ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

DIRECCIÓN DE POSGRADO Y FORMACIÓN CONTINUA

INFORME DE INVESTIGACIÓN

PREVIA LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES Y SISTEMAS DISTRIBUIDOS

MODALIDAD:

PROYECTO DE INVESTIGACIÓN Y DESARROLLO

TEMA:

PLAN DE FORTALECIMIENTO ANTE ATAQUES INFORMÁTICOS EN EL CENTRO DE DATOS DE LA ESPAM APLICANDO MECANISMO DE SEGURIDAD HONEYPOT

AUTORA:

LISBETH CAROLINA MENDOZA VARELA

TUTOR:

MGTR. RAMÓN JOFFRE MOREIRA PICO

CALCETA, MAYO 2022

DERECHOS DE AUTORÍA

LISBETH CAROLINA MENDOZA VARELA, declaro bajo juramento que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, que se han respetado los derechos de autor de terceros, por lo que asumo la responsabilidad sobre el contenido del mismo, así como ante la reclamación de terceros, conforme a los artículos 4, 5 y 6 de la Ley de Propiedad Intelectual.

A través de la presente declaración cedo los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido en el artículo 46 de la Ley de Propiedad Intelectual y su Reglamento.

LISBETH CAROLINA MENDOZA VARELA

Firmado digitalmente por LISBETH CAROLINA MENDOZA VARELA

Lisbeth Carolina Mendoza Varela

CERTIFICACIÓN DE TUTOR

MGTR. RAMÓN JOFFRE MOREIRA PICO., certifica haber tutelado el trabajo de titulación **PLAN DE FORTALECIMIENTO ANTE ATAQUES INFORMÁTICOS EN EL CENTRO DE DATOS DE LA ESPAM APLICANDO MECANISMO DE SEGURIDAD HONEYPOT**, que ha sido desarrollado por **LISBETH CAROLINA MENDOZA VARELA**, previo la obtención del título de Magister en **Tecnologías de la Información Mención Redes Y Sistemas Distribuidos** de acuerdo al Reglamento de unidad de titulación de los programas de Posgrado de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López**.**

Firmado electrónicamente por:
RAMON JOFFRE MOREIRA PICO

MGTR. RAMÓN JOFFRE MOREIRA PICO

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaramos que hemos **APROBADO** el trabajo de titulación **PLAN DE FORTALECIMIENTO ANTE ATAQUES INFORMÁTICOS EN EL CENTRO DE DATOS DE LA ESPAM APLICANDO MECANISMO DE SEGURIDAD HONEYPOT,** que ha sido propuesto, desarrollado y sustentado por **LISBETH CAROLINA MENDOZA VARELA** previa la obtención del título de Magister en Tecnologías de la Información mención Redes y Sistemas Distribuidos, de acuerdo al Reglamento de la unidad de titulación de los programas de Posgrado de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

Firmado digitalmente porRicardo Antonio Velez Valarezo

Mgtr. Ricardo A. Vélez Valarezo

MIEMBRO

Firmado digitalmente por DANIEL AGUSTIN MERA MARTINEZ

Mgtr. Daniel Mera Martínez

MIEMBRO

ANGEL ALBERTO VELEZ MERO
Firma digital
avelez@espam.edu.ec

Mgtr. Ángel A. Vélez Mero

PRESIDENTE

AGRADECIMIENTO

Agradecer a Dios por haberme acompañado y guiado en toda mi carrera, por ser la fortaleza de mis debilidades por haberme permitido conocer un logro más en mi vida, por haberme hecho conocer que sin él las cosas no son posibles.

A mi tutor en especial, por su ayuda, su paciencia, por el tiempo dedicado y los conocimientos brindados,

A toda mi familia por darme ánimo durante este proceso,

A mis padres por la vida y por enseñarme a vivirla,

A todas las personas que me apoyaron e hicieron posible que este trabajo se realice con éxito, y

A mis amigos de la vida y de la facultad, por el apoyo diario.

Lisbeth Carolina Mendoza Varela

DEDICATORIA

A Dios principalmente dedico este trabajo, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional, a mis hijos Daniel y Odeth por ser mi motivo de cada día de luchar y seguir adelante, también a mi esposo y familia por estar pendiente de mí y en especial a mi tutor por guiarme, apoyarme y ser paciente en todo el proceso.

Lisbeth Carolina Mendoza Varela

CONTENIDO GENERAL

CONTENIDO DE TABLAS

CONTENIDO DE FIGURAS

RESUMEN

Las redes de comunicaciones se encuentran expuestas a ataques cibernéticos generando grandes pérdidas económicas y problemas en el funcionamiento de los sistemas dentro del centro de datos. La presente investigación tiene como objetivo analizar la implementación de una herramienta de seguridad informática Honeypot T-pot, desplegada en una infraestructura virtualizada. La tecnología Honeypot, herramienta que simula servicios y aplicaciones vulnerables en una red, permite realizar el control, captura y análisis de los datos recolectados, lo cual establece las formas de ataque, ubicación geográfica del atacante, direccionamiento IP, comandos utilizados, movimientos del atacante, y los mecanismos para poder disminuir estas anomalías. Para la ejecución de esta investigación se instaló una batería de honeypot T-pot debido a la variedad de equipos de infraestructura que integra el centro de datos de la ESPAM MFL, la metodología utilizada fue cualitativa, la ejecución se la realizó mediante el método informático ciclo en V, y se contemplaron las fases de: especificaciones, diseño de alto nivel y de detalle, implementación, y finalmente la del test unitario, de integración y operacional. Como resultado se obtuvieron ataques detectados a la infraestructura, ataques analizados por la herramienta maltrail lo cual permitió el análisis e interpretación de los datos lo que ayudó a establecer mecanismos de hardenización en el firewall hacia la zona desmilitarizada, como conclusión la implementación del Honeypot facilitó la caza del enemigo, el mismo que se desplegó antes del firewall de manera independiente, con la finalidad de evitar daños en la red de producción donde se encuentran los servidores.

PALABRAS CLAVE

Honeypot, T-Pot, Virtualización, Infraestructura, Ciberseguridad, Atacantes, Firewall, Ciclo En V.

ABSTRACT

Communications networks are exposed to cyber-attacks that present great economic losses and problems in the operation of systems within the data center. The objective of this research is to analyze the implementation of a Honeypot T-pot computer security tool, deployed in a virtualized infrastructure. Honeypot technology, a tool that simulates vulnerable services and applications on a network, allows control, capture and analysis of the data collected, which establishes the forms of attack, geographical location of the attacker, IP address, commands used, movements of the attacker, and the mechanisms to reduce these anomalies. For the execution of this investigation, a T-pot honeypot battery was installed due to the variety of equipment and infrastructure that integrates the ESPAM MFL data center, the methodology used was qualitative, the execution was carried out through the cycle computer method in V, and the phases of: specifications, high-level and detailed design, implementation, and finally unit, integration and operational testing were considered. As a result, detected attacks on the infrastructure were obtained, attacks analyzed by the maltrail tool, which allowed the analysis and interpretation of the data, which helped to establish hardening mechanisms in the firewall towards the demilitarized zone, as a conclusion, the implementation of the Honeypot facilitated the enemy house the same one that was independently deployed before the firewall, in order to avoid damage to the production network where the servers are located.

KEY WORDS

Honeypot, T-Pot, Virtualization, Infrastructure, Cybersecurity, Attackers, Firewall, V-Cycle.

CAPÍTULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

Internet se encuentra entre los inventos más importantes del siglo XXI que han afectado nuestra vida. Hoy en día Internet ha cruzado todas las barreras y ha cambiado la forma que usábamos para hablar, jugar, trabajar, comprar, hacer amigos, escuchar música, ver películas, pedir comida, pagar la factura, saludar a su amigo en su cumpleaños / aniversario, etc.(Leguizamón-Páez et al., 2020).

Cabe indicar que la masificación, despliegue y uso del internet a nivel mundial crece continuamente y de esta manera también crecen las vulnerabilidades por la usabilidad de equipos inteligentes conectados al internet que son un blanco para ciberdelincuentes, Según (Nagurney & Shukla, 2017a) indica que los efectos de los ataques cibernéticos se están sintiendo en todo el mundo en múltiples sectores e industrias. Los daños incurridos incluyen directamente daños financieros, así como problemas de reputación, la pérdida de negocio, la incapacidad de proporcionar los servicios esperados, oportunidad costos y la pérdida de confianza.

En abril de 2016, se descubrió el ransomware Petya. Petya hace que los discos sean inaccesibles, sobrescribiendo el registro maestro de arranque (MBR) de la computadora infectada hasta que se paga el rescate. La investigación muestra que Petya es el primer significativo ransomware por poseer un diseño de criptosistema fuera de línea completo, que se coloca a bajo nivel. Según la Oficina Federal de Investigaciones (FBI), se produjeron pérdidas estimadas de alrededor de mil millones de dólares estadounidenses ($ 1 mil millones) en ataques de ransomware en el año 2016. (Imaji, 2019). El 27 de junio de 2017, el ataque de malware Petya'2017 (también conocido como NotPetya, SortofPetya, ExPetr, NotPetya, tuvo lugar en la red informática de Ucrania. La primera información indicaba que se trataba de otro ataque de ransomware, pero pronto se hizo evidente que el malware estaba cifrando irreversiblemente los discos(Jakubski, 2017).

Es importante mencionar que la Universidad de Standford confirmó que dos de sus sitios web de diferentes departamentos habían sido vulnerados, donde el equipo técnico comprobó que habían sido sujetos de un inyección de malware lo mismo que extrajeron información como nombres número de teléfono cuentas de correo y credenciales de inicio de sesión de la misma manera la universidad de Michigan fue otra de las universidades vulneradas, donde confirmó que tres de sus servidores habían sido hackeados.(Smartekh, 2012).

Sin embargo, el Reporte de Seguridad de Latinoamérica 2019 de la prestigiosa empresa de ciberseguridad ESET revela que, del análisis de los datos suministrados por empresas de toda Latinoamérica, más del 60% sufrieron incidentes de seguridad, mediante la inserción de malware en el año anterior del reporte. (ESET, 2019).

En el Ecuador la fiscalía general de Estado a través de su Boletín titulado “Los delitos informáticos van desde el fraude hasta el espionaje” informa, que el uso del Internet ofreció nuevas modalidades para ciberdelincuentes de aprovechar brechas de seguridad y se exponen información confidencial de organizaciones públicas y privadas.

Según (Cuzme-Rodríguez et al., 2019) la implementación de medidas de seguridad en las direcciones de TI dentro de las instituciones de educación superior (IES) han aumentado en los últimos años debido a un alta tasa de ciberataques destinados a encontrar vulnerabilidades en sus servicios web y redes de comunicación, con énfasis en segmentos gubernamentales e instituciones estratégicas.

Los directivos de la Policía Nacional del Ecuador, indican que estudiantes de una universidad privada, habrían realizado la contratación de ciberdelincuentes con la finalidad de falsificar y modificar las calificaciones en el sistema de gestión académica de la institución, (Tiempo, 2013).

La Escuela Superior Politécnica Agropecuaria de Manabí ESPAM MFL es una institución de educación superior al servicio de la comunidad estudiantil nacional como internacional, que brinda una serie de carrera tanto de grado como de posgrado basada en su modelos de gestión administrativa, para este efecto cuenta

con un centro de datos donde están alojados todos los servidores, físicos como virtuales los mismo que tienen las aplicaciones y bases de datos en producción; por este motivo la información concentrada dentro del centro de datos se considera de carácter crítico. Según el reporte de incidentes de octubre 2019 del Equipo de Respuesta ante Incidencias de Seguridad Informáticas (CSIRT) de la importante empresa CEDIA, Red Nacional de Investigación y Educación Ecuatoriana (CEDIA, 2019), se dieron más de 650 ataques a el centro de datos de la ESPAM MFL, y, según datos obtenidos por el administrador del Data Center se generan ataques diarios que superan los 65 intentos anómalos de penetrar la infraestructura tecnológica. Con base en lo expuesto, el autor se plantea la siguiente interrogante:

¿De qué manera fortalecer la seguridad informática de modo que permita detectar fallos y establecer políticas de protección al centro de datos a la ESPAM MFL?

1.2. JUSTIFICACIÓN

La Constitución de la República del Ecuador, en su artículo 66 reconoce y garantiza, como parte de los derechos de libertad: "19.- El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. 20. El derecho a la intimidad personal y familiar. 21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. (…)" (Constitución de la Republica de Ecuador, 2008).

El Art. 230, 231, 232 y 234 del Código Orgánico Integral Penal, detalla los Delitos contra la seguridad de los activos de los sistemas de información y comunicación, en los cuales hace referencia a la intercepción ilegal de los datos y transferencia electrónica de (Código Orgánico Integral Penal, 2014).
El Art. 58, 61 y 62 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, se basan en la divulgación de informacion sensible de las entidades y Daños informáticos.

La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) en su norma técnica de incidentes y vulnerabilidades, define las vulnerabilidades, como una falencia de los servicios informáticos lo cual permite a un ciberdelincuente, obtener accesos no autorizados a los sistemas y atentar contra la confidencialidad, integridad, disponibilidad. (ARCOTEL, 2018).

La seguridad informática en la actualidad es de vital importancia para la subsistencia de toda organización que tenga sus sistemas accesibles desde el internet siendo este un mecanismo indispensable, ya que existen ciberdelincuentes que están husmeando las redes, con la finalidad de perpetrarse en los sistemas informáticos institucionales donde puedan acceder a información confidencial, sin embargo estas acciones se pueden repeler con una correcta implementación de políticas y herramientas de seguridad.

El desarrollo del presente proyecto tienen un gran nivel de importancia dentro de la institución donde se realiza, por motivos de desconocimiento de las brechas de inseguridad con las que cuenta el centro de datos de la universidad, esta problemática da como pauta que los ciberdelincuentes se enfoquen en la institución para cometer sus delitos, el respaldo o monitoreo de ataques y vulnerabilidades no se encuentran caracterizadas, ni clasificadas bajo ningún documento o archivo, sin embargo la ejecución del presente trabajo cuenta con un alto nivel de prioridad para la implementación ya que dentro de la institución no se han realizado investigaciones similares que permitan la confidencialidad, el acceso controlado a los sistemas y la intrusión de extraños y que permita la disponibilidad y confiabilidad de los datos institucionales.

En cuanto a lo económico, la investigación se encuentra justificada en que la implementación de un sistema de detección de intrusos, prevendrá ataques, clasificará los tipos y corregirá las intrusiones por parte de delincuentes informáticos, esto permitirá la pronta aplicación de políticas de seguridad dentro de la infraestructura tecnológica de la institución y así evitar el secuestro de sistemas o información confidencial de la institucional que demanden costos adicionales al no tener la debida protección de los mismos, por ende el valor económico debe ser devengado con la aplicación de las debidas políticas y niveles de protección para una correcta recuperación de datos institucionales.

Con el despliegue del Honeypot se puede identificar a los atacantes potenciales de la red de la ESPAM MFL, atraerlos, conocer cuáles son los movimientos laterales que puedan hacer, verificar comando utilizados, y todo esto mediante la simulación falsa de los sistemas instituciones, es decir, sin comprometer los sistemas reales, tanto así, que al obtener dichos reportes es de gran utilidad para el fortalecimiento de las vulnerabilidades encontrada por parte de los atacantes.

Se realizó un estudio y análisis de la red para definir la ubicación del sistema Honeypot, para no afectar a la red de la institución y que este sea un aporte más a los mecanismos de defensa en profundidad.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Diseñar un plan de fortalecimiento de seguridad perimetral ante ataques informáticos para el centro de datos de la ESPAM MFL basado en sistemas Honeypot.

1.3.1. OBJETIVOS ESPECÍFICOS

- Establecer los elementos de un sistema de seguridad basado en Honeypot.
- Proponer un modelo de despliegue del Honeypot que permita determinar los recursos de infraestructura necesaria.
- Simular ataques en un ambiente controlado, que permita analizar y estudiar ataques reales en un ambiente de producción.
- Evaluar y contrastar el análisis y comportamiento de la herramienta Honeypot para fortalecer la seguridad en la zona perimetral.
- Desarrollar un plan de fortalecimiento informáticos para el centro de datos de la ESPAM MFL utilizando herramientas de Honeypot.

1.4. HIPÓTESIS, PREMISAS Y/O IDEAS A DEFENDER

La implementación de un sistema Honeypot permitirá mejorar la seguridad del centro de datos de la ESPAM MFL.

CAPÍTULO II. REVISIÓN BIBLIOGRÁFICA

El presente trabajo tiene como finalidad el despliegue de un plan de fortalecimiento ante ataques informáticos en el centro de datos de la ESPAM MFL aplicando mecanismos de seguridad Honeypot. En este capítulo se va a realizar la revisión bibliográfica que estará divida en 3 partes:

- ✓ Seguridad Informática Ámbitos Generales
- ✓ Revisar procesos de seguridad perimetral y zonas desmilitarizadas
- ✓ Estudiar las soluciones basadas en Honeypot, y su aplicación de mecanismos de prevención caza de enemigo.

2.1. SEGURIDAD INFORMÁTICA ÁMBITOS GENERALES

Analizar investigaciones relacionadas a políticas de seguridad de la información, mecanismos de seguridad informática aplicadas a centros de datos de educación superior.

La seguridad informática se debe entender como la base de un estado de bienestar y de ausencia de riesgo. Existen países como Estados Unidos y Rusia en donde la seguridad informática es un tema de carácter nacional. Para (Vaca Urbina, 2016) la ciberseguridad es un ciencia que se basa en políticas y normativas para la protección de la información internas y externas de la organización, siendo esta la encargada de mantener la integridad, de los datos, contra cualquier tipo de amenazas de atacantes, reduciendo los riesgos de vulnerabilidad de la infraestructura tecnológica.

(Muñoz, 2015). El valor de la información confidencial de la empresa no se le da le trato respectivo que permita salvaguardar los datos y mantenerlos protegido como un activo valioso para la organización, esto en concordancia con Maiwald (Caralli et al. 2010), cuando los ordenadores se conectan entre si mediante redes, se originan inconvenientes de seguridad y los problemas se aumentan en diferentes formas. Debido a que no se establecen políticas de seguridad, desconociendo los peligros de las vulnerabilidades que se presentan en varios escenarios, (MAIWALD, 2004), manifiesta que los ataques a los sistemas

informáticos de las universidades, tuvieron su impacto en cuanto a modificaciones de notas en alumnos; el mismo peligro corren las empresas frente a los ataques y acceso no controlado a los sistemas, en el cual la informacion se puede ver comprometida y filtrada, y ataques generados al sector público gubernamental donde la información puede ser eliminada o exponiendo la seguridad de los datos públicos.

2.2. REVISAR PROCESOS DE SEGURIDAD PERIMETRAL Y ZONAS DESMILITARIZADA

SEGURIDAD PERIMETRAL

En el libro Mundo Hacker (Ramos Varón et al., 2014) sobre seguridad centralizada, manifiesta que la seguridad consiste en analizar y detectar anomalías en redes de datos e intromisión para prevenir amenazas, se deben utilizar técnicas y herramientas de monitorización de paquetes entrantes como salientes y sistemas de detección y prevención de intrusos.

Existen un sinnúmero de aplicaciones para la seguridad centralizada que aportan a mantener seguras la infraestructura y arquitectura de comunicación, como firewalls de siguiente generación, Honeypot, Honeynets, reglas de iptables sobre sistemas de seguridad entre otras. Asegurando la integridad de la información, analizando sistemas de criptografía, y certificados SSL. Con estos mecanismos se pretende fortalecer la seguridad de la información no se vean comprometidas(Morales et al., 2020).

Los ataques informáticos crecieron de manera exponencial en un 65% entre los años 2019 y 2021, especialmente en organizaciones que intentan realizar cambios continuos en nuevas versiones de aplicaciones (Morales Carrillo et al., 2019). Definitivamente, la carencia de políticas de ciberseguridad en los centros de educación superior públicos genera inconvenientes, que con el transcurso del tiempo se van acrecentando, y conforme aumenta la posibilidad de ser objetivo de ciberdelincuentes, mayor es el impacto del riesgo. Los ataques con mayor frecuencia son suplantación de identidad, fuerza bruta mediante diccionarios,

inyección de SQL e ingeniería social o Phishing con la firme intención de perjudicaría al usuario en distintas formas.

La seguridad centralizada cumple un rol fundamental en el funcionamiento de un centro de datos de toda organización. Estos mecanismos de solución se centran en el filtrado de información en la red. El despliegue de sistemas de detección y prevención de intrusos, criptografía asimétrica, SSL son de vital importancia para fortalecer el acceso a los sistemas en producción alojados en los servidores, (Conejos, 2014).

La seguridad perimetral en su forma más básica está ligada a fortalecer las brechas de inseguridad de un sistema e infraestructura en producción aplicando métodos posibles de defensa de la infraestructura tecnológica, aplicando reglas de protección perimetral de la red, logrando establecer parámetros de confianza entre personal interno como conexiones externas hacia determinados servicios y denegando todo tipo de acceso anómalo o sospecho que puedan comprometer la infraestructura tecnológica de la organización.

2.3 ESTUDIAR LAS SOLUCIONES BASADAS EN HONEYPOT, Y SU APLICACIÓN DE MECANISMOS DE PREVENCIÓN CAZA DE ENEMIGO.

Lo sistemas basados en Honeypot se definen como sistemas de caza de enemigos, ubicándose en lugares estratégicos de la red de prueba o producción, dependiendo del tipo de solución que se esté desplegando con información que parece ser valiosa para los intrusos. Su configuración es realizada con la finalidad que dificulte el acceso directo a los servicios expuesto dentro del Honeypot, (Dios y Ortiz, 2018).

Una solución basada en Honeypot es un recurso computacional constantemente monitoreado, el mismo que busca ser probado, atacado. Con la firme intención de establecer mecanismos de caza del enemigo y adelantarse a los eventos anómalos que pueden suceder en una red de aplicaciones real, conocer los movimientos de los atacantes, para aprender de ellos y fortalecer el acceso a la infraestructura tecnológica (Monroy & Castro, 2009).

Los diferentes mecanismos empleados por un administrador de un Honeypot, es la de simular y representar un ambiente de producción el cual debe tener un servicio muy importante que capte la atención del ciberdelincuente, por ejemplo: un sistema que contenga un servidor de aplicaciones, un servidor de transferencia de archivos, un sistema de base de datos ya que estos son los sistemas más propensos a ser atacados y que también brinde un nivel de seguridad al atacante al momento de ejecutar alguna técnica o metodología de intrusión consiguiendo un doble objetivo, desviar la atención de los atacantes de la red que contiene la información valiosa y por otro lado, se construye perfiles que permitan analizar las estrategias que siguen para fortalecer el firewall de defensa (Eduard & Daniel, 2013).

Una infraestructura con mecanismo de Honeypot desplegado, permite el control de intrusiones con aplicaciones de reglas en un firewall, luego que se obtienen resultados, se analizan y se fortalece dicho firewall, el objetivo es crear una red donde se simulen los servicios institucionales y no los sistemas reales que se encuentran dentro de una DMZ.

2.4. TIPOS DE HONEYPOT

2.4.1. HONEYPOT DE PRODUCCIÓN

Los honeypot de producción tienen como finalidad proteger e informar las anomalías en una red de producción como mecanismo de defensa y están expuestos a ciberatacantes los 365 días del año. Esta herramienta de detección de ataques permiten complementar la protección de la red y los hosts.(Hernández y Lerma, 2007).

2.4.2. HONEYPOT DE INVESTIGACIÓN

Son desplegados con la intención de informar y reducir intromisiones a los sistemas de producción, estudiando comportamientos y amenazadas de cualquier tipo, siendo implementados en ambientes controlados, (Hernández y Lerma, 2007).

2.4.3. HONEYPOT DE BAJA INTERACCIÓN

Estos Honeypot trabajan emulando servicios y sistemas operativos configurados por el administrador del Honeypot, como FTP, probablemente permitirá la ejecución de algunos comandos FTP, sin la representación ni efectos colaterales a los sistemas y redes en producción (Hernández y Lerma, 2007).

2.4.4. HONEYPOT DE ALTA INTERACCIÓN

Este tipo de Honeypot componen una solución de difícil perpetración la cual, involucra la utilización de servicios reales implementados como sistemas de producción, implican aplicaciones las cuales se ejecutan de forma real, en algunos casos tienen interacción directa con la infraestructura de la institución. Si un Honeypot de alta interacción no se encuentra protegido por parte de un sistema de seguridad perimetral firewall, un atacante puede acceder a él para infiltrarse en el sistema que se ha de proteger o que a partir de ahí pueda hacer algún movimiento lateral de ataques en otro servidor de la red(Hernández y Lerma, 2007).

2.4.5. BATERÍAS DE HONEYPOT

Adbhoney:

Son específicamente diseñados para sistemas con tecnología Android, Debug, Bridge sobre TCP/IP (Trajanovski,2021).

Ciscoasa:

Son sistemas de caza de enemigos que permiten detectar vulnerabilidades CVE-2018-0101. Un DoS y vulnerabilidad de ejecución remota, (Cymmetria, 2018).

Citrixhoneypot:

Este crea un sitio web falso sobre el Protocolo de transferencia Segura de Hipertexto (HTTPS) en donde los posibles atacantes trataran de ingresar usando una forma de autenticación para vulnerar la seguridad de la página, (Hänninen,2020).

