Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

Maestría en Telecomunicaciones

Diseño de una red SOHO segura mediante el empleo de un honeypot en la red de la empresa SIITE para mitigar ataques cibernéticos

Trabajo de Titulación previo a la obtención del título de Magíster en Telecomunicaciones

AUTOR:

Ing. Welington Rafael González Ortega

DIRECTOR:

Ing. John Jossimar Tucker Yepez, Mg. Sc.

LOJA – ECUADOR

2023

Certificación

Loja, 26 de junio de 2023

Ing. John Jossimar Tucker Yepez, Mg. Sc.
DIRECTOR DE TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo proceso de la elaboración del Trabajo de Titulación denominado: **Diseño de una red SOHO segura mediante el empleo de un honeypot en la red de la empresa SIITE para mitigar ataques cibernéticos,** previo a la obtención del título de **Magíster en Telecomunicaciones,** de la autoría del estudiante **Welington Rafael González Ortega**, con **cédula de identidad N° 1900878834,** una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional, de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.

Ing. John Jossimar Tucker Yepez, Mg. Sc.
DIRECTOR DE TRABAJO DE TITULACIÓN

Autoría

Yo, **Welington Rafael González Ortega,** declaro ser autor del presente Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma:

Cédula de Identidad: 1900878834

Fecha: 26/6/2023

Correo electrónico: welington.gonzález@unl.edu.ec

Teléfono: 0988791719

Carta de autorización

Yo, **Welington Rafael González Ortega**, declaro ser autor del Trabajo de Titulación denominado: **Diseño de una red SOHO segura mediante el empleo de un honeypot en la red de la empresa SIITE para mitigar ataques cibernéticos**, como requisito para optar por el título de **Magíster Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los veintiséis días del mes de junio dos mil veintitrés.

Firmado electrónicamente por:
WELINGTON RAFAEL
GONZALEZ ORTEGA

Firma:

Autor: Welington Rafael González Ortega

Cédula: 1900878834

Dirección: Loja

Correo Electrónico: welington.gonzález@unl.edu.ec

Teléfono: 0988791719

DATOS COMPLEMENTARIOS:

DIRECTOR DEL TRABAJO DE TITULACIÓN: Ing. John Tucker Yepez, Mg. Sc.

Dedicatoria

A mi madre Flor y
querida Cecilia,
quienes han sido
fuente de amor y cariño
que me fortalecen y son
la razón de mi existencia.

Welington Rafael González Ortega

Agradecimiento

A mi madre por ser ejemplo de lucha perenne, amor sin condiciones y por haberme sabido inculcar valores inagotables.

A mis hermanos ser el manantial de apoyo, respeto y paciencia.

A esos amigos que te dan la confianza y te llenan o iluminan el camino para cumplir cada meta propuesta.

A mi tutor Ing. John Jossimar Tucker Yepez Mg.Sc, al personal docente y administrativo que nos brindaron su apoyo y conocimientos durante el desarrollo de esta meta.

Welington Rafael González Ortega

Índice de contenidos

Índice de Tablas:

Índice de Figuras:

Índice de anexos:

1. Título

Diseño de una red SOHO segura mediante el empleo de un honeypot en la red de la empresa SIITE para mitigar ataques cibernéticos.

2. Resumen

En el presente trabajo de investigación se diseñó una red SOHO (Small Office –Home Office) segura mediante el empleo de elementos activos y pasivos de ciberseguridad en la red de la empresa SIITE, el objetivo es mitigar ataques cibernéticos, proteger la red y analizar estrategias de ataque de los ciberdelincuentes, de manera que permita a los administradores de la red contrarrestar y tomar las medidas necesarias para evitar pérdidas de datos, daño a la reputación, interrupción del servicio, pérdidas de productividad y costos de recuperación, además se plantea un mecanismo de seguridad como políticas de seguridad, capacitación para personal técnico y operativo de la empresa, políticas para los equipos de red, equipos terminales, servidores, entre otros y finalmente se necesita identificar los riesgos cibernéticos más recurrentes en las empresas ecuatorianas para plasmarlos como posibles vectores de ataques.

Para el diseño de la red se utiliza software de simulación y/o virtualización, se emplean máquinas, servidores virtuales y software de diseño para plantear la topología lógica de la red a utilizar para una futura implementación de la red SOHO por parte de la empresa de telecomunicaciones.

Palabras Claves: *Honeypot, servidor web, SOHO.*

2.1. Abstract

In this project, a secure SOHO (Small Office – Home Office) network was designed through the use of active and passive cybersecurity elements in the SIITE company network, the objective is to mitigate cyber attacks, protect the network and analyze attack strategies. of cybercriminals, so that it allows network administrators to counteract and take the necessary measures to avoid data loss, reputation damage, service interruption, productivity losses and recovery costs, in addition a security mechanism is proposed such as security policies, training for technical and operational staff of the company, policies for network equipment, terminal equipment, servers, among others and finally it is necessary to identify the most recurring cyber risks in Ecuadorian companies to capture them as possible attack vectors .

For the design of the network simulation and/or virtualization software is used, machines, virtual servers and design software are used to propose the logical topology of the network to be used for a future implementation of the SOHO network by the service company. telecommunications.

Keywords: Honeypot, web server, SOHO.

3. Introducción

Las tecnologías digitales son fundamentales para potenciar el desarrollo y crecimiento de las empresas, ofreciendo beneficios económicos y sociales significativos. Estas empresas recopilan y almacenan datos e información transcendental, como bases de datos de clientes, productos o servicios. En consecuencia, se debe implementar equipos de telecomunicaciones que garanticen seguridad a la red de datos, de manera que se mitigue el riesgo de ataques a los sistemas de información.

La implementación de sólidas prácticas de políticas de seguridad reduce significativamente la posibilidad de que las redes de datos de las empresas sean víctimas de ataques. Además, estas prácticas permiten detectar vulnerabilidades existentes en las redes protegiendo así la infraestructura empresarial.

Es importante que las empresas implementen elementos activos de ciberseguridad de tal manera que estén preparados para enfrentar posibles ataques de seguridad, un gran porcentaje de las empresas mantienen redes planas, donde no existe preceptos básicos en el diseño de las redes como son la segmentación, la flexibilidad y la escalabilidad, convirtiéndose en redes vulnerables y de fácil acceso para los ciberdelincuentes.

Actualmente existen una diversidad de equipos de telecomunicaciones, software y herramientas de seguridad que permiten diseñar redes seguras y protegerlas contra ataques cibernéticos, en resumen, las empresas deben utilizar todos estos elementos para reducir los prejuicios que puedan suscitarse cuando un ciberdelincuente busque vulnerar los sistemas de información y redes de datos.

De igual manera la capacitación al personal de la empresa sobre el uso de políticas de seguridad es indispensable para proteger la integridad de los datos de la empresa, desafortunadamente las personas no tomamos conciencia del peligro que lleva navegar por el internet y muchas de las veces somos víctimas de ataques cibernéticos por eso es imperativo implementar campañas de ingeniería social donde el usuario este en la capacidad de identificar fraudes electrónicos protegiendo así la información personal y de la empresa u organización.

Objetivos:

Objetivo general

Diseñar una red segura utilizando honeypot y elementos activos en la red SOHO de la empresa SIITE.

Objetivos específicos

- Analizar y diseñar un mecanismo de seguridad informática que permita la recolección de patrones del atacante denominado honeypot para la empresa SIITE.
- Plantear políticas de seguridad que permitan a la empresa SIITE mitigar posibles ataques cibernéticos.
- Identificar los riesgos cibernéticos más recurrentes en las empresas ecuatorianas para plasmarlos como posibles vectores de ataques.

4. Marco Teórico

4.1. Red de datos

Es un conjunto de dispositivos interconectados entre sí que, mediante una serie de protocolos y medios físicos de interconexión, sean estos cableados o inalámbricos, son capaces de comunicarse, compartir recursos y transmitir información.

Estas redes están compuestas por diferentes componentes como servidores, enrutadores, conmutadores, concentradores, etc., todos estos dispositivos trabajan juntos para permitir la comunicación y el intercambio de datos, en la actualidad existen diferentes tipos de redes informáticas agrupadas por la cantidad de dispositivos y se describen brevemente a continuación:

4.1.1. Tipos de redes informáticas

4.1.1.1.Red de área personal (PAN)

Utilizada para conectar dispositivos de área personal como smartphone, tabletas, laptops, etc., diseñada para implementarse en hogares, oficinas pequeñas, vehículos entre otros espacios y suele cubrir un área reducida de pocos metros.

4.1.1.2.Redes de área local (LAN)

Es una red de área local, cubre unos cuantos cientos de metros y por lo general es ocupada por empresas pequeñas. Una red LAN es de tipo broadcast, es decir el mensaje que emite una computadora llega a todos los dispositivos de la red, pero solo reconoce la dirección de la computadora destino.

4.1.1.3.Red virtual de área local (VLAN)

Es una red virtual configurada en equipos de telecomunicaciones como router o switch tomando como base el número de puerto, la dirección física, Mac o dirección IP de los dispositivos o computadoras.

Permite crear redes lógicas aisladas en la misma red física, además se segmenta la red y se tiene el control del tráfico de la subred hacia cada dispositivo conectado la red virtual.

4.1.1.4.Redes de área metropolitana (MAN)

Permite la conexión de un mayor número de dispositivos ubicados en un área de extensión reducida como ciudades, en resumen, es un conjunto de varias redes LAN y pueden combinar redes de varias organizaciones en lugar de ser gestionadas por una sola organización.

4.1.1.5.Redes de área Amplia (WAN)

Una red de este tipo engloba grupos de redes distribuidas desde un país hasta un continente. Dado que soporta un número muy elevado de usuarios y servicios necesitan las conexiones más potentes: las de fibra óptica y las de radio.

4.1.2. Topologías de las redes de datos

Es la forma como se organizan y conectan los ordenadores o dispositivos de manera física y lógica en las redes de datos, a continuación, se detallan los más comunes:

4.1.2.1.Topologías físicas:

4.1.2.1.1. Topología en bus

Todos los dispositivos comparten la misma red entre sí de manera lineal, es decir se conectan al mismo medio físico (cable), presentan la desventaja que si falla la red en una parte del cableado deja de funcionar todo el sistema.

4.1.2.1.2. Topología en estrella

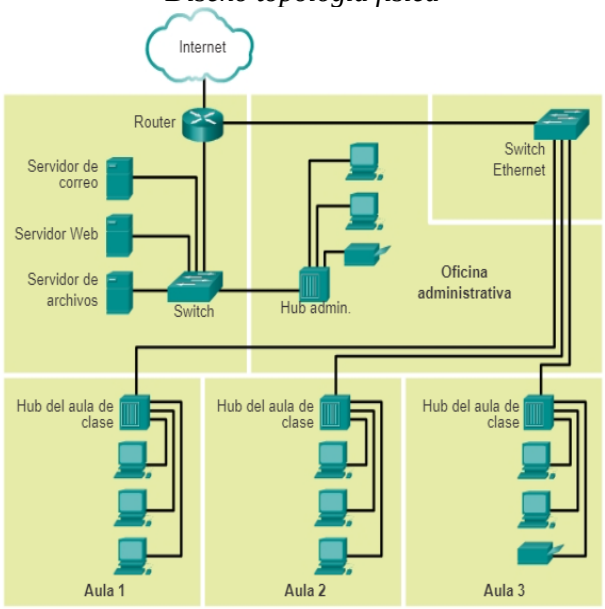
En esta topología existe un nodo central en donde se conectan todos los ordenadores, dispositivos o equipos, toda la transmisión y recepción de paquetes debe pasar por este nodo. Al existir un solo nodo se crea una vulnerabilidad en la red, considerando que este es el único equipo de borde de la red si deja de funcionar se cae la red de datos.

4.1.2.1.3. Topología en anillo

Todos los ordenadores se conectan a un mismo bus en forma de anillo o doble anillo. El cableado y mantenimiento de estas redes suele ser más engorroso, pero tiene la ventaja de que en el caso de que se rompa un conductor del anillo, la red no queda fuera de servicio.

Figura 1

Diseño topología física



Fuente:(Willians, 2004)

4.1.3. Red SOHO (Small Office Home Office)

Es una red de área local utilizada en entornos que tiene un número reducido de dispositivos u ordenadores conectados, es implementada en pequeñas empresas para gestionar recursos empresariales permitiendo la interconectividad y servicios ofrecidos por las empresas u organizaciones para compartir recursos e interconexión en oficinas pequeñas, hogares y oficinas conectadas a internet.

4.1.3.1.Características de la red SOHO

- Utilizada en oficinas pequeñas.
- Se canalizan a través de un único equipo de borde (router).
- Ofrece la asignación dinámica de direcciones IP (DHCP y DNS) a los clientes conectados.
- La red SOHO debe proporcionar acceso a la red local a dispositivos inalámbricos autorizados como ordenadores portátiles o teléfonos móviles actuando como un Access Point.
- En esta red se ofrecen más servicios como servidor de correo electrónico, servidor de archivos, etc. y esta es una gran diferencia con una red LAN doméstica.
- Debe facilitar la búsqueda y administración de archivo y documentos inmersos dentro de la red LAN de la empresa.

4.1.3.2.Requerimientos de una red tipo SOHO

4.1.3.2.1. Disponibilidad de acceso a Internet

Es necesario que la red SOHO de la empresa mantenga una conexión a internet, al menos con un solo enlace a través del equipo de borde del proveedor de Internet (ISP), de esta manera provee el acceso a internet a todos los usuarios que forman parte de la red.

4.1.3.2.2. Políticas de acceso a Internet

Debe existir una administración de la red para el control del ancho de banda y del acceso al contenido web que no sea autorizado por la empresa u organización, manteniendo un acceso eficiente y un mejor desempeño en los empleados de la empresa.

4.1.3.2.3. Seguridad en la red

Debe estar en la capacidad de implementar medidas y políticas de seguridad, actualmente se producen muchos ataques activos o pasivos y por las vulnerabilidades causadas por la falta de capacitación en los usuarios o actualización en los equipos de telecomunicaciones es fácil para personas no autorizadas causar daños en la red.

4.1.3.2.4. Flexible y escalable

Una red SOHO debe ser flexible a cambios, fácil de configurar y debe estar en la capacidad de facilitar a los técnicos encargados la administración y mantenimiento de la red.

4.2.Particularidades de una red LAN segura

4.2.1. Arquitectura de seguridad OSI.

La Arquitectura de seguridad OSI define los servicios y mecanismos de seguridad que se pueden utilizar en cada una de sus capas, de tal manera que se brinde seguridad a cada uno de los paquetes transmitidos y recibidos a través de la red garantizando la confidencialidad, integridad y disponibilidad de los datos.

Es este modelo es muy común hablar de los perímetros de seguridad dentro y son utilizados para brindar seguridad a una red de datos reduciendo la probabilidad de que intrusos malintencionados capturen información o causen daños críticos a la infraestructura de la empresa u organización, siendo uno de los objetivos del modelo OSI comunicar los datos de un perímetro a otro. (Branstad, 1987)

A continuación, se describe la función del modelo de seguridad OSI en cada una de las capas:

- **Capa física**: En esta capa es importante el mecanismo de cifrado, este permite la confidencialidad del flujo de tráfico a través de la red y contiene un dispositivo de cifrado y descifrado.
- **Capa de enlace**: La capa de enlace de datos solo permite dos servicios de seguridad que son: la conexión y confidencialidad de transmisión sin conexión.
- **Capa de red**: Su finalidad es dar acceso a la subred, la retransmisión y el enrutamiento y para ello se debe emplear protocolos de seguridad específicos para la capa de red.
- **Capa de transporte**: Los servicios de seguridad que proporciona la capa de transporte son:
    - Autenticación,
    - Control de acceso,
    - Confidencialidad de la conexión
    - Transmisión sin conexión
    - Integridad.
- **Capa de sesión:** La capa de sesión no contiene servicios de seguridad a la red.
- **Capa de presentación:** Permite garantizar la confidencialidad del flujo de tráfico utilizando un mecanismo de cifrado. Este mecanismo puede ser asociado con otros mecanismos de seguridad de la capa de aplicación. (Ramaswamy, 1990)

4.2.2. Elementos de seguridad

- **Activo**

Son todos aquellos elementos que son importantes para una organización, su objetivo es cumplir con la misión de la empresa, entre los activos tenemos la información, el hardware e incluso los seres humanos.

- **Amenaza**

Es una posibilidad de violación de la seguridad, existe cuando se da la circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar perjuicios en los activos de un sistema de información, considerado como un peligro posible que podría explotar una vulnerabilidad. (Libro Willians)

- **Ataque**

Es el acto inteligente y deliberado para eludir los servicios de seguridad y violar la política de un sistema, red o servicio.

Clasificación de los ataques

- **Ataque pasivo**

Se da en forma de escucha o de observación no autorizada de las transmisiones, el objetivo del atacante es obtener información que se esté transmitiendo, lo más común es la obtención de mensajes y el análisis de tráfico.

- **Ataque activo**

Mientras que un ataque pasivo se basa en la escucha, un ataque activo implica alguna modificación del flujo de datos, utiliza técnicas o estrategias de ataque para vulnerar y modificar la red de datos. (Willians, 2004)

Tipos de ataques:

- **Ataques a la autenticación:** Suplantación de identidades de internet.
- **Ataques a la disponibilidad:** Inhabilitación remota de máquinas.
- **Ataques a la confidencialidad:** Monitorización de conexiones de red.
- **Ataques a la integridad:** Defacemtent.

A continuación, se detallan algunos de los ataques más realizados en las redes de datos.

Fuerza bruta:

Este ataque se produce cuando se intenta irrumpir un sistema con un gran número de combinaciones de usuarios y contraseñas, por lo general esto ocurre en páginas web, y en equipos de telecomunicaciones.

DDos:

En este ataque pueden participar diferentes dispositivos para inundar o interrumpir el tráfico normal de un servidor o red objetivo, causando un cuello de botella en las redes de datos, normalmente a este tipo de dispositivos se los considera como una Botnet.

Phishing

Considerado como un ataque de ingeniería social, una técnica muy común es el correo electrónico usado para engañar y estafar a las personas, empresas u organizaciones, el objetivo es ganarse la confianza del usuario para obtener datos confidenciales como contraseñas, información bancaria entre otros.

Zero Day:

Sucede cuando los atacantes logran vulnerar la seguridad de la red antes de que los administradores puedan encontrar una solución, esta vulnerabilidad normalmente es conocida como ataque de día cero.

- **Vulnerabilidad**

Son deficiencias, fallas o brechas que tienen los activos o sistemas de información.

- **Impacto**

  Es la repercusión que se produce al plasmarse una amenaza en la red.

- **Salvaguardas**

Son los controles o acciones que se toman para propender por la seguridad de las redes, comunicaciones o sistemas de información.

- **Riesgo**

Es el compendio de todos los elementos mencionados como activos, amenazas, salvaguardas, etc. y el resultado de toda esta evaluación operación es el riesgo, este riesgo nunca va a ser cero, por ende, la organización debe llevar el riesgo a un punto que se pueda controlar o trasladar. (Estupiñan et al., 2013)

4.2.3. Equipos y dispositivos de red

- En una red LAN para PYMES pequeñas es importante que se identifique los dispositivos de la red, limitar el acceso físico y lógico a cada dispositivo, además se debe aplicar filtros o políticas de seguridad.
- Actualizar el firmware de los equipos de telecomunicaciones es primordial porque se reducen las vulnerabilidades y cerramos la puerta o acceso a los intrusos de atacar la red de la empresa.

4.2.3.1. Infraestructura de red

- El cableado estructurado es necesario porque permite mantener una red segura, este debe ser escalable, flexible, segura y eficiente.
- Debe contar con equipos de red administrables y al menos un dispositivo que brinde seguridad a la red.

4.2.4. Usuarios

- Para la empresa la información es primordial para su crecimiento y desarrollo, por lo tanto, es necesario capacitar al personal de la empresa y crear concienciación de seguridad de la información.

4.2.5. Diseño

- El diseño de servicios de seguridad requiere la definición de un protocolo de comunicación, establecimiento de cifrado y descifrado de información y asignación de claves.

