UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERIA, ARQUITECTURA Y URBANISMO

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

MECANISMOS DE SEGURIDAD PARA CONTRARRESTAR ATAQUES INFORMATICOS EN SERVIDORES WEB Y BASE DE DATOS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autores:
Bach. Izquierdo Cabrera Jaime
Bach. Tafur Callirgos Tania Elizabeth

Línea de Investigación:
Tecnologías de la Información

Pimentel – Perú
2017

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

MECANISMOS DE SEGURIDAD PARA CONTRARRESTAR ATAQUES INFORMATICOS EN SERVIDORES WEB Y BASE DE DATOS

Aprobación de la Tesis

Mg. Villegas Cubas Juan Elías
Presidente del jurado de tesis

Ing. Mejía Cabrera Heber Ivan
Secretario del jurado de tesis

Mg. Bravo Ruiz Jaime Arturo
Vocal del jurado de tesis

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

DEDICATORIA

A mis padres por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional sin importar nuestras diferencias de opiniones, a pesar de nuestra distancia física, siento que están siempre conmigo.

Jaime Izquierdo

A mi madre y a mi hermano por el apoyo incondicional y sus consejos para seguir adelante. A mis docentes y compañeros, quienes sin esperar nada a cambio compartieron sus conocimientos, y a todas aquellas personas que durante estos años estuvieron a mi lado apoyándome.

Tania Tafur

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

AGRADECIMIENTO

Agradecemos a nuestros padres por todo el apoyo brindado. A nuestros docentes por todos sus conocimientos transmitidos y por su apoyo constante durante la investigación. Al Ing. Juan Villegas Cubas por ser nuestro principal guía durante el desarrollo de la investigación.

Jaime Izquierdo – Tania Tafur

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

INDICE

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

INDICE DE FIGURAS

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

INDICE DE GRÁFICOS

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

INDICE DE TABLAS

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

RESUMEN

En esta investigación se realizó la comparación de mecanismos de seguridad que fueron capaces de contrarrestar ataques informáticos, con el propósito de capturar información de los intrusos y aumentar la seguridad en los servidores web y base de datos.

Se identificó los incidentes de seguridad de la información, encontrando entre ellos a los ataques informáticos con mayor impacto en servidores. Estos fueron analizados y posteriormente se implementó sus mecanismos de seguridad en el diseño de la red establecida. Se implementaron los mecanismos de seguridad, establecidos por los investigadores, el primer mecanismo constó con la clonación de una red espejo virtual (Honeynet) autocontenida, así mismo se implementó el segundo mecanismo Snort en Kali Linux.

Como resultados de la investigación se logró analizar y estudiar el impacto que ocasionaron los ataques, teniendo en cuenta el tiempo que queda indisponible el servidor, el mecanismo Honeynet obtuvo el menor tiempo de 0,8 segundo, frente a Snort que obtuvo 1,0 segundos. Así mismo se obtuvo como resultados el tiempo de respuesta que el mecanismo Snort logró reaccionar al 3,8 segundos, mientras que Honeynet reaccionó 3,6 segundos y rendimiento de los mecanismos de seguridad por cada ataque, se logró obtener un 97,5% de precisión, 99,2% de sensibilidad, 97% de especificidad y el 98,3% de exactitud en el mecanismo de seguridad Honeynet de generación III virtual autocontenida, frente al 97,9% de precisión, 98,0% de sensibilidad, 97,6% de especificidad y un 98% de exactitud del mecanismo Snort. A través de la investigación se hará mención de la problemática actual y las vulnerabilidades encontradas en los servidores especificados.

Palabras claves

Honeynet, Snort, Mecanismos de Seguridad, Ataques informáticos, Servidores, Rendimiento.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ABSTRACT

This investigation focus to compare the different security mechanisms capable to counter informatics attacks, with the intention to capture the information of the intruders and increase the security in the web service and database.

We identify different incidents about security information, and found between them the attacks with the most impact in the servers. This attacks was analysed and we implement different mechanisms of security in the red previously designed, established by the investigator, the first mechanism consist of a virtual mirror network clone (Honeynet) auto-content, also we implemented a second mechanism Snort in Kali Linux.

In our investigation we were able to study and analyse the impact of different attacks, focus at the server's time unavailable, the Honeynet mechanism obtained the lesser time with 0.8 second, Snort obtained 1 seconds. Also we found that Snort mechanism obtained the lesser answer time with 3.8 seconds, meanwhile Honeynet have a 3.6 second of reaction. The performance of this security mechanisms by attacks was a 97.5% of accuracy, 99.2% of sensibility, 97% of specificity and a 98.3% of accuracy in the Honeynet mechanism of virtual III generation auto-content, Snort had the 97.9% of accuracy, 98% of sensibility, 96.6% of specificity and 98% of accuracy. In our investigation we going to mention the actual problem and vulnerabilities what we found in the servers specify previously.

Key words

Honeynet, Snort, Security mechanism, informatics attacks, servers, performance

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

INTRODUCCIÓN

La seguridad de la información en las empresas pasa un tanto desapercibida y no es tomada con importancia, las empresas no creen conveniente invertir en ello, es por eso que existe un alto índice de fraudes, como robo de información, pérdidas económicas, entre otras, provocadas por ataques informáticos. Estudios realizados por ESET (2016), muestra cómo se encuentra el estado de la seguridad de la información en las empresas de Latinoamérica, demostrando que en el año 2015 un 78% de empresas reportaron haber sido víctimas de al menos un ataque informático.

Un Informe (CNCERT, 2015) demostró las pérdidas económicas que fueron generadas por los incidentes de seguridad más comunes durante el año 2015, entre ellas pérdidas de 10 millones de dólares en Perú, sin embargo los ataques día a día vienen incrementándose ocasionando otras perdidas como robos de información que suelen ser las más comunes.

(Mohammad D., Izzat A., & Emad A., 2013) demuestran que existen muchos métodos para acceder ilegalmente a servidores web o sitio web, ellos utilizaron SNORT, el cual definen como un mecanismos de seguridad de código abierto que sirve para detectar e impedir el acceso de los ataques. Finalmente mostraron la capacidad que posee para prevenir los posibles ataques que ingresaron a la red.

Según la investigación realizada por (De la Hoz, De la Hoz, Ortiz, & Ortega, 2012) afirmaron que los sistemas de detección de intrusos (IDS) clasificaron el tráfico de la red, detectando así solo las conexiones e intrusiones normales, mediante firmas; todo esto ocasiona algunos problemas ya que solo detectan intrusiones conocidas. Es por ello que en esta investigación se evaluó la eficiencia del modelo de detección propuesto, utilizando métricas de sensibilidad y especificidad.

(Casanovas E. & Tapia C., 2013) afirman que existen dispositivos de seguridad que son del tipo convencionales, entre los más conocidos se encuentran los sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS), firewall y antivirus, pero son vulnerables a la información cifrada y a los ataques. En la investigación demostraron las funcionalidades básicas de un mecanismo de seguridad que consta de crear una red espejo virtual trampa (Honeynet) se efectuó un análisis de la tecnología de Honeynet, de acuerdo a las pruebas realizadas el Honeywall demostró que puede brindar información detallada de los ataques.

La presente investigación pretende que los servidores web y base de datos puedan tener mayor seguridad en caso de ataques, es por ello que se realizó una evaluación mediante los resultados promedio de las pruebas realizadas y posteriormente la comparación de los mecanismos de seguridad seleccionados por medio de métricas.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPITULO I: PROBLEMA DE INVESTIGACIÓN

1.1. Situación Problemática

(Gadalméz, 2003). Actualmente los incidentes de seguridad que son relacionados con los sistemas de la información, vienen incrementándose de manera alarmante, provocando la necesidad de implementar mecanismos de seguridad, que reduzcan al mínimo los porcentajes de riesgos asociados a los incidentes de seguridad, debido a que muchos de estos llegan a ser desconocidos y traen consigo efectos negativos.

Estudios presentados en ESET SECURITY REPORT LATAM (2016), muestran el estado de seguridad informática en las empresas de Latinoamérica, en el año 2015 un 78% de empresas reportaron haber sido víctimas de al menos un ataque informático, como se muestra en la figura 1, la cual manifiesta que los incidentes han ido incrementando aproximadamente en 1% respecto a los años anteriores al 2015.

Empresas latinoamericanas que reportaron ataques 2014-2015

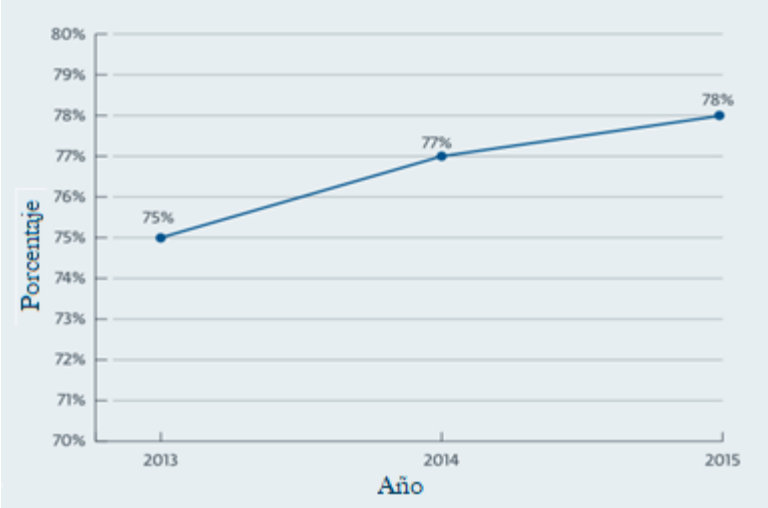


Figura 1: *Porcentaje de las empresas latinoamericanas que reportaron ataques en el periodo 2014-2015.*
Fuente: ESET SECURITY REPORT LATAM (2016).

También el reporte de ESET (2016) da a conocer el porcentaje de incidentes de seguridad informática, clasificándolas tanto por el tamaño de

las empresas segmentadas por pequeña, mediana y grande. Estos resultados llegan a indicar que, en promedio, la infección por malware llegó a ocupar el primer lugar con 40% de respuestas positivas, mientras que ataques como exploración de vulnerabilidades, Denegación de Servicio (DoS) 11% entre otros también figuran en el ranking latinoamericano.

Otro estudio denominado Informe de Ciberamenazas y Tendencias realizado por el Centro Criptológico Nacional de España por sus siglas CNCERT (2015) muestra las mayores pérdidas económicas por incidentes de seguridad informática, llegando a ser desde los 10 millones de dólares en pérdidas en Perú, 25 millones de dólares de pérdidas en Sudáfrica y Colombia, más de 50 millones de dólares en pérdidas en países como España e India y más de 100 millones de dólares en pérdidas en EEUU, Canadá y China.

Los ataques informáticos se han convertido en un problema importante en el mundo de hoy. (Rupinder, NagpaJ, & Chamotra, 2015) afirmaron que los dispositivos de seguridad convencional, tales como IPS y cortafuegos son lo suficientemente buenos para contrarrestar y registrar los ataques conocidos, pero en el caso de los ataques desconocidos los dispositivos de seguridad fallan. Para minimizar este problema es importante utilizar nuevas herramientas de seguridad que complementen a los dispositivos convencionales, tales como las redes trampa como dispositivos de seguridad activa.

Memari, Hashim & Samsudin (2014). Se refieren que algunas herramientas de seguridad no logran detectar los ataques informáticos a tiempo. Los métodos puramente defensivos de los ataques informáticos, como los IDS, encriptación de datos y servidores de seguridad, tratan de evitar la interacción con el atacante, pero ofrecen seguridad al momento que el atacante ingresa a la red y no logran detectar al ataque antes de causar

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

daños. Siendo así más propensos a ataques desconocidos y escaneo de vulnerabilidades.

Las vulnerabilidades en software pueden ser explotados y pueden dar lugar a importantes recursos perjudiciales. Para evitar este tipo de explotaciones, empresas de antivirus introduce nuevas firmas de virus en sus bases de datos. Almonin, A. A. (2015), este autor propuso un método para proteger los sistemas, este es llamado Honeynet, que es una red trampa, actúa como un sistema detector de vulnerabilidades (HVD) para detectar vulnerabilidades desconocidas en el software. El aumento del número de conexiones puede dar lugar a la amenaza de seguridad para la protección redes (sistemas no Honeynet) y para evitar este tipo de amenazas. Mediante la introducción de extensión HVD propuesto, esperar a tener la red más segura contra el software desconocido vulnerabilidades, y ayudó en la identificación de los enemigos del sistema.

Guevara, Santos y López (2016). Basados en la investigación los autores evalúan una técnica de mecanismo de seguridad para contrarrestar los ataques informáticos por medio de tiempo promedio, presión, taza de detección y taza de falsos positivos, como trabajos futuros ellos sugirieron que se realice la comparación de otras técnicas de mecanismos de seguridad como redes bayesianas, algoritmos de optimización y big data, para la mejora del rendimiento y la reducción del tiempo de respuesta de aquellos mecanismos.

Se logró evidenciar que las investigaciones realizadas a lo largo de los años mostraron resultados en donde las empresas han tenido impactos negativos, que fueron ocasionados por diferentes ataques informáticos tanto a servidores web y base de datos, los ataques informáticos que fueron seleccionados para la investigación suelen ser los más frecuentes a nivel latinoamericano según ESET SECURITY REPORT LATAM (2016). Así mismo las investigaciones se centraron en la identificación de ataques,

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

dejando como trabajos futuros los mecanismos de seguridad para dichos ataques informáticos, los cuales beneficiaran a las empresas para la toma de decisiones en cuanto a la seguridad que deberían implementar para contrarrestar y prevenir aquellos ataques informáticos más frecuente.

1.2. Formulación del problema

¿Podrán los mecanismos de seguridad informática implementados, contrarrestar los ataques frecuentes seleccionados?

1.3. Delimitación de la investigación

La presente investigación se realizó en el Laboratorio de Investigación de Sistemas Inteligentes y Seguridad de la Información (LABSIS) de la Universidad Señor de Sipán, en un periodo de 10 meses, iniciado en el mes de setiembre del 2016.

Se implementaron los mecanismos de seguridad informática, la red de espejo virtual denominado Honeynet de generación III virtual autocontenida, y el otro mecanismo implementado fue Snort en Kali Linux, estos mecanismos fueron implementados con la intención de contrarrestar y analizar el tráfico de la red establecida. Se analizaron los mecanismos por medio del tráfico de red y se compararon por medio de indicadores, para saber cuál es capaz de contrarrestar a los ataques informáticos identificados anteriormente.

1.4. Justificación e importancia de la investigación

Con el trabajo de investigación se pretendió atender la preocupación de la gran mayoría de empresas que trabajan con tecnología de la información (TI), al invertir en seguridad de la información. Aquellas empresas que hacen uso de servidores web y base de datos, gracias a la implementación de mecanismos de seguridad informática, se proporcionó

mayor seguridad en el intercambio de información tanto personal como empresarial.

En el aspecto tecnológico permitió ir en paralelo con los nuevos avances de la tecnología, así mismo se ha generado gran incremento de los ataques a servidores web y base de datos. Además, estos mecanismos de seguridad reforzaron la confidencialidad e integridad de los datos almacenados, manteniendo disponibles los servicios que brinda la empresa.

De esta manera, permitió conocer los resultados de los mecanismos de seguridad implementados, descubriendo los tipos de ataques informáticos y las nuevas herramientas, que dependieron de las pruebas realizadas a dichos servidores.

Los dispositivos que se encuentran en el grupo de los convencionales, tales como IDS, IPS, cortafuegos y/o antivirus, son vulnerables a la información cifrada y a los ataques desconocidos por su motor de análisis. Debido a esta situación se propuso implementar mecanismos de seguridad informática, los cuales sean capaces de contrarrestar aquellos ataques seleccionados. De allí la importancia de utilizar mecanismos de seguridad que contrarresten ataques informáticos a servidores web y de base de datos.

1.5. Limitaciones de la investigación

La investigación se vio limitada ya que existen pocas investigaciones, sobre mecanismos de seguridad, dejando como investigaciones futuras aquellos mecanismos capaces de contrarrestar los ataques informáticos a servidores, específicamente a web y base de datos. Y la comparación entre mecanismos para saber cuál de ellos es más efectivo en contrarrestar los ataques.

Por otro lado se utilizaron estadísticas (ESET Security Report 2016) de ataques informáticos, que fueron realizadas a nivel Latinoamericano y

otros países. La selección de los ataques con los que se trabajaron fue por conveniencia, puesto que los tres primeros no producen ningún efecto a los servidores web ni base de datos, eso quiere decir que estos ataques no cubren el ámbito al cual va dirigida la investigación.

1.6. Objetivos de la investigación

1.6.1. Objetivo general

Analizar los mecanismos de seguridad informática que contrarresten los ataques informáticos detectados en servidores web y base de datos.

1.6.2. Objetivos específicos

a. Identificar los ataques informáticos con mayor impacto en los servidores web y base de datos de Latinoamérica.
b. Seleccionar los mecanismos de seguridad.
c. Diseñar la red de datos para la simulación.
d. Implementar los mecanismos de seguridad que mitiguen a los ataques informáticos.
e. Evaluar los mecanismos de seguridad informática.
f. Comparar los mecanismos de seguridad informática.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPITULO II: MARCO TEORICO

2.1. Antecedentes de la investigación

Yánez Guevara (2013) "*Sistema de detección y prevención de intrusos para el control de la vulnerabilidad en los servidores de la facultad de Ingeniería de Sistemas, Electrónica e Industrial de la universidad técnica de Ambato - Ecuador"* (Tesis de grado). En este trabajo de investigación, los autores afirman que hoy en día es necesario que las instituciones deben de tomar ciertas medidas de seguridad informáticas, para así poder prevenir ataques de personas internas o externas a la institución o entidad. Los IDS e IPS permiten verificar la actividad de todos los usuarios que forman parte de la institución, así como también de aquellos usuarios que estén conectados solo a la red, también permitió mantener un buen control y monitorización sobre los posibles intentos de intrusiones a los sistemas de información; así mismo permitieron a los administradores de la red poder detectar a tiempo los ataques que ingresaban a la red, y lograr detenerlos sin ocasionar daños. Para ellos fue necesaria la implementación de IDS, para que la información que está alojada en los servidores de la facultad sean mejor administrada, tenga un mejor control y se pudiese detectar todas las vulnerabilidades posibles en los equipos que conforman en la facultad. Este trabajo aportó en que todos los servidores deben contar con seguridad frente a los ataques informáticos y sobre todo se debe investigar e implementar posibles mecanismos de seguridad para poder mitigar ataques informáticos que ya han causado daños.

Quinchaguano Duque (2016) "*Diseño e implementación de un prototipo de una Honeynet para la red de datos de la escuela Politécnica Nacional"* (Tesis de grado). Esta investigación se centró en conocer el comportamiento de los ataques y atacantes en el preciso momento donde trataron de obtener acceso o cuando se realizaron las actividades maliciosas a los sistemas. Describió el concepto de Honeynet como mecanismos de protección y la gran parte de implementaciones que se han ido dando con el

tiempo. Asimismo se presentaron los ataques más frecuentes que se dieron a la red EPN. El prototipo de Honeynet fue desarrollado por The Honeynet Project y se realizaron configuraciones correspondientes, luego se realizaron los ataques en la red local y se procedió a publicar la honeynet en internet para verificar si detectó o no los ataques. Se comprobó que si se puede evitar intrusiones externas a la red a través de accesos SSH con el manejo de claves robustas.

Berenguela & Cortes (2006) "*Metodología de Medición de Vulnerabilidades en Redes de Datos de Organizaciones*". (Tesis de grado) Los autores de esta investigación se centraron en una nueva metodología, creada mediante guías, con la intención de medir la seguridad informática de los datos, y brindando el conocimiento de la misma, aportando información para la creación de políticas de seguridad, para el beneficio de la misma red, así mismo facilitando al administrador el manejo de la red y el descubrimiento de sus vulnerabilidades. Este trabajo aportó a la investigación, porque describió y enseñó algunas de las herramientas existentes para medir las vulnerabilidades de redes, utilizando metodologías que permitan la retroalimentación.

Cantos, K. & Carangui, K. (2007). "*Análisis del sistema de seguridad en servidores Web para su correcta utilización*" (Tesis de grado). Su finalidad fue implantar medidas de protección dirigidas a asegurar las aplicaciones finales ofrecidas por los clientes, procurando que las mismas carezcan de vulnerabilidades que pueden ser aprovechadas de manera indebida por personas mal intencionadas. Esta investigación identificó las principales técnicas en relación al análisis del sistema de seguridad en servidores web, orientados a ciertas normas, reglas y mecanismos para garantizar la confidencialidad, confiabilidad e integridad de los datos. Concluye que la mejora es muy importante en cuanto a la seguridad de los Servidores Web.

Jácome, F. & Robado, M. (2014) "*Implementación de mecanismos de seguridad para contrarrestar infraestructuras críticas frente ataques informáticos en el laboratorio de redes de la Universidad Técnica de Cotopaxi ubicado en la ciudad de Latacunga, Provincia de Cotopaxi, en el periodo 2013"* (Tesis de grado). Esta tesis constó de un análisis de los principales mecanismos de seguridad en redes, así como las ventajas y características del mecanismo (IPSec) a implementar, el cual estuvo encargado de proteger la seguridad de la red de comunicación, asegurando el intercambio de paquetes de datos y garantizando la autenticación mutua, contrarrestando los ataques informáticos.

Luna, Soberanes, Juárez, & Rueda (2015). "*Sistema detector de intrusos ocupando una red neuronal artificial".* Universidad Autónoma del estado de México (Tesis de Maestría). La investigación afirmó que las técnicas basadas en Inteligencia Artificial para la detección de intrusos, exactamente las redes neuronales, son las que están demostrando un enfoque para combatir y atacar con todos los problemas detectados. Es una gran cantidad de información que se requiere para poder entrenar los sistemas de redes neuronales y un tiempo prudente para poder asimilarlos. En esta tesis, buscaron realizar una red neuronal artificial, que conjuntamente a un IDS, puedan tener baja tasa de falsos positivos, esto debido al correcto entrenamiento, que junto a la base de conocimientos pudieren dotarle a la red neuronal un aprendizaje de alto nivel, además de asegurar que reduzca la perdida de la información, mantenido estables los tiempos de entrenamiento de la red neuronal. Esta propuesta fue validada por las pruebas realizadas en un escenario, mediante un IDS basado en redes neuronales artificiales. De acuerdo a las pruebas realizadas, se obtuvieron como resultados la validez completa de la propuesta.

Vaca Jhonny (2014) "*Implementación de un prototipo de seguridad con Honeynet Virtuales para descubrir patrones de ataques y analizar el comportamiento y las condiciones de los intrusos, aplicando en el laboratorio*

de Tecnologías de la información y comunicación – LTIC". (Tesis de grado). El autor de esta investigación trabajó con un nueva tecnología llamada Honeynet utilizada para defensas de seguridad en la red, es como una red señuelo para atraer a los posibles intrusos, así mismo puede capturar la información de los atacantes y permite analizar dicha información. Analizó de manera rápida la situación en la que se encontraba el laboratorio LTIC, en relación a los servicios que brinda y a la seguridad de su red. Para ello implementó una red virtual utilizando la plataforma de virtualización VMware y la instalación de honeywall con una interfaz gráfica Walleyes. La Honeynet funcionó correctamente, detectando la gran variedad de ataques que se utilizaron para las pruebas. Llegó a la conclusión que las herramientas tradicionales generan gran cantidad de megas de ficheros, mientras que la Honeynet implementada le generó pequeñas cantidades de datos pero con gran valor.

2.2. Estado del arte

Las investigaciones referentes a mecanismos de seguridad informática y ataques informáticos han tomado gran importancia en todas las empresas, ya que actualmente es indispensable proteger la información.

Maestre. J., Sandoval. A. & García, L. (2015) *"Sistema inmunitario adaptativo para mitigación de ataques de denegación de Servicio"* Universidad Complutense de Madrid, España. En esta investigación los autores dieron a conocer el aumento de los ataques DoS en los últimos años, ocasionando aviso a las diferentes organizaciones. La gran parte de ataques que se identificaron se basaron en inundaciones de redes, lo cual ha incrementado un promedio de 70%. Es por ello que propusieron una nueva estrategia de defensa, haciendo uso de Sistemas Inmunitarios Artificiales (AIS) para la mitigación de ataques DoS. Cada uno de los agentes ha combinado sus funciones básicas, con estrategias propias de detección y mitigación de este tipo de ataques, el sistema fue evaluado en un entorno de experimentación simulado, el cual ha implicado las diferentes topologías de

red, congestión y ataques. Como resultados se demostró una importante mejora al considerar mecanismos de reacción adaptivos, frente a considerar sólo respuestas innatas.

De la Hoz et al. (2012) "*Efficient Assessment and Evaluation for Websites Vulnerabilities Using SNORT".* En este trabajo de investigación se detalla la definición de SNORT y sus diferentes reglas, es una herramienta de código abierto popular, que se utiliza para detectar e impedir el acceso de los ataques tanto a redes, sitios web y servidores. Se demostró diferentes métodos que fueron muy prácticos para diseñar e implementar, de manera que se muestre la seguridad con las que se puedes utilizar las reglas Snort, para realizar las pruebas los autores se centraron en tres tipos de ataques, inyección Sql, XSS y comando ejecución. Al finalizar se llegó a la conclusión que usando el sistema Snort IDS en una aplicación web vulnerable, logró mostrar la capacidad de este para prevenir los ataques que se realizaron a la red, así mismo que algunos ataques llegaron a causar un impacto mínimo en la red.

Kumar, Singh, Sehgal & Bhatia (2012). "*Distributed Honeynet System Using Gen III Virtual Honeynet".* En la actualidad se cuenta con múltiples problemas en la aplicación de seguridad a las redes con dispositivos tradiciones (IDS, IPS, firewall). En esta investigación se realizó una comparación del mecanismo de seguridad Honeynet, de sus diferentes generaciones, para saber cuál de las generaciones es más efectivo. Se presentó un único método para configurar y establecer un "sistema de honeynet distribuido" de las diferentes generaciones, en varias ubicaciones geográficas utilizando Honeynet Virtual de Gen I, Gen II y Gen III, en esta última se corrió Honeywall y se propuso una arquitectura distribuida Honeynet con la capacidad reconfigurable dinámicamente en términos de IP, sistema lrlas comunicaciones de redes de bots. Se llegó a la conclusión que Honeynet de generación III fue más eficiente para detectar ataques informáticos.

Douligeris & Mitrokotsa (2003) *"DDoS attacks and defense mechanisms: classification and state-of-the-art".* Como los ataques más frecuentes se encuentran la Denegación de Servicio (DoS) constituye una de las principales amenazas y entre los problemas de seguridad más difíciles en la Internet de hoy. De particular preocupación son los ataques de DDoS, cuyo impacto pueda ser proporcionalmente grave. Con poco o ningún aviso previo, un ataque DDoS puede agotar fácilmente los recursos informáticos y de comunicación de su víctima dentro de un corto período de tiempo. Debido a la gravedad de los mecanismos de defensa problema que muchos se han propuesto para combatir estos ataques. Esta investigación presentó un enfoque estructural al problema DDoS mediante el desarrollo de una clasificación de los ataques DDoS y mecanismos de defensa DDoS. Además, se describen las características importantes de cada categoría de ataque y de defensa del sistema y las ventajas y desventajas de cada sistema propuesto se describen. Para ser capaz de entender ataques DDoS que es necesario tener una clasificación formal. Se propone una clasificación de los ataques DDoS que combina eficazmente las clasificaciones propuestas por Mirkovic, Los primeros ataques a nivel se clasificaron en función del grado de automatización, la vulnerabilidad explotada, la dinámica del tipo de ataque y su impacto causado en los servidores o en la red. En el segundo nivel se reconocieron las características específicas de cada nivel de primera categoría. Como resultados los autores lograron poner orden a los mecanismos de ataque y defensa existentes, además ellos evaluaron la posibilidad de desarrollar algoritmos eficientes y eficaces para combatir los ataques.

Holgado & Villagrá (2016). "*Sistema de detección de fases de ataque basado en Modelos Ocultos de Markov". Los autores de e*sta investigación tuvieron presente que las organizaciones están cada vez más preocupadas por los posibles ataques de ciberseguridad en sus sistemas, es por ello que las empresas optan por solicitar sistemas de detección de intrusos (IDS), es

así que deciden usar Modelos ocultos de Markov para poder detectar la fase de los ataques, utilizaron distintas alertas reportadas por los IDS. Mostraron un diseño de un HMM para la predicción de la fase que pasa un ataque de intrusión final. Esta propuesta de HMM ayudó a la detección temprana de intrusiones, mediante la predicción de los pasos del atacante. Se seleccionó el número de estados para que se pueda construir la cadena de Markov, y así almacenar los tipos de observaciones, en la etapa de entrenamiento se consiguió las matrices de probabilidad, que estén más cercanas a la intrusión, este entrenamiento se realizó mediante dos algoritmos, los cuales fueron supervisados y no supervisado. Como resultado se obtuvo, el estado más probable en el que se encontró la intrusión y así se logró anticipar para cualquier intrusión.

Pérez, Britto & Isaza (2005) "*Aplicación de redes neuronales para la detección de intrusos en redes y sistemas de información".* En el trabajo de investigación, los autores expusieron de una manera concisa los conceptos de IDS y de redes neuronales, así mismo estudiaron la integración de ambas tecnologías, verificando si estas dos pueden lograr una solución al problema presentado de los ataques informáticos; para el procedimiento se analizaron tanto las ventajas y desventajas de las tecnologías con los sistemas de seguridad tradicionales, tratando de cubrir errores actuales y así mismo fortaleciendo sus características. Aquellos sistemas que son basados en reglas requieren de permanentes actualizaciones, para que si algún ataque que fue modificado ingrese, el sistema logré detectarlo con rapidez; para esto se realizó una serie de entrenamientos de diferentes algoritmos con sus respectivas funciones de transferencia. Se logró observar que los algoritmos con mejor desempeño fueron cuatro: Traincgb, Traincgp, Trainrp y Traincgf. Como conclusión, los autores presentaron que el sistema basado en redes neuronales permitió detectar paquetes de datos inseguros, esto fue con el previo entrenamiento, generando gran ventaja sobre los sistemas tradicionales.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Sabido, I., Román, F. y García, L (2016). "*Aplicaciones web vulnerables a propósito".* En la investigación se realizó un análisis y valoración de algunas aplicaciones que son vulnerables, se realizó la selección de aplicaciones, buscando las más conocidas, entre ellas se escogieron dos aplicaciones (WebGoat y Mutilliddae), ambas desarrolladas bajo OWASP, estas aplicaciones están hechas con la intención de comprobar las capacidades de las herramientas de análisis. Las herramientas automatizadas de código abierto para la búsqueda de vulnerabilidades web muy conocidos, que fueron utilizadas vienen en la distribución Kali Linux, estas son Vega 1.0 y Zaproxy 2.3, se realizó un análisis a ambas aplicaciones con dichas herramientas. Se llegó a concluir que las herramientas fueron capaces de detectar un porcentaje muy bajo del total. Vega fue la herramienta que más vulnerabilidades logró detectar.

Díaz, García, Muñoz, Maciá, & De Toro (2007). "*Una aproximación basada en Snort para el desarrollo e implantación de IDS híbridos".* En la investigación los autores se enfrentaron al problema de despliegue de detección de intrusiones basadas en anomalías, el primero se refirió a la utilización de tráfico de red en los entrenamientos de sistemas basados en firmas, el segundo se refirió a la detección de los ataques informáticos conocidos y desconocidos por los sistemas basados en firmas, esto se refiere al rendimiento; es por ello que los autores propusieron usar la versión más actualizada de Snort, con la finalidad de que pueda actuar tanto como detector y clasificador híbrido. Las modificaciones de SNORT fueron implementadas satisfactoriamente, ya que se comprobó la utilidad durante el desarrollo de un IDS híbrido para la detección de ataques informáticos en las cargas de las peticiones y paquetes HTTP.

Los autores Kwon, Hong, & Ju (2012). En su investigación "*DDoS attack forecasting system architectura using Honeynet".* Se centraron en que la detección ocurre después de que los ataques de red tienen dificultades para responder rápidamente a los ataques distribuidos masivos, tales como

DDoS que son los más frecuentes y causan grandes daños, dejando a la red saturada. Se propuso un sistema de seguridad proactiva a la previsión de Denegación de Servicio Distribuida (DDoS). Además, se propone la arquitectura de sistema de intrusión de previsión. También se diseñó la arquitectura de intrusión de internet de predicción mediante la realización de análisis de la física, perspectivas técnicas e informativas. Para obtener los factores de intrusión para las previsiones de ataque DDoS, Los Honeynets fueron desplegados en la universidad para recoger los datos necesarios (tales como los registros del sistema y los datos estadísticos de la organización de seguridad) para predecir los ataques DDoS y analizar con Hflow los datos recogidos de las redes trampa como un primer paso para estimar los factores de intrusión.

Sokol & Pisarcik (2013). *"Digital evidence in virtual honeynets based on operating system level virtualization".* Los autores trabajaron en la captura y análisis del tráfico de red con el fin de identificar las amenazas y los atacantes de la red, para que posteriormente, se logre obtener pruebas legales. Existen muchos métodos sugeridos para el análisis forense de la red, incluidos sistemas trampa y redes trampa. Así mismo, se centraron en las redes trampa virtuales basados en virtualización a nivel de sistema operativo, con el fin de desarrollar redes trampas virtuales se eligió una plataforma de virtualización de código abierto - OpenVZ y FreeBSD. Este uso de tecnologías de trampa permite a un usuario acceder a todos los bloques de memoria, sobre todo de los procesos, para identificar los honeypots en la que los procesos están corriendo, con esta información se podrá detectar todos los cambios de los procesos de intrusión después de penetrado el servidor. Propusieron tipos de sensores para capturar la evidencia digital recogida. Se realizó la implementación del primer tipo de sensores se compone de controlador de red virtual que captura los datos en la memoria el espacio del núcleo y la entrada punto en el sistema de archivos virtual (PROCFS) a través de la cual los datos están disponibles para el analizador de datos. En segundo tipo de sensor también implementó el

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

controlador de red virtual para la captura de datos. Se obtuvo como resultados que la comparación con otras tecnologías de virtualización ha proporcionado algunas ventajas para la red marco forense - red trampa, como el acceso directo a la memoria compartida y posibilidad de interactuar con la CPU de la máquina física, los dispositivos de red especializadas, el acceso directo a presentar sistema de contenedor desde el sistema de archivos host y el acceso para completar los procesos de árbol. Este trabajo aportó a la investigación con las ventajas que ofrecen las plataformas y la comparación de tecnologías de virtualización, ya que estos comparten un núcleo de sistema operativo.

Pérez & Martínez (2015). *Detectando botnets con dos modelos de abstracción: Flujos de tráfico e inspección de paquetes de red.* En los últimos años la detección de redes botnets se ha convertido en la principal prioridad. Los ataques por Denegación Distribuida de Servicio (DDoS) se han incrementado en dos años en más de un 20% debido a estas redes, donde los atacantes tienen a su disposición miles o millones de dispositivos comprometidos para ejecutar remotamente sus ataques DDoS. En este artículo se propuso la detección y mitigación de las redes botnets mediante un doble análisis de las fuentes de información. Primero, se realizó la monitorización de los flujos del tráfico de red y, posteriormente, confirmando el supuesto ataque mediante una inspección profunda de los paquetes de red. Los mecanismos de seguridad más destacados en esta investigación son BotHunter y BotMiner, en la detección de redes botnet, aunque focalizados en la inspección del payload de los paquetes de red. En el trabajo de investigación se presentó se realizó la detección y mitigación de redes botnets, mediante el análisis del tráfico de red a dos niveles distintos de abstracción: monitorizando, en primer lugar, los flujos del tráfico de red; y, en segundo lugar, un proceso de detección a más bajo nivel para confirmar que esa red botnet existe.

Rupinder et al. (2015). *Detección de tráfico malicioso en una red privada de la organización usando el sistema de Honeynet.* Esta investigación se refirió que a medida que el número de usuarios conectados a internet tiene aumento de muchos pliegues, los ataques cibernéticos se han convertido en un problema importante en el mundo de hoy. Los dispositivos de seguridad convencional, tales como IDS, IPS y cortafuegos son lo suficientemente buenos para contrarrestar y registrar los ataques conocidos, pero en el caso de los ataques desconocidos los dispositivos de seguridad llegan a fallar, no en su totalidad, pero ocasionan impactos sobre la información. Se exploró la posibilidad de utilizar redes trampa como dispositivos de seguridad activa que complementan las medidas de seguridad convencionales, tales como firewalls e IDS. Utilizaron un honeypot de baja interacción como la captura de los dispositivos en la red de la organización para capturar los datos maliciosos, el capturado de los datos se caracteriza además de ser segregado en tres grandes clases: el tráfico legítimo, tráfico debido a una mala configuración del sistema y el tráfico debido a la propagación de gusano o infección.

Las infraestructuras de red son cada vez más complicadas para proporcionar los servicios necesarios para la organización y reducir estas complicaciones. Otra razón para desplegar tal tipo de arquitectura de red trampa en una organización privada, no es desplegar hacia el exterior para detectar los ataques internos, considerando que se tuvo que encontrar 60% y 80% de ataques que están orientados internamente. Enfoque basado anomalía es sobre la base de la máquina de aprendizaje técnicas que se enteran de los exploits desconocidos.

Enfoque basado en firma es base sobre el tráfico de red a través de un resoplido para detectar la detección de algún malicioso conocido.

a) Mecanismo utilizado para el filtrado malicioso conocido el uso de bufido.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

b) Mecanismo utilizado para la detección de desconocido el tráfico malicioso.
c) Mecanismo para obtener las direcciones IP maliciosas de la honeyd desplegado en la zona DMZ para la detección de algunas anomalías.

Se obtuvo como resultados que Honeynet, permitió utilizar sistemas trampa para capturar gran cantidad de información, acerca del tráfico de red sospechoso e infectado. A si mismo Wireshark o firewall son dispositivos de seguridad, incapaces de detectar los ataques desconocidos internos de la red. Esta investigación aportó que existen dispositivos de seguridad los cuales logran capturar información de diferentes de ataques.

Herrera Zurita (2016) "*Aprendizaje automático para la detección de ataques informáticos"*. Escola d'enginyeria (EE), Universitat autónoma de Barcelona, España. El investigador encontró el problema que actualmente se dispone con internet desde casa, empresa, etc. Siendo expuestos a usuarios corrientes con diferentes intenciones, y que se produzcan muchos ciberataques que pueden afectar y causar grandes daños económicos.

Aprendizaje automático

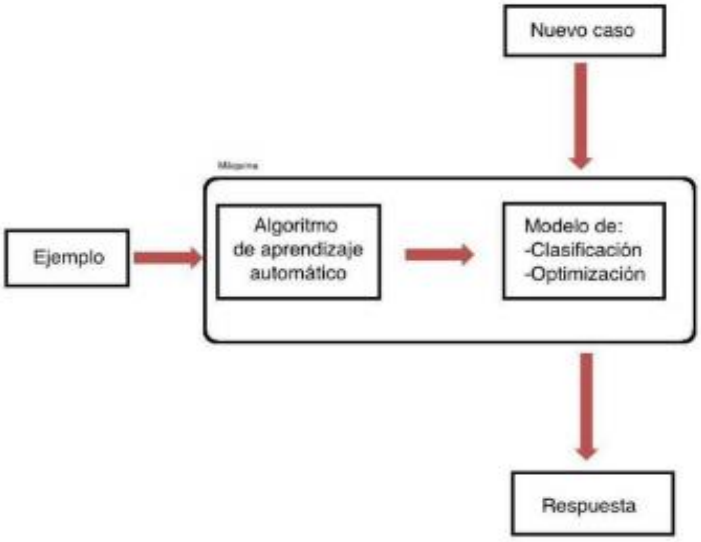


Figura 2: *Esquema aprendizaje automático.*
Fuente: Aprendizaje automático para la detección de ataques informáticos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Es por ello que en el este artículo se exploró la rama relativamente con el crecimiento de la inteligencia Artificial, como es el Aprendizaje Automático de las máquinas, por lo tanto, ellos se centraron en la predicción de un tipo de ataque malicioso como son los producidos por los accesos a URLs maliciosos. Se entendió que existen diferentes tipos de modelos dentro del Aprendizaje Automático y se optó por la utilización de modelos probabilísticos, dentro de ellos se indagó los algoritmos de clasificación supervisado los cuales eran Naive Bayes y K-vecinos más cercanos.