Conpot:

Se describe a Conpot como un honeypot de baja interacción, el cual permite emular una infraestructura industrial compleja, siendo fácil su implementación,

modificación y extensión. El objetivo es recopilar información sobre los motivos y métodos de los adversarios que apuntan a la entidad u organización, (Serrano y Ruiz, 2021).

Dicompot:

Digital imaging and cominications in medicine (MICOM) Honeypot, DICOM permite la integración de datos digitales de escáneres, cámaras de video, servidores, estaciones de trabajo, impresoras y hardware de red proporcionadas por diferentes compañías en un solo PACS.

Dionaea:

Un honeypot Dionea de baja interacción escrito en C y Python está diseñado para la simulación de servicios que contengan vulnerabilidades. Estos servicios pueden ser SMB, HTTP, FTP, MYSQL entre otros. Dionaea recopila información sobre las vulnerabilidades utilizados por el programa maligno de esta manera se obtiene una copia secuestrada del programa maligno utilizado, (Banfi,2021).

Elasticpot:

Este es un Honeypot que simula un servidor Elasticsearch vulnerable abierto al internet.

Heralding:

Honeypot simple que recompile credenciales, nada más. Actualmente se admiten los siguientes protocolos: ftp, telnet, ssh, rdp, http, https, etc, (Vestergaard,2020).

Honeysap:

Es un Honeypot enfocado en la investigación de baja interacción específico para los servicios de SAP. Su objetivo es aprender las técnicas y motivaciones detrás de los ataques contra los sistemas SAP.

Mailoney:

Honeypot interactivo SMTP que permite entre otras cosas capturar contraseñas y tipos de ataques.

Medpot:

Honeypot FHIR es un estándar para el intercambio de datos de atención médica, publicado por HL7.

Rdpy:

Honeypot para protocolo RDP escrito en Python emulado cliente y servidor.

2.4.6. COMPONENTES DE HERRAMIENTAS DE UNA BATERIA DE HONEYPOTS

Cockpit: Interfaz gráfica para contenedores docker, sobre sistemas operativo, reducidos, (Paz, 2020).

Cyberchef: aplicación para cifrado codec y análisis de paquetes. (Paz, 2020).

ELK Stack: visualización de batería T-pot (Paz, 2020).

Elasticsearch Head: administrador de cluster de Elasticsearch.

Fatt: permite la extraccion y caprura de trafico en tiempo real (Paz, 2020).

Spiderfoot: sistema experto en inteligencia de negocio de código abierto (Paz, 2020).

Suricata: Motor de monitoreo de seguridad de red. (Paz, 2020).

CAPÍTULO III. DESARROLLO METODOLÓGICO

3.1. DISEÑO DE LA INVESTIGACIÓN

La investigación se aplicó en el Centro de Datos de la Escuela Superior Politécnica Agropecuaria de Manabí ESPAM MFL aplicando mecanismo de seguridad Honeypot. La metodología utilizada en el proceso de investigación será introspectiva vivencial, cualitativa. La ejecución del presente proyecto se llevó a cabo con la utilización del método ciclo en V, siendo las fases detalladas a continuación las aplicadas, Fase de especificaciones, Fase de diseño de alto nivel y de detalle, Fase de Implementación, Fase de test unitario, de integración y operacional.

3.2. UBICACIÓN

El presente proyecto se realizó en la Escuela Superior Politécnica Agropecuaria de Manabí ESPAM MFL, dentro del centro de datos de la institución.

3.3. MÉTODOS Y TÉCNICAS

3.3.1. MÉTODO

La metodología utilizada en el proceso de investigación será introspectiva vivencial, cualitativa. La ejecución del presente proyecto se llevó a cabo con la utilización del método ciclo en V, siendo las fases detalladas a continuación las aplicadas, Fase de especificaciones, Fase de diseño de alto nivel y de detalle, Fase de Implementación, Fase de test unitario, de integración y operacional.

3.3.2. FASE DE ESPECIFICACIONES

Esta fase define los mecanismos que se llevan a cabo en el data center de la ESPAM MFL, siendo la caracterización de la infraestructura tecnológica el punto de origen, se planteó una entrevista al personal que labora en el área de tecnología y centro de datos para comprobar los requerimientos e inconvenientes de los servidores, obteniendo la información detallada y el nivel de seguridad de la información de la institución.

La seguridad hoy en día es fundamental para la supervivencia de toda institución exigiendo a los responsables de la protección de los datos a mantener la vanguardia tecnológica y desplegar diferentes tipos de prevención de anomalías como caza de enemigo honeypot, el cual tiene el propósito de detectar como los cibercriminales les están atacando, todo esto con la finalidad de establecer medidas de protección necesarias para que la infraestructura no sea vulnerada por ataques que se encuentran perpetrando la infraestructura.

(RZ, 2021) La función principal del Honeypot es detectar y obtener información del ataque informático, y, sobre todo, obtener la ubicación exacta de precedencia, para posteriormente fortalecer las reglas de firewall necesarias donde se encuentren vulnerabilidades. Los honeypot altamente confiables ya que les permite atraer atacantes, simular servicios reales y verificar sus movimientos dentro de los mismos, El posicionamiento de una infraestructura de honeypot debe estarán en un sistema aislado donde el administrador pueda visualizar, es decir, cuáles son los comandos utilizados, movimientos laterales, ingreso indebido entre otros y las brechas de seguridad que puedan ser explotadas.

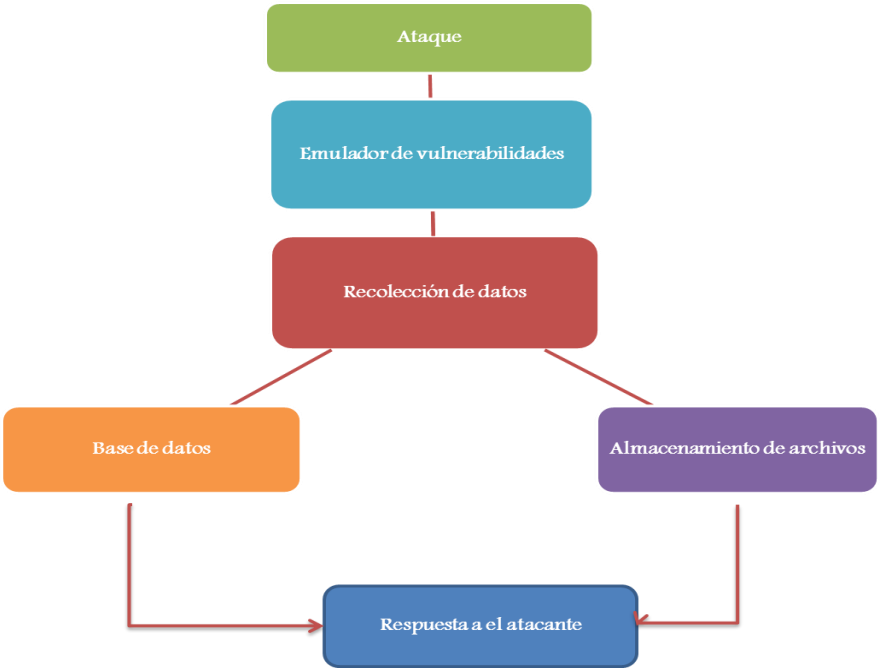


Figura 1. Modelo planteado de un honeypot

Fuente: Elaborado por el autor

Tabla 1 *Herramientas utilizadas en el caso de estudio.*

Componente	Características	Breve descripción
VMWare Workstation	VMWare Workstation	Plataforma de Virtualización de Sistemas Operativos
Honeypot	Tpot	Herramienta de seguridad informática para detectar y obtener información de ataques.
Firewall	pfSense	Herramienta de seguridad informática para filtrar tráfico de y bloquear accesos no autorizados
Kali Linux	Kali Linux Nessus	Herramienta de hacking ético y pruebas de penetración.
Metasploit	Metasploit	Herramienta de seguridad informática para realizar pruebas vulnerabilidades de la red.
Web server	Badblue	Herramienta capaz de transformar la máquina en un servidor Web.
SERVER APP	Lampião	Servidor de aplicaciones

Fuente: El autor

Beneficios del Uso de honeypot en los centros de datos

Los sistemas de caza de enemigos honeypot son un complemento para la seguridad centralizada que cualquier administrador de red debe aplicar, para minimizar riesgos de vulnerabilidad y conocer los diferentes movimientos y comandos que realiza un ciberdelincuente al momento de querer perpetuar la infraestructura tecnológica, capturando malware, y generando alerta sobre un ataque (WeLiveSecurity, 2020).

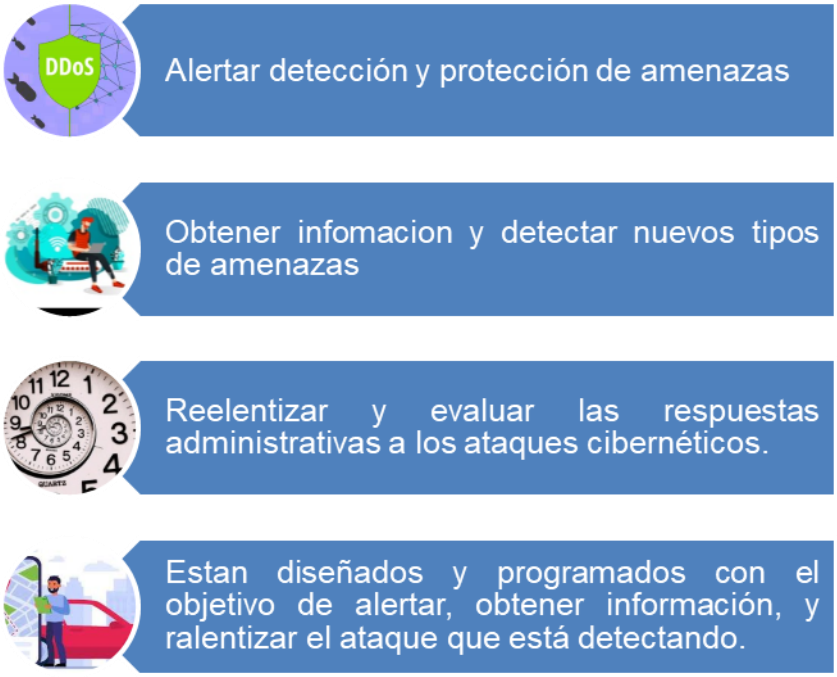


Figura 2 Beneficios del uso de honeypot

Fuente: Elaborado por el autor

3.3.3. FASE DE DISEÑO DE ALTO NIVEL Y DE DETALLE

En esta fase se realizó la topología conveniente para el despliegue de la infraestructura tecnológica del honeypot, con la finalidad de mejorar la seguridad tecnología del centro de datos de la ESPAM y minimizar las vulnerabilidades fortaleciendo el sistema de seguridad perimetral firewall, de modo que los sistemas se ejecuten con normalidad durante el día y la noche, aprovechando el sistema de caza de enemigo para conocer los movimientos de los atacantes.

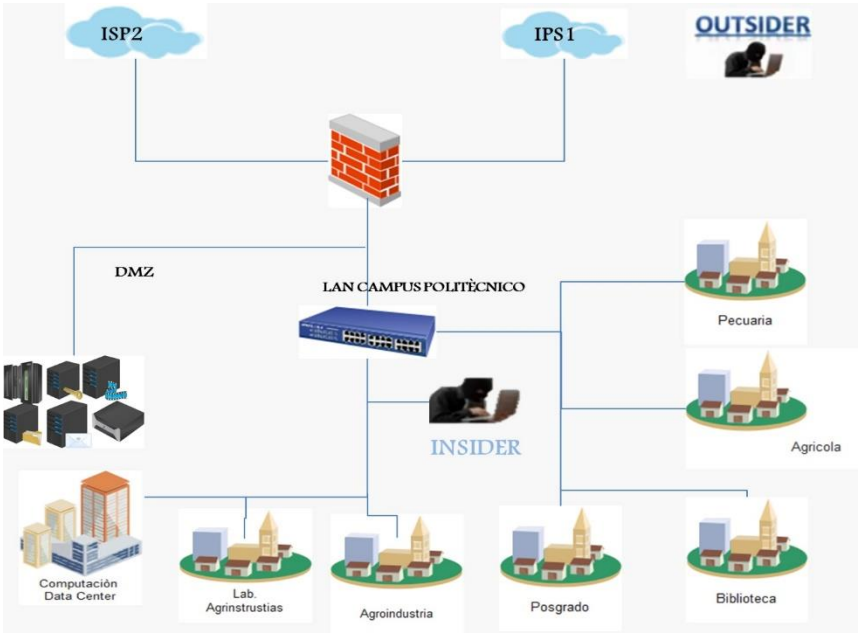


Figura 3 Escenario 1, arquitectura tecnología actual de la ESPAM MFL

Fuente: Moreira, C. (2018), administrador Data Center

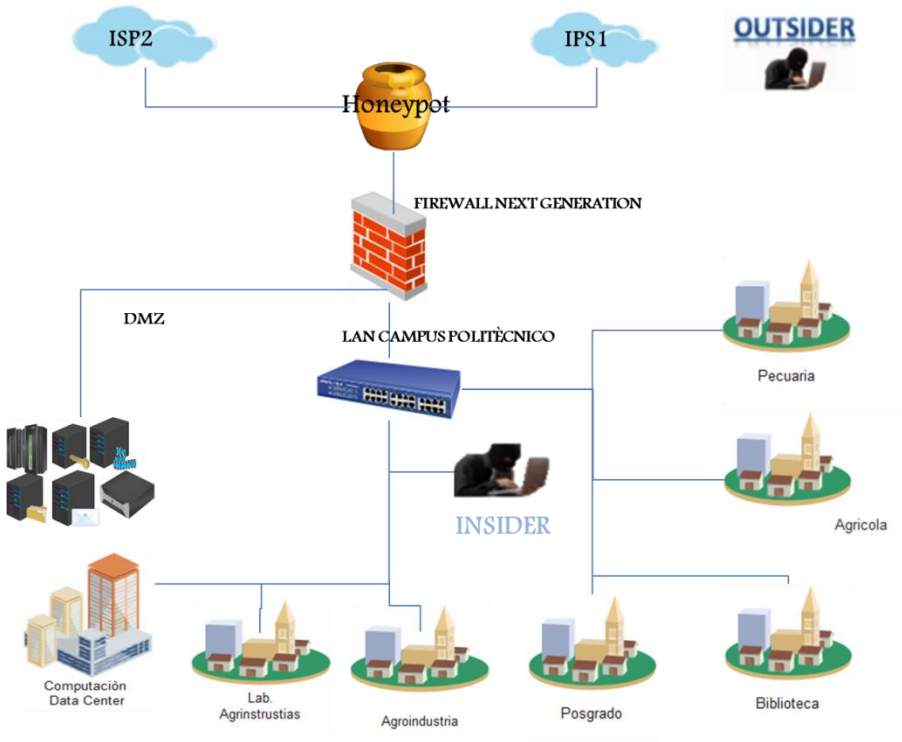


Figura 4. Diagrama de red propuesto para el despliegue del honeypot.

Fuente: Elaborado por el Autor

Análisis de Redes y Comunicación Redundante

La ESPAM MFL cuenta con un data center, pero carece de un sistema de honeypot para la caza de enemigo ciberdelincuentes y la generación de alertas ocasionadas por la intromisión de anomalías y ataques cibernéticos. En la actualidad la institución dispone de 1.620 ordenadores, de las cuales 705 son de uso administrativo y 905 destinadas para el uso académico en prácticas de laboratorios.

Esta tecnología permite a una organización conocer el nivel de seguridad con la cuenta el centro de datos y los sistemas en producción que se alojan en sus servidores con la implementación de este tipo de soluciones, se toman los correctivos necesarios para solventar los inconvenientes de seguridad obtenidos a partir del análisis de los resultados emitido por el sistema de honeypot, clasificando este tipo de sistema de acuerdo a la tabla 1.

Tabla 2. *Clasificación de los honeypot*

Clasificación	
Tipo de Ambiente	Investigación
	Producción
Ubicación en la red	En la DMZ
	Antes del firewall
	Detrás del firewall
	En la red LAN
Nivel de Interacción	Alta
	Baja

Fuente: Elaborada por el Autor.

La universidad dispone de un ancho de banda de 320MB, suministrada por CEDIA, y un enlace inalámbrico vía RADIO como enlace de backup alterno en caso de caída del servicio principal, para uso del centro de datos.

3.3.4. FASE DE IMPLEMENTACIÓN

Para la ejecución, se realizaron pruebas de intrusiones a los diversos servicios de honeypot con herramientas libres como HoneyDrive_3_Royal_Jelly, pentbox, Dionaea, Cowrie, Tpot, concluyendo que el último tiene un gran nivel de ergonomía y mejores características en cuanto a la centralización y gestión de herramientas incluidas dentro del mismo, así como otros componentes de soporte.

Infraestructura necesaria para el despliegue de T-Pot

Tabla 3.*Equipamiento necesario*

Características técnicas de hardware	
RAM	8 GB
CPU	4
HD	40 GB
CD/DVD SATA	1
ADAPTADOR DE RED	1 1 a 10 GB
Conexión a Internet	Disponible buen ancho de banda

Fuente: Elaborada por el autor.

La siguiente fase consistió en la configuración de la máquina virtual y la instalación del sistema operativo T-Pot que contendrán las diferentes aplicaciones de honeypot integradas todo en uno Adbhoney, Ciscoasa, Citrixhoneypot, Conpot, Cowrie, Dicompot, Dionaea.

Ataque a honeypot

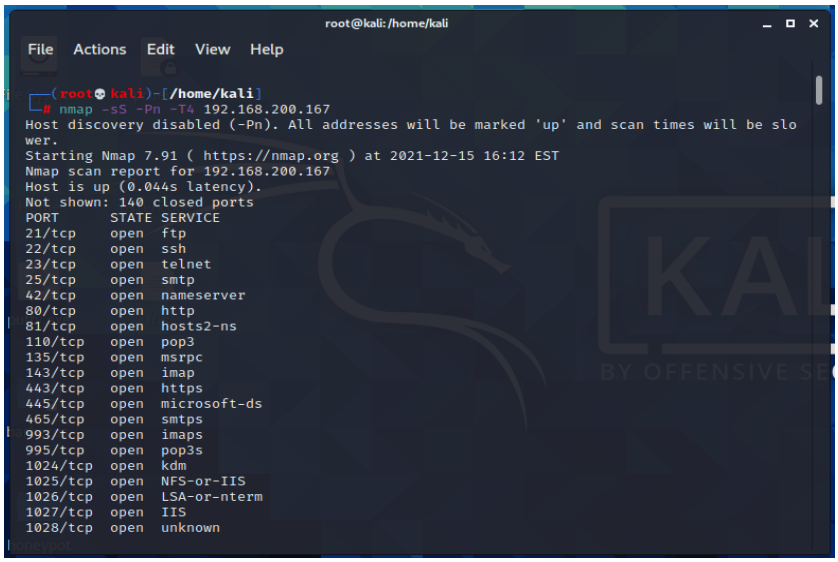


Figura 5. Escaneo de puertos a servidor honeypot con herramienta Kali Linux.

Fuente: Elaborada por el autor

Se procedió a realizar un scaneo de puerto a todo el segmento de red 192.168.200.167, cabe indicar que esa direccion IP pertenece a el sistema honeypot desplegado e instalado como mecanismo de caza de enemigo, obteniendo como resultado puertos abiertos desde el 21 hasta el puerto 65.000. dando como resultado el tipo de servicio abierto tal como se puede apreciar en la Figura 5.

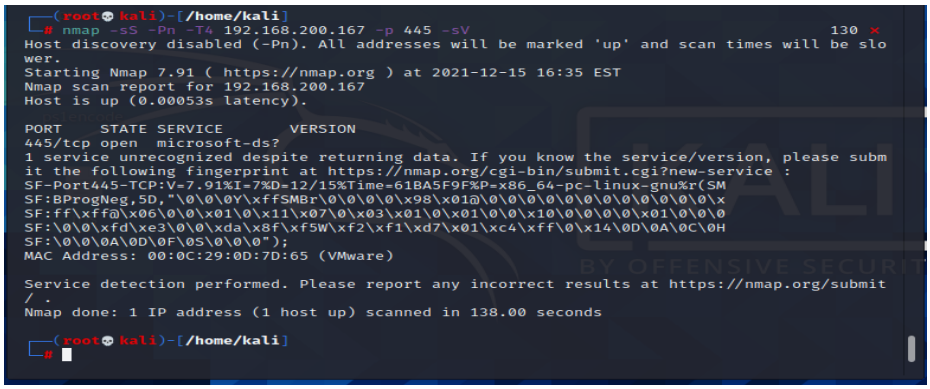


Figura 6. Escaneo de puertos sigiloso a servidor honeypot con herramienta Kali Linux

Fuente: Elaborada por el autor

Se realiza un escaneo sigiloso para conocer la versión de la aplicación y con esto tener mejor informacion para realizar el ataque cibernetico, obteniendo el resultado que muestra en la Figura 6.

nmap -sS -Pn -T4 192.168.200.167 -p 445 –sV

vulnerado el sistema por ssh

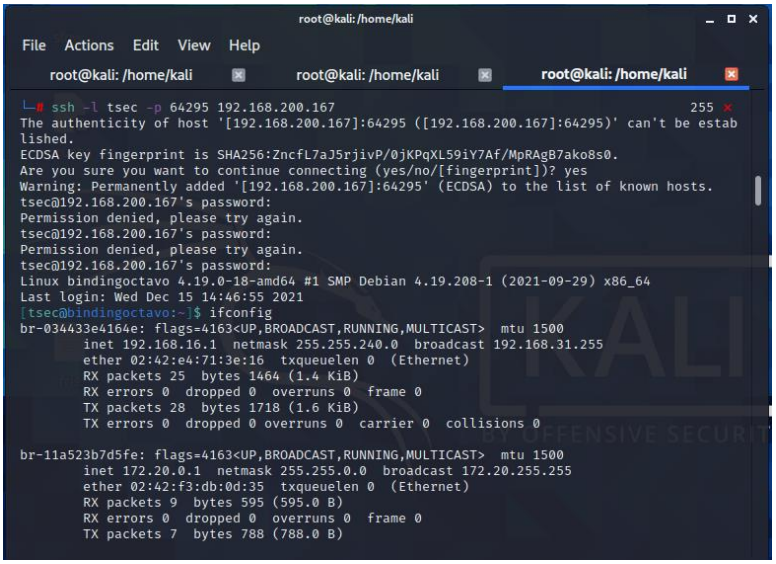


Figura 7. Equipo honeypot vulnerado con herramienta Kali Linux puerto 22 ssh.

Fuente: Elaborada por el autor.

Se realizó el ataque cibernetico hacia el puerto 22, como se indica en la Figura 7, que corresponde al servicio de ssh del sistema honeypot T-POT donde una vez dentro del sistema el atacante se encontro en una jaula practicamente, no pudo realizar ningún movimiento lateral ni realizar procesos de postexplotación lo que implica que el atacante termine por abandonar la mision.

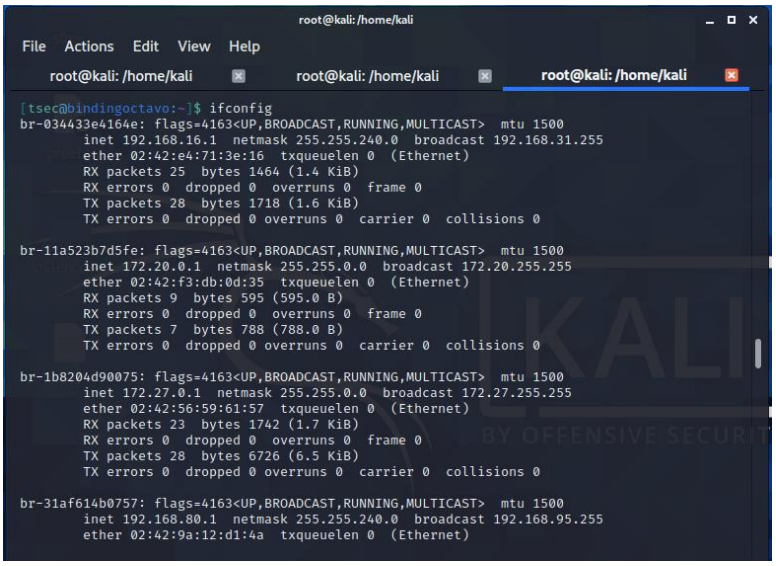


Figura 8. Proceso de revisión de interfaces de red equipo vulnerado

Fuente: Elaborada por el autor

Una vez dentro del sistema el atacante lo primero que realizó fue una verificación de los segmentos de red y las consulta de interfaces de red, mediante el comando ifconfig, como se aprecia en la Figura 8, donde se obtuvo como resultado, todas las tarjetas de interfaz de red simuladas por el sistema honeypot, comprobando al atacante que esto es una anomalía dando indicios a ganar privilegios de administración.

