
# UTMACH

## FACULTAD DE INGENIERÍA CIVIL

## CARRERA DE INGENIERÍA DE SISTEMAS

# ANÁLISIS Y DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD DE RED UTILIZANDO HERRAMIENTAS DE SEGURIDAD PERIMETRAL.

CAÑARTE VEGA ERICK ANTONIO
INGENIERO DE SISTEMAS

MACHALA
2020


# UTMACH

## FACULTAD DE INGENIERÍA CIVIL

## CARRERA DE INGENIERÍA DE SISTEMAS

# ANÁLISIS Y DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD DE RED UTILIZANDO HERRAMIENTAS DE SEGURIDAD PERIMETRAL.

CAÑARTE VEGA ERICK ANTONIO
INGENIERO DE SISTEMAS

MACHALA
2020


# UTMACH

## FACULTAD DE INGENIERÍA CIVIL

## CARRERA DE INGENIERÍA DE SISTEMAS

TRABAJO TITULACIÓN
PROPUESTAS TECNOLÓGICAS

# ANÁLISIS Y DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD DE RED UTILIZANDO HERRAMIENTAS DE SEGURIDAD PERIMETRAL.

CAÑARTE VEGA ERICK ANTONIO
INGENIERO DE SISTEMAS

VALAREZO PARDO MILTON RAFAEL

MACHALA, 17 DE DICIEMBRE DE 2020

MACHALA
2020

# ANÁLISIS Y DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD DE RED UTILIZANDO HERRAMIENTAS DE SEGURIDAD PERIMETRAL.

INFORME DE ORIGINALIDAD

| 9% | 9% | 1% | 5% |
|---|---|---|---|
| INDICE DE SIMILITUD | FUENTES DE INTERNET | PUBLICACIONES | TRABAJOS DEL ESTUDIANTE |

FUENTES PRIMARIAS

| | | |
|---|---|---|
| 1 | www.ambit-bst.com<br>Fuente de Internet | 1% |
| 2 | docplayer.es<br>Fuente de Internet | 1% |
| 3 | hdl.handle.net<br>Fuente de Internet | 1% |
| 4 | pt.scribd.com<br>Fuente de Internet | <1% |
| 5 | obsbusiness.school<br>Fuente de Internet | <1% |
| 6 | Submitted to Universidad Cesar Vallejo<br>Trabajo del estudiante | <1% |
| 7 | Submitted to Universidad Internacional de la Rioja<br>Trabajo del estudiante | <1% |
| 8 | Submitted to Escuela Politecnica Nacional | |

## CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

El que suscribe, CAÑARTE VEGA ERICK ANTONIO, en calidad de autor del siguiente trabajo escrito titulado ANÁLISIS Y DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD DE RED UTILIZANDO HERRAMIENTAS DE SEGURIDAD PERIMETRAL., otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

El autor como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 17 de diciembre de 2020

CAÑARTE VEGA ERICK ANTONIO
0705689297

## DEDICATORIA

El siguiente trabajo se lo dedico a todas esas personas que siempre me impulsan a hacer las cosas correctas, en especial a mi madre por su incondicional apoyo en el transcurso de mi formación Académica-Profesional y nunca dejar de creer en mí, ella es el reflejo del esfuerzo y dedicación, características de las cuales saqué gran parte.

De igual manera, a las personas que me apoyaron durante, no solo este proceso, si no durante toda mi vida estudiantil, dentro de mi segundo hogar, a mis compañeros de clase y a mis docentes que se convirtieron en mis amigos.

Sr. Cañarte Vega Erick Antonio

**AGRADECIMIENTO**

Agradezco a mis padres Marco y Narcisa, y hermana Nathaly por ser quienes siempre confiaron en mí e inspiran cada día a ser mejor persona, por sus valores y principios que me inculcaron desde pequeño y que aún conservo.

Además, quiero aprovechar la oportunidad para agradecer a mis docentes de la Escuela de Informática de la Universidad Técnica de Machala, por compartir no solo sus conocimientos académicos, sino que también, consejos que me sirvieron mucho en su momento, además de ayudarme cuando más lo necesitaba, y considerarme su amigo más que su estudiante.

Así mismo, al Ing. Valarezo Pardo Milton Rafael, por guiarme en el camino correcto durante el transcurso del proceso de titulación, y por su entereza al despejar todas mis interrogantes.

Sr. Cañarte Vega Erick Antonio

**RESUMEN**

En el ambiente empresarial, donde la información se ha convertido en el activo principal de las organizaciones, este se encuentra constantemente expuesto a que se pierda su confidencialidad, disponibilidad e integridad, ocasionados por acciones de agentes internos y externos, quienes ya sea intencionalmente o no, pueden alterar el flujo normal de las actividades dentro de las empresas. Y es que todos los días se genera millones de datos en las compañías desde las más pequeñas hasta las más grandes, que en muchas ocasiones no cuentan con una adecuada protección, lo que conlleva el riesgo que individuos mal intencionados aprovechen esto, para entrar a la red interna de la empresa y manipular o sustraer datos vitales (por lo general datos financieros) para las transacciones de las empresas. Cabe mencionar que incluso en muchos de los casos, estos individuos llegan a secuestrar la red de las empresas a cambio de una remuneración.

Este escenario presenta la problemática de ¿cómo gestionar mejor la seguridad de la información? dentro de la empresa, y es que es necesario identificar cuáles son las vulnerabilidades que presenta la red de la empresa para poder tomar medidas de protección frente a los riesgos que se presentan de manera externa o interna. Cuando se habla de riesgos, al menos en el presente caso, se trata de mencionar a los riesgos de manera digital, es decir que se hace mención principalmente a los ataques cibernéticos, los cuales desde que aparecieron han venido evolucionando y siendo cada día más sofisticados, y es por eso que es importante saber actuar en consecuencia a estos ataques, y es debido a esto que una buena arquitectura de red, puede marcar la diferencia en cuanto a la capacidad de reacción frente a los ataques provenientes de la red interna o de la web, con el fin de mitigar el impacto de las intromisiones mal intencionadas.

Una arquitectura de seguridad de red, se presenta como una solución frente a la problemática descrita anteriormente, ya que la misma adapta herramientas de seguridad perimetral de red, que tienen características que actúan en pro de la seguridad de la red. Por una parte, tenemos a la herramienta de seguridad por defecto de una red, siendo este el firewall, el cual permite definir reglas de filtrado

de paquetes de la red, que posibilita denegar o autorizar el uso de servicios. Por otro lado, se puede hacer uso de un Sistema de Prevención de Intrusos (IPS por sus siglas en inglés), el cual trabaja conjuntamente con el Firewall con el objetivo de comprobar el tráfico sospechoso de paquetes y así evitar el tráfico de paquetes maliciosos accedan al resto de la red corporativa. Así mismo, en los últimos años, en el uso de esta arquitectura, se ha optado por la implantación de sistemas trampa (o Honeypots en inglés), los cuales se usan con la finalidad de simular un sistema expuesto para distraer a los posibles ciberdelincuentes de la red interna real, evitando que este ataque directamente a la red, además de que permite ganar tiempo al administrador de la red, de contrarrestar a tiempo cualquier acción maliciosa que este individuo tenga.

El propósito de esta propuesta tecnológica entonces es el de analizar y diseñar una arquitectura de seguridad de red, que permita detectar intromisiones y proceder en consecuencia, mediante las herramientas de seguridad perimetral mencionadas anteriormente, para salvaguardar a la red de ataques cibernéticos cuya intención sea manipular la información de la empresa.

**Palabras claves:** Información, Seguridad, Ataques Cibernéticos, Arquitectura de Red, Firewall, IPS, Honeypot

**ABSTRACT**

In the business environment, where information has become the main asset of organizations, it is constantly exposed to the loss of its confidentiality, availability and integrity, caused by actions of internal and external agents, who either intentionally or not, can alter the normal flow of activities within companies. And it is that every day millions of data is generated in companies from the smallest to the largest, which in many cases do not have adequate protection, which carries the risk that ill-intentioned individuals take advantage of this, to enter the internal company network and manipulate or steal vital data (usually financial data) for business transactions. It is worth mentioning that even in many cases, these individuals even hijack the companies' network in exchange for remuneration.

This scenario presents the problem of how to better manage information security? within the company, and it is necessary to identify which are the vulnerabilities that the company network presents to be able to take protection measures against the risks that are presented externally or internally. When talking about risks, at least in the present case, it is about mentioning risks digitally, that is to say that mention is made mainly of cyber-attacks, which since they appeared have been evolving and becoming more sophisticated every day , and that is why it is important to know how to act accordingly to these attacks, and it is because of this that a good network architecture can make a difference in terms of the ability to react against attacks from the internal network or from the web, in order to mitigate the impact of malicious interference.

A network security architecture is presented as a solution to the problem described above, since it adapts network perimeter security tools, which have characteristics that act for network security. On the one hand, we have the default security tool of a network, this being the firewall, which allows defining network packet filtering rules, which makes it possible to deny or authorize the use of services. On the other hand, you can make use of an Intrusion Prevention System (IPS), which works together with the Firewall in order to check suspicious packet traffic and thus prevent malicious packets from entering to the rest of the

corporate network. Likewise, in recent years, in the use of this architecture, the implementation of cheating systems (or Honeypots in English) has been chosen, which are used in order to simulate an exposed system to distract potential cybercriminals from the real internal network, preventing this attack directly on the network, in addition to saving time for the network administrator, to counter in time any malicious action that this individual has.

The purpose of this technological proposal then is to analyze and design a network security architecture, which allows detecting intrusions and proceeding accordingly, through the perimeter security tools mentioned above, to safeguard the network from cyber-attacks whose intention is to manipulate company information.

**Keywords:** Information, Security, Cyber Attacks, Network Architecture, Firewall, IPS, Honeypot

# CONTENIDO

## INDICE DE TABLAS



## INDICE DE FIGURAS

## INDICE DE ANEXOS

## INTRODUCCIÓN

En un mundo interconectado, donde los datos son el eje central de las comunicaciones, el flujo de estos está expuesto a ser intervenidos, por individuos que buscan sacar beneficio de los datos de las empresas, sean medianas o grandes. Por otro lado, se sabe que los ataques cibernéticos, y/o actividades ilícitas cuyo denominador común es el uso de información y tecnología de la comunicación (TIC) [1], cada vez más sofisticados junto con las amenazas que se desconoce, llevan a planificar medidas dinámicas que proporcionen un análisis de seguridad, permitan prevenir, detectar y en su defecto responder a estos ataques.

Actualmente la seguridad de los sistemas informáticos dentro de una empresa requiere la implementación de controles que puedan ser gestionados a través de un adecuado enfoque de seguridad de la información [2].

Por otro lado, se puede decir que los problemas que las organizaciones enfrentan, no son únicamente tecnológicos, sino que en muchas ocasiones enfrentan malas políticas y procedimientos implementados para enfrentar amenazas de ciberdelincuencia, la cual cada día es más sofisticada, por lo que son necesarios mecanismos que actúen como barrera entre la red interna de la empresa y la red global. Es aquí donde nace el concepto de seguridad perimetral o fortalecimiento el cual se refiere al proceso de asegurar un sistema mediante la reducción de vulnerabilidades al mínimo [3].

El presente trabajo, propone el análisis y diseño de una arquitectura de seguridad de red, como una estrategia para detectar, proteger y suministrar de conocimiento transversal al administrador de la red, de posibles ataques cibernéticos, mediante herramientas de seguridad como HoneyPot (Sistemas Trampa), Firewall (Cortafuegos) y IPS (Sistemas de Prevención de Intrusos).

Se pretende que esta arquitectura sea tomada como guía para la identificación de amenazas potenciales que pudieran alterar la integridad de la información y definición de controles de mitigación y tratamiento de riesgos.

La estructura de este documento es de tres capítulos centrales, los cuales se detallan a continuación.

El **Capítulo 1** marca el contexto en el que se pretende desarrollar la arquitectura de seguridad planteada, y sus antecedentes más próximos con el fin de sugerir una solución a la necesidad detectada en este capítulo.

El **Capítulo 2**, por su parte, define el desarrollo de la arquitectura propuesta, desde la fundamentación de las herramientas utilizadas, pasando por los objetivos planteados, hasta el diseño y ejecución del prototipo.

En el **Capítulo 3**, se somete a evaluación la arquitectura diseñada, para comprobar los resultados positivos de la misma, frente a la necesidad que se pretende solucionar. Finalmente se describen conclusiones y recomendaciones a tener en cuenta para futuros trabajos.

# 1. CAPÍTULO I. DIAGNÓSTICO DE NECESIDADES Y REQUERIMIENTOS

## 1.1. ÁMBITO DE APLICACIÓN: Descripción del Contexto y Hechos de Interés.

Desde que las organizaciones adoptaron los sistemas computacionales como principal mecanismo de procesamiento de datos, estos, como cualquier otro mecanismo siempre han necesitado ser resguardados de amenazas que puedan alterar la integridad de los datos, que a priori son información vital de las empresas.

De acuerdo con el Foro Económico Mundial [4], y a su informe global de riesgos [5], sabemos que los ataques cibernéticos ocupan un lugar en el top diez (10) de riesgos a nivel mundial (Ver ***Anexo 1***), y esto en su mayor parte gracias a la globalización donde los datos empresariales se han convertido en los activos más valiosos para las mismas, las cuales optan por medidas de seguridad no muy sofisticadas para mitigar el impacto al ser atacado esta información, lo que representa una vulnerabilidad que puede ser explotada por los cibercriminales. Por citar un ejemplo reciente, basta con recordar el año 2017, donde se atacaron a aproximadamente a trecientos mil ordenadores en 150 países, por los virus NotPetya (que en realidad era una herramienta de penetración conocida como EternalBlue [6], pero se propago muy rápido atacando la vulnerabilidad en un protocolo de Windows en particular, que permite a los piratas informáticos ejecutar de forma remota su propio código en cualquier máquina sin parchear) y WannaCry ( que a diferencia del ransomware común, WannaCry no se propagó a través de archivos adjuntos de correo electrónico, sino que aprovechó la vulnerabilidad en el Sistema operativo Windows para propagarse automáticamente como un gusano por la red [7]) los cuales ocasionaron pérdidas millonarias en empresas a nivel mundial, se estima una perdida trimestral aproximada de $300.000.000,00 dólares americanos en las instituciones afectadas, siendo por lo tanto, virus más dañinos que los habituales [8].

Así mismo podemos darnos una idea de cómo los ataques cibernéticos son diarios, la reconocida empresa Kaspersky, en su Cybermap [9] , nos brinda un análisis en tiempo real de todos los ataques a nivel mundial, así pues nos damos cuenta que, a la fecha de realizado este trabajo Ecuador es el país Nro. 40 en

ser más atacado (ver ***Anexo 2***), posición considerable para nuestro medio. Si nos adentramos un poco más en estas estadísticas, podremos ver con más detalle cuales son los ataques más comunes detectados en nuestro país por la inteligencia de los algoritmos usados por Kaspersky, siendo los ataques a la red los más interesantes respecto a los demás. Aquí podremos ver que los ataques de intrusión son los más usuales (ver ***Anexo 3***), los cuales pretenden "explotar aplicaciones, servicios y sistemas operativos vulnerables o configurados incorrectamente de forma remota a través de una red para lograr la ejecución de código arbitrario y realizar actividades de red no autorizadas [10]". En este concepto descrito anteriormente, se plantean ideas que apuntan a la capacidad de reacción de las empresas para confrontar situaciones que pongan en riesgo la integridad de la información por ataques que provengan de la red interna y web.

El propósito de la presente propuesta tecnológica es el de analizar y diseñar una arquitectura de seguridad de red, que permita detectar ataques y consecuentemente actuar mediante herramientas de seguridad perimetral (FIREWALL, IPS, HONEYPOT), para proteger a la red de posibles pérdidas de información que puedan ocurrir por un ataque cibernético. Además de proporcionar información al administrador de la red sobre nuevos ataques, para que pueda tomar las medidas adecuadas frente a esta situación.

## 1.2. ESTABLECIMIENTO DE REQUERIMIENTOS

Aunque la ciberseguridad ha recibido un gran interés mundial en los últimos años, sigue siendo un espacio de investigación abierto [11]. Las soluciones de seguridad actuales en el ciberespacio basado en red brindan una puerta abierta a los atacantes al comunicarse primero antes de la autenticación, lo que deja un agujero negro para que un atacante ingrese al sistema antes de la autenticación.

Los requerimientos de la presente propuesta tecnológica, se apoyan de normas de seguridad, como la ISO 27001 e ISO 27002, sobre seguridad perimetral, para garantizar la protección de la información, por lo que se indagan herramientas y reglas de seguridad, considerando siempre reglas adecuadas para la protección de la red.

La arquitectura de seguridad de red analizada y diseñada, pretende garantizar el soporte y buena administración de redes en cualquier empresa, con el fin de proteja a la red de ataques provenientes del internet, además de aprovechar los recursos implementados y tener una visión ampliada del tráfico de la red por parte del administrador de la red.

Esta arquitectura de seguridad debe brindar control granular sobre el acceso de usuarios (o posibles atacantes) que se conecten de manera remota desde el internet, para así llevar un registro de la actividad de estos dentro de la red. Además de contar con sistemas de detección de intrusos (IDS) para monitorear todo el tráfico de la red y alertar sobre eventos sospechosos, así como un sistema trampa para conocer nuevas formas de instrucción por parte de los ciberdelincuentes, siendo la capacidad de bloqueo de ataques el punto más fuerte de la arquitectura de red propuesta.

Por otro lado, existen requerimientos específicos para cada elemento de seguridad, los cuales son utilizados como primer criterio para la selección de los Herramientas a utilizarse para construir la solución.

## 1.3. JUSTIFICACIÓN DEL REQUERIMIENTO A SATISFACER

La información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios [12], es así que la mayoría de empresas a nivel mundial realizan sus diversas transacciones desde la web y es que, debido a la incorporación de las tecnologías de la información, conlleva a que los especialistas en seguridad de redes mejoren sus arquitecturas, en pro de detectar intrusiones y almacenar dicha información para beneficio propio.

Por otro lado, se sabe que el manejo de información en los correos se ha convertido en una especie de cuello de botella, pues es allí donde llega mucha información que de una u otra manera es posible bloquear con un sistema de seguridad perimetral, pues, si bien es cierto, la implementación de un antivirus a los usuarios finales, permite proteger el servidor y/o computadores de programas maliciosos, pero no es suficiente para mitigar los ataques y amenazas provenientes del exterior, es por ello que, la implementación de una arquitectura de seguridad de red con políticas de seguridad es el paso que se debe dar para estar preparados ante cualquier eventualidad.

Las continuas amenazas, análisis de vulnerabilidades y sustracciones de información por parte de individuos externos e internos a los establecimientos públicos o privados, los cuales identifican y explotan las falencias en las redes informáticas, están ocasionando graves inconvenientes en su operatividad y sustentabilidad, con grandes daños sociales y económicos a las compañías.

