vez realizada la verificación del entorno físico, se identificaron 8 estándares que el data center no cumple. Entre estos estándares, destaca especialmente el parámetro de "Rack de servidores seguros". Se constató que este estándar no se cumple debido a que las puertas de los racks estaban abiertas y no contaban con seguro, al igual que el acceso al data center. Además, se observó que el servidor seleccionado para este trabajo de titulación estaba fuera de un rack, al igual que muchos otros servidores en el centro de datos.

Figura 18

Servidor situado fuera de un rack.

Nota. Constancia del incumplimiento de la seguridad física.

Verificación del entorno físico del cableado en donde se encuentra ubicado el servidor

Se llevó a cabo una inspección física detallada del cableado dentro de los racks. El principal objetivo de esta inspección fue verificar que el cableado cumpla con los estándares de seguridad y confiabilidad establecidos para los centros de datos de nivel TIER III. Una vez más, se evidenció el incumplimiento de los estándares de seguridad en el cableado de uno de los racks de servidores.

Tabla 2

Tabla detallada de incumplimientos el cableado en los rack del data center de las Dtics.

INCUMPLIMIENTO	DESCRIPCIÓN
Cableado suelto	Los cables no están sujetos adecuadamente al rack o al sistema de gestión de cables.
Longitudes inadecuadas	Las longitudes de cable son inapropiadas así que pueden causar congestión o problemas de rendimiento
Duplicación de cables	Existe presencia de cables duplicados que pueden generar confusión y problemas de identificación
Falta de etiquetado	Falta de etiquetado adecuado de los cables, lo que dificulta la identificación y el mantenimiento
Exposición a factores de riesgo	Cables expuestos a fuentes de calor o a condiciones ambientales adversas que pueden dañar el cable o afectar su rendimiento

Nota. Fallos en la disposición de cables en los bastidores de las DTICS.

En la inspección del data center, se detectaron cables sueltos y desordenados, así como la falta de etiquetado adecuado. Esta situación representa un riesgo potencial para la integridad y la seguridad de la infraestructura, ya que los cables expuestos a factores de riesgo como calor, humedad o interferencias electromagnéticas pueden comprometer el funcionamiento óptimo de los sistemas de redes y telecomunicaciones. Es crucial abordar estas deficiencias para garantizar un entorno de operación confiable y seguro.

Figura 19

Cables sueltos expuestos a factores de riesgos.

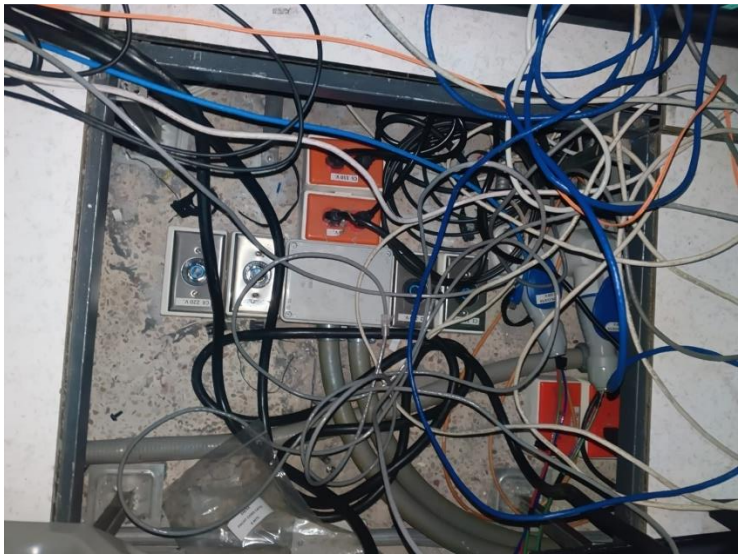
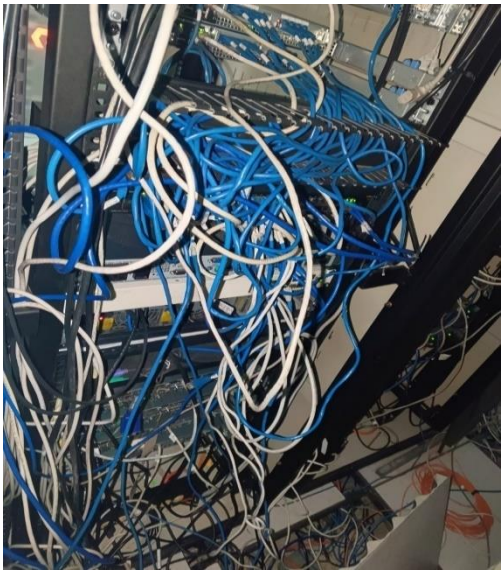


Figura 20

Falta de etiquetado en los cables.



Se lleva a cabo la organización cuidadosa de los cables dentro del rack, asegurando una disposición ordenada y eficiente. Esta acción facilita la identificación y el mantenimiento de las conexiones, contribuyendo así a una gestión más efectiva de la infraestructura del data center.

Figura 21

Cables ordenados.

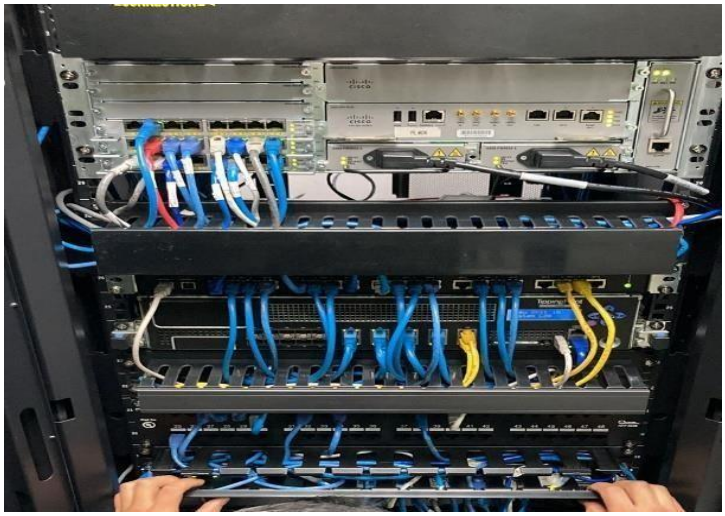
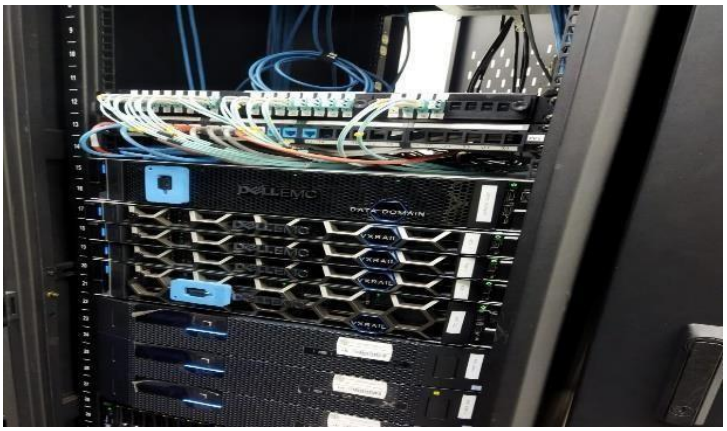


Figura 22

Cables con su etiquetado respectivo.



Análisis técnico de las características del servidor

Tras completar la inspección física del data center que alberga los servidores de la fuerza terrestre, se identificó la necesidad de intervenir en un servidor específico: el Proliant DL380 G7. Este servidor, vital para las operaciones, requería atención inmediata para garantizar su óptimo funcionamiento y contribuir al desempeño general de la infraestructura de tecnología de la información. Se asumió la responsabilidad de este servidor con el objetivo de realizar las acciones necesarias para su mantenimiento y hardenización, asegurando así su disponibilidad y confiabilidad para el cumplimiento de las misiones críticas.

Durante la revisión del servidor, se encontraron las especificaciones técnicas detalladas del equipo. Se constató que el servidor está equipado con 32 GB de memoria RAM y cuenta con dos procesadores Intel Xeon de 2.13 GHz cada uno. Además, se observó que el sistema operativo instalado es Ubuntu Server 20.04.6.

Figura 23

Características3 técnicas del servidor.

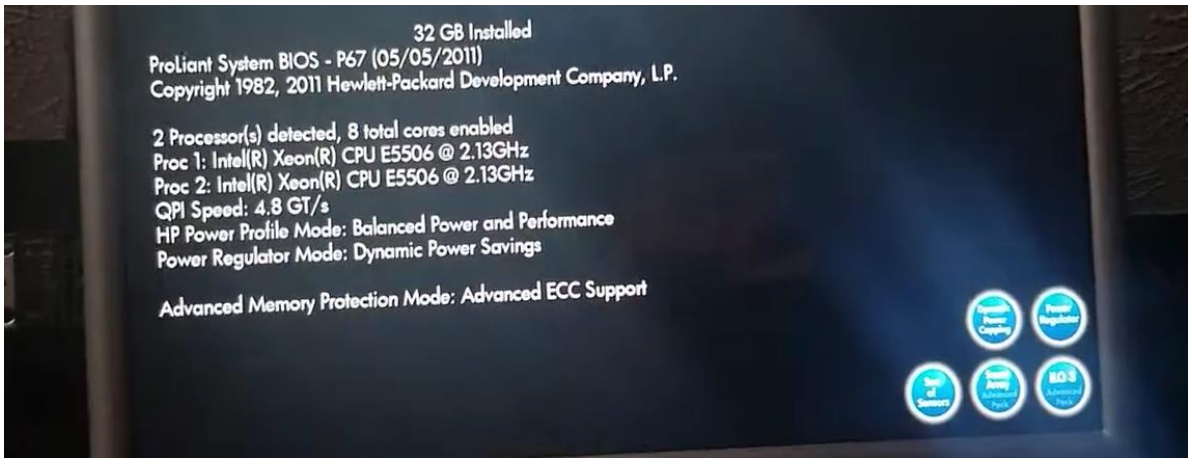
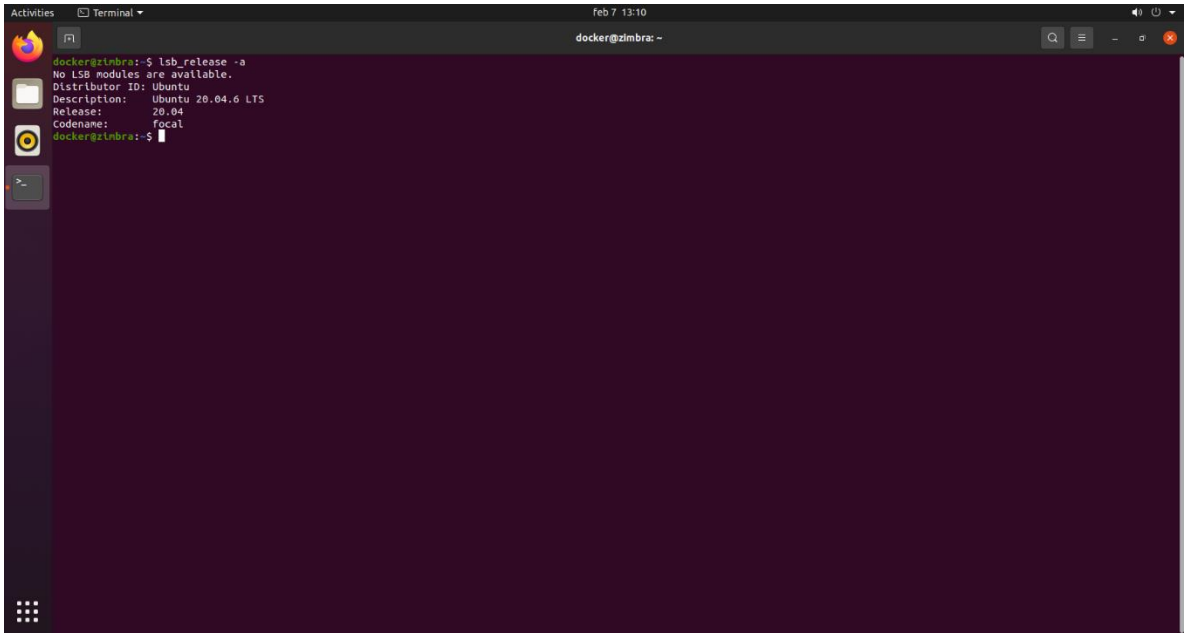


Figura 24

Sistema operativo Ubuntu Server 20.04.6 identificado en el servidor



Con esta información detallada sobre el hardware y el software del servidor en cuestión, se llevó a cabo una investigación exhaustiva sobre el software libre que se puede utilizar para el endurecimiento de servidores. El objetivo era identificar herramientas y soluciones de código abierto que puedan fortalecer la seguridad y la integridad del servidor en la infraestructura. Al aprovechar las capacidades del software libre, se pueden implementar medidas efectivas para proteger los activos de tecnología de la información, mitigar riesgos y garantizar un entorno de operación robusto y confiable.