2.3. Bases teóricas

2.3.1. Seguridad de la información

Definición

(López & Quezada, 2016, p. 26). La seguridad viene a ser una norma, la cual llega a estar en constante avance, de acuerdo a la tecnología. El objetivo principal de la seguridad de la información es que las organizaciones puedan cumplir con su misión y con todo lo que ya tienen implementado, ya sea implementado diferentes métodos que aporten con el cuidado y el estudio de riesgos, incidentes o vulnerabilidades de la información tanto de la organización como de sus clientes. El término seguridad para los autores se refiere a la prevención, detección y protección de aquellos sistemas que almacenan datos, ya sea a través de herramientas, reglas, técnicas o ciertos mecanismos de seguridad informáticos, así como también un conjunto de todos ellos, encargados de asignar una mayor protección a estos sistemas, para así evitar la destrucción o modificación de información, sea de manera intencional o accidental.

(Alegre & García, 2011, p. 10). En su libro se refiere a la seguridad de la información como la disciplina que comprende a las medidas preventivas y reactivas de los nuevos sistemas tecnológicos implementados, los cuales resguardan y protegen los datos, buscando cumplir los objetivos principales como la confidencialidad, disponibilidad e integridad.

Objetivos principales

(Aguilera Purificación, 2010, p. 8) Los objetivos principales ya descritos, se tienen que cumplir adecuadamente, el sistema debe de tener todas sus funcionalidades implementadas adecuadamente y con suficiente calidad, es decir, se cumple el objetivo de confiabilidad. También se cumplen cuando existe la protección suficiente resistencia contra el intento de entrada en el sistema. La norma ISO27002 describe a los principales objetivos:

Objetivos de seguridad informática

Figura 3: *Tríada de seguridad informática (confidencialidad - integridad - disponibilidad).*
Fuente: www.ssa-asesores.es/wordpress/blog/2015/02/23/integridad-de-la-información-marco-conceptual/

Disponibilidad

(François J., 2016, p. 49) Se refiere a que todas las personas autorizadas podrán acceder sin ningún problema a la información, en el momento en que lo requieran. Se encarga de proteger a los sistemas de determinados fraudes, como un borrado de datos no autorizado por personas internas o externas, de causas cualquier tipo de ataque DoS o de acceso a los datos, este viene a ser uno de los objetivos más importantes

Integridad

(François J., 2016, p. 49) Este objetivo es el encargado de que la información o los datos del sistema no hayan sido alterados por diferentes usuarios, ya sean no autorizados ni autorizados, para así evitar la pérdida de

datos y encontrarla sin errores. Normalmente es conocido como el segundo objetivo más importante. Y se presenta en dos fases:

a) Integridad de datos: Propiedad donde se verifica que los datos no hayan sido alterados, sea cuando se almacenaban o procesaban.
b) Integridad del sistema: Es propia del sistema, cuando realiza el manejo de información correcta, libre de manipulaciones de usuarios no autorizados.

Confidencialidad

Según (Aguilera Purificación, 2010, p. 9) se refiere al hecho en que la información o datos de una empresa, estén únicamente disponible para personas de manera autorizada. Intenta que los datos se guarden en privado y que no sea revelado ante usuarios no autorizados, o ajenos a la empresa.

Asimismo, existen otros objetivos más generales de la seguridad, entre los que pueden identificar los siguientes:

a) Conocer todos los riesgos de seguridad, que estén asociados a una empresa u organización.
b) Establecer un conjunto de requisitos de seguridad informática de acuerdo con los riesgos identificados, para satisfacer las diferentes necesidades de procesos de negocio.
c) Establecer la confianza en efectividad y eficacia de los mecanismos de seguridad informática.

2.3.2. Ataques informáticos

Definición

(Stallings, 2003, p. 85) en su libro define que los ataques informáticos cada vez se van incrementando con mayor fuerza y sofisticación. Se puede rescatar las principales razones por las que se ataca atacar una red:

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

a) Ventajas financieras, corporativas.
b) Empleados disgustados, descontentos, diversas extorsiones, fraudes.
c) Almacenamiento, servidores de correo (SPAM), anchos de banda.

Categorías del ataque

(López & Quezada, 2016, p. 62). Los ataques informáticos se definen como el aprovechamiento de vulnerabilidades de los sistemas y/o servidores que se encuentran en la red de datos, así mismo estos ataques siguen una serie categorías para completar sus objetivos:

a) (López & Quezada, 2016, p. 62) Interrupción: La detección del ataque viene a ser inmediata, puesto que el impacto causado por los ataque llegan a dejan un pequeño daño en alguna parte del sistema, esta categoría llega a afectar y atentar directamente contra la disponibilidad. Algunos daños se encuentran en esta categoría, por ejemplo: destrucción del disco duro y borrado de información.

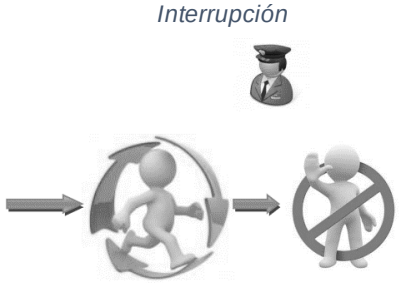


Figura 4: *Flujo de interrupción.*
Fuente: Ataque y defensa en redes informáticos.

b) (López & Quezada, 2016, p. 62) Intercepción: El daño que se puede causar en esta categoría, es el acceso a la diferente información por parte de personas ajenas a la empresa y no autorizadas. La detección llega a ser un tanto difícil, no suele dejar huellas, para cualquier rastreo. Estos tipos de ataques son los que van en contra de la confidencialidad causando diversos daños, por ejemplo: copias ilícitas de programas, escucha en línea de datos.

Intercepción

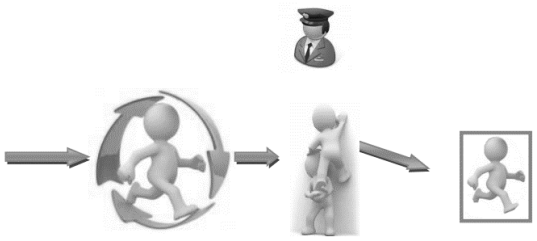


Figura 5: *Flujo de intercepción.*
Fuente: Ataques y defensa en redes informáticos.

c) (López & Quezada, 2016, p. 62) Suplantación: el daño que puede llegar a causar es la sustitución de datos o de información, ocasionando diversos problemas entre los usuarios que se encuentran dentro. La detección de estos es más difícil que los anteriores, son tomados como delitos de falsificación de información. Así mismo los ataques llegan a violar la autenticación. Se encuentran algunos, por ejemplo: la adulteración de mensajes en la red, registrar incorrectos en la base de datos, etc.

Suplantación

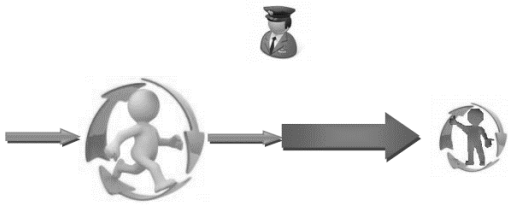


Figura 6: *Flujo de suplantación.*
Fuente: Ataque y defensa en redes informáticos.

d) (López & Quezada, 2016, p. 62) Modificación: Como su nombre bien lo dice, es cuando la información o los datos han sido modificados sin permiso alguno, esto lleva a ocasionar la alteración de los datos para el beneficio de los usuarios que lo realizaron. Se encuentra en el rango de detección difícil, ya que los ataques llegan a atentar sobre

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

la integridad de los datos. Se encuentra algunos, por las diferentes modificaciones de base de datos.

Modificación

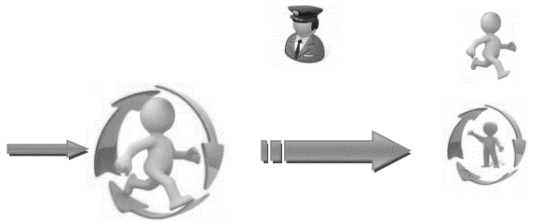


Figura 7: *Flujo de modificación.*
Fuente: Ataque y defensa en redes informáticos.

Pese a la gran cantidad de técnicas y herramientas de seguridad informáticas que se implementan en las empresas, puede llegar a ocurrir diferentes incidentes, clasificados en algún tipo de ataque, los cuales atenten contra los objetivos de la seguridad ya explicados. De acuerdo a la categorización de los ataques, se puede rescatar que existen tipos, tanto activos como pasivos, los cuales son capaces de interrumpir el funcionamiento de sistemas, servidores, computadores, etc.

Fases de ataques informáticos

(CROCFER, 2011) Se refiere a que existen diferentes etapas por la que pasa un ataque informático, las cuales como atacante sirve mucho ya que en cada uno de ellos se puede aprender y subestimar la seguridad ya sea del sistema, servidor o red. Desde el aspecto tecnológico y profesional de ingenieros de seguridad, estas fases o etapas se deben de aprovechar al máximo, ya que permite analizar de forma concisa por qué existen atacantes y por qué llevan a cabo los diferentes ataques.

Según (Gómez, 2011, p. 201 – 202). El autor en su libro nos da a conocer que los ataques informáticos contra ordenadores y redes, estos constan de cinco etapas o fases, las que se presentar definidas.

a) Búsqueda y conocimiento del sistema informático.

b) Exploración de todas las vulnerabilidades que posee el sistema.
c) Exploración y dar conocimiento de las vulnerabilidades detectadas.
d) Modificación o corrupción del sistema, esto se refiere a la modificación de diversos programas o ficheros que se encuentran en sistema, como instalar gusanos, troyanos, etc.
e) Eliminación de las huellas (pruebas) que puedan dejar rastro de los atacantes, así mismo la eliminación de los registro de las actividades realizadas por los atacantes, eliminando rastros del ataque y del robo de la información.

Fases de ataque informático

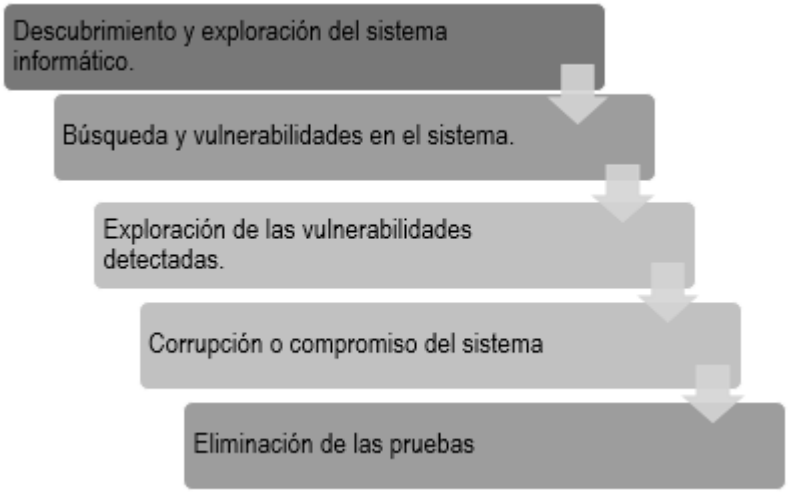


Figura 8: *Cinco de las fases más comunes de los ataque informático.*
Fuente: Enciclopedia de la Seguridad Informática.

Para que los ataques informáticos se puedan realizar satisfactoriamente, los intrusos deben de tener los conocimientos previos, así como las herramientas correctas, se debe de contar con una finalidad o mejor dicho el ataque debe de tener una misión para que el desarrollo de este sea más efectivo.

2.3.2.1. Ataques informáticos a servidores web

(Jimeno, Míguez, & Heredia, 2011, p. 173). Cuando se refieren a servidores, directamente nos imaginamos en los grandes, como son los de bases de datos y servidores web, ya que ellos cuentan con una gran

capacidad de almacenamiento, capaz de aguantar un sin número de conexiones concurrentes. En la gran sociedad de la información que nos rodea, en el mundo empresarial y en mundo de internet, todo se mueve por datos, datos que necesitan mucho espacio para almacenarse, así como mucha rapidez de consulta y transferencia de información.

Los primeros ataques que se realizaban a través de la red se aprovechaban de las vulnerabilidades de los protocolos TCP/IP. Conforme este conjunto de protocolos ha ido superando esas vulnerabilidades y se ha hecho más fuertes en el ámbito de la seguridad, los ataques se han dirigido a la capa de aplicaciones y principalmente a la web.

(Aguilera Purificación, 2010, p. 13) La gran mayoría de los ataques a servidores web es a nivel de software. También existen ataques dependientes de los sistemas operativos que se encuentran instalados en los servidores y del mal uso que se podría hacer de la configuración de los servidores o de las políticas de seguridad definidas. Los ataques informáticos son aquellos que consisten en explorar todas las vulnerabilidades existentes de un sistema informático, ya sea con un propósito desconocido por el usuario que administra el sistema, estos ataque llegan a causar grandes impactos con daños económicos.

Un ataque a un servidor web se puede realizar por diferentes razones.

a) Obtener o modificar información privilegiada de la empresa, información personal de algún usuario en concreto o información de cuentas bancarias.
b) Dañar el funcionamiento normal del servicio, desconfigurar la página web.
c) Usar el sistema para otro ataque diferente.
d) Utilizar recursos, principalmente el ancho de banda de las redes.

e) Dañar la imagen de la empresa o de la entidad de la página web

2.3.2.2. Ataques informáticos a servidores base de datos

(Telefónica Company, 2011) se refiere que existen sistemas de almacenamiento de grandes cantidad de datos, estos son conocidos como los sistemas gestores de base de datos; entre los más conocidos estan MySQL, Microsoft SQL Server, Oracle, entre otros. Esto se convierte en blanco para los hacker, los cuales realizan todo tipo de maniobras para llegar a acceder a dicha información, buscando diferentes vulnerabilidades de los gestores, en este caso es necesario solucionar problemas de seguridad, actualizando el software a la última versión, así como configurar el acceso de la aplicación o del sistema, el ataque más conocido a estos estos servidores es Injection SQL, qué causa grandes datos y se realiza tanto dentro como fuera de base de datos.

Las vulnerabilidades más comunes son:

a) Particularidad de privilegios de usuario

(Aguilera Purificación, 2010, p. 15) Algunas veces los usuarios de la misma empresa reciben acceso o privilegios en la base de datos, lo cual puede ocasionar un gran problema, es por ellos que se recomienda en modificar y revisar dichos privilegios que se otorgan a los usuarios, es muchas veces permite a aquellos usuarios a realizar modificaciones que no están encomendadas a ellos, ocasionando pérdidas de información.

b) Características de bases de datos innecesariamente habilitadas

(Aguilera Purificación, 2010, p. 15) La instalación de base de datos, cuanta con paquetes para esta instalación, lo cual ocasiona vulnerabilidades y entradas pequeñas para sufrir algún tipo de ataque. Es recomendable que los usuarios de la empresa, o el

personal encargado de TI detecten los paquetes que no utilizan y lo desactiven para que no ocasione problemas con el servidor.

c) Desbordamiento de búfer

(Aguilera Purificación, 2010, p.16) Quiere decir que atacantes con propósitos piratas dan acceso a diversa información de la empresa, ya sea enviándola por el uso de formularios. Por ejemplo si una cuenta bancaria ocupa 25 caracteres respectivamente, pero esta logra más caracteres de lo especificado, es recomendable la validación de estos campos para evitar el desborde de la información.

2.3.2.3. Tipos de ataques informáticos

(Gómez, 2011, p. 204) en su libro da a conocer algunos tipos de ataques informáticos existentes, los cuales se pueden diferenciar por ataques activos, que son los que producen grandes cambios en la información del sistema y también los ataques pasivos, lo cuales se encargan de limitar el uso de los recursos para acceder a la información guardad o intercambiada por el sistema.

(Ramos A. B. y Ribagorda G. A., 2004, p.46) También se presenta una relación de los principales tipos de ataques informáticos contra redes de datos y sistemas informáticos.

a) Ataques externos: Son iniciados por un individuo o grupos trabajando desde afuera de una empresa. Ellos no tienen acceso autorizado al sistema o red de computadoras de dicha empresa. Reúnen información para así abrirse camino dentro de la red, principalmente lo hacen a través de internet o servidores por marcado.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

b) **Ataques internos**: Estos tipos de ataques son los más comunes y catalogados como peligrosos, los ataques internos mayormente son iniciados por usuarios con acceso autorizado a una red de datos, comúnmente por usuarios internos a la empresa, o usuarios despedidos descontentos.

c) **Ataques a nivel de sistema**: Este tipo de ataque llega a atacar directamente al sistema operativo del servidor especificado, intentando obtener privilegios de administrador o más conocido como root mediante un terminal remoto. Estos ataques se basan en vulnerabilidades a la hora de configurar las políticas de acceso al servidor a través de un servicio mal configurado (como por ejemplo servicios Telnet y SSH), o bien explotar servicios vulnerables permitiendo desbordamiento de buffers que puede permitir ejecutar comando en el sistema operativo.

d) **Ataque a nivel de aplicación:** Este tipo de ataque es el que intenta la modificación de la información o de los datos, sin necesidad de ejecutar código en el sistema operativo (por ejemplo, modificación o borrado de contenido del sistema de gestión de portales como phpNuke, Mambo, o manipulación de algún gestor de base de datos SQL accediendo a través de Estaplicación phpMyAdmin vulnerable). Este ataque se basa en modificar información de los datos almacenados en una base de datos, peor no modificar nada del portal web. El atacante deberá tener un nivel de conocimiento medio. Este tipo de ataques es uno de los más populares y visibles.

e) **Ataques pasivos:** Estos tipos de ataques cumplen un rol importante ya que son encargados del control y monitoreo de tráfico de la red, Los atacantes desean capturar gran parte de la información que se transmite en la red de datos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

f) **Ataques de fuerza bruta:** Este tipo de ataque se realiza para "adivinar" una clave secreta tratando con todas las combinaciones posibles de caracteres hasta encontrar la correcta. Y es que acceder a las contraseñas de los usuarios no es fácil, ya que se guardan de manera encriptada y la única alternativa es adivinarlas u obtener mediante el uso de "sniffers" – programas que interceptan las comunicaciones y registran las contraseñas, sin embargo, cuando estas técnicas fallan, los hackers recurren a la fuerza bruta.

Entre los ataques más conocidos a las empresas se encuentran:

Denial of service (dos): (Castro, M., Díaz, G. y Alzórriz, I. 2014) Denegación de servicio, buscan dejar no disponible un servicio, una red o un sistema, agotando los recursos como el ancho de banda, espacio en disco, conexiones, etc. Este tipo de ataque no necesita ningún acceso previo al sistema, también los Distributed denial of service (DDoS) vienen a ser ataques prácticamente imparables.

(Areitio B. J, 2008, p.171) Se utiliza distintos atacantes ubicados en diferentes servidores de la red que está actuando, el tipo de ataque realizado por cada atacante sobre la víctima, así como la forma de sincronización, puede variar.

Exploración de vulnerabilidades: (Jimeno, Míguez, Matas & Pérez A, 2009, p. 161). Es una combinación de recolección de datos, obtención de información y políticas de seguridad. La exploración de vulnerabilidades, también es la segunda fase del ataque, en donde el atacante realiza la elaboración de un plan para lograr investigar.

Para el escaneo de puerto se utilizan diferentes herramientas, entre ellas tenemos a *Nmap,* que es un rastreador de puertos utilizado por casi cualquier profesional, esta herramienta fue diseñada para que

los usuarios y/o administradores de los sistemas les permitan determinar cuáles de los servidores están activos y que servicios ofrecen. Nmap permite a los usuarios, administradores de sistemas a hacer exploración de sus redes y de las máquinas para determinar que puertos se encuentran activos, y cuáles son sus vulnerabilidades.

2.3.3. Mecanismos de seguridad

Definición

(Areitio, 2008, p.34 – 35), el autor hace referencia a los mecanismos de seguridad como herramientas de seguridad, las cuales tienen que brindar protección de los bienes y servicios informáticos. Como su nombre lo dice, llega existir herramientas físicas, las cuales protegen el sistema o servidor, por ejemplo, las políticas de seguridad.

Clasificación según función

(Aguilera Purificación, 2010, p.17). Existen muchos y variados mecanismos de seguridad, estos se llegan a clasificar en tres, de acuerdo a la función que estos desempeñan:

a) Preventivos: Tienen como objetivo evitar aquellos ataques que fueron detectados, significa que actúan antes de que se produzca el ataque.

b) Detectores: Estos mecanismos tienen como objetivo actuar cuando el ataque se ha producido y antes de que este pueda causar daños al sistema o al servidor.

c) Correctores: Son aquellos que actúan después de que actuó el ataque y que causó algunos daños, tiene como objetivo corregir las consecuencias del daño.

Clasificación según categorías

Según (Stallings, W., 2004, p. 15) los mecanismos de seguridad informática se llegan a dividir en aquellos que se suelen llamar específicos, ya que implementan una capa de protocolo y aquellos que no son específicos de ninguna capa o servicio de seguridad. Los mecanismos de seguridad ISO 7498-2 se pueden clasificar en general en dos categorías:

a) Mecanismos de seguridad informática específicos: Estos son utilizados y encargados de proporcionar todos los objetivos de seguridad, como confidencialidad, integridad y autenticación, pueden ser incorporados en la capa de protocolo adecuada. Estos mecanismos pueden subdividirse en ocho tipos:

1. Cifrado de clave pública o asimétrico y clave privada o simétrico.
2. Firma digital basada en criptografía.
3. Mecanismos de control de acceso.
4. Mecanismos de integridad de datos.
5. Intercambio de autenticación.
6. Control de tráfico.
7. Control de encaminamiento.
8. Notarización.

En la tabla 1 se observa la relación que existe entre los servicios y los ocho tipos de mecanismos de seguridad ya mencionados.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 1. Relación de servicios y mecanismos de seguridad

	Mecanismo							
Servicio	Cifrado	Firma Digital	Control de acceso	Integridad de datos	Intercambio de autenticación	Control de tráfico	Control de encaminamiento	Notarización
Autenticación de entidades	x	x			x			
Autenticación del origen	x	x						
Control de acceso			x					
Confidencialidad con conexión	x						x	
Confidencialidad sin conexión	x						x	
Confidencialidad de un campo selectivo	x							
Confidencialidad del flujo de tráfico	x					x	x	
Integridad con conexión con recuperación	x			x				
Integridad con conexión sin recuperación	x			x				
Integridad con conexión de un campo selectivo	x			x				
Integridad sin conexión	x	x		x				
Integridad sin conexión de un campo selectivo	x	x	x					
No repudio del origen		x		x				x
No repudio del destinatario		x		x				x

Fuente: Estándar ISO 7498-2.

b) Mecanismos de seguridad generalizados: No son específicos para los servicios de responsabilidad-auditoría, recuperación de la seguridad.

1. Funcionalidad fiable.
2. Etiquetas de seguridad.
3. Detección de acciones.
4. Informa para la auditoria de seguridad.
5. Recuperación de la seguridad.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.3.3.1. Honeynet

(Rosado M. C. 2014 p. 43) Es el conjunto de honeypot, se define como un tipo concreto de honeypot altamente interactivo diseñado para la captura de información de los posibles atacantes. El objetivo de Honeynet es engañar al atacante, quiere decir, hacer creer al atacante que está en la red, en alguno de los sistemas operativos. Presenta tres requerimientos básicos para que sea realmente valiosa.

Arquitectura

(Heredia, & Mauricio, 2015) Una arquitectura llega a ser el diseño conceptual de un sistema. Es un modelo y una descripción de todos los requerimientos y las implementaciones de diseño para los diferentes elementos que conforman una Honeynet.

(Areitio B. J., 2008, p. 361) Honeypot o señuelo es un sistema diseñado para aprender nuevos tipos de ataques, va analizando la identidad de los atacantes, tipo de tácticas que utiliza, así como también las herramientas que va empleando.

a) Generación I: Desarrollada por The Honeynet Project en el año 1999, posee una forma sencilla de control y captura de datos, permitiendo así la recopilación de actividades de los atacantes.
b) Generación II: Se caracteriza por tener los mecanismos de control y captura de datos en un dispositivo de capa dos en modo puente, conocido como Honeywall, que no modifica los paquetes de la re, también brinda control de las conexiones que entran y salen de los honeypot.
c) Generación III: Posee la misma arquitectura que la generación II, pero tiene ciertas mejoras en cuanto al análisis avanzado de datos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

(Díaz, Alzórriz, Sancristóbal & Castro, 2014, p. 38) Honeynet Project cuenta definió requisitos primordiales los cuales garantizaron el funcionamiento correcto de la Honeynet. Estos requisitos son:

a) Control de datos: Es el que mantiene un monitoreo constante de todo el flujo de datos de la red, evitando que los atacantes la utilicen.

b) Captura de datos: Es más conocida como la captura de los movimientos y acciones que el atacante realiza en la Honeynet, el tráfico capturado es de buena ayuda. La captura de registros suelen enviarse al servidor inexistente para que capture la máquina que está en modo promiscuo. Sebek actúa para la captura de los datos del atacante sin que este se dé cuenta que está siendo observado.

c) Recolección y análisis de datos: Realiza un análisis de la información del atacante permitiendo relacionar los datos obtenidos, así mismo permite realizar ingeniería inversa y recolección de datos.

Honeywall

(Díaz, Alzórriz, Sancristóbal & Castro, 2014, p.9) Es la herramienta de captura de la Honeynet, distribución Linux basada en Centos, posee diferentes componentes:

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 2. Componentes de Honeywall

Componente	Descripción
Sebek	Es la herramienta que se encarga de capturar los datos, diseñada para los ataques.
SessionLimit	Control de sesiones
Walleye	Es el que proporciona una herramienta de análisis de datos.
Snort_inline	Versión modificada de Snort que toma decisiones del tráfico.
Iptables	Es un firewall de Linux integrado en el Kernel, se encarga del registro de los datos en el momento de la captura de los ataques.
Pcap	Interfaz de captura de datos del Kernel
Swatch	Herramienta la cual permite comunicar al encargado de administrar por correo electrónico
Hflow	Aporta con la información del flujo de tráfico y las reacciones correspondientes.

Fuente: Elaboración propia

Valhala

(Valero D. F., 2012) Fue desarrollado por Marcos Flávio Assunção, es una herramienta la cual permite ejecutar el concepto de honeypot para ajustar a las necesidades de la que red que se administra, cuenta con diversos servicios: WEB, FTP, TFTP, POP3, ECHO, DAYTIME.

Sebek

(Proyecto HIS, 2003) Fue creado por un miembro de Honeynet Project, es una herramienta que consiste en recoger información dentro de la red de Honeynet, consiste en la captura de datos diseñada para la captura de los atacantes a los Honeypots. Posee dos componentes, un cliente y un servidor, es instalado en los Honeypots.

2.3.3.2. Snort

Definición

(Areitio B. J., 2008, p. 411) Es una herramienta de seguridad completa utilizado para la creación de IDS. La gran capacidad para la captura y registro de paquetes TCP/IP hace que cuente con una alta popularidad. Mediante el mecanismo de alertar y generación de archivos log snort cuenta con amplias posibilidades para el envido de alertas en tiempo real.

Elementos de Snort

(Arboleda A. y Bedón C., 2005, cap.3) Se compone de los siguientes elementos:

a) Módulo de captura de tráfico: Se encarga de la captura de los paquetes de la red.
b) Decodificador: Este se encarga de formar las estructuras con todos los paquetes capturados, para así identificar los protocolos de las capas.
c) Preprocesadores: Son los que permiten extender las diferentes funcionalidades para la detección.
d) Motor de detección: Analiza todos los paquetes mediante reglas ya establecidas.
e) Pos-procesadores: Son las partes del software que son compilados con Snort las cuales se usan para poder modificar el motor de detección.
f) Módulos detectores: Permiten donde se almacenar todas las alertas y los paquetes de red de datos que las generaron.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Operación de Snort

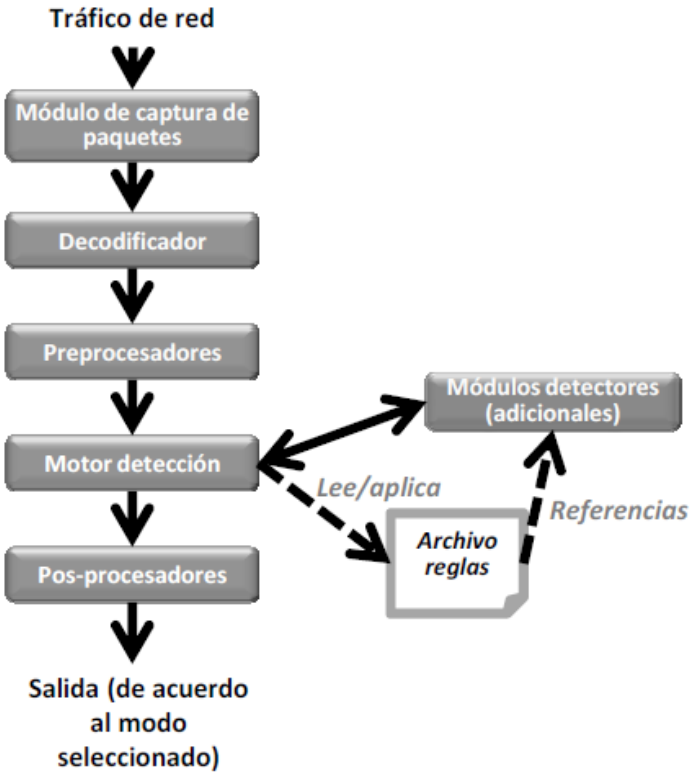


Figura 9. *Diagrama del funcionamiento de operación de Snort.*
Fuente: SnortTM diagrams for developers.

Tipos de Snort

a) HIDS (Host IDS): Sistema de detección de intrusos basado a un único servidor o host, este se encarga de controlar y visualizar los eventos, analizando las diferentes actividades, determinando a los usuarios y los procesos que se involucran en las acciones.

b) NIDS (Net IDS): Sistema de detección de intrusos basado en red, se encarga de proteger al sistema basado en red, este llega a actuar sobre una red, capturando y analizando paquetes de red de datos, así mismo se encarga de buscar los patrones de comportamiento.

2.3.4. Virtualización

(McNab C., 2008, p. 46) Gran parte de consultores de seguridad utilizan software de virtualización de servidores para fortalecer las

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

plataformas de prueba. Permite a un gran número de máquinas virtuales, ejecutando sistemas operativos y herramientas diferentes, ser ejecutadas en el mismo sistema físico. La virtualización permite simular sistemas operativos.

Arquitectura

Según (Jimeno G. M. et. al, 2009, p. 659) la arquitectura básica de una máquina virtual es claramente sencilla, puede almacenar varias máquinas virtuales de acuerdo a los recursos que se tenga disponible.

Arquitectura de virtualización

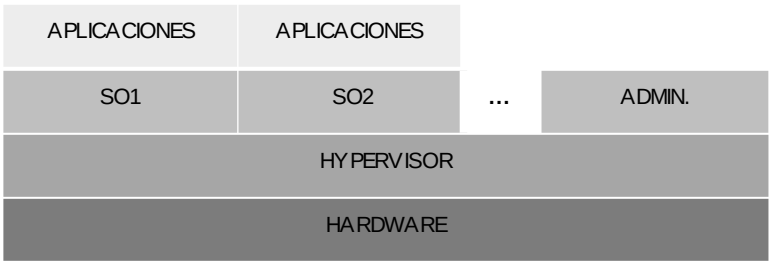


Figura 10. *Arquitectura básica de la virtualización de máquinas. Fuente: Elaboración propia.*

Tipos de máquinas virtuales

(Jimeno G. M. et. al, 2009, p. 661) Existen dos tipos de máquinas virtuales, dependiendo del grado de virtualización y abstracción de hardware.

a) Máquinas virtuales de sistema (System Virtual Machine): Permiten ejecutar un sistema operativo completo, este tipo de máquinas virtuales vienen a ser utilizadas en diferentes escenarios, como por ejemplo, varios sistemas operativos sobre el mismo servidor, simulaciones de hardware y consolidación de servidores.

Oracle VirtualBox

(Bejtlich R. 2005, p. 147) Software de virtualización gratuito y de código abierto creado por la empresa Innotek y posteriormente desarrollado por Oracle Corporation, es una solución recomendada a la hora de virtualizar, es para equipos de 32 y 64 bits. Permite la ejecución

de varias máquinas virtuales remotas por medio del protocolo RDP, los discos duros de los sistemas invitados son almacenados en un contenedor definido por defecto llamado Virtual Disk Image (VDI).

b) Máquinas virtuales de proceso (Process Virtual Machine): También son llamadas máquinas virtuales de aplicación, su principal objetivo es proporcionar un entorno virtual independiente a las aplicaciones. Como ejemplo se tiene a la máquina virtual de Java, la cual permite ejecutar el mismo programa compilado en Java en diferentes plataformas.

2.4. Definición de la terminología

a) DoS: Denial of services (denegación de servicio), es un ataque de fuerza bruta.

b) Exploits: Es un fragmento de software, o también secuencia de comandos o acciones, utilizada para aprovechar vulnerabilidades de seguridad del sistema para lograr conseguir un comportamiento no deseado del mismo.

c) FIREWALL: Llamados también cortafuegos, estos conforman la seguridad del sistema o una red, bloquear al acceso no autorizado, logrando la comunicaciones al mismo tiempo.

d) Honeynet: Son un conjunto de honeypots de alta o baja interacción. También son llamadas redes trampa, las cuales se pueden clasificar en virtuales, son diseñadas para capturar información del ataque y del atacante.

e) Honeypot: También conocido como sistema trampa o señuelo que trabaja en un solo ordenador, es una herramienta de la seguridad informática que actúa directamente con el ataque y sirve para brindar información de los atacantes.

f) IDS: También llamados sistema de detección de intrusos, que se encargan de monitorizar las redes y sistema que busca violaciones de políticas de seguridad.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

g) **IPS:** Sistema de prevención de intrusos, el cual se encarga de combinar las capacidades de bloqueo de un cortafuego y las de análisis de un IDS.
h) **Kali:** Es una distribución basada en Debian GNU/Linux.
i) **OSI:** Es un modelo de interconexión de sistemas abiertos, más conocido por sus siglas.
j) **Snort:** Es un Sniffer y un detector de intrusos basado en red. Un software con las capacidades de almacenamiento de datos, guarda bitácoras de texto y en base de datos, permite la verificación de toda la red.
k) **Url:** Es una referencia a un recurso web que especifica su ubicación en una red de ordenadores y un mecanismo para la recuperación de la misma
l) **Virtualbox:** Software de virtualización, es libre. Permite instalar sistemas operativos adicionales
m) **Vulnerabilidades:** Son todas las debilidades que posee un sistema, pueden ser utilizadas para infringir políticas de seguridad.
n) **Wireshark:** Antes conocido como Ethereal, se refiere a un analizador de protocolos, que es capaz de solucionar problemas de redes.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPITULO III: MARCO METODOLÓGICO

3.1. Tipo y diseño de la investigación

3.1.1. Tipo de la investigación

(Carpi & Anne, 2008) Hace referencia que la investigación comparativa es aquella que interpreta la relación entre dos o más variables, sean dependientes como independientes, logrando documentar las diferencias o semejanzas observadas entre los sujetos. Por ello, la comparación implica una observación en un marco natural, que no esté sujeto a fines experimentales.

En este proyecto de investigación el tipo de investigación es de tipo Comparativa Aplicada, dado a que en esta investigación se realizará la comparación de mecanismos de seguridad, de acuerdo a los ataques informáticos identificados, con el fin de evaluar si el producto final es capaz de contrarrestar dichos ataques.

3.1.2. Diseño de la investigación

(Cook & Campbell, 1986, p. 142) los autores hacen referencia que los cuasi-experimentos son como experimentos que se realizan por una asignación aleatoria, excepto en que no se puede presumir que los diversos grupos de tratamiento sean inicialmente semejantes dentro de los límites del error muestral.

El diseño de la presente investigación es Cuasi-Experimental.

3.2. Población y muestra

3.2.1. Población

La población se ha determinado tomando en cuenta los resultados de ESET (2015), quien muestra los incidentes de seguridad a las empresas de Latinoamérica, y que estos son 11 ataques más concurridos. El autor (Gómez, 2011) en su libro "*Enciclopedia de la Seguridad Informática"*, habla de la clasificación de ataques en general, entre ellos encontrando los

ataques externos, internos, a nivel de sistema, a nivel de aplicación, pasivos, activos y de fuerza bruta, también se refiere a los ataques que suelen ser más conocidos.

Estos tipos de ataques pueden ser neutralizados por diversos mecanismos de seguridad, los autores Guevara, Santos & López (2016), hacen referencia que existen reglas y técnicas de mecanismo de seguridad que en conjunto sirven para contrarrestar los ataques informáticos por medio de taza de detección y taza de falsos positivos, redes trampa, IDS. En este caso para los 11 ataques se consideran 4 mecanismos de seguridad libres Honeynet, Snort, OSSEC y Suricata.

3.2.2. Muestra

En la presente investigación se trabajó con dos tipos de ataques por conveniencia que pertenecen al top de incidentes de seguridad más comunes, los cuales son Exploración de vulnerabilidades y Denegación de Servicios. A estos se implementarán sus mecanismos de seguridad, en este caso serán dos mecanismos de seguridad informática, los cuales son Honeynet y Snort.

3.3. Hipótesis

Los mecanismos de seguridad informática implementados serán capaces de contrarrestar los ataques más frecuentes en servidores web y base de datos.

3.4. Variables

3.4.1. Variables dependientes

Contrarrestar ataques informáticos.

3.4.2. Variables independientes

Mecanismo de seguridad.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

3.5. Operacionalización

Variable Dependiente	Dimensiones	Indicadores	Formulas
Contrarrestar ataques informáticos	Indisponibilidad	Tiempo Indisponible del servidor	$Tindis = Tr - M$

Variable independiente	Dimensiones	Indicadores	Fórmula
Mecanismos de Seguridad	Tiempo	Tiempo de respuesta	$T = Tr - TI$
	Rendimiento	Precisión	$PR = \frac{VP}{VP + FP}$
		Sensibilidad	$SE = \frac{VP}{VP + FN}$
		Especificidad	$ES = \frac{VN}{VN + FP}$
		Exactitud	$EX = \frac{VP + VN}{VP + FP + FN + VN}$

3.6. Abordaje metodológico, técnicas e instrumentos de recolección de datos

3.6.1. Abordaje metodológico

La metodología que se utilizó para el trabajo de investigación fue la Gestión de la Seguridad informática, que se compone de cuatro procesos básicos, basados en el modelo PHVA.

Modelo PHVA - Procesos básicos

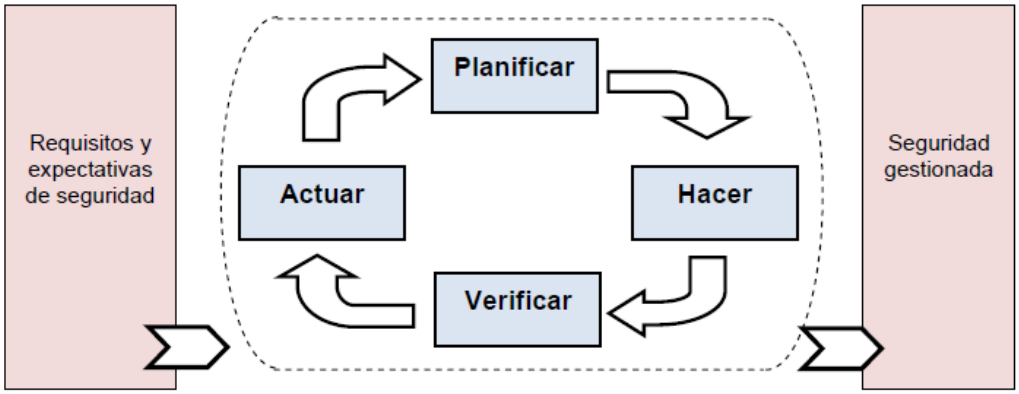


Figura 11. *Modelo PHVA aplicado a los procesos de Sistema de Gestión de la Seguridad Informática (SGSI).*
Fuente: Metodología para la Gestión de la Seguridad Informática.

