UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERIA

CARRERA DE SISTEMAS Y COMPUTACIÓN

Proyecto de Investigación previo a la obtención del título de Ingeniero en Sistemas y Computación.

TRABAJO DE TITULACIÓN

"IMPLANTACIÓN DE UN APLICATIVO PARA OPTIMIZAR LA GESTIÓN CENTRALIZADA DE LOGS EN UN AMBIENTE HONEYNET EN EL DATACENTER UNACH"

Autor:

BRYAM FABRICIO YUCTA SILVA

Tutor:

ING. DANNY VELASCO

Riobamba - Ecuador
Año 2019

PÁGINA DE REVISIÓN

PÁGINA DE REVISIÓN

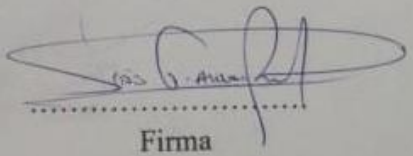
Los miembros del Tribunal de Graduación del proyecto de investigación de título: "Implantación de un aplicativo para optimizar la gestión centralizada de logs en un ambiente honeynet en el Datacenter UNACH". **Caso Práctico:** Sistema informático para el Datacenter de la Universidad Nacional de Chimborazo", presentado por el estudiante: Sr. Bryam Fabricio Yucta Silva, dirigido por: MsC. Danny Velasco.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en el cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:

MsC. Danny Velasco
Tutor del Proyecto

.....
Firma



MsC. Gonzalo Allauca
Miembro del Tribunal

.....
Firma

MsC. Marlon Silva
Miembro del Tribunal

.....
Firma

AUTORÍA DE LA INVESTIGACIÓN

AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad del contenido de este Proyecto de Graduación corresponde exclusivamente al Sr. Bryam Fabricio Yucta Silva autor del proyecto de investigación y al MsC. Danny Velasco, Director de Tesis y al patrimonio intelectual de la Universidad Nacional de Chimborazo.

Autor:

……..
Bryam Fabricio Yucta Silva
C.I. 060412486-7

Director del proyecto:

……
MsC. Danny Velasco

.

DEDICATORIA

El presente proyecto de investigación está dedicado principalmente a Dios, por haberme dado la salud y permitirme haber llegado hasta este momento tan importante de formación profesional, a mis padres Cesar y Carolina a mi hermana Jennifer quienes son el pilar fundamental en cada logro de mi vida, que con sus consejos me supieron orientar por el sendero de la superación y quienes me brindaron el apoyo incondicional, a los docentes de la Carrera de Sistemas y Computación, quienes me apoyaron día a día en la formación académica para llegar a ser profesionales de calidad, a mi tutor de Tesis el MsC. Danny Velasco por apoyarme con sus conocimientos obtenidos en su vida profesional para lograr el desarrollo del presente proyecto.

Bryam Fabricio Yucta Silva

AGRADECIMIENTO

Agradezco a Dios, por su infinito amor y permitirme concluir una etapa más en mi vida, agradezco a mi familia y seres queridos, por brindarme siempre su apoyo incondicional en cada paso que he dado, por darme la fortaleza para seguir siempre adelante, y en especial por darme la oportunidad de ser una excelente profesional.

Agradezco al Ing. Danny Velasco por brindarme su apoyarme en calidad de tutor de tesis, y haber impartido sus conocimientos para poder desarrollar un producto de calidad y apoyarme en la culminación de este presente proyecto de Investigación.

A los docentes de nuestra querida carrera por todas sus enseñanzas a lo largo de toda nuestra vida universitaria, a mis queridos amigos por la ayuda desinteresada brindada en cada obstáculo que en nuestra vida se presentó, gracias por el apoyo y los deseos de superación,

Bryam Fabricio Yucta Silva

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

RESUMEN

El presente proyecto de investigación trata sobre el despliegue de un aplicativo para la centralización de log, en la Universidad Nacional de Chimborazo, bajo la tecnología conocida como honeynet, herramienta que simula servicios y aplicaciones vulnerables, llamados honeypots de tal forma que atraiga atacantes, con el objetivo de capturar información de sus actividades en la red.

La honeynet, en su configuración, posee módulos de control y captura, que facilitan el análisis de los datos relacionados con los posibles intentos de accesos y actividades maliciosas llevadas a cabo dentro de ellas. El análisis de la información capturada servirá para determinar patrones de conexión que permita en desarrollos posteriores, identificar ataques, identificar servicios vulnerables o susceptibles a ataques, etc.

La investigación se lo realizo en un ambiente simulado en el cual se implanto la honeynet, así como los honeypot y como aplicativo de centralización Walleye, el cual es una interfaz web basada en GUI, encarga de guardar toda la información, ejecutando un servidor web al que se comunica de forma remota a través de una conexión SSL, en dicha interfaz se verá toda la información receptada y centralizada de la honeynet.

De acuerdo con los resultados obtenidos se optimizó el tiempo al momento de leer los datos en una sola interfaz, se disminuyó los procesos al analizar los archivos log, ya que se encuentran en un solo computador de manera centralizada.

PALABRAS CLAVES: Optimizar, honeypot, honeynet, log, honeywall, walleye

SUMMARY

ABSTRACT

This research deals with the deployment of an application for the centralization of information, at the Universidad Nacional de Chimborazo, under the technology known as honeynet, a tool that simulates vulnerable services and applications, called honeypots and thus attract attackers, with the aim of capturing information from their activities on the network.

The honeynet, in its configuration has control and capture modules that facilitate the analysis of data related to possible access attempts and malicious activities carried out within them. The analysis of the captured information will be used to determine connection patterns that will allow subsequent attacks, identify attacks, identify vulnerable services or susceptible to attacks, etc.

The research was made in a simulated environment in which the honeynet was implanted, as well as the honeypot and as a Walleye centralization application, which is a web interface based on GUI, responsible for storing all information, running a web server to which it communicates remotely through an SSL connection, this interface will see all the information received and centralized honeynet.

According to the results obtained, the time was optimized at the moment of reading the data in a single interface, the use of procreator and memory was reduced when analyzing all the data in a single computer in a centralized way, in addition, the management time of the tools incorporated in the honeynet was reduced.

KEY WORDS: Optimize, honeypot, honeynet, log, honeywall, walleye

Reviewed by Guerra, Mónica
Language Center Teacher

INTRODUCCIÓN

Las redes de datos en general son un medio de comunicación electrónico muy común en la actualidad y a medida que estas redes, aplicaciones y en particular el internet crece, también crece las posibilidades de vulnerabilidad lo que implica riesgos de ataques, esto se traduce en el daño y la pérdida que generan dichas amenazas.

En la actualidad existen herramientas y mecanismos de defensa que son usados en las redes de computadoras tales como, Firewalls, Sistemas de Detección de Intrusos (Intrusion Detection System IDS), Lista de Control de Accesos (Acces Control List ACL). Análisis realizados determinan que el problema con los mecanismos mencionados anteriormente radica es que, muchas veces no están configurados de manera correcta y generan una falsa sensación de seguridad. (Estrella Quijije, 2011)

La gestión centralizada de riesgos es un tema que se ha desarrollado en el último tiempo con la evolución de las Tecnologías de la Información, a pesar de que ha tenido una investigación por instituciones internacionales, no ha sido tan valorada como una solución de apoyo a la administración. El auge y la importancia que ha obtenido la seguridad de la información permite el desarrollo de nuevas tecnologías que impulsan y renuevan el desarrollo en la gestión centralizada de logs. (Avella Coronado, 2005)

Se implementa una honeynet en la red de datos de la Universidad Nacional de Chimborazo la cual se define como un conjunto de honeypot, que simula una red productiva, también se contará con la herramienta (Sebek), esta herramienta se encarga de vigilar cierto tipo de información que circula por la red, la cual emite una alerta al administrador de red en caso de alguna anomalía.

El objetivo primordial del proyecto de investigación es implementar una aplicación la cual se encarga de centralizar los archivos “logs” de la herramienta implementada en la honeynet, así como del firewall, que permita la toma adecuada de decisiones en un corto tiempo durante la gestión de la red de datos de la Universidad Nacional de Chimborazo.

1. CAPÍTULO I.

1.1 Problema

El creciente uso de redes de datos en todas en los últimos tiempos, así como la existencia de las vulnerabilidades en sistemas y aplicaciones, han constituido desde hace mucho tiempo el factor principal para el uso de métodos que proporcionen seguridad en las redes. Hay que considerar que en la actualidad el aumento del ancho de banda y el fácil acceso a la red, ha contribuido a una evolución en las técnicas de ataques, genera cambios en los escenarios típicos que producen amenazas para cualquier sistema conectado a una red.

En el entorno de la seguridad de redes existen mecanismos de defensa contra los ataques e intrusiones, que al trabaja en combinación con otras herramientas trata de reducir el impacto, el problema con dichos mecanismos es, que guardan demasiada información llamados log y al tener más de una herramienta, no se puede revisar la información al mismo tiempo es por ello la importancia de una centralización de log.

La Universidad Nacional de Chimborazo no dispone de un sistema centralizado de log, lo cual impide tener información detalla de las herramientas implementadas en la honeynet, así como lo servicios vulnerables ante un ataque, por lo cual se plantea la automatización del problema, con la implantación de una aplicación la cual tendrá la información clasificada de cada una de las herramientas implementadas en la honeynet, de esta forma al mostrar la información para una toma adecuada de decisiones. (Anexo 1)

1.2 Justificación

La infraestructura de gestión de logs varía de acuerdo con la cantidad de fuentes de datos integrados en el proceso y la cantidad de logs que estos generan, debido a esto, es importante en el diseño e implementación de la infraestructura, tener en cuenta los recursos necesarios para cumplir los objetivos del proceso, por tal motivo cada organización no puede imitar o guiarse por la infraestructura de otras organizaciones. (López Cruces, 2016)

Es necesario un servidor de registro central de log con las medidas de seguridad adecuadas. Con una buena planificación y una implementación rigurosa de configuraciones seguras, de tal forma se pueda proteger su red, dispositivos y la información. (Anusooya R, 2015)

La Universidad Nacional de Chimborazo ha adoptado por la centralización de log, que permita optimizar el tiempo y una tomar la mejor decisión al analizar los dato, con la honeynet se tendrá un sistema simulado de la red productiva, de esta forma se obtendrá la información a centralizar, con la implantación del aplicativo “walleye” se revisará la información de los archivos log de una forma organizada, centralizada y en una sola interfaz.

1.3 Objetivos

1.3.1 Objetivo General

Optimizar la gestión centralizada de logs en un ambiente honeynet mediante la implantación de un aplicativo en el Datacenter de la UNACH.

1.3.2 Objetivos Específicos

- Realizar un estudio de la herramienta Sebek implementada en la honeynet, así como la información receptada por el honeynet.
- Despliegue de la aplicación que permite la centralización de logs.
- Clasificar la información emitida por las herramientas para establecer un formato centralizado.
- Análisis de Resultados.

2. CAPÍTULO II

2.1 Marco Teórico

En este capítulo se presenta la fundamentación teórica necesaria para la elaboración del proyecto propuesto. Se describen en que consiste el diseño y la implantación del aplicativo que ayudara a optimizar la gestión centralizada de log en el Data Center de la Universidad Nacional de Chimborazo, así como el funcionamiento Honeynet.

2.2 HONEYNET

2.2.1 Definición

Antes de analizar el concepto de una Honeynet es preciso definir que es un Honeypot.

Se denomina honeypot al recurso de red destinado a ser atacado o comprometido con la finalidad de identificar, enviar y en cierta media, neutralizar los intentos de secuestrar sistemas y rede de información. (Honeynet UTPL,2011)

Puede considerarse como falso servidores posicionados en lugares estratégicos de una red de prueba, con información que parece ser valiosa para los intrusos. Se los configura de tal manera que se dificulte, pero que no sea imposible romper su seguridad, exponiéndolos deliberadamente y haciéndolos muy atractivos para hackers en busca de un objetivo.

Esta arquitectura crea una red altamente controlada, en la que se puede controlar y monitorear todo tipo de actividad de sistema y red. Los honeypots se colocan dentro de esta red. Una redecilla básica se compone de honeypots colocados detrás de una puerta de entrada transparente: el honeywall. Actúa como una puerta de enlace transparente, los intrusos no pueden detectar al honeywall y cumplen su función de registrar toda la actividad de la red que entra o sale de los honeypots. (Abbasi, 2010)

Las ventajas de la Honeynet son que, dado que cualquier tráfico que pasa por ella es ilegitimo por naturaleza, permite reducir el número de falsos positivos. Además, permite detectar nuevos tipos de ataques y entregar una notificación temprana de os incidentes. (Proyect H, 2016)

2.2.2 Uso de la Honeynet

La Honeynet provee la estrategia de detectar fallos y mejorar en la defensa, se usa en conjunto con otros mecanismos de seguridad. Al recoger información de las intrusiones y estudiarlas para

conocer nuevas amenazas y herramientas aun no documentadas, determina así patrones de ataques y los diferentes motivos de los intrusos. Pueden comprobar y desarrollar la capacidad de respuesta ante cualquier incidente.

En las universidades pueden ser usadas para estudiar tipos y patrones de ataques o simplemente para investigar amenazas como función principal. (Project T. H., 2007)

2.2.3 Arquitectura de la Honeynet

Una arquitectura es el diseño conceptual y la estructura operacional fundamental de un sistema. Es decir, es un modelo y una descripción funcional de los requerimientos y la implementación de diseño para los diferentes elementos que conforma una Honeynet.

La Honeynet no es un producto, es toda una arquitectura, una red con un ambiente totalmente controlado, es como una pecera con servicios, routers, computadoras personales, y todos los elementos de una red común, de esta forma los atacantes ingresan a dicha red y al realizar su trabajo sin darse cuenta permiten conocer patrones de ataques.

Para crear una arquitectura correctamente el Honeynet Proyect ha definido unos requisitos que garantiza el correcto funcionamiento y mantener un ambiente seguro para los sistemas contiguos a la red. Estos equipos son:

a) **Data Control**: El control de datos es la contención de la actividad dentro de la red. Determina los medios. En términos generales, la actividad del atacante se puede restringir de forma que se eviten dañar, abusar de otros sistemas, recursos a través de la red. Esto requiere una gran cantidad de planificación, ya que se requiere que el atacante tenga libertad para aprender de sus movimientos y, al mismo tiempo, no permita que nuestros recursos (honeypot + ancho de banda) se utilicen para atacar, dañar y abusar de otros hosts en el mismo o diferentes subredes. Los administradores de honeynet toman medidas cuidadosas para estudiar y formular una política sobre la libertad contra la contención de los atacantes e implementar esto de manera de lograr el máximo control de los datos y, sin embargo, el atacante no puede descubrirlos ni identificarlos como honeypot. La seguridad es un proceso y se implementa en capas; existen diversos mecanismos para lograr el control de datos, como firewall, conteo de conexiones salientes, sistemas de detección de intrusos. (Anusooya R, 2015)

b) **Captura de Datos:** La captura de datos implica la captura, el monitoreo y el registro de todas las amenazas y los actos de los atacantes dentro de la Honeynet. El análisis de estos datos capturados proporciona una visión de las herramientas, tácticas, técnicas y motivos de los atacantes. El concepto es lograr la máxima capacidad de registro en todos los nodos y, por lo tanto, registrar cualquier tipo de interacción del atacante sin que el atacante lo sepa. Este tipo de registro furtivo se logra al configurar herramientas y mecanismos en los honeypots para registrar toda la actividad del sistema y tener capacidad de registro de red en el honeywall. (Casanovas, 2015)

c) Recopilación de datos: Una vez que se capturan los datos, se reenvían de forma segura a un punto de recopilación de datos centralizado. Esto permite que los datos capturados de numerosos sensores Honeynet se recopilen de forma centralizada para su análisis y archivo. Las implementaciones pueden variar según los requisitos de la organización; sin embargo, las más recientes incorporan la recopilación de datos en la puerta de enlace de Honeywall. (R. C. & Anjali, 2011)

Siguiendo los requisitos de una Honeynet se han implementado y desarrollado tres generaciones, las cuales se diferencian en los métodos y técnicas que se usen para implementar dichos requisitos.

2.2.3.1 Generación I

Fue desarrollada por The Honeynet Project en el año de 1999. Incorpora de una forma sencilla el control y la captura de datos, permitiendo la recopilación máxima de las actividades efectuadas por los atacantes y simula un ambiente real. Requiere dos interfaces de red en su puerta de enlace: Una que se muestra hacia la red externa, y la otra que lo hace hacia la red interna, constituida por varios Honeypots. Las actividades de control y captura de datos las realiza un Firewall de capa tres, que actúa a su vez como una puerta de enlace en modo de Traductor de Direcciones de Red (Nat, Network Address Translation).

2.2.3.2 Generación II

Surgió en el año 2002 y se caracteriza por incorporar los mecanismos de control y captura de datos en un único dispositivo de capa dos trabaja en modo puente, conocido como Honeywall, que no modifica los paquetes de la red mientras se procesan, ni reducen por los intrusos. Brinda un control total en cuanto a las conexiones que entran y salen del honeypot, ya que a diferencia de la

arquitectura de primera generación no se limita la cantidad máxima de conexiones salientes posibles. Se ejecutan en sistemas operativos y aplicaciones reales.

La Gen II de Honeynet añade un Sistema de Prevención de Intrusos en la puerta de enlace Honeywall, configurado de forma que se modifiquen dinámicamente las reglas del firewall, en caso de detectarse actividades maliciosas, bloquea o modifica paquetes del mismo tipo en el futuro y evita que los honetpots se conviertan en los ataques de la red.

2.2.3.3 Generación III

La tercera generación de las honeynet apareció en el año 2005. Fundamentalmente, posee la misma arquitectura que la Gen II, pero experimenta ciertas mejoras en cuanto a la capacidad de gestión y análisis avanzado de datos. Introduce el concepto de Honeywall Roo, una herramienta open source de fácil implementación que integra las funciones de control, captura y análisis de datos.

2.2.3.4 Virtual Honeynet

La virtualización es una tecnología que permite ejecutar múltiples máquinas virtuales en una sola máquina física. Cada máquina virtual puede ser una instalación de sistema operativo independiente. Esto se logra por que los recursos de las máquinas físicas, como la CPU, la memoria, el almacenamiento y los periféricos, a través de software especializado en múltiples entornos. Por lo tanto, múltiples sistemas operativos virtuales pueden ejecutarse simultáneamente en una sola máquina física.

Una Honeynet virtual es una solución que facilita la ejecución, así como la portabilidad ya que se encuentra en una sola computadora.

2.3 Honeypots

Un honeypot se lo conoce como una trampa para detectar, desviar o de alguna manera contrarrestar los intentos de uso no autorizado de los sistemas de información.

Cuando un honeypot es atacado este puede capturar la actividad del atacante de acuerdo con direcciones IP, puertos usados, protocolos, entre otros. Dicha información es muy valiosa para conocer patrones o estrategias al momento de intentar vulnerar la seguridad de un sistema en la red.

2.3.1 SEBEK

Es una herramienta diseñada para capturar las actividades de un atacante en un honeypot, sin que el atacante lo sepa. Sebek se basa en una arquitectura cliente-servidor. El cliente Sebek se ejecuta en los honeypots, para capturar todas las actividades de los atacantes (pulsaciones de teclado, transferencia de archivos, contraseñas) y luego enviar los datos de forma encubierta al servidor. El servidor Sebek recopila y procesa estos datos.

El servidor normalmente se ejecuta en la puerta de enlace de Honeywall, pero también puede ejecutarse de forma independiente en un host remoto. Sebek se instala en el sistema como un módulo del kernel de Linux (LKM) que registra toda la actividad de datos asociada al invocar las llamadas estándar de "lectura" y "escritura" del sistema.

Esta actividad registrada se envía a la red en forma de paquetes Sebek. El módulo del núcleo de Sebek oculta estos paquetes de la vista de los atacantes. Este módulo en sí mismo se puede ocultar y se puede configurar para que se cargue con un nombre definido por el usuario para evitar que el atacante lo detecte. (Lance Spitzner. Sebek., s.f.)

2.4 Definición de Log

Se define como un registro de los eventos ocurridos dentro de los sistemas o redes de una organización. El log permite tener un registro de la actividad realizada durante un rango de tiempo en particular, permitiendo ser utilizado como evidencia para auditoria informática o verificación de algún riesgo informático por el motivo de que estos registros permiten almacenar información sobre que, quien, donde, cuándo y por qué ocurrió.

2.4.1 Gestión centralizada de log

A menudo, se encuentra con la necesidad de buscar determinada información en los logs del sistema, en el 95% de las ocasiones para tratar de solucionar problemas que afectan de algún modo a nuestra plataforma.

Es posible tener logs de todo tipo, unificado y en tiempo real, no solo almacenados, sino para poder consultar. Para el presente proyecto de investigación Walleye se utilizará para la recolección de datos, ya que ejecuta un servidor web donde se podrá revisar la información de los ataques.

2.5 Herramientas para la simulación

2.5.1 Software de Virtualización Oracle VM Virtual Box.

Para el diseño del prototipo se avisto el uso de máquinas virtuales y en este caso se eligió el software de virtualización a Oracle VM VirtualBox 6.0.

