"EVALUACIÓN DEL RENDIMIENTO DE HONEYPOT EN REDES TELEMÁTICAS."

"HONEYPOT'S PERFORMANCE EVALUATION IN TELEMATIC NETWORKING"

Giovanni Carlos Lorusso Montiel.
Universidad Iberoamericana Funiber – Unini, México
Orcid:0000-0002-3122-8142
namus15@gmail.com

Carlos E. UC Rios.
Universidad Iberoamericana Funiber – Unini, México
Orcid:0000-0003-1321-019X
carlos.uc@unini.edu.mx

RESUMEN

En una sociedad globalizada, la ciberdelincuencia se ha vuelto un problema importante, generando riesgos de información indispensable, como contraseñas, datos personales, entre otros. Sin mencionar, las grandes sumas de dinero que los ataques cibernéticos logran alcanzar cada año. Esta situación ha tomado tal magnitud, que las medidas de seguridad convencionales no son suficientes para brindarnos seguridad en un entorno digital. Por tal motivo, surge la necesidad de implementar nuevas herramientas de protección informática, de las cuales han destacado los "**Honeypots"**. Estos últimos ha tomado relevancia, además de proteger, proporcionar seguridad; se consideran sistemas de tipo "**trampa**" que sirve para observar los diferentes comportamientos de ciberataques para posteriormente analizar la intrusión, los métodos que se utilizaron. El presente artículo pretende como objetivo general, el estudio del comportamiento activo de un **Honeypot** para posteriormente determinar su rendimiento, precisar su grado de eficiencia en la detección y clasificación de intrusos de ciberataques. Para tal propósito, se implementará una metodología tecnológica, integrada por cinco (5) Fases: diagnóstico, diseño de un plan, recursos, monitoreo y evaluación, tal como lo plantea Arias (2016)**.** Se elaborará un estudio que implique el uso de un Honeypot con monitoreo constante en tres tipos de situaciones diferentes que simulen un ataque cibernético, en distintos grados de intensidad: sin ataques alguno, ataques inferiores a 5 ciclos por minutos (Ataques leves), ataques superiores a 10 ciclos por minutos (Ataques fuertes). Los resultados obtenidos son altamente aceptables; el honeypot obtuvo un 95% de eficiencia en la detección de ciber ataques simulados con un rendimiento de 95.4%.

Palabras clave: Antifraude - Honeypots, Ciberataque, Ciberseguridad, Rendimiento.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

ABSTRACT:

In a globalized society, cybercrime has become a major problem, generating risks of essential information, such as passwords, personal data, among others. Not to mention, the vast sums of money that cyberattacks manage to fetch each year. This situation has taken on such a magnitude that conventional security measures are not enough to provide us with security in a digital environment. For this reason, the need arises to implement new computer protection tools, of which the "Honeypots" have stood out. The latter has become relevant, in addition to protecting, providing security; They are considered "trap" type systems that serve to observe the different behaviors of cyberattacks to later analyze the intrusion, the methods that were used. The general objective of this article is to study the active behavior of a Honeypot to later determine its performance, specify its degree of efficiency in the detection and classification of cyber-attack intruders. For this purpose, a technological methodology will be implemented, consisting of five (5) phases: diagnosis, plan design, resources, monitoring, and evaluation, as proposed by Arias (2016). A study will be carried out involving the use of a Honeypot with constant monitoring in three different types of situations that simulate a cyber-attack, at different degrees of intensity: without any attacks, attacks of less than 5 cycles per minute (light attacks), attacks greater at 10 cycles per minute (Heavy Attacks). The results obtained are highly acceptable; the honeypot obtained 95% efficiency in detecting simulated cyber-attacks with a performance of 95.4%.

Keywords: Antifraud - Honeypots, Cyber-attack, Cyber-security, Performance.

INTRODUCCIÓN

En la actualidad el internet se ha introducido en nuestra vida de manera sorprendente. Por lo tanto, ocurre que cada vez más sean los ataques a los que están expuestos los dispositivos que poseen nuestras empresas, los atacantes quieren robar información importante que se encuentra en las computadoras infectando el ordenador, muchas veces es embarazoso liberarse del atacante una vez que infecte el ordenador. Sin embargo, se hace necesario la prevención de ataques para poder obtener seguridad en la red con la que estemos trabajando, además utilizando una buena monitorización podemos minimizar los ataques para proteger la información. Debe señalarse que es imposible que exista una seguridad perfecta, puesto que una de las primeras leyes de la seguridad informática es que si alguien dispone de tiempo y recursos podrá vulnerar el sistema más seguro, debemos tratar de poner la mayor cantidad de trampas que podamos a los atacantes, estudiar sus movimientos para anteponernos a los infortunios.

Este trabajo tiene como objetivo mostrar a los atacantes un sistema virtual que aparente el sistema real, con la intención de atraer (como la miel) a los atacantes simulando ser sistemas débiles o con fallas de seguridad, para atraerlos y monitorear todas las actividades que se realizan, de esa manera los ataques se efectuarán sobre ese sistema sin causar ningún daño al sistema real además de obtener información sobre las actividades ilícitas que realiza el atacante. El

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

desarrollo de este sistema conllevara una cantidad de beneficios para las organizaciones que la pongan en práctica. Por otra parte, el beneficio para las organizaciones será invaluable, pues con ello permitirá estar atento a los diferentes eventos u ataques haciéndolos visibles a través del servidor el cual detectará tempranamente.

Por otra parte, la creciente globalización de los sistemas informáticos, causada por la red de redes (**internet)**, ha traído ciertas consecuencias, como la vulnerabilidad de los sistemas de redes de comunicación. Esto último se puede ver reflejado en el aumento de los ataques cibernéticos que sufren los sistemas empresariales a medida que la tecnología avanza. Por tal motivo, diversos expertos recomiendan reducir el impacto de los ciber-ataques a través de herramientas informáticas especializadas; tales como antivirus, firewalls, entre otros. Sin embargo, estas no han podido ser suficientes del todo, en relación con pérdidas millonarias y de información relevantes. A consecuencia de lo anterior expuesto, surge la necesidad de una medida adicional que sea más efectiva, como es el caso de los Honeypots.

De igual forma, el termino Honeypot se traduce como **"tarro de miel"**, pero hace referencia a una herramienta informática de prevención de ataques cibernéticos. La idea principal es la de lucir como un sistema real, vulnerable de apariencia débil con relación a posibles atacantes. Su misión es la de atraer, desviar posibles ataques hacia sí misma. Del mismo modo, posee la capacidad de determinar a posibles sospechosos a través de la IP expuesta por ellos para determinar de esta manera, el nivel de vulnerabilidad existente de la red. En otras palabras, se trata de un método que protege al verdadero sistema, además, ayuda a develar detalles como la fuente principal de los ataques. Sistema sutil; que tiene sus ventajas al detectar a los posibles atacantes sospechosos; pero que al no ser implementado y usado correctamente; pudiera verse la red telemática vulnerable a ataques, robos de información, infección de virus en general, entre otros.

Así mismo, Casanova y otros. (2017)**,** realizaron una investigación sobre las redes de telefonía móvil como posible blanco de ataques debido a la gran información y datos que se pueden obtener, si se llegara a encontrar una puerta de acceso en un punto vulnerable de la red; y las redes señuelos como herramientas de defensa, con el fin de analizar y comprender las nuevas tecnologías que usa un atacante informático para realizar un ataque y poder así, determinando de esta manera el impacto que generaría en el sistema a proteger.