Planificar

Se realizó un análisis de investigaciones anteriores, de acuerdo a la información recolectada, se planteó la comparación de mecanismos de seguridad. Se establecieron los objetivos y procedimientos de seguridad informática, para el incremento de seguridad de la información en los servidores web y base de datos.

Hacer

Se realizó la correcta recolección de información sobre los problemas de seguridad informática presentados en las empresas latinoamericanas, se obtuvo análisis de empresas como ESET y CNCERT, donde demostraban que incidentes eran los más frecuentes, encontrando entre ellos a ataques como DoS, inyección SQL, entre otros.

Como objetivo fundamental se garantizó una adecuada implementación de los mecanismos de seguridad informática seleccionados en la red de datos establecida, además de su correcta aplicación de los mismos, para mantener la integridad, confidencialidad y disponibilidad de los datos. Después de las pruebas de ataques realizadas a cada servidor con su mecanismos implementado.

Verificar

Evaluar la correcta implementación de los mecanismos de seguridad informática y verificar el desempeño de ellos, por medio de las pruebas de ataques, tanto Denegación de servicio (DoS) como Exploración de vulnerabilidades, realizadas a cada servidor con su mecanismo, obteniendo como resultados las diferentes métricas de evaluación, como tiempos de indisponibilidad del servidor y de respuestas.

Actuar

Para la mejora de la seguridad informática en los servidores web y base de datos, se realizó la comparación de los mecanismos de seguridad, de acuerdo a los resultados arrojados por las pruebas realizadas anteriormente, para saber cuál es la reacción de los mecanismos frente a los ataques, en los tiempo de indisponibilidad del servidor y en los tiempos de respuesta de cada mecanismo.

3.6.2. Técnicas de recolección de datos

Las técnicas que se utilizaron en el trabajo de investigación para la recolección de los datos son:

Recopilación documental

Esta es una técnica de apoyó en la recopilación de información, la cual contiene antecedentes (documentos, artículos, libros y gráficos). Para la investigación estas fuentes fueron de tipo bibliográficas, las cuales en conjunto sirvieron como fundamento e inicialización y como complemento para el desarrollo de la investigación.

Recopilación de datos experimentales

Esta técnica se basa en la recolección de datos, de acuerdo a la experimentación, la cual consiste en el estudio de las características y reacción de los mecanismos de seguridad, así mismo en la observación constante que se hace a los ataques y mecanismos. Esta técnica permitió

recolectar los datos de la simulación de los mecanismos de seguridad, que luego servirán para comparar y analizar los resultados con la hipótesis.

3.6.3. Instrumentos de recolección de datos

a) Reportes proporcionados por los sistemas a utilizar.

b) Informes de entidades reconocidas como CISCO o ESET donde indica los ataques más comunes a los servidores.

c) Matriz de trabajos de investigación.

d) Capturas de pantallas de los resultados obtenidos por los mecanismos de seguridad informática.

e) Tablas de paquetes enviados a los mecanismos de seguridad informática.

3.7. Procedimientos para la recolección de datos

No se ha encontrado un método estándar para identificar los mecanismos de seguridad informáticos, por lo que se ha optado por utilizar un método propio. Debido a que la solución y desarrollo será en el Laboratorio de Investigación de Sistemas Inteligentes y Seguridad de la Información (LABSIS) de la Universidad Señor de Sipán, la primera fase comprendió un arduo estudio de campo del mismo. Entonces el método comprenderá las siguientes fases:

Fase 1: Identificación de ataques informáticos

Se procedió a una previa investigación de los ataques de seguridad informática más concurrentes, de acuerdo a eso se logró recolectar información estadística con tops de los ataques informáticos para su posterior selección.

Fase 2: Selección de mecanismos de seguridad

En esta fase se seleccionó los mecanismos de seguridad informática libres con los que se trabajó, esta fase se realizó gracias a las previas investigaciones y posteriormente se implementaron en la red de datos diseñada.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Fase 3: Implementación de mecanismos de seguridad

Esta fase comprendió el desarrollo de cada mecanismo de seguridad a la red de datos y sus pruebas frente a los ataques informáticos seleccionados anteriormente. En esta fase se realizaron las pruebas con los dos tipos de ataques a cada uno de los servidores tanto web como base de datos.

Fase 4: Evaluación de los mecanismos de seguridad

En esta fase se realizó el análisis de cada mecanismo de seguridad implementado, por medio de los resultados de cada uno de sus indicadores, los que son tiempo de indisponibilidad del servidor, tiempo de respuesta y el rendimiento de cada mecanismo, frente a los ataques informáticos.

Fase 5: Comparación de los mecanismos de seguridad

Esta fase permitió realizar la comparación de ambos mecanismos de seguridad de acuerdo a sus indicadores establecidos, para saber si estos fueron capaces de contrarrestar dichos ataques.

3.8. Plan de análisis estadístico de datos

Para el análisis de cada técnica de mecanismo de seguridad evaluado en cada prueba, se calculó los porcentajes de tiempo de indisponibilidad, tiempo de respuesta y rendimiento en la detección de ataques informáticos.

Los resultados de las pruebas realizadas serán evaluados utilizando las siguientes fórmulas:

Variable Dependiente: Contrarrestar ataques informáticos

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Impacto

1. Tiempo de indisponibilidad

Tabla 3. Análisis estadístico de tiempo indisponible del servidor

$Tindis = Tr - M$		
Variable	**¿Qué es?**	**¿Cómo se obtiene?**
T_r	Es el tiempo en el servidor queda indisponible.	Se del segundo donde el servidor queda indisponible por los ataques.
M	Es el momento en el que el mecanismo responde	Se obtiene del segundo donde el mecanismo reacciona frente a los ataques
$Tindis$	Es el porcentaje del tiempo indisponible.	Se obtiene del tiempo que queda indisponible el servidor menos el tiempo en que reacciona el mecanismo – expresado en segundos.

Fuente: Elaboración propia

Variable Independiente: Mecanismos de Seguridad

Tiempo

1. Tiempo de Respuesta

Tabla 4. Análisis estadístico de tiempo de respuesta

$T = T_r - T_i$		
Variable	**¿Qué es?**	**¿Cómo se obtiene?**
T_r	Es el tiempo en el reacciona el mecanismo.	Se captura la hora en la que el mecanismo reacciona
T_i	Es el tiempo en el que se inicia la prueba.	Se captura la fecha en la que se inicia la prueba.
T	Es el tiempo de respuesta que demora en contrarrestar los ataques.	Se obtiene con la resta del tiempo reacción – el tiempo inicial expresado en segundos.

Fuente: Elaboración propia

Rendimiento

1. Precisión

Tabla 5. Análisis estadístico de precisión

$$PR = \frac{VP}{VP + FP}$$

Variable	¿Qué es?	¿Cómo se obtiene?
VP	Son los verdaderos positivos del paquete de ataque seleccionado, enviados por el tráfico malicioso.	Se obtienen de los paquetes que son detectados como ataques por el mecanismo
FP	Son los falsos positivos de los paquetes del ataque seleccionado, enviados por el tráfico malicioso.	Se obtienen de los paquetes que no son detectados como ataques por el mecanismo
PR	Es la precisión con la que actúa el mecanismos de seguridad	Se obtiene de los verdaderos positivos (VP) sobre los verdades positivos (VP) más los falsos positivos (FP)

Fuente: Elaboración propia

2. Sensibilidad

Tabla 6. Análisis estadístico de sensibilidad

$$SE = \frac{VP}{VP + FN}$$

Variable	¿Qué es?	¿Cómo se obtiene?
VP	Son los verdaderos positivos de los paquetes del ataque seleccionado, enviados por el tráfico malicioso.	Se obtienen de los paquetes que son detectados como ataques por el mecanismo

FN	Son falsos negativos de los paquetes del ataque seleccionado, enviados por el tráfico normal.	Se obtienen de los paquetes que son detectados como ataques por el mecanismo
SE	Es la capacidad del mecanismo de seguridad para identificar resultados verdaderos positivos.	Se obtiene de los verdaderos positivos (VP) sobre los verdades positivos (VP) más los falsos positivos (FN)

Fuente: Elaboración propia

3. Especificidad

Tabla 7. Análisis estadístico de especificidad

$$ES = \frac{VN}{VN + FP}$$

Variable	¿Qué es?	¿Cómo se obtiene?
VN	Son verdaderos negativos de los paquetes del ataque seleccionado, enviados por el tráfico normal.	Se obtienen de los paquetes que no son detectados como ataques por el mecanismo.
FP	Son los falsos positivos de los paquetes del ataque seleccionado, enviados por el tráfico malicioso.	Se obtienen de los paquetes que no son detectados como ataques por el mecanismo
ES	Es la capacidad del mecanismo de seguridad para identificar los resultados negativos	Se obtiene de los verdaderos positivos (VP) sobre los verdaderos positivos (VP) más los falsos positivos. (FN)

Fuente: Elaboración propia

4. Exactitud

Tabla 8. Análisis estadístico de exactitud

$$EX = \frac{VP + VN}{VP + FP + FN + VN}$$

Variable	¿Qué es?	¿Cómo se obtiene?
VP	Son los verdaderos positivos del paquete de ataque seleccionado, enviados por el tráfico malicioso.	Se obtienen de los paquetes que son detectados como ataques por el mecanismo
VN	Son verdaderos negativos de los paquetes del ataque seleccionado, enviados por el tráfico normal.	Se obtienen de los paquetes que no son detectados como ataques por el mecanismo.
FP	Son los falsos positivos de los paquetes del ataque seleccionado, enviados por el tráfico malicioso.	Se obtienen de los paquetes que no son detectados como ataques por el mecanismo
FN	Son falsos negativos de los paquetes del ataque seleccionado, enviados por el tráfico normal.	Se obtienen de los paquetes que son detectados como ataques por el mecanismo
EX	Es el grado de cercanía de las mediciones de una cantidad al valor de la magnitud real	Se obtiene de los verdaderos positivos (VP) más los verdaderos negativos (VN) sobre la suma de os verdaderos positivos (VP) , falsos positivos (FP) , falsos negativos (FN) y verdaderos negativos. (VN)

Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Para la correcta evaluación de los mecanismos de seguridad se tomó en cuenta un cuadro de la clasificación de métricas de rendimiento.

Métricas de rendimiento

		Condición (según lo determinado por el "Gold Standard")		
		Condición **Positiva**	Condición **Negativa**	
Resultado de la prueba	Resultados **Positivos** de la prueba	**Verdadero Positivo**	Falso Positivo (error tipo I)	**Valor predictivo positivo (precisión)=** $\frac{\sum VerdaderosPositivos}{\sum ResultadosPositivos}$
	Resultados **Negativos** de la prueba	Falso Negativo (error tipo II)	**Verdadero Negativo**	**Valor predictivo negativo=** $\frac{\sum VerdaderosNegativos}{\sum ResultadosNegativos}$
		Sensibilidad= $\frac{\sum VerdaderosPositivos}{\sum CondiciónPositiva}$	**Especificidad=** $\frac{\sum VerdaderosNegativos}{\sum CondiciónNegativa}$	**Exactitud=** $\frac{\sum Verdaderos}{\sum ResultadosVerdaderosyNegativos}$

Figura 12. *Métricas de rendimiento a evaluar.*
Fuente: Modelo de detección de intrusiones en sistemas de red, realizando selección de características con FDR y entrenamiento y clasificación con SOM.

3.9. Criterios éticos

a) Veracidad: El ambiente en que se realizaron las pruebas sea objetivo y no subjetivo, donde los resultados fueron concordes a lo establecido.

b) Confidencialidad: La investigación guardó ética profesional al momento de la realización de pruebas, mantuvo en privacidad la información que contenían los servidores.

3.10. Criterios de rigor científico

a) Validez: La Operacionalización de las variables tanto dependiente como independiente y sus dimensiones descritas se evaluaron mediante indicadores establecidos y las técnicas de recolección de datos.

b) Fiabilidad: La configuración de ambos servidores, las pruebas realizadas y de los resultados obtenidos se toman como referencia

CAPITULO IV: RESULTADOS

4.1. Ejecución de ataques a la red

Se realizaron un total de 400 pruebas con diferentes números de paquetes enviados, obteniendo el promedio de los paquetes. Los paquetes se clasificaron por medio de:

a) Verdaderos positivos (VP), que viene a ser los paquetes del tráfico de ataque detectados como ataques.
b) Falsos positivos (FP), que son los paquetes del tráfico de ataque detectados como no ataques.
c) Falsos negativos (FN), que vienen a ser los paquetes del tráfico normal detectados como ataques.
d) Verdaderos negativos (VN), que son los paquetes del tráfico normal detectados como no ataques.

4.1.1. Mecanismo de seguridad Honeynet

Ataque DoS a Servidor web

Se realizaron 50 pruebas de ataques DoS al honeypot web, tanto para el tráfico con el ataque correspondiente como para el tráfico normal. *(Tabla 43 - ANEXO 1)*

Los valores obtenidos de las pruebas son los promedios que sirvieron como datos para los indicadores. El tiempo de indisponibilidad es:

$$T.indisp = 2s$$

El tiempo de respuesta fue la resta del tiempo de reacción del mecanismo y el tiempo inicial de la prueba, obteniendo como resultado promedio:

$$T = 4s$$

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

De acuerdo a los datos promedio obtenidos en la *(Tabla 44 – ANEXO 1)*, se lograron adecuar a las métricas de clasificador binario.

Tabla 9. Promedio de paquetes enviados al servidor web con ataque DoS

	HONEYNET	
	Detectado como ataque	**Detectado como no ataque**
Tráfico Ataque	1996	40
Tráfico Normal	5	1764

Fuente: Elaboración propia

Como resultados del indicador de rendimiento se obtienen los porcentajes:

Tabla 10. Métricas de evaluación de rendimiento en servidor web con Honeynet

Precisión	$\frac{\mathbf{1996}}{\mathbf{1996+40}}$	98,0%
Sensibilidad	$\frac{1996}{1996+5}$	99,7%
Especificidad	$\frac{1764}{1764+40}$	97,7%
Exactitud	$\frac{1996+1764}{1996+40+5+1764}$	98,8%

Fuente: Elaboración propia

Ataque DoS a servidor Base de Datos

Se realizaron 50 pruebas de ataques DoS al honeypot base de datos, tanto para el tráfico con el ataque correspondiente como para el tráfico normal. *(Tabla 45 – ANEXO 1)*

Los valores obtenidos de las pruebas son los promedios que sirvieron como datos para los indicadores. El tiempo de indisponibilidad es:

$$T.indisp = 2s$$

El tiempo de respuesta es la diferencia del tiempo de reacción del mecanismo y el tiempo inicial de la prueba, obteniendo como resultado promedio:

$$T = 5s$$

De acuerdo a los datos promedio obtenidos en la *(Tabla 46 - ANEXO 1)*, se lograron adecuar a las métricas de clasificador binario.

Tabla 11. Promedio de paquetes enviados a servidor base de datos con ataque DoS

	HONEYNET	
	Detectado como ataque	**Detectado como no ataque**
Tráfico Ataque	1947	42
Tráfico Normal	6	1747

Fuente: Elaboración propia

Como resultados del indicador de rendimiento se obtienen los porcentajes:

Tabla 12. Métricas de evaluación de rendimiento en servidor base de datos con Honeynet

Precisión	$\frac{\mathbf{1947}}{\mathbf{1947 + 42}}$	97,8%
Sensibilidad	$\frac{1947}{1947 + 6}$	99,6%
Especificidad	$\frac{1747}{1747 + 42}$	97,4%
Exactitud	$\frac{1947 + 1747}{1947 + 42 + 6 + 1747}$	98,6%

Fuente: Elaboración propia

Ataque Exploración de vulnerabilidades a servidor web

Se realizaron 50 pruebas de ataques Exploración de vulnerabilidades al honeypot web, tanto para el tráfico con el ataque correspondiente como para el tráfico normal. *(Tabla 47 - ANEXO 1)*

Los valores obtenidos de las pruebas son los promedios que sirvieron como datos para los indicadores. El tiempo de indisponibilidad es 0, ya que no deja indisponible al servidor, porque es un ataque pasivo.

$$T.indisp = 0s$$

El tiempo de respuesta es la diferencia del tiempo de reacción del mecanismo y el tiempo inicial de la prueba, obteniendo como resultado promedio:

$$T = 4s$$

De acuerdo a los datos promedio obtenidos en la *(Tabla 48 - ANEXO 1)*, se lograron adecuar a las métricas de clasificador binario.

Tabla 13. Promedio de paquetes enviados a servidor web con ataque Exploración de vulnerabilidades

	HONEYNET	
	Detectado como ataque	**Detectado como no ataque**
Tráfico Ataque	469	15
Tráfico Normal	5	397

Fuente: Elaboración propia

Como resultados del indicador de rendimiento se obtienen los porcentajes:

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 14. Métricas de evaluación de rendimiento en servidor web con Honeynet

Precisión	$\frac{\mathbf{469}}{\mathbf{469+15}}$	96,9%
Sensibilidad	$\frac{469}{469+5}$	98,9%
Especificidad	$\frac{397}{397+15}$	96,4%
Exactitud	$\frac{469+397}{469+15+5+397}$	97,8%

Fuente: Elaboración propia

Ataque de exploración de vulnerabilidades a servidor Base de datos

Se realizaron 50 pruebas de ataques Exploración de vulnerabilidades al honeypot base de datos, tanto para el tráfico con el ataque correspondiente como para el tráfico normal. *(Tabla 49 - ANEXO 1)*

Los valores obtenidos de las pruebas son los promedios que sirvieron como datos para los indicadores. El tiempo de indisponibilidad es 0, ya que no deja indisponible al servidor, porque es un ataque pasivo.

$$T.indisp = 0s$$

El tiempo de respuesta es la diferencia del tiempo de reacción del mecanismo y el tiempo inicial de la prueba, obteniendo como resultado promedio:

$$T = 5s$$

De acuerdo a los datos promedio obtenidos en la *(Tabla 50- ANEXO 1)*, se lograron adecuar a las métricas de clasificador binario.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 15. Promedio de paquetes enviados a servidor base de datos con ataque Exploración de vulnerabilidades

	HONEYNET	
	Detectado como ataque	**Detectado como no ataque**
Tráfico Ataque	461	12
Tráfico Normal	4	382

Fuente: Elaboración propia

Como resultados del indicador de rendimiento se obtienen los porcentajes:

Tabla 16. Métricas de evaluación de rendimiento en servidor base de datos con Honeynet

Precisión	$\frac{\mathbf{461}}{\mathbf{461+12}}$	97,3%
Sensibilidad	$\frac{461}{461+4}$	98,7%
Especificidad	$\frac{382}{382+12}$	96,6%
Exactitud	$\frac{461+382}{461+12+4+382}$	98,1%

Fuente: Elaboración propia

4.1.2. Mecanismo de seguridad Snort

Ataque DoS a servidor Web

Se realizaron 50 pruebas de ataques DoS al servidor web, tanto para el tráfico con el ataque correspondiente como para el tráfico normal. *(Tabla 51 - ANEXO 1)*

Los valores obtenidos de las pruebas son los promedios que sirvieron como datos para los indicadores. El tiempo de indisponibilidad es:

$$T.indisp = 3s$$

El tiempo de respuesta fue la resta del tiempo de reacción del mecanismo y el tiempo inicial de la prueba, obteniendo como resultado promedio:

$$T = 5s$$

De acuerdo a los datos promedio obtenidos en *(Tabla 52 - ANEXO 1)*, se lograron adecuar a las métricas de clasificador binario.

Tabla 17. Promedio de paquetes enviados a servidor web con ataque Dos

	SNORT	
	Detectado como ataque	**Detectado como no ataque**
Tráfico Ataque	1825	37
Tráfico Normal	4	1840

Fuente: Elaboración propia

Como resultados del indicador de rendimiento se obtienen los porcentajes:

Tabla 18. Métricas de evaluación de rendimiento en servidor web con Snort

Precisión	$\frac{\mathbf{1825}}{\mathbf{1825 + 37}}$	98,0%
Sensibilidad	$\frac{1825}{1825 + 4}$	98,1%
Especificidad	$\frac{1840}{1840 + 37}$	98,0%
Exactitud	$\frac{1825 + 1840}{1825 + 37 + 4 + 1840}$	98,1%

Fuente: Elaboración propia

Ataque DoS a servidor Base de Datos

Se realizaron 50 pruebas de ataques DoS al servidor base de datos, tanto para el tráfico con el ataque correspondiente como para el tráfico normal. *(Tabla 53 - ANEXO 1)*

Los valores obtenidos de las pruebas son los promedios que sirvieron como datos para los indicadores. El tiempo de indisponibilidad es:

$$T.indisp = 2s$$

El tiempo de respuesta fue la resta del tiempo de reacción del mecanismo y el tiempo inicial de la prueba, obteniendo como resultado promedio:

$$T = 5s$$

De acuerdo a los datos promedio obtenidos en *(Tabla 54 - ANEXO 1),* se lograron adecuar a las métricas de clasificador binario.

Tabla 19. Promedio de paquetes enviados a servidor base de datos con ataque Dos

	SNORT	
	Detectado como ataque	**Detectado como no ataque**
Tráfico Ataque	1865	40
Tráfico Normal	7	1833

Fuente: Elaboración propia

Como resultados del indicador de rendimiento se obtienen los porcentajes:

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 20. Métricas de evaluación de rendimiento en servidor base de datos con Snort

Precisión	$\frac{\mathbf{1865}}{\mathbf{1865+40}}$	98,8%
Sensibilidad	$\frac{1865}{1865+7}$	97,9%
Especificidad	$\frac{1833}{1862+40}$	97,8%
Exactitud	$\frac{1865+1833}{1865+40+7+1833}$	98,7%

Fuente: Elaboración propia

Ataque de Exploración de vulnerabilidades a servidor web

Se realizaron 50 pruebas de ataques Exploración de vulnerabilidades al servidor web, tanto para el tráfico con el ataque correspondiente como para el tráfico normal. *(Tabla 55 - ANEXO 1)*

Los valores obtenidos de las pruebas son los promedios que sirvieron como datos para los indicadores. El tiempo de indisponibilidad es 0, ya que no deja indisponible al servidor, porque es un ataque pasivo.

$$T.indisp = 0s$$

El tiempo de respuesta fue la resta del tiempo de reacción del mecanismo y el tiempo inicial de la prueba, obteniendo como resultado promedio:

$$T = 5s$$

De acuerdo a los datos promedio obtenidos en *(Tabla 56- ANEXO 1),* se lograron adecuar a las métricas de clasificador binario.

Tabla 21. Promedio de paquetes enviados a servidor web con ataque Exploración de vulnerabilidades

	SNORT	
	Detectado como ataque	**Detectado como no ataque**
Tráfico Ataque	467	12
Tráfico Normal	5	393

Fuente: Elaboración propia

Como resultados del indicador de rendimiento se obtienen los porcentajes:

Tabla 22. Métricas de evaluación de rendimiento en servidor web con Snort

Precisión	$\frac{\mathbf{467}}{\mathbf{467+12}}$	97,5%
Sensibilidad	$\frac{467}{467+5}$	97,0%
Especificidad	$\frac{393}{393+12}$	97,8%
Exactitud	$\frac{467+393}{467+12+5+393}$	98,0%

Fuente: Elaboración propia

Ataque de exploración de vulnerabilidades a servidor Base de datos

Se realizaron 50 pruebas de ataques Exploración de vulnerabilidades al honeypot base de datos, tanto para el tráfico con el ataque correspondiente como para el tráfico normal. *(Tabla 57 - ANEXO 1)*

Los valores obtenidos de las pruebas son los promedios que sirvieron como datos para los indicadores. El tiempo de indisponibilidad es 0, ya que no deja indisponible al servidor, porque es un ataque pasivo.

$$T.indisp = 0s$$

El tiempo de respuesta fue la resta del tiempo de reacción del mecanismo y el tiempo inicial de la prueba, obteniendo como resultado promedio:

$$T = 4s$$

De acuerdo a los datos promedio obtenidos en *(Tabla 58 - ANEXO 1)*, se lograron adecuar a las métricas de clasificador binario.

Tabla 23. Promedio de paquetes enviados a servidor base de datos con ataque Exploración de vulnerabilidades

	SNORT	
	Detectado como ataques	**Detectado como no ataque**
Tráfico Ataque	466	12
Tráfico Normal	4	388

Fuente: Elaboración propia

Como resultados del indicador de rendimiento se obtienen los porcentajes:

Tabla 24. Métricas de evaluación de rendimiento en servidor base de datos con Snort

Precisión	$\frac{\mathbf{466}}{\mathbf{466+12}}$	97,4%
Sensibilidad	$\frac{466}{466+4}$	99,1%
Especificidad	$\frac{388}{388+12}$	96,9%
Exactitud	$\frac{466+388}{466+12+4+388}$	97,2%

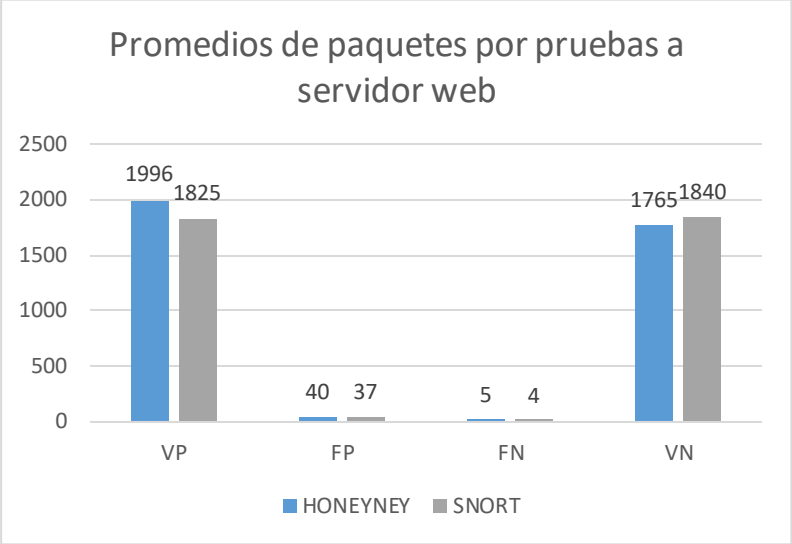
Fuente: Elaboración propia

4.2. Comparación de mecanismos de seguridad

En los siguientes gráficos se describen las comparaciones de ambos mecanismos, de acuerdo a los tipos de ataques a cada servidor.

Denegación de servicio

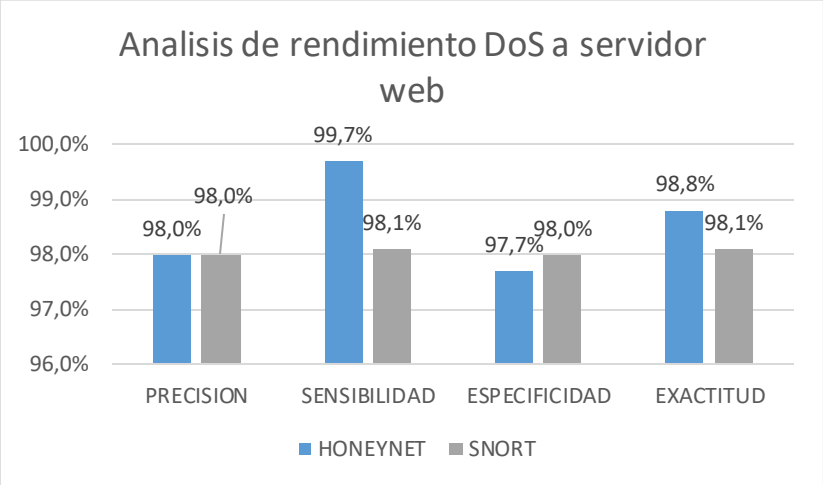
Servidores web



Gráfica 1. Resultados de promedios de paquetes enviados por prueba al servidor web

De las 50 pruebas realizadas mediantes el tráfico de ataque de denegación de servicio (DoS) y el tráfico normal a servidores web, se obtuvieron los promedios clasificados en verdaderos positivos (VP), falsos positivos (FP), falsos negativos (FN), verdaderos negativos (VN). De acuerdo a los paquetes enviados se obtiene una pequeña diferencia entre Honeynet y Snort.

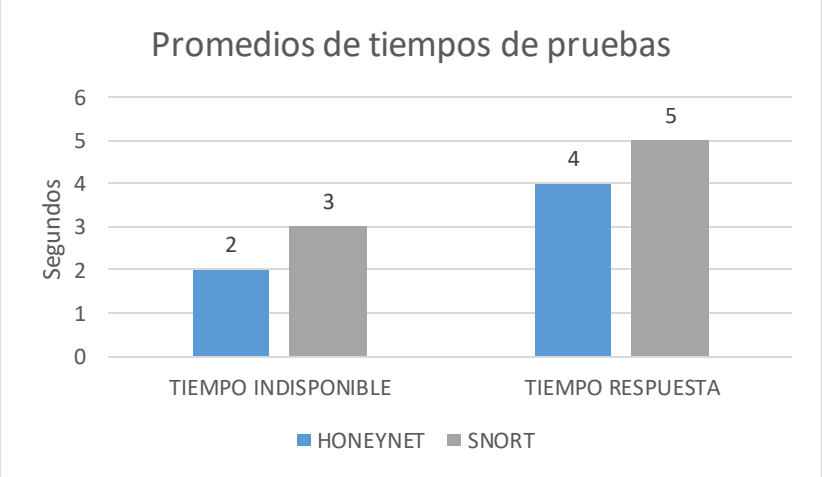
Rendimiento



Gráfica 2. Resultados de métricas de rendimiento de ambos mecanismos, con ataque DoS a servidor web

De acuerdo a los promedios obtenidos de las pruebas realizadas a ambos mecanismos, se observó que Snort y Honeynet muestran el mismo grado de asertividad (precisión), Snort muestra el 0,3% de capacidad que el mecanismo detecta al tráfico normal (especificidad), mientras que Honeynet tiene una ligera ventaja de 1,6% en sensibilidad y una pequeña ventaja de 0,7% en exactitud.

Tiempo de indisponibilidad y de respuesta



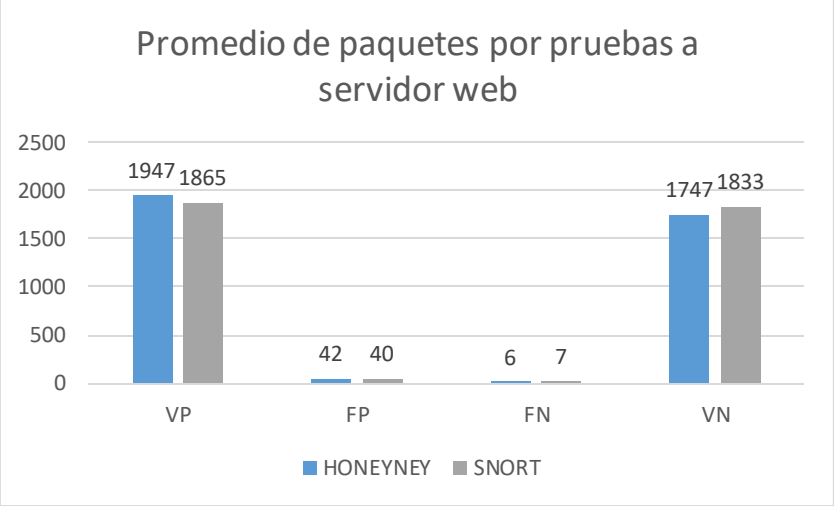
Gráfica 3. Promedios de tiempo de indisponibilidad del servidor web y del tiempo de respuesta de ambos mecanismos

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

El servidor web queda indisponible durante el ataque DoS en un tiempo promedio de 2 segundos teniendo el mecanismo de seguridad Honeynet, mientras que con el mecanismo Snort tiene un tiempo indisponible de 3 segundos, teniendo una pequeña ventaja el mecanismo Honeynet ya que el tiempo es menor.

El tiempo de respuesta del mecanismo Honeynet es al segundo 4 de iniciada la prueba, mientras que Snort responde al segundo 5, iniciada la prueba, esto significa que el mecanismo Honeynet reacciona un segundo antes.

Servidores base de datos

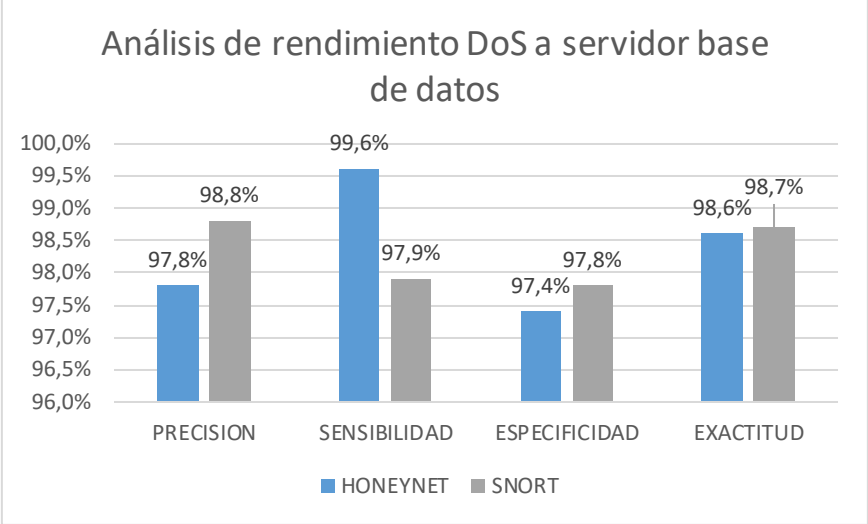


Gráfica 4. Resultados de promedios de paquetes enviados por prueba al servidor base de datos

De las 50 pruebas realizadas mediantes el tráfico de ataque de denegación de servicio (DoS) y el tráfico normal a servidores base de datos, se obtuvieron los promedios clasificados en verdaderos positivos (VP), falsos positivos (FP), falsos negativos (FN), verdaderos negativos (VN). De acuerdo a los paquetes enviados se obtiene una pequeña diferencia entre honeynet y snort.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

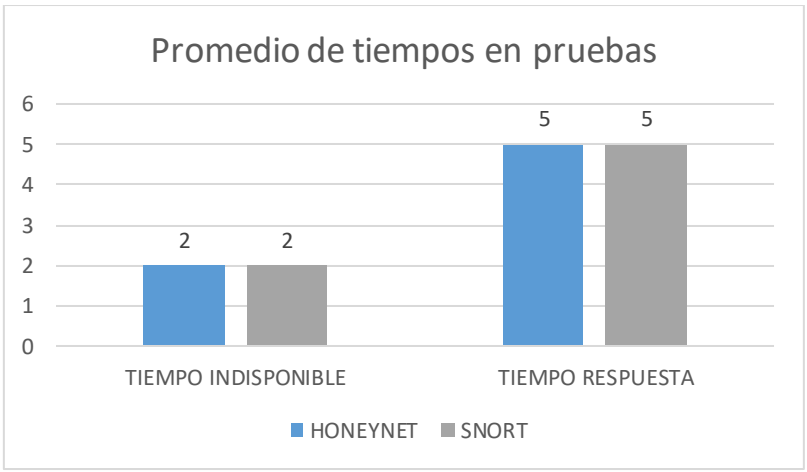
Rendimiento



Gráfica 5. Resultados de métricas de rendimiento de ambos mecanismos, con ataque DoS a servidor base de datos

De acuerdo a los promedios obtenidos de las pruebas realizadas a ambos mecanismos, se observó que Snort muestra un 1% más grado de asertividad (precisión), así como también 0,4% de capacidad que el mecanismo detecta al tráfico normal (especificidad) y una pequeña ventaja de 0,1% en exactitud, mientras que Honeynet tiene una ligera ventaja de 1,7% en sensibilidad.

Tiempo de indisponibilidad y de respuesta



Gráfica 6. Promedios de tiempo de indisponibilidad del servidor web y del tiempo de respuesta de ambos mecanismos

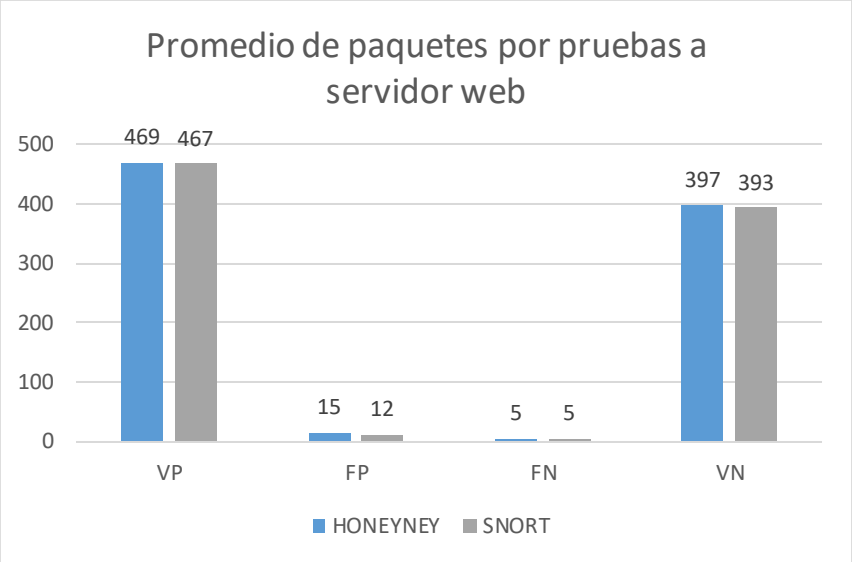
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

El servidor base de datos queda indisponible durante el ataque DoS en un tiempo promedio de 2 segundos teniendo tanto el mecanismo de seguridad Honeynet y el mecanismo Snort.

El tiempo de respuesta de ambos mecanismos es de 5 segundo iniciada la prueba, esto significa que los mecanismos reaccionaron al mismo tiempo.

Exploración de vulnerabilidades

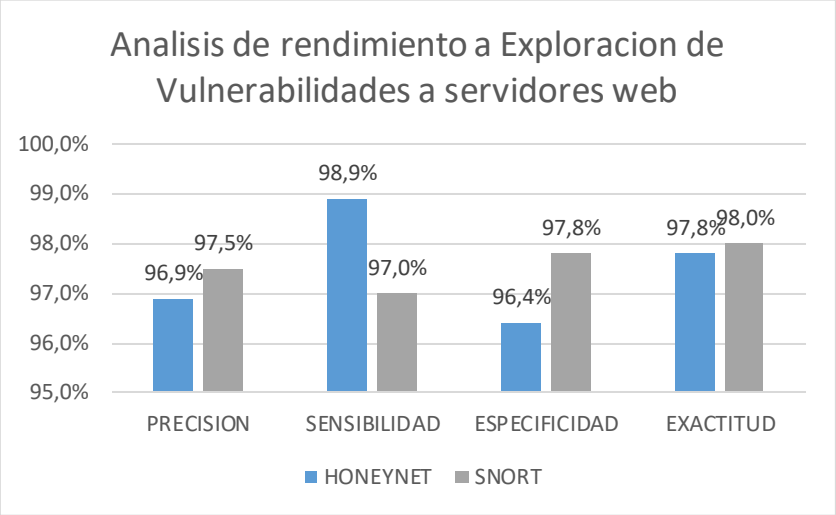
Servidor web



Gráfica 7. Resultados de promedios de paquetes enviados por prueba al servidor web

De las 30 pruebas realizadas mediantes el tráfico de ataque de Exploración de vulnerabilidades y el tráfico normal a servidores web, se obtuvieron los promedios clasificados en verdaderos positivos (VP), falsos positivos (FP), falsos negativos (FN), verdaderos negativos (VN). De acuerdo a los paquetes enviados se obtiene una pequeña diferencia entre Honeynet y Snort.