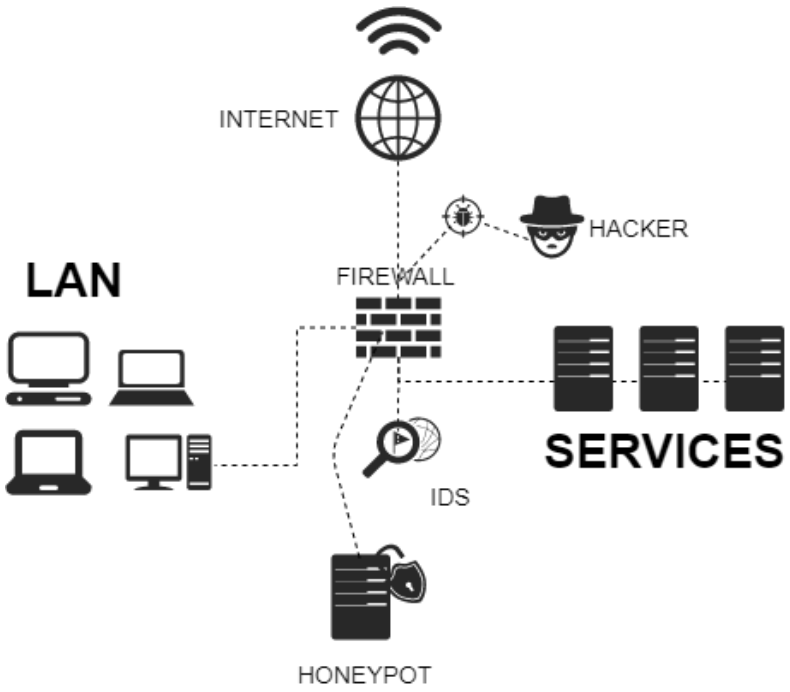
Es por estos motivos que se justifica la propuesta tecnológica del presente trabajo, por la necesidad de resguardar información a través del análisis y diseño de una arquitectura de seguridad de red que permita a las organizaciones detectar oportunamente a los intrusos que ingresan a su red a través de herramientas que puedan contrarrestar, descubrir y analizar las brechas en la seguridad que presentan los sistemas, identificando sus vulnerabilidades y las posibles medidas de prevención para garantizar la confidencialidad, disponibilidad, integridad y autenticidad de la información evitando pérdidas o modificaciones indebidas en la misma

# 2. CAPÍTULO II. DESARROLLO DEL PROYECTO

## 2.1. DEFINICIÓN DEL PROTOTIPO TECNOLÓGICO

La arquitectura piloto de la propuesta tecnológica del presente documento, está diseñada a partir de la estructura general de una topología de red, tal y como se muestra en la ***Figura 1***, esta cuenta con un esquema tradicional en estrella, con un entorno físico que simula la LAN, y un entorno virtualizado simulando la mayor parte de servicios, en la cual se ha implementado, las clásicas herramientas de seguridad, pero se ha implementado alternativas para hacer la red más segura, siendo estos un servidor de sistema trampa (Honeypot), y un firewall con un IDS, que permitan actuar en consecuencia, a los ataques cibernéticos.

**Figura 1.** Piloto de la Arquitectura de seguridad de Red



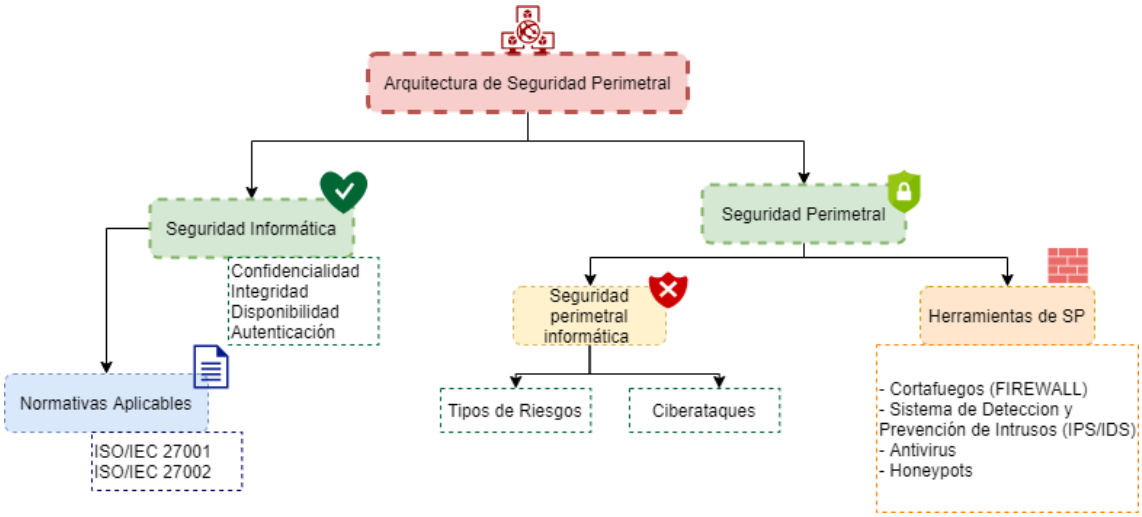

**Fuente:** Elaboración del Autor

Por un lado, tenemos al entorno físico, que actúa como la LAN del autor, con terminales propios, y dispositivos móviles, los cuales se unen internet a la red interna del hogar, a través de dispositivos de ruteo entre las redes, y por otro lado tenemos al entorno virtualizado, mediante máquinas virtuales, que brindaran los servicios (DNS, Correo, Almacenamiento) básicos para una mediana empresa que corresponden a la situación de un entorno real, que puede ser atacado.

## 2.2. FUNDAMENTACIÓN TEÓRICA DEL PROTOTIPO

La fundamentación teórica que da soporte a la realización de la propuesta tecnológica del presente documento, se describe en la ***Figura 2*** como mapa conceptual.

**Figura 2.** Mapa Conceptual de la Fundamentación teórica del prototipo




**Fuente:** Elaboración del Autor

### 2.2.1. Arquitectura de Seguridad Perimetral

#### 2.2.1.1. Seguridad de la Información

La seguridad de la información se suele confundir a menudo con la seguridad informática, aunque ambos términos están interrelacionados. Así que para entender que es la seguridad de la información vale conocer de que va la seguridad informática (seguridad digital), la cual según [13] se puede definir como cualquier medida que prohíba la ejecución de operaciones no autorizadas que puedan ocasionar daños sobre la información o comprometer su confidencialidad, autenticidad o integridad, hasta disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados a un sistema o red informática. Mientras que para [14], es el conjunto de medidas preventivas y reactivas que las organizaciones deben generar y aplicar

Por otro lado, la norma ISO/IEC 17799 [15] define a la seguridad de la información de forma más simple, describiéndola como la preservación de su confidencialidad, su integridad y su disponibilidad (medidas conocidas por su

acrónimo “CIA” en inglés: *Confidenciality, Integrity, Availability*). Todo lo dicho anteriormente, se identifica en la ***Figura 3***.

**Figura 3.** Seguridad de la Información según la ISO/IEC 17799:2005


**Fuente:** ISO/IEE 19977:2005 [15]

La metodología usada para la seguridad de la información está centrada en pilares de la información que hacen que la información sea evaluada y por ende protegida frente a cualquier contratiempo. Estos pilares protegen diversos aspectos que, como se ve en la ***Figura 3***, son la confidencialidad, integridad, disponibilidad y ahora ultimo gracias a la ISO/IEC 27001 [16], se rescata la Autenticidad. Para entender mejor estos pilares se describen en el siguiente apartado.

#### 2.2.1.1.1. Confidencialidad

De acuerdo con [17] la Confidencialidad de datos y de la información del sistema es “ el requisito que intenta que la información privada o secreta no se revele a individuos no autorizados”. Para muchas instituciones la confidencialidad se encuentra frecuentemente por detrás de la disponibilidad y de la integridad en términos de importancia. Para algunos sistemas y para tipos específicos de datos como los autenticadores la confidencialidad es de extrema importancia. Uno de los ejemplos más claros de la aplicación de esta técnica es la criptografía, la cual permite encriptar información, que solo pueda ser receptada por usuarios que tengan permisos para descifrar esta información, haciendo muy complicada la compresión de estos datos por parte de los demás usuarios.

#### 2.2.1.1.2. Integridad

Así mismo [17], describe la integridad como el mecanismo que, se encarga de garantizar que la información del sistema no haya sido alterada por usuarios no autorizados, evitando la perdida de consistencia. La integridad presenta dos facetas, descritas en la ***Tabla 1***.

**Tabla 1.** Facetas de la Integridad de la Información

| Integridad de datos | Integridad del sistema |
|---|---|
| Es la propiedad de que los datos no hayan sido alterados de forma no autorizada, mientras se almacenan, procesan o transmiten | Es la cualidad que posee un sistema cuando realiza la función deseada, de manera no deteriorada y libre de manipulación no autorizada. |

**Fuente:**[17]

La integridad, por lo general, es el pilar de seguridad más significativo después de la disponibilidad, ya que, si se la aplica de la manera correcta, permite detectar cualquier incoherencia con exactitud, credibilidad y confianza, cada dato que se transfiere de manera sospechosa.

#### 2.2.1.1.3. Disponibilidad

Se podría describir a la disponibilidad de la información como un requisito necesario para garantizar que el sistema trabaje continuamente, con precipitación y que no se prohíba el servicio a ningún usuario autorizado.

La disponibilidad protege al sistema contra determinados inconvenientes como los intentos deliberados o accidentales de eliminar datos sin previa autorización, o de causar cualquier tipo de censura del servicio o de acceso a los datos y de los intentos de utilizar el sistema o los datos para propósitos maliciosos. Como ya se mencionó anteriormente, se puede decir que la disponibilidad, es uno de los pilares de seguridad más importante de toda organización, ya que si la información no está disponible cuando se la requiere, la organización puede caer en un estancamiento al no darle movimiento a sus transacciones diarias por estos datos, ahora considerados activos para las organizaciones.

#### 2.2.1.1.4. Autenticación

La autenticación es la técnica que se correlaciona con la confidencialidad, ya que esta comprueba la identidad de un usuario dentro de un sistema. Al ser considerado como un nuevo objetivo de la seguridad, este debe considerar y evaluar la generación de claves únicas privadas para dichos usuarios, ya que, al ser almacenadas en servidores locales por las empresas, sugiere una amenaza de suplantación de identidad de su legítimo usuario.

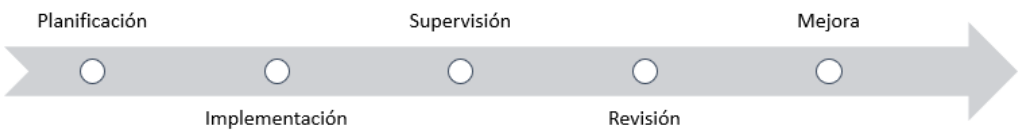
#### 2.2.1.1.5. Normativas Aplicables

Así como en la cotidianidad de las cosas, siempre existen leyes que controlan o gestionan ciertas áreas de las empresas. Es basado en esta premisa que la Organización Internacional de Estandarización (ISO), ha creado normativas de gestión para las empresas, y creo las siguientes normativas para la gestión de riesgos dentro de las organizaciones:

##### 2.2.1.1.5.1. ISO/IEC 27001

Hablar de esta normativa, conlleva mucho tiempo, es por eso que existe todo un apartado y certificación de esta normativa. Esta normativa de gestión define el sistema de gestión de la seguridad de la información, que debe ser planificada, implementada, supervisada, revisada y mejorada (ver ***Figura 4***) y esto conlleva a definir responsabilidades especificas establecidas para medir y revisar objetivos de seguridad, e incluso realizar auditorías a la interna de la organización.

**Figura 4.** Tratamiento de la información según la ISO 27001




**Fuente:** Elaboración del Autor

De acuerdo con [18], lo que en verdad importa de la ISO 27001 es que los riesgos sean analizados de forma que pueda ser corregidos y mejorados, gracias a una planificación e implementación previa que permita la revisión de los mismos. Aunque hay que mencionar que esta normativa no cuenta con

una guía de implementación, sino más bien solo presentan un listado de controles que pueden ser aplicados.

#### 2.2.1.1.5.2. ISO/IEC 27002

La normativa ISO/IEC 27002 [19], toma como referencia la anterior normativa para establecer una guía de controles de riesgo, y así poder, como lo dice [18], proporcionar recomendaciones de mejores prácticas en la gestión de la seguridad de la información. La versión de 2013 de esta normativa cuenta con catorce dominios y métricas, que sirven de guía para su correcta implantación en las organizaciones las mismas que se mencionan en [18], de las cuales se puede hacer mención algunas que se consideran importantes para el presente trabajo en la ***Tabla 2***.

**Tabla 2**. Métricas ISO/IEC 27002

| **Dominio** | **Métricas** |
|---|---|
| Políticas de seguridad | • Cobertura de las políticas<br>• Grado de despliegue y adopción de las políticas en la organización. |
| Control de Accesos | Porcentaje de sistemas y aplicaciones corporativas identificadas por la organización basadas en reglas de acceso definidas por roles. |
| Cifrado | Porcentaje de sistemas que contienen datos valiosos o sensibles para los cuales se han implantado totalmente controles criptográficos apropiados. |
| Seguridad de las Telecomunicaciones | Estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas, y número de ataques potenciales de hacking repelidos, clasificados en: *insignificantes-preocupantes-críticos.* |

**Fuente:**[18]

En resumen, esta normativa es un marco metodológico confiable, que puede ser implementado en cualquier tipo de organización sea esta pública o privada.

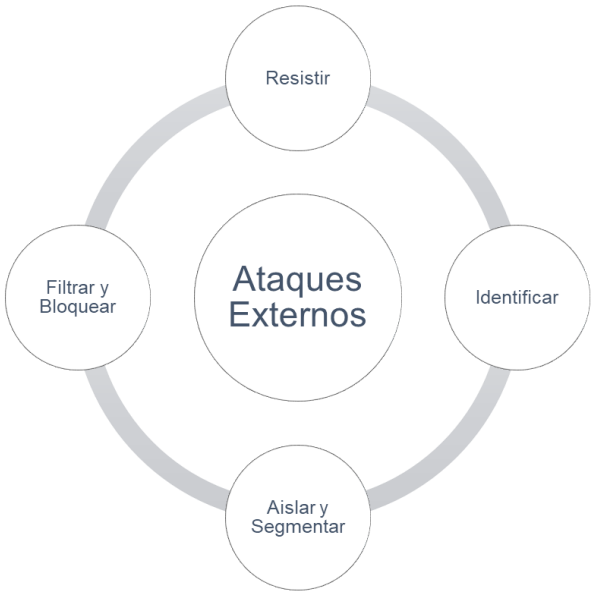
#### 2.2.1.2. Seguridad perimetral

La seguridad perimetral, conlleva a conocer y gestionar los riesgos dentro del área de una empresa, con la ayuda de elementos y sistemas que permitan proteger los perímetros en instalaciones sensibles de ataques de intrusos. Estos elementos varían dependiendo del área, podremos dar ejemplos como radares, video sensores, infrarrojos, entre otros.

##### 2.2.1.2.1. Seguridad perimetral informática

En informática, la seguridad perimetral no se aleja mucho del concepto general, ya que su razón de ser es la de proteger al perímetro de la organización, pero a diferencia de un espacio físico, esta trabaja en un espacio lógico protegiendo la red interna de la institución de amenazas de la red. Esta debe cumplir con cuatro objetivos claros, descritos en la ***Figura 5***.

**Figura 5.** Objetivos de la Seguridad Perimetral Informática




**Fuente:** Elaboración del Autor

Estos objetivos podrían describirse como las funciones principales por las cuales se implementa la seguridad perimetral, estas son: identificar, aislar, segmentar, filtrar, bloquear y resistir cualquier ataque externo mediante herramientas de seguridad perimetral (Firewalls, IPS, HoneyPots…etc.)

Pera antes de hablar de estas herramientas, es necesario conocer un poco a que riesgos y amenazas de ataques se enfrenta una empresa diariamente.

#### 2.2.1.2.2. Tipos de Riesgos

Ya conocemos que la información, actualmente es considerado como el activo más importante dentro de una organización, es por eso que es importante analizar los tipos de riesgos que puedan alterar o robar los datos vitales de las empresas (ver ***Tabla 3***).

**Tabla 3.** Tipos de Riesgos

| Tipo de Riesgo | Descripción |
|---|---|
| **Ataques Externos** | Los ciberdelincuentes siempre tienen en su punto de mira a las compañías y sus sistemas, con el objetivo de sustraer información (bancaria o de otra índole comercial o personal), destruir sus sistemas o manipular sus recursos. |
| **Errores Humanos** | La intervención humana en los procesos informáticos siempre está expuesta a que se cometan faltas (intencional o no). |
| **Desastres Naturales** | Es posible que se den escenarios que pongan en peligro los activos informáticos de la compañía como inundaciones o sobrecargas en la red eléctrica. |
| **Situaciones Extraordinarias** | Las crisis a menudo reducen los niveles de alerta y protección y llevan a los ciberdelincuentes a aprovecharse de esta situación operando bajo esquemas maliciosos. |

**Fuente:** [20]

La seguridad en los últimos años se ha enfocado en las políticas de seguridad interna, sin dejar de lado de considerar las amenazas externas, es por eso que en el apartado siguiente se mencionan los ciberataques más comunes que los intrusos usan para aprovechar vulnerabilidades y adentrarse en nuestra red podemos ser víctimas en la red.

#### 2.2.1.2.3. Ciberataques

De acuerdo con [21], los ataques cibernéticos más frecuentes que representan un riesgo para las organizaciones son:

- **Pishing**

  En términos simples y de acuerdo además con [22] es un tipo de ataque donde los ciberdelincuentes obtienen acceso a una red mediante spam en el correo electrónico u otros métodos de ingeniería social donde, al dar clic a un enlace o descargar un archivo malicioso, la víctima proporciona datos e información confidencial y así obtienen acceso a la red.
- **DDoS (Denegación de servicio distribuida)**

  Es un ataque en el que múltiples orígenes se dirigen a un servidor web, sitio web u otro dispositivo de red; saturándolos de mensajes, paquetes y solicitudes de conexión hasta conseguir que el sistema o red sea "bloqueado", con esto los datos y el sistema en general no están a disposición de los usuarios. Y es que este tipo de ataques de acuerdo con [23],pueden incapacitar rápidamente a una víctima, causando enormes pérdidas de ingresos
- **Malware**

  Es un software diseñado específicamente para obtener acceso o dañar una computadora sin aprobación del propietario. Según [24] el malware contiene gusanos, errores informáticos, planes teóricamente inapropiados y otros programas que también pueden dañar una máquina. En todo el mundo, el uso de este tipo de virus en Internet está afectando a numerosas empresas y personas, perdiendo información valiosa para las actividades diarias que realizan.
- **Ataques con contraseña**

  Estos ataques utilizan algún tipo de sistema automatizado para realizar el ataque utilizando varias combinaciones de contraseña (como una lista de diccionario) para intentar ingresar. Los medidores de seguridad de contraseñas ayudan a los usuarios a seleccionar contraseñas seguras.
- **Ransomware**

  Estos son los ataques más peligrosos, ya que una vez ingresado, el delincuente bloquea y encripta los dispositivos en una red para evitar que

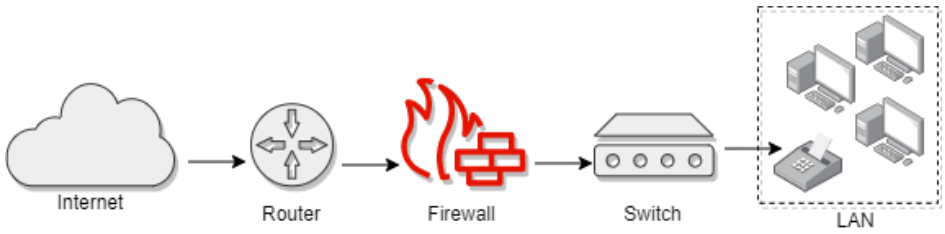
alguien los use a menos que se pague un rescate, dicho de otro modo, el objetivo de este ataque es el de secuestrar la red. Es así que, en concordancia con [24] se expresa que este tipo de ataques se ha convertido en uno de los programas maliciosos más extendidos que representan una seria amenaza tanto para las personas como para las organizaciones comerciales.

#### 2.2.1.3. Herramientas de Seguridad Perimetral

##### 2.2.1.3.1. Cortafuegos (FIREWALL)

Los cortafuegos son filtros entre la red privada de la organización y la red pública [25]. Siendo este, el primer elemento que actúa para permitir o denegar el tráfico de redes, debido a que permite definir políticas y reglas de acceso ayudando a proteger las máquinas de los ataques de un cracker [26]. En la ***Figura 6*** , tenemos la integración y la ubicación principal del cortafuegos.

