UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Configuración de una honeynet para la evaluación de ataques cibernéticos en un modelo de redes cisco, 2020

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniera de Sistemas

AUTORAS:

Neyra García, Yaritza Yasmin (ORCID: 0000-0002-6064-2692)

Valle Lopez, Susan Yackelin (ORCID: 0000-0002-0984-9313)

ASESOR:

Mgtr. Milner David Liendo Arévalo (ORCID: 0000-0002-7665-361X)

LÍNEA DE INVESTIGACIÓN:

Auditoria De Sistemas Y Seguridad De La Información

PIURA – PERÚ

2022

DEDICATORIA

Dedico esta tesis a mis padres que me han apoyado en todo lo que ellos pudieron a nuestros amigos que estuvieron ahí para apoyarnos muchas gracias, para ellos está hecha esta dedicatoria.

Dedico esta tesis a todos aquellos que creyeron en mí, en especial a mis padres que me han apoyado en todo el transcurso del desarrollo de mi tesis de manera moral y económica, igualmente mi amigo Maicol Sullón por su apoyo cuando lo necesitábamos y a nuestros amigos que nos motivaban a seguir, muchas gracias, para ustedes le dedico esta tesis.

AGRADECIMIENTO

Principalmente a nuestro asesor el Mgtr. Milner David Liendo Arévalo por ser la guía para lograr culminar nuestra tesis.

También a los docentes de la Escuela Académico Profesional de Ing. de Sistemas, en especial al Ing. Teófilo Correa que nos proporcionó ayuda en conocimientos y a nuestra universidad Cesar Vallejo- Filial Piura.

Índice de Contenidos

DEDICATORIA ii
AGRADECIMIENTO iii
RESUMEN vi
ABSTRACT vii
I. INTRODUCCIÓN 1
II. MARCO TEÓRICO 5
III. MÉTODO 15
3.1. Tipo y Diseño de Investigación 15
3.2. Variables y operacionalización 17
3.3. Población, muestra y muestreo 17
3.4 Técnicas e Instrumentos de recolección de Datos 18
3.5 Procedimiento 19
3.6 Método de Análisis de datos 20
3.7 Aspectos Éticos 20
IV. RESULTADOS 21
V. DISCUSIÓN 28
VI. CONCLUSIONES 31
VII. RECOMENDACIONES 32
REFERENCIAS 33
ANEXOS: 36

Índice de tablas

Tabla 1 Clasificación de Ataque 13
Tabla 2 Prueba de ataques e intrusiones 21
Tabla 3 Prueba de ataques a servicios de red 24
Tabla 4 Vulnerabilidades 25

Índice de gráficos y figuras

Gráfica 1 Intrusiones Pretest - Posttest 22
Gráfica 2 Tipos de ataques 22
Gráfica 3 Exploits y malware pre y post 23
Gráfica 4 Ataques a servicios de red 24
Gráfica 5 Procedencia de los ataques 25

Figura 1: Esquema Organizacional de la Honeynet..... …..12
Figura 2: Esquema de Prueba pre-.test y post-test 16

Índice de Ilustración

Ilustración 2 Red Pretest 26
Ilustración 3 Red Post Test Con HoneyPot 26
Ilustración 4 Nube de etiqueta de usuario y contraseña 27

RESUMEN

Esta investigación se plantea como objetivo principal, determinar la configuración de una Honeynet para la evaluación de ataques cibernéticos en un modelo de redes cisco 2020. En cuanto a la metodología, el tipo de investigación es aplicada y estudio de tipo descriptivo. Se utiliza la Honeypot, como tecnología que propone en una red local aplicaciones y servicios en estado de vulnerabilidad, como una trampa denominada Honeynet, que se utilizó para monitorear los eventos y estudiar intentos de intrusión.

En lo que respecta a los resultados del diseño propuesto se analizó y selecciono el tipo de Honeynet, en base al contexto actual de la red de datos, se implementó servidores y se configuró servicios de directorio activo, dns, dhcp, ftp, servidor de archivos y web. La información capturada sirvió para determinar patrones de conexión que permitieron identificar ataques y servicios susceptibles a ser atacados con la finalidad de proteger en forma proactiva los elementos que componen las redes de producción. En lo que respecta a sus conclusiones se tiene que se recomienda la honeynet virtual autocontenida, cuando los recursos de hardware son limitados, además el uso de software de código abierto proporciono facilidades a la libre adaptabilidad de la honeynet en la investigación.

Palabras Clave: Honeypot, honeynet, ciberataques, vulnerabilidades

ABSTRACT

He main objective of this research is to determine the configuration of a Honeynet for the evaluation of cyber attacks in a Cisco 2020 network model. Regarding the methodology, the type of research is applied and descriptive study. The Honeypot is used as a technology that proposes applications and services in a state of vulnerability in a local network, such as a trap called Honeynet, which was used to monitor events and study intrusion attempts. Regarding the results of the proposed design, the type of Honeynet was analyzed and selected, based on the current context of the data network, servers were implemented and active directory services, dns, dhcp, ftp, file server were configured. and web. The information captured was used to determine connection patterns that made it possible to identify attacks and services susceptible to being attacked in order to proactively protect the elements that make up the production networks. With regard to its conclusions, the self-contained virtual honeynet is recommended, when hardware resources are limited, in addition the use of open source software provided facilities for the free adaptability of the honeynet in research.

Keywords: Honeypot, honeynet, cyber-attacks, vulnerabilities

I. INTRODUCCIÓN

Durante este periodo de emergencia mundial causada por la pandemia del COVID-19 muchas usuarios de red y empresas se han vuelto víctimas de los llamados ciberdelincuentes, los cuales con diversas habilidades y técnicas son capaces de poder acceder a nuestra información íntima y financiera y a su vez crear diferentes páginas web con el objetivo de suplantar la identidad de marcas o entidades conocidas y así poder engañar a los consumidores tal como se detectó con la creación de una supuesta página web de la OMS que tenía el objetivo de robar dinero y datos de las personas que aportaban en dicho portal web, también están aquellos que son capaces de ingresar al sistema de una empresa y robar información valiosa, tal como le ocurrió a la empresa de entretenimiento HBO quien sufrió el robo de varios capítulos de su serie "Juego de Tronos" los cuales fueron subidos a la red pese a que esta empresa cuenta con sistemas de seguridad la cual fue vulnerada por los piratas informáticos a través de nuevos ataques que no estaban dentro del catálogo de registros de ataques del sistema (Versatile virtual honeynet management, 2016). Ante este tipo de actividades existen herramientas que no son utilizadas para la seguridad informática, debido a que las personas no tienen conocimiento sobre ello o simplemente ignoran la utilidad de estas herramientas siendo una de ellas la Honeynet, la cual tiene la función de actuar como un señuelo esperando a que un ciber atacante trate acceder a la red de datos y genere algún daño permanente o robe información de acceso privado con la cual hace mal uso (HoneyMix: Toward SDN-based Intelligent Honeynet, 2016). Ante esto algunas organizaciones invierten grandes cantidades de dinero en diferentes sistemas de seguridad, que brindan la protección necesaria para sus empresas, pero estas solo están preparadas para ataques ya conocidos demostrando así una gran vulnerabilidad ante nuevos ataques informáticos, de ahí surge la idea de usar honeynets pues a través de esto podemos estudiar el comportamiento del atacante, de donde proviene el ataque y que tan grave es, y con esta información recolectada poder estudiarla y analizarla para poder tomar

diferentes medidas y generar protocolos que sirvan para contrarrestar los ataques y poder defenderse ante ataques futuros (Verdejo Alvarez, 2016).

Por ende con la implementación de Honeynet se puede crear un sistema con equipos vulnerables para atraer a los atacantes, esto nos va a poder permitir analizar y conocer las vulnerabilidades de nuestro sistema, conocer las nuevas técnicas y herramientas de ataque desconocidas hasta ahora para nosotros, desviar la atención del atacante para salvar el sistema principal, disuadiéndolo y ganar tiempo para tomar las medidas necesarias para poder reaccionar y rechazar el ataque y localizarlo (HONEYPROXY: Design and Implementation of Next-Generation Honeynet via SDN, 2018) . Sin embargo, la realidad nos muestra que, aunque las amenazas a las redes han ido en aumento las empresas poco o nada han hecho por cubrir aquellas vulnerabilidades exponiéndose, a los ciberataques y robo de información confidencial y esto ha empeorado ahora que estamos en tiempos de crisis por la pandemia mundial lo cual demuestra cuan indefensa son las redes ante ataques cibernéticos (Taxonomy of Honeynet Solutions, 2015). De igual manera se observa que en las municipalidades y organizaciones del estado son vulnerables a ataques y robo de información debido a la falta de cultura en ciberseguridad, viéndose expuesta a constantes ataques como ejemplo se tuvo a la municipalidad distrital de Huambos-Trujillo la misma que es muy propensa a posibles ataques cibernéticos, técnicas de ataque tales como: desbordamiento de memoria, secuestro de la sesión, denegación del servicio, fuerza bruta y ataques de diccionario utilizando métodos como el rompimiento de claves, a través de estos se pudo analizar cuál era la situación de vulnerabilidad en la que se encontraba la municipalidad de Huambos (Harlyn Mayanga, 2018). En nuestra realidad se observa que muchas empresas y organizaciones están expuestas a ciberataques exponiendo sus datos confidenciales; y que solo reaccionan cuando el ataque ya sucedió y poco o nada hacen para prevenirlo (Software-Defined HoneyNet: Towards Mitigating Link Flooding Attacks, 2017).

Esta lo que respecta a su justificación teórica Palmay López (2017), concluye que una Honeynet, es una red de computadoras más compleja, que permite que el atacante pueda acceder a más información, por la disposición de sistemas dispuestos para ser atacados, y por lo mismo tiene la funcionalidad de recopilar más datos acerca del ataque. Se realiza una investigación con el propósito de aportar conocimiento existente sobre el uso de las Honeynet, como instrumento para la ciberdefensa con el objetivo de ser atacada y recaudar así más información sobre la interacción de los atacantes con el sistema (Giraldo Giraldo, 2015).

Su justificación practica se debe a la existencia de la necesidad de indagar más acerca del uso de las Honeynet en un contexto más controlado, empoderando la gestión de sus procesos internos al que simula la trampa, así como la utilización de equipos reales cuyos resultados podrían ser estudiados y analizados, para ser incorporado como conocimiento a las ciencias de la ciberseguridad de datos y que estas sirvan para que las organizaciones puedan tomar las medidas necesarias en sus protocolos de seguridad por el bienestar de la empresa, además sirve para evitar futuros ataques similares, mediante la implementación de políticas de seguridad, facilitando de forma eficiente y eficaz gestionar la seguridad de la información por una red de datos (Palmay López, 2017).

En cuanto a la justificación Metodológica, para el desarrollo de la investigación, se utilizaron modelos, técnicas y tipos de ataque, haciendo uso para su valoración técnicas de investigación cuantitativa orientado al análisis y síntesis de los datos recogidos en la Honeynet. Se aplica una serie de fases para su configuración en un ambiente controlado para no afectar las redes de producción en el estudio, con el propósito de conocer las diversas técnicas y métodos que se utilizan lograr vulnerar la seguridad de una organización (W. Zhang, y otros, 2020).

Se buscará dar respuesta a la siguiente pregunta, ¿Como se configura una Honeynet para la evaluación de ataques cibernéticos en un modelo de redes cisco 2020? Los problemas específicos de la investigación fueron los siguientes:

¿Cómo se implementa la Honeynet para la evaluación de ataques e intrusiones en un modelo de redes cisco 2020?

¿Cómo se configura la Honeynet para la evaluación de ataques a los servicios de red en un modelo de redes cisco 2020?

¿Cómo se evalúan las vulnerabilidades de la red mediante una Honeynet, en un modelo de redes Cisco 2020?

Como objetivo general se formula: Determinar la configuración de una Honeynet para la evaluación de ataques cibernéticos en un modelo de redes cisco 2020, y en lo que respecta a los objetivos específicos se tienen los siguientes:

Determinar la Honeynet para la evaluación de ataques e intrusiones en un modelo de redes cisco 2020

Configurar una Honeynet para la evaluación de ataques de los servicios de red en un modelo de redes cisco 2020

Determinar las vulnerabilidades mediante una Honeynet, en un modelo de redes Cisco 2020.

Para esto se plantea la siguiente hipótesis general de la investigación: La configuración de una Honeynet mejora la evaluación de ataques cibernéticos en un modelo de redes cisco 2020 y como hipótesis especificas se tiene las siguientes:

La implementación de la Honeynet mejora la evaluación de ataques e intrusiones en un modelo de redes cisco 2020

La configuración de una Honeynet mejora evaluación de ataques de los servicios de red en un modelo de redes cisco 2020

La determinación de las vulnerabilidades mejora con una Honeynet, en un modelo de redes Cisco 2020. (Flores Guerrero, y otros, 2018).

II. MARCO TEÓRICO

En lo que respecta a los antecedentes se describen antecedentes, que dan a conocer información relacionada a el tema de investigación, como sistemas de detección de ataques informáticos, configuración de Honeynet para determinar formas de ataques e investigaciones para la detección de código malicioso Backdoor y DDoS (Matías Koller, y otros, 2015). Las teorías relacionadas están enfocadas a definir la Honeynet, Honeypot, ciberataque, asimismo la clasificación de los ataques y en el marco conceptual el uso de la Honeynet, Las armas cibernéticas, seguridad informática, agente, sistema Multi-Agente, tipos de seguridad, virtualización, tipos de Honeynet y detección de intrusos (Tirado Ríos, y otros, 2017).

En los antecedentes tenemos un sistema de redes de datos de empresas, para detectar ataques, así mismo Honeypot para la corrección de vulnerabilidades, diseño e implementaciones utilizando software libre y detección de amenazas de código malicioso

Según Flores Guerrero, y otros (2018), en su tesis titulada “Sistema para la detección de ataques a redes de datos de empresas soportado en HoneyPots”, el objetivo principal fue la implementación de un sistema para el análisis de información en redes de empresas, de los datos obtenidos de los atacantes en los honeypots. La metodología que permitió el desarrollo de este proyecto investigativo tuvo carácter aplicado, bibliográfico y experimental. Entre sus conclusiones se tiene que este sistema de detección brinda información procesada, simple y grafica de las actividades de los intrusos que ingresen a la red, y facilita la toma de medidas preventivas sobre futuros atacantes, además de poder actualizar las políticas de seguridad para evitar replicas o ataques con patrones similares. Se recomienda Mejorar los plugins para incrementar la interacción con los atacantes, el plugings SIP´y Protección antiDDoS.