4.3.Seguridad de la información

Tiene como fin la protección la información, así como el acceso, uso o afectación no autorizada de los sistemas de información, la seguridad debe ser considerada como un conjunto de medidas y políticas que mitiguen el riesgo en las redes de datos de las organizaciones que permiten proteger y resguardar la:

- Confidencialidad
- Integridad y
- Disponibilidad de la información

En la actualidad el elemento activo de una empresa u organización es la información y tal así requiere protección ante cualquier ataque o amenaza que ponga en peligro a la organización sea esta pública o privada. (Vergara Quiroz, 2017)

Características

- La seguridad de la información se apoya en las políticas de seguridad establecidas por las empresas u organizaciones.
- Además de reducir el impacto de los riesgos y amenazas entre otros beneficios, mejora la planificación y la gestión de la seguridad de la empresa.
- Debe ser básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de los usuarios de la red.
- La confidencialidad asegura que solamente aquellas personas que cuenten con autorización puedan acceder a la información.
- La disponibilidad es el acceso a los sistemas y a la información en el momento que las personas lo requieran.
- Se debe asegurar o garantizar la integridad, es decir debe estar libre de modificaciones no autorizadas y los datos deben llegar tal cual fueron enviados. (Figueroa-Suárez et al., 2018)

4.4.Técnicas de seguridad

- Implementación de firewall
- Implementar políticas de seguridad
- Capacitación de ciberseguridad
- Implementación de herramientas de ciberseguridad.

En este proyecto se estudia el diseño de la red SOHO mediante el empleo de un servidor denominado honeypot considerado como mecanismo de seguridad, a continuación, se detallan algunos conceptos básicos, ventajas, desventajas y beneficios del honeypot:

4.4.1. Honeypot

Es un servidor de seguridad que permite detectar las vulnerabilidades y las técnicas que utilizan los ciber atacantes o adversarios de tal manera que permita mitigar los ataques producidos a la red interna o externa. (Lacerda et al., 2017)

Características

- Dispone de herramientas y tácticas diseñadas para capturar y analizar el tráfico generado en este sistema, con esto se provee un alto grado de detección de intrusos.
- Tiene la capacidad de recopilar información de ataques pasivos y activos lo que permite detectar posibles riesgos o vulnerabilidades sobre la red.
- Desvía la atención de los atacantes de la red que contiene información valiosa y permite analizar las estrategias que siguen para desarrollar estrategias de defensa para contrarrestar estos ataques.
- Utiliza recursos mínimos para su funcionamiento. (Shi et al., 2019)

Ventajas

Simplicidad

Los honeypot de baja interacción son fáciles de implementar y configurar, se necesita una conexión a internet y se definen los parámetros correspondientes para su funcionamiento.

Flexibilidad

Un honeypot de media interacción permite configurar los servicios necesarios para obtener varios resultados y no queda atado a resolver un problema en específico.

Recursos

No necesita grandes cantidades de recursos para funcionamiento, utiliza poca memoria y sus costos de implementación son relativamente bajos.

Valor de los datos

Toda actividad dirigida hacia los honeypots es sospechosa por naturaleza, la cual representa un gran valor, toda la actividad capturada puede ser un escaneo, una prueba o un ataque reduciendo los tiempos de detección y de análisis malicioso en la red. (Ángeles García, 2012)

4.4.1.1.Riesgos al implementar un honeypot

- Los honeypot de alta interacción presentan mayor riesgo y compromiso con el sistema operativo sobre el cual se ejecuta, un intruso puede hacer mal uso de los recursos de un honeypot usándolo como arma en contra de los equipos y lograr infiltrarse dentro de la red.
- El valor de un honeypot consiste en ser comprometido, atacado y probado con el fin de aportar información a los administradores de la red, obteniendo información muy valiosa para el desarrollo de procedimientos y metodologías.
- Este honeypot debe estar ubicado en una zona desmilitarizada (DMZ) de la red de la empresa, debe ser accesible desde internet de manera que se pueda acceder a los servicios alojados, al estar aislado de la red de datos el riesgo disminuye y el intruso se enfocaría en la DMZ protegiendo la red interna.
- Configurar y monitorear correctamente permite tomar las medidas o estrategias necesarias para mitigar estos ataques, un error puede permitir que el honeypot sea una puerta de acceso a la red de las empresas y el ciber atacante puede tomar a favor este servidor para encontrar vulnerabilidades.

4.4.1.2.Ubicación del honeypot

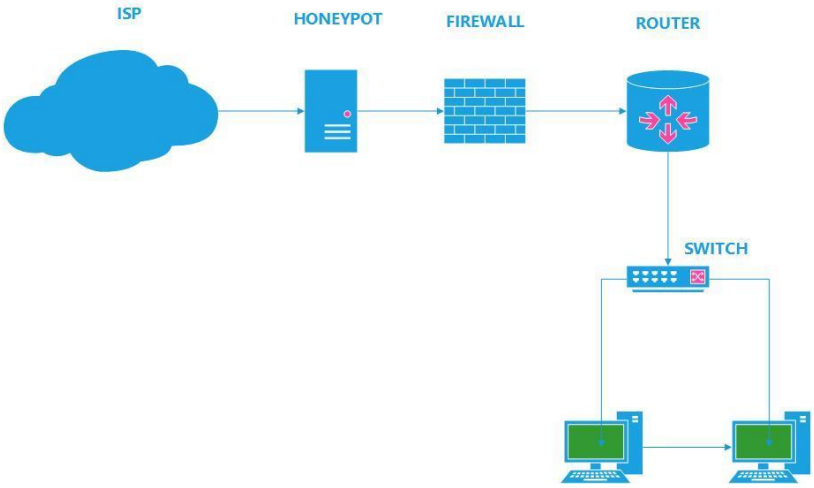
La ubicación del honeypot dependerá de los requerimientos que tenga la organización en base a sus objetivos, a continuación, se presentan algunas ubicaciones recomendadas:

– **Honeypot antes del Firewall**

La red LAN no se ve comprometida porque el honeypot está ubicado entre el proveedor de servicio de internet y el firewall, sin embargo, esto puede generar un gran consumo de ancho de banda porque es lo primero que encuentra un atacante en la red.

Figura 2

Diseño ubicación de honeypot antes del firewall



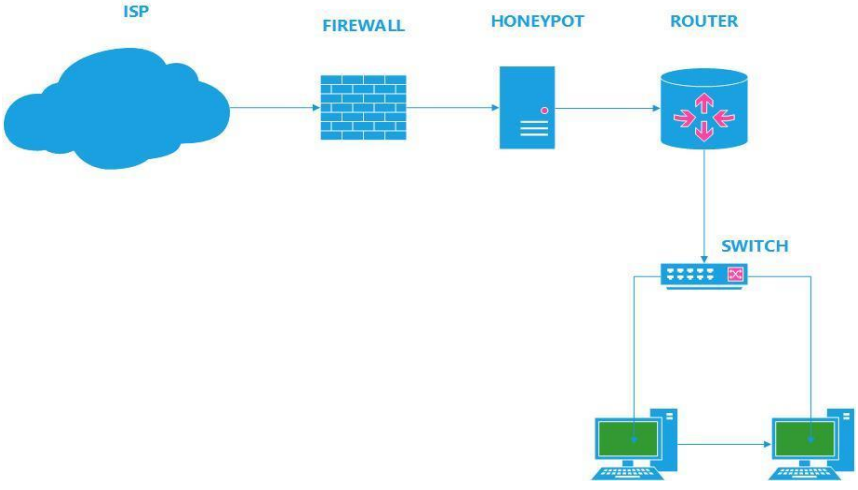
Fuente: El autor

- **Honeypot después del Firewall**

En el firewall se debe crear reglas para permitir el acceso al internet al honeypot, de manera que este sea accesible a los servicios configurados para los ciber atacantes, en la siguiente figura se presenta un diseño de red donde se ubica el honeypot después del firewall.

Figura 3

Diseño ubicación de honeypot después del firewall



Fuente: El autor

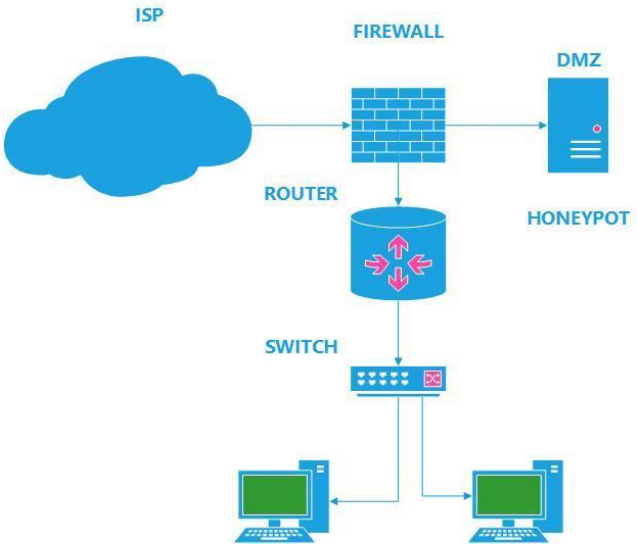
Honeypot en la zona desmilitarizada (DMZ)

Considerando que una DMZ es una red segura y aislada para alojar servicios y aplicaciones que deben estar accesibles desde el exterior, (granja de servidores), por lo general está situada entre la red interna y externa y tiene medidas de seguridad para impedir el acceso no autorizado a la red interna.

Permite tener la posibilidad de detectar ataques internos y externos, es necesario que se configure los parámetros de acceso desde el firewall, este honeypot está aislado de la red local y se considera una de las mejores ubicaciones. (Eduard & Daniel, s. f.)

Figura 4

Diseño ubicación de honeypot en DMZ.



Fuente: El autor

4.4.1.3.Clasificación de los honeypot

Baja interacción

Este tipo de honeypot capturan información básica de los ataques cibernéticos, es usado para detectar pruebas de escaneo y analizar el tráfico malicioso, se activa entre uno a dos servicios y consumen menos recursos que los honeypot de media alta interacción.

Media Interacción

El nivel de interacción aumenta y el intruso logra observar mayores funcionalidades en cuanto a los servicios que trata de vulnerar.

Alta interacción

Estos honeypot capturan mayor información sobre las técnicas de ataque, se tiene la libertad para interactuar con un sistema y servicios reales y se obtiene información extensa sobre las amenazas. Este tipo de honeypot tiene un mayor riesgo porque atacantes más experimentados pueden acceder potencialmente al sistema operativo y pueden usarlo para dañar otros sistemas que no son honeypot. (Lara Rocha & López Cante, 2013)

4.4.1.4.Tipos de honeypot

Producción

Diseñado para la seguridad y defensa de las redes, se implementan de manera colateral a las redes de datos, infraestructuras en sistemas y ambientes reales y son utilizados para proteger a las organizaciones y mitigar riesgos.

Investigación

Su objetivo es recolectar información sobre la actividad maliciosa en la red, utilizado para tener una visión más clara sobre las operaciones, estrategias y los motivos de los ataques, estudio de patrones etc.

Esos son difíciles de manejar y desplegar, pero son capaces de reunir una gran cantidad de información.

Físicos

Se considera un honeypot físico cuando se utiliza hardware o equipamiento real hecho específicamente para trabajar con este tipo de servicios, esto puede significar mayor costo y mantenimiento para la empresa que lo va a implementar.

Virtuales

Son honeypots emulados sobre software de virtualización como Virtualbox, Vmware, etc., se puede tener un equipo servidor donde se simulan varios honeypots en un solo software de virtualización significando menor costo de implementación.(Lara Rocha & López Cante, 2013).

4.4.1.5.Honeypots más comunes

- **Kippo**

Es un honeypot SSH de interacción media diseñado para ataques de fuerza bruta, permite obtener toda la interacción del shell realizada por el atacante, pueden ser usados en Windows, GNU/Linux y BSD.

Características

- Sistema de archivos falso con la capacidad de agregar o eliminar archivos.
- Posibilidad de agregar contenidos de archivos falsos para que el atacante pueda 'catear' archivos como /etc/password. Solo se incluyen contenidos de archivo mínimos.(Tamminen, 2014/2023).

- **Honeyd**

Utilizado para crear hosts virtuales que pueden configurarse para ejecutar servicios arbitrarios en diferentes sistemas operativos, proporciona mecanismos para la detección y evaluación de amenazas y disuade a los adversarios al ocultar sistemas reales en medio de sistemas virtuales.(*Developments of the Honeyd Virtual Honeypot*, s. f.).

- **Artillery**

Es una combinación de honeypot, es una herramienta de monitoreo y sistema de alerta de intrusos, se la considera como una plataforma para detectar vulnerabilidades y configuraciones inseguras de los sistemas Linux y Windows.

Características

- Se pueden configurar múltiples puertos comunes para que sean atacados e inmediatamente sean bloqueadas las IPs.
- Supervisa registros SSH y busca intentos de fuerza bruta.
- Enviará un correo electrónico cuando ocurran ataques e informará el tipo de ataque.

- **HoneyBOT**

Considerado con el primer honeypot de interacción híbrida, es utilizado para atraer a los atacantes de la red, simula servicios y protocolos como echo, ftp, telnet, smtp, http, pop3, etc., y es ideal para la investigación de seguridad de redes como parte de un IDS de alerta temprana.(Irvene et al., 2018)

5. Metodología

5.1.Antecedentes

La empresa denominada Servicios Integrados de Ingeniería en Electrónica y Telecomunicaciones (SIITE), cuya visión es ser una empresa líder a nivel regional en proyectos de ingeniería de electrónica y telecomunicaciones contando con la optimización de recursos, personal capacitado y comprometido respetando el ambiente y la comunidad.

En este proyecto de tesis se busca realizar un diseño para mejorar la red de telecomunicaciones implementada en la empresa SIITE, por lo tanto, se utilizó la metodología experimental e investigativa,

Al mismo tiempo se coordinó una visita técnica en las dependencias de la empresa realizando un levantamiento de información del estado actual de la red, equipos de telecomunicaciones, número de equipos terminales, usuarios, servicios, así como políticas de seguridad utilizadas.

En base a esta información se empieza a trabajar en el tema y objetivos plateados como es el diseño de una red SOHO segura mediante el empleo de un honeypot en la empresa SIITE, mecanismos, políticas de seguridad y los riesgos cibernéticos más recurrentes en las empresas ecuatorianas con los cuales se obtendrán las conclusiones de este trabajo de tesis.

5.1.1. Servicios y departamentos

Tabla 1.
Servicios proporcionados

Departamento	Personal asignado	Servicios
Gerencia	1	Seguridad electrónica. Proyectos y estudios de telecomunicaciones. Proyectos y estudios eléctricos.
Secretaria	1	
Contabilidad	1	
Departamento técnico	1	

Fuente: El autor

5.1.2. Dispositivos y equipos activos

Tabla 2.
Equipos activos

Dispositivos	Función
PCs	3
Laptops	4
Cámaras	6
Dispositivos IoT	5
VTO (Frente de calle)	1
VTH (Pantalla táctil)	1

Fuente: El autor

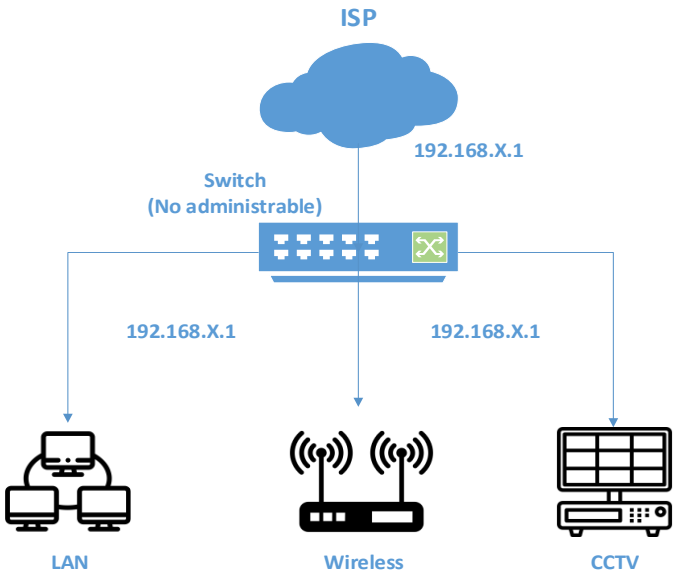
5.2.Diseño de la red SOHO

5.2.1. Red actual

En la Figura 5 se presenta el diseño de la topología actual de la empresa SIITE, a continuación, se detalla el estado actual de la red LAN de la empresa:

- Mantienen una red plana, es decir todos los dispositivos se encuentran en la misma subred por ende no hay segmentación de red.
- No aplican políticas de seguridad en los equipos de red, equipos terminales.
- El personal de la empresa no cuenta con una capacitación para el uso adecuado de políticas de seguridad.
- No existe un firewall que permita el control y filtrado de los paquetes entrantes y salientes en la red.

Figura 5
Diseño actual de red LAN



Fuente: El autor

5.2.1.1.Equipos utilizados:

Tabla 3.
Equipos utilizados en la empresa.

Modelo	Función
NEXXT Axis200R	Switch
Huawei HG8245H	Router
AP - HUAWEI	Access Point
Grabador CS-X3	NVR

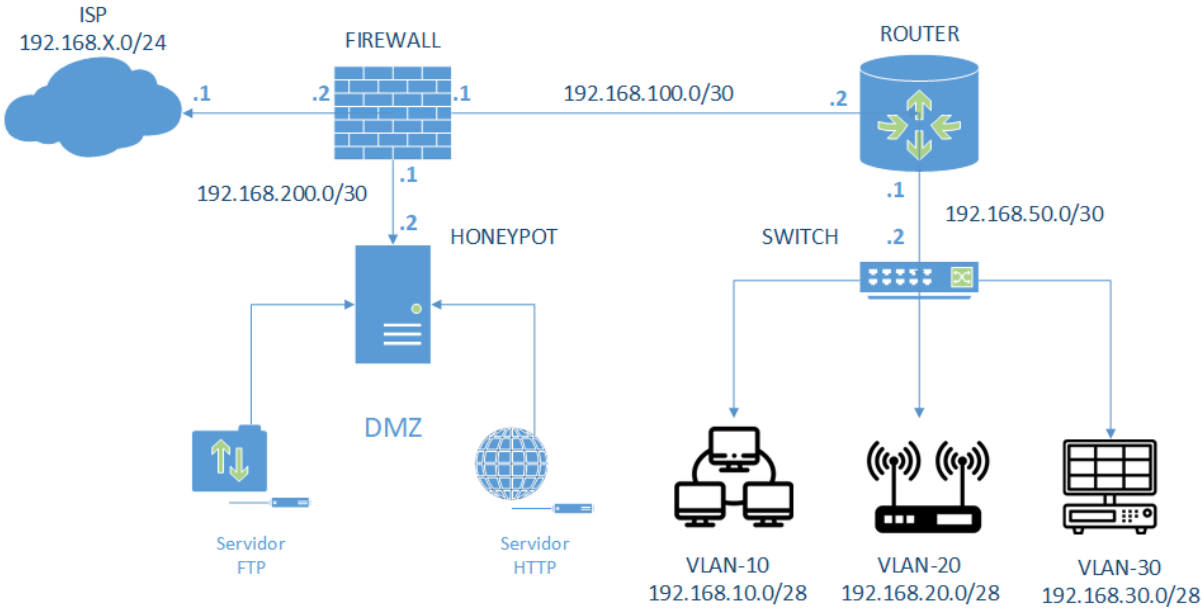
Fuente: El autor

5.2.2. Red Proyectada

Se propone el siguiente diseño o topología de red que puede ser implementada en la red LAN de la empresa, esta se representa en la Figura 6, es importante mencionar que la red 192.168.x.0/24, se representa así por temas de seguridad y evitar intervenciones futuras que pongan en riesgo los recursos de hardware y software de la empresa SIITE.

5.2.2.1.Topología

Figura 6
Diseño o topología propuesta



Fuente: El autor

En la Tabla 4 se propone los equipos que se pueden utilizar para el despliegue de la red LAN SOHO en la empresa SIITE.

5.2.2.2.Equipos utilizados:

Tabla 4.
Equipos utilizados para el diseño.

Equipo	Marca	Funcionalidad
Router- Mikrotik	RB3011UiAS-RM	Permite segmentar y controlar el tráfico de la red.
Switch - Aruba	JL686A	Administración de las VLANs de la red.
	Características	
Server	Ram	16 GB
	Procesador	I5
	Fuente de poder	850W
	Tarjeta gráfica	2gb
	Disco duro	1000 Gb

Fuente: El autor

5.2.2.3.Software utilizado:

Tabla 5.
Software utilizado para el diseño

Servidores	Equipo	Funcionalidad
GNS3	Server	Permite la virtualización de equipo de manera virtual.
Honeypot - Honeydrive	Server	Concentrar a los intrusos en este servidor – honeypot.
Firewall - Pfsense	Server	Crear políticas de seguridad en la red.