Análisis técnico de las herramientas de software libre para la hardenizacion del servidor

En la investigación realizada en diversos sitios web de seguridad informática, se encontraron las siguientes opciones:

- Fail2Ban: Es una herramienta de prevención de intrusiones que escanea registros de archivos y bloquea direcciones IP que muestran signos de comportamiento malicioso, como intentos de inicio de sesión fallidos repetidos.
- OSSEC: Un sistema de detección de intrusos de host de código abierto que realiza análisis de registros, detección de rootkits y monitoreo de integridad de archivos en servidores.
- SNORT: Es un sistema de detección de intrusiones de red de código abierto que monitorea y analiza el tráfico en busca de actividades sospechosas o maliciosas. Detecta amenazas como intentos de intrusión, escaneos de puertos y ataques de denegación de servicio mediante reglas predefinidas. Es altamente configurable y se usa en entornos empresariales y domésticos para mejorar la seguridad de la
- ModSecurity: Un firewall de aplicaciones web (WAF) de código abierto que protege las aplicaciones web mediante la detección y prevención de ataques comunes, como inyecciones SQL y cross-site scripting (XSS).
- AIDE (Advanced Intrusion Detection Environment): Similar a Tripwire, AIDE verifica la integridad de los archivos del sistema mediante la comparación de las firmas de archivos con una base de datos almacenada previamente, alertando sobre cualquier cambio sospechoso.
- Lynis: Una herramienta de auditoría de seguridad que realiza análisis de seguridad automatizados en sistemas basados en Unix y Linux, proporcionando recomendaciones para mejorar la seguridad del servidor.

Tabla 3

Tabla comparativa de las herramientas de software libre para hardenizar servidores con sistema operativo 20.04.

Herramienta	Funcionalidad	Plataformas	Instalación en Ubuntu Server
Fail2Ban	Prevención de intrusiones mediante bloqueo de direcciones IP	Linux, Unix	Disponible en repositorios
Snort	Sistema de detección de intrusiones de red	Linux, Unix	Disponible en repositorios
ModSecurity	Protección de aplicaciones web contra ataques comunes	Linux, Unix	Disponible en repositorios
AIDE	Monitoreo de la integridad de archivos del sistema	Linux, Unix	Disponible en repositorios
Lynis	Auditoría de seguridad y recomendaciones de mejoras	Linux, Unix	Descarga e instalación manual

Herramienta Fail2Ban en el servidor

Después de verificar y seleccionar dos herramientas de software libre para endurecer el servidor, Fail2Ban y Snort, el siguiente paso es proceder con su instalación y ejecución. Este proceso implica seguir las instrucciones de instalación específicas de cada herramienta en el sistema operativo Ubuntu Server 20.04, garantizando que se configuren correctamente según las necesidades de seguridad del entorno. Una vez instalada, se ejecutará y configurará según las mejores prácticas de seguridad, lo que ayudará a fortalecer la infraestructura del servidor y a mitigar posibles amenazas y vulnerabilidades. Es importante realizar pruebas y ajustes adicionales según sea necesario para garantizar que las herramientas estén funcionando de manera efectiva y proporcionando la protección adecuada para los servidores.

Al ingresar al sistema Docker, una plataforma de software que permite empaquetar, distribuir y ejecutar aplicaciones en contenedores, se observó que no tenía acceso de superusuario, el cual es necesario para administrar todo el sistema operativo. Los contenedores son entornos aislados que contienen todo lo necesario para ejecutar una aplicación, incluidas las bibliotecas, dependencias y configuraciones, lo que garantiza que la aplicación se ejecute de manera consistente en cualquier entorno.

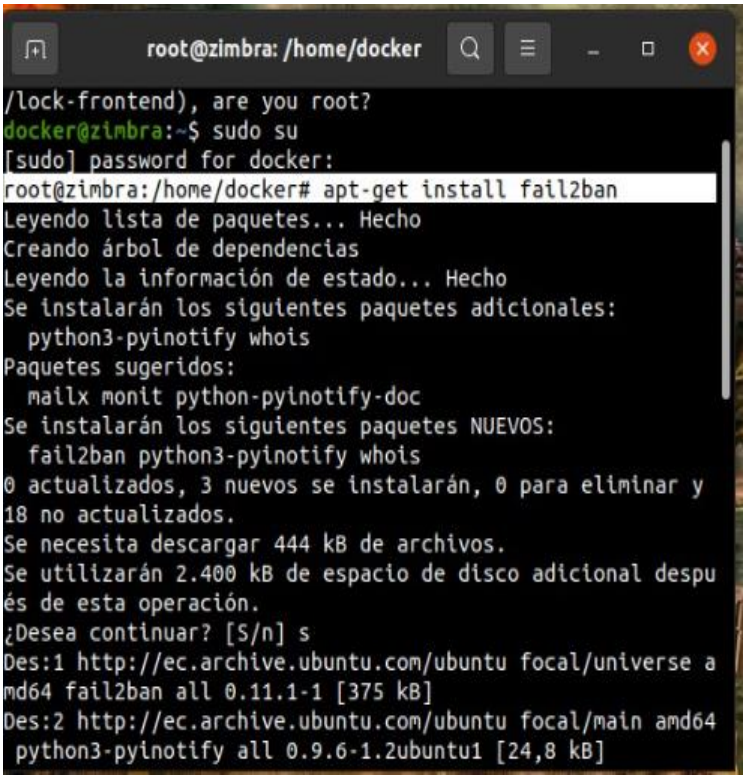
En el Ejército Ecuatoriano, Docker se utiliza para simplificar y optimizar la gestión de aplicaciones, facilitando despliegues rápidos y consistentes en diferentes entornos de servidores. Esto permite mejorar la eficiencia operativa y la escalabilidad de los sistemas tecnológicos utilizados por el ejército.

Instalación de la herramienta Fail2Ban en el servidor

Por tanto, como paso inicial en el fortalecimiento de la seguridad, se procederá a instalar y configurar Fail2Ban para mitigar riesgos asociados a ataques de fuerza bruta y otros ataques automatizados, garantizando así un entorno digital más robusto y protegido.

Figura 25

Instalación de fail2ban para monitoreo para detectar automáticamente a patrones de actividad sospechosa en los registros del servidor.



Ejecución de Fail2Ban en el servidor

Una vez completada la instalación de Fail2Ban en el servidor Ubuntu, se procede a verificar su funcionalidad mediante pruebas prácticas. Para ello, se empleará Putty como cliente de acceso remoto para establecer conexión con el servidor. A través de Putty, se introducirá deliberadamente una contraseña incorrecta durante el proceso de autenticación. De esta manera, se podrá evaluar la capacidad de Fail2Ban para detectar y responder a este tipo de comportamiento malicioso. Después del intento de acceso con contraseña incorrecta, se observará si Fail2Ban bloquea temporalmente la dirección IP del origen del intento, confirmando así que el sistema de seguridad está funcionando de manera efectiva. Este

procedimiento proporcionará la tranquilidad necesaria al saber que el servidor Ubuntu está protegido y que Fail2Ban está cumpliendo su función en la defensa contra posibles ataques.

Figura 26

Uso de PuTTY para tratar de acceder a el servidor.

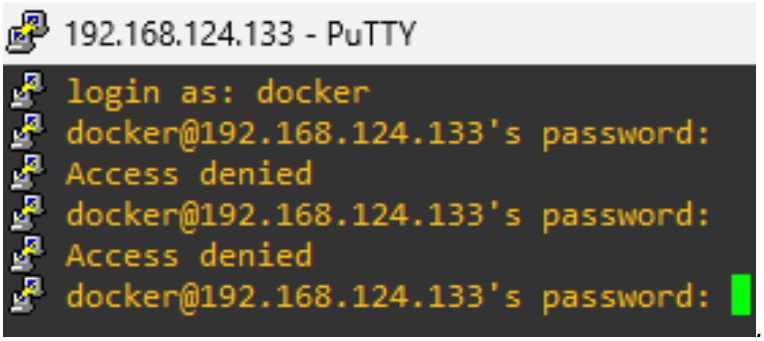
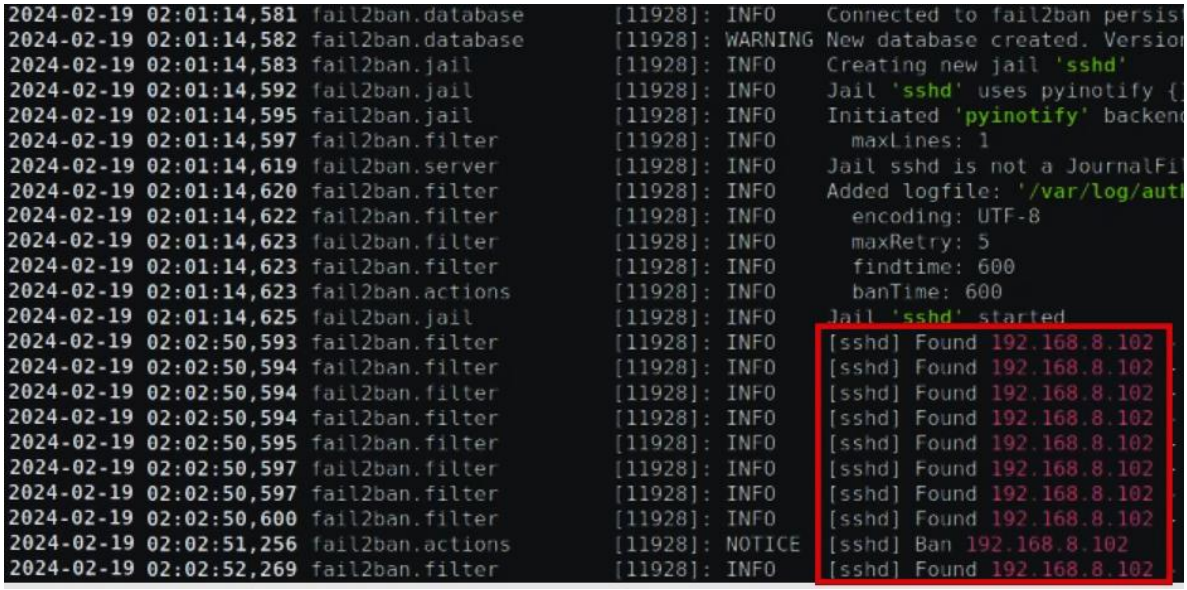


Figura27

Registro de la dirección IP que intento acceder al servidor mediante fail2ban.



Después de realizar una prueba controlada de acceso remoto utilizando Putty y una contraseña incorrecta, se ha verificado que Fail2Ban está funcionando correctamente en el servidor Ubuntu. Al ingresar la contraseña incorrecta, Fail2Ban detectó el comportamiento malicioso y tomó medidas inmediatas para mitigar el riesgo al bloquear temporalmente la

dirección IP del origen del intento. Esta respuesta automática demuestra la efectividad de Fail2Ban en la detección y respuesta ante intentos de acceso no autorizados, asegurando así la protección y la integridad del servidor contra posibles amenazas cibernéticas. Con la confirmación de que Fail2Ban está operando adecuadamente, se puede tener la confianza de contar con una capa adicional de seguridad para el entorno digital.

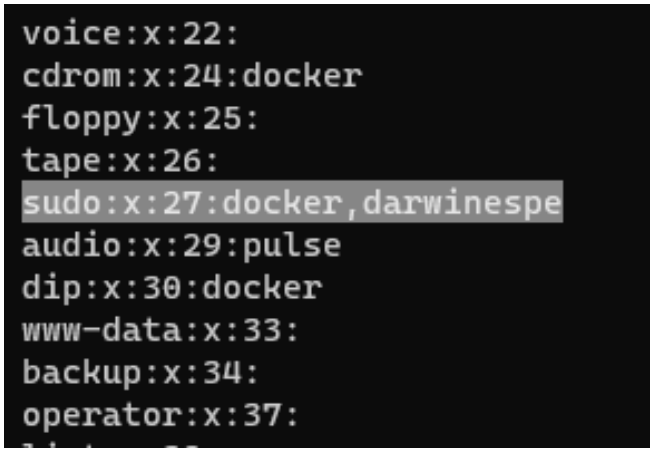
Privilegios de los Usuarios en el servidor

A continuación, se llevará a cabo el análisis de usuarios en el servidor, así como el seguimiento de sus actividades. Esto implica revisar las cuentas de usuario existentes para asegurar que tengan los permisos y recursos adecuados para sus tareas. También se prestará atención a las actividades de los usuarios, registrando y auditando sus acciones para garantizar la seguridad y cumplir con las políticas establecidas. Además, se implementarán restricciones de acceso y privilegios según sea necesario, limitando el acceso a recursos sensibles y proporcionando privilegios solo a aquellos usuarios que los requieran para realizar sus funciones.

Con el comando "nano /etc/group", se puede verificar la información sobre los grupos de usuarios en el sistema. Este archivo contiene detalles como los identificadores de grupo (GID) y los usuarios que pertenecen a cada grupo. Esto ayuda a administrar los permisos y privilegios de los usuarios en el sistema, permitiendo una gestión eficiente de los recursos y una configuración adecuada de los niveles de acceso.

Figura 28

Grupo de supe usuarios del servidor.