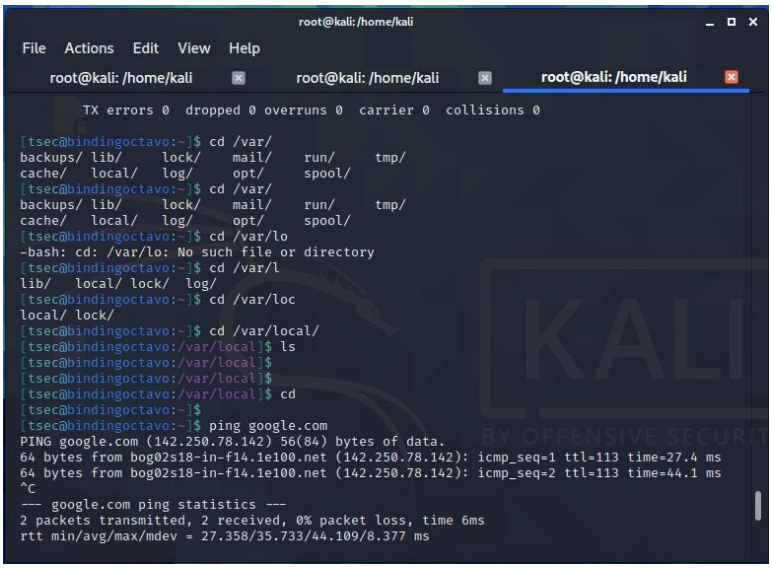


Figura 9. Proceso de escala de privilegio equipo honeypot vulnerado

Fuente: Elaborada por el autor

La gráfica muestra los diferentes comandos y rutas por el cual el atacante empieza a moverse en busca de obtener alguna información, con la finalidad de realizar procesos de escala de privilegios dentro del sistema, como se puede visualizar en la Figura 9.

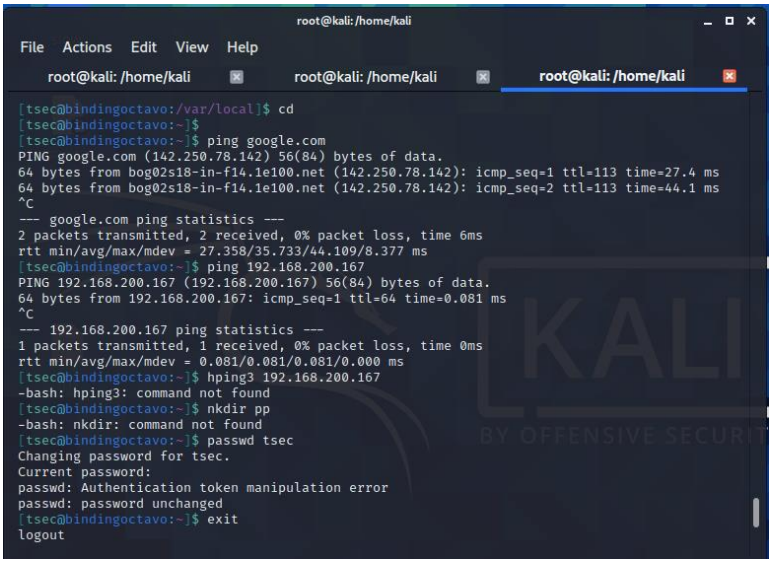


Figura 10. Proceso de enjaulamiento y caza de enemigo, atacante abandona la misión.

Fuente: Elaborada por el autor.

La Figura 10 muestra que el atacante realiza el ingreso y ejecucion de varios comando, trata de comprobar que tenga salida a internet y el resultado es satisfactorio con la unica anomalia que no puede descargar absolutamente nada, debido a que no tiene privilegios y se encuentra dentro de un sistema de caza de enemigos.

Sistema de honeypot detectando los taques

Se ingresa a la herramienta honeypot mediante la interfaz web,como se observa en la Figura 11, luego a la bateria de honeypot y se escoge la opcion de elastic, dentro de la herramienta de visualizacion de informaición como es el dashboard, se identifican los diferentes ataques cibernéticos detectados, la gráfica estadística y la región de donde proviene el ataque.

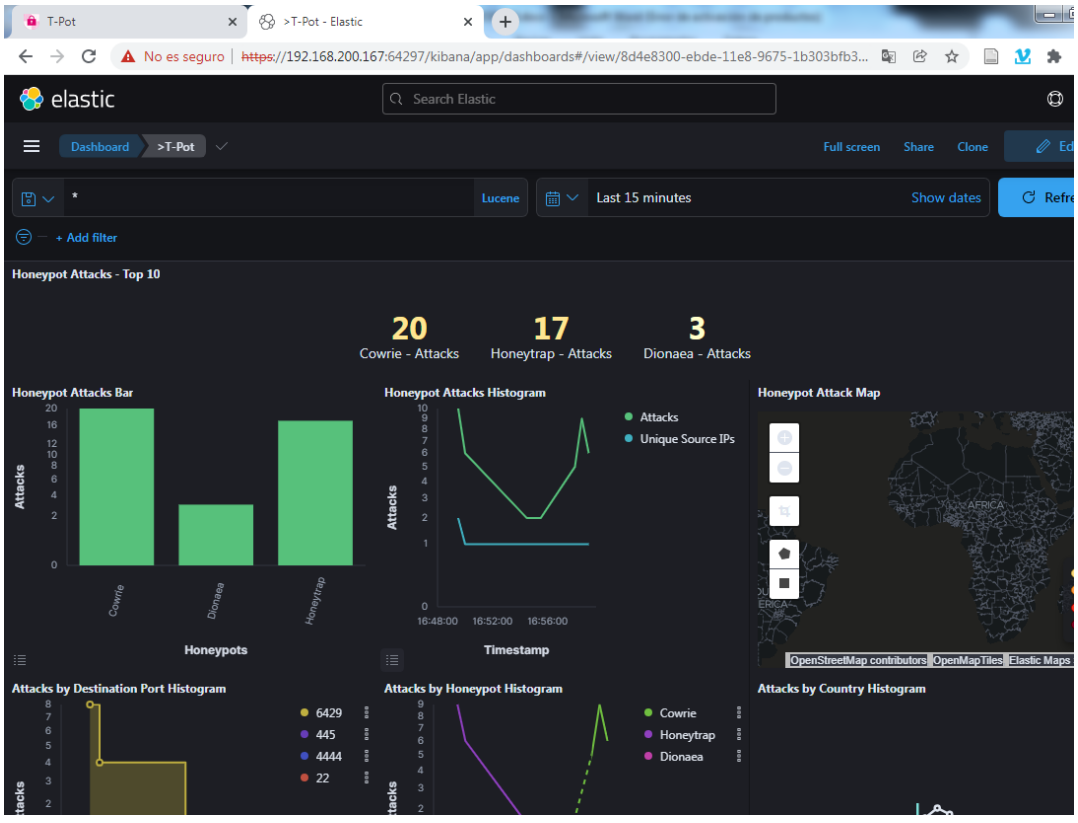


Figura 11. Ataques detectados por el honeypot y visualizado en elástica T-pot.

Fuente: Elaborada por el autor.

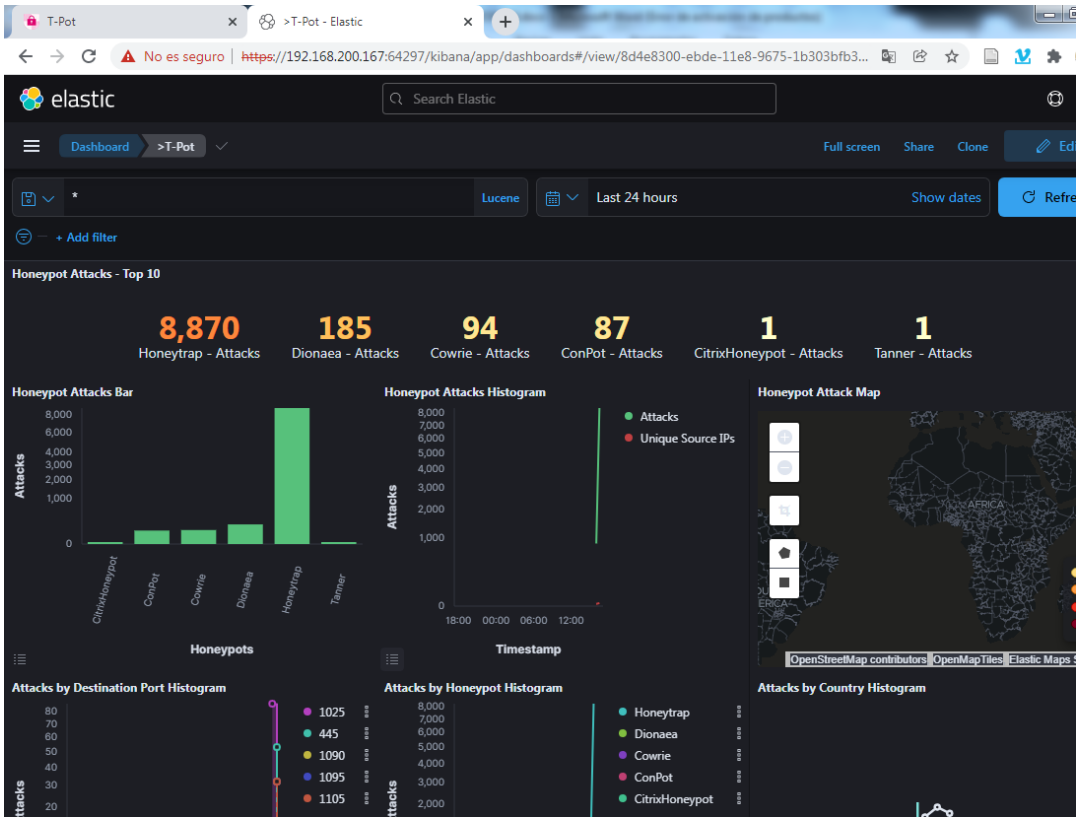


Figura 12. Ataques detectados por la batería de honeypot Honeytrap, Dionea, Cowrie, Conpot, Citrixhoneypot, Tanner.

Fuente: Elaborada por el autor.

Dentro la solución de T-POT existe una bateria de honeypot para diferentes infraestructuras como para diferentes arquitecturas, los ataques generados anteriormente fueron detectados por Honeytrap, Dionea, Cowrie, ConPot, CitrixHoneypot, Tanner, herramientas que se encuntran integradas dentro de honeypot T-pot, las mismas que tienen su impacto en diferentes tecnologias con la finalidad de mitigar y cazar los enemigos cibernetico, así se pueder ver en la Figura 12.

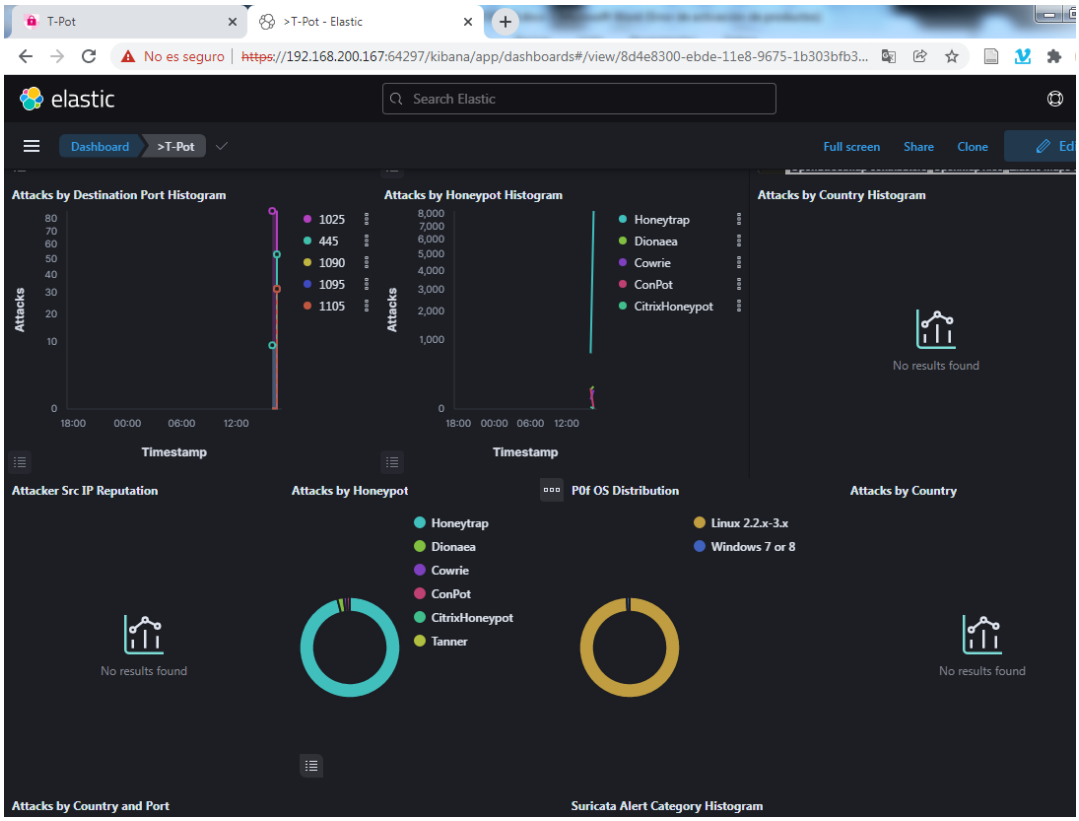


Figura 13. Ataques detectados por la batería de honeypot Honeytrap, Dionea, Cowrie, Conpot, Citrixhoneypot, Tanner reportados mediante dashboard.

Fuente: Elaborada por el autor.

La siguiente grafica muestra estadisticas fundamentales de los ataques identificados en cada una de sus tecnologias, estos resultados son fundamental para la toma de desiciones y asi fortalecer la seguridad centralizada.

Sistema honeypot registra todos los comando utilizados por el atacante cibernetico.

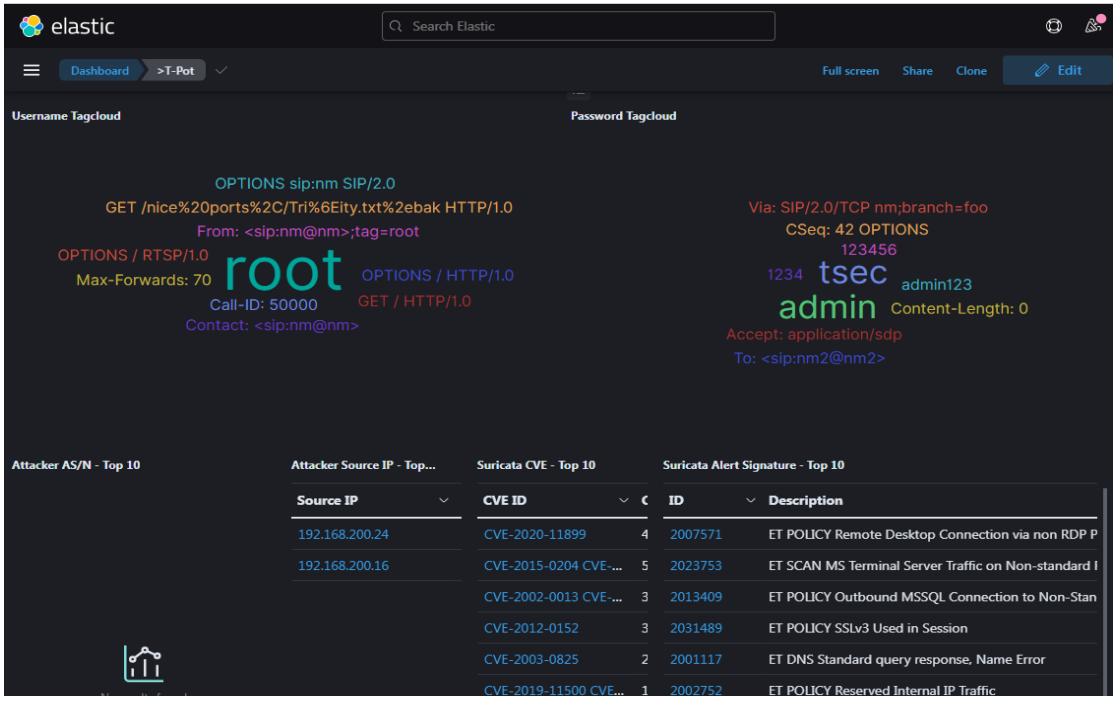


Figura 14. Comandos ingresados por el atacante, procesos de escala de privilegio información obtenida para fortalecer el firewall.

Fuente: Elaborada por el autor.

La Figura 14 muestra todos los comando usuario y claves que estuvo probando el atacante, asi como las diferentes rutas por la cuales quizo realizar procesos de escala de privilegios,estos resultados son de mucha importancia porque se empieza a ver como piensa un ciberdelincuente.

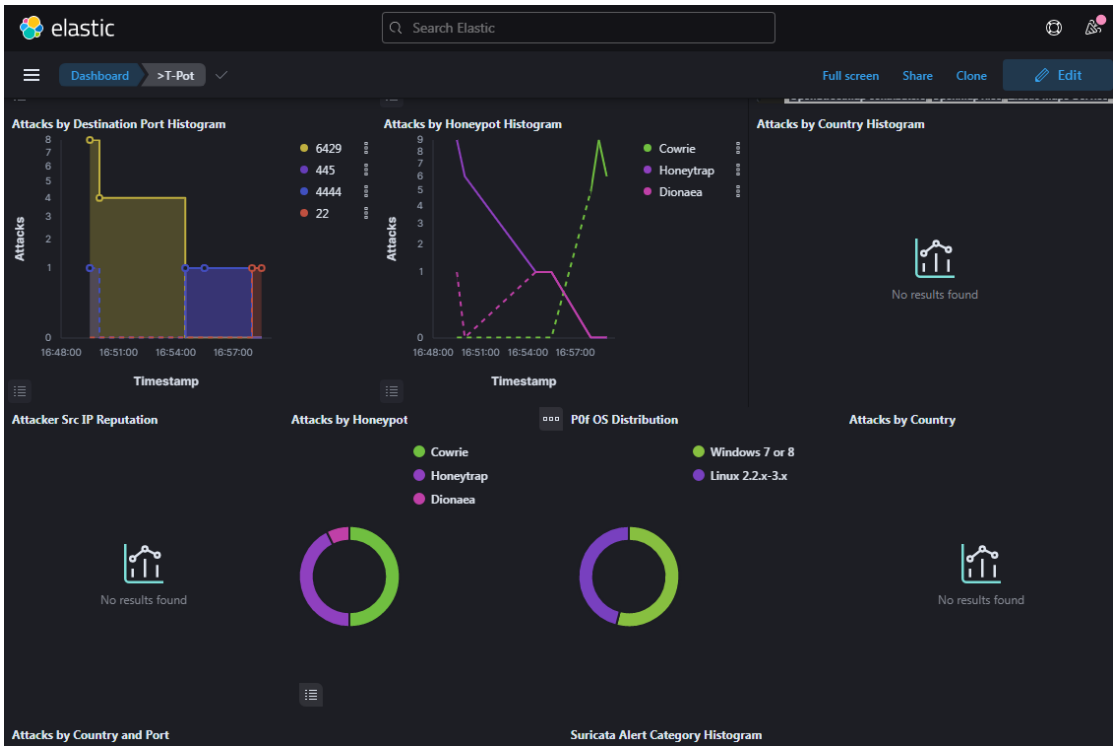


Figura 15. Resultados obtenidos mediante herramienta de visualización de información sobre los ataques detectados post el honeypot.

Fuente: Elaborada por el autor.

Los resulatdos visualizados en la Figura 15, muestran las anomalías detectadas por el sistemas honeypot, se obtienen mediante diferentes gráficos estadísticos como histogramas, estos ataques son clasificados por la tecnología y solucion integrada en T-pot, identificando el sistema operativo atacado y el sistema operativo del atacante.

La Figura 16 muestra el usuario y claves que estuvo probando el atacante, la ip origen y la ip destino a donde se estaba dirigiendo el ataque cibernetico, el identificador del procesos del ataque como la respectiva descripcion de la brecha de inseguridad.

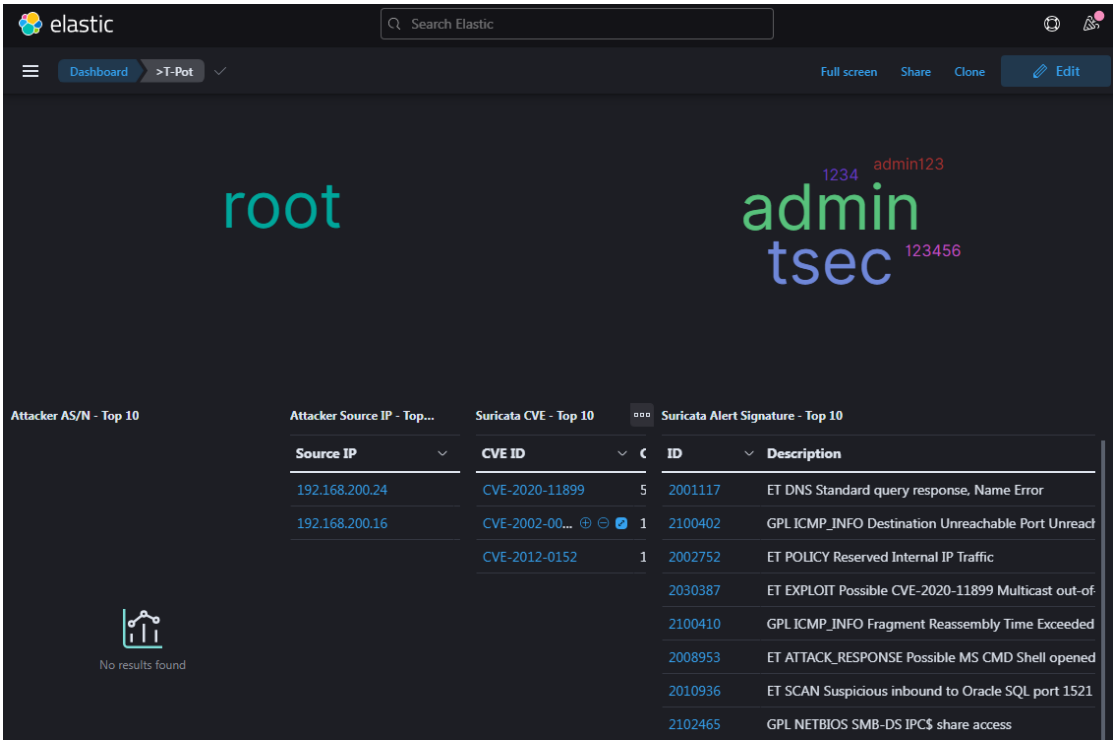


Figura 16. Proceso detectado por el honeypot sobre el usuario y clave que ingreso como método de ataque. Identificación de direccionamiento ip maquinas víctimas, identificador del proceso y la descripción de la anomalía.

Fuente: Elaborada por el autor.

La figura 17 muestra el sistema de deteccion de intruso Suricata, el mismo que muestra 391 eventos, estos pueden ser clasificados como positivos o falsos positivos, en este caso son eventos anómalos que pueden afectar la infraestructura tecnologica.

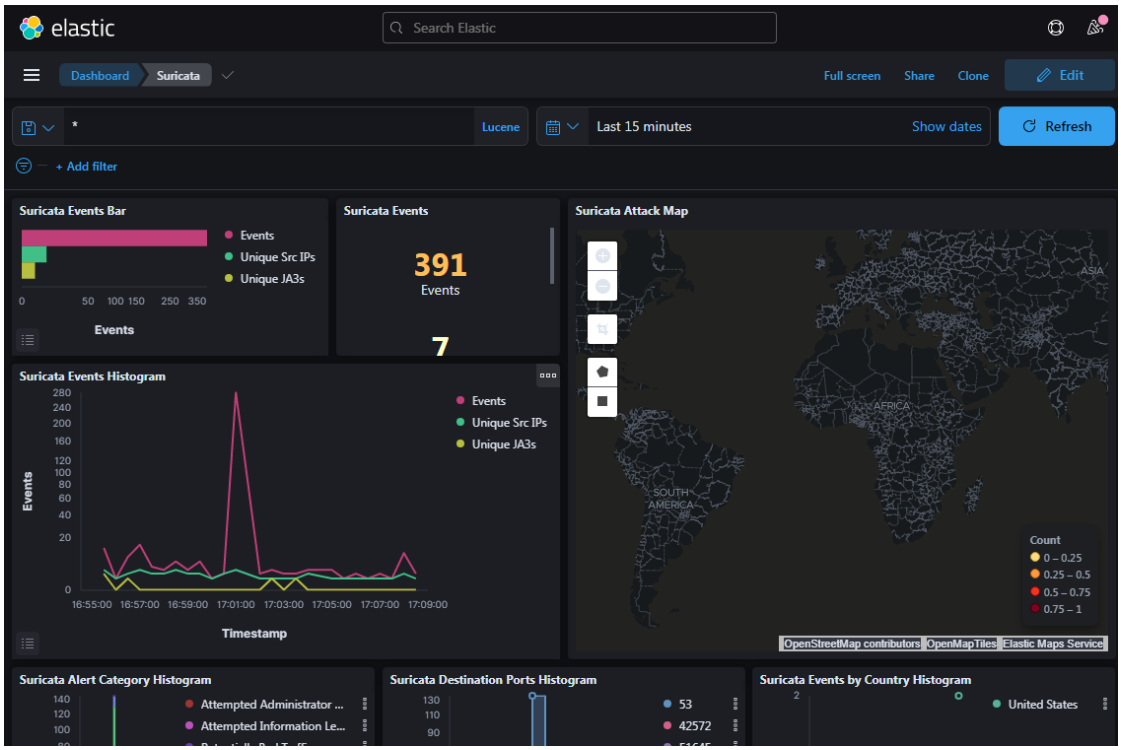


Figura 17. Anomalías detectadas por sistema IDS suricata.