VirtualBox es un potente producto de virtualización x86 y AMD64 / Intel64 para empresas y para uso doméstico. VirtualBox no solo es un producto extremadamente rico en funciones y alto rendimiento para clientes empresariales, sino también es la única solución profesional que está disponible gratuitamente como software de código abierto según los términos de la Licencia Pública General de GNU (GPL) versión 2. (Oracle, 2018)

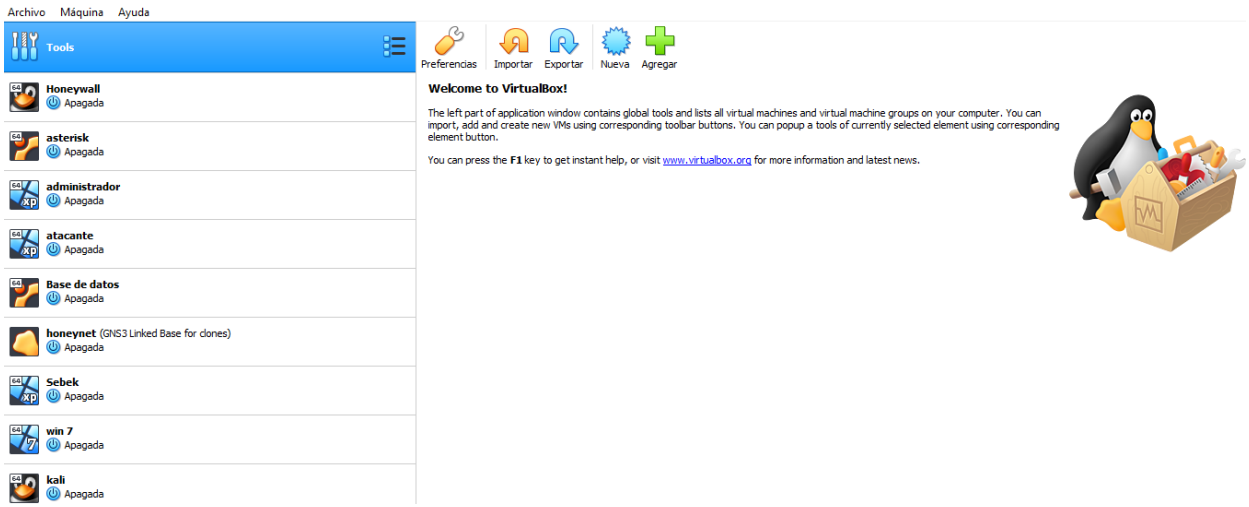


Ilustración 1: Pantalla de Inicio Virtual Box
Elaborado por: Bryam Yucta

Actualmente, VirtualBox se ejecuta en hosts de Windows, Linux, Macintosh y Solaris y admite una gran cantidad de sistemas operativos invitados, incluidos, entre otros, Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10).), DOS / Windows 3.x, Linux (2.4, 2.6, 3.xy 4.x), Solaris y Open Solaris, OS / 2 y OpenBSD.

VirtualBox se está desarrollando activamente con lanzamientos frecuentes y tiene una lista cada vez mayor de características, sistemas operativos invitados compatibles y plataformas en las que se ejecuta. VirtualBox es un esfuerzo comunitario respaldado por una empresa dedicada: se alienta

a todos a contribuir, mientras que Oracle garantiza que el producto siempre cumple con los criterios de calidad profesional. (Oracle, 2018).

2.5.2 Honeywall Roo

El propósito del CDROM Honeywall es automatizar la instalación y el mantenimiento de una red trampa y proporcionar soporte de análisis de datos para todas las actividades dentro de la red trampa. La implementación del Honeynet fue una tarea extenuante, ya que implica la configuración avanzada y la integración de herramientas de seguridad

Honeywall se basó inicialmente en Fedora durante bastante tiempo como su sistema operativo base, pero debido a las frecuentes actualizaciones que se realizan en fedora, ahora se basa en CentOS.

Para el presente proyecto de investigación se utiliza la versión Linux Roo 1.4. Hw 20080424215739 basado en CentOS. Esta herramienta incluye varios componentes claves para la honeynet.

Componente	Descripción
Snort	Sistema de detección de intrusos basado en reglas, capaz de realizar el análisis del tráfico de la red en tiempo real y registrarlo.
Snort_inline	Es una versión modificada del Snort que toma decisiones sobre el tráfico saliente siempre y cuando tenga ataques conocidos.
Session Limit	Control límite de sesiones.
Sebek	Es una herramienta de captura de daros diseñada para capturar el ataque sobre las actividades de un honeypot.
Walleye	Proporciona al administrador herramientas de análisis de datos de manera remota. Los administradores pueden acceder a todos los datos capturados por Snort_Inline y Sebek, estos dos incluyen la dirección IP datos transferidos y acciones de los atacantes.
Pcap	Interfaz de captura de datos del kernel de Linux.
Iptables	Firewall de Linux integrado en el kernel, usado para limitar los paquetes en el control de datos y para registrar los datos en la captura de datos.

Swatch	Herramienta que comunica al administrador por medio de un correo electrónico
Argus + Hflow	Información de flujos de tráfico y relaciones
Menú	Una interfaz gráfica usada para el mantenimiento y control de la honeynet
Mysql	Un servidor de base de datos utilizado para almacenar y relacionar el contenido capturado.

Tabla 1 Componentes de la Honeywall
Elaborado por: Bryam Yucta

2.5.3 Walleye

Es una interfaz basada en web para la configuración, administración y análisis de datos de Honeywall. Es una interfaz gráfica de usuario basada en web o GUI. Se puede acceder de forma remota a través de la web a través de un cliente de navegador web. Esto brinda una gran accesibilidad y facilidad de control remoto al administrador de Honeywall. Por razones de seguridad, se puede acceder a esta interfaz a través del puerto 443 (HTTPS utilizando certificados seguros basados en SSL)

2.5.4 GNS3

GNS3 (Graphic Network Simulation o Simulación Grafica de Redes) Es un software de código abierto el cual permite diseñar topología de red complejas y poner en marcha simulaciones sobre ellos.

3. CAPITULO III

3.1 Metodología

El desarrollo de esta tesis tiene un enfoque exploratorio para entender la red de investigación honeynet y las herramientas implementadas en la misma. Posteriormente, se realiza un estudio descriptivo de los paquetes ingresado al Walleye. Finalmente, se abarca un estudio relacional en el cual se analiza los datos obtenidos sobre la gestión centralizada de log.

Es preciso mencionar que para el desarrollo del presente proyecto de investigación se lo realizo en un ambiente simulado de la Infraestructura de la red implementada en el datacenter de la UNACH, utilizando dos servicios DNS y WEB los cuales servirán para ser atacados.

3.2 Hipótesis

3.2.1 Comprobación de la hipótesis

La comprobación de la hipótesis estadística es una regla que basada en una hipótesis nula H_0 ayuda a decidir si ésta se acepta o no. Para la justificación de la hipótesis se utilizó el método Anova nos dice que es nula al establecer que todas las medias de la población son iguales mientras que la hipótesis alternativa estables que al menos una es diferente.

3.2.2 Planteamiento de la Hipótesis

Hi= La implantación de un aplicativo optimizará la gestión centralizada de logs en el data center de la Universidad Nacional de Chimborazo.

Ho= La implantación de un aplicativo no optimizará la gestión centralizada de logs en el data center de la Universidad Nacional de Chimborazo.

3.2.3 Nivel de Significancia

El valor de significancia es de $\alpha = 0.05 = 5\ \%$

3.3 Identificación de variables

3.3.1 Variable Independiente

Implantación de un aplicativo.

3.3.2 Variable Dependiente

Optimizar la gestión centralizada de logs en un ambiente honeynet en el datacenter de la UNACH.

3.4 Operacionalización de variables

VARIABLE	TIPO	DEFINICIÓN CONCEPTUAL	DIMENSIÓN	INDICADORES
La implantación de un aplicativo	INDEPENDIENTE	Es el aplicativo implantado el cual tendrá la información centralizada de cada log	Ontología de dominio	-Términos, atributos y relaciones -Cantidad de datos ingresados a la red
Optimizar la gestión centralizada de logs en un ambiente honeynet en el datacenter de la UNACH.	DEPENDIENTE	Mediciones de tiempo y recursos para la optimización a la gestión centralizada de log	Aplicativo implantado	- Impacto - Fallo del Sistema - Escaneo de Ataques - Facilidad de Ataques - Acciones Correctivas.

Tabla 2 Tabla de Operación de Variables
Elaborado por: Bryam Yucta

3.5 DISEÑO DE LA INVESTIGACIÓN

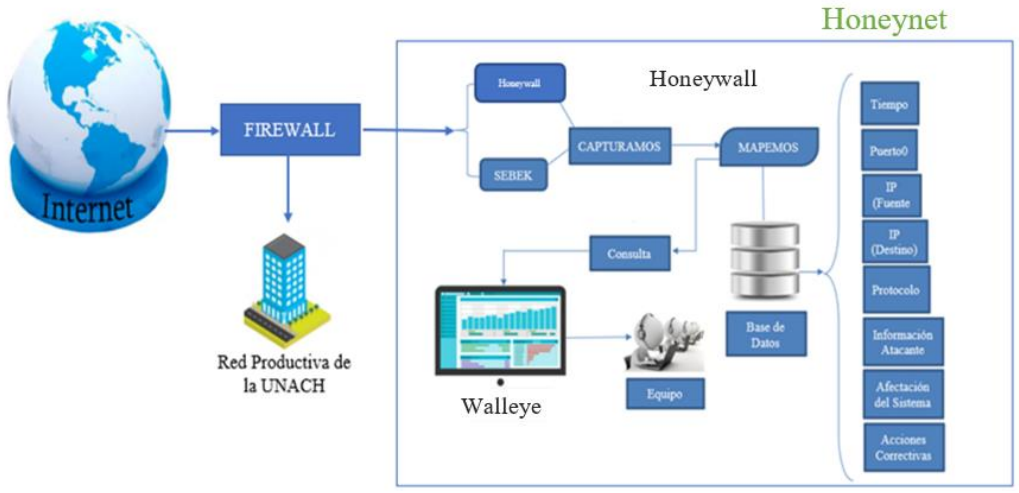


Ilustración 2: Infraestructura de la Honeynet
Elaborado por: Bryam Yucta

CAPITULO IV

4. RESULTADOS Y DISCUSION

La presente investigación pretende optimizar el tiempo que utiliza los administradores en la gestión de los archivos log, generados por los ataques a los servidores DNS y Web ingresados través la red, para lo cual se realizará un estudio comparativo entre el estado actual de la gestión de logs en el Datacenter Institucional de la UNACH y la gestión de logs una vez desplegado el aplicativo Walleye sobre un escenario simulado implementado a través del uso de GNS3.

Los parámetros de medición y las ponderaciones de las mismas que se establecen en la presente investigación son las siguientes:

4.1 PONDERACIÓN DE PARÁMETROS

4.1.1 Ponderación IMPACTO

NIVEL	DESCRIPCIÓN	PONDERACIÓN
Ninguno	• No registra impacto	0
Bajo	• Acceso remoto • Problemas de enrutamiento	1
Medio	• Recopilación de la información • Divulgación de código de archivos no disponibles para su visualización • Modificación de contenidos web	2
Alto	• Denegación de servicios • Ejecución remota de código malicioso arbitrario • Accesos no autorizados • Modificación de privilegios de usuarios	3

Tabla 3 Ponderación de Impacto
Elaborado por: Bryam Yucta

4.1.2 Ponderación del Fallo del Sistema

Nivel	Descripción	Ponderación
Ninguno	• No afecta el sistema	0
Parcial	• Falla Aplicación, servicio o modulo que no afecta a todo el sistema	1
Total	• Colapsa todo el sistema	2

Tabla 4
Ponderación Fallo del Sistema
Elaborado por: Bryam Yucta

4.1.3 Ponderación de Escaneo de Ataques

Nivel	Descripción	Ponderación
Ninguno	• No a registra impacto	0
Remoto	• Puertas traseras • Vector de ataques • Encabezados HTTP modificados para evitar controles de acceso de escritura	1
Combinado	• Solicitud de petición seguida de petición remota • CGI subyacente.	2
Local	• Por medio de anfitriones • Desencadenante de código malicioso • Acceso a credenciales • Obtención de usuario y contraseñas	3

Tabla 5 Ponderación Escaneo de ataques
Elaborado por: Bryam Yucta

4.1.4 Ponderación de Facilidad de Ataque

Nivel	Descripción	Ponderación
Ninguno	• No registra	0
Trivial	• Carece de importancia	1
Simple	• No requiere código • Credenciales obtenidas	2
Moderado	• Numerosas herramientas y scripts	3

Tabla 6: Ponderación Facilidad de Atauques
Elaborado por: Bryam Yucta

4.1.5 Ponderación de Acción Correctiva

NIVEL	DESCRIPCIÓN	PONDERACIÓN
Ninguno	• No registra impacto	0
Bajo	• Revisar el host comprometido • Regla registra y ejecutada • Barrido de ping	1
Moderada	• Bloquear solicitudes entrantes • Trafico sospechoso • Asegurarse de Aplicación de parches y actualización de versiones	2
Alto	• Desactivar gestión de contenidos • No permitir accesos administrativos a fuentes remotas	3

Tabla 7 Ponderación de Acción Correctiva
Elaborado por: Bryam Yucta

4.2 MEDICIONES EN EL ESCENARIO DE ESTADO ACTUAL.

La ilustración 12, muestra la infraestructura funcional del Datacenter institucional para la gestión de logs cuando se producen ataques a sus servidores.

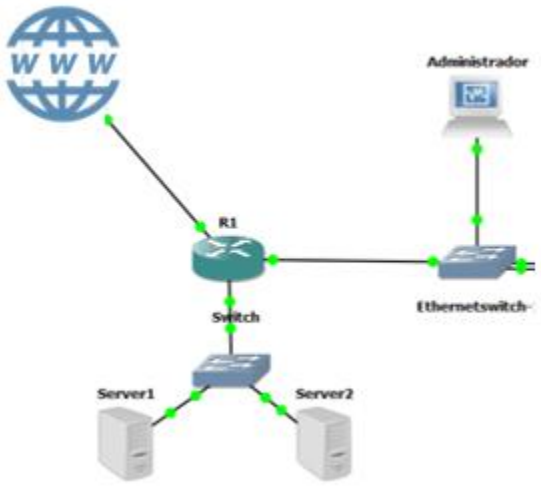


Ilustración 2 Infraestructura Actual
Elaborado por: Bryam Yucta

4.2.1 Cuadro de ataques con estado actual

A continuación, se presenta la recolección de los ataques generados en el estado actual de la infraestructura de la red de datos de la UNACH

Ataque Detectado (Ver Talas en Anexo 7)	Impacto	Fallo Sistema	Escaneo de ataque	Facilidad de ataque	Acción Correctiva	Total
AD 1.1	3	2	2	1	1	9
AD 2.1	2	2	2	1	1	8
AD 3.1	2	2	1	2	0	7
AD 3.2	2	2	3	2	1	10
AD 3.3	3	2	1	1	1	8
AD 4.1	3	2	3	2	0	10
AD 4.2	3	2	2	1	0	8
AD 5.1	3	2	2	2	1	10
AD 5.2	3	1	1	1	0	6
AD 6.1	3	2	2	2	1	10
AD 6.2	3	2	3	1	0	9
AD 7.1	3	2	2	1	1	9
AD 7.2	3	2	1	1	1	8
AD 7.3	3	1	2	2	0	8
AD 8.1	2	2	3	1	0	8
AD 8.2	3	2	2	1	0	8
AD 8.3	3	2	3	2	1	11
AD 8.4	3	2	3	1	0	9
AD 8.5	3	2	2	1	1	9
AD 9.1	3	1	2	2	0	8
AD 9.2	3	2	2	1	1	9
Total	59	39	44	29	11	182

Tabla 8 Detalle de Ataques
Elaborado por: Bryam Yucta

4.2.2 Representación gráfica de los datos

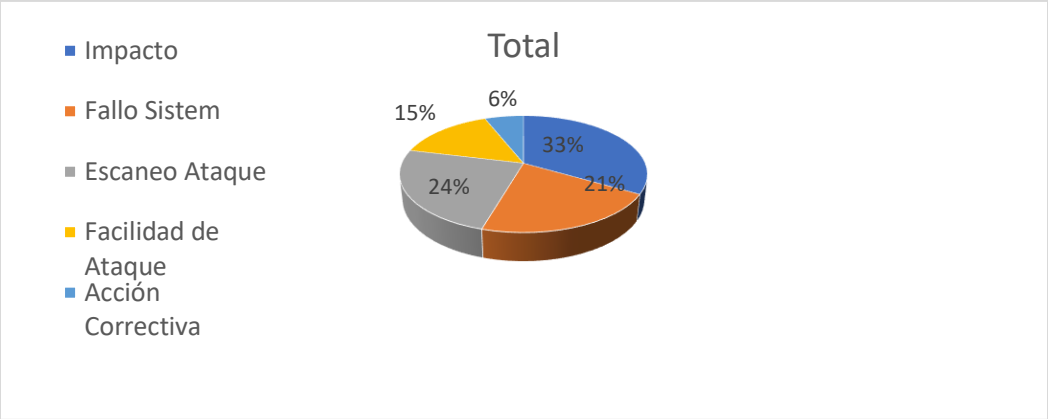


Ilustración 3 Graficar de los datos
Elaborado por: Bryam Yucta

Interpretación

Como se puede observar en la Ilustración 3, la información capturada en el cual el 33% representa el impacto del ataque, 24% representa al escaneo de ataque, el 21 % representa al fallo del sistema, el 15% facilidad de ataque y el 6% representa las acciones correctivas.

Como se puede observar para el estado actual al momento de analizar los datos no se utiliza un sistema automatizado que ayude con la integración y centralización de los datos es decir se lo realiza por separado.

Como se muestra en la imagen anterior de los 21 ataques a la red, se realizará una comparación del tiempo utilizado para analizar cada uno de los archivos log generados por los ataques en el cual nos da un periodo de 1 hora para comparar y analizar la información de ataques a la red

Cabe mencionar que la información fue simulada en el escenario actual de la red de producción y corroborada por el administrador de red en base a una entrevista sobre el tiempo que utiliza para el análisis de los archivos log.

A continuación, se realizará las pruebas en el escenario en el cual se encuentra desplegado nuestro aplicativo Walleye, en el cual se pretende disminuir el tiempo utilizado para la gestión de log.

4.3 MEDICIONES EN EL ESCENARIO SIMULADO CON GNS3 CON EL APLICATIVO WALLEYE.

La implementación que se utilizó para esta investigación es una Honeynet virtual con honeypots, en la cual se debe, determinar los puertos a exponer, así como las direcciones IP.

- Cantidad de datos que se pueden enviar por unidad de tiempo (segundo, minuto, hora, días)
- Puertos TCP, UDP, ICMP y otros
- Direcciones IP permitidas y no permitidas

Limitación de Conexión	
Cantidad de datos a ser enviados	50
Conexiones	TCP, UDP
Servicios	SSH, NETBIOS, HTTP, DNS, FTP
Puertos	21, 22, 25, 43, 80, 53, 443
IP Permitidas	IP de los honeypots
IP no Permitidas	IP de la red de producción

Tabla 9: Limitación de Conexión
Elaborado por: Bryam Yucta

4.3.1 Infraestructura Walleye

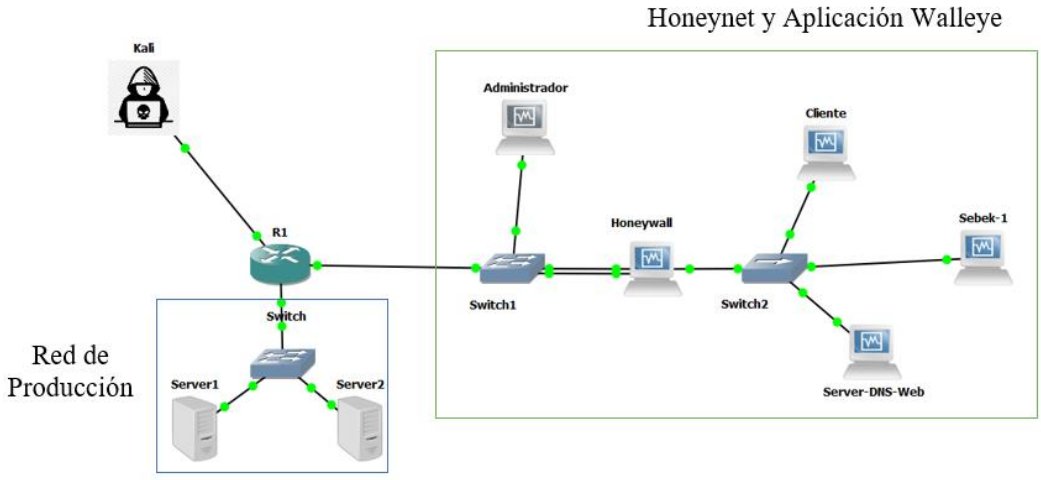


Ilustración 4 Infraestructura desplegado Walleye
Elaborado por: Bryam Yucta

4.3.2 Captura de datos

Se utilizó snort-line y Sebek para registrar y reportar las acciones de los ataques. Esto lo hace en base a los checksum que es el mecanismo para desencadenar alertas de análisis de la información

4.4 Cuadro de ataques capturados por la Honeynet

Ataque Detectado (Revise el anexo 8)	Impacto	Fallo Sistema	Escenario de ataque	Facilidad de ataque	Acción Correctiva	Total
AD 1.1	1	1	1	1	2	6
AD 2.1	2	1	2	1	2	8
AD 3.1	0	1	2	0	2	5
AD 3.2	1	1	2	0	2	6
AD 3.3	0	1	3	1	3	8
AD 4.1	2	1	2	1	2	8
AD 4.2	1	1	2	1	3	8
AD 5.1	1	1	1	1	2	6
AD 5.2	1	1	1	1	3	7
AD 6.1	1	1	2	1	3	8
AD 6.2	1	0	3	1	3	8
AD 7.1	2	1	1	1	2	7
AD 7.2	0	1	2	1	2	6
AD 7.3	2	1	2	1	3	9
AD 8.1	2	0	1	1	3	7
AD 8.2	1	0	1	1	3	6
AD 8.3	2	0	1	0	2	5
AD 8.4	1	0	1	1	3	6
AD 8.5	1	1	1	1	2	6
AD 9.1	2	1	2	1	3	9
AD 9.2	1	1	1	1	3	7

Total	25	16	34	18	53	146

Tabla 10 Datos de Ataques capturados por el Honeywall
Elaborado por: Bryam Yucta

4.4.1 Recolección de datos

La actividad en la red trampa (Honeynet) se registró a través de las herramientas Sebek y Snort_line. El honeywall simuló un Gateway que distrajo al atacante y lo motivó a ingresar en la red y generar ataques sobre la misma.

