ANÁLISIS DE EFECTIVIDAD DEL USO DE HONEYNET ANTE ATAQUES INFORMÁTICOS APLICADO A PYMES

JORGE ALEJANDRO HOYOS BOLAÑOS

233006A_611

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2021

ANÁLISIS DE EFECTIVIDAD DEL USO DE HONEYNET ANTE ATAQUES INFORMÁTICOS APLICADO A PYMES

JORGE ALEJANDRO HOYOS BOLAÑOS

Proyecto de grado para la obtención del título de

Especialidad en Seguridad Informática

Monografía

Director

ING. JOEL CARROLL VARGAS M. Sc

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2021

Nota de aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Nacional Abierta y a Distancia para optar al título de Especialista en Seguridad Informática

Jurado_____

Jurado_____

Bogotá, Cundinamarca 20 de abril de 2019

DEDICATORIA

En dedicación a nuestro señor, por la sapiencia, que me brindo durante los días en los que desarrolle este trabajo, por brindarme el conocimiento para lograr alcanzar mis objetivos.

A mi hijo Pablo Nicolás Hoyos Castro, por brindarme la inspiración y las fuerzas para mejorar cada día más como persona, como padre y como profesional.

AGRADECIMIENTOS

A mis tutores de la UNAD por brindarme sus conocimientos y orientación en este largo trayecto de aprendizaje en pro de una mejora profesional y personal.

CONTENIDO

TABLA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

"En el ámbito de la seguridad dirigida a las tecnologías y más puntualmente hablando de la seguridad en sistema de cómputo, se pueden encontrar diversos elementos y herramientas que las empresas optan o emplean para cubrir esta necesidad, entre estas se pueden encontrar firewall, detectores de intrusos IDS, preventores de intrusos IPS, sniffers, antivirus, e incluso soluciones desconocidas no solo para usuarios si no incluso para el propio profesional, y estas herramientas se denominan Honeypots y Honeynets, una solución que podría llegar a brindar una importante protección de seguridad a nivel de sistemas.

Normalmente, dentro de aquellos que por lo menos han oído hablar de esta herramienta, muchos no sabrían indicar cuál es su utilidad, en que arquitectura de seguridad se puede desplegar, con que otras herramientas de seguridad deberían o podrían trabajar de forma conjunta, etc. Para este estudio se hablará puntualmente de los Honeynets, estos por simple intuición se puede determinar de que se trataría, no es sino el conjunto de los Honeypots.

Ahora, desde un punto de vista conceptual puede ser diferente a las herramientas de seguridad que habitualmente se despliegan en una red, pero no así desde un punto de vista funcional, ya que al final, como cualquier herramienta de seguridad recolecta datos, para su análisis y una posterior propuesta de medidas correctoras ante las posibles brechas de seguridad que existan en un sistema o red.

Desde un punto de vista básico, el rol que juegan los Honeynets en la red de una compañía son:

- Potenciación de IDS y Firewall
- Investigación
- Respuesta a incidentes
- Análisis Forense
- Engaño a los atacantes
- Disuasión"[1].

Conceptos previos

[1] RAMOS VARÓN, Antonio ángel. BARBERO MUÑOZ, Carlos A. GONZÁLEZ CAÑAS, Juan M. PI COUTO RAMOS, Fernando. SERRANO APARICIO, Enrique. Seguridad perimetral, monitorización y ataques en redes. Bogotá: Ra-ma, 2015. 81p

“Es importante antes de adentrarse en la materia del funcionamiento del honeynet, se debe tener claro que son y cuál es su funcionamiento.

Se puede decir como alguna definición de los honeynet, que es un recurso de seguridad basado en un sistema de ficheros, directorios y servicios lo más parecido posible a un sistema real, cuyo principio radica en ser probado, atacado o comprometido, por lo que se podría tratar como una herramienta de detección y respuesta ante potenciales ataques y detectar las firmas de estos, con ello queda claro de que si es una herramienta de detección.

Referente a que sea también tratado como una herramienta de respuesta, una vez recolectada la información sobre el comportamiento de un potencial atacante, se analiza el proceso a la hora de ejecutar un ataque, como por ejemplo si se ha empleado una herramienta de escaneo de puertos y servicios, herramientas de detención de vulnerabilidades o cualquier otra, además de las firmas de las herramientas que se empleen primero para realizar la penetración a las redes o sistemas y posteriormente el ataque, dando lugar por parte de los recursos encargados de la seguridad de la red o sistemas del despliegue de las respuestas y contramedidas ante este tipo de amenazas.

Los Honeynets son por lo tanto herramientas que recogen información y evidencias sobre las potenciales amenazas y vulnerabilidades de redes y sistemas para obtener el conocimiento necesario para ejecutar un procedimiento de respuesta global ante potenciales ataques.

No solo es importante conocer los patrones y firmas de un potencial atacante, sino que también es importante conocer su comportamiento y habilidades. Otro beneficio que da el emplear dichas herramientas es, poder detectar potenciales atacantes de sistemas de producción y redirigirlos a los Honeynets.[2]”

Elementos que interactúan en el ambiente para el honeynet

Para entender mejor los conceptos que interactúan en un ambiente de honeynet, a continuación, se explicarán cada uno de ellos según concepto propio del autor de este trabajo.

RED: La red, se refiere al conjunto de equipos y software interconectados entre sí por medio de dispositivos físicos y también inalámbricos.

[2] RAMOS VARÓN, Antonio ángel. BARBERO MUÑOZ, Carlos A. GONZÁLEZ CAÑAS, Juan M. PI COUTO RAMOS, Fernando. SERRANO APARICIO, Enrique. Seguridad perimetral, monitorización y ataques en redes. Bogotá: Ra-ma, 2015. 82p

DMZ: La DMZ se le conoce en el ámbito de redes como una red desmilitarizada, esto que significa, que es una zona que va a permitir un tráfico de una zona insegura a una zona segura. Es decir que se trata de una zona donde se puede ser atacados pero la red interna va a estar segura, esta zona por lo general se emplea para servicios web o servicios que deben ser requeridos que tengan acceso desde afuera (Internet), un ejemplo claro es un servicio web, este es accedido a su front desde afuera pero a su vez debe conectarse a un servidor de base de datos que está en la red interna, mediante el uso de reglas en el firewall esto es controlado.

Firewall: Básicamente el firewall puede ser un appliance(hardware) o un software o servicio configurado para el bloqueo no autorizado a la red y solo permitir conexiones autorizadas.

Una mirada introspectiva a la seguridad informática

Los informes constantes respecto a vulnerabilidades en los sistemas de información, la manera de aprovechar las fallas, tanto de carácter humano, en procedimientos o referentes a tecnología, sobre una infraestructura de sistemas, sin duda brinda un escenario perfecto para el cultivo de tendencias relacionadas con intrusos informáticos, dichos intrusos poseen diversos motivos, objetivos y estrategias, que sin duda desconciertan a profesionales en el ámbito de la seguridad informática ya que tales modalidades de ataques y penetraciones a sistemas varían de un caso a otro[3].

Sin embargo, haciendo uso de la criminalística enfocada a los sistemas se contará con un espacio de análisis de estudio que permite una reflexión profunda sobre los hechos y las evidencias. ¿Como se relaciona esto con el uso de Honeynet? Sin duda el problema radica en encaminar el buen uso y beneficios tecnológicos de los honeynet para lograr mejorar la ciber seguridad en las PYMES y convertirlo a su vez en una herramienta criminalística que permita la identificación de posibles vulnerabilidades, el objetivo sin duda es prevenir un ataque, sin embargo, si se presenta un ataque este permitirá recolectar información probatoria la cual ayudara a identificar los responsables o ayudara a prevenir un nuevo ataque[4].

Un problema adyacente a la seguridad informática es que la ideología de las PYMES, es creer que por su categoría como pequeñas y medianas empresas nunca van a tener problemas de seguridad informática, y que esto solo pasa a las grandes

[3]CANO MARTÍNEZ, Jeimy J. Computación
Forense Descubriendo los rastros informáticos. México: AlfaOmega, 2009. 27p

[4] CANO MARTÍNEZ, Jeimy J. Computación
Forense Descubriendo los rastros informáticos. México: AlfaOmega, 2009. 27p

empresas, ya que son las que más dinero poseen y que por esta razón los ciber delincuentes se interesan más en ellas y menos en las PYMES, sin embargo esto es erróneo, ya que en muchas ocasiones presentan más problemas de seguridad informática que las grandes empresas, y sin duda esto ha llamado la atención de los ciber delincuentes, pues ven allí grandes oportunidades para obtener recompensas, por ello el objetivo es brindar un apoyo mediante el uso del honeynet ayudar a identificar criterios y protocolos para controlar las posibles vías mediante las cuales puede verse afectada la seguridad e integridad de los datos en las PYMES ya sean internos o externos.

Por lo tanto la propuesta busca la recolección de la mayor cantidad datos informativos en cuanto a las ventajas y beneficios que las tecnologías de honeynet le traerán a las PYMES para ayudarlas en la lucha contra los actos perjudiciales de los ciber criminales e identificación de las vulnerabilidades que pueden permitir dichos ataques, la masificación de estas buenas prácticas y uso de herramientas de seguridad permitirán lograr el objetivo de entenderlas y emplearlas para salvaguardar la información. Como principal medida entonces es desarrollar un consolidado de los datos investigados y poder definir estrategias que permitan una conceptualización clara de lo que es un honeynet, sus características y la justificación del uso de su arquitectura en la red de las PYMES, así como sus beneficios, que a lo largo del trabajo se manejaran y pueden ayudar a mejorar la ciber seguridad.

Como variables aleatorias se determina el proceso de ataques informáticos, los cuales serán insumo para la interpretación de los administradores, de modo que permite identificar los modos de operación, los tipos de ataques y demás factores variables que conlleva un ataque, con esto se podrán determinar métodos que van a permitir ya sea mitigarlos o crear procesos para dar solución a las vulnerabilidades detectadas.

Se verá el tratamiento de algunas limitantes sobre las herramientas honeynet en cuanto a su implementación.

RESUMEN

La monografía consiste en ahondar de una manera clara y sucinta la realización de un análisis de efectividad de un honeynet en una red en producción e identificar sus ventajas y desventajas; para lograr tal fin se realizara el levantamiento documental de información respecto a la seguridad informática con el propósito de comprender el enfoque que se le da a la administración de las redes en las organizaciones, es preciso indicar que cada administración del ambiente de una red es diferente por lo tanto lo que se desea es realizar un compendio de estudio derivado del levantamiento documental de información de diversas implementaciones de honeynet y formar un vademécum único. Para implementaciones genéricas o bases sin importan el ambiente u esquema que se tenga de la red, si no que dicho estudio permita a los administradores de redes implementar de una manera segura y confiable un ambiente honeynet como se indicó, el cual sea escalable según se requiera.

Es posible hacer un análisis de red, teniendo en cuenta topologías, recursos entre otros y diseñara un esquema particular de honeynet acoplado a ese ambiente partiendo de la implementación base. Para ello es necesario la identificación de las herramientas que usan para vulnerar la seguridad informática.

Estudiar ambientes simulados de pruebas con el fin de medir la seguridad y revisión del comportamiento de los equipos conectados al ambiente con el honeynet. Finalmente, realizar un ataque al sistema, con ello se evaluarán las alertas dadas por el sistema honeynet convergiendo en dos puntos paralelos, el del lado del ataque y el lado administrativo del sistema.

Debido a los diversos ataques informáticos en las PYMES se hace inevitable e imperioso realizar el análisis de uso del honeynet y validar los pros y contras y brindar a las PYMES una herramienta; si es aplicable según el análisis posterior al apoyo de la seguridad informática. Al concluir, se presenta un esquema de infraestructura empleando un servidor de virtualización el cual albergara dos o tres máquinas virtuales según lo necesario de Honeypots para conformar la red de honeynet con ello realizar la recolección de información de los ataques realizados.

Se indicará la configuración tanto del servidor virtual que albergará las maquinas HoneyPot como la instalación y configuración de cada HoneyPot, todo ello con el debido soporte de imágenes que garanticen la instalación y la toma de información recolectada para posteriormente materializar las acciones que se toman de cara a estas vulnerabilidades con el propósito de aumentar la seguridad según los patrones o modos de operación de los ataques registrados.

Palabras clave: Seguridad Informática, Honeynet, Software Libre, Vulnerabilidades, Ciberseguridad, ciberataques.

ABSTRACT

The monograph consists of deepening in a clear and succinct way the analysis of the effectiveness of a honeynet in a production network and identify its advantages and disadvantages; In order to achieve such an end, a documentary survey of in-depth information regarding computer security will be carried out with the purpose of understanding the approach given to network administration in organizations. It is necessary to indicate that each administration of a network environment is different; therefore, what is desired is to carry out a study compendium derived from the documentary survey of information from various honeynet implementations and to form a unique vademécum. For generic implementations or bases regardless of the environment or scheme that you have of the network, if not that this study allows network administrators to implement a safe and reliable honeynet environment as indicated, which is scalable as required.

It is possible to make a network analysis, taking into account topologies, resources among others and will design a particular honeynet scheme coupled to that environment starting from the base implementation.

To do this, it is necessary to identify the tools used to violate computer security.

Study simulated test environments in order to measure security and review the behavior of equipment connected to the environment with the honeynet.

Finally, to carry out an attack to the system, with it the alerts given by the honeynet system will be evaluated converging in two parallel points, the one of the sides of the attack and the administrative side of the system.

Due to the various computer attacks in SMEs it is inevitable and imperative to perform the analysis of the use of a honeynet and validate the pros and cons of its use and provide SMEs with a tool, if applicable according to the analysis after the support of computer security. In conclusion, an infrastructure scheme is presented using a virtualization server which will host two or three virtual machines as needed Honeypots to form the honeynet network with it to collect information from the attacks performed.

The configuration of the virtual server that will host the HoneyPot machines as well as the installation and configuration of each HoneyPot will be indicated, all this with the due support of images that guarantee the installation and the collection of information to later materialize the actions that are taken in the face of these

vulnerabilities with the purpose of increasing security according to the patterns or modes of operation of the registered attacks.

Keywords: Computer Security, Honeynet, Free Software, Vulnerabilities, Cybersecurity, cyber-attacks.

1. DESCRIPCIÓN DEL PROBLEMA

1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo contribuye el uso de tecnologías de honeynet en el mejoramiento de la ciber seguridad en las PYMES y que tan efectiva puede ser?

1.2 PLANTEAMIENTO DEL PROBLEMA

El adelanto de las tecnologías de información y comunicaciones han tenido a lo largo de la historia, una contribución para que las organizaciones ya sean pequeña o gran empresa, se vean obligadas a crecer competitivamente mejorando sus productos y servicios, esto las obliga a mostrarse no solo localmente sino que también internacionalmente, esto implicara un gran manejo de información con la luego de sus análisis les permitirá tomar decisiones sobre el lineamiento que deberá seguir su negocio, esto también conlleva a unificaciones con el objetivo de mantenerse en el negocio o innovar en sus productos y servicios entre muchos otros aspectos, sin embargo; esto a su vez trae de fondo amenazas, y los ataques por los hackers o individuos con conocimientos en sistemas con el objetivo de lucrarse u obtener algún tipo de ganancia aumentan y más aún sobre las pequeñas y medianas empresas[5].

En este sentido, el objetivo de los hackers o similares se dirige a las PYMES, ¿por qué razón?, por el simple hecho de que la seguridad es muy básica o incluso limitada, ven pues una oportunidad de explotación de captura fácil de información confidencial, una gran empresa puede tener los recursos suficientes para mantener su sistema lo mejor posible en cuanto a seguridad. Una pequeña empresa apenas mantendrá una seguridad básica, es decir desde control de navegación aplicando configuraciones por defecto de proxys y reglas bases en sus dispositivos de firewall, y por ello es más vulnerable según opinión propia del autor de este trabajo.

De acuerdo con lo anterior, Sin duda alguna, el uso de esta herramienta (honeynet) ayudará a visualizar a futuro como se llevan a cabo estos ataques y brindara las estadísticas necesarias para poder implementar planes de seguridad con los cuales las PYMES estarán de alguna forma más seguras.

Ahora bien, el uso de un honeynet también ayudará a la detección de implementaciones incorrectas en servidores de datos, servidores web, FTP y cualquier servicio que se encuentre activo en la red, esto suele ocurrir debido a que se dejan valores de configuración por defecto, servicios que no son requeridos o

[5] Revista Científica Dominio de las Ciencias. Las Tics en las empresas. {En línea}. {5 de enero 2018} disponible en: (https://dialnet.unirioja.es/descarga/articulo/6313252.pdf)

utilizados ejecutándose, al igual que el uso de usuarios predefinidos o por defecto, esto sin duda da pie a vulnerabilidades las cuales podrán ser explotadas, pues individuos con conocimientos elevados en sistemas (Hackers) podrían usarlos para acceder al sistema. El apoyo recibido por parte del honeynet será fundamental para que sean detectados, permitiendo la toma de acciones preventivas o incluso correctivas según sea el caso. También se podrán detectar aquellos servidores que han cumplido su ciclo de vida de acuerdo a cada política local de la empresa como ejemplo cito la política local de la empresa en la cual labora la cual indica que como máximo un servidor puede tener no más de 5 años en operación, este podrá ser sustituido o validar si se puede ampliar el ciclo de vida, ya sea actualizando software y si es posible hardware, esto debido a que por fábrica se pierde el soporte care pack este tipo de soporte cubre fallos o novedades que presenten los servidores, en muchos casos luego de más de 5 años el care pack se vence y es muy costoso su renovación o por la misma evolución de la tecnología los servidores se vuelven obsoletos, estos servidores o equipos implican desactualizaciones en sus sistemas operativos y hardware dando pie a posibles fallas de seguridad las cuales facilitan los ataques.

Para dar importancia al problema planteado y la relevancia que tiene el proponer esta solución, se citan de manera estadística los datos de afectación de la falta de seguridad informática y que pueden poner en riego el negocio de cualquier PYME.

- “El costo a nivel mundial de delito cibernético podrá llegar a $2 billones en el 2019, y este valor se triplico respecto al año 2015 y el valor para entonces se encontraba en 500 mil millones. LABERIS, Bill. Informática forense Colombia, 20 estadísticas reveladoras de cibercrimen.

- El costo en cifras de cibercrimen solo es una pequeña fracción según The Global Risks Report 2016, puesto que una gran parte de los ciberdelitos no es detectada, como caso verosímil se tiene el espionaje industrial y asalto a proyectos patentados, y esto es debido a que el acceso ilícito a datos y documentos confidenciales son difíciles de detectar.

- En el 2018 se determinó un 38% más de incremento de incidentes de ciberseguridad.

- Un 48% de las violaciones referentes a seguridad respecto a datos son generados por actos perversos. Muchos de estos por error humano o por posibles fallas del sistema.

- Las PYMES, que cuenten con más de 1.0000 colaboradores, no son inmunes al delito cibernético, por el contario. Según el informe de Keeper Security, un 50% de organizaciones PYMES reportaron haber tenido al menos un ciberataque para los últimos 12 meses.