Según Harlyn Mayanga Adrián Narciso (2018), en su tesis de Implementación de una Honeypot, para corregir vulnerabilidades en la red de comunicaciones de la Municipalidad Distrital de Huambos”, realizada en la Universidad Señor de Sipán**.** El objetivo principal fue implementar una

Honeypot sobre la red de la municipalidad para detectar y corregir las vulnerabilidades. Se estudio el desarrollo de la Honeypot en un entorno real dentro una organización, desde su implementación y configuración a su posterior análisis de funcionamiento en donde evalúa si la Honeypots es capaz de cumplir sus funciones correctamente frente al ataque de un intruso y cómo reacciona ante ello. Se utilizo el método de observación, documentación junto al uso de niveles de operadores en un sistema SIAF, obteniendo como resultados comparativos que de los 750 ataques previamente registrados antes de la ejecución de la honeynet los cuales obtuvieron como resultado que solo el 15% de ataques ingreso a la red marcando una gran diferencia con el primer resultado anterior en donde un 79% había ingreso antes de la configuración de la honeynet, con esto se obtuvo como resultado final que un 85% de los ataques no tuvo éxito, mejorando desde de la implementación de la Honeynet, obteniendo como conclusión final que se logró el éxito de la implementación de esta herramienta. (Harlyn Mayanga, 2018)

Según Heredia Terán, Carlos Mauricio (2016) en su tesis titulada de implementó una Honeynet sobre la red de comunicaciones de datos, utilizando software Libre en la Universidad Nacional de Loja, en Ecuador. El objetivo es diseñar e implementar una honeynet con el fin de que esta logre reunir información sobre los movimientos del intruso, asimismo detecte que vulnerabilidades posee la red de la UNL antes de que el atacante saque provecho de esta y conociendo los riesgos a los cuales los sistemas se están exponiendo. Esta investigación expone que base debe tener una honeynet virtual para lograr una excelente funcionalidad, con un buen diseño de una topología de la honeynet, luego se puedo implementar en un área de trabajo para que con su posterior uso pueda conocer los riesgos que presenta una red ante una posible amenaza. Se utilizó los métodos de observación y documentación y se obtuvo como resultado que fue exitoso en razón de que con la implementación de la honeynet se pudo determinar los servicios vulnerables, intrusiones y el porcentaje de tráfico que circula por esta, para que a partir de estos se generen normas que brinden más seguridad a la red. (Heredia Terán, 2016)

Según Arequipa Chiquito, Mónica Paulina y Guañuna Quilligana, Juan Andrés (2017)**,** diseñaron una Honeynet en un servidor web, enrutado con OSPFv2, para la detección de código malicioso, DDoS y Backdoor; realizada en la Universidad Politécnica Salesiana Sede Quito**.** El objetivo principal es analizar y diseñar una honeynet de baja interacción, con el fin de estar alerta ante amenazas de código malicioso, troyanos y ataques de denegación en una red MPLS conectada con OSPFv2 la cual brinda servicios de comunicación en una red. En esta investigación se puede conocer la configuración de una honeynet, en la cual no se necesitan herramientas de última tecnología, para que este método de seguridad logre ser una herramienta de apoyo en las diferentes organizaciones, con el fin de poder obtener conocimiento de los medios utilizados por el atacante sin ser detectado, dando oportunidad a que las organizaciones elaboren medidas de protección necesarias ante estas situaciones. En este proyecto de tesis se logró concluir con éxito el diseño de esta herramienta según los resultados evaluados a través del análisis global de ataques realizados, con el ataque de denegación, el honeywall al recibir cada paquete realiza una alerta mientras que, con el código malicioso, backdoor y DDOS realizados de forma independiente el ataque de denegación de servicio ingresa a través de otro puerto.

Según Azizov, (2020) realizó una investigación denominada Arquitectura DMZ Perimetral: Una implementación corporativa; su objetivo principal fue implementar una arquitectura DMZ Perimetral corporativa. Entre sus conclusiones tenemos, que el enfoque principal de las pruebas realizadas ha sido demostrar la viabilidad y la funcionalidad de los componentes integrados en el sistema. La cohesión de los diversos sistemas y componentes en el sistema ha sido el mayor desafío para poder llevar a cabo el proyecto. La exploración del sistema de cortafuegos integrado ha sido definitivamente el elemento más explorado de todo el sistema, donde se han estudiado diversas herramientas, tanto integradas como opcionales que las componen. **Matías Koller, y otros** (2015) realizó una investigación denominada cuyo objetivo fue la implementación de una honeynet sobre los servicios de VoIP, para analizar los datos de los ataques y desarrollar las mejoras pertinentes. Entre

sus resultados se tiene que se aplicó sobre un sistema honeypot Artemisa, herramientas con diversas tecnicas y metodos de ataque para comprobar la eficacia y desempeño en la deteccion de intrusiones. Los tipos de ataques fueron escaneo de internos, Ataques por Flooding y Ataques por escaneo. Se determinó que, en la central Philips del gobierno de Córdoba, el 75% de los ataques fueron de flooding. Entre sus conclusiones se tuvo que la Honeynet, no quedó indispuesta en cuanto a su funcionalidad, por falta de recursos, ante los constantes ataques a su red de datos.

Tirado Ríos, y otros (2017) realizó una investigación de seguridad Informática, como un mecanismo de salvaguarda de la información en las empresas, el objetivo fue el análisis de técnicas y métodos de ataques más utilizados por hackers y su consecuente forma de prevención o de mitigación en las empresas. Entre sus resultados determinó que el ataque de fuerza bruta, fue el más relevante en las intrusiones en UNAN-CERT. Y en sus conclusiones describe que el ataque de fuerza bruta, se realiza mediante diversas herramientas, por lo que se creó la denominada "regla de los tres strikes", que consiste en un bloqueo de los 03 intentos de intrusión.

Valdiviezo Avalo (2020), en su investigación se planteó mejorar la detección de intrusiones mediante el desarrollo de una Red Honeypot para la Municipalidad Distrital de Víctor Larco Herrera. Entre los resultados tenemos que el número de vulnerabilidades sin la red Honeypot disminuyó de 23 y con la red Honeypot 18, el número de Intrusiones Identificadas sin la red Honeypot incremento de 0 a y con la red Honeypot se obtuvo 3. En las conclusiones se consiguió mejorar la detección del 100% de intrusiones con el desarrollo de una Red Honeypot en la infraestructura de Red de la Municipalidad Distrital de Víctor Larco Herrera. determinar el número de intrusiones en la Infraestructura de Red de la Municipalidad, logrando detectar el 100% de intrusiones

Campoverde Armijos (2017), cuyo objetivo fue la implementación de dos Honeypot y analizar los posibles ataques que cada uno de ellos pueden recibir en un entorno corporativo. La metodología utilizada fue de análisis forense consiste en la recopilación de evidencias luego de corroborar que los sistemas informáticos han sido atacados. En los resultados se tuvo que

realizar un ataque, primero se ejecutó un escaneo de la maquina víctima para revisar cuales son los puertos y servicios que están corriendo, el atacante con sistema operativo Kali Linux con permisos de superusuario, se utilizó la herramienta medusa para el acceso a servidores ssh a través de fuerza bruta, ataques de inclusión remota de archivos (RFI) y ataque a través de un escáner de vulnerabilidades. En sus conclusiones Podemos afirmar que se cumplieron los objetivos propuestos en este trabajo, dado que se implementaron dos tipos de Honeypot en una arquitectura de red virtual, se recabó información de los posibles tipos de ataques, se usó una herramienta externa para mostrar estadísticas y obtener información acerca del tipo de ataque que se ejecutaron.

Martínez Contreras (2018), cuyo objetivo fue determinar los alcances de los procesos de monitorización de los ataques en una Honeypot. En cuanto a los resultados se configuró una honeypot sobre una red de comunicación de datos, con la implementación de políticas de seguridad para conceptualizar los alcances de esta. En cuanto a sus conclusiones se logra la conceptualización de los honeypot en un ambiente controlado, mediante la identificación, el conocimiento y comprensión de las técnicas y métodos de ataque en la red, así como el comportamiento de los atacantes.

Urcuqui¸Christian, y otros (2017), cuyo objetivo fue determinar clasificadores de aprendizaje automático para detectar malware en sitios web. Entre sus resultados se tiene que de los datos obtenidos de la capa de aplicación podemos deducir lo siguiente: el tamaño promedio de las URL es más mayor en las maliciosas (benignas 53,31 y malignas 85,45), que el número de caracteres especiales es mayor en las páginas maliciosas (benignas 10,81 y maliciosas 17,20), se presentan mayores índices de servidores maliciosos en Apache y NGINX. Entre sus conclusiones se tiene que gran parte de los honeypots hoy en día son deficientes en la documentación y también en sus actualizaciones, además se tiene que a través de un honeypot de baja interacción y un conjunto de datos reciente, es posible identificar una página web maliciosa con un resultado de exactitud del algoritmo J48 del 98,76 % con todas las características y un 96,05 % para solo tres variables.

Gaona-García, y otros (2016) plantearon la implementación en escenarios de trabajo de honeynet de un modelo ontológico para identificar tipos de ataques más comunes. En los resultados se tiene que como parte del modelo ontológico que se planteó, se creó una propiedad llamada Tiene riesgos, que deriva de las clases, que se generan de acuerdo a la cantidad de ataques que se escogen, los mismos que se les asigna propiedades y constructores. Entre sus conclusiones se utiliza razonadores ontológicos, los mismos que están relacionados a los ataques a la seguridad web, creándose instancias **Jurado Pallarés (2016)** cuyo objetivo fue realizar un análisis de las intrusiones al integrar diferentes Honeypots en una red Honeynet. Entre los resultados en los 30 días de investigación, se detallan tanto los sensores de la Universidad Autónoma de Madrid y de una red domestica; se contabilizó 496493 ataques, 59847 ataques Secure Shell, 82041 a Servicios Web y 354605 ataques a Telnet. Según la estadística de ataques existe un 30% de ataques internos, además de un gran porcentaje de SQL injectionl. Se concluye que las Honeynets, son herramientas de gran utilidad para descubrir técnicas y métodos de ataques, así como lograr identificar patrones de uso tanto internos como externos.

Cuesta-Quintero, y otros (2018) cuyo objetivo fue el diseño de un sistema de detección de intrusos a través de una red Honeynet para entornos de red cableada sobre IPV6. Entre los resultados de los ataques TCH-IPv6 a nivel de enlace local realizados durante las pruebas y detectados por 6Guard, en el caso de un enfoque más específico de atacantes, se produciría un problema para detectar un ataque RA / NA falso debido a la ausencia de un puerto espejo de conmutación, a pesar de que el principio de ataque sigue siendo el mismo. El módulo Globalpot fue el más activo en la detección de ataques, mientras que solo hubo informes esporádicos del módulo Análisis de eventos. En sus conclusiones se tiene que la ejecución y visualización de los ataques a través de la Honeynet se realizó satisfactoriamente excepto en algunos casos en donde para 6Guard, su precisión de detección disminuye. Estas imprecisiones se deben a falta de funciones mínimas como por ejemplo el Puerto Espejo. Sin embargo, esto no es obstáculo para el Honeypot en reconocer información de los ataques.

De Diego de Diego, y otros (2017), cuyo objetivo fue el diseño de una Honeynet para el análisis del tráfico y muestras de malware, cuyo objetivo principal fue identificar y clasificar diferentes muestras de malware. Entre sus resultados que en la honeypot de tipo Kippo, se relaciona con ataques de fuerza bruta, de zonas con IP de la zona de Asia y los análisis de malware, provenientes de otros países con alta incidencia en estados unidos. En lo que respecta a sus conclusiones que es esencial asegurar nuestros sistemas, recibimos numerosos ataques diarios, por ello, es imprescindible el sentido común para evitar ataques de ingeniería social, además de una sólida política de seguridad para evitar estos tipos de ataques.

En cuanto a las teorías relacionadas se tiene a la Honeypot, Honeynet, vulnerabilidades en redes, IP v4, ciberataque, la clasificación de ataques y simulación de red y virtualización. La metodología aplicada para el desarrollo de la investigación es la metodología de Hacking Ético.

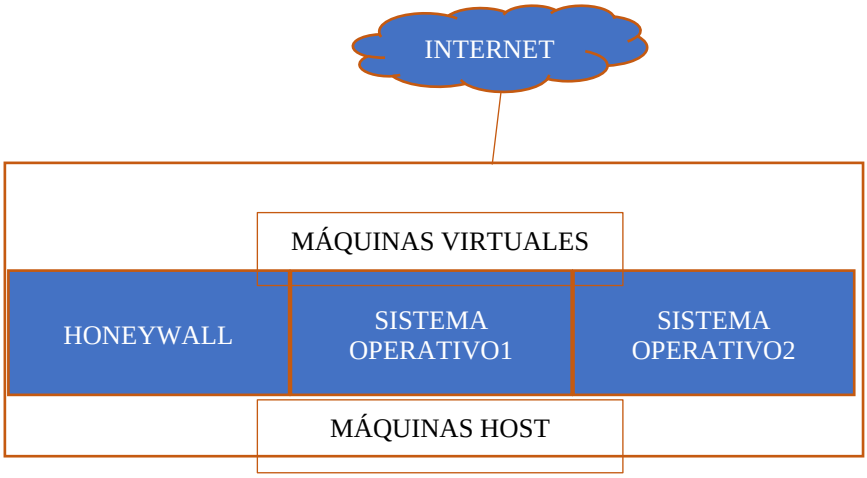
Una honeypot, es una herramienta que actúa como una trampa para un atacante donde este interactúa con ella dándose a ver con vulnerabilidad y de esta manera el delincuente informático piensa que está atacando al servidor, con el propósito de hacer un análisis acerca de donde viene el ataque y los datos obtenidos de este (Pimenta Rodrigues, y otros, 2017). Las honeynets son el conjunto de varias honeypots de media o alta interacción la cual está constituida por una red de sistemas, con el propósito de ser empleada para contrarrestar los ataques que puedan sufrir una red o un sistema y así aprender sobre las herramientas, actividades y motivos que alientan a este tipo de usuarios atacantes. (Correa Guerrero, 2016) Una honeynet, es una red de computadoras más compleja, que permite que el atacante pueda acceder a más información ya que tiene más sistemas dispuestos para ser atacados, y por ende tiene la funcionalidad de recopilar más datos acerca del ataque (W. Zhang, y otros, 2020).

La vulnerabilidad en redes, es una característica de debilidad de una red de datos, la cual es susceptible de ser explotada por una amenaza, intencional o accidentalmente, permitiendo que se pueda acceder a información de acceso privado, debido a que la red presenta puntos críticos débiles. (Voutssas M., 2010)

IPv4, en la actualidad cumple con la funcionalidad de transferir datos desde una red hacia otras, de esta manera proporcionando conexiones entre diferentes equipos informáticos basados en direcciones IP. (Ortega Bernal, 2010)

Un ciberataque, es la violación o acceso a información privada de una organización. Así mismo como las diferentes modalidades utilizadas por intrusos, ciberdelincuentes o hackers para vulnerar un sistema informático. (Dios León, y otros, 2018)

Figura 1: Esquema Organizacional de la Honeynet



Según la naturaleza de los ataques, la clasificación más común es pueden clasificarse en: Ataques pasivos donde ocurren intrusiones en un sistema sin consecuencias, por lo general se hacen para demostrar las vulnerabilidades de un sistema y también los ataques activos ocurre la intrusión al sistema para dañarlo, modificando o eliminar archivos, son ataques más perjudiciales y con consecuencias más graves (Carcelén Méndez, y otros, 2017).