Fuente: El autor

Para realizar el diseño de la topología de red que se presenta en la Figura 6 se utilizó el programa ofimático Visio y para la virtualización del funcionamiento de cada uno de los equipos y servidores como el router Mikrotik, Aruba, Firewall y Honeydrive (Honeypot) se utilizó GNS3, para esto fue necesario el uso de un equipo informático con las características mencionadas en la Tabla 4, a continuación, se presenta la instalación y configuración de cada uno de los equipos y software descritos anteriormente:

5.3.Software

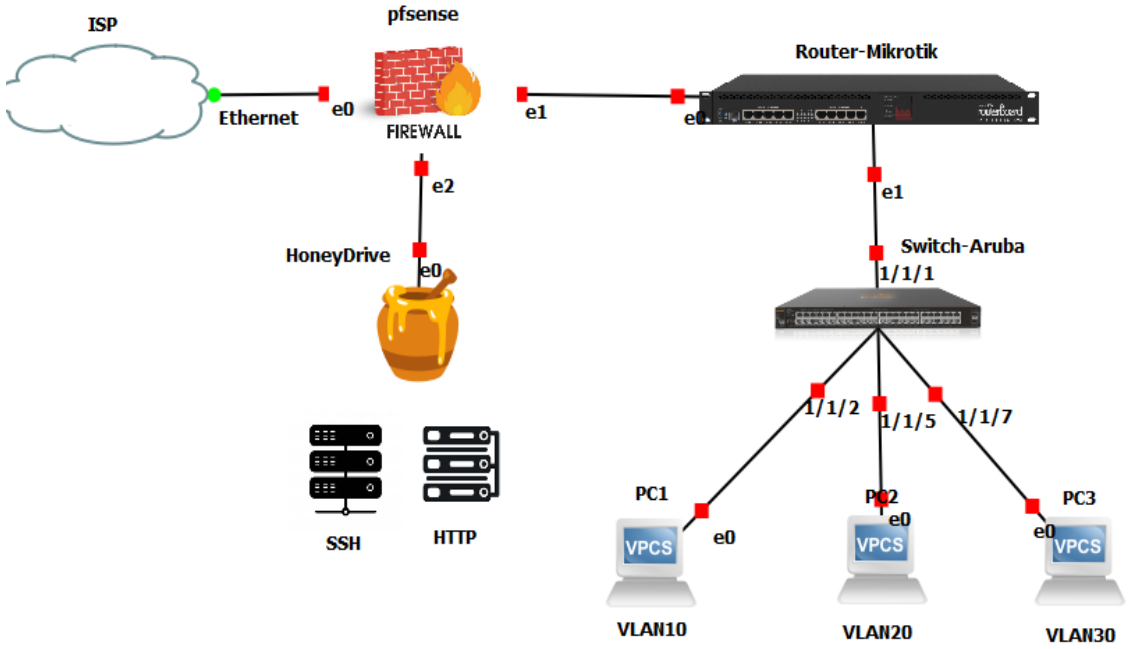
5.3.1. GNS3

Este software permite virtualizar, diseñar y construir topologías o realizar prácticas de laboratorio de red previo a su implementación, es decir se utilizan máquinas virtuales de equipos y servidores en tiempo real para configurar los equipos presentados en el diseño y en las tablas anteriormente, a continuación, se presenta el diseño realizado en GNS3 representado en la

Figura **7**.

Figura 7

Diseño representado en GNS3



Fuente: El autor

5.4.Equipos

5.4.1. Router Mikrotik

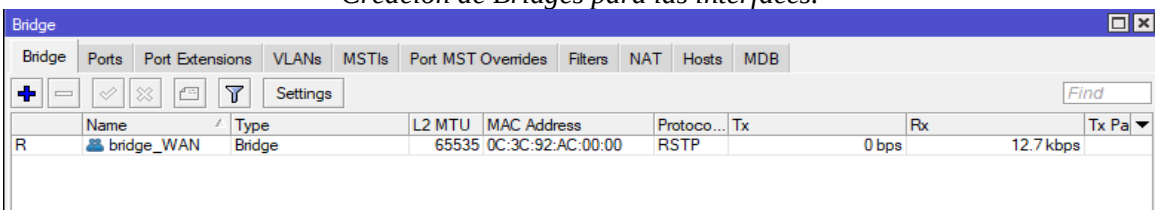
5.4.1.1.Configuración de Mikrotik

5.4.1.1.1. Bridge

Se creó el bridge_WAN para la WAN (ether1), y tres interfaces para las cada una de las VLANs propuestas, estas redes virtuales lógicas permitirán segmentar y aislar el tráfico, optimizando el ancho de banda y reduciendo la congestión de la red SOHO de la empresa, se presenta en la Figura 8.

Figura 8

Creación de Bridges para las interfaces.



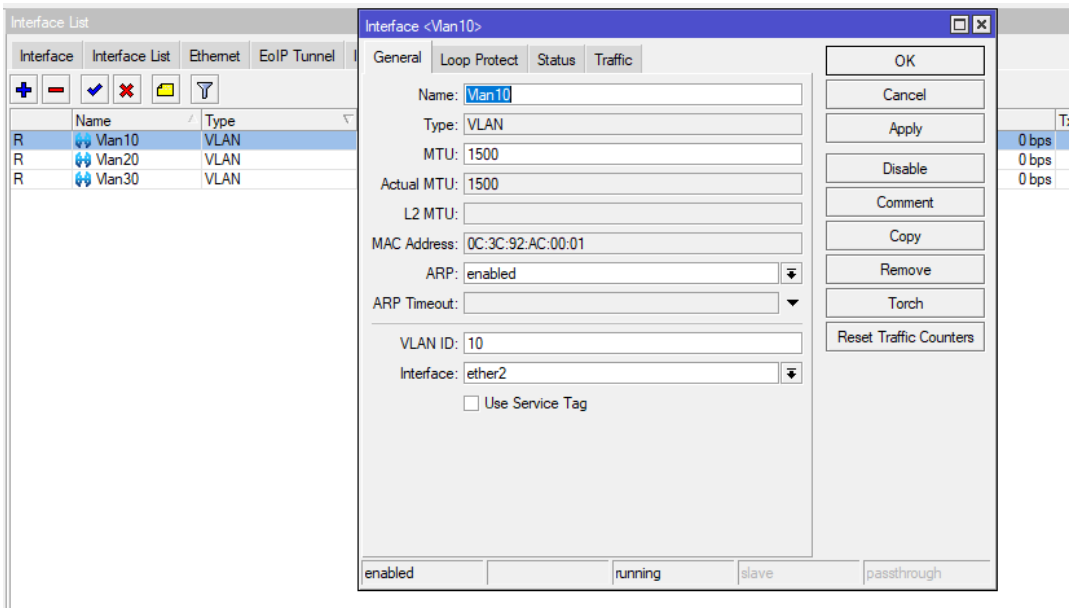
Fuente: El autor

5.4.1.1.2. VLANs

Se crearon tres VLANs descritas en la **¡Error! No se encuentra el origen de la r eferencia.**, en la Figura 9 se puede observar los parámetros configurados para la VLAN 10, procedimiento que se realiza para cada VLAN.

Figura 9

Creación de las VLANs



Fuente: El autor

Tabla 6.

Descripción de las VLANs

VLANs	Nombre	ID	Red
1	LAN	10	192.168.10.0/24
2	WIFI	20	192.168.20.0/24
3	CCTV	30	192.168.30.0/24

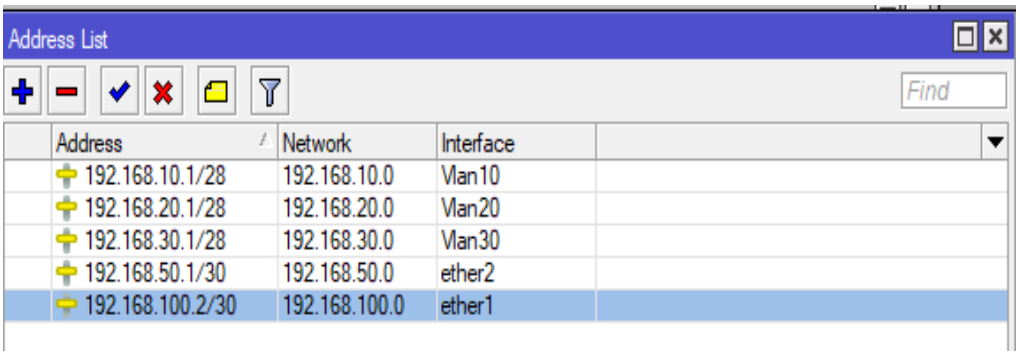
Fuente: El autor

5.4.1.1.3. Address List

En la Figura 11 se puede observar que se asigna el direccionamiento IP para el ether1, ether2 y para cada una de las VLANs creadas, este direccionamiento es necesario para el enrutamiento, control del tráfico y para las políticas de seguridad.

Figura 10

Direccionamiento IP



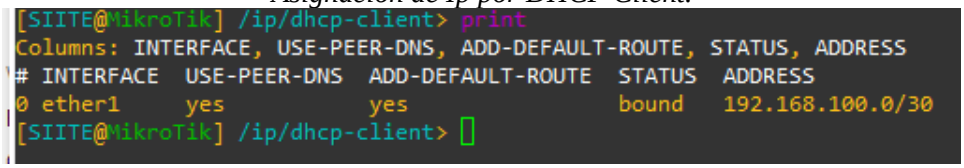
Fuente: El autor

5.4.1.1.4. DHCP Client

Permite que una interface Ethernet pueda solicitar una dirección IP, en este caso el router Mikrotik lo detecta automáticamente, en la Figura 11.

Figura 11

Asignación de Ip por DHCP Client.



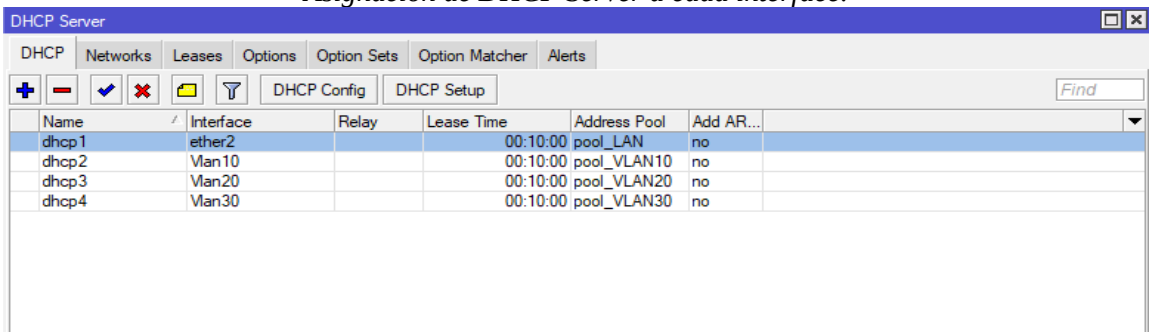
Fuente: El autor

5.4.1.1.5. DHCP Server

Se procede a crear los DHCP server para cada VLAN, esto permitirá asignar una IP de manera automática a cada uno de los dispositivos conectados en el router Mikrotik y el switch.

Figura 12

Asignación de DHCP Server a cada interface.



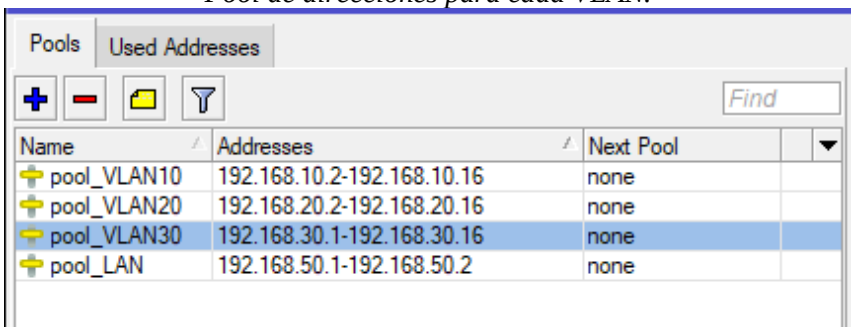
Fuente: El autor

5.4.1.1.6. Pool de direcciones

En la Figura 13 se muestra el pool de direcciones creadas para cada VLAN, reduciendo así la exposición de la red a posibles ataques externos, ya que los dispositivos solo pueden recibir una dirección de pool.

Figura 13

Pool de direcciones para cada VLAN.



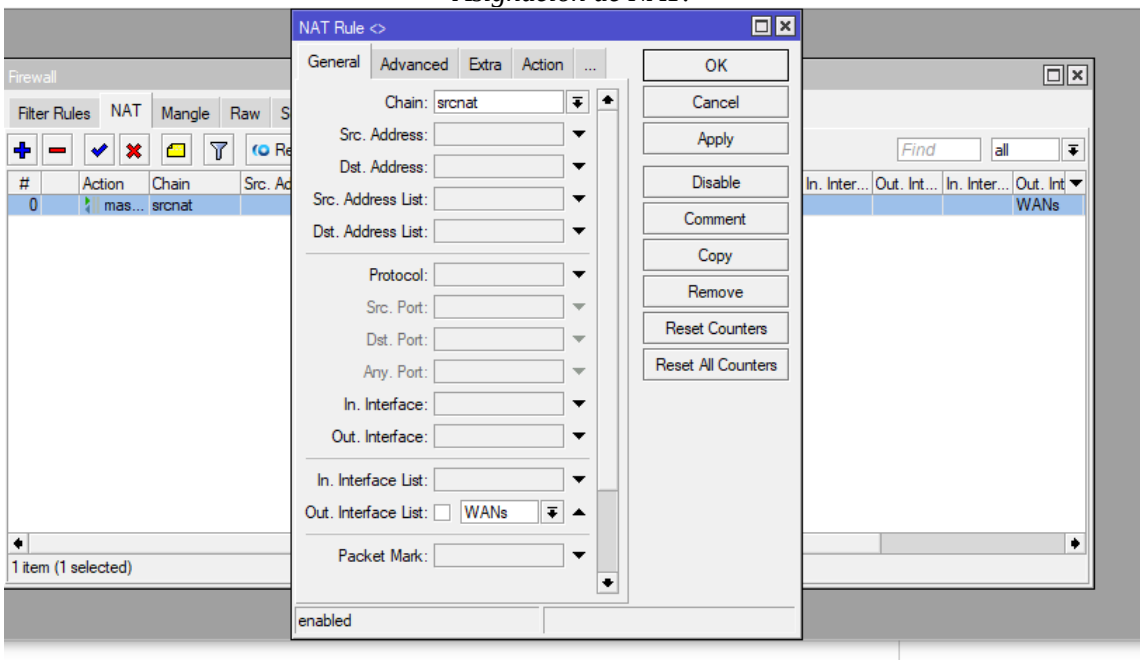
Fuente: El autor

5.4.1.1.7. NAT (Network Address Translator)

Se crea una NAT en el router Mikrotik, utilizazda para dar salida a Internet a cada dispositivo conectado al router o al switch que estará enlazado con una troncal hacia el router.

Figura 14

Asignación de NAT.



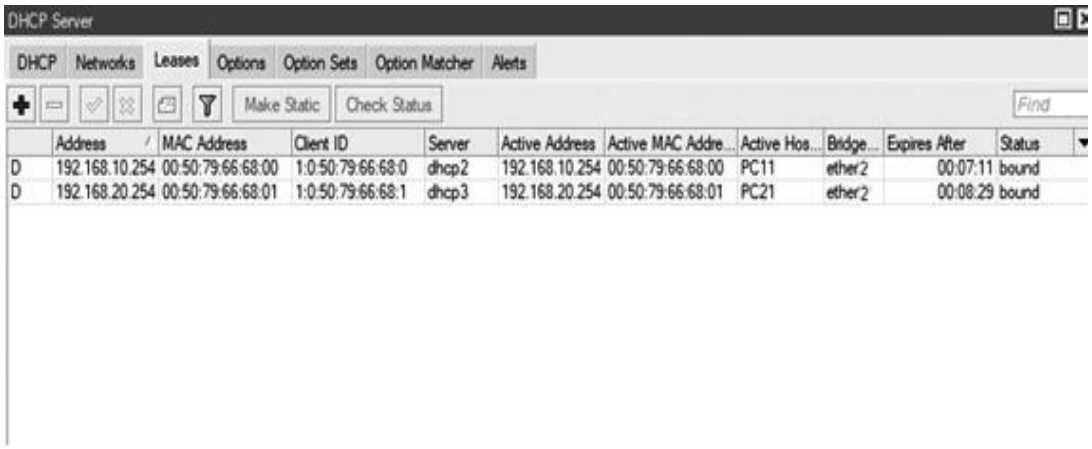
Fuente: El autor

5.4.1.1.8. Leases

En la Figura 15**¡Error! No se encuentra el origen de la referencia.** se puede observar que se han comenzado a conectar los dispositivos a cada una de las VLANs configuradas en el router Mikrotik desde el switch.

Figura 15

Leases conectados a las interfaces del Mikrotik



Fuente: El autor

5.4.2. Switch

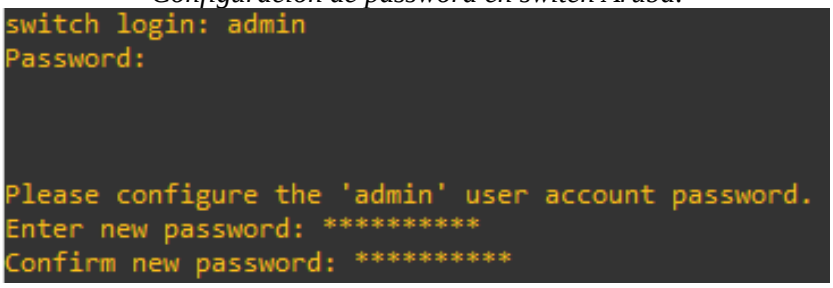
El switch es utilizado para la creación de las VLANs, esto permite dividir una red física en varias subredes lógicas, segmentando la red por función, ubicación o departamento.

5.4.2.1.Configuración de Switch Aruba

Al inicializar el switch con el CLI, por seguridad se configura una contraseña inicial tal como se muestra en la Figura 16.

Figura 16

Configuración de password en switch Aruba.



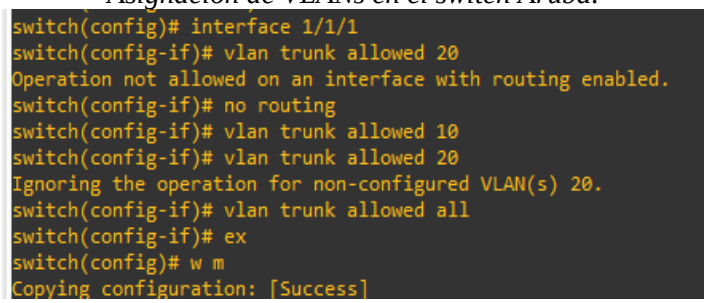
Fuente: El autor

5.4.2.1.1. VLANs

Se configura la interfaz 1/1/1 como troncal permitiendo que el tráfico de las VLANs se propague entre el switch y el router Mikrotik, en la Figura 17 se observa los parámetros configurados.

Figura 17

Asignación de VLANs en el switch Aruba.

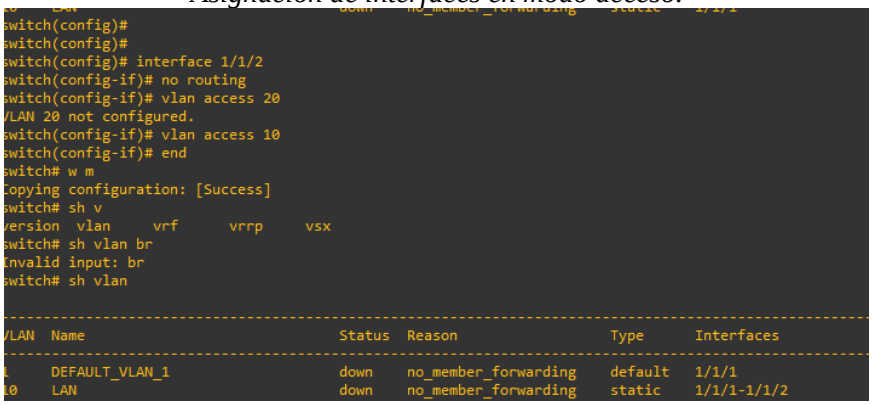


Fuente: El autor

En la Figura 18 se presentan los parámetros configurados al switch al asignar las VLANs, para este ejemplo se le asignó la interfaz 1/1/2 a la VLAN 10 en modo acceso, de esta manera se va asignando las interfaces del switch.