En relación con la problemática expuesta, León y Bonilla (2017), realizaron un diseño de infraestructura con la inclusión de dos equipos que permitan implementar los Honeypots para la recolección de información sobre posibles ataques. Se presenta la configuración y pasos para su instalación, así como imágenes que permitan validar su instalación y la información recolectada para posteriormente ejemplificar una de las acciones que se toma frente a estas vulnerabilidades para aumentar la seguridad conforme a patrones de ataque encontrados.

Cabe considerar por otra parte, el trabajo realizado por *Matus* Mihok. (2017), el cual explica el funcionamiento de cada herramienta de los honeypots; analizando los resultados obtenidos en una serie de scripts implementados en Python, con el fin

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

de analizar la red. Así mismo, examinar el mecanismo de seguridad basado en tres tipos de diferentes honeypots de baja interacción (inferiores a 5 ciclos por minuto) de códigos abiertos; los cuales identifican las amenazas y los métodos utilizados en contra de cada red. De esta manera, con herramientas de visualización, se observaron los posibles ataques y medidas en las cuales se identifican las partes de red vulnerables. Además, se usaron herramientas para la intrusión de trafico de red y pruebas de testeo para verificar la eficiencia del sistema honeypot implementado.

Por último, cabe señalar a Martínez (2018)**,** en su trabajo de investigación, emplea un proceso de optimización de los honeypots; así mismo, se realizan consideraciones a la forma, uso y responsabilidad de la utilización de los honeypots. Logra analizar la implementación de los honeypots de acuerdo con su arquitectura lógica y en cómo dicha arquitectura, se relaciona con los demás elementos de la red local.

Por lo tanto, la tecnología va creciendo de forma desproporcionada la cual va estrechamente ligada a la seguridad en las conexiones de internet de las compañías, esto ha variado mucho, las compañías buscan actualizase cada día para mejorar sus servicios, así como también busca que su personal se actualice para que se servicio sea más confiable al momento de trabajar con redes.

Por tal motivo, diversos expertos recomiendan reducir el impacto de los ciber-ataques a través de herramientas informáticas especializadas; tales como antivirus, firewalls, NIDS, DMZ, entre otros. Sin embargo, estas no han podido ser suficientes del todo, en relación con pérdidas millonarias y de información relevantes. A consecuencia de lo anterior expuesto, surge la necesidad de una medida adicional que sea más efectiva, como es el caso de los Honeypots.

FUNDAMENTACIÓN TEÓRICA

Honeypot

El termino Honeypot apareció por primera vez en el libro **"El hueco del cuco "(1990)** de Clifford Stolls**,** en el cual habla de la organización "The Honeynet Project", cuya función principal fue la investigación de sistemas de prevención y detección de intrusos. Sin embargo, autores como Spitzner (2017), define al Honeypot como **"un recurso en cómo se configura para ser usado, atacado e inclusive comprometido".**

Analizando la traducción literal de Honeypot, se trata de **"tarro de miel"**. En este caso se usa estratégicamente dicho significado para hacer referencia al sistema que aparenta ser débil o fácilmente vulnerable hasta tal punto de parecer atractivo para un ciber-atacante. En pocas palabras, un honeypot viene a ser, una trampa informática para identificar, desviar o contrarrestar algún intento de violación de la seguridad de una red de información. El conjunto de dos o más honeypots, se considera un sistema honeynet.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

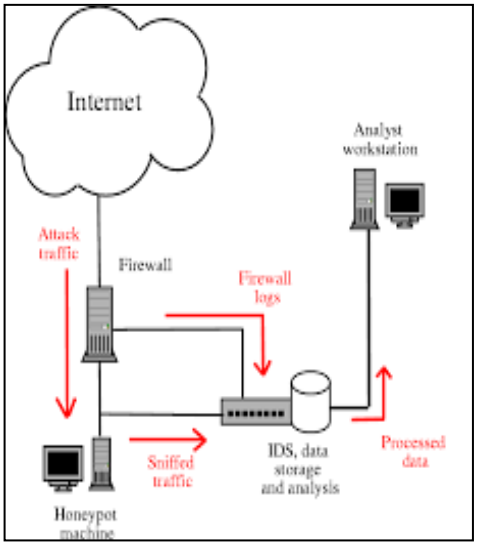

Figura A

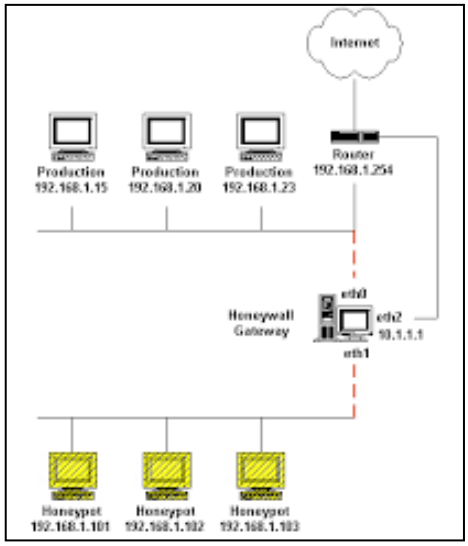

Figura B

Figura 1. Estructura de una Honeynet (2 o mas Honeypots).
Fuente: Google, 2013

En la figura 1.A, se puede observar la estructura de una honeynet **(Red trampa**) desde el punto de vista técnico, es una red de sistemas de producción o servidores, diseñada para ser comprometida y conformada por varias Honeypots. La figura B, muestra otra forma de conectar el honeypot al servidor principal, lo importante es demostrar el punto crucial que asegura el éxito de la honeynet es la creación de un ambiente que permita monitorizar todos y cada uno de los movimientos que el posible intruso llegue a ejecutar dentro de ella.

Es importante destacar, que los Honeypots también tiene la función de recopilar información acerca de estrategias y patrones del presunto atacante. En este mismo orden de ideas, un honeypot puede contener en una computadora, datos o un sitio de red que parecen ser parte de otra red. Cualquiera sea el caso, se deben aislar y proteger, con la intención de monitorearla y obtener la mayor información posible sobre lo ciber atacantes.

Durante la década de 2016 y 2017, se presentaron varios casos de malware que, debido a su manera de operar, se definían como **Botnet** (red de dispositivos que operan de forma automática). Estos ataques aprovechaban las vulnerabilidades presentes en dispositivos **IoT,** o bajas medidas de seguridad como credenciales por defecto, para acceder a ellos, controlarlos o borrar sus datos. Estos fueron Tsunami**,** Amnesia (una modificación del anterior, que borraba los datos de los dispositivos), Gafgyt y BrickerBot.

En la figura 2, se observa a un servidor dedicado central y un conjunto de estaciones que conforman una red con servidor dedicado (**honeypot)** y sus terminales (**Botnet)**. Es necesario mencionar que este tipo de servidor consigna todos sus recursos a proporcionar la información, así como también atender las

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

peticiones de otro ordenador u ordenadores que han contratado sus servicios, a la vez permite instalar aplicaciones que serán de ayuda y beneficios para la empresa.