Según los efectos o daños que podrían incurrirse en forma ilícita, los daños son los siguientes: Acceso, modificación e interrupción, denegación de servicio, falsificación y de configuración.

Acceso, es la manipulación de los recursos informáticos. Aquí tenemos eavesdropping, técnica que consiste en ser casi imperceptible en el momento de su ataque, para escuchar en forma secreta el tráfico de una red. Snooping, consiste en interceptar información privada de una red sin modificarla.

Modificación, consiste en acceder para modificar la integridad de la información; tenemos Hombre en medio, donde el atacante es capaz de escuchar, modificar y retransmitir el tráfico de una red. Fuerza bruta, procedimiento utilizado para determinar las contraseñas de acceso a un sistema o servicio. Tampering es la modificación o eliminación sin autorización de los datos. Interrupción, se tiene la denegación de servicio, consiste en atentar con la disponibilidad de las redes, imposibilitando el uso de los servicios y recursos de la red. Denegación de servicio distribuido, su propósito es lograr rebasar la capacidad de procesamiento de los equipos y el ancho de banda de la que se dispone. Falsificación, tenemos IPSpoofing cuyo propósito es suplantar o clonar la dirección IP para tener el beneficio de la confianza entre dos hosts. Configuración, el escaneo de puertos para recopilar información de potenciales víctimas recopilando información de puertos abiertos, cerrados o protegidos por el sistema. Asimismo, el escaneo de vulnerabilidades, para determinar deficiencias en los sistemas operativos y aplicaciones (Dios León, y otros, 2018).

Tabla 1 Clasificación de Ataque

ATAQUE	RED DE DATOS	SERVIDORES	EQUIPOS	SELECCIÓN
Parásitos	SI	SI	NO	NO
Virus Macro	SI	SI	NO	NO
Troyano	SI	SI	NO	NO
Bombas lógicas	SI	SI	NO	NO
Gusanos	SI	SI	NO	NO
Applets malignos	SI	SI	NO	NO
Ingeniería social	NO	SI	NO	NO
Shoulder surfing	SI	SI	NO	NO
Puertas traseras	SI	SI	SI	SI
Exploit	SI	SI	SI	SI
Shell	SI	SI	SI	SI
Ataques de autentificación	SI	SI	NO	NO

Ip splicing	SI	SI	NO	NO
Programas trampa	SI	SI	NO	NO
Fuerza bruta	SI	SI	NO	NO

El PROYECTO requiere del siguiente equipamiento: 01 Router Cisco, 01 Switch de 04 puertos, 02 Tarjetas de red PCI 10/100, 02 laptops y 02 pcs de escritorio. En cuanto al marco conceptual se conceptualiza el uso de la Honeynet, Las armas cibernéticas, seguridad informática, agente, sistema Multi-Agente, tipos de seguridad, virtualización, tipos de Honeynet y detección de intrusos.

Ataques informáticos, un ataque es toda aquella acción que comprometa e implique la violación de la seguridad, confidencialidad, integridad o integridad de un sistema de información. Asimismo, como técnicas que utilizan los intrusos, hackers o crackers para explotar las vulnerabilidades que presente un sistema, aplicación o red de comunicación de datos (Dios León, y otros, 2018).

III. METODOLOGÍA

3.1. Tipo y Diseño de Investigación

3.1.1. Tipo de Investigación

Por el tipo de investigación, tiene las características metodológicas de una investigación aplicada. Según Esteban Nieto (Esteban Nieto, 2018) se denomina así, porque basada en la investigación básica o pura, se formularon hipótesis de trabajo, con el propósito de encaminar una solución en la vida practica de la sociedad. El desarrollo de esta investigación se realiza para dar a conocer el funcionamiento de una herramienta de ciberseguridad denominado Honeynet que no son más que conjunto de varias Honeypots de alta interacción que actúan sobre una red entera, diseñada para ser atacada y poder así recobrar y extraer información valiosa sobre posibles atacantes y sus métodos de ataque y ubicación (Versatile virtual honeynet management, 2016). El uso y aplicación de las Honeynet permite poder detectar los nuevos métodos e interacción de ataque, después de ser atacado se recolecta la información de los datos obtenidos y estos son procesados, estudiados y analizados con el objetivo de implementar un plan de medidas para la seguridad de red de la organización y a su vez sumar al conocimiento de la base de datos sobre ataques informáticos (Taxonomy of Honeynet Solutions, 2015).

3.1.2. Nivel de Investigación

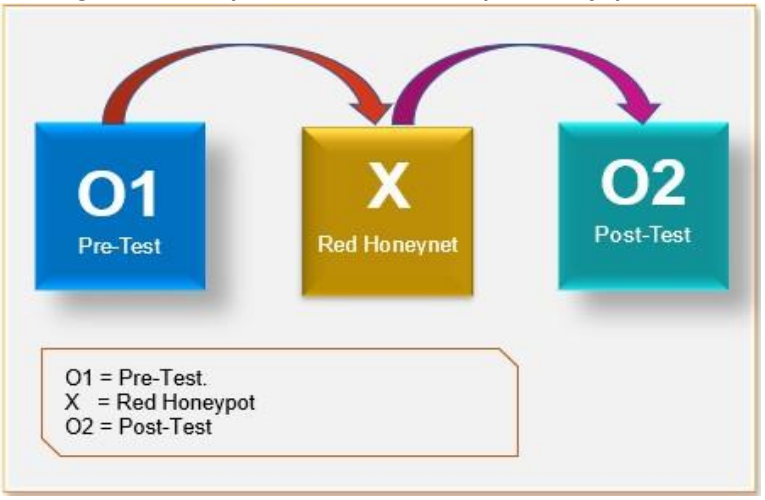
La presente investigación corresponde a un estudio de tipo descriptivo con un enfoque cuantitativo, en el cual se procedió a recolectar los datos de las diferentes pruebas de ciberataques obteniendo información que nos ayudó a evaluar la eficacia con la que trabaja la Honeynet y proponer y generar políticas de seguridad de red de información (Esteban Nieto, 2018).

La investigación, busca poder identificar y describir las vulnerabilidades y riesgos a las que están expuestas los sistemas de red a través del uso de una Honeynet en un entorno virtual usando IPv4 el cual será expuesto a diferentes pruebas de ciberataques con el fin de poder obtener información que nos ayude a proponer y generar políticas de seguridad de red de información y evaluar la eficacia con la que trabaja la Honeynet (Software-Defined HoneyNet: Towards Mitigating Link Flooding Attacks, 2017).

3.1.3. Diseño de Investigación

En el presente trabajo de investigación se utilizará un diseño pre experimental mediante la realización del método de prueba Pre-Test y Post-Test, a través de este método se realizará el debido análisis que permitirá obtener los resultados esperados, y de esta manera se poder evaluar el desenvolvimiento de la honeynet virtualizada configurada con ipv4 al recibir ciberataques simulados, por diferentes tipos de ataque, para evaluar su efectividad como herramienta de seguridad.

Figura 2: Esquema de Prueba pretest y post-test



3.2. Variables y operacionalización

Variable: Configuración de una Honeynet (Towards a Grid-wide, High-fidelity Electrical Substation Honeynet, 2017)
Indicadores:

- Nivel de Respuesta
- Nivel de Satisfacción
- Nivel de Interacción
- Configuración de la red

Variable: Ataques Cibernéticos (HONEYPROXY: Design and Implementation of Next-Generation Honeynet via SDN, 2018) Se utilizará fichas de registro

- Número de ataques registrados
- Numero de intrusiones
- Número de ataques a servicios de red
- Procedencia de los ataques
- Numero de vulnerabilidades

3.3. Población, muestra y muestreo

De acuerdo con (Hernández-Sampieri, y otros, 2017), indica que los recursos analizados anteriormente, son la base para la gestión del conocimiento y será el soporte para las actividades de los procesos que demanda el emprendimiento de exploración, uno de sus elementos esenciales es la población y la muestra, dado que detalla a quien se va a estudiar (población) y en qué cantidad (muestra).

3.3.1. Población

Se considera el criterio de población al grupo total de individuos, elementos o medidas que tienen algunas propiedades recurrentes observables en un espacio y en un instante preciso. Cuando se va a realizar alguna exploración debe de tenerse presente algunas propiedades fundamentales al elegir la gente bajo estudio: Homogeneidad, Tiempo y Espacio (Hernández-Sampieri, y otros, 2017). La cantidad de la población para esta investigación está

conformada por los 10 tipos de ataques considerados según el daño que podrían incurrir.

3.3.2. Muestra

Según (Hernández-Sampieri, y otros, 2017) “La muestra es un subgrupo de la multitud de interés sobre el cual se recolectarán datos, y que debe definirse y delimitarse de seguro con precisión, además de que debe ser representativo de la población”.

En este trabajo de investigación la muestra está conformada por toda la población, es decir se considera a todos los 10 tipos de ataques conocidos.

3.4 Técnicas e Instrumentos de recolección de Datos

Para lograr el cumplimiento de los objetivos trazados se han considerado las siguientes técnicas e instrumentos:

3.4.1. Técnicas

La técnica que se efectuará será observación por que mediante ella pudimos analizar y evaluar la vulnerabilidad que presenta una honeynet al simularle ataques informáticos como el malware o el ataque de puertos. Según Hernández Sampieri, y otros (2015), la técnica de la observación es aquella que es consciente y se orienta hacia un objetivo o fin determinado. El observador debe comprender con total cabalidad el proceso, fenómeno u objeto a observar, para que sea capaz dentro del conjunto de características de este, seleccionar aquellos aspectos que son susceptibles y que contribuyen a la demostración de la hipótesis.

3.4.2. Instrumentos

Para la recolección de los datos se utilizará el instrumento ficha de registro.

Variable: Configuración de una Honeynet (Towards a Grid-wide, Highfidelity Electrical Substation Honeynet, 2017) Indicadores:

- Nivel de Respuesta
- Nivel de Satisfacción
- Nivel de Interacción
- Configuración de la red
- Nivel de respuesta

Variable: Ataques Cibernéticos (HONEYPROXY: Design and Implementation of Next-Generation Honeynet via SDN, 2018)

Se utilizará fichas de registro

- Número de ataques registrados
- Numero de intrusiones
- Tipos de Ataque
- Cantidad ataques a servicios de red
- Procedencia de los ataques
- Numero de vulnerabilidades

También se realizará la validez del Instrumento y confiabilidad del Instrumento por parte de la Opinión del Juicio de Expertos, que es el conjunto de opiniones brindadas por profesionales expertos del tema.

3.5 Procedimiento

Consistirá en un primer momento en la aplicación del instrumento para la recolección de datos en cual se hará uso de las técnicas de observación y fichaje según la operación a realizarse las cuales serían:

Operación Pretest: En esta primera fase se va registrar las vulnerabilidades de estos ataques de recolección de datos se expondrá al sistema de red a diversos ataques cibernéticos simulados para poder obtener en primera instancia una primera base de datos de la interacción directa del atacante con la red, en donde la información será registrada a través de diferentes fichas de indicadores las cuales servirán para realizar un posterior análisis estadístico (Cohen, y otros, 2019)

Operación Post-test En esta segunda fase de recolección de datos se expondrá al sistema de red a diversos ataques cibernéticos simulados en donde la Honeynet detecte las vulnerabilidades y procede al

encapsulamiento de estas amenazas y a la vez obteniendo datos del atacante Previo a esto se realizó el estudio de diferentes programas con el objetivo de poder determinar cuál es el más adecuado para garantizar el óptimo funcionamiento de la Honeynet entre los cuales destacan: Footprinting, Scanning, Framework Metasploit, Kali, Exploits y Payload Meterpreter (Cohen, y otros, 2019).

3.6 Método de Análisis de datos

Para esta investigación se procederá a evaluar el rendimiento de la Honeynet a través de los datos obtenidos de la ejecución del Pre-Test y el Post-Test para analizar los datos numéricos obtenidos, a través de la aplicación de la estadística descriptiva.

Para el procedimiento del análisis de los datos se realiza la codificación y clasificación de los datos la cual será tabulada en un cuadro Excel para poder analizar y realizar una tabla de frecuencia de datos, tabla de contingencia y una matriz de doble entrada utilizándose las frecuencias reales y su relación porcentual por ítem. La información final obtenida de los resultados se representará mediante el uso de gráficos de barras.

3.7 Aspectos Éticos

Se reconoce la autoría intelectual de cada una de las fuentes de información citadas parcial o totalmente en el contenido de esta investigación. Se evidencia que los instrumentos utilizados en la investigación fueron validados por expertos en el tema con el único propósito de ser transparentes; y que los resultados obtenidos son auténticos. Además, se guarda la confiabilidad de la identidad de cada una de las personas que intervinieron en el estudio, así como de la información institucional utilizada.

IV. RESULTADOS

Se describen en este capítulo los resultados obtenidos en la investigación, considerando los objetivos planteados, en lo que respecta a los ataques e intrusiones se tiene “números de ataques registrados”, “Numero de intrusiones” y “tipos de ataques” en cuanto a servicios de red se consideró “Nivel de ataques a servicios de red”, “Procedencia de los ataques” y el “número de vulnerabilidades”, tanto en el pretest (sin la Honeynet), como para el post-test (con la Honeynet), utilizando el software IBM SPSS para la estadística de comparación.

Hipótesis específica HE1

$HE1_0$: La implementación de la Honeynet no mejora la evaluación de ataques e intrusiones en un modelo de redes cisco 2020

$HE1_a$: La implementación de la Honeynet mejora la evaluación de ataques e intrusiones en un modelo de redes cisco 2020

Tabla 2 Prueba de ataques e intrusiones

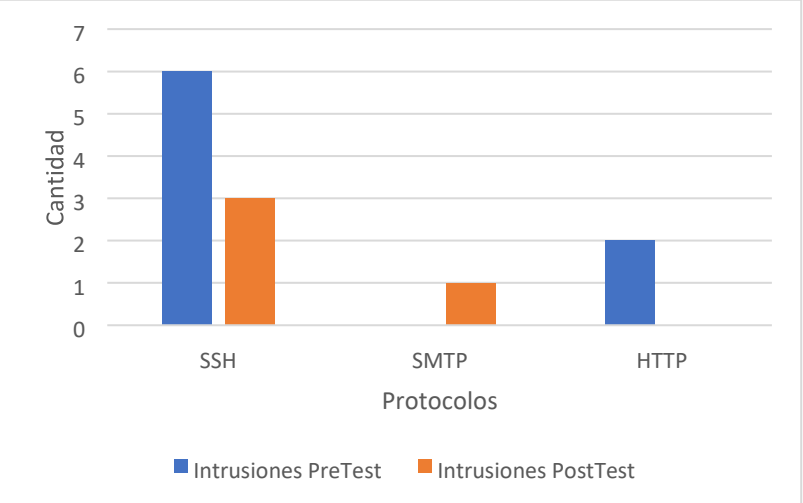
Prueba de muestras relacionadas					
	Diferencias relacionadas		t	gl	Sig. (bilateral)
	Media	Desviación típ.			
Evaluación de Ataques PostTest - Evaluación de Ataques PreTest	6,818	3,065	10,434	21	0,000

Como el nivel de significación 0.000 es menor que 1.72 (21 grados de libertad en T Student) se rechaza la hipótesis nula ($HE1_0$) y se acepta la hipótesis alternativa ($HE1_a$), con el uso de la Honeynet mejora la evaluación del número de ataques registrados de 9.41 a 2.59.