**Figura 6.** Implantación por defecto del Firewall




**Fuente:** Elaboración del Autor

Es oportuno situar el firewall entre el router que conecta con internet y el equipo o switch que conecta a la red LAN. Así como también, definir el orden correcto de las reglas definidas en el firewall, ya que cuando un paquete de datos pasa por este, se analiza por cada regla definida hasta que una regla afecte (acepte o deniegue) dicho paquete, después de esto ya no se considera ninguna regla previa definida. Cuando se definen reglas muy permisibles al principio, las reglas posteriores puede que no se apliquen, y esto hace que la configuración del firewall no sirva de nada. Existen algunos tipos de firewall, de los cuales se pueden describir algunos como los presentados en la ***Tabla 4***

**Tabla 4.** Tipos de Firewall

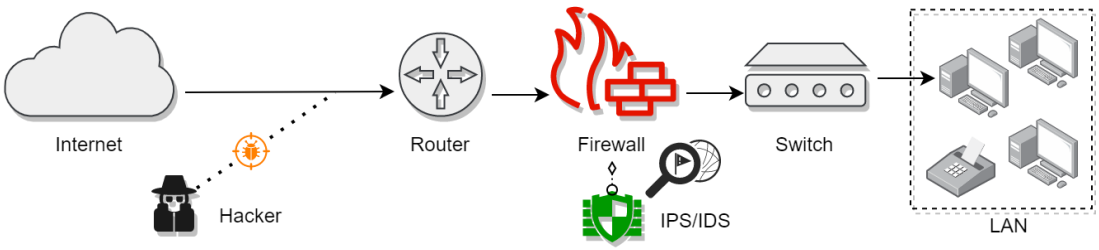
| Firewall | Objetivo |
|---|---|
| De filtrado de Paquetes | Se encarga de tomar decisiones de procesamiento basadas en direcciones de red, puertos o protocolos. |
| Puerta de enlace a nivel de circuito | Comprueba la validez de las conexiones (es decir, circuitos) en la capa de transporte (TCP) |
| De inspección con estado | realiza un seguimiento del estado de la conexión. |
| Puerta de enlace de nivel de aplicación | Usado para operan en la capa de aplicación del modelo OSI, filtrando el acceso según las definiciones de la aplicación. |
| De próxima generación | Trabaja en la identificación y control de aplicaciones, autenticación basada en el usuario. |

**Fuente:**[27]

#### 2.2.1.3.2. Sistema de Detección y Prevención de Intrusos (IDS/IPS)

Herramienta utilizada para proteger la infraestructura de manejo de la información, cuya función principal es monitorear y detectar comportamientos y eventos sospechosos tanto en host como en red.

**Figura 7.** Implantación básica del IPS/IDS




**Fuente:** Elaboración del Autor

Tal como se puede identificar en la ***Figura 7***, estos sistemas trabajan conjuntamente con el firewall, detectando eventos inusuales que coincidan con las reglas definidas o a través de patrones de comportamiento inusual.

La implementación de estos sistemas, suele ser tanto en la red como en un host especifico, los cuales se pueden explicar a continuación:

- **Implementación en Red. –** Monitorea el tráfico de la red, interviniendo entre los atacantes sigilosamente.
- **Implementación en Host. –** Monitorea todo el tráfico dirigido a un equipo especifico, además de las conductas atípicas en el sistema.

De acuerdo con [28] y [29], sus principales diferencias frente a los Firewalls son:

- Mantienen vigilia frente a los ataques internos de la red.
- Detectan ataques provenientes desde los mismo Firewalls
- Analizan los registros de los dispositivos de la red (Firewalls, Routers, etc.)
- Complementan a otras herramientas, para crear una seguridad robusta.

#### 2.2.1.3.3. Antivirus

El antivirus es un software de seguridad especial que tiene como objetivo brindar una mejor protección que la que ofrece el sistema operativo subyacente (como Windows o Mac OS X) [30]. El antivirus en ocasiones se usa para desinfectar los programas infectados o para limpiar completamente el virus del sistema operativo.

El antivirus tiene una extensa variedad de bases de datos que se actualizan asiduamente con licencias y/o firmas en contra de virus actuales, que analizan los programas y dispositivos de la red, evitando la propagación de virus a través de estas firmas de protección. La mayoría de los usuarios no han utilizado antivirus o utilizan software antivirus caducado, por lo que el sistema puede infectarse con malware [31].

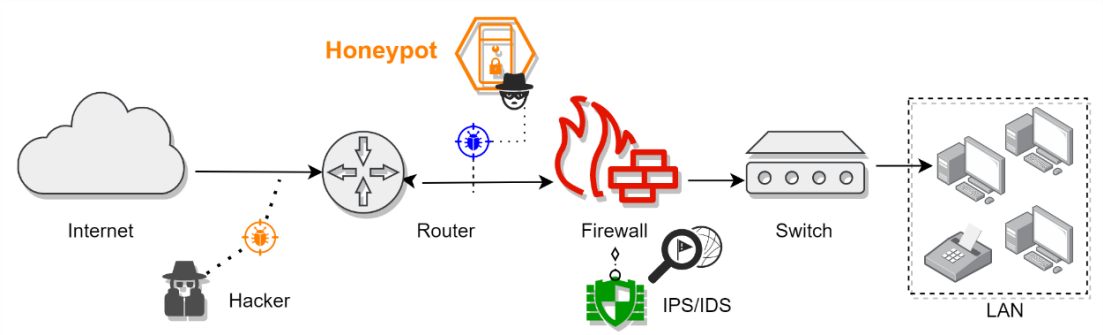
Actualmente, existen una gran cantidad de empresas que ofrecen un software antivirus, y aunque su objetivo sea el mismo, ofrecen muchas características que, dependiendo de los requerimientos de la empresa, y su fujo de red, son eficientes, contando con varios planes de licenciamiento de firmas.

#### 2.2.1.3.4. HoneyPots

En cuanto a los Honeypots o conocidos como sistemas trampa, son equipos que aparentan estar desprotegidos, actuando como señuelos ´para detectar y monitorear posibles ataques.

El objetivo principal de los Honeypots es atraer al ciberdelincuente, y desviarlo de la red LAN, de la empresa, para monitorear sus actividades y analizar los ataques que este realice, manteniendo a salvo al sistema real (ver ***Figura 8***).

**Figura 8.** Implantación básica del Honeypot




**Fuente:** Elaboración del Autor

De acuerdo con [32], estos sistemas tienen algunas ventajas, descritas a continuación:

- Genera menor cantidad de alarmas falsas ya que no usan tráfico legitimado.
- Almacena información valiosa al registrar solo actividad ilegitima
- Prescinde de firmas de ataques en contraste a los IDS
- Detecta nuevos ataques permitiendo exponer las vulnerabilidades del sistema.
- Permite actuar a tiempo, e implementar medidas necesarias para futuros intentos de ataques.

Por otro lado, es necesario conocer algunas desventajas de los sistemas trampa:

- Puede ser usado por hackers para atacar otros sistemas.

- Monitorea solo interacciones hechas directamente con el sistema trampa.
- Puede ser detectado por los atacantes.

Estos sistemas, tienen varios objetivos y nivel de interacción con los atacantes, por lo que es necesario conocer su división la cual es descrita en la ***Figura 9*** y ***Figura 10***, para tener conocimiento sobre muchos de los tipos de sistemas trampa que pueden usar las empresas, dependiendo del tamaño y necesidades de la organización.

**Figura 9.** Tipos de Honeypot - Según su Interacción


**Fuente:** [33], [34]

**Figura 10.** Tipos de Honeypot - Según su Objetivo


**Fuente:** [34]

Es necesario mencionar que en algunas ocasiones se implantan sistemas trampa de alta interacción que es un conglomerado de varios Honeypots, y así capturar toda la información del ciberdelincuente, aunque tienen una compleja configuración para filtrar las reglas de control para monitorear y capturar toda la información de los intentos de ataques, y así mejorar la seguridad a base de detectar las amenazas y vulnerabilidades de la red.

## 2.3. OBJETIVOS DEL PROTOTIPO

### 2.3.1. Objetivo General

Diseñar de una arquitectura de seguridad de red mediante herramientas de seguridad perimetral (FIREWALL, IPS, HONEYPOT), para proteger a la red de posibles pérdidas de información que puedan ocurrir por un ataque cibernético.

### 2.3.2. Objetivos Específicos

- Analizar aspectos relevantes de las arquitecturas de seguridad de red perimetral, para que sirvan de guía en del desarrollo de la propuesta tecnológica.
- Instalar y configurar las herramientas de seguridad (Firewall, IPS, HONEYPOT) mediante un entorno de virtualización.
- Instalar y configurar servicios elementales que ocupa una empresa mediante un entorno de virtualización para simular un ambiente controlado en la que actuará la arquitectura.
- Evaluar la arquitectura de seguridad de red en un ambiente controlado para comprobar la funcionalidad de las herramientas previamente configuradas.

## 2.4. DISEÑO DEL PROTOTIPO

De acuerdo con la norma ISO 27001, se definen las reglas del diseño e implantación del prototipo y la gestión de controles de seguridad para la gestión vulnerabilidades mediante herramientas de código abierto y así garantizar se cumplan con la integridad, disponibilidad, confiablidad y autenticidad [35] de los sistemas de información de una empresa.

### 2.4.1. Entorno de Virtualización

#### 2.4.1.1. Software de Virtualización

Para el entorno de virtualización, se utilizó el paquete de software de virtualización de código abierto multiplataforma x86 “Oracle VM VirtualBox” [36], como principal gestor de Sistemas Operativos en maquina virtuales, que simulan el uso de los servicios y la interconexión para las pruebas de testeo de la arquitectura de red propuesta.

Se escogió este software, ya que presenta características óptimas para trabajar con varias máquinas virtuales simultáneamente gestionando adecuadamente los servicios y procesos a realizar. Además, VirtualBox es funcionalmente idéntico en todas las plataformas de host, y se utilizan los mismos formatos de archivo e imagen [37].

De acuerdo con [38], VirtualBox presenta algunos beneficios hay que tomar en consideración, estos son:

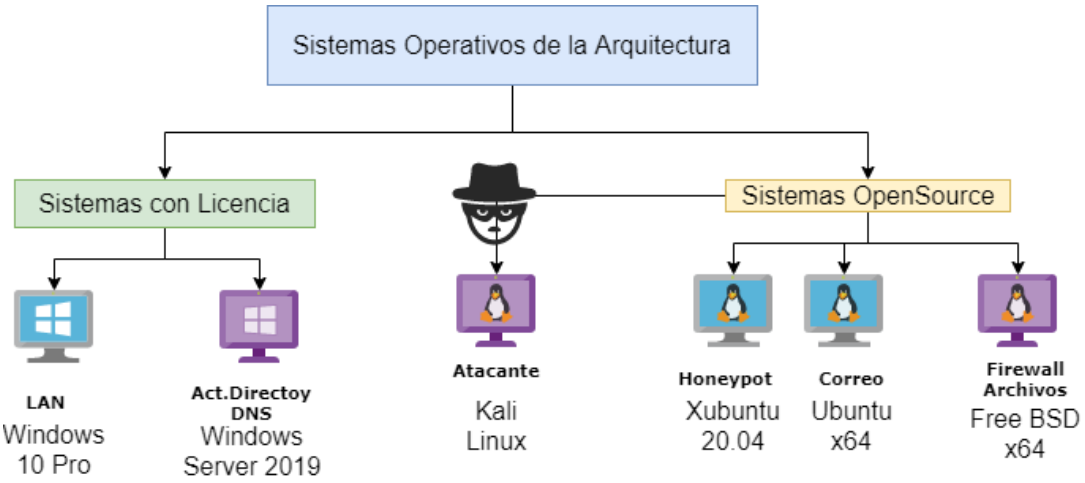
- Admite varios sistemas operativos de host e invitados
- Fácil de usar
- Ligero
- Licencia menos restrictiva.
- Archivo de configuración en xml

#### 2.4.1.2. Sistemas Operativos

Para la arquitectura propuesta se optó por sistemas operativos conocidos y actuales, que faciliten la familiaridad con el entorno que se pretende

desarrollar. La ***Figura 11***, describe los sistemas operativos utilizados en el presente proyecto.

**Figura 11.** Sistemas Operativos de la Arquitectura




**Fuente**: Elaboración del Autor

### 2.4.1.3. Tecnologías de Servicios de la Arquitectura

**Windows Server**

Windows Server ofrece a los clientes una infraestructura de nube escalable, consciente de multiusuario, que ayuda a las fuerzas de trabajo distribuidas y móviles de las organizaciones a conectarse de manera más segura en los instaladores y que permite responder a las necesidades de negado más rápido y de forma más eficiente. Además, Windows Server presenta un rendimiento relativamente mejor para Snort en condiciones de carga de tráfico normal moderada [39].

**Squirrelmail**

De acuerdo con [40], el cliente de correo electrónico SquirrelMail, es un interesante, extensible, funcional y robusto software para correo y que permite acceder al usuario a su correo electrónico desde el navegador de su predilección. Además [41], menciona que es un proyecto de código abierto y es una función de correo muy estable.

**FreeNAS**

FreeNas es un sistema operativo BSD simple que me ayudará a crear un almacenamiento compartido entre …. computadoras para realizar la teletransportación [42] y almacenamiento seguro.

#### 2.4.1.4. Tecnologías de seguridad perimetral de la Arquitectura

**PFSENSE Firewall** [43]

PFSense es un software de firewall gratuito de código abierto altamente configurable basado en FreeBSD. Tiene muchas características relevantes, como límites de velocidad y alarmas, soporte para múltiples usuarios, OpenVPN para proporcionar acceso remoto seguro, servidor DHCP y funciones tradicionales de firewall de filtrado [44].

**SNORT** [45]

Es un sistema de detección y prevención de intrusiones en la red (NIDS / NIPS) [46]. El programa detecta intentos de intrusión analizando el tráfico de la red en tiempo real. El programa utiliza conjuntos de reglas llamadas Sourcefire VRT, que se actualizan periódicamente. A pesar de que el programa en sí es gratuito, la difusión de estas reglas se limita a la suscripción paga.

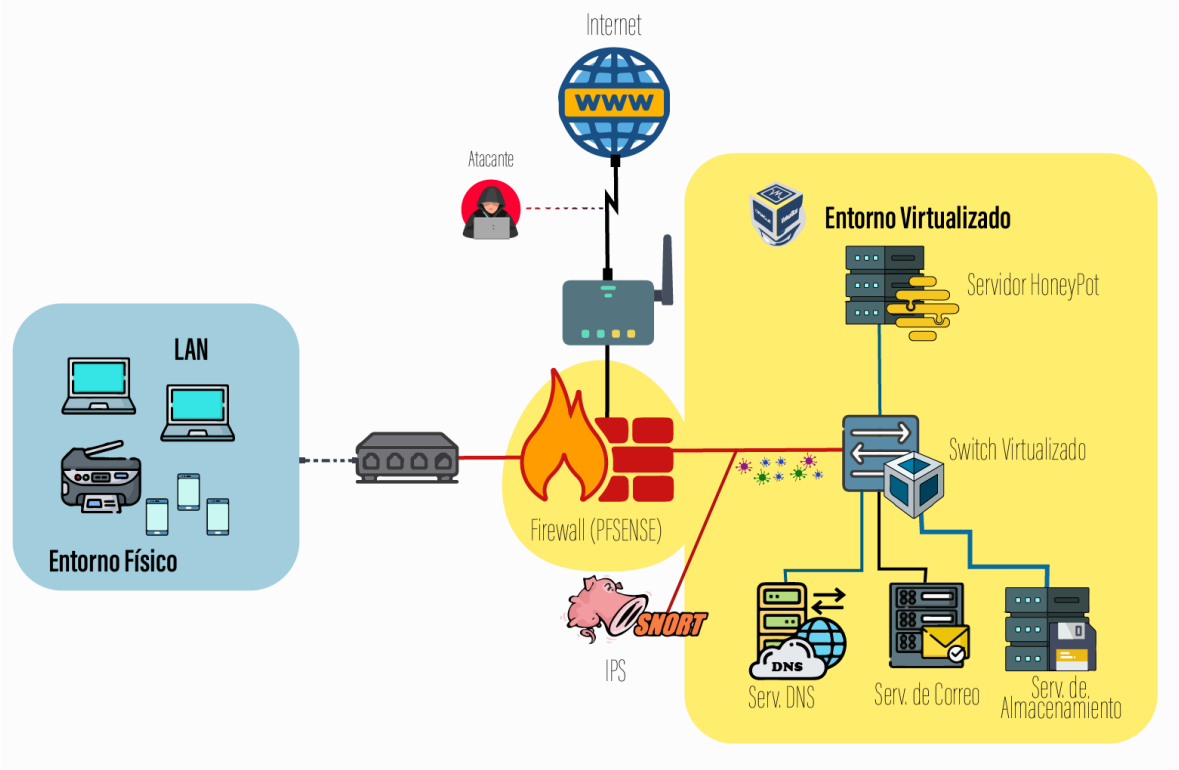
**KIPPO SSH** [47]

Según [48],es un Honeypot de baja interacción y su función reside en hacer una simulación de un servidor SSH y está pensado para recibir ataques de forma sucia. Hemos decidido hacer uso de este porque nos permite obtener mucha información sobre los atacantes, incluso, nos facilita los pedidos que ha ejecutado el atacante, permitiéndonos reproducir la sesión. Asimismo, cabe mencionar que el Honeypot Kippo tiene un propio sistema de visualización, que nos permite acceder mediante una IP de esta manera podemos monitorizarlo desde otra máquina o dispositivo.

### 2.4.2. Diseño de Arquitectura

El diseño de la propuesta se basa en la configuración de una red con acceso a internet anclada a cuatro servidores virtuales para representar las aplicaciones críticas y un firewall para simular la seguridad perimetral (ver ***Figura 12***). Para esta propuesta se establece un direccionamiento IPV4 para la maquina anfitrión de la red LAN y para los servidores virtuales. El acceso al internet se da gracias al Router dedicado con IPV4 de acuerdo al proveedor.

**Figura 12.** Arquitectura de Seguridad Perimetral de Red




**Fuente:** Elaboración del Autor

### 2.4.3. Direccionamiento

En la ***Tabla 5*** podemos identificar el esquema de direccionamiento de IP's para las redes LAN y WAN de la maquina anfitrión y la red del entorno virtualizado, lo que permite el funcionamiento de la arquitectura propuesta.

**Tabla 5.** Direccionamiento IP de la Arquitectura de Seguridad Perimetral de Red

| EQUIPO | DIRECCIONAMIENTO DE INTERFACES | | |
|---|---|---|---|
| | ETH0 | ETH1 | VIRTUAL |
| | RED WAN (Internet) | RED LAN | RED DMZ |
| Maquina Anfitrión | 192.168.1.10 | 192.168.2.1 | X |
| MV01: Firewall PFSENSE | 192.168.1.14 | 192.168.2.1 | 192.168.8.1 |
| MV02: Servidor Honeypot | X | X | 192.168.8.9 |
| MV03: Windows Server | X | X | 192.168.8.10 |
| MV04: Servidor de Correo | X | X | 192.168.8.11 |
| MV05: Servidor de Almacenamiento | X | X | 192.168.8.12 |

**Fuente:** Elaboración del Autor

## 2.5. EJECUCIÓN Y/O ENSAMBLAJE DEL PROTOTIPO

### 2.5.1. Instalación del Sistema de Virtualización

Como ya sé mencionó anteriormente el sistema de virtualización optado para la presente propuesta tecnológica, es uno de los mejores softwares de virtualización del mercado. Y es que la instalación VirtualBox es super sencilla, solo basta descargar el ejecutable del sitio oficial, y ejecutarlo como un programa de computadora.

En la ***Figura 13***, vemos la pantalla principal del administrador de máquinas virtuales, que permitirá gestionar el entorno virtualizado.