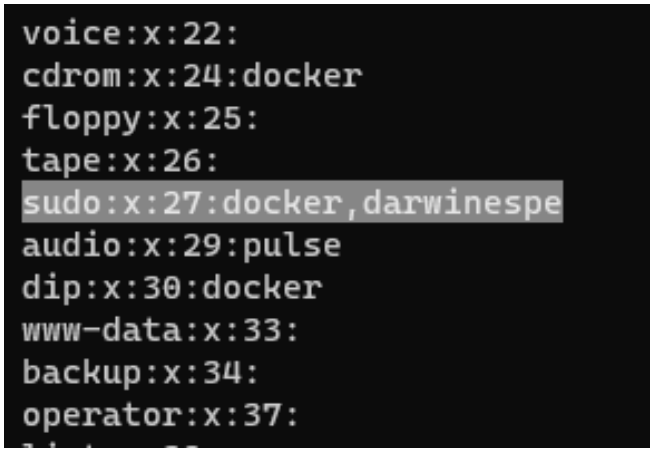


A continuación, se llevará a cabo el análisis de usuarios en el servidor, así como el seguimiento de sus actividades. Esto implica revisar las cuentas de usuario existentes para asegurar que tengan los permisos y recursos adecuados para sus tareas. También se prestará atención a las actividades de los usuarios, registrando y auditando sus acciones para garantizar la seguridad y cumplir con las políticas establecidas. Además, se implementarán restricciones de acceso y privilegios según sea necesario, limitando el acceso a recursos sensibles y proporcionando privilegios solo a aquellos usuarios que los requieran para realizar sus funciones. Este análisis y seguimiento permitirá mantener un entorno de computación seguro y bien administrado, protegiendo la integridad de los datos y asegurando un uso eficiente de los recursos del sistema.

Con el comando "nano /etc/group", se puede verificar la información sobre los grupos de usuarios en el sistema. Este archivo contiene detalles como los identificadores de grupo (GID) y los usuarios que pertenecen a cada grupo. Esto ayuda a administrar los permisos y privilegios de los usuarios en el sistema, permitiendo una gestión eficiente de los recursos y una configuración adecuada de los niveles de acceso.

Figura 29

Grupo de super usuarios del servidor.

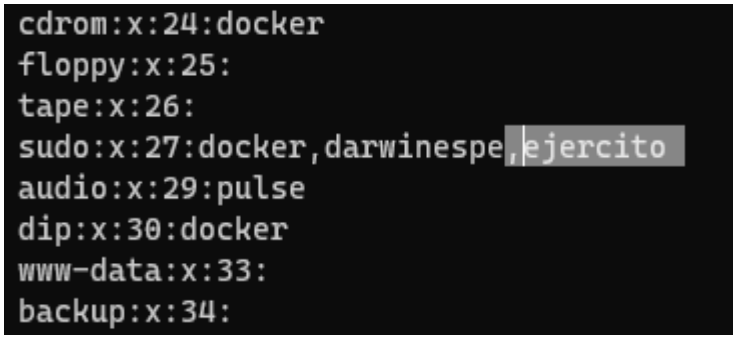


Como se puede evidenciar, existen dos usuarios establecidos como superusuarios en el sistema. Estos usuarios tienen acceso completo al sistema y pueden realizar cambios críticos que afectan a todo el sistema operativo, como instalar software, modificar configuraciones del sistema y administrar usuarios. En este caso, al realizar la hardenización del servidor, se ha tenido acceso a estos privilegios. Es importante gestionar cuidadosamente estos privilegios y limitar su acceso solo a usuarios autorizados para garantizar la seguridad y la integridad del sistema.

Para agregar otro superusuario en Ubuntu Server, se le asigna al grupo correspondiente utilizando la línea de comando. Esto implica agregar el nuevo usuario al grupo "sudo" para otorgarle los privilegios de superusuario. Esto permite que el nuevo usuario ejecute comandos con privilegios de superusuario al usar "sudo" antes de los comandos específicos.

Figura 30

Registro de un usuario con todos los privilegios.



De igual manera se puede agregar diferentes usuarios a otro grupo ellos cuales van a heredar los permisos que el mismo les asigne.

Grupos de trabajo para los usuarios

Figura 31

Asignación de usuario a un grupo de trabajo.

Los grupos de trabajo que encontramos son los siguientes:

- **root:x:0**: Este es el grupo del usuario root, el superusuario del sistema. Tiene el máximo nivel de privilegios y puede realizar cualquier acción en el sistema.
- **daemon:x:1:** Grupo asociado con los demonios del sistema, programas que se ejecutan en segundo plano y realizan tareas específicas del sistema. Tienen privilegios limitados y están destinados a ejecutar servicios del sistema.

- **bin:x:2:** Contiene usuarios que necesitan acceso a los ejecutables binarios del sistema. Es un grupo fundamental para la funcionalidad básica del sistema, pero sus privilegios son limitados.
- **sys:x:3:** Similar al grupo bin, pero se enfoca en los archivos del sistema y su configuración. Los usuarios en este grupo pueden acceder a recursos críticos del sistema, pero sus privilegios están restringidos.
- **adm:x:4**: Este grupo generalmente tiene acceso a los registros del sistema y a otras funciones administrativas. Puede leer ciertos archivos de registro y realizar otras tareas de administración, pero no tiene los mismos privilegios que el usuario root.
- **tty:x:5:** Usuarios en este grupo pueden acceder a terminales virtuales. Tienen permisos limitados y están restringidos a ciertas operaciones relacionadas con las terminales.
- **disk:x:6:** Este grupo tiene permisos para acceder a dispositivos de almacenamiento como discos duros y unidades USB. Puede montar y desmontar dispositivos de almacenamiento, pero no tiene privilegios de superusuario.
- **lp:x:7:** Grupo asociado con la administración de impresoras. Los usuarios en este grupo pueden administrar impresoras y enviar trabajos de impresión, pero no tienen acceso a funciones de administración del sistema.
- **mail:x:8:** Usuarios en este grupo pueden acceder y administrar correos electrónicos. Tienen permisos limitados relacionados con la administración de correo electrónico, pero no pueden realizar tareas de administración del sistema.
- **news:x:9**: Este grupo está relacionado con la gestión de noticias o grupos de noticias en el sistema. Los usuarios en este grupo pueden acceder y administrar noticias, pero sus privilegios están restringidos.
- **uucp:x:10:** Este grupo está relacionado con la comunicación entre computadoras a través de dispositivos seriales. Los usuarios en este grupo pueden realizar tareas

relacionadas con la comunicación de datos a través de puertos seriales, como la transferencia de archivos.

- **man:x:12:** Usuarios en este grupo tienen acceso a las páginas del manual del sistema. Pueden ver y consultar la documentación del sistema, pero no tienen privilegios de administración.
- **proxy:x:13:** Grupo asociado con la configuración de servidores proxy. Los usuarios en este grupo pueden configurar y administrar servidores proxy, pero sus privilegios están restringidos.
- **kmem:x:15:** Grupo que proporciona acceso a la memoria del kernel. Los usuarios en este grupo pueden acceder a ciertos recursos relacionados con la memoria del kernel, pero sus privilegios están restringidos para garantizar la seguridad del sistema.
- **dialout:x:20:** Usuarios en este grupo pueden acceder a dispositivos de comunicación como módems y puertos serie para realizar conexiones de marcado. Tienen permisos limitados relacionados con la comunicación de datos a través de dispositivos de marcado.
- **fax:x:21:** Grupo asociado con la configuración y administración de servicios de fax en el sistema. Los usuarios en este grupo pueden configurar y administrar servicios de fax, pero no tienen privilegios de superusuario.
- **voice:x:22:** Este grupo está relacionado con la administración de servicios de voz en el sistema. Los usuarios en este grupo pueden configurar y administrar servicios de voz, pero sus privilegios están restringidos.
- **cdrom:x:24**: Usuarios en este grupo tienen acceso a dispositivos de CD-ROM. Pueden montar y desmontar discos CD-ROM, pero sus privilegios están limitados a operaciones relacionadas con el CD-ROM.
- **floppy:x:25:** Grupo asociado con dispositivos de disquete. Los usuarios en este grupo

pueden acceder y realizar operaciones en dispositivos de disquete, pero sus privilegios están restringidos.

- **tape:x:26**: Este grupo proporciona acceso a dispositivos de cinta magnética. Los usuarios en este grupo pueden acceder y realizar operaciones en dispositivos de cinta magnética, pero sus privilegios están limitados.
- **sudo:x:27:** Grupo que permite a los usuarios ejecutar comandos con privilegios de superusuario utilizando el comando "sudo". Los usuarios en este grupo tienen permisos limitados para ejecutar ciertos comandos como superusuario.
- **audio:x:29:** Usuarios en este grupo tienen acceso a dispositivos de audio. Pueden reproducir y grabar audio, pero sus privilegios están limitados a operaciones relacionadas con el audio.
- **dip:x:30:** Este grupo está asociado con la administración de conexiones de acceso telefónico. Los usuarios en este grupo pueden configurar y administrar conexiones de acceso telefónico, pero sus privilegios están restringidos.
- **www-data:x:33**: Grupo asociado con el servidor web Apache. Los archivos y directorios del servidor web suelen ser propiedad de este grupo, que tiene permisos limitados para acceder y manipular archivos relacionados con el servidor web.
- **backup:x:34:** Este grupo está relacionado con las copias de seguridad del sistema. Los usuarios en este grupo pueden realizar operaciones de copia de seguridad y restauración, pero sus privilegios están limitados a tareas específicas de copia de seguridad.
- **operator:x:37:** Grupo que proporciona acceso a ciertas tareas de administración del sistema. Los usuarios en este grupo pueden realizar operaciones de administración, pero sus privilegios están restringidos y son más limitados que los del usuario root.
- **list:x:38:** Grupo asociado con la administración de listas de correo. Los usuarios en

este grupo pueden acceder y administrar listas de correo, pero sus privilegios están restringidos.

- **irc:x:39:** Este grupo está relacionado con la administración de servidores de chat IRC. Los usuarios en este grupo pueden configurar y administrar servidores de chat IRC, pero sus privilegios están limitados.
- **src:x:40:** Grupo que proporciona acceso a archivos fuente. Los usuarios en este grupo pueden acceder y modificar archivos fuente, pero sus privilegios están limitados a operaciones relacionadas con el desarrollo de software.
- **gnats:x:41:** Este grupo está asociado con el sistema de seguimiento de errores GNATS. Los usuarios en este grupo pueden acceder y administrar el sistema de seguimiento de errores, pero sus privilegios están restringidos.
- **shadow:x:42**: Grupo que proporciona acceso a archivos de contraseñas cifradas. Los usuarios en este grupo pueden acceder a los archivos de contraseñas cifradas, pero sus privilegios están limitados y están restringidos a ciertas operaciones relacionadas con la autenticación de usuarios.
- **utmp:x:43:** Grupo asociado con archivos de registro de sesiones de usuarios. Los usuarios en este grupo pueden acceder a los registros de sesiones de usuarios, pero sus privilegios están limitados y están restringidos a ciertas operaciones relacionadas con el seguimiento de sesiones de usuarios.
- **video:x:44**: Grupo que proporciona acceso a dispositivos de video. Los usuarios en este grupo pueden acceder y realizar operaciones en dispositivos de video, pero sus privilegios están limitados a operaciones relacionadas con el video.
- **sasl:x:45:** Este grupo está asociado con la autenticación y seguridad de correo electrónico. Los usuarios en este grupo pueden acceder y administrar servicios de autenticación SASL, pero sus privilegios están limitados.

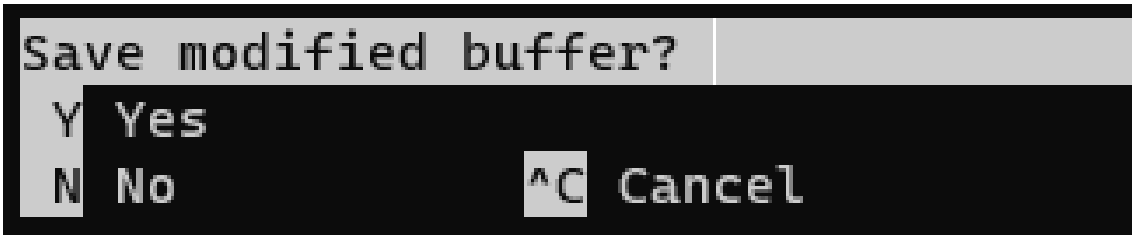
- **plugdev:x:46:** Grupo asociado con dispositivos externos que se conectan al sistema. Los usuarios en este grupo pueden acceder y realizar operaciones en dispositivos externos conectados al sistema, pero sus privilegios están limitados a operaciones relacionadas con la conexión de dispositivos.
- **staff:x:50:** Grupo que proporciona acceso a ciertas tareas administrativas y de desarrollo. Los usuarios en este grupo tienen privilegios adicionales en comparación con los usuarios normales, pero no tienen privilegios de superusuario.
- **games:x:60:** Este grupo está relacionado con la administración de juegos en el sistema. Los usuarios en este grupo pueden acceder y administrar juegos instalados en el sistema, pero sus privilegios están restringidos.
- **users:x:100:** Grupo que incluye a todos los usuarios normales del sistema. Los usuarios en este grupo tienen permisos básicos para acceder y utilizar recursos del sistema, pero no tienen privilegios de superusuario.
- **nogroup:x:65534:** Este grupo se utiliza como un grupo de "ningún grupo" o "ninguna asociación". Los archivos o recursos que no tienen un grupo asignado a menudo se asignan a este grupo.
- **systemd-journal:x:101**: Grupo asociado con el registro del sistema a través de systemd. Los usuarios en este grupo pueden acceder y administrar los registros del sistema registrados por systemd.
- **systemd-network:x:102:** Grupo relacionado con la administración de la red a través de systemd. Los usuarios en este grupo pueden acceder y administrar la configuración de red controlada por systemd.
- **systemd-resolve:x:103**: Grupo asociado con la resolución de nombres a través de systemd. Los usuarios en este grupo pueden acceder y administrar la resolución de nombres controlada por systemd.