Fuente: Elaborada por el autor.

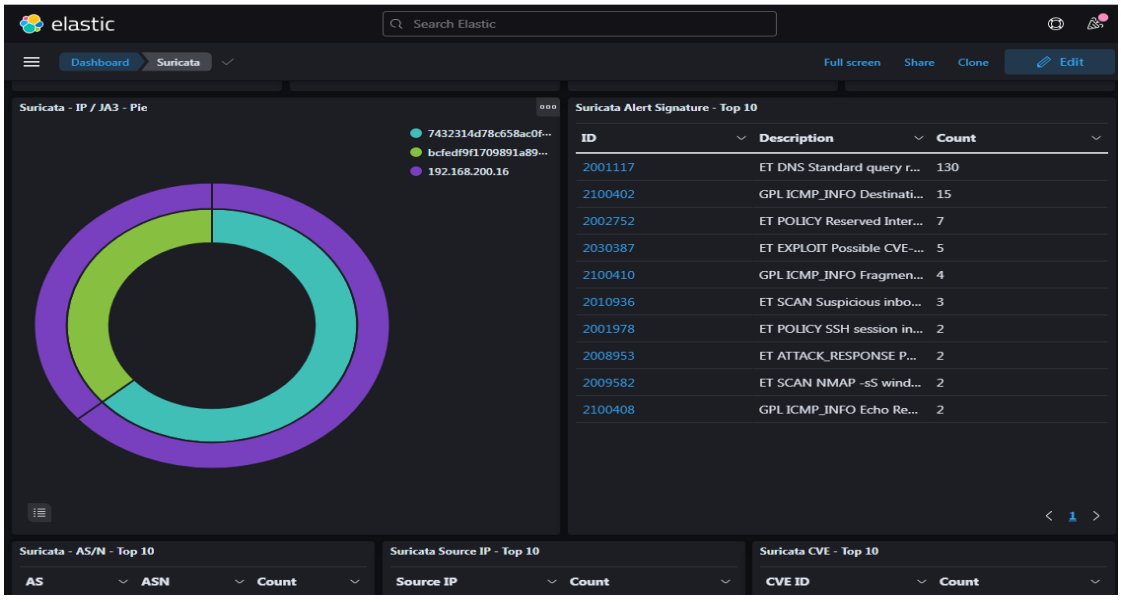


Figura 18. Anomalías detectadas por sistema de detección de intrusos IDS suricata.

Fuente: Elaborada por el autor

Vulneraribilidades y direcciones ip origen y destino

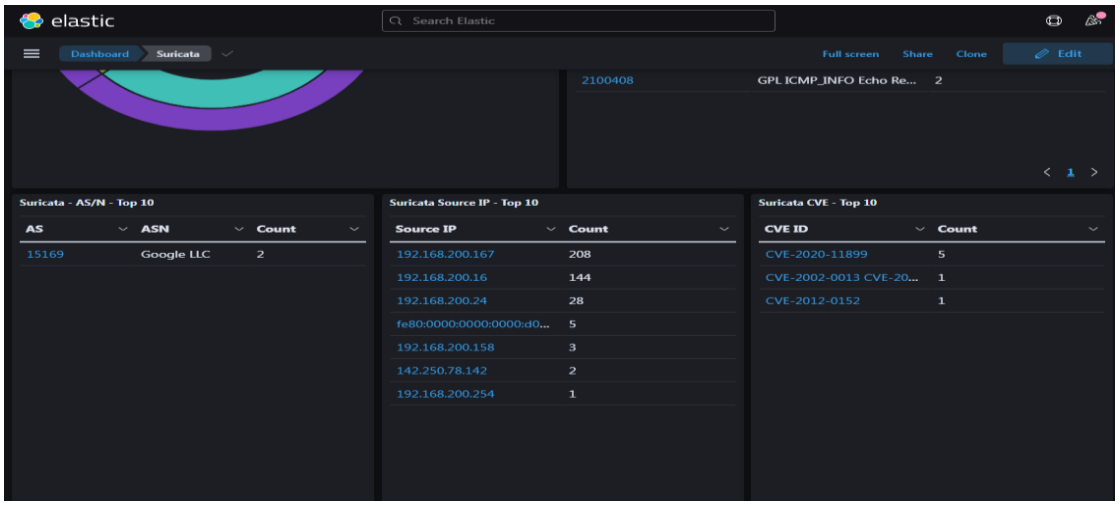


Figura 19. Reporte de direcciones IPs con servicios de inseguridad detectadas por sistema IDS suricata.

Fuente: Elaborada por el autor.

El servidor de balanceo de carga nginx detento

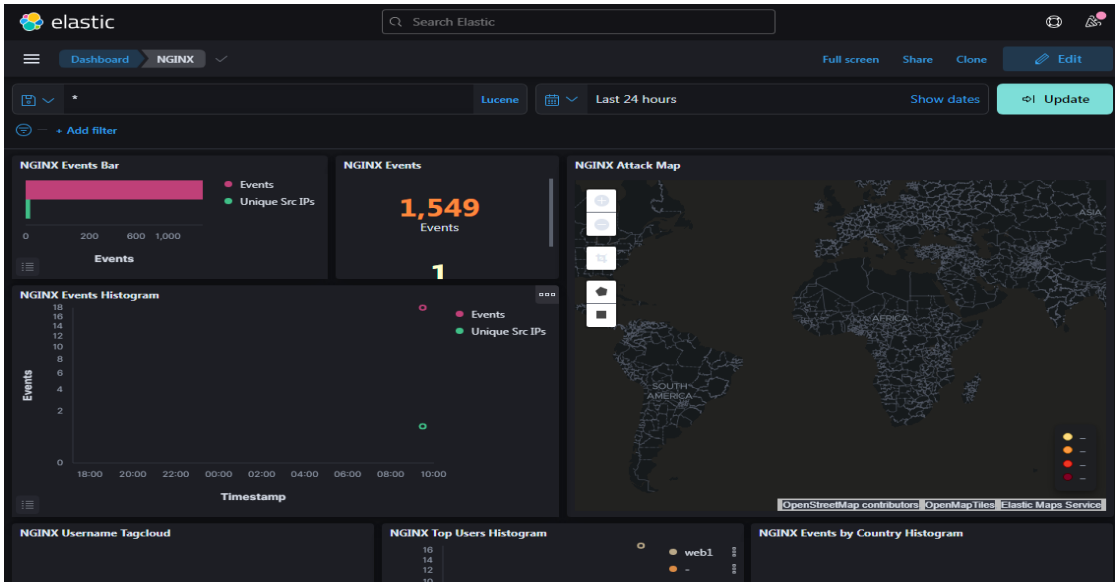
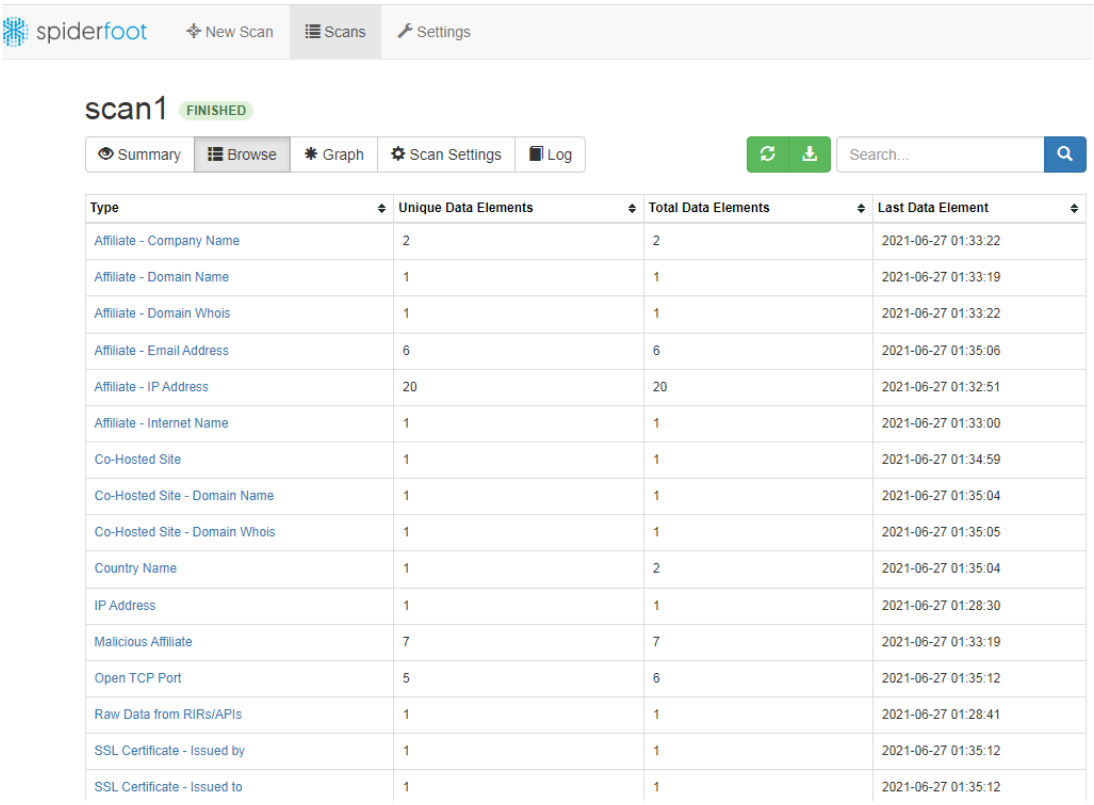


Figura 20. Reporte de anomalías detectadas a el sistema de balanceo de carga de la ESPAM MFL detectadas por sistema IDS suricata.

Fuente: Elaborada por el autor.

Por el usuario de monitoreo de la solucion

Honeytrap



Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Company Name	2	2	2021-06-27 01:33:22
Affiliate - Domain Name	1	1	2021-06-27 01:33:19
Affiliate - Domain Whois	1	1	2021-06-27 01:33:22
Affiliate - Email Address	6	6	2021-06-27 01:35:06
Affiliate - IP Address	20	20	2021-06-27 01:32:51
Affiliate - Internet Name	1	1	2021-06-27 01:33:00
Co-Hosted Site	1	1	2021-06-27 01:34:59
Co-Hosted Site - Domain Name	1	1	2021-06-27 01:35:04
Co-Hosted Site - Domain Whois	1	1	2021-06-27 01:35:05
Country Name	1	2	2021-06-27 01:35:04
IP Address	1	1	2021-06-27 01:28:30
Malicious Affiliate	7	7	2021-06-27 01:33:19
Open TCP Port	5	6	2021-06-27 01:35:12
Raw Data from RIRs/APIs	1	1	2021-06-27 01:28:41
SSL Certificate - Issued by	1	1	2021-06-27 01:35:12
SSL Certificate - Issued to	1	1	2021-06-27 01:35:12

Figura 21. descubrimiento de activos en la red.

Fuente: elaborada por el autor.

Spiderfoot, permite realizar un descubrimiento de activos en la red, para inteligencia de amenazas, evaluación de seguridad y monitoreo de superficie de ataques, para este caso se lo utilizó para escananear todas las aplicaciones y sistemas servidores dentro del DMZ del centro de datos de la ESPAM MFL, con los datos obtenidos se logra fortalecer la seguridad centralizada, tal como se observa en la Figura 21.

Registro de los movimientos del atacante

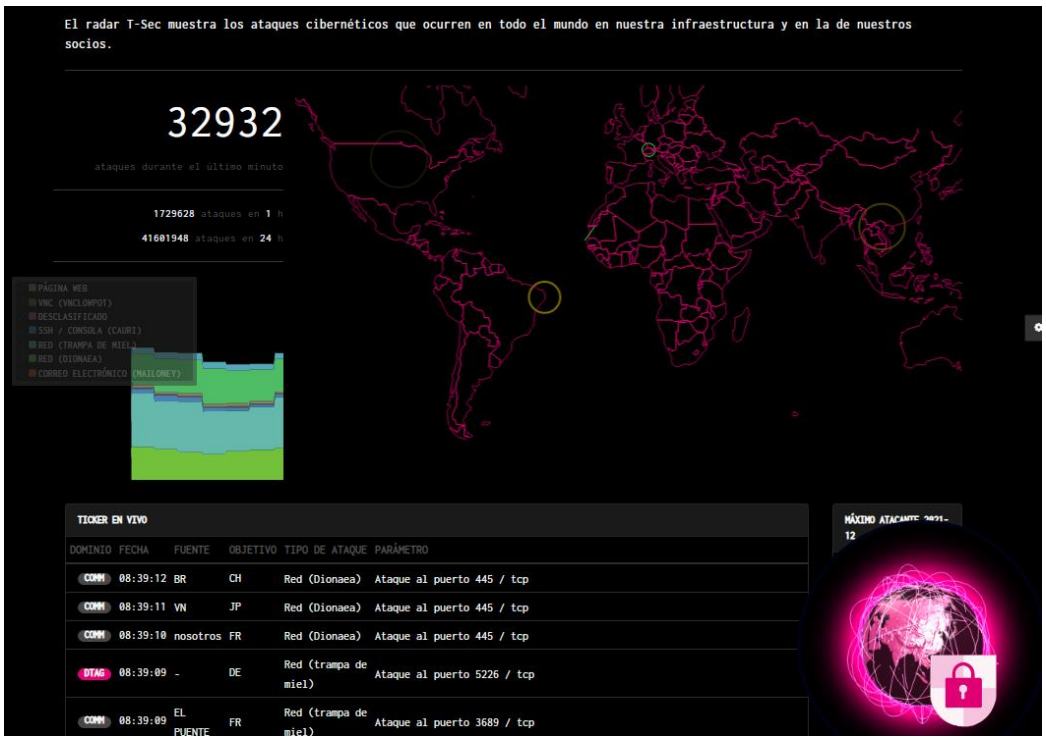


Figura 22. registro de movimientos del atacante

Fuente: elaborada por el autor

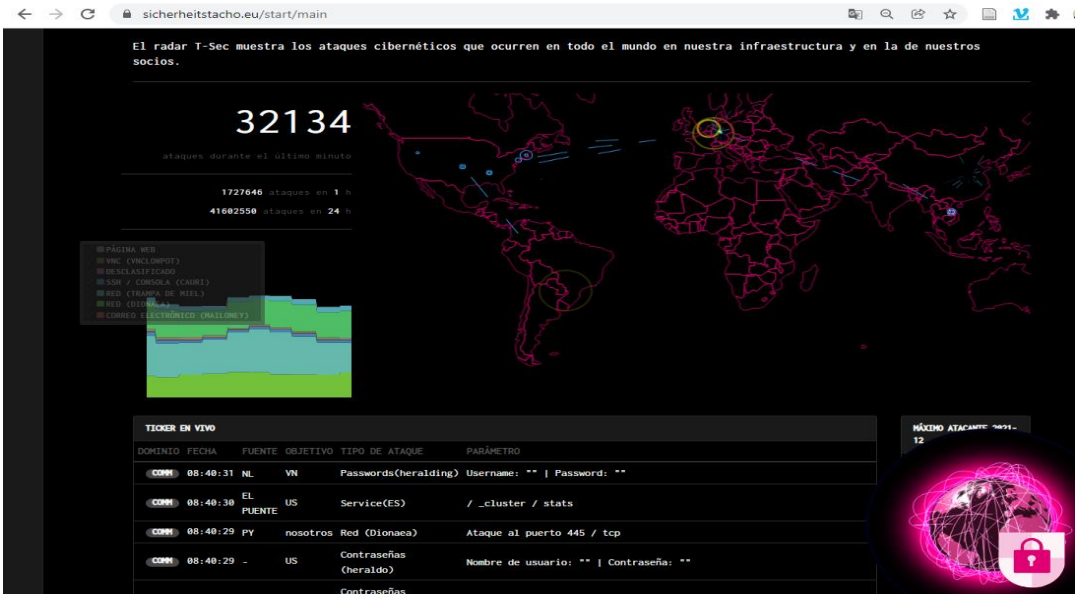


Figura 23. registro de movimientos del atacante

Fuente: elaborada por el autor

El ataque se realizó en un ambiente controlado y el vector de ataque que se utilizó es de tipo denegación de servicio DDOS mediante hping3, se enviaron paquetes manipulados, controlando el tamaño, la cantidad y la fragmentación de los paquetes para sobrecargar el objetivo y evitar o atacar los firewalls. Cabe indicar que dentro del ataque se utiliza una bandera de tipo --flood --rand-source el mismo que permite manipular las direcciones ip haciendo creer que los ataque proviene de diferentes regiones, continentes o países y ocultar la verdadera dirección ip del atacante, asi se puede observar en las figuras 22 y 23.

La tabla 4 muestra el ataque generado, con las banderas necesarias para generar la denegación de servicio.

Tabla 4. *Ataques y comandos generados*

Herramienta	**Ataque generado**	**Indicadores**
Kali Linux 2020.04	sudo hping3 -c 100000 -S -w 256 -p 8000 -d 65000 --flood --rand-source 192.168.200.155	sudo: otorga los privilegios necesarios para ejecutar hping3 hping3: llama a el programa hping3 -c: especifica la cantidad de paquetes a enviar -S: Especifica el paquete SYN -w: Especifica la longitud de la carga util del paquete -p: especifica el puerto por el cual se va a realizar el ataque -d: Establece el tamaño del paquetes

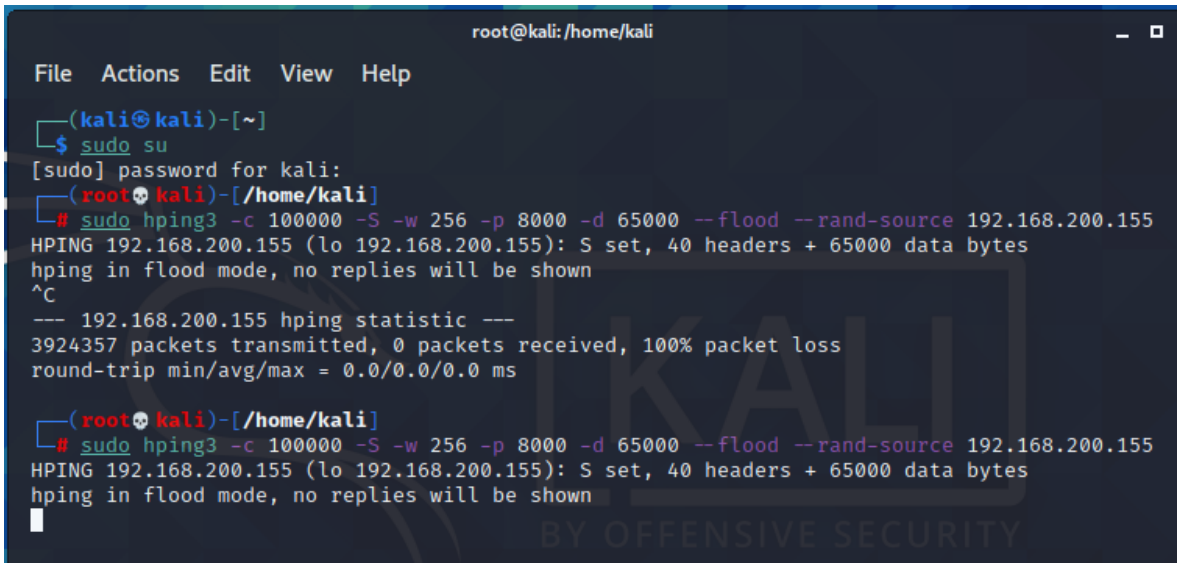


Figura 24. Ataques cibernéticos mediante herramienta Kali Linux

Fuente: Elaborada por el autor

Se utilizó un vector de ataque muy completo, desde el punto de vista de un ambiente controlado, lo cual permite que la ip del atacante sea randomica, esta es una tecnica de desviacion de identidad y geolocalizacion, el parametro que identifa esta accion es src_ip, ver Figura 24.

Implementación de IDS/IPS

Para la implementación del firewall Pfsense y la integración de IDS/IPS Suricata, con las respectivas reglas, lo que van a permitir la prevención y detección de intrusos en un sistema convergente, así mismo una herramienta de monitoreo de red con gestión y administración vía web llamada Ntop.

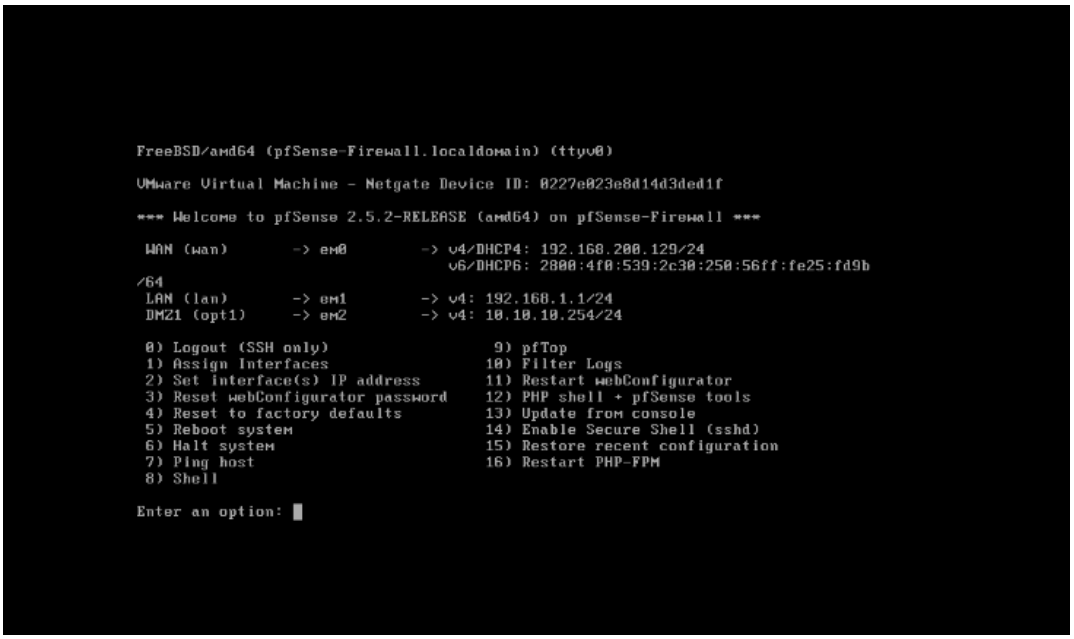


Figura 25. Instalación de Firewal Pfsense.

Fuente: Elaborada por el autor.

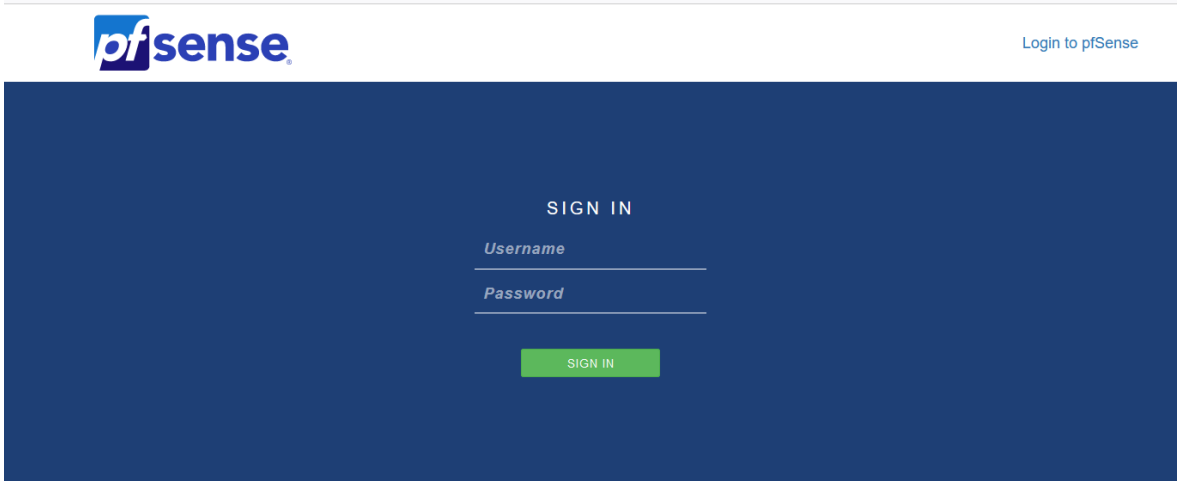


Figura 26. login de Pfsense.

En la Figura 26 se muestra la Instalación, configuración y asignación de interfaces de red para el firewall Pfsense, el cual tendrá 3 interfaces de red como son: WAN, LAN y DMZ.Ingreso al dashboard del Pfsense.