Figura 18

Asignación de interfaces en modo acceso.



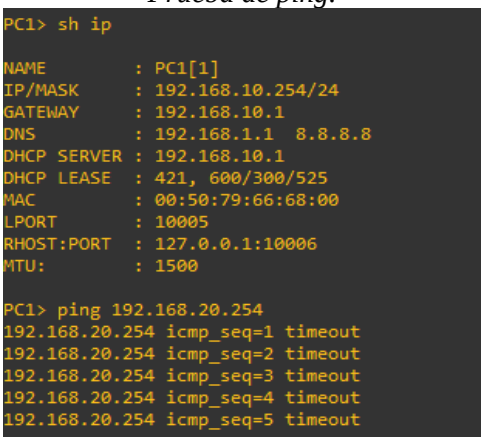
Fuente: El autor

5.4.2.1.2. Ping (ICMP)

En la Figura 19 se comprueba que al hacer una petición ICMP desde el equipo que pertenece a la VLAN10 no tiene respuesta desde el equipo que pertenece a la VLAN 20, y se verifica que las subredes están aisladas entre sí.

Figura 19

Prueba de ping.



Fuente: El autor

5.4.3. Pfsense

5.4.3.1.Instalación y configuración del Pfsense

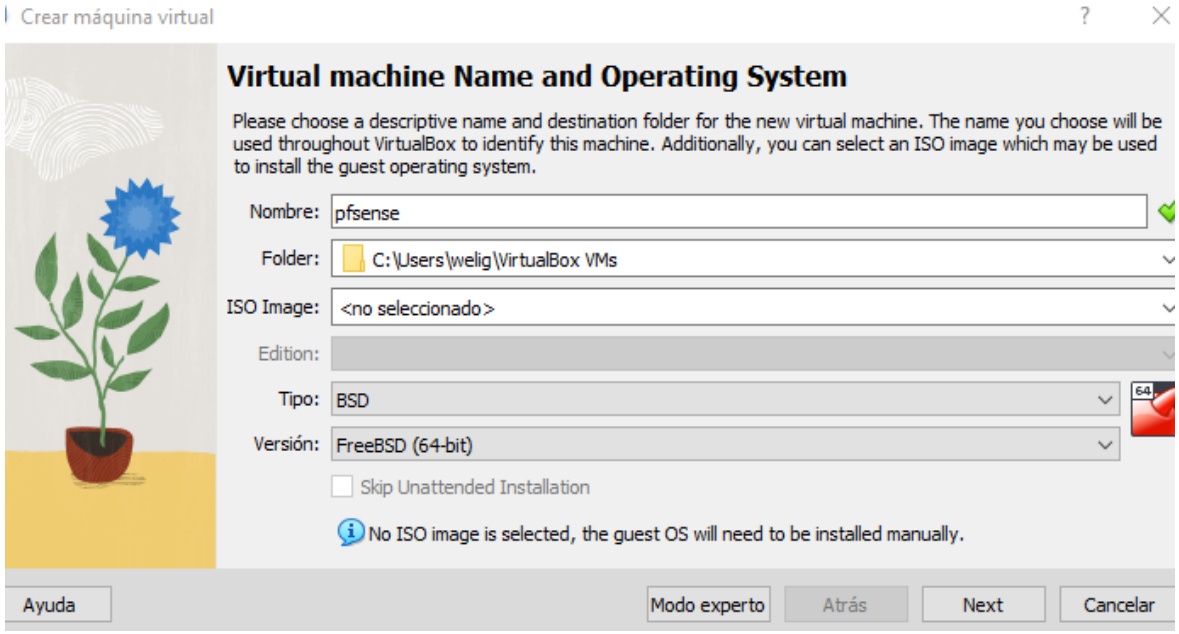
Se procede a descargar la ISO con la arquitectura AMD (64bits) del Pfsense de la página oficial https://www.Pfsense.org/download/, posteriormente se la instala en una máquina virtual de Virtual Box, a continuación, se presenta el proceso de instalación:

5.4.3.1.1. Instalación

Utilizando Virtual Box se crea una máquina virtual Pfsense, tal cual se muestra en la Figura 20.

Figura 20

Creando máquina virtual en Virtual Box

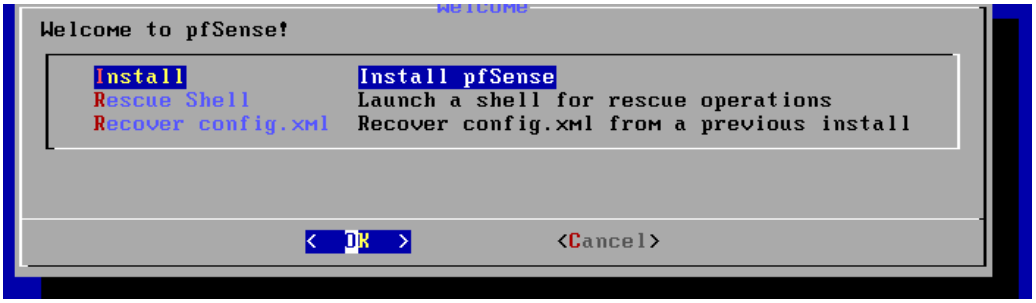


Fuente: El autor

Después de cargar el archivo en el Virtual Box se procede a iniciar la máquina, el proceso de instalación se presenta desde la Figura 21 a la Figura 25.

Figura 21

Proceso de instalación de Pfsense

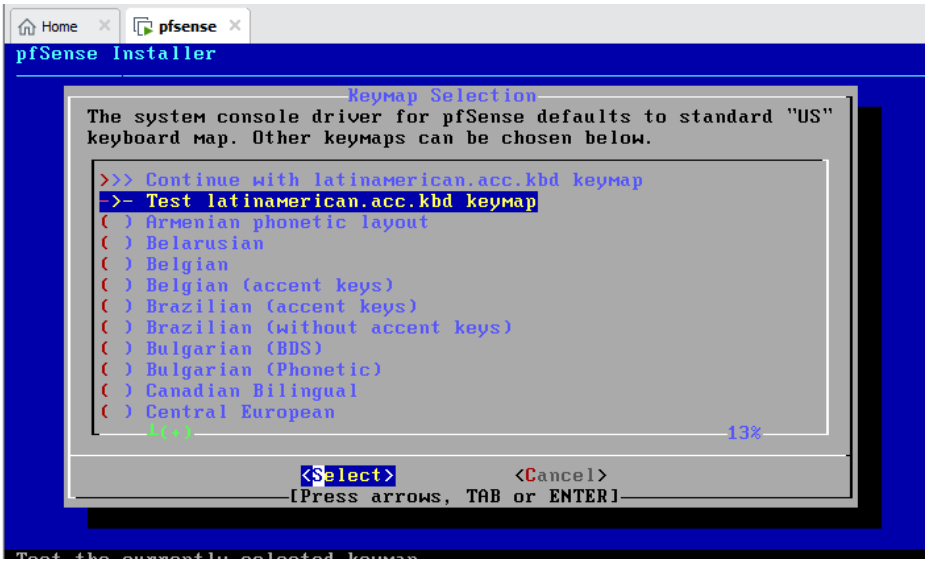


Fuente: El autor

Se procede a elegir el idioma latinamericam.acc.kbd, utilizado para la distribución del teclado dentro del Pfense, tal cual se muestra en la Figura 22.

Figura 22

Selección del idioma del teclado.

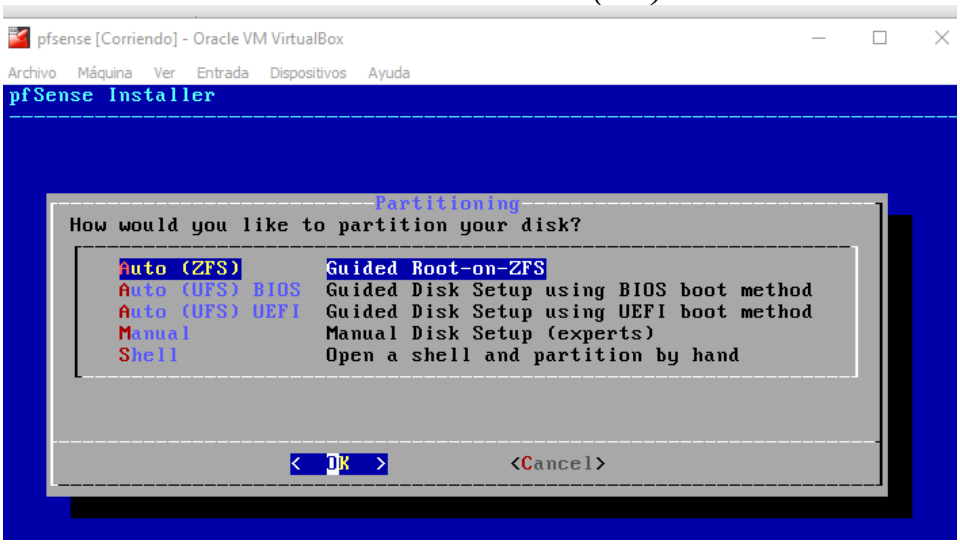


Fuente: El autor

En la Figura 23 se selecciona la partición del disco, en nuestro caso se seleccionó de manera automática creando una sola partición para montar el firewall Pfsense.

Figura 23

Selección del modo auto (ZFS)

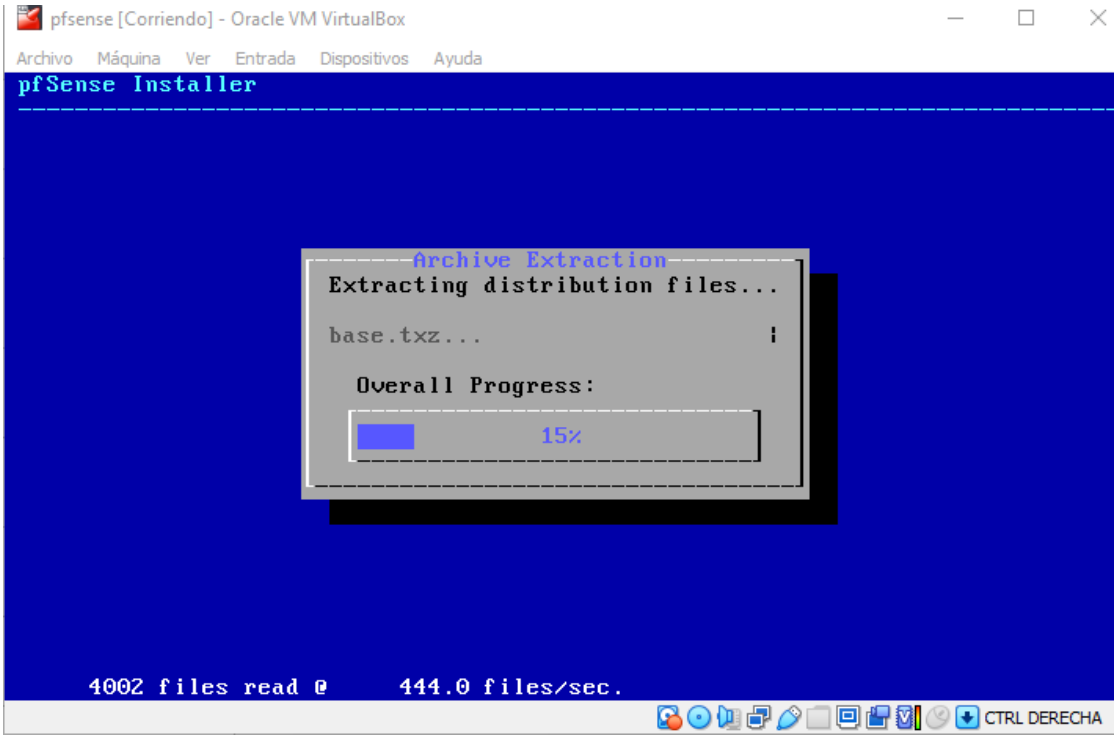


Fuente: El autor

Como se observa es necesario la extracción de los archivos dentro del firewall Pfsense, posteriormente inicia la instalación tal cual se muestra en la Figura 25.

Figura 24

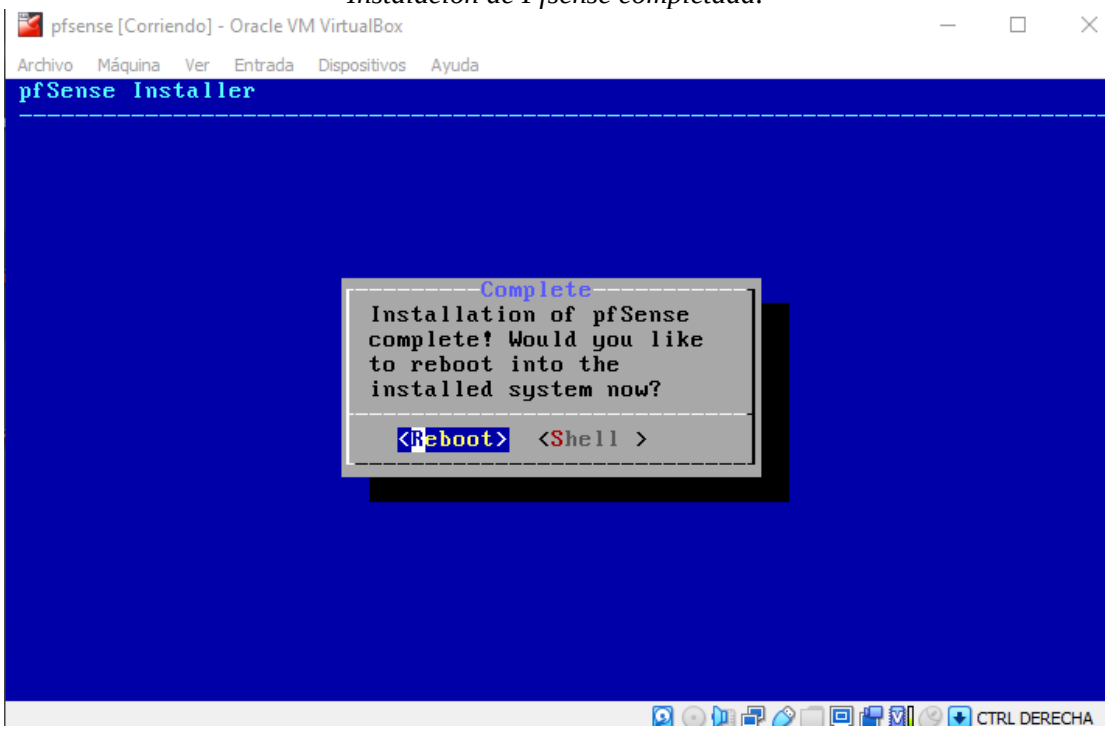
Proceso de instalación y carga de los archivos de Pfsense.



Fuente: El autor

Figura 25

Instalación de Pfsense completada.



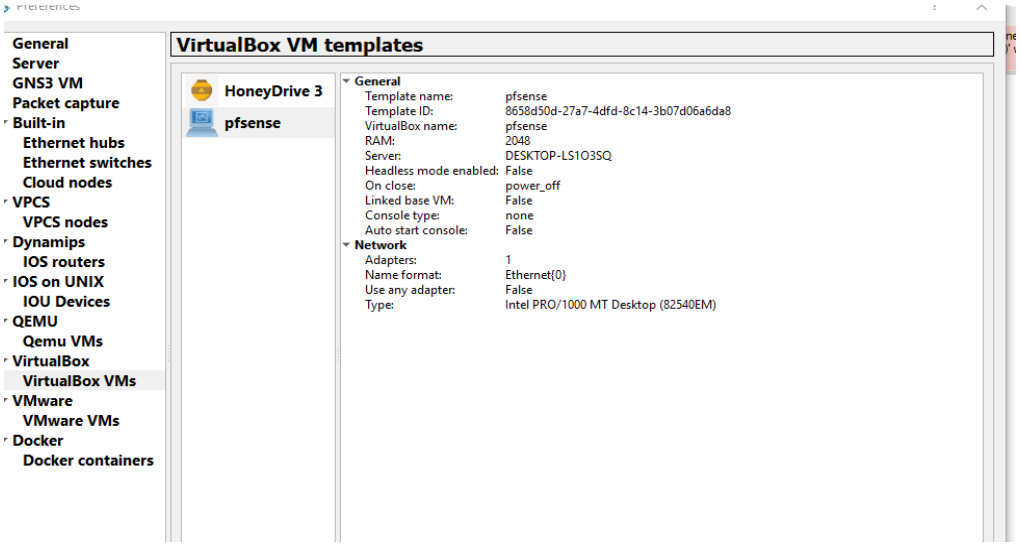
Fuente: El autor

5.4.3.1.2. Configuración

Después de haber finalizado el proceso de instalación se debe agregar la máquina virtual Pfsense en el menú preferencias dentro de VirtualBox en VirtualBox VMs templates.

Figura 26

Configuración de Pfsense en GNS3.

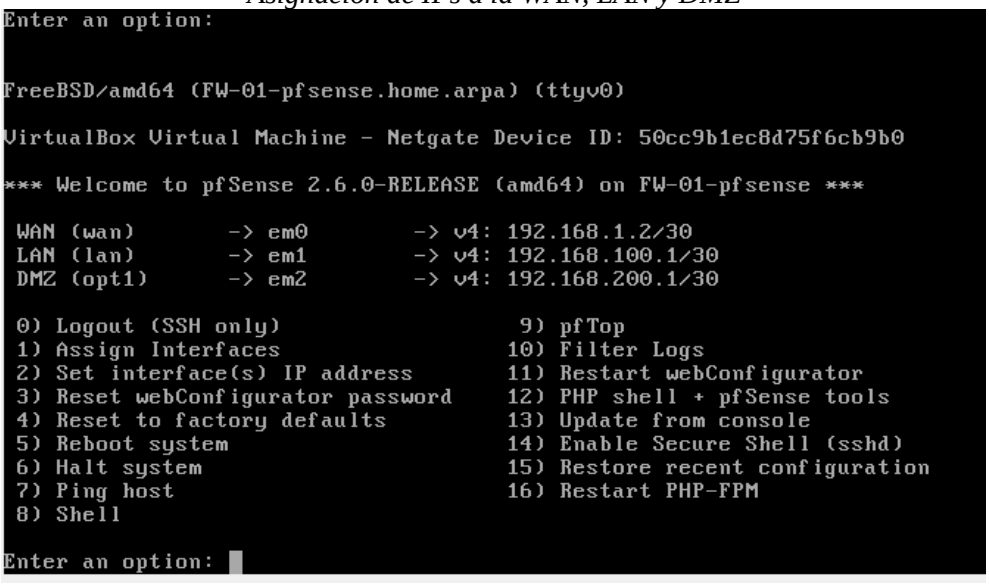


Fuente: El autor

Se configuró la WAN con IP estática 192.168.X.2/30 y la subred con la IP 192.168.100.0/30 para la interfaz LAN, tal cual se presenta en el diseño de la Figura 6, posteriormente se realizó un ping al Domain Name Server (DNS) público de la empresa google para verificar la conectividad a internet.