**Figura 13.** Pantalla Principal de Oracle VM VirtualBox


**Fuente**: Elaboración del Autor

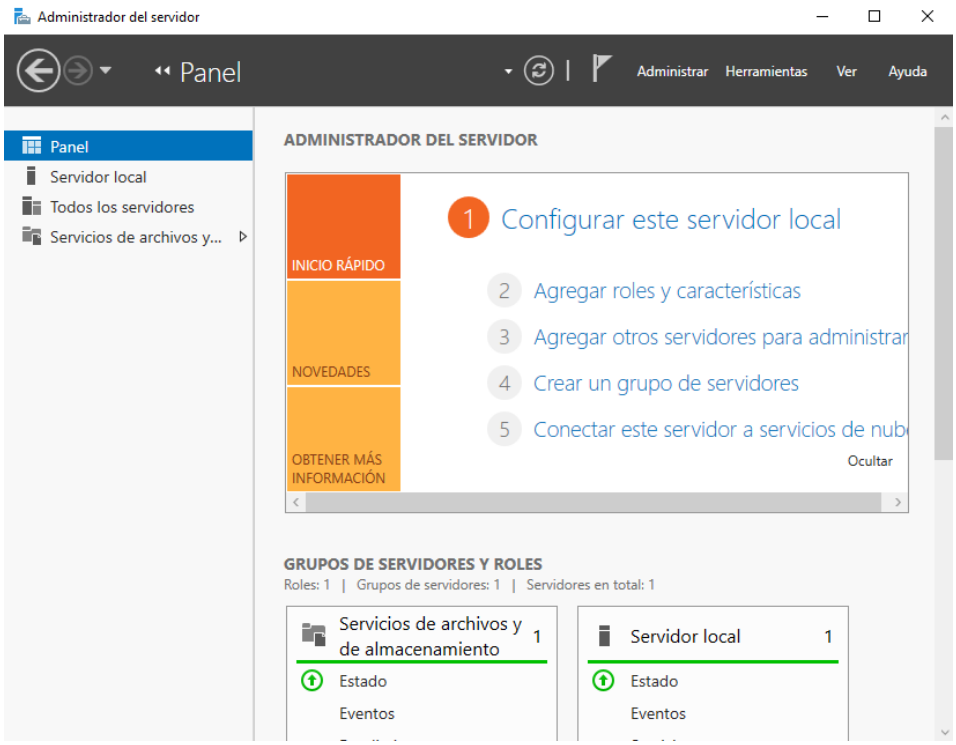
### 2.5.2. INSTALACIÓN Y CONFIGURACIÓN DE SERVICIOS

#### 2.5.2.1. Instalación y Configuración de Windows Server 2019

Para el manejo del servicio de DNS se optó por usar el sistema operativo de grandes características, como lo es Windows Server en su última versión 2019, dentro de una máquina virtual.

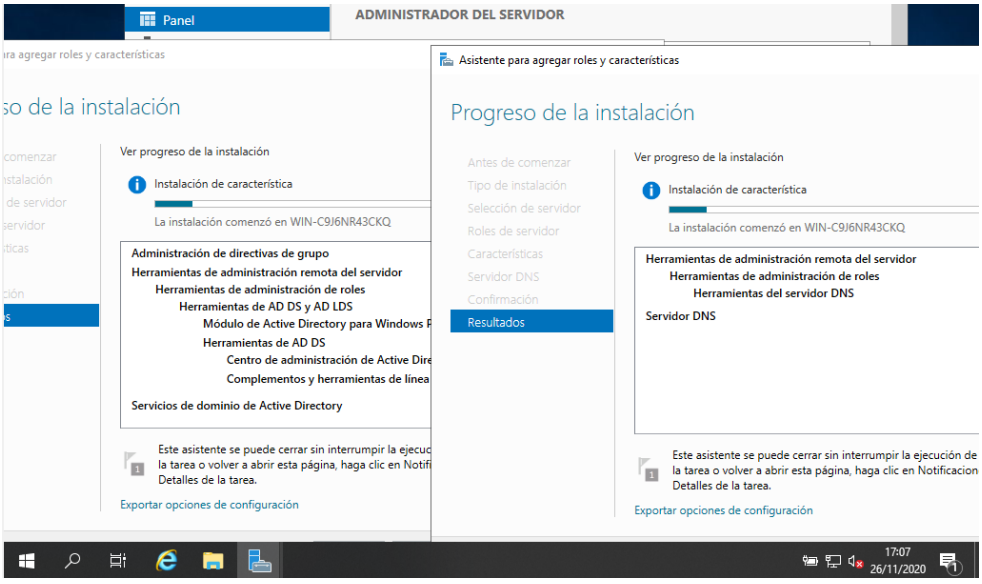
Este servidor presenta un panel de administración es muy intuitivo y fácil de gestionar, por lo que, se pudo instalar DNS y AD DC sin mayor problema (ver ***Figura 14*** y ***Figura 15***).

**Figura 14.** Panel de Administración - Windows Server 2019




**Fuente:** Elaboración del Autor

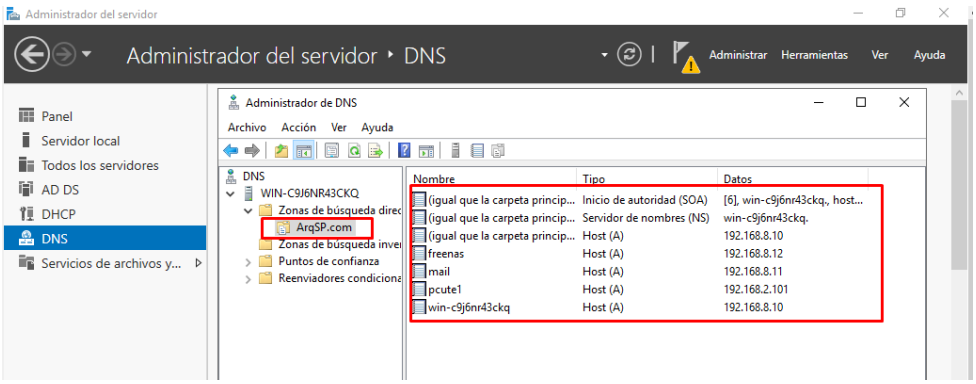
**Figura 15.** Instalación de Servicios DNS y AD DS




**Fuente:** Elaboración del Autor

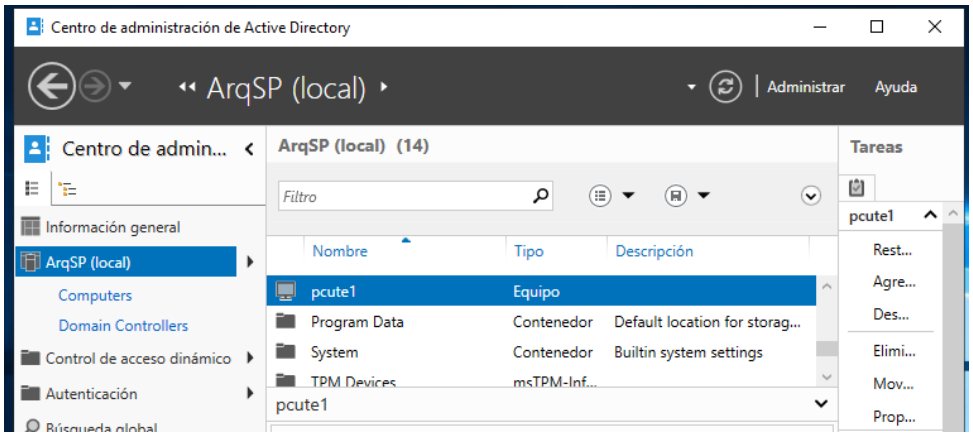
En la configuración de los servicios de DNS y AC DC se creó un dominio con el nombre de ArqSP.com y se agregó Host y usuarios dentro de la red virtualizada (ver ***Figura 16*** y ***Figura 17***)

**Figura 16.** Configuración de DNS - Windows Server 2019




**Fuente:** Elaboración del Autor

**Figura 17.** Configuración de AC DC - Windows Server 2019

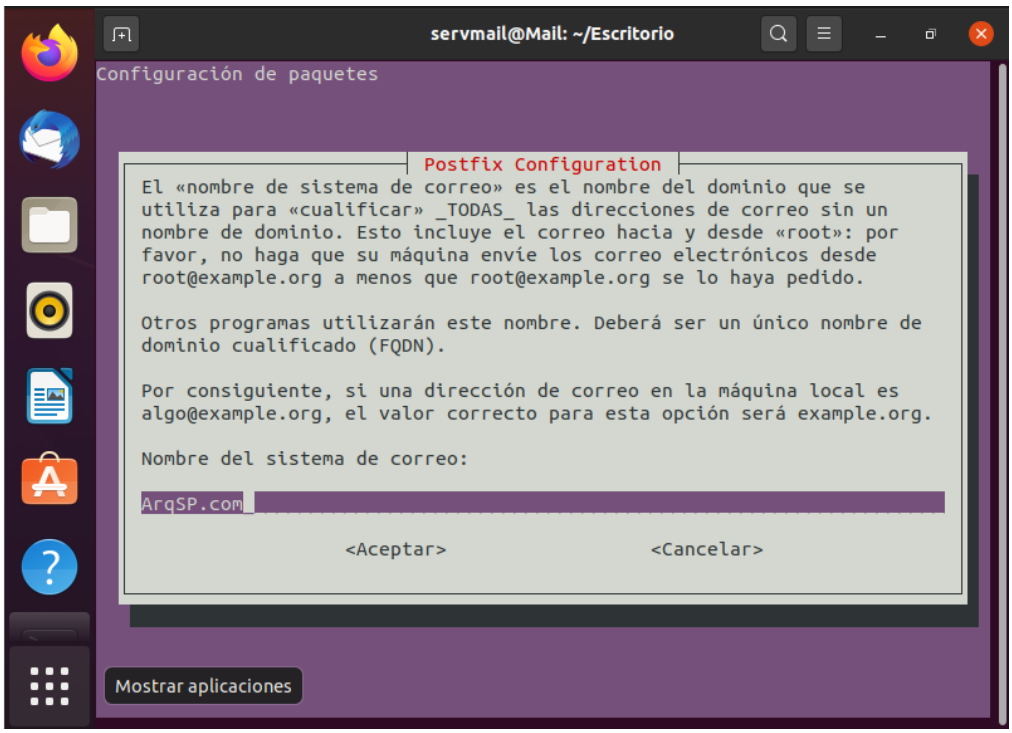



**Fuente:** Elaboración del Autor

### 2.5.2.2. Instalación y Configuración de Servidor de Correo

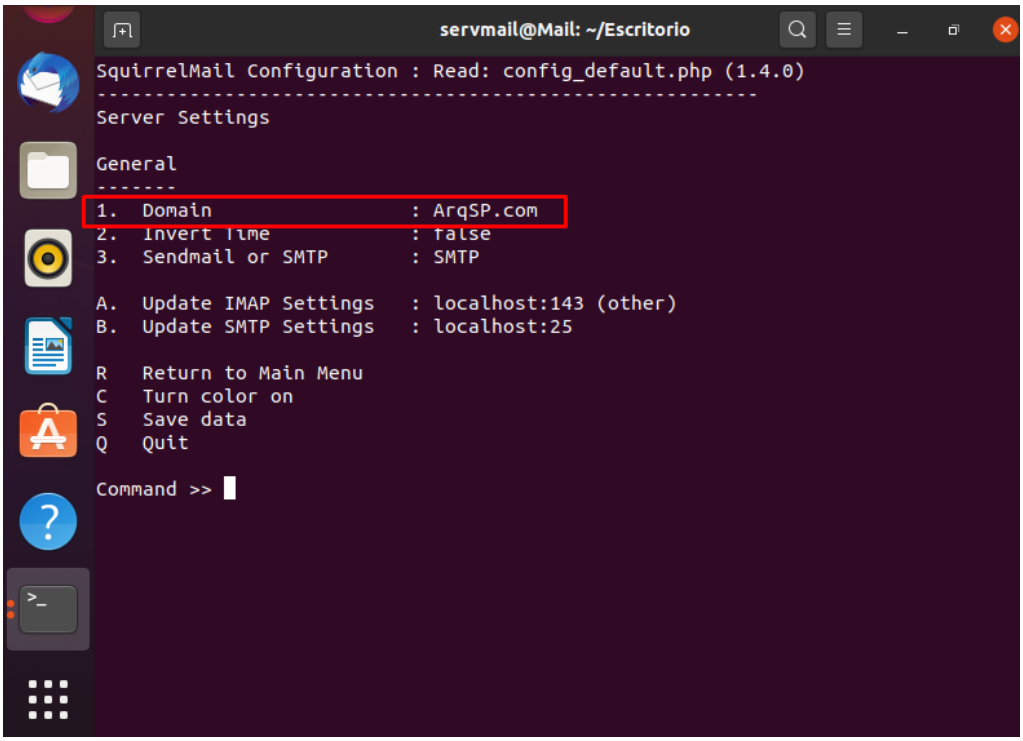
Con el fin de levantar un servidor de correo dentro de la arquitectura de red propuesta, se optó por la instalación del sistema operativo Ubuntu dentro de una máquina virtual. En esta se instaló las herramientas Postfix y SquirreMail, como el servidor por defecto de correo de la Arquitectura y el nombre del servidor de correo es el mismo que el definido anteriormente en Windows Server (ver ***Figura 18*** y ***Figura 19***).

**Figura 18.** Configuración de sistema de correo Postfix




**Fuente:** Elaboración del Autor

**Figura 19.** Configuración de SquirrelMail

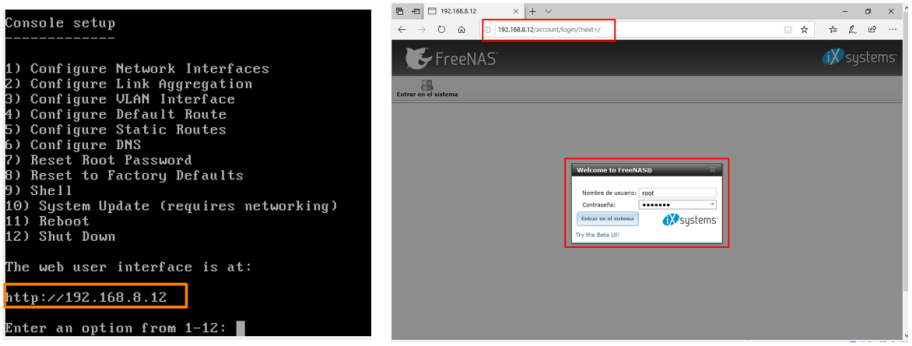



**Fuente:** Elaboración del Autor

### 2.5.2.3. Instalación y Configuración de Servidor de Archivos

En cuanto al servidor de Archivos se utiliza un sistema Open Source que permite a los usuarios de la red, la gestión y almacenamiento de información dentro de un repositorio seguro mediante FTP. Luego de la instalación esta presenta un menú de opciones y la dirección IP del servidor a la que se puede acceder mediante las credenciales previamente configuradas ( ***Figura 20*** ).

**Figura 20.** Postinstalación y Acceso al servidor - FreeNAS




**Fuente:** Elaboración del Autor

Ya dentro de la interfaz del servidor FreeNAS, es necesario configurar el servicio como un dominio y habilitar FTP para facilitar el intercambio de ficheros (***Figura 21***).

**Figura 21.** Configuración de repositorio de dominio - FreeNAS

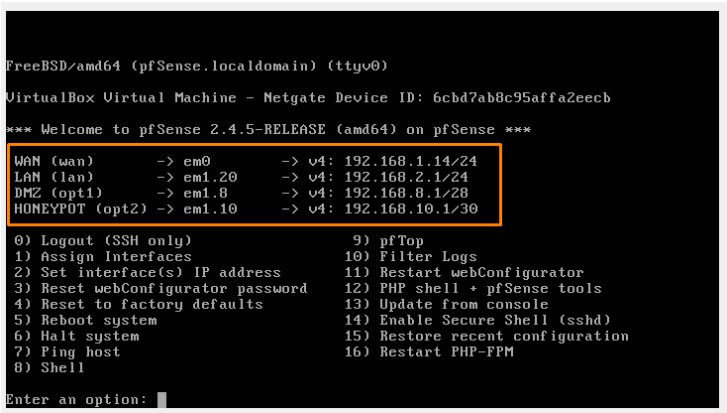

**Fuente:** Elaboración del Autor

### 2.5.3. INSTALACIÓN Y CONFIGURACIÓN DE LAS HERRAMIENTAS DE SEGURIDAD PERIMETRAL

#### 2.5.3.1. Instalación y Configuración de PFSense (Firewall)

Para la propuesta tecnológica se optó por un sistema cortafuegos basado en BSD Free que presenta diversas características en su versión estándar que, aunque es la versión gratuita, es una de las mejores herramientas de Firewall que existen. En la ***Figura 22***, se muestra la configuración de las interfaces que manejará pfsense dentro de la arquitectura.

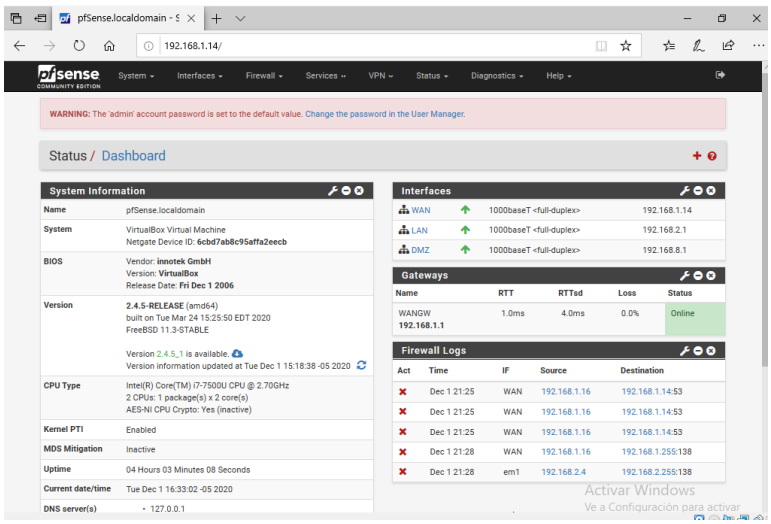
**Figura 22.** Postinstalación y Configuración de Interfaces - PFSense




**Fuente:** Elaboración del Autor

En la ***Figura 23***, se enseña la información general, las interfaces, gateways, y alguno que otro registro dentro del Firewall.

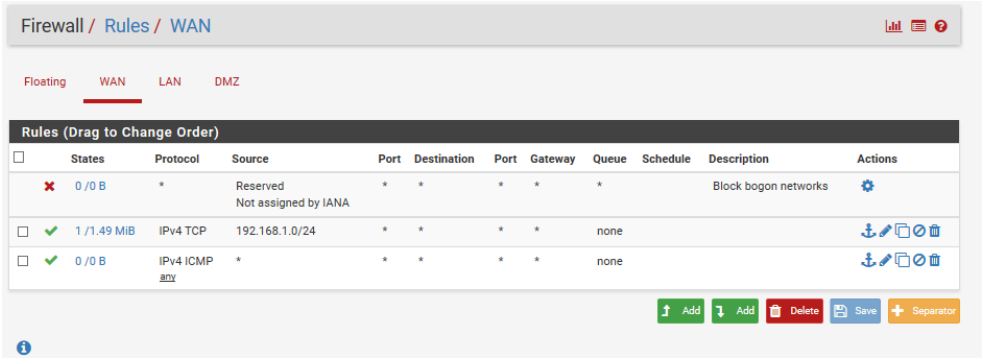
**Figura 23.** Panel de Administración - PFSense




**Fuente:** Elaboración del Autor

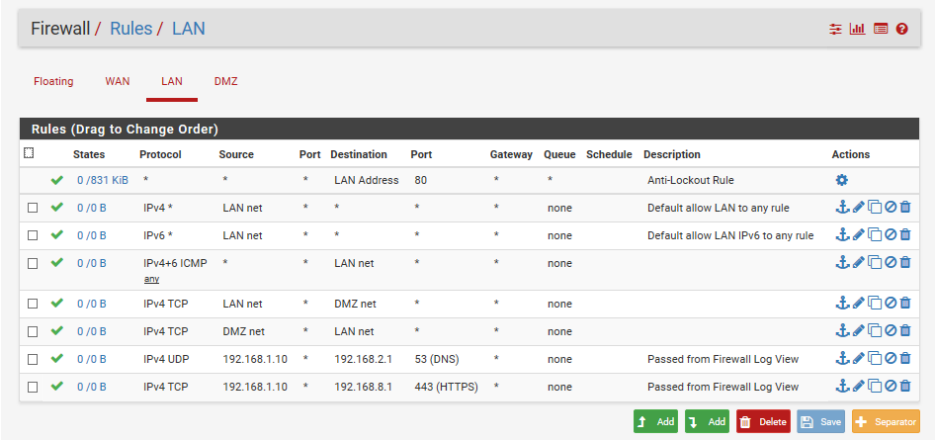
Mediante el panel de administración se configuran las interfaces de las redes agregadas, y se definen reglas de filtrado para cada una de estas (ver ***Figura 24***, ***Figura 25*** y ***Figura 26***).