- Se estima que el costo medio de una transgresión de datos donde el delito sea el robo de activos fue de $ 879,582. Esto genera un gasto adicional para la restauración de estos y el costo sería de $ 955,429.

- Para combatir el delito cibernético se estima un gasto el cual superará los $ 80 mil millones, por lo que las organizaciones se centrarán más en la detección y respuestas ya que los enfoques preventivos no logran tener el éxito en el bloqueo de ataques maliciosos.

- Se ha realizado un gasto inconmensurable en seguros cibernéticos, principalmente en los EE. UU., De $ 1 mil millones hace dos años a $ 2.5 mil millones en 2016. Por lo tanto, los expertos estiman un crecimiento en los próximos cinco años.

- En 2016, el 62% de las compañías emplearon servicios de seguridad administrados para sus defensas contra el delito cibernético.

- Solo el 38% de las organizaciones encuestadas para el" Informe Global de Ciberseguridad Global de 2015" de ISACA pensaban que estaban preparadas para enfrentar los sofisticados ataques del cibercrimen.

- De los 1.000 líderes de TI encuestados para el" Informe de Defensa Cyberthreat 2016 de Invincea ", tres cuartos informaron que sus redes habían sido violadas en el último año, y el 62% dijeron que esperan sufrir un ciberataque exitoso en algún momento de este año.

- El phishing es una técnica de cibercrimen la cual consiste en engañar a un usuario sobre su cuenta en línea al hacerse pasar por una página legítima. De acuerdo con el DBIR de Verizon, el 30% de los correos electrónicos de suplantación de identidad (phishing) en realidad están abiertos, y el 12% de los afectados hacen clic en el enlace o archivo adjunto infectante.

• Una encuesta de Osterman Research de 540 organizaciones en América del Norte, el Reino Unido y Alemania reveló que casi la mitad había sufrido ataques ransomware en el último año”[6].

De lo anterior, se puede destacar con mayor fundamento la importancia del manejo de un sistema honeynet con el fin de desviar a un posible atacante de los servidores principales y demostrar su efectividad para tal fin.

Para apoyar el análisis de viabilidad y efectividad del uso de honeynet existen datos estadísticos de los cuales se puede apoyar, la compañía de antivirus Kaspersky Lab demostró estadísticamente la efectividad del uso de honeynet para identificar el volumen de ataques por los que un dispositivo de la red puede verse comprometido, se identificó que durante un periodo de 24 horas sobre un honeynet hubo decenas de miles de intentos de conexión por puerto telnet, esto demuestra la importancia del análisis de uso de un honeynet en las PYMES, el precursor de los honeynet Lance Spitner dejo durante un año un honeynet recolectando información, los resultados fueron los esperados gracias al honeynet y la información recabada logro determinar que los intentos de conexión se realizaban hasta 14 veces al día empleando herramientas de ataques automatizadas.

[6] LABERIS, Bill. Informática forense Colombia, 20 estadísticas reveladoras de cibercrimen. {En línea}. {12 de diciembre del 2017} Disponible en: (https://www.informaticaforense.com.co/20-estadisticas-reveladoras-de-cibercrimen/).

2. JUSTIFICACIÓN

Con el adelanto de las tecnologías y el creciente conocimiento en los sistemas y programación, sumado al uso inadecuado de los mismos por parte de personas inescrupulosas por la búsqueda de bienes ajenos y beneficio propio han venido de forma paralela los ataques enfocados a en las PYMES, estos se pueden soportar con datos estadísticos los cuales indican que el 71% de los ataques de ransomware tiene como objetivo las PYMES[7], entre muchos otros ataques; precisamente porque son blancos más fáciles y que están en crecimiento y por la razón de que los entornos de seguridad son bajos o incluso carecen de ellos. Razón por la cual se pretende realizar la presente nomografía, la cual va a permitir vislumbrar los pros y contras que permitiría la implementación de un honeynet en la organización, ayudara a las PYMES en mejorar sus sistemas de seguridad, con el fin de que puedan tener a salvo el bien más preciado, la información. Con ello se estará no solo apoyando al crecimiento de conocimiento en el ámbito de la ciberseguridad, sino que también se estará brindando la posibilidad de que cualquier empresa que está en crecimiento tenga la visión y misión de proteger de una mejor forma sus sistemas informáticos brindando el conocimiento necesario para que sus áreas de TI tengan las herramientas idóneas para poner en marcha un proyecto de honeynet con una baja inversión y solo haciendo uso de sus propios recursos.

El honeynet es una herramienta que puede ser catalogada como alternativa al problema mencionado y que se considera un recurso más de la red, el cual puede ser atacado. El honeynet se encargará de capturar toda la información relacionada a los diferentes tipos de ataques, con sistemas, aplicaciones y servicios reales.

Por lo tanto, se hace necesario la realización de este trabajo con el fin de identificar, evitar y de algún modo neutralizar los intentos de intrusiones sobre los sistemas y el ambiente de red corporativo. Siendo monografía, se pretende recopilar la mayor cantidad de información con el fin de realizar un compendio de toda esta y formar un compilado de las mejores prácticas e implementaciones de un honeynet con el fin de otorgar un conocimiento propio y punto de vista personal con el propósito de apoyar a las PYMES a implementar de la mejor forma sin correr riesgos esta herramienta tan valiosa y desconocida a su vez de lo que es y cómo funciona el honeynet, es muy importante lo anteriormente indicado, ya que el honeynet se vuelve un elemento más de la red y por ende si este es implementado de forma incorrecta se puede correr el riesgo de que un intruso lo emplee para tener acceso a la red en general.

[7] https://www.pandasecurity.com/es/mediacenter/empresas/ciberseguridad-pymes-ransomware/.

Existen en el mercado herramientas que permiten capturar volúmenes inconmensurables de información, lo que los hace difícil de interpretar y entender alargando el tiempo de análisis lo cual genera pérdida de tiempo para anteponerse nuevamente a posibles ataques, con honeynet aun cuando el volumen de datos que esta herramienta recoge puede verse poco pero con gran valor ya que es suficiente para permitir un análisis rápido ya que esta pequeña cantidad de datos permite la captura de toda la actividad sea un escaneo, pruebas o un ataque mismo, de esta manera la detección se hace más rápida y en corto tiempo.

Finalmente, el uso de un honeynet permitirá entonces conocer a un nivel más detallado los ataques y vulnerabilidades de los sistemas y la red. Viendo así el Honeynet desde una perspectiva teórico y práctico de una forma más fácil o digerible por decirlo, al momento de su uso, logrando una administración amigable en los procesos internos luego de la presentación o generación de un ataque, buscar estrategias de seguridad más eficientes y eficaces permitiendo la obtención granular de información de los ataques con el fin de poder ser estudiada para lograr la identificación de las vulnerabilidades y poder aplicar acciones para mitigarlas. De esta forma el trabajo permite mostrar de una manera lógica el funcionamiento del sistema en la red con el objetivo de que esta sea vista como una excelente alternativa y herramienta de seguridad.

3. OBJETIVOS DEL PROYECTO

3.1 OBJETIVO GENERAL

Establecer mediante la búsqueda conceptualizada e implementación de una metodología la cual permita analizar la efectividad del uso de honeynet para las PYMES.

3.2 OBJETIVOS ESPECÍFICOS

.

- Analizar la efectividad de los esquemas de ataques informáticos obtenidos por el honeynet y validar las repercusiones que estos tienen frente a la seguridad informática en las PYMES.

- Enunciar e implementar procedimientos de seguridad apoyados en los reportes obtenidos del honeynet.

- Elaborar instructivos de seguridad informática basado en los datos obtenidos por el honeynet y aplicarlos al SGC como soporte ante auditorias de sistema internas y externa.

- Enunciar e implementar una arquitectura viable para el Honeynet de baja interacción.

- Formular e Implementar herramientas con el fin de aumentar la seguridad interna y externa.

4. MARCO CONCEPTUAL Y TEÓRICO

4.1 Estado del Arte:

Los honeynet no se tratan de una nueva tecnología, este concepto hizo su aparición en la década de los 80s, en los años siguientes se vinieron desarrollando una seria de programas y scripts, que sirvieron como base de los HoneyPot para formar una red llamada honeynet, sin embargo no fue sino hasta 1999, que el investigador lance Spitzner en compañía de otros investigadores, implantaran una red casera la cual consto de tan solo 6 computadores los cuales los dejaron activos durante un año de esto se obtuvo una base de conocimiento concerniente a la forma de operar de los atacantes sobre un servidor y la red en general, de esta forma y a partir de allí es cuando se consolida el concepto de honeynet, por lo tanto el doctor Spitzner y sus colaboradores dan inicio al proyecto.

Los HoneyPot se les puede encontrar de diversos tipos, es decir no se encuentran sujetos a restricciones en cuanto a servicios o sistemas operativos, en teoría cualquier sistema operativo puede convertirse en HoneyPot, la clasificación realmente depende del enfoque a emplear, el nivel de interacción del atacante entre otros aspectos. Y cuando se habla de honeynet es la unificación de varios Honeypots esto se le conoce también como una red de honeys o honeynet como se indicó anteriormente.

4.2 Delimitación del proyecto

Teniendo en cuenta la amplia temática contextualizada sobre el tema de honeynet, y teniendo presente la proyección de las tecnologías basada en los recursos y tecnología existente, la gestión documental se centrara en conceptualizar la mejor practica para realizar la monitorización de los ataques en línea en las PYMES y poder definir las políticas o estrategias metodológicas para hacer imperceptibles el honeynet con el fin de lograr una recolección de información más significativa e importante.

4.3 Marco Conceptual:

4.3.1 Concepto de Honeynet

Se nombra honeynet al software y conjunto de computadores los cuales actúan como señuelo para los atacantes, simulan ser sistemas vulnerables a ataques, sin embargo, es una herramienta de sistemas de seguridad informática dispuesta para capturar información sobre los atacantes y los métodos que estos emplean, un honeynet puede actuar como disuasivo para que un atacante pierda el interés sobre

servicios o sistemas más importantes en la red, como servidores, firewall entre otros, y advierte al administrador del sistema de un ataque.

Algunos honeynet son programas que simulan sistemas operativos que realmente no existen físicamente, se les suele conocer como Honeypots de baja interacción, son usados principalmente como medida de seguridad[8].

Otros se emplean en sistemas operativos nativos, estos son capaces de reunir información mucho más relevante, estos se les conoce como honeynet de alta interacción.

La tecnología que nos va a permitir conocer detalladamente los ataques e identificación de vulnerabilidades en la red y en los sistemas de información son los honeynet. “Un honeynet en el ámbito de la seguridad informática se puede definir como un recurso más de la red el cual se encuentra de forma voluntaria a vulnerabilidades para que un intruso pueda examinarla y atacarla directamente como se mencionó anteriormente”[9].

Sin embargo, es preciso aclarar que está directamente no es una solución a un problema de seguridad; ya que la función principal es recolectar la mayor cantidad de información importante sobre el ataque y mediante esta permitir a futuro prevenirlas dentro del ámbito de la red.

El presente trabajo consiste en mostrar de una manera concisa la forma correcta de implementar un honeynet, con el objetivo de recopilar información referente a las actividades de intrusión que se estén llevando a cabo sobre la red y los sistemas de información existentes.

Consiguiendo con ello, detectar las vulnerabilidades que poseen dichos elementos (Red y sistemas de información) mucho antes de que estas sean vulneradas o explotadas.

“La herramienta sutilmente da una ventaja al proveer de la inteligencia necesaria para conocer los riesgos que cuenta la red y demás sistemas de información.

---

[8] Honeypot. {En línea}. {19 de julio 2019}. Disponible en: (https://es.wikipedia.org/wiki/Honeypot)

[9] ESTRELLA QUIJIJE, Gustavo Daniel. Diseño del prototipo de una HoneyPot virtual que permitirá mejorar el esquema de seguridad en las redes de la carrera de ingeniería en sistemas computacionales y networking. 2011 p370. Tesis de grado (Ingeniería en sistemas computacionales). Universidad de Guayaquil. Facultad de ciencias matemáticas y físicas.

La premisa fundamental con la que cuenta el honeynet, es permitir al administrador de sistemas o ente encargado de la seguridad estar un paso adelante del intruso o enemigo, permitiendo adquirir los conocimientos suficientes referente a cada posible amenaza y a su vez cual sería el modus operandi de los atacantes, con el objetivo de dar los suficientes instrumentos para la implementación de una arquitectura de seguridad a su vez proactiva que no solo permita la defensa si no también prevenirlas antes de que se ejecuten"[10].

Hoy día las nuevas tecnologías también nos permiten identificar a detalle un ataque o vulnerabilidades de las redes, estas tecnologías se les conoce como Honeypots. Un Honeypot, en el campo de la seguridad en redes de información, se define como un recurso de la red que se encuentra voluntariamente vulnerable para que el atacante pueda examinarla, atacarla[11]. De forma directa.

4.3.2 Uso del Honeynet

El uso de la herramienta honeynet combinado con otras tales como Openvas, Nessus, Nmap, CrowdStrike entre otras permitirán recoger información de las intrusiones que se hayan presentado y estudiarlas para poder conocer la amenaza en incluso su origen, esto permitirá generar unos datos estadísticos que generaran patrones de conducta de ataques y los diferentes detalles que motivan a los intrusos.

Los Honeynets también permitirán comprobar y desarrollar la capacidad de respuesta ante cualquier incidente. En los ambientes corporativos u organizacionales pueden ser usadas para estudiar tipos y patrones de ataque o simplemente para investigar amenazas como objetivo principal[12].

4.4 ARQUITECTURAS DEL HONEYNET

[10] HEREDIA TERÁN, Carlos Mauricio. Diseño e implementación de una honeynet para la red de datos de la Universidad Nacional de Loja, utilizando software Libre. Ecuador. 2015, 108p. Tesis de grado. Universidad Nacional de Loja, Ecuador, Loja.

[11] PAZMIÑO Mayra, AVILÉS Jorge, ABAD ROBALINO Cristina Lucia. Diseño preliminar de una honeynet para estudiar patrones de ataques en las redes de datos de la ESPOL. 2009, 4p. Ensayo (Grupo de visualización científica y sistemas distribuidos). Facultar de ingeniería en electricidad y computación. Escuela superior politécnica del litoral. Campus Gustavo Galindo.

[12] HEREDIA TERÁN, Carlos Mauricio. Diseño e implementación de una honeynet para la red de datos de la Universidad Nacional de Loja, utilizando software Libre. Ecuador. 2015, 108p. Tesis de grado. Universidad Nacional de Loja, Ecuador, Loja.

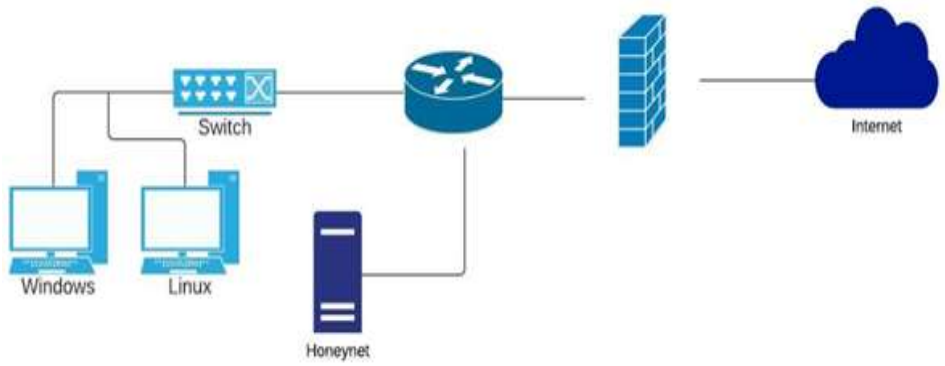
Un aspecto importante para tener en cuenta en las diversas implementaciones de una red de honeynets además de cuál va a ser su funcionamiento, es determinar cuál será el lugar donde se ubicará en una red. Para ello se cuentan con diferentes arquitecturas que se pueden diseñar dependiendo de los requerimientos y objetivos a conseguir, desde la más simple que es un honeypot de baja interacción simulando servicios básicos para conformar la red de honeynet en máquinas virtuales las cuales se estarán ejecutando en una sola maquina física. Hasta complejas honeynet donde se desplieguen conjuntos de Honeypots contactados entre sí y que son monitorizados y administrados proactivamente[13].

“Honeynet Proyect propone dos modelos a seguir, lo cual ha definido dos tipos de arquitecturas básicas para los honeynets denominados GEN1, GENII y GENIII, donde GEN se refiere a Generación

4.4.1 GEN I

Se refiere a la primera generación en desarrollarse. Una red es situada detrás de un dispositivo de control de acceso, generalmente un cortafuego, como se puede observar en la siguiente figura 1.

Figura 1. Honeynet GenI



Fuente Seguridad perimetral, monitorización y ataques en redes

Estas tecnologías de Gen I implementan el control de datos y captura de datos, son medidas básicas pero efectivas.

En el anterior diagrama, se puede ver un cortafuego de capa 3 separando la Honeynet en tres redes diferentes. Específicamente, la Honeynet, internet y la red

[13] RAMOS VARÓN, Antonio ángel. BARBERO MUÑOZ, Carlos A. GONZÁLEZ CAÑAS, Juan M. PI COUTO RAMOS, Fernando. SERRANO APARICIO, Enrique. Seguridad perimetral, monitorización y ataques en redes. Bogotá: Ra-ma, 2015. 89p

administrativa. Cualquier paquete entrando o saliendo de la Honeynet tiene que pasar a través del firewall y del Router. El firewall es la principal herramienta para controlar las conexiones entrantes y salientes. El Router se emplea como suplemente al filtrado. El Firewall está configurado para permitir cualquier conexión entrante, pero controla las conexiones salientes.

El firewall mantiene un seguimiento de cuantas conexiones se realizan desde un Honeypot saliendo a internet. Luego de que el Honeypot ha alcanzado un determinado límite de conexiones salientes, el firewall bloqueara cualquier nuevo intento. Esto proporciona al blackhat la flexibilidad para ejecutar aquello que necesite, mientras que ofrece la protección automática contra el abuso.

El Router actúa como control de acceso en la capa dos, esto indica que ningún Honeynet debe depender de una sola fuente para el control de datos. Esto es principalmente para la protección contra spoofing, DoS o ataques basados en ICMP, ya que el Router solo permitirá los paquetes que tengan la dirección ip de Origel del Honeynet.

Este tipo de arquitectura es eficaz contra ataques automatizados, o contra atacantes de niveles básicos. Pero no son de gran utilidad contra ataques más avanzados. Desafortunadamente este tipo de esquemas de Generación I son poco atractivos consistiendo básicamente en instalaciones por defecto de sistemas operativos”[14].