Figura 27

Asignación de IPs a la WAN, LAN y DMZ

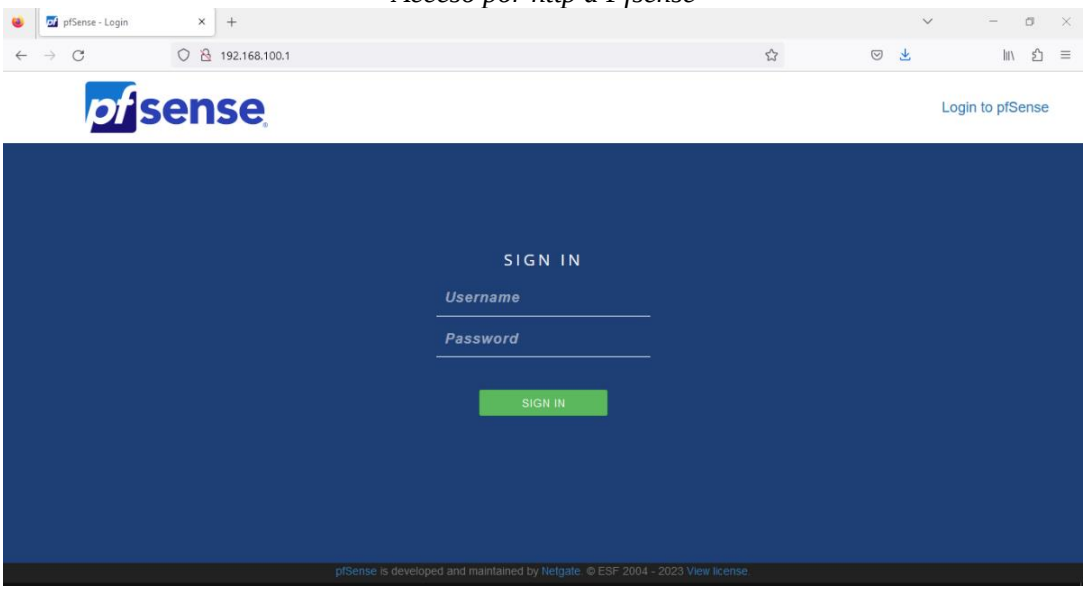


Fuente: El autor

Una vez configurada la interfaz LAN con la dirección IP correspondiente, se accede por http, en la Figura 28 se presenta el acceso desde el navegador, verificando que Pfsense se instaló correctamente en GNS3.

Figura 28

Acceso por http a Pfsense

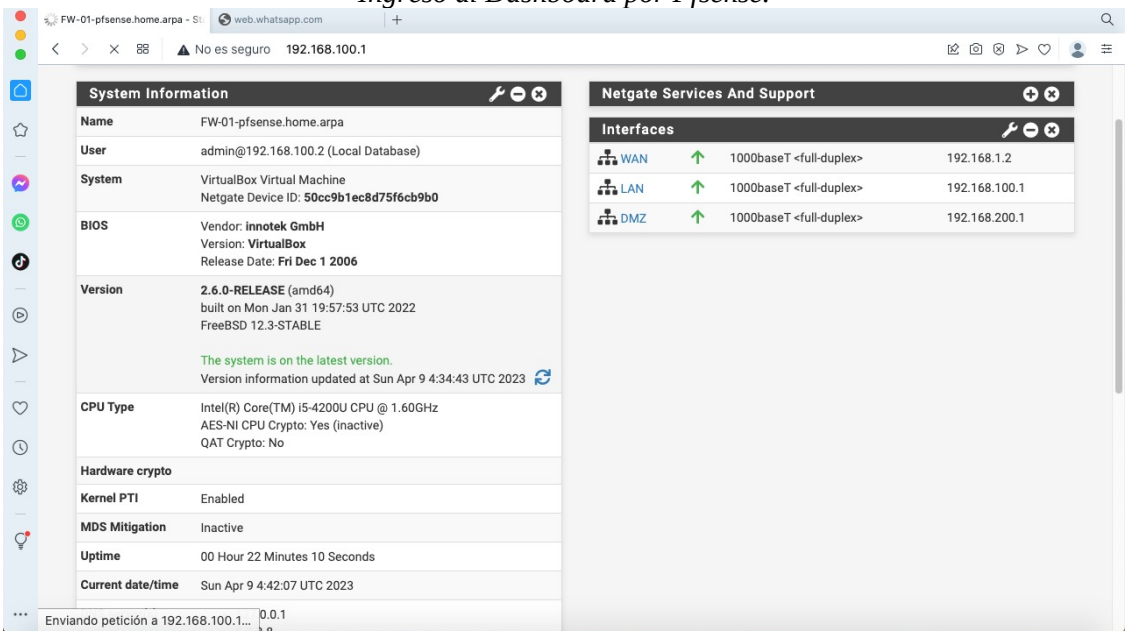


Fuente: El autor

En la Figura 29 se presenta que la configuración ingresada en Pfsense se realizó correctamente y se encuentran configurados los parámetros de red para la WAN, LAN y DMZ.

Figura 29

Ingreso al Dashboard por Pfsense.



Fuente: El autor

5.4.4. Honeypot

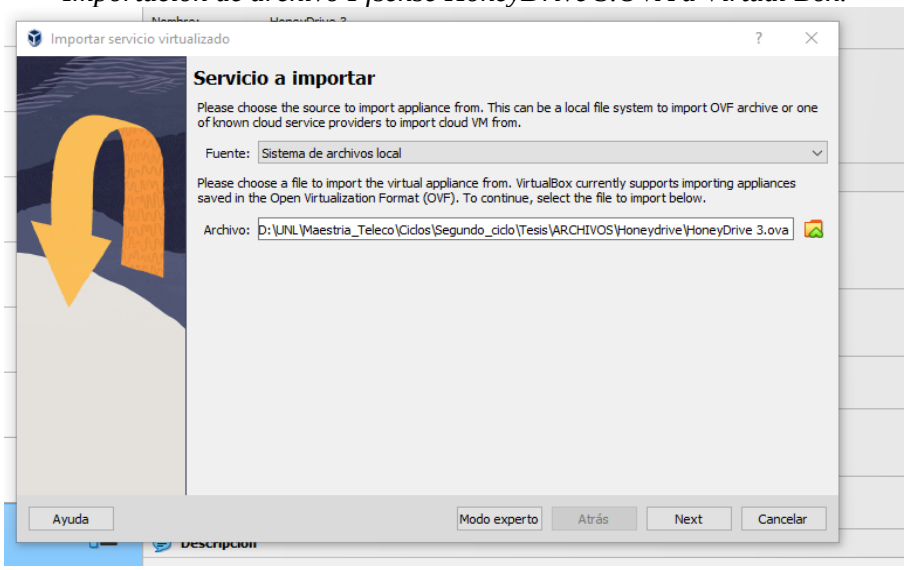
5.4.4.1.Instalación y configuración del Honeypot.

5.4.4.1.1. Instalación

Se descarga el archivo HoneyDrive3.OVA desde la página web https://sourceforge.net/projects/honeydrive/ para montarlo sobre VirtualBox, después se importa el archivo en el visualizador tal como se muestra en la Figura 30.

Figura 30

Importación de archivo Pfsense HoneyDrive 3.OVA a Virtual Box.



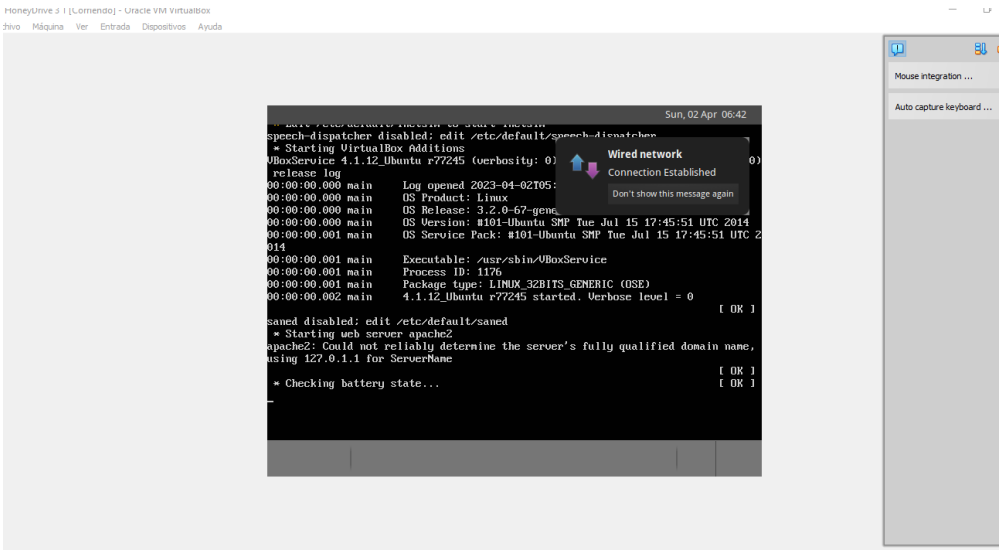
Fuente: El autor

Una vez configurado los parámetros necesarios se procede a iniciar la máquina virtual, en la

Figura **31** se muestra parte del proceso de inicialización del honeypot honeydrive.

Figura 31

Proceso de inicialización de honeypot



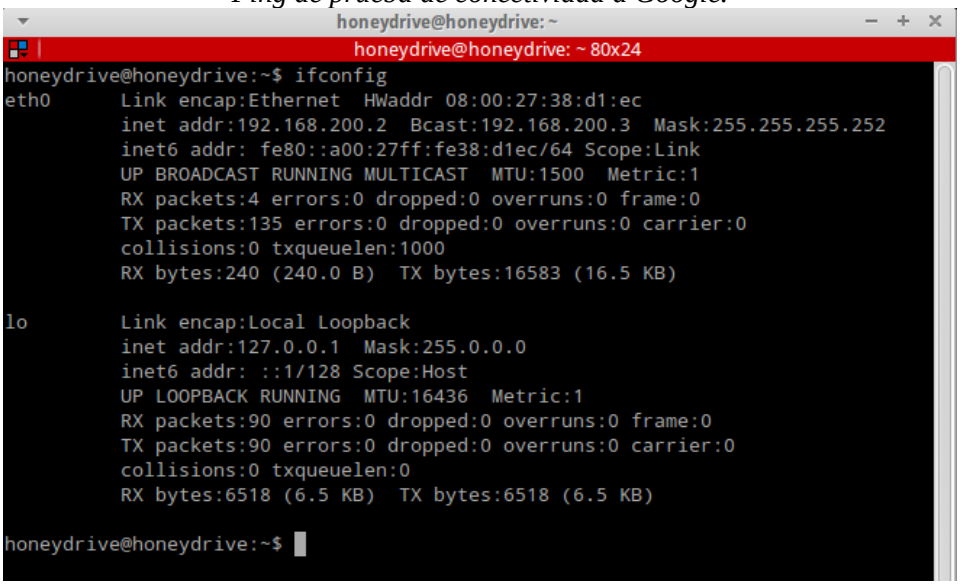
Fuente: El autor

5.4.4.1.2. Configuración

Una vez que se inicializa el honeypot honeydrive este se abre automáticamente, como se puede observar en la Figura 32 tenemos el servidor funcionando correctamente y se hace un ping al DNS público de la empresa google para verificar la conectividad a internet.

Figura 32

Ping de prueba de conectividad a Google.

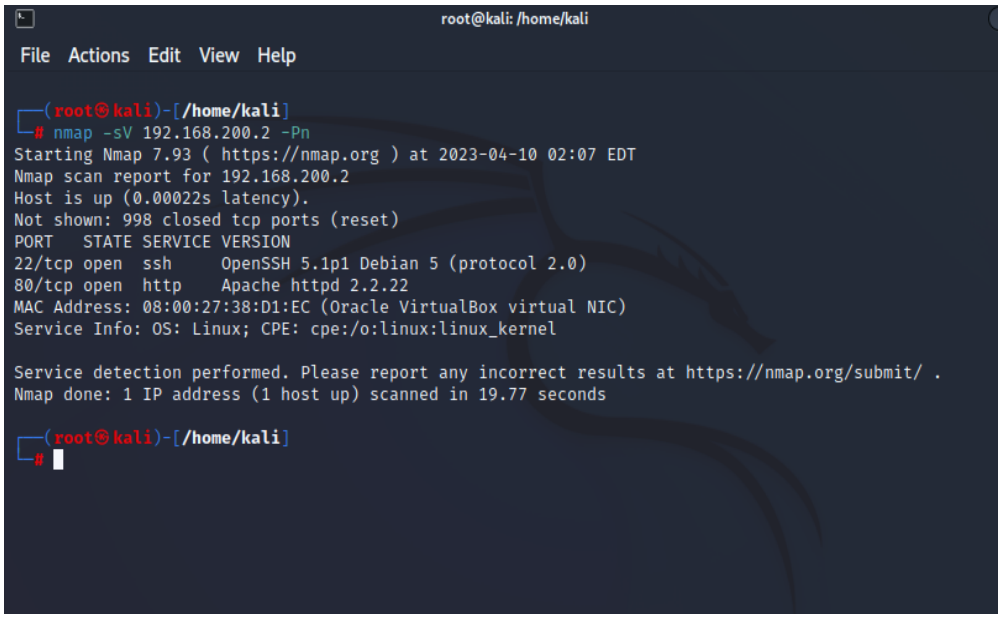


Fuente: El autor

En la Figura 33 se pueden constatar que se utilizó la herramienta nmap para el análisis de los puertos y servicios que están habilitados en el honeypot honeydrive, verificando que los servicios SSH y HTTP están habilitados en el puerto 22 y 80 correspondientemente.

Figura 33

Identificación de puertos y servicios a honeypot.



Fuente: El autor

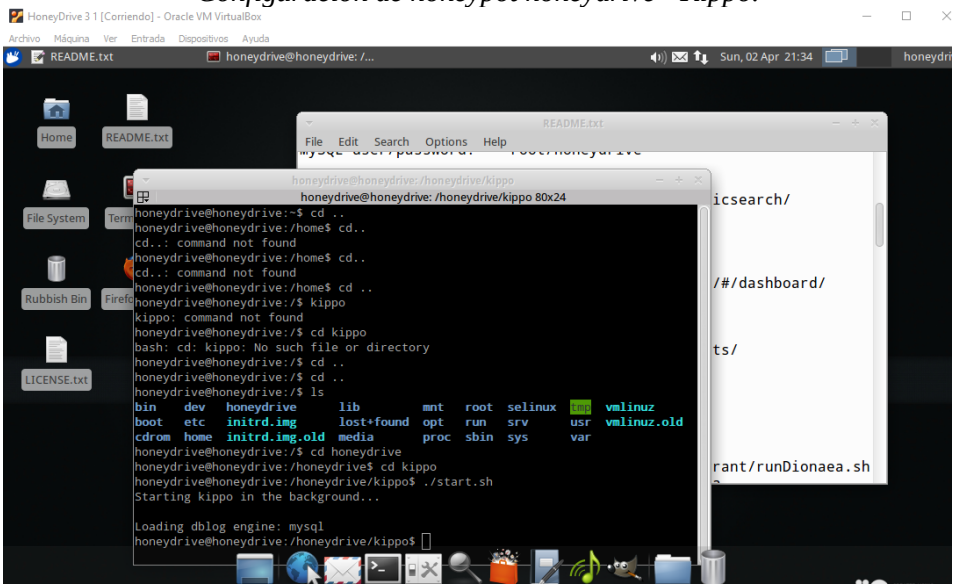
5.5.Honeypot honeydrive - Kippo.

Se inicia el honeypot Kippo, para esto se abre la consola terminator y se coloca el siguiente directorio /honeydrive/kippo, posteriormente se escribe el siguiente comando: ./start.sh tal como se muestra en la

Figura **34**.

Figura 34

Configuración de honeypot honeydrive - Kippo.

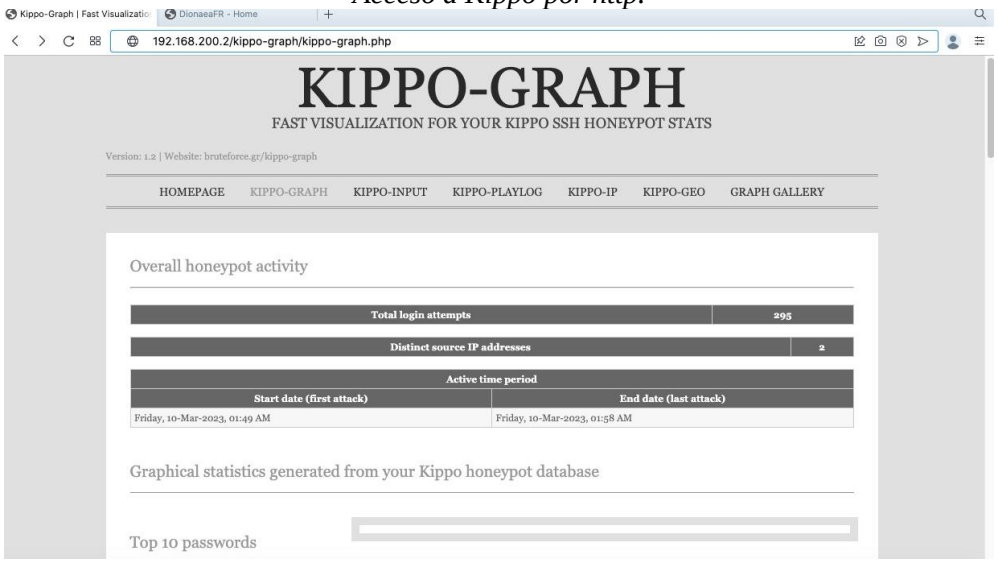


Fuente: El autor

Cuando se inicializa el honeypot honeydrive - Kippo ya se puede acceder por la web utilizando la dirección IP asignada.

Figura 35

Acceso a Kippo por http.



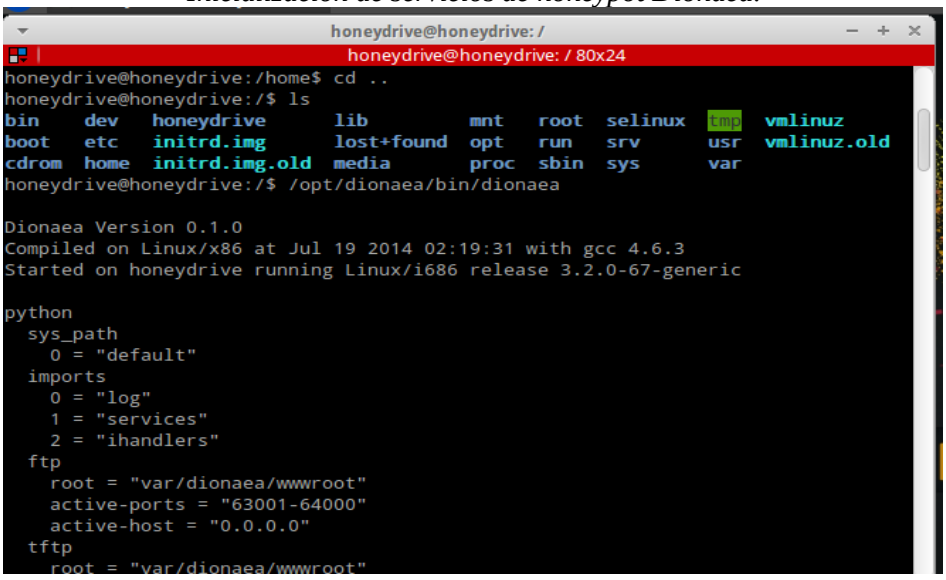
Fuente: El autor

5.6.Honeypot honeydrive - Dionaea

En la Figura 36 se presenta el proceso para inicializar el honeypot honeydrive - Dionaea.

Figura 36

Inicialización de servicios de honeypot Dionaea.

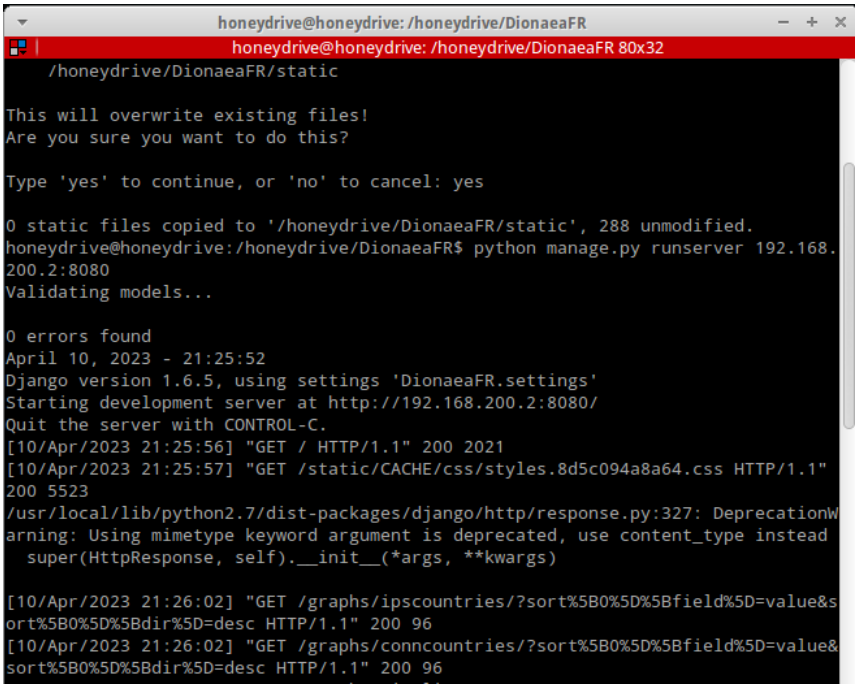


Fuente: El autor

Se debe habilitar el acceso a la interfaz web por el puerto 8080, en la Figura 37 se muestra este proceso, mientras que en la Figura 38 se muestra la interfaz gráfica desde el navegador Opera.