El trafico recolectado por la Honeynet, reportó los siguientes resultados estadísticos de tráfico (ataques) en los puertos: HTTP y DNS

4.4.2 Análisis de los datos

En nuestra investigación se utilizó Walleye para analizar e integrar los datos de las herramientas instalas en los honeypots (Sebek.).

4.5 DETALLE DEL TRÁFICO GENERADO EN LA HONEYNET

4.5.1 Detalle del tráfico HTTP

HTTP	**Agosto**
HTTP Client Error	1
HTTP Request Not Found	25
HTTP Server Error	871
HTTP Sever Slow Response Time	0
Capa de Transporte	
TCP Connection Refused	13
TCP Fast Retransmissions	7
TCP Low Window	13,72
TCP Repeated Connect Attempt	97
TCP Reset Connection	98
Retransmissions	236
TCP Slow ACK	144
TCP Too Many Retransmissions	54
TCP Window Frozen	3,27
TCP Zero Window Too Long	2

Tabla 11 Trafico HTTP
Elaborado por: Bryam Yucta

4.5.2 Detalle del Trafico de DNS

DNS	Agosto
DNS Host or Domain Not Exist	31,44
DNS Server Error	20
DNS Server Slow Response Time	1,311

Tabla 12 Trafico DNS
Elaborado por: Bryam Yucta

4.5.3 Análisis de la Información Obtenida

Una vez que determinados los parámetros se procedió a analizar los datos capturado en la Honeynet, para ello se utiliza la herramienta Walleye la que ofrece la centralización de la información mediante su interfaz web donde a través de snort-line y Sebek, muestra las alertas de los ataques registrados. Este proceso es crucial con el fin de determinar si el sistema ha sido vulnerado y comprobar que la gestión centralizada de log ha sido mejorada; para que el administrador de la red realice los correctivos en un menor tiempo.

4.5.4 Representación gráfica de los datos obtenidos por el Walleye

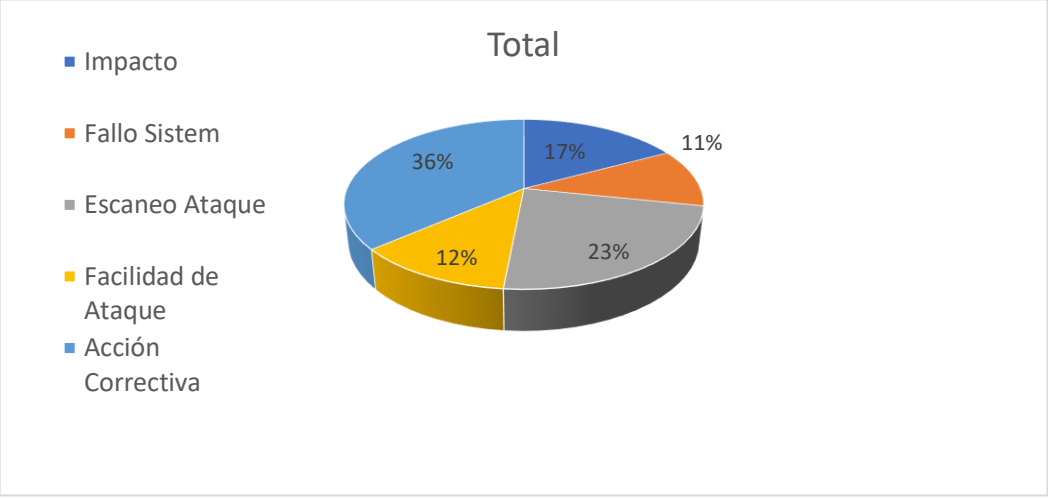


Ilustración 5 Grafica generada por el Honeywall
Elaborado por: Bryam Yucta

La ilustración 5, muestra el total de los 21 ataques capturados por la honeynet y honeypots, en el cual el 36% representa las acciones correctivas, 23% representa el escaneo de ataques, el 17 % representa al impacto, el 12% representa a la facilidad de ataque y el 11% representa el fallo del sistema. Como se puede observar se tiene simulada la infraestructura completa de la honeynet, junto con el despliegue del aplicativo Walleye, el cual contiene un formato centralizado para optimizar la gestión de logs.

4.6 DEMOSTRACION ESTADISTICA.

Para la demostración estadística se utilizó el software R el cual nos permite comparar median el análisis estadístico de ANOVA el cual nos permite un análisis de varianza, prueba de que las medias de dos o más poblaciones son iguales.

Con respecto a la hipótesis Anova nos dice que es nula al establecer que todas las medias de la población don iguales mientras que la hipótesis alternativa estables que al menos una es diferente.

```
> AnovaModel.1 <- aov(variable ~ factor, data = StackedData)

> summary(AnovaModel.1)
             Df Sum Sq Mean Sq F value Pr(>F)
factor        9 110.08  12.231   43.98 <2e-16 ***
Residuals   200  55.62   0.278
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
```

```
> with(StackedData, numSummary(variable, groups = factor, statistics = c("mean", "sd")))
                        mean        sd data:n
Acción.Correctival   0.5238095 0.5117663     21
Acciones.Correctiva2 2.5238095 0.5117663     21
Escaneo.de.ataquel   2.0952381 0.7003401     21
Escaneo.de.ataque2   1.6190476 0.6690434     21
Facilidad.de.ataquel 1.3809524 0.4976134     21
Facilidad.de.ataque2 0.8571429 0.3585686     21
Fallo.Sistemal       1.8571429 0.3585686     21
Impactol             2.8095238 0.4023739     21
Impacto2             1.1904762 0.6796358     21
Sistema.Fallo2       0.7619048 0.4364358     21
```

Ilustración 6 Prueba Estadística
Elaborado por: Bryam Yucta

Como se observa en la Ilustración 6 se obtienes un p_valor del -0.05% eso quiere decir que se rechaza la hipótesis nula y se acepta la hipótesis alternativa la cual es “La implantación de un aplicativo optimizará la gestión centralizada de logs en el data center de la Universidad Nacional de Chimborazo.

A continuación, se presenta el análisis de la variancia de las medias de cada uno de los datos relacionado el estado actual con la implementación del aplicativo.

Comparación (ANOVA)	Media	Desviación Estándar	p-valor
Escaneo.de.ataque1	2.095.238	0.7003401	0.0298
Escaneo.de.ataque2	1.619.048	0.6690434	
Acción.Correctiva1	0.5238095	0.5117663	1.41e-15
Acciones.Correctiva2	25.238.095	0.5117663	
Facilidad.de.ataque1	13.809.524	0.4976134	0.000345
Facilidad.de.ataque2	0.8571429	0.3585686	
Impacto1	2.809.524	0.4023739	1.14e-11
Impacto2	1.190.476	0.6796358	
Fallo.Sistema1	18.571.429	0.3585686	5.2e-11
Sistema.Fallo2	0.7619048	0.4364358	

Tabla 13: Análisis de variancia por cada valor
Elaborado por: Bryam Yucta

CONCLUSIONES

- La implementación de la Honeynet y el uso de la herramienta Sebek sobre la infraestructura de red simulada con GNS3 permitió evidenciar una mejorar al momento de analizar ataques, pues el registro de las actividades de un atacante y sus tácticas o métodos de ataque contra servicios o aplicaciones implementadas como DNS y WEB; es automática y centralizada.

- Mediante la metodología utilizada en la presente investigación y la relación estadística entre los ataques sobre la red de datos actual de la UNACH y el ambiente simulado incorporando la Honeynet, mediante el método estadístico Anova se evidenció una mejora significativa que sostiene el uso y despliegue del aplicativo Walleye para optimizar la gestión centralizada de log.

- Se valida el formato establecido por Walleye, como formato para el análisis de archivos de revisión grafica de logs, es así que el análisis estadístico con Anova entre el estado actual de la red y la infraestructura simulada con una Honeynet muestra un valor de significancia de 0,02 a favor del ambiente simulado.

RECOMENDACIONES

- Para la implementación de la honeynet virtual autocontenida es recomendable manejar recursos hardware que permitan la instalación de varios honeypot, en los cuales se puedan implementar servicio sobre diferentes sistemas operativos y así obtener una gran cantidad de información, pero manejando un ambiente más realista y que un atacante realice con toda libertad sus actividades.

- Investigar herramienta que permitan capturar tráfico de red para incorporar en la interfaz web Walleye y entender de mejor manera la información centralizada en la honeynet, además definir una política sobre el tiempo de lectura de los archivos log según como el administrador de red lo crea necesario.

- Se recomienda tomar medidas de seguridad ya que la implementación de la honeynet no garantiza la seguridad de los datos, la implementación de la Honeynet se en fines investigativos.

BIBLIOGRAFIA

Alkudhir, B., Chairetakis, E., & Mystridis, P. (05 de 2013). School of Information Science, Computer and Electrical Engineering. Obtenido de School of Information Science, Computer and Electrical Engineering.

Avella Coronado, J. d., Calderon Barrios, L. F., & Mateus Díaz, C. A. (2013). GUÍA METODOLÓGICA PARA LA GESTIÓN CENTRALIZADA DE REGISTROS. Riobamba.

Board, T. C. (s.f.). Common event expression. Obtenido de http://cee.mitre.org/docs/CEE_Architecture_Overview-v0.5.pdf

Bullard, C. (06 de 2017). http://qosient.com/argus/. Obtenido de http://qosient.com/argus/: http://qosient.com/argus/. 2013.

Casanovas, E., & Tapia, C. (6 de 2015). Honeynets como herramienta de prevención e investigación de. Obtenido de Honeynets como herramienta de prevención e investigación de.

Chanaluisa, D. A., Meza, A. L., & Tasipanta, J. V. (2012). "IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN Y ADMINISTRACIÓN. Quito.

Chuvakin, A., Schmidt, K., & Phillips, C. (s.f.). The authoritative guide ti understanding the conceps surrounding logging and log managrmrnt syngress. Publishing, 2013., Logging and Log Management.

Esteves Cardoso, L., & Cortasio Reuther, P. (s.f.). SGS:Log. Obtenido de SGS:Log: http://lrodrigo.sgs.lncc.br/wp/wp-content/uploads/2014/06/TCC-Larissa-e-Paula-v2.pdf

Gómez, Yordy Rafael ;. (2011). Implementación de un Servidor Syslog. Santa Clara.

Kühnel, J. (2013 de 08 de 30). Department of Computer Science and Engineering. Obtenido de https://www.kuehnel.org/bachelor.pdf

Lance Spitzner. Sebek. (s.f.). Obtenido de Lance Spitzner. Sebek.: http://www.honeynet.org /project /sebek. 2010.

López Cruces, C. (2016). Diselo e implentacion de ujna aplicacion web para el analisis centralizado de logs de seguridad. Madrid España.

Maven, A. (s.f.). Obtenido de https://maven.apache.org/

R. C., J., & Anjali, S. (7 de 2012). "Honeypots: A New Paradigm to Information Security. Obtenido de "Honeypots: A New Paradigm to Information Security: https://www.iacr.org/books/2015_tf_joshi_honeypots.pdf

R.Anusooya, , J.Rajan, & S.A.V.SatyaMurty. (03 de 05 de 2015). International Research Journal of Engineering and Technology (IRJET). Obtenido de IMPORTANCE OF CENTRALIZED LOG SERVER AND LOG ANALYZER.

Snort Team. Snort Official Documentation. . (s.f.). Obtenido de Snort Team. Snort Official Documentation. : https://www.snort.org/docs

Spring, P. S. (s.f.). Obtenido de http://spring.io/

The Honeynet Project. Project Chapters. (2013). Obtenido de The Honeynet Project. Project Chapters.: The Honeynet Project. Project Chapters.

Zalewski, M., & Stearns, W. (2013). Passive OS Fingerprinting Tool. Obtenido de Passive OS Fingerprinting Tool: www.stearns.org/ p0f

Ota, T., Rontani, M., Tarucha, S., Nakata, Y., Song, H. Z., Miyazawa, T., ... & Yokoyama, N. (2005). Few-electron molecular states and their transitions in a single InAs quantum dot molecule. Physical review letters, 95(23), 236801.

ANEXOS

Anexo1: Oficio de aceptación del Proyecto

UNIVERSIDAD NACIONAL DE CHIMBORAZO
CENTRO DE TECNOLOGÍAS EDUCATIVAS
ADMINISTRACIÓN DE RED INSTITUCIONAL
Ext.: 1302

s por la Ciencia y el Saber

Oficio No. 004-ADR-UNACH-2018
Riobamba, 11 de Enero de 2018

Ing. Daniel Haro.
DIRECTOR DEL CENTRO DE TECNOLOGÍAS EDUCATIVAS DE LA UNACH
Presente.

De mi consideración:

Luego de expresarle un cordial saludo, me permito hacerle llegar el informe de factibilidad, de que el señor Bryam Fabricio Yucta Silva, realice su trabajo de grado (tesis), solicitado mediante oficio 1178-CTE-UNACH-2017.

Al respecto debo informar que el área de Infraestructura y Redes cuenta con equipos que tienen la característica de emitir registros de los eventos y alarmas de los mismos, sin embargo no cuenta con un Sistema de Registro de Logs Centralizado, propuesta por el señor estudiante.

Por lo tanto es factible la realización del trabajo de tesis en el Centro de Tecnologías Educativas.

Por la favorable atención, anticipo mi más sincero agradecimiento.

Atentamente,

Ing. Javier Haro Mendoza
Administrador de Red Institucional
UNACH

UNIVERSIDAD NACIONAL DE CHIMBORAZO
CENTRO DE TECNOLOGÍAS EDUCATIVAS
RECEPCION DE DOCUMENTOS
Fecha: 11 ENE 2018 Hora: 10:00
FIRMA DE RESPONSABILIDAD

Ilustración 7 Permiso para Realizar la Investigación
Elaborado por: Bryam Yucta

Anexo 2: Resumen del Proyecto

Resumen del Proyecto		
Características	**Producto**	**Especificaciones**
Máquina Física	Windows 10 pro	**Proveedor de Hardware:** Asus k555L **Procesador:** Intel Core (TM) i7-5500U CPU @ 2.40GHz. **Tipo de sistema:** S.O. X64 64 bits **Ram:** 12 GB. **Almacenamiento:** 500 GB **Red:** Realtek PCIe GbE Family Controller
Sistema Operativo Invitado 1	Centos. Honeywall Roo 1.4	Máquina virtual de un procesador **Ram:** 924 MB **Almacenamiento:** 150 GB **eth0:** Red-Nat **eth1:** Red-Nat **eth2:** host-only
Sistema Operativo Invitado 2	Ubuntu 14.04 Servitor DNS WEB	Máquina virtual de un procesador **Ram:** 2048 MB **Almacenamiento:** 100 GB **Eth0:** Red-at
Sistema Operativo Invitado 3	Windows XP Sebek	Máquina virtual de un procesador **Ram:** 512 **Almacenamiento:** 100 GB **Etch0:** Red-Nat
Sistema Operativo Invitado 4	Windows XP Administrador	Máquina virtual de un procesador **Ram:** 512 MB **Almacenamiento:** 100 GB **Eth0:** Host-Only
Sistema Operativo Invitado 5	Kali-Linux Atacante	Máquina virtual de un procesador **Ram:** 248 MB **Almacenamiento:** 100 GB **Eth0:** Red-Nat

Tabla 14: Resumen del Prototipo

Elaborado por: Bryam Yucta

Anexo 3: Instalación de Honeywall en Virtual Box e Instalación de Sebek

El Honeywall tendrá 3 interfaces de red, dos en modo “Red Nat” y una en modo “Host-Only”.

RED NAT: es la cual funciona como el router de nuestra casa, es decir, los equipos que estén dentro de la misma red Nat podrán comunicarse entre sí.

Host Only: Con esta opción, la máquina virtual que está conectada a nuestro esquipo real es invisible a otros dispositivos en la LAN. Es decir, crea una red aislada a la LAN real.

Para la creación de las máquinas virtuales en virtual box tendrá que dar clic en la opción de nuevo y se muestra la siguiente imagen.

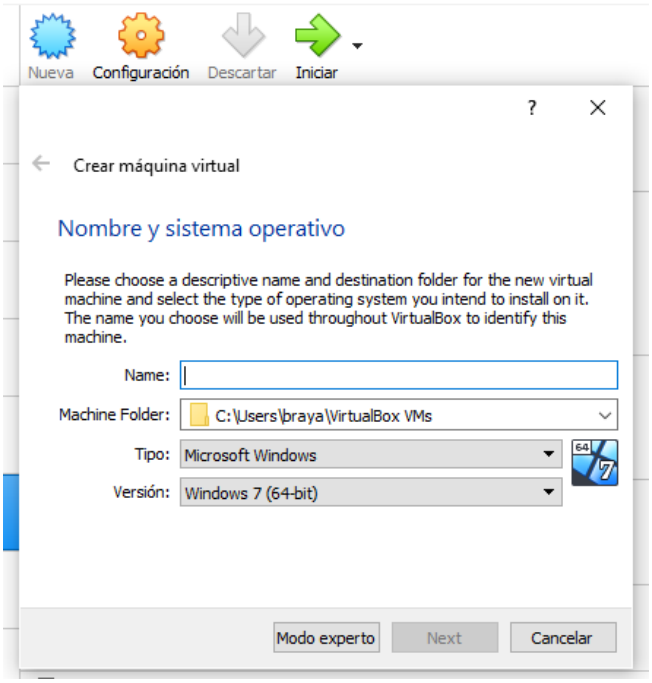


Ilustración 8: Creación de Máquina virtual
Elaborado por: Bryam Yucta

A continuación, se ingresa un nombre a nuestra máquina, en la siguiente ventana se da clic en siguientes teniendo en cuenta la configuración de la memoria RAM y el almacenamiento. (Anexo2).

Una vez creada la máquina se puede iniciar y pedirá un sistema de arranque, se ingresa la imagen del sistema operativo a instalar, en este caso el honeywall.

La máquina nombrada (honeynet) necesita ser configurada con mínimo 256 Mb de RAM y como máximo 900 Mb, en este caso tiene 924 Mb, aunque no redirecciona más que 900 Mb, y tiene 3

interfaces de red, 2 de ellas configuradas como Redes NAT, y ambas en la misma subred como se encuentra configurada con la subred 192.168.56.0/24, y otra interfaz en modo host-Only Ethernet.

Instalación y Configuración de Sebek

El servidor Sebek puede estar localizado en el mismo Honeywall o en un servidor remoto. Esta herramienta de seguridad se puede ejecutar en plataformas Linux o Windows, se lo puede descargar desde la web desde la siguiente ubicación: http://old.honeynet.org/index.html

Se crea una máquina virtual con las características antes mencionada (Anexo2), Se descarga el archivo de instalación, Sebek-Win32-3.0.5 para Windows.

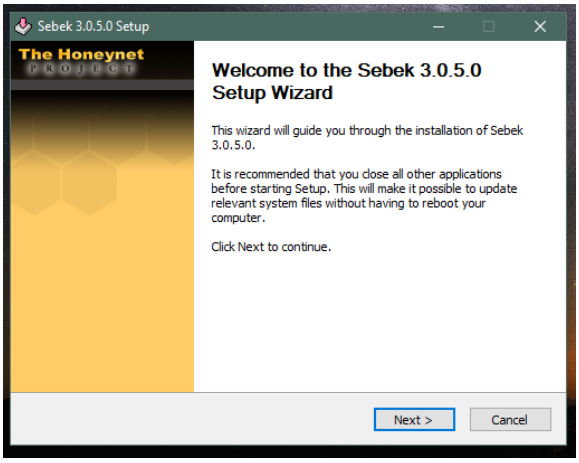


Ilustración 9 Instalación de Sebek
Realizado por: Bryam Yucta

Al dar clic en siguiente se acepta los acuerdos de la licencia.

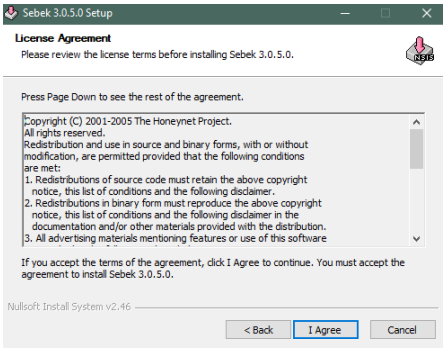


Ilustración 10: Acuerdos de Licencia
Elaborado por: Bryam Yucta

Se asigna la dirección de instalación.

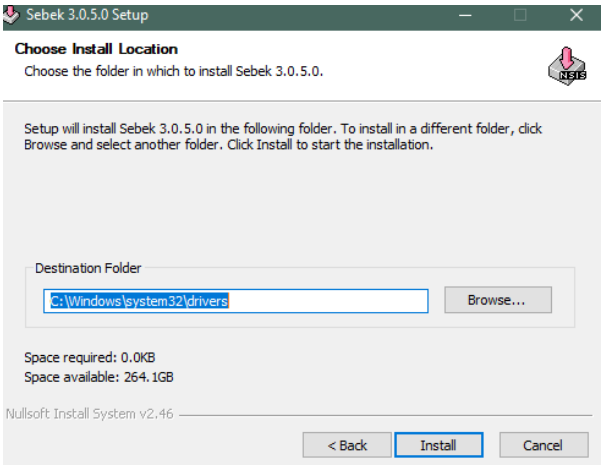


Ilustración 11: Dirección de Instalación
Elaborado por: Bryam Yucta

Al dar clic en instalar inicia el proceso de instalación de los drivers.