**Figura 24**. Definición de Reglas para WAN - PFSense



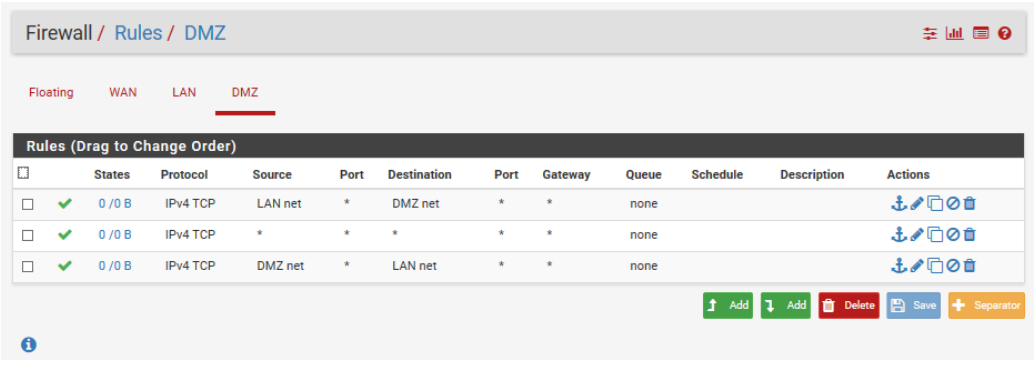

**Fuente:** Elaboración del Autor

**Figura 25.** Definición de Reglas para LAN - PFSense




**Fuente:** Elaboración del Autor

**Figura 26.** Definición de Reglas para DMZ - PFSense

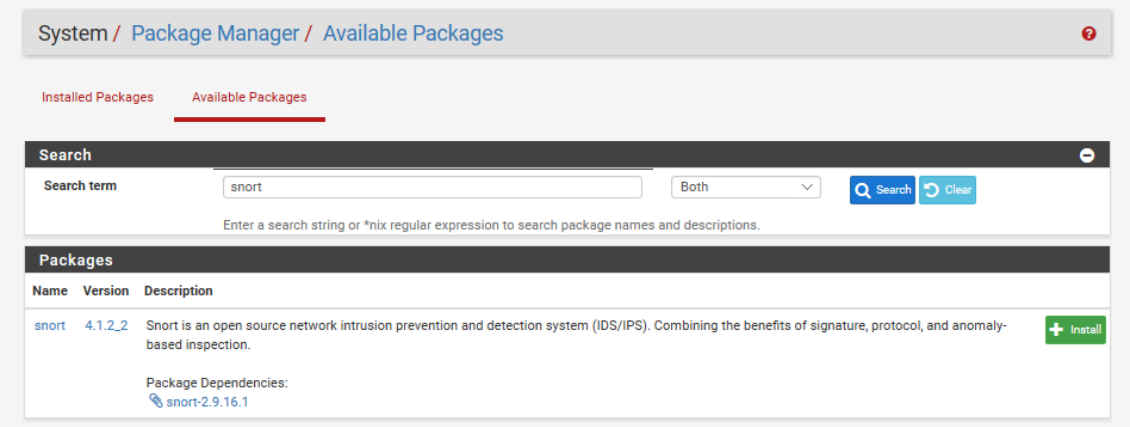



**Fuente:** Elaboración del Autor

### 2.5.3.2. Instalación y Configuración de SNORT

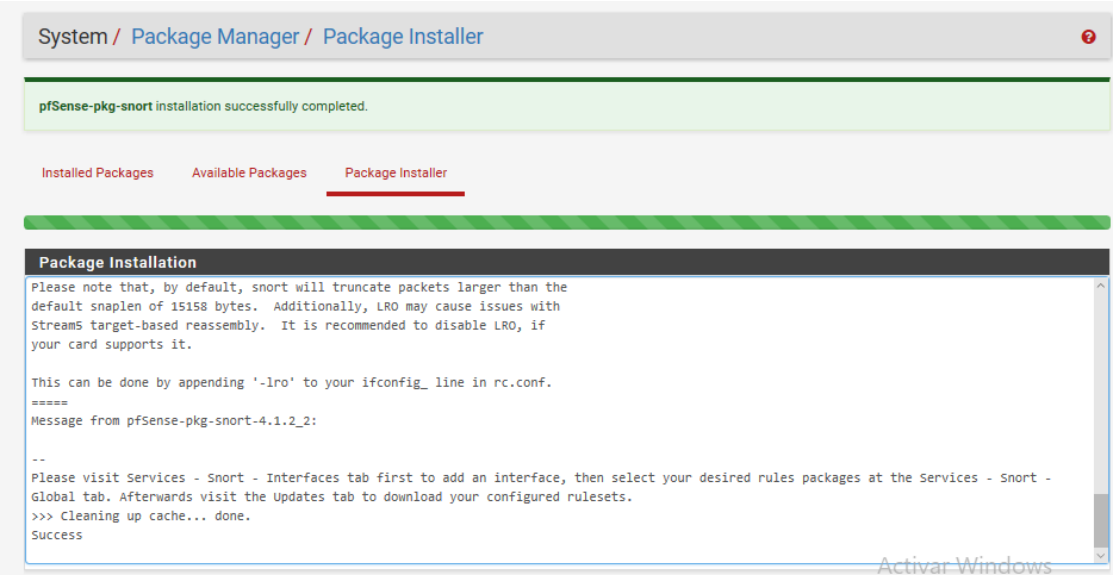
Gracias a la implementación de PFSense, se facilitó la instalación del paquete de detección y prevención de intrusos SNORT, dentro de Administrador de paquetes del firewall, buscamos al IPS y seleccionamos la opción de instalar. (ver ***Figura 27*** y ***Figura 28***)

**Figura 27.** Administrador de paquetes – Selección de SNORT




**Fuente:** Elaboración del Autor

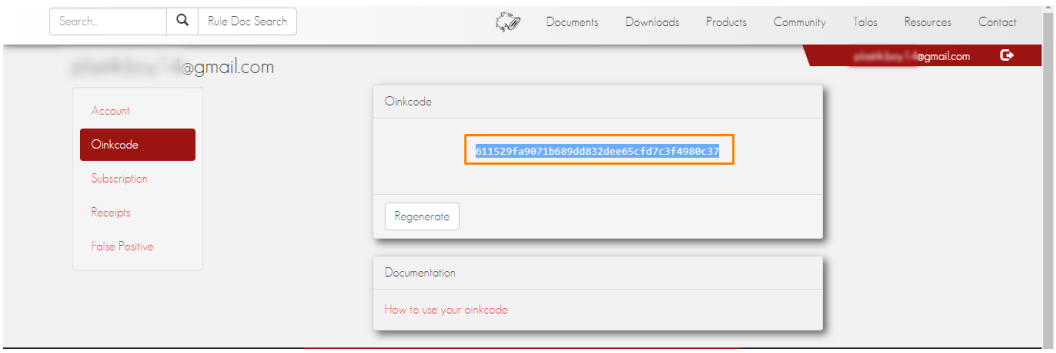
**Figura 28.** Instalación Completada – SNORT




**Fuente:** Elaboración del Autor

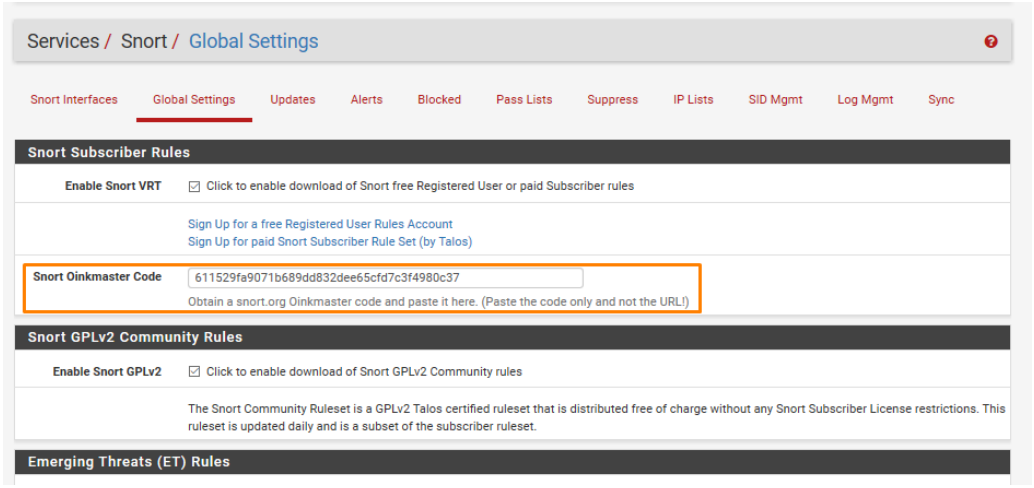
Para descargar las reglas que SNORT proporciona, fue necesario crearse una cuenta en el sitio oficial de este IPS, y generar el OINKCODE, que nos posibilita la descarga de estas reglas (ver ***Figura 29***, ***Figura 30*** y ***Figura 31***).

**Figura 29.** Generación de Oinkcode - SNORT



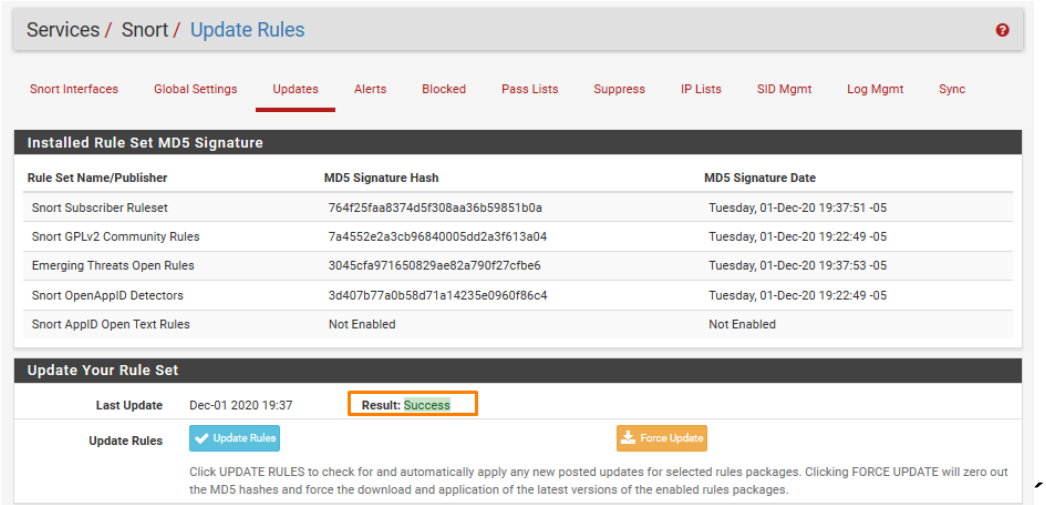

**Fuente:** Elaboración del Autor

**Figura 30.** Configuración Globales - SNORT




**Fuente:** Elaboración del Autor

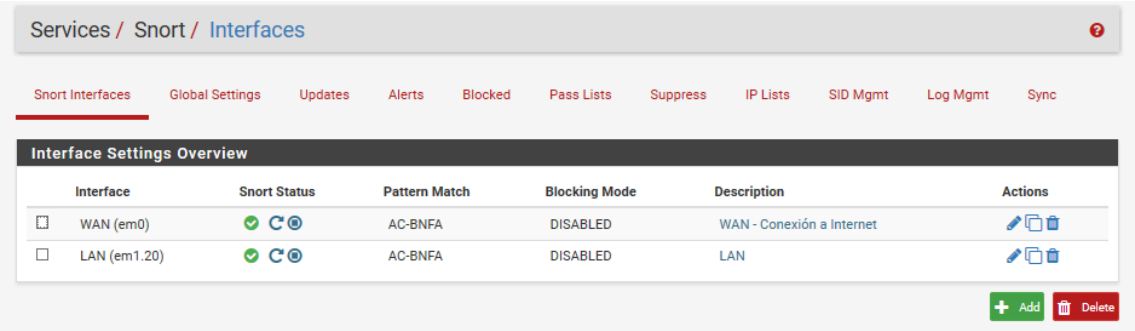
**Figura 31.** Instalación Completa de Reglas - SNORT




**Fuente:** Elaboración del Autor

En la **Figura 32**, podemos ver las reglas definidas para las interfaces WAN y LAN de la Arquitectura mediante SNORT.

**Figura 32.** Reglas Definidas para WAN y LAN - SNORT




**Fuente:** Elaboración del Autor

### 2.5.3.3. Instalación y Configuración del Honeypot (HoneyDrive / KIPPO)

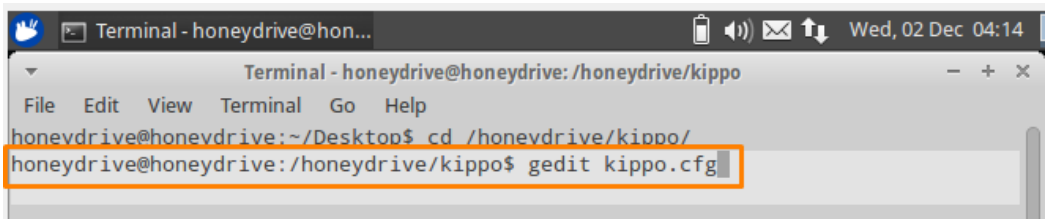
HoneyDrive es la herramienta que permite controlar el acceso a la red, su instalación es muy fácil, y se puede descargar desde su página oficial, La ***Figura 33***. muestra que luego de instalarla en una máquina virtual se tendrá un sistema operativo Linux XUBUNTU.

**Figura 33.** Instalación Completada - HoneyDrive


**Fuente:** Elaboración del Autor

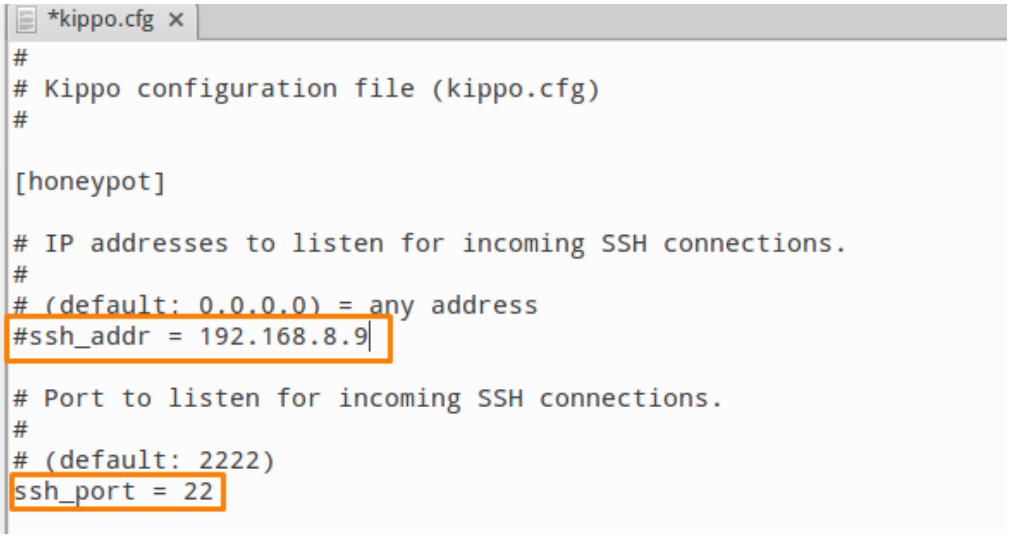
Este sistema operativo, presenta el sistema trampa KIPPO SSH, cuyo objetivo es obtener información sobre los ataques de fuerza bruta, exploits y/o malwares que pueden atravesar la red. El código de desarrollo para el honeypot Kippo está disponible gratuitamente [49].Para activar este servicio es necesario editar el archivo *kippo.cfg* y agregar la dirección IP del servidor y puerto para el acceso del servicio SSH (ver ***Figura 34*** y ***Figura 35***).

**Figura 34.** Terminal de Honeydrive - Editar Kippo.cfg




**Fuente:** Elaboración del Autor

**Figura 35.** Archivo de configuración - Kippo

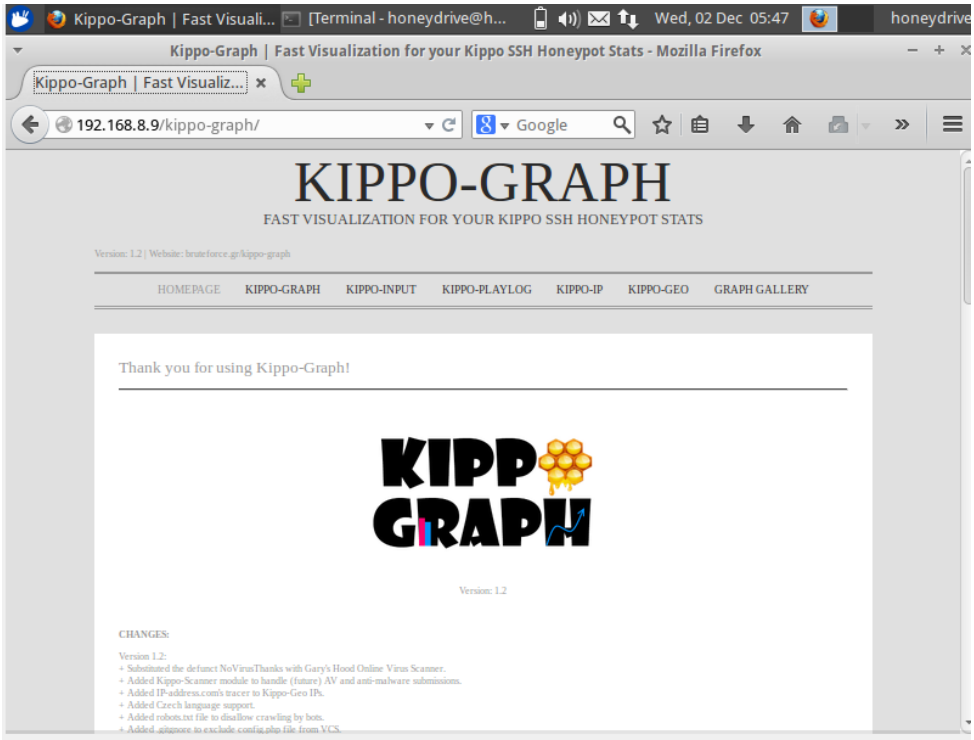



**Fuente:** Elaboración del Autor

Al terminar de configurar el sistema trampa, al ser este un Honeypot de baja interacción, tiene un bajo perfil dentro de la red DMZ donde se encuentra el resto de servicios de la Arquitectura.

Para iniciar el servidor de Kippo SSH, es necesario habilitarlo en la terminal de HoneyDrive dentro del directorio /honeydrive/kippo, e iniciarlo mediante el comando ./start.sh y luego se puede acceder con la IP de servidor al panel de administración del Honeypot (ver ***Figura 36***).

**Figura 36.** Panel de Administración - KIPPO SSH




**Fuente:** Elaboración del Autor

Si se desea configurar con más detalle este servidor, en el escritorio de Honeydrive, se encuentra un archivo denominado README.txt, que contiene más configuraciones disponibles para Kippo SSH.

# 3. CAPÍTULO III. EVALUACIÓN DEL PROTOTIPO

## 3.1. PLAN DE EVALUACIÓN

Para evaluar la arquitectura propuesta, es necesario definir un plan de evaluación, que compruebe el uso de las herramientas, y presente una ventaja frente a posibles amenazas que pudiéramos enfrentar en un escenario real.

### 3.1.1. Evaluación de Riesgos de la Seguridad de la Información

La evaluación de la gestión de riesgos de la presente propuesta tecnológica, se guio en las normativas aplicables ISO 27001/ ISO 27002, las cuales presentan buenas prácticas para la gestión de riesgos de seguridad de la información. Esta evaluación simula dos posibles tipos de ataques, interno (usuario de la LAN) y externo (Atacante mediante la interfaz de la WAN). La ***Tabla 6*****,** define las

herramientas usadas para efectuar los ataques y los protocolos vulnerables por defecto.