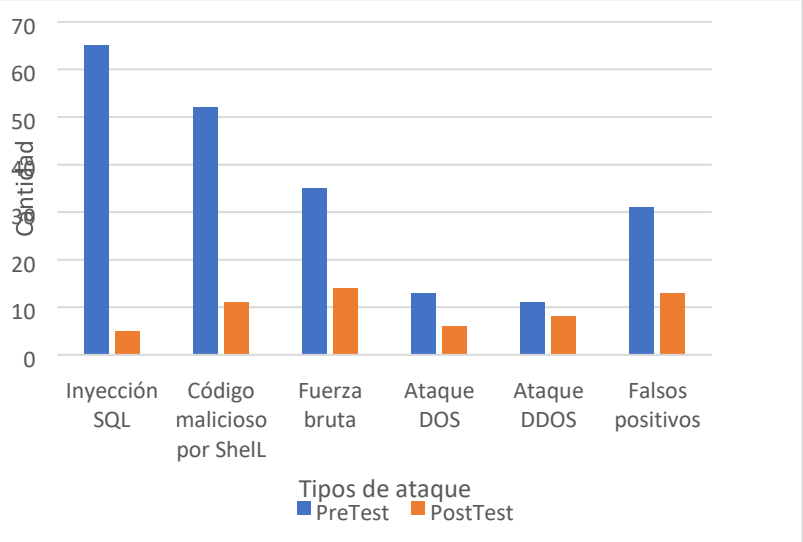
En lo que respecta al indicador número de intrusiones, mediante un servidor remoto sin la Red Honeypot, se muestra mediante el ua-tester de Kali Linux y nmap, un total de 08 intrusiones, 06 mediante acceso remoto a SSH y 02 con HTTP y con la Honeypot, 04 intrusiones, 03 mediante acceso remoto a SSH y 01 con SMTP como se muestra en la gráfica **1**.

En los tipos de ataque, en el pre Test tenemos de inyección SQL y código malicioso por Shell, son los ataques más representativos dentro de los eventos fatales que se suscitaron en la red y configurando la Honeynet se evidenciaron ataques vía SSH por fuerza bruta y DDOS tipo Port Flood por SMTP, como se muestra en la gráfica **2**

Gráfica 1 Intrusiones Pretest - Post-test

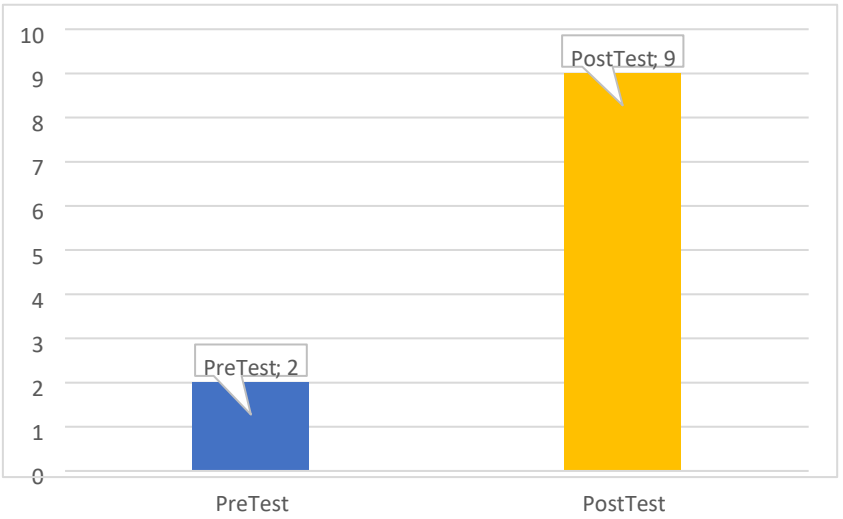


Gráfica 2 Tipos de ataques



Además, en lo que respecta a exploits y malware en el Pretest se realizó un análisis periódico mediante antivirus, se detectó 02 malware de tipo spyware, uno llamado BB2F6240402F765A9D0D650B79CD2560.xls.malware(Red October) y el Dropper.Generic_c.NZR; y en el Post-test, utilizando Dionaea, software que está específicamente diseñado para capturar malware, contabilizó un total de 09 malwares. Esto 07 ataques de diferencia entre la red actual sin Honeynet y la red con Honeynet, como se muestra en la gráfica 3, se debe a la mejora en la evaluación, con la implementación de esta; pues debido a la configuración de servicios en los servidores como directorio activo, dns, web, dhcp y otros, atraen a los potenciales atacantes a la red.

Gráfica 3 Exploits y malware pre y post



Hipótesis específica HE2

$HE2_0$: La configuración de una Honeynet no mejora evaluación de ataques de los servicios de red en un modelo de redes cisco 2020

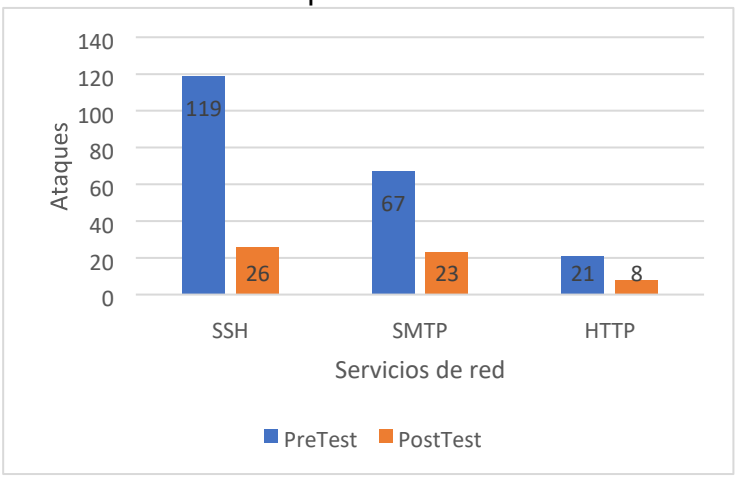
$HE2_a$: La configuración de una Honeynet mejora evaluación de ataques de los servicios de red en un modelo de redes cisco 2020

Tabla 3 Prueba de ataques a servicios de red

Prueba de muestras relacionadas					
	Diferencias relacionadas		t	gl	Sig. (bilateral)
	Media	Desviación típ.			
Ataques Servicios de Red (PostTest) - Ataques Servicios de Red (Postest)	0,818	0,958	4,006	21	0,001

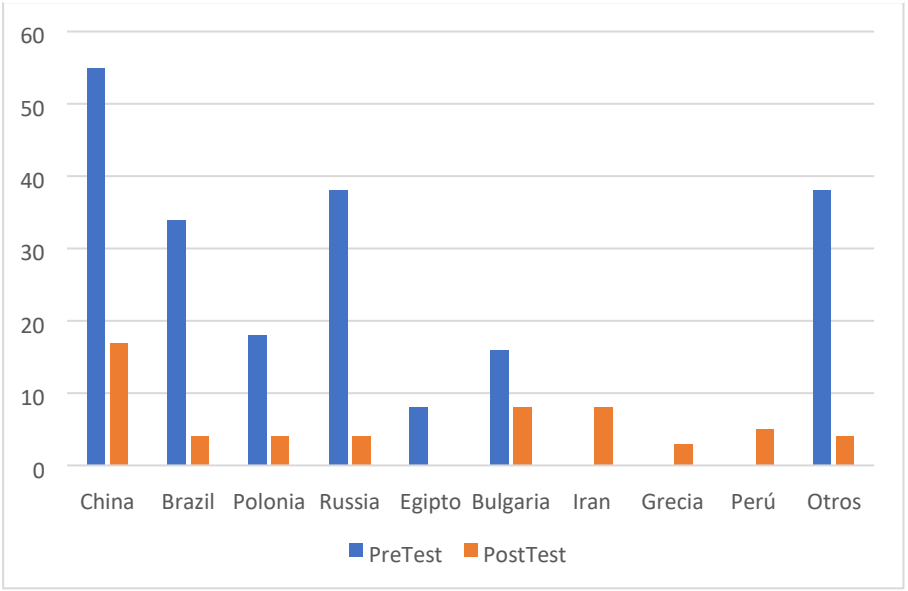
Como el nivel de significación 0.001 en la Tabla 3, es menor que 1.72 (21 grados de libertad en T Student) se rechaza la hipótesis nula ($HE2_0$) y se acepta la hipótesis alternativa ($HE2_a$), con el uso de la Honeynet mejora la evaluación del número de ataques de los servicios de red de 1.41 a 0.59. Tal como se muestra en la gráfica 5 mediante las herramientas de Kali Linux, en el pretest, el 57.49% de los ataques es mediante intentos de inicio de sesión remoto vía SSH por fuerza bruta, 32.37% ataques DDOS tipo Port Flood por SMTP y un 10.14% vía HTTP; y con la configuración de la Honeynet, de los ataques suscitados el 45.61% es vía SHH, 40.35% mediante SMTP y 14.04% HTTP.

Gráfica 4 Ataques a servicios de red



En la procedencia de los ataques, según gráfica 6, en el pretest, se determinó que el 26.57% de los ataques provienen de China, seguidos de Rusia y Brasil con 38% y 34% respectivamente. En el posttest la procedencia de los ataques indica que el 29.82% de los ataques provienen de China, seguidos de Irán, Bulgaria y Perú con 14.04%, 14.04% y 8.77%. Además, algunos IP son reincidentes en estos tipos de ataques que generalmente son automatizados mediante software como Putty, Go, OpenSSH, LibSSh2 entre otros.

Gráfica 5 Procedencia de los ataques



Hipótesis específica HE3

$HE3_0$: La determinación de las vulnerabilidades no mejora con una Honeynet, en un modelo de redes Cisco 2020.

$HE3_a$: La determinación de las vulnerabilidades mejora con una Honeynet, en un modelo de redes Cisco 2020.

Tabla 4 Vulnerabilidades

Prueba de muestras relacionadas					
	Diferencias relacionadas		t	gl	Sig. (bilateral)
	Media	Desviación típ.			
Vulnerabilidades PostTest - Vulnerabilidades PreTest	16,500	1,915	17,234	3	0,000

Como el nivel de significación 0.000 es menor que 2.35 (3 grados de libertad en T Student) se rechaza la hipótesis nula ($HE3_0$) y se acepta la hipótesis alternativa ($HE3_a$), con el uso de la Honeynet mejora la evaluación del número de vulnerabilidades de 33.50 a 17.0.

En la ilustración 1 se muestra el diseño la red sin Honeynet mediante Packet Tracert, donde utilizando herramientas de Kali Linux (nmap, brute-force entre otros) se realiza un monitoreo de eventos sospechosos en la red. Para la detección de las vulnerabilidades en este diseño, se utilizó un exploit denominado eternalblue el cual es explotado usando Metasploit, obteniendo acceso a través de una Shell System. Se determinó un total de 29 vulnerabilidades en los puertos FTP, SSH y SMTP. En el Pre Test, sin la honeynet se tiene un promedio de 33.5 vulnerabilidades

Ilustración 1: Red Pretest

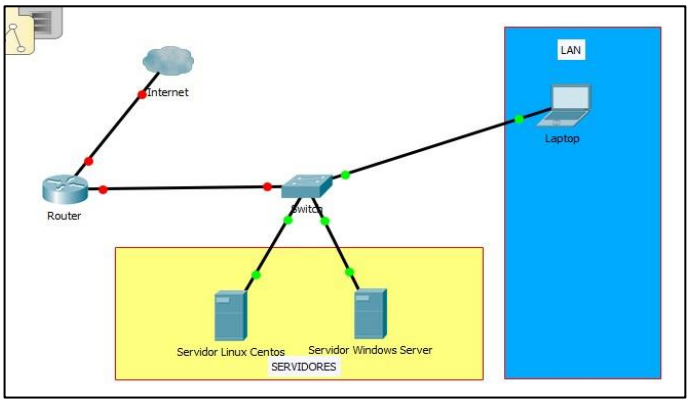
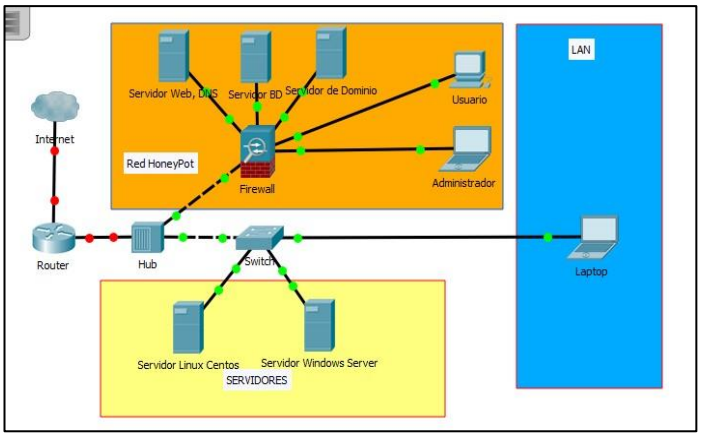


Ilustración 2: Red Post Test Con Honeypot



Con implementación de la Honeynet en un modelo de redes Cisco 2020 como se muestra en la ilustración 2, se evidencio 17 vulnerabilidades; lo que implica que un promedio de 16.5 vulnerabilidades se lograron superar en el servicio SSH y SMTP; debido a la actualización del sistema operativo y de algunos servicios para la configuración de la Honeynet.

Se determinó que el usuario root y la contraseña 123456, es el más utilizado en los ataques tal como se muestra en la ilustración 3.

Ilustración 3 Nube de etiqueta de usuario y contraseña

V. DISCUSIÓN

En forma general con la configuración de la Honeynet se logró la evaluación de los ataques cibernéticos en un modelo de redes cisco 2020, asimismo se mejoró la evaluación de ataques e intrusiones mediante la Honeynet pues de un total de 08 intrusiones, 06 mediante acceso remoto a SSH y 02 con HTTP y con su configuración, se determinó 04 intrusiones, 03 mediante acceso remoto a SSH y 01 con SMTP. Entre los tipos de ataques se tuvo inyección SQL y código malicioso por Shell sin la Honeynet; configurando la Honeynet se evidenciaron ataques vía SSH por fuerza bruta y DDOS tipo Port Flood. En lo que respecta a la evaluación de ataques de los servicios de red de 57.49% de los ataques de inicio de sesión remoto vía SSH, 10.14% ataques DDOS por SMTP y un 8% vía HTTP sin Honeynet, y se obtuvo que el 45.61% de los ataques es mediante intentos de sesión remoto vía SSH, 40.35% ataques DDOS tipo Port Flood por SMTP y 14.04% mediante HTTP con la Honeynet; asimismo en lo que respecta a las vulnerabilidades en el Pre Test de 29 vulnerabilidades en los puertos FTP, SSH y SMTP, y en Posstest se tuvo 19 vulnerabilidades, 15 en SMTP y 4 en SSH.