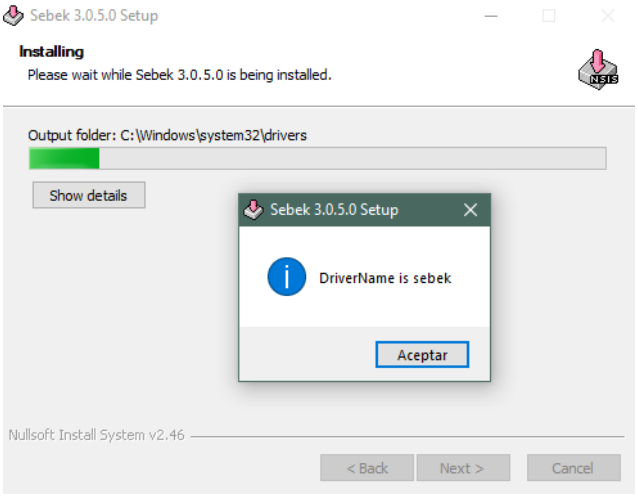


Ilustración 12: Instalación de Los Archivos
Elaborado por: Bryam Yucta

Al dar clic en aceptar se finaliza la instalación.

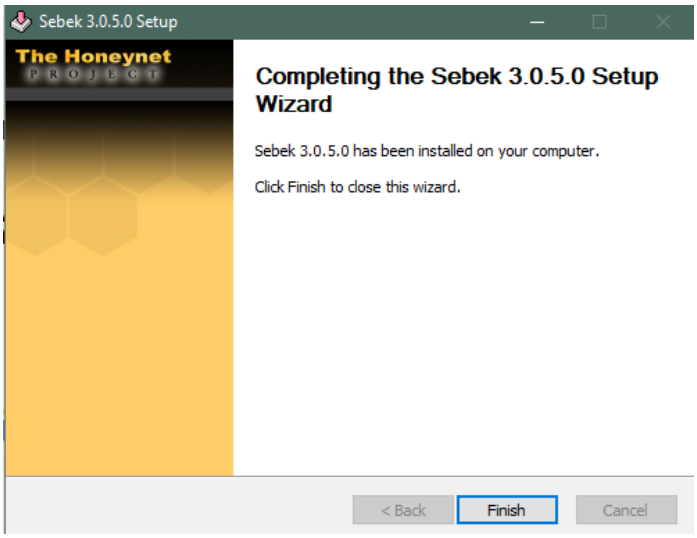


Ilustración 13: Instalación de drivers completa

Elaborado por: Bryam Yucta

Una vez terminada la instalación de Sebek, Se inicia la configuración para que pueda comunicarse con el honeywall.

Para lo cual se ejecuta el archivo “Configuration Wizard.exe”.

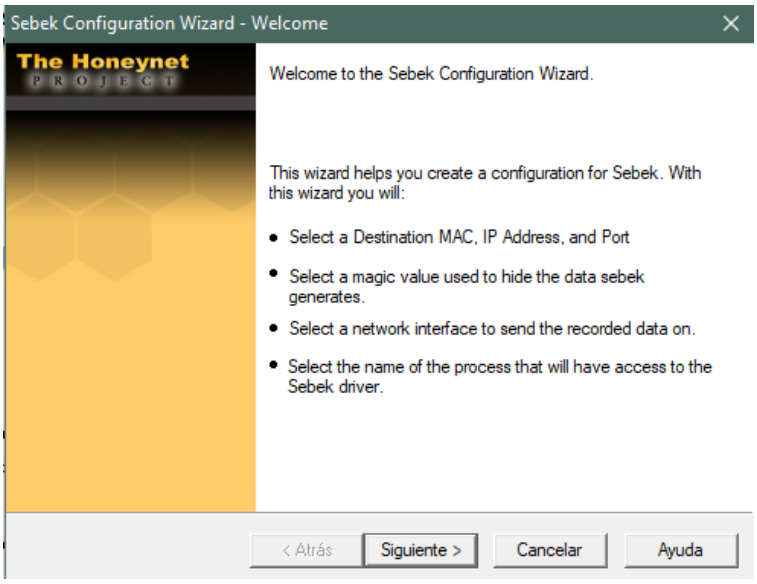


Ilustración 14: Configuración de Wizard
Elaborado por: Bryam Yucta

Se ubica los drivers Instalados.

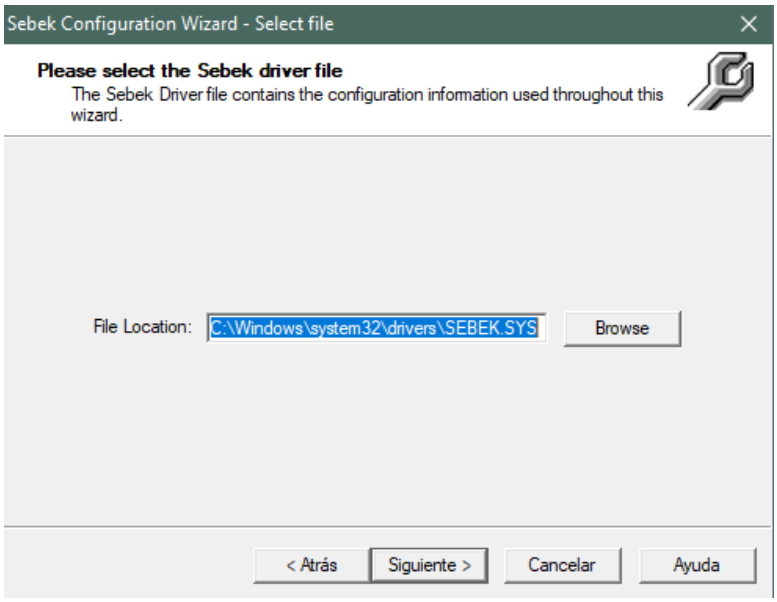


Ilustración 15: Ubicación de los Drivers

Elaborado por: Bryam Yucta

Configurar la IP, dirección MAC y puerto de destino del Honeywall.

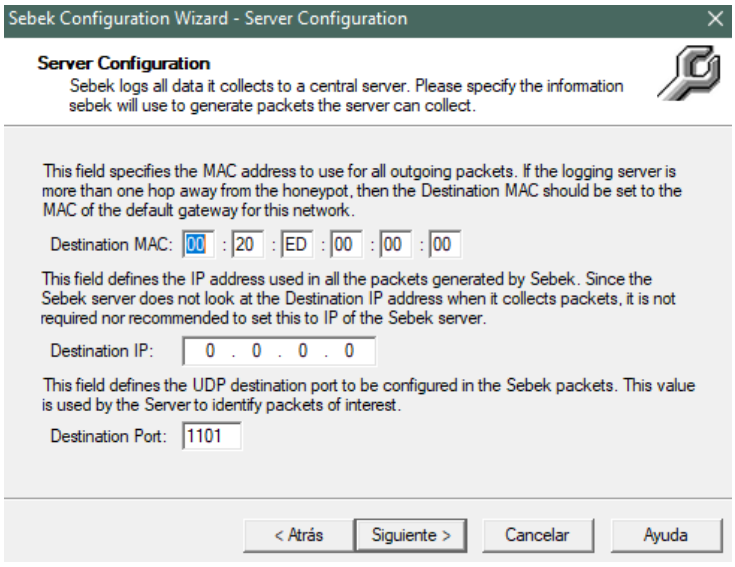


Ilustración 16: Dirección IP, MAC, puerto de destino

Elaborado por: Bryam Yucta

En la siguiente pantalla se tomará el valor por defecto. A continuación, se escoge la interfaz de comunicación con el servidor Sebek.

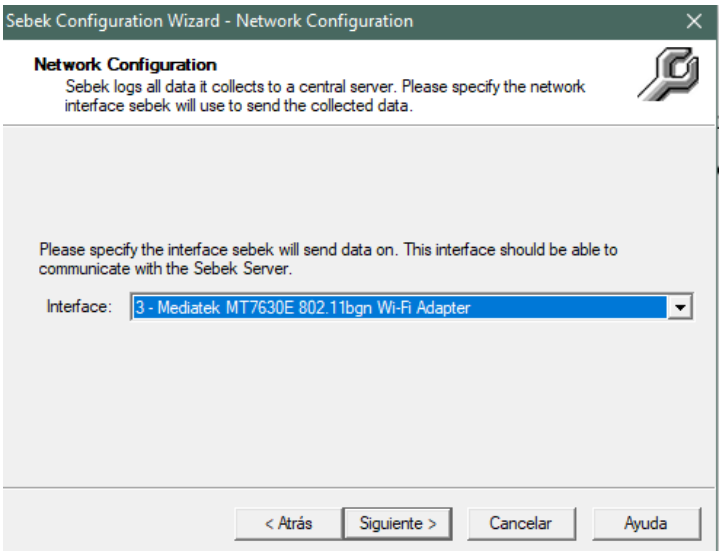


Ilustración 17: Interfaz de comunicación

Elaborado por: Bryam Yucta

A continuación, se elige la configuración por defecto.

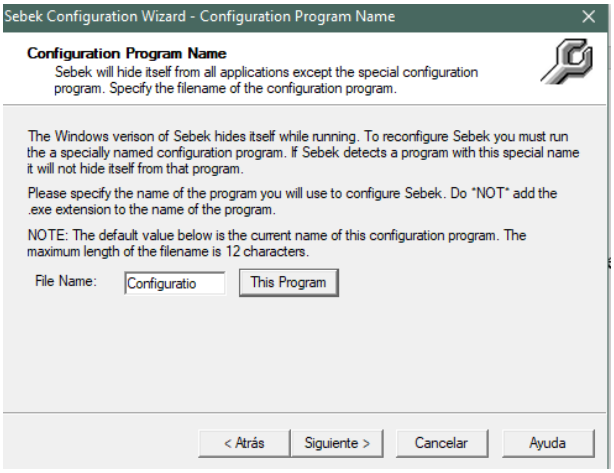


Ilustración 18: Programa por defecto

Elaborado por: Bryam Yucta

Termina la configuración de Sebek

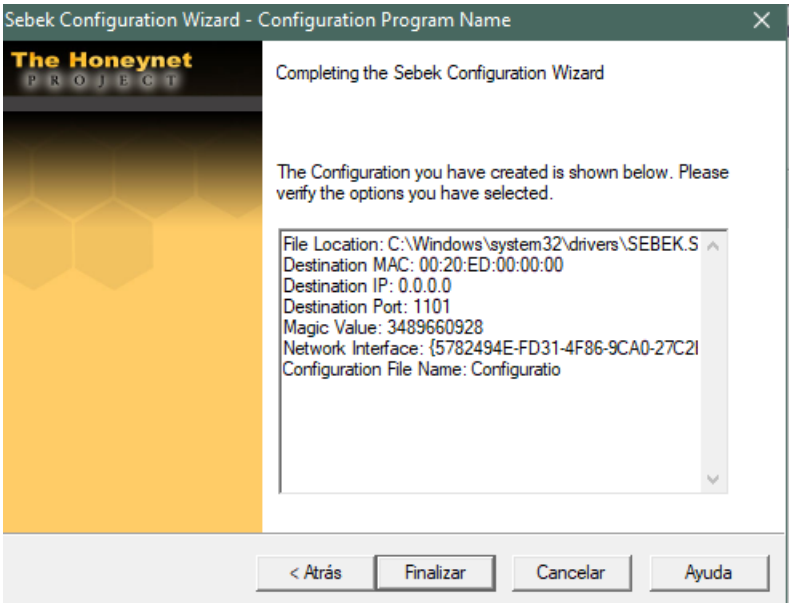


Ilustración 19: Finalización de la Configuración Sebek
Elaborado por Bryam Yucta

Anexo 4: Contenido de Walleye

A continuación, se explica el contenido de nuestra página web Walleye.

Al hablar de seguridad tenemos el ingreso por primera vez a la página, con el cual se ingresa con el usuario **roo** y la contraseña **honey** al dar siguiente se tendrá que cambiar la contraseña de dicho usuario tal como se muestra en la siguiente imagen.

Ilustración 20 Inicio de Sesión

Elaborado por: Bryam Yucta

Al dar clic en cambiar contraseña se regresa automáticamente al inicio de sesión y se tendrá que ingresar con el usuario roo y con la nueva contraseña. Como se observa en la imagen, se muestra una tabla donde indica el tráfico generado y capturado además cuenta con una gráfica y por último si se filtra por archivos Pcap o según el protocolo que se necesite capturar.

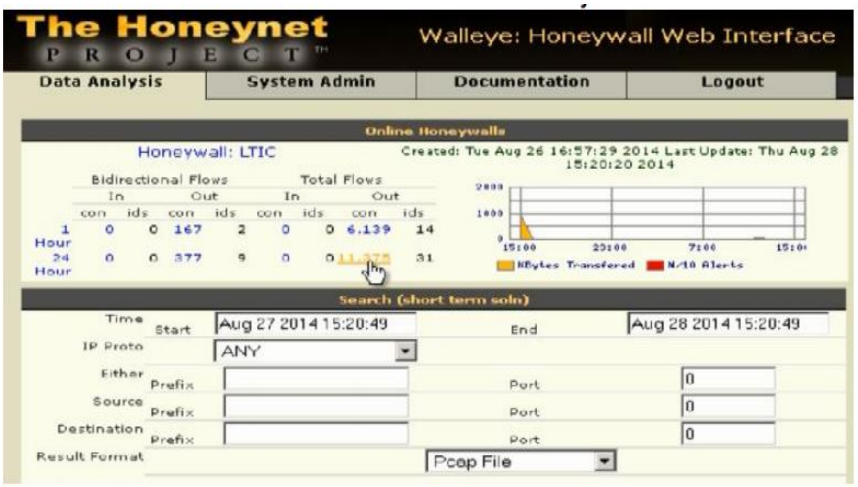


Ilustración 21 Página principal

Elaborado por: Bryam Yucta

En el apartado Honeywall: LTIC nos da una tabla de la entrada y salida de los datos en el cual si se da clic en la parte de Horas se podrá observar la información recentada por nuestra aplicación, como se indicó anteriormente tendremos información de los honeypots y servicios implantados en la honeynet de esta forma podremos revisar los datos centralizados además contamos con el sistema de alertas que podrá alertar de acuerdo a nuestro requerimiento con un correo electrónico de esta forma se podrá analizar la información y optimizar el tiempo ante una toma adecuada de decisiones.

Ilustración 22 Ataque NMAP

Elaborado por: Bryam Yucta

La página web cuenta con dos opciones las cuales son Administración y documentación

Administración del Sistema: Cuenta con la facilidad de administrar de una forma gráfica nuestro honeynet además de poder ver la información receptada de los ataques

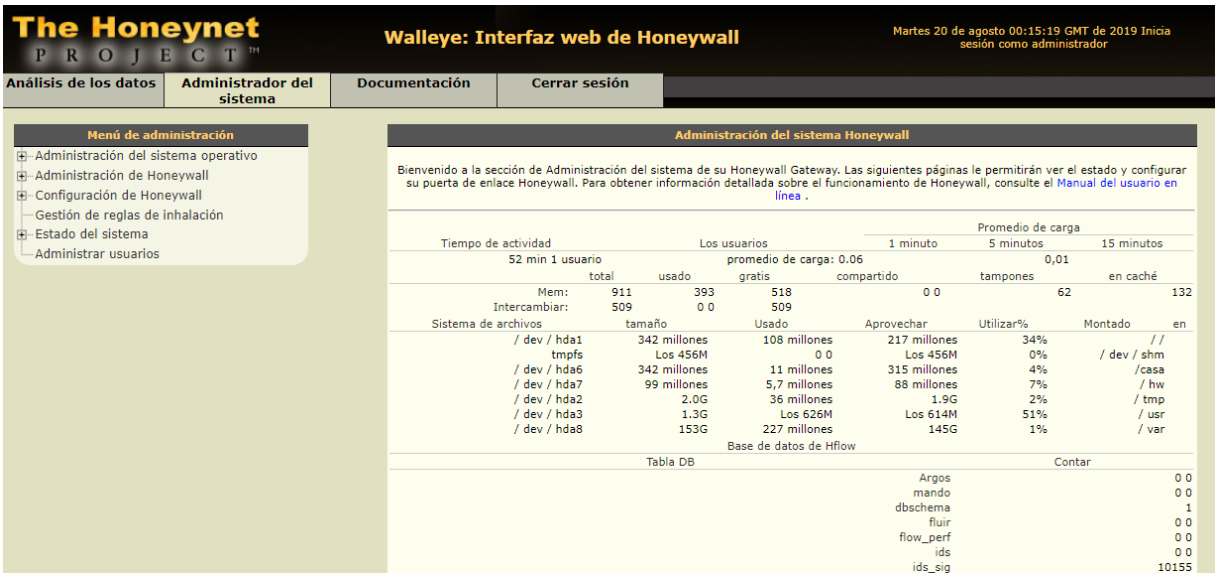


Ilustración 23 Administración del Sistema

Elaborado por: Bryam Yucta

Al dar clic en la parte que dice Administración de sistema operativo en el cual se encuentra las siguientes opciones:

- Limpiar directorio de registro: Elimina todos los archivos de registro del honeywall y los guarda en /var/log,
- Configuración de demonio SSH: Esta opción es la más importante ya que es por el medio en el cual se puede comunicar con el honeywall.

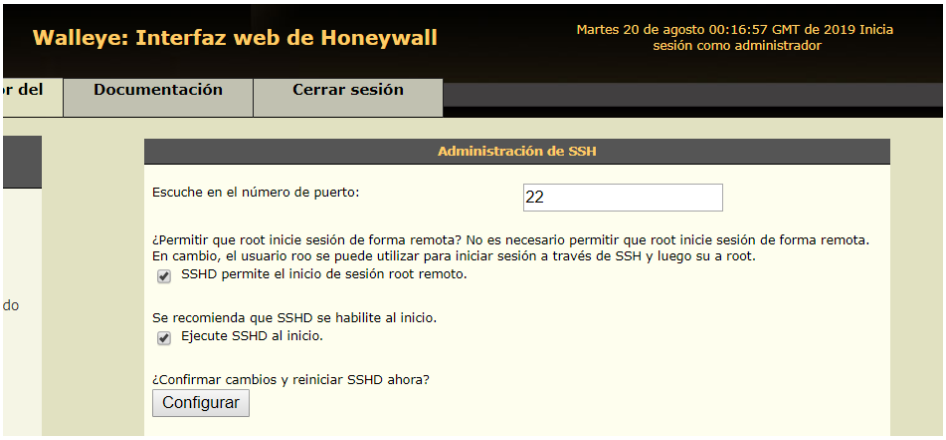


Ilustración 24 Demonio SSH

Elaborado por: Bryam Yucta

- Cambiar el nombre del Host: ayuda a cambiar el nombre del host.
- Configuración de teclado: Como lo dice ayuda a ver la distribución del teclado para el honeywall
- Reiniciar honeywall.

Administración de Honeywall

Se cuenta con tres opciones las cuales son:

- Administración de archivos de configuración: en el cual ayuda sacar un archivo de configuración para poder exportarlo.
- Bloqueo de emergencia: En caso de un fallo esta opción ayuda a bloquear el tráfico de entrada y salida, excepto la interfaz de administración.
- Reiniciar procesos de Honeywall: Permite iniciar/reiniciar procesos que se ejecutan en el honeywall como: Snort, Pcap, P0f, Sebekd, argus, Hflowd.

Ilustración 25Procesos de honeywall

Elaborado por: Bryam Yucta

Configuración de Honeywall: Revisa la configuración de nuestra honeynet.

- Información IP: cuneta con la información de las interfaces de red, así como la dirección IP de los honeypots.

Ilustración 26 Información IP

Elaborado por: Bryam Yucta

- Gestión Remota: El propósito de esta sección es configurar la administración remota y el acceso al honeywall.

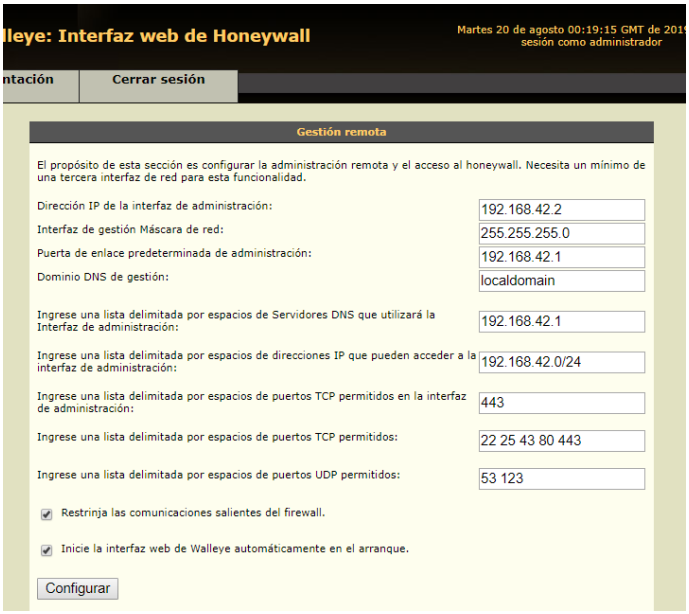


Ilustración 27 Gestión remota

Elaborado por: Bryam Yucta

- Límite de conexión: es uno de los métodos de control de datos, se cuenta las conexiones salientes y, cuando se cumple un cierto límite.

Ilustración 28 Límite de conexión

Elaborado por: Bryam Yucta

- Manejo de DNS: Se ingresa las direcciones IP de nuestro honeypots separados por un espacio, de la misma forma las direcciones de los DNS, es decir los honeypots podrá conectarse libremente y esta actividad no se registra, cuenta o alerta.
- Alertando: Alertas por correo electrónico se generan para cualquier actividad saliente. Esto es una indicación que un sistema se ha visto comprometido o que está ocurriendo una actividad no autorizada.
- Resumen del honeywall: Permite configurar informes de resumen diario de la actividad del honeywall. Estos informes van a la misma dirección de correo electrónico que utiliza para las alertas.
- Listas en blanco y negro: Afecta directamente al firewall es decir que lista negra significa soltar e ignorar y lista blanca significa permitir e ignorar, de esta forma los honeypots ignoraran alguna información.
- Sebek: una de las principales herramientas para captura de datos.