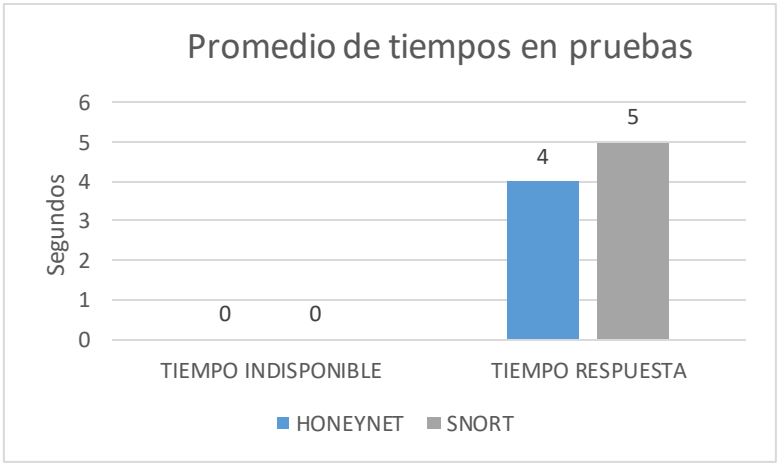
Rendimiento



Gráfica 8. Resultados de métricas de rendimiento de ambos mecanismos, con ataque Exploración de vulnerabilidades a servidor web

De acuerdo a los promedios obtenidos de las pruebas realizadas a ambos mecanismos, se observó que Snort muestra un 0,6% más grado de asertividad (precisión), así como también 1,4% de capacidad que el mecanismo detecta al tráfico normal (especificidad) y una pequeña ventaja de 0,2% en exactitud, mientras que Honeynet tiene una ligera ventaja de 1,9% en sensibilidad

Tiempo de indisponibilidad y de respuesta



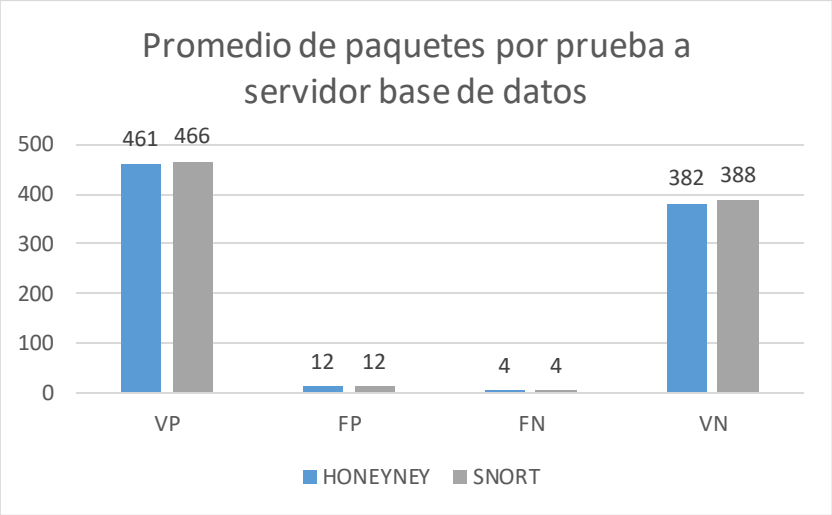
Gráfica 9. Promedios de tiempo de indisponibilidad del servidor web y del tiempo de respuesta de ambos mecanismos

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

El servidor web no queda indisponible durante el ataque Exploración de vulnerabilidades, ya que dicho ataque es pasivo.

El tiempo de respuesta del mecanismo Honeynet es al 4 segundo iniciada la prueba, mientras que Snort al segundo 5, esto significa que lo el mecanismo Honeynet tiene una ventaja de 1 segundo.

Servidor base de datos

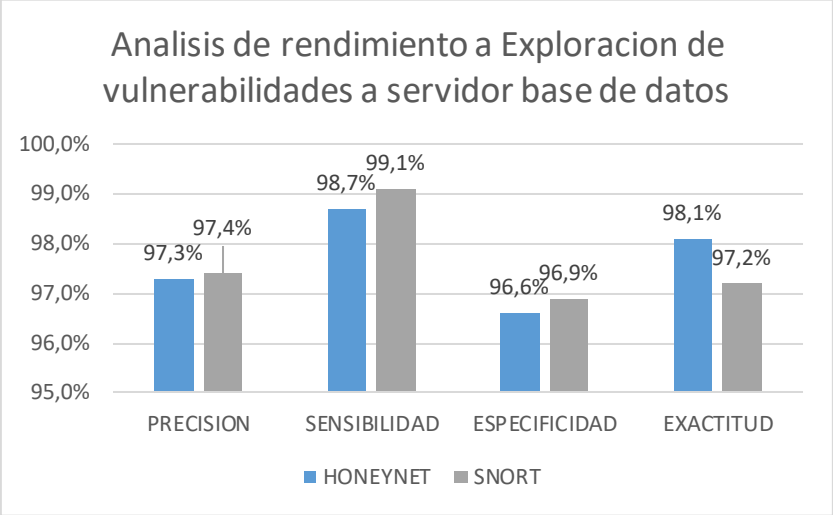


Gráfica 10. Resultados de promedios de paquetes enviados por prueba al servidor base de datos

De las 50 pruebas realizadas mediantes el tráfico de ataque de Exploración de vulnerabilidades y el tráfico normal a servidores a base de datos, se obtuvieron los promedios clasificados en verdaderos positivos (VP), falsos positivos (FP), falsos negativos (FN), verdaderos negativos (VN). De acuerdo a los paquetes enviados se obtiene una pequeña diferencia entre Honeynet y Snort.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

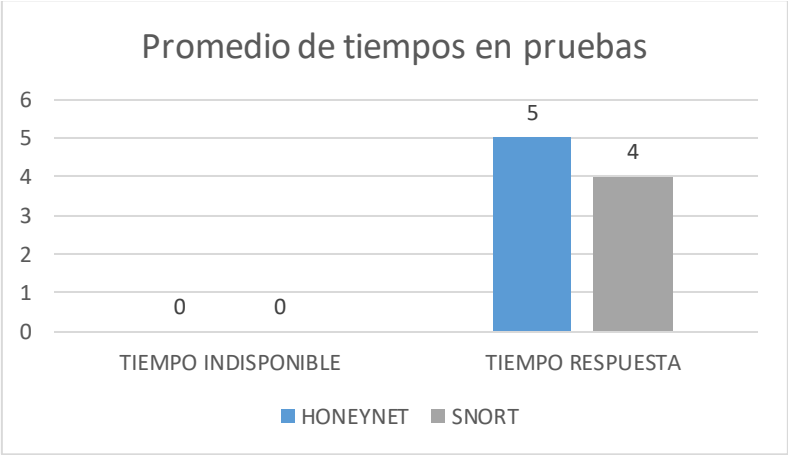
Rendimiento



Gráfica 11. Resultados de métricas de rendimiento de ambos mecanismos, con ataque Exploración de vulnerabilidades a servidor base de datos

De acuerdo a los promedios obtenidos de las pruebas realizadas a ambos mecanismos, se observó que Snort muestra un 0,1% más grado de asertividad (precisión), así como también 0,3% de capacidad que el mecanismo detecta al tráfico normal (especificidad) y una ligera ventaja de 0,4% en sensibilidad, mientras que Honeynet tiene una pequeña ventaja de 0,9% en exactitud.

Tiempo de indisponibilidad y de respuesta



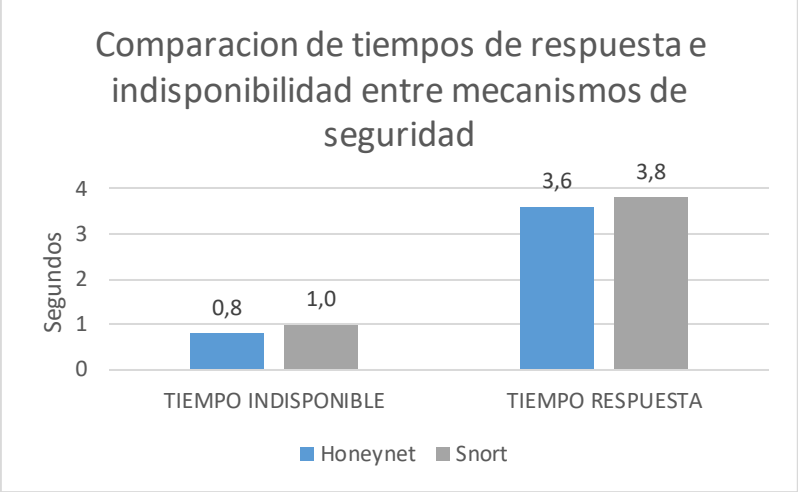
Gráfica 12. *Promedios de tiempo de indisponibilidad del servidor base de datos y del tiempo de respuesta de ambos mecanismos*

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

El servidor base de datos no queda indisponible durante el ataque Exploración de vulnerabilidades, ya que dicho ataque es pasivo.

El tiempo de respuesta del mecanismo Honeynet es de 5 segundos, mientras que el mecanismo Snort es de 4 segundos iniciada la prueba, esto significa que el mecanismo Snort tiene una ventaja de 1 segundo al momento de reaccionar.

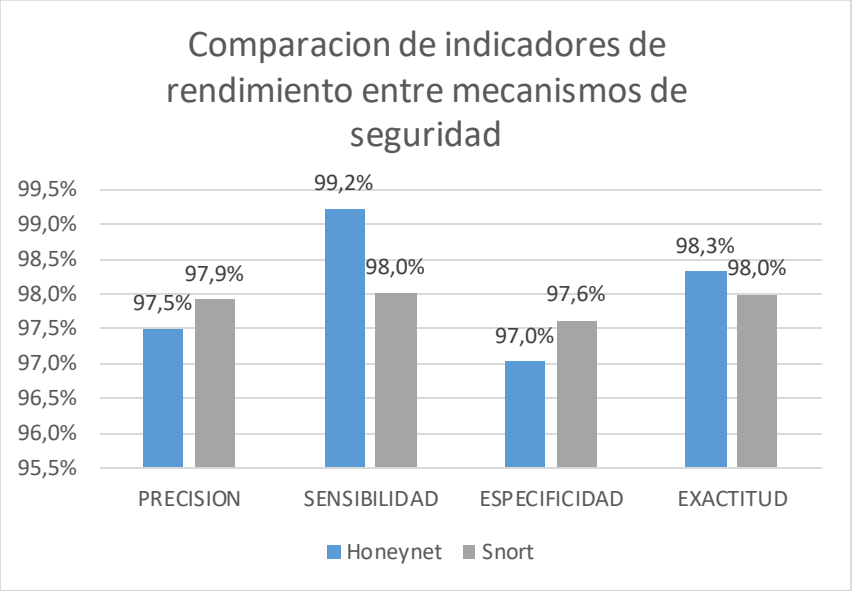
4.2.1. Resultados de los mecanismos con sus respectivos indicadores



Gráfica 13. Comparación de tiempos entre ambos mecanismos.

De acuerdo al promedio de tiempo indisponible de las 200 pruebas realizadas, se mostró como resultado que el mecanismo Honeynet mantiene el menor tiempo indisponible de los servidores frente al mecanismo Snort con una diferencia mínima de 0,2 segundos. Mientras que en el tiempo de respuesta el mecanismo Snort reaccionó a un promedio de 3,8 segundos, mientras que Honeynet reaccionó a los 3,6 segundos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe



Gráfica 14. Comparación de indicadores de rendimiento entre los mecanismos de seguridad.

De las 200 pruebas por cada mecanismo de seguridad, se obtuvo como resultados que el mecanismo Snort tiene una mayor precisión frente al mecanismo Honeynet, esto quiere decir que Snort tiene mayor grado de asertividad en la detección de ataques.

El mecanismo Honeynet obtuvo una ligera ventaja frente a Snort en el indicador de sensibilidad, eso quiere decir que Honeynet es 1,2% capaz de detectar los ataques que ingresan a la red. Mientras que Snort tiene una mayor capacidad de clasificar el tráfico normal.

Honeynet es el mecanismo que presenta la menor taza de error frente a la detección de ataques y tráfico normal de la red.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPITULO V: PROPUESTA DE LA INVESTIGACIÒN

La propuesta de la investigación tiene como objetivos analizar los mecanismos de seguridad que contrarresten los ataques informáticos detectados en servidores web y base de datos, para ello se identificó los diferentes ataques más frecuentes en los servidores, por medio de informes de entidades internacionales.

Así mismo en esta investigación se implementó una de red local que cuenta con un servidor web y un servidor de base de datos, utilizada para descubrir sus vulnerabilidades mediante los ataques seleccionados previamente. Posteriormente se realizó una previa recolección de información referente a los mecanismos de seguridad libres para su selección e implementación.

Se realizaron un total de 200 pruebas por cada mecanismo seleccionado para obtener bajo margen de error en los resultados de las pruebas y poder realizar su evaluación de acuerdo a los indicadores ya descritos, para comparar después ambos mecanismos.

El desarrollo de los objetivos alcanzados de esta investigación fue descrito detalladamente en los siguientes puntos:

5.1. Identificar los ataques informáticos con mayor impacto en los servidores

Según ESET Security Report 2016, se centra en conocer los principales ataques informáticos a empresas clasificadas por el tamaño, dando como resultado el top 11 de los ataques informáticos más frecuentes, dependiendo de las clasificaciones de pequeña, mediana y grande empresa, en la figura 13, se muestran estos ataques.

Incidentes de seguridad en empresas Latinoamericanas

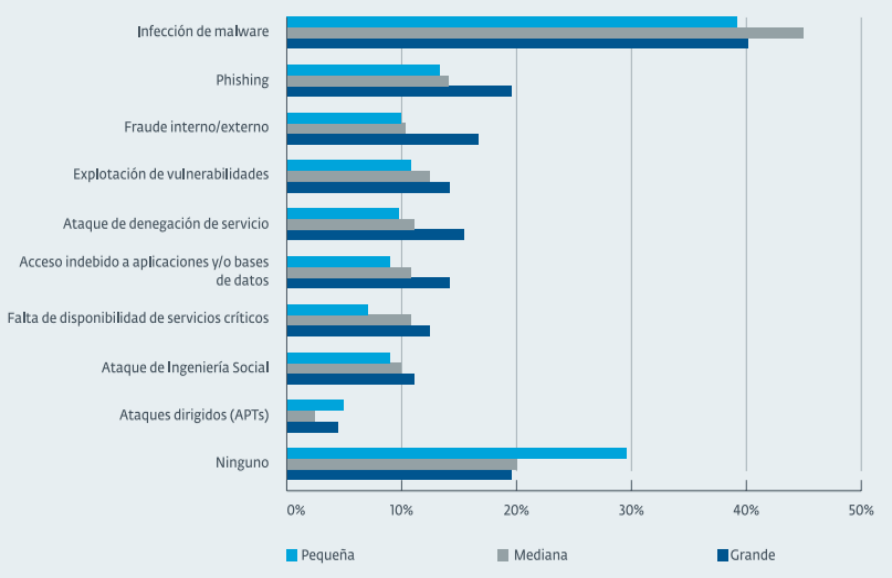


Figura 13. *Incidentes de Seguridad de la información en las empresas de Latinoamérica por tamaño de empresa.*
Fuente: ESET SECURITY REPORT LATAM (2016)

De acuerdo las fuentes verificadas la selección de ataques que se utilizaron fue por conveniencia, siendo estos, exploración de vulnerabilidades y ataques de denegación de servicio. Las cuales se especifican en las limitaciones de la investigación.

5.2. Seleccionar los mecanismos de seguridad informática

De acuerdo a los mecanismos de seguridad encontrados, solo dos fueron seleccionados para este trabajo de investigación, para que posteriormente sean implementados de acuerdo a la red establecida por los investigadores.

Honeynet

Según los autores (Dios, S. y Ortiz, P. 2014) realizaron una comparación de Honeynet, la cual la clasificaban según sus tres generaciones, donde se permitió apreciar las diferencias reflejadas entre las tres generaciones existentes, después del breve análisis, los autores llegan a la conclusión de que Honeynet de generación III cumple con los objetivos de control, captura y análisis de datos.

Comparación de generaciones de Honeynet

	Gen I	Gen II	Gen III
Control de Datos	Si	Si	Si
Captura de Datos	Si	Si	Si
Análisis de Datos	No	No	Si
Nivel de Operación	Capa de Red	Capa de Enlace	Capa Enlace
Detectable	Fácilmente	Dificilmente	Dificilmente
Información Cifrada	No Captura	Si Captura	Si Captura
Interfaz Web	No	No	Si
Informes Automatizados	No	No	Si

Figura 14. *Comparación de las tres generaciones de Honeynet.*
Fuente: "Diseño lógico y simulación de una red espejo virtual (HONEYNEY) para la detección de intrusos"

Los autores (Heredia, T. y Mauricio, C.) de acuerdo a los tipos de Honeynet virtuales existente, realizaron la comparación de estas Honeynet virtuales, explicando brevemente cada una de ellas y mostrando su respectivo esquema.

Tabla 25. Tipos de Honeynet Virtual

Tipos de Honeynet Virtual	
Honeynet Virtual Híbrida	**Honeynet Virtual Auto contenida**
Es aquella que se encarga de incorporar los sistemas reales y virtuales. Donde el honeywall logra efectuar el control, captura el análisis de datos en un sistema aislado, mientras que la virtualización de los honeypots se realiza en un solo equipo. Este tipo de solución aporta seguridad y flexibilidad.	Es aquella que emplea únicamente una máquina física para ejecutar toda la Honeynet. Donde se utiliza la virtualización para el ahorro de máquinas físicas y donde cada sistema operativo contenido dentro de ella actúa independientemente. Su mayor ventaja es el ahorro de costos al minimizar la inversión de recursos físicos.

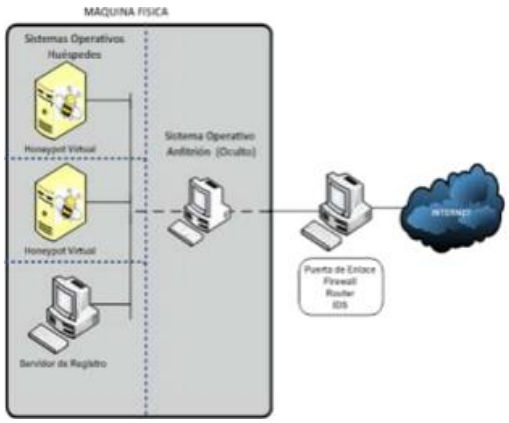


Figura 15. *Esquema de Honeynet Virtual Híbrida.*

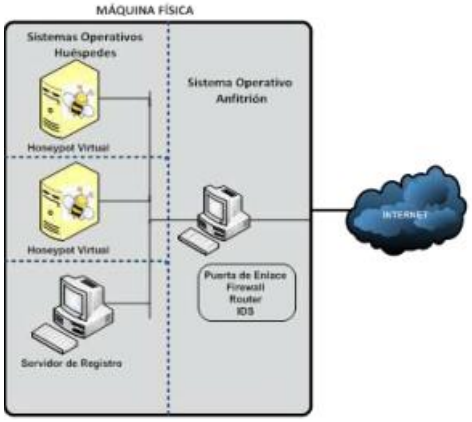


Figura 16. *Esquema de Honeynet Virtual Autocontenida.*

Fuente: Honeynet Virtual Híbrida en el entorno de red.

Posterior al análisis de la clasificación de Honeynet se seleccionó a Honeynet de generación III virtual autocontenida, porque a diferencia de las anteriores generaciones, esta logra permitir un buen análisis de datos y el ahorro de costos, con la virtualización de los sistemas operativos, en el momento de la simulación de la red de datos.

El segundo mecanismo de seguridad informática seleccionado fue:

Snort en Kali Linux

Los autores (Harpreet S. y Manpreet K. 2017) en su investigación afirmaron que Snort es de código libre y uno de los más antiguos, en la investigación argumentan que Snort es más rápido, ya que se puede ejecutar a velocidades de bit bit/s. Snort fue implementado en el Sistema operativo Linux.

Tabla 26. Modos existentes en Snort

MODOS DE SNORT	
Sniffer	**NIDS**
• Solo actúa como registro de paquetes. • Se aplica filtros para optimizar los resultados. • No es necesario un archivo de configuración.	• Analiza los paquetes enviados a los servidores. • Utiliza sus reglas para averiguar si hay alguna red. • Define un conjunto de reglas.

Fuente: Elaboración propia

La selección de Snort fue en modo NIDS, porque permite capturar, analizar y detectar los ataques que van dirigidos hacia los servidores, los cuales se encuentran en la red de dato.

Con la selección de los dos mecanismos de seguridad informática, se procedió a diseñar la red de datos donde se simularon ambos servidores, los cuales son servidor web y base de datos, cada uno de ellos con los mecanismos respectivos.

5.3. Diseño de la red de datos para la simulación

La presente investigación contó con el diseño de la red en el esquema físico y en el esquema lógico, la topología utilizada es estrella.

Esquema físico

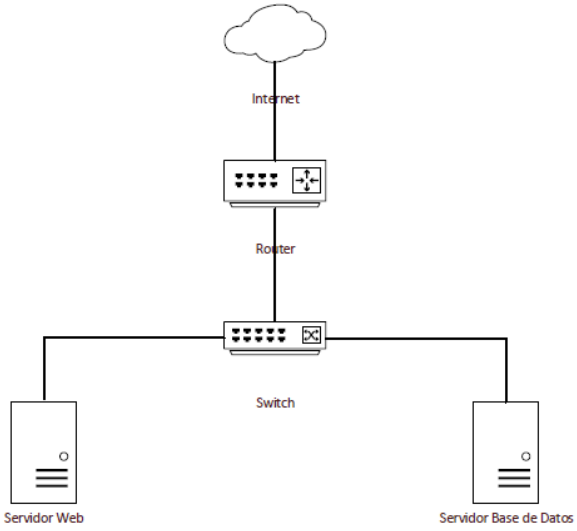


Figura 17. *Esquema físico de la red establecida.*
Fuente: Elaboración propia

Esquema lógico

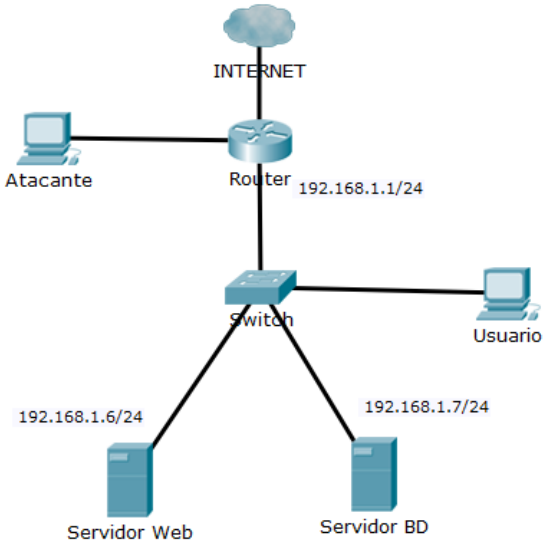


Figura 18. *Esquema lógico de la red establecida.*
Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

En la siguiente tabla se muestra las direcciones lógicas de la red 192.168.1.0/24

Tabla 27. Direcciones lógicas de la red establecida.

TABLA DE DIRECCIONES LÓGICAS	
	IP
Router	192.168.1.1
Broadcast	192.168.1.255
Gateway	192.168.1.1
DNS	192.168.1.3
Servidor web	192.168.1.6
Servidor base de datos	192.168.1.7
Pc atacante	192.168.1.71

Fuente: Elaboración propia

5.3.1. Instalación de servidor web y servidor base de datos

(Jimeno et. al, 2011) afirma que hoy en día al hablar de servidores, primero se piensa en aquellos servidores base de datos y servidores web, son los más utilizados, y estos son los que cuentan con gran capacidad de almacenamiento, que pueden tolerar con un número increíble de conexiones concurrentes.

La investigación, estará conformada por servidores Base de Datos, entre ellos tenemos los más utilizados.

Tabla 28. Servidores base de datos más utilizados - 2015

Servidores Base de datos	MySql
	PostgreSql
	Microsft SQL Server
	Oracle
	Microsft Access

Fuente: Netcraft.

En la figura 19 se muestra las estadísticas de los servidores web más utilizados en los años anteriores, también el porcentaje de los servidores en el mes de Enero y Febrero del año 2017

Servidores web más utilizados - 2016

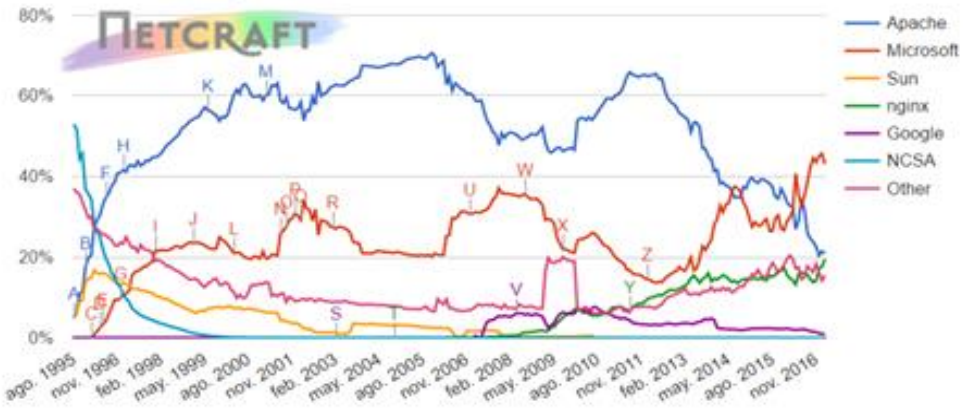


Figura 19. *Estadística de servidores web más utilizados en el año 2016.*
Fuente: Netcraft

Servidores más utilizados en enero y febrero 2017

Developer	January 2017	Percent	February 2017	Percent	Change
Microsoft	821,905,283	45,66%	773,552,454	43,16%	-2,50
Apache	387,211,503	21,51%	374,297,080	20,89%	-0,63
nglnx	317,398,317	17,63%	348,025,788	19,42%	1,79
Google	17,933,762	1,00%	18,438,702	1,03%	0,03

Figura 20. *Porcentajes del servidor más utilizado en los meses enero y febrero – 2017.*
Fuente: Netcraft.

Los reportes de Netcraft, sirvieron como referencia para la selección de los servidores por conveniencia de los investigadores, puesto que son los más utilizados actualmente.

Tabla 29. Servidores web y Base de datos seleccionados.

SERVIDORES WEB	Apache
SERVIDORES DE BASE DE DATOS	MySQL

Fuente: Elaboración propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

De acuerdo a los servidores seleccionados. Para la instalación de los dos servidores se utilizó el software de virtualización VirtualBox, el cual facilitó la creación y configuración de máquinas virtuales necesarias y concordes a la red definida.

Tabla 30. Especificaciones técnicas de VirtualBox

ESPECIFICACIONES TECNICAS SOFTWARE DE VIRTUALIZACIÓN	
Procesador	Core i7
Memoria RAM	16GB DDR4
Disco duro	1TB
Tarjeta de red	Intel PRO/100 MT Desktop
Software	Virtual Box (64-bit)

Fuente: Elaboración propia

Tabla 31. Especificaciones técnicas del servidor web

ESPECIFICACIONES TECNICAS SERVIDOR WEB	
Procesador	Core i7
Memoria RAM	3GB DDR4
Disco duro	21GB
Tarjeta de red	Intel PRO/100 MT Desktop
Sistema Operativo	Ubuntu server 16.04 LTS (64-bit)

Fuente: Elaboración propia

Tabla 32. Especificaciones técnicas del servidor base de datos

ESPECIFICACIONES TECNICAS SERVIDOR BASE DE DATOS	
Procesador	Core i7
Memoria RAM	1GB DDR4
Disco duro	20GB
Tarjeta de red	Intel PRO/100 MT Desktop
Sistema Operativo	Windows 7 (64-bit)

Fuente: Elaboración propia

En la figura 21 se muestra la máquina virtual del servidor web, en Ubuntu Server y el servidor base de datos en Windows 7. *(ANEXO II)*

Servidor web y base de datos

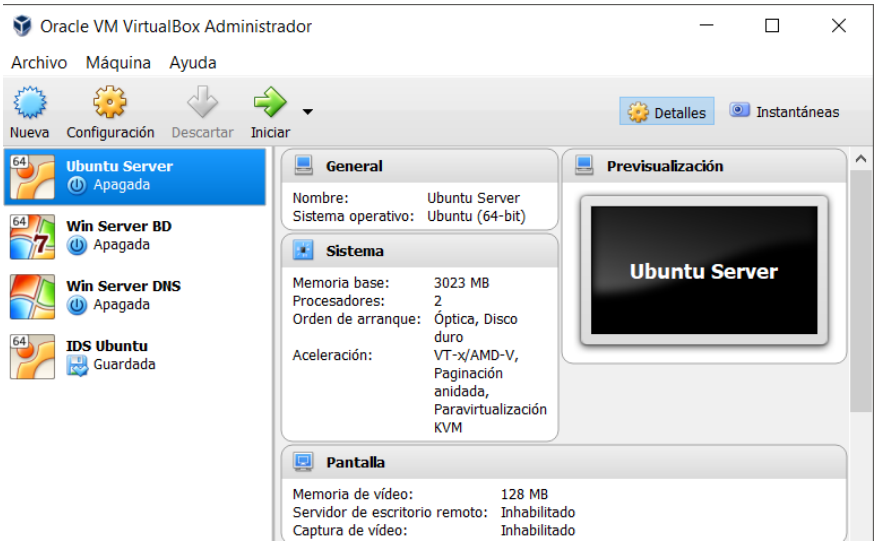


Figura 21. *Servidor web y base de datos instalado.*
Fuente: Elaboración propia

5.3.2. Instalación de maquina atacante

Se instaló una máquina virtual Kali Linux (64 bits), está maquina es utilizada para realizar los tipos de ataques identificados y seleccionados anteriormente. *(ANEXO V)*

Para la instalación de esta máquina se tuvieron en cuenta ciertas especificaciones técnicas mostradas en la siguiente tabla:

Tabla 33. Especificaciones técnicas de la PC atacante

ESPECIFICACIONES TECNICAS MAQUINA ATACANTE	
Procesador	Core i5
Memoria RAM	1GB DDR4
Disco duro	20GB
Tarjeta de red	Intel PRO/100 MT Desktop
Sistema Operativo	Kali (64-bit)

Fuente: Elaboración propia

5.3.3. Ejecución de ataques

Ataques DoS

Los ataques de Denegación de servicio atacan directamente al puerto especificado, enviando peticiones al mismo. El ataque se realizó por Slowloris, una herramienta compilada de kali desarrollada en el lenguaje de perl.

Ataque a servidor base de datos sin mecanismo de seguridad

Se realizó el ataque de DoS al servidor base de datos, ip es 192.168.1.7 y puerto 8080. Mediante el siguiente comando:

#cd Escritorio
#perl ./slowloris.pl –dns [ip] –port [puerto]

Al recargar la página se verificó que el servidor colapsó por el número de peticiones enviadas y no se logró tener acceso. Se utilizó wireshark para realizar la capturar el tráfico generado en la red local durante el ataque, se muestra todos paquetes infectados.

Tráfico de servidor base de datos

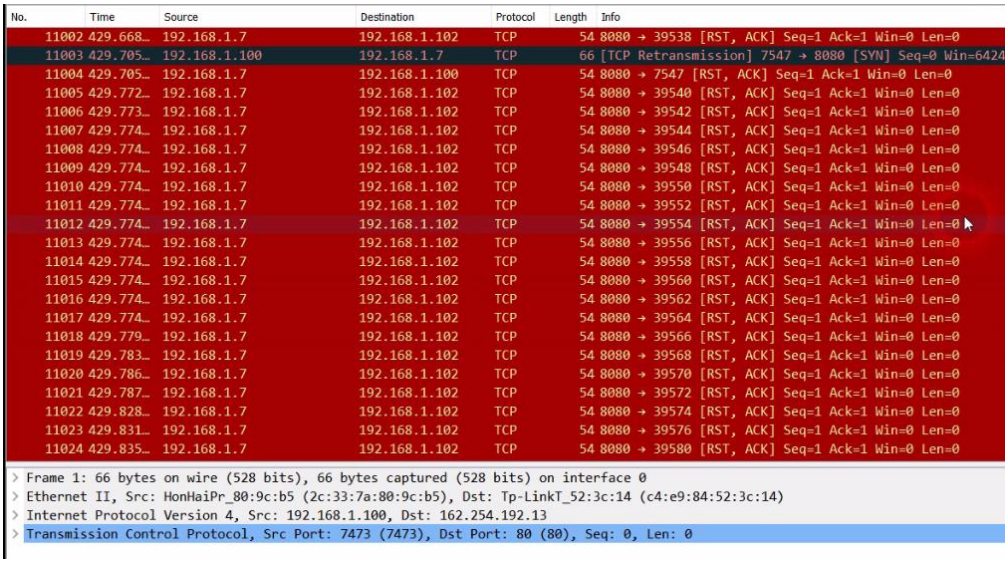


Figura 22. *Peticiones enviadas directamente al servidor y a su puerto.*
Fuente: Elaboración propia

Ataque a servidor web sin mecanismo de seguridad

Se realizó el ataque de DoS al servidor web, ip es 192.168.1.8 y puerto 80. Mediante el siguiente comando:

#perl ./slowloris.pl –dns 192.168.1.8 -port

Después de ejecutado el comando, el ataque ha iniciado enviando las peticiones al puerto de destino.

Ejecución de ataque DoS

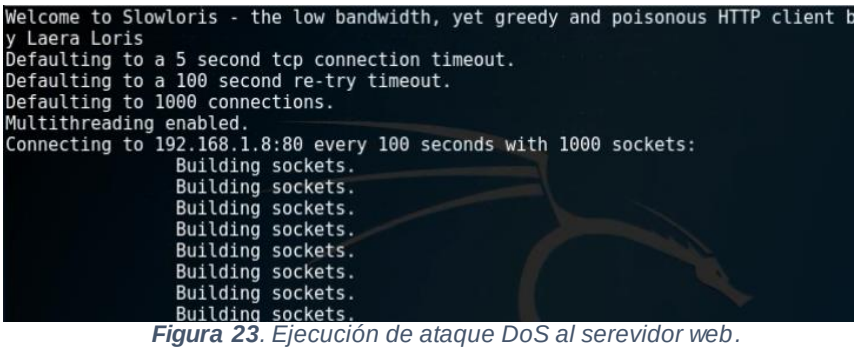


***Figura 23**. Ejecución de ataque DoS al serevidor web.*
Fuente: Elaboración propia

Al recargar la página web se verificó que el servidor colapsó por el número de peticiones enviadas y no se logró ingresar. Se utilizó wireshark para realizar el capturar el tráfico generado en la red local durante el ataque, se muestra todos paquetes infectados.

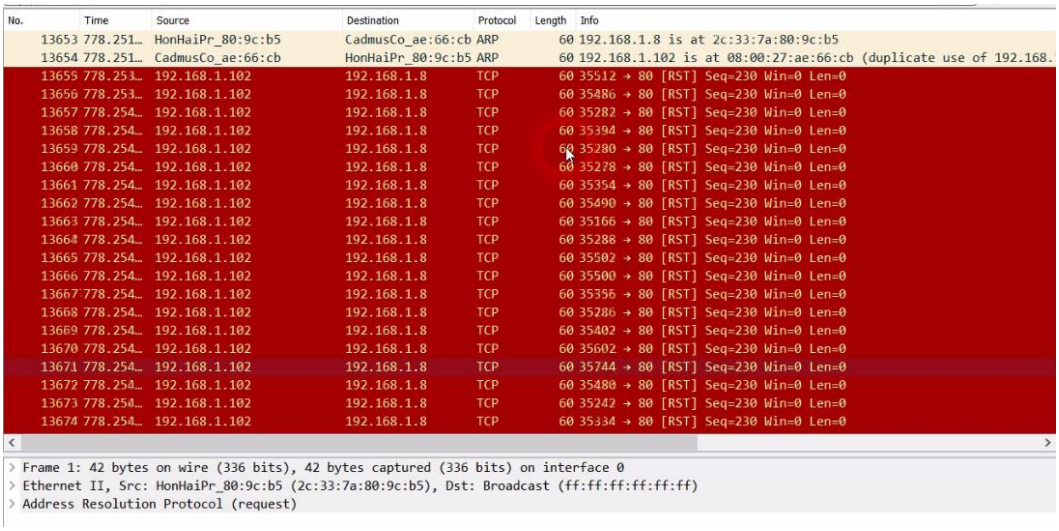


***Figura 24**. Peticiones enviadas directamente al servidor web y a su puerto.*
Fuente: Elaboración propia

Ataque de exploración de vulnerabilidades a la red

Este ataque realiza el escaneo de la red, así como de los servidores para encontrar los puertos que están habilitados y cuál de ellos es vulnerable. Se realiza por la herramienta *nmap* en Kali**.**

Tabla 34. Comandos de exploración de vulnerabilidades

COMANDO	FUNCIÓN
nmap –sV	Se encarga de verificar y mostrar las versiones de los puertos.
nmap –O	Permite visualizar el sistema operativo de la víctima o de la red.
nmap –n –Pn [ip] –p- --script=vuln	Permite visualizar todas las vulnerabilidades y los puertos que se encuentran abiertos.

Fuente: Elaboración propia.

El siguiente comando acompañado de la ip, realiza un escaneo de toda la red local, mostrando como resultados todos los puertos.

 # nmap 192.168.1.0/24

Ataque al servidor base de datos

El al ejecutar el comando *nmap [ip del servidor],* en este caso sería *nmap 192.168.1.7* muestra los puertos que están habilitados del servidor.

Ataque Exploración de vulnerabilidades

Figura 25. *Ataque de exploración de vulnerabilidades.*
Fuente: Elaboración propia

El comando *nmap –sV [ip],* se encarga de verificar y mostrar las versiones de los puertos. En la figura se observa alguno de ellos.

Ataque para verificar puertos

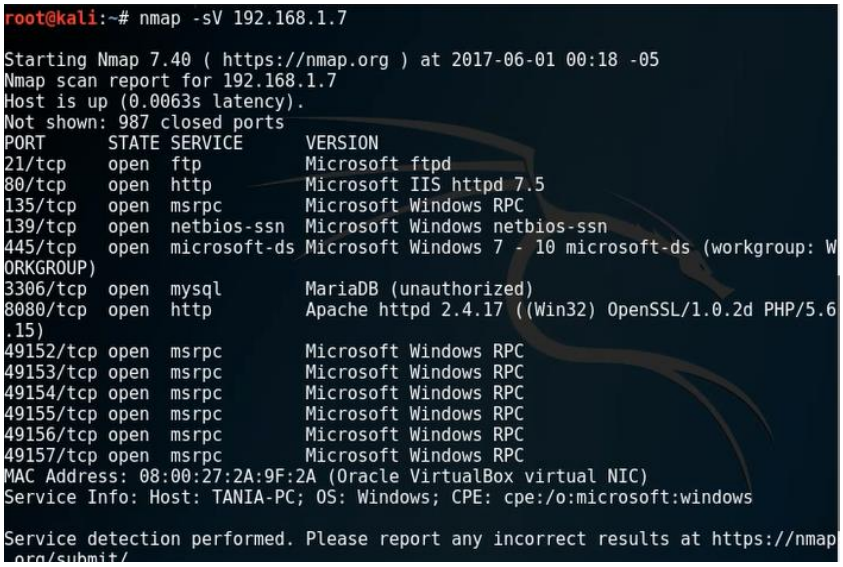


Figura 26. *Ataque de exploración de vulnerabilidades para verificar sus puertos. Fuente: Elaboración propia*

El comando *nmap –O [ip],* muestra todos los sistemas operativos (SO) que posee el servidor.