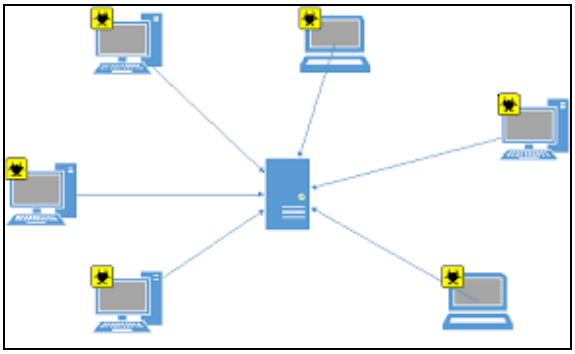

Figura 2. Estructura de un sistema de red.
Fuente: Torres, 2014

Para profundizar más en el funcionamiento de este tipo de sistemas, se debe mencionar que cuando un Honeypot sufre un ataque, este puede capturar, dependiendo la configuración, la actividad del atacante de acuerdo con los datos como las direcciones IP, puertos usados, protocolos usados, entre otros. Dicha información es extremadamente importante, contribuye a determinar los patrones o estrategias que se emplean para vulnerar la seguridad de una red. Además, puede ser usada para detectar el origen de un programa maligno, desarrollar firmas para IDS (Detección de intruso) o IPS, entre otros.

Para lograr todo lo anteriormente descrito se debe crear lo que se conoce como una **Honeynet,** el cual trata de un conjunto de Honeypots agrupados de alta interacción que contienen sistemas operativos y servicios, dispuesto con la intención de lograr mayor interacción con los atacantes. Entre los servicios que se pueden contener en dicho conjunto se encuentran correo electrónico, base de datos, Web, NTP, FTP, equipos de conectividad como router, entre otros.

Toda la Honeynet se configura dentro de un en sistema operativo, ya sea Linux o Windows, de tal manera que cualquier actividad dentro de esta es considerada maliciosa o no autorizada, activando herramientas como IDS, firewall y sus correspondientes logs de actividad para analizar la información recolectada y encontrar detalles sobre el ataque. Permitiendo detectar a tiempo lo que estan haciendo, a la vez usar la informacion para impedir obtener la informacion que desean.

Tipos de Honeypots

Conociendo el funcionamiento de los Honeypots que exponen las vulnerabilidades de las redes; sin mencionar que poseen una taza leve (estadísticamente hablando), proporcionan falsos positivos perfeccionando los sistemas de seguridad, se expondrá a continuación según sus tipos. De acuerdo

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

con Spitzner (2017)**,** dichos sistemas se pueden clasificar según su uso y la forma de implementación en: Honeypots de producción y Honeypots de investigación. Además, existen Honeypots físicos y virtuales, que se derivan de la clasificación anterior.

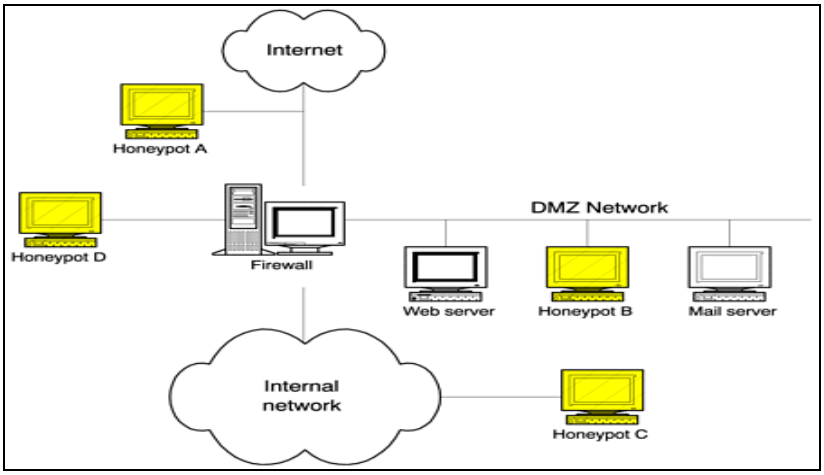

Figura 3. Estructura y ubicación del Honeypot.
Fuente: Acién 2018

En la figura 3, se puede observar la estructura de una honeynet (2 o más honeypots); donde están los honeypots de software virtuales y el físico que es un servidor dedicado actuando como un honeypot físico. Cabe destacar que la forma de instalar el honeypot dependerá de la necesidad de la organización, como también de los recursos con que cuenten para su instalación, puesta en marcha, así como su mantenimiento.

De igual manera, según Acién A. (2018)**,** los honeypots se pueden clasificar en base a diferentes criterios, que nos permiten saber detalles sobre su comportamiento o estructura real. Además de conocer el desafío del honeypot es hacerse atractivo a su atacante, detectar su comportamiento y respuesta por la tanto se pueden clasificar en base a la interacción que tengan con las conexiones entrantes, esto los divide en:

En la figura 4, se observa la clasificación del honeypot, la cual se realiza teniendo a cuenta los siguientes criterios el ambiente donde se va a implementar y el nivel de interacción, todo esto nos permite entender su operación, utilización al momento de implementar su utilización dentro de la red o servidor. Posteriormente nos dará a conocer los diferentes tipos y categorías existentes.

Baja interacción: son honeypots que tienen respuesta básica a ciertos comandos, pero no van más allá, reproducen una parte limitada del comportamiento real del sistema. Estos Honeypots emulan servicios y/o sistemas operativos. Su instalación es fácil, al emular servicios o sistemas, se considera un recurso de riesgo limitado. He aquí su principal desventaja, por ser un sistema emulado, el nivel de interacción es menor, por tanto, la información recogida también lo es. Las soluciones de Honeypot más comunes de baja interacción son: Nepenthes, Honyed,

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

Honeytrap, TinyHoneypot, hay distribuciones de Linux que reúnen a estos Honeypots como Backtrack Kali Linux5, y HoneyDrive.

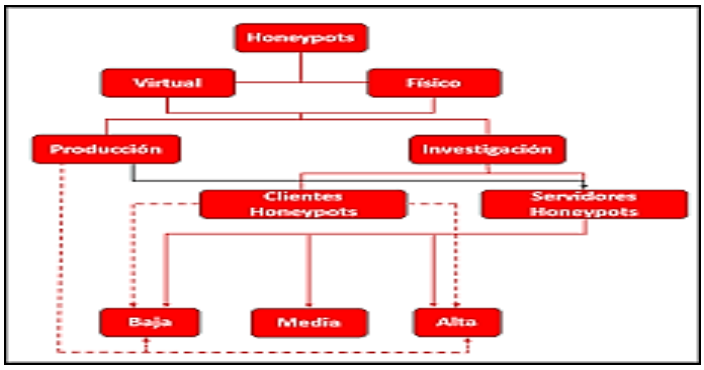

Figura 4. Diagrama estructural del honeypot.
Fuente: Acién, 2018

Alta interacción: ofrecen un sistema con las características que el dispositivo real, con acceso total al atacante, las vulnerabilidades son completamente explotables. Se pueden recopilar más datos, pero también suponen un riesgo mayor, la razón es que el sistema se puede ver comprometido. Este tipo de Honeypots son más difíciles de implementar, Spitzner (2017), señala que no emulan servicios ni sistemas, sino que los servicios son montados sobre sistemas operativos completos, y esto implica un riesgo inherente en su uso hacia la red de una organización. A diferencia de los anteriores, estos Honeypots recolectan gran cantidad de información que dependerá de la complejidad de estos. En vista de que se ha aumentado el riesgo, estos Honeypots requieren de controles específicos para que no se conviertan en plataformas de ataques hacia la red de producción. En consecuencia, podemos mencionar además que existen Honeypots físicos y virtuales, derivados de la clasificación anterior.

	Alta interacción	Baja interacción
Simulación	Simulan servicios reales, aplicaciones o dispositivos. Su identificación suele ser compleja.	Simulan servicios o sistemas operativos. Tiene muchas posibilidades de detectarse como trampa fácilmente.
Amenazas	Descubrir nuevos ataques o comportamientos anómalos anteriormente no detectados.	Descubrir herramientas automatizadas o de vulnerabilidades ya conocidas en servicios concretos.
Información	Capturan una gran cantidad de información de gran valor por contener en ocasiones registros de ataques no conocidos. Su implementación es perfecta para investigaciones y análisis en profundidad.	La cantidad de recursos recopilados es limitada. No son muy aconsejables si se quiere realizar un análisis en profundidad del sistema.

Cuadro 1. Honeypot De alta y baja interacción. **Fuente**: Acién, 2018

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

Honeypot de Producción

Estos Honeypots se ubican en la red de producción de una organización, proporcionando servicios similares a dicha red. Como objetivo, el Honeypot de producción busca desviar el riesgo de un ataque de la red de producción y ayudar a asegurarla de acuerdo con las actividades que los intrusos realicen en el Honeypot. Si el intruso obtiene de alguna forma el control del Honeypot de producción, este puede bloquear las conexiones salientes, limitando el accionar del atacante solo al interior de este. El Honeypot de producción captura y defiende.

Componente	Especificación técnica
Procesador	Intel Dual Core 2 GHz
Memoria RAM	2 Gb
Disco duro	250 Gb
Adaptador de Red	Fast Ethernet 10/100 Mbps

Tabla 1. Requerimientos de Hardware para el Honeypot.
Fuente: Lorusso, 2021

Honeypot de Investigación

Su propósito es ser atacado, pero con el objetivo de ser también una herramienta didáctica que permita aprender de patrones y estrategias de los atacantes y si se requiere, para formular estrategias de defensa de los sistemas contra amenazas nuevas o existentes. Es usado en centros académicos, sectores gubernamentales, etc. Este Honeypot solo captura información para ser analizada. Este tipo de Honeypot suele tener su propia conexión hacia Internet, totalmente aislado, evitando así la necesidad de defender la red de producción de posibles ataques que se produzcan desde el Honeypot y permitiendo solo la captura información. Volviendo a la clasificación de los Honeypots, tanto de producción como de investigación pueden ser de alta o baja interacción, de acuerdo con el grado de interacción con los atacantes y el riesgo que eso implica.

Figura 5. Explicacion de los tipos de honeypots.
Fuente: Del Valle E. (2019).

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

Cabe mencionar que Del Valle E. (2019), afirma que la herramienta de Honeynet está enfocada en una red compleja de sistemas que permiten por su diseño ser sondeada, atacada y comprometida por un determinado intruso que trate interferir o apropiarse de la información, de una red completa conformada por un sin número de sistemas que están a la expectativa de recibir ataques y encargados de monitorear el control de acciones. También suele ser recurso que suele ser un real blanco cuyo trabajo es que este sea atacado para obtener información del atacante.

El presente estudio se llevará a cabo como una investigación tecnológica, la cual puede ser definida, de acuerdo con Del Valle E. (2019)**,** como aquella que "tiene como fin obtener un conocimiento para lograr modificar la realidad en estudio, vinculando la investigación y la transformación" (: p.80). En este orden de ideas se puede decir que se busca cambiar la realidad existente, a través de la obtención de un conocimiento práctico en vez de un conjunto de explicaciones teóricas.

En cuanto al diseño de investigación, se elige la investigación de campo experimental. De acuerdo con Verona y otros (2016). La de campo o investigación directa es la que se efectúa en el lugar y tiempo en que ocurren los fenómenos objeto de estudio, ya que esta cuenta con la característica de recolectar información directamente de la realidad, en otras palabras, se reunirán los datos desde las fuentes primarias, es decir el monitoreo continuo de los Honeypots.

Cabe mencionar que la presente investigación se llevará a cabo a través de dos fases: La primera en la que se llevarán a cabo actividades exploratorias y de recolección de datos para la construcción de documentos, la segunda fase que se centrará en diseñar un modelo de análisis de sistema de red Honeypots, el cual se instalará para registra toda la información posible sobre el sistema de ciberseguridad que luego será empleada para evaluar la eficiencia y formarán parte de la investigación científica experimental.

También existen varios tipos de honeynets. Arias E. (2020), sostiene que de acuerdo con el desarrollo que este tipo de red ha experimentado, y pueden ser llamadas generaciones de honeynets: Honeynets de primera generación (Gen I), honeynets de segunda generación (Gen II) y honeynets de tercera generación (Gen III). Los cuales se diferencian en los métodos y técnicas que se usen para implementar dichos requisitos.

Cabe resaltar un aspecto importante en esta investigación científica: **"La evaluación del rendimiento del Honeypot"**. Definido por León C. Camilo A. – Bonilla D. María (2017), de la siguiente forma: "El rendimiento del Sistema de Información o de la maquina es la cantidad de trabajo realizado por un sistema informático. Dependiendo del contexto, un alto rendimiento de equipo puede incluir uno o más de los siguientes:Tiempo de respuesta corto para una determinada pieza de trabajo0, Alto throughput (tasa de procesamiento de trabajo), Baja utilización de recursos computacionales, Alta disponibilidad del sistema de computación o de la aplicación, Rápida (o muy compacta) compresión y descompresión de datos, Gran ancho de banday Tiempo corto de transmisión de datos"

Luego de lo expuesto anteriormente, queda confirmado que el rendimiento de un sistema informático puede ser evaluado en medibles términos técnicos, utilizando uno o más de los parámetros mencionados anteriormente. No obstante,

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

dicho concepto tiene un enfoque técnico-científico, por lo cual se expone la definición de Martínez C. Kevin (2018), en el cual menciona que “La palabra rendimiento en el equipo, quiere decir lo mismo que el rendimiento de otros contextos; significa ¿Qué tan bien está haciendo el sistema su trabajo?, ¿Qué es lo que se espera que haga?"

Ahora, ya que dicho artículo de investigación involucra la participación de software, se debe dar una definición en este ámbito. De acuerdo con Verona y otros (2016) “En un producto de software el rendimiento se mide como la capacidad del sistema de utilizar los recursos de hardware de forma eficiente”, en otras palabras, el rendimiento de un software tiene que ver con el uso que este da a los recursos externos para dar una respuesta rápida y cumplir con su propósito, además, se puede decir que se trata de un aspecto de la calidad de software.

Otro punto que destaca Verona es que para evaluar el rendimiento de un software se deben emplear pruebas de rendimiento, las cuales define como aquellas que “tienen como objetivo estresar el sistema realizando demandas fuera de los límites para los que fue diseñado el software”. Por su parte, Acien. (2018). Acién, menciona que “Este tipo de prueba se realiza, desde una perspectiva, para determinar lo rápido que realiza una tarea un sistema en condiciones particulares de trabajo. También puede ser utilizada para validar y verificar algunos atributos de calidad, tales como la escalabilidad, fiabilidad y el uso de los recursos”.

METODOLÓGIA

Este trabajo de investigación, pretende analizar los objetivos propuestos, así mismo resolver un problema existente, enmarcado en una exploración de campo experimental; según García (2017). “tiene como fin obtener un conocimiento para lograr modificar la realidad de estudio, vinculando la investigación y la transformación, en otras palabras, posibilita el análisis sistemático de un determinado problema con el objeto de describirlo, explicar sus causas y efectos, comprender su naturaleza y elementos que lo conforman, o predecir su ocurrencia; los datos se recaban directamente de la realidad, provenientes de fuentes primarias y puede ser de tipo exploratorio, descriptivo y explicativo. Esta investigación describe las siguientes fases:

Diagnosticar la viabilidad de la implementación del Sistema Honeypots.

Diseño del modelo para establecer las políticas y herramientas aplicables en la identificación de debilidades.

Instalación de equipos y/o recursos necesarios para la Honeypot.

Registrar y evaluar las incidencias y rendimiento del diseño preliminar de un Honeypot.

Evaluar el comportamiento y rendimiento de Honeypot en las redes telemáticas. Así mismo por su naturaleza científica experimental, no necesita de recolección de información, sin embargo, se utilizará un cuestionario con 16 preguntas en la primera fase exploratoria para la detección y clasificación de los posibles intrusos en relación con los ciber-ataques, con escala de Likert, también se recogerá información de los datos del Monitoreo y la evaluación que se llevará a cabo en el sistema de Honeypots en su proceso dinámico. En la segunda fase se diseña

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

un modelo de análisis de sistema de red honeypots, la cual registra la información obtenida; y en una siguiente fase se realiza la evaluación del sistema por medio de instrumentos de medición de rendimiento a través de informes o reportes directos del sistema de ciberseguridad. Los datos obtenidos en este punto serán analizados evaluados e interpretados de esta manera, y así poder justificar la naturaleza de dicho proyecto científico experimental. De esta forma, este proyecto de investigación no presenta población específica como tampoco una muestra determinada. Sin embargo, se utilizarán 25 estudiantes de laboratorio para efectos solo de entrevistas y encuestas.

EVALUACIÓN DEL RENDIMIENTO DE HONEYPOT

El sistema honeypot es un conjunto de Bots (computadoras terminales) conectadas y enlazadas unas a otras y al mismo tiempo, gobernadas por un servidor central que simula la actuación de un honeypot. Este servidor central que opera como honeypot, presenta puertos el cual se comunica con otros equipos, bien sea internos o externos a través de internet. Es administrado con protocolos y códigos afines entre los equipos. Si dicho protocolo o códigos fueran distintos al conocido; el honeypot considerará un posible sospechoso. **¿Cómo sabrá el honeypot si se enfrenta a un posible atacante?** El honeypot, enviara un código a través de un ping al posible sospechoso; si el posible sospechoso, no responde a la petición, será más que suficiente para que el honeypot agregue al posible intruso en una lista de desconocidos, intrusos o sospechosos.

Si el honeypot, recibiera una respuesta del ping enviado a través de uno de sus puertos; el honeypot determinará a través de dicha respuesta, si es un Ip conocido o no lo es. Por ejemplo, un honeypot podría tener puertos que respondan a un escaneo de puertos, Ip o contraseñas débiles. Los puertos vulnerables podrían dejarse abiertos a propósito, para así, atraer a posibles atacantes o sospechosos al entorno de la red honeypot, en lugar de la verdadera red telemática en servicio. Dichos procesos son monitoreados y guardados en el historial de operación de la red. Al monitorear el tráfico que ingresa al honeypot, se puede evaluar lo siguiente a continuación:

Procedencia de los cibercriminales;
Nivel de amenaza.
M*odus operandi* que se está empleando;
Datos o aplicaciones interesados por sospechosos;
Eficiencia de las medidas de seguridad empleadas para identificar y detener a los ciberataques.

Llegado a este punto es necesario plantear el objetivo principal del presente artículo de investigación, el cual trata de monitorear el rendimiento de un sistema Honeypot en la detección y clasificación de intrusos en ciber-ataques y cuyos resultados generarán políticas de seguridad en cuanto medidas preventivas se refiere, verificar los puntos de acceso del sistema, con el fin de tomar las medidas necesarias para poder contrarrestar los riesgos u atacantes.

Con lo anteriormente mencionado queda claro que se obtendrán datos directamente de los Honeypots, por los que se analizarán a través de la siguiente

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

estructura: Control de datos, procesamiento de datos, captura de datos y análisis de los datos.

En este mismo orden de ideas, las técnicas de análisis de datos en esta investigación se fundamentan en:

La Monitorización constante de la red a través de software abierto: Se encarga de determinar la cantidad de solicitudes entrantes y salientes de la red honeypot ubicada detrás del firewall de la red telemática. También habrá un administrador de sistemas visualizando toda actividad en el proceso de tráfico de la red.

Evaluación de resultados obtenidos: Se refiere a que, terminado todos los procesos de evaluación de la red, se procederá a estudiar dichos resultados para determinar a través de procesos estadísticos, software y análisis numérico, el punto de inflexión optimo y así poder precisar, si el rendimiento de la red es óptimo o no.

Anteriormente se ha mencionado que la investigación se llevará a cabo en dos fases. La primera fase ya descrita, la segunda fase se diseñará un modelo de análisis de sistema de red Honeypot, este trabajo se realizará de manera más profunda en la revisión de intrusos lo cual permitirá simplificar los procesos a los cuales será sometido el sistema, cabe destacar que también se pueden simular ataques para saber la efectividad del honeypot en la red por lo cual se presentan dos tipos de red: Red telemática y Red de Honeypot sobre la red telemática.

A ambas redes se le realizaron pruebas de monitoreo por separado y trabajando en conjunto. Todo lo anterior con el propósito de determinar el rendimiento y el grado de eficacia de la red Honeypot. Además, se busca identificar el nivel de seguridad, usando como principal método el antivirus Kaspersky. Tal como lo menciona su fabricante, **Kaspersky Anti-Virus** es un antivirus que realiza una excelente combinación de protección reactiva y preventiva, protegiéndote eficazmente de todo tipo de programas malignos. Adicionalmente, Kaspersky **Anti-Virus,** también se encarga de proteger el registro de la computadora y todo el sistema contra programas potencialmente peligrosos como los spyware.

Para verificar lo anterior se efectúan tres pruebas de ataques simulados que se explica a continuación:

El sistema de red de honeypot con servidor dedicado que opera como honeypot físico (también existen honeypots y honeynets virtuales que operan en el servidor). Determina a través de la base de datos, los Ip conocidos bien sea internos o externos de la red.

Si el Ip es conocido (el servidor sabrá que es conocido a través de múltiples peticiones de ping enviadas), dicho servidor actuara de manera normal. Si el Ip es irreconocible, el servidor lo tomara como un posible sospechoso y lo agregara a una lista negra. Obviamente, si el servidor envía peticiones y no son contestadas o reconocidas, el servidor tomara a este como un posible sospechoso y atacante.

El servidor al recibir múltiples peticiones de respuestas simultaneas, tomara al cliente como un atacante directo, debido a la saturación de peticiones. Inmediatamente, lo invitará y lo atraerá a la red de honeypot para proteger a la red telemática de dicho atacante.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

El honeypot además de detectar posibles atacantes, los distrae atrayéndoles hacia sí misma. Los absorbe, los engloba y trata de descubrir los intereses de los atacantes. Ejemplo: La información interesada, datos, claves, entre otras.

Las fases que se usaron en este proyecto para medir el rendimiento del honeypot, fueron de tres pruebas de ataques. Una, donde no hubo ataque (para determinar el comportamiento del honeypot). Dos, con ataques inferiores a 5 ciclos por minutos (5 minutos o ataques leves). Tres, con ataques fuertes, superiores a los 10 ciclos por minutos (10 o más minutos o ataques fuertes). Cabe destacar que aun haciendo uso del honeypot, se necesitan programas de protección y seguridad. El honeypot no elimina intrusos; solo los atrae y distrae.

Después de haber evaluado las tres fases, se crearon gráficos para visualizar mejor, los datos obtenidos. Se aplicaron fórmulas que miden el rendimiento de las máquinas y se obtuvo un resultado óptimo en cuanto al rendimiento del honeypot.

Dichas fases son tres y son las siguientes:

Monitoreo de red Honeypot sin ataques: La red se mostró sin complicaciones. Esta prueba se efectuó con el propósito de verificar que la red de Honeypot se encontraba funcionando plenamente y también para efectos comparativos al momento de la evaluación del rendimiento.

Monitoreo de red Honeypot con ataques menores a 10 ciclos simulados (Leve): En esta prueba de 8 minutos se pudo observar que la red Honeypot identifico muchos más atacantes con respecto a Kaspersky. En este caso la red detecto una cantidad de 60% con respecto a Kaspersky que solamente detecto un 40% de las amenazas.

Monitoreo de Honeypot con ataques mayores a 10 ciclos simulados (Altos): El sistema Honeypot cumplió óptimamente su labor en identificar a ciber atacantes simulados, se encargó en desviar a un 70% de atacantes hacia la red ficticia. En esta prueba de duración de 12 minutos, la red Honeypot demostró un nivel de rendimiento óptimo; su desempeño en identificar a intrusos fue exitoso. Consistió en una monitorización del comportamiento del honeypot, un servidor dedicado que emulaba la función del honeypot y un software libre programado para honeypot Dbt (Direct Base Transfer o transferencia de datos directo). Esta monitorización logro medir el tiempo de duración y posteriormente, medir su rendimiento a través de una fórmula matemática que mide el rendimiento:

$$(CPI = \sum_{i=1}^{n}(CPIi \,.\, FIi) \;.$$

Donde **CPI**, representa los ciclos por instrucción, y **Fi**, representa la frecuencia de instrucción. Tomando en consideración, sus ciclos con relación a porcentajes de productividad y según los recursos usados por dicha red. Todos los ataques fueron simulados en la entrada de Xploits (**Virus**) al servidor. El Honeypot detectaba todos los ataques que fueron simulados para el estudio de su comportamiento y finalmente, determinar su rendimiento total. Se aclara que cada ciclo, representa un minuto de duración; entonces, si los ciclos son inferiores a cinco por minutos, se hablara entonces de ataques leves; por el contrario, si los ciclos superan los diez ciclos por minutos, se hablara entonces de ataques fuertes. Cabe resaltar que, los ataques fueron simulados usando distintos tipos de computadoras

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

que, en conjunto y sincronizadas entre sí; atacaban al servidor de honeypot cada determinado tiempo. Es allí, como se puede determinar el rendimiento del honeypot.

RESULTADOS DE INVESTIGACIÓN

En cuanto a los resultados obtenidos, primeramente, se debe analizar las siguientes graficas a continuación: Dichos resultados se pueden ver reflejados en las siguientes graficas:

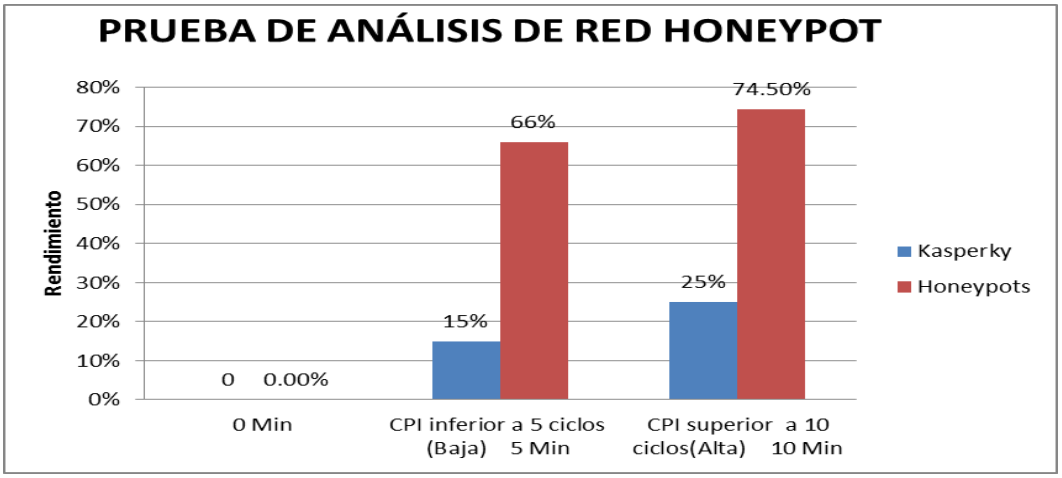

Gráfico 1. Rendimiento de Honeypot.
Fuente: Lorusso, 2021

En la gráfica 1, se puede observar como el honeypot se comporta en relación con el antivirus Kaspersky**.** En su inicio, el honeypot no mostro cambios; debido a que no hubo ataques. Sin embargo, en la siguiente fase de análisis, la red detecto el primer ataque durante los cinco primeros minutos por lo que fue detectado e inmediatamente anulado por la red honeypot. Posteriormente detecto más amenazas, pero su rendimiento y plan de acción permitió mantener la red fuera de peligro. Se observa también en la gráfica, las coordenadas de eje Y, denotan la cantidad de porcentajes y las coordenadas del eje X, denotan los ciclos por minutos. En ciclos inferiores a 5 ciclos por minutos, se observa el rendimiento del honeypot en conjunto con el antivirus de la red. El Honeypot mostro un 66% en su rendimiento. En ciclos superiores a 10 por minutos, el honeypot mostro un rendimiento en porcentajes de 74.50% en relación con el antivirus de la red.

El análisis de red demuestra un rendimiento óptimo por parte de la red. A continuación, se observa en la siguiente gráfica:

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

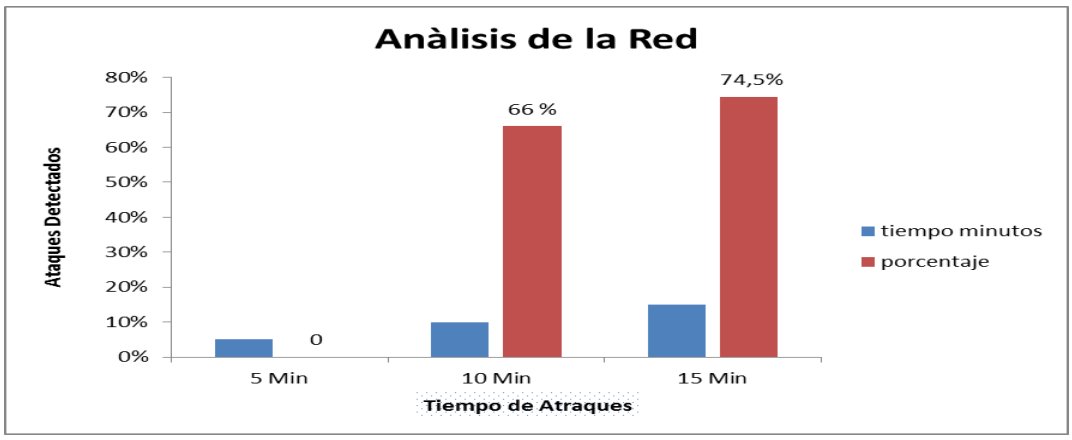

Gráfico 2. Ataques detectados.
Fuente: Lorusso,2021

Aun así, será necesario determinar matemáticamente a través de una formula ya mencionada anteriormente, que determinará el rendimiento de la red Honeypot. Para ello se empleará la siguiente ecuación, en la que se toma en cuenta los ciclos por eventos efectuados que fueron de 5.3 ciclos por instrucción. Cada ciclo representa 1 minuto de tiempo. Los valores de X1, X2, X3, serán de 1,2,3 correspondientemente: X1 = 1; X2 = 2, X3 = 3. La siguiente fórmula empleada a continuación, determinará los ciclos finales de instrucción de toda la red honeypot que posteriormente con dicho resultado, se aplicará otra fórmula que medirá el rendimiento definitivo de la red. Dicha fórmula es la siguiente: MIPS = F(MHz) / CPI (segs). Los valores de cada CPIi en la formula, vienen dadas por el porcentaje calculado a cada una de ellas. 69% resultado de 100% es de 0.69. 0,88 (88%), resultado del 100%, 0.95 (95%), resultado del 100% $CPI = \sum_{i=1}^{n}(CPIi\,.FIi) = 0.69x1 + 0.88x2 + 0.95x3 =$ 5.3 ciclos de instrucción. Esto indica que al aplicar la fórmula para calcular el ciclo por instrucción por cada vez que el honeypot se sometió a estudio, arrojo un resultado de 5.3 ciclos por instrucción. Ahora, para calcular MIPS (millonésima parte de instrucción x segundo), y determinar cuánto tiempo demora cada instrucción en ejecutarse, tenemos que emplear la fórmula de cálculo de frecuencia del procesador.

MIPS= F(MHz)/CPI= 166Mhz / 5.3 ciclos de segs = 31.32 MHz/segs;

En donde, la frecuencia estará representada en MHz y los ciclos de segundos, estará representada en segundos: El MIPS total es de = 31.32 MHz/segs. Después de haber implementado el Honeypot, se comprobó su correcta actividad juntamente con sus instrumentos, por lo que se procede a realizar un análisis e interpretación de los datos obtenidos por las distintas evaluaciones de ciclos en la que se sometió el honeypot a estudio. Finalizando dichos resultados obtenidos y convirtiéndolos a porcentajes; será de 95.4% de rendimiento en su totalidad, después de las pruebas efectuadas.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

Tipo de instrucción	Porcentajes de uso	Ciclos de tiempo
Operaciones Aritmético-lógicas	69%	1 min
Carga desde Memoria	88%	2 mins
Almacenamiento en Memoria	95%	3 mins

Tabla 2. Medidas De Rendimiento Del Honeypot.
Fuente: Lorusso, 2021

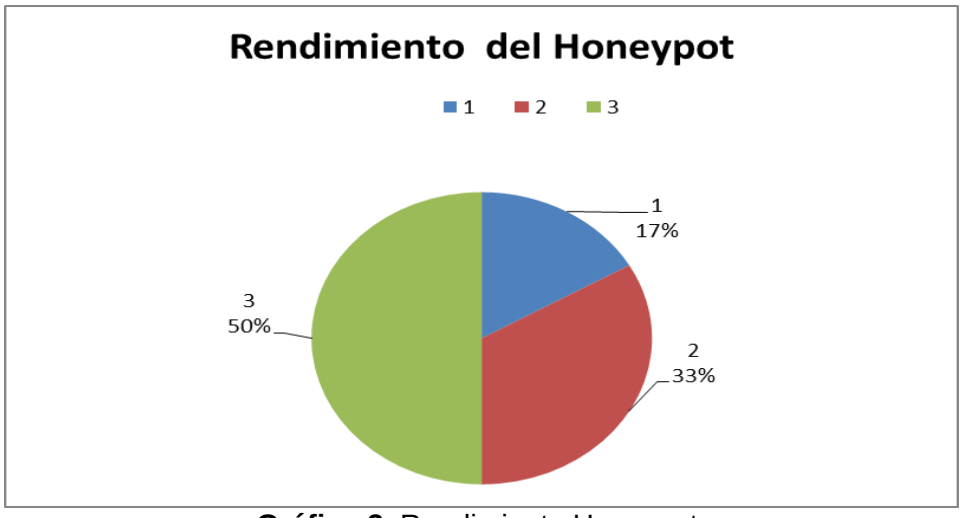

Gráfico 3. Rendimiento Honeypot.
Fuente: Lorusso, 2021

También se pudo apreciar los diferentes eventos que afectaron a la red. Todo esto gracias a la interfaz del Honeypot, el cual mostró que el mayor ataque con 150K y el menor evento cerca de 35K (K=Tasa de rendimiento), además se pudo promediar un 90K de eventos aproximadamente. Además, permitió determinar los ataques realizados, donde el color celeste representa el rendimiento del honeypot con relación a ataques simulados, fue de un 17%. El color naranja representa del segundo ciclo, el rendimiento de un 33%; de igual forma, el color gris en su último ciclo de ataques simulados, que representa un 50% de rendimiento, en operaciones de ataques simulados. El honeypot, también determino el lugar de procedencia de dichos ataques.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

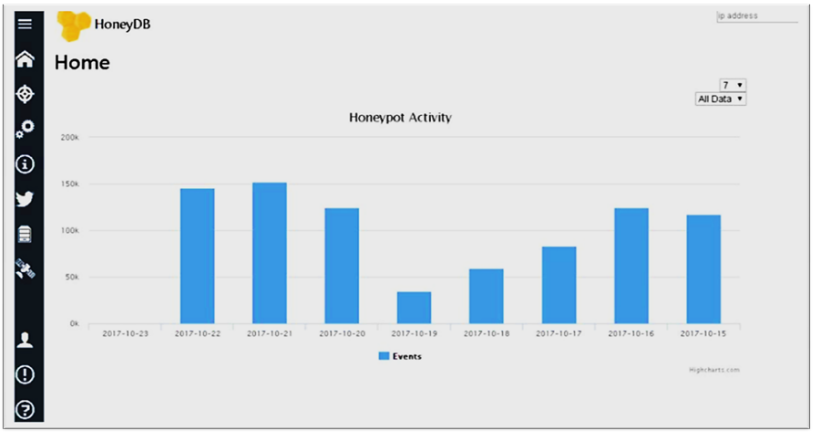

Gráfico 4. Estadísticas de actividades de honeypot en cuanto a tiempo.
Fuente: Lorusso, 2021.

Claramente, se observa en este gráfico, las actividades marcadas por el servidor de honeypot. Evalúa sus actividades y/o eventos efectuados según el tiempo de iteración. En las coordenadas de Y, se expresa el porcentaje en escala de diez en diez. En la coordenada X, la fecha del evento. Sencillamente, es un reporte impreso por el mismo honeypot para indicar los eventos efectuados.

DISCUSIÓN Y CONCLUSIONES

Como se ha planteado, el avance de internet ha traído diversas vulnerabilidades para las redes de información, por tal motivo, se hace necesaria la implementación de medidas de seguridad que puedan sustentarse y mantener la información a salvo, también que reduzca las pérdidas financieras. Para ello existen varias herramientas que ofrecen resultados aceptables, sin embargo, dejan holguras de vulnerabilidades, por ello los sistemas Honeypots han tomado importancia.

Cabe mencionar que dicha investigación, se sometió a diferentes pruebas y/o fases; cuya intención fue la de determinar los niveles de rendimiento y seguridad en situaciones de peligro nulo, inferiores a ciclos de 5 minutos (o leves) y superiores a 10 ciclos por minutos (o fuertes). Los resultados de estas pruebas demostraron que una red Honeypot posee niveles óptimos de interacción en cuanto a su rendimiento.

Después de una apropiada configuración en la red Honeynet, puede simular un sistema Firewall (barrera protectora honeypot) y tener inclusive resultados satisfactorios, que simplemente, el empleo de métodos aislados e independientes tal como es el caso de antivirus. Además, con los complementos adecuados puede permitir analizar e interpretar el comportamiento del tráfico en la red de datos, brindando un control del contenido, denegación de puertos innecesarios y también, permiten el monitoreo de paquetes de programas dentro de sistemas informáticos y red de datos. Por consiguiente, se puede afirmar que el honeypot alcanzó un máximo de 95.4% de rendimiento absoluto, un porcentaje excelente, lo cual es un indicativo de buen rendimiento y también como medida de seguridad. Se recomienda el uso de dichas redes en distintas organizaciones para evitar ser

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

víctimas de ciber ataques, los cuales podrían afectar negativamente el desempeño del sistema de cualquier organización.

RECOMENDACIONES:

Debido a la cantidad de información recogida se recomienda que los discos de almacenamientos de la máquina que actúa como Honeywall posea una capacidad de almacenamiento de entre 100 a 400 TB (terabytes) y de procesamiento 100 TB,utilizar un sistema operativo basado en GNU/Linux, para evitar así, que sea infectada por datos descargados.

Prudencia al implementar la red honeypot; debido a la complicidad, protección de datos y responsabilidades por cualquier daño que sea posible de causar desde el atacante. Por tanto, es importante un monitoreo constante de la red y la ubicación del Honeypot en una zona segura, donde no comprometa a ningún sistema y evitar así que alguna de las redes sufra daños.

Evaluar exhaustivamente la infraestructura disponible antes de realizar el diseño de la Honeynet, a fin de evitar posibles cuellos de botella que podrían ocasionar el mal funcionamiento de la red.

Una vez que los resultados de vulnerabilidades hayan sido obtenidos, se debe planificar y ejecutar de una política de seguridad que permita gestionar y reparar dichas vulnerabilidades informáticas.

Actualizar constantemente la base de datos del servidor IDS (detección de intruso), a fin de poder gestionar nuevas vulnerabilidades que se sigan descubriendo, así como tratar en lo posible de eliminar los falsos ataques o falsas advertencias.

Continuar con la investigación acerca de tecnologías involucradas en la seguridad informática como es el caso de los honeypots y Honeynets, puesto que este nos brindara un mecanismo proactivo de alertas frente a posibles ataques informáticos.

BIBLIOGRAFÍA

Acién A. (2018). Análisis de vulnerabilidades en IoT, para el despliegue de honeypots [Máster Universitario, Universidad de Málaga]. Repositorio Académico de la Universidad de Málaga. https://riuma.uma.es/xmlui/bitstream/handle/10630/18710/Memoria%20TFM%20Final.pdf?sequence=1&isAllowed=y

Avilés J. (2016). Captura y análisis de los ataques informáticos que sufren las redes de datos de la ESPOL, implantando una honeynet con miras a mejorar la seguridad informática en redes de datos del Ecuador. [Tesis de grado, Escuela Superior Politécnica del Litoral]. Repositorio Académico de la Escuela Superior Politécnica del Litoral. https://www.dspace.espol.edu.ec/bitstream/123456789/7781/1/D-39239.pdf

Botnet implements honeypot to facilitate finding more victims. Netlab. 12 Marzo 2021.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022

Del Valle E. (2019). Análisis de la herramienta honeynet para mejorar la seguridad informática en el laboratorio de telecomunicaciones de la carrera de ingeniería en computación y redes [Proyecto de Investigación, Universidad Estatal del sur de Manabí]. Repositorio Académico de la Universidad Estatal del sur de Manabí. http://repositorio.unesum.edu.ec/bitstream/53000/1956/1/UNESUM-ECU-REDES-2019-65.pdf

Fernández A. (2017). Desarrollo de una herramienta honeypot para un uso eficiente en seguridad informática [Trabajo Fin de Grado, Universidad de Jaén]. Repositorio Académico de la Universidad de Jaén. http://tauja.ujaen.es/bitstream/10953.1/5940/1/TFG_Cruz_FernandezDeMoya-Alejandro.pdf

García A. (2017). Metodología de la investigación. P.80, México, México

Verona y otros (2016). Pruebas de rendimiento a componentes de software utilizando programación orientada a aspectos. [Articulo original, Instituto Superior Politécnico José Antonio Echeverría]. Repositorio Académico del Complejo de Investigaciones Tecnológicas Integradas (CITI). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59362016000300006

León C. Camilo A. - Bonilla D. María A. (2017). Análisis De Ataques Informáticos Mediante Honeypots Para El Apoyo De Actividades Académicas En La Universidad Distrital Francisco José De Caldas. FACULTAD TECNOLÓGICA INGENIERIA EN TELEMÁTICA BOGOTÁ D.C.

Casanovas Coanisi y otros (2017). Honeypots Web como Herramientas de Análisis de Ciberataques sobre una Red de Telefonía Móvil. 5to Congreso Nacional de Ingeniería Informática / Sistemas de Información Aspectos Legales y Profesionales y Seguridad Informática.

Martínez C. Kevin (2018). Honeypot, Hacia Un Protocolo De Seguridad Más Eficiente Y Competitivo. Universidad Nacional Abierta Y A Distancia Escuela De Ciencias Básicas, Tecnología E Ingenieria Especialización En Seguridad Informática.

Matus Mihok (2017). Funcionamiento de los honeypots y análisis de los resultados. 2017. Proyecto virginia, Usa.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 21 Edición No .1 – Año 2022