En cuanto a la mejora la evaluación de ataques e intrusiones, se planteó según la teoría relacionada tanto para ataques pasivos o activos según Carcelén Méndez, y otros (2017). Los resultados del estudio fueron un total de 207 ataques en el PreTest y 57 en el PostTest, de estas hubieron 08 intrusiones, 06 mediante acceso remoto a SSH y 02 con HTTP sin Honeynet a 04 intrusiones, 03 mediante acceso remoto a SSH, 01 SMTP mediante la implementación de la Honeynet y que el 26.57% de los ataques provienen de China, 18.36% Rusia y 16.43% Brasil, estos resultados fueron semejantes a los resultados de la investigación obtenidos por De Diego y otros (2017) porque encontró que de un registro 29342 ataques, el 12.62% fueron exitosos en el puerto 22 procedentes de china y en menor medida de Polonia, Vietnam y Holanda, las credenciales utilizadas fueron admin-admin, root-root; Yucta (2019) en sus resultados tiene que la información capturada el 33% representa el impacto del ataque, 24% representa al escaneo de ataque, el 21 % representa al fallo del sistema, el 15% facilidad de ataque y el 6%

representa las acciones correctivas, asimismo se evidencio en el registro de actividades tácticas y métodos del atacante; León y otros (2017) en sus resultados los ataques de eran provenientes de china y los servicios más atacados LDAP.udp 23.3%, telnet 13.6%, NTP 26.4%, TFTP 12.2%, dns.udp 7.3%, SSH 7.1%, SMTP 5.3%, SIP 2.2%, HTTP 2.1% y SNMP 0.5%. Sin embargo, estos resultados fueron diferentes a Valdiviezo (2020) , quienes encontraron, en el indicador número de Intrusiones sin la Red Honeypot fue de 0 y con la Red Honeypot fue de 3, esto se debía a que no contaba con herramientas de escaneo de vulnerabilidades configuradas.

En cuanto a la configuración de una Honeynet mejora evaluación de ataques de los servicios de red, se enmarco en la teoría planteada por Correa Guerrero (2016) para aprender sobre las actividades, servicios de red y motivos que alientan a los atacantes. Según los resultados se determinó que el 57.49% de los ataques de inicio de sesión remoto fue vía SSH, 32.37% ataques DDOS por SMTP y un 10.14% vía HTTP en el Pretest, con la Honeynet el 45.61% de los ataques es vía SSH, 40.35% ataques DDOS por SMTP y 14.04% mediante HTTP. Esto debido que al configurarla se actualizó algunos servicios de sistema operativo y de los servicios, además del firewall que se implementó para la protección del servidor Centos de Linux. Estos resultados fueron semejantes a lo encontrado por Carcelén y otros (2017) quien determinó que los servicios expuestos corresponden a FTP (21), SSH (22), DNS (53), DHCP y el puerto 1000 de TCP por el webmin; Quinchaguano (2016) en sus resultados se alertó se alertó del ataque ADMkillDNS y ADMdnsfuckr en el puerto 53, Cross Site Scripting a través de SSH o FTP, accediendo con acreditación root, asimismo se observa que el 33.94% de ataques provienen de China a través de SSH (puertos 22, 42 y 1125) y Palmay (2017) detectó escaneo de puertos, en intervalos menores a 01 minuto, ataque DOS al puerto 3306 base de datos mysql por intervalos de 02 minutos, y fuerza bruta para descifrar contraseñas con la herramienta Jhon the Ripper, Ataque de inyección de código a Mysql, puerto 22 del servicio SSH y Ataque de denegación de servicio TCP/SYN (FLOODING). Sin embargo, si difieren de Harlyn (2018), quien encontró que en el escaneo

comprobó que el 70 % corresponde a MS09-001 Microsoft Windows SMB Vulnerabilidad, 20 % corresponde a MS08-067 Microsoft Windows Server Service Crafted RPC, y un 10 % corresponde a MS17-010 Security Update for Microsoft Windows SMB Server, todas estas vulneravilidades correspondientes al puerto 445 TCP y de los 50 ataques al servicio SMB Netbios puerto 445 el 79 % de ataques tuvieron éxito y un 21% fallo por tiempo de espera.

En la determinación de las vulnerabilidades mejora con una Honeynet, planteado según la teoría enmarcada, para determinar deficiencias en los sistemas operativos y aplicaciones, según Dios León, y otros (2018). En el Pre Test de 29 vulnerabilidades evidenciadas en los puertos FTP, SSH y SMTP, se tuvo 19 vulnerabilidades, 15 en SMTP y 4 en SSH, esto debido a la actualización por parte del sistema operativo de algunos servicios e implementación del firewall al configurar la Honeynet, estos fueron semejantes a los resultados de los estudios de Valdiviezo (2020) pues el número de vulnerabilidades de la Infraestructura de Red sin la Red Honeypot fue de 23 y con la Red Honeypot fue de 18, lo cual representa una disminución de 5 vulnerabilidades encontradas, esto debido a la implementación de Kippo dado que el puerto 22 representaba una alta vulnerabilidad; Dios (2018) encontró en sus resultados del total de tráfico de paquetes considerado no malicioso, ingresaron 8 paquetes a la Honeynet, lo que representa un 100% de paquetes obtenidos por el IDS Snort y con los algoritmos de detección de intrusos el 62.5% fueron representados como ataques lo que permitió alimentar nuevas reglas de seguridad y 03 representaron el 37.5% los cuales resultaron ser falsos positivos. Sin embargo, los resultados fueron diferentes en algunas vulnerabilidades encontradas por Quinchaguano (2016) quien mediante el software de análisis llamado McCafee Vulnerability Mangener (MVM) detecto 02 vulnerabilidades de riesgo alto asociado al Web Server, 04 de nivel medio asociado al HTTP, DNS, 01 asociado al SSH Y 03 considerados de nivel bajo tanto FTP, PHP e ICMP.

VI. CONCLUSIONES

- Mediante la Honeynet se logró la evaluación de ataques e intrusiones en un modelo de redes, evaluándose 08 intrusiones a los protocolos SSH y HTTP en la red actual y 04 con la Honeynet; asimismo conocer los tipos de ataques más representativos como inyección SQL, código malicioso Shell fuerza bruta y DDOS tipo Port Flood. Se logro mejorar la evaluación del registro de número de ataques de 9.41 a 2.59, debido a la eliminación de eventos sospechosos que eran considerados como ataques a la red.
- Con la configuración de la Honeynet para la evaluación de ataques de los servicios de red, se determinó que entre el 57.49% y 45.61% los ataques fueron por sesión remoto vía SSH, 32.37% y 40.35% ataques DDOS por SMTP y entre 10.14% y 14.04% vía HTTP. Se logro mejorar la evaluación del número de ataques de los servicios de red de 1.41 a 0.59, debido a la precisión en cuanto a la determinación de los falsos positivos dentro de los ataques en la red.
- Se determino las vulnerabilidades mediante una Honeynet, el Pre Test de 29 vulnerabilidades en los puertos FTP, SSH y SMTP, y en Posstest se tuvo 19 vulnerabilidades, 15 en SMTP y 4 en SSH. Mejorando la evaluación de 33.50 a 17.0, debido a actualizaciones de sistema operativo y servicios para la configuración de la Honeynet.
- Finalmente se determinó que la configuración de una Honeynet, mejora la evaluación de ataques cibernéticos en un modelo de redes cisco 2020, mediante la evaluación de las dimensiones ataques e intrusiones, los servicios de red y las vulnerabilidades. Por lo tanto, se considera que se alcanza a demostrar las hipótesis específicas de la investigación.

VII. RECOMENDACIONES

- Para futuros investigaciones se recomienda el uso de técnicas de inteligencia artificial para la detección de patrones de ataques Cibernéticos en una Honeynet.
- Se recomienda un estudio de las acciones a realizar ante los resultados recopilados en una Honeynet, para facilitar a las organizaciones la adopción de estrategias para la protección de las vulnerabilidades de cada red.
- En futuras investigaciones se podría determinar la correlación entre los ataques, herramientas y comportamientos de los atacantes en la red.
- Se recomienda el estudio de la configuración de varias Honeypots, con el propósito de obtener más cantidad de información y determinar patrones de comportamiento entre los atacantes a las redes.

REFERENCIAS

1. **Arequipa Chiquito, Mónica Paulina y Guañuna Quilligana, Juan Andrés. 2017.** Análisis y diseño de un honeynet, para detectar amenazas de código malicioso, Backdoor y DDoS sobre una red MPLS enrutada con OSPFv2 que brinda servicios web. Ecuador : Universidad Politecnica Salesiana.
2. **Azizov, Danis. 2020.** Arquitectura DMZ Perimetral: Una implementación corporativa. s.l. : Universidad Autónoma de Barcelona.
3. **Baray, Hector Luis Avila. 2006.** Introduccion a la Metodologia de la Investigacion. electronica . Chihuahua,Mexico : s.n. pág. 174.
4. **Campoverde Armijos, Jorge Ismael. 2017.** Honeypot como herramienta de prevención de ciberataques. s.l. : Universidad de Buenos Aires.
5. **Carcelén Méndez, Dennis Fabricio y Ríos Mendoza, Carlos Alfredo. 2017.** Desarrollo de un prototipo Honeynet como medida de seguridad para la red informática de la UPS sede Quito Campus Sur. Quito, Ecuador : Universidad Politécnica Salesiana.
6. **Castro-León, Marcela, y otros. 2015.** Servicios y Seguridad, un enfoque basado en estrategias de ataque y defensa. Barcelona, España : s.n.
7. **Chagoya, E.R. 2008.** Métodos y técnicas de investigación.
8. **Christian, Urcuqui¸ y Navarro, Andres. 2017.** Machine Learning Classifiers to Detect Malicious Websites. 2017.
9. **Cohen, Néstor y Gómez Rojas, Gabriela. 2019.** Metodología de la investigación. ¿Para qué? Buenos Aires, Argentina : Editorial Teseo, 2019.
10. **Correa Guerrero, A.E. 2016.** Simulación de un honeypot para detectar ataques y vulnerabilidades en redes IPV6. s.l., 2016.
11. **Cuesta-Quintero, Fabián Ranulfo, y otros. 2018.** Sistema de detección de intrusos a través de una red Honeynet para entornos de red cableada sobre IPV6. ISSN: 16927257 - Volumen 1 – Número 33 - 2018.
12. **De Diego de Diego, Santiago y Romero López, Gustavo. 2017.** Honeynet para el análisis del tráfico y muestras de malware. s.l. : Enseñanza y Aprendizaje de Ingeniería de Computadores. Número 7.
13. **Dios León, S.Y. y Ortíz Pretel, D.A. 2018.** Diseño lógico y simulación de una red espejo virtual (Honeynet) para la detección de intrusos informáticos en zona perimetral. 2018.
14. **Esteban Nieto, Nicomedes Teodoro. 2018.** Tipos de investigación.
15. **Flores Guerrero, Ivan Dario y Quintana Martínez, Jesús Manuel. 2018.** Sistema de detección de ataques informáticos a redes de datos empresariales soportado en HoneyPots. Cartagena, Colombia : Universidad de Cartagena.

16. **Gaona-García, Paulo, Montenegro-Marín, Carlos y JBarón Velandia, Julio. 2016.** Modelo ontológico para la predicción de ataques informáticos a partir de Honeynets virtualizadas. s.l. : Revista LOGOS CIENCIA & TECNOLOGÍA.
17. **Giraldo Giraldo, Erik Michel. 2015.** Sistema multi-agente deliberativo para la obtención y análisis de datos en Honeynet. Manizales : s.n.
18. **Harlyn Mayanga, Adrián Narciso. 2018.** Implementación de Honeypot para la Corrección de Vulnerabilidades en la Red de Datos de la Municipalidad Distrital de Huambos. s.l. : Universidad Señor de Sipán.
19. **Heredia Terán, Carlos. 2016.** Diseño e Implementación de una Honeynet para la red de datos de la Universidad Nacional de Loja, utilizando software Libre. Ecuador : Universidad nacional de Loja.
20. **Hernández Sampieri, Roberto, Fernández Collado, Carlos y Baptista Lucio, María del Pilar. 2015.** Metodología de la Investigación. México : Mc Graw Hill. ISBN: 978-14562-2396-0.
21. **Hernández-Sampieri, R., Fernández-Collado, R. y Baptista-Lucio, P.,. 2017.** Selección de la muestra.
22. HoneyMix: Toward SDN-based Intelligent Honeynet. **Wonky, Han, y otros. 2016.** s.l. : Arizona State University.
23. HONEYPROXY: Design and Implementation of Next-Generation Honeynet via SDN. **Kyung, Sukwha, y otros. 2018.** s.l. : Laboratory of Security Engineering for Future Computing (SEFCOM). NSF-ACI-1642031.
24. **Jurado Pallarés, Diego. 2016.** Análisis y estudio de HoneyPots complejos: Honeynets. 2016.
25. **León Cuervo, Camilo Andrés y Bonilla Díaz, María Alejandra. 2017.** Análisis de ataques informáticos mediante Honeypots para el apoyo de actividades académicas en la universidad distrital. Bogotá : Universidad distrital Francisco José de Caldas.
26. **Martinez Contreras, Kevin David. 2018.** Honeypot, hacia un protocolo de seguridad más eficiente y competitivo. Sucre, Colombia : s.n..
27. **Matías Koller, Juan y Gabriel Bísaro, Mauricio. 2015.** Análisis y desarrollo de mejoras a un sistema honypot para mitigar ataques en servicios de VoIP. 2015. ISSN 2301-1092.
28. **Ortega Bernal, H.J. 2010.** Análisis e implementación de un sistema de video streaming en redes Dual Stack IPV4/IPV6.
29. **Palmay López, María Cristina. 2017.** Propuesta de mejores prácticas para el establecimiento de políticas de seguridad informática basado en Honeynet virtuales. Riobamba, Ecuador : s.n.
30. **Pimenta Rodrigues, Gabriel Arquelau, y otros. 2017.** Cybersecurity and Network

Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection. s.l. : Aplied Sciences.