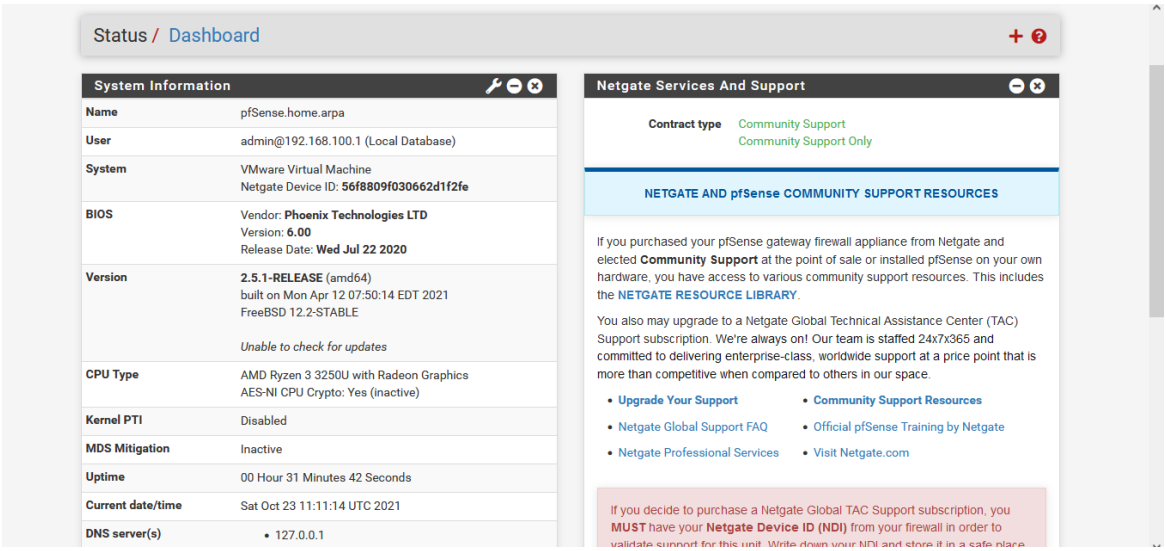


Figura 27. Dashboard de Pfsense

Fuente: Elaborada por el autor

Gestión y administración del firewall, ver Figura 27.

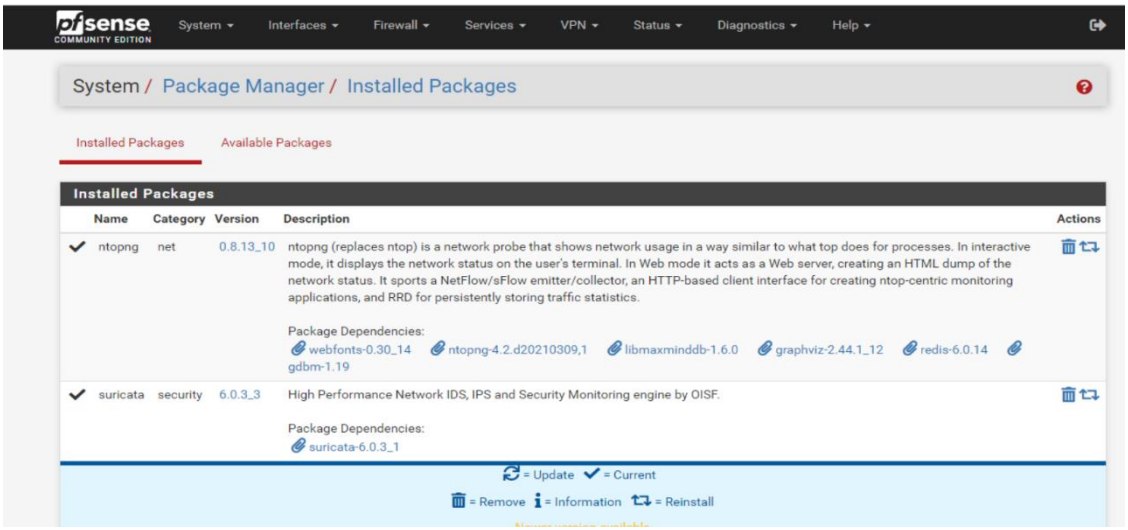


Figura 28. Instalación de IDS/IPS Suricata.

Fuente: Elaborada por el autor.

En la Figura 28, se detalla la instalación de IDS/IPS suricata y sistema de monitoreo de red Ntop.

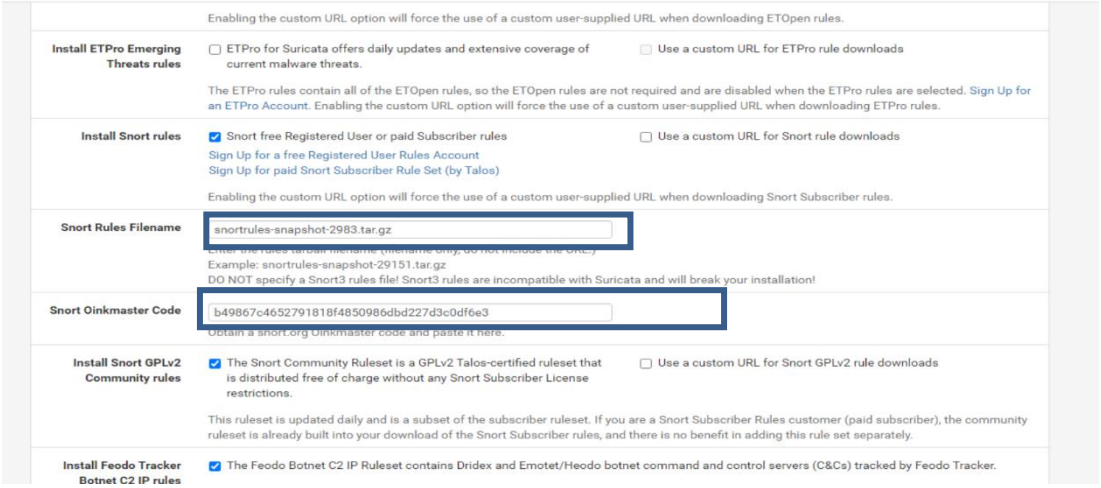


Figura 29. Configuración de reglas.

Fuente: Elaborada por el autor.

Configuración de reglas mediante Snort, utilizando el paquete de reglas y oinkcode y exportación y selección de reglas tanto en la interfaz WAN y LAN, tal como se detalla en la Figura 29.

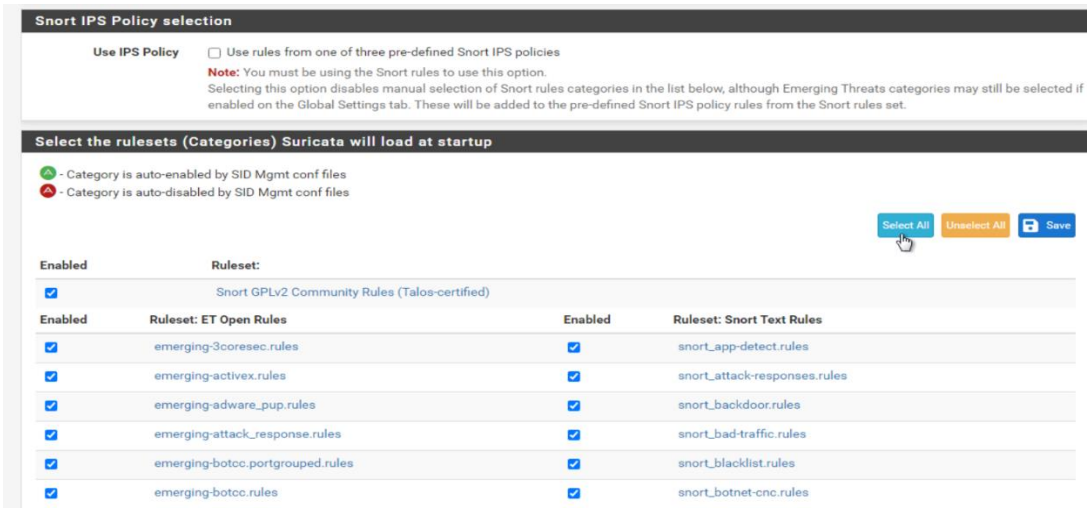


Figura 30. Agregando paquete de reglas.

Fuente: Elaborada por el autor.

En la Figura 30 se agregan los paquetes de las reglas del firewall.

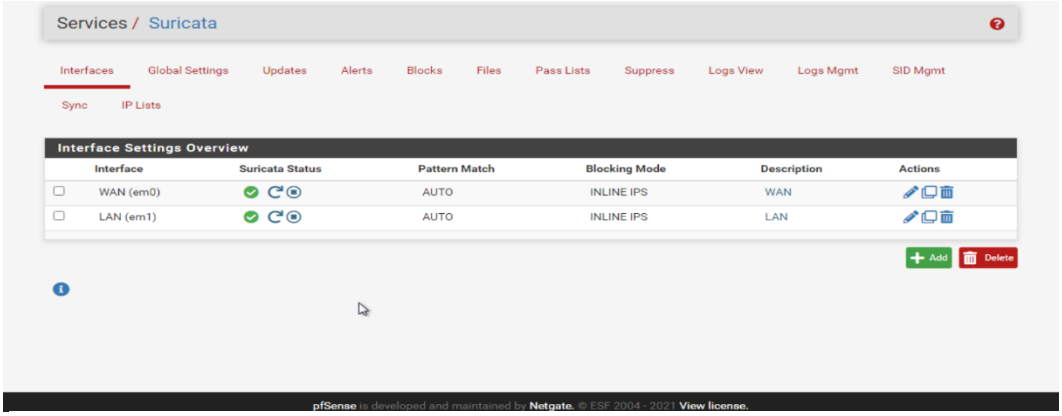


Figura 31. Puesta en marcha de interfaces.

Fuente: Elaborada por el autor.

En la Figura 31, se muestra la puesta en marcha de las interfaces configuradas del IDS/IPS.

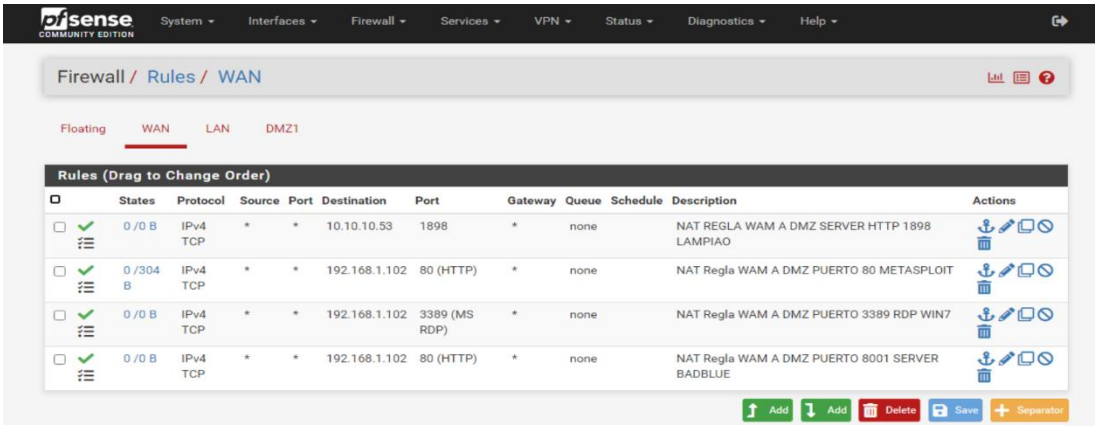


Figura 32. Configuración de reglas para perpetrar intrusiones.

Fuente: Elaborada por el autor.

En la Figura 32 se configura las reglas para mitigar intrusiones de las herramientas badblue, Lampião y mestasploit.

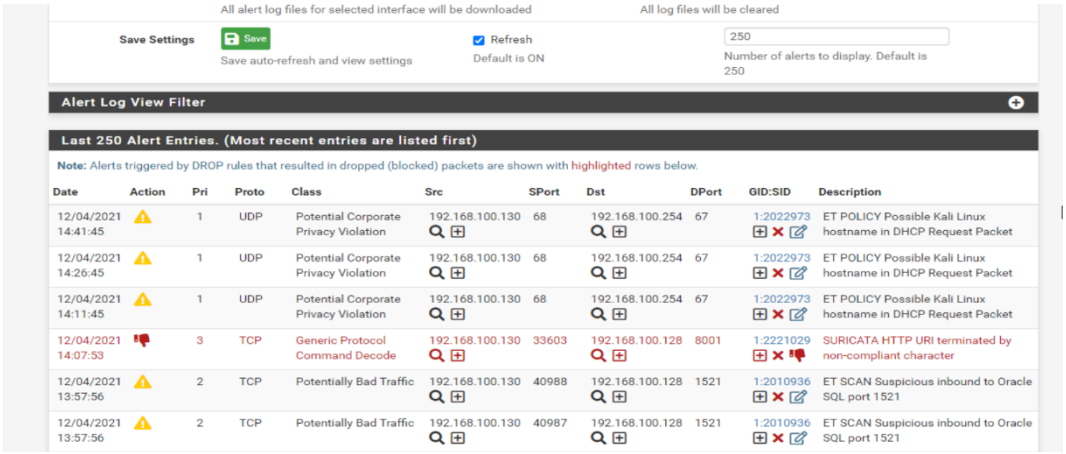


Figura 33. Reportes del IDS/IPS

Fuente: Elaborada por el autor

Reporte de IDS/IPS Suricata a través de las alertas que se visualizan en la Figura 33, con respecto a la configuración de reglas establecidas para repeler un ciberataque en ambiente controlado.

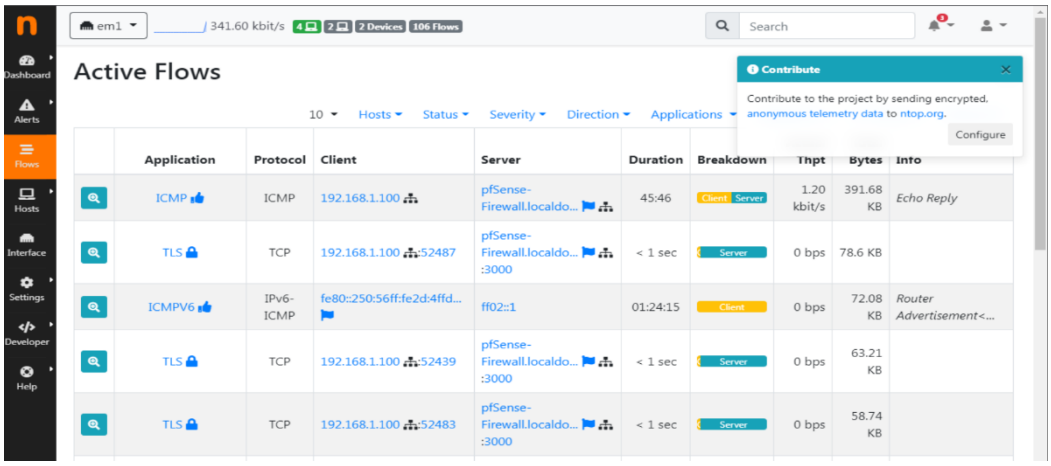


Figura 34. Gestión y Administración de instrusiones con Ntop

Fuente: Elaborada por el autor

En la Figura 34 se observa el panel de Gestión y administración de intrusiones en red mediante la herramienta Ntop, control de flujos, alertas, etc.

3.3.5. FASE DE TEST UNITARIO, DE INTEGRACIÓN Y OPERACIONAL

Conforme a la información generada en la fase de diseño de caso de estudio aplicando mecanismos de ciberseguridad basados en sistemas honeypots, se procedió a realizar la instalación y configuración de las herramientas, en un entorno virtual, a través de la plataforma de virtualización VMWare Workstation. Cabe señalar que el host anfitrión de este entorno virtual, se ubicó en un segmento de red aislado a la red corporativa de la ESPAM, MFL, de tal manera, que se logró integrar los nuevos componentes, sin interrumpir la red existente o crear puntos de vulnerabilidad.

En primer lugar, se desplegó un escenario de evaluación, para lo cual se instaló el firewall pfSense y se configuró con 3 interfaces de red: WAN, LAN1 y DMZ1. Se procedió a configurar los parámetros del firewall accediendo desde un navegador web a la IP asignada al puerto LAN1, donde se establecieron reglas de tráfico de red de todas las interfaces del firewall pfSense; se configuró la primera interfaz como WAN; la segunda interfaz denominada DMZ1 fue configurada como DMZ. Además, se habilitó en el firewall pfSense el paquete IDS/IPS Suricata, se desplego la herramienta de monitorización de red Ntop para evaluar el volumen de paquetes entrantes y salientes, luego, se procedió a levantar en la LAN1, las herramientas de Pentesting Metasploit Y Kali Linux, los sistemas operativos de usuario final Lampiao, Windows 7.

Posteriormente, en un segundo periodo de evaluación, se procedió a desplegar el siguiente escenario, en el que se dio de alta en la DMZ (DMZ1), la solución Honeypot T-Pot, cuyo objetivo es atraer los ataques de los piratas informáticos mediante la visualización de servicios y puertos abiertos que son potencialmente vulnerables, desviando sus actividades del tráfico legítimo para poder monitorear y analizar los métodos y tendencias de ataque actuales.

Por otra parte, cabe resaltar que, ambos escenarios, se encontraban expuestos a ciberataques desde el exterior; en este sentido, como parte del experimento, el investigador generó ataques de fuerza bruta (Brute Force Attack) y de denegación de servicio (Denial of Service Attack - DoS) desde un equipo Kali Linux localizado externamente (WAN).

Finalmente, es preciso señalar que, para realizar las mediciones de los escenarios de evaluación, se procedió con la monitorización de los componentes de la red mediante Ntop de los escenarios de evaluación a través de las herramientas instaladas en el firewall pfSense y herramienta de hacking y posthacking como Kali Linux. Una vez que se obtuvieron los datos del tráfico de las comunicaciones de los dos escenarios de evaluación, se procedió a el análisis correspondiente.

El test unitario obtenidos durante la fase de implementación del entorno de pruebas se llevó a cabo, lo que nos permitió negar o aceptar la hipótesis propuesta y así poder concluir sobre lo observado en el caso de estudio. Para esta fase, se consideró las métricas señaladas en la Tabla 6; los valores de los parámetros de ancho de banda, paquetes recibidos y enviados, se obtuvieron mediante el uso de las herramientas Bandwidth y Ntopng, incluidos en el software pfSense. Además, se monitorizó el número de eventos sospechosos con el paquete IDS/IPS Suricata de pfSense y el número de vulnerabilidades detectadas con la herramienta Nessus incluida en Kali Linux LAN1.

3.3.6. INSTRUMENTOS

Se utilizó el siguiente instrumento de recolección de información:

- Entrevistas

3.3.7. TÉCNICAS

- Observación

3.3.8. FUENTES DE INFORMACIÓN

Primarias

Las principales fuentes que serán los informantes a los cuales se les va aplicar una entrevista, director de Tecnología, Administrador del centro de datos, personal técnico de tecnología de la ESPAM MFL.

Secundaria

- Investigaciones sobre la misma temática y revistas electrónicas.
- Artículos científicos de alto impacto.
- Libros especializados electrónicos.

3.3.9. RECURSOS

Recursos de oficina.

- Materiales de Oficina, Computadores.
- Google drive.
- Internet.

Recursos técnicos.

Herramientas de simulación de ciberseguridad ofensiva y defensiva.

3.3.10. PLANTEAMIENTO DE LA HIPÓTESIS

La implementación de un sistema Honeypot permitirá mejorar la seguridad del centro de datos de la ESPAM MFL.

3.3.11. DETERMINACIÓN DE LAS VARIABLES

Variable Dependiente

Sistema de ciberseguridad.

Variable Independiente

Prevención de ataques informáticos aplicando seguridad basada en componentes de Honeypot.

Operacionalización de las variables

Variables	Definición Conceptual	Dimensiones	Indicadores
Sistema de ciberseguridad	Los sistemas de ciberseguridad se utilizan para la protección de informacion de las organizaciones	Disponibilidad	Sistema disponible sin sufrir afectación a los servicios
			Información disponible a personal
		Integridad	Información se mantenga inalterada ante accidentes o intentos

		maliciosos.
		Prevenir modificaciones no autorizadas
		Modificar la información mediante autorización
		Información accesible a personal autorizadas.
	Confidencialidad	
		Prevención de la divulgación no autorizada de la información

Variables	Definición Conceptual	Dimensiones	Indicadores
Prevención de ataques informáticos aplicando seguridad basada en componentes de Honeypot.	La prevención de ataques informáticos es un mecanismo de seguridad con la finalidad de salvaguardar la información aplicando componentes de firewall de siguientes generaciones integrados con sistemas de honeypot como alternativa de engaño a un ciberdelincuente.	Tráfico anormal.	Recolectar datos para establecer el comportamiento anormal de la red.
		Supervisar alteración de aplicaciones.	Crea una lista blanca para especificar cuáles aplicaciones pueden ser ejecutadas.
		Vigilar transferencia de datos.	Atención a movimiento poco común de datos.
		Alertar.	Objetivo de detectar, pero sin realizar ninguna acción más.
		Obtener	Adquirir información sobre el ataque que está detectando.

	información.	
		Ralentizar el ataque que está detectando.
	Ralentizar.	

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

De acuerdo a Wang et al.2020, la tecnología de seguridad basada en honeypot, puede combatir eficazmente los ataques a la red. Así mismo, Sekar et al. 2018, opina que el mecanismo basado en honeypot puede representar un gran obstáculo para los intrusos y piratas informáticos en la red. De la misma manera Ali y Kumar 2017, señalan que Honeypot es uno de los mejores métodos para la captura de malware. Igualmente, Patel et al. 2019, establece que los honeypots constituyen una buena mejora para el sistema de seguridad.

Después del despliegue e implementacion del Honeypot, se comprobó su correcto funcionamiento conjuntamente con la bateria de soluciones que integra, se procede a analizar e interpretar los datos obtenidos mediante al herramienta maltrail, para establecer conclusiones, la recolección de datos se realizó durante 7 dias a partir de su implemetacion, cabe mencionar que para la produccion diaria de este tipo de soluciones se nececita almacenamiento ilimitado debido a los millones de log que genera.

Como se aprecia en la figura 35, los ataque han sido detectados por la herramineta de defensa, donde se puede verificar la clasificacion de la amenaza que esta intentado perpretar la infraestuctura, se observa que los ataques están siendo dirigidos a la direccion ip dst_port 192.168.200.155 que es la direccion de un servidor dentro del dmz, el puerto por el cual estan tratando de acceder al sistema es dst_port 8000 mediante una conexión tcp.

También, todo el tráfico sea este malicioso o sospechoso quedará registrado y podrá ser accedido a través del navegador, cuya interfaz permite filtrar los eventos además de clasificar por nivel de gravedad, mostrar la dirección/protocolo de origen y destino.

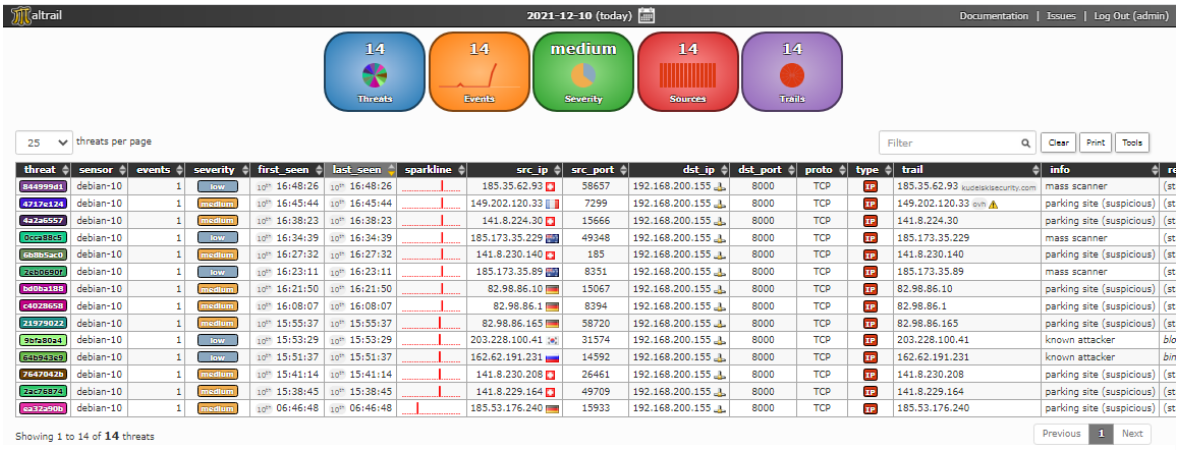


Figura 35. Ataques detectados por la herramienta maltrail

Fuente: Elaborada por el autor

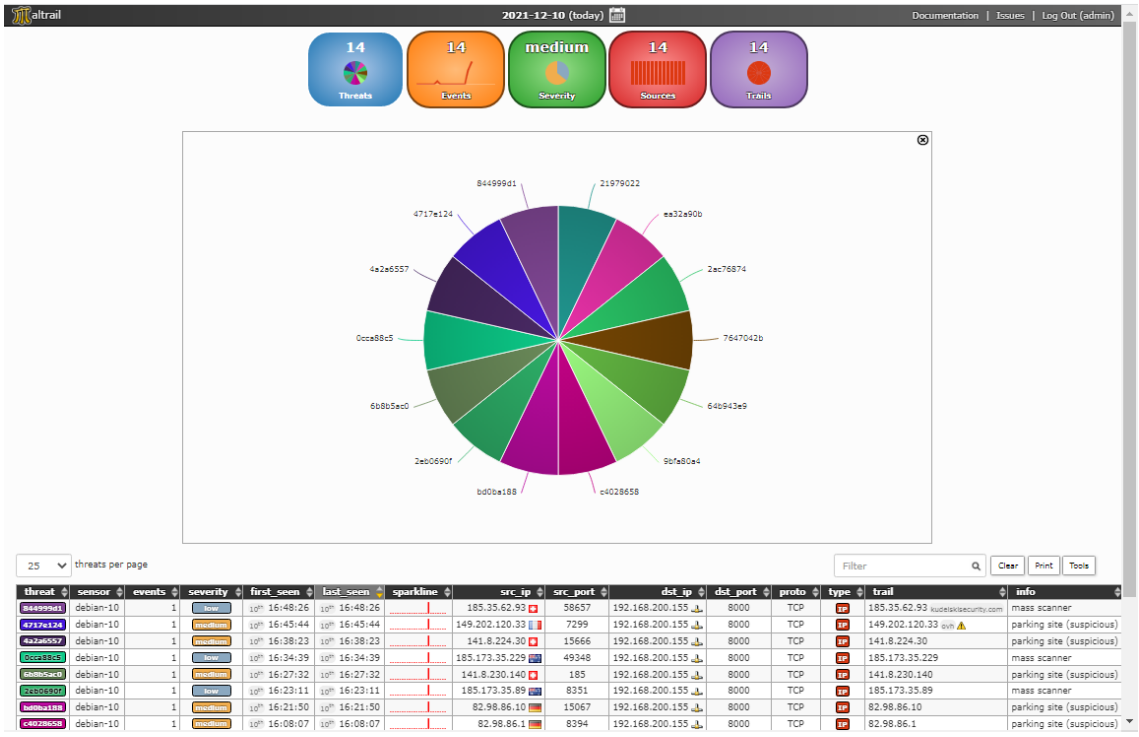


Figura 36. Ataques detectados por la herramienta maltrail y representado con grafico estadístico.