**Tabla 6.** Herramientas de Ciberataque - Evaluación de la Arquitectura

| Evaluación de la arquitectura | | | | | |
|---|---|---|---|---|---|
| **Herramienta** | **Protocolos Vulnerables** | | | | **Ataque Realizado** |
| | **SSH** | **FTP** | **TCP/IP** | **HTTP/S** | |
| PuTTY SSH | X | X | | | Ataque por contraseña |
| Medusa | X | | X | | Ataque de Fuerza Bruta |
| Nmap | X | X | X | X | Escaneo de Puertos |
| Legión | X | X | X | X | Penetración a la Red |
| Metasploit | X | X | X | | Ataque de Exploits |

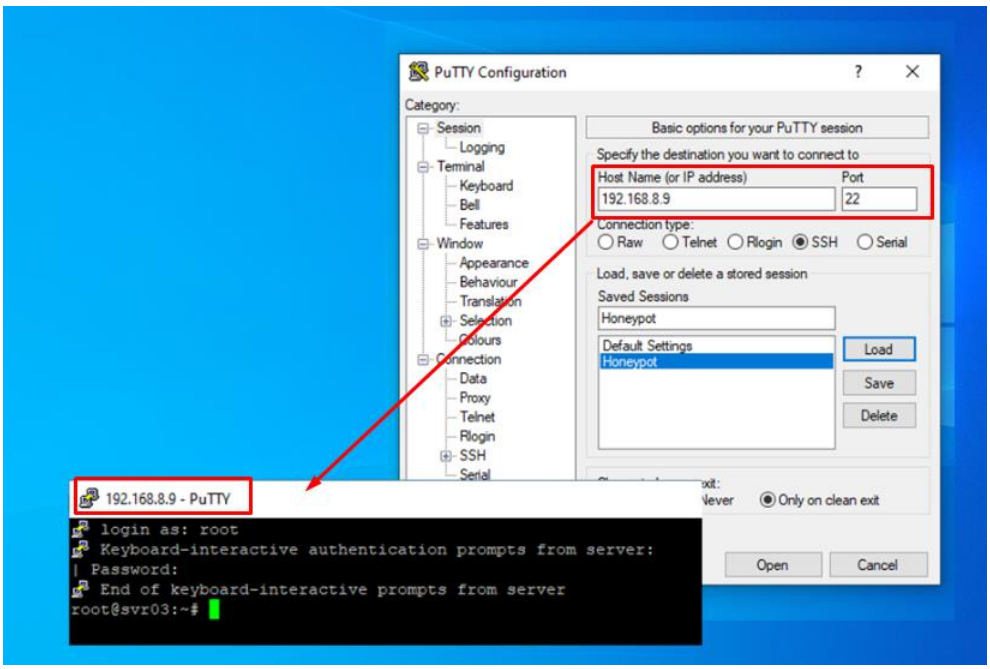
**Fuente:** Elaboración del Autor

## 3.2. RESULTADOS DE LA EVALUACIÓN

### 3.2.1. Conexión SSH entre Usuarios de la LAN y el servidor de Honeypot

La ***Figura 37***, muestra la configuración para la conexión remota entre un usuario de la LAN y red del Honeypot a través de PuTTY SSH.

**Figura 37.** Resultados - Conexión SSH entre Windows 10 y Honeypot

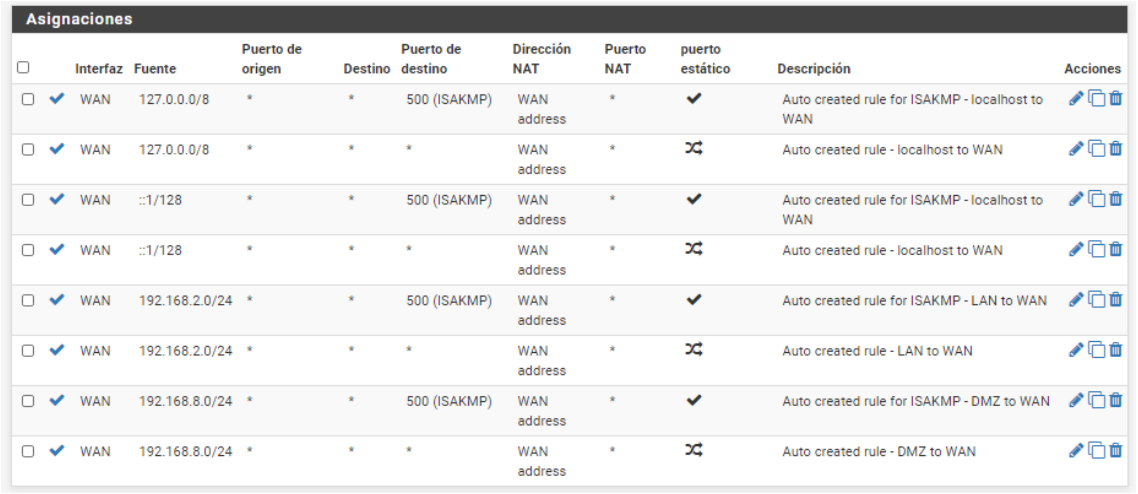



**Fuente:** Elaboración del Autor

### 3.2.2. Ping y Desvió de paquetes entre el atacante y el servidor de Honeypot

Para simular la conexión entre un supuesto atacante proveniente de la red externa o WAN, es necesario, configurar reglas de desvío en el Firewall (ver ***Figura 38***), para que pueda ser desviado correctamente.

**Figura 38.** Reglas NAT - PFSense



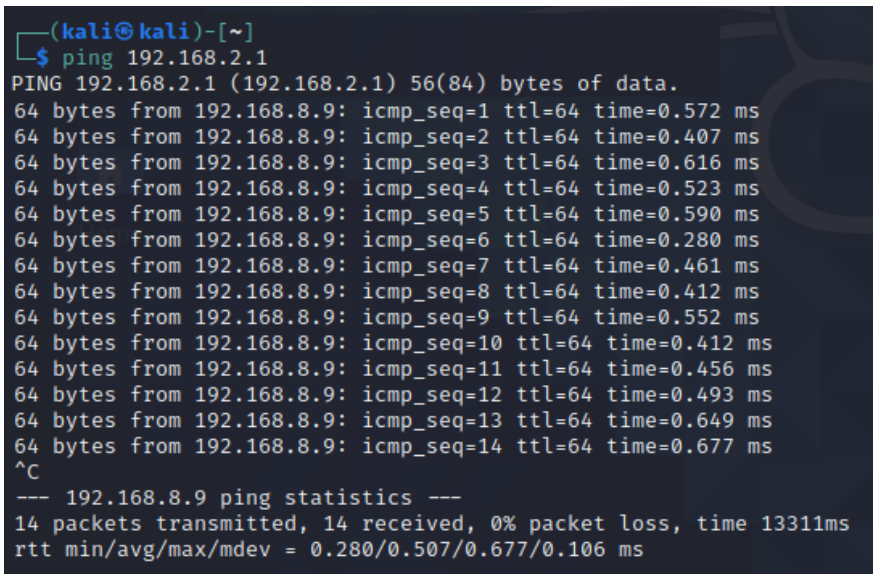
**Asignaciones**

| | Interfaz | Fuente | Puerto de origen | Destino | Puerto de destino | Dirección NAT | Puerto NAT | puerto estático | Descripción | Acciones |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ ✔ | WAN | 127.0.0.0/8 | * | * | 500 (ISAKMP) | WAN address | * | ✔ | Auto created rule for ISAKMP - localhost to WAN | |
| ☐ ✔ | WAN | 127.0.0.0/8 | * | * | * | WAN address | * | ⇄ | Auto created rule - localhost to WAN | |
| ☐ ✔ | WAN | ::1/128 | * | * | 500 (ISAKMP) | WAN address | * | ✔ | Auto created rule for ISAKMP - localhost to WAN | |
| ☐ ✔ | WAN | ::1/128 | * | * | * | WAN address | * | ⇄ | Auto created rule - localhost to WAN | |
| ☐ ✔ | WAN | 192.168.2.0/24 | * | * | 500 (ISAKMP) | WAN address | * | ✔ | Auto created rule for ISAKMP - LAN to WAN | |
| ☐ ✔ | WAN | 192.168.2.0/24 | * | * | * | WAN address | * | ⇄ | Auto created rule - LAN to WAN | |
| ☐ ✔ | WAN | 192.168.8.0/24 | * | * | 500 (ISAKMP) | WAN address | * | ✔ | Auto created rule for ISAKMP - DMZ to WAN | |
| ☐ ✔ | WAN | 192.168.8.0/24 | * | * | * | WAN address | * | ⇄ | Auto created rule - DMZ to WAN | |

**Fuente:** Elaboración del Autor

La ***Figura 39***, muestra la conexión exitosa entre ambas tramas de red.