Ilustración 29 Sebek

Elaborado por: Bryam Yucta

- Roach Motel Mode: Bloqueará todo el tráfico saliente de los honeypots.
- Lista de variables de cerca: permite filtrar el tráfico a sistemas o rede específicos.
- Gestión de datos: revisa el tiempo que se tendrá para guardar la información generada.
- Gestión de reglas: ayuda a la configuración de las reglas de snort.

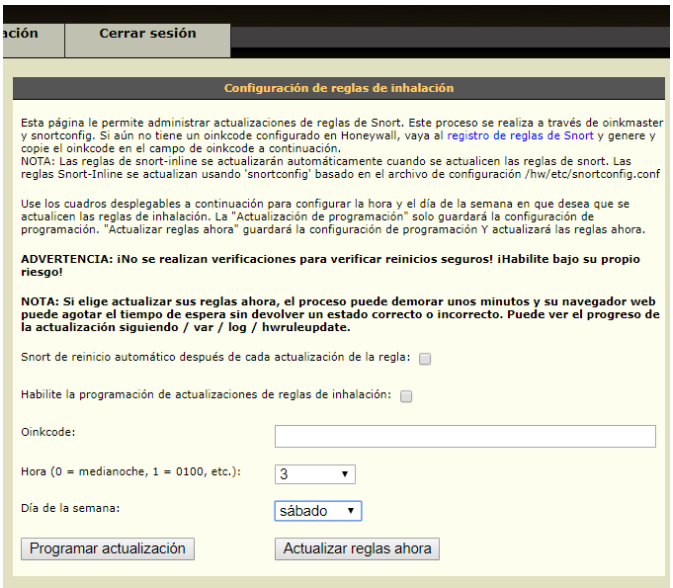


Ilustración 30 Reglas de Snort

Elaborado por: Bryam Yucta

Documentación

Información detallada para la configuración y mantenimiento de la honeynet, así como el control de datos.

Ilustración 31 Documentación

Elaborado por: Bryam Yucta

Hay que tomar en cuenta que la implementación la honeynet ayuda a tener un ambiente simulado ante lo servicios que brinda la Universidad Nacional de Chimborazo de esta forma con la ayuda de los diferente honeypots implementado en la honeynet tendremos la facilidad de capturar toda la información referente a los ataques que ingresan diariamente a la institución.

Anexo 5: Instalación y Configuración del Honeywall

Instalación y Configuración del Honeywall

En el programa de virtualización Oracle Virtual Box, se crea una nueva máquina virtual con las especificaciones antes mencionadas, se inicia el Sistemas Operativo Roo 1.4.

HW 20080424215739

Esta será la pantalla de bienvenida de Honeywall, indica que todos los datos del disco duro serán borrador tras su instalación.

Ilustración 32: Pantalla de Bienvenida de Honeywall

Elaborado por: Bryam Yucta

El sistema formateará el disco e instalará el honeywall

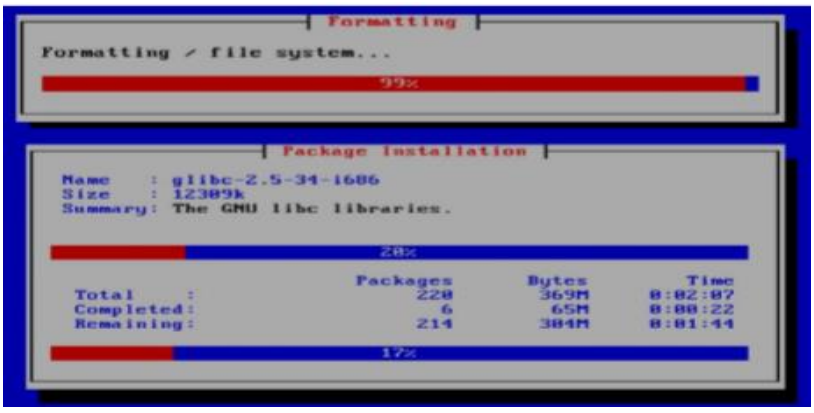


Ilustración 33: Instalación del Honeywall

Elaborado por: Bryam Yucta

Al terminar la instalación mostrará la pantalla de ingreso, el usuario por defecto “roo” y la contraseña “honey”. Para la configuración de Honeywall se ejecuta “su -” y la contraseña “honey”.

Ilustración 34: Pantalla de Ingreso del Honeywall
Elaborado por: Bryam Yucta

En la siguiente pantalla se escoge la opción “Honeywall Configuration”.

Ilustración 35: Menú de Honeywall
Elaborado por: Bryam Yucta

En el método de configuración inicial tiene 3 opciones:

Floppy: Permite cargar configuraciones existentes en el disco.

Defaults: Cargará las configuraciones por defecto.

Interview: Se configura por primera vez.

Como es la primera vez se escoge la tercera opción.

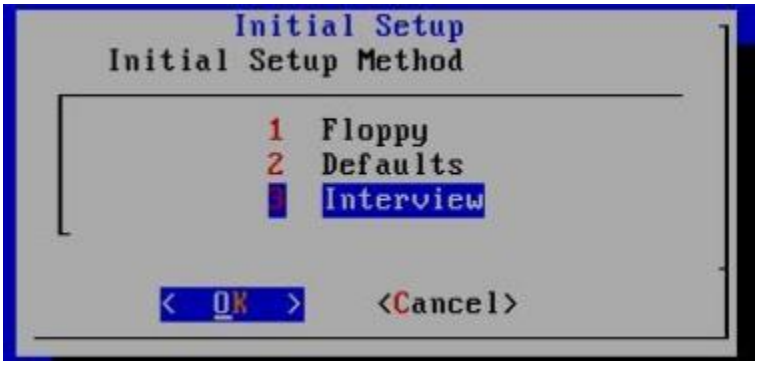


Ilustración 36: Configuración de Honeywall

Elaborado por: Bryam Yucta

En las siguientes pantallas se acepta los acuerdos.

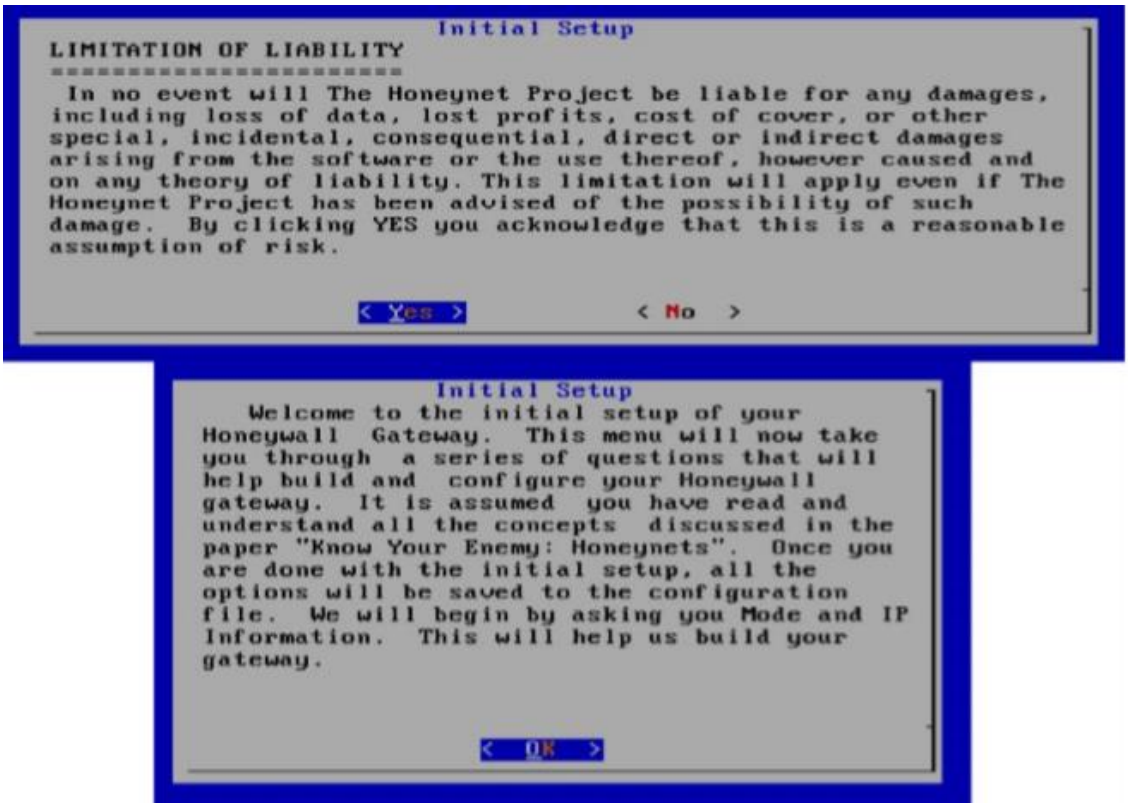


Ilustración 37: Acuerdo de Honeywall

Elaborado por: Bryam Yucta

Ingresar la dirección IP de los honeypots, si hay más de dos direcciones separar por espacio.

192.168.56.102 192.168.56.103 192.168.42.2

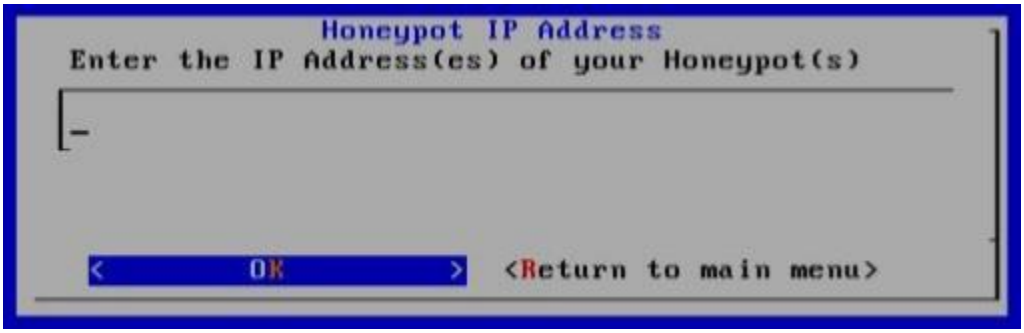


Ilustración 38: IPs de los honeypots

Elaborado por: Bryam Yucta

Ingresa la dirección de red en formato CIDR

192.168.56.0/24

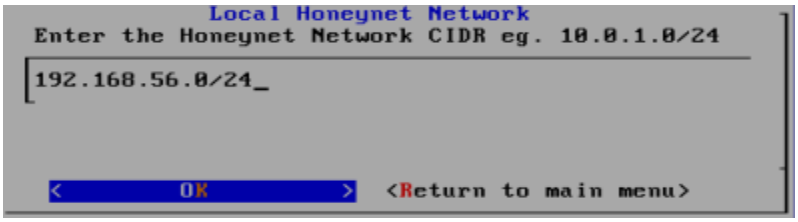


Ilustración 39: Dirección IP CIDR

Elaborado por: Bryam Yucta

Ingresar la dirección de broadcast de la red

192.168.56.255

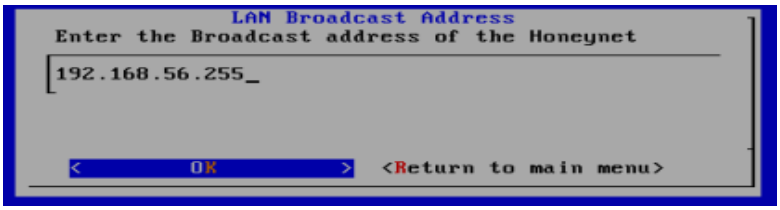


Ilustración 40: Dirección de Broadcast de la red

Elaborado por: Bryam Yucta

Indica que la primera parte de la configuración ha terminado y se acepta

Ilustración 41: Primera configuración terminada

Elaborado por: Bryam Yucta

Tarjeta de red conectará a la administración remota

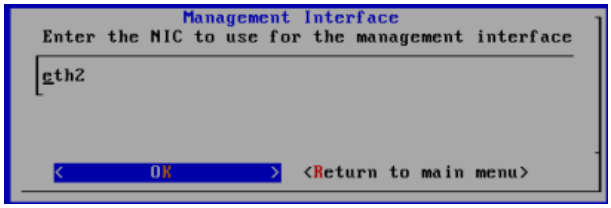


Ilustración 42: Red Administración

Elaborado por: Bryam Yucta

Pregunta si se quiere configurar la interfaz de administración remota.

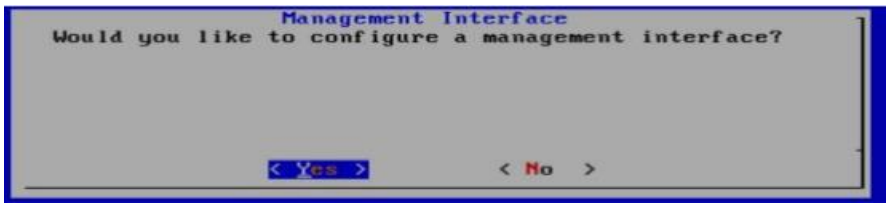


Ilustración 43: Aceptar la configuración remota

Elaborado por: Bryam Yucta

En la siguiente ventana se ingresa la dirección IP de Administración. 192.168.42.2

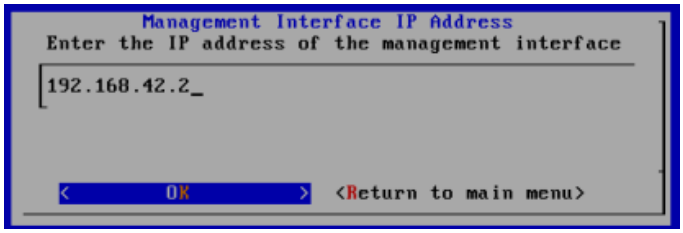


Ilustración 44: Dirección IP Administración

Elaborado por: Bryam Yucta

Se ingresa la dirección IP de (Gateway) o de entrada según nuestra configuración es: 192.168.42.1

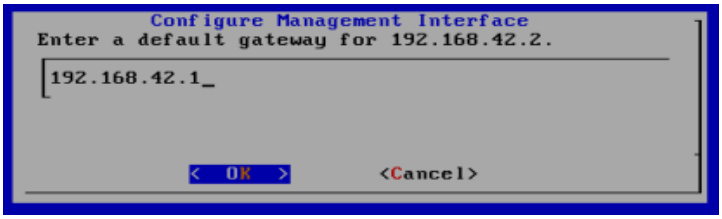


Ilustración 45: Gateway de Administración
Elaborado por: Bryam Yucta

Solicita el nombre del equipo en nuestro caso lo dejare por defecto localhost.

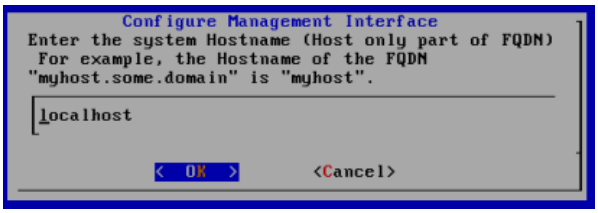


Ilustración 46: Nombre del equipo
Elaborado por: Bryam Yucta

Pide que se ingresa un dominio DNS por lo cual dejare por defecto.

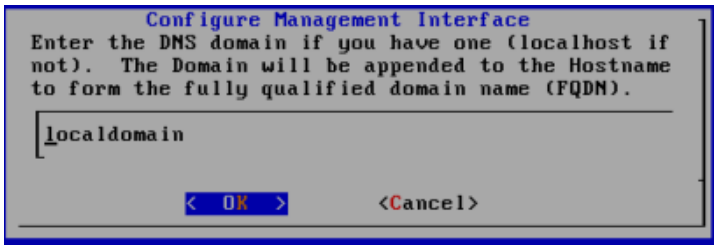


Ilustración 47: Dominio DNS

Elaborado por: Bryam Yucta

A continuación, se introduce la dirección IP del servidor DNS, para el uso del honeywall, en este caso 192.168.42.1, ya que es la primera IP de nuestra Red-Nat y junto con 192.168.42.2 que es la de administración, son las únicas IPS de esta red.

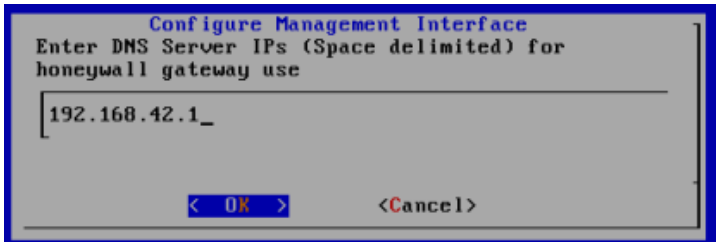


Ilustración 48: IP DNS Server

Elaborado por: Bryam Yucta

Una vez configurados los parámetros, la interfaz esta activada.

Ilustración 49: Activar la Interfaz

Elaborado por: Bryam Yucta

Y en la ventana siguiente se da clic en yes

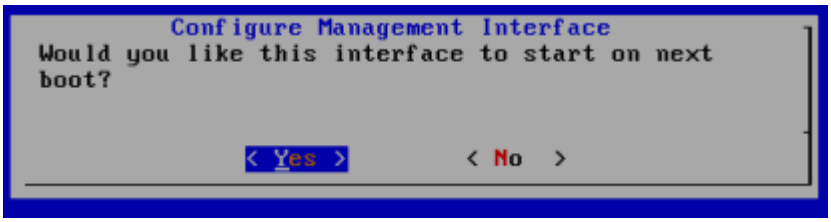


Ilustración 50: Iniciar Interfaz

Elaborado por: Bryam Yucta

Para una comunicación segura se configura el SSH

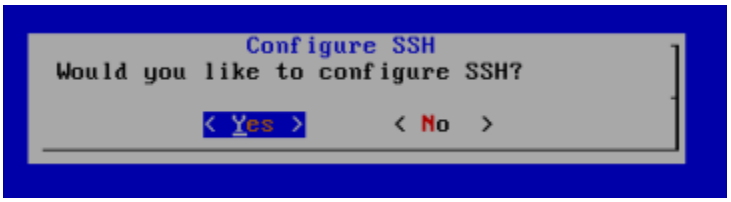


Ilustración 51: Configuración del SSH

Elaborado por: Bryam Yucta

En este caso se inicia sesión como super usuario, en la pantalla se da clic en yes

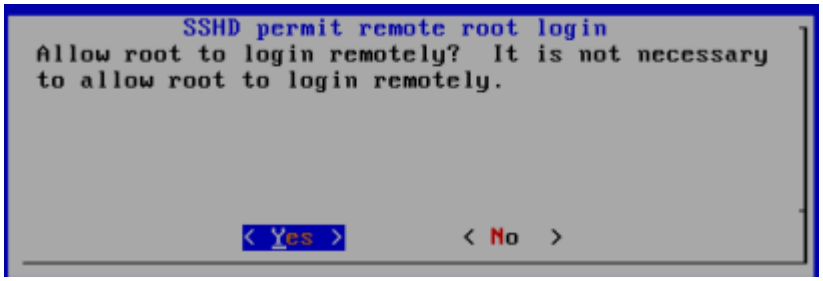


Ilustración 52: Ingresar como Súper Usuario

Elaborado por: Bryam Yucta

Se pedirá que cambien las contraseñas para los usuarios, en nuestro caso roo y root, pasaremos al siguiente paso.

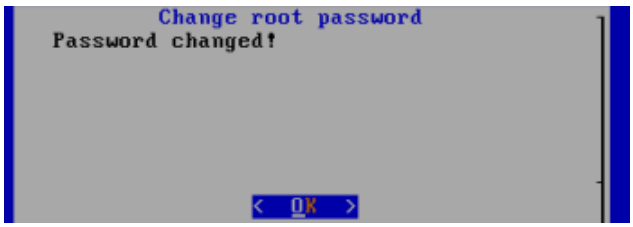


Ilustración 53: Cambio de contraseña de roo y root

Elaborado por: Bryam Yucta

Después como se ve en la captura, se solicita los puertos TCP, así como el puerto 22 que permite la gestión de mantenimiento, en este caso se ingresa el 443.

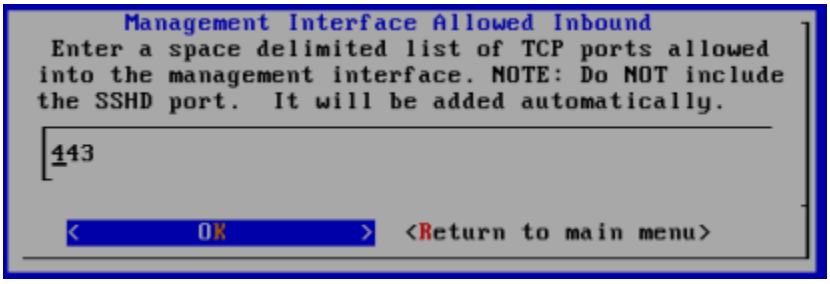


Ilustración 54: Puerto de mantenimiento

Elaborado por: Bryam Yucta

La red desde la cual se podrá acceder a la interfaz de mantenimiento en este caso la subred completa 192.168.42.0/24, aunque solo tiene dos IPS en uso la 192.168.42.1 y 192.168.42.2

Ilustración 55: Dirección IP de mantenimiento

Elaborado por: Bryam Yucta

De la misma forma se actica el uso de la interfaz web para el análisis de datos y mantenimiento, recuerde el uso del puerto 443.