- **systemd-timesync:x:104:** Grupo relacionado con la sincronización de tiempo a través de systemd. Los usuarios en este grupo pueden acceder y administrar la sincronización de tiempo controlada por systemd.
- **crontab:x:105**: Grupo asociado con el uso del servicio cron para programar tareas. Los usuarios en este grupo pueden acceder y administrar las tareas programadas a través de cron.
- **messagebus:x:106:** Grupo asociado con el servicio de bus de mensajes en el sistema. Los usuarios en este grupo pueden acceder y utilizar el servicio de bus de mensajes para la comunicación entre aplicaciones.
- **input:x:107:** Grupo asociado con dispositivos de entrada como teclados y ratones. Los usuarios en este grupo pueden acceder y utilizar dispositivos de entrada en el sistema.
- **kvm:x:108:** Grupo asociado con la virtualización de Kernel-based Virtual Machine (KVM). Los usuarios en este grupo pueden acceder y utilizar funciones relacionadas con la virtualización KVM en el sistema.

Después de asignar usuarios a los diversos grupos de trabajo, se debe guardar las configuraciones realizadas. Esto asegura que los cambios realizados se reflejen en el sistema incluso después de reiniciar o actualizar. En entornos de sistemas basados en Unix, como Ubuntu Server, las configuraciones se almacenan en archivos de configuración específicos. Este proceso es crucial para asegurar la coherencia y la integridad de las configuraciones del sistema, así como para mantener la seguridad y la eficiencia en la gestión de usuarios y grupos.

Figura 32

Almacenar configuraciones realizadas.

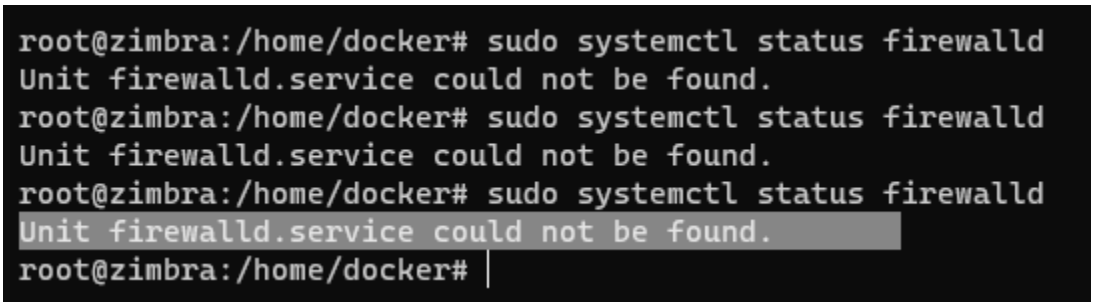


Instalación de firewall para el servidor

Continuando con la hardenización, se ha observado que el servidor carece de FirewallD, una herramienta de firewall dinámico empleada en sistemas operativos basados en Linux, como Ubuntu. Este software actúa como un firewall de red que regula y supervisa el tráfico entrante y saliente en una computadora o red. FirewallD simplifica la gestión del firewall al permitir la configuración mediante perfiles predefinidos que establecen reglas de filtrado de paquetes para diversos niveles de seguridad y necesidades de uso. Esta característica facilita a los usuarios la configuración de reglas de firewall sin tener que redactar reglas de iptables complicadas manualmente. En resumen, FirewallD añade una capa adicional de seguridad al controlar qué tipo de tráfico se permite pasar a través del sistema y cómo se gestiona.

Figura 33

Inexistencia de FirewallD en el servidor.



Para reforzar la seguridad en el servidor con Ubuntu Server 20.04, se procederá con la instalación y configuración de FirewallD. Al implementar FirewallD, se podrán establecer

políticas de filtrado de paquetes que gestionen el tráfico de red entrante y saliente, permitiendo únicamente las conexiones esenciales y bloqueando aquellas que representen posibles riesgos para la integridad y la confidencialidad de los datos. Esta medida fortalecerá significativamente la defensa del servidor frente a posibles ataques externos, proporcionando un entorno más seguro y protegido para las operaciones críticas en la red.

Figura 34

Instalación de FirewallD.

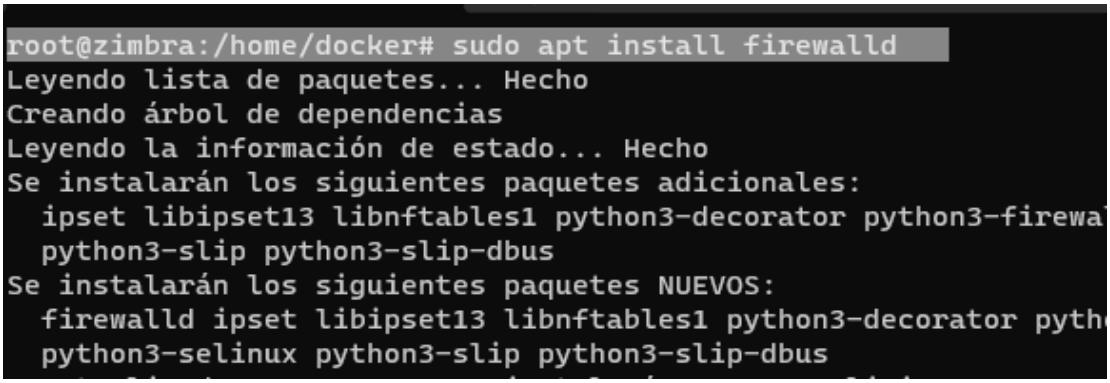
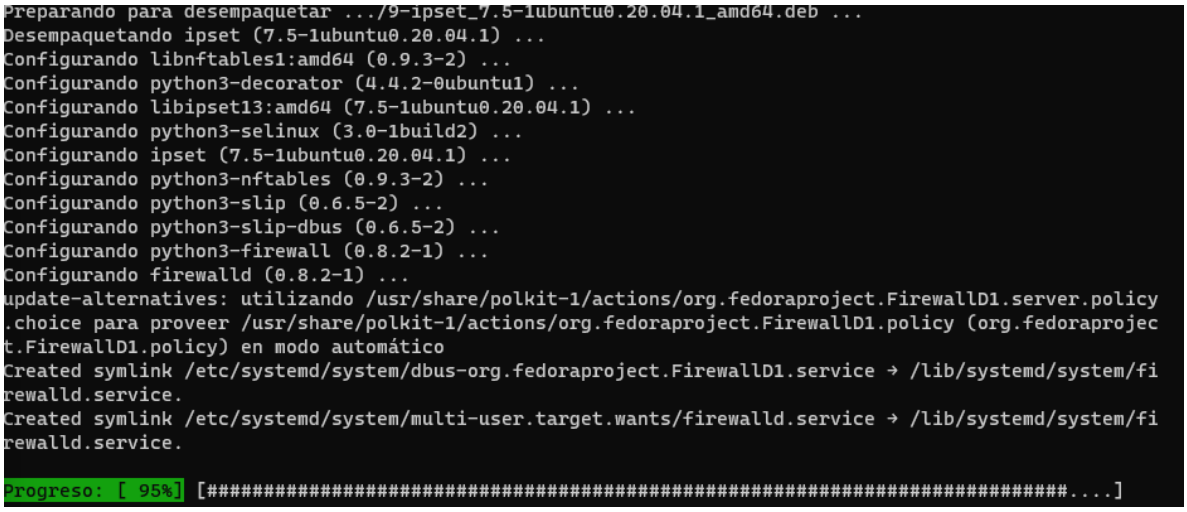


Figura 35

Progreso de la Instalación.

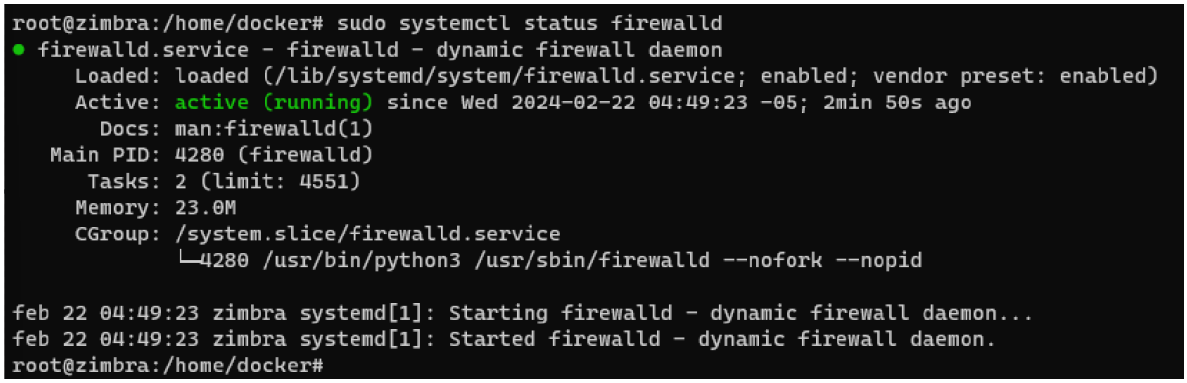


Una vez instalada el FirewallD se verifica su estado de funcionamiento

Funcionamiento del firewall en el servidor

Figura 36

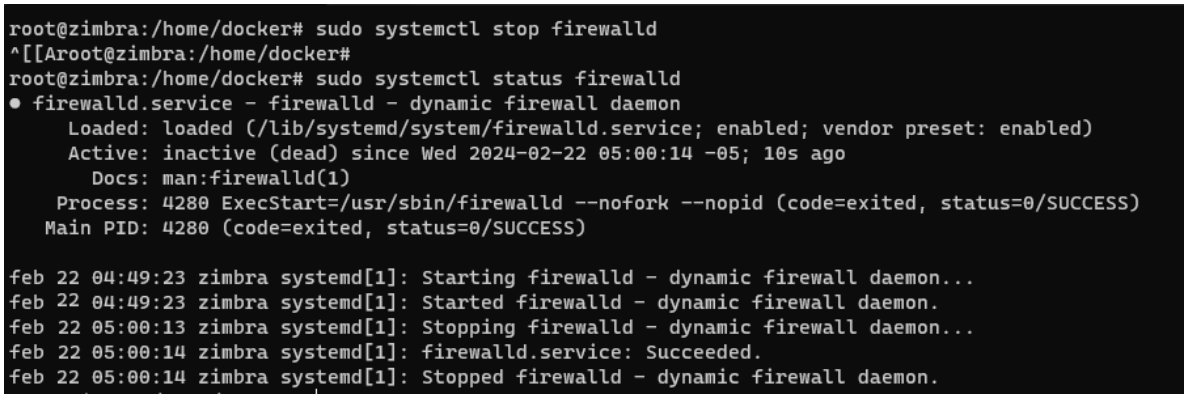
Servicio activo y en ejecución.



En ocasiones, debido a labores de mantenimiento y configuración en los sistemas, es necesario detener temporalmente el servicio de FirewallD en el servidor Ubuntu. Esta acción permite realizar ajustes y cambios en la configuración del firewall sin interferencias, facilitando la implementación de actualizaciones de software, la resolución de problemas o la realización de tareas de mantenimiento planificadas. Sin embargo, es importante recordar que al detener el FirewallD, se expone momentáneamente el sistema a posibles amenazas externas, por lo que se debe realizar esta acción de manera consciente y bajo medidas de seguridad adicionales si es necesario. Una vez completadas las labores de mantenimiento requeridas, se recomienda reiniciar el servicio de FirewallD para restaurar la protección y mantener la seguridad del servidor. Esta acción se realizará con el comando **"sudo systemctl stop firewalld".**

Figura 37

*Detención del FirewallD***.**



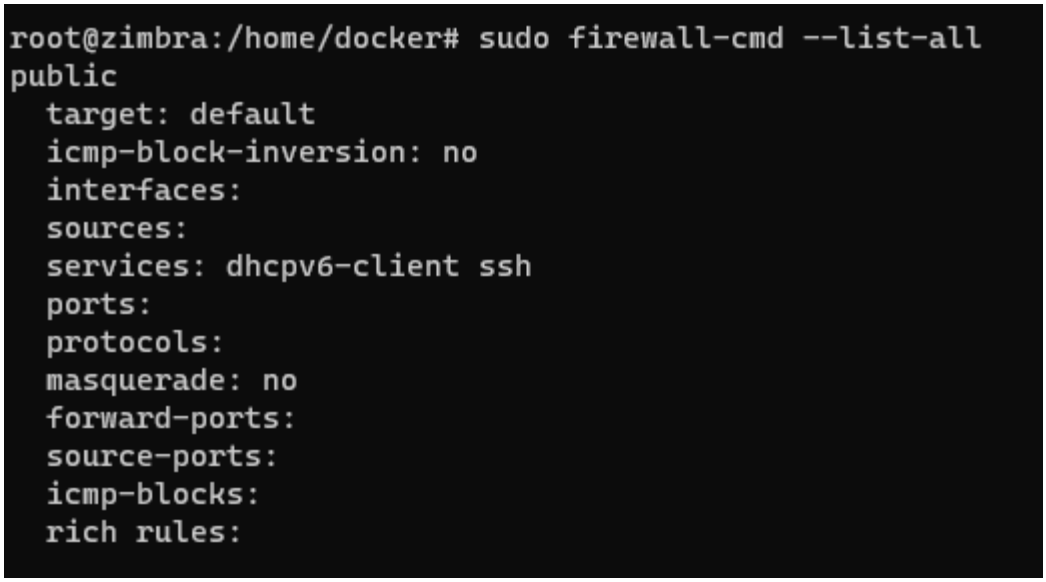
Reglas del firewall

FirewallD tiene reglas que son directivas que especifican cómo debe gestionarse el tráfico de red en un sistema Ubuntu Server. Estas reglas determinan qué tipo de conexiones se permiten y cuáles se bloquean, brindando un control preciso sobre la seguridad de la red. Las reglas pueden configurarse para permitir el acceso a servicios específicos, como HTTP, SSH o DNS, desde determinadas direcciones IP o rangos de direcciones, mientras se bloquea el acceso no autorizado. Además, es posible establecer reglas de reenvío de puertos para redireccionar el tráfico desde un puerto externo a uno interno, así como crear reglas de NAT para traducir direcciones IP y puertos.