**Figura 39.** Conexión Atacante con Honeypot



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.8.9: icmp_seq=1 ttl=64 time=0.572 ms
64 bytes from 192.168.8.9: icmp_seq=2 ttl=64 time=0.407 ms
64 bytes from 192.168.8.9: icmp_seq=3 ttl=64 time=0.616 ms
64 bytes from 192.168.8.9: icmp_seq=4 ttl=64 time=0.523 ms
64 bytes from 192.168.8.9: icmp_seq=5 ttl=64 time=0.590 ms
64 bytes from 192.168.8.9: icmp_seq=6 ttl=64 time=0.280 ms
64 bytes from 192.168.8.9: icmp_seq=7 ttl=64 time=0.461 ms
64 bytes from 192.168.8.9: icmp_seq=8 ttl=64 time=0.412 ms
64 bytes from 192.168.8.9: icmp_seq=9 ttl=64 time=0.552 ms
64 bytes from 192.168.8.9: icmp_seq=10 ttl=64 time=0.412 ms
64 bytes from 192.168.8.9: icmp_seq=11 ttl=64 time=0.456 ms
64 bytes from 192.168.8.9: icmp_seq=12 ttl=64 time=0.493 ms
64 bytes from 192.168.8.9: icmp_seq=13 ttl=64 time=0.649 ms
64 bytes from 192.168.8.9: icmp_seq=14 ttl=64 time=0.677 ms
^C
--- 192.168.8.9 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13311ms
rtt min/avg/max/mdev = 0.280/0.507/0.677/0.106 ms
```

**Fuente:** Elaboración del Autor

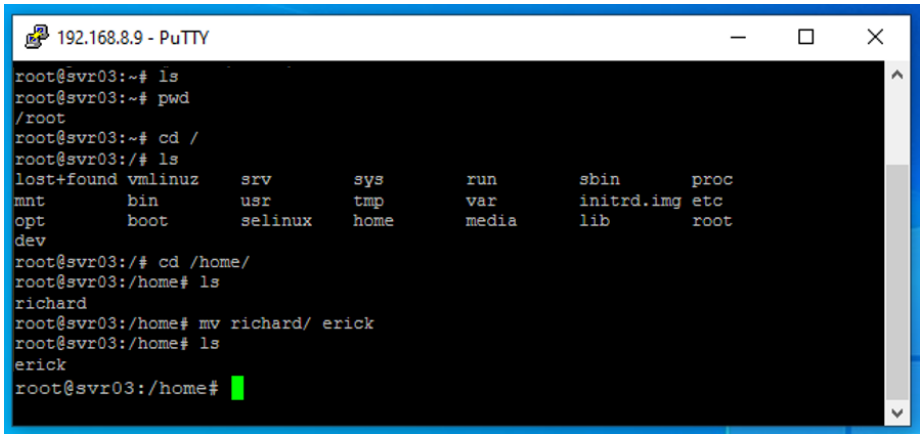
Con estas configuraciones ya está preparado el escenario para realizar los ataques al servidor de Honeypot que se tiene instalado.

### 3.2.3. ATAQUES

#### 3.2.3.1. PuTTY SSH

El cliente de SSH, PuTTY, facilito el ataque y permitió realizar cambios al directorio /home/ del servidor de Honeypot, mediante el puerto de SSH. Este ataque se lo hizo del lado de la LAN, con Windows 10 (***Figura 40***).

**Figura 40**. Ataque con PuTTY SSH

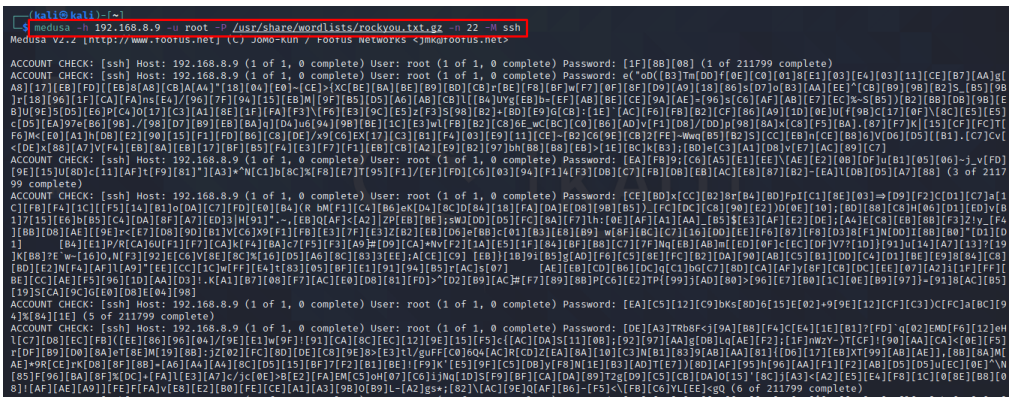



**Fuente:** Elaboración del Autor

#### 3.2.3.2. Medusa

Esta herramienta se usó por lado del atacante simulado, para realizar un ataque de fuerza bruta al honeypot basado en diccionarios de palabras (***Figura 41***).

**Figura 41.** Ataque con Medusa

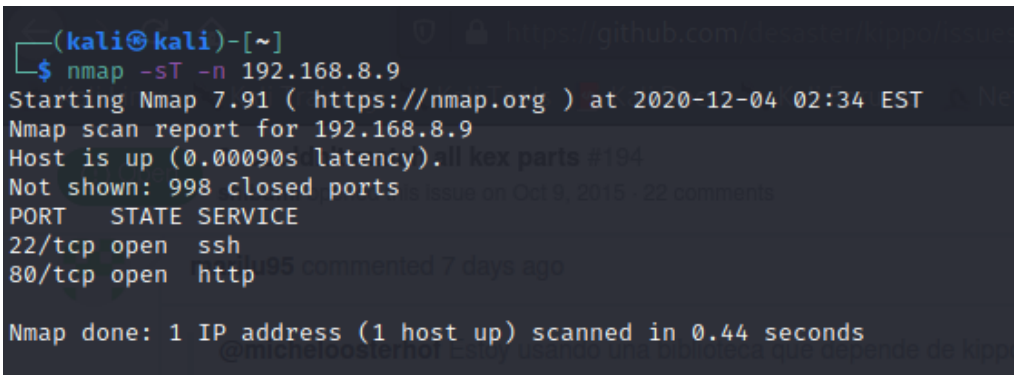



**Fuente:** Elaboración del Autor

### 3.2.3.3. Nmap

Mediante a Nmap, se realiza un escaneo de puertos (***Figura 42***), y se observa que los puertos que están siempre abiertos en el honeypot son 22 (ssh) y 80 (http), suelen ser más, pero por motivos que hay un solo atacante en la red, los demás puertos no son atacados.

**Figura 42.** Ataque con Nmap

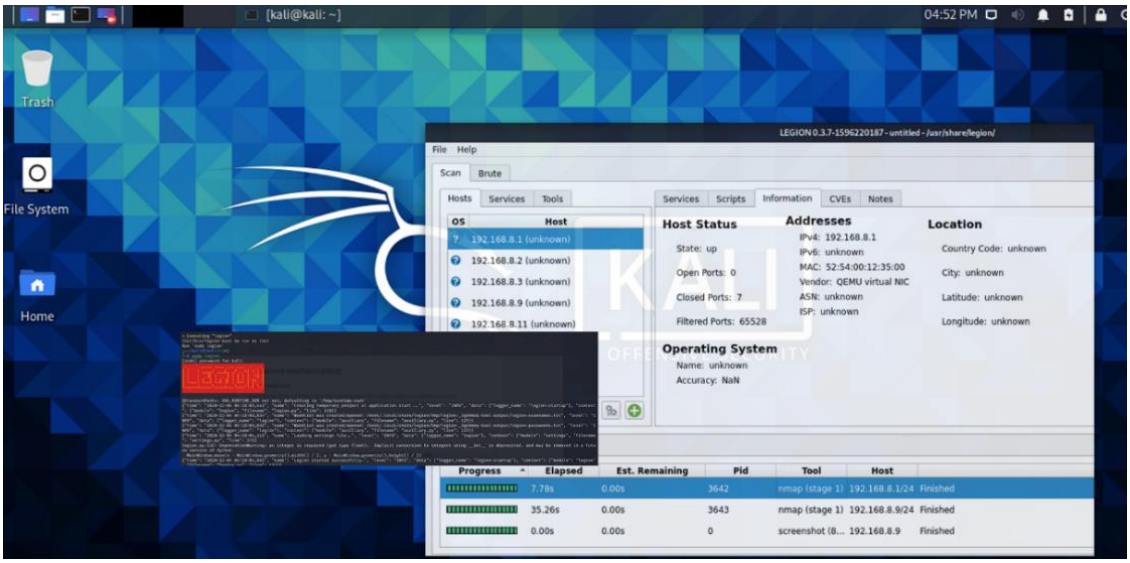



**Fuente:** Elaboración del Autor

### 3.2.3.4. Legion-Darck

La herramienta Legion-Dark, permite realizar un marco de prueba de penetración de red (***Figura 43***), y escanear todos los equipos que se encuentran en la red, identificando características importantes de los mismos.

**Figura 43.** Ataque con Legion-Dark

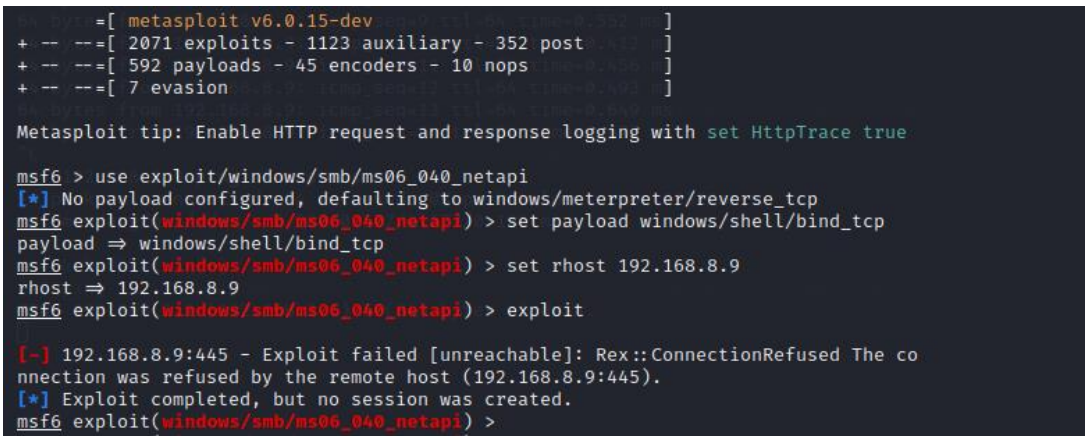



**Fuente:** Elaboración del Autor

### 3.2.3.5. Metasploit Framework Community

Con la herramienta Metasploit se crea un exploit dentro del servidor de Honeypot para analizar las vulnerabilidades de la misma (***Figura 44***).

**Figura 44.** Ataque con Metasploit Framework Community




**Fuente:** Elaboración del Autor

Luego de estos ataques podemos fijarnos que el honeypot capto toda la información necesaria de estas intromisiones dentro del administrador de KIPPO GRAPHS (***Anexo 4***), como por ejemplo las direcciones IP que ingresaron a la red del honeypot (***Anexo 5***).

Por otro lado, muestran las gráficas de la base de datos del honeypot (***Anexo 6***), así como los usuarios principales que ingresaron al sistema trampa (***Anexo 7***) y sus contraseñas (***Anexo 8*** y ***Anexo 9***). En definitiva, también identifica quien acceso a la red con éxito ( ***Anexo 10*** y ***Anexo 11***), además de su dirección IP (***Anexo 12***, ***Anexo 13***, ***Anexo 14***) y las conexiones remotas con SSH (***Anexo 15***).

Si verificamos el administrador de Snort, nos encontramos que se han detectado y bloqueado las alertas provenientes desde la red externa (***Anexo 16***), así como el rendimiento del tráfico de las redes de la arquitectura propuesta (***Anexo 17***).

## 3.3. CONCLUSIONES

- Una arquitectura de seguridad de red perimetral se presenta como una gran medida de resguardo frente a posibles ataques, sean estos internos o no, por lo que se debe tener analizar criterios como los servicios, criticidad, disponibilidad, fiabilidad, accesos y presupuesto para su implementación.
- El firewall PFSense, es una solución open source muy potente e intuitiva que reúne tecnologías avanzadas de protección de la red, la cual permite gestionar de gran medida la arquitectura, además trabaja muy bien con el IPS Snort ,el cual es capaz de examinar todo el flujo de la red y aporta elementos de seguridad apreciados en la red, lo mismo que el sistema trampa de baja interacción “Kippo”, que refleja toda la información posible de los ataques hechos por intrusos dentro de la red de empresa o de hogar.
- Actualmente, se implementan un sinfín de servicios dentro de una empresa, pero lo que casi siempre se opta por implementar dentro de una red son los servidores de DNS, AC DC, Correo y Archivos, los cuales permiten en gran medida simular una arquitectura en un ambiente controlado.
- Después de evaluar la funcionalidad de las herramientas de seguridad perimetral implementadas, se obtienen algunos resultados favorables para el administrador de la red, el cual, con la información de ataques generado por las herramientas, puede elaborar reglas de seguridad más adecuadas frente a posibles nuevos ataques.

## 3.4. RECOMENDACIONES

- De ser el caso de que la arquitectura presente se llegase a implementar en una empresa pequeña, se recomienda al administrador de la red, realizar un estudio más a profundidad de estas herramientas de seguridad implementadas, para su correcta adaptación con los dispositivos reales de la nueva red.
- Se recomienda además la adquisición de equipos físicos de seguridad perimetral, como el uso de un servidor dedicado de firewall que presente más características de seguridad empresarial, protegiendo a los equipos y servidores alojados en la red.
- Por otro lado, es recomendable analizar con detalle la información, obtenida en el sistema trampa implementado, sobre ataques de intrusos para tomar medidas como cambiar, permitir y denegar puertos cuando sea necesario, restringir acceso remoto al usuario root o limitar inicios de sesión. Esto será un gran acierto frente a posibles nuevos ataques.

## 3.5. REFERENCIAS BIBLIOGRÁFICAS


[1] M. Yar, “The Novelty of ‘Cybercrime’: An Assessment in Light of Routine Activity Theory,” *Eur. J. Criminol.*, vol. 2, no. 4, pp. 407–427, 2005, doi: 10.1177/147737080556056.

[2] F. J. Valencia-Duque and M. Orozco-Alzate, “Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000,” *RISTI - Rev. Iber. Sist. e Tecnol. Inf.*, no. 22, pp. 73–88, 2017, doi: 10.17013/risti.22.73-88.

[3] H. Emmanuel and R. Luna, “Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT),” *ReCIBE. Rev. electrónica Comput. Informática, Biomédica y Electrónica*, vol. 4, no. 1, p. VI, 2015.

[4] Marsh and McLennan, “The World Economic Forum.” https://es.weforum.org/.

[5] “Informe Global de Riesgos 2020.” https://www.marsh.com/mx/insights/research/global-risks-report-2020.html (accessed Oct. 13, 2020).

[6] R. A. Lika, D. Murugiah, S. N. Brohi, and D. A. P. V. Ramasamy, “NotPetya: Cyber Attack Prevention through Awareness via Gamification,” *2018 Int. Conf. Smart Comput. Electron. Enterp. ICSCEE 2018*, pp. 1–6, 2018, doi: 10.1109/ICSCEE.2018.8538431.

[7] N. B. Schirrmacher, J. Ondrus, and F. T. C. Tan, “Towards a response to ransomware: Examining digital capabilities of the WannaCry attack,” *Proc. 22nd Pacific Asia Conf. Inf. Syst. - Oppor. Challenges Digit. Soc. Are We Ready?, PACIS 2018*, 2018.

[8] “WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017 | Malware | The Guardian.” https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.

[9] Kaspersky, “STATISTICS | Real-time map of cyber threats Kaspersky.” https://cybermap.kaspersky.com/es/stats#country=35&type=ids&period=w .

[10] Kaspersky, “Kaspersky Threats — Intrusion.”

https://threats.kaspersky.com/en/class/Intrusion/ (accessed Oct. 14, 2020).

[11] D. Puthal, S. P. Mohanty, P. Nanda, and U. Choppali, “Building Security Perimeters to Protect Network Systems Against Cyber Threats [Future Directions],” *IEEE Consum. Electron. Mag.*, vol. 6, no. 4, pp. 24–27, 2017, doi: 10.1109/MCE.2017.2714744.

[12] A. Ladino *et al.*, “Fundamentos De Iso 27001 Y Su Aplicación En Las Empresas,” *Fundam. Iso 27001 Y Su Apl. En Las Empres.*, vol. 1, no. 47, pp. 334–339, 2011, doi: 10.22517/23447214.1177.

[13] Á. G. Vieites, *Seguridad en Equipos Informáticos*, RA-MA S.A. Madrid: Grupo Editorial RA-MA., 2014.

[14] C. R. Sampedro Guamán, S. A. Machuca Vivar, D. P. Palma Rivera, and F. A. Carrera Calderón, “Percepción de seguridad de la información en las pequeñas y medianas empresas en santo domingo,” *Investig. Operacional*, vol. 40, no. 3, pp. 421–428, 2019.

[15] ISO, “ISO - ISO / IEC 17799: 2005 - Tecnología de la información - Técnicas de seguridad,” 2005. https://www.iso.org/standard/39612.html.

[16] ISO, “La norma ISO 27001,” *La norma ISO 27001;Aspectos claves su implementación*, p. 21, 2003, [Online]. Available: https://www.isotools.org/pdfs-pro/ebook-ohsas-18001-gestion-seguridad-salud-ocupacional.pdf.

[17] J. AREITIO BERTOLIN, *Seguridad de la información. Redes, informática y sistemas de información*. Paraninfo Cengage Learning, 2008.

[18] C. De la Torre, M. Dela Torre, M. De la Torre, and A. De la Torre, “Planteamientos Básicos para la Implementación de las normas ISO 27001 e ISO 27002,” p. 39, 2017.

[19] ISO, “ISO - ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls.” https://www.iso.org/standard/54533.html.

[20] “Análisis de riesgos informáticos y ciberseguridad.” https://www.ambit-bst.com/blog/análisis-de-riesgos-informáticos-y-ciberseguridad#.