Ataque de exploración de vulnerabilidades

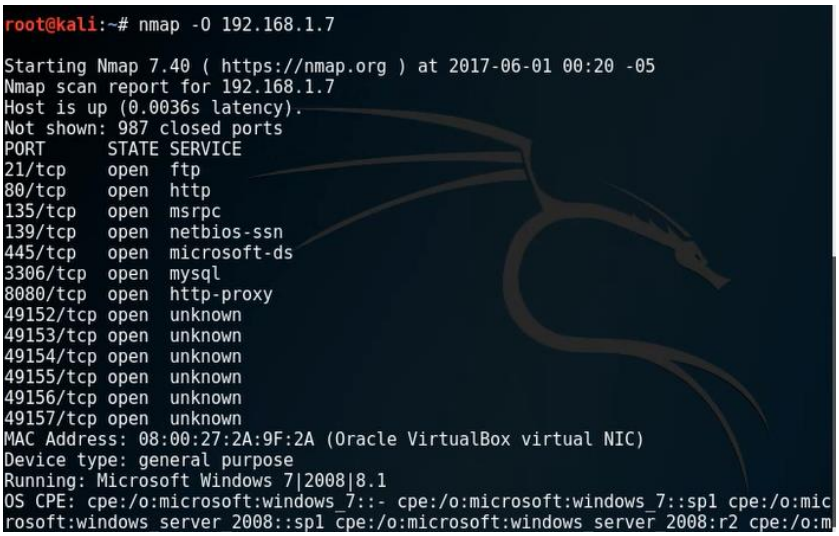


Figura 27. *Ataque de Exploración de vulnerabilidades, donde muestra los sistemas operativos. Fuente: Elaboración propia*

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

El comando *nmap –n –Pn [ip],* permite visualizar todas las vulnerabilidades encontradas y los puertos por los cuales se pueden ingresar.

Ataque de exploración de vulnerabilidades

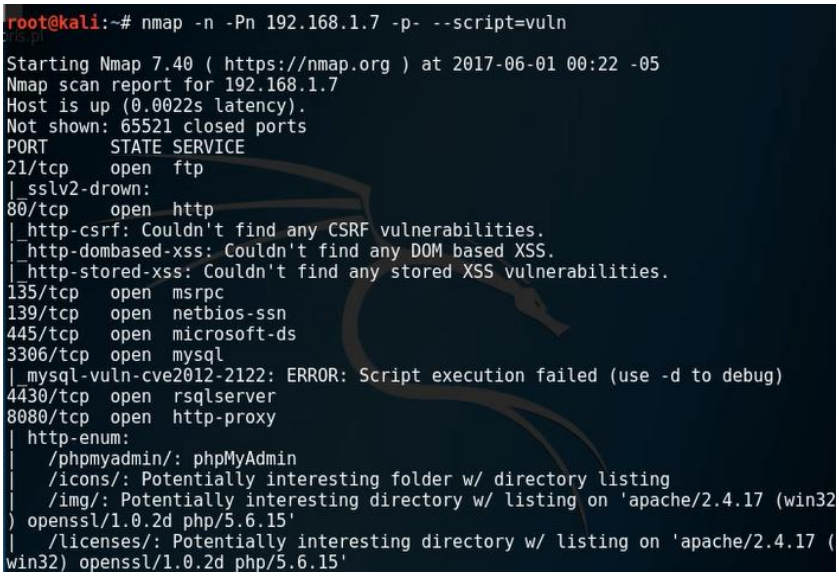


Figura 28. *Ataque de Exploración de vulnerabilidades para visualizar a los puertos vulnerables.*
Fuente: Elaboración propia

Ataque al servidor web

El al ejecutar el comando *nmap [ip del servidor],* en este caso sería *nmap 192.168.1.7* muestra los puertos que están habilitados del servidor

Ataque de Exploración de vulnerabilidades

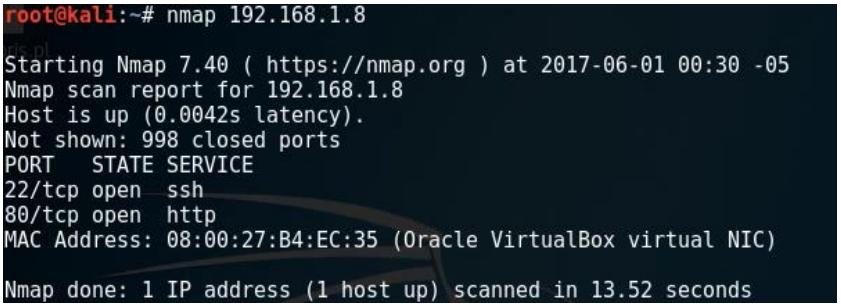


Figura 29*. Implementación de ataque exploración de vulnerabilidades, para mostrar el servidor.*
Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

El comando *nmap –sV [ip],* se encarga de verificar y mostrar las versiones de los puertos. En la figura se observa alguno de ellos.

Ataque de expresión de vulnerabilidad

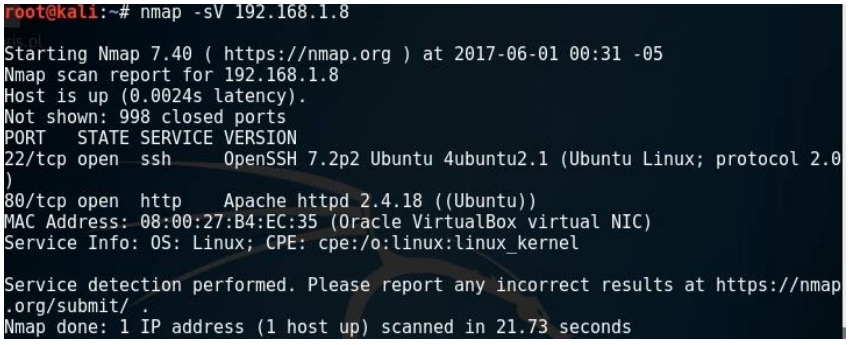


Figura 30. *Ataque de exploración de vulnerabilidades y mostrar las versiones de los puertos.*
Fuente: Elaboración propia

El comando *nmap –O [ip],* muestra todos los sistemas operativos (SO) que posee el servidor.

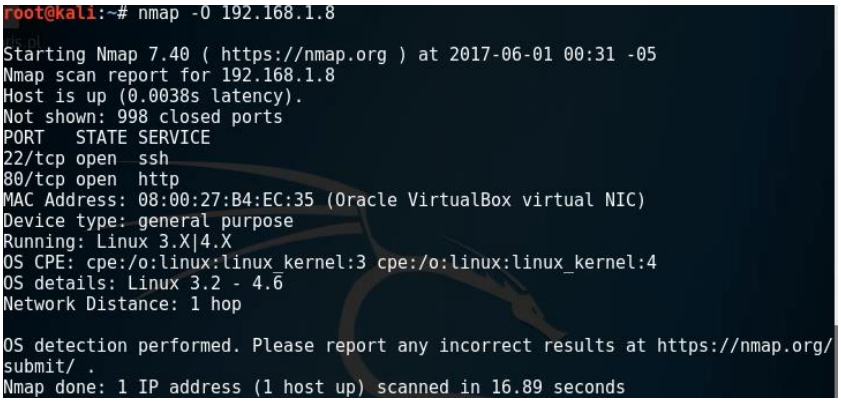


Figura 31. *Ataque de exploración de vulnerabilidades, para ver los sistemas operativos instalados.*
Fuente: Elaboración

El comando *nmap –n –Pn [ip],* permite visualizar todas las vulnerabilidades encontradas y los puertos por los cuales se pueden ingresar.

Ataque de exploración de vulnerabilidades

```
root@kali:~# nmap -n -Pn 192.168.1.8 -p- --script=vuln

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-01 00:32 -05
Nmap scan report for 192.168.1.8
Host is up (0.010s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.8
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.1.8/contact.html
|     Form id: submit
|     Form action: index.html
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubunt
u)'
|   /images/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ub
untu)'
|_  /js/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu
)'
```

Figura 32. *Ataque exploración de vulnerabilidades donde se muestran todos puertos vulnerables.*
Fuente: Elaboración propia

Se utilizó wireshark para realizar el capturar el tráfico generado en la red local durante el ataque, se muestra todos paquetes infectados

Tráfico de red local

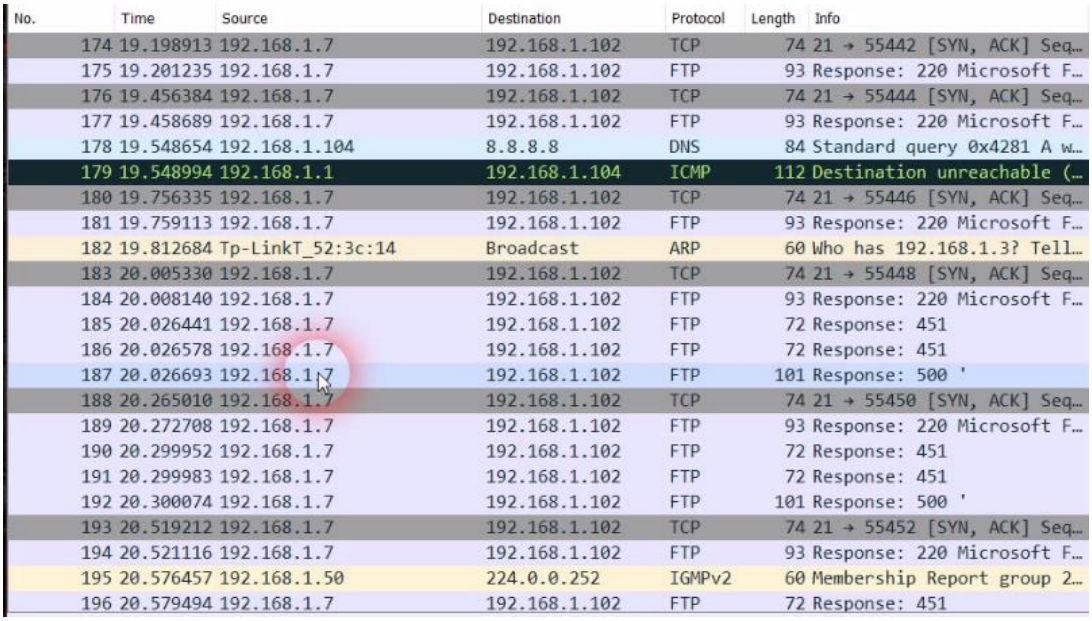
No.	Time	Source	Destination	Protocol	Length	Info
1711	36.238161	192.168.1.8	192.168.1.102	TCP	60	541 → 51446 [RST, ACK] Seq=
1712	36.238240	192.168.1.7	192.168.1.102	TCP	54	514 → 51446 [RST, ACK] Seq=
1713	36.238482	192.168.1.8	192.168.1.102	TCP	60	9666 → 51446 [RST, ACK] Seq
1714	36.240538	192.168.1.7	192.168.1.102	TCP	54	24444 → 51446 [RST, ACK] Se
1715	36.241394	192.168.1.7	192.168.1.102	TCP	54	6025 → 51446 [RST, ACK] Seq
1716	36.241468	192.168.1.8	192.168.1.102	TCP	60	1040 → 51446 [RST, ACK] Seq
1717	36.241499	192.168.1.8	192.168.1.102	TCP	60	3826 → 51446 [RST, ACK] Seq
1718	36.241513	192.168.1.8	192.168.1.102	TCP	60	55055 → 51446 [RST, ACK] Se
1719	36.241540	192.168.1.8	192.168.1.102	TCP	60	800 → 51446 [RST, ACK] Seq=
1720	36.241569	192.168.1.7	192.168.1.102	TCP	54	8649 → 51446 [RST, ACK] Seq
1721	36.241601	192.168.1.7	192.168.1.102	TCP	54	1031 → 51446 [RST, ACK] Seq
1722	36.242380	192.168.1.7	192.168.1.102	TCP	54	1096 → 51446 [RST, ACK] Seq
1723	36.242424	192.168.1.8	192.168.1.102	TCP	60	8300 → 51446 [RST, ACK] Seq
1724	36.242497	192.168.1.7	192.168.1.102	TCP	54	10628 → 51446 [RST, ACK] Se
1725	36.242578	192.168.1.8	192.168.1.102	TCP	60	9503 → 51446 [RST, ACK] Seq
1726	36.242625	192.168.1.7	192.168.1.102	TCP	54	1100 → 51446 [RST, ACK] Seq
1727	36.242701	192.168.1.8	192.168.1.102	TCP	60	6502 → 51446 [RST, ACK] Seq
1728	36.243381	192.168.1.7	192.168.1.102	TCP	54	1107 → 51446 [RST, ACK] Seq
1729	36.243442	192.168.1.8	192.168.1.102	TCP	60	9001 → 51446 [RST, ACK] Seq
1730	36.244368	192.168.1.8	192.168.1.102	TCP	60	6668 → 51446 [RST, ACK] Seq
1731	36.244421	192.168.1.7	192.168.1.102	TCP	54	1247 → 51446 [RST, ACK] Seq

Figura 33. *Análisis de tráfico generado de la red local.*
Fuente: Elaboración propia

La siguiente figura nos muestra el tráfico que fue capturado por wireshark, donde nos indica el ip destinatario, el protocolo a donde ingresaron los paquetes de tráfico.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tráfico de red local



No.	Time	Source	Destination	Protocol	Length	Info
174	19.198913	192.168.1.7	192.168.1.102	TCP	74	21 → 55442 [SYN, ACK] Seq…
175	19.201235	192.168.1.7	192.168.1.102	FTP	93	Response: 220 Microsoft F…
176	19.456384	192.168.1.7	192.168.1.102	TCP	74	21 → 55444 [SYN, ACK] Seq…
177	19.458689	192.168.1.7	192.168.1.102	FTP	93	Response: 220 Microsoft F…
178	19.548654	192.168.1.104	8.8.8.8	DNS	84	Standard query 0x4281 A w…
179	19.548994	192.168.1.1	192.168.1.104	ICMP	112	Destination unreachable (…
180	19.756335	192.168.1.7	192.168.1.102	TCP	74	21 → 55446 [SYN, ACK] Seq…
181	19.759113	192.168.1.7	192.168.1.102	FTP	93	Response: 220 Microsoft F…
182	19.812684	Tp-LinkT_52:3c:14	Broadcast	ARP	60	Who has 192.168.1.3? Tell…
183	20.005330	192.168.1.7	192.168.1.102	TCP	74	21 → 55448 [SYN, ACK] Seq…
184	20.008140	192.168.1.7	192.168.1.102	FTP	93	Response: 220 Microsoft F…
185	20.026441	192.168.1.7	192.168.1.102	FTP	72	Response: 451
186	20.026578	192.168.1.7	192.168.1.102	FTP	72	Response: 451
187	20.026693	192.168.1.7	192.168.1.102	FTP	101	Response: 500 '
188	20.265010	192.168.1.7	192.168.1.102	TCP	74	21 → 55450 [SYN, ACK] Seq…
189	20.272708	192.168.1.7	192.168.1.102	FTP	93	Response: 220 Microsoft F…
190	20.299952	192.168.1.7	192.168.1.102	FTP	72	Response: 451
191	20.299983	192.168.1.7	192.168.1.102	FTP	72	Response: 451
192	20.300074	192.168.1.7	192.168.1.102	FTP	101	Response: 500 '
193	20.519212	192.168.1.7	192.168.1.102	TCP	74	21 → 55452 [SYN, ACK] Seq…
194	20.521116	192.168.1.7	192.168.1.102	FTP	93	Response: 220 Microsoft F…
195	20.576457	192.168.1.50	224.0.0.252	IGMPv2	60	Membership Report group 2…
196	20.579494	192.168.1.7	192.168.1.102	FTP	72	Response: 451

Figura 34. *Análisis de tráfico generado de la red local establecida.*
Fuente Elaboración propia

Ya realizados los ataques se obtienen los siguientes resultados:

Tabla 35. Resultados de ataques realizados a la red sin mecanismo de seguridad.

SERVIDOR	ATAQUE	PAQUETES ENVIADOS	ATAQUE REALIZADO EFECTIVAMENTE
WEB	DoS	1948	SI
	Exploración de vulnerabilidades	1314	SI
Base de Datos	DoS	1824	SI
	Exploración de vulnerabilidades	1624	SI

Fuente: Elaboración propia

5.4. Implementar los mecanismos de seguridad informática que mitiguen a los ataques informáticos.

5.4.1. Implementación de mecanismo de seguridad Honeynet

El primer mecanismo de seguridad seleccionado es Honeynet. El diseño físico de la red se muestra en la siguiente figura:

Esquema lógico

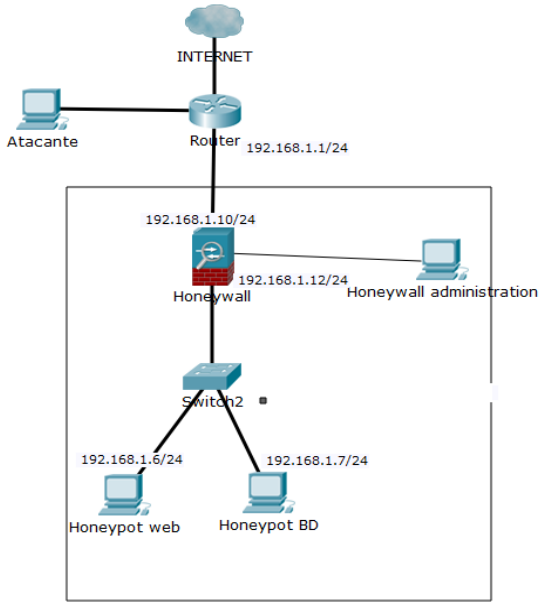


Figura 35. *Esquema lógico de Honeynet.*
Fuente: Elaboración propia

La tabla 36, muestra la configuración de las direcciones lógicas.

Tabla 36. Direcciones lógicas del Mecanismo Honeynet

TABLA DE DIRECCIONES LÓGICAS	
DISPOSITIVOS	**IP**
Router	192.168.1.1
Honeywall	192.168.1.10
Honeywall administration	192.168.1.12
Honeypot web	192.168.1.6
Honeypot base de datos	192.168.1.6

Fuente: Elaboración propia

Los requerimientos del ordenador que se utilizó para la implementación de Honeynet virtual auto-contenida tuvieron las siguientes características técnicas:

Tabla 37. Especificaciones Técnicas de componentes de Honeynet

HONEYNET	
Componentes	**Especificaciones técnicas**
VirtualBox versión 5.1.22	• Procesador Core i5 64-bits • Memoria RAM 6GB
Honeywall	• Procesador Core i5 64-bits • Memoria RAM 2GB • Disco duro 8GB • Memoria de video 16MB • Tres adaptadores de red Intel PRO/100 MT Desktop (bridge, host-only, bridge)
Honeypot (Windows 7)	• Procesador Core i5 64-bits • Memoria RAM 2GB • Disco duro 25GB • Memoria de video 43MB • Adaptador de red Intel PRO/100 MT Desktop
Honeypot (Windows xp)	• Procesador Core i5 64-bits • Memoria RAM 512MB • Disco duro 10GB • Memoria de video 16MB • Adaptador de red Intel PRO/100 MT Desktop

Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Uno de los componentes de Honeynet es Honeywall. En la instalación de la Honeywall Virtual, se lograron configurar tres adaptadores de red, dos en modo "Bridge" (puente) y una en modo "Host-only".

Tabla 38. Descripción de interfaces de Honeywall

INTERFACES DEL HONEYWALL	
Interface de Red 1 (Bridge)	El honeywall se comunicará con la red externa
Interface de Red 2 (Host-only)	El honeywall se comunicará con los honeypots.
Interface de Red 3 (Bridge)	Para la administración remota del honeywall (Walleyes).

Fuente: Elaboración propia

A través de VirtualBox se configuró tres redes virtuales que permitan la comunicación de la red local con la Honeynet.

Tabla 39. Detalle de interfaces y máquinas virtuales de Honeywall

Máquina virtual	**Interfaces**	**VirtualBox**	**Detalle**
Honeywall	eth0	bridge	Conecta el honeywall con la red
	eth1	host-only	Conecta el honeywall con los honeypot
	eth2	bridge	Permite la administración remota de honeywall (Walleyes)
Honeypot 1 (Win Server BD)	eth1	net	Conecta el honeypot con el honeywall
Honeypot 2 (Win xp web)	eth1	net	Conecta el honeypot con el honeywall

Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Iniciación de Honeynet Project, para la configuración de la red. *(ANEXO III)*

Instalación de Honeynet Project

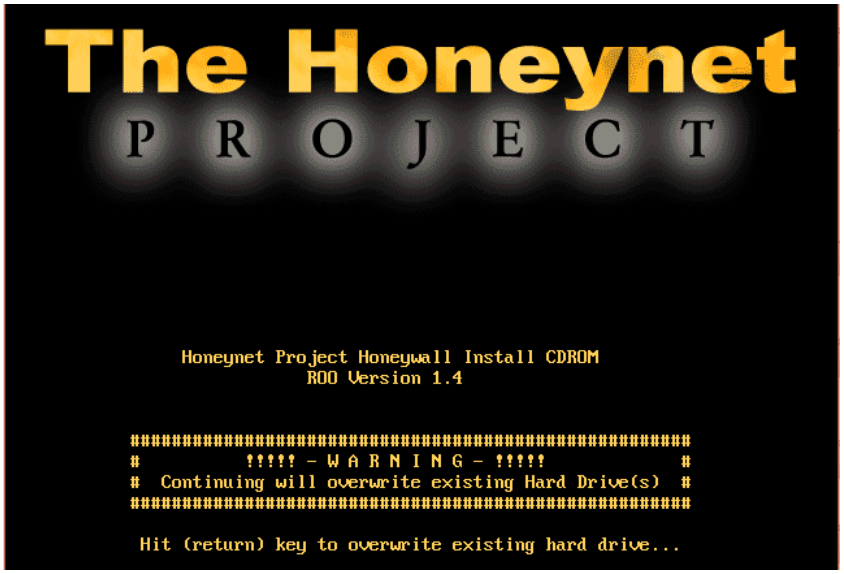


Figura 36. *Pantalla de inicio de Project Honeynet.*
Fuente: Elaboración propia

Configuración de ip pertenecientes a los honeypot definidos en la red.

Configuración de Ip de Honeypots

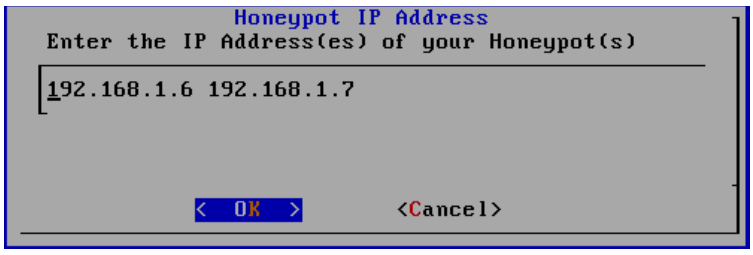


Figura 37. *Pantalla de configuración de Honeypots en Project Honeynet.*
Fuente: Elaboración propia

Instalación de Honeypots

Se seleccionó el proyecto Valhala Honeypot 1.9 para Windows cuenta con interfaz gráfica, es un honeypot de baja interacción, se logra aumentar su interacción con la conexión realizada al Honeywall. Cuenta con dos honeypot, uno de ellos simula el servidor web y el otro el servidor base de datos con sus respectivos servicios.

Honeypot web con ip 192.168.1.6

Interfaz gráfica de honeypot web

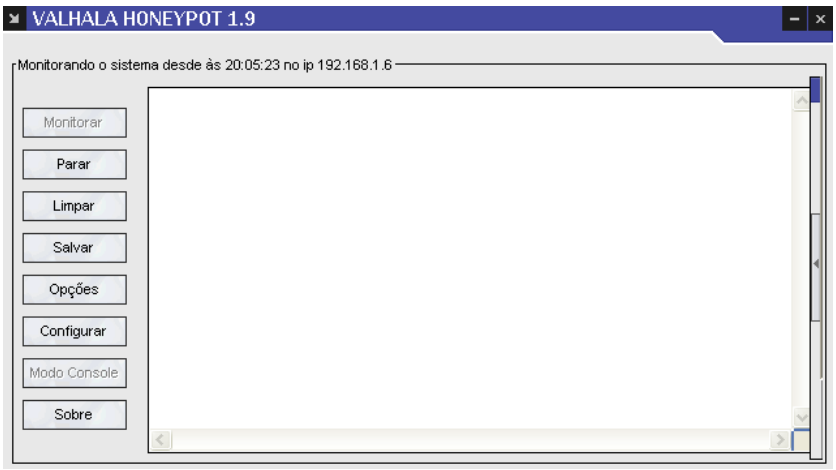


Figura 38. *Valhala, interfaz de honeypot web que simula el servidor web.*
Fuente: Elaboración propia

Se procedió a configurar los servicios WEB, FTP, SMTP, para la realización de pruebas.

Servicios de Honeypot

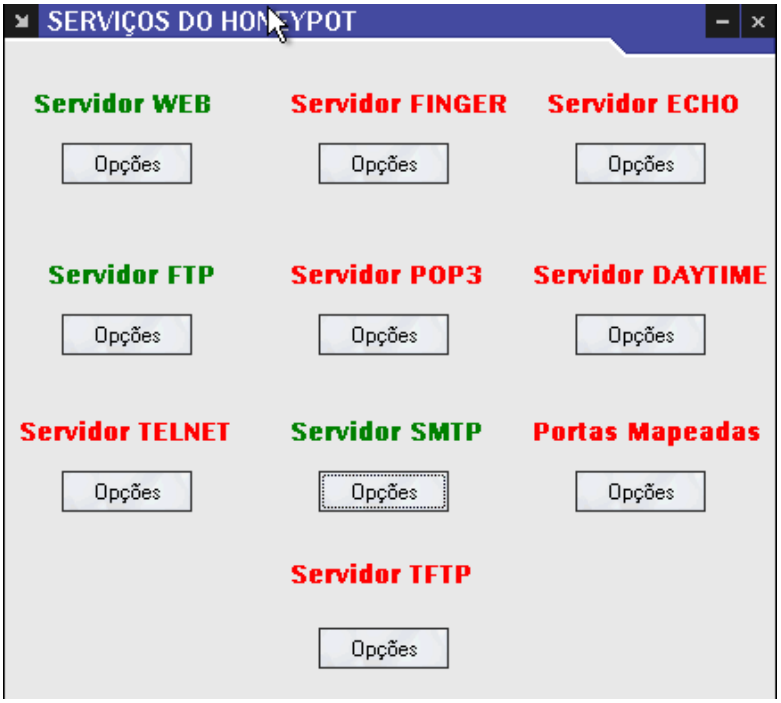


Figura 39. *Servicios Honeypot en Valhala.*
Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Honeypot base de datos ip 192.168.1.7

Interfaz gráfica de Honeypot base de datos

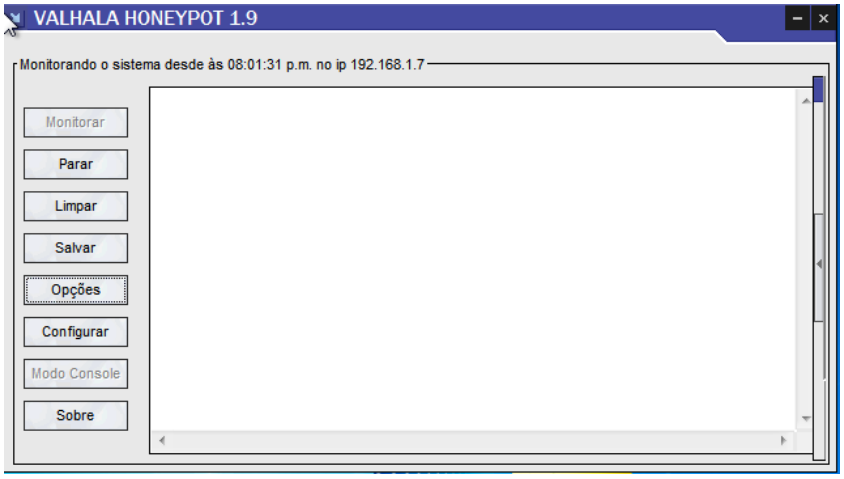


Figura 40. *Valhala, interfaz de honeypot base de datos que simula el servidor web.*
Fuente: Elaboración propia

El honeypot que simula al servidor base de datos no cuenta con los servicios activados de Valhala, pero si cuenta con el servidor MySql. Seguidamente se verificó la correcta conexión de los honeypot.

Conexión de Honeypots con máquina externa

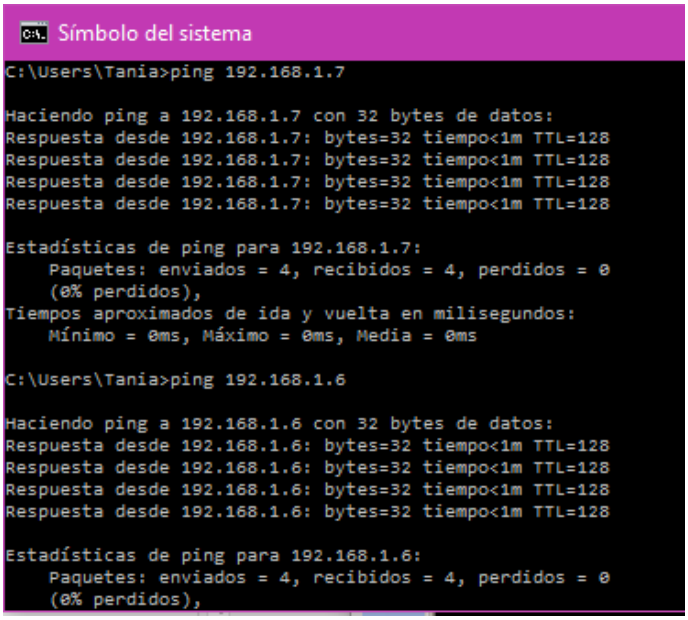


Figura 41. *Conexión entre la máquina externa y los Honeypots.*
Fuente: Elaboración propia

SERVIDOR WEB

Ataques DoS

Se realizaron los ataques de Denegación de Servicio al mecanismo Honeynet que simula el servidor web, se muestra algunos de los resultados de las pruebas realizadas.

Registro de ataques en Honeywall

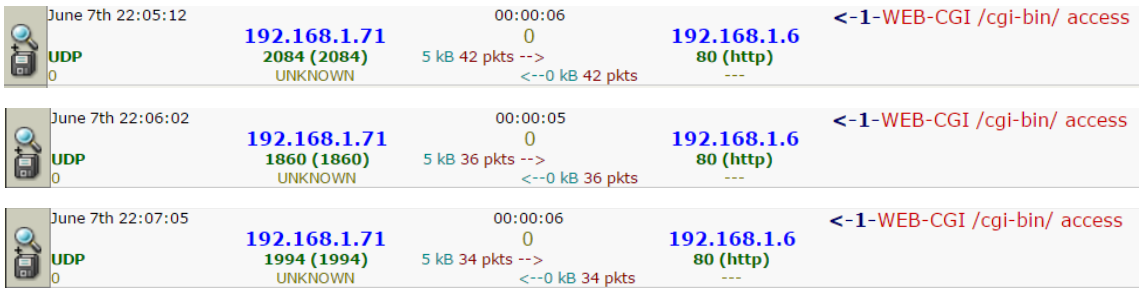


Figura 42. *Resultados de pruebas en Honeywall, servidor web.*
Fuente: Elaboración propia

Exploración de vulnerabilidades

Se realizaron los ataques de Exploración de vulnerabilidades al mecanismo Honeynet que simula el servidor web.

SERVIDOR BASE DE DATOS

Ataque DoS

La administración de Honeywall muestra los ataques con los paquetes que llegaron al servidor.

Registro de ataques en Honeywall

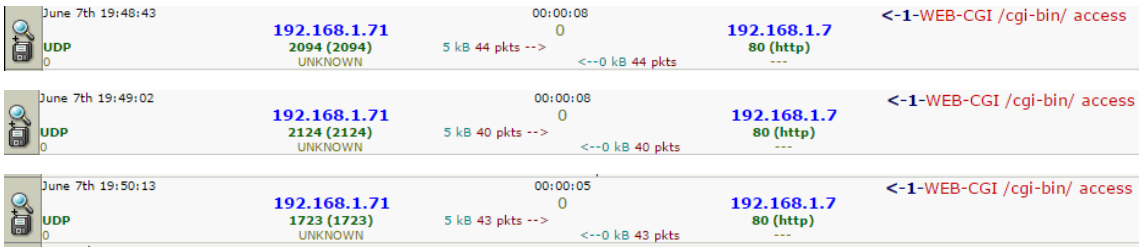


Figura 43. *Resultados de pruebas en Honeywall, servidor web.*
Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5.4.2. Implementación de mecanismo de seguridad Snort

El segundo mecanismo de seguridad seleccionado es Snort. El diseño físico de la red se muestra en la siguiente figura:

Esquema lógico

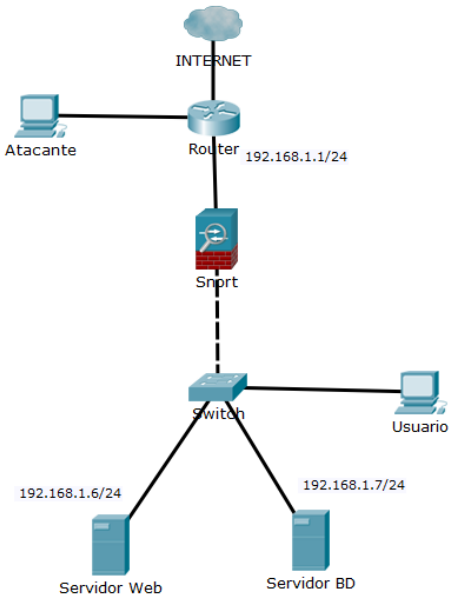


Figura 44. *Esquema lógico de Snort*

La siguiente tabla cuenta con la configuración de las direcciones lógicas en los diferentes dispositivos de la red.

Tabla 40. Direcciones lógicas de Snort

TABLA DE DIRECCIONES LÓGICAS	
DISPOSITIVOS	**IP**
Router	192.168.1.1
Servidor web	192.168.1.6
Servidor base de datos	192.168.1.7
Snor	192.168.1.10

Fuente: Elaboración propia

Los requerimientos del ordenador utilizado para la implementación de Honeynet virtual auto-contenida tienen las siguientes características técnicas:

Tabla 41. Especificaciones técnicas de componentes de Snort

SNORT	
Componentes	**Especificaciones técnicas**
VirtualBox versión 5.1.22	• Procesador Core i7 64-bits • Memoria RAM 16GB
Snort (Kali Linux)	• Procesador Core i7 64-bits • Memoria RAM 2GB • Disco duro 15GB • Memoria de video 36MB • Tres adaptadores de red Intel PRO/100 MT Desktop (bridge, bridge)

Fuente: Elaboración propia

En la instalación de Snort, se configuran 2 adaptadores de red, ambos en modo “Bridge”.

Tabla 42. Interfaces que conforman Snort

INTERFACES DE SNORT	
Interface de Red 1 (Bridge)	El snort se comunicará con el Router.
Interface de Red 2 (Bridge)	Para la comunicación con los servidores.

Fuente: Elaboración propia

Configuración de Snort

Configuración de la red e ips de servidores a Snort *(ANEXO IV)*

Configuración de la red para Snort

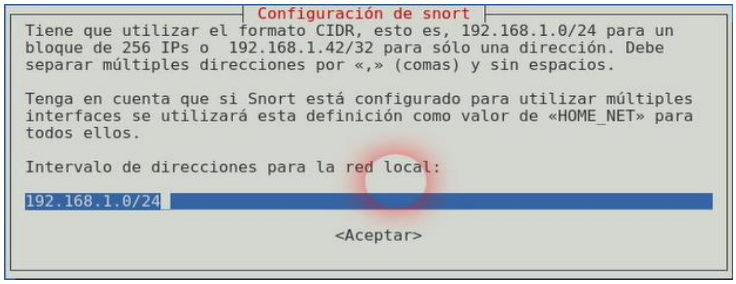


Figura 45. *Configuración de la red correspondiente para que funcione Snort.*
Fuente: Elaboración propia

Comprobación de instalación de snort.

Comprobación de instalación de Snort

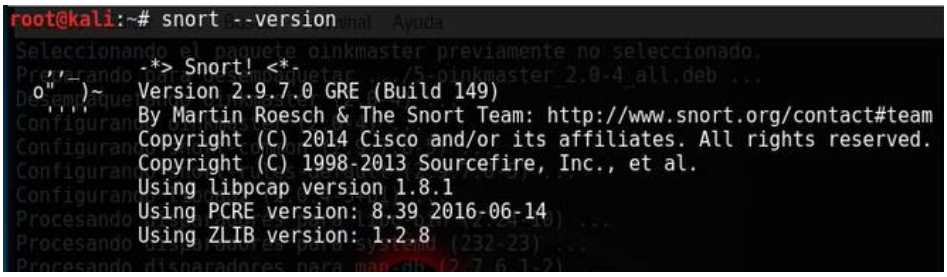


Figura 46. *Versión de Snort y la comprobación de instalación.*
Fuente: Elaboración propia

Para la realización de pruebas, se basó en el trabajo de investigación del autor De la Hoz Correa (2016) titulado *"Mapas auto-organizativos probabilísticos y análisis en componentes de conexiones para la detección de anomalías en redes de computadores*" donde realizo 50 ejecuciones por cada característica.

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

Mediante las pruebas realizadas y el análisis de resultados, ambos mecanismos detectaron y lograron contrarrestar los ataques DoS y exploración de vulnerabilidades en servidores web y base de datos.

Los resultados obtenidos en el indicador rendimiento y tiempo de respuesta en ambos mecanismos tienen una mínima diferencia.

El mecanismo de seguridad Snort en Kali Linux, llegó a ser más preciso al momento de detectar el tráfico malicioso y el tráfico normal, refiriéndose a la especificidad. Mientras que el mecanismo de seguridad Honeynet obtuvo mayor porcentaje de exactitud y capacidad en la clasificación del trafico normal (sensibilidad).

En el indicador de tiempo de respuesta de los mecanismos de seguridad informática, se obtuvo una diferencia de 0.25 segundos, siendo mínima y no afectando en mayor medida a los servidores.

Con el debido conocimiento y estudio, las herramientas que se utilizaron para la implementación de los mecanismos de seguridad son relativamente factibles y rápidas de configurar, su administración se vuelve más sencilla a través de diferentes módulos que disponen de interfaz gráfica.

6.2. Recomendaciones

Se recomienda realizar todos backups posibles de los servidores de la red, donde operan los mecanismos, con el fin de que la información no sufra daños.

El mecanismo de seguridad Honeynet tienen integrado un sistema de envío de logs, el cual funciona en el mismo equipo físico, se recomienda trabajar con el sistema de logs fuera del mecanismo para proteger la integridad de los datos y los servicios comprometidos, sin que la confiabilidad de los datos se vea afectada.

Ya que muchas arquitecturas integran a Snort como mecanismo de seguridad, se recomienda realizar una comparación para conocer el rendimiento frente a los ataques relacionados.

El mecanismo de seguridad Honeynet de generación III virtual autocontenida, captura y almacena gran cantidad de información, por lo que se recomienda contar con un equipo de alta capacidad en memoria y procesamiento, capaz de soportar la implementación de dicho mecanismo de seguridad.

Los datos generados por mecanismos implementados pueden ser analizados mediante un análisis forense digital para conocer las tácticas más utilizadas por los atacantes y determinar los diferentes patrones de comportamiento de ataques que utilizan para implicar los sistemas.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

REFERENCIAS

Aguilera, L. P. (2010). Libro: Seguridad informática. Editorial. Editex. Consultado en: https://books.google.com.pe/books?id=Mgvm3AYIT64C&printsec=frontcover&dq=seguridad+informatica,+aguilera&hl=es&sa=X&ved=0ahUKEwjwqczG2pjUAhWBSiYKHUfpBB0Q6AEIlDAA#v=onepage&q=seguridad%20informatica%2C%20aguilera&f=false

Alegre, R.M. y García-Cervigón, A. (2011). Sistemas microinformáticos y redes. Seguridad informática. (Edición 11). Editorial: Paraninfo. Consultado en: https://books.google.com.pe/books?id=c8kni5g2Yv8C&pg=PA10&dq=objetivos+de+seguridad+informatica&hl=es&sa=X&ved=0ahUKEwjszNvL1pjUAhWI2yYKHREFCFYQ6AEIJDAB#v=onepage&q=objetivos%20de%20seguridad%20informatica&f=false

Almonin, A. A. (2015). *Detection of unknown vulnerabilities using Honeynet.* IEEE Anti-Cybercrime (ICACC), 2015 First International Conference. Sudan. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7351929&queryText=honeynet&ranges=2012_2015_Year

Arboleda A. y Bedón C. (2005). *SnortTM diagrams for developers.* Se encuentra en: http://afrodita.unicauca.edu.co/~cbedon/snort/snort.html

Arce, M. E. (2014). Ciencia y Tecnología. http://www.emol.com/noticias/tecnologia/2014/08/06/673702/los-ataques-ciberneticos-cada-vez-mas-complejos-y-dificiles-de-detectar.html

Areitio B. J. (2008). *SEGURIDAD DE LA INFORMACIÓN*. *Redes, informática y sistemas de información.* Editorial: Paraninfo. p. 31, 34.

