HONEYPOT, HACIA UN PROTOCOLO DE SEGURIDAD MÁS EFICIENTE Y COMPETITIVO.

KEVIN DAVID MARTÍNEZ CONTRERAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

2018

HONEYPOT, HACIA UN PROTOCOLO DE SEGURIDAD MÁS EFICIENTE Y COMPETITIVO.

KEVIN DAVID MARTÍNEZ CONTRERAS

Anteproyecto De Grado

Monografía

Ing. HERNANDO JOSE PEÑA HIDALGO

Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

2018

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Corozal - Sucre, 25 de noviembre de 2017

DEDICATORIA

Dedico este trabajo a mi Dios principalmente, por la fortaleza diaria que me brinda cada día al despertar, y su inagotable amor, gracias a la inteligencia, entendimiento y sabiduría que me proporciona para la realización de mis sueños y metas.

A mi madre Margareth Contreras, por ser la copiloto de todo este viaje, desde pequeño y hasta mis días presentes, y se, que en los que siguen, estará allí motivándome por seguir siempre adelante.

A mi familia, por el apoyo infinito en todos mis proyectos personales y profesionales, y al gran amor que me expresan.

Kevin Martínez Contreras

AGRADECIMIENTOS

Al cuerpo de docentes de la Universidad Nacional Abierta y a Distancia, CCAV Corozal, y al resto de tutores que me orientaron y guiaron desde mi etapa como profesional y los que siguen aportando en mi formación continua.

TABLA DE CONTENIDO

pág.

INTRODUCCION 13

1. DESCRIPCION DEL PROBLEMA 14

1.1. PLANTEAMIENTO DEL PROBLEMA 14

1.2. FORMULACIÓN DEL PROBLEMA 15

2. JUSTIFICACIÓN 16

3. OBJETIVOS DE PROYECTO 17

3.1. OBJETIVO GENERAL 17

3.2. OBJETIVOS ESPECÍFICOS: 17

4. DELIMITACIÓN DEL PROYECTO 18

5. MARCO REFERENCIAL 19

5.1. MARCO TEÓRICO 19

5.1.1. El Concepto De Honeypot 19

5.1.2. Categorías De Un Honeypot Por Interacción 20

5.1.2.1. Baja Interacción 20

5.1.2.2. Alta Interacción: 21

5.1.3. Categorías De Un Honeypot Por Localización 21

5.1.3.1. Honeypot por producción 21

5.1.3.2. Honeypot por investigación: 21

5.1.4. Categorías De Un Honeypot Por Implementación 22

5.1.4.1. Honeypots Físicas.....22

5.1.4.2. Honeypots Virtuales.....22

5.2. MARCO CONCEPTUAL.....22

5.3. MARCO LEGAL.....25

6. DISEÑO METODOLOGICO.....29

6.1. CRONOGRAMA 30

6.2. RECURSOS NECESARIOS PARA EL DESARROLLO DEL PROYECTO....31

7. PROPUESTA DE IMPLEMENTACION DE HONEYPOT COMO PROTOCOLO DE SEGURIDAD, EFICIENTE Y COMPETITIVO.....32

7.1. IDENTIFICANDO FUENTES DE INFORMACION PARA LA APROPIACIÓN CONCEPTUAL DE UN HONEYPOT.....32

7.2. CONFIGURACION DE UN HONEYPOT EN LA RED 33

7.3. OPTIMIZACION DE UN HONEYPOT 38

7.4. IMPLEMENTACION DE UN HONEYPOT, REFERENCIADO A LA ESTRUCTURA LOGICA 40

8. PRUEBA EXPERIMENTAL 44

8.1. ¿QUÉ ES KIPPO? 44

8.2. CARACTERÍSTICAS DE KIPPO 44

8.3. REQUISITOS DE INSTALACIÓN. 45

8.4. CONFIGURACION E INSTALACION DE KIPPO 45

8.4.1. Instalación de dependencias 46

8.4.2. Descarga y configuración de kippo: 46

8.4.3. Ejecución de Kippo 48

8.4.4. Sesión de ataque a honeypot 49

9. RESULTADO A ENTREGAR 53

10. DIVULGACIÓN 55

CONCLUSIONES 56

REVISIÓN Y RECOPILACIÓN BIBLIOGRÁFICA: 57

ANEXOS 60

LISTA DE TABLAS

pág.

Tabla 1 Cronograma de Actividades.....30

LISTA DE FIGURAS

pág.

Figura 1 Diseño de un Honeypot 19
Figura 2. Front of Firewall 33
Figura 3. Behind the Firewall 35
Figura 4. Zona Desmilitarizada 36
Figura 5. Honeypot de Baja Implicación 40
Figura 6. Honeypot de implicación media 42
Figura 7. Honeypot de implicación alta 42
Figura 8. Ejecución de kippo 48
Figura 9. Maquinas Virtuales 49
Figura 10. Monitoreo Logs del atacante 50
Figura 11. Monitoreo Logs del atacante 51
Figura 12. Monitoreo Shell Victima 52

LISTA DE ANEXOS

pág.

ANEXO I RESUMEN ANALÍTICO ESPECIALIZADO - RAE.....60

HONEYPOT, HACIA UN PROTOCOLO DE SEGURIDAD MÁS EFICIENTE Y COMPETITIVO

INTRODUCCION

Un Honeypot es una herramienta que más a fondo se cataloga como una arquitectura la cual es diseñada para ser vulnerada dentro de un ambiente controlado; esta red permite la monitorización de los ataques en ella, con el fin de registrar los datos del atacante y el ataque en sí, de esta manera se permite estudiar un mejor sistema de seguridad el cual logre fortalecer la capa de protocolo de seguridad dentro de la misma red y evitar futuros ataques.

La siguiente monografía busca definir de manera clara y concisa lo que es un honeypot, tomando consulta de las investigaciones realizadas y de proyectos vigentes que siguen estudiando este tipo de arquitectura, permitiendo así buscar innovar en el sistema o protocolo de red, utilizado para la captura de datos en los diferentes ataques. En este orden de ideas, con el ejercicio de la monografía, se desarrollará un consolidado de investigaciones y definiciones estratégicas que den paso a una mejor conceptualización, caracterización y justificación de la arquitectura en red propuesta por un Honeypot.

1. DESCRIPCION DEL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

La seguridad en las redes es un tema que a muchos nos compete, y sin importar si son organizaciones grandes, medianas o pequeñas, cual sea el tamaño, siempre debe existir los diferentes protocolos de seguridad que permitan la buena gestión de la información que se procesa, e indistintamente de la información que administren las organizaciones, el respaldo a la integridad, confidencialidad y disponibilidad de las mismas ocupa el primer lugar para de esta forma lograr una mejor gestión de la información, por tal los mecanismos de seguridad implementados deben obedecer al control y a salvaguardar los datos que se procesan en caso de una vulneración de la seguridad.

Ahora bien, muchas entidades permiten hasta cierto punto la instrucción consentida, pero ¿qué es esto?, mediante la adopción de honeypot, un "honeypot" no es un sistema de detección de intrusiones, pero puede ayudar a mejorar sus métodos de detección y aportar nuevos patrones de ataque. Es un sistema diseñado para engañar a los intrusos, poder estudiar sus actividades, y así aprender de sus métodos. Se basa en la idea de "conocer al enemigo" para poder combatirlo.

De esta forma las organizaciones, toleran algunas irrupciones en su sistema con el fin de detectar las vulnerabilidades ocasionadas por el ataque y de esta forma, diseñar un mejor protocolo de seguridad, pero, no obstante, los ataques son cada vez más profesionalizados, tomando las contramedidas correctas y evitar este tipo de detecciones de intrusos. Esta realidad está tomando auge y son las desventajas

que este sistema de detecciones debe corregir y evitar crear huésped invisible dentro del sistema de red.

1.2. FORMULACIÓN DEL PROBLEMA

¿En qué medida una red honeypot puede minimizar su riesgo de detección al ser atacada dentro de una red local o intranet, y como a partir de ello, maximizar su potencial de monitorización a los intrusos?

2. JUSTIFICACIÓN

La presente monografía, se enfocara a estudiar la concepción de la red de honeypot desde un ámbito más practico e intuitivo, que logre determinar una mejor gestión de los procesos internos que se hacen al momento de los ataques, buscando las alternativas que permitan desarrollar un protocolo de seguridad más eficiente y eficaz, y que pone a consideración la utilización de metodologías algorítmicas que emulen el paso a paso coordinado del proceso de obtención de datos durante el ataque informático y así mismo ser invisible operativamente al momento que se obtenga la información del proceso de vulnerabilidad al sistema y de servicios que hayan sido sometido para abrir las puertos de entrada al sistema. Así el presente trabajo permitiría mostrar la lógica operacional del sistema de red de los honeypot de tal forma que su metodología sea adaptable a las configuraciones futuras de los protocolos de seguridad utilizados en base a los *honeypot*.

3. OBJETIVOS DE PROYECTO

3.1. OBJETIVO GENERAL

Determinar mediante exploración conceptual y prueba experimental, los alcances de un honeypot, en la cual se pueda reflejar en los procesos de monitorización.

3.2. OBJETIVOS ESPECÍFICOS:

- ✓ Identificar las fuentes de información necesaria para llevar a cabo la conceptualización apropiada de un Honeypot.
- ✓ Explorar la ruta adecuada para la optimización de la red de honeypot
- ✓ Identificar las incidencias de un honeypot en la configuración de red.
- ✓ Analizar la arquitectura de un honeypot para su correcta implementación.
- ✓ Analizar el funcionamiento de un honeypot a partir de una prueba experimental.

4. DELIMITACIÓN DEL PROYECTO

Dada la amplitud de la temática expuesta y las proyecciones tecnológicas que se pueden realizar de acuerdo a los recursos, tecnologías existentes, los diferentes protocolos de seguridad y normas que permitan su gestión eficientes en distintas condiciones, esta investigación monográfica se centrara en la conceptualización lógica del algoritmo de eficiencia para una mejor monitorización de los procesos del ataque en curso y de definir la estrategia metódica para hacer más invisible a los honeypot, y así lograr una mejor captura de la información de los intrusos a los sistemas de información.

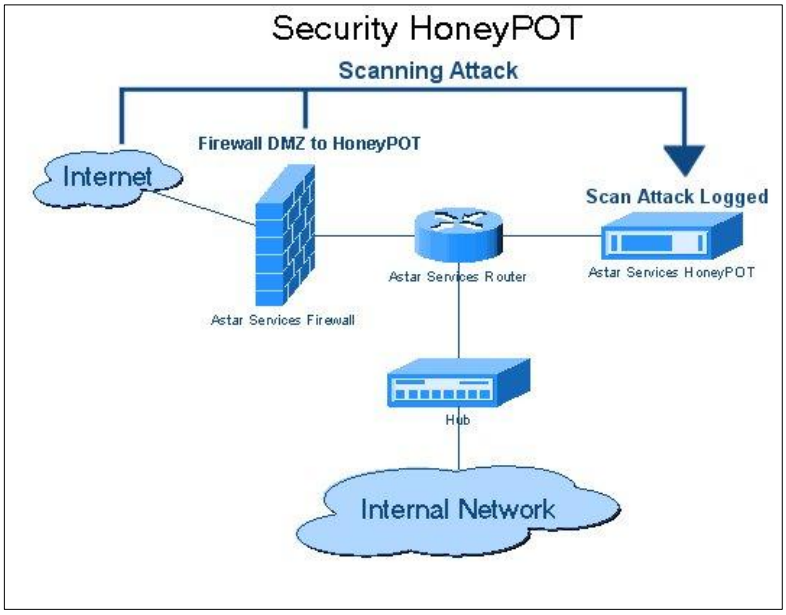
5. MARCO REFERENCIAL

5.1. MARCO TEÓRICO

5.1.1. El Concepto De Honeypot

Entre los términos que serán tratados a lo largo del desarrollo de la presente monografía y que da vida al mismo, es el del concepto de “Honeypot”, que, en términos más cortos, es el de un sistema señuelo de una red que pueda ser atacada y de esta forma monitorizar todas las acciones que realiza el intruso, con el fin de contrarrestar las vulnerabilidades existentes y descubierta durante todo el tiempo del ataque.

Figura 1 Diseño de un Honeypot



Fuente: https://es.wikipedia.org/wiki/Honeypot

Lance Spitzner, define un Honeypot como: “A security resource who’s value lies in being probed, attacked or compromised. Has no production value, anything going to or from a honeypot is likely a probe, attack or compromise”. “*Un recurso de seguridad que es valor reside en ser sondeado, atacado o comprometida ".* Esto significa que todo lo que designamos como un honeypot, es nuestra expectativa y la meta de tener el sistema sondeado, atacado, y potencialmente explotados. Tenga en cuenta, los Honeypots no son una solución. No lo hacen nada 'arreglo'. En cambio, los Honeypots son una herramienta.

La forma de utilizar esa herramienta depende del administrador en turno y de lo que se va a tratar de lograr. Un honeypot puede ser un sistema que simplemente emula otros sistemas o aplicaciones, crea un entorno en prisión, o puede ser un sistema integrado estándar. Independientemente de cómo se construye y utiliza la trampa, su valor radica en el hecho de que es atacado.

5.1.2. Categorías De Un Honeypot Por Interacción

Los honeypot puede categorizarse debido a su comportamiento dentro de la misma red, desde la configuración mínima de un ordenador que analiza el tráfico de una red sencilla, hasta un complejo entramado de ordenadores bajo una misma red, acatando distintas ordenes de servicio. Estos honeypot, están clasificados de acuerdo a las siguientes categorías:

5.1.2.1. Baja Interacción

El sistema concebido dentro de esta categoría de honeypot, está dada por la limitada interacción del atacante dentro de la red y que está sujeta a las configuraciones mismas de los servicios que emula la red, esto con la intención de

obtener de forma cuantitativa información de los diferentes ataques y/o acciones delictivas dentro de la red monitoreada.

5.1.2.2. Alta Interacción:

Son del tipo de Honeypot de solución compleja, dado que, su aplicación es realizada en entornos reales, es decir, montados debidamente en hardware, sin el uso de simuladores, dando por hecho la utilización de aplicaciones nativas que se accionan de manera local

5.1.3. Categorías De Un Honeypot Por Localización

Según su localización, un honeypot puede situarse dentro de estos dos sistemas;

5.1.3.1. Honeypot por producción

Estos sistemas son utilizados en ambientes reales de trabajo en organizaciones para la protección de la misma, lo que implica que estará sujeta a constantes ataques cibernéticos.

5.1.3.2. Honeypot por investigación:

La implementación de este estos Honeypot, son de carácter netamente educativo, la cual estará apoyada bajo el concepto de demostración, con el fin de un estudio más profundo en los patrones de comportamiento de los ataques y amenazas dentro de la red.

5.1.4. Categorías De Un Honeypot Por Implementación

Los Honeypot, pueden debidamente implementarse según los fines de la organización.

5.1.4.1. Honeypots Físicas

El señuelo ejecutado está dentro de una maquina física, este tipo de configuraciones de honeypot está dado bajo la premisa de despliegue de Honeypots con alta interacción.

5.1.4.2. Honeypots Virtuales

El señuelo ejecutado está dentro de una máquina virtual, siendo esta de carácter limitado a los recursos de hardware y software, aunque son de bajo coste, cuando se quieren construir más señuelos.

5.2. MARCO CONCEPTUAL

La importancia de la información, como activo importante en el mundo actual, donde las masas, la económica, la sociedad como tal, esta delineada mente vinculada a cómo opera esta, en el diario vivir de la gente.

Los datos son los activos más importantes de cualquier organización, pequeña o grande, del sector en la cual se quiera ubicar, la información y el procesamiento misma, abarca el continuo desarrollo de los sistemas, cuales quiera sea el contexto. Así mismo, se espera que, la seguridad que se tenga con los datos, la administración misma sea la mejor y de manera segura; es por ello que el uso de protocolos de seguridad, permitirán tener un respaldo en un alto porcentaje de salvaguardar la información.

Ahora bien, que pasaría, si es decisión de la organización, implementar un grado de permeabilidad ante los ataques informáticos, y de esta manera, evaluar el comportamiento de estos intrusos, con el fin de analizar dicho tráfico, realizar los diagnósticos correspondientes y emitir reglas, normas y políticas de prevención ante dichos ataques; para la presente monografía, se toma como base dicha situación como insumo, para proponer la conceptualización de los Honeypot, como herramientas de seguridad informática.

Entendiendo lo anterior, se define a esta herramienta como:

Honeypot: Sistema señuelo, es una herramienta de seguridad diseñada para ser sondeada, atacada y comprometida, que tiene la capacidad de detectar y registrar estas acciones.

Lo anterior está asociada a la seguridad de la información, como eje central de todo este proceso, y dado el cual es necesario conocer las siguientes como premisas que imperan dentro de todo este proceso:

Seguridad de la Información: Conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma, además garantizando la irrrefutabilidad.

En este orden de ideas, se es necesario validar los siguientes conceptos que permitan, caracterizar en que forma la implementación de un honeypot arrojara los resultados pertinentes que den paso a la mejor gestión de los controles de seguridad.

Integridad: Los activos o la información solo pueden ser modificados por las personas autorizadas y de la forma autorizada.

Confidencialidad: La información o los activos informáticos son accedidos por las personas autorizadas en el momento requerido.

Disponibilidad: Los activos informáticos son accedidos por las personas autorizadas en el momento requerido.

Irrrefutabilidad (No Repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

5.3. MARCO LEGAL

Dado que la utilización de Honeypot en un ambiente controlado, infiere en la integridad de los elementos y/o activos hardware y software, se usó y mención de las siguientes disposiciones legales, amparadas bajo la norma y ley de garantías y protección a los datos, los cuales se mencionan a continuación:

LEY 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Artículo 1°. Adiciónase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: **Interceptación de datos informáticos**. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema

informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

LEY ESTATUTARIA 1581 DE 2012 - (octubre 17): Por la cual se dictan disposiciones generales para la protección de datos personales.

La Ley 1266 de 2008 define los siguientes tipos de datos de carácter personal:

a) Dato privado: “Es el dato que por su naturaleza íntima o reservada sólo es relevante para el Titular”.

b) Dato semiprivado: “Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su Titular sino a cierto sector o grupo de personas oa la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV” de la Ley 1266.

c) Dato público: “Es el dato calificado como tal según los mandatos de la Ley o de la Constitución Política ytodos aquellos que no sean semiprivados o privados”, de conformidad con la Ley 1266 de 2008. “Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas”.

6. DISEÑO METODOLOGICO

El presente ante-proyecto de grado corresponde a la línea de investigación Gestión De Sistemas: Auditoria de Sistemas.

El tipo de investigación es Documental.

A partir de este tipo de Investigación, se dará paso a la búsqueda de información correspondiente al tema seleccionado mediante fuentes bibliográficas que permitan la recopilación de los datos concernientes al objeto de exploración. La recopilación bibliográfica está basada en documentos que detallan la originalidad y causa de la temática en desarrollo, así como trabajos de investigación, ensayos, artículos de revistas indexadas, documentos académicos, videoclips entre otras fuentes vinculadas al tema de estudio seleccionado.

La selección de este tipo de investigación, garantizara la posesión del material que soportara todo el desarrollo de la presente monografía, entendiéndose esta como la ruta de exploración, ordenamiento, selección de la información más pertinente, procesamiento de la misma y la aplicabilidad final de esta, con el fin de separar las partes que la componen para un mejor proceder de los datos contenidos, todo ello para su respectiva conclusión positiva, encaminada siempre a generar conocimiento, mediante el debate misma de la información y el proceder de ordenamiento documental.

6.1. CRONOGRAMA

Tabla 1 Cronograma de Actividades

ACTIVIDAD	MES 1	MES 2	MES 3	MES 4
Selección del Tema	x			
Delimitación del tema	x			
Investigación Bibliográfica		x		
Investigación de Campo		X		
Redacción previa			X	
Revisión de contenidos, forma y finalización del escrito			X	X

Fuente: Autor

6.2. RECURSOS NECESARIOS PARA EL DESARROLLO DEL PROYECTO

Para este proyecto se necesitará la compilación y búsqueda de temáticas que aterrice la conceptualización de los Honeypot, y que están basadas en la investigación de teorías, manuales, videoclips, tesis, ensayos, artículos académicos que den fe del cuerpo temático expuesto durante toda la monografía. Todas estas referencias bibliográficas estarán debidamente identificadas con el fin de no caer en vacíos de descontextualización con la teoría expuesta a largo de todo el proyecto.

7. PROPUESTA DE IMPLEMENTACION DE HONEYPOT COMO PROTOCOLO DE SEGURIDAD, EFICIENTE Y COMPETITIVO

7.1. IDENTIFICANDO FUENTES DE INFORMACION PARA LA APROPIACIÓN CONCEPTUAL DE UN HONEYPOT

Hablar de Honeypot es remontarse a los años 1999, cuando Lance Spitzner fundador del Proyecto Honeynet, publicara un artículo refiriéndose al término en mención.

La presente monografía está apoyada en los trabajos de investigación que Spitzner desarrollo para dar paso a este sistema de monitoreo (señuelo) de intrusos cibernéticos. Partiendo así mismo de las contribuciones de diferentes autores y organizaciones que han buscado la cada vez optimización de este sistema de monitoreo.

Partiendo del concepto original, Spitzner cita: A honeynet is a network of high interaction honeypots that simulates a production network and configured such that all activity is monitored, recorded and in a degree, discreetly regulated. (en español: "Una honeynet es una red de internet de alta interacción de tipo honeypot, que simula una red de producción y está configurada de manera tal que toda la actividad en ella, esta monitoreada, grabada y en un grado, discretamente regulada")

Así mismo se dispone de concatenar los anteriores resultados bibliográficos con el articulo precedido por Spitzner, titulado: “Honeypot: Tracking Hackers”, el cual se encuentra disponible para su respectivo estudio, el cual permita el enriquecimiento técnico y conceptual sobre los Honeypot.

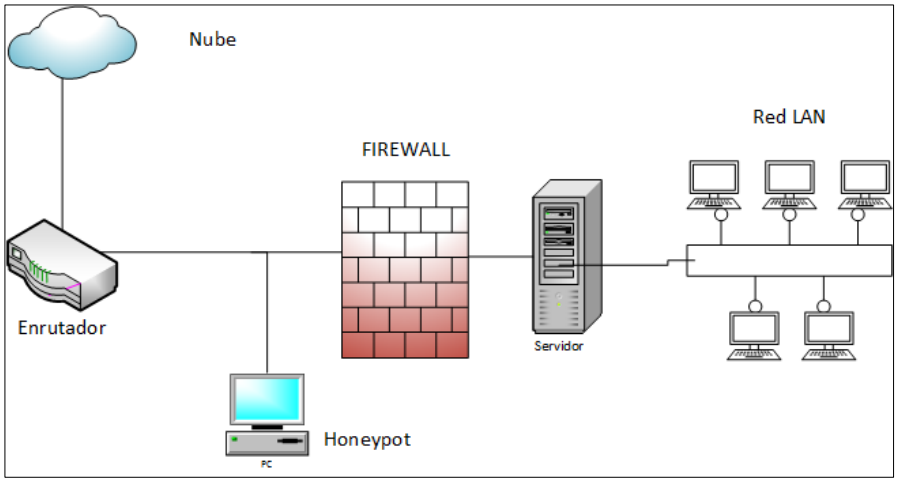
7.2. CONFIGURACION DE UN HONEYPOT EN LA RED

Al momento de la configuración de la red, y hablamos del posicionamiento lógico de la topología, se debe ser cuidadoso en la implementación de los Honeypot, puesto que la presencia de este, en la configuración de la red incidirá en el tráfico de datos que es dirigido hacia la red local, desde afuera, o la o disposición que se mantenga la red dentro de la organización.

Partamos de las siguientes situaciones, donde la disposición de los honeypot, puede incidir en la configuración de la red misma.

- ***Front of firewall*: (Antes del firewall):**

Figura 2. Front of Firewall



Fuente: Autor

La localización del honeypot antes del firewall, conlleva a que se incremente el riesgo externo, el cual es inherente al honeypot. La disposición del honeypot, permitirá que no halla peligro para el resto de la red, como se puede evidenciar en la imagen anterior.

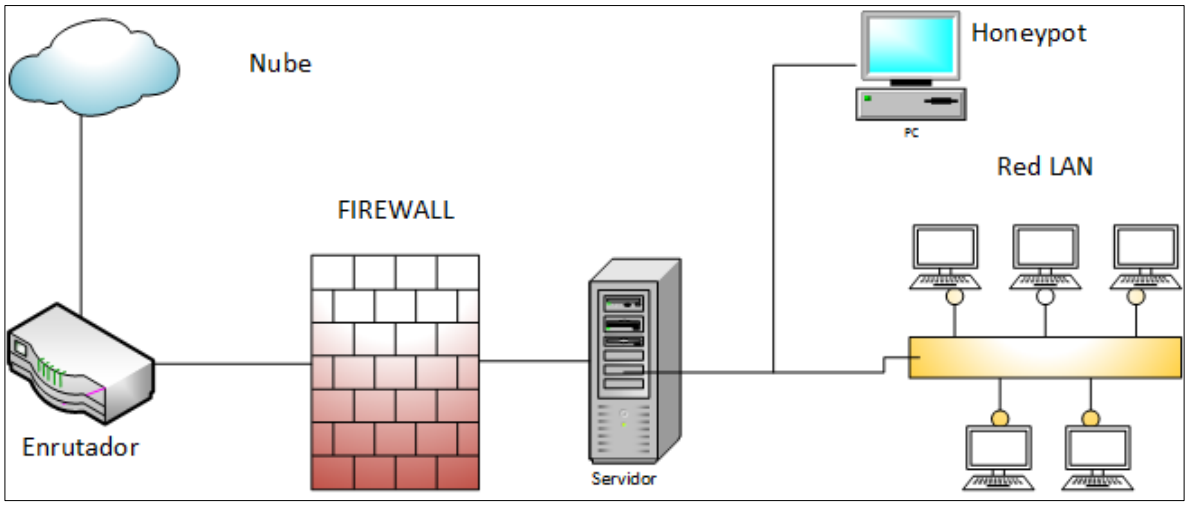
La incidencia de este honeypot antes del firewall, impedirá que se activen otras alarmas configuradas dentro de la red, como pueden ser IDS, dado que los ataques son recibidos por el Honeypot. Aunque es posible que esta configuración este entre las más usadas, hay que tener en cuenta que al estar expuesto el Honeypot como señuelo, conllevara a un alto tráfico, que es generado por los ataques constantes, precisamente por la posición en la cual se encuentra.

Siguiendo la lógica de la estructura de la red anterior, los ataques se encontrarán de primera mano con el dispositivo, lo que posibilita que al ser constantemente atacado y debido a ello el tráfico aumenta, el consumo de ancho de banda empezara a crecer espontáneamente.

Ahora bien, por esta misma configuración del honeypot antes del firewall, evitara la monitorización de los ataques internos que se puedan presentar dentro de la red local, lo cual, conlleva a tomar correctivos en la organización lógica de la red, tomando las respectivas precauciones de seguridad, conforme a las políticas, normas y estándares de la entidad.

➢ ***Behind the firewall*** **(Detrás del firewall):**

Figura 3. Behind the Firewall



Fuente: Autor

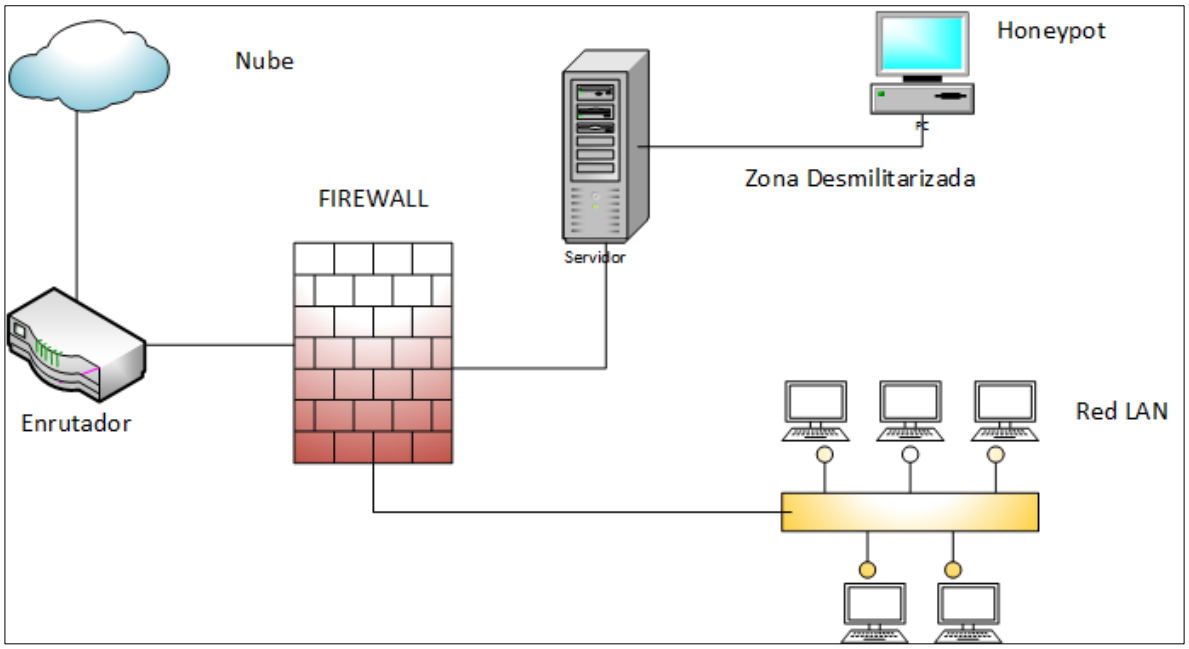
La disposición del honeypot en esta parte, creara cierto incentivo en la red interna, dado que identificara ataques que se realicen desde la misma red donde está ubicado, así mismo, obtendrá datos del firewall, identificando debilidades en cuanto a configuración, además de inspeccionar maquinas alteradas por virus o gusanos que comprometan toda la red.

Conforme a la figura, el honeypot queda dispuesto detrás del firewall, lo que estará condicionado por las reglas de filtro del firewall. En esta parte, el honeypot incide en la configuración de la red de la organización, dado que se debe modificar las reglas del firewall para que este, pueda asimilar algunos tipos de acceso al honeypot, por los atacantes fuera de la red. Ahora bien, este punto es muy importante analizar, dado que existe un elemento que es miembro de la red interna, el cual es vulnerable y que está equipado para recibir trafico externo con el fin de capturar las peticiones hechas desde la red externa, al ser esto realidad, hay un alto grado de comprometimiento de toda la red local, dado el caso que los ataques puedan tener acceso al honeypot y, por ende, una fácil penetración al resto de la red.

Dentro de este escenario, una situación favorable, es que al estar expuesto el Honeypot, entran a jugar sistemas de monitoreo como IDS, Firewall, lo que recibirán muchas alertas de ataque. Ante esta situación, se debe corresponder modificaciones al sistema de red, lo que conlleva a implementar más medidas de prevención y corrección antes cualquier escape o fuga de peticiones dañinas.

- ***Zona desmilitarizada:***

Figura 4. Zona Desmilitarizada



Fuente: Autor

A partir de esta configuración de la red, con la incidencia del Honeypot en él, se tendrá ciertas ventajas dentro de esta arquitectura, partiendo de la detección de ataques tanto externos como internos, ajustando de manera gradual las reglas del firewall, esto puesto que se encuentra en una zona donde el acceso es público, esta ubicación, reúne dos zonas, aislados por el firewall, lo que evita que la red local pueda sufrir imprevistos a causa de los ataques que son dirigidos al honeypot.

Sin embargo, la detección de ataques internos, se condiciona, puesto que al estar aisladas las dos zonas, el atacante de la red local, no accederá a la zona desmilitarizada manteniendo su objetivo en la red local, donde se encuentra el honeypot; además de esto, el atacante si puede enviar peticiones a los servidores públicos de la zona desmilitarizada, así como otros ataques externos.

El grado de incidencia de los honeypot, va acorde de la posición de este dentro de la red, lo que conlleva a modificar las condiciones en la que normalmente se venían estableciendo el cuerpo de seguridad para la red local; es importante resaltar, que todas las posiciones anteriormente descritas, en cada una de las situaciones, va acorde al nivel de seguridad a implementar, las políticas de la empresa y a la acogida eventualmente de este sistema de monitoreo y señuelo.

7.3. OPTIMIZACION DE UN HONEYPOT

La información, hoy en día, es el activo que mueve las masas, desde la posición geoespacial, hasta los datos que permiten una transacción bancaria, son utilizados como insumos para ir mejorando cada día más, las soluciones a las necesidades que crecen con la constante evolución de la tecnología; es por ello y ante los ataques comunes, del cual podríamos ser víctimas, sino se toman los debidos controles, para una constante seguridad.

Al emplear Honeypots en un sistema de red, se deben centrarse una ruta de recomendaciones que permitan que el sistema creado este siempre bajo control de quienes están facultados en la administración de la información recolectada y de la que es puesta en compromiso.

- Creación de políticas de seguridad en toda la organización, donde se definan las normas y las respectivas responsabilidades de los usuarios y administrativos, en cuando a la configuración eficiente de equipos, y a la información que hay en estos.

- La implementación de Honeypot conlleva a exponer información que puede resultar perjudicial para la empresa, por lo que instalación de herramientas de monitoreo como IDS, IPS, Firewall entre otros controles y aplicativos acopladas a estas, permitirán un respaldo y tranquilidad de la información que se encuentra en juego.

- La administración de claves dentro de la organización y las correspondientes actualizaciones de estas, permitirán que, durante el proceso de la implementación de los Honeypots, no sea vea afectado la confidencialidad de la información en un punto máximo.

- El seguimiento continuo al tráfico de la red, mejorara los análisis de datos, lo que creara un perfil más claro sobre los movimientos de los atacantes, el cual conllevara a tomar las medidas necesarias para hacer uso de mecanismo que contrarresten dichos ataques a futuro.

- Documentar la información recibida a través del honeypot, con el fin de dar soporte de garantía a los análisis que permiten perfilar el comportamiento de los atacantes.

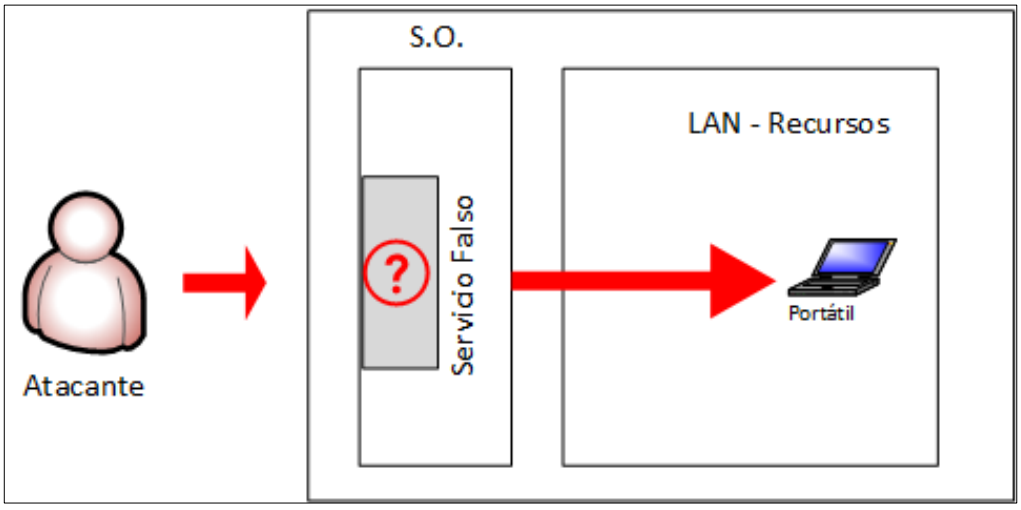
- El respaldo de los datos, juega un papel importante, dado a que se deben tener las precauciones para que la información recibida, este debidamente guardada ante situaciones de colapso o desperfecto.

7.4. IMPLEMENTACION DE UN HONEYPOT, REFERENCIADO A LA ESTRUCTURA LOGICA

En esta apartado, se analizará de manera más específica la arquitectura de implementación de un honeypot, con el fin de lograr los objetivos, tal cual sean definidos por el administrador en la recolección de la información al momento del ataque. Esto constituye que tanto nivel de implicación, se es permitido al atacante, y con los registros de las peticiones hechas al sistema señuelo, analizar, cuantificar y desarrollar un sistema de defensa eficiente, a partir de los resultados obtenidos durante el ataque.

Partimos de la más ***baja implicación*** por parte del atacante y que incide en la captura de los datos por parte del administrador de sistemas, esto puede ser analizado mediante la siguiente gráfica:

Figura 5. Honeypot de Baja Implicación



Fuente: Autor

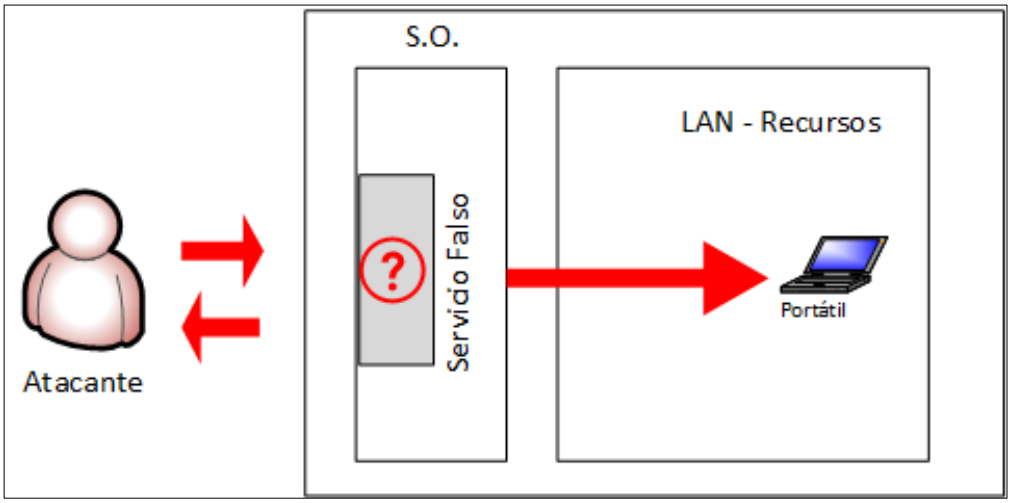
Este tipo de servicios prestados por los honeypot, cubren de manera superficial algunos ataques; esta configuración confiere al sistema, servicios falsos que son

implementados mediante procesos de escucha en un puerto o puertos TCP/IP seleccionados previamente. En esta situación, el honeypot, como señuelo, cumplirá una activad de rendimiento bajo, dado que el tráfico que pasa por él, es captado como malicioso y luego analizado, gastando en ello, tiempo de análisis.

Dado que son sistemas de baja implicación, no es posible por parte del atacante acceder a más recursos locales de la red, reduciendo así el riesgo en el área local. Pero lo que se puede tomar como ventaja, es usado como debilidad, puesto que, dado el caso, el atacante podría acceder por medios alternativos a los servicios de la red local.

Seguimos con el nivel de ***implicación media***, en este punto, hay un concepto importante a mencionar, y es la interacción del atacante con el sistema. En este punto, la implementación es obtenida a bases de servicios falsos que procesan las peticiones del atacante, estos son mejores estructurados que en el apartado anterior; la evidencia de este sistema es que potencializa al atacante de encontrar fallas de seguridad, lo que la penetración de este a la red local, se le facilitara. Dado estas circunstancias, el nivel de interacción del atacante aumentará lo cual le permitirá al administrador, recolectar mayor y mejores datos, con el fin de analizarlos y contrarrestarlos a futuro.

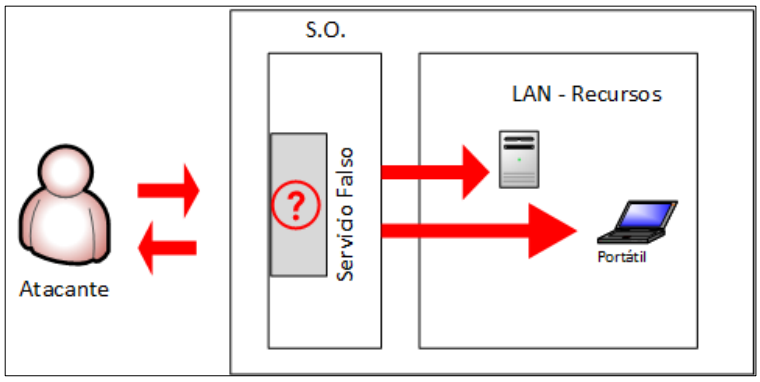
Figura 6. Honeypot de implicación media



Fuente: Autor

Finalizamos con el nivel de ***alta implicación***, que permite un grado de complejidad alto dentro del sistema de red local, dado que el riesgo crece, por la alta interacción del atacante con los servicios obtenidos.

Figura 7. Honeypot de implicación alta



Fuente: Autor

Todo esto lleva implícito mayores posibilidades de recolectar una información con más argumentos que son el resultado del análisis hecho, ante los datos obtenidos durante el proceso de ataque, además de que la complejidad de los ataques aumentan considerablemente al tener una tasa de penetración más alta que la anterior; es necesario recalcar que la mayoría de los ataques, son directos al centro administrativo, con el fin de obtener dichos privilegios tanto de la maquina o red local y a sus recursos, esto es posible dada las condiciones de la alta implicación que conlleva el honeypot utilizado.

8. PRUEBA EXPERIMENTAL

La siguiente prueba experimental, dará claridad sobre el funcionamiento de un honeypot, dado a su nivel de interacción y al tipo en cuestión.

Actualmente, se encuentra una gran variedad de honeypot, de diversas clases, interacciones y nivel de complejidad. Se remite al lector en el siguiente vínculo a consultar una lista de los honeypot más destacados actualmente, el cual se encuentra alojado en la siguiente ruta en github: https://github.com/paralax/awesome-honeypots

Para la presente prueba experimental, se hara uso de la herramienta de honeypot: ***Kippo.*** El cual puede ser descargado o clonado del siguiente repositorio alojado en github: https://github.com/desaster/kippo

8.1. ¿QUÉ ES KIPPO?

Kippo, es del tipo honeypot SSH, de interacción media, el cual fue diseñado para el monitoreo de ataques de fuerza bruta, y la interacción dentro de la Shell por parte del atacante. Kippo, tiene una curva de aprendizaje de instalación baja, lo cual es importante a la hora de su implementación y puesta en marcha, lo que indica que puede ser estudiado y configurado acorde a los objetivos de quien lo utiliza.

8.2. CARACTERÍSTICAS DE KIPPO

✓ Posee un sistema de fichero falso, agregado a la Shell, el cual le da capacidad al atacante de agregar y/o eliminar archivos.
✓ Se puede agregar contenido de ficheros falsos, para que el atacante perciba una interacción real con el contenido.

✓ Posee la capacidad de monitorear en tiempo real las ejecuciones del atacante y de registrar las pulsaciones y acciones del atacante desde el momento en que comienza con el ataque.

8.3. REQUISITOS DE INSTALACIÓN.

- Un sistema operativo (probado en Debian, CentOS, FreeBSD y Windows 7)
- Python 2.5+
- Trenzado de 8.0 a 15.1.0
- PyCrypto
- Interfaz Zope

8.4. CONFIGURACION E INSTALACION DE KIPPO

Para la ejecución de Kippo, se necesitará una serie de instalación de dependencias para su correcto funcionamiento.

El ambiente de trabajo es implementado en la distro de GNU/Linux Ubuntu Mate, el cual es basado en Debían. Para la experiencia práctica se hace uso de dos entornos virtualizados de la misma distro. Una distro, con nombre: ***honeypotuser*** es utilizada para la configuración y ejecución del honeypot, y en la cual será objetivo de ataque, en este caso se hará prueba por ssh para verificar su correcto funcionamiento. La segunda maquina a utilizar con nombre ***honey*** hará las veces de atacante, la cual es configurada con el servidor ssh para la puesta en marcha del honeypot.

El ambiente de prueba, es bajo condiciones seguras sin afectar a terceros. Solo con fines netamente académicos.

8.4.1. Instalación de dependencias

En la distro de Linux, se debe primeramente actualizar el sistema, y seguidamente instalar las siguientes dependencias para el correcto funcionamiento de Kippo.

```
apt-get update && apt-get upgrade
```

```
apt-get install python-dev openssl python-openssl python-pyasn1 python-
```

8.4.2. Descarga y configuración de kippo:

A través del repositorio alojado en github, se puede clonar o descargar el archivo.

```
git clone https://github.com/desaster/kippo.git
```

Después de descargar el repositorio, se debe entrar a la carpeta y darle permisos de acceso mediante el siguiente comando, esto con el fin de no tener errores de accesibilidad para el momento de su ejecución.

```
$ chmod 777 –R kippo
```

En la carpeta descargada se deberán visualizar los siguientes elementos, entre los cuales hay archivos y carpetas

```
data/ doc/ honeyfs/ kippo.cfg.dist log/ start.sh* txtcmds/ dl/ fs.pickle kippo/
kippo.tac README.md stop.sh utils/
```

Se procede a configurar el archivo: ***kippo.cfg.dist*** el cual es debe ser renombrado a ***kippo.cfg*** de la siguiente forma:

```
# mv Kippo.cfg.dist Kippo.cfg
```

En este orden de ideas, se continua con la configuración del archivo ***kippo.cfg*** el cual se asignarán los parámetros bajo el cual se pondrá en marcha la herramienta honeypot.

En esta parte, se debe tener en cuenta que parámetros opta el usuario a configurar, es decir, rutas de acceso al honeypot, puertos a asignar, etc. En este caso, se estará trabajando con SSH, el cual hará uso del puerto 22, para efectos de seguridad se sugiere cambiar dicho puerto. Por defecto kippo escucha en el puerto 2222

A manera de ejemplo, se permite la configuración del archivo ***kippo.cfg***

```
[honeypot]
ssh_port = 2222
hostname = ONserver
log_path = log
download_path = dl
contents_path = honeyfs
filesystem_file = fs.pickle
data_path = data
txtcmds_path = txtcmds
rsa_public_key = data/ssh_host_rsa_key.pub
rsa_private_key = data/ssh_host_rsa_key
dsa_public_key = data/ssh_host_dsa_key.pub
dsa_private_key = data/ssh_host_dsa_key
exec_enabled = true
fake_addr = 10.0.0.0
ssh_version_string = SSH-2.0-OpenSSH_5.5p1 Debian-6+squeeze2
interact_enabled = true
interact_port = 5000
```

Nota: Para que kippo sea accesible a través del puerto 22, se procede a realizar el reenvió de puertos, a través del uso de ***iptables*** de la siguiente forma:

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-port 2222
```

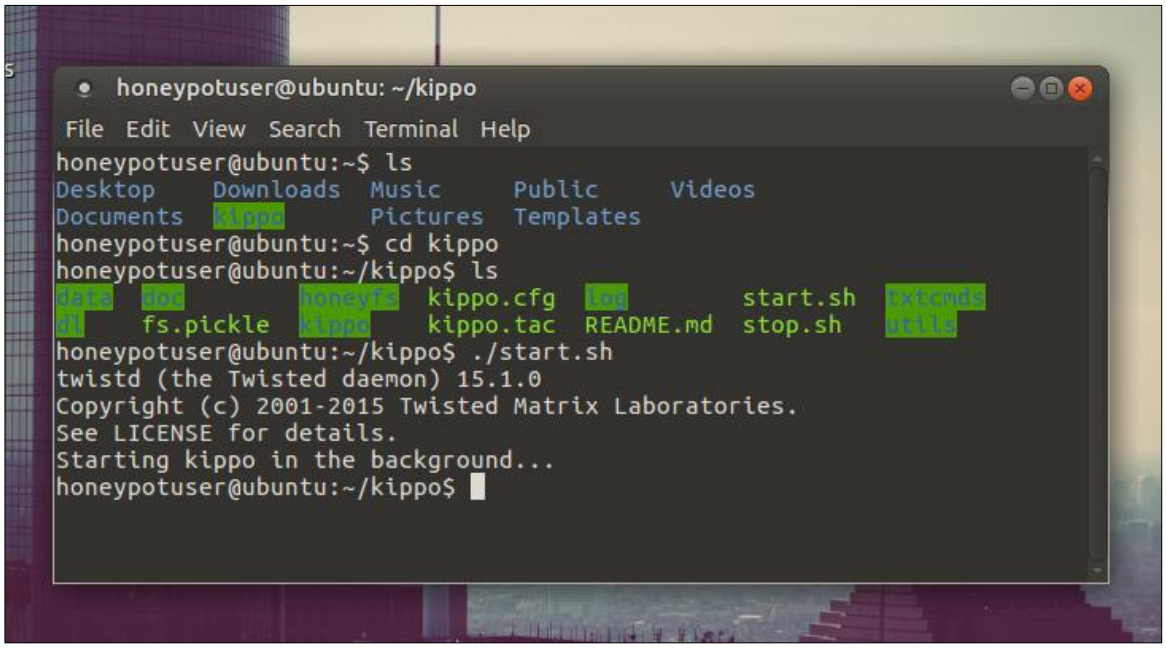
8.4.3. Ejecución de Kippo

Realizado el checklist de la instalación de dependencias, configuracion e instalación, se procede a la ejecución de kippo.

Para la ejecución de kippo, basta con escribir los siguientes comandos, haciendo uso del archivo ***start.sh*** que se encuentra dentro de la carpeta de kippo.

```
$ ./start.sh
```

Figura 8. Ejecución de kippo



Fuente: Autor

En esta parte de la prueba experimental, se ha ejecutado kippo, para la escucha y monitoreo de las acciones del atacante.

8.4.4. Sesión de ataque a honeypot

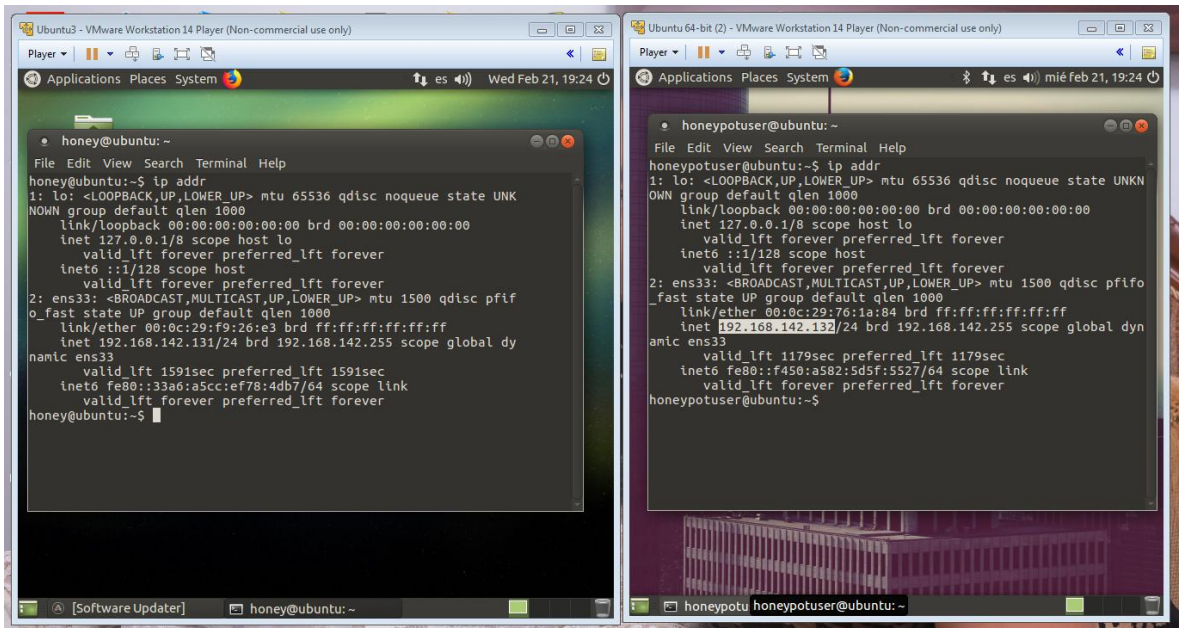
Para la presente experiencia se hace uso de máquinas virtuales, con el fin de que de proceder a un ambiente de trabajo controlado y con fines netamente académicos.

Maquina atacante: honey: IP: 192.168.142.131

Maquina víctima: honeypotuser: IP: 192.168.142.132

En las siguientes gráficas, se observa la ip con las cuales están configuradas las máquinas virtuales, y que harán las veces de ataque y víctima.

Figura 9. Maquinas Virtuales

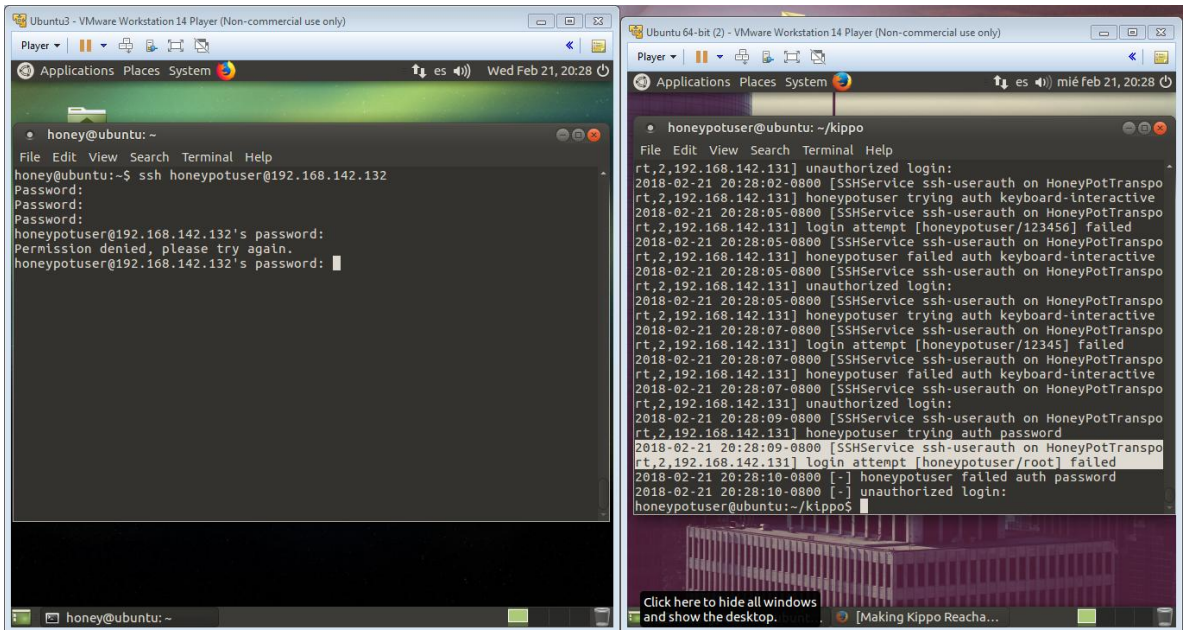


Fuente: El Autor

En la siguiente gráfica, se empieza con el intento de acceso mediante la Shell de Ubuntu por medio de SSH. En un primer momento, y asumiendo que se sabe el usuario e ip de la víctima, se procede a aplicar conexión por SSH a la maquina víctima. La conexión se realiza de la siguiente manera:

```
$ ssh honeypotuser@192.168.142.132
```

Figura 10. Monitoreo Logs del atacante



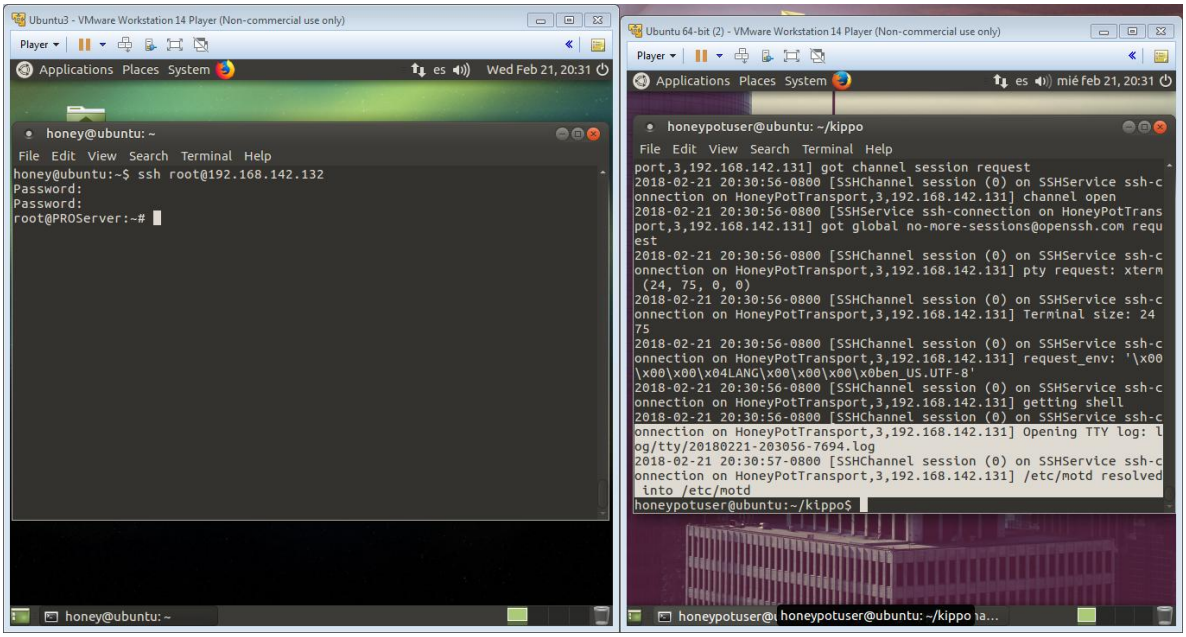
Fuente: El Autor

En la otra consola, se puede observar los log generados desde el momento en que se enciende el honeypot, hasta los intentos de conexión. Esto se hace mediante el siguiente comando, dentro de la carpeta de kippo

```
$ cat log/kippo.log
```

En esta parte de la experiencia práctica, el intento de conexión es exitoso. Por lo cual la maquina víctima es alcanzada, pero el atacante ha accedido al sistema de fichero falso, el cual puede observarse en la siguiente gráfica, de un lado, la conexión al host víctima, del otro lado, el registro o monitoreo de tal acción.

Figura 11. Monitoreo Logs del atacante



Fuente: El Autor

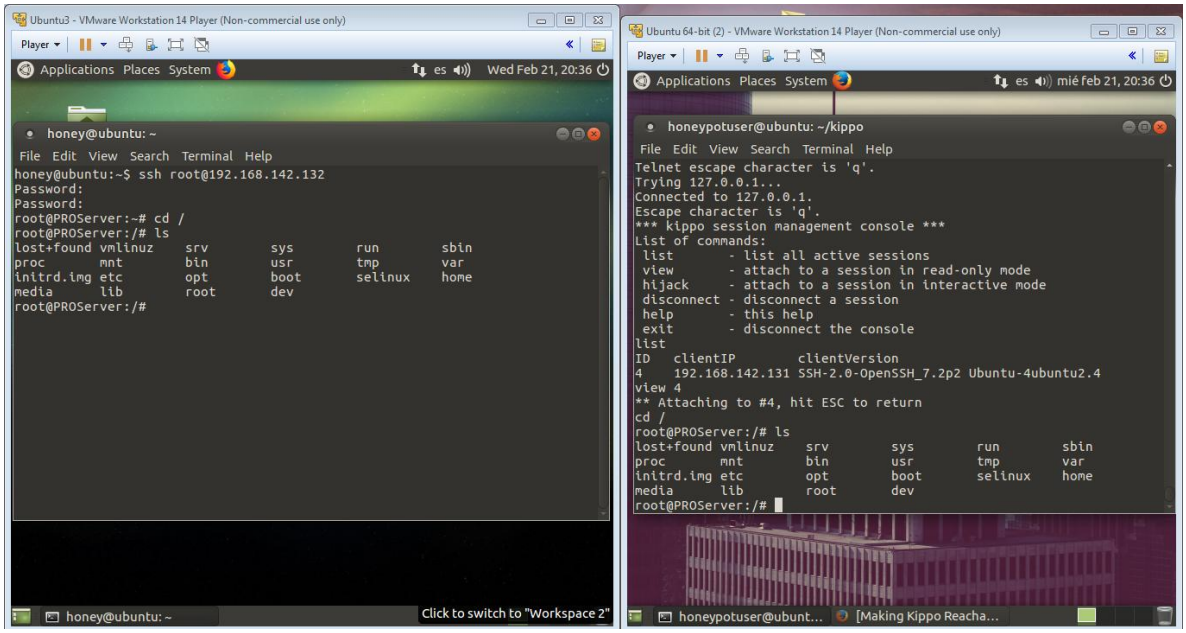
La importancia de un honeypot, es que cumpla con el propósito de monitoreo a las acciones del atacante, y a partir de allí, y de la misma configuración realizada al honeypot, realizar los ajustes para que el atacante tengo limitado el espacio de acceso al sistema.

Por último, y haciendo uso de la herramienta telnet, se procede a monitorear en tiempo real las acciones del atacante. Esto se hace mediante el siguiente comando, y ejecutado dentro del host víctima:

```
$ telnet -e q 127.0.0.1 5000
```

Dentro de la configuración del honeypot se hace uso del puerto 5000, el cual se deja libre, con el fin de ejecutar una pequeña consola de administración básica, el cual nos podrá listar las sesiones activas dentro de la Shell víctima, así mismo visualizar en tiempo real los comandos y acciones que el atacante está realizando dentro del host victima

Figura 12. Monitoreo Shell Victima



Fuente: El Autor

9. RESULTADO A ENTREGAR

La presente investigación monográfica, contemplara la conceptualización de Honeypot como herramienta para la monitorización de acciones intrusas dentro de la red establecida para tal fin. Abordando una serie de conceptos y referentes bibliográficos que permitirán su comprensión ideal, en pro de un mejor aprovechamiento de este tipo herramientas en el mundo de la seguridad informática. Todo este conglomerado de conceptos, teorías y demás aceptaciones literarias técnico-pedagógicas, están basadas en la investigación previa a fuentes y expertos dedicados y conocedores de la temática.

Partiendo de la asimilación de las fuentes de información que corresponden a la instancia de investigación y consulta, desarrollada durante todo el tiempo de realización de la monografía, el cual es manifestada a lo largo del documento en mención y que resalta la temática abordada sobre los Honeypot.

Se muestra la configuración de un honeypot en la red, validando la lógica de la estructura de las redes, acorde a las topologías que son implementadas dentro de la misma; para ello se hizo énfasis en la adopción de una posición del honeypot, el cual fue causa de factores que intervienen en o no en la funcionalidad correcta de la herramienta. En este sentido la configuración del honeypot, se logra gracias a los objetivos con el cual la empresa traza para lograr así los fines de la organización.

Se emplea un proceso de optimización de los honeypot, abordando políticas de seguridad manifiesta a las funciones de estas herramientas, así mismo se realizan consideraciones a la forma, uso y responsabilidad de utilización de los honeypot.

Por último se logra, analizar la implementación de los honeypot acorde a su arquitectura lógica, y como está entre en función con los elementos de la red local.

10. DIVULGACIÓN

Con el fin de fortalecer la academia, en la conceptualización de la herramienta de Honeypot, y seguir con la transferencia de conocimiento, el presente proyecto será publicado en los repositorios de la Universidad Nacional Abierta y a Distancia, para consulta pública de la comunidad educativas, de las organizaciones, entidades, gubernamentales o no, sin ánimo de lucro y empresas privadas, que permitan tener un clara asimilación conceptual sobre esta herramienta y en la implementación de este en sus políticas de seguridad.

CONCLUSIONES

Con el desarrollo de la presente monografía, se logra identificar, conocer y comprender, dentro de este ejercicio investigativo la conceptualización de los honeypot, como herramientas usadas dentro del contexto de la seguridad de la información, para la extracción y análisis de los comportamientos de los atacantes en la red; dando aplicabilidad a este, dentro de un amiente controlado, y que mantiene los debido protocolos de seguridad establecidos, suponiendo posibles eventos fuera de los objetivos.

Así mimo, y abordando las leyes que rigen en el estado colombiano, se logró identificar las áreas en las que se puede estar violando causalmente la manipulación de datos, aun conociéndose la libre administración de estos con previo consentimiento de los usuarios; esto es, debido a que, en la implementación de los honeypot y la configuración de estos, los atacantes tienen acceso a ciertos elementos dentro de la red local.

Por último, se logra analizar la viabilidad de esta herramienta, atendiendo a conceptos frente al uso, configuración e implementación de los honeypot, logrando así los objetivos propuestos en la presente monografía, lo que corresponde como un insumo para su análisis progresivo y a futuros estudios que permitan un mayor aprovechamiento de estos, y en qué áreas y situaciones pueden resultar factibles este tipo de tecnologías.

REVISIÓN Y RECOPILACIÓN BIBLIOGRÁFICA:

F.Pouget, M. Daicer. Honeypot-Based Forensics. Disponible En: Ftp://Ftp.Mirror.Ac.Za/Www.Honeynet.Org/Papers/Individual/Auscert_Fullpaper_Bis.Pdf

Gallego, Eduardo, López De Vergara, Jorge. Honeynets: Aprendiendo Del Atacante. Disponible En: Https://Web.Dit.Upm.Es/~Jlopez/Publicaciones/Mundointernet04.Pdf

González Gómez, Diego. Sistema De Detección De Intrusos {En Línea}. Disponible En: Https://Www.Dgonzalez.Net/Papers/Ids/Html/Cap04.Htm

Gutierrez, C. Honeypots: alternativas para analizar códigos maliciosos. Tomado de: https://www.welivesecurity.com/la-es/2013/01/21/honeypots-alternativas-analizar-codigos-maliciosos/

Honeynet security consoles and honeypot legal issues. Disponible en: http://searchsecurity.techtarget.com/feature/Honeynet-security-consoles-and-honeypot-legal-issues

Honeypots, Monitorizando A Los Atacantes. Disponible En: Http://Www.Egov.Ufsc.Br/Portal/Sites/Default/Files/Honeypots_Monitorizando_A_Los_Atacantes.Pdf

Kippo. Herramienta honeypot de interacción media. SSH. Disponible en: https://github.com/desaster/kippo

P. Niels. A Virtual Honeypot Framework. Disponible En: Http://Static.Usenix.Org/Event/Sec04/Tech/Full_Papers/Provos/Provos_Html/

Ruda, Rafael. Como Crear Un Honeypot Paso A Paso. Disponible En: Http://Www.Segu-Info.Com.Ar/Terceros/?Autor=Ruda

S. Lance. Future of Honeypots. Disponible en: http://www.blackhat.com/presentations/bh-federal-03/bh-fed-03-spitzner.pdf

SANS Institute InfoSec Reading Room. A primer on US laws related to honeypot deployments. Disponible en: https://www.sans.org/reading-room/whitepapers/legal/cyberlaw-101-primer-laws-related-honeypot-deployments-1746

Spitzner, L. Honeypots: ¿Are They Illegal? Disponible en: https://www.symantec.com/connect/articles/honeypots-are-they-illegal

--------Tracking Hackers. Disponible en: http://www.it-docs.net/ddata/792.pdf

Tesis de Seguridad De La Información. Diseño y Desarrollo de Honeynets Virtuales Utilizando VMWARE, Para La Detección de Intrusos Informáticos. Disponible en: http://www.segu-info.com.ar/tesis/

The hony Project. Confusion About Honeypots. Disponible en: http://www.honeynet.org/node/458

The Value Of Honeypots, Part One: Definitions And Values Of Honeypots. Disponible En: Https://Www.Symantec.Com/Connect/Articles/Value-Honeypots-Part-One-Definitions-And-Values-Honeypots

ANEXOS

ANEXO I RESUMEN ANALÍTICO ESPECIALIZADO - RAE

1. Información General	
Tema	Conceptualización sobre Honeypot, referenciado las características, configuraciones y estructura semántica en su implementación.
Titulo	HONEYPOT, HACIA UN PROTOCOLO DE SEGURIDAD MÁS EFICIENTE Y COMPETITIVO.
Autor(es)	Kevin David Martínez Contreras
Director	Ing. Hernando José Peña Hidalgo
Fuente Bibliográfica	F.Pouget, M. Daicer. Honeypot-Based Forensics. Disponible En: Ftp://Ftp.Mirror.Ac.Za/Www.Honeynet.Org/Papers/Individual/Auscert_Fullpaper_Bis.Pdf Gallego, Eduardo, López De Vergara, Jorge. Honeynets: Aprendiendo Del Atacante. Disponible En: Https://Web.Dit.Upm.Es/~Jlopez/Publicaciones/Mundointernet04.Pdf González Gómez, Diego. Sistema De Detección De Intrusos {En Línea}. Disponible En: Https://Www.Dgonzalez.Net/Papers/Ids/Html/Cap04.Htm Gutierrez, C. Honeypots: alternativas para analizar códigos maliciosos. Tomado de: https://www.welivesecurity.com/la-es/2013/01/21/honeypots-alternativas-analizar-codigos-maliciosos/ Honeynet security consoles and honeypot legal issues. Disponible en: http://searchsecurity.techtarget.com/feature/Honeynet-security-consoles-and-honeypot-legal-issues

	Honeypots, Monitorizando A Los Atacantes. Disponible En: Http://Www.Egov.Ufsc.Br/Portal/Sites/Default/Files/Honeypots_Monitorizando_A_Los_Atacantes.Pdf P. Niels. A Virtual Honeypot Framework. Disponible En: Http://Static.Usenix.Org/Event/Sec04/Tech/Full_Papers/Provos/Provos_Html/ Ruda, Rafael. Como Crear Un Honeypot Paso A Paso. Disponible En: Http://Www.Segu-Info.Com.Ar/Terceros/?Autor=Ruda S. Lance. Future of Honeypots. Disponible en: http://www.blackhat.com/presentations/bh-federal-03/bh-fed-03-spitzner.pdf SANS Institute InfoSec Reading Room. A primer on US laws related to honeypot deployments. Disponible en: https://www.sans.org/reading-room/whitepapers/legal/cyberlaw-101-primer-laws-related-honeypot-deployments-1746
Año	2017
Resumen	Un Honeynet es una herramienta, más a fondo una arquitectura la cual es diseñada para ser vulnerada dentro de un ambiente controlado; esta red permite la monitorización de los ataques en ella, con el fin de registrar los datos del atacante y el ataque en sí, de esta manera se permite estudiar un mejor sistema de seguridad el cual logre fortalecer la capa de protocolo de seguridad dentro de la misma red y evitar futuros ataques. La siguiente monografía busca definir de manera clara y concisa lo que es un honeypot, tomando consulta de las investigaciones realizadas anteriormente y de proyectos vigentes que siguen estudiando este tipo de

	arquitectura, permitiendo así buscar innovar en el sistema o protocolo de red utilizado para la captura de datos en los diferentes ataques. De esta forma, con el ejercicio de la monografía, se dará reunión a un consolidado de investigaciones y definiciones estratégicas que den paso a una mejor conceptualización, caracterización y justificación de la arquitectura en red propuesta por un Honeynet.
Palabras Claves	Honeynet; Honeypot; Arquitectura; Red; Intruso;
Contenidos	Portada Nota de Aceptación Dedicatoria Agradecimientos Tabla de contenido Lista de Tablas Lista de Figuras Introducción Descripción del problema: - Planteamiento del problema - Formulación del problema Justificación Objetivos - General - Específicos Delimitación del proyecto Marco de Referencia - Teórico - Conceptual - Legal Diseño Metodológico Cronograma Recursos Necesarios Resultados a entregar Divulgación

	Conclusiones Revisión Bibliográfica Anexos.

2. Descripción del problema de investigación

La seguridad en las redes es un tema que a muchos nos compete, y sin importar si son organizaciones grandes, medianas o pequeñas, cual sea el tamaño, siempre debe existir los diferentes protocolos de seguridad que permitan la buena gestión de la información que se procesa, e indistintamente de la información que administren las organizaciones, el respaldo a la integridad, confidencialidad y disponibilidad de las mismas ocupa el primer lugar para de esta forma lograr una mejor gestión de la información, por tal los mecanismos de seguridad implementados deben obedecer al control y a salvaguardar los datos que se procesan en caso de una vulneración de la seguridad.

Ahora bien, muchas entidades permiten hasta cierto punto la instrucción consentida, pero ¿qué es esto?, mediante la adopción de honeypot, un "honeypot" no es un sistema de detección de intrusiones, pero puede ayudar a mejorar sus métodos de detección y aportar nuevos patrones de ataque. Es un sistema diseñado para engañar a los intrusos, poder estudiar sus actividades, y así aprender de sus métodos. Se basa en la idea de "conocer al enemigo" para poder combatirlo.

De esta forma las organizaciones, toleran algunas irrupciones en su sistema con el fin de detectar las vulnerabilidades ocasionadas por el ataque y de esta forma, diseñar un mejor protocolo de seguridad, pero, no obstante, los ataques son cada vez más profesionalizados, tomando las contramedidas correctas y evitar este tipo de detecciones de intrusos. Esta realidad está tomando auge y son las desventajas que este sistema de detecciones debe corregir y evitar crear huésped invisible dentro del sistema de red.

FORMULACIÓN DEL PROBLEMA

¿En qué medida una red honeypot puede minimizar su riesgo de detección al ser atacada dentro de una red local o intranet, y como a partir de ello, maximizar su potencial de monitorización a los intrusos?

3. Objetivos

OBJETIVO GENERAL

Determinar mediante exploración conceptual y prueba experimental, los alcances de un honeypot, en la cual se pueda reflejar en los procesos de monitorización.

OBJETIVOS ESPECÍFICOS:

- ✓ Identificar las fuentes de información necesaria para llevar a cabo la conceptualización apropiada de un Honeypot.
- ✓ Explorar la ruta adecuada para la optimización de la red de honeypot
- ✓ Identificar las incidencias de un honeypot en la configuración de red.
- ✓ Analizar la arquitectura de un honeypot para su correcta implementación.

4. Metodología

El presente ante-proyecto de grado corresponde a la línea de investigación Gestión De Sistemas: Auditoria de Sistemas.

El tipo de investigación es Documental.

A partir de este tipo de Investigación, se dará paso a la búsqueda de información correspondiente al tema seleccionado mediante fuentes bibliográficas que permitan la recopilación de los datos concernientes al objeto de exploración. La recopilación bibliográfica está basada en documentos que detallan la originalidad y causa de la temática en desarrollo, así como trabajos de investigación, ensayos, artículos de revistas indexadas, documentos académicos, videoclips entre otras fuentes vinculadas al tema de estudio seleccionado.

La selección de este tipo de investigación, garantizara la posesión del material que soportara todo el desarrollo de la presente monografía, entendiéndose esta como la ruta de exploración, ordenamiento, selección de la información más pertinente, procesamiento de la misma y la aplicabilidad final de esta, con el fin de separar las partes que la componen para un mejor proceder de los datos contenidos, todo ello para su respectiva conclusión positiva, encaminada siempre a generar conocimiento, mediante el debate misma de la información y el proceder de ordenamiento documental.

5. Referentes Teóricos

Se hace consulta en diferentes fuentes en la web sobre la conceptualización de la herramienta honeypot, así como su funcionamiento, configuración dentro de un entorno de red, su implementación, y puesta en marcha; con los elementos anteriores, se realiza una descripción conforme a la consulta anteriormente realizada.

6. Referentes Conceptuales

Se postulan diferentes conceptos usados a lo largo de todo el proyecto de monografía con el fin de analizar la conceptualización y comprensión de todo el material expuesto a lo largo de la monografía. Se interioriza en conceptos como honeypot, seguridad de la información, integridad, confidencialidad, disponibilidad y no repudio, que ayudaran a una mejor y clara comprensión de la temática.

7. Resultados

La presente investigación monográfica, contemplara la conceptualización de Honeypot como herramienta para la monitorización de acciones intrusas dentro de la red establecida para tal fin. Abordando una serie de conceptos y referentes bibliográficos que permitirán su comprensión ideal, en pro de un mejor aprovechamiento de este tipo herramientas en el mundo de la seguridad informática. Todo este conglomerado de conceptos, teorías y demás

aceptaciones literarias técnico-pedagógicas, están basadas en la investigación previa a fuentes y expertos dedicados y conocedores de la temática.

Partiendo de la asimilación de las fuentes de información que corresponden a la instancia de investigación y consulta, desarrollada durante todo el tiempo de realización de la monografía, el cual es manifestada a lo largo del documento en mención y que resalta la temática abordada sobre los Honeypot.

Se muestra la configuración de un honeypot en la red, validando la lógica de la estructura de las redes, acorde a las topologías que son implementadas dentro de la misma; para ello se hizo énfasis en la adopción de una posición del honeypot, el cual fue causa de factores que intervienen en o no en la funcionalidad correcta de la herramienta. En este sentido la configuración del honeypot, se logra gracias a los objetivos con el cual la empresa traza para lograr así los fines de la organización.

Se emplea un proceso de optimización de los honeypot, abordando políticas de seguridad manifiesta a las funciones de estas herramientas, así mismo se realizan consideraciones a la forma, uso y responsabilidad de utilización de los honeypot.
Por último se logra, analizar la implementación de los honeypot acorde a su arquitectura lógica, y como está entre en función con los elementos de la red local.

8. Conclusiones

Con el desarrollo de la presente monografía, se logra identificar, conocer y comprender, dentro de este ejercicio investigativo la conceptualización de los honeypot, como herramientas usadas dentro del contexto de la seguridad de la información, para la extracción y análisis de los comportamientos de los atacantes en la red; dando aplicabilidad a este, dentro de un amiente controlado, y que

mantiene los debido protocolos de seguridad establecidos, suponiendo posibles eventos fuera de los objetivos.

ANEXOS

ANEXO I RESUMEN ANALÍTICO ESPECIALIZADO - RAE

1. Información General	
Tema	Conceptualización sobre Honeypot, referenciado las características, configuraciones y estructura semántica en su implementación.
Titulo	HONEYPOT, HACIA UN PROTOCOLO DE SEGURIDAD MÁS EFICIENTE Y COMPETITIVO.
Autor(es)	Kevin David Martínez Contreras
Director	Ing. Hernando José Peña Hidalgo
Fuente Bibliográfica	F.Pouget, M. Daicer. Honeypot-Based Forensics. Disponible En: Ftp://Ftp.Mirror.Ac.Za/Www.Honeynet.Org/Papers/Individual/Auscert_Fullpaper_Bis.Pdf Gallego, Eduardo, López De Vergara, Jorge. Honeynets: Aprendiendo Del Atacante. Disponible En: Https://Web.Dit.Upm.Es/~Jlopez/Publicaciones/Mundointernet04.Pdf González Gómez, Diego. Sistema De Detección De Intrusos {En Línea}. Disponible En: Https://Www.Dgonzalez.Net/Papers/Ids/Html/Cap04.Htm Gutierrez, C. Honeypots: alternativas para analizar códigos maliciosos. Tomado de: https://www.welivesecurity.com/la-es/2013/01/21/honeypots-alternativas-analizar-codigos-maliciosos/ Honeynet security consoles and honeypot legal issues. Disponible en: http://searchsecurity.techtarget.com/feature/Honeynet-security-consoles-and-honeypot-legal-issues

	Honeypots, Monitorizando A Los Atacantes. Disponible En: Http://Www.Egov.Ufsc.Br/Portal/Sites/Default/Files/Honeypots_Monitorizando_A_Los_Atacantes.Pdf P. Niels. A Virtual Honeypot Framework. Disponible En: Http://Static.Usenix.Org/Event/Sec04/Tech/Full_Papers/Provos/Provos_Html/ Ruda, Rafael. Como Crear Un Honeypot Paso A Paso. Disponible En: Http://Www.Segu-Info.Com.Ar/Terceros/?Autor=Ruda S. Lance. Future of Honeypots. Disponible en: http://www.blackhat.com/presentations/bh-federal-03/bh-fed-03-spitzner.pdf SANS Institute InfoSec Reading Room. A primer on US laws related to honeypot deployments. Disponible en: https://www.sans.org/reading-room/whitepapers/legal/cyberlaw-101-primer-laws-related-honeypot-deployments-1746
Año	2017
Resumen	Un Honeynet es una herramienta, más a fondo una arquitectura la cual es diseñada para ser vulnerada dentro de un ambiente controlado; esta red permite la monitorización de los ataques en ella, con el fin de registrar los datos del atacante y el ataque en sí, de esta manera se permite estudiar un mejor sistema de seguridad el cual logre fortalecer la capa de protocolo de seguridad dentro de la misma red y evitar futuros ataques. La siguiente monografía busca definir de manera clara y concisa lo que es un honeypot, tomando consulta de las investigaciones realizadas anteriormente y de proyectos vigentes que siguen estudiando este tipo de

	arquitectura, permitiendo así buscar innovar en el sistema o protocolo de red utilizado para la captura de datos en los diferentes ataques. De esta forma, con el ejercicio de la monografía, se dará reunión a un consolidado de investigaciones y definiciones estratégicas que den paso a una mejor conceptualización, caracterización y justificación de la arquitectura en red propuesta por un Honeynet.
Palabras Claves	Honeynet; Honeypot; Arquitectura; Red; Intruso;
Contenidos	Portada Nota de Aceptación Dedicatoria Agradecimientos Tabla de contenido Lista de Tablas Lista de Figuras Introducción Descripción del problema: - Planteamiento del problema - Formulación del problema Justificación Objetivos - General - Específicos Delimitación del proyecto Marco de Referencia - Teórico - Conceptual - Legal Diseño Metodológico Cronograma Recursos Necesarios Resultados a entregar Divulgación

	Conclusiones Revisión Bibliográfica Anexos.

2. Descripción del problema de investigación

La seguridad en las redes es un tema que a muchos nos compete, y sin importar si son organizaciones grandes, medianas o pequeñas, cual sea el tamaño, siempre debe existir los diferentes protocolos de seguridad que permitan la buena gestión de la información que se procesa, e indistintamente de la información que administren las organizaciones, el respaldo a la integridad, confidencialidad y disponibilidad de las mismas ocupa el primer lugar para de esta forma lograr una mejor gestión de la información, por tal los mecanismos de seguridad implementados deben obedecer al control y a salvaguardar los datos que se procesan en caso de una vulneración de la seguridad.

Ahora bien, muchas entidades permiten hasta cierto punto la instrucción consentida, pero ¿qué es esto?, mediante la adopción de honeypot, un "honeypot" no es un sistema de detección de intrusiones, pero puede ayudar a mejorar sus métodos de detección y aportar nuevos patrones de ataque. Es un sistema diseñado para engañar a los intrusos, poder estudiar sus actividades, y así aprender de sus métodos. Se basa en la idea de "conocer al enemigo" para poder combatirlo.

De esta forma las organizaciones, toleran algunas irrupciones en su sistema con el fin de detectar las vulnerabilidades ocasionadas por el ataque y de esta forma, diseñar un mejor protocolo de seguridad, pero, no obstante, los ataques son cada vez más profesionalizados, tomando las contramedidas correctas y evitar este tipo de detecciones de intrusos. Esta realidad está tomando auge y son las desventajas que este sistema de detecciones debe corregir y evitar crear huésped invisible dentro del sistema de red.

FORMULACIÓN DEL PROBLEMA

¿En qué medida una red honeypot puede minimizar su riesgo de detección al ser atacada dentro de una red local o intranet, y como a partir de ello, maximizar su potencial de monitorización a los intrusos?

3. Objetivos

OBJETIVO GENERAL

Determinar mediante exploración conceptual y prueba experimental, los alcances de un honeypot, en la cual se pueda reflejar en los procesos de monitorización.

OBJETIVOS ESPECÍFICOS:

- ✓ Identificar las fuentes de información necesaria para llevar a cabo la conceptualización apropiada de un Honeypot.
- ✓ Explorar la ruta adecuada para la optimización de la red de honeypot
- ✓ Identificar las incidencias de un honeypot en la configuración de red.
- ✓ Analizar la arquitectura de un honeypot para su correcta implementación.

4. Metodología

El presente ante-proyecto de grado corresponde a la línea de investigación Gestión De Sistemas: Auditoria de Sistemas.

El tipo de investigación es Documental.

A partir de este tipo de Investigación, se dará paso a la búsqueda de información correspondiente al tema seleccionado mediante fuentes bibliográficas que permitan la recopilación de los datos concernientes al objeto de exploración. La recopilación bibliográfica está basada en documentos que detallan la originalidad y causa de la temática en desarrollo, así como trabajos de investigación, ensayos, artículos de revistas indexadas, documentos académicos, videoclips entre otras fuentes vinculadas al tema de estudio seleccionado.

La selección de este tipo de investigación, garantizara la posesión del material que soportara todo el desarrollo de la presente monografía, entendiéndose esta como la ruta de exploración, ordenamiento, selección de la información más pertinente, procesamiento de la misma y la aplicabilidad final de esta, con el fin de separar las partes que la componen para un mejor proceder de los datos contenidos, todo ello para su respectiva conclusión positiva, encaminada siempre a generar conocimiento, mediante el debate misma de la información y el proceder de ordenamiento documental.

5. Referentes Teóricos

Se hace consulta en diferentes fuentes en la web sobre la conceptualización de la herramienta honeypot, así como su funcionamiento, configuración dentro de un entorno de red, su implementación, y puesta en marcha; con los elementos anteriores, se realiza una descripción conforme a la consulta anteriormente realizada.

6. Referentes Conceptuales

Se postulan diferentes conceptos usados a lo largo de todo el proyecto de monografía con el fin de analizar la conceptualización y comprensión de todo el material expuesto a lo largo de la monografía. Se interioriza en conceptos como honeypot, seguridad de la información, integridad, confidencialidad, disponibilidad y no repudio, que ayudaran a una mejor y clara comprensión de la temática.

7. Resultados

La presente investigación monográfica, contemplara la conceptualización de Honeypot como herramienta para la monitorización de acciones intrusas dentro de la red establecida para tal fin. Abordando una serie de conceptos y referentes bibliográficos que permitirán su comprensión ideal, en pro de un mejor aprovechamiento de este tipo herramientas en el mundo de la seguridad informática. Todo este conglomerado de conceptos, teorías y demás

aceptaciones literarias técnico-pedagógicas, están basadas en la investigación previa a fuentes y expertos dedicados y conocedores de la temática.

Partiendo de la asimilación de las fuentes de información que corresponden a la instancia de investigación y consulta, desarrollada durante todo el tiempo de realización de la monografía, el cual es manifestada a lo largo del documento en mención y que resalta la temática abordada sobre los Honeypot.

Se muestra la configuración de un honeypot en la red, validando la lógica de la estructura de las redes, acorde a las topologías que son implementadas dentro de la misma; para ello se hizo énfasis en la adopción de una posición del honeypot, el cual fue causa de factores que intervienen en o no en la funcionalidad correcta de la herramienta. En este sentido la configuración del honeypot, se logra gracias a los objetivos con el cual la empresa traza para lograr así los fines de la organización.

Se emplea un proceso de optimización de los honeypot, abordando políticas de seguridad manifiesta a las funciones de estas herramientas, así mismo se realizan consideraciones a la forma, uso y responsabilidad de utilización de los honeypot.
Por último se logra, analizar la implementación de los honeypot acorde a su arquitectura lógica, y como está entre en función con los elementos de la red local.

8. Conclusiones

Con el desarrollo de la presente monografía, se logra identificar, conocer y comprender, dentro de este ejercicio investigativo la conceptualización de los honeypot, como herramientas usadas dentro del contexto de la seguridad de la información, para la extracción y análisis de los comportamientos de los atacantes en la red; dando aplicabilidad a este, dentro de un amiente controlado, y que

mantiene los debido protocolos de seguridad establecidos, suponiendo posibles eventos fuera de los objetivos.