Las reglas que tiene después de instalar FirewallD son las siguientes:

Figura 38

Reglas del FirewallD.



- **Target (Objetivo):** "default" indica que estas reglas se aplicarán al comportamiento predeterminado del firewall.
- **icmp-block-inversion (Inversión de bloqueo ICMP):** "no" significa que no se aplicará ninguna inversión al bloquear los mensajes ICMP. Esto implica que los mensajes ICMP estarán bloqueados según lo especificado en las reglas.
- **Interfaces:** No se especifica ninguna interfaz, lo que significa que estas reglas se aplicarán a todas las interfaces de red del sistema.
- **Sources (Orígenes):** No se especifica ningún origen, por lo que estas reglas se aplicarán a todo el tráfico, independientemente de su origen.
- **Services (Servicios):** Se permitirá el tráfico asociado con los servicios DHCPv6-client y SSH.
- **Ports (Puertos):** No se especifican puertos individuales para permitir o bloquear.
- **Protocols (Protocolos):** No se especifican protocolos individuales para permitir o bloquear.

- **Masquerade:** "no" indica que no se habilitará el masquerade, que es una técnica de red para ocultar la dirección IP de origen de los paquetes salientes.
- **Forward-ports (Reenvío de puertos):** No se especifican puertos para reenviar.
- **Source-ports (Puertos de origen):** No se especifican puertos de origen.
- **icmp-blocks (Bloqueo de ICMP):** No se especifican bloqueos de mensajes ICMP.
- **Rich rules (Reglas ricas):** No se especifican reglas ricas adicionales. Las reglas ricas son reglas de firewall más avanzadas que permiten una mayor flexibilidad en el control del tráfico de red.

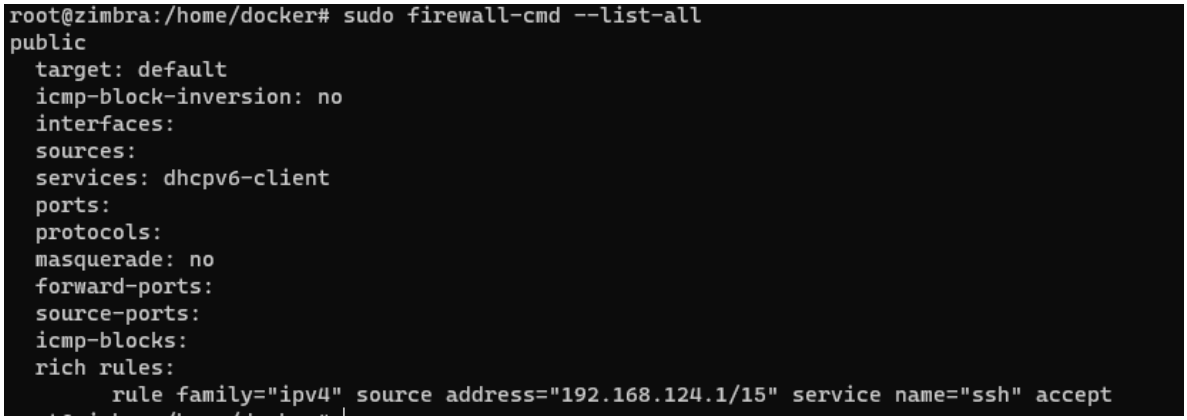
Configuración de acceso remoto al servidor

Por solicitud de las DTIC, se ha establecido que el acceso remoto al servidor debe limitarse a un rango específico de direcciones IP. En respuesta a esta petición, se realiza la configuración de estas restricciones en el servidor Ubuntu. Esto garantizará que solo las direcciones IP autorizadas dentro del rango designado puedan acceder al servidor de forma remota, aumentando así la seguridad de nuestros sistemas.

Para implementar esta restricción de acceso remoto basada en un rango de direcciones IP específico, se utiliza reglas enriquecidas o "rich rules" en nuestro servidor Ubuntu. Estas reglas avanzadas permiten definir con precisión los criterios de filtrado del tráfico de red. Para la cual se emplea el comando: **“sudo firewall-cmd –permanent –add-rich-rule= 'rule family=ipv4 source addres=192.168.124.1/15 service name=ssh accept '”.** De esta manera el servidor será mucho más seguro al momento de tener accesos remotos

Figura 39

Rich Rule para SSH.

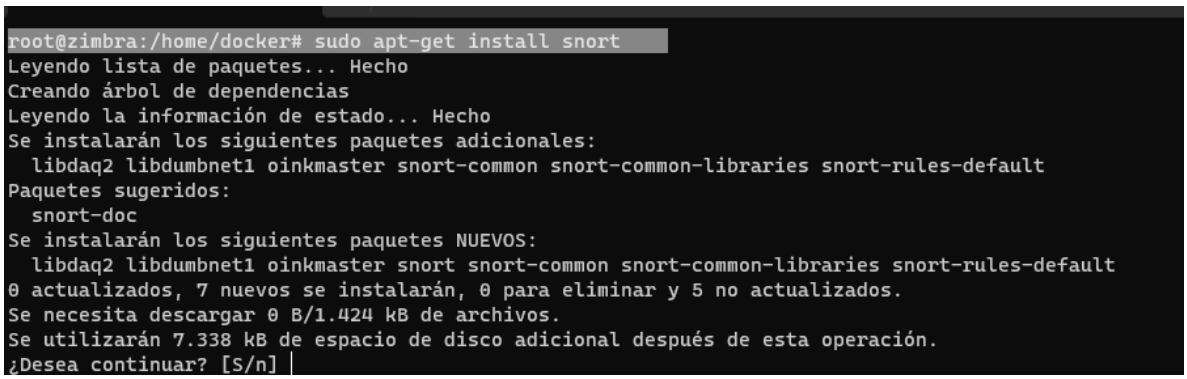


Instalación de la herramienta Snort en el servidor

Después de completar la configuración de las reglas de filtrado avanzadas para SSH en el servidor, el siguiente paso es instalar Snort para la detección de intrusos. Snort, como un sistema de detección de intrusos en red (IDS), jugará un papel vital en la protección proactiva de la infraestructura contra posibles amenazas y actividades maliciosas. Al implementar Snort, se fortalecerán aún más las defensas de la red al monitorear de manera activa y detectar patrones de tráfico sospechoso o comportamientos inusuales, brindando así una capa adicional de seguridad para los sistemas y datos críticos del servidor.

Figura 40

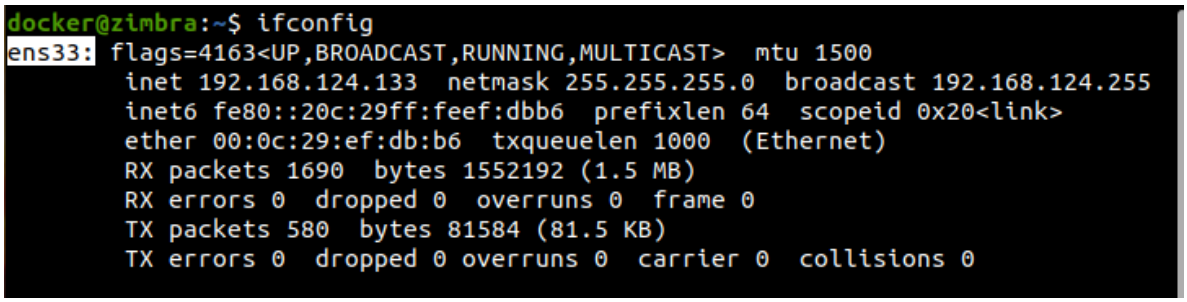
Instalación de Snort.



Para continuar con la configuración debemos agregar la interfaz la cual se verifica con el comando “**ifconfig”,** dando como resultado en este caso la interfaz: ens33

Figura 41

Verificación de interfaz del servidor.



Configuración de la herramienta Snort en el servidor

Figura 42

Configuración de snort con la interfaz ens33.

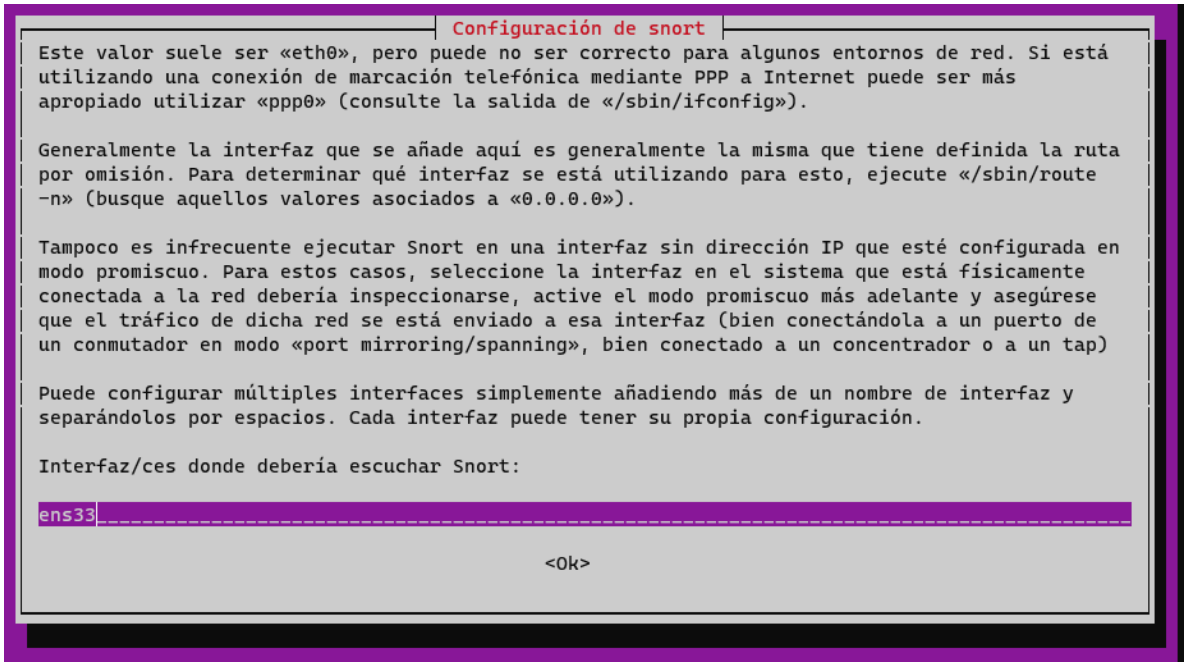
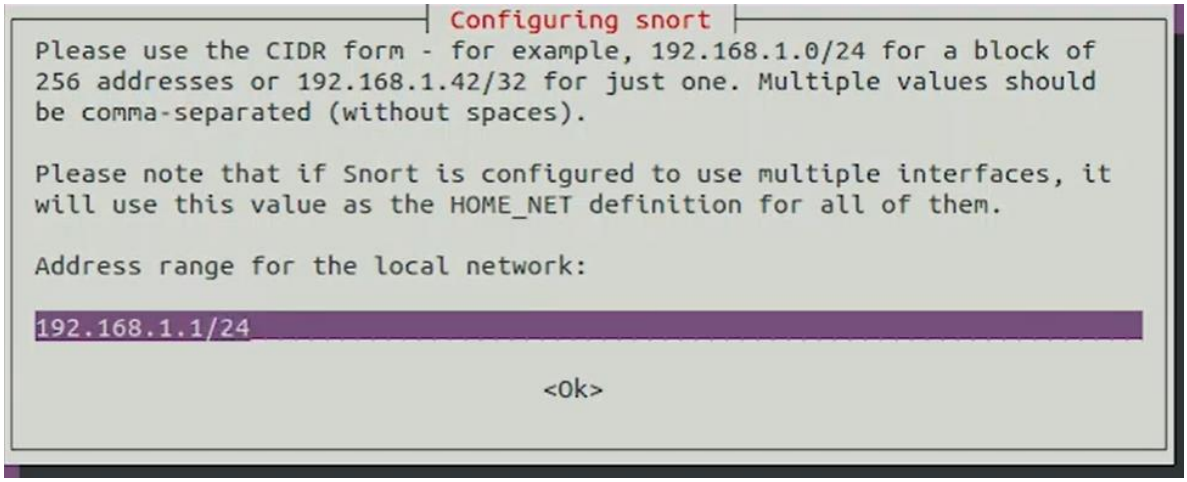


Figura 43

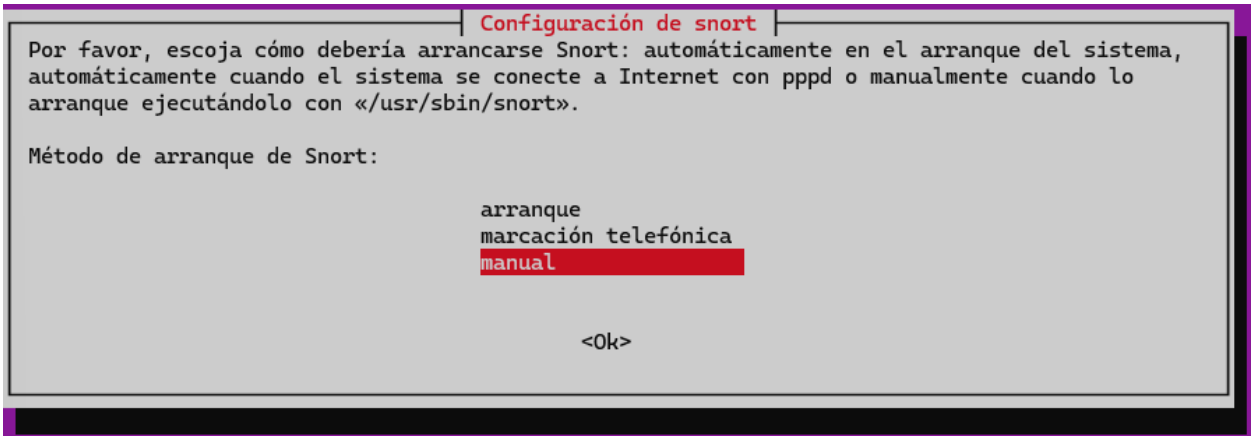
Asignación de rango de direcciones IP.



Una vez instalado en el servidor se procede a la reconfiguración de los paquetes de snort mediante el comando **“dpkg-reconfigure snort”**, y nuestra configuración será de modo manual

Figura 44

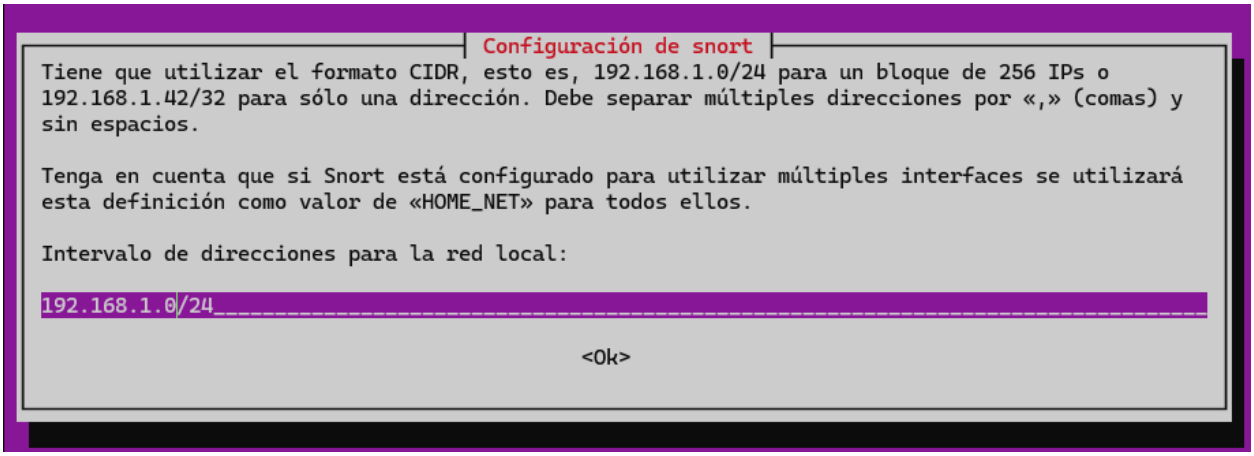
Reconfiguración inicial de snort.



Se debe seguir laa las recomendaciones de snort

Figura 45

Formato CIDR.



Una vez llegada al apartado de configuración sobre el reporte diarios de snort, daremos en aceptar para que llegue la información al mail asignado, al cual asignaremos el correo institucional del departamento de seguridad de las DTIC.

Figura 46

Aceptación de resúmenes mediante email.

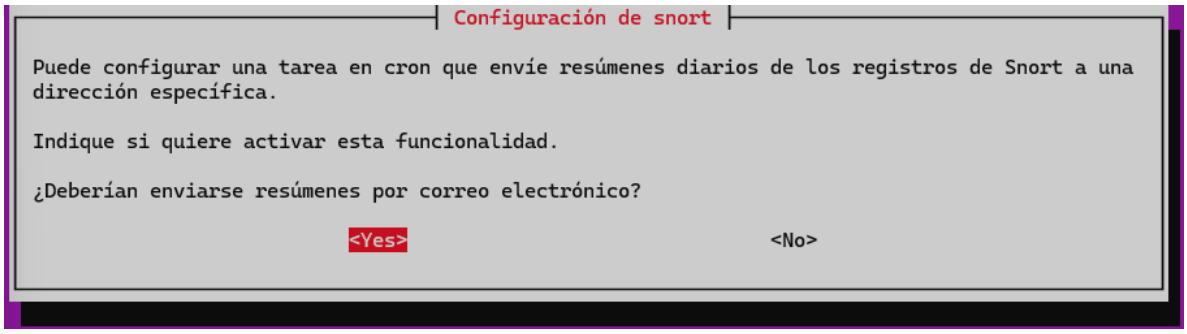
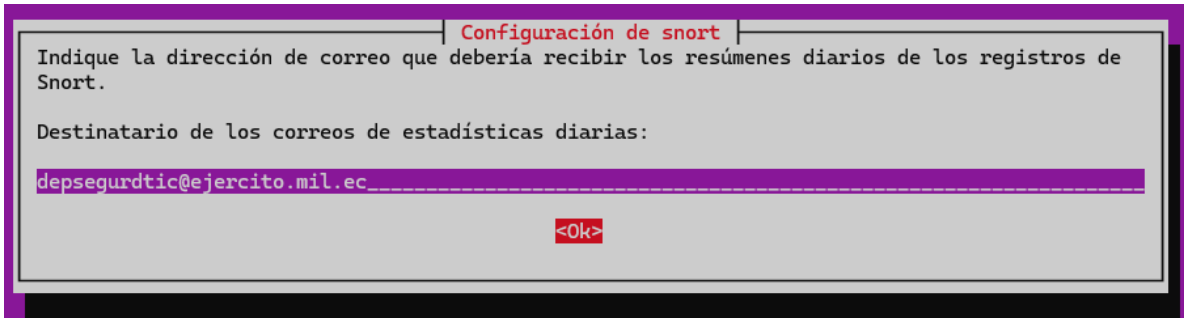


Figura 47

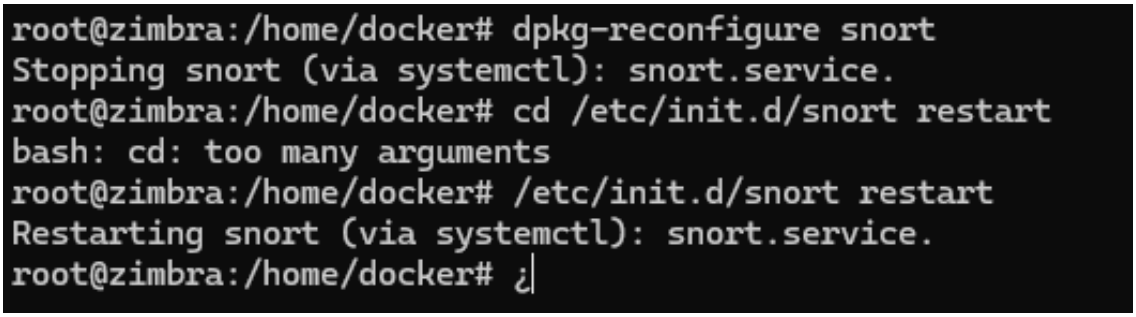
Asignación de email.



Posterior a esta configuración se debe reiniciar snort

Figura 48

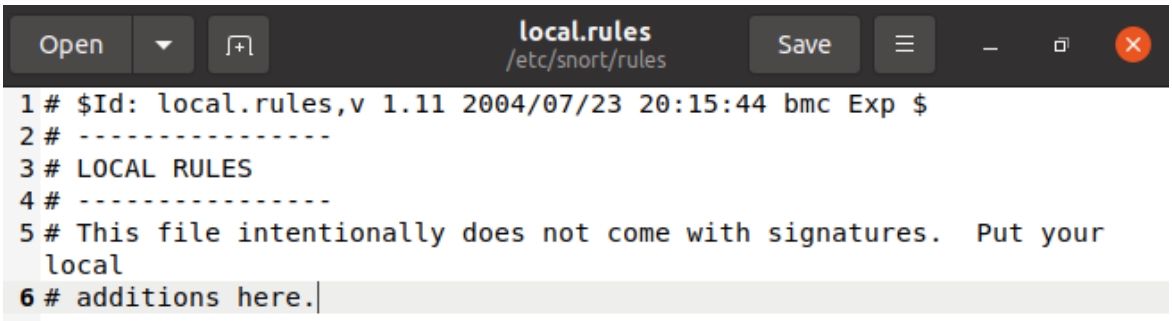
Reinicio del software.



Una vez reiniciado snort, abrimos un archivo el cual define las reglas, que especifican qué tipos de tráfico de red deben ser detectados y cómo deben ser manejados.

Figura 49

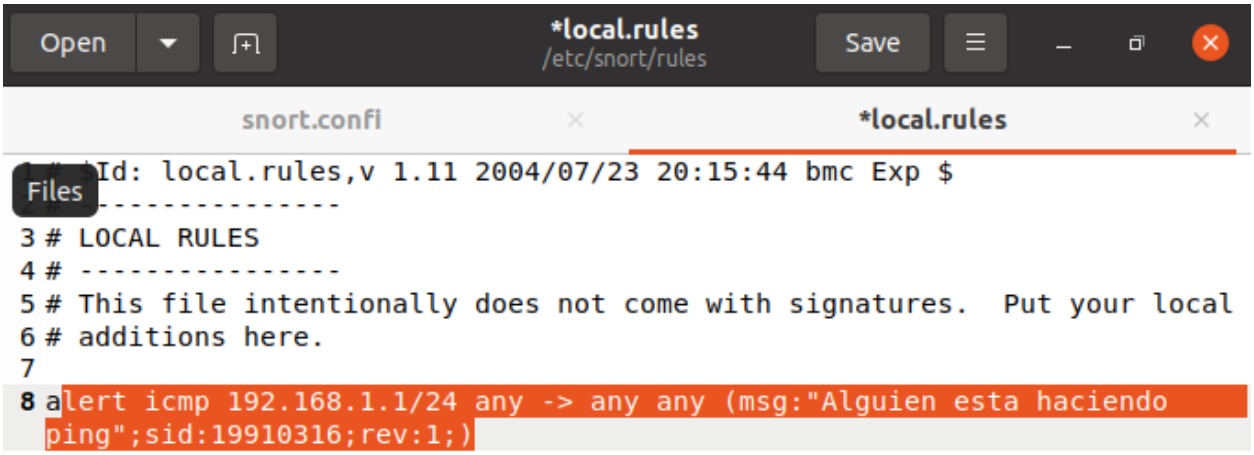
Archivo para determinar reglas.



En el archivo agregamos una nueva regla que contiene el protocolo ICMP, el cual nos dará un mensaje de alerta cuando se detecte un ping no autorizado. Y procedemos a guardarlas

Figura 50

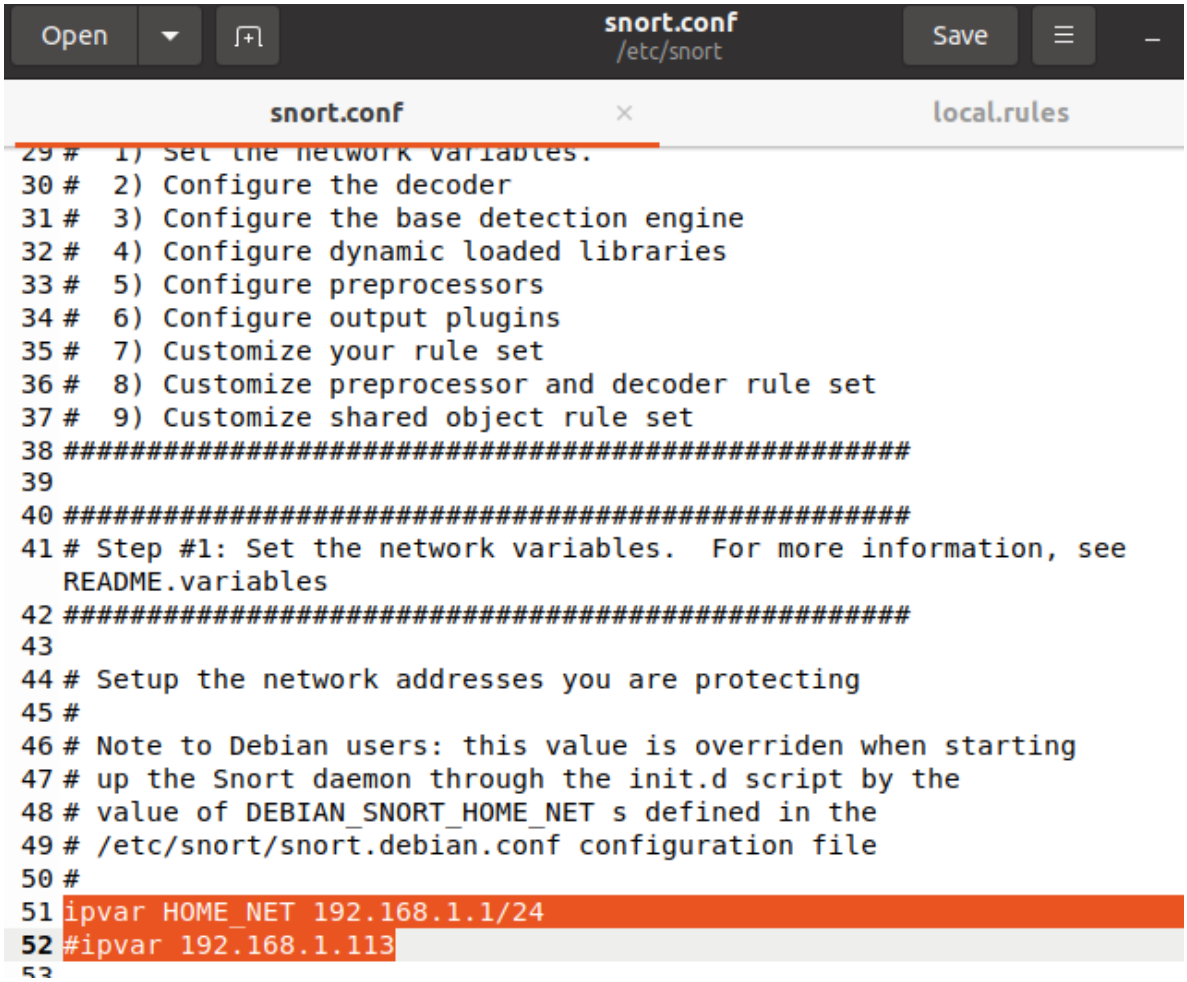
Ingreso de una nueva regla.



Posterior a esto se procede a configurar la regla ipvar. Estas líneas de configuración en un archivo de configuración de un sistema de detección de intrusiones definen la variable HOME_NET, que representa la red, asignándole un rango de direcciones IP específico. Para ello usamos el comando **"gedit /etc/snort/snort.conf".**

Figura 51

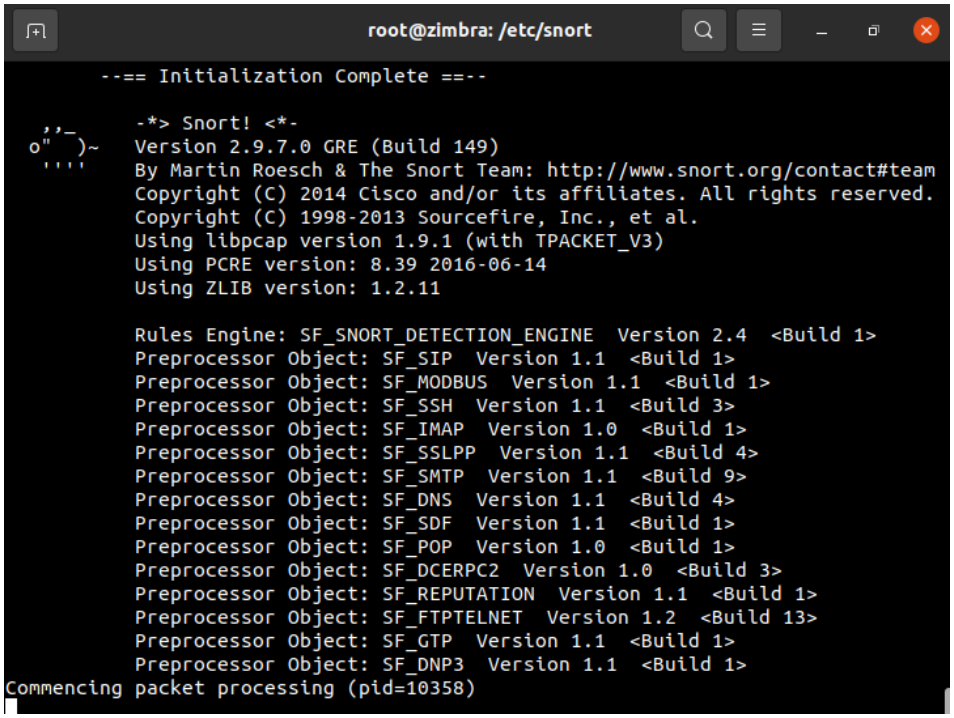
Asignación de rango de direcciones IP.



Una vez guardad la última configuración, se debe utilizar el siguiente comando **“snort -A console -c snort.conf -i ens33**”, este comando inicia Snort y lo configura para mostrar alertas en la consola en tiempo real, utilizando el archivo de configuración "snort.conf" y escuchando el tráfico en la interfaz de red "ens33".

Figura 52

Inicio de snort.



Para verificar su funcionamiento, se realiza un ping al servidor desde otro ordenador que este en el mismo segmento de red, para ello se verifica la IP del servidor

Figura 53

Verificación IP del servidor.

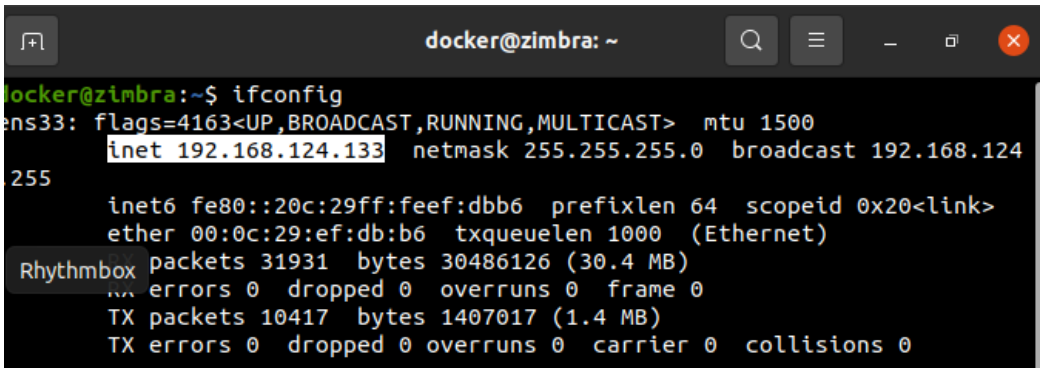
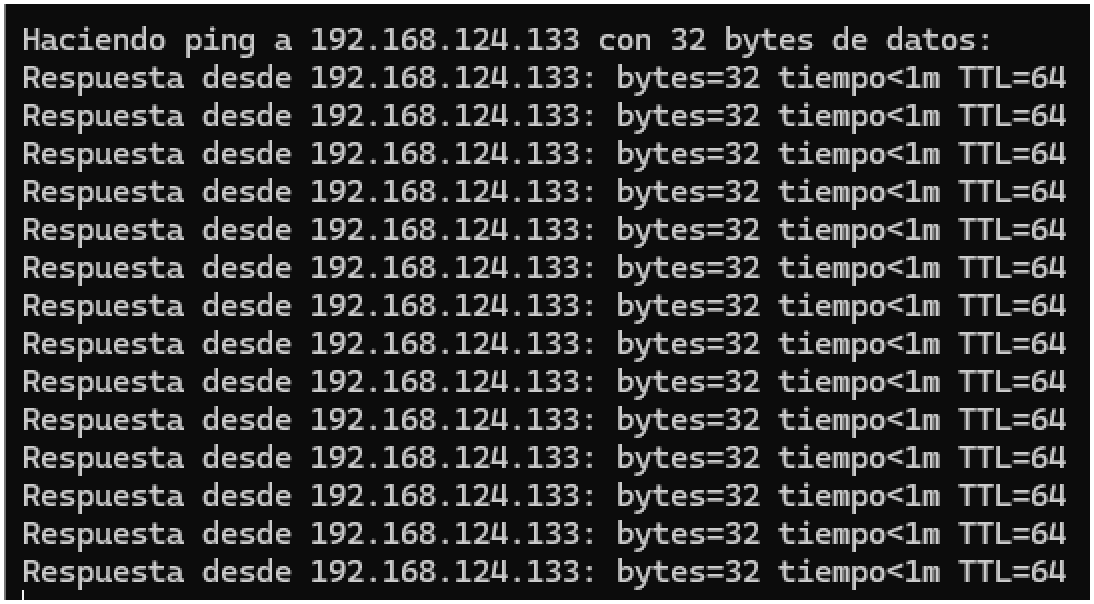


Figura 54

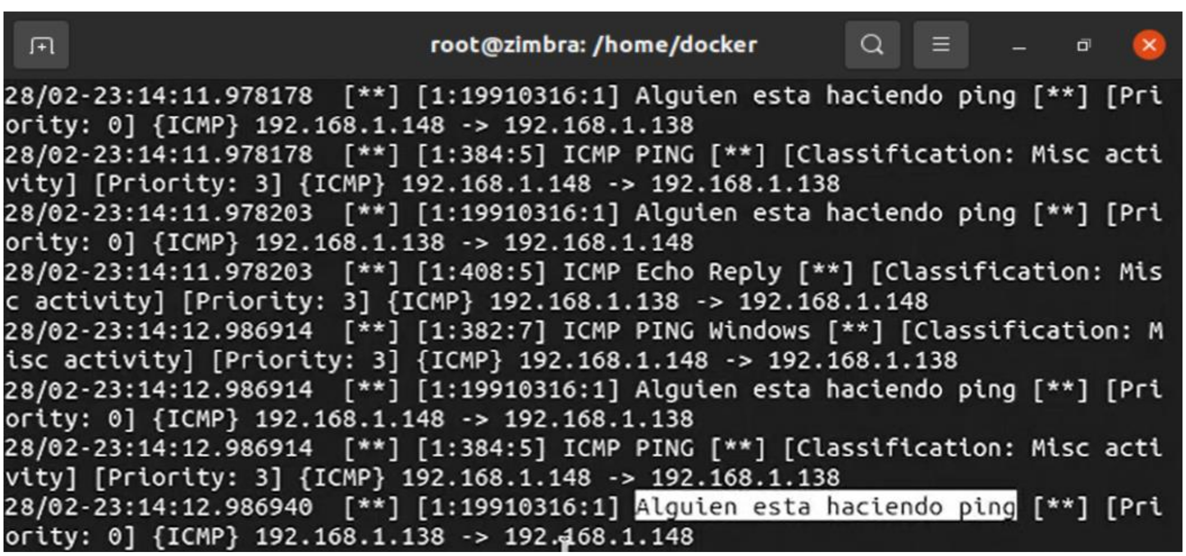
Ping al servidor desde CMD.



Y como resultado se obtiene la detección de un ping externo hacia el servidor mediante el mensaje previamente configurado en la figura 24.

Figura 55

Registro de ping en el servidor Ubuntu mediante el software snort.



Snort y Fail2ban son dos herramientas ampliamente utilizadas en la seguridad de redes, aunque difieren en sus enfoques y funcionalidades. Snort es un sistema de detección de intrusiones (IDS) de código abierto que se centra en analizar el tráfico de red en busca de patrones de comportamiento malicioso o ataques conocidos. Utiliza reglas predefinidas para identificar y alertar sobre posibles amenazas en tiempo real. Por otro lado, Fail2ban es una herramienta de prevención de intrusiones que se enfoca en proteger servicios específicos, como SSH o HTTP, contra ataques de fuerza bruta mediante la monitorización de registros de registro y la prohibición automática de direcciones IP que muestran comportamientos sospechosos. Como se demostró anteriormente mientras Snort se centra en la detección de intrusiones en la capa de red, Fail2ban se enfoca en proteger servicios específicos a nivel de aplicación.

Capítulo IV

Conclusiones y Recomendaciones

Conclusiones

- Se ha llevado a cabo una exhaustiva investigación sobre los diversos mecanismos y herramientas disponibles para proporcionar seguridad a los servidores de datos. Este análisis permitió una comprensión profunda de que la instalación y uso combinado de Snort y Fail2Ban en el servidor de la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre (DTIC) en Quito proporciona una estrategia integral y efectiva para fortalecer la seguridad y protección de la red.

- A través de la investigación bibliográfica y el análisis de las mejores prácticas en seguridad informática, se identificó que, por un lado, Snort, con su capacidad para detectar y alertar sobre actividades maliciosas en tiempo real mediante reglas de detección de intrusos basadas en firmas, protocolos y comportamientos de red, ofrece una defensa proactiva contra una amplia gama de amenazas cibernéticas. Esto permite a los administradores de sistemas identificar y responder rápidamente a posibles ataques, protegiendo así los datos críticos y la infraestructura de la red contra intrusiones no autorizadas. Por otro lado, Fail2Ban complementa la seguridad del servidor al monitorear activamente los registros del sistema en busca de patrones de actividad maliciosa, como intentos de acceso fallidos o ataques de fuerza bruta. Al bloquear automáticamente direcciones IP sospechosas que intentan acceder al servidor de forma no autorizada, Fail2Ban reduce significativamente el riesgo de

comprometer la seguridad del sistema y protege la integridad de los datos almacenados en el servidor.

- Se llevaron a cabo pruebas para evaluar el funcionamiento de los mecanismos de seguridad implementados durante el proceso de hardenización. Además, se elaboró un manual de usuario detallado para proporcionar orientación sobre la configuración, uso y mantenimiento de estos mecanismos. Esto garantiza que el personal esté capacitado para utilizar eficazmente las medidas de seguridad implementadas y que se asegure su correcto funcionamiento a lo largo del tiempo.

Recomendaciones

- Durante el proceso de hardenización, es importante documentar cada paso realizado, incluyendo la configuración de los mecanismos de seguridad, las pruebas realizadas y los resultados obtenidos. Esta documentación servirá como referencia futura y facilitará la elaboración del manual de usuario.

- Antes de implementar los mecanismos de seguridad en el servidor de producción, es recomendable realizar pruebas en entornos controlados, como laboratorios de pruebas o servidores de pruebas. Esto permite evaluar el rendimiento y la efectividad de los mecanismos de seguridad en un ambiente seguro y sin riesgos para la información crítica.

- Durante el análisis de los diferentes mecanismos, herramientas y protocolos de seguridad, es importante asegurarse de utilizar fuentes confiables y actualizadas de información. Esto incluye investigar en libros, revistas especializadas, documentos técnicos y sitios web de organizaciones de seguridad reconocidas.

Bibliografía

Aleph. (Marzo de 2021). *¿Qué es un spyware adware y spam?* Obtenido de https://aleph.org.mx/que- es-un-spyware-adware-y-spam

Altube, R. (Noviembre de 2021). *Qué es y características principales. .* Obtenido de Kali Linux: https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/

Áreatecnológica. (2022). *Redes Informáticas.* Obtenido de https://www.areatecnologia.com/redes- informaticas.htm

Bello, E. (Octubre de 2022). *Conoce las herramientas de ciberseguridad para proteger tu empresa. .* Obtenido de https://www.iebschool.com/blog/herramientas-ciberseguridad-digital-business/

Caiza. (Marzo de 2019). *Diseño de un proceso de hardening para servidores.* Obtenido de https://repositorio.uisek.edu.ec/bitstream/123456789/3346/1/TESIS_AnaCaiza.pdf

Cámara Valencia. (noviembre de 2018). *Qué es un ciberataque y qué tipos existen. .* Obtenido de https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y- que-tipos-existen/#Malware

Castellnou, R. (Mayo de 2021). *Las herramientas de seguridad informatica que protegerán tu empresa. .* Obtenido de https://www.captio.net/blog/herramientas-seguridad-informatica

Ciberseguridad, R. d. (01 de Marzo de 2024). *Modelo ecuatoriano de gobernanza en ciberdefensa.* Obtenido de https://revistas.flacsoandes.edu.ec/urvio/article/download/2571/2105?inline=1

CISCO. (2019). *Protocolos y comunicación de red.* Obtenido de https://www.uv.mx/personal/angelperez/files/2019/02/CCNA_ITN_Chp3.pdf

Cisco. (2022). *Red de Área Metropolitana.* Obtenido de http://ciscoredes.mex.tl/frameset.php?url=/1950700_MAN---RED-DE--REA-METROPOLITANA-.html

Cisco. (2022). *Red de Área Metropolitana.* Obtenido de http://ciscoredes.mex.tl/frameset.php?url=/1950700_MAN---RED-DE--REA-METROPOLITANA-.html

CISCO. (Marzo de 2022). *¿Qué es la ciberseguridad?* Obtenido de https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html#~tipos-de-amenazas

Cloudflare. (2022). *¿Qué es el modelo OSI? .* Obtenido de https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/

Cruz, O. (2017). *Procso de Hardening de servidores.* Obtenido de file:///C:/Users/USER/Documents/TESIS/cruzoscar2017.pdf

De Luz, S. (05 de Octubre de 2022). *Qué son, tipos y para qué sirven.* Obtenido de VLANs:https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

Digicert. (s.f.). *¿En qué consisten el malware, los virus, el spyware y las cookies?* Obtenido de 2017: https://www.websecurity.digicert.com/es/es/security-topics/what-are-malware-viruses- spyware-and-cookies-and-what-differentiates-them

DTIC. (Marzo de 2024). *Dirección de Tecnologías de la Información y Comunicaciones.* Obtenido de https://www.ccffaa.mil.ec/direccion-de-tecnologias-de-la-informacion-y-comunicaciones/

Edu.ec., U. T. (Marzo de 2024). *De la seguridad informática.* Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/29958/1/Tesis_1606msi.pdf

Educa Sistemas. (Mayo de 2018). *Interacción de Protocolos.* Obtenido de https://educasistemas.wordpress.com/2017/05/18/interaccion-de-protocolos/

Fernández, Y. (Junio de 2020). Obtenido de https://www.xataka.com/basics/cual-es-la-diferencia- malware-virus-gusanos-spyware-troyanos-ransomware-etcetera

G4s. (Noviembre de 2020). *¿qué son los spyware y adware?* Obtenido de https://www.g4s.com/es

González. (Octubre de 2018). *Qué es un ciberataque y qué tipos existen.* Obtenido de https://ayudaleyprotecciondatos.es/2018/10/08/ciberataque/

Google. (2022). *Topología Híbrida.* Obtenido de .https://sites.google.com/site/tecnologia4a16/tipos-de redes/redes-lan/conceptos-necesarios/topologia-hibrida

Higo. (Julio de 2022). *Red WAN ¿Qué es y cómo funciona?* Obtenido de https://higo.io/glosario-contable/r/red-wan-que-es-y-como-funciona/

Hwang, D. (2021). *Red de área local o LAN.* Obtenido de https://www.computerweekly.com/es/definicion/Red-de-area-local-o-LAN

IBM. (2020). *¿Qué es la ciberseguridad?* Obtenido de https://www.ibm.com/es-es/topics/cybersecurity

ICA. (2022). *Los 9 tipos ciberataque que deberías conocer.* Obtenido de https://www.grupoica.com/blog/-/blogs/9-tipos-ciberataque-debes-conocer

Implika. (Abril de 2021). *Formación en Nuevas Tecnologías.* Obtenido de https://www.implika.es/blog/que-son-redes-informaticas

Incibe. (Diciembre de 2020). *Amenaza vs vulnerabilidad: cómo diferenciarlos. .* Obtenido de https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-diferenciarlos#:~:text=Definici%C3%B3n%20de%20vulnerabilidad%20y%20amenaza&text=Una%20cuesti%C3%B3

IONOS, D. G. (Junio de 2022). *Kali Linux: ¿qué es Linux para hackers?* Obtenido de https://www.ionos.es/digitalguide/servidores/configuracion/kali-linux/

ISO 27001. (2018). *Referencias Normativas ISO 27000.* Obtenido de https://normaiso27001.es/referencias- normativas-iso-27000/#def361

ISO, 2. (2018). *Referencias Normativas ISO 27000.* Obtenido de https://normaiso27001.es/referencias- normativas-iso-27000/#def361

ISO/IEC-JTC-1/SC-7. (2001). *ISO/IEC 9126-1:2001, Software engineering — Product quality — Part 1: Quality model.* ISO/IEC JTC 1/SC 7 Software and systems engineering.

Itca. (2022). *Ataques pasivos vs ataques activos. .* Obtenido de https://virtual.itca.edu.sv/Mediadores/cms/u46_ataques_pasivos_vs_ataques_activos.html

Jurado, Á. (Julio de 2019). *Amenazas de seguridad física.* Obtenido de https://www.inesem.es/revistadigital/gestion-integrada/amenazas- seguridad-fisica-sistemas-de-informacion/

Kali. (Noviembre de 2022). *La distribución de pruebas de penetración más avanzada.* Obtenido de https://www.kali.org/

Karina P. (2020). http://dspace.unach.edu.ec/bitstream/51000/10128/1/Pinduisaca%20G%2c%20Karina%20P.%282022%29%20MANUAL%20DE%20IMPLEMENTACI%c3%93N%20DE%20UN

%20PROCESO%20HARDENING%20PARA%20MITIGAR%20VULNERABILIDADES%20EN%20EL%20SERVIDOR%20WEB%20NGINX%20DE%20LA%20UNACH.pdf.

Limones, E. (Abril de 2021). *Topología de redes informáticas.* Obtenido de https://openwebinars.net/blog/topologia-de-redes-informaticas/

Maribel. (Mayo de 2017). *Amenazas Físicas y Lógicas. .* Obtenido de https://sites.google.com/site/seguridadinformaticafpb/tipos-de-amenazas/11amenazasfisicasylogicas

Martínez Ramírez, C. (Junio de 2020). *Confidencialidad, integridad y disponibilidad.* Obtenido de https://es.linkedin.com/pulse/confidencialidad-integridad-y-disponibilidad-martinez-ramirez

Neira, B. (2017). *Implementacion de un servidor web.* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/14162/1/GT001840.pdf

Oas.org. (Marzo de 2024). *Desafios del riesgo cibernetico.* Obtenido de https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Org.ec. (Marzo de 2024). *ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR.* Obtenido de ttps://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Process. (Mayo de 2022). *Protocolo de red: qué es y sus características.* Obtenido de https://autmix.com/blog/que-es-protocolo-red#que-es-un-protocolo-de-red

Robledano, A. (Junio de 2019). *Qué es TCP/IP.* Obtenido de https://openwebinars.net/blog/que-es-

Sain, G. (Febrero de 2016). *¿Qué es la ciberguerra? Pensamiento Penal, 1. .* Obtenido de https://www.pensamientopenal.com.ar/doctrina/42952-es-ciberguerra

Silva, D. (Agosto de 2021). *¿Qué es la seguridad de la información?* Obtenido de https://www.zendesk.com.mx/blog/que-es-seguridad-de-informacion/

Softwarelab. (Junio de 2021). *¿Qué es la ingeniería social? Los 5 ejemplos principales.* Obtenido de https://softwarelab.org/es/que-es-ingenieria-social/

Solano, D. O. (2017). *Analisis de Vulnerabilidades y acciones correctivas sobre un sistema web. .* Obtenido de https://www.dspace.espol.edu.ec/retrieve/45e4491d-5352-4463-8569- 19d44988922c/D-106382.pdf

Tinet. (2022). *Tipos de redes.* Obtenido de https://usuaris.tinet.cat/acl/html_web/redes/topologia/topologia_2.html

Tokio. (Agosto de 2022). *Tipos de ataques informáticos: ¿cuáles son y cómo operan?* Obtenido de https://www.tokioschool.com/noticias/tipos-ataques-informaticos/

TokioSchool. (Junio de 2021). *Red VLAN*. Obtenido de ¿En qué consiste?https://www.tokioschool.com/noticias/que-es-vlan/

UAEH. (2022). *Tipos de Redes (LAN, MAN, WAN). .* Obtenido de http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/136_tipos_de_redes_lan_man_wan.html

UCM. (2022). *Proyecto de Innovación Software libre para ciencias e ingenierías.* Obtenido de https://www.ucm.es/pimcd2014-free-software/metasploit

UCSP. (Junio de 2022). *Todo lo que tienes que saber sobre la seguridad de redes. .* Obtenido de https://postgrado.ucsp.edu.pe/articulos/que-es-seguridad-redes/

UNAD. (2022). *Seguridad Informática.* Obtenido de https://soniaespitia.github.io/LecturasSeguridadInformatica/

UNIR. (Enero de 2022). *Topología de red: qué es y cuáles son los tipos más habituales.* Obtenido de .https://ecuador.unir.net/actualidad-unir/topologia-red/

Xringarchery. (Marzo de 2019). *Consejo de piratería: persistencia y pivoteo para principiantes en Metasploitable 2.* Obtenido de https://xringarchery.wordpress.com/2019/03/23/hacking-tip-persistence-in-metasploitable-2/

Zscaler. (2022). *¿Qué es un cortafuegos de próxima generación? .* Obtenido de https://www.zscaler.es/resources/security-terms-glossary/what-is-next-generation-firewall

Anexos