Bejtlich R. (2005) *El tao de la monitorización de seguridad en redes.* Editorial: Person Prentice Hall. España. p. 147

Berenguela & Cortes (2006) *Metodología de Medición de Vulnerabilidades en Redes de Datos de Organizaciones*. (Tesis de grado) Instituto Profesional INACAP La Serena, Chile. Seguridad de la Informática

Cantos, K. y Carangui, K. (2007). Análisis del sistema de seguridad en servidores Web para su correcta utilización (Tesis de grado)

Carpi, A., & Anne E., E. (2008). Visionleraning. Obtenido de Comparación en la Investigacion Científica: http://www.visionlearning.com/es/library/Proceso-de-la-Ciencia/49/Comparaci%C3%B3n-en-la-Investigacion-Cient%C3%ADfica/152

Christos Douligeris, Aikaterini Mitrokotsa (2003). DDoS attacks and defense mechanisms: classification and state-of-the-art Departamento de Informática de la Universidad de Pireo, 80 Karaoli y Dimitriou Str, Pireo 18534, Grecia

Cook, T.D. y Campbell, D.T. (1986). The causal assumptions of quasiexperimental practice. Synthese, 68, 141-180.

Díaz, García, Muñoz, Maciá, & De Toro (2007). Una aproximación basada en Snort para el desarrollo e implantación de IDS híbridos. Journal IEEE Latin America Transactions, Vol. 5, No. 6.

Díaz O. G., Alzórriz A. I., Sancristóbal R. E. y Castro G. M., (2014) Procesos y Herramientas para la seguridad de redes. pag. 38. Encontrado en: https://books.google.com.pe/books?id=dG4lAwAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false

Dios, L. S. y Ortiz, P. D. (2014). Diseño lógico y simulación de una red espejo virtual (Honeynet) para la detección de intrusos informáticos en zona perimetral. Facultad de Ciencias Físicas y Matemáticas. Universidad Nacional de Trujillo, La Libertar, Perú.

De la Hoz, De la Hoz, Ortiz, & Ortega, (2012) *Modelo de detección de intrusiones en sistemas de red, realizando selección de características con FDR y entrenamiento y clasificación con SOM*. Universidad de la Costa. Colombia.

Feng, R. Guo, D. Wang, B. Zhang (2009) Research on the active DDoS filtering algorithm based on IP flow, en 5th International Conference on Natural Computation, vol. 4, pp. 628-632, 2009.

François J. (2016) La seguridad informática en la PyME Encontrado en: https://books.google.com.pe/books?id=LKE5_6gzBmgC&pg=PA336&dq=confidencialidad,+integridad+de+datos&hl=es&sa=X&ved=0ahUKEwjmqZPR79DUAhWBNSYKHdWfBloQ6AEIKTAB#v=onepage&q=confidencialidad%2C%20integridad%20de%20datos&f=false

Harpreet Sandhu & Manpreet Kaur (2017) en su investigación, Review paper on Snort and reviewing its applications in different fields.

Herrera Zurita, A. (2016). Aprendizaje automático para la detección de ataques informáticos. Escola d'enginyeria (EE), Universitat autonoma de Barcelona, España.

Holgado, P., y Villagrá, V. (2016) Sistema de detección de fases de ataque basado en Modelos Ocultos de Markov. Departamento de Ingenieria y Sistemas Telemáticos. Universidad Politécnica de Madrid Avenida Complutense, España.
http://jornadasciberseguridad.riasc.unileon.es/archivos/ActasJNIC2016.pdf

Jácome, F. y Robayo, M. (2014). Implementación de mecanismos de seguridad para contrarrestar infraestructuras críticas frente ataques informáticos en el laboratorio de redes de la Universidad Técnica de Cotopaxi ubicado en la ciudad de Latacunga, Provincia de Cotopaxi, en el periodo 2013. (Tesis de grado) Universidad Técnica de Cotopaxi.

Jimeno, M. T., Miguez, C., Heredia, E. y Caballero M. (2011) Libro: Destripa a la red. Edición 2011. pag (173 - 204)

Jimeno G. M., Míguez P. C., Matas G. A. y Pérez A. J. (2009) Libro: La biblia Hacker. Edición 2009. España.

Gadalméz, P. (2003), Seguridad Informática. Actualidad TIC. http://web.iti.upv.es/actualidadtic/2003/07/2003-07-seguridad.pdf

Geng, Y. Huang, AB Whinston (2002), La defensa de la infraestructura inalámbrica contra el desafío de los ataques DDoS. Redes y aplicaciones móviles, pp. 213-223

Gómez Vieites, A. (2011). Libro: Enciclopedia de la Seguridad Informática – 2da edición. Editorial Alfaomega pag (201 - 207)

Guevara, C., Santos, M. y López, V. (2013) Sistema de Detección de Intrusos aplicando Selección Negativa en Perfiles de Usuario. Facultad de Informática, Universidad Complutense de Madrid, España. http://jornadasciberseguridad.riasc.unileon.es/archivos/JNIC2013.pdf

Luna Domínguez, J. E. (2015). Sistema detector de intrusos ocupando una red neuronal artificial (Tesis de Maestría) Universidad Autónoma del estado de México.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Maestre. J., Sandoval. A. y García, L. (2015). Sistema inmunitario adaptativo para mitigación de ataques de denegación de Servicio. Departamento de Ingeniería del Software e Inteligencia Artificial, Universidad Complutense de Madrid, España.
[Online] http://jornadasciberseguridad.riasc.unileon.es/archivos/JNIC2015.pdf

McNab C. (2008). Seguridad de redes. Segunda edición. España

Memari, Hashim y Samsudin, (2014). Design of a hybrid virtual honeynet based on LXC virtualization for network security. Department of Computer and Communication Systems Engineering, Faculty of Engineering, University Putra Malaysia (UPM), pag 120 – 129

Mohammad D., Izzat A. y Emad A. (2013). Efficient Assessment and Evaluation for Websites Vulnerabilities Using SNORT. International Journal Security and Its Applications Vol. 7, N°.1. Yarmouk University, Jordania

Montenegro, C., Gaona, E. y Gaona, P. (2010) Plataforma de seguridad basado en autenticidad de contenidos sobre conjunto de especificaciones SCORM. Ingeniería y Competitividad, Volumen 12 No. 2, p. 51 - 68 - Universidad Distrital, Bogotá, Colombia.

Orellana, L. y Hernández, R. (2003) Seguridad en Redes de Datos. (Tesis de grado) Universidad Don Bosco, El Salvador.

Perdisci, J. Zhang, W. Lee (2008) BotMiner: Clustering analysis of network traffic for protocol- and structure-independent botnet detection, en 17th Conference on Security Symposium, pp. 139-154.

Pérez, Britto & Isaza (2005). Aplicación de redes neuronales para la detección de intrusos en redes y sistemas de información. Scientia et Technica Año XI, No 27, Universidad Tecnologica de Pereira – Colombia.

Pérez y Martínez (2015). Detectando botnets con dos modelos de abstracción: Flujos de tráfico e inspección de paquetes de red. Universidad de Murcia, Murcia, España.

Quinchaguano Duque, D (2016) Diseño e implementación de un prototipo de una Honeynet para la red de datos de la escuela Politécnica Nacional. Escuela Politécnica Eléctrica y Electrónica, Quito, Ecuador.

Revista digital INESEM. Encontrada en: http://revistadigital.inesem.es/nuevas-tecnologias/los-gestores-de-bases-de-datos-mas-usados/

Ramos A. B. y Ribagorda G. A. (2004) Libro: Avances en criptología y seguridad de la información. España. Encontrado en: https://books.google.com.pe/books?id=ibSu6896I_YC&printsec=frontcover&hl=es#v=onepage&q&f=false

Rupinder, K., NagpaJ, S. y Chamotra, S. (2015). "Detección de tráfico malicioso en una red privada de la organización usando el sistema de Honeynet". Annual IEEE India Conference (INDICON), India. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7443563&queryText=honeynet&ranges=2012_2015_Year

Scarfone, K., y Peter Mell (2007). Guide to intrusion detection and prevention systems (idps). NIST special publication 800.2007.

Sabido, I., Román, F. y García, L (2016). Aplicaciones web vulnerables a propósito. Departamento de Ingeniería del Software e Inteligencia Artificial (DISIA), Universidad Complutense de Madrid, España. http://jornadasciberseguridad.riasc.unileon.es/archivos/ActasJNIC2016.pdf

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Silva Trujillo, A. (2016) Nuevos ataques estadísticos de revelación de identidades en redes de comunicaciones anónimas. Madrid.

Stallings, W. (2004). Libro: Fundamentos de seguridad en redes. Aplicaciones y estándares - Segunda Edición. Editorial Pearson Educación, S.A., (pag. 14) Madrid.

Sokol, P. y Pisarcik, P. (2013) Digital evidence in virtual honeynets based on operating system level virtualization. Universidad de Pavol Jozef Šafárik en Košice. http://spi.unob.cz/papers/2013/2013-14.pdf

Vaca, Jhonny (2014) Implementación de un prototipo de seguridad con Honeynet Virtuales para descubrir patrones de ataques y analizar el comportamiento y las condiciones de los intrusos, aplicando en el laboratorio de Tecnologías de la información y comunicación –LTIC. Pontificia Universidad Católica del Ecuador, Quito.

Valero D. F. (2012) Binary – TI, Seguridad de la información BIT A BIT. Descargado de: http://www.binaryti.com/2012/02/valhalla-honeypot.html

Yánez Guevara, D. F. (2013) Sistema de detección y prevención de intrusos para el control de la vulnerabilidad en los servidores de la facultad de Ingeniería de Sistemas, Electrónica e Industrial de la universidad técnica de Ambato-Ecuador.

Kwon, Hong, & Ju (2012). En su investigación DDoS arquitectura del sistema de previsión ataque con Honeynet. IEEE Network Operations and Management Symposium (APNOMS). http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6356055&queryText=honeynet&ranges=2012_2015_Year

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ANEXOS

ANEXO I

Tabla 43. Clasificación de paquetes en pruebas de ataque DoS realizados a Servidor web mediante el mecanismo Honeynet

HONEYNEY – (HONEYPOT WEB)				
N° de prueba	Tráfico con ataque DoS		Tráfico normal	
	N° de paquetes			
	Detectado como ataque	Detectado como no ataque	Detectado como ataque	Detectado como no ataque
Prueba 01	2042	42	0	1984
Prueba 02	1824	36	6	1720
Prueba 03	1960	34	5	1820
Prueba 04	2010	46	7	1872
Prueba 05	2000	42	5	1876
Prueba 06	1880	38	6	1742
Prueba 07	1978	42	0	1805
Prueba 08	2036	40	0	1790
Prueba 09	1885	41	7	1702
Prueba 10	1999	37	6	1845
Prueba 11	1994	40	0	1723
Prueba 12	1968	45	6	1820
Prueba 13	2065	41	0	1712
Prueba 14	2034	39	8	1902
Prueba 15	2030	41	8	1845
Prueba 16	1908	39	7	1788
Prueba 17	1978	41	5	1856
Prueba 18	2112	37	8	1899
Prueba 19	2007	39	0	1900
Prueba 20	2058	43	0	1885
Prueba 21	1988	43	7	1789
Prueba 22	2060	39	6	1712
Prueba 23	1740	43	6	1669
Prueba 24	1785	32	0	1678
Prueba 25	1994	43	7	1800
Prueba 26	2148	41	5	1978
Prueba 27	2021	45	6	1987
Prueba 28	2044	39	6	1899
Prueba 29	1842	39	8	1726

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Prueba 30	1950	48	0	1814
Prueba 31	2030	36	9	1593
Prueba 32	2040	38	5	1655
Prueba 33	1991	34	0	1452
Prueba 34	2136	43	6	1747
Prueba 35	2120	47	2	1666
Prueba 36	1881	50	0	1607
Prueba 37	2059	31	8	1522
Prueba 38	1838	46	4	1960
Prueba 39	2158	37	8	1763
Prueba 40	2185	39	5	1523
Prueba 41	2022	41	7	1905
Prueba 42	1904	48	9	1499
Prueba 43	2049	33	6	1978
Prueba 44	2069	37	5	1525
Prueba 45	1927	38	3	1539
Prueba 46	1967	42	4	1911
Prueba 47	2117	48	4	1422
Prueba 48	1936	33	6	1772
Prueba 49	2001	44	5	1923
Prueba 50	2043	42	6	1726
PROMEDIO	**1996**	**40**	**5**	**1765**

Fuente: Elaboración propia

Tabla 44. Tiempo de respuesta del mecanismo Honeynet frente a ataque DoS de las pruebas realizadas a servidor web

N° de pruebas	Tiempo inicial de la prueba	Tiempo de reacción del mecanismo	Tiempo de respuesta
Prueba 01	10:05:12	10:05:16	0:00:04
Prueba 02	10:05:32	10:05:37	0:00:05
Prueba 03	10:05:53	10:05:57	0:00:04
Prueba 04	10:06:13	10:06:18	0:00:05
Prueba 05	10:06:34	10:06:39	0:00:05
Prueba 06	10:06:54	10:06:58	0:00:04
Prueba 07	10:07:16	10:07:20	0:00:04
Prueba 08	10:07:36	10:07:41	0:00:05
Prueba 09	10:07:56	10:08:01	0:00:05
Prueba 10	10:08:17	10:08:21	0:00:04
Prueba 11	10:08:37	10:08:42	0:00:05

Prueba 12	10:08:57	10:09:01	0:00:04
Prueba 13	10:09:17	10:09:22	0:00:05
Prueba 14	10:09:37	10:09:41	0:00:04
Prueba 15	10:09:58	10:10:03	0:00:05
Prueba 16	10:10:18	10:10:22	0:00:04
Prueba 17	10:10:38	10:10:43	0:00:05
Prueba 18	10:10:59	10:11:03	0:00:04
Prueba 19	10:11:19	10:11:24	0:00:05
Prueba 20	10:11:39	10:11:44	0:00:05
Prueba 21	10:11:59	10:12:04	0:00:05
Prueba 22	10:12:20	10:12:24	0:00:04
Prueba 23	10:12:40	10:12:45	0:00:05
Prueba 24	10:13:00	10:13:04	0:00:04
Prueba 25	10:13:21	10:13:26	0:00:05
Prueba 26	10:13:43	10:13:47	0:00:04
Prueba 27	10:14:03	10:14:08	0:00:05
Prueba 28	10:14:23	10:14:27	0:00:04
Prueba 29	10:14:45	10:14:50	0:00:05
Prueba 30	10:15:06	10:15:10	0:00:04
Prueba 31	3:18:42	3:18:47	0:00:05
Prueba 32	3:19:04	3:19:08	0:00:04
Prueba 33	3:19:24	3:19:28	0:00:04
Prueba 34	3:19:45	3:19:49	0:00:04
Prueba 35	3:20:05	3:20:09	0:00:04
Prueba 36	3:20:25	3:20:29	0:00:04
Prueba 37	3:20:47	3:20:52	0:00:05
Prueba 38	3:21:07	3:21:11	0:00:04
Prueba 39	3:21:27	3:21:31	0:00:04
Prueba 40	3:21:48	3:21:52	0:00:04
Prueba 41	3:22:08	3:22:13	0:00:05
Prueba 42	3:22:30	3:22:35	0:00:05
Prueba 43	3:22:50	3:22:54	0:00:04
Prueba 44	3:23:12	3:23:16	0:00:04
Prueba 45	3:23:33	3:23:38	0:00:05
Prueba 46	3:23:53	3:23:57	0:00:04
Prueba 47	3:24:13	3:24:18	0:00:05
Prueba 48	3:24:35	3:24:39	0:00:04
Prueba 49	3:24:55	3:24:59	0:00:04
Prueba 50	3:25:16	3:25:21	0:00:05
TOTAL			0:00:04

Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 45. Clasificación de paquetes en pruebas de ataque DoS realizadas a servidor base de datos mediante el mecanismo Honeynet.

HONEYNET – (HONEYPOT BASE DE DATOS)				
N° de prueba	Tráfico con ataque DoS		Tráfico normal	
	N° de paquetes			
	Detectado como ataque	Detectado como no ataque	Detectado como ataque	Detectado como no ataque
Prueba 01	2050	44	0	1750
Prueba 02	2084	40	10	1882
Prueba 03	1680	43	9	1743
Prueba 04	1971	49	5	1615
Prueba 05	2054	41	7	1791
Prueba 06	1936	45	11	1780
Prueba 07	1888	50	8	1720
Prueba 08	1956	44	8	1699
Prueba 09	1931	52	9	1865
Prueba 10	2080	46	0	1750
Prueba 11	1930	45	6	1654
Prueba 12	1836	54	6	1540
Prueba 13	2095	48	0	1745
Prueba 14	2272	41	9	1810
Prueba 15	1900	38	8	1478
Prueba 16	1908	37	9	1684
Prueba 17	1898	39	0	1700
Prueba 18	1730	37	0	1601
Prueba 19	2071	47	10	1900
Prueba 20	1920	55	11	1700
Prueba 21	1913	48	9	1689
Prueba 22	1802	39	8	1773
Prueba 23	1980	45	10	1655
Prueba 24	1731	42	0	1612
Prueba 25	1952	41	9	1746
Prueba 26	1928	45	9	1850
Prueba 27	1850	51	7	1701
Prueba 28	1620	40	15	1512
Prueba 29	1806	42	10	1600
Prueba 30	1880	48	0	1520
Prueba 31	1999	37	5	1782

Prueba 32	2010	39	7	1900
Prueba 33	1990	37	4	1870
Prueba 34	1999	37	5	1782
Prueba 35	1878	35	9	1736
Prueba 36	2152	44	7	1856
Prueba 37	1972	41	0	1860
Prueba 38	1896	38	5	1684
Prueba 39	2002	43	7	1886
Prueba 40	1956	44	0	1875
Prueba 41	1986	39	4	1890
Prueba 42	1894	37	6	1789
Prueba 43	1957	38	0	1860
Prueba 44	2066	31	6	1920
Prueba 45	1998	36	8	1778
Prueba 46	2110	39	5	1980
Prueba 47	2003	40	7	1874
Prueba 48	1990	36	8	1756
Prueba 49	1799	43	8	1563
Prueba 50	1880	38	6	1667
PROMEDIO	**1947**	**42**	**6**	**1747**

Fuente: Elaboración propia

Tabla 46. Tiempo de respuesta del mecanismo Honeynet frente a ataque DoS de las pruebas realizadas a servidor base de datos

N° de pruebas	Tiempo inicial de la prueba	Tiempo de reacción del mecanismo	Tiempo de respuesta
Prueba 01	19:48:43	19:48:48	0:00:05
Prueba 02	19:49:03	19:49:07	0:00:04
Prueba 03	19:49:24	19:49:29	0:00:05
Prueba 04	19:49:44	19:49:48	0:00:04
Prueba 05	19:50:05	19:50:09	0:00:04
Prueba 06	19:50:25	19:50:29	0:00:04
Prueba 07	19:50:45	19:50:50	0:00:05
Prueba 08	19:51:05	19:51:10	0:00:05
Prueba 09	19:51:26	19:51:31	0:00:05
Prueba 10	19:51:46	19:51:50	0:00:04
Prueba 11	19:52:06	19:52:11	0:00:05
Prueba 12	19:52:27	19:52:32	0:00:05

Prueba 13	19:52:47	19:52:52	0:00:05
Prueba 14	19:53:07	19:53:11	0:00:04
Prueba 15	19:53:28	19:53:32	0:00:04
Prueba 16	19:53:48	19:53:53	0:00:05
Prueba 17	19:54:09	19:54:14	0:00:05
Prueba 18	19:54:29	19:54:33	0:00:04
Prueba 19	19:54:49	19:54:54	0:00:05
Prueba 20	19:55:09	19:55:13	0:00:04
Prueba 21	19:55:31	19:55:36	0:00:05
Prueba 22	19:55:52	19:55:57	0:00:05
Prueba 23	19:56:12	19:56:17	0:00:05
Prueba 24	19:56:32	19:56:36	0:00:04
Prueba 25	19:56:52	19:56:56	0:00:04
Prueba 26	19:57:12	19:57:17	0:00:05
Prueba 27	19:57:33	19:57:37	0:00:04
Prueba 28	19:57:53	19:57:58	0:00:05
Prueba 29	19:58:15	19:58:20	0:00:05
Prueba 30	19:58:35	19:58:39	0:00:04
Prueba 31	4:42:15	4:42:19	0:00:04
Prueba 32	4:42:36	4:42:41	0:00:05
Prueba 33	4:42:56	4:43:01	0:00:05
Prueba 34	4:43:16	4:43:22	0:00:06
Prueba 35	4:43:36	4:43:41	0:00:05
Prueba 36	4:43:57	4:44:01	0:00:04
Prueba 37	4:44:17	4:44:21	0:00:04
Prueba 38	4:44:37	4:44:42	0:00:05
Prueba 39	4:44:58	4:45:02	0:00:04
Prueba 40	4:45:18	4:45:22	0:00:04
Prueba 41	4:45:38	4:45:43	0:00:05
Prueba 42	4:45:59	4:46:03	0:00:04
Prueba 43	4:46:19	4:46:23	0:00:04
Prueba 44	4:46:39	4:46:44	0:00:05
Prueba 45	4:47:00	4:47:06	0:00:06
Prueba 46	4:47:20	4:47:24	0:00:04
Prueba 47	4:47:40	4:47:44	0:00:04
Prueba 48	4:48:00	4:48:05	0:00:05
Prueba 49	4:48:21	4:48:25	0:00:04
Prueba 50	4:48:42	4:48:46	0:00:04
TOTAL			0:00:05

Fuente. Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 47. Clasificación de paquetes en pruebas de ataque Exploración de vulnerabilidades realizadas a Servidor web mediante el mecanismo Honeynet

HONEYNEY – (HONEYPOT WEB)				
N° de prueba	Tráfico con ataque Exploración de Vulnerabilidades		Tráfico normal	
	N° de paquetes			
	Detectado como ataque	Detectado como no ataque	Detectado como ataque	Detectado como no ataque
Prueba 01	478	12	0	403
Prueba 02	465	15	4	420
Prueba 03	502	20	5	487
Prueba 04	488	16	6	453
Prueba 05	467	15	8	320
Prueba 06	479	14	5	423
Prueba 07	501	18	7	476
Prueba 08	489	17	8	453
Prueba 09	448	12	5	419
Prueba 10	511	16	0	416
Prueba 11	443	17	0	387
Prueba 12	458	21	6	408
Prueba 13	476	18	0	395
Prueba 14	412	21	9	310
Prueba 15	468	18	8	388
Prueba 16	474	17	9	324
Prueba 17	435	23	0	372
Prueba 18	459	17	2	401
Prueba 19	481	14	7	348
Prueba 20	421	15	8	382
Prueba 21	483	8	7	421
Prueba 22	413	10	8	356
Prueba 23	487	15	6	380
Prueba 24	432	20	0	372
Prueba 25	463	21	5	401
Prueba 26	478	18	5	340
Prueba 27	435	14	7	313
Prueba 28	461	18	5	370
Prueba 29	456	13	6	398
Prueba 30	430	15	0	357
Prueba 31	530	13	6	477

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Prueba 32	508	17	3	470
Prueba 33	427	18	8	309
Prueba 34	450	18	3	387
Prueba 35	514	11	8	422
Prueba 36	488	10	7	306
Prueba 37	454	18	4	309
Prueba 38	523	6	5	370
Prueba 39	552	5	7	432
Prueba 40	406	8	3	388
Prueba 41	478	8	2	364
Prueba 42	475	8	1	476
Prueba 43	428	11	9	379
Prueba 44	537	10	3	467
Prueba 45	517	19	1	415
Prueba 46	426	10	0	478
Prueba 47	427	11	1	422
Prueba 48	457	6	9	418
Prueba 49	495	15	7	431
Prueba 50	488	17	8	456
PROMEDIO	**469**	**15**	**5**	**397**

Fuente: Elaboración propia

Tabla 48. Tiempo de respuesta del mecanismo Honeynet frente a ataque Exploración de vulnerabilidades de pruebas realizadas a servidor web

N° de pruebas	Tiempo inicial de la prueba	Tiempo de reacción del mecanismo	Tiempo de respuesta
Prueba 01	3:44:28	3:44:33	0:00:05
Prueba 02	3:44:48	3:44:52	0:00:04
Prueba 03	3:45:09	3:45:14	0:00:05
Prueba 04	3:45:29	3:45:34	0:00:05
Prueba 05	3:45:49	3:45:54	0:00:05
Prueba 06	3:46:09	3:46:13	0:00:04
Prueba 07	3:46:30	3:46:34	0:00:04
Prueba 08	3:46:52	3:46:56	0:00:04
Prueba 09	3:47:13	3:47:17	0:00:04
Prueba 10	3:47:33	3:47:37	0:00:04
Prueba 11	3:47:55	3:48:00	0:00:05
Prueba 12	3:48:15	3:48:20	0:00:05
Prueba 13	3:48:35	3:48:39	0:00:04

Prueba 14	3:48:57	3:49:02	0:00:05
Prueba 15	3:49:17	3:49:21	0:00:04
Prueba 16	3:49:38	3:49:43	0:00:05
Prueba 17	3:49:59	3:50:04	0:00:05
Prueba 18	3:50:19	3:50:23	0:00:04
Prueba 19	3:50:40	3:50:44	0:00:04
Prueba 20	3:51:00	3:51:04	0:00:04
Prueba 21	3:51:20	3:51:24	0:00:04
Prueba 22	3:51:40	3:51:45	0:00:05
Prueba 23	3:52:01	3:52:06	0:00:05
Prueba 24	3:52:21	3:52:25	0:00:04
Prueba 25	3:52:41	3:52:45	0:00:04
Prueba 26	3:53:01	3:53:06	0:00:05
Prueba 27	3:53:21	3:53:25	0:00:04
Prueba 28	3:53:42	3:53:47	0:00:05
Prueba 29	3:54:04	3:54:09	0:00:05
Prueba 30	3:54:24	3:54:28	0:00:04
Prueba 31	3:54:45	3:54:49	0:00:04
Prueba 32	3:55:06	3:55:11	0:00:05
Prueba 33	3:55:26	3:55:30	0:00:04
Prueba 34	3:55:46	3:55:51	0:00:05
Prueba 35	3:56:07	3:56:12	0:00:05
Prueba 36	3:56:27	3:56:33	0:00:06
Prueba 37	3:56:47	3:56:52	0:00:05
Prueba 38	3:57:08	3:57:13	0:00:05
Prueba 39	3:57:29	3:57:35	0:00:06
Prueba 40	3:57:51	3:57:55	0:00:04
Prueba 41	3:58:11	3:58:16	0:00:05
Prueba 42	3:58:31	3:58:36	0:00:05
Prueba 43	3:58:52	3:58:57	0:00:05
Prueba 44	3:59:12	3:59:18	0:00:06
Prueba 45	3:59:34	3:59:39	0:00:05
Prueba 46	3:59:54	3:59:59	0:00:05
Prueba 47	4:00:14	4:00:19	0:00:05
Prueba 48	4:00:36	4:00:42	0:00:06
Prueba 49	4:00:56	4:01:00	0:00:04
Prueba 50	4:01:17	4:01:22	0:00:05
TOTAL			0:00:05

Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 49. Clasificación de paquetes en pruebas de ataque Exploración de vulnerabilidades realizadas a Servidor base de datos mediante el mecanismo Honeynet

HONEYNEY – (HONEYPOT BASE DE DATOS)				
N° de prueba	Tráfico con ataque Exploración de Vulnerabilidades		Tráfico normal	
	N° de paquetes			
	Detectado como ataque	Detectado como no ataque	Detectado como ataque	Detectado como no ataque
Prueba 01	418	10	2	340
Prueba 02	501	17	0	416
Prueba 03	499	12	4	427
Prueba 04	423	9	5	354
Prueba 05	456	11	0	369
Prueba 06	471	17	0	401
Prueba 07	500	15	5	416
Prueba 08	413	13	9	447
Prueba 09	465	12	4	405
Prueba 10	432	16	2	409
Prueba 11	400	16	4	367
Prueba 12	461	11	0	398
Prueba 13	432	12	7	385
Prueba 14	416	15	5	310
Prueba 15	478	8	8	388
Prueba 16	433	11	2	324
Prueba 17	456	13	0	372
Prueba 18	421	10	6	347
Prueba 19	419	14	9	364
Prueba 20	487	10	7	391
Prueba 21	452	8	0	351
Prueba 22	450	10	4	356
Prueba 23	417	12	6	380
Prueba 24	405	9	0	352
Prueba 25	420	15	5	323
Prueba 26	471	13	7	340
Prueba 27	436	14	6	325
Prueba 28	398	14	8	320
Prueba 29	417	11	3	363
Prueba 30	485	9	0	346
Prueba 31	461	16	4	419

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Prueba 32	454	11	0	400
Prueba 33	520	13	6	377
Prueba 34	464	10	2	354
Prueba 35	558	5	6	435
Prueba 36	493	10	7	310
Prueba 37	550	18	4	460
Prueba 38	466	19	8	362
Prueba 39	434	13	7	375
Prueba 40	528	6	8	333
Prueba 41	437	7	8	417
Prueba 42	443	10	3	346
Prueba 43	485	8	5	323
Prueba 44	484	17	0	485
Prueba 45	541	5	5	423
Prueba 46	406	11	0	445
Prueba 47	525	17	1	480
Prueba 48	517	6	8	408
Prueba 49	543	18	1	482
Prueba 50	417	7	4	414
PROMEDIO	**461**	**12**	**4**	**382**

Fuente: Elaboración propia

Tabla 50. Tiempo de respuesta del mecanismo Honeynet frente a ataque Exploración de vulnerabilidades de las pruebas realizadas a servidor base de datos

N° de pruebas	Tiempo inicial de la prueba	Tiempo de reacción del mecanismo	Tiempo de respuesta
Prueba 01	4:17:41	4:17:45	0:00:04
Prueba 02	4:18:01	4:18:06	0:00:05
Prueba 03	4:18:22	4:18:27	0:00:05
Prueba 04	4:18:42	4:18:46	0:00:04
Prueba 05	4:19:03	4:19:07	0:00:04
Prueba 06	4:19:23	4:19:28	0:00:05
Prueba 07	4:19:43	4:19:48	0:00:05
Prueba 08	4:20:03	4:20:08	0:00:05
Prueba 09	4:20:24	4:20:29	0:00:05
Prueba 10	4:20:45	4:20:49	0:00:04
Prueba 11	4:21:05	4:21:10	0:00:05
Prueba 12	4:21:26	4:21:31	0:00:05
Prueba 13	4:21:46	4:21:51	0:00:05

Prueba 14	4:22:06	4:22:10	0:00:04
Prueba 15	4:22:28	4:22:33	0:00:05
Prueba 16	4:22:48	4:22:52	0:00:04
Prueba 17	4:23:09	4:23:14	0:00:05
Prueba 18	4:23:29	4:23:33	0:00:04
Prueba 19	4:23:50	4:23:54	0:00:04
Prueba 20	4:24:10	4:24:14	0:00:04
Prueba 21	4:24:30	4:24:35	0:00:05
Prueba 22	4:24:51	4:24:56	0:00:05
Prueba 23	4:25:11	4:25:15	0:00:04
Prueba 24	4:25:32	4:25:37	0:00:05
Prueba 25	4:25:52	4:25:56	0:00:04
Prueba 26	4:26:12	4:26:17	0:00:05
Prueba 27	4:26:33	4:26:37	0:00:04
Prueba 28	4:26:53	4:26:58	0:00:05
Prueba 29	4:27:15	4:27:19	0:00:04
Prueba 30	4:27:35	4:27:40	0:00:05
Prueba 31	4:27:56	4:28:00	0:00:04
Prueba 32	4:28:16	4:28:21	0:00:05
Prueba 33	4:28:36	4:28:40	0:00:04
Prueba 34	4:28:56	4:29:00	0:00:04
Prueba 35	4:29:17	4:29:22	0:00:05
Prueba 36	4:29:39	4:29:43	0:00:04
Prueba 37	4:29:59	4:30:04	0:00:05
Prueba 38	4:30:19	4:30:23	0:00:04
Prueba 39	4:30:40	4:30:44	0:00:04
Prueba 40	4:31:01	4:31:05	0:00:04
Prueba 41	4:31:23	4:31:28	0:00:05
Prueba 42	4:31:43	4:31:47	0:00:04
Prueba 43	4:32:03	4:32:08	0:00:05
Prueba 44	4:32:24	4:32:28	0:00:04
Prueba 45	4:32:44	4:32:48	0:00:04
Prueba 46	4:33:04	4:33:09	0:00:05
Prueba 47	4:33:26	4:33:31	0:00:05
Prueba 48	4:33:46	4:33:50	0:00:04
Prueba 49	4:34:08	4:34:12	0:00:04
Prueba 50	4:34:29	4:34:34	0:00:05
TOTAL			**0:00:04**

Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 51. Clasificación de paquetes en pruebas de ataque DoS realizadas a Servidor web mediante el mecanismo Snort

SNORT WEB				
N° de prueba	Tráfico con ataque DoS		Tráfico normal	
	N° de paquetes			
	Detectado como ataque	Detectado como no ataque	Detectado como ataque	Detectado como no ataque
Prueba 01	1684	34	7	1931
Prueba 02	1784	29	4	1780
Prueba 03	1984	24	5	1939
Prueba 04	1648	31	1	1979
Prueba 05	1752	41	4	1792
Prueba 06	1845	25	9	1907
Prueba 07	1762	53	0	1990
Prueba 08	1942	40	8	1926
Prueba 09	1845	42	2	1849
Prueba 10	1684	34	4	1853
Prueba 11	1845	29	0	1903
Prueba 12	1801	37	0	1754
Prueba 13	1730	34	0	1949
Prueba 14	1908	37	0	1979
Prueba 15	1761	38	5	1748
Prueba 16	1901	33	5	1897
Prueba 17	1884	35	4	1856
Prueba 18	1874	31	4	1841
Prueba 19	1974	36	1	1894
Prueba 20	1852	33	1	1727
Prueba 21	1963	43	5	1790
Prueba 22	1749	34	3	1756
Prueba 23	1780	49	6	1989
Prueba 24	1984	38	9	1918
Prueba 25	1870	24	3	1938
Prueba 26	1980	38	9	1765
Prueba 27	1879	34	7	1859
Prueba 28	1830	39	6	1771
Prueba 29	1874	42	4	1761
Prueba 30	1984	24	1	1832
Prueba 31	1823	50	5	1838

Prueba 32	1700	30	0	1750
Prueba 33	1730	38	8	1718
Prueba 34	1769	25	5	1871
Prueba 35	1784	42	6	1810
Prueba 36	1755	47	8	1779
Prueba 37	1856	30	7	1730
Prueba 38	1781	32	0	1819
Prueba 39	1772	27	8	1919
Prueba 40	1914	50	4	1761
Prueba 41	1840	50	1	1781
Prueba 42	1814	43	7	1776
Prueba 43	1752	30	2	1828
Prueba 44	1715	46	4	1799
Prueba 45	1759	49	4	1744
Prueba 46	1838	33	8	1896
Prueba 47	1848	44	4	1822
Prueba 48	1798	41	1	1869
Prueba 49	1936	52	2	1919
Prueba 50	1731	26	6	1716
PROMEDIO	**1825**	**37**	**4**	**1840**

Fuente: Elaboración propia.

Tabla 52. Tiempo de respuesta de mecanismo Snort frente a ataque DoS de las pruebas realizadas a servidor web.

N° de pruebas	Tiempo inicial de la prueba	Tiempo de reacción del mecanismo	Tiempo de respuesta
Prueba 01	22:55:37	22:55:42	0:00:05
Prueba 02	22:55:57	22:56:02	0:00:05
Prueba 03	22:56:17	22:56:21	0:00:04
Prueba 04	22:56:38	22:56:43	0:00:05
Prueba 05	22:56:58	22:57:03	0:00:05
Prueba 06	22:57:18	22:57:22	0:00:04
Prueba 07	22:57:38	22:57:42	0:00:04
Prueba 08	22:57:59	22:58:04	0:00:05
Prueba 09	22:58:20	22:58:25	0:00:05
Prueba 10	22:58:41	22:58:45	0:00:04
Prueba 11	22:59:01	22:59:06	0:00:05
Prueba 12	22:59:22	22:59:26	0:00:04
Prueba 13	22:59:44	22:59:49	0:00:05

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Prueba 14	23:00:04	23:00:08	0:00:04
Prueba 15	23:00:26	23:00:31	0:00:05
Prueba 16	23:00:47	23:00:52	0:00:05
Prueba 17	23:01:07	23:01:11	0:00:04
Prueba 18	23:01:27	23:01:31	0:00:04
Prueba 19	23:01:47	23:01:51	0:00:04
Prueba 20	23:02:07	23:02:11	0:00:04
Prueba 21	23:02:28	23:02:32	0:00:04
Prueba 22	23:02:48	23:02:52	0:00:04
Prueba 23	23:03:09	23:03:14	0:00:05
Prueba 24	23:03:30	23:03:34	0:00:04
Prueba 25	23:03:52	23:03:57	0:00:05
Prueba 26	23:04:12	23:04:17	0:00:05
Prueba 27	23:04:32	23:04:36	0:00:04
Prueba 28	23:04:52	23:04:56	0:00:04
Prueba 29	23:05:13	23:05:18	0:00:05
Prueba 30	23:05:34	23:05:39	0:00:05
Prueba 31	11:04:37	11:04:43	0:00:06
Prueba 32	11:04:57	11:05:02	0:00:05
Prueba 33	11:05:17	11:05:23	0:00:06
Prueba 34	11:05:38	11:05:43	0:00:05
Prueba 35	11:05:58	11:06:04	0:00:06
Prueba 36	11:06:19	11:06:24	0:00:05
Prueba 37	11:06:39	11:06:46	0:00:07
Prueba 38	11:06:59	11:07:05	0:00:06
Prueba 39	11:07:21	11:07:26	0:00:05
Prueba 40	11:07:42	11:07:47	0:00:05
Prueba 41	11:08:04	11:08:09	0:00:05
Prueba 42	11:08:24	11:08:29	0:00:05
Prueba 43	11:08:45	11:08:52	0:00:07
Prueba 44	11:09:05	11:09:09	0:00:04
Prueba 45	11:09:25	11:09:31	0:00:06
Prueba 46	11:09:45	11:09:50	0:00:05
Prueba 47	11:10:06	11:10:10	0:00:04
Prueba 48	11:10:26	11:10:33	0:00:07
Prueba 49	11:10:48	11:10:53	0:00:05
Prueba 50	11:11:08	11:11:14	0:00:06
TOTAL			0:00:05

Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 53. Clasificación de paquetes en pruebas de ataque DoS realizadas a Servidor Base de datos mediante el mecanismo Snort

SNORT BASE DE DATOS				
N° de prueba	Tráfico con ataque DoS		Tráfico normal	
	N° de paquetes			
	Detectado como ataque	Detectado como no ataque	Detectado como ataque	Detectado como no ataque
Prueba 01	1789	44	9	1784
Prueba 02	2070	35	13	1868
Prueba 03	2110	32	3	1843
Prueba 04	1790	31	9	1730
Prueba 05	1771	38	9	1934
Prueba 06	1933	36	1	1989
Prueba 07	1789	31	0	1883
Prueba 08	2030	46	0	1798
Prueba 09	2028	42	14	1938
Prueba 10	1844	31	8	1883
Prueba 11	1866	47	0	1909
Prueba 12	1969	39	14	1910
Prueba 13	2060	45	7	1943
Prueba 14	1910	32	4	1911
Prueba 15	2003	35	3	1988
Prueba 16	1820	30	0	1729
Prueba 17	1911	35	4	1791
Prueba 18	1947	33	0	1816
Prueba 19	1879	44	3	1749
Prueba 20	2050	42	0	1868
Prueba 21	1973	40	3	1896
Prueba 22	1852	47	7	1958
Prueba 23	1784	44	12	1781
Prueba 24	2061	32	4	1797
Prueba 25	1728	38	13	1965
Prueba 26	1759	41	13	1826
Prueba 27	1779	45	12	1923
Prueba 28	1815	33	1	1778
Prueba 29	1802	34	13	1828
Prueba 30	1817	47	4	1847
Prueba 31	1910	43	6	1843

Prueba 32	1716	33	9	1809
Prueba 33	1696	38	8	1781
Prueba 34	1750	47	14	1719
Prueba 35	1935	45	0	1727
Prueba 36	1805	39	15	1812
Prueba 37	1815	47	10	1799
Prueba 38	1890	46	15	1723
Prueba 39	1709	43	11	1745
Prueba 40	1745	42	1	1808
Prueba 41	1719	35	0	1769
Prueba 42	1821	47	13	1761
Prueba 43	1793	35	5	1830
Prueba 44	1838	51	11	1776
Prueba 45	1849	40	5	1727
Prueba 46	1815	52	11	1769
Prueba 47	1943	48	1	1908
Prueba 48	1943	48	1	1859
Prueba 49	1768	42	15	1815
Prueba 50	1855	41	14	1853
PROMEDIO	**1865**	**40**	**7**	**1833**

Fuente: Elaboración propia

Tabla 54. Tiempo de respuesta del mecanismo Snort frente a ataque DoS de las pruebas realizadas a servidor base de datos.