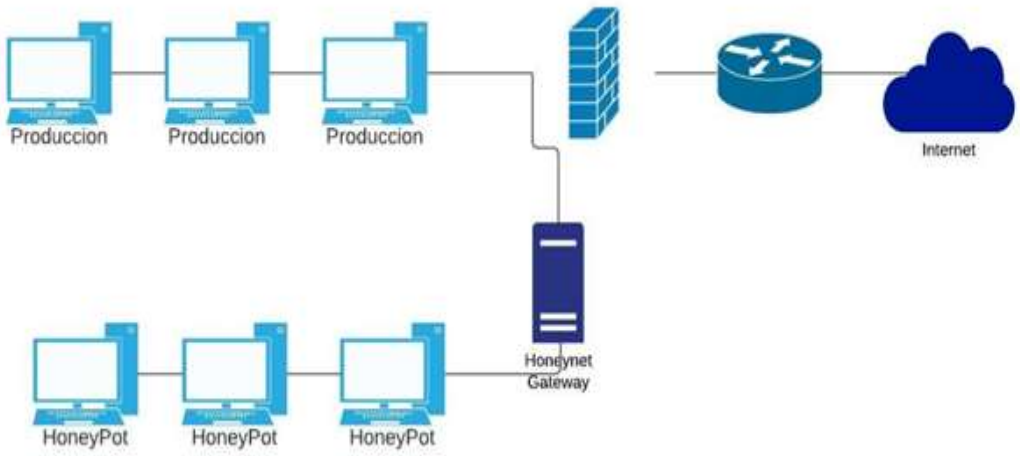
4.4.2 GEN II

“Empleando viajes y nuevas técnicas, la Honeynet GenII mejora la flexibilidad, gestión y seguridad de los despliegues de las Honeynets. Esta arquitectura fue pensada para solventar muchos de los problemas existentes en la generación anterior. Esta arquitectura es mucho más fácil de implementar, se hace más difícil su detección y su mantenimiento es mucho más seguro.

Como se podrá observar en la siguiente Fig 2, la primera diferencia con respecto a la arquitectura vista en la GenI es que se emplea un Honeynet Gateway, esto quiere decir que actúa como un proxy de alguna manera, manejando una puerta de enlace de red trampa, combinando los elementos de IDS y firewall los cuales aparecía por separados en la anterior generación”[15].

[14] Temas para la Educación, Revista digital para profesionales de la enseñanza, 2009, Federación de Enseñanza de CC.OO. de Andalucía ISSSN: 1989-4023
[15] Temas para la Educación, Revista digital para profesionales de la enseñanza, 2009, Federación de Enseñanza de CC.OO. de Andalucía ISSSN: 1989-4023

Figura 2. Honeynet GenII



Temas para la Educación, Revista digital para profesionales de la enseñanza, 2009, Federación de Enseñanza de CC.OO. de Andalucía ISSSN: 1989-4023

4.4.3 Nivel de Interacción del honeynet

Para esta clasificación se centraliza en la manera de interacción directamente del HoneyPot con el atacante, por lo tanto, esta clasificación se divide en:

4.4.4 "Baja Interacción: Estos cuentan con la característica de emular servicios o sistemas operativos, pero solo permiten una interacción limitada por parte del atacante y son útiles para obtener información cuantitativa acerca de los ataques.

Al manejar una interacción limitada y trabajar en un ambiente controlado se reduce el riesgo, pero sin embargo se vuelve útil solamente ante ataques específicos y automáticos, pues para un atacante se hace fácil identificar que se trata de una emulación"[16].

4.4.5 Alta Interacción: Los HoneyPot de alta interacción ya son como tales sistemas físicos con servicios reales en operación, pero que son vulnerables y que están expuestos en una red para capturar información sobre los ataques que les realizan.

4.4.6 Tipo de implementación: Se puede manejar dos variaciones al momento del uso del honeynet:

[16] AMAYA GUTIÉRREZ, Camilo. Honeypots: alternativas para analizar códigos maliciosos. {En línea}. {21 enero 2013}.. Disponible en: (https://www.welivesecurity.com/la-es/2013/01/21/honeypots-alternativas-analizar-codigos-maliciosos/)

Físico: Esto se refiere a un servidor de carácter nativo como puede tratarse de un servidor o un pc de escritorio.

Virtualizado: Para este caso se trata de un servidor virtualizado es decir carente de arquitectura física propia. Para ello se emplea software de virtualización o un appliance sobre el que se ejecuta.

4.4.7 Entorno virtualizado vs Entorno físico

Realmente escoger entre un entorno virtualizado o un entorno fisco depende de las necesidades o alcances a los que se quieran llegar, usar entornos virtualizados ayuda a la optimización de la infraestructura con la que se cuente, es decir se puede ahorrar en la misma y a su vez aprovechar al máximo la infraestructura actual.

Según lo requerido en cuanto a software, hardware y presupuesto la virtualización puede ser una excelente solución, es importante indicar que para tener servicios virtualizados es importante también ver en donde se van a configurar, es cierto como se mencionó que esto ayuda a minimizar costos en infraestructura pero se debe tener presente que el equipo o servidor a usar debe contar con un excelente performance ya sea para albergar una o las máquinas virtuales que se requieran, entre más máquinas virtuales a emplear mejor debe ser el performance del servidor o pc a usar, para garantizar un óptimo funcionamiento tanto del ambiente nativo como del mismo ambiente virtualizado y no tener problemas más adelante, una propiedad más de los ambientes virtualizados es la facilidad de escalabilidad, respaldos y migraciones, ya que por ser este tipo de ambientes se facilitan dichas acciones.

Si se cuenta con recursos suficientes se pueden adquirir equipos físicos para las implementaciones requeridas. Para la propuesta indicada se pueden trabajar desde los dos ambientes según la posibilidad y alcance de la PYME.

4.5 Casos de estudio de honeynet

4.5.1 Honeypots para la detección de ataques informáticos realizados a instituciones financieras: Caso de Estudio Normativa Nacional – ASFI

Este es un artículo desarrollado por Rolando Gonzales, Ever Leaños, Fernando Salvatierra y Ricardo León de la facultad de ciencias y tecnología de UTEPSA. En este articulo los ingenieros plantearon la herramienta "honeypot" para detectar vulnerabilidades mediante la simulación de una red financiera con ayuda del software GNS3 y VirtualBox, con los cuales se virtualizarán los posibles ataques a la red.

"Para la elaboración del análisis de riesgo exigido por la ASFI, se realizó un previo análisis de la Sección 7 del reglamento para la gestión de seguridad de la información con la finalidad de determinar los parámetros a seguir al momento de realizar un diseño de red que cumpla con el reglamento de seguridad de la información, siendo las instituciones financieras un lugar donde la protección de la información es vital. Posteriormente se realizó un estudio acerca de los diferentes tipos de ataques que afectan a las instituciones de alto riesgo, como lo son las entidades financieras. Además, se profundizo algunos factores que hacen posible dichos ataques. Con esta investigación queda clara la importancia de mantener segura la información. Luego se continuó con el desarrollo de un esquema de infraestructura de red mediante el uso de los parámetros que se vieron en la sección 7 del reglamento para la gestión de seguridad de la información que impone la ASFI. En el diseño se cumplieron los diferentes artículos a tomar en cuenta cuando se realiza el desarrollo de un análisis para la seguridad de la información El tipo de asumido fue la Investigación aplicada, ya que, al virtualizar una infraestructura de red se pudo evidenciar los diferentes intentos de ataques para así tomar datos de estos para el análisis de los métodos usados por los atacantes en la actualidad. Esta acción se llevó a cabo a través de la implementación de Honeypots[17]".

4.5.2 Segundo caso práctico, citado textualmente para su comprensión

"Análisis de un caso real Desde un punto de vista práctico, una vez que se ha detectado o se sospecha que la integridad del sistema ha podido ser vulnerada por algún tipo de intrusión, es conveniente hacer una copia de la información que hay en el sistema. Dependiendo de la situación, puede ser conveniente incluso hacer

[17] Gonzales Rolando, Leaños Ever, Rodriguez Fernando, León Ricardo
Honeypots para la detección de ataques informáticos realizados a instituciones financieras caso práctico: Normativa Nacional – ASFI, Revista Utepsa Investiga

una copia de los procesos que se están ejecutando en ese momento en el equipo, del espacio de intercambio (swap), de las conexiones activas, etc.

Para realizar una copia de las particiones del sistema de ficheros, en los equipos Unix, se puede usar el comando dd. Las copias obtenidas pueden volcarse en una partición libre del propio equipo o a un fichero (cosa poco recomendable, ya que el contenido del sistema atacado debería modificarse lo menos posible), sin embargo, es preferible enviar los contenidos a otro equipo empleando, por ejemplo, el programa Netcat (nc).

El siguiente ejemplo muestra cómo se podría realizar esta copia, transfiriendo el contenido de la partición sda4 del equipo víctima al equipo de control.

En el equipo víctima se ejecutaría:

dd if=/dev/hda2 - | nc equipo_remoto -p 100

y en el equipo remoto se recibiría el fichero:

nc -l -p 10 > disco-hda2

También se pueden enganchar los discos a un equipo y realizar la copia a bajo nivel, empleando discos duros de iguales características (mismo modelo) y haciendo la copia mediante dd.

En sistemas operativos como Windows NT, que no disponen de un procedimiento de Backups a bajo nivel, se puede utilizar el procedimiento empleado para sistemas Unix: arrancar el equipo desde un disco de rescate o instalación de Linux/Unix (menos recomendable por aquello de modificar datos del sistema) y proceder a realizar la copia de los dispositivos a bajo nivel.

En cualquier caso, es conveniente realizar estas copias a bajo nivel para poder restaurar los datos en caso de que ocurra algún problema al analizar los ficheros, además esto permitirá el análisis de los archivos buscando las fechas de modificación de estos.

Todo este proceso (es decir, los pasos dados para la copia de los datos del sistema) debería quedar registrado y documentado en algún sitio de forma automática. En estos casos, comandos como script pueden resultar muy útiles.

Una vez que se ha realizado la copia y la migración de los datos al equipo remoto donde se va a efectuar al análisis, se debe proceder a la recopilación de datos relacionados con el tipo de sistema y su entorno: versión del sistema operativo,

particiones utilizadas, fecha en la que se detectó el ataque, fecha en la que se desconectó de la red el equipo y cualquier otra modificación que pudiese tener relevancia para el análisis.

Posteriormente, se procederá a montar las imágenes de las particiones para comenzar el análisis de las mismas en el equipo remoto. Para esto se puede usar el mecanismo de loop-back disponible en Linux, que permite el montaje de los ficheros imagen de la partición en el equipo Unix, pudiendo así acceder a archivos de estos sistemas de ficheros:

Mount -o loop, ro, ncexec /home/forensic/disco-hda2 /analisis

Mount -o loop, ro, ncexec /home/forensic/disco-hda3 /analisis/var

Una vez montadas las particiones, se utilizará fundamentalmente el paquete TCT para realizar el análisis. El primer paso será la obtención de los tiempos de Modificación/Acceso/Cambio (tiempos MAC) de todos los ficheros del sistema. Es fundamental capturar estos tiempos antes de emprender cualquier acción sobre los ficheros del equipo atacado que pueda modificar su valor. La secuencia de accesos a los ficheros permitirá crear una línea temporal que muestre los acontecimientos ocurridos en el sistema.

Mediante las herramientas ils e ils2mac1 se podrán obtener los tiempos MAC de los nodos-i borrados de las particiones. El fichero resultante será combinado, a su vez, con el fichero obtenido tras la ejecución de grave- robber2 sobre el sistema de ficheros anterior, para, de esta forma, tener los tiempos MAC tanto de los nodos-i borrados como de los nodos-i activos. La secuencia de comandos usada para hacer esto podría ser la que se detalla a continuación:

**# /root/tct-1.07/bin/grave-robber -o LINUX2 **

-c home/analisis/disco -m -d ./resultados

**# /root/tct-1.07/bin/ils /home/analisis/raiz-hda4 **

| /root/tct-1.07/extras/ils2mac > raiz-hda4.ilsbody

**# /root/tct-1.07/bin/ils /home/analisis/var-hda3 **

 # cat raiz-hda4.ilsbody var-hda3.ilsbody > body-deleted

 # cat body body-deleted > body-full

**# /root/tct-1.07/bin/mactime -p home/analisis/disco/etc/passwd **

**-g home/analisis/disco /etc/group -b body-full 08/04/2001 **

Mactime.txt

Al final de este proceso se obtiene un listado completo (contenido en el fichero ‘fichero.txt’) de los tiempos MAC de todos los ficheros del sistema (incluidos los borrados) que hayan modificado alguno de sus tiempos MAC desde ’fecha’.

La siguiente acción a realizar, una vez obtenidos los tiempos MAC, es comprobar todos los programas y ficheros de configuración instalados en el equipo.

En muchas intrusiones, lo primero que hace el atacante es modificar los programas y herramientas del sistema para ocultar su acceso; además, suelen modificar los ficheros de configuración para crear nuevos usuarios, permitir accesos desde determinadas máquinas, etc., de forma que puedan acceder al equipo más cómodamente con posterioridad.

Por todo lo comentado anteriormente, es conveniente que no se empleen los programas instalados en el propio equipo, sino versiones que se tengan compiladas estáticamente siempre que se tenga que realizar el análisis sobre el mismo equipo atacado y no se pueda usar otro sistema para realizarlo. El motivo de utilizar ficheros compilados estáticamente se debe a que no emplean llamadas a librerías del sistema susceptibles de ser modificadas por los atacantes. Por esa misma razón no es conveniente que se emplee el sistema operativo de la máquina atacada, ya que puede ser modificado mediante módulos para ocultar los procesos y ficheros del atacante. Sin embargo, aunque se usen programas compilados estáticamente, esto no evita que la información mostrada pueda ser errónea, ya que existen rootkits que pueden modificar, mediante módulos, el propio núcleo del sistema operativo. Un ejemplo sería Adore.

Si no se dispone de una base de datos de integridad en un dispositivo externo para poder comprobar la integridad de los ficheros (ayudándose de herramientas como, por ejemplo, Tripwire), se pueden usar técnicas como comparar los ficheros binarios existentes en el sistema con los de la instalación original (cuando no estén empaquetados) o con los que hay en otro equipo con la misma versión y parches del sistema operativo, empleando comandos como cmp.

La mayoría de los sistemas operativos disponen de un sistema de verificación de paquetes instalados.

La base de datos se mantiene en el propio equipo (por lo que el atacante puede modificarla) pero de todas maneras puede emplearse muchas veces para comprobar qué ficheros se han modificado.

Aunque es habitual que algunos ficheros cambien de permisos o de contenido, por ejemplo, al añadir usuarios al fichero de password, después de realizar algunas instalaciones que producen cambios en los formatos, etc.; no suele ser habitual que

comandos como /bin/ls sean modificados, lo que puede indicar que se trata de una versión troyanizada.

Para comprobar la consistencia de los paquetes instalados en el sistema atacado, buscando especialmente errores de chequeo de md5, se puede usar la utilidad rpm (o su equivalente si existe en el sistema operativo atacado) con las opciones adecuadas como, por ejemplo:

Rpm -V -a -root=home/analisis/disco/ > consistencia_rpm
Cat consistencia_rpm | grep ^..5
s.5….T c /etc/services
s.5….T c /etc/localtime
s.5….T c /etc/Info-dir
..5….T c /etc/mime.types
s.5….T c /etc/httpd/conf/httpd.conf
s.5….T /usr/lib/umb-scheme/slibcat
s.5….T c /etc/inetd.conf
s.5….T c /etc/rc.d/rc.sysinit
s.5….T c /etc/sysconfig/pcmcia
s.5….T /bin/netstat
s.5….T /sbin/ifconfig
SM5..T /bin/ps
SM5..T /usr/bin/top
s.5….T c /etc/pam.d/rlogin
s.5….T /var/log/senmail.st
s.5….T c /etc/syslog.conf
s.5….T c /usr/sbin/tcpd
s.5….T c /etc/pam.d/login
SM5..T c /etc/ftpaccess
s.5….T c /etc/ftpusers

La aparición de modificaciones en ficheros como: netstat, ifconfig, ps, top, ls, top, tcpd..., se sugeriría la posibilidad de que se haya instalado un rootkit en el sistema.

Un método para saber si los ficheros modificados son versiones troyanizada de los originales es examinar los ficheros sospechosos buscando cadenas que delaten esta posibilidad. Normalmente, la información que se obtiene de este estudio suele ser rutas de directorios y ficheros que no deberían aparecer en el sistema, por ejemplo:

 # strings -a home/análisis/disco/bin/ps > strings_ps

 # cat strings_ps

…

/dev/xdta

NR PID STACK ESP EIP TMOUT ALARM STAT TTY TIME COMMAND

PID TTY MAJFLT MINFLT TRS DRS SIZE SWAP RSS SHRD LIB DT COMMAND

PID TTY STAT TIME PAGEIN TSIZ DSIZ RSS LIM %MEM COMMADN

El fichero ‘‘‘/dev/xdta” resulta ser un fichero de configuración que contiene un listado con todos los procesos que no mostraría el comando ps (aunque se estuvieran ejecutando), para no delatar la presencia de intrusos en el equipo.

Sin embargo, el método anterior no siempre da buenos resultados ya que en los ataques más recientes se están empezando a utilizar ficheros que se ejecutan comprimidos por lo que no es posible visualizar las cadenas de texto que contienen otras técnicas de ofuscación que impiden obtener información útil empleando el método anterior.

Una vez analizadas las cadenas de los programas supuestamente modificados, se debe intentar recuperar el contenido de los ficheros borrados (el número de nodo-i que tenía asociado cada archivo antes de ser borrado se puede obtener del fichero de tiempos MAC generado anteriormente).

Para recuperar el contenido de estos ficheros se puede usar el comando icat, incluido en el TCT. Este programa devuelve toda la información que encuentra sobre el nodo-i que se le pasa como parámetro realizando la búsqueda en la imagen de la partición indicada.

Anteriormente se han obtenido, mediante el comando ils, los nodos-i actualmente vacíos que hubiesen contenido información en el periodo en el que se produjo el

incidente. Para obtener una copia de estos ficheros se puede emplear el comando icat, en lugar de realizar una búsqueda mediante un editor.

root/tct-1.07/bin/icat var-hda3 12216 > fich-12216

root/tct-1.07/bin/icat raiz-hda4 92962 > fich-92962

root/tct-1.07/bin/icat raiz-hda4 92961 > fich-92961

root/tct-1.07/bin/icat var-hda3 26422 > fich-26422

root/tct-1.07/bin/icat var-hda3 40645 > fich-40645

root/tct-1.07/bin/icat raiz-hda4 2404 > fich-2404

root/tct-1.07/bin/icat raiz-hda4 90629 > fich-90626

root/tct-1.07/bin/icat raiz-hda4 92570 > fich-92570

root/tct-1.07/bin/icat raiz-hda4 92571 > fich-92571

root/tct-1.07/bin/icat var-hda3 26421 > fich-26421

root/tct-1.07/bin/icat raiz-hda4 166537 > fich-166537

root/tct-1.07/bin/icat var-hda3 38613 > fich-38613

root/tct-1.07/bin/icat var-hda3 38614 > fich-38614

root/tct-1.07/bin/icat var-hda3 38615 > fich-38615
root/tct-1.07/bin/icat var-hda3 38617 > fich-38617

Luego de realizar el proceso anteriormente indicado, la siguiente tarea será averiguar el tipo de cada fichero para abrirlo con el programa adecuado (el comando file, o sus análogos en cada sistema operativo, pueden facilitar esta tarea).

Posteriormente, se deberá analizar el contenido de cada uno de estos ficheros. Así, por ejemplo, los ficheros de texto pueden contener trozos de logs borrados deliberadamente por el intruso, los ficheros ejecutables pueden corresponder a programas utilizados por el atacante, los ficheros comprimidos pueden ser paquetes instalados.

File fich*> tipos

$cat tipos

fich-12216: International language text

fich-92962: ASCII text

fich-92961: ASCII text

fich-26422: empty

fich-40645: data

fich-2404: gzip compressed data, deflated, last modified:

Wed Jul 11 19:25:03 2001, os: Unix

fich-90626: English text

fich-92570: ASCII text

fich-92571: ASCII text

fich-26421: empty

fich-166537: English text

fich-38613: ASCII text

fich-38614: empty

fich-38615: ASCII text

fich-38617: ASCII text

En este punto, si fuese necesario, se procedería al desensamblado de los ficheros ejecutables para determinar cómo mayor exactitud su funcionalidad. Recolectada y analizada esta información básica (que puede dar una idea muy aproximada de lo que ha pasado en el sistema), se procederá al estudio del fichero de tiempos MAC que se generó anteriormente. Este análisis tratará de establecer una línea temporal que muestre la secuencia de acontecimientos ocurrida en el sistema.

A continuación, se observa un extracto de los datos que genera el programa mactime, y una pequeña reseña de la información que se puede obtener de estos (la salida ha sido ligeramente modificada para ajustarla a la página). Como ejemplo se muestra la información que aparece cuando se modifica el fichero ps. A continuación, se puede observar la creación del fichero de configuración (dev/xmx) que se había detectado anteriormente.

**Aug 06 01 09:57:55 **

627271 ..c -rw-r—r--root root <raíz-hda4-dead-2404>

Aug 06 01 09:58:00

4096 m.c drwxr-xr-x root root /home/analisis/disco/bin

1195 .a. -rwxr-xr-x root root /home/analisis/disco/bin/chown

35300 ..c -rwxr-xr-x root root /home/analisis/disco/bin/netstat

33280 ..c -rwxr-xr-x root root /home/analisis/disco/bin/ps

36864 m.c. drwxr-xr-x root root /home/analisis/disco/dev

241 m.c -rw-r--r-- root root /home/analisis/disco/dev/xdta

145 m.c -rw-r--r-- root root /home/analisis/disco/dev/xmx

19840 ..c -rwxr-xr-x root root /home/analisis/disco/sbin/ifconfig

21816 .ac -rwxr-xr-x root root /home/analisis/disco/usr/bin/crontab

21816 mac -rwsr-xr-x root root /home/analisis/disco/usr/bin/ct

53588 ..c -rwxr-xr-x root root /home/analisis/disco/usr/bin/top

4096 m.c drwxr-xr-x root root /home/analisis/disco/usr/sbin

27055 .ac -rwxr-xr-x root root /home/analisis/disco/usr/sbin/in.rexedcs

267360 ..c -rwxr-xr-x root root /home/analisis/disco/usr/sbin/syslogd

14224 ..c -rwxr-xr-x root root /home/analisis/disco/usr/sbin/tcpd

En primer lugar, se puede observar que por la proximidad de las fechas en las que se modifican los ficheros es muy posible que se trate de la ejecución de un script, ya que se crean varios ficheros en el mismo instante de tiempo en el análisis completo de este ataque se puede verificar esta hipótesis, recuperando el script empleado entre los ficheros borrados por el atacante.

En la primera entrada de tiempos se accede a varios ficheros del sistema para obtener información del equipo. El fichero “raiz-hda4-dead-2404” es el fichero comprimido de la instalación que es borrado posteriormente por el atacante. Por último, se puede observar la creación y modificación de diversos ficheros en los directorios del sistema, que reemplazan a los binarios originales del equipo. Mediante la recuperación del script lanzado por el atacante, se puede comprobar que algunos de estos ficheros eran las versiones reales de los demonios del sistema, como “/usr/bin/ct”, versión original del programa crontab.

Los ficheros instalados por el atacante en el directorio “/dev” contenían la configuración de los binarios del rootkit, indicando qué procesos y conexiones se debían ocultar a los administradores. En la última fase del análisis en realidad, no tiene por qué ser la última, puede ser incluso la primera o ir intercalándose, procediéndose a examinar el flujo de tráfico capturado por un IDS. El objetivo es establecer y corroborar todos los datos hallados en el sistema.

En general, los pasos a seguir suelen dividirse en:

1. Análisis de los flujos de datos para agruparlos según las distintas conexiones capturadas. En estos casos conviene la utilización de algún tipo de script que facilite y automatice esta labor, puesto que la cantidad de información con la que se puede llegar a trabajar (del orden de varios gigabytes) hace inviable un tratamiento manual.

2. Almacenamiento de la información de cada conexión en un fichero donde sea fácilmente identificable: origen y destino de la conexión, fecha y hora de comienzo y finalización, puerto utilizado y tamaño de la misma.

3. Establecer, en su caso, si existe algún tipo de desfase horario entre el sistema de control (IDS, Firewall) y el equipo analizado. Esto es fundamental para poder comparar los datos de las conexiones almacenadas con la información que ha quedado registrada en el equipo atacado.

4. Estudio de las conexiones y búsqueda de datos que faciliten la identificación del atacante. El orden seguido al examinar las conexiones puede disminuir el tiempo que es necesario emplear, por eso conviene empezar por las que parezcan más prometedoras. Una vez analizada y clasificada toda la información almacenada en el IDS se pudo determinar que el ataque se produjo aprovechando una vulnerabilidad del proceso rpc.statd. Posteriormente, el atacante realizó una conexión ftp desde el propio equipo para bajarse los programas necesarios para completar la intrusión. Un análisis más en profundidad de las conexiones permitió obtener un listado de las actividades desarrolladas por el atacante: desde la conexión a un servidor para descargarse el archivo con los ficheros troyanizados, hasta la instalación de estos[18]”.

[18] SEGURIDAD INFORMATICA HONEYPOTS

4.6 Tipos de Honeypots

Como se ha podido observar durante el desarrollo del trabajo, se han enmarcado los conceptos propios de los Honeypots para la conformación de una red de Honeynets, ahora, es importante mencionar algunos Honeypots que se emplean actualmente.

4.6.1 Honeypots de Baja interaction:

4.6.1.1 Specter "Intrusion Detection System"

"El Specter es un honeypot inteligente basado en sistemas de detección de intrusos, vulnerables y atractivos a los atacantes, este sistema proporciona servicios como PHP, SMTP,FTP, POP3, HTTP, y TELNET que atraen fácilmente a los atacantes, pero en realidad son trampas que pretenden recolectar información.

4.6.1.2 Honeyd El Honeyd es un honeypot que crea hosts virtuales en la Red. los anfitriones pueden ser configurados para ejecutar servicios arbitrarios y su personalidad puede ser adaptado de modo que parezcan estar ejecutando ciertos sistemas operativos. Honeyd mejora la seguridad Cibernética proporcionando mecanismos para la detección y evaluación.

4.6.1.3 KFSensor El KFSensor es un honeypot que se ejecuta sobre Windows basado en sistema de detección de intrusos (IDS), actúa para atraer y detectar piratas informáticos y gusanos, vulnerables mediante la situación de los servicios del sistema y troyanos.

4.6.1.4 PatriotBox

El PatriotBox usa como señuelo el sistema de detección de intrusos (IDS), en entornos de red empresarial de forma efectiva la detección temprana de las amenazas de intrusos. También utiliza ayuda para reducir el spam en internet ya que simula un servidor de correo de retrasmisión abierta.

4.6.2 Algunos Honeypots de Alta interacción:

4.6.2.1 ManTrap : Puede crear "software jaula" y similar una red virtual de una máquina. para ello emula una variedad de diferentes maquinas (FTP, HTTP, SMTP,ODBC) en una sola ManTrap de acogida. este Honeypot es configurable para alertar a una gran variedad de alertas y puede enviar correo a cualquier

dirección e-mail o un dispositivo con capacidad SNMP para alertar a los administradores del sistema que alguien ha entrado a la "jaula""[19].

4.7 El intruso y sus técnicas

Jeimy Cano presenta la siguiente definición para este aspecto "La inseguridad es y continuara siendo la constante en un mundo interconectado. En este sentido, la mente de los atacantes y apasionados por la inseguridad informática continuará produciéndose y avanzando, pues cada vez más habrá retos y desafíos que sortear con la tecnología actual y futura. En consecuencia, estudiar la mente de los atacantes, el estilo de los hackers, sus técnicas, es una manera de aprender de las vulnerabilidades, y como la materialización de estas puede utilizarse para establecer los rastros requeridos para seguir a los atacantes"[20].

4.7.1 La mente de los intrusos

"Al referirse a la mente de los intrusos, es hacer alusión a las motivaciones, es decir los disparadores que generan tales acciones. Revisar la mente de los atacantes es adentrarse en un terreno donde la imaginación es más relevante que el conocimiento. No se puede comparar un intruso cuya motivación está más allá del reto y el reconocimiento por las capacidades mostradas, con un hacker que trata de demostrar que el manual está mal y se requiere completarlo con cada nueva experiencia y comportamiento inesperado del sistema". Ibid., p.26. A continuación, se identificará cada perfil del atacante en su contexto.

4.7.2 Ciberterrorista: En el contexto de un mundo digital e interconectado y global el terrorismo cambia sus estrategias de acciones y emplea los medios electrónicos para sustraer información, efectuar tareas de inteligencia e interactuar con todos sus simpatizantes mediante una red de comunicación eficaz, practica y efectiva. El terrorista sabe que su causa vale y merece la pena y que debe dedicarle toda la coordinación para que este acto no tenga pie a fallas por la causa. Por lo tanto, la red misma se convierte en su perfecta aliada ya que es un espacio virtual y omnipresente que le va a permitir estar en cualquier lugar al mismo tiempo y en ninguno a su vez. Ibid., p.28

El ciberterrorista, genera inestabilidad en los sistemas incertidumbre sobre la operación y fallas de las comunicaciones, formando un ambiente adecuado para

[19] https://honeypots.wordpress.com/2009/05/05/tipos-de-honeypot/
[20] CANO MARTÍNEZ, Jeimy J. Computación
Forense Descubriendo los rastros informáticos. México: AlfaOmega, 2009. P19

iniciar una guerra de desinformación y actuar para generar sensación de pérdida de control, lo cual llevara a las autoridades a un ambiente de crisis. Ibid., p.28.

4.7.3 Los Phreakers: Ellos creen en la telefonía sin costo, en un mundo libre para construir y crear lazos de conexión más allá del mundo real. Entiende que los dispositivos de comunicaciones codifican y decodifican señales para sincronizarse y lograr la transmisión de la información, pero claramente también saben que existen dispositivos que rarifican y controlan el uso del canal de las telecomunicaciones, el objetivo es evadir os controles establecidos ya sea por convicción propia o por alguna recompensa personal o económica. Ibid., p.29

4.7.4 Los Script Kiddies: Son todos aquellos que revisan y conocen las acciones de los hackers, phreakers y similares, y utilizan las mismas herramientas y técnicas que estos, con el fin de penetrar e inutilizar sistemas de comunicaciones o tecnologías de información, su enfoque es más regido por curiosidad y ver que tan real son las alarmas de los hackers y similares, estos establecen un perfil de posibles atacantes que pueden generar algún tipo de conmoción en las PYMES. Ibid., p.30

Su identificación es relativamente fácil, los scripts Kiddies son personas que gustan de experimentar en sus máquinas y alardean de sus supuestos logros ante las demás personas, son de mucho cuidado ya que pueden perder el control de sus actos y generar fallas o incidentes de grandes magnitudes, sin que ellos mismos lo pueden detectar, al hacer un uso indebido de las herramientas de hackeo que existen en internet por ello esto los hace bastante inestables y peligrosos. Ibid., p30.

4.7.5 Crackers: Se refieren a ellos como el “el lado oscuro de la fuerza”, haciendo referencia a la película de star wars; el quebrar, destruir y desestabilizar son términos que se consolidan con sus acciones. El Cracker tiene como misión vulnerar un sistema con una motivación de venganza o económica, son individuos cuyo resentimiento los ciega y lo llevas a emplear sus conocimientos para traspasar la línea de los permitido y lo legal. En definitiva, se puede decir que es un mercenario el cual está listo para actuar para el mejor postor, tiene claro que las tecnologías siempre van a contener fallas, por lo cual las conoce y las estudia para crear nuevas formas de vender sus servicios. No para proteger a las PYMES si no para crearlas y esperar el tiempo necesario para usarlas en contra y explotar tales vulnerabilidades. Estas acciones son las que los difieren enormemente de un hacker, se puede decir que el cracker es un hacker en desgracia ética y personal. Ibid., p.31

4.7.6 Desarrollador de Virus: Se puede decir que es un hacker desfigurado, es movido no por la tecnología en si ni por sus desafíos, sino que es controlado por

ella, es una persona o grupo que se alejó del lado positivo de la tecnología y tomo caminos más escabrosos y bajos, tratando de escapar de una realidad, la suya la cual es efímera y desorientada por actos impulsivos que solo buscan dañar a los demás y a si mismo sin tenerlo claro. Ibid., p.32

4.7.7 Empleados: En este perfil se puede encontrar el empleado o persona insatisfecha las cuales han terminado no de la mejor forma en su empresa o compañía, esta es una realidad innegable en toda organización, como ser humano busca alcanzar sus objetivos o metas dentro de la organización, estas pueden ser frustradas por x o y motivo generando un escenario de posible amenaza. Ibid., p.34

4.7.8 Insiders: Puede ser cualquier persona interna de la organización, que por una acción o detonante decidió actuar del lado criminal, colocando en riesgo la infraestructura tecnología de la organización, esto también se puede dar por frustraciones laborales, personales o familiares, también por celos profesionales, que actúan como se mencionó como un detonante. A demás si la persona cuenta con conocimientos empíricos y curiosidad puede llegar a ser un script kiddie y la perseverancia de un hacker, esto podría gestar un incidente de seguridad de grandes magnitudes. Ibid., p.34

5 Marco Legal

“Para tener contextualizado en un marco sobre la ley, un honeynet es un elemento ajeno a la red por lo tal se hace llamado a la 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”[21].

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

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”. Ibid., p.26

5.2 “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

[21] MARTÍNEZ CONTRERAS, Kevin David. Honeypot, hacia un protocolo de seguridad más eficiente y competitivo. 2018, 67p. Proyecto de grado (especialización en seguridad informática). Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería

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". Ibid., p.26

5.3 "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". Ibid., p.26

5.4 "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". Ibid., p.26

5.5 "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". Ibid., p.27

5.6 "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". Ibid., p.27

5.6.1 "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 o a 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". Ibid., p.27

“c) Dato público: “Es el dato calificado como tal según los mandatos de la Ley o de la Constitución Política y todos 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”. Ibid., p.28.

6. Ciberseguridad en las empresas:

La información de los usuarios ha venido tomando un carácter relevante e importante en los entornos de seguridad tecnológica, es así como existes leyes donde se ampara la seguridad del usuario una de estas es la LOPD, las cuales se han venido modificando con el fin de ir mejorándolas mucho más.

En concreto, la ciberseguridad hace referencias “al conjunto de técnicas o procedimientos que velan por la seguridad de los usuarios que comparten información entre sistemas de cómputo”[22]. Ya hace un largo tiempo la ciberseguridad ha tenido una gran aceptación, debido al auge de los nuevos sistemas de hackeo que han ido evolucionando con el tiempo.

Enfocándolo en el ambiente empresarial, esto supone un cambio informático para este caso dentro de las PYMES, obligando a realizar cambio de objetivos en cuanto a seguridad se refiere por el mismo hecho del auge tecnológico e informático y nuevas técnicas de hackeo, que lleva directamente a pensar en la seguridad de la información de los usuarios y compañía planteando nuevas estrategias y controles para las mismas.

Esto quiere decir, que “la ciberseguridad implica que las empresas deben estar preparadas para cualquier ataque que reciban, cuenten con planes o métodos de reacción y que acciones deben implementar para que no sean atacadas deliberada y sorpresivamente”[23].

Es importante tener presente que activos deben ser aplicados en las metodologías de seguridad, esto se refiere a bases de datos, archivos, metadatos, hardware, sitios

[22] Economía Simple. {En línea. {24 julio 2018}. Disponible en: (https://www.economiasimple.net/glosario/ciberseguridad)

[23] ¿Qué es ciberseguridad? | definición de ciberseguridad. {En línea}. {2016}. Disponible en: (https://www.economiasimple.net/glosario/ciberseguridad).

web, software en fin todo lo relacionado o susceptible a correr riesgos por pérdida de información o robo.

A continuación, se mencionarán tres fuentes de las cuales pueden provenir ataques, es preciso indicar que existen muchas más, en el momento se mencionaran solo tres:

6.1 Hackers: Estos, buscan vulnerabilidades en los sistemas de información valiéndose de programas y conocimientos en sistemas para buscar cierta información de los usuarios y obtenerla con fines lucrativos o dañar la imagen de un usuario o compañía, esto siempre apuntando a un beneficio propio, aunque también existen los hackers éticos, aquellos que se encargan de buscar falencias en los sistemas o software y advierten de ellos a las compañías.

6.2 Errores de programación: Un fallo en el código fuente de un programa puede ser usado como vulnerabilidad y permitir sustraer información confidencial.

6.3 Eventos naturales: sin duda es algo no controlado o fácil de proveer, ya que las eventualidades naturales o físicas se pueden presentar y perjudicar la información de manera directa o indirecta de los usuarios y empresas.

7. Estadísticas de ciber-crímenes en Colombia

De acuerdo con un estudio realizado por Symantec en el año 2017, Colombia se registró como el sexto país en Latinoamérica con el mayor número de ciberataques.

Las modalidades más usadas fueron, BOTS, Spam y el Phishing, y de igual manera otro delito informático más usado el de robo de datos a clientes bancarios.

Se afirma de acuerdo con los datos estadísticos el ciber-crimen mueve anualmente cerca de 10.000 billones de dólares, en Colombia es difícil realizar un estimado en dinero.

A continuación, se muestra los delitos informáticos en tiempo real desde el 1 de abril hasta el 7 de abril del 2019.

Figura 3. Sitio Web de la Policía Nacional de Colombia

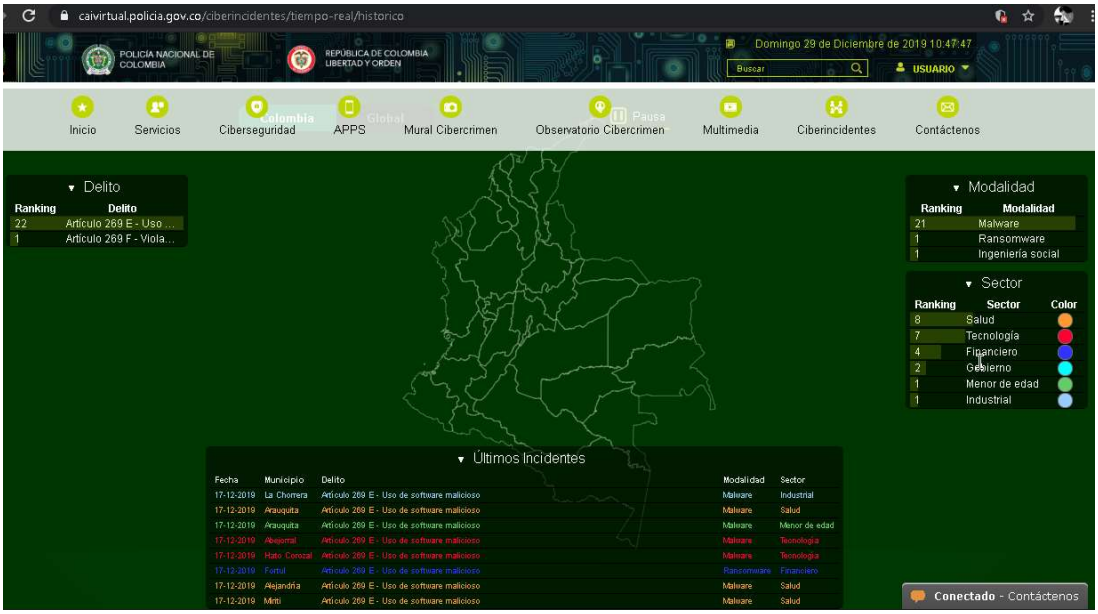


Diagrama de ataques en Línea reporte en línea de los ataques constantes que se presentan a cada minuto, la página muestra los ataques que más se realizan y las zonas y los categoriza. (Ciber incidentes | Centro Cibernético Policial)

Es por ello, la necesidad de hacer le ver a las PYMES, la importancia de aplicar la seguridad en sus entornos, de ahí la importancia de dicho trabajo y el valor implícito que le dará a la información, y los mecanismos para lograr tal fin, de esta forma pues se le brindaran los conocimiento y fundamentos orientado al buen uso de los honeynet.

Ahora para cumplir uno de los objetivos específicos en cuanto a determinar cuáles son los riesgos informáticos a los que se someten las PYMES se realizara a continuación el análisis identificación de estos, “las PYMES son un vasto mundo económico aunque no lo parezcan, se puede decir que las PYMES representan el 99.9% de los establecimientos productivos, contribuyen con el 80% del empleo en el país y aportan el 40%de productos interno bruto nacional”[24], por esto y más se hacen apetecidas ante posibles ataques informáticos, algunos de estos riesgos o peligros en cuanto a seguridad informática son:

- **Suplantación y robo de identidad:** Este ataque es denominado spear phishing es un meto en el que un hacker logra obtener información confidencial, sin

[24] Elempleo.com. Pymes, la base del mercado laboral. {En línea}. {9 de febrero 2018}. Disponible en: (https://www.elempleo.com/co/noticias/investigacion-laboral/pymes-la-base-del-mercado-laboral-5510)

embargo, este tipo de ataques no se presenta de manera general en las PYMES si no que pone foco en un individuo o grupo de individuos en específico, normalmente. el delincuente informático emplea el correo electrónico que puede parecer similar al de un remitente de confianza y le pide información confidencial mediante el uso de webs, que sin saber el usuario está construida con malware y riesgos.

- **Riesgos en redes Wi-Fi:** En bares, restaurantes y muchos lugares públicos que ofrecen wi-fi de manera gratuita, aunque para los usuarios o clientes es incentivo por la oportunidad de usar internet de manera libre, para los negocios son una ventana abierta para los ataques informáticos, no solo se habla de los riesgos de las redes inalámbricas sino también a las vulnerabilidades del cifrado WPA2 de dichas redes. En estos casos, los ciberdelincuentes puedan descubrir contraseña Wi-Fi y así tener acceso al tráfico de usuarios y dispositivos que la emplean. Por otro lado, cuando la red es gratuita y abierta, cualquier persona ajena a la compañía puede conectarse y como si no se tiene las debidas protecciones se podría presentar un robo de la información interceptando la transferencia de los datos a través de la utilización de programas como sniffers.

- **Falta de prevención ante los ataques:** Este quizás puede ser la ideología más errada, la cual es que se dice que por ser pequeña no están en el foco de la mira de los ciberataques, esto es normal ya que creen que el delincuente informático es una persona de carne y hueso a la que no le interesan los datos de una peque empresa. Sin embargo, en muchas ocasiones estos ataques informáticos son de maquina a máquina, es decir son indiscriminados y lo único que puede detenerlos es la prevención y protección.

- **Ransomware:** Es una de las amenazas de seguridad más conocidas a nivel internacional, se hizo más conocido desde el ataque del WannaCry del año pasado que afecto a un sin número de compañías a nivel mundial. El funcionamiento de este ataque es de la siguiente manera, un usuario descarga un archivo malicioso o visita una web comprometida, en ese instante bloquea el acceso a la web y en los casos más preocupantes piden un rescate de la información o web para liberarla del secuestro este fue el caso del año 2017 del WannaCry.

Se ha identificado que el ransomware, cada vez está afectando más a las PYMES, como ya se indicó al principio del trabajo, de acuerdo con lo mencionado anteriormente en cuanto a la ideología que muchas de estas tienen en cuanto a la seguridad informática.

Se pueden plantear el uso de buenas prácticas con el objetivo de restar los riesgos en cuanto a ciberseguridad en las PYMES. Sin embargo, es preciso indicar que no existe una solución única para todos los riesgos de ciberseguridad. Uno de estos

motivos es que los ataques siempre están en constante evolución, haciéndose más sofisticados y difíciles de detectar. No obstante, existes algunas recomendaciones básicas que pueden ayudar a proteger las PYMES de cualquier amenaza cibernética.

Uso de antivirus y firewall.

- Verificar las actualizaciones de seguridad del sistema operativo
- Realizar Backups
- Protección de la navegación de la organización
- Sentido común
- Realizar test de penetración
- Monitorear la red
- Revisión y análisis de registros
- Políticas de uso de contraseñas

No obstante, lo que apremia en este compendio es darle una mayor seguridad a las PYMES y para ello es el uso del honeynet como un apoyo más consolidado a la seguridad informática y que de manera conjunta con estos consejos básicos lograr el objetivo de mantener la información y la compañía a salvo.

8. METODOLOGÍA

Teniendo en cuenta que el fin buscado es la implementación del honeynet y determinar su efectividad en los ambientes corporativos para PYMES, se realizara el estudio y análisis de la información que se obtenga de los ataques sobre la misma, y que el ambiente de los honeynet está en un ciclo constante de captura y análisis de datos, se considera que la metodología apropiada para llevar a cabo el desarrollo del proyecto es la metodología en espiral que aunque trate de una metodología empleada para desarrollo de software, se puede acoplar a las necesidades del trabajo.

Esta metodología cuenta con las siguientes fases:

1. Análisis de requerimientos

2. Diseño del servicio o sistema

3. Implementación

4. Realización de pruebas

8.1 Fase 1: Análisis de requerimientos: En esta fase se realizará el análisis del estado del arte que fue construido en el documento referente a los honeynet y Honeypots, identificando lo que es requerido para la correcta implementación e identificación de su efectividad.

8.2 Fase 2: Diseño del servicio o sistema: Cuando se tenga toda la compilación de los estudios documentales y definido los requerimientos se podrán proceder con el diseño del sistema, este diseño se fundamente en la arquitectura misma del sistema y de cómo se debe conformar basado en las mejores prácticas.

Para esta etapa se estudiaron diversos proyectos alusivos al tema, con el fin de dar el enfoque que se requería en cuanto al análisis de efectividad del honeynet y sentar las bases necesarias y pilares requeridos para garantizar la solidez del trabajo basándose en casos prácticos y estudios relevantes sobre el tema, Se escoge una solución que aunque no es libre, da unas prestaciones muy interesantes a la aplicación del honeynet y que por su versatilidad y manejo intuitivo se convirtió en la herramienta perfecta para el proyecto. De igual manera se revisaron herramientas bajo licenciamiento GPL Linux pero la implementación y la misma configuración del honeynet resultan bastante complejas en los cuales el costo que se ahorraría en implementación de software comerciales se gastaría en la administración y capacitación de la herramienta en Linux, pues se requiere de personal experto en Linux para su implementación y administración, por lo cual y con justificación se

seleccionó una herramienta bajo Windows la cual permite una gran variedad de usos y reportes y que a su vez no es complicada de implementar, configurar y usar.

8.3 Fase 3: Implementación

En la implementación del honeynet, se empleará un HoneyPot de baja interacción y algunos escenarios con el fin de aplicar ciento por ciento el valor real del producto entregado sumado a la documentación y conocimiento transmitido.

8.4 Actividades para desarrollar dentro de la fase 3

A continuación, se enumeran las etapas que intervienen en la fase de implementación con el fin de realizar el desarrollo del proyecto, se manejaran dos etapas:

8.4.1 Etapa 1: Denominado Implementación Honeypot para conformar posteriormente una red de Honeypots y se obtendrá la honeynet.

1. Instalación atendida Honeypot KF Sensor.
2. Implementación máquina virtual y configuración Windows 10 o Windows Server 2012 o superior
3. Implementación y configuración servicio KF Sensor
4. Duplicación del servicio en varios servidores para la honeynet
5. Configuración de varios sistemas operativos señuelo y protocolos

8.4.2 Etapa 2: Denominado análisis de información basado en los reportes obtenidos

1. Obtención de la información de los ataques:
2. Análisis de la información para creación de base de conocimiento
3. Efectuar ataques controlados para demostración
4. Post-Análisis de los ataques realizados
5. Realización de pruebas: En dicha fase la cual se desarrollará al final de la implementación se podrán observar una serie de acciones de ataques ejecutadas sobre la red con el fin de obtener el insumo para la generación de log y demás insumos para las documentaciones e informes requeridos.

9. ARQUITECTURA HONEYNET BAJA INTERACCION

Se define la arquitectura como el diseño conceptual y estructural de forma operacional de un sistema, es decir es un modelo funcional de los requerimientos y las implementaciones de diseño para los diferentes elementos que conforman un honeynet.

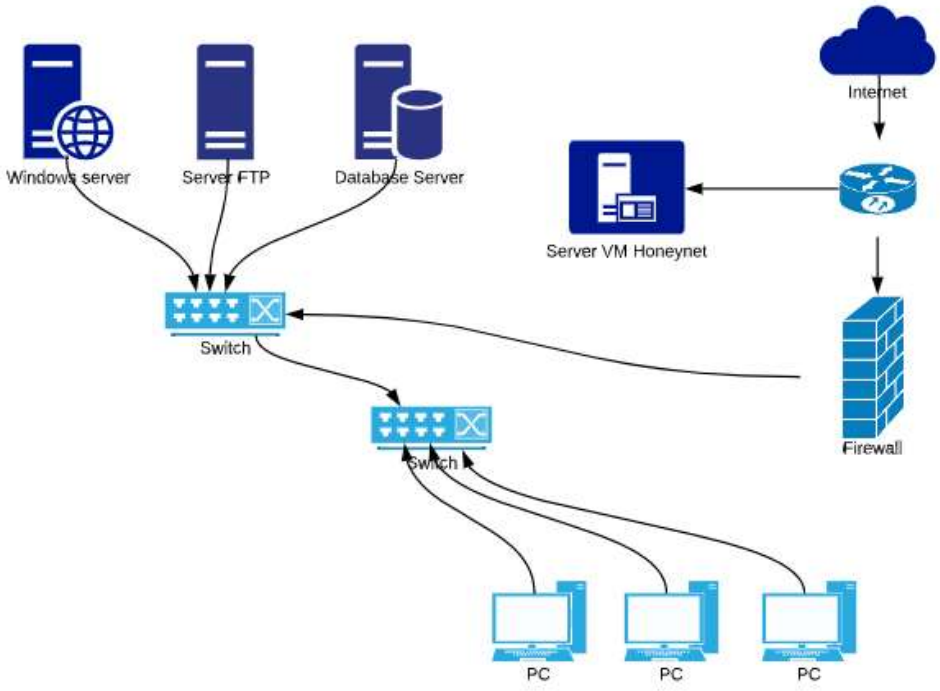
Los honeynet son una arquitectura consolidada y no simplemente un producto, estos forman parte en el ambiente de red el cual puede ser totalmente controlado, es decir los honeynet se mezclan entre los diferentes elementos de sistemas existentes, llámense servidores, routers, computadores personales en general, mientras esto ocurre el administrador de sistemas será observador de como los atacantes intervienen en ellos.

Para mantener este ambiente controlado. Es primordial en la arquitectura del honeynet mantener siempre los dispositivos de seguridad perimetral en conjunto con él, esto es de vital importancia para mantener segura la red.

Luego de evaluar las diferentes arquitecturas se optó por la arquitectura de baja interacción.

Dentro de la red se podrán desplegar delante del firewall que protege la red interna, inmediatamente después del firewall en DMZ, o por último dentro de la red interna, segmentada y aislada del resto del sistema.

Figura 4. Arquitectura Honeynet



Arquitectura Honeynet esta es la arquitectura simple de un honeynet de baja interacción Fuente: el autor

9.1 Recolección y Análisis de datos:

Como se ha mencionado el honeynet permitirá la recolección de datos, este será el insumo para permitir la generación de datos estadísticos, los cuales podrán apoyar a la generación de indicadores con los cuales se podrá medir el estado de la seguridad en las PYMES.

Otro factor importante es que con los datos obtenidos se podrán generar estudios con el fin de buscar patrones de ataques y aquellos que se pueden definir como objetos de investigación.

El administrador deberá clasificar la información para poder cumplir los objetivos y fundamentar la teoría que se pretende demostrar.

9.2 Seguridad Informática:

La seguridad informática es la forma de velar por cómo se debe proteger la infraestructura tecnológica y de comunicaciones, en ello se puede a lucir que se

refiere a los programas, software y computadores de la compañía y que sean usadas de forma correcta.

La seguridad informática realiza una serie de análisis de riesgos tales como identificación de activos, identificación de vulnerabilidades y amenazas tanto de software como de hardware y mitigar o reducir los indicadores de riesgo que se puedan dar en la compañía.

9.3 Seguridad de la Información:

La seguridad de la información son las buenas prácticas que podemos implementar en los ambientes de producción de cada organización o compañía, para ello se debe recalcar medias preventivas y reactivas si es el caso ante cualquier situación que atente contra el bien más valioso de una compañía la cual es la información, ella se encargara de custodiar la protección, confidencialidad y disponibilidad de la información.

Ahora, lo que se pretende es que las PYMES, no sean foco de los atacantes informáticos, y demostrar el potencial que esta herramienta puede brindar a tal grado que se logre una barrera más de protección ante dichos ataques, y de esta forma identificar los patrones de comportamiento de dichos atacantes y poder analizar el tráfico entrante para realizar los análisis pertinentes para generar reglas, políticas y mejores prácticas para evitar tales eventualidades.

10. IMPLEMENTACION CENTRALIZADA DEL HONEYNET

10.1 Etapa 1

10.1.1 Instalación Windows 10 o Windows server 2012 o superior como máquina virtual:

Para contar con un ambiente virtualizado se propone como opción la implementación de Proxmox o si se tiene el rol de Hyper-V de Windows no se tiene ningún inconveniente cualquier plataforma de virtualización es óptima.

Ahora, la instalación del software seleccionado **KF Sensor** se puede hacer en una maquina o servidor que ya cuente con el sistema operativo Windows ya sea servidor o desktop, se recomienda hacer la implementación en un ambiente virtualizado.

KF Sensor:

Es el software seleccionado para la implementación del Honeypot que se empleara, este es un Honeypot de baja interacción, el programa lo que hace es simular servicios en el nivel de aplicación de la capa OSI. Como no introduce más elementos en las demás capas, como drivers adicionales ni varia la pila de IP, hace que se reduzca el riesgo de detección y el poder comprometerlo. Puede también gestionar multitud de puertos y direcciones IP.

Ventajas del Honeypot KF Sensor:

Algunas ventajas con la que cuenta la herramienta son:

- Identificación de firmas de ataques.
- No se generan falsos positivos
- Sin oberhead
- Se pueden detectar ataques de red a sistemas basados en Windows.
- Gestión remota
- Detección en tiempo real.
- Puede interactuar con otros sistemas de seguridad tales como IDS y antivirus sin afectación sobre estos últimos
- Puede detectar ataques de día 0. Antonio A. R. V, Carlos A. B. M, Juan M. G. C. Fernando P. R (2015

KF Sensor se compone de los siguientes elementos:

KF Sensor Server: Este componente provee las funcionalidades principales del sistema. No emplea interfaz gráfica y se ejecuta en segundo nivel, escucha los puertos TCP/UDP e interactúa con los posibles atacantes, generando alarmas.

KF Sensor Server: Interfaz gráfica del sistema

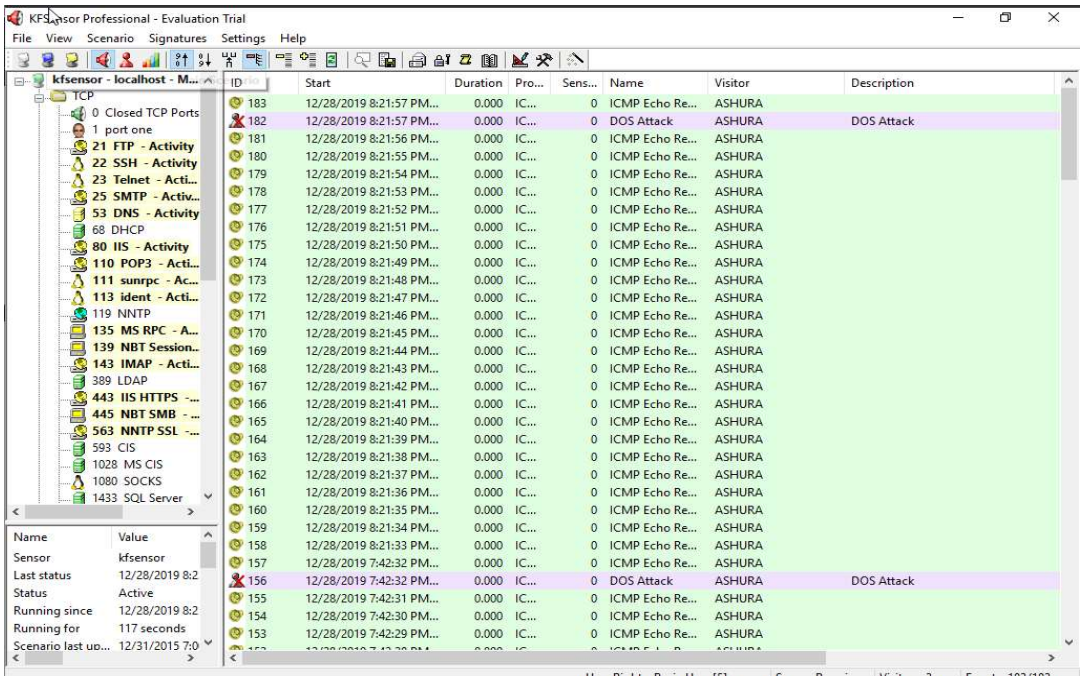
Instalación del Honeypot **KF Sensor** sobre Windows 10 virtualizado

Para la instalación del software se debe hacer primero la descarga de la siguiente url www.keyfocus.net/kfsensor. y descargar el ejecutable

Para el correcto funcionamiento del software es necesario realizar la instalación de las librerías WinPcap, eso con el fin de colocar la tarjeta de red en modo promiscuo para poder capturar los paquetes.