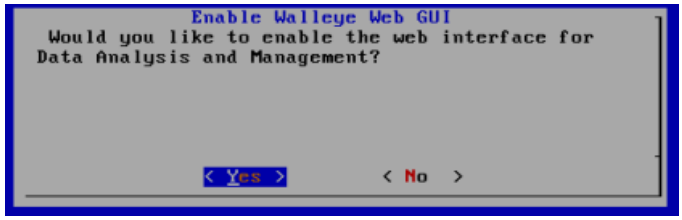


Ilustración 56: Activar el uso de la interfaz web

Elaborado por: Bryam Yucta

Se registran las comunicaciones salientes.

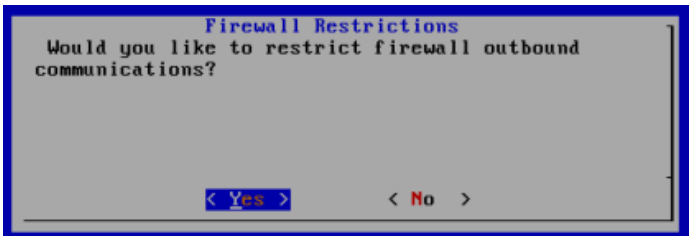


Ilustración 57: Restringir comunicación

Elaborado por: Bryam Yucta

A continuación, se autoriza los siguientes puertos TCP.

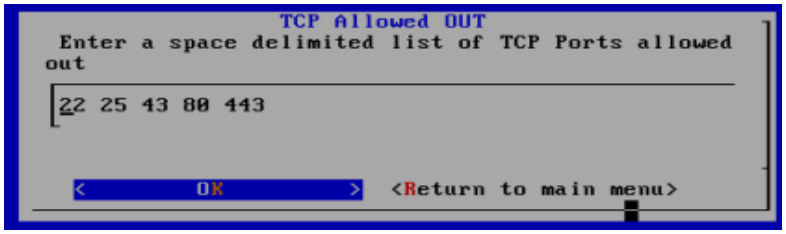


Ilustración 58: Autorizar puertos

Elaborado por: Bryam Yucta

De la misma forma los puertos UDP.

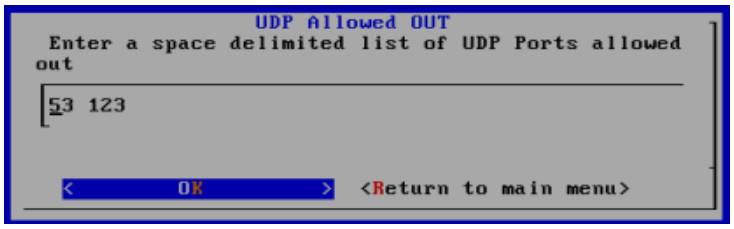


Ilustración 59: Puertos UDP
Elaborado por: Bryam Yucta

Se culmina esta parte de la configuración.

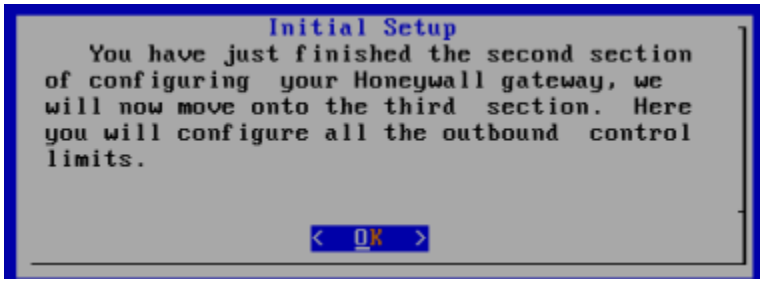


Ilustración 60: Terminar la configuración

Elaborado por: Bryam Yucta

En las siguientes pantallas se configura la escala de tiempo para la recolección de datos.

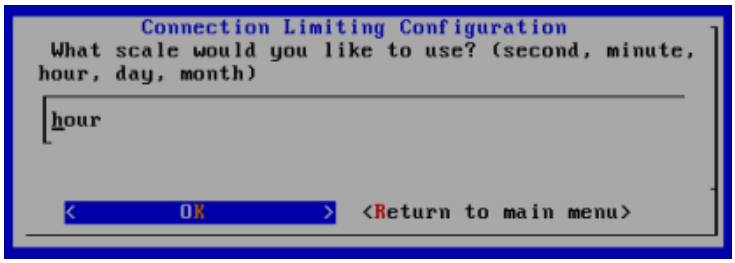


Ilustración 61: Hora

Elaborado por: Bryam Yucta

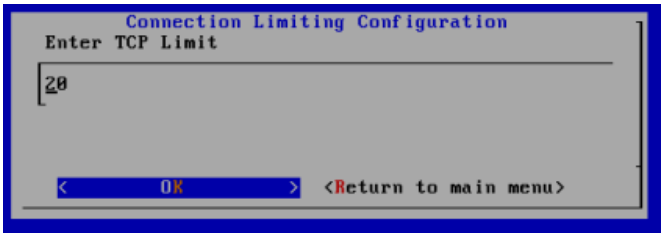


Ilustración 62: TCP 20

Elaborado por: Bryam Yucta

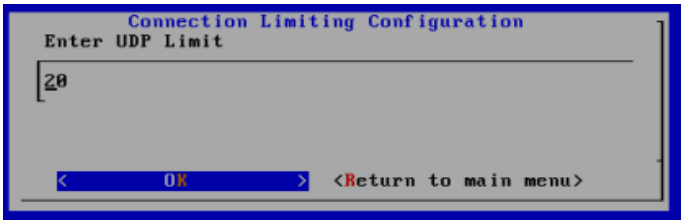


Ilustración 63 UDP 20
Elaborado por: Bryam Yucta

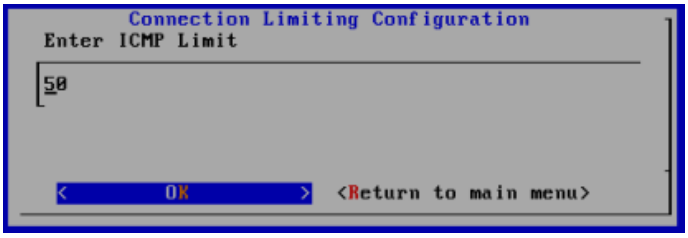


Ilustración 64 ICMP 50
Elaborado por: Bryam Yucta

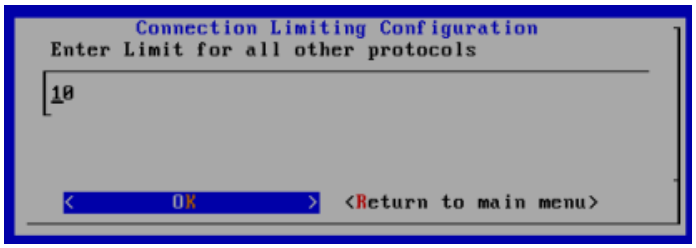


Ilustración 65: Limite de protocolo
Elaborado por: Bryam Yucta

En la siguiente ventana clic en YES. es para que el firewall envié paquetes a snort-line

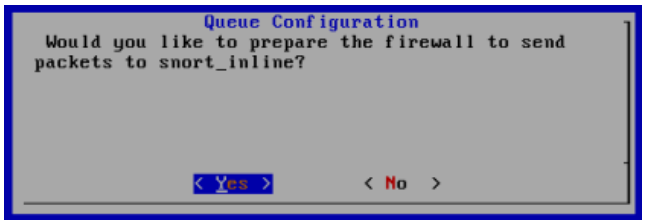


Ilustración 66: Paquetes de snort_line
Elaborado por: Bryam Yucta

A continuación, se solicita que ingrese el path al archivo donde el firewall encontrará las IPS de los equipos para que sean rechazados.

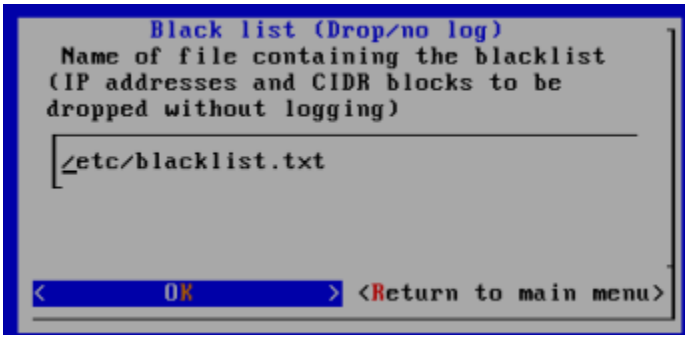


Ilustración 67: Black list
Elaborado por: Bryam Yucta

En la siguiente ventana clic en OK, es para los equipos que se pueden conectar.

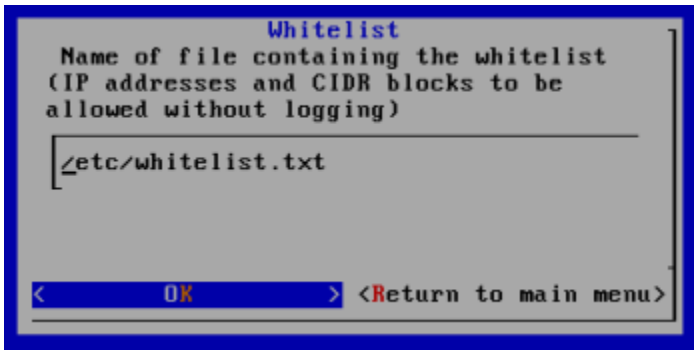


Ilustración 68: Wistelist
Elaborado por: Bryam Yucta

Preguntará si desea que se utilicen ambos archivos para la ejecución de filtros clic en SI.

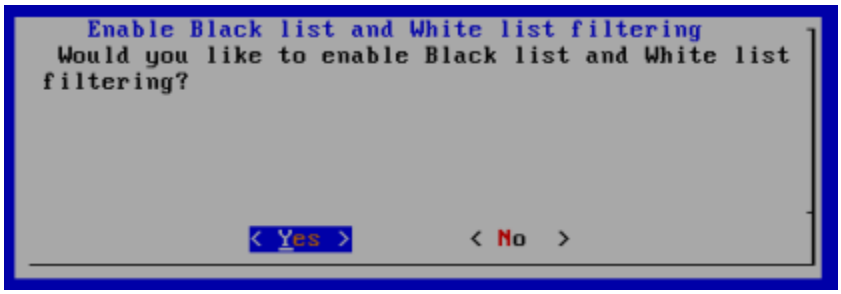


Ilustración 69: Archivos filtro
Elaborado por: Bryam Yucta

En la siguiente ventana clic en NO ya que pregunta sobre el desactivar la opción de filtrado de captura escrita.

Ilustración 70: Captura de filtrado escrito
Elaborado por: Bryam Yucta

En la siguiente ventana se deja por defecto, ya que se configura que ninguna dirección bajo ningún concepto se conecten con nuestros honeypots.

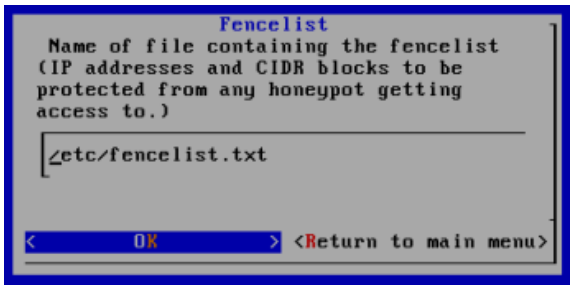


Ilustración 71: Configurar restricciones
Elaborado por: Bryam Yucta

Clic en NO.

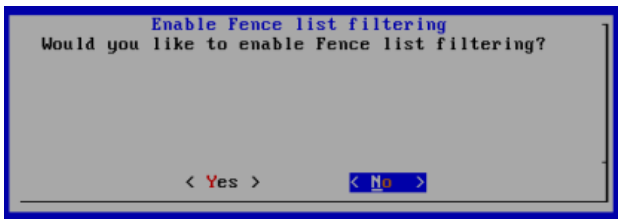


Ilustración 72: Captura de listas cercanas
Elaborado por: Bryam Yucta

Si se desea activar el modo Roach motel, que desactiva todo el tráfico saliente de nuestro honeypots clic en NO.

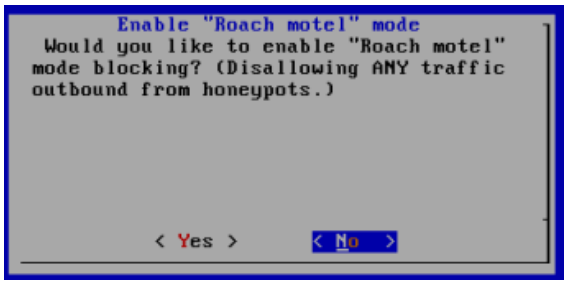


Ilustración 73: Roach motel
Elaborado por: Bryam Yucta

Para terminar la tercera parte de la configuración se mostrará una pantalla en la cual clic en OK.

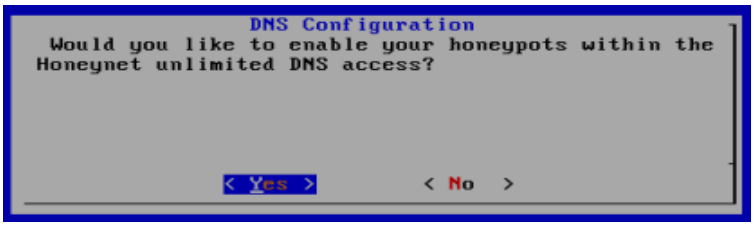


Ilustración 74: Pantalla de Servidores DNS
Elaborado por: Bryam Yucta

Clic en NO para la restricción de acceso ilimitado de los honeypots hacia servidores DNS externos.

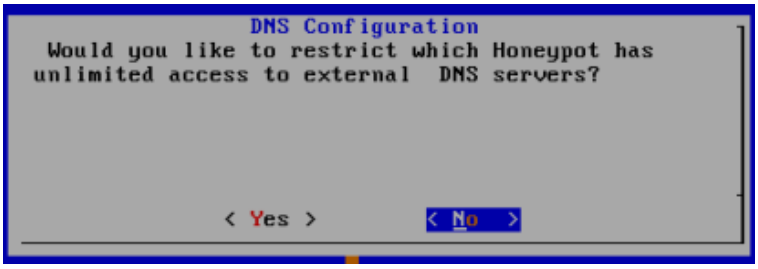


Ilustración 75: Restricción para acceso ilimitado
Elaborado por: Bryam Yucta

Y también se restringe a cuál servidor DNS puede tener acceso ilimitado

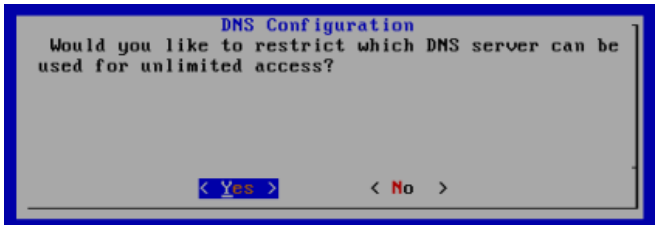


Ilustración 76: Restricción de servidor DNS
Elaborado por: Bryam Yucta

A continuación, se indica cual es la dirección IP del servidor DNS

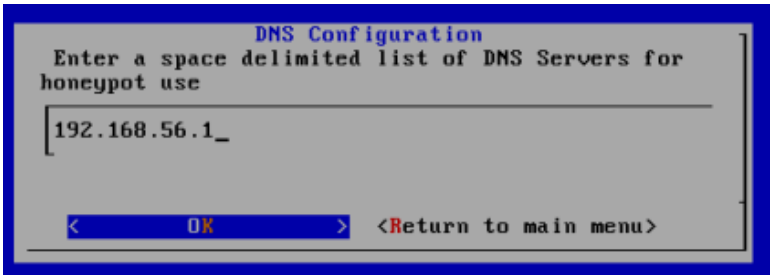


Ilustración 77: Dirección IP del servidor DNS
Elaborado por: Bryam Yucta

Y se habrá finalizado la quinta sección de configuración de honeywall como se observa a continuación.

Ilustración 78: Configuración terminada
Elaborado por: Bryam Yucta

Para finalizar se configura la sección de alertas, a continuación, se configura las alertar del Email.

Ilustración 79: Configuración de Alertas
Elaborado por: Bryam Yucta

Pedirá que se introduzca un email, pero en este caso se toma la opción por defecto, y avisa que se debe autorizar el tráfico saliente en el puerto 25, de esta forma se asegura el servidor de email acepte el correo con origen en nuestro honeywall.

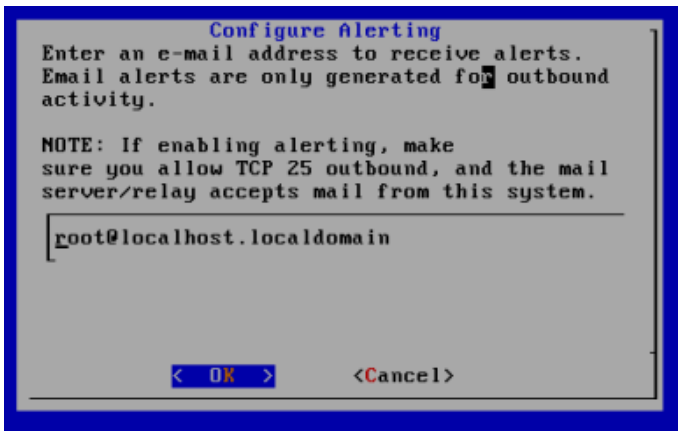


Ilustración 80: Configuración del Correo
Elaborado por: Bryam Yucta

Se activa el sistema con las alertas activadas al inicio.

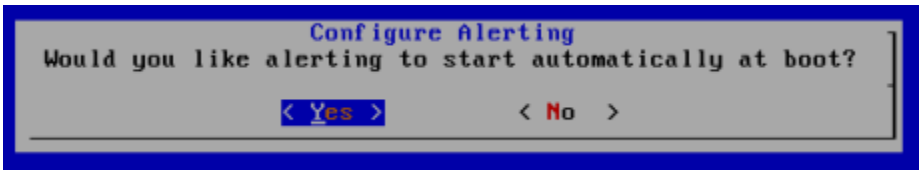


Ilustración 81: Configuración de alertas de inicio
Elaborado por: Bryam Yucta

Se configura para ver como nuestro honeywall Gateway va a manejar los paquetes producidos por nuestro honeypot de alta interacción Sebek, por tanto, clic en sí.

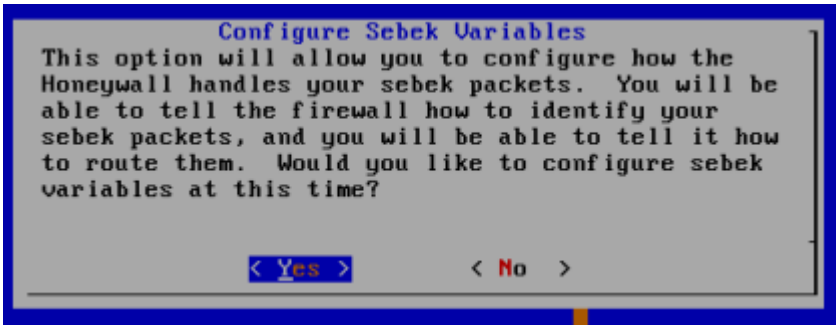


Ilustración 82: Interacción con Sebek
Elaborado por: Bryam Yucta

Se ingresa la dirección IP de destino de los paquetes de Sebek en este caso: 192.168.56.254

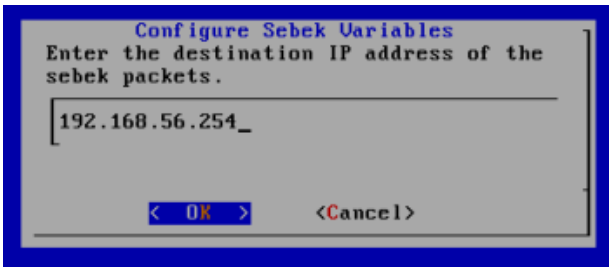


Ilustración 83: IP de destino de Sebek
Elaborado por: Bryam Yucta

Y por supuesto el puerto de destino.

Ilustración 84: Puerto de destino

Elaborado por: Bryam Yucta

Preguntara por lo que se desee que realice con los paquetes Sebek que reciba, pues se selecciona que los acepte y que cree un registro de estos.

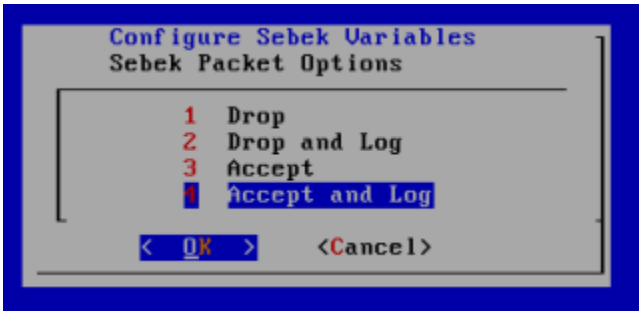


Ilustración 85: Archivos log de Sebek

Elaborado por: Bryam Yucta

Y se finaliza la configuración de nuestra honeywall, en la ventana siguiente clic en OK e indicará que se va a reiniciar.