Fuente: Elaborada por el autor

La Figura 37 muestra curva de crecimiento de los ataques detectados, cabe indicar que se realizaron intrusiones en ambiente controlado y ataques a la arquitectura de red en ambiente de producción por lo que estos datos son considerados críticos.

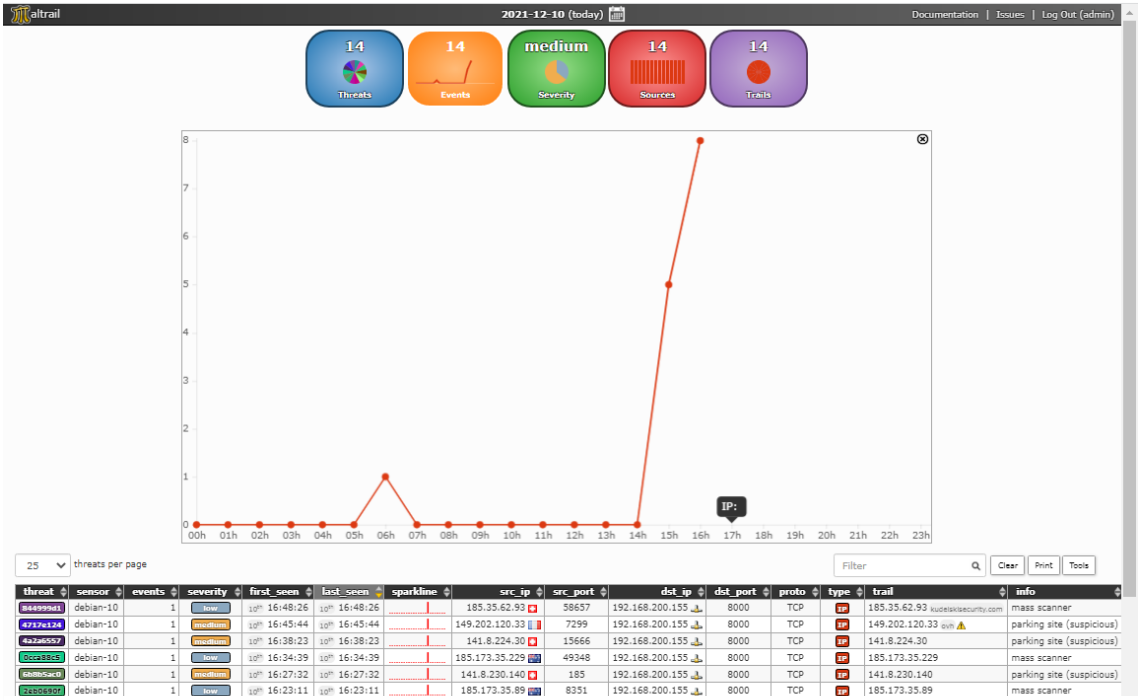


Figura 37. Ataques detectados por maltrail y representando la curva de crecimientos de ataques intensos

Fuente: Elaborada por el autor

En la tabla 5**.** Se puede apreciar el direccionamiento ip que detecta el sistema de monitorización de amenazas, el país del cual proviene el ataque, la ciudad en algunos casos, la latitud, longitud y el proveedor de servicio de internet.

Tabla 5.*Identificación de ataques detectados por origen, ciudad, latitud, longitud e isp*

IP ATACANTE	PAIS	Latitud	Longitud	ISP
185.35.62.93	Switzerland	47.144901275635	8.1550998687744	Nagravision SA
149.202.120.33	France	48.858200073242	2.338700056076	OVH SAS
141.8.224.30	Switzerland	47.144901275635	8.1550998687744	Confluence Networks
185.8.230.140	Germany	51.299301147461	9.4910001754761	
185.173.35.89	Australia	-33.867198944092	151.19970703125	SoftLayer Technologies
82.98.86.165	Germany	51.299301147461	9.4910001754761	Plus.line AG
203.228.100.41	Korea, Republic of	36.28279876709	127.41300201416	Korea Telecom

Fuente: Elaborada por el autor

Como se puede observar en la Figura 38, Un ataque generado en un ambiente controlado creó todas las alertas necesarias para tomar las medidas correctivas, ocultando la verdadera dirección ip del atacante.

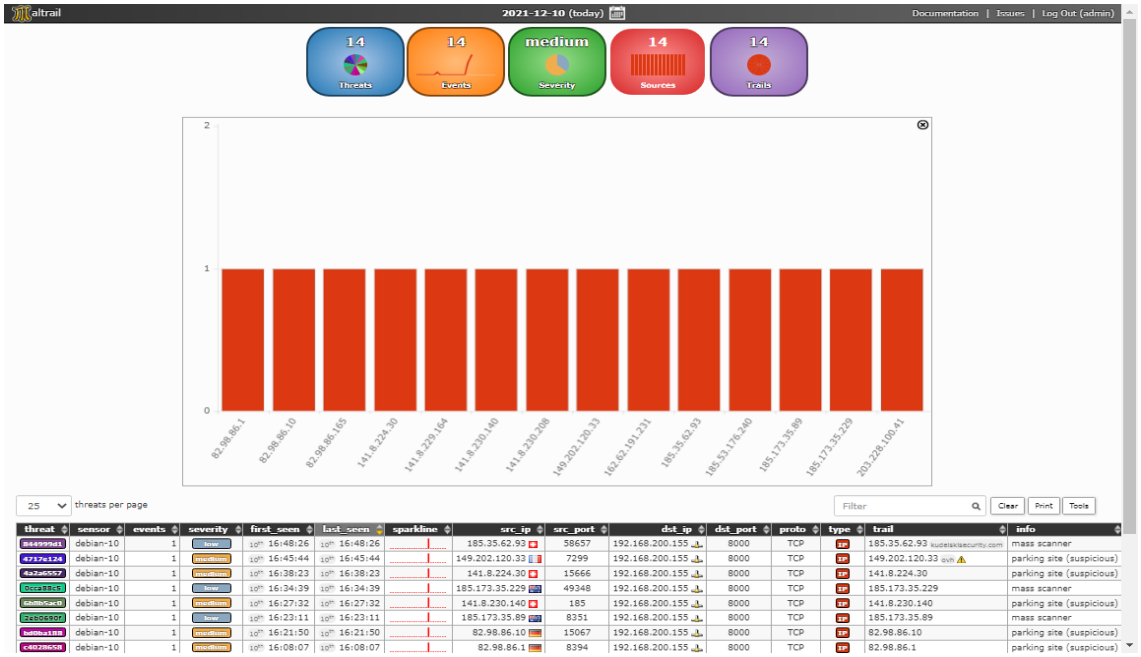


Figura 38. Ataques detectados y representados mediante diagramas de barras por maltrail.

Fuente: Elaborada por el autor.

Tabla 6. *Métricas consideradas para evaluar el entorno de prueba de caso de estudio.*

Componente	Características	Breve descripción
Volumen de datos transferidos utilizando la red	Ancho de banda	Promedio de cantidad de datos que se pueden transferir en un lapso de tiempo específico. Se expresó en kbit/s.
	Trafico entrante	Volumen de tráfico entrante. Se expresa en MB.
	Trafico saliente	Volumen de tráfico saliente. Se expresa en MB.
	Número eventos sospechosos	Cantidad de alertas recibidas en IDS. Se expresa en número enteros.
Incidentes de Seguridad	Número de vulnerabilidades detectadas	Cantidad de vulnerabilidades detectadas en Pentesting. Se expresa en número enteros.

Verificación de volumen de datos transferidos utilizando la red

El volumen de datos transferidos se evaluó con las mediciones de ancho de banda, paquetes recibidos y paquetes enviados de los equipos de usuario final Metasploit, Lampiao y Windows 7 que se realizaron en dos periodos de evaluación distintos; en la Tabla 7 se observa los resultados obtenidos en el primer escenario, mientras que en la Tabla 8 se presentan los resultados obtenidos en el segundo escenario; donde se observa que el segundo escenario presenta una disminución en el volumen de datos transferidos, en relación con el primero.

Tabla 7.*Métricas de volumen de datos transferidos obtenidos en el Escenario de Evaluación 1.*

		Metasploit 10.10.10.50	**Lampiao Debian 10 10.10.10.51**	**Windows 7 10.10.10.52**
Volumen de datos transferidos	Ancho de banda	31.77 kbits/s	25.83 kbits/s	38.12 kbits/s
	Paquetes Recibidos	1500 MB	498.9 MB	2100 MB
	Paquetes Enviados	508.6 MB	1200 MB	292.3 MB

Tabla 8. *Métricas de volumen de datos transferidos obtenidos en el Escenario de Evaluación 2*.

		Metasploit 10.10.10.50	**Lampiao Debian 10 10.10.10.51**	**Windows 7 10.10.10.52**
Volumen de datos transferidos	Ancho de banda	24.28 kbits/s	21.65 kbits/s	26.28 kbits/s
	Paquetes Recibidos	99 MB	101.6 MB	212.7 MB
	Paquetes Enviados	14.6 MB	12.4 MB	8.8 MB

Verificación de Incidentes de Seguridad

La cantidad de incidentes de seguridad se evaluó con las mediciones de número de eventos sospechosos y número de vulnerabilidades detectadas de los equipos de usuario final Metasploit, Lampiaoy Windows 7 que se realizaron en dos periodos de evaluación distintos; en la tabla 9 se observan los resultados obtenidos en el primer escenario, mientras que en la tabla 10 se muestran los resultados de segundo escenario; donde se observa que el segundo escenario presenta una disminución en la cantidad de incidentes de seguridad en relación al primero.

Tabla 9. *Métricas de incidentes de seguridad obtenidos en el Escenario de Evaluación 1.*

		Metasploit 10.10.10.50	**Lampiao Debian 10 10.10.10.51**	**Windows 7 10.10.10.52**
Incidentes de seguridad	Número de eventos sospechosos	28557	17747	8588
	Número de vulnerabilidades detectadas	14	14	14

Tabla 10. *Métricas de incidentes de seguridad obtenidos en el Escenario de Evaluación 2*

		Metasploit 10.10.10.50	**Lampiao Debian 10 10.10.10.51**	**Windows 7 10.10.10.52**
Incidentes de seguridad	Número de eventos sospechosos	12980	7784	3143
	Número de vulnerabilidades detectadas	9	6	8

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Estableciendo elementos de un sistema de seguridad basado en honeypot se logró desplegar una batería de honeypot integral para cualquier tipo de arquitectura de red e infraestructura tecnológica, sea esta física o virtualizada, independientemente del sistema hipervisor o sistema operativo anfitrión, muy independiente de la tecnología utilizada
- La implementación del modelo del honeypot, T-pot, facilitó la caza de enemigos ya que esta tecnología se incorpora antes del firewall como método de prevención simulando los mismos servicios o demonios desplegados dentro del DMZ.
- La simulación de ataques cibernético a la infraestructura tecnológica permitió validar la seguridad de los servidores dentro del DMZ, logrando hardenizar y establecer políticas de seguridad a nivel de firewall, minimizando los riesgos de vulnerabilidad.
- El despliegue de un sistema ids/ ips bien definido con reglas claras logró identificar y neutralizar brechas de inseguridad y conexiones reversas desde el DMZ hacia el exterior

5.2. RECOMENDACIONES

- Realizar análisis de vulnerabilidades y el monitoreo constante de las redes del centro de datos de la ESPAM MFL, establecer protocolos de seguridad que permitan disponer de un mejor control de la seguridad de la información y sistemas informáticos contenido en los servidores de la institución.
- Se recomienda que dentro del centro de datos se invierta en tecnología de seguridad informática, debido a que la seguridad debe ser considerada como un proceso de mejoramiento continuo, en donde los nuevos requerimientos de seguridad de la información se ajusten a los cambios que se enfrenta día a día la ciberseguridad.

- Realizar constantemente pruebas a los sistemas informáticos que tiene en producción la institución dentro de sus servidores, con la finalidad de minimizar riesgos de vulnerabilidad en el código fuente, aplicando pruebas de testing como caja negra y caja blanca como el respectivo pententing web.
- Como se diseñó una Honeypots en infraestructura virtualizada, es fundamental automatizar los sistemas mediante un sistema vcenter que permita de manera programada y automática realizar copias de seguridad de las instancias de máquinas virtuales

BIBLIOGRAFÍA

Borbúa, R. V., Chicango, R. P. R., & Herrera, L. R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa/ Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance. URVIO. Revista Latinoamericana de Estudios de Seguridad, 20, 31-45. https://doi.org/10.17141/urvio.20.2017.2571

Chuquilla, A., Guarda, T., & Ninahualpa Quiña, G. (2019). Ransomware—WannaCry Security is everyone's. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 1-4. https://doi.org/10.23919/CISTI.2019.8760749

Código Orgánico Integral Penal, (2014).

Conejos, J. B. (2014). Sistema de seguridad perimetral programable inteligent. *Ingeniería del agua*, *18*(1), ix. https://doi.org/10.4995/ia.2014.3293

Constitución de la Republica de Ecuador, (2008).

Cuzme-Rodríguez, F., León-Gudiño, M., Suárez Zambrano, L., & Domínguez-Limaico, H. (2019). *Offensive Security: Ethical Hacking Methodology on the Web* (pp. 127-140). https://doi.org/10.1007/978-3-030-02828-2_10

Data-Team. (2018). *CW - CIBERSEGURIDAD. Retrieved September 3, 2019, from Revista datta website: Http://revista.datta.com.ec/publication/db5b382a/mobile/*. http://revista.datta.com.ec/publication/db5b382a/mobile/

Eduard, A., & Daniel, L. (2013). *Honeypot: Ventajas y Desventajas como Mecanismo para la Prevención de Intrusos Informáticos*. 6.

FBI. (2019). *Ransomware Prevention and Response for CISOs* [File]. Federal Bureau of Investigation. https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

Hernández, M. J., & López, L. (2007, abril). *Aplicaciones prácticas de Honeypots en la protección y monitorización de redes de información—ProQuest*. https://bv.unir.net:2210/docview/2135188934/7AB9A64F39324BC7PQ/1?accountid=142712

Imaji, A. O. (2019). Ransomware Attacks: Critical Analysis, Threats, and Prevention methods. *Fort Hays State University*.

IONOS, D. G. (2021). *¿Qué es un honeypot?* IONOS Digitalguide. https://www.ionos.es/digitalguide/servidores/seguridad/honeypot-seguridad-informatica-para-detectar-amenazas/

Jakubski, K. (2017). *Petya'2017. Kierunkowe ataki cybernetyczne (Petya'2017. Directional cyber attacks)*.

Leguizamón-Páez, M. A., Bonilla-Díaz, M. A., León-Cuervo, C. A., Leguizamón-Páez, M. A., Bonilla-Díaz, M. A., & León-Cuervo, C. A. (2020). Análisis de ataques informáticos mediante Honeypots en la Universidad Distrital Francisco José de Caldas. *Ingeniería y competitividad*, *22*(2). https://doi.org/10.25100/iyc.v22i2.8483

Memari, N., Hashim, S. J. B., & Samsudin, K. B. (2014). Towards virtual honeynet based on LXC virtualization. *2014 IEEE REGION 10 SYMPOSIUM*, 496-501. https://doi.org/10.1109/TENCONSpring.2014.6863084

Monroy, J. I. A., & Castro, M. R. P. (2009). *INGENIERO EN COMPUTACIÓN ESPECIALIZACIÓN SISTEMAS DE INFORMACIÓN*. 236.

Morales Carrillo, J. J., Avellan Zambrano, N., Mera, S., & Bravo, M. (2019, mayo). *Ciberseguridad y su aplicación en las Instituciones de Educación Superior—ProQuest*. https://bv.unir.net:2210/docview/2318537201/2052AF55ABD24F46PQ/7?accountid=142712

Morales, F., Toapanta, S., & Toasa, R. M. (2020, marzo). *Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información—ProQuest*. https://bv.unir.net:2210/docview/2385756526/9A8BAD7686224036PQ/1?accountid=142712

Morgan, S. (2018, octubre 19). Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021. *Cybercrime Magazine*. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

Muñoz, M. (2015). *Estado actual de equipos de respuesta a incidentes de seguridad informática/Present state of Response Teams computer security incidents—ProQuest*. https://bv.unir.net:2210/docview/1690433358/fulltextPDF/BD7154921A0494CPQ/6?accountid=142712

Nagurney, A., & Shukla, S. (2017a). Multifirm models of cybersecurity investment competition vs. Cooperation and network vulnerability. *European Journal of Operational Research*, *260*(2), 588-600. https://doi.org/10.1016/j.ejor.2016.12.034

Norma Técnica para coordinar la Gestión de Incidentes y Vulnerabilidades que afecten a la Seguridad de las Redes y Servicios de Telecomunicaciones, (2018).

Patel, M., Mugut, N., Telkar, S.: IMPLEMENTATION AND BEHAVIOUR ANALYSIS OF HONEYPOT. 6, 7 (2019).

li, P.D., Kumar, T.G.: Malware capturing and detection in dionaea honeypot. In: 2017 Innovations in Power and Advanced Computing Technologies (i-PACT). pp. 1–5. IEEE, Vellore (2017). https://doi.org/10.1109/IPACT.2017.8245158

Sekar, K.R., Gayathri, V., Anisha, G., Ravichandran, K.S., Manikandan, R.: Dynamic Honeypot Configuration for Intrusion Detection. In: 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). pp. 1397–1401. IEEE, Tirunelveli (2018). https://doi.org/10.1109/ICOEI.2018.8553956.

Nagurney, A., & Shukla, S. (2017b). Multifirm models of cybersecurity investment competition vs. Cooperation and network vulnerability. *European Journal of Operational Research*, *260*(2), 588-600. https://doi.org/10.1016/j.ejor.2016.12.034

Ramos Varón, A. A., Gonzales Cañas, J. M., Picouto Ramos, F., & Serrano Aparicio, E. (2014). *Seguridad perimetral, monitorización y ataques en redes—Grupo Editorial RA-MA*. https://www.ra-ma.es/libro/seguridad-perimetral-monitorizacion-y-ataques-en-redes_48501/, https://www.ra-ma.es/libro/seguridad-perimetral-monitorizacion-y-ataques-en-redes_48501/

RZ, R. Z. (2021, noviembre 1). *Qué son los Honeypot, para qué sirven y cómo funcionan* [Https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/]. RedesZone. https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/

Smartekh, G. (2012, octubre 23). *100 Universidades Hackeadas.* https://blog.smartekh.com/100-universidades-hackeadas

Tiempo, T. (2013, marzo 2). *En Ecuador, estudiantes contratan hacker para que modifique sus notas*. El Tiempo. https://www.eltiempo.com/archivo/documento/CMS-12631694

Vaca Urbina, G. (2016). *Introducciòn a la Seguridad Informatica*. https://bv.unir.net:2769/es/lc/unir/titulos/40458?as_all=%22seguridad__informatica%22&as_all_op=unaccent__icontains&prev=as

WeLiveSecurity, W. (2020, julio 31). *Qué es un honeypot y cómo implementarlo en nuestra red*. WeLiveSecurity. https://www.welivesecurity.com/la-es/2020/07/31/que-es-honeypot-como-implementarlo-nuestra-red/

Norma Técnica para coordinar la Gestión de Incidentes y Vulnerabilidades que afecten a la Seguridad de las Redes y Servicios de Telecomunicaciones, (2018).

Borbúa, R. V., Chicango, R. P. R., & Herrera, L. R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa/ Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, *20*, 31-45. https://doi.org/10.17141/urvio.20.2017.2571

Chuquilla, A., Guarda, T., & Ninahualpa Quiña, G. (2019). Ransomware—WannaCry Security is everyone's. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 1-4. https://doi.org/10.23919/CISTI.2019.8760749

Código Orgánico Integral Penal, (2014).

Conejos, J. B. (2014). Sistema de seguridad perimetral programable inteligent. *Ingeniería del agua*, *18*(1), ix. https://doi.org/10.4995/ia.2014.3293

Constitución de la Republica de Ecuador, (2008).

Cuzme-Rodríguez, F., León-Gudiño, M., Suárez Zambrano, L., & Domínguez-Limaico, H. (2019). *Offensive Security: Ethical Hacking Methodology on the Web* (pp. 127-140). https://doi.org/10.1007/978-3-030-02828-2_10

Data-Team. (2018). *CW - CIBERSEGURIDAD. Retrieved September 3, 2019, from Revista datta website: Http://revista.datta.com.ec/publication/db5b382a/mobile/*. http://revista.datta.com.ec/publication/db5b382a/mobile/

Eduard, A., & Daniel, L. (2013). *Honeypot: Ventajas y Desventajas como Mecanismo para la Prevención de Intrusos Informáticos*. 6.

FBI. (2019). *Ransomware Prevention and Response for CISOs* [File]. Federal Bureau of Investigation. https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

Hernández López, M. J. (2007, junio). *Practical applications of Honeypots in the protection and monitoring of information networks—ProQuest*. https://bv.unir.net:2210/docview/2135188934/B54EF13DEEC04C76PQ/1?accountid=142712

Hernández, M. J., & López, L. (2007, abril). *Aplicaciones prácticas de Honeypots en la protección y monitorización de redes de información—ProQuest*. https://bv.unir.net:2210/docview/2135188934/7AB9A64F39324BC7PQ/1?accountid=142712

Imaji, A. O. (2019). Ransomware Attacks: Critical Analysis, Threats, and Prevention methods. *Fort Hays State University*.

IONOS, D. G. (2021). *¿Qué es un honeypot?* IONOS Digitalguide. https://www.ionos.es/digitalguide/servidores/seguridad/honeypot-seguridad-informatica-para-detectar-amenazas/

Jakubski, K. (2017). *Petya'2017. Kierunkowe ataki cybernetyczne (Petya'2017. Directional cyber attacks)*.

Leguizamón-Páez, M. A., Bonilla-Díaz, M. A., León-Cuervo, C. A., Leguizamón-Páez, M. A., Bonilla-Díaz, M. A., & León-Cuervo, C. A. (2020). Análisis de ataques informáticos mediante Honeypots en la Universidad Distrital Francisco José de Caldas. *Ingeniería y competitividad*, *22*(2). https://doi.org/10.25100/iyc.v22i2.8483

Memari, N., Hashim, S. J. B., & Samsudin, K. B. (2014). Towards virtual honeynet based on LXC virtualization. *2014 IEEE REGION 10 SYMPOSIUM*, 496-501. https://doi.org/10.1109/TENCONSpring.2014.6863084

Monroy, J. I. A., & Castro, M. R. P. (2009). *INGENIERO EN COMPUTACIÓN ESPECIALIZACIÓN SISTEMAS DE INFORMACIÓN*. 236.