Figura 37

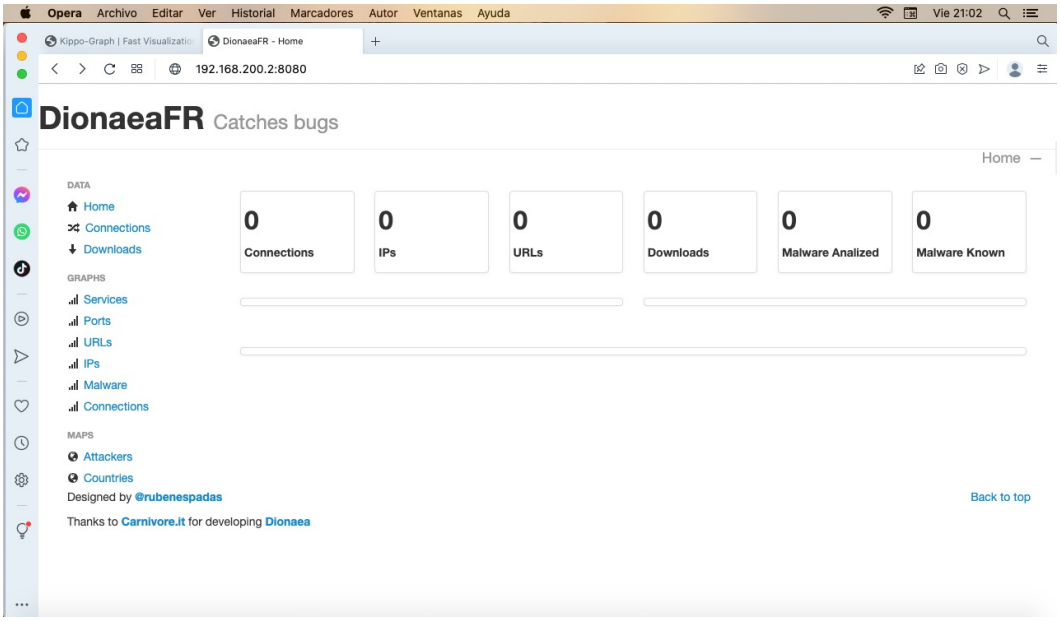
Configuración para acceder a la interfaz web por el puerto 8080.



Fuente: El autor

Figura 38

Interfaz gráfica de Dionaea.



Fuente: El autor

6. Resultados

6.1. Analizar y diseñar un mecanismo de seguridad informática que permita la recolección de patrones del atacante denominado honeypot para la empresa SIITE.

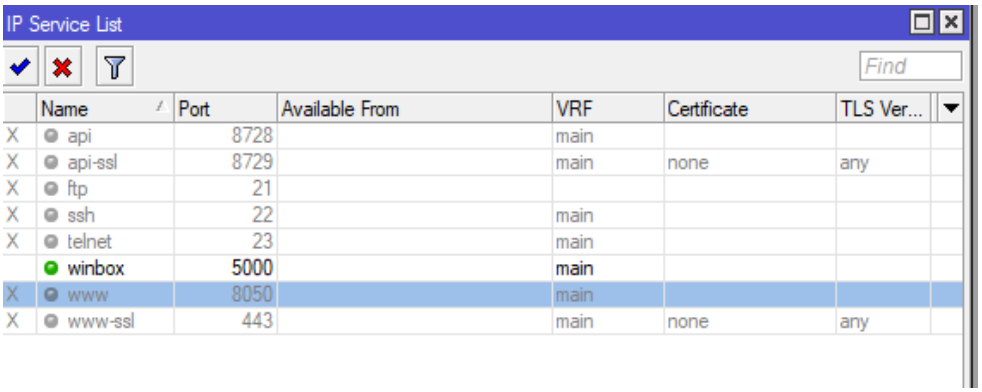
En base al diseño de la red SOHO planteado en la metodología, a continuación, se detallan las políticas de seguridad de cada uno de los elementos activos de la red:

6.1.1. Análisis e implementación de políticas de seguridad en el router Mikrotik.

A continuación, se describen algunas políticas de seguridad implementadas en el router Mikrotik, cuyo objetivo es proteger la red SOHO y mitigar el riesgo de que ciber atacantes accedan a los recursos e información de la empresa SIITE.

Es importante como administradores de la red controlar el acceso al router, para esto se deshabilitaron algunos servicios y solo se dejó habilitado el acceso por el puerto 5000 con el servicio winbox el cual permite mediante la interfaz gráfica la visualización de la configuración de los dispositivos Mikrotik.

Figura 39
Deshabilitar servicios acceso al Mikrotik

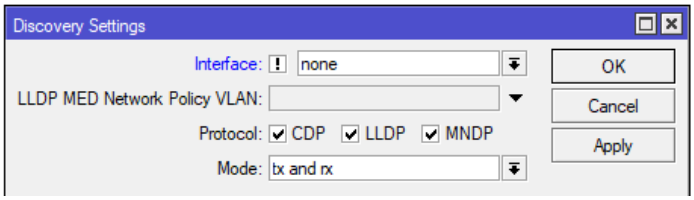


Fuente: El autor

Es importante tomar en cuenta que los vecinos (neighbors) activos se mantengan ocultos en la red, de manera que no sean vistos por otros equipos de interconexión, protegiendo la integridad de los datos e información de los usuarios y/o equipos terminales, en la

Figura 40 se muestra los parámetros ingresados para ocultar los neighbors.

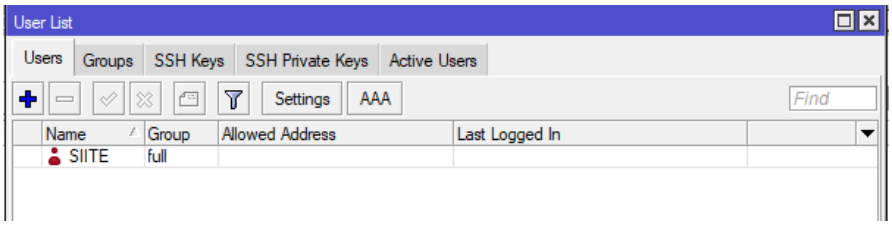
Figura 40
Ocultando neighbors activos



Fuente: El autor

Una de las políticas de seguridad para nuestros equipos de la red es realizar el cambio de las credenciales de acceso, así como los nombres de usuarios que vienen por defecto, por ende, se procedió a cambiar el nombre de usuario del router Mikrotik, tal como se muestra en la Figura 41.

Figura 41
Cambio de usuario

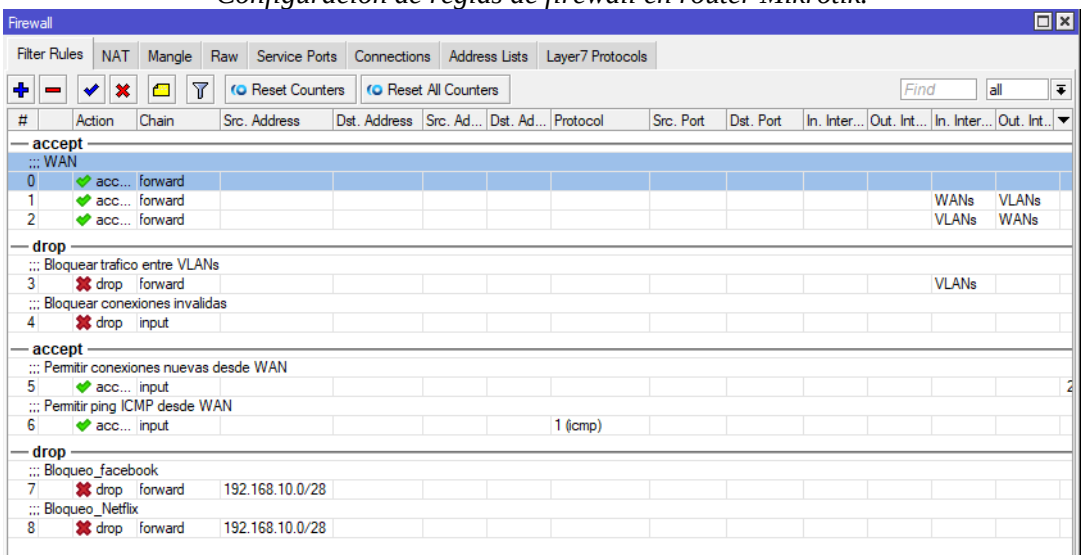


Fuente: El autor

Es importante manejar políticas de seguridad en la red WAN y LAN, brindando seguridad a los dispositivos, sistemas y datos de la empresa contra amenazas externas e internas, en la Figura 42 se muestran las reglas configuradas en el firewall.

Figura 42

Configuración de reglas de firewall en router Mikrotik.



Fuente: El autor

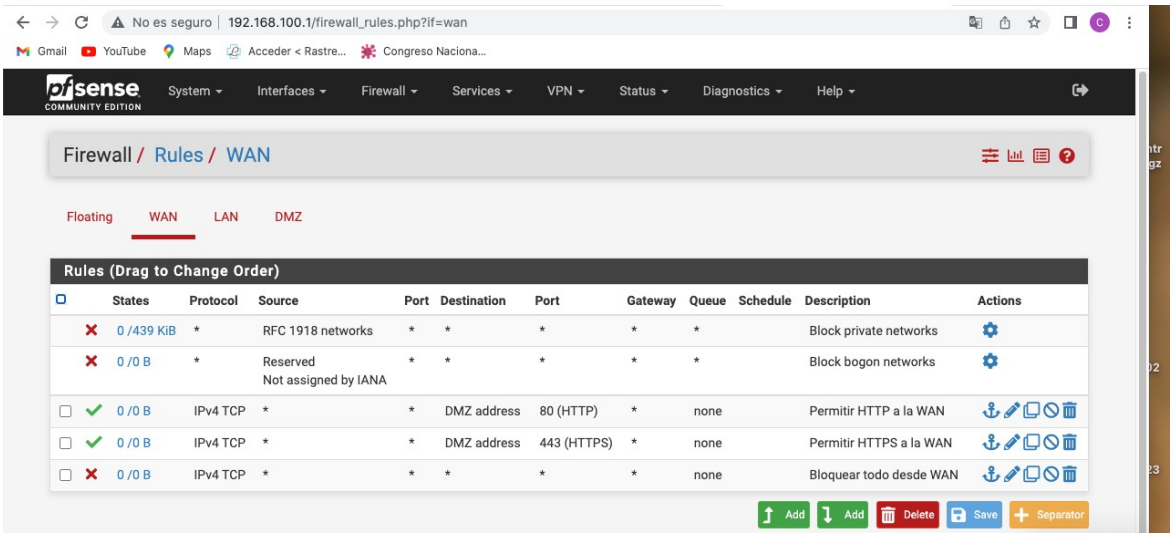
6.1.2. Análisis e implementación de políticas de seguridad en el firewall Pfsense

Una vez realizado el diseño de la red se plantean las políticas de seguridad en la red WAN, LAN Y DMZ, tomando como referencia el diseño o topología de red presentado en la Figura 6, a continuación, en la Figura 43 a la

Figura 45 se presentan los parámetros configurados en el firewall Pfsense:

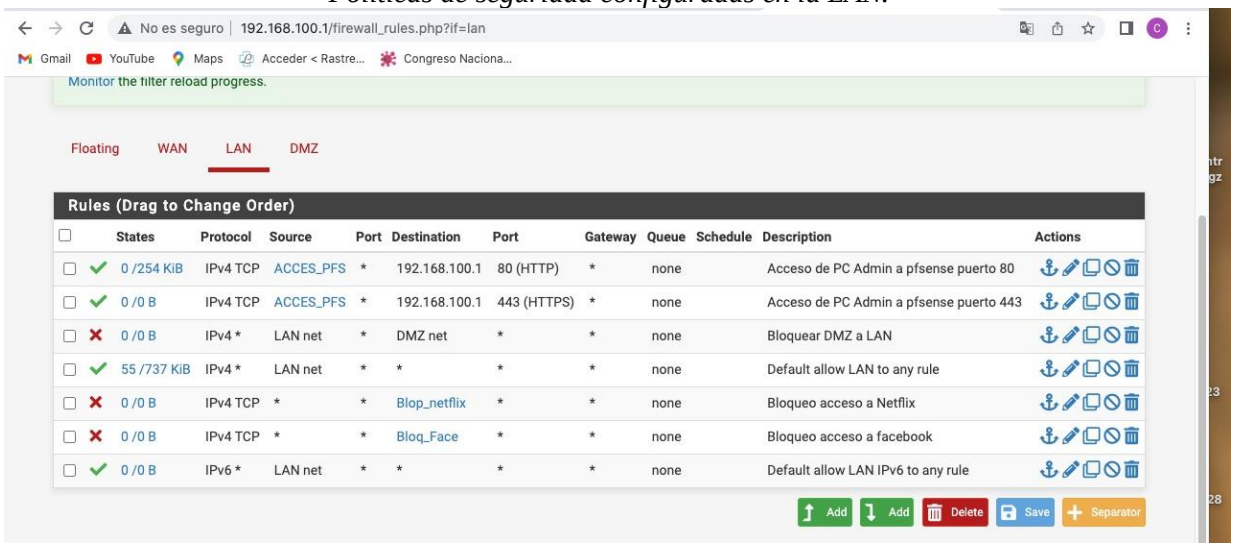
Figura 43

Políticas de seguridad configuradas en la WAN.



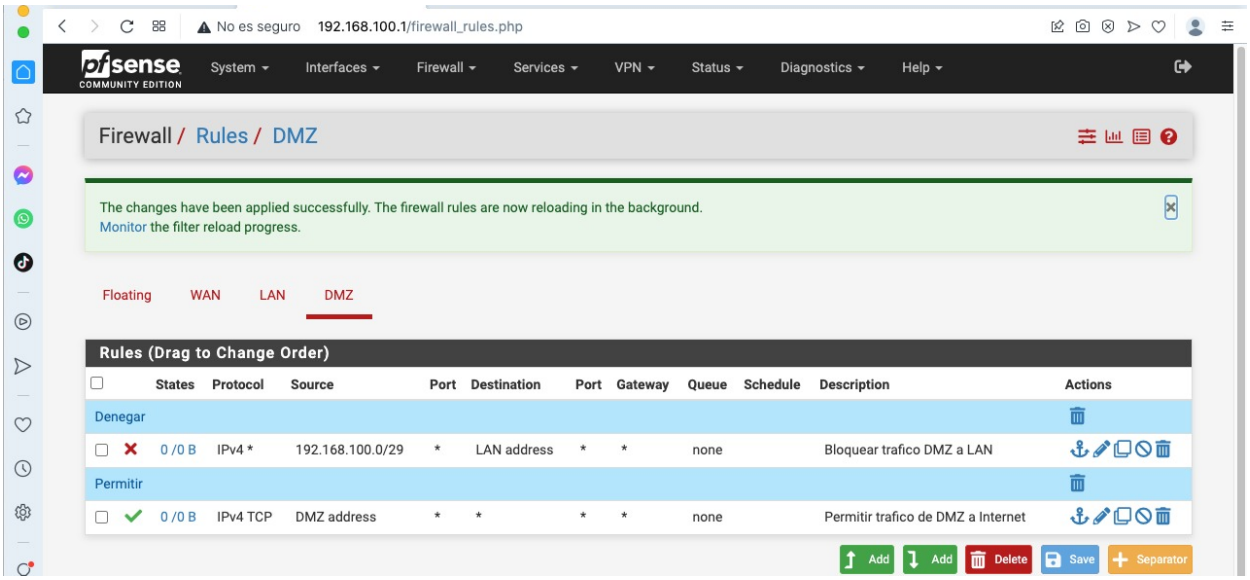
Fuente: El autor

Figura 44
Políticas de seguridad configuradas en la LAN.



Fuente: El autor

Figura 45
Políticas de seguridad configuradas en la DMZ.



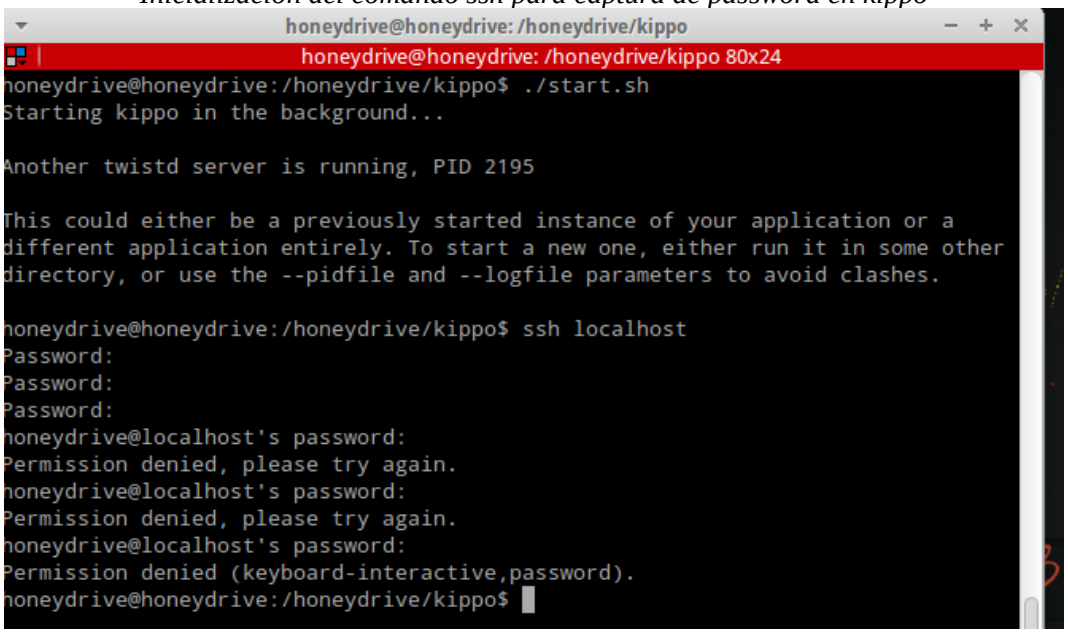
Fuente: El autor

6.1.3. Análisis de los resultados de honeypot honeydrive - Kippo

A continuación, se realiza un ataque de fuerza bruta al servicio SSH del honeypot honeydrive - kippo, el cual consiste en ingresar algunas credenciales (password), para esto se debe dirigir al directorio /honeydrive/kippo, e inicializar kippo con ./start.sh y colocar el siguiente comando: ssh localhost, inmediatamente el sistema pide que se ingrese algunos password los cuales quedan registrados en el servidor kippo.

Figura 46

Inicialización del comando ssh para captura de password en kippo

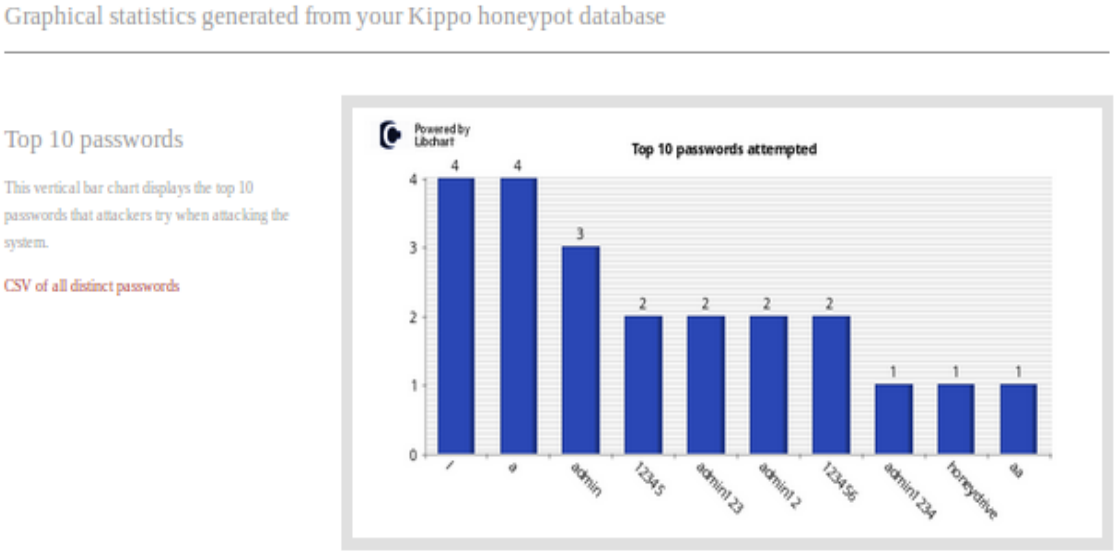


Fuente: El autor

En la Figura 47 se muestran las credenciales capturadas por el honeypot honeydrive – kippo en el proceso anterior representado en la Figura 46, obteniendo una base de datos de las contraseñas más comunes utilizadas por los intrusos al momento de atacar una red LAN.