Ilustración 86: Finalizar la configuración

Elaborado por: Bryam Yucta

Anexo 6 Configuración de servicios DNS y WEB

Una vez instalado Ubuntu server 14.04 se procede a actualizar todos los paquetes con el comando "**apt-get update**"

Una vez actualizado los paquetes se instalaras nuestro servidor bind9 estos lo hacemos con el comando **"apt-get install bind9**"

A continuación, cambiamos nuestra tarjeta de red a estática

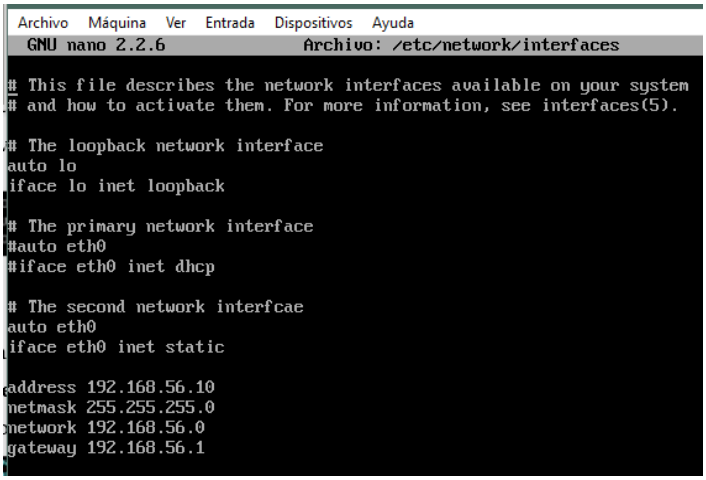


Ilustración 87: Interfaz de red estática
Elaborado por: Bryam Yucta

A continuación, vamos a configurar la zona directa e inversa la cual nos va ayudara con la comunicación con el servidor DNS

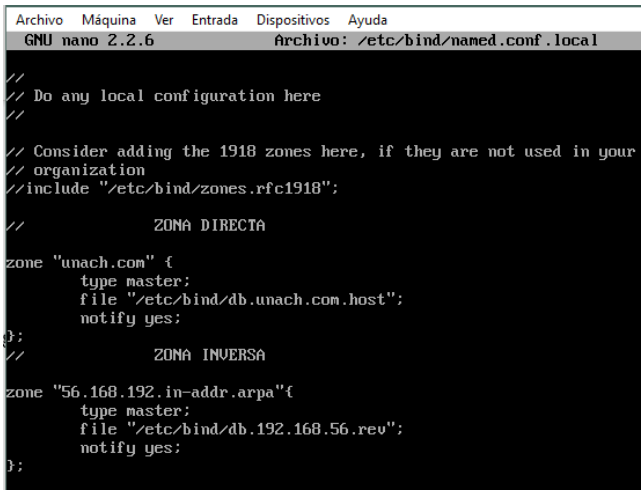


Ilustración 88 Zona directa e inversa
Elaborado por: Bryam Yucta

Para continuar se debe verificar que la sintaxis del archivo “named.conf.local” esté correcta esto lo realiza con el siguiente comando “named-checkconf” y el nombre del archivo, luego de esto crearemos los archivos que definirán los valores y registros de las zonas declaradas en el punto anterior.

```
 GNU nano 2.2.6                Archivo: db.unach.com.host

;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     unach.com. root.unach.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@                       IN      NS      unach.com.
unach.com.              IN      A       192.168.56.10
dns.unach.com.          IN      A       192.168.56.10
dns2.unach.com.         IN      A       192.168.56.5
pc1.unach.com.          IN      A       192.168.56.11
pc2.unach.com.          IN      A       192.168.56.12
```

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
 GNU nano 2.2.6                Archivo: db.192.168.56.rev

;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     unach.com. root.unach.com. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      unach.com.
10      IN      PTR     unach.com.
10      IN      PTR     dns.unach.com.
5       IN      PTR     dns2.unach.com.
11      IN      PTR     pc1.unach.com.
12      IN      PTR     pc2.unach.com.
```

Ilustración 89 Archivo rev y host
Elaborado por: Bryam Yucta

Reiniciar el servidor DNS para actualizar los cambios esto se lo realiza de la siguiente manera:

```
root@ubuntu:/etc/bind# /etc/init.d/bind9 restart
 * Stopping domain name service... bind9
waiting for pid 1008 to die

 * Starting domain name service... bind9
root@ubuntu:/etc/bind#
```

Ilustración 90 Reiniciar bind9
Elaborado por: Bryam Yucta

Se comprueba la resolución DNS inversa y directa

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@ubuntu:~# nslookup
> 192.168.56.10
Server:         192.168.56.10
Address:        192.168.56.10#53

10.56.168.192.in-addr.arpa      name = unach.com.
10.56.168.192.in-addr.arpa      name = dns.unach.com.
> unach.com
Server:         192.168.56.10
Address:        192.168.56.10#53

Name:   unach.com
Address: 192.168.56.10
> 192.168.56.11
Server:         192.168.56.10
Address:        192.168.56.10#53

11.56.168.192.in-addr.arpa      name = pc1.unach.com.
> 192.168.56.12
Server:         192.168.56.10
Address:        192.168.56.10#53

12.56.168.192.in-addr.arpa      name = pc2.unach.com.
```

Ilustración 91 Prueba del Servidor DNS
Elaborado por: Bryam Yucta

Una vez terminada la instalación y configuración del servidor DNS, realizaremos la instalación y configuración de nuestro servidor web Apache2

Como primer paso debemos actualizar nuestro Ubuntu y a continuación ejecutar el siguiente comando.

```
root@servidor:/home/proyecto# apt-get install apache2
```

Ya configurado nuestra dirección IP estáticas la cual se comunicará con nuestro servidor DNS

Editamos el archivo "**vim /etc/hosts"** de la siguiente manera.

Ilustración 92 Archivo hosts
Elaborado por: Bryam Yucta

Para poder alojar una página web debemos crear un directorio virtual dentro de /var/www con el siguiente comando

"mkdir –p /var/www/proyecto":

En el cual con el comando nano crearemos nuestro archivo index.html

Para que nuestro archivo se muestre en el servidor web editaremos el siguiente archivo "000-default.conf" pero como creamos otro directorio llevara el nombre del mismo es decir se realizado una copia

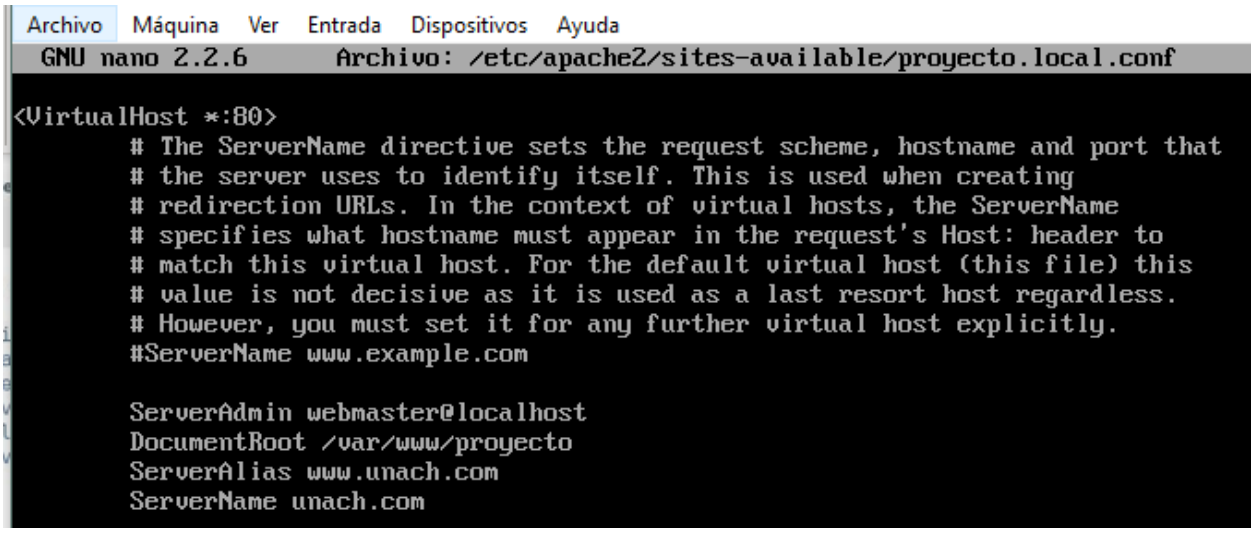


Ilustración 93 Comunicación del Servidor
Elaborado por: Bryam Yucta

Anexo 7 Recolección De Ataques Capturados Según el estado Actual
Detalle del ataque AD 1.1

Mensaje	ATTACK RESPONSES Microsoft cmd.exe banner
Resumen	Este evento se genera cuando un banner de cmd.exe de Windows es detectado en una sesión TCP.
Impacto	Acceso remoto
Información Detallada	Este evento indica que un banner de cmd.exe de Windows ha sido detectado en una sesión TCP. Esto indica que alguien tiene la capacidad de generar un símbolo del sistema de comandos de DOS sobre TCP.
Fallo del Sistema	Sistemas operativos Windows.
Escaneo de ataque	Un atacante podría estar utilizando una puerta trasera para generar un DOS shell de comando obteniendo así acceso a la operación sistema y todos los datos en el host.
Facilidad de ataques	Simple
Acciones correctivas	Actualice a la última versión no afectada del software.

Tabla 15 Detalle de Ataque 1 Estado Actual
Elaborado por Bryam Yucta

Detalle del ataque AD 2.1

Mensaje	Destino ICMP Comunicación inalcanzable con destino El host está prohibido administrativamente
Resumen	Este evento se genera cuando no se puede alcanzar un destino ICMP (La comunicación con el host de destino es administrativamente Prohibido) el datagrama se detecta en la red
Impacto	Este mensaje se genera cuando un datagrama no puede atravesar la red. Esto podría ser una indicación de enrutamiento o problemas de red
Información Detallada	Esta regla genera eventos informativos sobre la red. Grande los números de estos mensajes en la red podrían indicar enrutamiento problemas, dispositivos de enrutamiento defectuosos o hosts configurados incorrectamente.
Fallo del Sistema	Ninguno conocido
Escaneo de ataque	Ninguno conocido
Facilidad de ataques	Numerosas herramientas y scripts pueden generar estos tipos de ICMP datagramas
Acciones correctivas	Esta regla detecta información de red informativa, por lo que no La acción correctiva es necesaria.

Tabla 16 Detalle de Ataque 2

Estado Actual Elaborado por Bryam Yucta

Detalle del ataque AD 3.1

Mensaje	ICMP L3retriever Ping
Resumen	Este evento se genera cuando se realiza una solicitud de eco ICMP desde un host que ejecuta el escáner de seguridad L3 "Retriever 1.5"
Impacto	Recopilación de información. Una solicitud de eco ICMP puede determinar si un host está activo
Información Detallada	El comando ping utiliza una solicitud de eco ICMP para obtener un Respuesta de eco ICMP de un anfitrión en vivo que escucha. Una solicitud de eco que se origina en un host que ejecuta el escáner de seguridad L3 "Retriever 1.5" contiene una carga útil única en la solicitud de mensaje.
Fallo del Sistema	Todo
Escaneo de ataque	Ninguno conocido
Facilidad de ataques	siempre
Acciones correctivas	Bloquee las solicitudes entrantes de eco ICMP.

Tabla 17 Detalle de Ataque 3 Estado Actual
Elaborado por Bryam Yucta

Detalle del ataque AD 4.1

Mensaje	NETBIOS DCERPC NCACN-IP-TCP IActivation remoteactivation little endian overflow attempt
Resumen	Este evento se genera cuando se realiza una solicitud de eco ICMP desde un host que ejecuta el escáner de seguridad L3 "Retriever 1.5"
Impacto	Negación de servicio. Posible ejecución de código arbitrario que conduce a acceso administrativo remoto no autorizado
Información Detallada	Existe una vulnerabilidad en el servicio RPCSS de Microsoft que maneja RPC DCOM solicita tal ejecución de código arbitrario o una Denegación de La condición de servicio se puede emitir contra un host enviando datos a través de RPC. El modelo de objetos componentes distribuidos (DCOM) maneja DCOM solicitudes enviadas por clientes a un servidor utilizando RPC. Una solicitud mal formada al host que ejecuta el servicio RPCSS puede generar un búfer condición de desbordamiento que presentará al atacante la oportunidad ejecutar código arbitrario con los privilegios del sistema local cuenta. Alternativamente, el atacante también podría causar el servicio RPC

	dejar de responder solicitudes RPC y, por lo tanto, provocar una Denegación de servicio condición para ocurrir
Fallo del Sistema	Todo
Escaneo de ataque	Ninguno conocido
Facilidad de ataques	siempre
Acciones correctivas	Bloquee las solicitudes entrantes de eco ICMP.

Tabla 18 Detalle de Ataque 4 Estado Actual
Elaborado por Bryam Yucta

Detalle del ataque AD 5.1

Mensaje	NETBIOS SMB-DS lsass Ds Roler Actualizar servidor de nivel inferior pequeño intento de desbordamiento endian unicode
Resumen	Este evento se genera cuando se intenta explotar un búfer condición de desbordamiento en productos de Microsoft a través de la seguridad local Servicio de Subsistema de Autoridad (LSASS).
Impacto	Ejecución remota de código arbitrario.
Información Detallada	Existe una vulnerabilidad en LSASS que puede presentar a un atacante con la oportunidad de ejecutar el código de su elección en un host afectado.
Fallo del Sistema	Microsoft Windows 2000, 2003 and XP systems.
Escaneo de ataques	Un atacante necesita hacer una solicitud especialmente diseñada para LSASS servicio que podría contener código dañino para obtener mayor acceso al sistema.
Facilidad de ataques	Moderado
Acciones correctivas	Aplique los parches provistos por el proveedor apropiado

Tabla 19 Detalle de Ataque 5 Estado Actual
Elaborado por Bryam Yucta

Detalle del ataque AD 6.1

Mensaje	WEB-CGI formmail access
Resumen	Este evento se genera cuando se intenta explotar un conocido vulnerabilidad en la aplicación web CGI Formmail que se ejecuta en un servido
Impacto	Varias vulnerabilidades incluyen acceso al servidor, divulgación de información, retransmisión de spam y anonimato de correo.
Información Detallada	Este evento se genera cuando se intenta acceder al perl script cgi Formmail. Las primeras versiones (1.6 y anteriores) tenían varias vulnerabilidades (motor de spam, capacidad de ejecutar comandos bajo la identificación del servidor y establecer variables de entorno) y debe actualizarse de inmediato. Los spammers aún pueden usar versiones más nuevas para anonimizar el correo electrónico y derrotar los controles de retransmisión de correo electrónico.
Fallo del Sistema	Todo
Escaneo de ataque	Ninguno conocido
Facilidad de ataques	siempre
Acciones correctivas	Bloquee las solicitudes entrantes de eco ICMP.

Tabla 20 Detalle de Ataque 6 Estado Actual
Elaborado por Bryam Yucta

Anexo 8 Recolección De Ataques Capturados por la Honeynet
Ataque detectado 1: AD1

Ilustración 94 Detección de Ataque 1
Elaborado por: Bryam Yucta

Detalle de ataque AD 1.1

Tabla 21 RESPUESTAS DE ATAQUE Microsoft cmd.exe banner

Mensaje	RESPUESTAS DE ATAQUE Microsoft cmd.exe banner
Resumen	Este evento se genera cuando un banner de cmd.exe de Windows es detectado en una sesión TCP.
Impacto	Acceso Remoto
Información Detallada	Este evento indica que un banner de cmd.exe de Windows ha sido detectado en una sesión TCP. Esto indica que alguien tiene la capacidad de generar un símbolo del sistema de comandos de DOS sobre TCP.
Fallo del Sistema	Sistema Operativo Windows
Escaneo de ataques	Escenario de ataque Un atacante podría estar utilizando una puerta trasera pasa generar un DOS Shell de comando obteniendo así acceso al sistema operativo y todo
Facilidad de ataques	Simple
Acciones correctivas	Acción correctiva verifique si el anfitrión tienes signos de compromiso

Elaborado por: Bryam Yucta

Ataque detectado 2: AD2

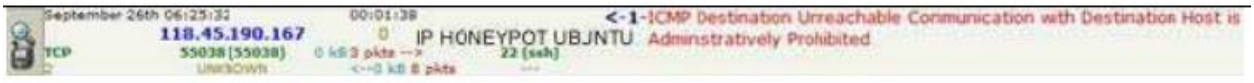


Ilustración 95 Detección de Ataque 2
Elaborado por: Bryam Yucta

Detalle de Ataque AD 2.1

Mensaje	Destino ICMP Comunicación inalcanzable con destino El host está prohibido administrativamente
Resumen	Este evento se genera cuando no se puede alcanzar un destino ICMP (La comunicación con el host de destino es administrativamente Prohibido) el datagrama se detecta en la red
Impacto	Este mensaje se genera cuando un datagrama no puede atravesar el red. Esto podría ser una indicación de enrutamiento o problemas de red
Información Detallada	Esta regla genera eventos informativos sobre la red. Grande los números de estos mensajes en la red podrían indicar enrutamiento problemas, dispositivos de enrutamiento defectuosos o hosts configurados incorrectamente.
Fallo del Sistema	Ninguno conocido.
Escaneo de ataques	Ninguno conocido.
Facilidad de ataques	Numerosas herramientas y scripts pueden generar estos tipos de ICMP datagramas
Acciones correctivas	Esta regla detecta información de red informativa, por lo que no La acción correctiva es necesaria.

Tabla 22 Destino ICMP Comunicación inalcanzable con destino
Elaborado por: Bryam Yucta

Ataque detectado3; AD3

Ilustración 96 Detección de ataque 3
Elaborado por: Bryam Yucta

Datadle del ataque AD 3.1

Mensaje	ICMP L3retriever Ping
Resumen	Este evento se genera cuando no se puede alcanzar un destino ICMP (La comunicación con el host de destino es administrativamente Prohibido) el datagrama se detecta en la red
Impacto	Recopilación de información. Una solicitud de eco ICMP puede determinar si un host está activo.

Información Detallada	El comando ping utiliza una solicitud de eco ICMP para obtener un Respuesta de eco ICMP de un anfitrión en vivo que escucha. Una solicitud de eco que se origina en un host que ejecuta el escáner de seguridad L3 "Retriever 1.5" contiene una carga útil única en la solicitud de mensaje.
Fallo del Sistema	Todas
Escaneo de ataques	Un atacante puede intentar determinar hosts en vivo en una red antes de lanzar un ataque
Facilidad de ataques	Simple
Acciones correctivas	Bloquee las solicitudes entrantes de eco ICMP

Tabla 23 ICMP L3retriever Ping
Elaborado por: Bryam Yucta

Detalle del ataque 3.2

Mensaje	ICMP PING CyberKit 2.2 Windows
Resumen	Este evento se genera cuando se realiza una solicitud de eco ICMP desde un Host de Windows que ejecuta el software CyberKit 2.2
Impacto	Recopilación de información. Una solicitud de eco ICMP puede determinar si un host está activo.
Información Detallada	El comando ping utiliza una solicitud de eco ICMP para obtener una respuesta de eco ICMP de un host en vivo que escucha. Una solicitud de eco que se origina en un host de Windows que se ejecuta El software CyberKit 2.2 contiene una carga útil única en la solicitud de mensaje
Fallo del Sistema	Todas
Escaneo de ataques	Un atacante puede intentar determinar hosts en vivo en una red antes de lanzar un ataque
Facilidad de ataques	Simple
Acciones correctivas	Bloquee las solicitudes entrantes de eco ICMP

Tabla 24 ICMP PING CyberKit 2.2 Windows
Elaborado por: Bryam Yucta

Detalle del ataque AD3.3

Mensaje	ICMP PING NMAP
Resumen	Este evento se genera cuando un ping ICMP generalmente generado por Se detecta nmap.

Impacto	Esto podría indicar un escaneo completo por nmap que a veces es indicativo de comportamiento potencialmente malicioso.
Información Detallada	El ping ICMP de Nmap, por defecto, envía cero datos como parte del ping. Nmap normalmente hace ping al host a través de icmp si el usuario tiene privilegios de root, y utiliza un tcp-ping de lo contrario.
Fallo del Sistema	Todas
Escaneo de ataques	Como parte de un intento de recopilación de información, un atacante puede usar nmap para ver qué hosts están vivos en una red determinada. Si se usa nmap para el escaneo de puertos como root, el ping icmp ocurrirá de manera predeterminada a menos que el usuario especifica lo contrario
Facilidad de ataques	Trivial. Nmap requiere poca o ninguna habilidad para operar
Acciones correctivas	Si detecta otro tráfico sospechoso desde este host (es decir, un escaneo de puertos), siga el procedimiento estándar para evaluar qué amenaza puede representar esto. Si solo detecta el ping icmp, esto puede haber sido simplemente un 'ping barrer 'y puede ser ignorado.

Tabla 25 ICMP PING NMAP
Elaborado por: Bryam Yucta

Ataque detectado 4: AD4

Ilustración 97 Detección de Ataque 4
Elaborado por: Bryam Yucta

Detalle del ataque AD 4.1

Mensaje	NETBIOS DCERPC NCACN-IP-TCP Inactivation remote activation little endian overflow attempt
Resumen	Este evento se genera cuando se intenta explotar una conocida vulnerabilidad en el servicio RPCSS de Microsoft para RPC.
Impacto	Negación de servicio. Posible ejecución de código arbitrario que conduce a acceso administrativo remoto no autorizado
Información Detallada	Existe una vulnerabilidad en el servicio RPCSS de Microsoft que maneja RPC DCOM solicita tal ejecución de código arbitrario o una Denegación de la condición de servicio se puede emitir contra un host enviando datos a través de RPC.

	El modelo de objetos componentes distribuidos (DCOM) maneja DCOM solicitudes enviadas por clientes a un servidor utilizando RPC. Una solicitud mal formada al host que ejecuta el servicio RPCSS puede generar un búfer condición de desbordamiento que presentará al atacante la oportunidad ejecutar código arbitrario con los privilegios del sistema local cuenta. Alternativamente, el atacante también podría causar el servicio RPC dejar de responder solicitudes RPC y, por lo tanto, provocar una Denegación de servicio condición para que ocurra.
Fallo del Sistema	Windows NT 4.0 Workstation and Server Windows NT 4.0 Terminal Server Edition Windows 2000 Windows XP Windows Server 2003
Escaneo de ataques	Un atacante puede hacer una solicitud de enlace DCERPC seguida de una solicitud de activación remota DCERPC DCOM maliciosa.
Facilidad de ataques	Sencillo. El código de Expoit existe
Acciones correctivas	Si aplica los parches provistos por el proveedor apropiado

Tabla 26 NETBIOS DCERPC NCACN-IP-TCP
Elaborado por: Bryam Yucta

Detalle del ataque AD 4.2

Mensaje	NETBIOS SMB-DS IPC$ Unicode share access
Resumen	Este evento se genera cuando se intenta obtener acceso a recursos privados usando Samba.
Impacto	Recopilación de información y compromiso de integridad del sistema. Posible acceso administrativo no autorizado al servidor
Información Detallada	Este evento se genera cuando se intenta utilizar Samba para obtener acceso a recursos compartidos privados o administrativos en un host.
Fallo del Sistema	Todos los sistemas que usan Samba para compartir archivos. Todos los sistemas que utilizan archivos e impresiones compartidas para Windows.