N° de pruebas	Tiempo inicial de la prueba	Tiempo de reacción del mecanismo	Tiempo de respuesta
Prueba 01	22:34:43	22:34:48	0:00:05
Prueba 02	22:35:03	22:35:07	0:00:04
Prueba 03	22:35:24	22:35:28	0:00:04
Prueba 04	22:35:44	22:35:49	0:00:05
Prueba 05	22:36:06	22:36:10	0:00:04
Prueba 06	22:36:26	22:36:31	0:00:05
Prueba 07	22:36:46	22:36:51	0:00:05
Prueba 08	22:37:07	22:37:11	0:00:04
Prueba 09	22:37:29	22:37:34	0:00:05
Prueba 10	22:37:50	22:37:54	0:00:04
Prueba 11	22:38:12	22:38:17	0:00:05
Prueba 12	22:38:33	22:38:37	0:00:04
Prueba 13	22:38:55	22:39:00	0:00:05

Prueba 14	22:39:15	22:39:20	0:00:05
Prueba 15	22:39:37	22:39:42	0:00:05
Prueba 16	22:39:57	22:40:02	0:00:05
Prueba 17	22:40:17	22:40:21	0:00:04
Prueba 18	22:40:38	22:40:43	0:00:05
Prueba 19	22:41:00	22:41:04	0:00:04
Prueba 20	22:41:20	22:41:24	0:00:04
Prueba 21	22:41:41	22:41:46	0:00:05
Prueba 22	22:42:01	22:42:05	0:00:04
Prueba 23	22:42:22	22:42:27	0:00:05
Prueba 24	22:42:42	22:42:46	0:00:04
Prueba 25	22:43:04	22:43:08	0:00:04
Prueba 26	22:43:24	22:43:29	0:00:05
Prueba 27	22:43:44	22:43:48	0:00:04
Prueba 28	22:44:04	22:44:08	0:00:04
Prueba 29	22:44:26	22:44:31	0:00:05
Prueba 30	22:44:46	22:44:50	0:00:04
Prueba 31	10:34:08	10:34:14	0:00:06
Prueba 32	10:34:30	10:34:35	0:00:05
Prueba 33	10:34:51	10:34:57	0:00:06
Prueba 34	10:35:12	10:35:18	0:00:06
Prueba 35	10:35:34	10:35:39	0:00:05
Prueba 36	10:35:54	10:36:00	0:00:06
Prueba 37	10:36:15	10:36:22	0:00:07
Prueba 38	10:36:35	10:36:41	0:00:06
Prueba 39	10:36:56	10:37:02	0:00:06
Prueba 40	10:37:18	10:37:23	0:00:05
Prueba 41	10:37:40	10:37:46	0:00:06
Prueba 42	10:38:00	10:38:06	0:00:06
Prueba 43	10:38:21	10:38:27	0:00:06
Prueba 44	10:38:41	10:38:45	0:00:04
Prueba 45	10:39:02	10:39:08	0:00:06
Prueba 46	10:39:22	10:39:28	0:00:06
Prueba 47	10:39:42	10:39:48	0:00:06
Prueba 48	10:40:03	10:40:10	0:00:07
Prueba 49	10:40:25	10:40:30	0:00:05
Prueba 50	10:40:46	10:40:52	0:00:06
TOTAL			0:00:05

Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 55. Clasificación de paquetes en pruebas de ataque Exploración de vulnerabilidades realizadas a Servidor web mediante el mecanismo Snort.

SNORT WEB				
N° de prueba	Tráfico con ataque Exploración de Vulnerabilidades		Tráfico normal	
	N° de paquetes			
	Detectado como ataque	Detectado como no ataque	Detectado como ataque	Detectado como no ataque
Prueba 01	434	16	2	375
Prueba 02	475	14	4	417
Prueba 03	399	14	5	380
Prueba 04	516	12	7	393
Prueba 05	494	9	2	382
Prueba 06	395	11	6	361
Prueba 07	401	14	7	375
Prueba 08	489	8	1	413
Prueba 09	510	15	0	419
Prueba 10	453	10	5	375
Prueba 11	433	11	6	410
Prueba 12	519	12	0	418
Prueba 13	404	8	2	417
Prueba 14	520	11	8	355
Prueba 15	482	14	6	403
Prueba 16	400	10	3	405
Prueba 17	520	16	8	396
Prueba 18	507	13	5	371
Prueba 19	426	8	5	400
Prueba 20	509	9	8	404
Prueba 21	404	17	3	424
Prueba 22	421	15	1	367
Prueba 23	441	14	3	413
Prueba 24	426	15	7	404
Prueba 25	403	12	2	388
Prueba 26	440	10	1	394
Prueba 27	487	9	7	384
Prueba 28	465	8	4	371
Prueba 29	447	11	8	361
Prueba 30	518	8	8	372
Prueba 31	489	19	8	356

Prueba 32	514	5	6	384
Prueba 33	516	13	8	365
Prueba 34	417	17	2	387
Prueba 35	475	6	8	460
Prueba 36	446	17	1	331
Prueba 37	432	12	4	451
Prueba 38	413	9	1	378
Prueba 39	516	12	9	323
Prueba 40	491	10	4	376
Prueba 41	463	6	7	309
Prueba 42	540	13	8	481
Prueba 43	456	12	3	432
Prueba 44	412	14	9	404
Prueba 45	494	19	0	436
Prueba 46	541	5	7	417
Prueba 47	427	18	3	429
Prueba 48	557	8	6	448
Prueba 49	481	9	7	302
Prueba 50	521	17	8	434
PROMEDIO	**467**	**12**	**5**	**393**

Fuente: Elaboración propia

Tabla 56. Tiempo de respuesta del mecanismo Snort frente a ataque Exploración de vulnerabilidades de las pruebas realizadas a servidor web.

N° de pruebas	Tiempo inicial de la prueba	Tiempo de reacción del mecanismo	Tiempo de respuesta
Prueba 01	1:34:28	1:34:33	0:00:05
Prueba 02	1:34:49	1:34:54	0:00:05
Prueba 03	1:35:09	1:35:13	0:00:04
Prueba 04	1:35:30	1:35:35	0:00:05
Prueba 05	1:35:50	1:35:54	0:00:04
Prueba 06	1:36:11	1:36:16	0:00:05
Prueba 07	1:36:31	1:36:35	0:00:04
Prueba 08	1:36:51	1:36:55	0:00:04
Prueba 09	1:37:12	1:37:17	0:00:05
Prueba 10	1:37:32	1:37:36	0:00:04
Prueba 11	1:37:52	1:37:56	0:00:04
Prueba 12	1:38:13	1:38:18	0:00:05
Prueba 13	1:38:33	1:38:37	0:00:04

Prueba 14	1:38:53	1:38:57	0:00:04
Prueba 15	1:39:15	1:39:20	0:00:05
Prueba 16	1:39:35	1:39:39	0:00:04
Prueba 17	1:39:55	1:39:59	0:00:04
Prueba 18	1:40:17	1:40:22	0:00:05
Prueba 19	1:40:37	1:40:42	0:00:05
Prueba 20	1:40:57	1:41:02	0:00:05
Prueba 21	1:41:17	1:41:21	0:00:04
Prueba 22	1:41:38	1:41:42	0:00:04
Prueba 23	1:41:58	1:42:02	0:00:04
Prueba 24	1:42:18	1:42:23	0:00:05
Prueba 25	1:42:40	1:42:44	0:00:04
Prueba 26	1:43:00	1:43:05	0:00:05
Prueba 27	1:43:20	1:43:25	0:00:05
Prueba 28	1:43:40	1:43:44	0:00:04
Prueba 29	1:44:00	1:44:04	0:00:04
Prueba 30	1:44:20	1:44:25	0:00:05
Prueba 31	11:26:45	11:26:50	0:00:05
Prueba 32	11:27:05	11:27:10	0:00:05
Prueba 33	11:27:25	11:27:30	0:00:05
Prueba 34	11:27:46	11:27:50	0:00:04
Prueba 35	11:28:06	11:28:11	0:00:05
Prueba 36	11:28:26	11:28:32	0:00:06
Prueba 37	11:28:48	11:28:53	0:00:05
Prueba 38	11:29:08	11:29:12	0:00:04
Prueba 39	11:29:30	11:29:34	0:00:04
Prueba 40	11:29:50	11:29:55	0:00:05
Prueba 41	11:30:12	11:30:18	0:00:06
Prueba 42	11:30:32	11:30:37	0:00:05
Prueba 43	11:30:53	11:30:58	0:00:05
Prueba 44	11:31:15	11:31:21	0:00:06
Prueba 45	11:31:35	11:31:40	0:00:05
Prueba 46	11:31:55	11:31:59	0:00:04
Prueba 47	11:32:16	11:32:20	0:00:04
Prueba 48	11:32:38	11:32:43	0:00:05
Prueba 49	11:32:58	11:33:02	0:00:04
Prueba 50	11:33:18	11:33:23	0:00:05
TOTAL			0:00:05

Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 57. Clasificación de paquetes en pruebas de ataque Exploración de vulnerabilidades realizadas a Servidor Base de datos mediante el mecanismo Snort.

SNORT BASE DE DATOS				
N° de prueba	Tráfico con ataque Exploración de Vulnerabilidades		Tráfico normal	
	N° de paquetes			
	Detectado como ataque	Detectado como no ataque	Detectado como ataque	Detectado como no ataque
Prueba 01	509	14	8	415
Prueba 02	448	13	8	394
Prueba 03	436	15	0	411
Prueba 04	495	12	7	383
Prueba 05	443	12	0	397
Prueba 06	478	10	6	366
Prueba 07	410	11	6	406
Prueba 08	503	17	0	385
Prueba 09	519	16	8	357
Prueba 10	490	8	6	412
Prueba 11	470	9	0	401
Prueba 12	450	17	8	360
Prueba 13	473	16	0	379
Prueba 14	478	13	5	423
Prueba 15	407	16	5	378
Prueba 16	395	13	8	368
Prueba 17	420	16	0	371
Prueba 18	463	15	5	354
Prueba 19	394	8	5	389
Prueba 20	424	12	2	351
Prueba 21	437	9	4	376
Prueba 22	465	16	0	351
Prueba 23	404	8	4	352
Prueba 24	477	17	8	382
Prueba 25	476	16	5	395
Prueba 26	422	9	2	408
Prueba 27	514	8	8	382
Prueba 28	454	14	3	364
Prueba 29	480	14	2	384
Prueba 30	453	13	7	401
Prueba 31	490	14	1	385

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Prueba 32	428	11	2	429
Prueba 33	535	12	3	450
Prueba 34	422	7	4	386
Prueba 35	441	6	0	336
Prueba 36	494	8	0	401
Prueba 37	453	11	7	482
Prueba 38	472	17	5	421
Prueba 39	560	5	8	305
Prueba 40	508	13	3	413
Prueba 41	539	19	5	470
Prueba 42	429	16	6	475
Prueba 43	495	5	5	465
Prueba 44	445	18	2	324
Prueba 45	428	11	0	307
Prueba 46	459	10	1	334
Prueba 47	419	13	9	393
Prueba 48	548	6	6	424
Prueba 49	506	9	4	318
Prueba 50	524	16	3	406
PROMEDIO	**466**	**12**	**4**	**388**

Fuente: Elaboración propia

Tabla 58. Tiempo de respuesta del mecanismo Snort frente a ataque Exploración de vulnerabilidades de las pruebas realizadas a servidor base de datos.

N° de pruebas	Tiempo inicial de la prueba	Tiempo de reacción del mecanismo	Tiempo de respuesta
Prueba 01	2:14:54	2:14:59	0:00:05
Prueba 02	2:15:15	2:15:19	0:00:04
Prueba 03	2:15:35	2:15:39	0:00:04
Prueba 04	2:15:56	2:16:00	0:00:04
Prueba 05	2:16:16	2:16:20	0:00:04
Prueba 06	2:16:37	2:16:42	0:00:05
Prueba 07	2:16:57	2:17:01	0:00:04
Prueba 08	2:17:17	2:17:21	0:00:04
Prueba 09	2:17:38	2:17:43	0:00:05
Prueba 10	2:17:58	2:18:02	0:00:04
Prueba 11	2:18:18	2:18:22	0:00:04
Prueba 12	2:18:39	2:18:44	0:00:05
Prueba 13	2:18:59	2:19:03	0:00:04

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Prueba 14	2:19:19	2:19:23	0:00:04
Prueba 15	2:19:41	2:19:45	0:00:04
Prueba 16	2:20:01	2:20:05	0:00:04
Prueba 17	2:20:21	2:20:26	0:00:05
Prueba 18	2:20:43	2:20:47	0:00:04
Prueba 19	2:21:03	2:21:07	0:00:04
Prueba 20	2:21:23	2:21:28	0:00:05
Prueba 21	2:21:43	2:21:48	0:00:05
Prueba 22	2:22:04	2:22:09	0:00:05
Prueba 23	2:22:24	2:22:29	0:00:05
Prueba 24	2:22:44	2:22:48	0:00:04
Prueba 25	2:23:06	2:23:11	0:00:05
Prueba 26	2:23:26	2:23:30	0:00:04
Prueba 27	2:23:46	2:23:50	0:00:04
Prueba 28	2:24:06	2:24:11	0:00:05
Prueba 29	2:24:26	2:24:31	0:00:05
Prueba 30	2:24:46	2:24:50	0:00:04
Prueba 31	11:54:29	11:54:34	0:00:05
Prueba 32	11:54:49	11:54:54	0:00:05
Prueba 33	11:55:10	11:55:15	0:00:05
Prueba 34	11:55:30	11:55:34	0:00:04
Prueba 35	11:55:52	11:55:57	0:00:05
Prueba 36	11:56:13	11:56:18	0:00:05
Prueba 37	11:56:33	11:56:39	0:00:06
Prueba 38	11:56:54	11:56:58	0:00:04
Prueba 39	11:57:15	11:57:21	0:00:06
Prueba 40	11:57:35	11:57:40	0:00:05
Prueba 41	11:57:56	11:58:02	0:00:06
Prueba 42	11:58:16	11:58:21	0:00:05
Prueba 43	11:58:38	11:58:43	0:00:05
Prueba 44	11:58:58	11:59:02	0:00:04
Prueba 45	11:59:18	11:59:24	0:00:06
Prueba 46	11:59:39	11:59:44	0:00:05
Prueba 47	11:59:59	12:00:03	0:00:04
Prueba 48	12:00:20	12:00:25	0:00:05
Prueba 49	12:00:40	12:00:46	0:00:06
Prueba 50	12:01:02	12:01:07	0:00:05
TOTAL			0:00:05

Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ANEXO II

Instalación de servidor web

Se inicia la máquina virtual luego se procede a colocar la ISO del sistema operativo, en este caso Ubuntu 16.04 LTS luego de arrancar el sistema operativo nos pide el lenguaje a utilizar en donde seleccionamos español.

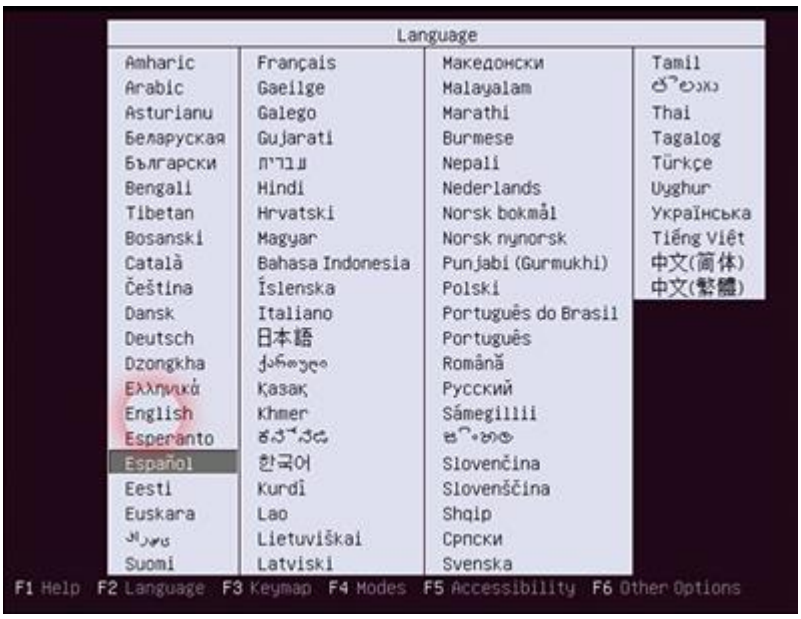


Figura 47. *Configuración de Idioma.*
Fuente: Elaboración propia

Luego de ello se tiene que seleccionar la ubicación: Perú

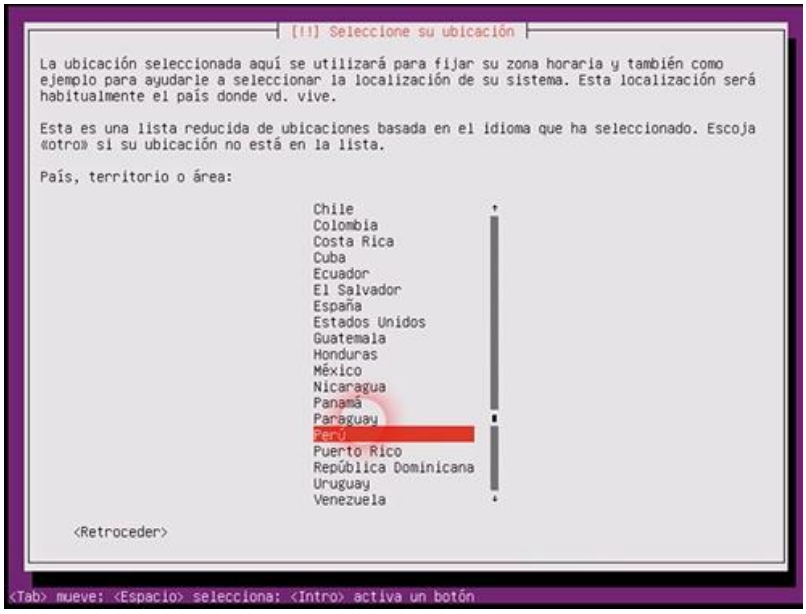


***Figura 48**. Configuración de país.*
Fuente: Elaboración propia.

Posteriormente se configura el teclado, en esta opción se selecciona latinoamericano.

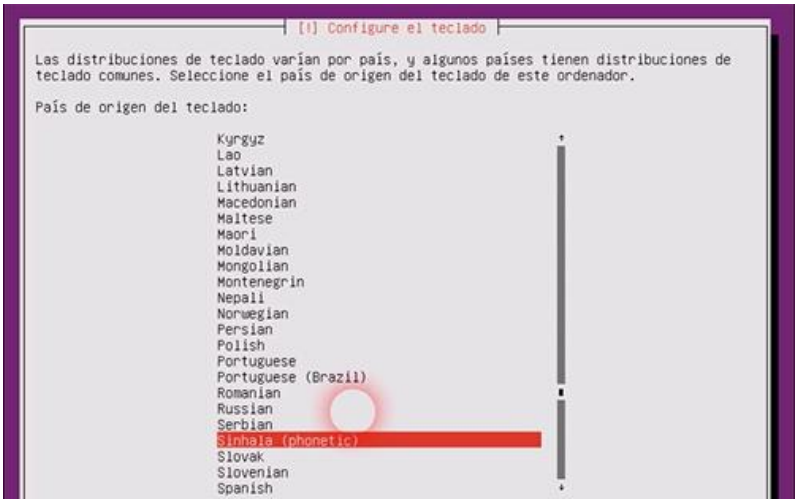


***Figura 49.** Configuración de teclado.*
Fuente: Elaboración propia.

Luego empieza a cargar las configuraciones e intentando conectar a internet.

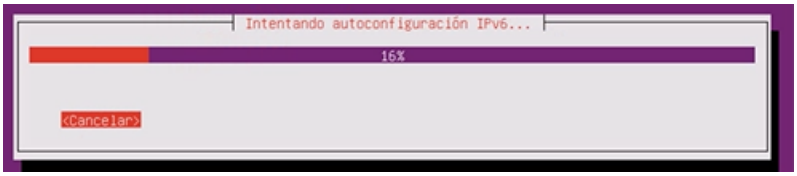


Figura 50. *Carga del sistema.*
Fuente: Elaboración propia.

Cuando no puede configurar automáticamente la dirección ipv4 podemos configurar manualmente introduciendo los siguientes parámetros.

Tabla 59. Direcciones lógicas de Honeynet

Dirección ipv4	192.168.1.6
Mascara de red	255.255.255.0
pasarela	192.168.1.1
Dirección DNS	192.168.1.3
Nombre de maquina	Ubuntu

Fuente: Elaboración propia

Previamente se tiene que seleccionar la opcion: Configurar la red manualmente.

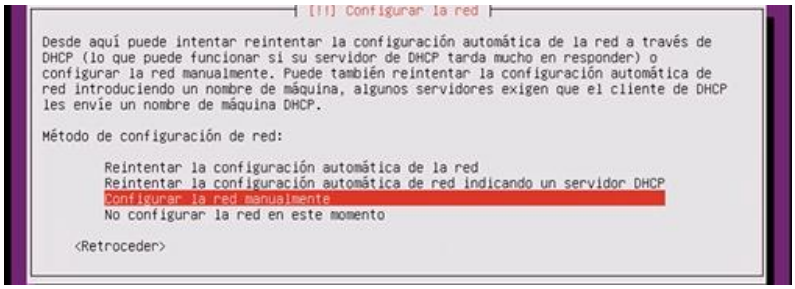


Figura 51. *Configuración de red.*
Fuente: Elaboración propia.

Posteriormente se creará la cuenta de usuario, para ello ingresamos los siguientes parámetros:

usuario	Jaime
password	123456

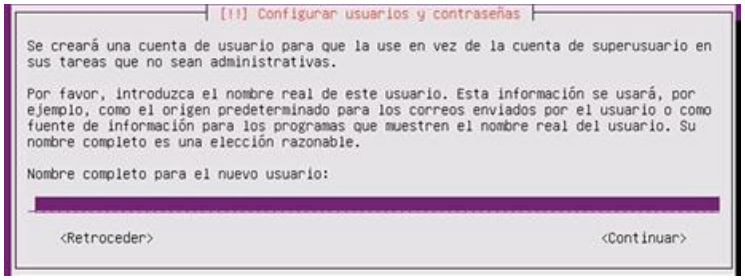


Figura 52. *Configuración de usuario.*
Fuente: Elaboración propia.

El gestor de volúmenes lógicos configura automáticamente las particiones de los discos, para este caso solo se selecciona el disco a formatear.

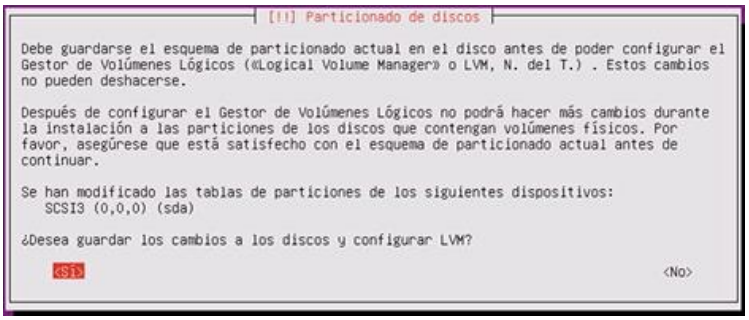


Figura 53. *Partición de discos.*
Fuente: propia.

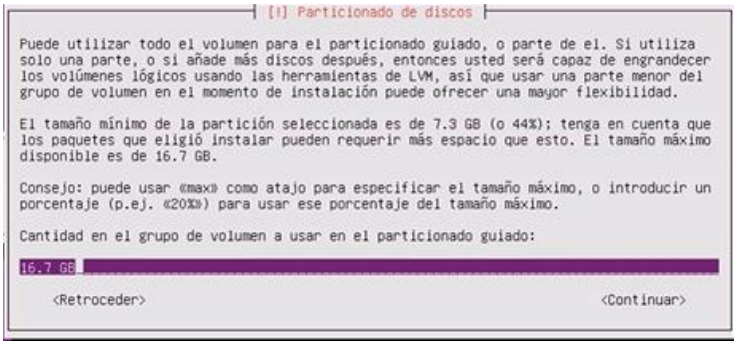


Figura 54. *Partición de discos.*
Fuente: Elaboración propia.

Luego se instala el sistema, la espera puede ser de unos 20 minutos aproximadamente.

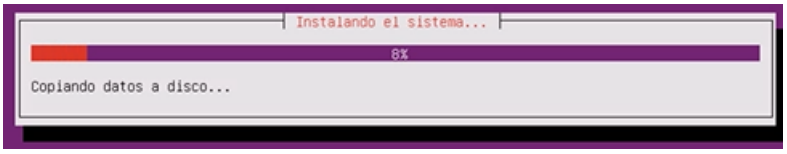


Figura 55. *Instalación de sistema.*
Fuente: Elaboración propia.

Al finalizar la instalación el sistema se reinicia y luego se muestra el escritorio de Ubuntu.

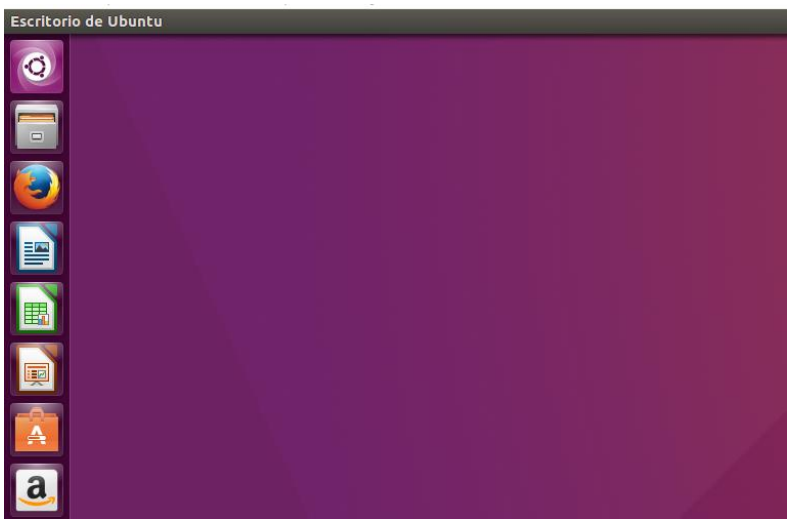


Figura 56. *Pantalla principal.*
Fuente: Elaboración propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ANEXO III

Instalación de Honeywall

Se inicia la máquina virtual con el archivo del sistema operativo, esta es la pantalla de bienvenida.

Figura 57. Imagen de bienvenida Honeynet.
Fuente. Elaboración propia

Se inicia el sistema.

```
Initializing IPsec netlink socket
NET: Registered protocol family 1
NET: Registered protocol family 17
Using IPI No-Shortcut mode
ACPI: (supports S0 S1 S4<6>Time: tsc clocksource has been installed.
 S5)
Freeing unused kernel memory: 232k freed
Write protecting the kernel read-only data: 383k

Greetings.
anaconda installer init version 11.1.2.36 starting
mounting /proc filesystem... done
creating /dev filesystem... done
mounting /dev/pts (unix98 pty) filesystem... done
mounting /sys filesystem... done
input: AT Translated Set 2 keyboard as /class/input/input0
input: ImExPS/2 Generic Explorer Mouse as /class/input/input1
trying to remount root filesystem read write... done
mounting /tmp as ramfs... done
running install...
running /sbin/loader
```

Figura 58: carga del sistema.
Fuente: Elaboración propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

El sistema procede a formatear el disco duro, para poder instalar el honeywall.

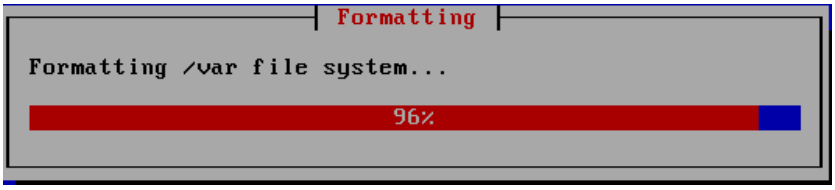


Figura 59: formateo de sistema.
Fuente: Elaboración propia.

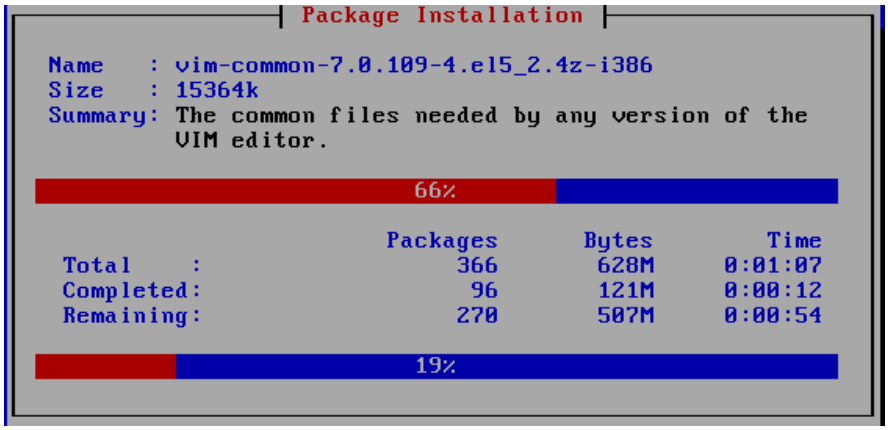


Figura 60: instalación de sistema.
Fuente: Elaboración propia.

Se procede a instalar los paquetes de honeywall.

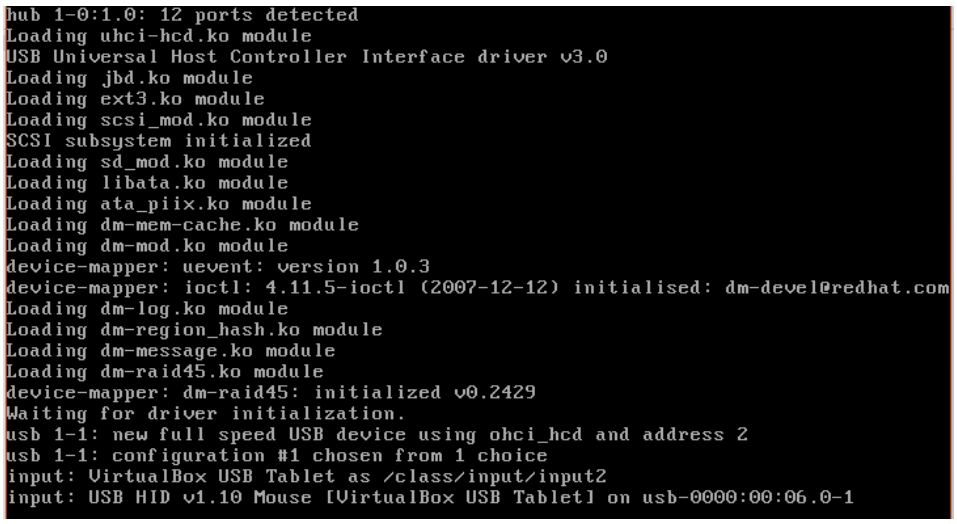


Figura 61: Carga de sistema.
Fuente: Elaboración propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Al terminar la instalación se muestra la pantalla de ingreso, donde el usuario por defecto es:

User	Roo
Password	Honey

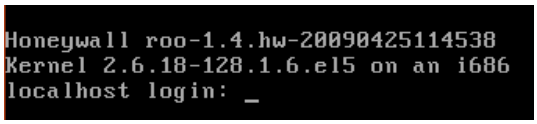


Figura 62: Inicio de sistema.
Fuente: Elaboración propia.

Posteriormente se configure el honeywall, para ello se selecciona la opción 4.

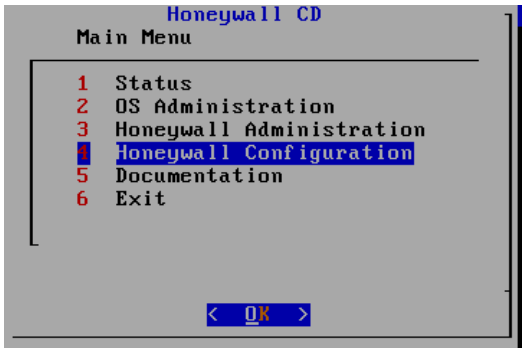


Figura 63: Configuración de sistema.
Fuente: Elaboración propia.

Para realizar la configuración manual se selecciona la opción 3.

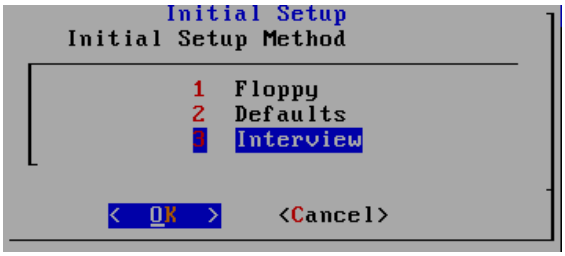


Figura 64: Método inicial.
Fuente: Elaboración propia.

Esta es la pantalla de inicio para la configuración manual donde se tiene que aceptar.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

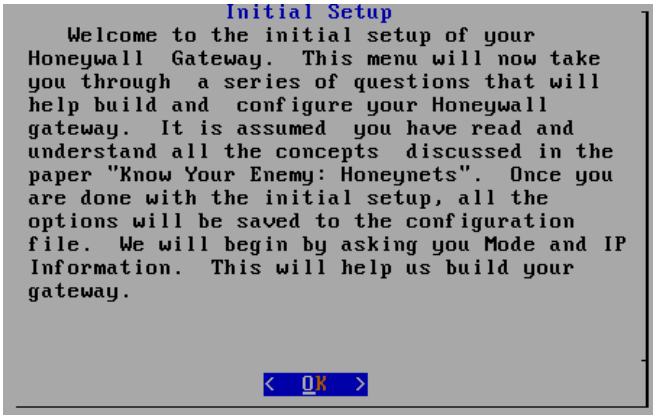


Figura 65: Mensaje de inicio.
Fuente: propia.

Se coloca las direcciones lógicas de los honeypots separados de un espacio.

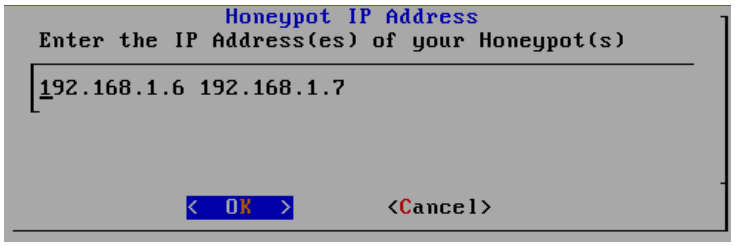


Figura 66: Ingreso de Honeypots.
Fuente: Elaboración propia.

Se inserta la red en la cual el honeywall se encuentra.

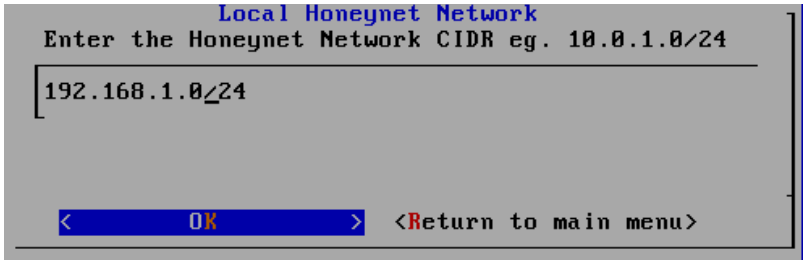


Figura 67. *Ingreso de red.*
Fuente: Elaboración propia.

Automáticamente el sistema encuentra las interfaces eth0 y eth1 para su configuración.

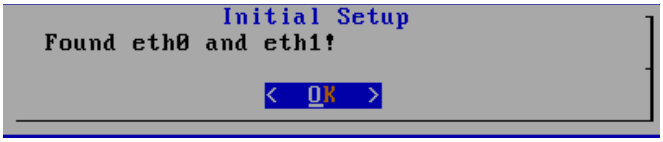


Figura 68. *Búsqueda de interfaces.*
Fuente: Elaboración propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Se agrega el broadcast de la red.

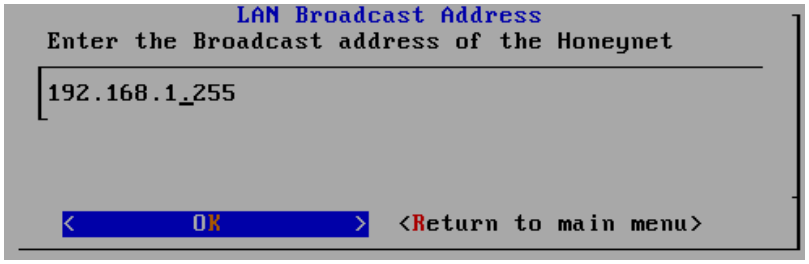


Figura 69. *Broadcast de red.*
Fuente: Elaboración propia.

Luego se configura la interfaz de mantenimiento el cual es la interfaz eth2.

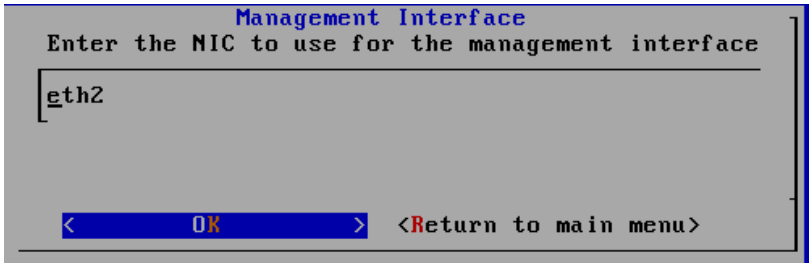


Figura 70. *Nic de la red.*
Fuente: Elaboración propia.

Verifica que dicha interfaz se encuentre habilitada.

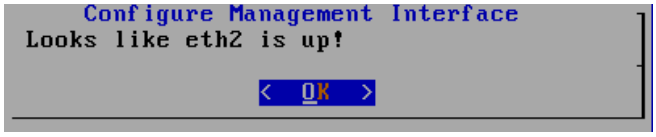


Figura 71. *Mensaje del sistema, de verificación de eth2.*
Fuente: Elaboración propia

Se configura la dirección lógica de la interfaz eth2.