Figura 47

Top password utilizados

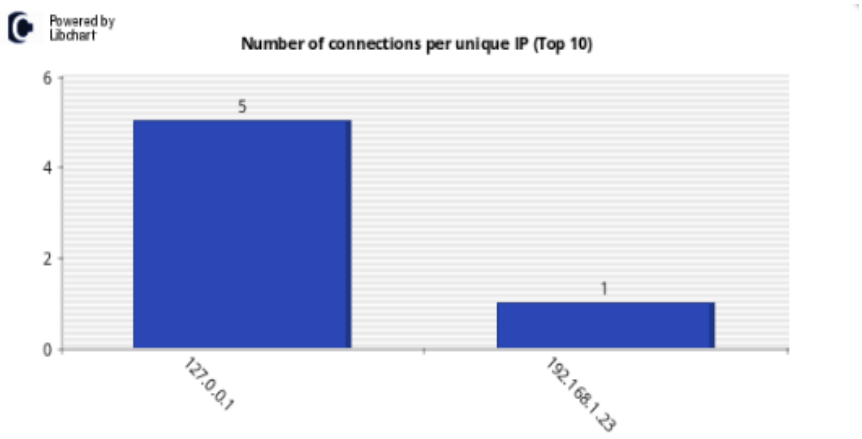


Fuente: El autor

En la Figura 48 se muestran las IPs utilizadas durante el ataque SSH, estas quedan registradas en el honeypot honeydrive - Kippo y pueden ser observadas desde la interfaz web.

Figura 48

IPs registradas en honeypot Kippo.



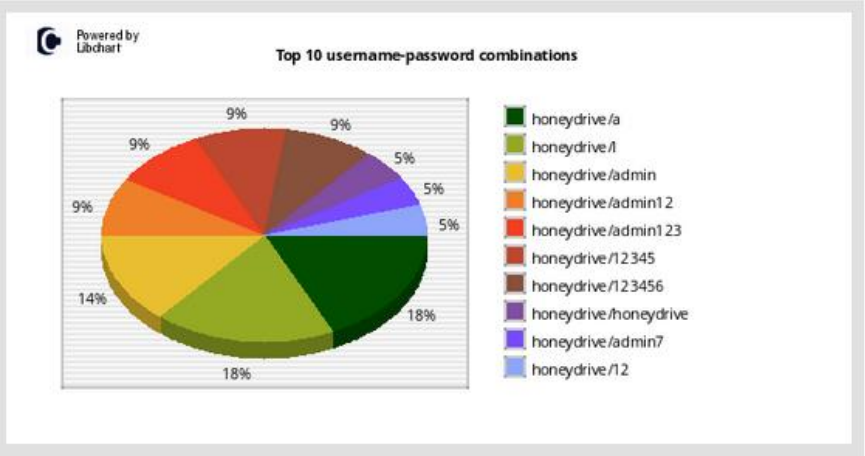
Fuente: El autor

Como se observa en la

Figura **49** también podemos obtener el top 10 de combinaciones de los nombres de usuario (username) y contraseñas (passwords) utilizados durante el ataque SSH.

Figura 49

Top 10 combinaciones de usuarios y contraseñas.



Fuente: El autor

Dentro de la interfaz web podemos obtener información de geolocalización como es el número de pruebas, la ciudad, región, direcciones IPs públicas o privadas e incluso se puede verificar si el ataque se produce con malware malintencionado., esto se muestra en la Figura 50.

Figura 50

Información de Geolocalización.

Geolocation information gathered from the top 10 IP addresses probing the system

The following table displays the top 10 IP addresses connected to the system (ordered by volume of connections).

ID	IP Address	Probes	City	Region	Country Name	Code	Latitude	Longitude	Hostname	Lookup
1	127.0.0.1	5							127.0.0.1	
2	192.168.1.23	1							192.168.1.23	

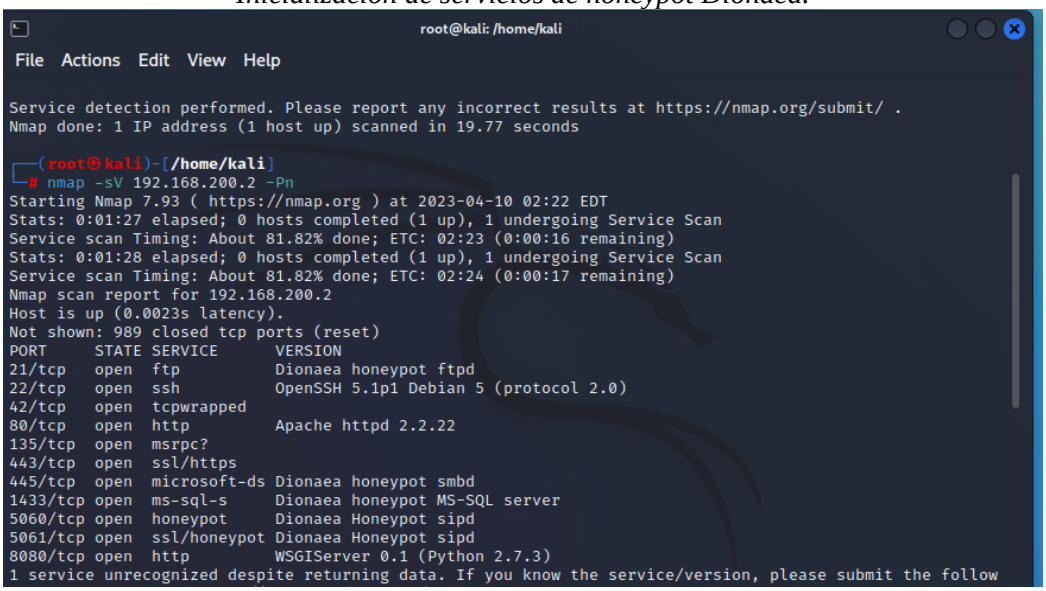
Fuente: El autor

6.1.4. Análisis de los resultados de honeypot honeydrive - Dionaea.

El uso del honeypot honeydrive- Dionaea permite simular una variedad de servicios, en la Figura 51 se muestra los servicios iniciados por este honeypot, estos estarán abiertos para que el intruso pueda acceder con facilidad mientras que los administradores de la red observan cada uno de sus movimientos y estrategias de ataque.

Figura 51

Inicialización de servicios de honeypot Dionaea.

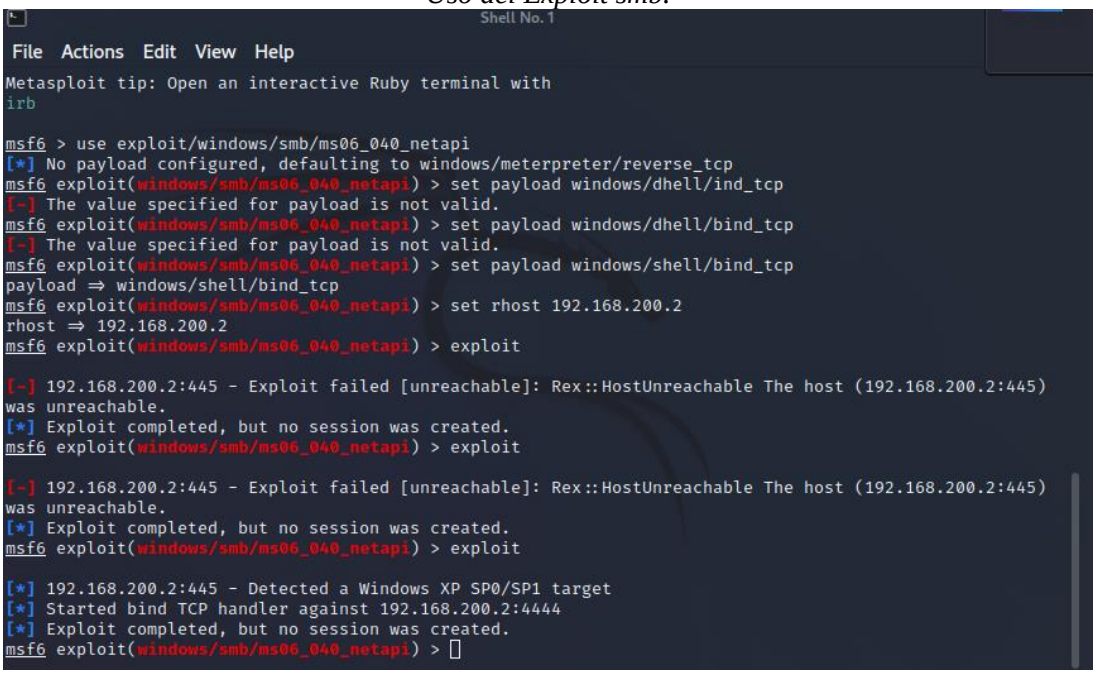


Fuente: El autor

En la Figura 51 se constata que existe el servicio mircosoft-ds activo, como ejemplo se va a utilizar un exploit para ingresar por el protocolo SMB el cual regula el acceso a archivos y directorios, recursos de la red como impresoras, enrutadores o interfaces liberados para la red, en la Figura 52 se ingresa los códigos necesarios para iniciar este ataque utilizando el módulo **exploit/windows/smb/ms06_040_netapi**.

Figura 52

Uso del Exploit smb.

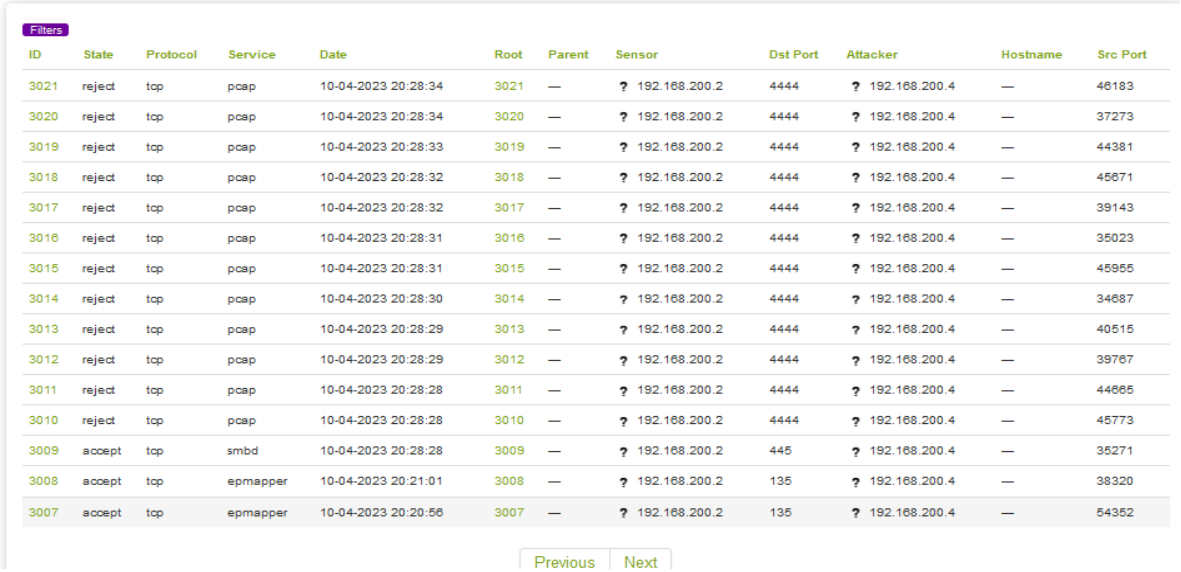


Fuente: El autor

En la Figura 53 se presenta información capturada por el honeypot honeydrive - Dionaea como las IPs, puertos y servicios que quedan registrados en la base de datos del honeypot, información importante para el análisis de las brechas de seguridad y de vulnerabilidades en la empresa.

Figura 53

Ips, protocolos, puertos y servicios registrados en Dionaea.



Filters

ID	State	Protocol	Service	Date	Root	Parent	Sensor	Dst Port	Attacker	Hostname	Src Port
3021	reject	tcp	pcap	10-04-2023 20:28:34	3021	—	? 192.168.200.2	4444	? 192.168.200.4	—	46183
3020	reject	tcp	pcap	10-04-2023 20:28:34	3020	—	? 192.168.200.2	4444	? 192.168.200.4	—	37273
3019	reject	tcp	pcap	10-04-2023 20:28:33	3019	—	? 192.168.200.2	4444	? 192.168.200.4	—	44381
3018	reject	tcp	pcap	10-04-2023 20:28:32	3018	—	? 192.168.200.2	4444	? 192.168.200.4	—	45671
3017	reject	tcp	pcap	10-04-2023 20:28:32	3017	—	? 192.168.200.2	4444	? 192.168.200.4	—	39143
3016	reject	tcp	pcap	10-04-2023 20:28:31	3016	—	? 192.168.200.2	4444	? 192.168.200.4	—	35023
3015	reject	tcp	pcap	10-04-2023 20:28:31	3015	—	? 192.168.200.2	4444	? 192.168.200.4	—	45955
3014	reject	tcp	pcap	10-04-2023 20:28:30	3014	—	? 192.168.200.2	4444	? 192.168.200.4	—	34687
3013	reject	tcp	pcap	10-04-2023 20:28:29	3013	—	? 192.168.200.2	4444	? 192.168.200.4	—	40515
3012	reject	tcp	pcap	10-04-2023 20:28:29	3012	—	? 192.168.200.2	4444	? 192.168.200.4	—	39767
3011	reject	tcp	pcap	10-04-2023 20:28:28	3011	—	? 192.168.200.2	4444	? 192.168.200.4	—	44665
3010	reject	tcp	pcap	10-04-2023 20:28:28	3010	—	? 192.168.200.2	4444	? 192.168.200.4	—	45773
3009	accept	tcp	smbd	10-04-2023 20:28:28	3009	—	? 192.168.200.2	445	? 192.168.200.4	—	35271
3008	accept	tcp	epmapper	10-04-2023 20:21:01	3008	—	? 192.168.200.2	135	? 192.168.200.4	—	38320
3007	accept	tcp	epmapper	10-04-2023 20:20:56	3007	—	? 192.168.200.2	135	? 192.168.200.4	—	54352

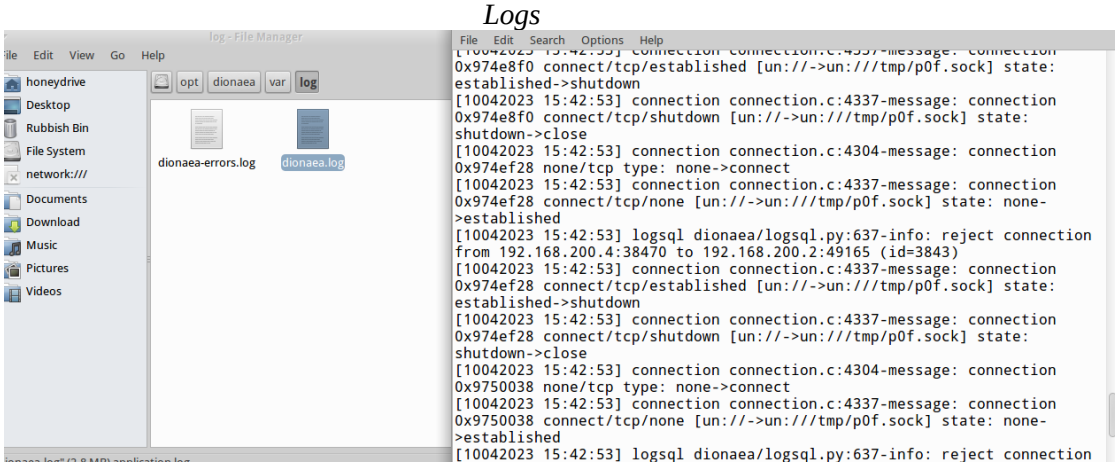
Previous Next

Fuente: El autor

El honeypot honeydrive - Dionaea almacena la información capturada de los ataques y lo almacena en su base de datos y en un historial de registro (log), en la Figura 54 se presenta el registro del ataque realizado para que posteriormente pueda ser analizado por los administradores de red y plantear o actualizar sus métodos de seguridad en la red de la empresa.

Figura 54

Logs



Fuente: El autor

6.2. Plantear políticas de seguridad que permitan a la empresa SIITE mitigar posibles ataques cibernéticos.

A continuación, se plantean o sugieren algunas políticas de seguridad que pueden ser implementadas y/o utilizadas en la empresa SIITE:

6.2.1. Políticas de seguridad de los Equipos de red

La seguridad física de los equipos de red es esencial para garantizar la seguridad de las información y datos de una empresa u organización, entre algunas de las políticas de seguridad que se recomienda a la empresa SIITE son:

- Los equipos de red deben ser ubicados en un lugar seguro y protegido, como en un rack o armario de telecomunicaciones o en lo posible en un cuarto de telecomunicaciones, donde solo personal autorizado tenga acceso.
- Se puede instalar un sistema de monitoreo de video para supervisar el acceso a la sala o al armario de los equipos de red.
- Delegar personal del área de las TICs para supervisar las actividades realizadas por personal técnico ajeno a la empresa u organización cuando estos sean autorizados a realizar mantenimiento a los equipos de la red.
- Se debe realizar respaldos regulares de la configuración de los equipos de la red, esto permitirá restablecer el sistema y protegerlos contra posibles fallas del sistema o daños físicos.
- Se debe realizar un mantenimiento regular a los equipos de red a fin de garantizar que estén funcionando correctamente, garantizar la disponibilidad de los recursos de la red y la seguridad de la red.
- Está prohibido que personal no autorizado de la empresa u organización intente modificar los parámetros de los equipos de telecomunicaciones, esto le compete únicamente a personal de las TICs.

6.2.2. Políticas de seguridad de Equipos terminales

- Se deben establecer medidas de control de acceso, como el uso de contraseñas seguras, el bloqueo automático de pantalla y la autenticación de usuarios para evitar que personas no autorizadas puedan acceder a los dispositivos.

- Se recomienda llevar a cabo inspecciones y mantenimiento regular de los equipos terminales para garantizar el funcionamiento y detectar cualquier problema de seguridad.
- Proporcionar capacitación y concienciación a los empleados sobre las políticas de seguridad para equipos terminales y la importancia de proteger la información considerada como el elemento activo más importante de una empresa.
- Proteger a los equipos terminales con un antivirus centralizado, esto permite tener la visibilidad de las amenazas detectadas, actualización y seguridad de los equipos de la red.
- Establecer políticas claras sobre el uso adecuado de los equipos de usuario, incluyendo la prohibición de la instalación de software no autorizado por el departamento de las TICs.

6.2.3. Políticas de seguridad para servicios y servidores

- Es indispensable la actualización de software y parches de seguridad de forma regular para corregir vulnerabilidades y mitigar el riesgo de ataques.
- Los datos almacenados en el servidor deben ser protegidos mediante encriptación y copias de seguridad regulares para garantizar la integridad y disponibilidad de los datos.
- Mantener activos solo los servicios y puertos que se estén ocupando, evitando que sea la puerta de entrada para personas no autorizadas en la red.
- Trabajar con protocolos seguros como HTTPS para servicios de la web o SMTPS para la prestación de servicio de correo electrónico.
- Implementar herramientas de monitoreo de seguridad y análisis de registros para detectar posibles amenazas y tomar medidas o estrategias preventivas para contrarrestar los ataques.

6.2.4. Políticas de Backups

- Realizar copias de seguridad de manera semanal, estas deben ser definidas en función del volumen de datos que se manejan y de la importancia de la información.
- Las copias de seguridad deben ser almacenadas en un lugar seguro y protegido contra daños físicos, robo y acceso no autorizado.
- Se deben realizar pruebas regulares para verificar que las copias de seguridad se puedan restaurar correctamente y que los datos estén íntegros.
- Es importante documentar todas las políticas de backup y las estrategias adoptadas para garantizar que el personal tenga acceso a esta información.

6.3. Identificar los riesgos cibernéticos más recurrentes en las empresas ecuatorianas para plasmarlos como posibles vectores de ataques.

Las empresas ecuatorianas pueden estar expuestas a diferentes tipos de ataques, a continuación, se detallan los más comunes suscitados en empresas ecuatorianas:

- Entre el año 2017 al 2021 según las estadísticas de la fiscalía general del estado se tiene que tan solo en la revelación ilegal de base de datos estipulado en el artículo 229 del Código Orgánico Integral Penal (COIP), en la intersección ilegal de datos contemplado en el art.230 (COIP), en los ataques de la integridad de sistemas informáticos correspondiente al art. 232 (COIP) y en el acceso no consentido a un sistema informático, telemático o de telecomunicaciones, contemplado en el art.234 (COIP) hay un total de 2,179 ciberdelitos tipificados y denunciados en la fiscalía.

- El Ransomware es un tipo de ataque muy frecuente en empresas ecuatorianas, es el caso la empresa pública Corporación Nacional de Telecomunicaciones (CNT), este tipo de ataque aprovecha las vulnerabilidades del sistema e impide a los usuarios acceder a sus equipos y a sus archivos, en donde el ciberdelincuente exige el pago de un rescate para liberar los archivos, sin embargo, esto no garantiza la recuperación total de la información. (Díaz, 2021)
- El Phishing es un tipo de ataques que aumentó en tiempo de pandemia (COVID), se incrementó el uso de dispositivos para el teletrabajo y más ciber atacantes se infiltraron para obtener información de los usuarios, es común encontrar ataques por correo electrónico, mensajes de texto o mensajes de whatsapp por parte de fuentes aparentemente confiables y que incluyen enlaces falsos y maliciosos que pueden poner en riesgo la información. El objetivo de este ataque cibernético es acceder a datos confidenciales como información personal y datos bancarios (números de cuenta y contraseñas).(Villacís, 2022)

7. Discusión

7.1.Contrastación empírica

La nueva era digital está transformando significativamente nuestra forma de vivir, comunicarse y trabajar, esta era aporta un sin número de beneficios, pero hay que ser conscientes que las redes digitalizadas son sensibles a amenazas cibernéticas.

Durante el desarrollo del proyecto de tesis se propone el diseño para una futura implementación en la red SOHO de la empresa SIITE, además se aportan políticas de ciberseguridad que son fundamentales para salvaguardar los derechos de los usuarios aumentando la privacidad, así como la seguridad y confianza al usar las nuevas tecnologías.

Al realizar el estudio de la red SOHO de la empresa SIITE se pudo observar que existen equipos no administrables (Switch), representando problemas de seguridad, control de tráfico, congestión de la red, segmentación, falta de escalabilidad, entre otros, por ende, se recomienda implementar equipos de capa 3 administrables que eliminen los problemas presentados en la red tal cual se muestra en la metodología.

Se plantea una Zona desmilitarizada (DMZ) y dentro de esta se ubica un honeypot honeydrive, el cual incluyen contiene Kippo y Dionaea, estos simulan varios servicios y/o puertos que están accesibles para los ciber atacantes o intrusos en la red, para este caso de estudio se realizó un ataque desde una máquina virtual a los servicios SSH y HTTP de los honeypots, se observó que capturan información como direcciones púbicas, información de geolocalización, credenciales utilizadas, malware utilizado, etc.

En resumen, con esta información se puede identificar como los ciber atacantes penetraron el sistema y que es lo que están haciendo dentro, e incluso capturar piezas de malware, lo que permite a los administradores o al personal de ciberseguridad plantear nuevos métodos de seguridad o mantener una configuración más compleja en la red LAN de las empresas.

El uso del firewall dentro de la topología planteada permite el control y tráfico que entra y sale de la red LAN y DMZ hacia la WAN, es decir permite controlar quien tiene acceso a la red y que tipo de tráfico está permitido, esto también aporta a mejorar el rendimiento de la red y ayuda a los administradores a identificar y solucionar problemas de la red.

7.2. Limitaciones:

La empresa no tiene un contrato con el proveedor de servicios de internet para obtención o denominación de una IP publica, por lo tanto, no se pudo conectar para hacer una simulación en tiempo real, sin embargo, se realizó una simulación en la red local para la obtención de la información.

La empresa no maneja sistemas de interconexión (router) tal como como lo pudimos observar del estado actual de la red, por el cual se podría realizar un Bypass de la IP pública y poder realizar un Cloud Hosted Router (CHR).

La investigación fue clave para el desarrollo del presente proyecto de tesis, existe información muy importante en páginas de investigación que son de pago, por ende, esta fue una de las limitaciones, pero se realizó una investigación de otras fuentes bibliográficas y así obtener el conocimiento necesario para el desarrollo del presente proyecto de tesis.

7.3.Aspectos relevantes

La seguridad de las redes de las empresas debe ser un trabajo continuo, por ende, deben tomar medidas contra las amenazas y estar preparados para los diversos ataques cibernéticos que se producen al utilizar las tecnologías de información, es trabajo de las empresas proteger la información relevante, a sus clientes, usuarios y/o equipos terminales presentes en sus espacios de trabajo.

El uso de un diseño de redes y de equipos que brinden seguridad a las empresas permite protegerse contra ciber atacantes, la mayoría de empresas ecuatorianas no implementan redes seguras y por ende son víctimas de pérdidas de información, bloqueo de cuentas y equipos, etc., en el presente estudio se presenta una topología de red que permitirá a pequeñas empresas tomarlo como referencia para implementarlo en sus redes empresariales, y se plantean algunas políticas de seguridad de tal manera que se pongan en marcha mejores prácticas que deben seguirse para proteger la información, los sistemas y los recursos de la empresa.

8. Conclusiones

- El diseño propuesto busca crear una red segmentada en donde los dispositivos de la red se dividan en grupos lógicos, limitando el acceso de los recursos de la red, lo que ayuda a reducir el tráfico y a mejorar el rendimiento general del sistema.

- El análisis de los ataques realizados en las empresas ecuatorianas ayuda a disminuir las vulnerabilidades de las redes de telecomunicaciones y motiva a las empresas a implementar políticas de seguridad en sus sistemas de información, además que son considerados como los vectores de ataque más utilizados por los ciberdelincuentes.

- El uso de honeypots se enfoca en capturar información de las estrategias producidas por los ciberdelincuentes, además permite a los analistas de redes realizar una auditoría y utilizar esta información para mejorar la seguridad y mitigar los riesgos de pérdidas de información y recursos de la empresa.

- En el presente trabajo de titulación se han propuesto algunas políticas de seguridad recomendadas para servidores y servicios, y cada organización debe adaptarlas a sus necesidades específicas. Es importante tener en cuenta que la seguridad no es un proceso único, sino que debe ser una tarea continua y activa.

- Al implementar políticas de seguridad en la red SOHO de la empresa SIITE, estamos brindando mayor seguridad a los equipos de red, equipos terminales, usuarios y clientes, reduciendo el riesgo de robos, daños y accesos no autorizados, brindando mayor protección de la información confidencial y la continuidad de las operaciones de la empresa.

9. Recomendaciones

- Evitar el uso de equipos no administrables, con estos equipos no se puede controlar el tráfico de la red ni la asignación de direcciones IPs, no brinda seguridad dejando el sistema vulnerable a ataques externos e internos y no permite la creación de políticas de red.

- Es importante tener en cuenta que la administración y seguridad de la red debe estar en un monitoreo constante y activo, se recomienda analizar los equipos que se van a implementar y verificar que cumplan con los parámetros de seguridad necesarios para mantener una red segura, así como mantener actualizados los equipos de redes para reducir las vulnerabilidades o fallas de seguridad.

- Realizar una capacitación sobre el uso constante de las políticas de seguridad mencionadas en este proyecto de tesis, así como campañas de concienciación de phishing, de tal manera que los usuarios de la red se sientan seguros al navegar por la red LAN de la empresa.

- Antes de adquirir un firewall se recomienda evaluar las necesidades de seguridad de la empresa, tomar en cuenta los tipos de amenazas a los que están expuestas la red, además también es importante considerar la escalabilidad y que pueda manejar el crecimiento de la empresa.

10. Referencias bibliográficas

Ángeles García, J. C. (2012). *Computo forense mediante la tecnología honeypot* [Thesis]. http://tesis.ipn.mx:8080/xmlui/handle/123456789/10700

Branstad, D. K. (1987). Considerations for security in the OSI architecture. *IEEE Network*, *1*(2), 34-39. https://doi.org/10.1109/MNET.1987.6434189

Developments of the Honeyd Virtual Honeypot. (s. f.). Recuperado 24 de marzo de 2023, de https://www.honeyd.org/

Eduard, A., & Daniel, L. (s. f.). *Honeypot: Ventajas y Desventajas como Mecanismo para la Prevención de Intrusos Informáticos*.

Estupiñan, A. del C. A., Pulido, J. A., & Jaime, J. A. B. (2013). Análisis de riesgos en seguridad de la información. *Revista Ciencia, Innovación y Tecnología*, *1*, 40-53.

Irvene, C., Formby, D., Litchfield, S., & Beyah, R. (2018). HoneyBot: A Honeypot for Robotic Systems. *Proceedings of the IEEE*, *106*(1), 61-70. https://doi.org/10.1109/JPROC.2017.2748421

Lara Rocha, M. Á., & López Cante, D. C. (2013). Honeypot virtualizado para ambientes académicos y de investigación. *instname:Universidad Piloto de Colombia*. http://repository.unipiloto.edu.co/handle/20.500.12277/2584

Ramaswamy, R. (1990). Traffic flow confidentiality security service in OSI computer network architecture. *IEEE TENCON'90: 1990 IEEE Region 10 Conference on Computer and Communication Systems. Conference Proceedings*, 649-652 vol.2. https://doi.org/10.1109/TENCON.1990.152690

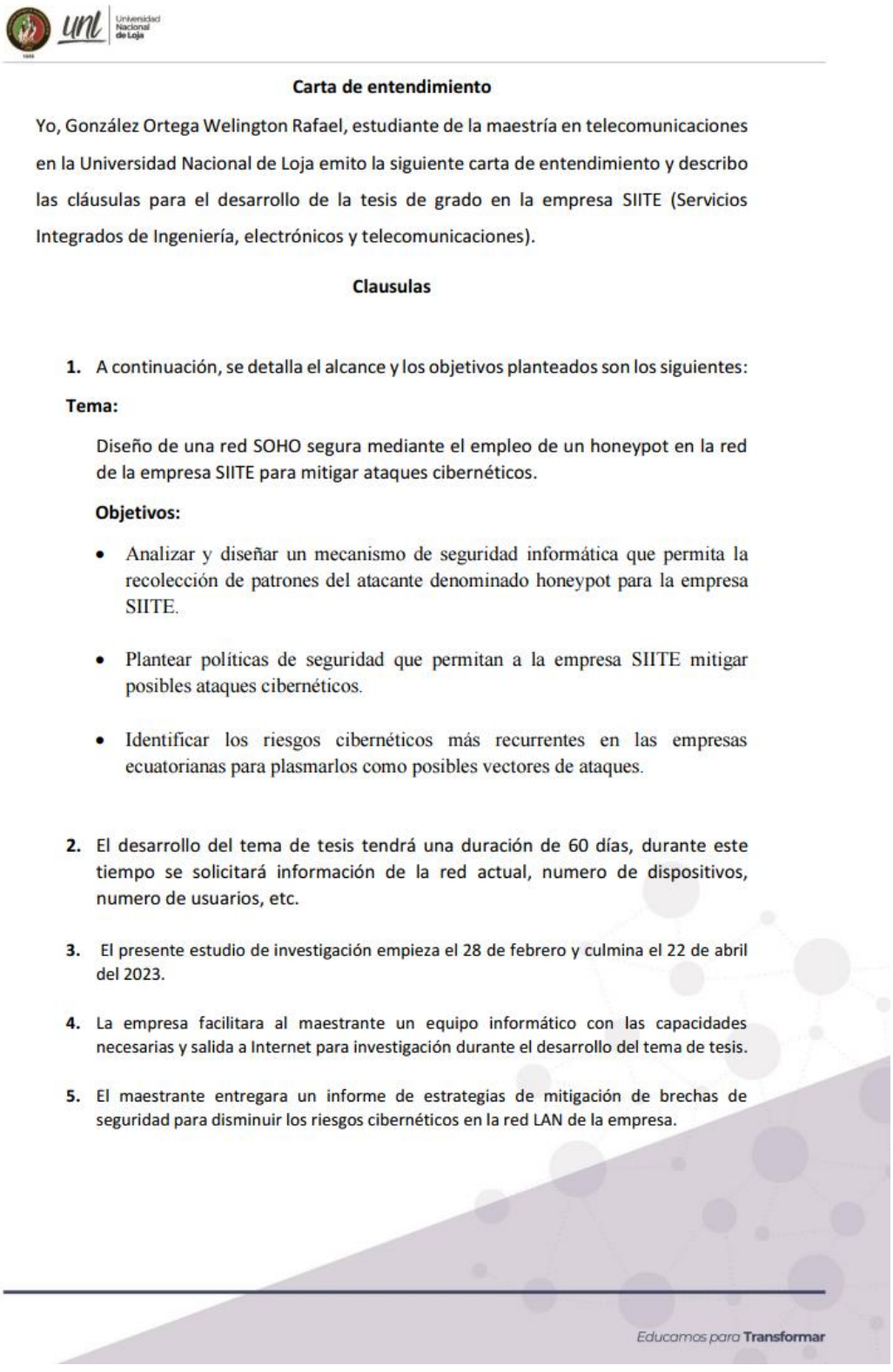
Shi L., Li Y., & Ma M. (2019). Latest Research Progress of Honeypot Technology. 电子与信息学报, *41*(2), 498-508. https://doi.org/10.11999/JEIT180292

Tamminen, U. (2023). *Kippo* [Python]. https://github.com/desaster/kippo (Original work published 2014)

Willians, S. (2004). *Fundamentos de Seguridad en Redes Aplicaciones y Estándares* (2.ª ed.).

11. Anexos

Anexo 1. Carta de entendimiento de compromiso con la empresa SIITE.



Carta de entendimiento

Yo, González Ortega Welington Rafael, estudiante de la maestría en telecomunicaciones en la Universidad Nacional de Loja emito la siguiente carta de entendimiento y describo las cláusulas para el desarrollo de la tesis de grado en la empresa SIITE (Servicios Integrados de Ingeniería, electrónicos y telecomunicaciones).

Clausulas

1. A continuación, se detalla el alcance y los objetivos planteados son los siguientes:

Tema:

Diseño de una red SOHO segura mediante el empleo de un honeypot en la red de la empresa SIITE para mitigar ataques cibernéticos.

Objetivos:

- Analizar y diseñar un mecanismo de seguridad informática que permita la recolección de patrones del atacante denominado honeypot para la empresa SIITE.
- Plantear políticas de seguridad que permitan a la empresa SIITE mitigar posibles ataques cibernéticos.
- Identificar los riesgos cibernéticos más recurrentes en las empresas ecuatorianas para plasmarlos como posibles vectores de ataques.

2. El desarrollo del tema de tesis tendrá una duración de 60 días, durante este tiempo se solicitará información de la red actual, numero de dispositivos, numero de usuarios, etc.
3. El presente estudio de investigación empieza el 28 de febrero y culmina el 22 de abril del 2023.
4. La empresa facilitara al maestrante un equipo informático con las capacidades necesarias y salida a Internet para investigación durante el desarrollo del tema de tesis.
5. El maestrante entregara un informe de estrategias de mitigación de brechas de seguridad para disminuir los riesgos cibernéticos en la red LAN de la empresa.

Educamos para Transformar

Aceptados los términos de la presente Carta de Entendimiento, se firma en la ciudad de Loja, el 28 de febrero del 2023.

Firmado electrónicamente por:
GONZALO RAMON JARAMILLO

Ing. Gonzalo Ramon Jaramillo.

Gerente de Siite

Firmado electrónicamente por:
WELINGTON RAFAEL GONZALEZ ORTEGA

Ing. Welington Rafael González Ortega

Maestrante

Anexo 2. Registro de reuniones con la empresa SIITE.

En el presente documento se detallan las reuniones programadas con la empresa SIITE:

REGISTRO DE REUNIONES CON LA EMPRESA SIITE		
Tema de titulación:	**"DISEÑO DE UNA RED SOHO SEGURA MEDIANTE EL EMPLEO DE UN HONEYPOT EN LA RED DE LA EMPRESA SIITE PARA MITIGAR ATAQUES CIBERNÉTICOS"**	
Nombres y apellidos del/los aspirante/s:	Welington Rafael González Ortega	
FECHA	**TEMA**	**Firma**
06-03-2023	Recabar información del estado actual de la red SOHO de la empresa SIITE.	
08-03-2023	Análisis de la cantidad de dispositivos conectados a la red SOHO de la empresa SIITE.	
13-03-2023	Recabar información de las políticas implementadas en la red SOHO de la empresa SIITE.	

El presente registro, se firma en la ciudad de Loja el 18 de abril del 2023.

Firmado electrónicamente por: GONZALO RAMON JARAMILLO

Ing. Gonzalo Ramon Jaramillo.

Gerente de Siite

Firmado electrónicamente por: WELINGTON RAFAEL GONZALEZ ORTEGA

Ing. Welington Rafael González Ortega

Maestrante

Educamos para Transformar

Anexo 3. Registro de tutorías con el director del trabajo de titulación.

REGISTRO DE TUTORÍAS	
Tema de titulación:	**"DISEÑO DE UNA RED SOHO SEGURA MEDIANTE EL EMPLEO DE UN HONEYPOT EN LA RED DE LA EMPRESA SIITE PARA MITIGAR ATAQUES CIBERNÉTICOS"**
Nombres y apellidos del/los aspirante/s:	Welington Rafael González Ortega

FECHA	TEMA	OBSERVACIONES / RECOMENDACIONES	ENLACE
01-03-2023	Revisión de tema	El revisa el tema y los objetivos planteados en el trabajo de titulación.	Zoom
06-03-2023	Introducción	Se empieza a plantear la introducción y resumen del trabajo de investigación.	
13-03-2023	Diseño de la red	Junto con el director del trabajo de titulación se plantea un nuevo diseño para la red SOHO de la empresa SIITE.	
15-03-2023	Marco Teórico	Se definieron las variables del trabajo de titulación.	
20-03-2023	Corrección - Marco Teórico	Se realizo correcciones de la primera, segunda y tercera variable propuestas en el trabajo de titulación.	
22-03-2023	Metodología	Se propone como plantear la metodología y se definen los temas a desarrollar.	
27-03-2023	Corrección - Metodología	Se realizo correcciones del diseño de la nueva red.	
29-03-2023	- Resultados	Se plantean los resultados obtenidos.	
01-04-2023	Corrección Resultados	Se realizo cambios en el planteamiento de los resultados obtenidos.	
03-04-2023	Discusión	El director sugiere temas para plantear la discusión.	
10-04-2023	Corrección - Discusión	Se realiza correcciones en el planteamiento de la discusión	
11-04-2023	Conclusiones y Recomendaciones	En base a los resultados obtenidos se plantean las conclusiones y recomendaciones más importantes.	
11-04-2023	Corrección Conclusiones y Recomendaciones.	El director sugiere cambios en el planteamiento de las conclusiones.	
19-04-2023	Correcciones	Se realizaron correcciones en metodología y resultados.	

Anexo 4. Certificado de traducción de resumen

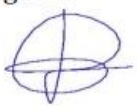
CERTIFICATION

Loja, May 14th, 2023

I, **Nathali del Cisne Cuenca Collaguazo**, certify that I am fluent in the English and Spanish language and that the above document is an accurate translation of the document entitle: **"Diseño de una red SOHO segura mediante el empleo de un honeypot en la red de la empresa SIITE para mitigar ataques cibernéticos"**

Name: Nathali del Cisne Cuenca Collaguazo
License number: 1008-2018-1987008
Phone number: 0991032122
Mail: mcuencacollaguazo@gmail.com

Signed:



C.I.1105775330