Morales Carrillo, J. J., Avellan Zambrano, N., Mera, S., & Bravo, M. (2019, mayo). *Ciberseguridad y su aplicación en las Instituciones de Educación Superior—ProQuest*.

https://bv.unir.net:2210/docview/2318537201/2052AF55ABD24F46PQ/7?accountid=142712

Morales, F., Toapanta, S., & Toasa, R. M. (2020, marzo). *Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información—ProQuest*. https://bv.unir.net:2210/docview/2385756526/9A8BAD7686224036PQ/1?accountid=142712

Morgan, S. (2018, octubre 19). Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021. *Cybercrime Magazine*. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

Muñoz, M. (2015). *Estado actual de equipos de respuesta a incidentes de seguridad informática/Present state of Response Teams computer security incidents—ProQuest*. https://bv.unir.net:2210/docview/1690433358/fulltextPDF/BD7154921A0494CPQ/6?accountid=142712

Nagurney, A., & Shukla, S. (2017a). Multifirm models of cybersecurity investment competition vs. Cooperation and network vulnerability. *European Journal of Operational Research*, *260*(2), 588-600. https://doi.org/10.1016/j.ejor.2016.12.034

Nagurney, A., & Shukla, S. (2017b). Multifirm models of cybersecurity investment competition vs. Cooperation and network vulnerability. *European Journal of Operational Research*, *260*(2), 588-600. https://doi.org/10.1016/j.ejor.2016.12.034

Ramos Varón, A. A., Gonzales Cañas, J. M., Picouto Ramos, F., & Serrano Aparicio, E. (2014). *Seguridad perimetral, monitorización y ataques en redes—Grupo Editorial RA-MA*. https://www.ra-ma.es/libro/seguridad-perimetral-monitorizacion-y-ataques-en-redes_48501/, https://www.ra-ma.es/libro/seguridad-perimetral-monitorizacion-y-ataques-en-redes_48501/

RZ, R. Z. (2021, noviembre 1). *Qué son los Honeypot, para qué sirven y cómo funcionan* [Https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/]. RedesZone. https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/

Smartekh, G. (2012, octubre 23). *100 Universidades Hackeadas.* https://blog.smartekh.com/100-universidades-hackeadas

Tiempo, T. (2013, marzo 2). *En Ecuador, estudiantes contratan hacker para que modifique sus notas*. El Tiempo. https://www.eltiempo.com/archivo/documento/CMS-12631694

Vaca Urbina, G. (2016). *Introducciòn a la Seguridad Informatica*. https://bv.unir.net:2769/es/lc/unir/titulos/40458?as_all=%22seguridad__informatica%22&as_all_op=unaccent__icontains&prev=as

WeLiveSecurity, W. (2020, julio 31). *Qué es un honeypot y cómo implementarlo en nuestra red*. WeLiveSecurity. https://www.welivesecurity.com/la-es/2020/07/31/que-es-honeypot-como-implementarlo-nuestra-red/

Baca Urbina, G. (2016). Introducción a la seguridad informática. Grupo Editorial Patria. https://bv.unir.net:2769/es/lc/unir/titulos/40458

Muñoz, M., & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática/Present state of response teams

computer security incidents. Revista Ibérica De Sistemas e Tecnologias De Informação, , 1-15. Retrieved from http://www.espaciotv.es:2048/referer/secretcode/scholarly-journals/estado-actual-de-equipos-respuesta-incidentes/docview/1690433358/se-2?accountid=142712

MAIWALD, ERIC. 2004. FUNDAMENTOS DE SEGURIDAD DE REDES - Margen Libros. edited by MCGRAW-HILL / INTERAMERICANA DE MEXICO. Retrieved February 9, 2015 (http://mx.casadellibro.com/libro-fundamentos-de-seguridadde-redes/9789701046241/997462).

Caralli, Richard A., Julia H. Allen, Pamela D. Curtis, David W. White, and Lisa R. Young. 2010. CERT ® Resilience Management Model. Retrieved (http://www.cert.org/ resilience/download/CERT-RMM_v1.0.pdf).

Norma Técnica para coordinar la Gestión de Incidentes y Vulnerabilidades que afecten a la Seguridad de las Redes y Servicios de Telecomunicaciones, (2018).

Borbúa, R. V., Chicango, R. P. R., & Herrera, L. R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa/ Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, *20*, 31-45. https://doi.org/10.17141/urvio.20.2017.2571

Chuquilla, A., Guarda, T., & Ninahualpa Quiña, G. (2019). Ransomware—WannaCry Security is everyone's. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 1-4. https://doi.org/10.23919/CISTI.2019.8760749

Código Orgánico Integral Penal, (2014).

Conejos, J. B. (2014). Sistema de seguridad perimetral programable inteligent. *Ingeniería del agua*, *18*(1), ix. https://doi.org/10.4995/ia.2014.3293

Constitución de la Republica de Ecuador, (2008).

Cuzme-Rodríguez, F., León-Gudiño, M., Suárez Zambrano, L., & Domínguez-Limaico, H. (2019). *Offensive Security: Ethical Hacking Methodology on the Web* (pp. 127-140). https://doi.org/10.1007/978-3-030-02828-2_10

Data-Team. (2018). *CW - CIBERSEGURIDAD. Retrieved September 3, 2019, from Revista datta website: Http://revista.datta.com.ec/publication/db5b382a/mobile/*. http://revista.datta.com.ec/publication/db5b382a/mobile/

Eduard, A., & Daniel, L. (2013). *Honeypot: Ventajas y Desventajas como Mecanismo para la Prevención de Intrusos Informáticos*. 6.

FBI. (2019). *Ransomware Prevention and Response for CISOs* [File]. Federal Bureau of Investigation. https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

Hernández López, M. J. (2007, junio). *Practical applications of Honeypots in the protection and monitoring of information networks—ProQuest*. https://bv.unir.net:2210/docview/2135188934/B54EF13DEEC04C76PQ/1?accountid=142712

Hernández, M. J., & López, L. (2007, abril). *Aplicaciones prácticas de Honeypots en la protección y monitorización de redes de información—ProQuest*. https://bv.unir.net:2210/docview/2135188934/7AB9A64F39324BC7PQ/1?accountid=142712

Imaji, A. O. (2019). Ransomware Attacks: Critical Analysis, Threats, and Prevention methods. *Fort Hays State University*.

IONOS, D. G. (2021). *¿Qué es un honeypot?* IONOS Digitalguide. https://www.ionos.es/digitalguide/servidores/seguridad/honeypot-seguridad-informatica-para-detectar-amenazas/

Jakubski, K. (2017). *Petya'2017. Kierunkowe ataki cybernetyczne (Petya'2017. Directional cyber attacks)*.

Leguizamón-Páez, M. A., Bonilla-Díaz, M. A., León-Cuervo, C. A., Leguizamón-Páez, M. A., Bonilla-Díaz, M. A., & León-Cuervo, C. A. (2020). Análisis de ataques informáticos mediante Honeypots en la Universidad Distrital Francisco José de Caldas. *Ingeniería y competitividad*, *22*(2). https://doi.org/10.25100/iyc.v22i2.8483

Memari, N., Hashim, S. J. B., & Samsudin, K. B. (2014). Towards virtual honeynet based on LXC virtualization. *2014 IEEE REGION 10 SYMPOSIUM*, 496-501. https://doi.org/10.1109/TENCONSpring.2014.6863084

Monroy, J. I. A., & Castro, M. R. P. (2009). *INGENIERO EN COMPUTACIÓN ESPECIALIZACIÓN SISTEMAS DE INFORMACIÓN*. 236.

Morales Carrillo, J. J., Avellan Zambrano, N., Mera, S., & Bravo, M. (2019, mayo). *Ciberseguridad y su aplicación en las Instituciones de Educación Superior—ProQuest*. https://bv.unir.net:2210/docview/2318537201/2052AF55ABD24F46PQ/7?accountid=142712

Morales, F., Toapanta, S., & Toasa, R. M. (2020, marzo). *Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información—ProQuest*.

https://bv.unir.net:2210/docview/2385756526/9A8BAD7686224036PQ/1?accountid=142712

Morgan, S. (2018, octubre 19). Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021. *Cybercrime Magazine*. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

Muñoz, M. (2015). *Estado actual de equipos de respuesta a incidentes de seguridad informática/Present state of Response Teams computer security incidents—ProQuest*. https://bv.unir.net:2210/docview/1690433358/fulltextPDF/BD7154921A0494CPQ/6?accountid=142712

Nagurney, A., & Shukla, S. (2017a). Multifirm models of cybersecurity investment competition vs. Cooperation and network vulnerability. *European Journal of Operational Research*, *260*(2), 588-600. https://doi.org/10.1016/j.ejor.2016.12.034

Nagurney, A., & Shukla, S. (2017b). Multifirm models of cybersecurity investment competition vs. Cooperation and network vulnerability. *European Journal of Operational Research*, *260*(2), 588-600. https://doi.org/10.1016/j.ejor.2016.12.034

Ramos Varón, A. A., Gonzales Cañas, J. M., Picouto Ramos, F., & Serrano Aparicio, E. (2014). *Seguridad perimetral, monitorización y ataques en redes—Grupo Editorial RA-MA*. https://www.ra-ma.es/libro/seguridad-perimetral-monitorizacion-y-ataques-en-redes_48501/, https://www.ra-ma.es/libro/seguridad-perimetral-monitorizacion-y-ataques-en-redes_48501/

RZ, R. Z. (2021, noviembre 1). *Qué son los Honeypot, para qué sirven y cómo funcionan* [Https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/]. RedesZone. https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/

Smartekh, G. (2012, octubre 23). *100 Universidades Hackeadas.* https://blog.smartekh.com/100-universidades-hackeadas

Tiempo, T. (2013, marzo 2). *En Ecuador, estudiantes contratan hacker para que modifique sus notas*. El Tiempo. https://www.eltiempo.com/archivo/documento/CMS-12631694

Vaca Urbina, G. (2016). *Introducciòn a la Seguridad Informatica*. https://bv.unir.net:2769/es/lc/unir/titulos/40458?as_all=%22seguridad__informatica%22&as_all_op=unaccent__icontains&prev=as

WeLiveSecurity, W. (2020, julio 31). *Qué es un honeypot y cómo implementarlo en nuestra red*. WeLiveSecurity. https://www.welivesecurity.com/la-es/2020/07/31/que-es-honeypot-como-implementarlo-nuestra-red/

Baca Urbina, G. (2016). Introducción a la seguridad informática. Grupo Editorial Patria. https://bv.unir.net:2769/es/lc/unir/titulos/40458

Muñoz, M., & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática/Present state of response teams computer security incidents. Revista Ibérica De Sistemas e Tecnologias De Informação, , 1-15. Retrieved from http://www.espaciotv.es:2048/referer/secretcode/scholarly-journals/estado-actual-de-equipos-respuesta-incidentes/docview/1690433358/se-2?accountid=142712

MAIWALD, ERIC. 2004. FUNDAMENTOS DE SEGURIDAD DE REDES - Margen Libros. edited by MCGRAW-HILL / INTERAMERICANA DE MEXICO.

Retrieved February 9, 2015 (http://mx.casadellibro.com/libro-fundamentos-de-seguridadde-redes/9789701046241/997462).

Wang, K., Tong, M., Yang, D., Liu, Y.: A Web-Based Honeypot in IPv6 to Enhance Security. Information. 11, 440 (2020). https://doi.org/10.3390/info11090440.

ANEXOS

ANEXO 1.

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MFL

Maestría En Tecnología De Información Y Comunicación Mención En Redes Y Telecomunicaciones

Información de la entrevista

Fecha_____ **hora**_____

Nombre de entrevistado

_____

Cargo

_____

Email

_____

Teléfono

_____

Datos del entrevistador

Nombres

_____

Email

_____

- Que caracteriza a una amenaza interna en el ámbito de la ciberseguridad

- Cuenta el centro de datos de la ESPAM MFL con herramientas para centro de monitoreo de amenazas

- Conoce usted la importancia de un sistema de caza de enemigo como Honeypot

- Como considera el despliegue de un sistema de honeypot o caza de enemigo para el centro de datos de la ESPAM MFL

- Como detecta los ataques cibernéticos a la ESPAM MFL

- ¿Posee algún tipo de red privada o de uso confidencial, es decir limitada solo a usuarios autorizados?

- . ¿Antes de implantar nuevos servicios o aplicaciones se realiza alguna evaluación para determinar los posibles riesgos de seguridad?

- ¿Se utiliza firewalls u otros controles de acceso en los perímetros de la red para proteger los recursos?

- ¿Se hace uso de alguna red DMZ para separar redes internas y externas de los servicios albergados en la ESPAM MFL?

- ¿Con los mecanismos de seguridad que poseen actualmente, se ha logrado detectar y mitigar algún tipo de intrusión?

- ¿Qué tipo de intrusiones han sido capaz de detectar los mecanismos de seguridad que hay implementados (Spoofing, Sniffing, Rootkit)? Y frecuencias.

- ¿Existe algún método que Uds. usen para proceder analizar los ataques a la seguridad que sufre la red ejemplo Análisis Forense?

- ¿Una vez detectado la intrusión se realiza algún procedimiento para corregir la vulnerabilidad existente?

ANEXO 2.

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

PLAN DE FORTALECIMIENTO INFORMÁTICO PARA EL CENTRO DE DATOS DE LA ESPAM MFL UTILIZANDO HERRAMIENTAS DE HONEYPOT.

Marzo 2022

CONTENIDO

1. INTRODUCCIÓN

El objetivo de presente documento es definir un Plan de fortalecimiento informático para el centro de datos de la ESPAM MFL utilizando herramientas de Honeypot, que permita mejorar aspectos de seguridad, disponibilidad y confidencialidad en los sistemas distribuidos y centralizados de la institución, mediante la implementación de mecanismos de caza de enemigos y el despliegue de una batería de soluciones de honeypot que se integre a la infraestructura y arquitectura tecnológica.

El plan presenta un sistema honeypot vulnerable con la finalidad de atraer a ciberdelincuentes, conocer sus movimientos y mediante esta información fortalecer el firewall perimetral, agregar políticas y reglas que permitan hardenizar al sistema de seguridad centralizado en el centro de datos en la ESPAM MFL .

el Plan de fortalecimiento, permitirá tomar medidas y aplicar estrategias que logren mejorar la seguridad y minimizar brechas de inseguridad, mitigar posibles riesgos, las mismas que pueden ser propensa a eventos maliciosos comprometiendo la seguridad de la información y aplicaciones que se encuentran dentro de los servidores de la zona DMZ.

2. ALCANCE

Este plan de acción abarca lo siguiente:

- ✓ Identificación de la ubicación específica del sistema honeypot dentro de la arquitectura de red del centro de datos de la ESPAM MFL
- ✓ Detectar ataques cibernéticos para fortalecer las vulnerabilidades del firewall perimetral del DMZ.
- ✓ Establecer nuevas reglas de firewall y reglas de port forwarding como mecanismos de hardenización de la seguridad.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Desarrollar un Plan de fortalecimiento informático que permita mejorar el estado de la Ciberseguridad en el centro de datos de la ESPAM MFL utilizando herramientas de Honeypot

3.2. OBJETIVOS ESPECÍFICOS

- ✓ Analizar las herramientas honeypot T-pot y caza de enemigo como mecanismos de detección de intrusos
- ✓ Diseñar la topología de red del Honeypots en el centro de datos de la ESPAM MFL
- ✓ Implementar y desplegar el honeypot, y realizar pruebas de ataques a la red
- ✓ Realizar una guía de implementación del honeypot en los servidores de la ESPAM MFL que permita aplicar reglas de firewall para mejorar la seguridad en la red de datos.

4. NATURALEZA DE HONEYPOT

4.1. HONEYPOT DE PRODUCCIÓN

Son aquellos que se utilizan para proteger a las organizaciones en ambientes reales de operación. Se implementan de manera colateral a las redes de datos o infraestructuras y están sujetos a ataques constantes los 365 días del año. Esta herramienta de detección de ataques permiten complementar la protección de la red y los hosts.(Hernández López, 2007)

4.2. HONEYPOT DE INVESTIGACIÓN

Son implementados con la finalidad de proteger redes, además constituyen recursos educativos de naturaleza demostrativa y de investigación cuyo objetivo se centra en estudiar patrones de ataque y amenazas de todo tipo en ambientes controlados. Gran parte de la atención actual de despliegue se centra en los Honeypot para la investigación, que son utilizados para recolectar información sobre las acciones de los intrusos. El proyecto Honeynets, por ejemplo, es una organización para la investigación sobre seguridad voluntaria, sin ánimo de lucro que utiliza los Honeypot para recolectar información sobre las amenazas del ciberespacio.(Hernández López, 2007)

4.3. HONEYPOT DE BAJA INTERACCIÓN

Estos Honeypot trabajan emulando servicios y sistemas operativos configurados por el administrador del Honeypot, como FTP, probablemente permitirá ejecutar algunos comandos FTP adicionales, pero no representa un blanco de importancia crítica que probablemente no está ligado a un servidor FTP que contenga información sensible. Los Honeypot que tienen un grado bajo de interactividad se basan fundamentalmente en la imitación de sistemas o aplicaciones reales. Los servicios y las funciones solo se simularán en la medida que hagan posible un ataque(IONOS, 2021).

4.4. HONEYPOT DE ALTA INTERACCIÓN

Este tipo de Honeypot constituyen una solución compleja, implica la utilización de sistemas operativos y aplicaciones reales montados como sistemas de

producción, involucran aplicaciones reales que se ejecutan de manera normal, muchas veces en relación directa a servicios como bases de datos, directorios de archivos compartidos. Si un Honeypot de alta interacción no se encuentra protegido por parte de un sistema de seguridad perimetral firewall, un atacante puede acceder a él para infiltrarse en el sistema que se ha de proteger o que a partir de ahí pueda hacer algún movimiento lateral de ataques en otro servidor de la red(Hernández & López, 2007).

4.5. BATERÍAS DE HONEYPOT

Adbhoney:

Honeypot de baja interacción diseñado para Android Debug Bridge sobre TCP/IP

Ciscoasa:

Un Honeypot de baja interacción para el componente Cisco ASA capaz de detectar CVE-2018-0101. Un DoS y vulnerabilidad de ejecución remota de código.

Citrixhoneypot:

Detecta y registra los intentos de exploración y explotación de CEV-2019-19781.

Conpot:

Es un Honeypot de sistema de control industrial de bajo nivel de servidor interactivo diseñado para ser fácil de implementar, modificar y ampliar. Al proporcionar una gama de protocolos de control industrial comunes, creamos los conceptos básicos para construir su propio sistema, capaz de emular infraestructuras complejas para convencer a un adversario de que acaba de encontrar en enorme complejo industrial.

Cowrie:

Cowrie es un Honeypot SSH y Telnet de interacción media a alta diseñado para registrar ataques de fuerza bruta y la interacción de la Shell realizada por el atacante. En modo de interacción media (Shell) emula un sistema UNIX en Python, en modo de interacción alta (proxy) funciona como un proxy SSH y telnet para observar el comportamiento del atacante a otro sistema.

Dicompot:

Digital imaging and cominications in medicine (MICOM) Honeypot, DICOM permite la integración de datos digitales de escáneres, cámaras de video, servidores, estaciones de trabajo, impresoras y hardware de red proporcionadas por diferentes compañías en un solo PACS.

Dionaea:

La intención de Dionaea es atrapar el malware que explota las vulnerabilidades expuestas por los servicios ofrecidos a una red, el objetivo final es obtener una copia del malware, los protocolos soportados son HTTP, MSQL, MySQL, MQTT, SIP, SIMB, TFTP, UPnP entre otros.

Elasticpot:

Este es un Honeypot que simula un servidor Elasticsearch vulnerable abierto al internet

Glutton:

Glutton proporciona SSH y un proxy TCP. El proxy SSH funciona como un MITM entre el atacante y el servidor para registrar todo en texto sin formato.

Heralding:

Honeypot simple que recompile credenciales, nada más. Actualmente se admiten los siguientes protocolos: ftp, telnet, ssh, rdp, http, https, pop3, pop3s, imap, imaps, smtp, vnc, postgresql y sockes5.

Honeypy:

Un Honeypot de baja interacción con la capacidad de ser mas de un Honeypot de interacción media. El nivel de interacción está determinado por la funcionalidad del complemento utilizado. Se pueden crear complementos para emular servicios basados en UDP o TCP para proporcionar más interacción.

Honeysap:

Es un Honeypot enfocado en la investigación de baja interacción específico para los servicios de SAP. Su objetivo es aprender las técnicas y motivaciones detrás de los ataques contra los sistemas SAP.

Honeytrap:

Es una herramienta de seguridad de red escrito para obsevar ataques contra servicios TCP o UDP.

Mailoney:

Honeypot interactivo SMTP que permite entre otras cosas capturar contraseñas y tipos de ataques

Medpot:

Honeypot FHIR es un estándar para el intercambio de datos de atención médica, publicado por HL7

Rdpy:

Honeypot para protocolo RDP escrito en Python emulado cliente y servidor.

Snare:

Es un sensor de Honeypot de aplicación web que atrae todo tipo de actividad de internet.

Tanner:

TANNER es un servidor de clasificación y análisis de datos remotos para evaluar las solicitudes HTTP y componer la respuesta que SNARE entiende.

5. ENFOQUE

El plan va enfocado a la implementación y despliegue de un servidor honeypot dentro del centro de datos de la ESPAM MFL, tomando como referencia la topología de red del data center actual y proponiendo una nueva solución, incorporando el honeypot en un punto estratégico de la red de datos del DMZ, como mecanismo de caza de enemigos y que a través de los resultados obtenidos se hace un análisis comparativo del antes y el después, emitiendo recomendaciones para el buen uso, efectivo y eficiente de la zona desmilitarizada.

La institución cuenta con un ancho de banda de 150 MB, suministrada por CEDIA, dedicada a la comunidad universitaria, y un enlace redundante de 80 MB, contratado con CEDIA de manera inalámbrica vía RADIO como enlace de backup alternativo en caso de caída del servicio principal, para uso del centro de datos, esto permite realizar un balanceo de carga de los proveedores del servicio de internet.

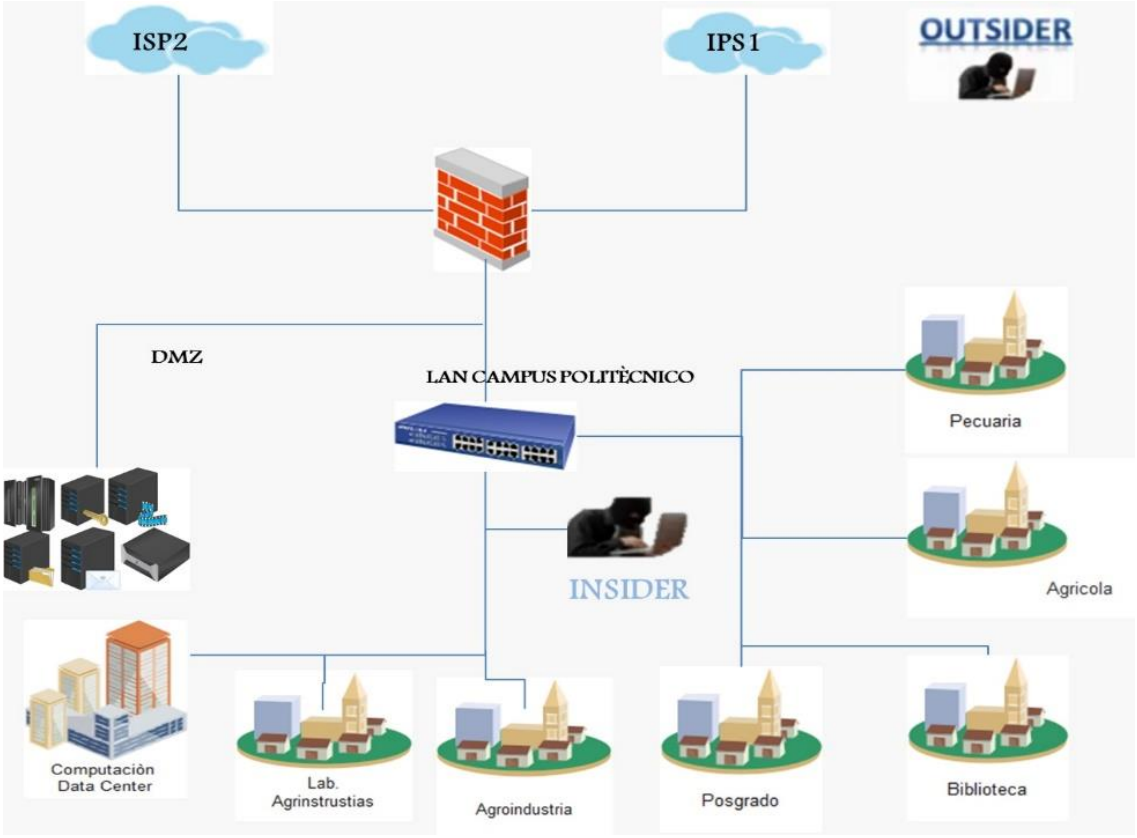


Figura 39. Diagrama de infraestructura actual de la ESPAM MFL

Fuente: C. Moreira, administrador del centro de datos

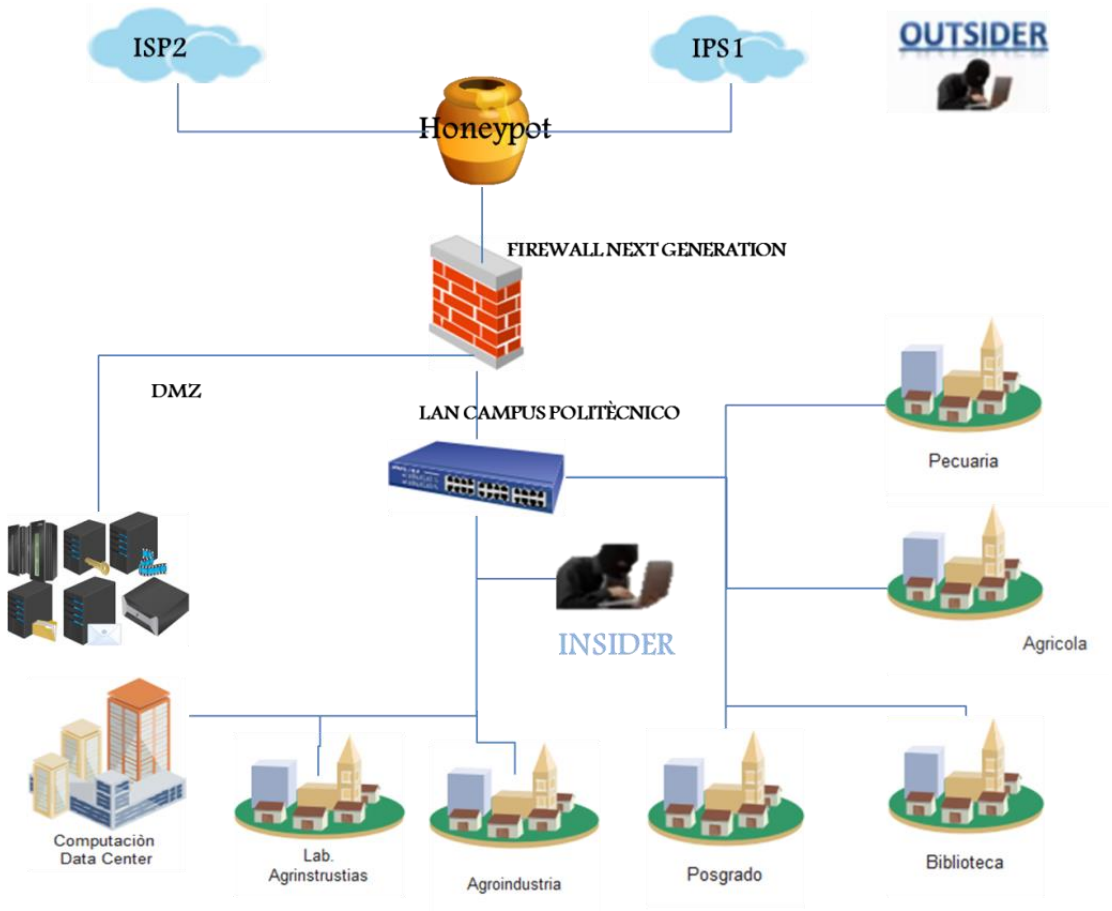


Figura 40. Diagrama de red propuesto para el despliegue del honeypot.