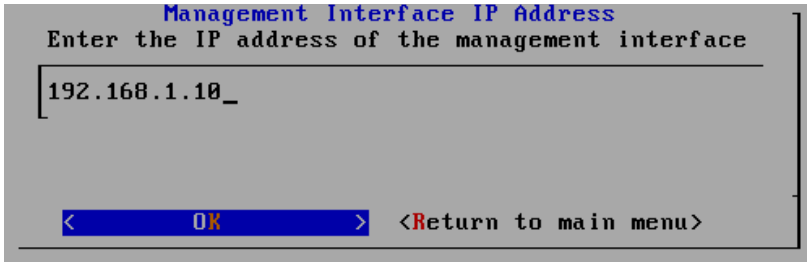


Figura 72. *Configuración de sistema.*
Fuente: Elaboración propia.

Posteriormente se inserta la máscara de red.

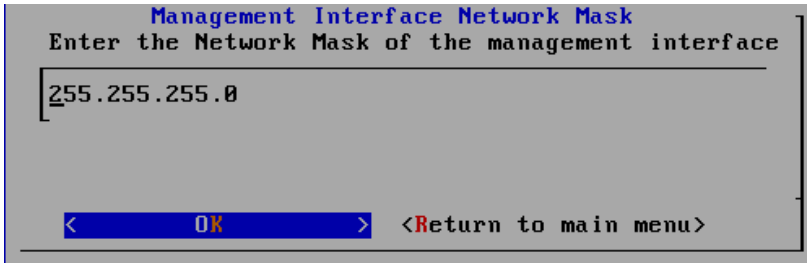


Figura 73. *Configuración de sistema.*
Fuente: Elaboración propia.

Después de ello se inserta el Gateway predeterminado.

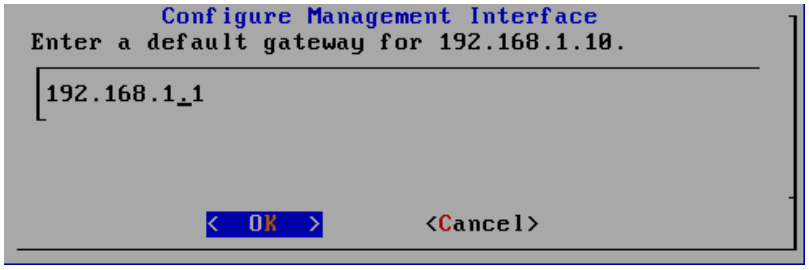


Figura 74. *Configuración de sistema.*
Fuente: Elaboración propia.

Se configura el nombre del sistema, en este caso mantiene el nombre por defecto.

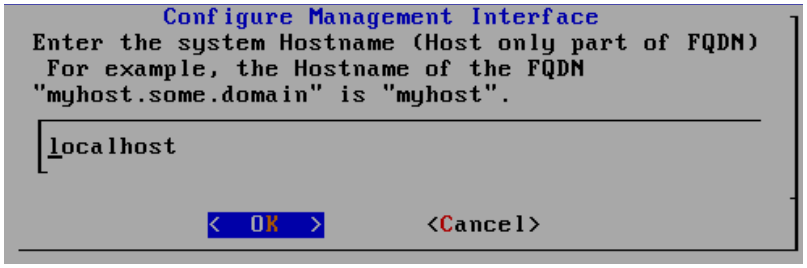


Figura 75. *Configuración de sistema.*
Fuente: Elaboración propia.

Se configura el dominio de la red, en este caso se deja como predeterminado.

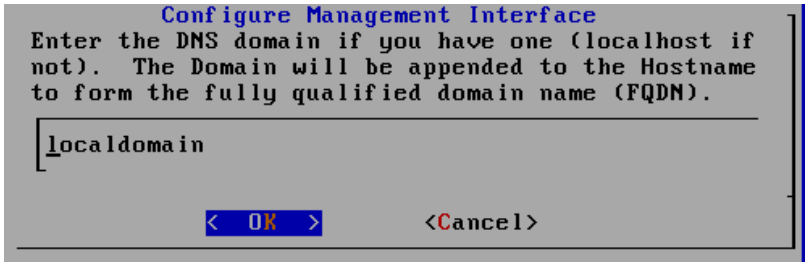


Figura 76. *Configuración de sistema.*
Fuente: Elaboración propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Se ingresa la dirección lógica del DNS.

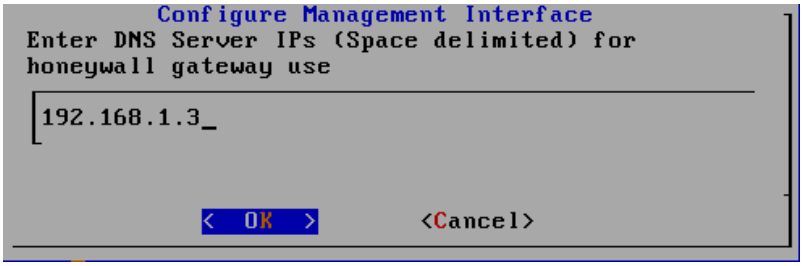


Figura 77. *Configuración de sistema.*
Fuente: Elaboración propia.

Se activa la interfaz recién configurada.

Figura 78. *Configuración de sistema.*
Fuente: Elaboración propia.

Se configura el SSH para un acceso remoto, en este caso no se necesita.

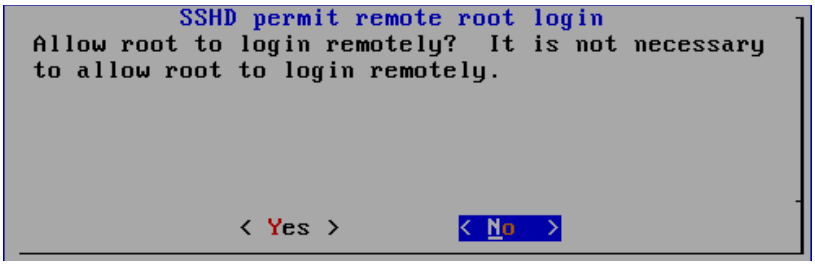


Figura 79. *Configuración de sistema.*
Fuente: Elaboración propia.

Se ingresa el puerto SSHD en este caso se deja como predeterminado.

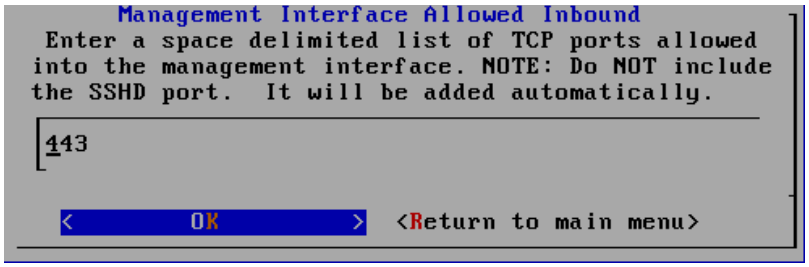


Figura 80. *Configuración de sistema.*
Fuente: Elaboración propia.

Se agrega las direcciones de los dispositivos que pueden acceder mediante SSHD, en este caso ninguno.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

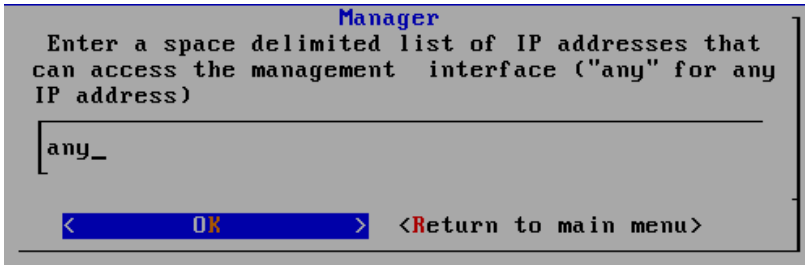


Figura 81. *Configuración de sistema.*
Fuente: Elaboración propia.

Se activa la interfaz web llamada Walleye

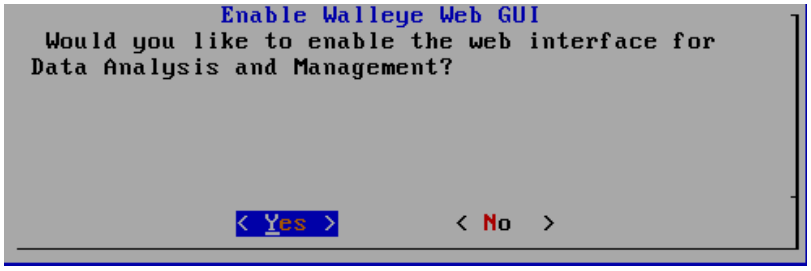


Figura 82. *Configuración de sistema.*
Fuente: Elaboración propia.

Una vez configurado se pasa a la siguiente sección.

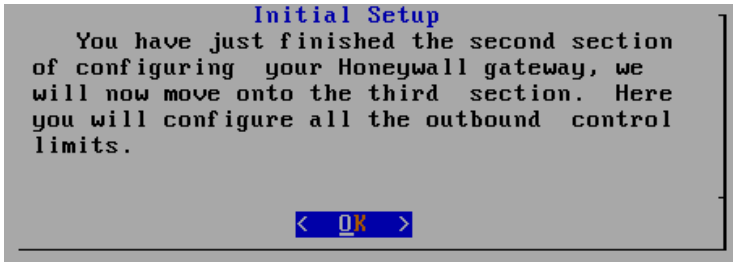


Figura 83. *Configuración de sistema.*
Fuente: Elaboración propia.

En la configuración de conexiones se deja el valor por defecto.

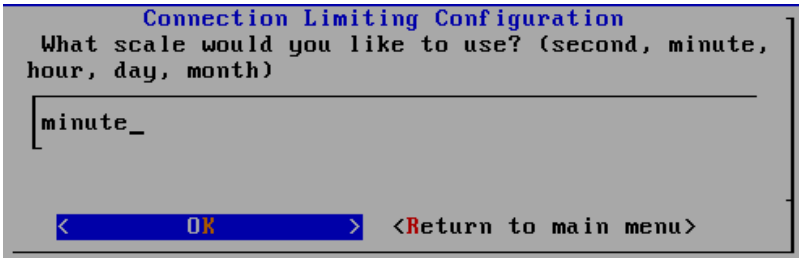


Figura 84. *Configuración de sistema.*
Fuente: Elaboración propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Se ingresa el TCP, en este caso se deja el valor predeterminado.

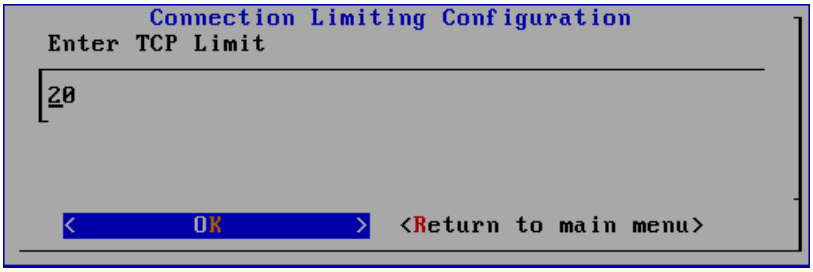


Figura 85. *Configuración de sistema.*
Fuente: Elaboración propia.

Se ingresa el límite de conexiones UDP, este valor se deja como defecto.

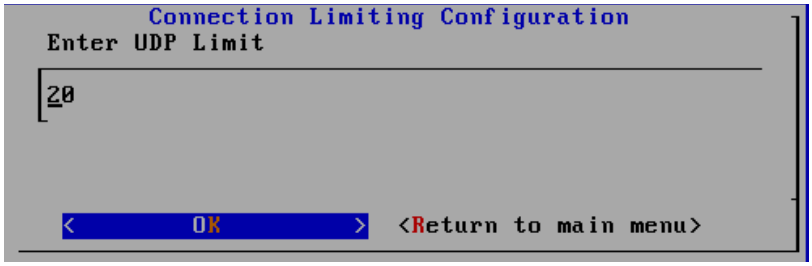


Figura 86. *Configuración de sistema.*
Fuente: Elaboración propia.

Se ingresa el límite de conexiones ICMP, este valor se deja como defecto.

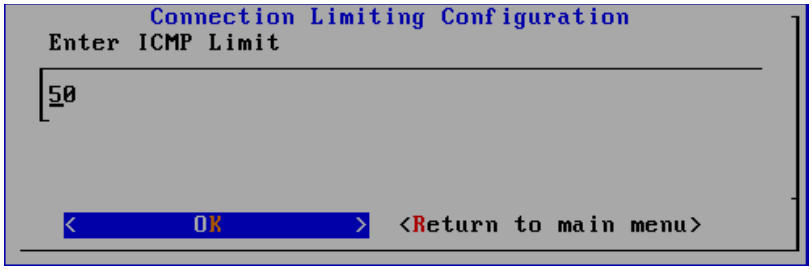


Figura 87. *Configuración de sistema.*
Fuente: Elaboración propia.

Se ingresa el límite de conexiones de los demás protocolos, este valor se deja como defecto.

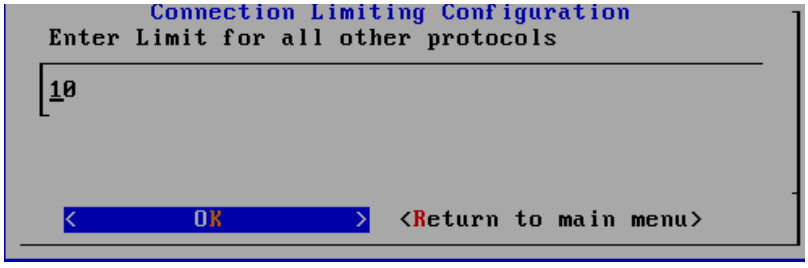


Figura 88. *Configuración de sistema.*
Fuente: Elaboración propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Se configura la lista blanca y negra que es un filtro de direcciones que pueden acceder o no a los honeypots.

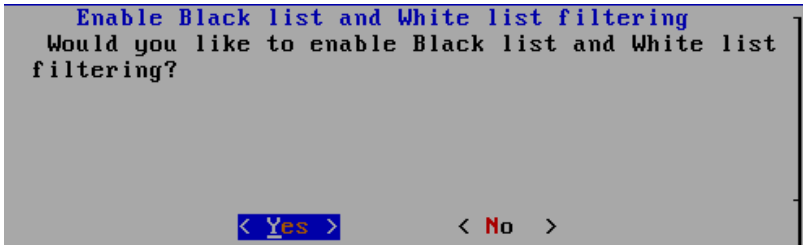


Figura 89. *Configuración de sistema.*
Fuente: Elaboración propia.

Se ingresa la dirección donde se encontrará el archivo de lista de acceso.

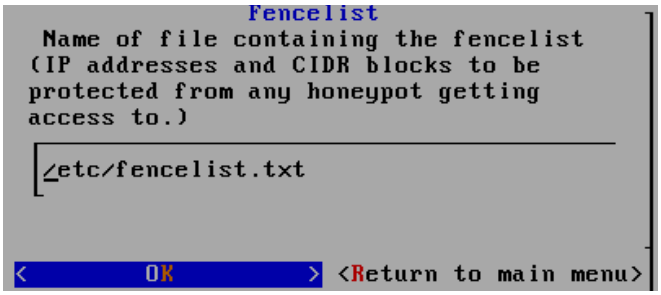


Figura 90. *Configuración de sistema.*
Fuente: Elaboración propia.

Luego ello se pasa a configurar otra seccion del honeywall.

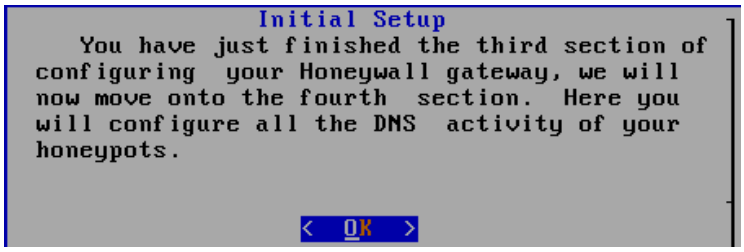


Figura 91. *Configuración de sistema.*
Fuente: Elaboración propia.

Se configura el acceso al servidor DNS por parte de los honeypots, en este caso accedemos el permiso.

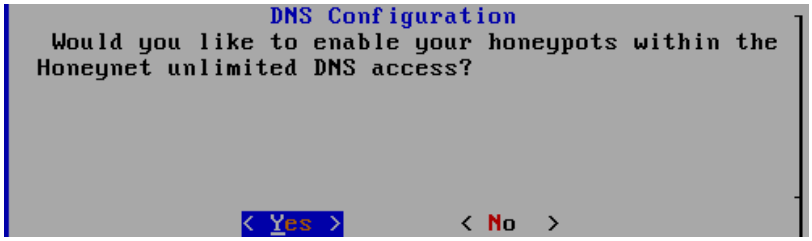


Figura 92. *Configuración de sistema.*
Fuente: Elaboración propia.

Se restringe el acceso a servidores DNS externos.

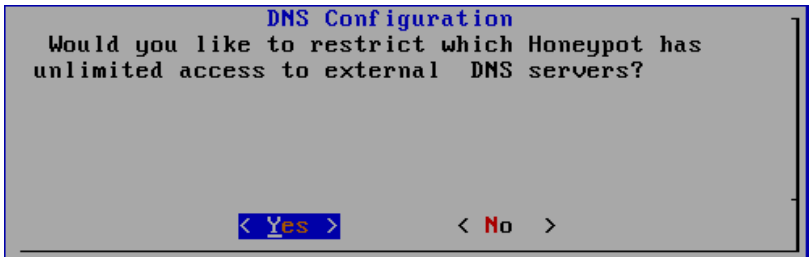


Figura 93. *Configuración de sistema.*
Fuente: Elaboración propia.

Se agrega las direcciones de los honeypots que tienen acceso a servidores DNS externos.

Figura 94. *Configuración del sistema.*
Fuente: Elaboración propia.

Se agrega los servidores DNS que usaran los Honeypots separados por un espacio

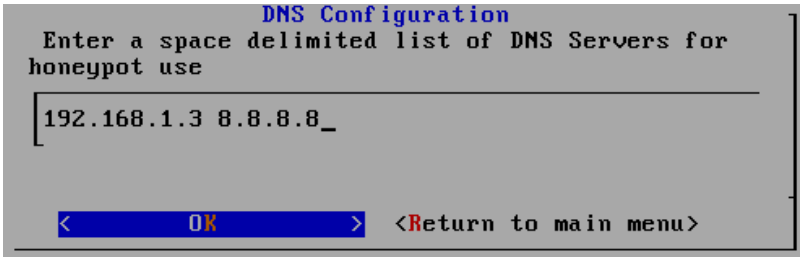


Figura 95. *Configuración de sistema.*
Fuente: Elaboración propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Una vez culminado se procede a configurar el Sebek que es un acceso remoto a los datos recolectados por el honeywall.

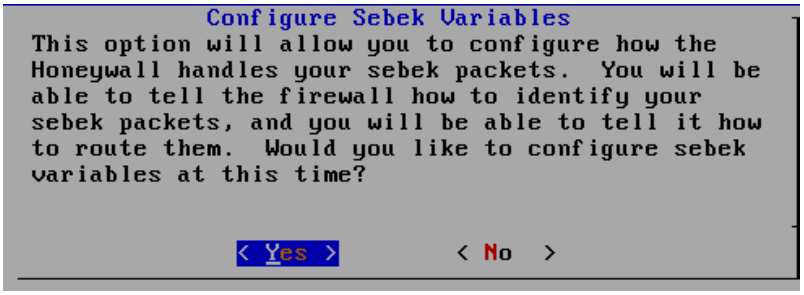


Figura 96. *Configuración de sistema.*
Fuente: Elaboración propia.

Se configura la dirección del dispositivo que administrará el honeywall.

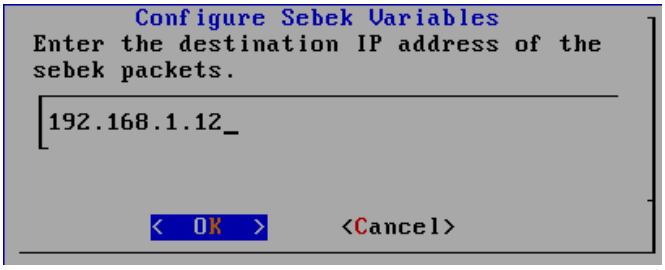


Figura 97. *Configuración de sistema.*
Fuente: Elaboración propia.

Se configura el puerto UDP por el que el sebek podra recibir los paquetes.

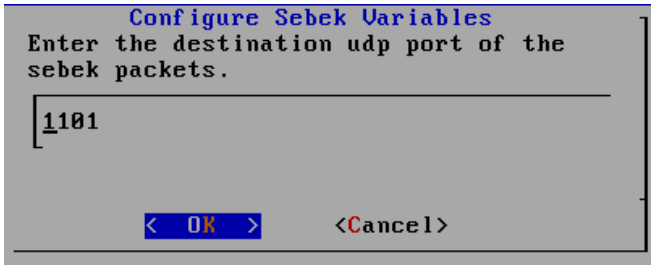


Figura 98*. Configuración de sistema.*
Fuente: Elaboración propia.

Se confirma la configuración de Sebek.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

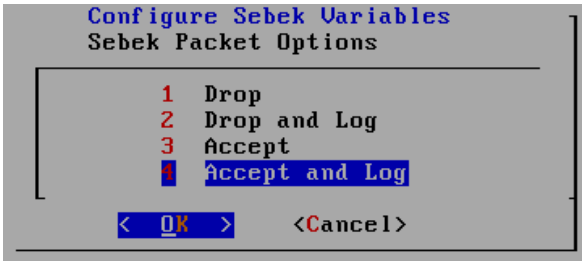


Figura 99. *Configuración de sistema.*
Fuente: Elaboración propia.

Se finaliza la configuración.

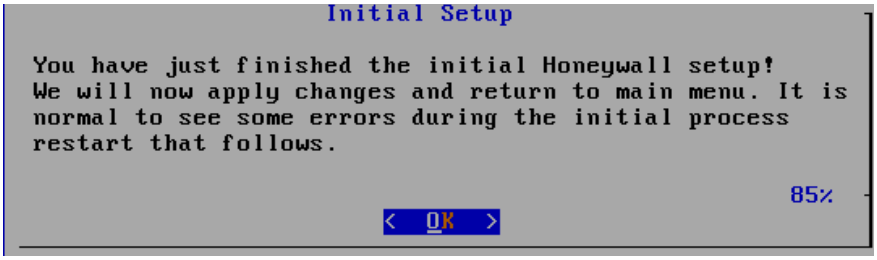


Figura 100. *Configuración de sistema.*
Fuente: Elaboración propia.

Se ingresa desde otro dispositivo (Windows 10) con IP 192.168.1.12/24 hacia https://192.168.1.10

Figura 101. *Configuración de sistema.*
Fuente: Elaboración propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ANEXO IV

Instalación de Snort

Una vez instalado el sistema operativo Kali y configurado las interfaces de red se ingresa a la consola de comandos. Luego de ello se escribe el siguiente comando para la descarga de Snort.

```
root@kali:~# apt-get install snort
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libdaq2 oinkmaster snort-common snort-common-libraries snort-rules-default
Paquetes sugeridos:
  snort-doc
Se instalarán los siguientes paquetes NUEVOS:
  libdaq2 oinkmaster snort snort-common snort-common-libraries
  snort-rules-default
0 actualizados, 6 nuevos se instalarán, 0 para eliminar y 4 no actualizados.
Se necesita descargar 2.230 kB de archivos.
Se utilizarán 7.325 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

Figura 102. *Instalación de sistema.*
Fuente: Elaboración propia

Una vez instalado se procede a configurar, inicialmente Snort solicita la dirección de la red en la que estará conectada.

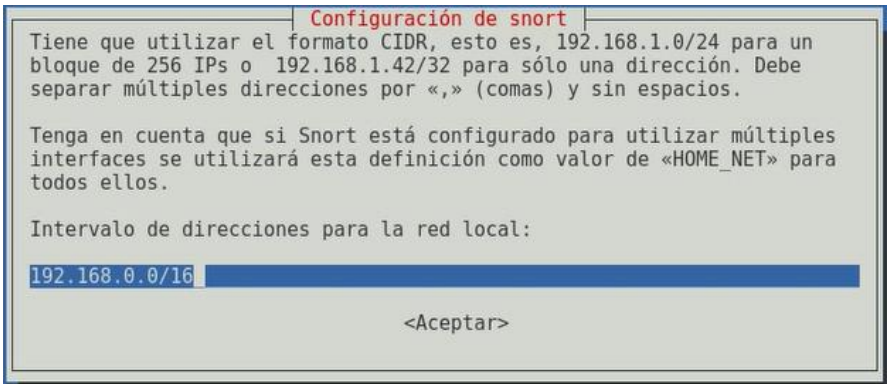


Figura 103. *Configuración de la red en Snort.*
Fuente: Elaboración propia

Luego de ello se procede a reiniciar Snort

```
root@kali:~# sudo dpkg-reconfigure sn
sniffjoke               snmpd                   snort-common-libraries
snmp                    snort                   snort-rules-default
snmpcheck               snort-common
root@kali:~# sudo dpkg-reconfigure snort
[ ok ] Stopping snort (via systemctl): snort.service.
root@kali:~# sudo /etc/init.
```

Figura 104. *Reiniciar Snort. Fuente:*
Elaboración propia

Luego de comprobar que la ejecución es correcta se verifica la versión de Snort.

Figura 105. *Comprobación de instalación de Snort.*
Fuente: Elaboración propia

Para analizar la red en tiempo real se ingresa al programa Wireshark que viene instalado en Kali

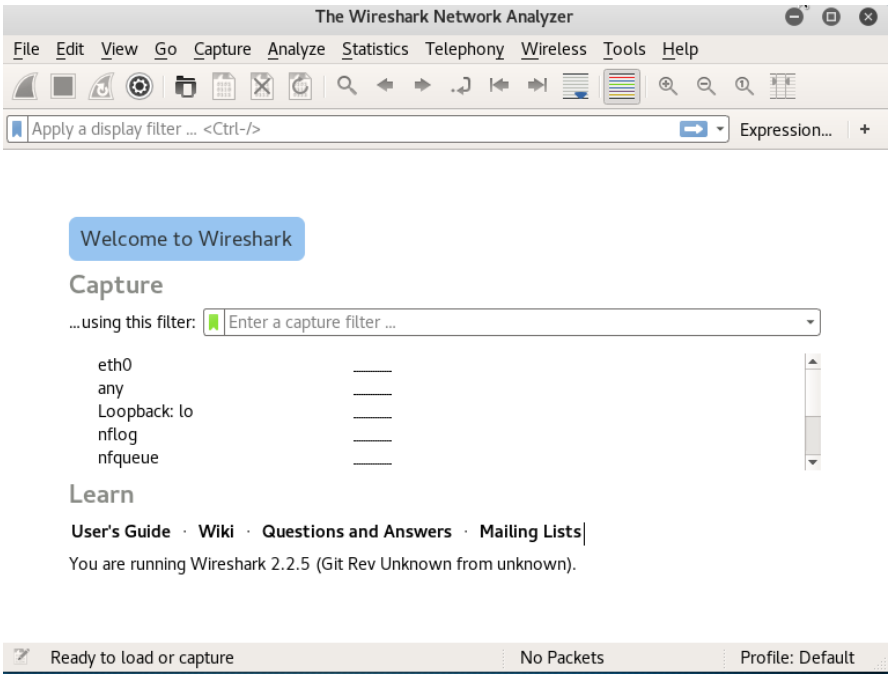


Figura 106. *Wireshark.*
Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ANEXO V

Instalación de Kali

Se inicia la máquina virtual luego se procede a colocar la ISO del sistema operativo, en este caso Kali luego de arrancar el sistema operativo nos pide el lenguaje a utilizar en donde seleccionamos español.

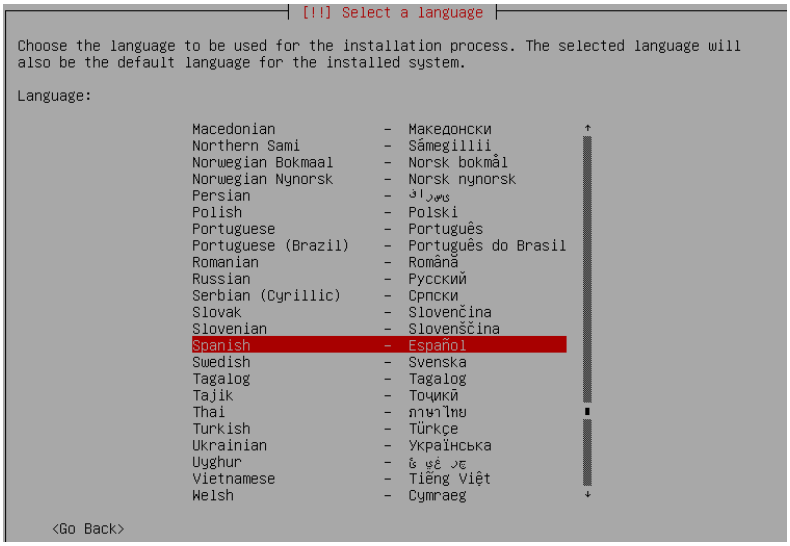


Figura 107. *Configuración de idioma.*
Fuente: Elaboración propia

Seleccionamos la ubicación para fijar la zona horaria.

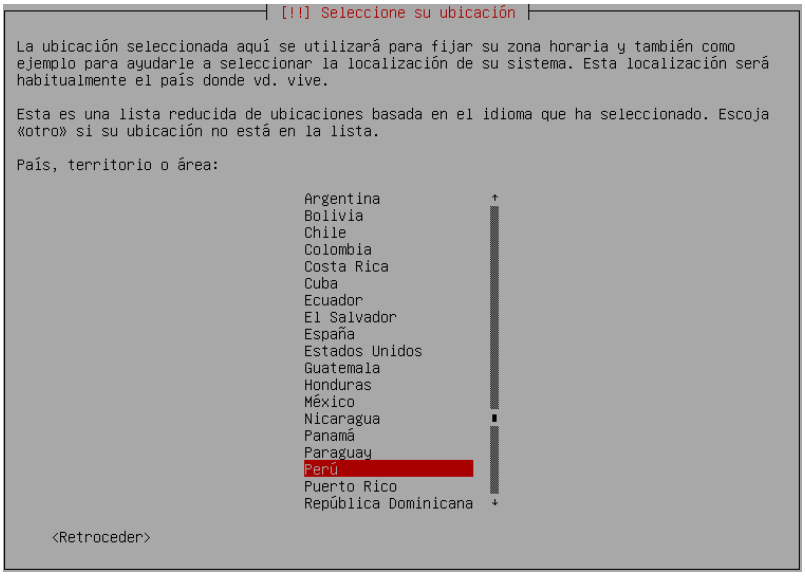


Figura 108*. Configuración de país.*
Fuente: Elaboración propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Seleccionamos el tipo de teclado.

Figura 109. *Configuración de teclado.*
Fuente: propia.

Se observa la carga de algunos componentes adicionales.

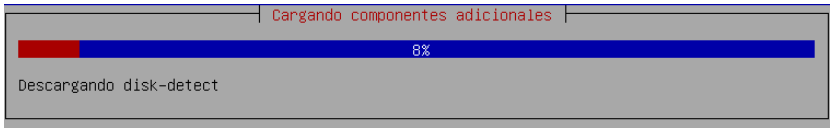


Figura 110. *Carga del sistema.*
Fuente: Elaboración propia.

Posteriormente se configura la red, para ello se ingresa el nombre de la máquina.

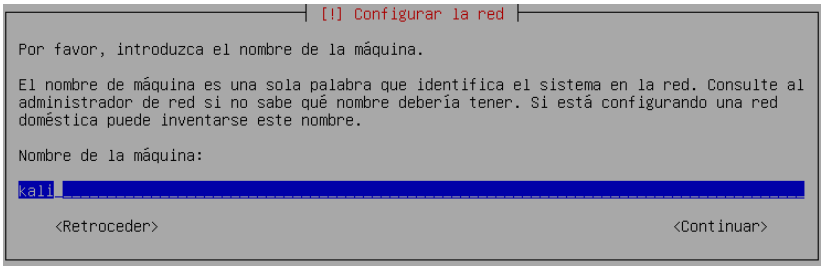


Figura 111. *Configuración de red.*
Fuente: Elaboración propia.

Se ingresa la contraseña del superusuario.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

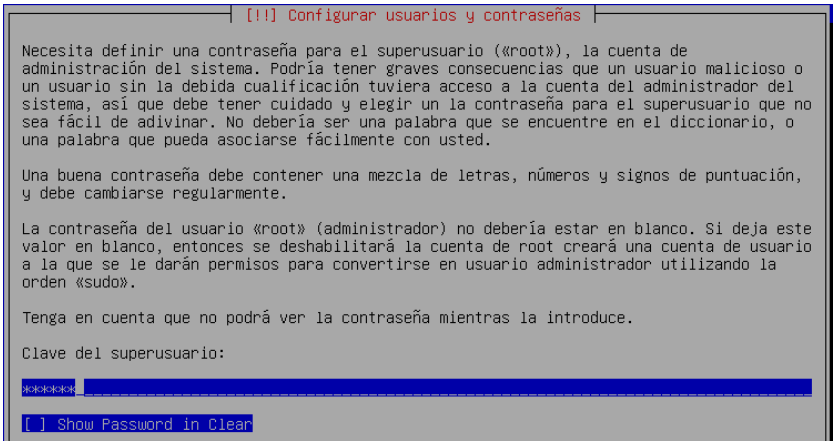


Figura 112. *Configuración de usuarios.*
Fuente: Elaboración propia.

Se vuelve a ingresar la contraseña para su verificación.

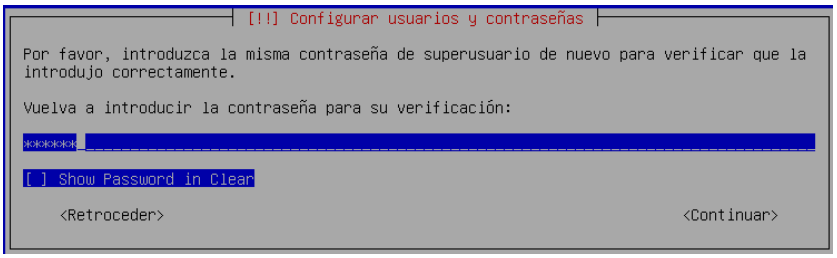


Figura 113. *Configuración de usuarios.*
Fuente: Elaboración propia.

Se observa la carga del sistema.

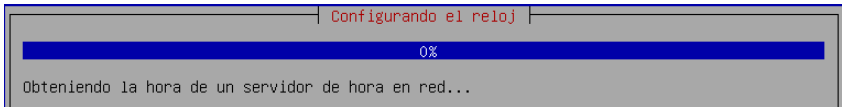


Figura 114. *Carga del sistema.*
Fuente: Elaboración propia.

Seleccionamos el método de particionado.

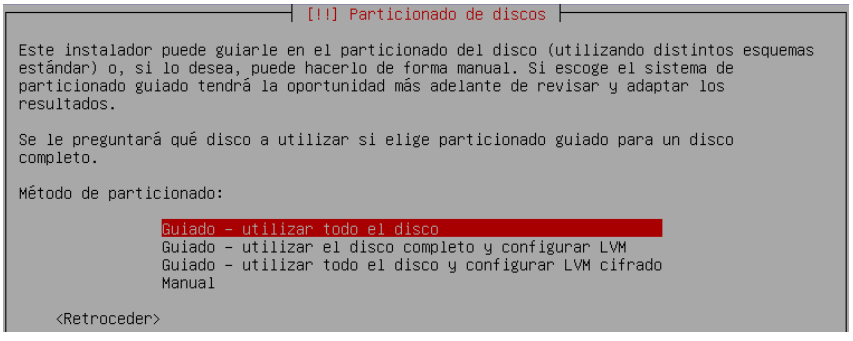


Figura 115. *Configuración de partición.*
Fuente: Elaboración propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Seleccionamos el esquema de la partición.

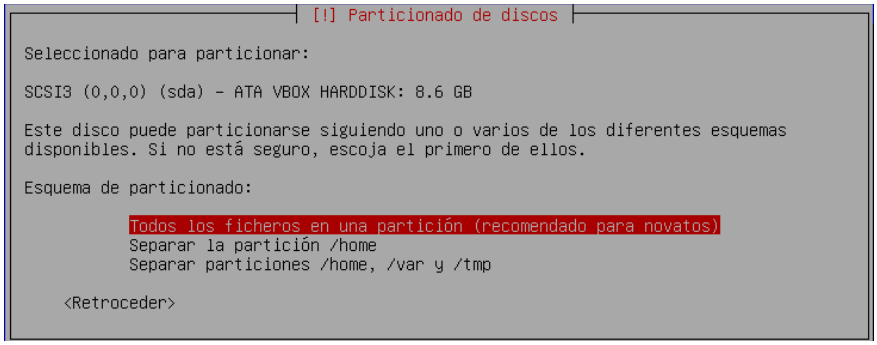


Figura 116. *Configuración de partición.*
Fuente: propia.

Se observa la instalación del sistema.

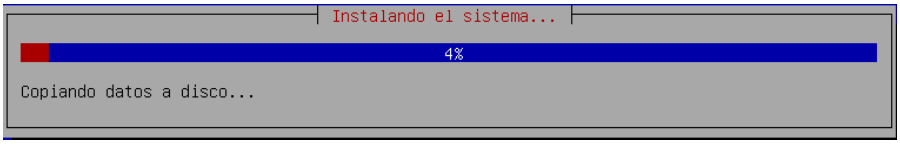


Figura 117. *Carga del sistema.*
Fuente: Elaboración propia.

Se selecciona la instalación del cargador de arranque.

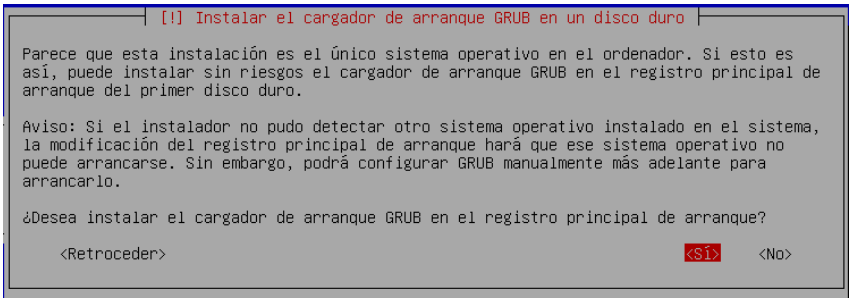


Figura 118. *Instalación de cargador.*
Fuente: Elaboración propia.

Se observa la instalación del arranque GRUB.

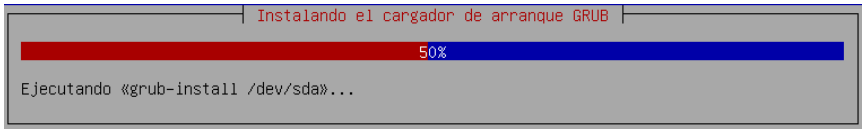


Figura 119. *Carga del sistema.*
Fuente: Elaboración propia.

Se observa un mensaje de la instalación completada.

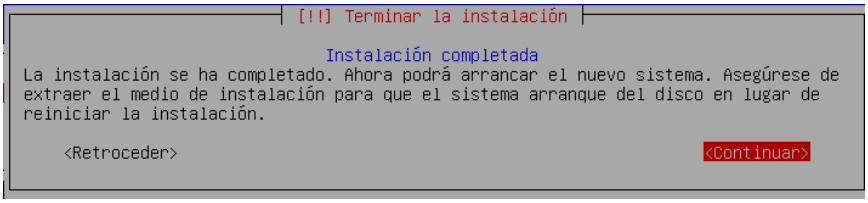


Figura 120. *Mensaje final.*
Fuente: Elaboración propia.

Luego de reiniciar el sistema se observa la pantalla principal.

Figura 121. *Pantalla principal.*
Fuente: Elaboración propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe