|  |
| --- |
| **UNIVERSIDAD TECNOLÓGICA DE PANAMÁ**  **FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES**  **SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN**  **TÍTULO DEL PROYECTO**  “IMPLEMENTACIÓN DE UNA HONEYNET”  **PROFESORA**  LEGUIAS, ISABEL  **INTEGRANTES**  CEDEÑO, MANUEL  CEDEÑO, MARÍA  GONZÁLEZ, ERICK  **TRABAJO PARA OPTAR AL TÍTULO DE**  **LICENCIATURA EN DESARROLLO DE SOFTWARE**  AÑO  2018 |

1. **PLANTEAMIENTO DEL PROBLEMA.**
   1. **Título de la Investigación**

“Implementación de una Honeynet”

* 1. **Introducción**

La información que circula en una red de datos puede ser manipulada por expertos en el área de redes, pero a su vez existen atacantes que usan esa información a su conveniencia, un usuario en una computadora dentro de una red de datos ingresa a un sistema de aplicación a través de Internet o localmente, el atacante puede usar un software que permite capturar tramas de la red robando información de gran importancia.

La seguridad de la información es un tema prioritario. Muchos saben que la tarea de mantener un servidor o un equipo cualquiera, conectado a una red, representa uno de los mayores riesgos que puede haber. En cualquier momento el sistema puede ser comprometido y a su vez, la información.

Una Honeynet es una herramienta de investigación que surge como una herramienta de seguridad diseñada para ser sondeada, atacada y comprometida por hipotéticos intrusos. Es un tipo de Honeypot que consiste en una red diseñada para ser comprometida por intrusos. Sirve para estudiar las técnicas utilizadas por los intrusos que han comprometido la seguridad de la red. El objetivo principal es conocer al enemigo, aprender de él, en definitiva es una herramienta diseñada con propósitos académicos.

Se componen de entornos de redes, conjuntos de aplicaciones de análisis y monitoreo, y dispositivos de almacenamiento de eventos. Luego de realizada su instalación y configuración de todos estos componentes, la honeynet queda dispuesta para recibir ataques, con la intención de mantener un ambiente controlado para el estudio de los eventos ocurridos. Luego, mediante el análisis de esos eventos, es posible comprender los objetivos, tácticas e intereses de los atacantes sobre el entorno propuesto.

En el presente trabajo veremos más a detalle sobre los Honeynets, todos sus alcances y limitantes, sus objetivos entre otros puntos que iremos resaltando.

* 1. **Problema de la Investigación**
     1. Enunciado del problema de investigación

Las primeras referencias de las Honeypot datan desde 1990 en el libro “El huevo del cuco” de Clifford Stolls, pero es el proyecto Honeynet quien utilizo las Honeypots como concepto y se convirtió en la organización que dio impulso a esta tecnología. Luego del reconocimiento que se dio a esta herramienta muchas organizaciones desarrollaron proyectos de implementación y sacaron beneficios de esta.

Las honeynet o honeypot son un sistema de red de trampa o también una herramienta de investigación de entornos que son diseñadas para permitir ataques y obtener informaciones del atacante. No obstante, son usados para estudiar cómo operan dichos atacantes o llamados hackers, pero todo está basado en una red discreta la cual es monitoreada y controlada.

En la actualidad las vulnerabilidades son crecientes o exponenciales, en lo cual las informaciones se ven afectadas por entes (hackers) que quieren realizar algún tipo de daño, se vuelve tan común ver personas que buscan la manera de vulnerar sistemas para obtener informaciones y luego utilizarla contra la empresa como chantajes, etc.

Haciendo referencia al punto anterior nos damos cuenta que debemos invertir en implementaciones de tecnologías como lo es una honeynet, el cual es una red de tráfico que corre en tiempo real en sistemas operativos y software detectando algún tipo de ataque y así proteger nuestra información, en un ambiente de pruebas o señuelos.

* + 1. Formular el problema de investigación
* ¿Cómo una honeynet ayuda a detectar vulnerabilidades en un sistema operativo y software?
* ¿Cómo recolectar información en una Honeynet?
* ¿Hasta qué límite podría cubrir la implementación de una Honeynet en nuestros sistemas?
  1. **.Objetivos de la Investigación**
     1. Objetivo general

Implementar el uso de una honeynet para recolectar información del atacante y evitar futuras vulnerabilidades.

* + 1. Objetivos específicos:
* Brindar herramientas técnicas que permitan proteger la red de ataques informáticos externos o internos.
* Implementar el uso de las honeynet en el sistema operativo y softwares para recolectar informaciones.
* Documentar y analizar las herramientas de seguridad utilizadas en el nodo central y las necesarias para la implantación de la Honeynet.
* Hacer pruebas de efectividad de la Honeynet y analizar los resultados.
  1. **Justificación de la Investigación:**

Las redes y sus aplicaciones, y en particular Internet, han introducido nuevas posibilidades que también implican riesgos. Éstos surgen a partir de las vulnerabilidades que poseen los sistemas. La existencia de vulnerabilidades implica amenazas, cuya concreción son los ataques.

Las vulnerabilidades pueden ser aprovechadas, con diversos fines, por muchas clases de atacantes: expertos o legos; interesados en el recurso de información que piensan comprometer, o motivados por intenciones en contra de la organización que atacan. En los últimos años, la frecuencia de aparición de ataques ha crecido considerablemente. Este hecho, unido a las vulnerabilidades, descubiertas o latentes, en todo tipo de sistemas operativos y aplicaciones, convierte a cualquier organización en una víctima potencial. Este panorama plantea la necesidad de disponer de instrumentos que permitan descubrir y analizar los agujeros de seguridad que pueda presentar un sistema, así como las técnicas y herramientas utilizadas por los posibles atacantes.

Los dueños de las empresas en Panamá no cuentan con el conocimiento amplio de que es un ataque a una red por ende son propensos a que terceras personas tengan acceso a información confidencial, cabe destacar que se busca implementar el uso de una red Honeynet para el estudio y estructuración que nos permita crear una red de seguridad solida y segura.

Para prevenir o mitigar cualquier tipo de amenaza es necesario conocer y comprender las vulnerabilidades constitutivas del entorno. Una de las metodologías para esto es crear un ambiente de red controlado, pero a la vez lo suficientemente atractivo para los atacantes, que permita detectar comportamientos maliciosos, para estudiarlos, entenderlos y actuar en consecuencia, ya sea de una manera proactiva o reactiva, sin perjudicar el ambiente de producción de la organización. Este es el fundamento de las Honeynets.

* 1. **Alcance o limitaciones:**

La propuesta que incluye la implementación de Honeynet, para la detección de intrusos informáticos permitirá:

1. Proteger la red de ataques externos e internos.
2. Monitorizar accesos a la red no autorizada o posibles ataques, así como registrarlos y activar las alarmas correspondientes.
3. Engañar a posibles atacantes mediante redes falsas simuladas y registrar dichos eventos.

Entre las limitaciones de la honeynet tenemos:

1. El hardware necesario de la máquina que alberga a la Honeynet.
2. El software que es usado para virtualizar.
3. Si el atacante toma en su poder la máquina anfitriona tendría control sobre toda la Honeynet y sería un peligro para los sistemas reales.
4. **MARCO TEÓRICO O CONCEPTUAL**

La idea de Honeypot es desarrollada con el término Honeynet (Red Trampa). Esta expresión fue adoptada por The Money Project; una organización no lucrativa, fundada por Lance Spitzner [1].

La primera vez que se hace uso del término honeynet o Honeypot es cuando en 1999 se inicia el proyecto honeynet y su fundador Lance Spitzner publica un texto llamado “To Build a Honeypot”. A partir de ahí se plantea el primer modelo de Honeypot llamado Gen I. Posterior mente en el año 2002 se plantea el modelo GEN II el cual hace una serie de cambios a la arquitectura propuesta en la GEN I [5].

* GEN I

Esta arquitectura simple fue la primera en desarrollarse, en 1999. Una red es situada detrás de un dispositivo de control de acceso, generalmente un cortafuego, como se muestra en la siguiente figura. Las tecnologías Gen I implementan el Control de Datos y la Captura de Datos son medidas simples pero eficaces [1].

La mayoría de los textos de la colección Conoce a tu enemigo fueron escritos utilizando estas tecnologías. No son tan efectivas como las GenII, pero a través de su simplicidad y de la cantidad de pruebas hechas durante años, potencialmente poco pueden fallar [7].

* GEN II

Basada en la combinación de viejas y nuevas técnicas, la Honeynet GenII puede mejorar la flexibilidad, gestión, y seguridad de los despliegues de las honeynets. Esta arquitectura de Honeynets fue desarrollada en 2002, y fue pensada para solventar muchos de los problemas existentes en el modelo anterior. Con respecto a las tecnologías Gen I, esta arquitectura es más fácil de implementar, más difícil de detectar y tiene un mantenimiento más seguro [1].

La finalidad de las Honeynets GenII es crear una solución que sea más fácil de desarrollar y aún más difícil de detectar. El Control de Datos en GenII ofrece al agresor mayores posibilidades para interactuar con los sistemas comprometidos, teniendo mayor control sobre sus actividades y haciendo más difícil que este control sea detectado. Esperamos que al darle al agresor más flexibilidad en sus acciones, especialmente en conexiones salientes, podamos recoger mayor información de ellas. Esto se consigue creando una respuesta más inteligente y flexible a las acciones del blackhat [7].

Cada tráfico desde y hacia un Honeypot es sospechoso, en general es una actividad no autorizada. Por consiguiente, todos los datos recogidos por un Honeypot son datos desordenados en primera instancia, para después ser tabulados, donde en general no se produce una gran cantidad de registros porque los sistemas se están ejecutando en esa máquina [6].

La seguridad de la información es un tema prioritario. Para nadie es un secreto que la tarea de mantener un servidor o un equipo cualquiera, conectado a una red, representa uno de los mayores riesgos posibles. En cualquier momento el sistema puede ser comprometido por un tercero y junto con él, la información [1].

La difusión de virus y gusanos por Internet es, desgraciadamente, algo muy común, al igual que otro tipo de ataques más dirigidos. El número de ataques por mes, crece a un ritmo vertiginoso, sólo hay que mirar las estadísticas que ofrece cualquier compañía antivirus o entidad dedicada a la vigilancia y respuesta ante incidentes de seguridad [2].

Actualmente la comunicación entre computadores ha cobrado una importancia vital en el mundo de la seguridad informática y el volumen de redes conectadas entre sí a lo largo del mundo supera cualquier expectativa inicial. La importancia de los datos que una empresa mueve a lo largo de sus canales de información es considerable y por ello las empresas invierten gran cantidad de recursos económicos y humanos para resguardar su seguridad, en la actualidad, se continúa con la investigación y se plantean nuevas aplicaciones y proyectos como el Honey-Droid un Smartphone Honeypot [3].

Identificar y localizar las actividades de los atacantes es el problema más serio, en la medida en que se debe hacer dentro del tráfico producido en la red, realizando un sniffer del tráfico y estudiando los distintos paquetes que utiliza el atacante con el fin de observarlo [1].

En el Área de Tecnologías Informática existe muchos mecanismos de salvaguardar la información, el principal riesgo es la falta de conocimiento sobre estos, ya que día a día aparecen nuevas herramientas de monitoreo de la red al igual que aparecen las amenazas [4].

Debido a los problemas derivados de la incapacidad de reducir la ventana de vulnerabilidad, y de detectar ataques sobre vulnerabilidades desconocidas, se están proponiendo algunas alternativas.

También existen iniciativas en el mundo académico dirigidas a detectar ataques a medida que se estén produciendo (incluso si son ataques desconocidos) [2].

Una Honeynet es una herramienta de investigación. Es un tipo de Honeypot que consiste en una red diseñada para ser comprometida por intrusos. Sirve para estudiar las técnicas utilizadas por los intrusos que han comprometido la seguridad de la red. El objetivo principal es conocer al enemigo, aprender de él, en definitiva es una herramienta diseñada con propósitos académicos [1].

No es un sistema solitario, sino una red. Esta red puede estar compuesta por distintos sistemas trampa, tales como Linux, Windows, Solaris, routers, conmutadores, etc. El hecho de proporcionar un entorno de red aporta un ambiente más creíble, más real desde el punto de vista del intruso, del atacante de la red. Un entorno de sistemas heterogéneos permite además, captar la atención de más intrusos, algunos de los cuales están especializados en atacar determinados sistemas operativos o servicios. Por otra parte, permite aprender un mayor y variado número de tácticas de ataque [1].

Los Honeynets son herramientas de seguridad con un punto de vista diferente al tradicional, que es un comportamiento defensivo, tradicionalmente se intenta defender de ataques una red, mediante cortafuegos, medios de cifrado o sistemas de detección de intrusos (IDS). Los Honeynets son herramientas diseñadas básicamente para aprender y adquirir experiencia en el área de seguridad [1].

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 [8].

Una Honeynet [9, 10] es básicamente un conjunto o red de varios Honeypots, que forman entre todos una red preparada para recibir ataques y capturar toda información relacionada con ellos.

Esta red debe simular una red real, tanto en topología, como en número de sistemas y heterogeneidad. Gracias a que tenemos una red y no un único sistema (como ocurría con los Honeypots), podemos tener un mayor nivel de interacción con el intruso, dándole toda la libertad de acción que creamos necesaria para nuestros propósitos. Citar también que las Honeynets utilizan un equipo para captura de datos y también para control de conexiones, de modo que un intruso, a pesar de poder hacerse con el control de los Honeypots, no pueda salir de esta red trampa.

La corriente actual del concepto Honeynet se basa en que estos sistemas, por definición, no deben tener valor productivo alguno (todo tráfico que reciba será sospechoso), así como que deben ser generalmente sistemas con muchos servicios externos, y a ser posible con sistemas operativos muy vulnerables. Cualquier intento de conexión a una Honeynet es probablemente un tanteo, un ataque o un intento de comprometer el sistema. Esto puede ser una gran ventaja, ya que podemos tener la certeza de que únicamente analizaremos tráfico y acciones de entidades (ya sean programas o personas) no autorizadas [2].

**BIBLIOGRAFÍA**

[1] Federación de Enseñanza de CC.OO. de Andalucia. (2009). HoneyNets, una desconocida en la seguridad informática. 2010, Sitio web: https://www.feandalucia.ccoo.es/docu/p5sd6337.pdf

[2] CERT/CC Statistics 1988-2005 http://www.cert.org/stats/cert\_stats.html

[3] S. L. a. M. L. Collin Mulliner, “Poster: HoneyDroid - Creating a Smartphone,” Technische Universit¨at Berlin, 2011.

[4] P. A. W. Leonardo, “http://repo.uta.edu.ec/,” Noviembre 2012. Disponible en: http://repositorio.uta.edu.ec/handle/123456789/2894.

[5] Miguel Lara & Diana López. (2013). Honeypot virtualizado para ambientes académicos y de investigación. 2013, de Facultad Ingeniería de Sistemas especialización en seguridad informática Sitio web: http://polux.unipiloto.edu.co:8080/00001041.pdf

[6] Olivier Thonnard, Jouni Viinikka, Corrado Leita, Marc Dacier, “Automating the Analysis of Honeypot Data,” de Automating the Analysis of Honeypot Data , Cambridge, MA, USA, Springer Berlin Heidelberg, 2008, pp. pp 406-407.

[7] Honeynet Project. (2003). Conoce a tu enemigo: Honeynets. 25 de Julio del 2003, de Honeynet Project

Sitio web: http://his.sourceforge.net/honeynet/papers/honeynet/

[8] Eduardo Gallego, Jorge Lopez. (2004). Honeynets: Aprendiendo del Atacante. 2004, de Departamento de Ingeniería de Sistemas Telemáticos, Universidad Politécnica de Madrid Sitio web: http://www.dit.upm.es//~jlopez/publicaciones/mundointernet04.pdf

[9] Spitzner, L. Honeypots: Tracking Hackers. Addison-Wesley, ISB 0321108957, 2003.

[10] The Honeynet Project. Know Your Enemy: Learning About Security Threats, 2nd Edition. Addison-Wesley, ISBN 0321166469, 2004.