Fuente: Elaborado por el Autor

6. GLOSARIO DE TÉRMINOS

Tabla 11. Glosario de términos

TÉRMINOS	DEFINICIÓN
DMZ	Una DMZ (Zona Desmilitarizada) o Red Perimetral, es una red que se ubica entre la red interna (LAN) de una organización y la red pública (internet) que incorpora segmentos de red para acceder a los equipos internos de la empresa y la red pública (España, 2011).
HONEYPOT	Honeypot es considerado un sistema de tipo “trampa” que sirve para observar los diferentes comportamientos de ciberataques para posteriormente analizar la intrusión y los métodos que se utilizaron (Gonzales, et al. 2019).
CENTRO DE DATOS	El lugar donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización, que adquiere el carácter de Alta Disponibilidad (Arizala y Ortiz, 2010).
HONEYNETS	Se nombra honeynet al software y conjunto de computadores los cuales actúan como señuelo para los atacantes, simulan ser sistemas vulnerables a ataques (Hoyos, J. 2021).
FIREWALL	Un cortafuegos es un dispositivo de seguridad de red que supervisa el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad (CISCO, 2021)
ATAQUES CIBERNÉTICOS	Un ciberataque definido como un delito cibernético puede tener múltiples consecuencias cuya

	gravedad dependerá de cada caso y de la intención del delincuente (Izaguirre, J. 2018).
HOSTS	Un host o anfitrión es un ordenador que contiene datos o programas que otras computadoras pueden acceder de a través de una red o modem, (ECURED, 2017)
CIBERESPACIO	Es escenario espacial que existía al interior de las computadoras y sus interconexiones (Martinez, et, al 2014).
FTP	(siglas en inglés de File Transfer Protocol, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol) (Lopez, J. 2016)
Adbhoney	es un honeypot de baja interacción que usa el protocolo Android Debug Bridge que simula teléfonos, TVs conectados al host (Trajanovski, T. 2021)
Ciscoasa:	Es un honeypot se desempeña a manera de baja interacción en el componente Cisco Adaptive Security Appliance (ASA) capaz de detectar CVE2018-0101
Citrixhoneypot:	este crea un sitio web falso sobre el Protocolo de transferencia Segura de Hipertexto (HTTPS) en donde los posibles atacantes trataran de ingresar usando una forma de autenticación para vulnerar la seguridad de la página (Hänninen.2020)
Conpot:	Es un honeypot de baja interacción, el cual permite emular una infraestructura industrial compleja, siendo fácil su implementación, modificación y extensión. El objetivo es recopilar información sobre los motivos y métodos de los adversarios que apuntan a la entidad u organización (Serrano C y Rúiz M. 2021)

Cowrie:	un Honeypot Cowrie simula ser un servidor SSH y Telnet con una interacción alta, además de registrar las formas en que actúa un atacante para intentar penetrar el sistema (Zymberi, I. 2021)
Dicompot:	es un honeypot que simula un servidor de Imagen Digital y Comunicación en medicina (DICOM) completamente funcional con un toque, el cual es un estándar de transmisión de imágenes médicas y datos entre hardware de propósito médico(Keri, M. 2020)
Dionaea	un honeypot Dionea de baja interacción escrito en C y Python está diseñado para la simulación de servicios que contengan vulnerabilidades (Banfi, J. 2020).
CEDIA	Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia.

7. IMPLEMENTACIÓN DE HONEYPOT EN EL CENTRO DE DATOS DE LA ESPAM MFL

Para la ejecución, se realizaron pruebas de sistemas honeypot con herramientas libres como HoneyDrive_3_Royal_Jelly, pentbox, Dionaea, Cowrie, Tpot demostrando este último ser más ergonómico y con más características para poder realizar una administración centralizada haciendo uso del sistema operativo nativo de debían con demonios honeypot, así como otros componentes de soporte. Esto nos permite ejecutar múltiples demonios honeypot en la misma interfaz de red, manteniendo un pequeño espacio y restringiendo cada honeypot dentro de su propio entorno.

Infraestructura necesaria para el despliegue de T-Pot

Tabla 12.Equipamiento necesario

Características técnicas de hardware	
RAM	8 GB
CPU	4
HD	40 GB
CD/DVD SATA	1
ADAPTADOR DE RED	1 1 a 10 GB
Conexión a Internet	Disponible buen ancho de banda

Fuente: Elaborada por el autor

Herramientas.

Tabla 13. herramientas empleadas

Herramientas de software	Especificaciones
Sistemas Operativo T-pot	Debían Server 5-64 bits
Batería de honeypot	Debían Server 5-64 bits
Honetdrive-3, Pentbox, Dioanaea, Cowrie, T-pot	Debían Server 5-64 bits
Cockpit	Debían Server 5-64 bits
Cyberchef	Debían Server 5-64 bits
Elasticsearch	Debían Server 5-64 bits
Kibana	Debían Server 5-64 bits
SecurityMeter	Debían Server 5-64 bits
Spiderfoot	Debían Server 5-64 bits
Lampiao Server	Debían 10 64 bit
Fristilead	Debían 10 64 bit
Windows 7	Windows 7 64 bits
Pfsense 3.0	Debían 64 bits
Metasploit	Debían 64 bits

Fuente: Elaborada por el autor

Hardenizando del sistema operativo anfitrión

Debido a que esta máquina estará expuesta a potenciales ataques, es conveniente aislar el sistema operativo de la red principal del DMZ, debido a que toda la atención estará definida en los servicios simulados por Honeypot y no en los servicios brindado por el centro de datos. Por ello, se parte de las siguientes medidas de seguridad adoptadas:

- Configuración del firewall pfsense con reglas definidas.

- Cambiar y reforzar la contraseña de usuario.
- Desactivar el usuario root.
- Desactivar servicios innecesarios.
- Actualizaciones del sistema.
- Reforzar el acceso mediante SSH.

8. ANÁLISIS DE VULNERABILIDADES.

Después del despliegue e implementacion del Honeypot, se comprobó su correcto funcionamiento conjuntamente con la bateria de soluciones que integra por lo que se procede a realizar un análisis e interpretación de los datos obtenidos mediante al herramienta maltrail, para establecer conclusiones, la recolección de datos se realizó durante 7 dias a partir de su implemetacion, cabe mencionar que para la produccion diaria de este tipo de soluciones se nececita almacenamiento ilimitado debido a los millones de log que genera.

Como se aprecia en la figura 3, los ataque han sido detectados por la herramineta de defensa, donde se puede verificar la clasificacion de la amenaza que esta intentado perpretar la infraestuctura, se observa que los ataques están siendo dirigidos a la direccion ip dst_port 192.168.200.155 que es la direccion de un servidor dentro del dmz, el puerto por el cual estan tratando de acceder al sistema es dst_port 8000 mediante una conexión tcp.

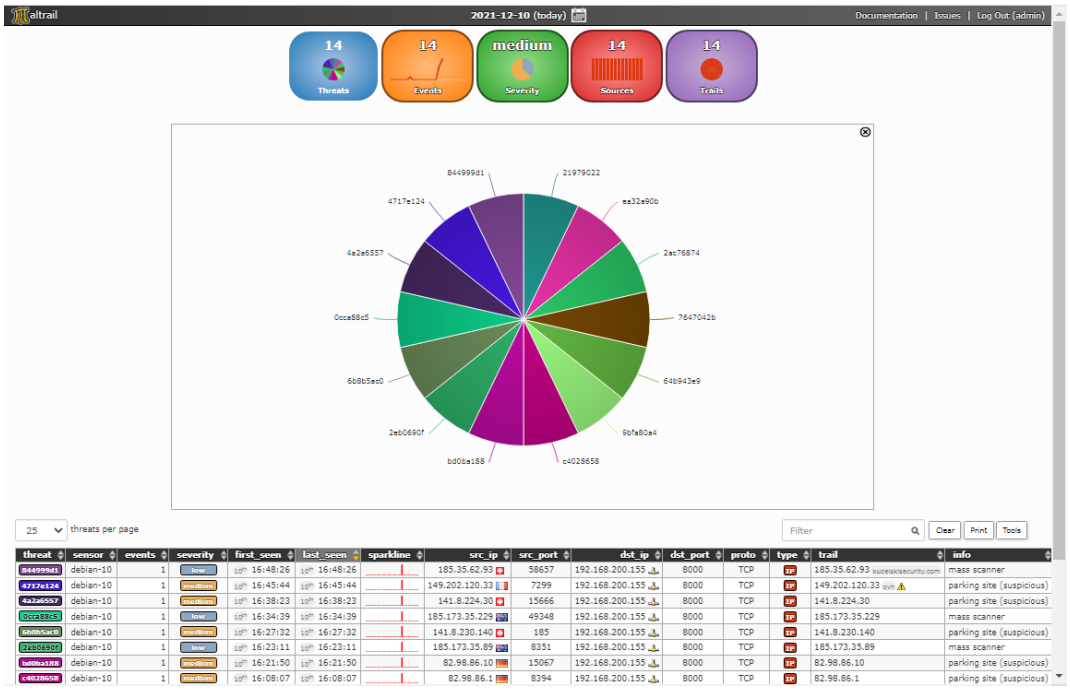


Figura 41. Ataques detectados por la herramienta maltrail

Fuente: Elaborada por el Autor

Como se puede apreciar en la figura 4, todo el tráfico sea este malicioso o sospechoso quedará registrado y podrá ser accedido a través del navegador, cuya interfaz permite filtrar los eventos además de clasificar por nivel de gravedad, mostrar la dirección/protocolo de origen y destino.

Fuente: Elaborada por el autor

Figura 42. Ataques detectados por la herramienta maltrail representación mediante gráficos estadísticos por direccionamiento IP

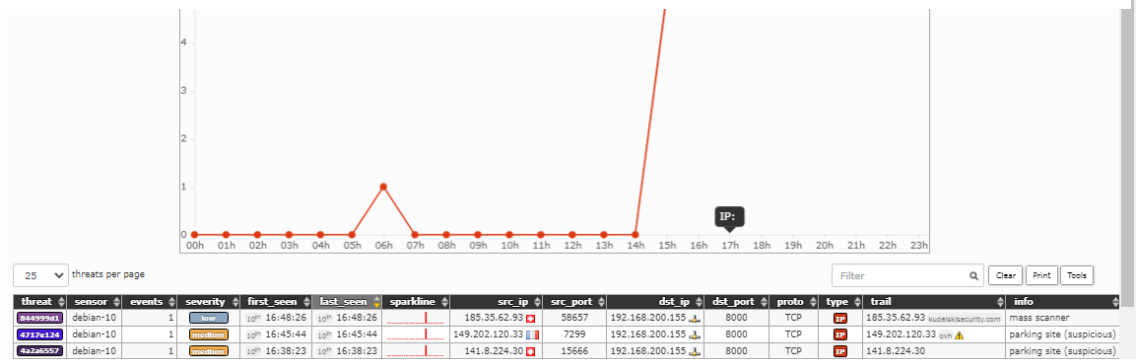


Figura 43. Ataques detectados por maltrail y representando la curva de crecimientos de ataques intensos

La figura 5 muestra la gráfica estadística de los ataques detectados, cabe indicar que se realizaron ataque cibernético en ambiente controla y ataques a la arquitectura de red en ambiente de producción por lo que estos datos son considerados críticos.

Fuente: Elaborada por el autor

En la tabla 4**.** Se puede apreciar el direccionamiento ip que detecta el sistema de monitorización de amenazas, el país del cual proviene el ataque, la ciudad en algunos casos, la latitud, longitud y el proveedor de servicio de internet

Tabla 14. Identificación de ataques detectados por origen, ciudad, latitud, longitud e isp

IP ATACANTE	**PAIS**	**Latitud**	**Longitud**	**ISP**
185.35.62.93	Switzerland	47.144901275635	8.1550998687744	Nagravision SA
149.202.120.33	France	48.858200073242	2.338700056076	OVH SAS
141.8.224.30	Switzerland	47.144901275635	8.1550998687744	Confluence Networks
185.8.230.140	Germany	51.299301147461	9.491000175476	
185.173.35.89	Australia	-33.867198944092	151.199707031255	SoftLayer Technologies
82.98.86.165	Germany	51.299301147461	9.491000175476	Plus.line AG
203.228.100.41	Korea, Republic of	36.28279876709	127.413002014166	Korea Telecom

Fuente: Elaborada por el autor

Como se puede observar en la figura 6. Un ataque generado en un ambiente controlado creo todas las alertas necesarias para tomar las medidas correctivas, ocultando la verdadera dirección ip del atacante.

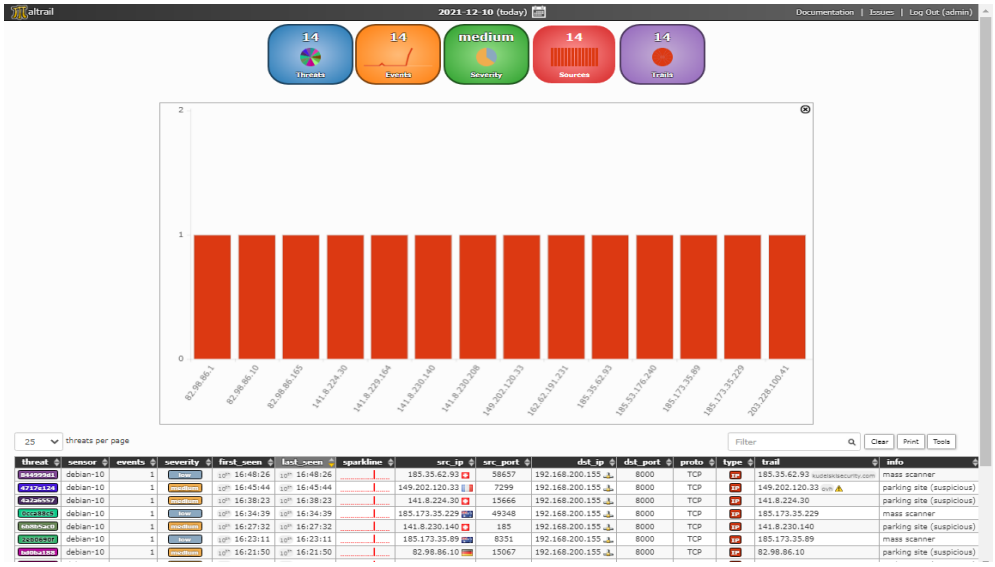


Figura 44. Ataques detectados y representados mediante diagramas de barras por maltrail

Fuente: Elaborada por el autor

Una vez capturados y analizados los ataques, se realizó la implementación de nuevas reglas que permitieron mitigar en su totalidad las brechas de inseguridad presentados durante el despliegue del Honeypot, como se observa en la figura 7 las nuevas reglas comprenden el bloqueo y permisión en las interfaces, LAN, WAN Y DMZ en la ejecución del sistema de detección y prevención de intrusos

REGLAS EN EL FIREWALL EN LA INTERFAZ LAN

State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schendule	Description
0/0B	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none		Regla DNS
0/0B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none		Regla HTTP NAVEGACON
0/0B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none		Regla HTTPS NAVEGACON SEGURA
0/0B	IPv4 TCP	LAN net	*	*	22 (SSH)	*	none		Regla SSH

REGLA PARA HABILITAR EL PUERTO RDP 3389 DEL SYS ADMIN

State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schendule	Description
0/0B	IPv4 TCP	Single host or alias 192,168,1,101	*	*	3389 (RDP)	*	none		Regla RDP SYS ADMIN 3389

CREACION DE REGLAS DESDE LA LAN HACIA EL DMZ

State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schendule	Description
0/0B	IPv4 TCP	LAN net	*	DMZ1 net	1898 (other)	*	none		Regla LAN a DMZ HTTP 1898 Lampiao
0/0B	IPv4 TCP	LAN net	*	DMZ1 net	5900 (vnc)	*	none		Regla LAN a DMZ SERVER VNC 5900
0/0B	IPv4 TCP	LAN net	*	DMZ1 net	445 (SMB)	*	none		Regla LAN a DMZ SERVER SMB 445

HABILITAR REGLAS DE PORT FORWARD EN LA WAN

Interface	Protocol	Source Address	Source port	Dest Address	Dest Port	NAT IP	NAT Ports	Description
WAN	TCP	*	*	WAN Address	1898	10.10.10.50	1898	DNAT Port forward 1898 Lampiao server http
Luego ir a la reglas de firewall a la WAN y activar el log								
WAN	TCP	*	*	WAN Address	HTTP (80)	192.168.1.100	HTTP (80)	DNAT Port forward PUERTO 80 http Metasploit
Luego ir a la reglas de firewall a la WAN y activar el log								
WAN	TCP	*	*	WAN Address	3389	192.168.1.101	3389	DNAT Port forward RDP 3389 Windows 7
Luego ir a la reglas de firewall a la WAN y activar el log								

Figura 45. Nuevas reglas de configuración del IDS/IPS

Fuente: Elaborada por el autor

9. RESPONSABLES

Según la contraloría general del estado en el apartado 410 TI, manifiesta que las instituciones públicas o privadas deben tener una dirección de Tics, el mismo que está conformado por un comité informático precedido por el director, y a su vez tendrá un coordinador de TI, el área tecnológica dispondrá del personal capacitado para las diferentes actividades presentadas en la dirección.

Dentro del orgánico funcional de la ESPAM MFL, no existe esta figura de director sino de coordinador, pero dentro del orgánico estructural del departamento existe una unidad de data center la cual cuenta con un experto en administración de servidores, redes y seguridad, por lo que para el cumplimiento de este plan de fortalecimiento informático deberá ser asignado al coordinador de la unidad de tecnología y el administrador del centro de datos, debido a que en la actualidad no se cuenta con un director de TI.

10. CONCLUSIONES Y RECOMENDACIONES

10.1. CONCLUSIONES

El adecuado uso de la herramienta honeypot T-pot, permitió desplegar la tecnología a toda la infraestructura del centro de datos de la ESPAM MFL, debido a la batería de soluciones honeypot que integra, tanto como para equipos de comunicación como para infraestructura de virtualización.

El diseño de la topología permitió hacer una comparativa del antes y el después, los ataques en su etapa inicial no eran identificado su origen solo se reflejaba la ip destino, puerto destino y servicio al cual iba dirigido pero mediante la implementación del honeypot t.pot se pudo conocer con exactitud los comandos utilizados por el ciber delincuente, ip origen puerto origen, ip destino puerto destino e ubicación geográfica aun cuando el ataque es ramdomico.

La elaboración de la guía de implementación permitió el fácil entendimiento de los mecanismos que integra el honeypot, cuyo despliegue es aplicable como método de prevención de anomalías dentro del cualquier institución que cuente con un centro de datos y una zona desmilitarizada (DMZ), con la finalidad de prevenir ataques cibernéticos.

10.2. RECOMENDACIONES

Se recomienda a la Escuela Superior Agropecuaria de Manabí tener como prioridad la seguridad de la información, basado en herramientas de monitorización de amenazas que permitan detectar anomalías y salvaguardar la información contenidas en el centro de datos.

Capacitar al personal técnico de la unidad de tecnología en temas de ciberseguridad, con la finalidad de conocer los nuevos métodos y vectores de ataques que pueden afectar a la infraestructura tecnológica y por ende a la información que se almacena dentro de los servidores.

Para mantener el control en aspectos de ciberseguridad, es necesario aplicar estrategia y monitoreo constante, para que a futuro los sistemas no sean objetivos

de ataques, y para sus efectos estos controles de riesgos deberán ser mitigados mediante la creación de nuevas reglas dentro del firewall.

11. BIBLIOGRAFÍA

Arizala y Ortiz. (2010). Distribución correcta de computadores desktop en el rack para un gran centro de datos [fotografía]. Recuperado de http://dspace.espoch.edu.ec/bitstream/123456789/557/1/18T00449.pdf

Banfi, J. 2020. «POC: CAPTURA DE MALWARE CON EL HONEYPOT DIONAEA - PARTE I,» UNAM, [En línea]. Available: https://revista.seguridad.unam.mx/numero23/poc-captura-de-malware-con-el-honeypotdionaea-parte-i.

CISCO, 2021. ¿Qué es un cortafuegos?. Disponible en: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Cymmetria, «CiscoASA Honeypot,» Github, 16 Agosto 2018. [En línea]. Available: https://github.com/Cymmetria/ciscoasa_honeypot

ECURED. 2017. Contextos en que es usado el término host. Disponible en: https://www.ecured.cu/Host

España, M. (2011). Guía de Implementación de una DMZ (Zona Desmilitarizada) para la Empresa ITCORP. Dsiponible en: http://repositorio.ug.edu.ec/bitstream/redug/6746/1/TesisCompleta%20-%20354%20-%202011.pdf

Gonzales R, Leaños E, Rodríguez F, Saca R. (2019). Honeypots para la detección de ataques informáticos realizados a instituciones financieras Caso de estudio: Normativa Nacional – ASFI: Disponible en: http://www.utepsa.edu/v2/Descargas/Investigacion/Honeypots%20para%20la%20detecci%C3%B3n%20de%20ataques%20inform%C3%A1ticos%20realizados%20a%20instituciones%20financieras%20Caso%20de%20estudio%20Normativa%20Nacional%20-%20ASFI.pdf

Hänninen,M. 2020. «Organisaation sisäverkon tilannekuvan parantaminen hunajapurkkituotteita hyödyntäen,» Theseus, vol. |, nº 1, p. 41.

Hernández López, M. J. (2007, junio). Practical applications of Honeypots in the protection and monitoring of information networks—ProQuest. https://bv.unir.net:2210/docview/2135188934/B54EF13DEEC04C76PQ/1?accountid=142712

Hernández, M. J., & López, L. (2007, abril). Aplicaciones prácticas de Honeypots en la protección y monitorización de redes de información—ProQuest. https://bv.unir.net:2210/docview/2135188934/7AB9A64F39324BC7PQ/1?accountid=142712

Hoyos, J. (2021). ANÁLISIS DE EFECTIVIDAD DEL USO DE HONEYNET ANTE ATAQUES INFORMÁTICOS APLICADO A PYMES. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/40338/jahoyosb.pdf?sequence=1&isAllowed=y

IONOS, D. G. (2021). ¿Qué es un honeypot? IONOS Digitalguide. https://www.ionos.es/digitalguide/servidores/seguridad/honeypot-seguridad-informatica-para-detectar-amenazas/

Izaguirre, J. 2018. Análisis de los Ciberataques Realizados en América Latina. Disponible en: https://repositorio.uide.edu.ec/bitstream/37000/3782/13/An%C3%A1lisis%20de%20los%20Ciberataques%20Realizados%20en%20Am%C3%A9rica%20Latina.pdf

Keri, M. 2020. «DICOM Honeypot,» Github,. [En línea]. Available: https://github.com/nsmfoo/dicompot

Lopez, J. 2016. Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos en Red. Disponible en: http://dis.um.es/~lopezquesada/documentos/IES_1617/SRI/curso/UT6/UT6.pdf

Martínez L; Ceceñas, P y Ontiveros V. 2014. Virtualidad, ciberespacio y comunidades virtuales. Disponible en: http://www.upd.edu.mx/PDF/Libros/Ciberespacio.pdf

Serrano C y Rúiz M. 2021. «Diseño e implementación de un honeypot en la línea de negocio Facturación electrónica en la empresa jaime torres c y cia,» Bogotá.

Trajanovski, T. 2021 An Automated and Comprehensive Framework for IoT Botnet Detection and Analysis (IoT-BDA), Manchester: School of Computer Science, The University of Manchester, UK,

Zymberi, I. 2021 «Honeypots: A Means of Sensitizing Awareness of Cybersecurity Concerns,»[En línea]. Available: https://www.theseus.fi/bitstream/handle/10024/496070/Zymberi_Ilirjana.pdf?sequence= 2&isAllowed=y