Escaneo de ataques	Son posibles muchos vectores de ataque desde un directorio simple transversal para acceder directamente a los recursos compartidos administrativos de Windows.
Facilidad de ataques	Sencillo. No se requiere software de explotación.
Acciones correctivas	Asegúrese de que el sistema esté utilizando una versión actualizada del software y ha aplicado todos los parches suministrados por el proveedor.

Tabla 27 NETBIOS SMB-DS IPC$ Unicode share access
Elaborado por: Bryam Yucta

Ataque detectado 5: AD5

Ilustración 98 Detección de Ataque 5
Elaborado por: Bryam Yucta

Detalle del ataque AD5.1

Mensaje	NETBIOS SMB-DS lsass Ds Roler Actualizar servidor de nivel inferior pequeño intento de desbordamiento endian unicode
Resumen	Este evento se genera cuando se intenta explotar un búfer condición de desbordamiento en productos de Microsoft a través de la seguridad local Servicio de Subsistema de Autoridad (LSASS).
Impacto	Ejecución remota de código arbitrario.
Información Detallada	Existe una vulnerabilidad en LSASS que puede presentar a un atacante con la oportunidad de ejecutar el código de su elección en un host afectado.
Fallo del Sistema	Microsoft Windows 2000, 2003 and XP systems.
Escaneo de ataques	Un atacante necesita hacer una solicitud especialmente diseñada para LSASS servicio que podría contener código dañino para obtener mayor acceso al sistema.
Facilidad de ataques	Moderado
Acciones correctivas	Aplique los parches provistos por el proveedor apropiado

Tabla 28 NETBIOS SMB-DS lsass Ds Roler Actualizar servidor de
Elaborado por: Bryam Yucta

Ataque detectado 6: AD 6

Ilustración 99 Detección de Ataque 8
Elaborado por: Bryam Yucta

Detalle del ataque AD 6.1

Mensaje	WEB-CGI awstats Access
Resumen	Este evento se genera cuando se intenta acceder al cgi script awstats.pl.
Impacto	Posible ejecución de comandos del sistema.
Información Detallada	Adavanced Web Statistics (awstats) se usa para procesar el servidor web registra archivos y produce informes del uso del servidor web. Algunas versiones de awstats no desinfectan correctamente la entrada del usuario. Esta puede presentar a un atacante la oportunidad de suministrar el sistema comandos a través del parámetro "archivo de registro". Para que el ataque sea exitoso el parámetro "actualizar" también debe tener el valor establecido en "1". Esta El evento indica que se ha intentado acceder a awstats.pl script cgi.
Fallo del Sistema	Awstats 6.1 and prior
Escaneo de ataques	Un atacante puede proporcionar comandos de su elección como valor para el parámetro del archivo de registro al encerrar los comandos en caracteres de tubería.
Facilidad de ataques	Sencillo. No se requiere software de explotación.
Acciones correctivas	Asegúrese de que el sistema esté utilizando una versión actualizada del software.

Tabla 29 WEB-CGI awstats Access
Elaborado por: Bryam Yucta

Detalle del ataque AD6.2

Mensaje	WEB-CGI formmail access
Resumen	Este evento se genera cuando se intenta explotar un conocido vulnerabilidad en la aplicación web CGI Formmail que se ejecuta en un servidor.
Impacto	Varias vulnerabilidades incluyen acceso al servidor, divulgación de información, retransmisión de spam y anonimato de correo.
Información Detallada	Este evento se genera cuando se intenta acceder al perl script cgi Formmail. Las primeras versiones (1.6 y anteriores) tenían varias vulnerabilidades (motor de spam, capacidad de ejecutar comandos bajo la identificación del servidor y establecer variables de entorno) y debe actualizarse de inmediato. Los spammers aún pueden usar versiones más nuevas para anonimizar el correo electrónico y derrotar a los controles de retransmisión de correo electrónico

Fallo del Sistema	Todos los sistemas que ejecutan Form mail
Escaneo de ataques	Se puede agregar información a la URL para usar su puerta de enlace de correo evitando los controles de relé SMTP. La información del encabezado HTTP puede ser manipulado para evitar métodos de control de acceso en script. Permite explotaciones SMTP que normalmente solo están disponibles para personas de confianza usuarios (locales) como Sendmail% hack.
Facilidad de ataques	Sencillo.
Acciones correctivas	Asegúrese de que el sistema esté utilizando una versión actualizada del software y ha aplicado todos los parches suministrados por el proveedor.

Tabla 30 WEB-CGI formmail access
Elaborado por: Bryam Yucta

Ataque detectado 7: AD7

Ilustración 100 Detección de Ataque 7
Elaborado por: Bryam Yucta

Detalle del ataque 7.1

Mensaje	WEB-CGI guestbook.cgi access
Resumen	Este evento se genera cuando se intenta explotar un conocido vulnerabilidad en una aplicación web CGI que se ejecuta en un servidor.
Impacto	Recopilación de información y compromiso de integridad del sistema. Posible acceso administrativo no autorizado al servidor o solicitud. Posible ejecución de código arbitrario de los atacantes que eligen algunos casos.
Información Detallada	Este evento se genera cuando se intenta ganar acceso no autorizado a una aplicación CGI que se ejecuta en un servidor web. Algunas aplicaciones no realizan verificaciones estrictas al validar Las credenciales de un host cliente que se conecta a los servicios ofrecidos en Un servidor host. Esto puede conducir a un acceso no autorizado y posiblemente privilegios escalados a los del administrador. Datos almacenados en la máquina puede verse comprometida y confiar en las relaciones entre El atacante puede explotar el servidor víctima y otros hosts. Si la aplicación CGI no realiza verificaciones de entrada estrictas,

	También puede ser posible que un atacante ejecute binarios del sistema o código malicioso de los atacantes que eligen.
Fallo del Sistema	Todos los sistemas que ejecutan aplicaciones CGI
Escaneo de ataques	Un atacante puede acceder a un mecanismo de autenticación y suministrar sus propias credenciales para obtener acceso. Alternativamente, el atacante puede explotar las debilidades para obtener acceso como administrador al proporcionar entrada de su elección al script CGI subyacente.
Facilidad de ataques	Sencillo.
Acciones correctivas	Asegúrese de que el sistema esté utilizando una versión actualizada del software y ha aplicado todos los parches suministrados por el proveedor.

Tabla 31 WEB-CGI guestbook.cgi access
Elaborado por: Bryam Yucta

Detalle del ataque AD 7.2

Mensaje	WEB-FRONTPAGE /_vti_bin/ access
Resumen	Este evento se genera cuando se intenta explotar un conocido vulnerabilidad en un servidor web que ejecuta Microsoft FrontPage Server Extensiones.
Impacto	Recopilación de información y compromiso de integridad del sistema. Posible acceso administrativo no autorizado al servidor o solicitud. Posible ejecución de código arbitrario de los atacantes. eligiendo en algunos casos. Denegación de servicio es posible.
Información Detallada	Este evento se genera cuando se intenta comprometer un host que ejecuta Extensiones de servidor de Microsoft FrontPage. Muchos conocidos existen vulnerabilidades para esta plataforma y los escenarios de ataque son legión. En particular, esta regla genera eventos cuando el directorio Se accede a _vti_bin. Este directorio contiene archivos confidenciales que pueden ser utilizado en un ataque contra el servidor.
Fallo del Sistema	Todos los sistemas que ejecutan Extensiones de servidor de Microsoft FrontPage
Escaneo de ataques	Son posibles muchos vectores de ataque desde un simple recorrido de directorio hasta explotación de las condiciones de desbordamiento de búfer.
Facilidad de ataques	Sencillo.
Acciones correctivas	Asegúrese de que el sistema esté utilizando una versión actualizada del software y ha aplicado todos los parches suministrados por el proveedor

Tabla 32 WEB-FRONTPAGE
Elaborado por: Bryam Yucta

Detalle de ataques AD 7.3

Mensaje	WEB-FRONTPAGE posting
Resumen	Este evento se genera cuando se intenta utilizar una página de inicio cliente para conectar y / o publicar contenido en un servidor de Frontpage Servidor web IIS con extensiones habilitadas
Impacto	Un atacante puede modificar su contenido web, acceder a archivos privilegiados o modificar los privilegios de otros usuarios en el host virtual habilitado para Frontpage.
Información Detallada	Microsoft Frontpage es una gestión y publicación de contenido web aplicación, que también viene con extensiones de servidor para Microsoft Servidores web IIS y Apache. Las extensiones permiten a los servidores mostrar contenido dinámico, así como realizar ciertos niveles de Administración del servidor web.
Fallo del Sistema	Todos los sistemas que ejecutan FPSE en IIS.
Escaneo de ataque	Un atacante puede obtener el nombre de usuario y la contraseña de FPSE mediante el rastreo, ingeniería social o adivinanzas de fuerza bruta. Después de iniciar sesión con éxito en el sistema, el atacante puede alterar el contenido web, modificar el inicio de sesión información para otros usuarios y generalmente controla el servidor web.
Facilidad de ataques	Después de obtener las credenciales de inicio de sesión, el ataque es trivial.
Acciones correctivas	Deshabilite FPSE si no es necesario para la administración de contenido web.

Tabla 33 WEB-FRONTPAGE posting
Elaborado por: Bryam Yucta

Ataque detectado 8: AD8

Ilustración 101 Detección de Ataque 7
Elaborado por: Bryam Yucta

Detalle del ataque AD 8.1

Mensaje	WEB-IIS view source via translate header
Resumen	Este evento se genera cuando se intenta crear una URL que contiene el texto 'Traducir: f' en un intento de ver la fuente del archivo código.
Impacto	La recogida de información. Este ataque puede permitir la divulgación de El código fuente de los archivos que normalmente no están disponibles para su visualización.
Información Detallada	Microsoft Internet Information Services (IIS) 5.0 contiene secuencias de comandos motores para admitir varios tipos de archivos avanzados como .ASP y .HTR archivos. Esto permite la ejecución del procesamiento del lado del servidor. IIS determina qué motor de scripting es apropiado para usar dependiendo en la

	extensión del archivo. Si un atacante elabora una solicitud de URL que termina en 'Traducir: f' y seguido de una barra inclinada '/', IIS no puede enviar el archivo al motor de secuencias de comandos adecuado para el procesamiento. En cambio, devuelve el código fuente del archivo referenciado al navegador.
Fallo del Sistema	Microsoft IIS 5.0
Escaneo de ataque	Sencillo. Los guiones de ataque están disponibles gratuitamente
Facilidad de ataques	Sencillo. Existen hazañas
Acciones correctivas	Aplique el parche suministrado por el proveedor apropiado.

Tabla 34 WEB-IIS view source via translate header
Elaborado por: Bryam Yucta

Detalle del ataque AD8.2

Mensaje	WEB-MISC backup access
Resumen	Este evento se genera cuando se intenta explotar un conocido vulnerabilidad en un servidor web o una aplicación web residente en un web servidor.
Impacto	Recopilación de información y compromiso de integridad del sistema. Posible acceso administrativo no autorizado al servidor. Posible ejecución de código arbitrario de los atacantes que eligen en algunos casos.
Información Detallada	Este evento se genera cuando se intenta comprometer un host que ejecuta un servidor web o una aplicación vulnerable. Existen muchas vulnerabilidades conocidas para cada implementación y Los escenarios de ataque son legión. Algunas aplicaciones no funcionan verificaciones estrictas al validar las credenciales de un host cliente conectarse a los servicios ofrecidos en un servidor host. Esto puede llevar a acceso no autorizado y posiblemente privilegios escalados a los del administrador. Los datos almacenados en la máquina pueden verse comprometidos y Las relaciones de confianza entre el servidor víctima y otros hosts pueden ser explotado por el atacante.
Fallo del Sistema	Todos los sistemas que utilizan un servidor web.
Escaneo de ataque	Son posibles muchos vectores de ataque desde un simple recorrido de directorio hasta explotación de las condiciones de desbordamiento de búfer
Facilidad de ataques	Sencillo. Existen hazañas
Acciones correctivas	Asegúrese de que el sistema esté utilizando una versión actualizada del software y ha aplicado todos los parches suministrados por el proveedor.

Tabla 35 WEB-MISC backup access
Elaborado por: Bryam Yucta

Detalle del ataque AD 8.3

Mensaje	WEB-MISC ftp attempt
Resumen	Este evento se genera cuando se intenta explotar un conocido vulnerabilidad en un servidor web o una aplicación web residente en un web servidor.
Impacto	Recopilación de información y compromiso de integridad del sistema. Posible acceso administrativo no autorizado al servidor. Posible ejecución de código arbitrario de los atacantes que eligen en algunos casos
Información Detallada	Este evento se genera cuando se intenta comprometer un host que ejecuta un servidor web o una aplicación vulnerable en un web servidor. Existen muchas vulnerabilidades conocidas para cada implementación y los escenarios de ataque son legión. Algunas aplicaciones no realizan verificaciones estrictas al validar las credenciales de un host cliente que se conecta a los servicios ofrecidos en un servidor host. Esto puede conducir a un acceso no autorizado y posiblemente privilegios escalados a los del administrador. Datos almacenados en la máquina puede verse comprometida y confiar en las relaciones entre. El atacante puede explotar el servidor víctima y otros hosts.
Fallo del Sistema	Todos los sistemas que utilizan un servidor web.
Escaneo de ataque	Son posibles muchos vectores de ataque desde un simple recorrido de directorio hasta explotación de las condiciones de desbordamiento de búfer.
Facilidad de ataques	Sencillo. Existen hazañas
Acciones correctivas	Asegúrese de que el sistema esté utilizando una versión actualizada del software y ha aplicado todos los parches suministrados por el proveedor.

Tabla 36 WEB-MISC ftp attempt
Elaborado por: Bryam Yucta

Detalle del ataque AD 8.4

Mensaje	WEB-MISC Phore cast remote code execution attempt
Resumen	Este evento se genera cuando se intenta explotar un conocido vulnerabilidad en un servidor web o una aplicación web residente en un servidor web
Impacto	Recopilación de información y compromiso de integridad del sistema. Posible acceso administrativo no autorizado al servidor. Posible ejecución de código arbitrario de los atacantes que eligen en algunos casos.

Información Detallada	Este evento se genera cuando se intenta comprometer un host que ejecuta un servidor web o una aplicación vulnerable en un servidor web. Existen muchas vulnerabilidades conocidas para cada implementación y Los escenarios de ataque son legión. Algunas aplicaciones no realizan verificaciones estrictas al validar Las credenciales de un host cliente que se conecta a los servicios ofrecidos en Un servidor host. Esto puede conducir a un acceso no autorizado y posiblemente privilegios escalados a los del administrador. Datos almacenados en la máquina puede verse comprometida y confiar en las relaciones entre El atacante puede explotar el servidor víctima y otros hosts.
Fallo del Sistema	Todos los sistemas que utilizan un servidor web.
Escaneo de ataque	Son posibles muchos vectores de ataque desde un simple recorrido de directorio hasta explotación de las condiciones de desbordamiento de búfer.
Facilidad de ataques	Sencillo. Existen hazañas
Acciones correctivas	Asegúrese de que el sistema esté utilizando una versión actualizada del software y ha aplicado todos los parches suministrados por el proveedor.

Tabla 37 WEB-MISC Phore cast remote code execution attempt
Elaborado por: Bryam Yucta

Detalle de ataque AD 8.5

Mensaje	WEB-PHP admin.php access
Resumen	Este evento se genera cuando se intenta explotar una vulnerabilidad de autenticación en un servidor web o una aplicación en ejecución en ese servido
Impacto	Recopilación de información y compromiso de integridad del sistema. Posible acceso administrativo no autorizado al servidor o solicitud.
Información Detallada	Este evento se genera cuando se intenta comprometer un host que ejecuta un servidor web o una aplicación vulnerable servidor. Existen muchas vulnerabilidades conocidas para cada implementación y los escenarios de ataque son legión. Algunas aplicaciones no realizan verificaciones estrictas al validar las credenciales de un host cliente que se conecta a los servicios ofrecidos y un servidor host. Esto puede conducir a un acceso no autorizado y posiblemente privilegios escalados a los del administrador. Datos almacenados en la máquina puede verse comprometida y confiar en las relaciones entre. El atacante puede explotar el servidor víctima y otros hosts.
Fallo del Sistema	Todos los sistemas que utilizan un servidor web.
Escaneo de ataque	Un atacante puede acceder al mecanismo de autenticación y suministrar sus propias credenciales para obtener acceso. Alternativamente el atacante puede explotar las debilidades para obtener acceso como administrador.
Facilidad de ataques	Sencillo. Existen hazañas

Acciones correctivas	No permitir el acceso administrativo de fuentes externas a la red protegida

Tabla 38 WEB-PHP admin.php access
Elaborado por: Bryam Yucta

Ataque detectado 9

Ilustración 102 Detección de Ataque 9
Elaborado por: Bryam Yucta

Detalle del ataque AD 9.1

Mensaje	WEB-PHP Advanced Poll booth.php access
Resumen	Este evento se genera cuando se intenta explotar un conocido vulnerabilidad en la aplicación web PHP que se ejecuta en un servidor
Impacto	Recopilación de información y compromiso de integridad del sistema. Posible acceso administrativo no autorizado al servidor o solicitud. Posible ejecución de código arbitrario de los atacantes. eligiendo en algunos casos.
Información Detallada	Este evento indica que se ha intentado explotar una vulnerabilidad conocida en PHP. Esta aplicación no funciona verificaciones estrictas al manejar la entrada del usuario, esto puede conducir a el atacante puede ejecutar código PHP, incluir archivos php y posiblemente recuperar archivos confidenciales del servidor que ejecuta la solicitud.
Fallo del Sistema	Todos los sistemas funcionando
Escaneo de ataque	Un atacante puede acceder a un mecanismo de autenticación y suministrar sus propias credenciales para obtener acceso. Alternativamente, el atacante puede explotar las debilidades para obtener acceso como administrador al proporcionar entrada de su elección al script PHP subyacente.
Facilidad de ataques	Sencillo. No se requiere código de explotación.
Acciones correctivas	Asegúrese de que el sistema esté utilizando una versión actualizada del software y ha aplicado todos los parches suministrados por el proveedor.

Tabla 39 WEB-PHP Advanced Poll booth.php access
Elaborado por: Bryam Yucta

Detalle del ataque AD 9.2

Mensaje	WEB-PHP viewtopic.php access
Resumen	Este evento se genera cuando se intenta explotar un conocido vulnerabilidad en la aplicación PHP phpBB.
Impacto	La divulgación de información posiblemente conduzca a un sistema serio compromiso. Afectar

Información Detallada	Algunas versiones de phpBB Grupo phpBB sufren de una vulnerabilidad eso permite que un atacante inyecte consultas SQL de su elección. Esto puede dar lugar a la divulgación de contraseñas y otra información. almacenado en la base de datos. Los datos contenidos en la base de datos también pueden ser corrompido por una consulta SQL maliciosa.
Fallo del Sistema	Grupo phpBB phpBB 2.0.4, 2.0.5
Escaneo de ataque	El atacante puede ejecutar uno de los scripts de explotación disponibles públicamente.
Facilidad de ataques	Sencillo. No se requiere código de explotación.
Acciones correctivas	Actualice a la última versión no afectada del software.

Tabla 40 WEB-PHP viewtopic.php access
Elaborado por: Bryam Yucta

Anexo 9 Análisis de paquetes por el Walleye

En la esquina superior izquierda se encuentra el registro de los ataques al darle clic, se encuentra con información valiosa la cual se explica cada uno de los componentes a continuación.

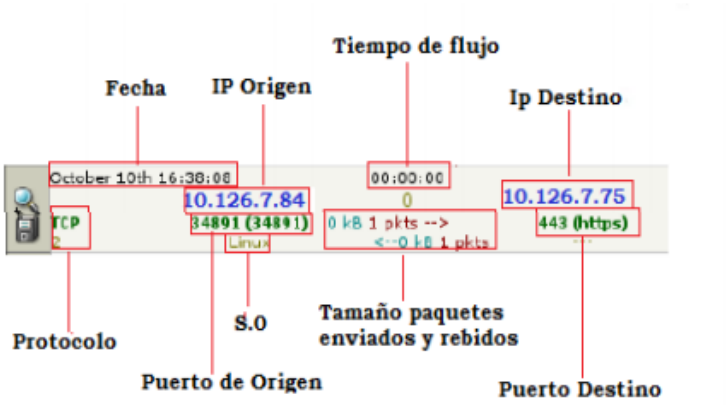


Ilustración 103: Paquete capturado en el Walleye
Elaborado por: Bryam Yucta

- **Fecha:** Permite identificar la fecha, hora, minuto y segmento de ingreso del paquete al honeypot.
- **IP Origen:** Captura la IP que genero el paquete, aquí se puede identificar en el caso de un posible ataque, desde que dirección IP se ha enviado el paquete.
- **IP Destino:** En este caso se refiere a la dirección IP del Honeypot.
- **Protocolo:** Especifica que protocolo ha generado el paquete.
- **S.O:** Identifica el sistema operativo o la distribución a la que pertenece la máquina que ha enviado el paquete.