31. **Quinchaguano Duque, David Francisco. 2016.** Diseño e implementación de un prototipo de una Honeynet para la red de datos de la escuela politécnica nacional. Quito, Ecuador : s.n..
32. Software-Defined HoneyNet: Towards Mitigating Link Flooding Attacks. **Kim, Jinwoo y Shin, Seungwon. 2017.** DSN-W.2017.10.
33. Taxonomy of Honeynet Solutions. **Fan, Wenjun, Du, Zhihui y Fernández, David. 2015.** s.l. : TSI Telecomunicación,Universidad Politécnica de Madrid.
34. **Tirado Ríos, Normandi Rocío, y otros. 2017.** Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. ISSN 1390-9304.
35. Towards a Grid-wide, High-fidelity Electrical Substation Honeynet. **Mashima, Daisuke, Chen, Binbin y Gunathilaka, Prageeth. 2017.** s.l. : Advanced Digital Sciences Center.
36. **Valdiviezo Avalo, Jormy Jean Franco. 2020.** Desarrollo de una Red Honeypot para la Detección de Intrusiones en la Municipalidad. Trujillo, Perú : s.n.
37. **Verdejo Alvarez, Gabriel. 2016.** Seguridad en Redes IP.
38. Versatile virtual honeynet management. **Fan, Wenjun, Fernández, David y Du, Zhihui. 2016**, IET Journals. ISSN 1751-8709.
39. **Voutssas M., J. 2010.** Preservación documental digital y seguridad informática. Investigación bibliotecológica. Vol. 24, ISSN 0187-358X..
40. **W. Zhang, B. Zhang, Y. Zhou, H. He y Z. Ding. 2020.** Honeynet Based on Multiport Honeypots for Capturing IoT Attacks. s.l. : Journals y Magazines.
41. **Yucta Silva, Bryam Fabricio. 2019.** Implantación de un aplicativo para optimizar la gestión centralizada de logs en un ambiente honeynet en el datacenter UNACH. Riobamba, Ecuador : s.n.

ANEXOS:

Anexo 1: Instrumentos de evaluación

Ficha de Registro	
Autor (es):	
Organización:	
Fecha Inicio:	
Fecha Fin:	

Variable	Indicador	Fórmula
Ataques Cibernéticos	Número de ataques registrados	Según Voutssas M, J (2010), define el riesgo como la probabilidad de que un evento nocivo ocurra combinado con su impacto o efecto nocivo en la organización. Se materializa cuando una amenaza actúa sobre una vulnerabilidad y causa un impacto.

IP origen o regla	SRC Ports	SRC Pkts	SRC Bytes	DST Pkts	DST Bytes

Ficha de Registro	
Autor (es):	
Organización:	
Fecha Inicio:	
Fecha Fin:	

Variable	Indicador	Fórmula
Ataques Cibernéticos	Número de intrusiones	Consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio.

Honeypots				Remote Host		
Flags	Host	Connections	IDS events	Host	Connections	IDS events

IP origen o regla	Tiempo	SRC Ports	SRC Pkts	SRC Bytes	DST Pkts	DST Bytes

Ficha de Registro	
Autor (es):	
Organización:	
Fecha Inicio:	
Fecha Fin:	

Variable	Indicador	Fórmula
Ataques Cibernéticos	Tipo de ataque	consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio.

Computador o IP	Nombre de Ataques	Cantidad	Ingreso		Parches de seguridad
			SI	NO	

Ficha de Registro	
Autor (es):	
Organización:	
Fecha Inicio:	
Fecha Fin:	

Variable	Indicador	Fórmula
Ataques Cibernéticos	Numero de ataque a los servicios de red	Danvers (1994) aporta una clara y completa definición de interactividad diciendo que es el término que describe la relación de comunicación entre un usuario/actor y un sistema.

Fecha y hora de Inicio	Fecha y hora de Finalización	Protocolo	IP Origen	IP Destino	Tipo de formato (Pcap File, Web Walleye)

Nivel de ataque

Protocolo	Puerto Origen	Sistema Operativo del atacante	Paquetes enviados/recibidos, tamaños	Puerto Destino

Ficha de Registro	
Autor (es):	
Organización:	
Fecha Inicio:	
Fecha Fin:	

Variable	Indicador	Fórmula
Ataques Cibernéticos	Procedencia de los ataques	Consiste en conocer la ubicación geográfica del atacante, mediante la dirección IP.

IP	Nombre de Ataques	Cantidad	Procedencia

Ficha de Registro	
Autor (es):	
Organización:	
Fecha Inicio:	
Fecha Fin:	

Variable	Indicador	Fórmula
Ataques Cibernéticos	Numero de vulnerabilidad	La vulnerabilidad en redes, es una característica de debilidad de una red de datos, la cual es susceptible de ser explotada por una amenaza, intencional o accidentalmente, permitiendo que se pueda acceder a información de acceso privado, debido a que la red presenta puntos críticos débiles. (Voutssas M. 2010)

Puerto	Estado	Servicio	Nivel de riesgo	Vulnerabilidad

Ficha de Registro		
Autor (es):		
Organización:		
Fecha Inicio:		
Fecha Fin:		
Variable	**Indicador**	**Fórmula**
Configuración de una Honeynet	Configuración de la red Nivel de Respuesta	Swan, Frederick, y Carroll (1981): es el juicio evaluativo o cognitivo que analiza si el producto o servicio produce un resultado bueno o pobre o si el producto es sustituible o insustituible.

Evaluación de la configuración de la Honeynet				
Características de la Honeynet.				
Equipo Server	Virtualizado ( )	Físico ( )		
Equipos PC	Cantidad de Equipos			
	Equipo N°1:	Sistema Operativo		
		Windows	Linux	Otro
	Equipo N°2:	Windows	Linux	Otro
Laptops	Cantidad de Equipos			
	Equipo N°1:	Sistema Operativo		
		Windows	Linux	Otro
	Equipo N°2:	Windows	Linux	Otro
Nivel de Respuesta.				

Rango de Respuesta		
N°	Cantidad de Ataques	Nivel
1	50 - 200	Bajo
2	200 – 500	Medio
3	500 a más.	Alto

Equipo Server	Nivel de Respuesta	Herramientas/Software	Rangos (Medida)

Ficha de Registro	
Autor (es):	
Organización:	
Fecha Inicio:	
Fecha Fin:	

Variable	Indicador	Fórmula
Configuración de una Honeynet	Nivel de Respuesta Nivel de Satisfacción	Swan, Frederick, y Carroll (1981): es el juicio evaluativo o cognitivo que analiza si el producto o servicio produce un resultado bueno o pobre o si el producto es sustituible o insustituible.

Bidirectional Flows				Total, Flows			
IN		OUT		IN		OUT	
Con	Ids	Con	Ids	Con	Ids	Con	Ids

Ficha de Registro	
Autor (es):	
Organización:	
Fecha Inicio:	
Fecha Fin:	

Variable	Indicador	Fórmula
Configuración de una Honeynet	Nivel de Interacción	Danvers (1994) aporta una clara y completa definición de interactividad diciendo que es el término que describe la relación de comunicación entre un usuario/actor y un sistema.

Numero	IP Fuente	Paquetes en bit	Ubicación de IP

Protocolo	Mes:		
	BYTES	PACKETS	CONEC

Anexo 2:

Tabla de operacionalización

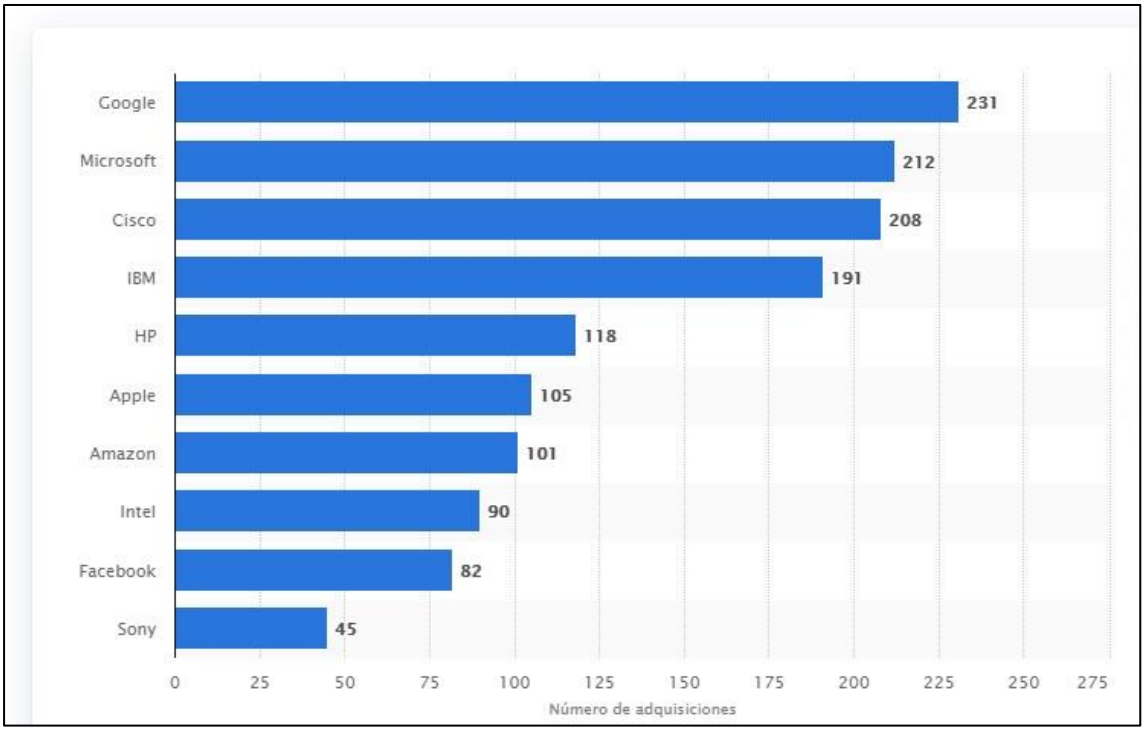
Variables	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de Medición
Configuración de una Honeynet (Dios León, y otros, 2018).	La Honeynet son Honeypots de alta interacción que consta de una red de sistemas, con la finalidad de aprender sobre las herramientas, tácticas y motivos que alientan a este tipo de usuarios (Verdejo Alvarez, 2016).	La honeynet tiene como dimensiones la red Ipv4, Honeypot y los riesgos de seguridad de la red los cuales trabajan con indicadores de nivel de respuesta, satisfacción e interacción (Azizov, 2020).	Honeypot (Correa Guerrero, 2016)	Nivel de Respuesta (Towards a Grid-wide, Highfidelity Electrical Substation Honeynet, 2017)	Escala (Baray, 2006)
				Nivel de Satisfaction (Towards a Grid-wide, Highfidelity Electrical Substation Honeynet, 2017)	Escala (Baray, 2006)
			(Baray, 2006)versión 4 (IPV4)	Nivel de Interacción (Towards a Grid-wide, Highfidelity Electrical Substation Honeynet, 2017)	Nominal (Baray, 2006)
			Modelo de Red (W. Zhang, y otros, 2020	Modelo de la red (Towards a Grid-wide, Highfidelity Electrical Substation Honeynet, 2017)	Nominal (Baray, 2006)

Variables	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de Medición
Ataques Cibernéticos (HONEYPROXY: Design and Implementation of NextGeneration Honeynet via SDN, 2018)	Un ataque cibernético es una acción delictiva que se realiza para acceder a información privada, con el objetivo de apropiarse de ella o pedir dinero a cambio de volver a liberar la información. (HONEYPROXY: Design and Implementation of Next-Generation Honeynet via SDN, 2018)	Los ataques cibernéticos tienen como dimensiones las vulnerabilidades de red y ciberataques. Y como indicadores Nivel de vulnerabilidad, Respuesta, Interacción de ataque y Registro de ataques. (HONEYPROXY: Design and Implementation of	Ataques e intrusiones (Software-Defined HoneyNet: Towards Mitigating Link Flooding Attacks, 2017)	Número de ataques registrados HONEYPROXY: Design and Implementation of NextGeneration Honeynet via SDN, 2018)	Nominal (Baray, 2006)
				Número de intrusiones HONEYPROXY: Design and Implementation of NextGeneration Honeynet via SDN, 2018)	Nominal (Baray, 2006)
				Tipos ataques HONEYPROXY: Design and Implementation of NextGeneration Honeynet via SDN, 2018)	
				Numero de Ataques HONEYPROXY: Design and Implementation of NextGeneration Honeynet via SDN, 2018)	Nominal (Baray, 2006)

		Next-Generation Honeynet via SDN, 2018)	Servicios de red (Software-Defined HoneyNet: Towards Mitigating Link Flooding Attacks, 2017)	Procedencia de los ataques HONEYPROXY: Design and Implementation of NextGeneration Honeynet via SDN, 2018)	Ordinal (Baray, 2006)
			Vulnerabilidades (Software-Defined HoneyNet: Towards Mitigating Link Flooding Attacks, 2017).	Numero de vulnerabilidades HONEYPROXY: Design and Implementation of Next-Generation Honeynet via SDN, 2018)	Nominal (Baray, 2006)

Anexo 3: Cisco en el Ámbito empresarial

Ranking de las empresas tecnológicas con mayor número de adquisiciones a nivel mundial realizadas entre 1991 y 2019



Anexos 4: MATRIZ DE CONSISTENCIA

<table>
<tr><th>Problema</th><th>Objetivos</th><th>Hipótesis</th><th>Variables</th><th>Dimensión</th><th>Indicador</th><th>Método</th></tr>
<tr><td>Principal</td><td>General</td><td>General</td><td>Dependiente</td><td rowspan="3">Ataques e intrusiones</td><td>Número de ataques registrados</td><td rowspan="11">Tipo de Investigación
Explicativa – Experimental

Diseño de investigación
No Experimental

Población
Registros de ataques cibernéticos

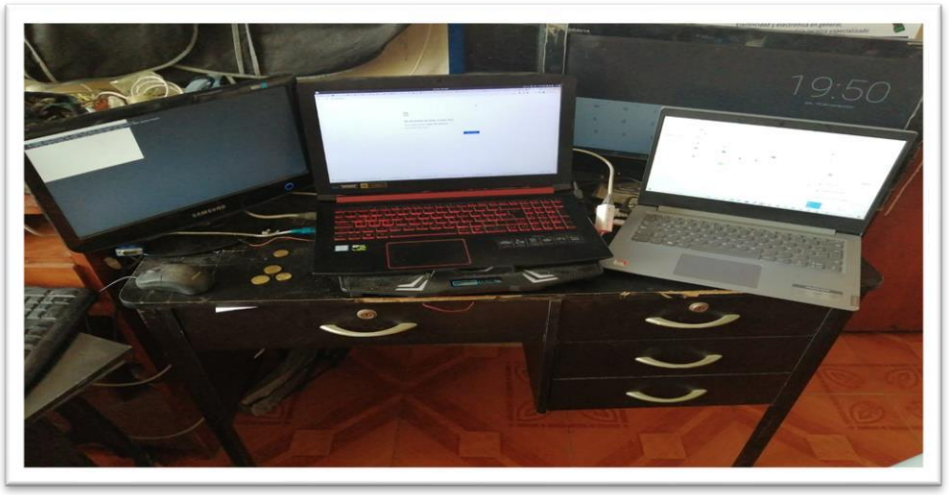
Muestra
Toda la muestra

Muestreo
Muestreo aleatorio simple

Técnica
Observación

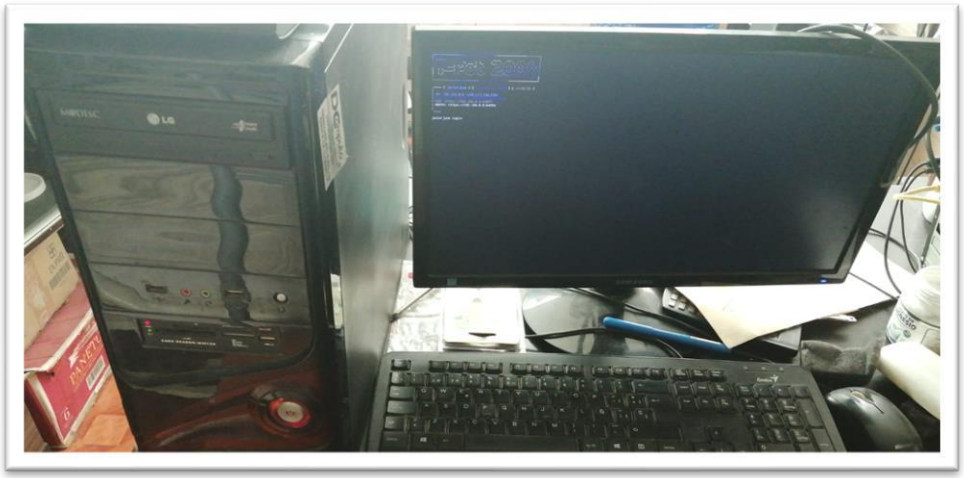
Instrumento
Ficha de registro</td></tr>
<tr><td rowspan="3">¿Cómo se configura una Honeynet para la evaluación de ataques cibernéticos en un modelo de redes cisco 2020?</td><td rowspan="3">Determinar la configuración de una Honeynet para la evaluación de ataques cibernéticos en un modelo de redes cisco 2020</td><td rowspan="3">La configuración de una Honeynet mejora la evaluación de ataques cibernéticos en un modelo de redes cisco 2020.</td><td rowspan="4">Evaluación de ataques Cibernéticos</td><td>Numero de intrusiones</td></tr>
<tr><td>Tipos de Ataque</td></tr>
<tr><td rowspan="2">Servicios de red</td><td>Número de ataques a servicios de red</td></tr>
<tr><td>Procedencia de los ataques</td></tr>
<tr><td>Especificos</td><td>Especificos</td><td>Especificos</td><td>Independiente</td><td rowspan="2">Vulnerabilidades</td><td>Numero de vulnerabilidades</td></tr>
<tr><td>P1: ¿Cómo se implementa la Honeynet para la evaluación de ataques e intrusiones en un modelo de redes cisco 2020?</td><td>O1: Determinar la Honeynet para la evaluación de ataques e intrusiones en un modelo de redes cisco 2020</td><td>H1: La implementación de la Honeynet mejora la evaluación de ataques e intrusiones en un modelo de redes cisco 2020</td><td rowspan="3">Configuración de una Honeynet</td><td rowspan="2">Honeypot</td><td>Nivel de Respuesta</td></tr>
<tr><td>P2: ¿Cómo se configura la Honeynet para la evaluación de ataques a los servicios de red en un modelo de redes cisco 2020?</td><td>O2: Configurar una Honeynet para la evaluación de ataques de los servicios de red en un modelo de redes cisco 2020</td><td>H2: La configuración de una Honeynet mejora evaluación de ataques de los servicios de red en un modelo de redes cisco 2020</td><td>Nivel de Satisfacción</td></tr>
<tr><td>P3: ¿Cómo se evalúan las vulnerabilidades de la red mediante una Honeynet, en un modelo de redes Cisco 2020?</td><td>O3: Evaluar las vulnerabilidades mediante una Honeynet, en un modelo de redes Cisco 2020</td><td>H3: La determinación de las vulnerabilidades mejora con una Honeynet, en un modelo de redes Cisco 2020.</td><td>Protocolo de Internet versión 4 (IPV4)</td><td>Nivel de Interacción</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Modelo de Red</td><td>Configuración de la red</td></tr>
</table>

Anexos 5: Evidencias

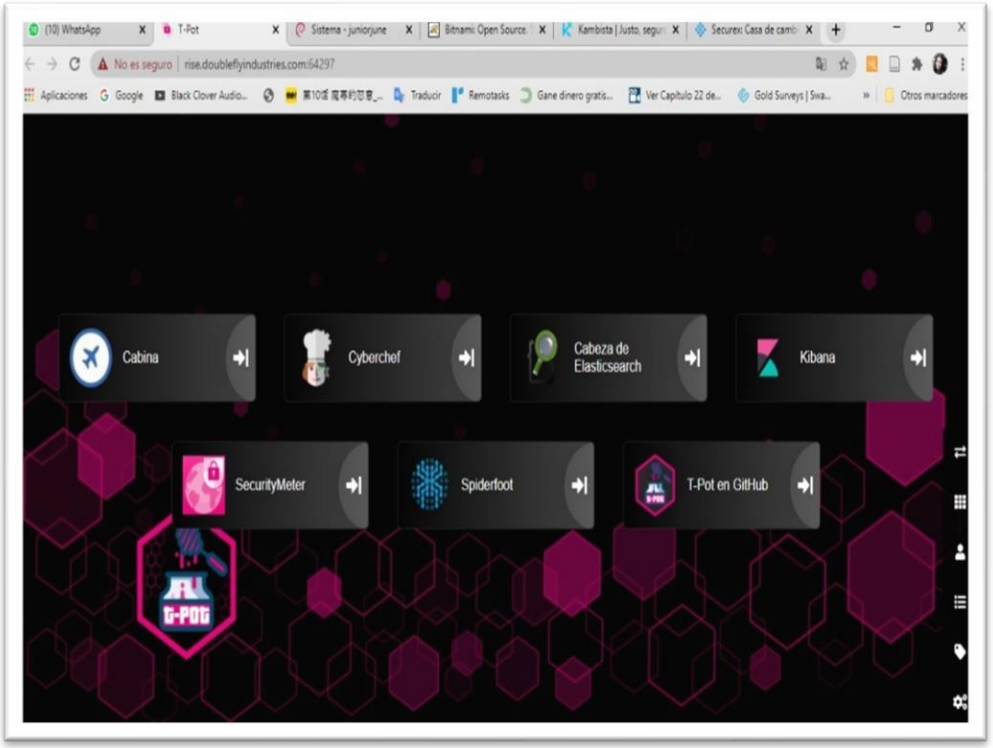


Laptops usadas para ingresar al sistema de la Honeynet

Servidor basado en Linux con CentOS 7



Computadora usada para con el sistema operativo T-pot Os usado para la Honeynet



Interfaz de acceso a las herramientas de la Honeynet

Registro de ataques

Protocol	Direction	TIPO
(IP or Rule) 222.186.169.192	lfd: (sshd) Failed SSH login from 222.186.169.192 (CN/China/-): 5 in the last 3600 secs - Wed Jul 29 13:16:46 2020	SSH
(IP or Rule) 218.92.0.224	lfd: (sshd) Failed SSH login from 218.92.0.224 (CN/China/-): 5 in the last 3600 secs - Wed Jul 29 13:31:17 2020	SSH
(IP or Rule) 222.186.180.8	lfd: (sshd) Failed SSH login from 222.186.180.8 (CN/China/-): 5 in the last 3600 secs - Wed Jul 29 13:34:12 2020	SSH
(IP or Rule) 222.186.173.215	lfd: (sshd) Failed SSH login from 222.186.173.215 (CN/China/-): 5 in the last 3600 secs - Wed Jul 29 13:39:52 2020	SSH
(IP or Rule) 61.177.172.168	lfd: (sshd) Failed SSH login from 61.177.172.168 (CN/China/-): 5 in the last 3600 secs - Wed Jul 29 13:48:23 2020	SSH
(IP or Rule) 218.92.0.248	lfd: (sshd) Failed SSH login from 218.92.0.248 (CN/China/-): 5 in the last 3600 secs - Wed Jul 29 14:02:48 2020	SSH

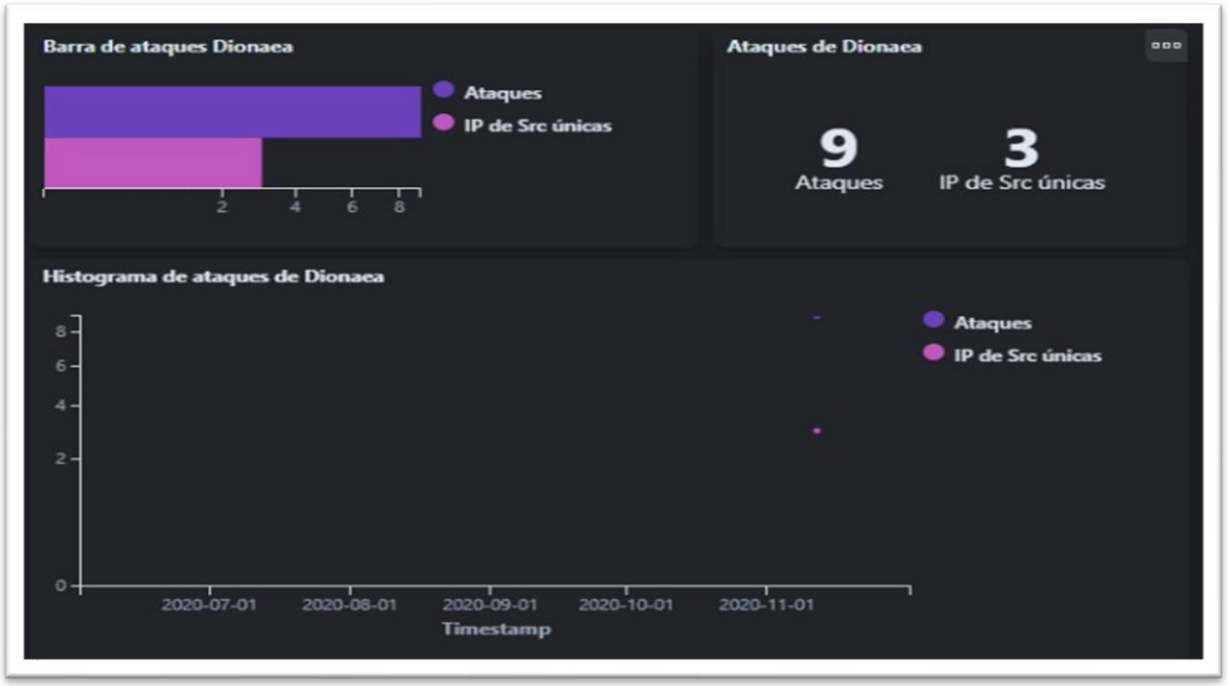
Detalle de ataques

[Wed Oct 07 03:14:43.337748 2020] [:error] [pid 31429:tid 140496265459456] [client 176.113.115.214:48288] [client 176.113.115.214] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(?i:\\\\b(?:(?:s(?:t(?:d(?:dev(_pop|_samp)?)?|r(?:_to_date|cmp))|u(?:b(?:str(?:ing(_index)?)?|(?:dat|tim)e)|m)|e(?:c(?:_to_time|ond)|ssion_user)|ys(?:tem_user|date)|ha(1|2)?|oundex|chema|ig?n|pace|qrt)|i(?:s(null|_(free_lock|ipv4_compat|ipv4_mapped|ipv4| ..." at ARGS:content. [file "/usr/local/apache/modsecurity-owasp-old/base_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "125"] [id "950001"] [rev "2"] [msg "SQL Injection Attack"] [data "Matched Data: md5(found within ARGS:content: <php>die(@md5(HelloThinkCMF))</php>"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "190.117.184.238"] [uri "/"] [unique_
id "X314835r8pVD63FEHLjcdwAAANQ"]

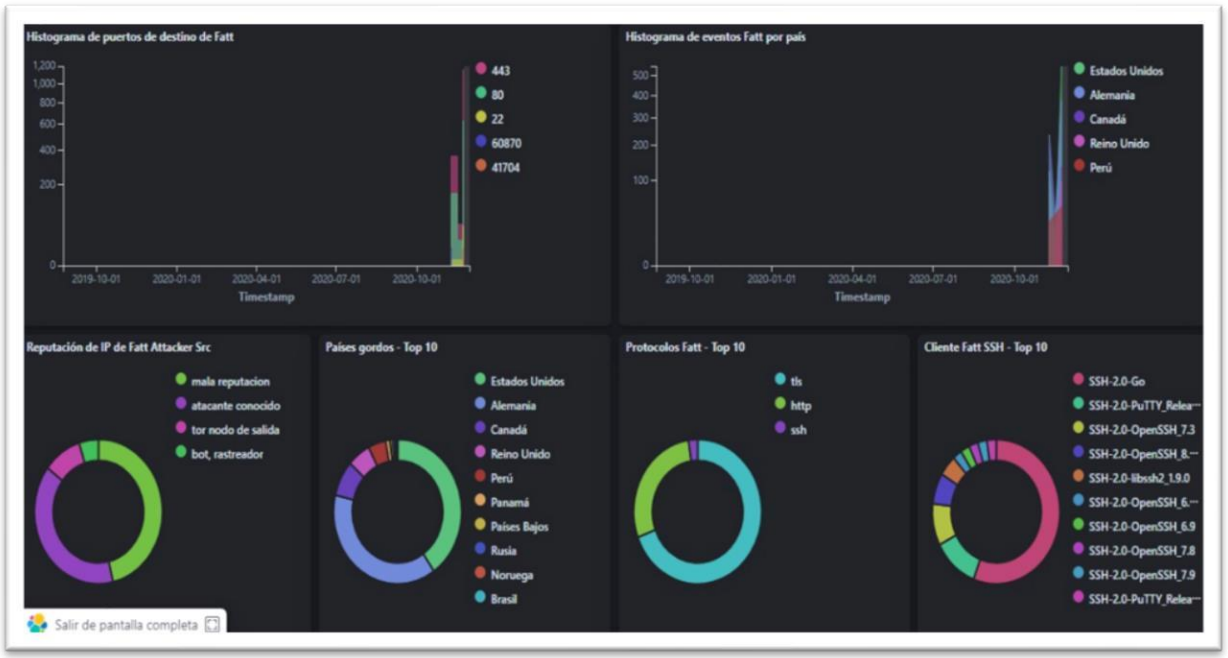
[Wed Oct 07 03:15:39.114839 2020] [:error] [pid 21468:tid 140496290637568] [client 176.113.115.214:48474] [client 176.113.115.214] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(?i:\\\\b(?:(?:s(?:t(?:d(?:dev(_pop|_samp)?)?|r(?:_to_date|cmp))|u(?:b(?:str(?:ing(_index)?)?|(?:dat|tim)e)|m)|e(?:c(?:_to_time|ond)|ssion_user)|ys(?:tem_user|date)|ha(1|2)?|oundex|chema|ig?n|pace|qrt)|i(?:s(null|_(free_lock|ipv4_compat|ipv4_mapped|ipv4| ..." at ARGS:content. [file "/usr/local/apache/modsecurity-owasp-old/base_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "125"] [id "950001"] [rev "2"] [msg "SQL Injection Attack"] [data "Matched Data: md5(found within ARGS:content: <php>die(@md5(HelloThinkCMF))</php>"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "190.117.184.238"] [uri "/"] [unique_
id "X315K7bZLEkYL8Mr-wSXhQAAAFE"]

[Wed Oct 07 03:17:26.683294 2020] [:error] [pid 2189:tid 140501323867904] [client 176.113.115.214:48630] [client 176.113.115.214] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(?i:\\\\b(?:(?:s(?:t(?:d(?:dev(_pop|_samp)?)?|r(?:_to_date|cmp))|u(?:b(?:str(?:ing(_index)?)?|(?:dat|tim)e)|m)|e(?:c(?:_to_time|ond)|ssion_user)|ys(?:tem_user|date)|ha(1|2)?|oundex|chema|ig?n|pace|qrt)|i(?:s(null|_(free_lock|ipv4_compat|ipv4_mapped|ipv4| ..." at ARGS:content. [file "/usr/local/apache/modsecurity-owasp-old/base_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "125"] [id "950001"] [rev "2"] [msg "SQL Injection Attack"] [data "Matched Data: md5(found within ARGS:content: <php>die(@md5(HelloThinkCMF))</php>"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "190.117.184.238"] [uri "/"] [unique_i
d "X315liCUCPD1QUWXdAmhSgAAAAg"]

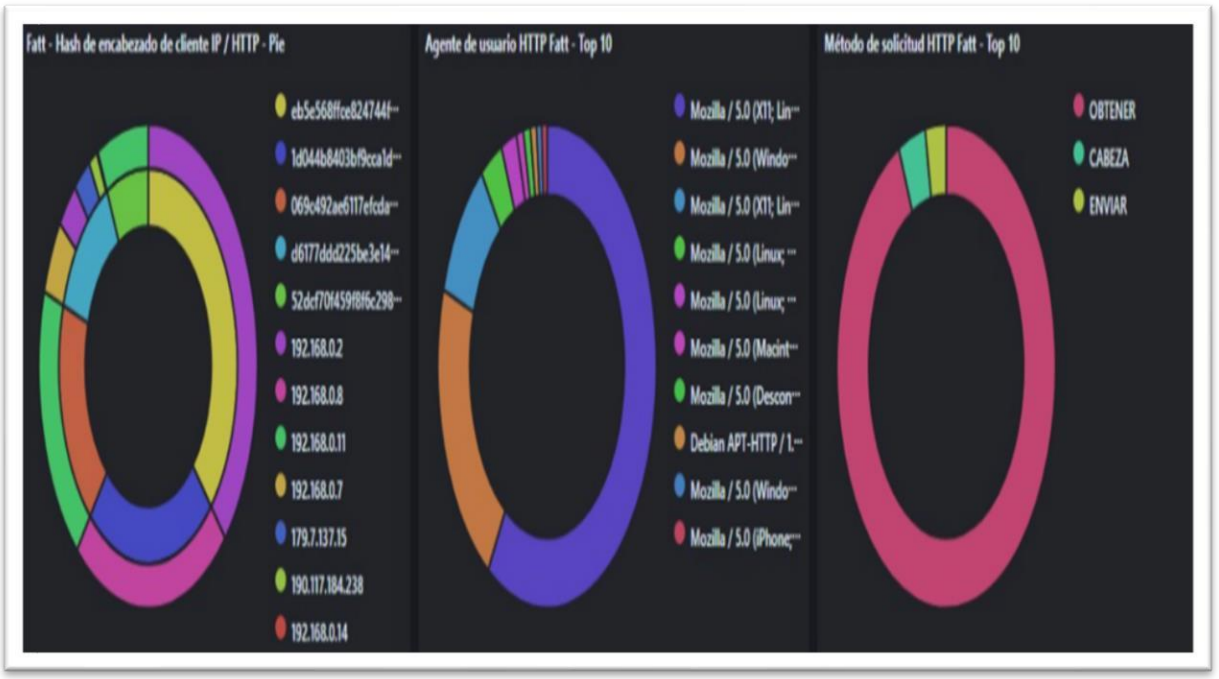
Barra de ataques de Dionaea



Ataque a email



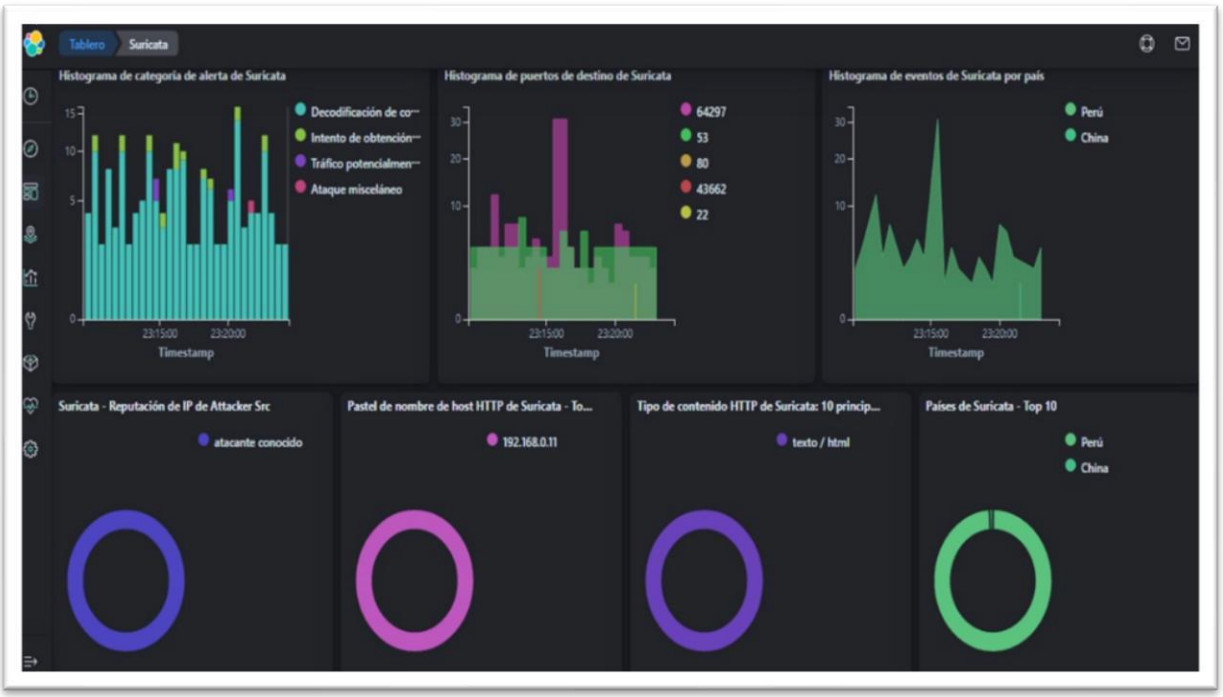
Ataques HTTP



Histograma de usuarios

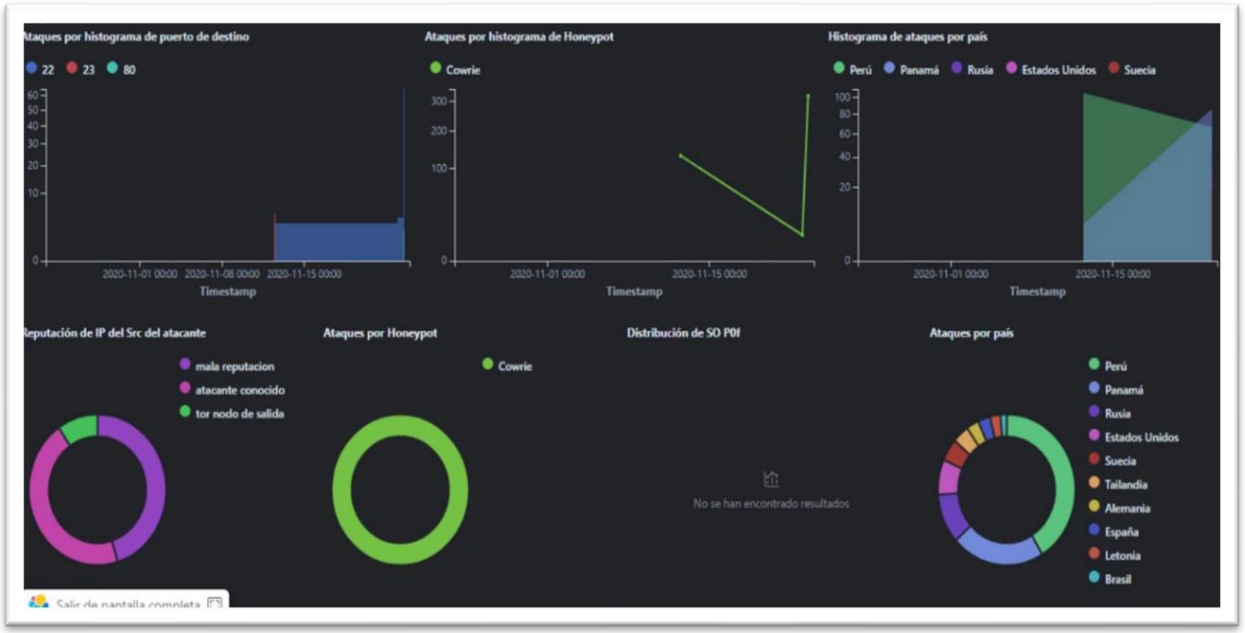
Reporte general por tipo

Histogramas de alertas

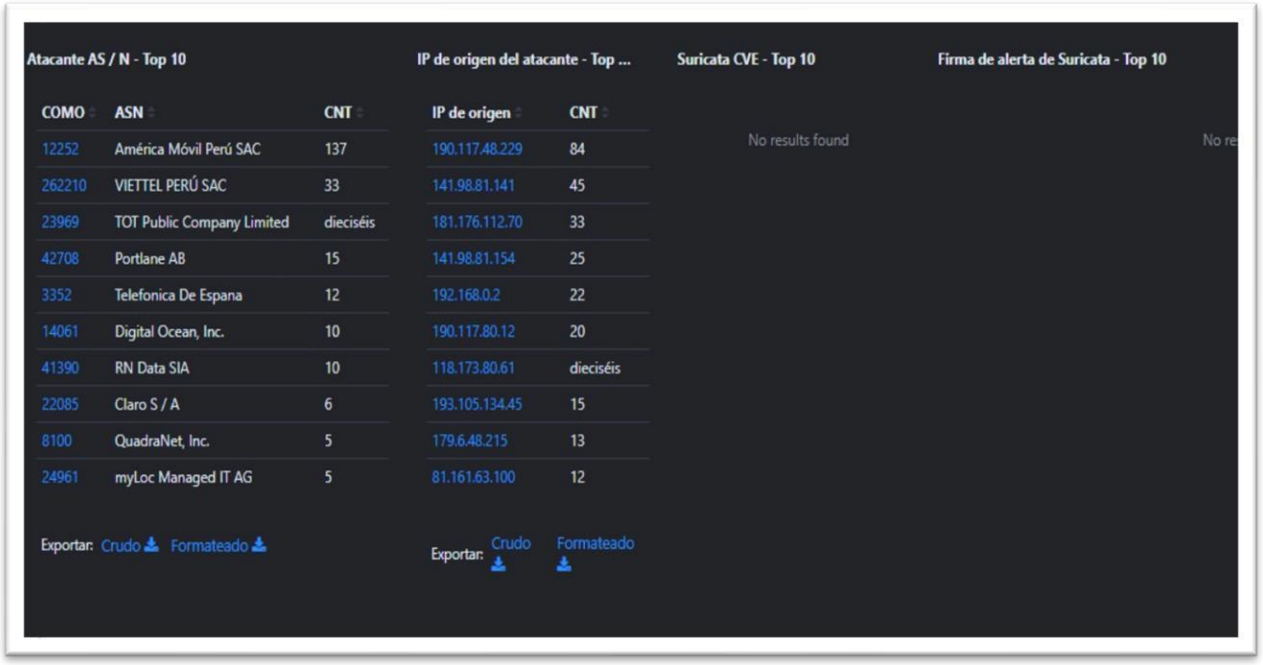


Reporte de ataque SSH

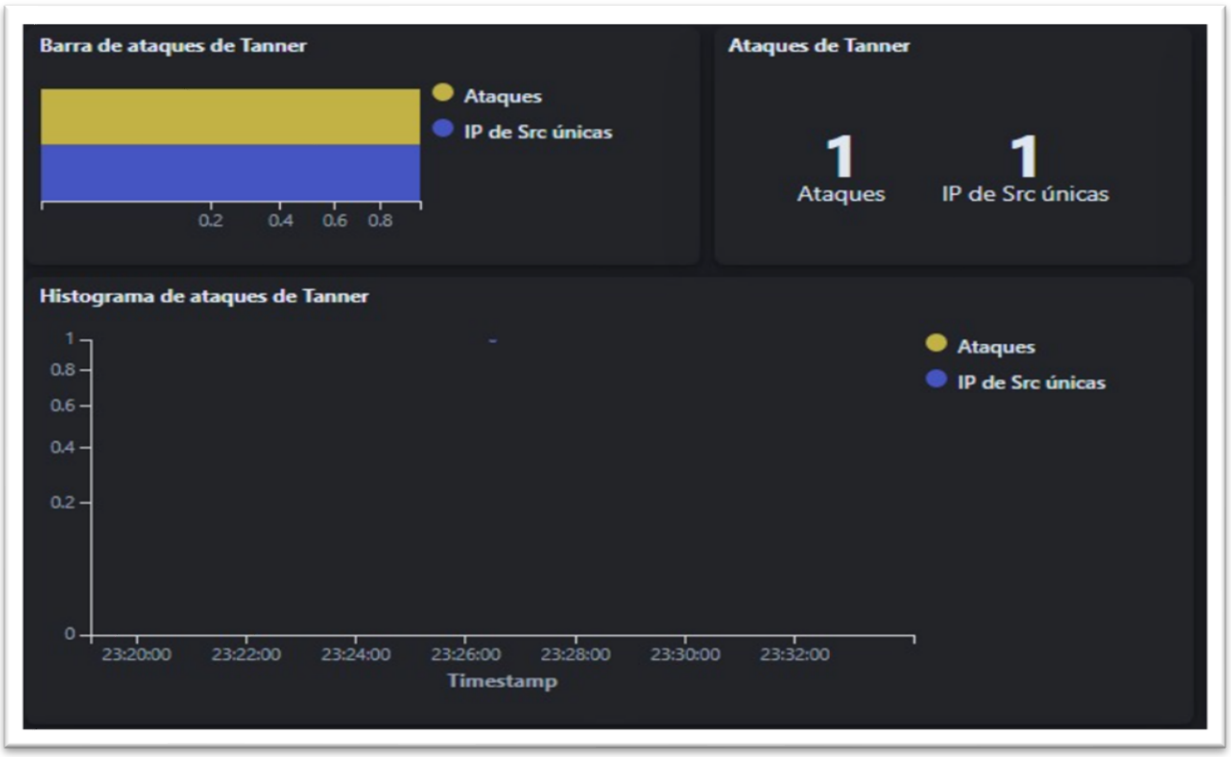
Histograma de ataques



Top de atacantes



Reporte de peticiones HTTP/HTTPS general



Reporte de ataques por puerto