[21] K. Networks, “Los ciberataques más comunes que afectan a las empresas,” 2020. https://www.kionetworks.com/blog/ciberseguridad/los-ciberataques-mas-comunes-que-afectan-a-las-empresas.

[22] J. Chen and C. Guo, “Online Detection and Prevention of Phishing Attacks,” in *2006 First International Conference on Communications and Networking in China*, Oct. 2006, pp. 1–7, doi: 10.1109/CHINACOM.2006.344718.

[23] N. Z. Bawany, J. A. Shamsi, and K. Salah, “DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions,” *Arab. J. Sci. Eng.*, vol. 42, no. 2, pp. 425–441, 2017, doi: 10.1007/s13369-017-2414-5.

[24] M. Alazab, M. Alazab, A. Shalaginov, A. Mesleh, and A. Awajan, “Intelligent mobile malware detection using permission requests and API calls,” *Futur. Gener. Comput. Syst.*, vol. 107, pp. 509–521, 2020, doi: 10.1016/j.future.2020.02.002.

[25] C. Jim, “Tipos de Cortafuegos.” Técnico en seguridad informatica perimetral, Ecuador, 2020.

[26] C. A. Ocampo, Y. Viviana, C. Bermúdez, and G. R. Solarte Martínez, “Sistema de detección de intrusos en redes corporativas Intrusion Detection System in Corporate Networks,” *Sci. Tech. Año XXII*, vol. 22, no. 1, pp. 122–170, 2017.

[27] “Tipos de firewall: características y recomendaciones de uso | OBS Business School.” https://obsbusiness.school/es/blog-investigacion/propiedad-intelectual-y-seguridad-de-la-informacion/tipos-de-firewall-caracteristicas-y-recomendaciones-de-uso (accessed Nov. 26, 2020).

[28] M. Molina, K. Johanna, P. Meneses, and Z. Silgado, “Firewall : Una Solución de seguridad Informática,” *Rev. UIS Ing.*, 2009.

[29] L. Villela, “IMPLEMENTACIÓN DE UN SISTEMA DE PREVENCIÓN DE INTRUSOS EN LA VLAN DE SERVIDORES DE LA EMPRESA SONDA DE COLOMBIA S.A.,” *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2013.

[30] J. Koret and E. Bachaalany, “The Antivirus Hacker’s Handbook,” *Antivirus Hacker’s Handb.*, pp. 2–14, 2015, doi: 10.1002/9781119183525.

[31] Z. A. Hamed, I. M. Ahmed, and S. Y. Ameen, “Protecting Windows OS Against Local Threats Without Using Antivirus,” vol. 29, no. 12, pp. 64–70, 2020.

[32] C. Jim, “SISTEMA TRAMPA.” Técnico en seguridad informatica perimetral, Ecuador.

[33] A. Belqruch and A. Maach, “SCADA security using SSH honeypot,” *ACM Int. Conf. Proceeding Ser.*, vol. Part F1481, 2019, doi: 10.1145/3320326.3320328.

[34] H. López, M. José, L. Reséndez, and C. Francisco, “Aplicaciones Prácticas de los Honeypots en la Protección y Monitoreo de Redes de Información,” *CienciaUAT*, vol. 1, no. 2007–7521, pp. 8–12, 2007.

[35] D. Gordon Revelo and R. Pacheco Villamar, “Análisis de Estrategias de Gestión de Seguridad Informática con Base en la Metodología Open Source Security Testing Methodology Manual ( OSSTMM ) para la Intranet de una Institución de Educación Superior,” *Comput. e Informática*, vol. 7, no. 1, pp. 1–21, 2018, [Online]. Available: http://repositorio.uees.edu.ec/handle/123456789/2410.

[36] “Oracle VM VirtualBox.” https://www.virtualbox.org/.

[37] D. K. Damodaran, B. R. Mohan, M. S. Vasudevan, and D. Naik, “Performance Evaluation of VMware and VirtualBox,” vol. 29, pp. 23–28, 2012.

[38] J. Meinke and L. Peng, “SELECTING AND USING VIRTUALIZATION SOLUTIONS – OUR EXPERIENCES WITH VMWARE AND VIRTUALBOX,” *J. Comput. Sci. Coll.*, vol. 28, no. 1, 2012.

[39] K. Salah and A. Kahtani, “Performance evaluation comparison of Snort NIDS under Linux and Windows Server,” *J. Netw. Comput. Appl.*, vol. 33, no. 1, pp. 6–15, 2010, doi: 10.1016/j.jnca.2009.07.005.

[40] W. Caspi and S. Flores, “CONFIGURACION E IMPLEMENTACION DE UN SERVIDOR DE CORREO UTILIZANDO HERRAMIENTAS OPEN SOURCE EN EL INSTITUTO TECNOLOGICO SUPERIOR ‘ANGEL POLIBIO CHAVES’ DEL CANTON GUARANDA.,” UNIVERSIDAD ESTATAL DE BOLIVAR FACULTAD, 2011.

[41] V. Balu and M. Saraswathi, “Implementation of SAAS Compiler in Intranet,” *Int. J. Comput. Appl.*, vol. 107, no. 8, pp. 17–19, 2014, doi: 10.5120/18771-0075.

[42] L. Karteri, A. Çenga, I. Tafa, and J. Fejzaj, “Virtualization and live migration in VirtualBox,” vol. 12, no. 10, pp. 7–11, 2014.

[43] “pfSense® - World’s Most Trusted Open Source Firewall.” https://www.pfsense.org/.

[44] C. Ye, P. P. Indra, and D. Aspinall, “Retrofitting Security and Privacy Measures to Smart Home Devices,” *2019 6th Int. Conf. Internet Things Syst. Manag. Secur. IOTSMS 2019*, pp. 283–290, 2019, doi: 10.1109/IOTSMS48152.2019.8939272.

[45] “Snort - Network Intrusion Detection & Prevention System.” https://www.snort.org/.

[46] B. Sergey, “Intrusion Detection System and Intrusion Prevention System with Snort provided by Security Onion .,” *Bachelor’s Thesis Inf. Technol. MAMK Univ. Appl. Sci.*, no. May, 2016.

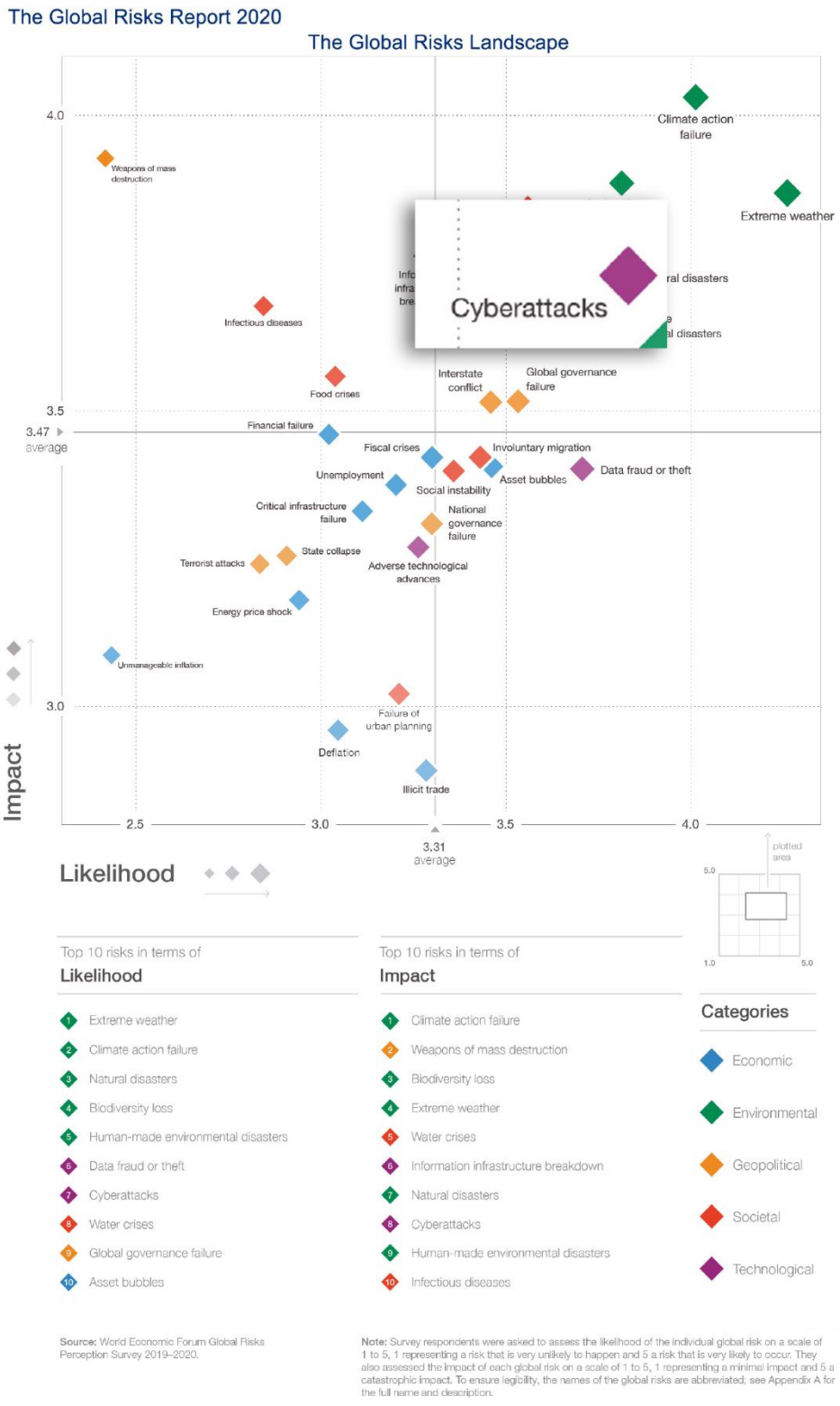
[47] “HoneyDrive download | SourceForge.net.” https://sourceforge.net/projects/honeydrive/ (accessed Dec. 03, 2020).

[48] L. Honeypots and D. Guerra, “Honeypots. L’art de la Guerra,” pp. 1–14, 2020.

[49] S. Dowling, M. Schukat, and E. Barrett, “Improving adaptive honeypot functionality with efficient reinforcement learning parameters for automated malware,” *J. Cyber Secur. Technol.*, vol. 2, no. 2, pp. 75–91, 2018, doi: 10.1080/23742917.2018.1495375.

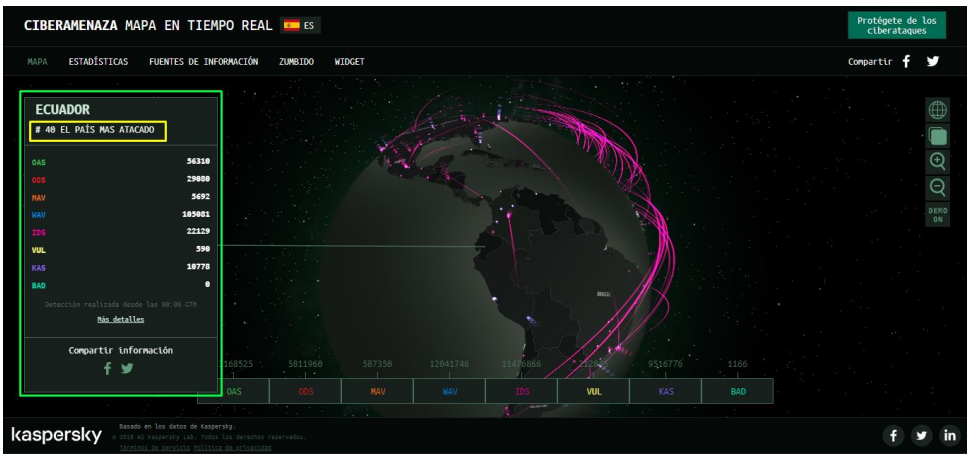
## ANEXOS

**Anexo 1.** Informe Global de Riesgos 2020



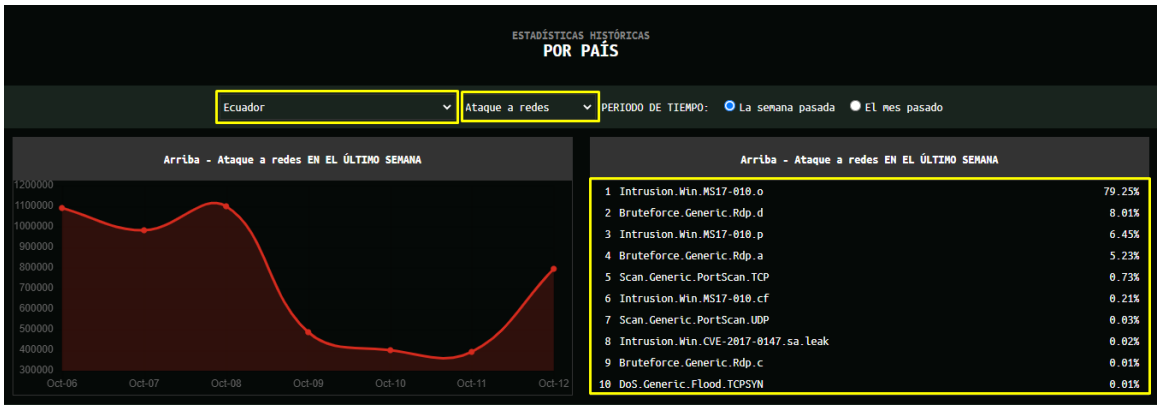

**Fuente:** Foro Económico Mundial [4]

**Anexo 2.** Estadísticas Generales de Ataques Cibernéticos en Ecuador




**Fuente:** Mapa de Amenazas Cibernéticas | Kaspersky [9]

**Anexo 3**. Ataques de Red en Ecuador (06-oct-2020 al 12-oct-2020)




**Fuente:** Estadísticas de Ataques de Red por País | Kaspersky [9]

**Anexo 4.** Actividad General del Honeypot - Kippo

Overall honeypot activity

| Total login attempts | 13326 |
|---|---|
| Distinct source IP addresses | 4 |

| Active time period | |
|---|---|
| Start date (first attack) | End date (last attack) |
| Thursday, 03-Dec-2020, 18:37 PM | Friday, 04-Dec-2020, 08:16 AM |

**Fuente:** Kippo Graph

**Anexo 5.** Actividad de IP recopilada del sistema honeypot - Kippo

IP activity gathered from the honeypot system

Click column heads to sort data, rows to display attack details.

| Total identified IP addresses: 4 | | | |
|---|---|---|---|
| IP address | Sessions count | Success | |
| 192.168.8.11 | 27008 | 0 | 2020-12-04 10:48:52 |
| 192.168.2.5 | 1 | 1 | 2020-12-04 06:03:55 |
| 192.168.2.4 | 2 | 1 | 2020-12-04 02:21:10 |
| 192.168.8.10 | 2 | 1 | 2020-12-03 23:12:00 |

10 CSV of all recent IP activity

**Fuente:** Kippo Graph

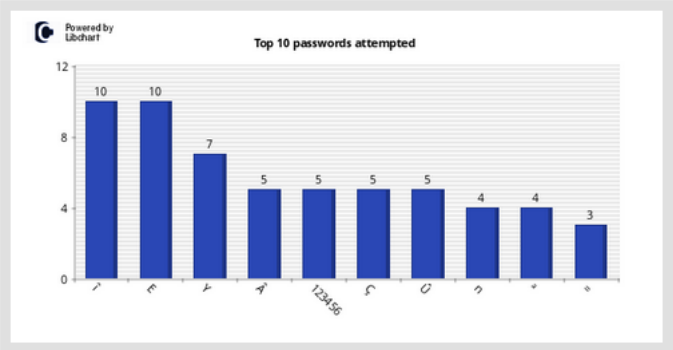
**Anexo 6.** Estadísticas gráficas generadas a partir de su base de datos de honeypot - Kippo

Graphical statistics generated from your Kippo honeypot database

Top 10 passwords

This vertical bar chart displays the top 10 passwords that attackers try when attacking the system.

CSV of all distinct passwords



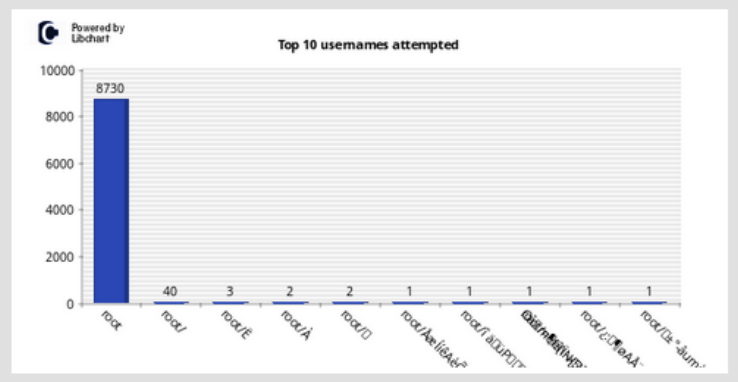

**Fuente:** Kippo Graph

**Anexo 7.** Los 10 nombres de usuario principales - Kippo

Top 10 usernames

This vertical bar chart displays the top 10 usernames that attackers try when attacking the system.

CSV of all distinct Usernames



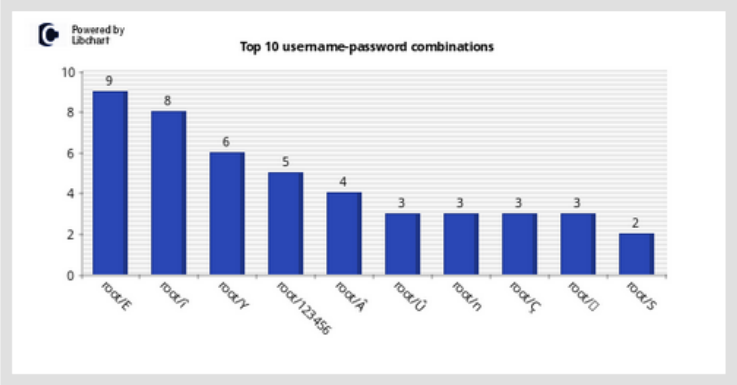

**Fuente:** Kippo Graph

**Anexo 8.** Los 10 mejores combos de pases de usuario - Kippo

Top 10 user-pass combos

This vertical bar chart displays the top 10 username and password combinations that attackers try when attacking the system.

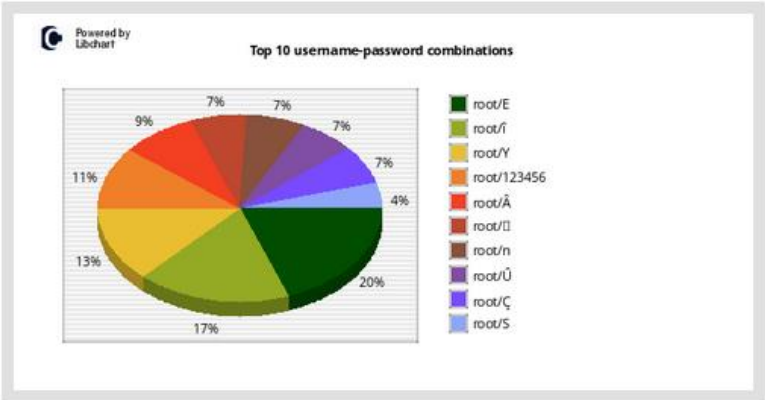
CSV of all distinct combinations




**Fuente:** Kippo Graph

**Anexo 9.** Las 10 mejores combinaciones de pases de usuario - Kippo

This pie chart displays the top 10 username and password combinations that attackers try when attacking the system.



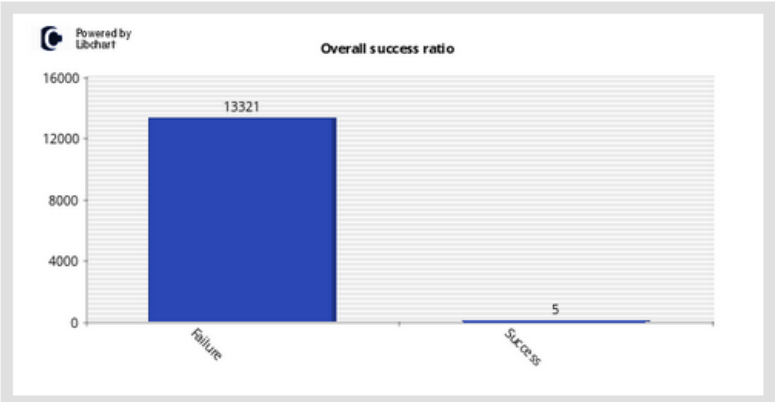

**Fuente:** Kippo Graph

**Anexo 10.** Ratio de éxito - Kippo

Success ratio

This vertical bar chart displays the overall attack success ratio for the particular honeypot system.

CSV of all successfull attacks



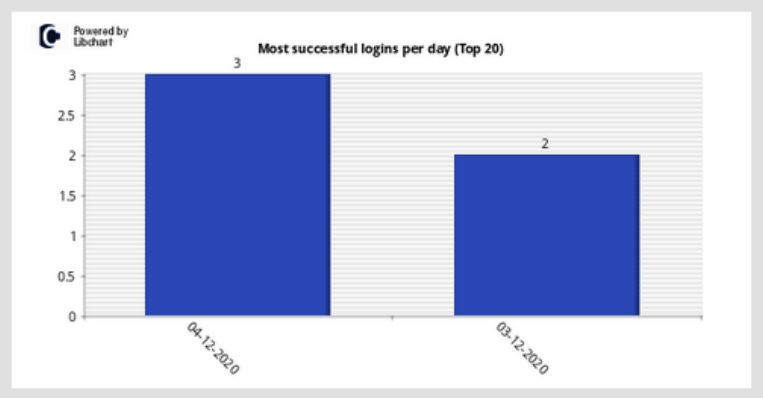

**Fuente:** Kippo Graph

**Anexo 11.** Éxitos por día / semana - Kippo

Successes per day/week

This vertical bar chart displays the most successful break-ins per day (Top 20) for the particular honeypot system. The numbers indicate how many times correct credentials were given by attackers.

CSV of all successful logons



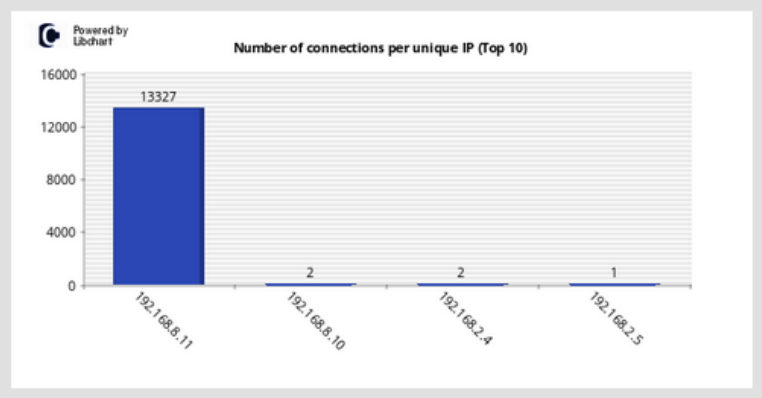

**Fuente:** Kippo Graph

**Anexo 12.** Conexiones por IP - Kippo

Connections per IP

This vertical bar chart displays the top 10 unique IPs ordered by the number of overall connections to the system.

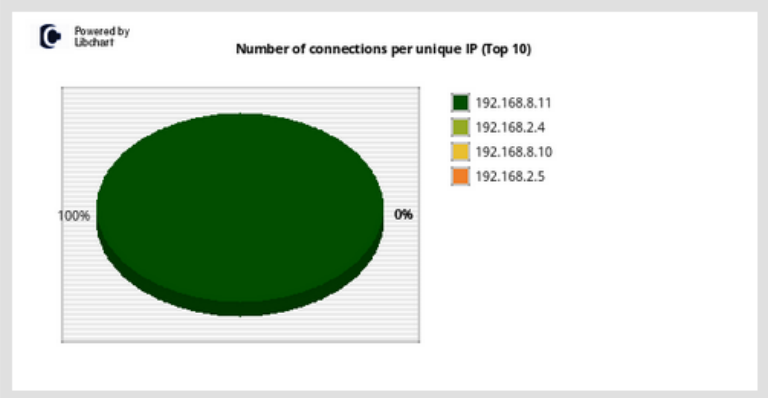
CSV of all connections per IP




**Fuente:** Kippo Graph

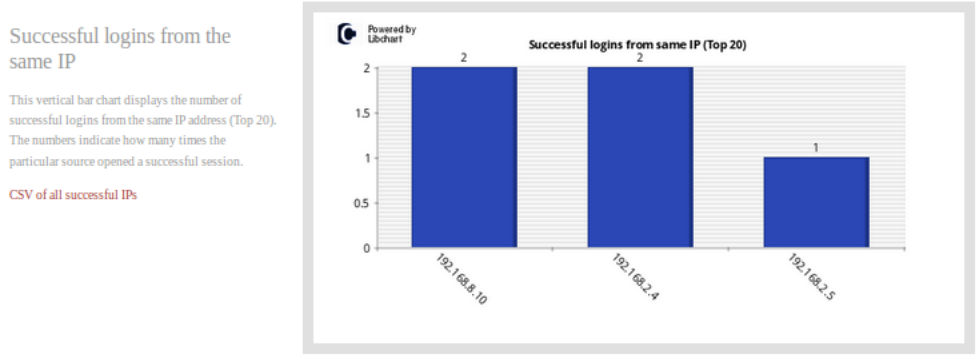
**Anexo 13.** Número de conexiones por IP única (Top 10) - Kippo

This pie chart displays the top 10 unique IPs ordered by the number of overall connections to the system.



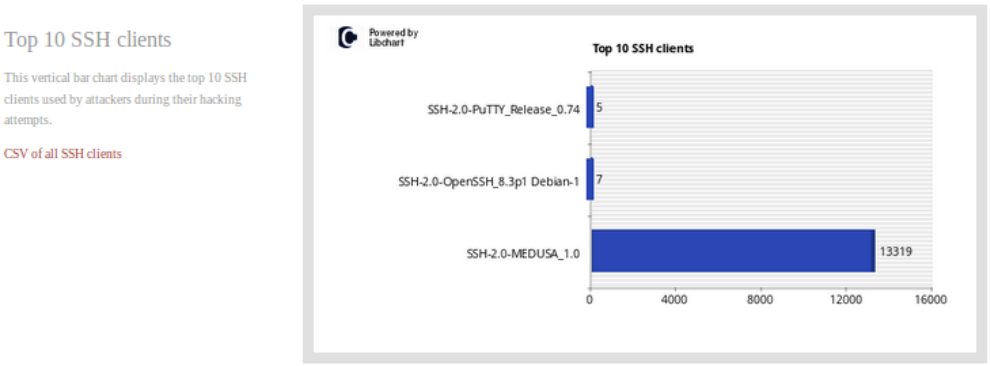

**Fuente:** Kippo Graph

**Anexo 14.** Inicios de sesión exitosos desde la misma IP - Kippo



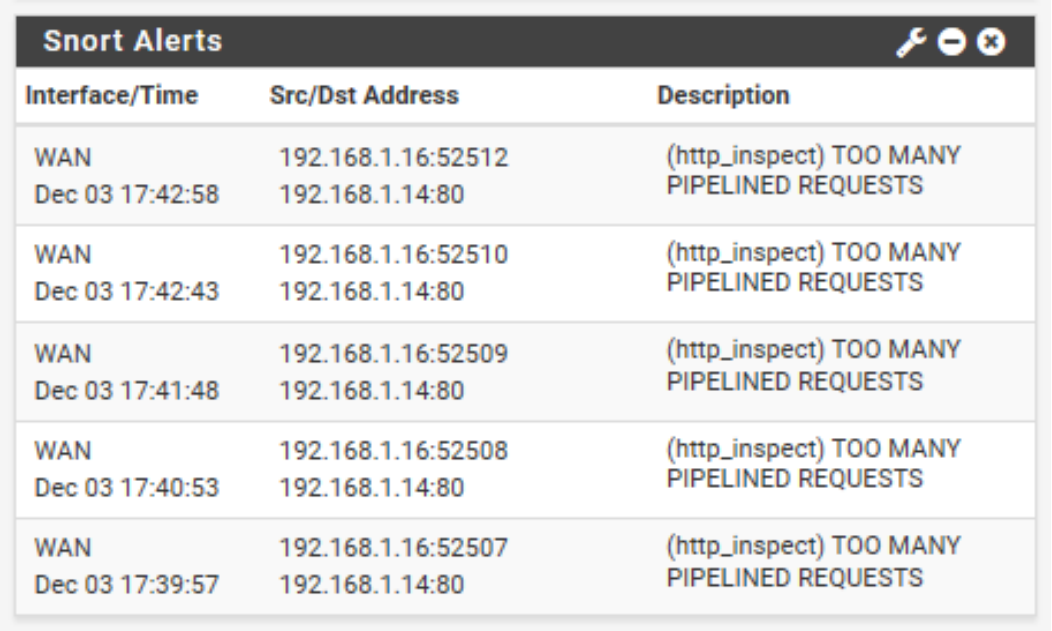

**Fuente:** Kippo Graph

**Anexo 15.** Los 10 principales clientes SSH - Kippo




**Fuente:** Kippo Graph

**Anexo 16.** Alertas de Instrusión - Snort

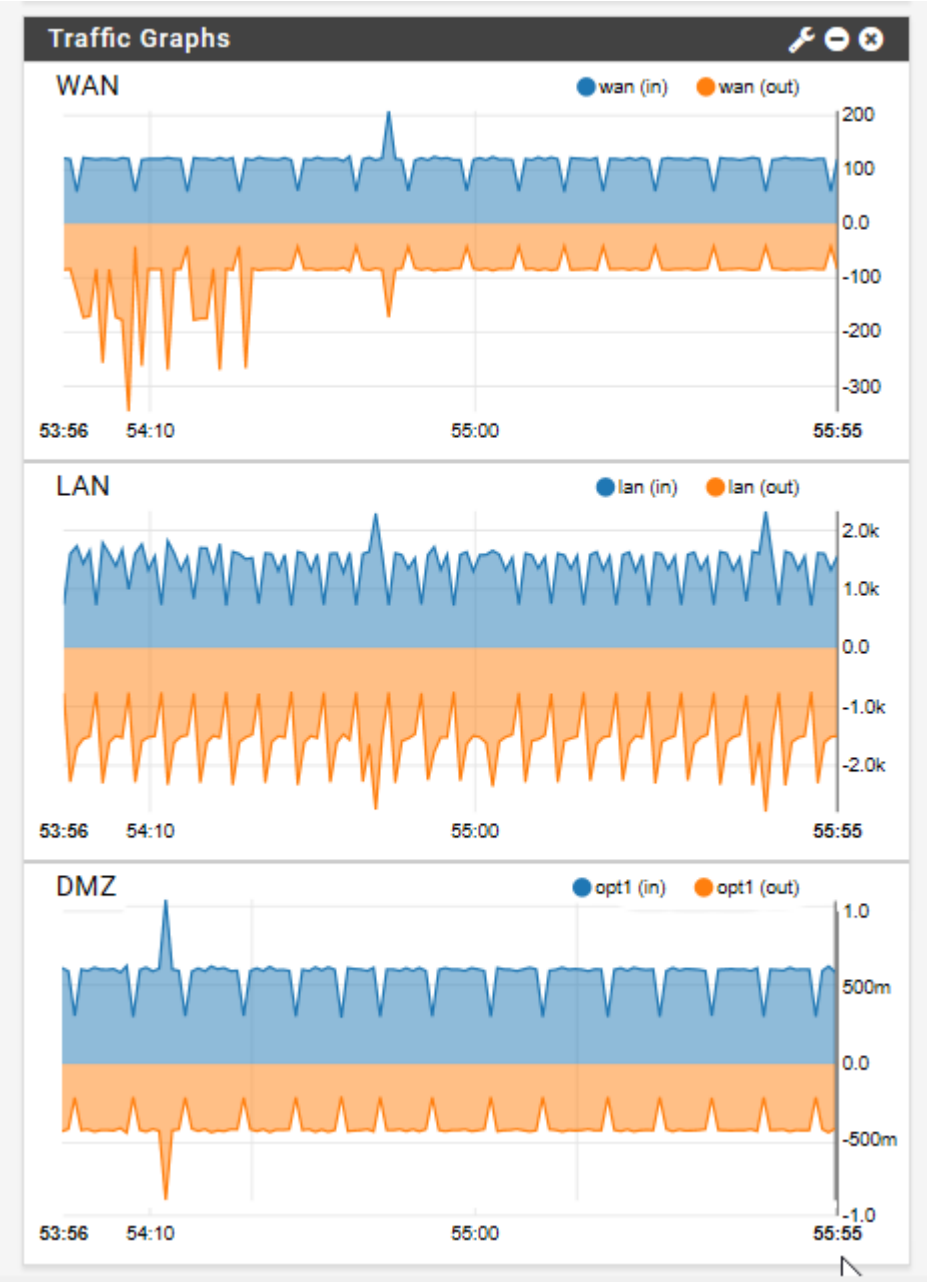


**Snort Alerts**

| Interface/Time | Src/Dst Address | Description |
|---|---|---|
| WAN<br>Dec 03 17:42:58 | 192.168.1.16:52512<br>192.168.1.14:80 | (http_inspect) TOO MANY PIPELINED REQUESTS |
| WAN<br>Dec 03 17:42:43 | 192.168.1.16:52510<br>192.168.1.14:80 | (http_inspect) TOO MANY PIPELINED REQUESTS |
| WAN<br>Dec 03 17:41:48 | 192.168.1.16:52509<br>192.168.1.14:80 | (http_inspect) TOO MANY PIPELINED REQUESTS |
| WAN<br>Dec 03 17:40:53 | 192.168.1.16:52508<br>192.168.1.14:80 | (http_inspect) TOO MANY PIPELINED REQUESTS |
| WAN<br>Dec 03 17:39:57 | 192.168.1.16:52507<br>192.168.1.14:80 | (http_inspect) TOO MANY PIPELINED REQUESTS |

**Fuente:** PFSense

**Anexo 17.** Trafico de las Redes de la Arquitectura




**Fuente:** PFSense