A continuación, se mostrará la interfaz del software y se realizará una descripción básica de cada una de las funciones más importantes.

Figura 5. Interfaz del HONEPOT KF Sensor



Interfaz del HoneyPot KF Sensor Fuente el autor

Una de las características de la herramienta es poder generar reportes, los cuales serán fundamentales para tomar medidas de carácter importante sobre la seguridad en la compañía.

Para ello se debe realiza la instalación de un motor de Base de datos, para una mejor comodidad y bajar costos se realizará la instalación de MySQL.

Instalación de MySQL

Con el fin de optimizar y hacer mucho más fácil la instalación de MySQL, esta se realizará empleando la suite de XAMPP, el cual es software de entornos web para su correspondiente publicación, pero que en su herramienta permite la instalación del gestor de Base de Datos MySQL, para este caso práctico se usara la instalación del motor de base de datos como se indicó[25].

Se procede con la descarga del programa, para ello se accede a la página web https://www.apachefriends.org/es/download.html y se procede con la descarga de la última versión del XAMPP. Seguido de ello se procede con la instalación. Apache Friends (2019).

La instalación es muy versátil e intuitiva solo se debe tener cuidado de seleccionar todos los elementos de la plataforma para su correcta funcionalidad.

Recomendación: Es importante que el motor de base de datos se encuentre instalado en otro servidor o pc. Esto porque razón, debido a que el HoneyPot KFsensor instala librerías propias de MySQL y por ello, al momento de hacer la instalación del motor de MySQL este no funcionara correctamente, también porque es una buena práctica que la base de datos se encuentre en un servidor diferente.

Configuración de la base de datos para los reportes en Kfsensor

Para lo siguiente, a continuación, se realiza la configuración para preparar la conexión al servidor de base de datos como de puede denotar en la fig. 6.

[25] SEIDLER, Oswald Kai, VOGELGESANG, Kay. {En línea}. {2020} disponible en: (https://www.apachefriends.org/es/index.html)

Figura 6. Configuración de la conexión al servidor de Base de Datos

Configuración de la conexión al servidor de Base de Datos. Fuente el autor

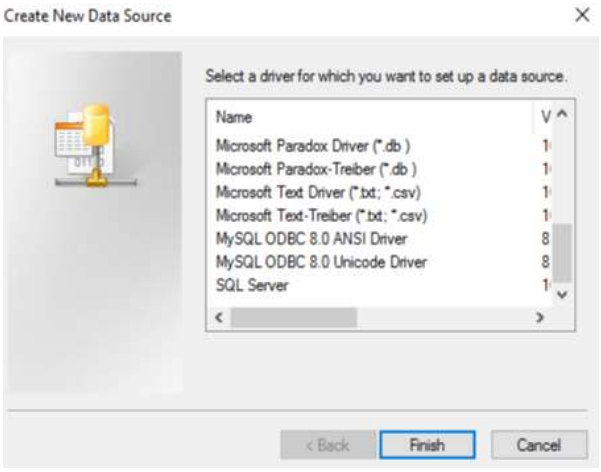
Posteriormente, se debe definir la conexión ODBC a la Base de Datos.

En la opción que dice “Define ODBC” se realizara el procedimiento de conexión

Pero para ello, debe tenerse instalado el drive de conexión este se puede obtener del siguiente enlace https://dev.mysql.com/downloads/connector/odbc/.

Luego de tener el conector instalado (Tener cuidado de instalar el instalador de 32Bits, ya que el HoneyPot es de 32bits), se procede con la creación de la conexión como se indicó anteriormente.

Figura 7. Creación de conexión ODBC



Creación de conexión ODBC fuente el autor

Se procede con la selección del conector correcto y se finaliza la creación de la conexión como se mostró en la fig. 7.

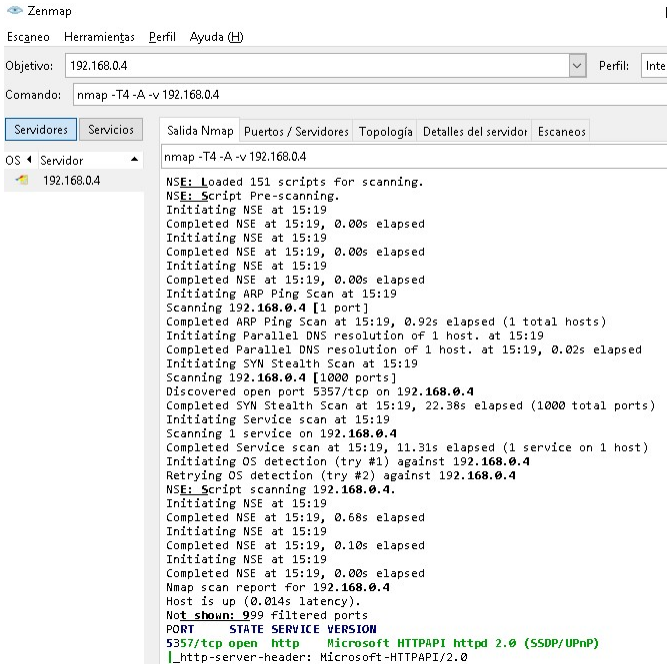
Luego de tener el servicio instalado, se debe repetir el proceso en varias máquinas virtuales con el fin de crear la red de Honeypots para dar paso a la creación de la red de honeynet. Con esto se tendría por completada la etapa 1, finalizando con la configuración de varios sistemas operativos con diversos servicios y protocolos.

10.2 Etapa 2:

10.2.1 PRUEBA DE ESCANEO DE SERVICIOS

A continuación, se realizará una prueba de funcionalidad del HoneyPot. Para ello, se ejecutará una prueba de descubrimiento de puertos, que es lo que inicialmente un atacante realizaría. Luego, del escaneo con la utilizad zenmap, se recolecto la siguiente información fig.8 y fig. 9.

Figura 8. Descubrimiento de puertos y servicios



Descubrimiento de puertos fuente el autor

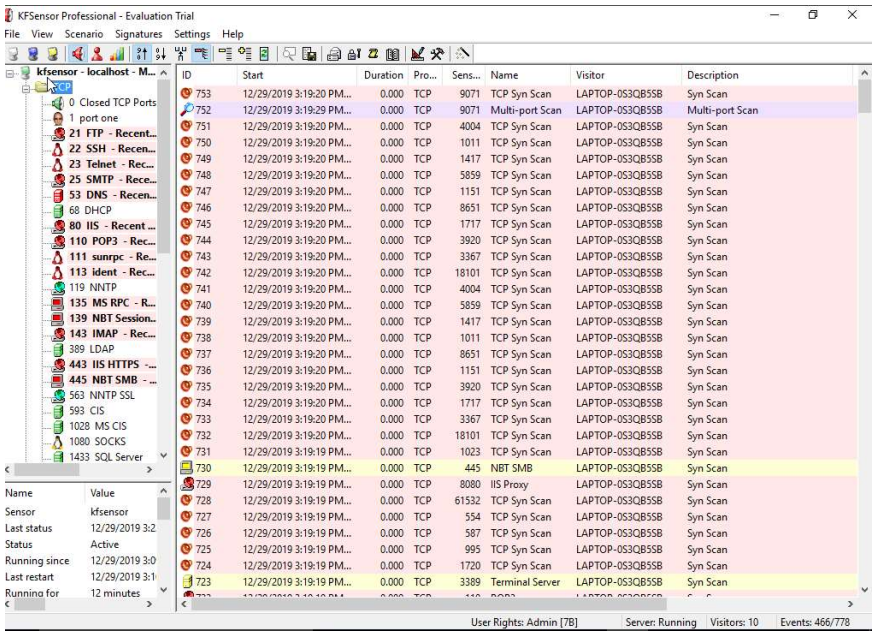
Figura 9. Descubrimiento de puertos y servicios II

```
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: AC:B5:7D:62:5E:7F (Liteon Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1511 - 1607 (93%), Microsoft Windows 8.1 R1 (92%), Microsoft Windows Server 2016 (92%), Microsoft Windows 7
Professional or Windows 8 (92%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (92%), Microsoft Windows Vista SP2, Windows 7 SP1,
or Windows Server 2008 (92%), FreeBSD 6.2-RELEASE (92%), Microsoft Windows Phone 7.5 or 8.0 (90%), Microsoft Windows 10 1607 (90%), Microsoft Windows 10 1511
(90%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.019 days (since Sun Dec 29 14:51:58 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT      ADDRESS
1   14.09 ms 192.168.0.4

NSE: Script Post-scanning.
Initiating NSE at 15:19
Completed NSE at 15:19, 0.00s elapsed
Initiating NSE at 15:19
Completed NSE at 15:19, 0.00s elapsed
Initiating NSE at 15:19
Completed NSE at 15:19, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.06 seconds
           Raw packets sent: 2090 (97.080KB) | Rcvd: 23 (1.260KB)
```

Fuente el autor

De lo cual, el HoneyPot identifico lo siguiente como se muestra en la fig.10:

Figura 10. Vista en el sistema Honeypots



Fuente el autor

CREACIÓN DE LOG

De la siguiente manera se pueden obtener los logs, los cuales dan información importante como qué tipo de ataque se efectuó, ip de origen, puerto e incluso el método que se empleó, como se puede observar en la fig.11 y fig. 12

Figura 11. Generación de logs de eventos

Fuente el autor

Figura 12. Generación de logs de eventos

ID	Start	Duration	Protocol	Sensor Port	Name
1822	1/1/2020 11:02:53 AM....	0.000	TCP	8080	IIS Proxy
1821	1/1/2020 11:02:53 AM....	0.000	TCP	1720	TCP Syn Scan
1820	1/1/2020 11:02:53 AM....	0.000	TCP	80	IIS
1819	1/1/2020 11:02:53 AM....	0.000	TCP	139	NBT Session Service
1818	1/1/2020 11:02:53 AM....	0.000	TCP	8888	TCP Syn Scan
1817	1/1/2020 11:02:53 AM....	0.000	TCP	23	Telnet
1816	1/1/2020 11:02:53 AM....	0.000	TCP	443	IIS HTTPS
1815	1/1/2020 11:02:53 AM....	0.000	TCP	554	TCP Syn Scan
1814	1/1/2020 11:02:53 AM....	0.000	TCP	995	TCP Syn Scan
1813	1/1/2020 11:02:53 AM....	0.000	TCP	110	POP3
1812	1/1/2020 11:02:53 AM....	0.000	TCP	135	MS RPC
1811	1/1/2020 11:02:53 AM....	0.000	TCP	993	TCP Syn Scan
1810	1/1/2020 11:02:53 AM....	0.000	TCP	199	TCP Syn Scan
1809	1/1/2020 11:02:52 AM....	0.000	TCP	199	TCP Syn Scan
1808	1/1/2020 11:02:52 AM....	0.000	TCP	993	TCP Syn Scan
1807	1/1/2020 11:02:52 AM....	0.000	TCP	135	MS RPC
1806	1/1/2020 11:02:52 AM....	0.000	TCP	110	POP3
1805	1/1/2020 11:02:52 AM....	0.000	TCP	995	TCP Syn Scan
1804	1/1/2020 11:02:52 AM....	0.000	TCP	554	TCP Syn Scan
1803	1/1/2020 11:02:52 AM....	0.000	TCP	443	IIS HTTPS
1802	1/1/2020 11:02:52 AM....	0.000	TCP	23	Telnet
1801	1/1/2020 11:02:52 AM....	0.000	TCP	8888	TCP Syn Scan
1800	1/1/2020 11:03:00 AM....	0.000	TCP	443	Multi-port Scan Warning
1799	1/1/2020 11:02:52 AM....	0.000	TCP	139	NBT Session Service
1798	1/1/2020 11:02:01 AM....	0.000	ICMP	0	ICMP Echo Request
1797	1/1/2020 11:02:01 AM....	0.000	ICMP	0	DOS Attack
1796	1/1/2020 11:02:00 AM....	0.000	ICMP	0	ICMP Echo Request
1795	1/1/2020 11:01:59 AM....	0.000	ICMP	0	ICMP Echo Request
1794	1/1/2020 11:01:58 AM....	0.000	ICMP	0	ICMP Echo Request
1793	1/1/2020 11:01:57 AM....	0.000	ICMP	0	ICMP Echo Request
1792	1/1/2020 11:01:56 AM....	0.000	ICMP	0	ICMP Echo Request

Fuente el autor

EL principal objetivo de los esquemas es brindar de forma detallada el ataque puntual que se está realizando.

A continuación, se expresa como podría en el Honeypot crear un esquema para un ataque de DDos y catalogarlo según el caso.

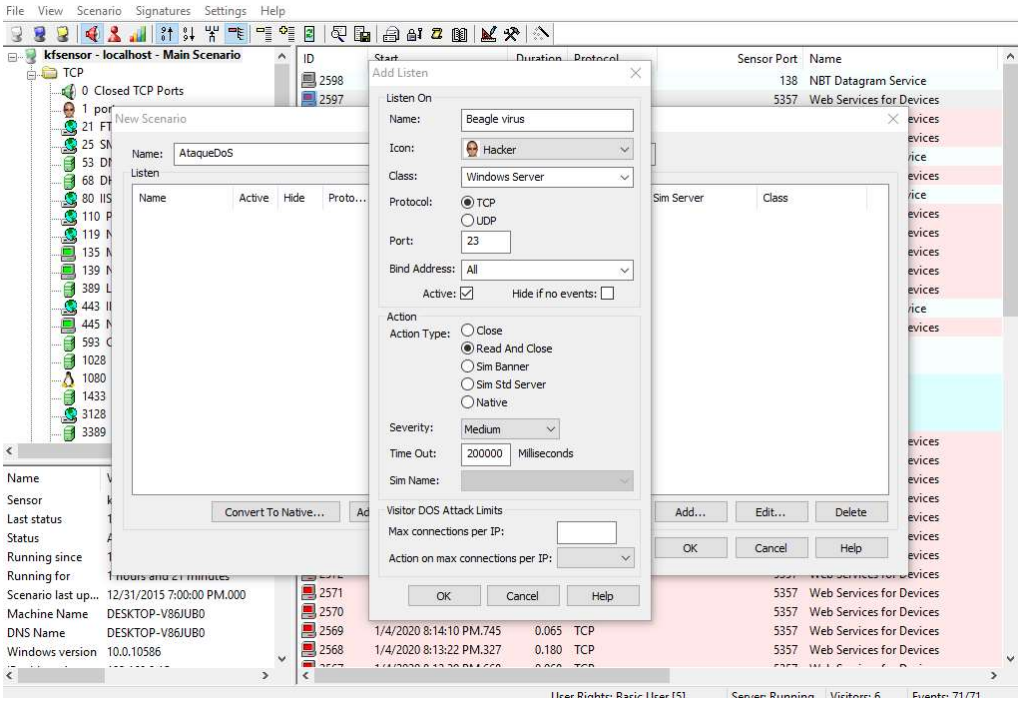
En el Honeypot KFsensor, permite el manejo de escenarios, para el caso práctico estos eran nuestros esquemas para crear según para cada tipo de ataque y tener un mejor control sobre los mismos y permitir identificar las vulnerabilidades que usa propiamente el ataque.

Con el fin de poder construir de una forma más acertada el tipo de ataque para el escenario, se toma como referencia cuales son los puertos más usados por el ataque DDoS. De los cuales se conoce que son los siguientes,

Puertos usados comúnmente para ataque DDoS: Puerto 23/TCP y puerto 2323TCP.

Por lo cual en el Honeypots se crea el escenario personalizado indicando los puertos mencionados fig. 13.

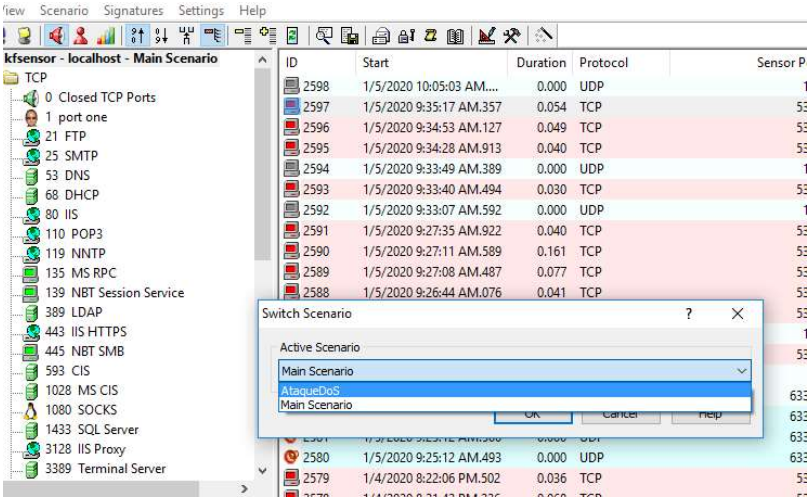
Figura 13. Creación de Escenarios



Fuente el autor

Luego, de tener el escenario creado en el sistema de Honeypot, se procede a realizar la activación de este como se observa en la fig. 14.

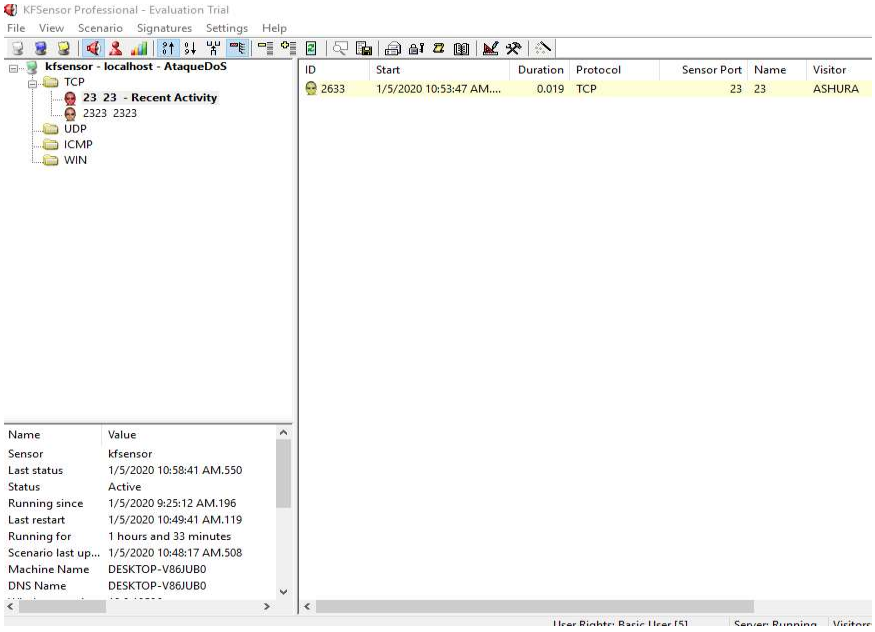
Figura 14. Selección de Escenario personalizado



Fuente el autor

Posterior a la activación del escenario, se procede a realizar la prueba de penetración y generar el esquema correspondiente al ataque de DDoS, fig. 15.

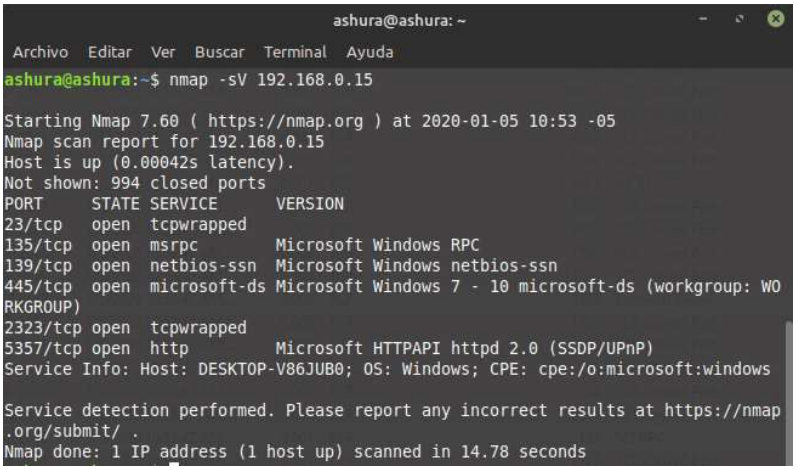
Figura 15. Generación de Esquemas para el ataque DDoS



Fuente el autor

Desde le pc atacante se realiza el descubrimiento de puertos para preparar el ataque DDoS, fig. 16.

Figura 16. Descubrimiento de puertos desde maquina atacante

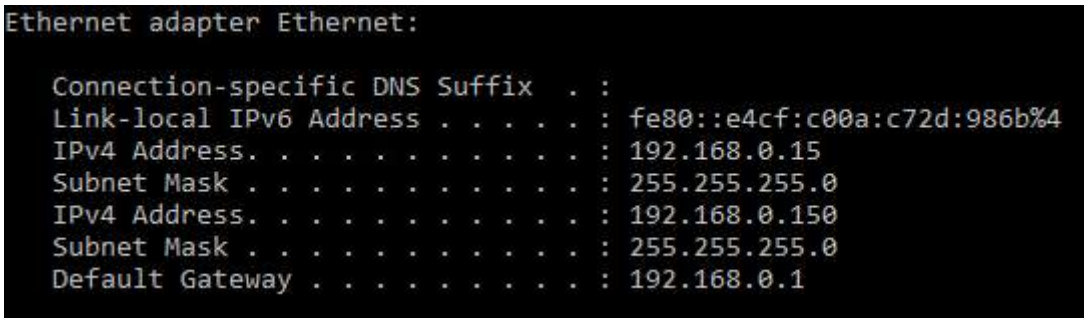


Fuente el autor

Como se puede apreciar, en la anterior imagen se identifica una novedad, la cual consiste en que al realizar el escaneo de puertos le está dando información al atacante de la ip real del Honeypots, esto no sería conveniente ya que interpretaría que no se trata realmente de un servidor si no de un desktop, puesto que en la parte de “Service Info: Host: DESKTOP-V86JUB0” , por lo tanto se debe enmascara u ocultar la identidad real del sistema de HoneyPot. Para ello se realiza lo siguiente:

Como se puede comprobar esta sería la ip real del sistema de Honeypot fig. 17.

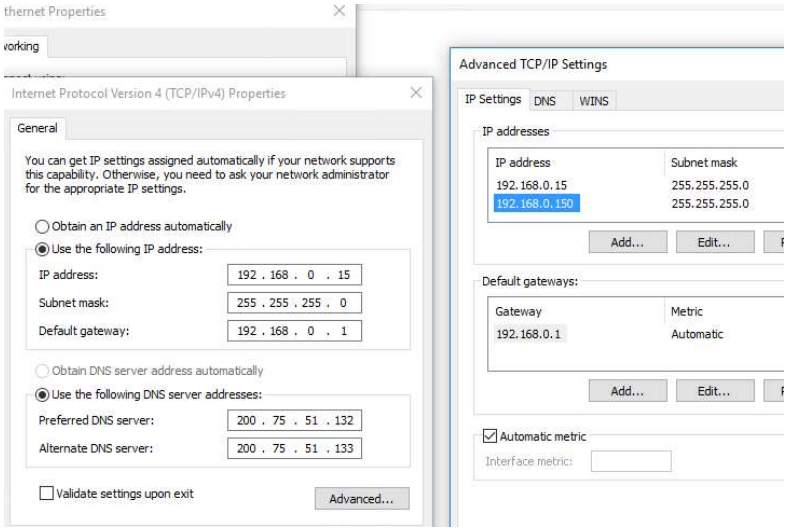
Figura 17. ip real servidor HoneyPot



Fuente el autor

El objetivo es encubrir la ip real, esto se logra creando una ip virtual a la máquina. En las propiedades de red, en opciones avanzadas se puede lograr la creación de una ip virtual, como se observa en la fig.18.

Figura 18. Creación de ip virtual



Fuente el autor

Sin embargo, si se hace nuevamente un escaneo el hostname del sistema de Honeypot seguirá siendo el mismo, aunque la ip sea otro, como se denota en la fig. 19.

Figura 19. Hostname e ip nuevo escaneo de puertos

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-05 11:37 Hora est. PacYfico, SudamUrica
Nmap scan report for 192.168.0.150
Host is up (0.16s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE            VERSION
23/tcp   open  tcpwrapped
135/tcp  open  msrpc              Microsoft Windows RPC
445/tcp  open  microsoft-ds       Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
2323/tcp open  tcpwrapped
3389/tcp open  ssl/ms-wbt-server?
5357/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: AC:B5:7D:62:5E:7F (Liteon Technology)
Service Info: Host: DESKTOP-V86JUB0  OS: Windows; CPE: cpe:/o:microsoft:windows
```

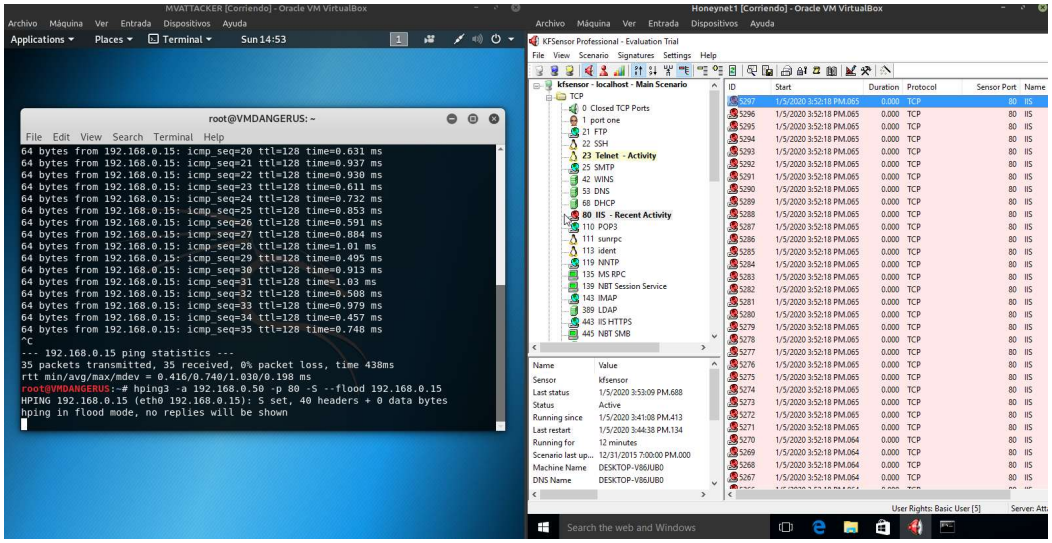
Fuente el autor

Para solucionar esto se crea un nuevo registro en la entrada del servicio de DNS del controlador de dominio. Crea un así un nuevo host apuntando a la ip 192.168.0.150 y se crean en las zonas directa e inversas los registros PTR. Con ello cualquier solicitud a la ip 19.2168.0.150 mostrar el nombre de un servidor.

Ejecución ataque de denegación de servicio DDoS simple

Ataque DoS: Se caracteriza por el uso de Scripts preparados para realizar ataques de denegación de servicios a los equipos informáticos analizados siempre y cuando sean vulnerables a este tipo de ataques, fig.20.

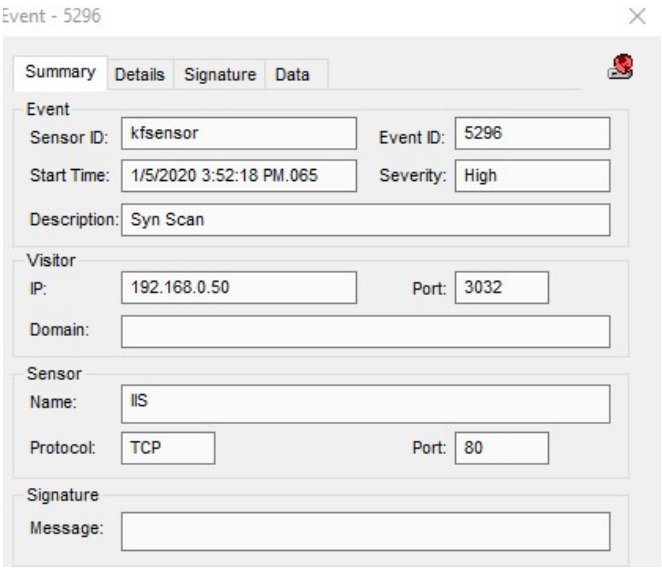
Figura 20. Ataque de denegación de servicios DoS



Fuente el autor

Como se pudo observar en la anterior fig. 20, se realiza un ataque de DoS sobre el puerto 80, el cual corresponde al servicio web. El HoneyPot detecta el ataque y se puede generar el esquema correspondiente para posteriormente realizar las acciones correspondientes.

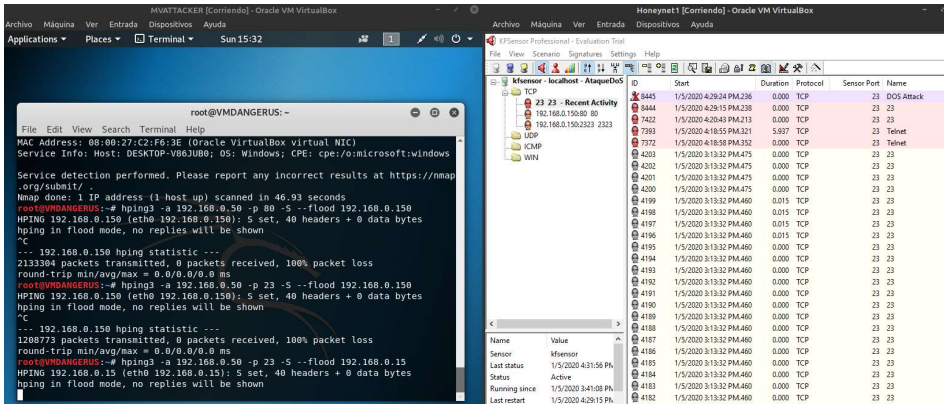
Figura 21. Datos relevantes del ataque, mostrador por el Honeypot



Fuente el autor

En la fig. 21, se puede observar del esquema obtenido los datos como la ip atacante, la severidad del ataque y el puerto y protocolo.

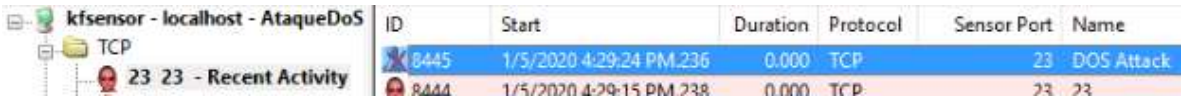
Figura 22. Ataque denegación de servicio al puerto 23



Fuente el autor

En la fig. 22, se observa un nuevo ataque al puerto 23, empleando el mismo método denegación de servicios, el objetivo de este es realizar la saturación al puerto 23 protocolo tcp y saturar las conexiones al servicio RDP conexión por terminal; impidiendo entonces poder realizar conexiones remotas al servido.

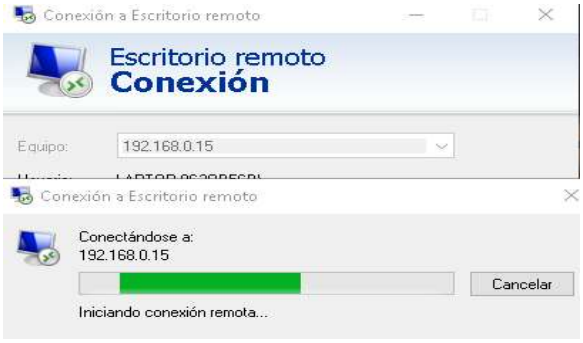
Figura 23. Vista del reporte del HoneyPot



Fuente el autor

En la fig. 23, se observa el reporte del servicio de Honeypot identificando el tipo de ataque.

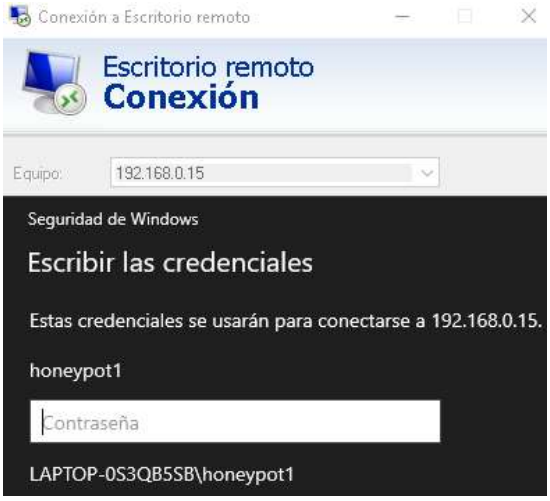
Figura 24. Verificación de servicio RDP-Conexión Remota



Fuente el autor

En la figura 24, se puede constatar la caída del servicio de conexión por RDP o conexión remota. Se realiza el intento de conexión desde uno de los pc de la red al servidor virtual y no permite la conexión. Luego se detiene el ataque y ya es posible acceder por RDP nuevamente al servidor.

Figura 25. Conexión restablecida por RDP al servidor



Fuente el autor

En la fig. 25, ya se puede observar que el servicio luego de la detención del ataque sea restablecido.

De esta forma, se pueden construir los demás escenarios para la obtención de los esquemas por parte del sistema de Honeypot.

Procedimientos de seguridad generados a partir de análisis de reportes del honeynet

Para implementar los debidos procedimientos de seguridad luego de los análisis obtenidos por la honeynet, se deberá tener presente los siguientes aspectos:

- ❖ Formación en seguridad de la información del personal
- ❖ Gestión y tramite de incidencias
- ❖ Control y supervisión de los accesos a los sistemas de la empresa
- ❖ Eficiencia y cumplimiento en el mantenimiento del sistema de gestión de la seguridad de la información.
- ❖ Efectividad de las herramientas contra código malicioso
- ❖ Mantenimiento de los equipos informáticos y sistemas de información.

Para una buena gestión de dichos procedimientos se deberá contar con:

- Responsable
- Objetivo
- Métrica
- Frecuencia
- Formula
- Indicador
- Medición

Con los anteriores elementos, el responsable de la seguridad valora los datos obtenidos de acuerdo con la frecuencia estimada para cada indicador, que luego será mencionado en el documento de revisión del sistema.

Este documento o informe deberá contener los siguientes valores:

"Objetivo: Se especificará la función de seguridad objeto de evaluación, se identificará la finalidad hacia la cual deben dirigirse los recursos y esfuerzos para dar cumplimiento a las métricas"[26].

[26] GÓMEZ FERNÁNDEZ, Luis. FERNÁNDEZ RIVERO, Pedro Pablo. Como implementar un SGSI según ISO/IEC 27001 y su aplicación en el esquema nacional de seguridad. Bogotá: AlfaOmega, 2019. 163p

“Métrica: Se describirá como van a ser cuantificados los atributos y convertidos a indicadores, que serán base para la toma de decisiones” Ibid,. p.163

“Indicador: Se refiere a la meta o el propósito que se desea alcanzar, expresada por valores numéricos, que van a permitir evaluar el nivel de seguridad y progreso en el tiempo
“. Ibid,. p.163

“Frecuencia: Se definirán y programarán claramente los intervalos en los cuales se llevará a cabo cada medición”. Ibid,. p.163

“Frecuencia: Se establecerá el modo para realizar, calcular, expresar o resolver las métricas establecidas”. Ibid,. p.163

“Mediciones: Se obtendrán los valores de las métricas, obtenidas como resultado de la formulación anterior”. Ibid,. p.163

“Estas mediciones aportaran información que servirá para adoptar decisiones o determinar la eficiencia de los controles de seguridad implementados”. Ibid,. p.163, (Ver Anexo A Tabla 2)

Documentación del procedimiento de gestión de incidencias

Notificación de incidencias

“En el registro de incidencias, se deberán registrar cada una de ellas que sean detectadas, entendiéndose como incidencia toda aquella anomalía que afecte o pudiera afectar la seguridad de los datos y la red. Asimismo, se deberá notificar si es detectada una vulnerabilidad o debilidad en el sistema que pueda comprometer la seguridad de la información”. Ibid,. p.131

Gestión y tratamiento de incidencias

“La gestión de la incidencia o de la vulnerabilidad se iniciará con la identificación de la causa o posibles causas que dieron paso a la misma, de igual manera los efectos que estas mismas causan. Este suministro de información debe salir de los análisis obtenidos de los reportes y estudios del honeynet”. Ibid,. p.132

“El tratamiento de la incidencia o vulnerabilidad se deberá manejar de dos maneras:

- Corrector
- Preventivo

El tratamiento corrector tratará de resolver la problemática causada por la incidencia, mientras que el preventivo establecerá los medios y/o métodos precisos con el fin de evitar la repetición de esta o la reducción de la vulnerabilidad". Ibid,. p.132

"Con el fin de reducir los riegos que resultan de la explotación de vulnerabilidades técnicas publicadas, el departamento de sistemas hará un seguimiento para identificar nuevas vulnerabilidades en los activos definido en el inventario, y determinar que parches o modificaciones se deben hacer y aplicarlas". Ibid,. p.132

Requisitos de documentación

- "Registro de incidencias ". Ibid,. p.132

Referencias

- "Política de seguridad". Ibid,. p.132
- "ISO/IEC 27002". Ibid,. p.132
- "Manuales de funcionamiento y uso de los equipos electrónicos". Ibid,. p.132, Anexos (Ver Anexo B)

11 generación de instructivos de seguridad informática a partir de los datos generados por la red de honeynet

De los datos e informes obtenidos por la red de honeynet se puede partir para la realización de los instructivos de seguridad que se aplicaran al modelo de SGSI, con el fin de no solo contar con un soporte documental ante auditorias, sino que se tendrá una herramienta documental para prevenir y/o corregir las novedades que a seguridad en la empresa a nivel de sistemas se pueda presentar.

Como bien se puede observar los reportes cuentan en especial con la identificación de los puertos que cada servicio emplea para su funcionamiento.

Para conocer un poco de que trata los puertos y protocolos a continuación una breve descripción por conocimiento ya que es importante entender el concepto.

11.1 WELL KNOWN PORTS

Los sistemas se comunican entre si identificándose por su dirección ip. Pero en cada uno de ellos, se identifican distintos protocolos a nivel de aplicación, como por ejemplo el servicio de FTP, este se diferencia por su número de puertos, a si pues para el puerto del servicio FTP le corresponde el 21, que es el puerto estándar para el servicio, sin embargo este puerto es muy vulnerable, y por lo tanto se recomienda

manejar el servicio con seguridad, para ello se tiene el puerto 22, que corresponde al servicio SFTP con seguridad.

Algunos ejemplos de puertos y sus servicios

20/tcp

21/tcp FTP file Trasnfer Protocol (Protocolo de transferencia de ficheros)

23/tcp Telnet, comunicaciones de texto insegura

25/tcp SMTP, Simple mail Transfer Protocol (Protocolo simple de transferencia de correo)

69/udp TFTP, Trivial File Transfer Protocol (Protocolo Trivial de transferencia de ficheros)

80/tcp HTTP, HyperText Transfer Protocol (Protocolo de transferencia de hypertexto)

110/tcp POP3, Post Office Protocol

161/udp SNMP, Simple Network Management Protocol.

443/tcp HTTPS/SSL, Utilizado para el acceso seguro a sitios web

11.2 PROTOCOLOS

La información se transmite de múltiples maneras sobre la internet y la misma red, para comprender un poco mejor de que va el tema, lo que se debe saber es que la información se organiza, para ello existen dos maneras:

- Conmutación de circuitos: cuando la comunicación es establecida, se reserva el canal; este puede ser físico o virtual, donde se reserva cierta cantidad de ancho de banda.

- Conmutación de paquetes: La información se agrupa en tramos de datos y se transmite la información del origen y del destino.

Internet se basa en la conmutación de paquetes para transmitir la información. El tramo de datos se denomina paquetes de datos o datagramas.

A la hora de transmitir un paquete a través de la red, el ordenador agrega las cabeceras de los distintos protocolos. A este proceso s ele llama encapsulamiento y sigue en orden inverso, a lo que se le llama niveles de red.

11.3 PROTOCOLOS A NIVEL DE RED

Básicamente el protocolo de internet (IP) es el lenguaje sobre el que se basan las trasmisiones que se producen en la red. Actualmente, la versión más empelada es la IPV4, versión 4. Sin embargo, de manera paulatina se está sustituyendo por la versión 6 IPV6.

Ya con la obtención del conocimiento respecto a que son los protocolos y los puertos y de acuerdo con los reportes de la red honeynet se puede iniciar con la creación de los instructivos de seguridad.

11.4 Ejemplo construcción de instructivo de seguridad informática

Es importante recordar que los instructivos se emplean para la descripción de una operación en concreto.

Es la manera de cómo se describe la relación de una tarea con pasos claros y exactos. Se pueden extraer de los procedimientos.

Para el caso, estos se determinarán de acuerdo con los incidentes o vulnerabilidades que a lo largo del análisis sobre los informes arrojados por la honeynet.

A continuación, se proponen algunos instructivos siguiendo lo antes indicado:

- Instructivo para empleo seguro de protocolos de red
- Instructivo para empleo seguro sobre servicios web
- Instructivo para uso de recursos compartidos

Instructivos para los servicios perimetrales:

- Instructivo elaboración y validación de reglas en el firewall
- Instructiva elaboración de ACL para filtrado de contenido web (Servicio Proxy)

Ejemplo Instructivo para empleo seguro sobre servicios web. (Ver Anexo C)

11.5 Arquitectura y estrategia Honeypots

“Un aspecto muy importante para tener en cuenta en la implementación de la red de honeynet además de la función que va a desempeñar, es determinar cuál será el lugar donde se ubicará en la red”[27].

“Existen distintas arquitecturas que se pueden diseñar dependiendo de los requerimientos y objetivos a conseguir, desde la más simple que sería el Honeypot de baja interacción simulando servicios básicos, pasando por crear varios Honeypots en máquinas virtuales que se están ejecutante en una misma maquina física, hasta complejas honeynet donde se despliegan un conjunto de Honeypots conectados entre sí y que son monitorizados y gestionados proactivamente. En este caso se va a manejar una red de Honeypots creados en un mismo equipo, pero serán de baja interacción. Sin embargo, conformaran una red de Honeypots de la manera más simple y básica posible”. Ibid,. p.89

11.6 Herramientas de seguridad interna y externa

Adicional a las herramientas convencionales tales como firewall, proxys, antivirus, se propone adicionar la red de honeynet como un ítem más al marco de tales herramientas, con el fin de aumentar en las PYMES la seguridad tanto a nivel interno como a nivel externo, es importante recordar la importancia de la seguridad perimetral, su monitoreo y que ataques se pueden presentar en la red, y con dichas herramientas los administradores de sistemas tendrán la suficiente destreza y conocimiento para afrontarlas haciendo uso de ellas.

12. DISEÑO DE DOCUMENTO PARA IDENTIFICACIÓN DE PERFILES DE INTRUSOS

12.1 PERFILES DE INTRUSOS

“A continuación, se nombrarán algunos perfiles los cuales serán tratados en el documento con el fin de realizar la categorización del ciberdelincuente según el tipo de ataque efectuado.

- Ciberterrorista
- Script Kiddies
- Crackers
- Desarrollador de virus

[27] RAMOS VARÓN, Antonio ángel. BARBERO MUÑOZ, Carlos A. GONZÁLEZ CAÑAS, Juan M. PI COUTO RAMOS, Fernando. SERRANO APARICIO, Enrique. Seguridad perimetral, monitorización y ataques en redes. Bogotá: Ra-ma, 2015. 204p.

- ❖ Atacante interno

12.1.1 Ciberterrorista: Se caracteriza por generar o provocar inestabilidad en los sistemas informáticos, crea incertidumbre sobre la operación y provoca fallas de las comunicaciones

Técnicas empleadas: Algunas de sus técnicas más usadas son

- Ataques electrónicos o armas de pulso electromagnético
- Ataques a las rede computacionales
- Ataques físicos

Ataques electromagnéticos o armas de pulso electromagnético: son estas armas las que aprovechan el poder de la energía electromagnética con el fin de afectar los sistemas informáticos.

Bombas Lógicas: permiten introducir código digital malicioso directamente en las ondas de transmisión, los resultados de este tipo de ataques son altamente negativos para los sistemas de información, puesto que pueden afectar la memoria electrónica, el software y hardware del sistema.

Ataques a las redes computacionales o virus informático: Este tipo de ataques cibernéticos están sustentados en el uso de programas de sistemas o código malicioso elaborado para ejecutar acciones puntuales en contra de los sistemas de información e informáticos, este tipo de ataques altera la seguridad del software y altera el funcionamiento de los programas residentes.

Ataques Físicos: Se refieren a todos aquellos ataques que se perpetran contra la infraestructura de los sistemas informáticos.

Ingeniería social: Consiste en la manipulación psicológica con el objetivo de obtener datos sensibles de los usuarios, tales como información confidencial o personal o que ejecuten cualquier tipo de acción que pueda beneficiar al ciberdelincuente.

Script Kiddies: Las herramientas usadas por estos ciberdelincuentes realmente son las existentes en internet, esto debido a que las usan personas que no cuentan con conocimientos en sistemas y las usan sin saber cómo es su funcionamiento, realmente estos son los más dañinos y que generan más números de ataques.

Crackers: el cracker busca hacer siempre reingeniería o ingeniería inversa, con el fin de que un programa licenciado pueda ser usado de forma gratuita, o busca también quitar la protección de licencia y tiempo de prueba en un programa" [28].

Las herramientas usadas son:

- **Bytecode viewer**
- **Codelogic**
- **Wintrasnlator**
- **Apktool**
- **Borg disassembler** (Ver Anexo D Tabla 4)

[28] CANO MARTÍNEZ, Jeimy J. Computación Forense Descubriendo los rastros informáticos. México: AlfaOmega, 2009. 329p

13. RECURSOS IMPLEMENTACIÓN DEL PROYECTO

La materia prima para usar para lograr la implementación de dicho proyecto es la búsqueda investigativa del tema los cuales permiten consolidar la conceptualización de los honeynet, fundamentándose en manuales, ensayos, videoclips e investigaciones académicas, pilares que fundamentaran la monografía. Para ello se respetarán las fuentes bibliográficas identificándolas correctamente con el finde evitar lagunas semánticas respecto a la investigación expuesta durante el proyecto.

14. ENFOQUE DE IMPLEMENTACIÓN DE HONEYNET COMO APOYO AL PLAN DE SEGURIDAD BASE PARA LAS PYMES

14.1 EXPLORACIÓN Y TIPIFICACIÓN DE CONCEPTOS DE UN HONEYNET A PARTIR DE LAS FUENTES INVESTIGATIVAS SELECCIONADAS

Un honeynet es un software o conjunto de computadores los cuales tiene como única función atraer o incitar a un ataque, ¿Cómo lo hacen?, emplean un comportamiento de un equipo en la misma red con la diferencia de que este simula ser vulnerable o débil ante cualquier tipo de ataque ejecutado sobre él.

El concepto de honeynet fue instaurado gracias a Lance Spitzner, en su proyecto honeynet con el objetivo de usarlo como un sistema de monitoreo de intrusiones cibernéticas. Durante estos últimos años se ha venido masificando el concepto y sus funciones, así como las mejoras que se le han realizado desde su base hasta versiones más robustas y complejas.

De una manera retrospectiva se puede indicar que los honeynet sirven para la recolección de información sobre cada uno de los ataques que se han cernido sobre él, con dicha información se pueden recrear e identificar las técnicas que fueron empleadas para el ataque y así poder prevenir futuros agresiones.

Otro de los veneficios o bondades del honeynet es que permite visualizar en tiempo real estos ataques, los cuales nos permitirá como se mencionó que técnicas se están empleando, pero también las herramientas, códigos, scripts, y que servicios están siendo vulnerados.

Otro aspecto importante que brinda el honeynet, es la disuasión a los atacantes a que selecciones otros elementos diferentes en la red, esto que quiere decir, pues que el atacante seleccionará el honeynet como si víctima y con ello se lograr mantener los demás elementos de la red como servidores, routers entre otros fuera del alcance de posibles ataques, esto activará la alarma y advertirá al administrador de sistemas que se está realizando un ataque sobre su red.

15. DATOS IMPORTANTES PARA TENER EN CUENTA

Es importante recordar que el honeynet no va a reemplazar los sistemas de seguridad que se tengan actualmente, es simplemente un nivel más de protección que se va a adicionar, ¿Qué es lo ideal?, contar con un sistema de firewall ya sea básico de acuerdo con el alcance que se ha tratado en el proyecto y que va arraigado a las PYMES, por lo tanto, se asume que cuentan con un sistema de seguridad perimetral, aunque sea básico.

El honeynet, se puede configurar en la zona LAN o DMZ, la zona LAN es donde residen todos los elementos de la red, tales como servidores, computadores, switchs, routers, impresoras de red etc. La DMZ es una zona de distención o también se le conoce como zona desmilitarizada, en esta zona van principalmente aquellos servicios que son empleados para publicaciones por medio de internet. El concepto igualmente usado es de una zona insegura a una zona segura.

De cierta forma, se puede afirmar que los honeynet son una variante de los sistemas de detección de intrusos tales como los IDS, sin embargo, radican en que su enfoque es más de recolección de información y se camuflan bajo el manto del engaño.

16. CONCLUSIONES

En el presente proyecto de monografía, se desarrolló una metodología propia la cual va a permitir identificar la efectividad de una red de honeynet aplicada a las PYMES. La metodología indicada en este trabajo está enfocada en las pautas para un correcto diseño e implementación de una red de honeynet, la cual cumple a cabalidad con los objetivos planteados.

Enmarcado en el desarrollo de la presente monografía se puede denotar lo siguiente:

Se analizo la efectividad de los esquemas de ataques informáticos mediante el uso de las herramientas que provee la red de honeynet, tales como reportes, creación de reglas parametrizables, indicación de origen del ataque, generación de perfiles criminalístico, subdivisión de los tipos de ataques que se generen en la red corporativa, identificación de vulnerabilidades o servicios con configuraciones incorrectas las cuales pueden ser explotadas para ataques tanto internos como externos, con ello se demostró la importancia que tiene su uso frente a la seguridad informatica.

Se implementaron los procedimientos de seguridad, gracias a los reportes obtenidos por la red de honeynet en los cuales se pueden observar los diferentes tipos de ataques que se realizaron sobre el ambiente honeynet, permitiendo como se indicó la elaboración del procedimiento gestión de incidencias.

Con los datos obtenidos del honeynet, se construyen instructivos de seguridad informatica permitiendo con ello un apoyo documental al sistema de gestión de seguridad de la información, esto es un soporte importante ante auditorias de sistemas, las cuales evalúan ciertos aspectos de la seguridad en las compañías.

Con el adelanto del actual trabajo de monografía se desarrollado el concepto de Honeypots y Honeynets permitiendo implementar una arquitectura de red de honeynet versátil mediante la implementación de una metodología la cual permito de una manera clara identificar los factores claves para el mejor modelado de red de honeynet permitiendo conceptualizar un ambiente de monitoreo controlado de la red y a su vez detectar cualquier evento inusual sobre la misma.

Finalmente, con la implementación de esta herramienta se brindará un factor adicional a las demás herramientas existentes, fortaleciendo la seguridad en los sistemas de las PYMES.

Para dar respuesta a la pregunta realizada en la investigación ¿Cómo contribuye el uso de tecnologías de honeynet en el mejoramiento de la ciber seguridad en las PYMES y que tan efectiva puede ser?

Proponiendo el empleo de una metodología diferente, propia y con fundamentos teóricos y metódicos con el fin de que la herramienta honeynet permita dar la información necesaria para conocer a los intrusos y sea herramienta colaborativa a los administradores de TI a determinar las posibles vulnerabilidades, para tener criterios para aplicar mejores estrategias de seguridad.

Por lo cual se puede decir que este trabajo ha cumplido con los objetivos y propuesta indicadas, y mostrando la importancia y significado a lo que se refiere a la seguridad en las redes corporativas.

Analizar la efectividad de los esquemas de ataques informáticos:

En el presente trabajo, se demostró cual efectivo puede ser los esquemas que el honeynet genera y como estos ayudaran a la creación de controles los cuales van a permitir consolidar contramedidas que ayudaran a proteger la red.

Tabla 1. Cuadro de Esquemas

Protocolo			Servicios	Sistema Operativo	Nom-Esquema	Categorización
TCP	**UDP**	**Puerto**				
X			80	All	Servicio Web	Alto
X			21	All	Servicio web	Alto
X			445	All	SMB (Servicio compartido de archivos)	Alto
X			3389	All	Conexiones remotas	Alto
Fuente Autor						

1. Implementar protocolo seguro https
2. Implementar protocolo seguro sftp
3. Actualizar la versión smb a smb3 o a su última versión
4. Utilización de VPN, doble autenticación, claves o password complejo o robusto, modificación del puerto por defecto 3389, implementar políticas de seguridad para el manejo de usuarios, implementar NLA y reglas de firewall.

Enunciar e implementar procedimientos de seguridad:

Estos esquemas serán el pilar para los procedimientos de seguridad que sin duda son parte importante en una administración de una red de sistemas, por ello es imprescindible emplear un sistema que apoye dando el insumo o resultados para la creación de dichos procedimientos como es el caso del honeynet. Importante resaltar que un procedimiento permitirá de una forma más genérica describir el estado actual de la seguridad en la red e identificar que subprocesos o actividades de seguridad serán requeridas más adelante.

A continuación, para aclarar un poco más el concepto de procedimiento se realizará la construcción de este a manera de base.

Ver Anexo E

De acuerdo con los procedimientos que se obtuvieron, se hace referencia a los instructivos de seguridad, pues es de vital importancia contar con los soportes necesarios cuando de auditorías se trata y más aún cuando se enfocan especialmente a la seguridad de sistemas y de redes. El honeynet con los reportes generados permitirán obtener indicadores e implementar mejoras si ha de ser necesario.

Elaborar instructivos de seguridad:

Los instructivos de seguridad serán detallados de acuerdo con la información dada por el honeynet y permitan realizar las actividades necesarias para mantener los sistemas y la red segura de posibles ataques o vulnerabilidades.

Ejemplo de instructivo de seguridad

Categorización de servicios

Proceder con la identificación de los puertos de cada servicio

Servicios:

IIS

SQL

Recursos Compartido SMB

FTP

Conexión por Terminal RDP

Otros Servicio: Usualmente se hace necesario usar puertos a un determinado servicio diferente de los anteriormente indicados, el rango de puertos es 65536 números, del 0 al 65535 obviando por supuesto los puertos por defecto de los servicios conocidos.

1. Identificación del servicio:

IIS (Internet Information Service): el puerto por defecto del IIS es el 80 esto corresponde a http,

Este puerto suele ser vulnerable y permite que atacantes se aprovechen del mismo

Implementación de seguridad para el puerto 80 IIS:

Identificación desde el honeynet - Evidenciar el ataque

Figura 26. Identificación de conexiones

Fuente el autor

Identificación de origen del Ataque:

Ataque Interno:

a. Si el ataque es de origen interno, procede con el bloqueo de la ip identificada, para ello se debe proceder en realizar el cambio de reglas en el Firewall.
b. Realizar el cambio de puerto usando https, esto quiere decir usar un certificado valido.
c. Mejorar la seguridad de los aplicativos webs para ello se debe validar con el área de desarrollo in-house si se cuenta con él, si el servicio es tercerizado, se debe hablar con el proveedor para corregir errores de seguridad.

Ataque Externo:

a. Es necesario al igual que se identificó en el ataque interno utilizar el protocolo seguro https y un certificado valido y vigente.

b. Si se observa reiterados ataques desde una misma ip realizar bloqueo por regla de firewall.

Implementación de seguridad para el puerto 21 FTP:

Identificación desde el honeynet - Evidenciar el ataque

Figura 27. Identificación conexiones

Fuente el autor

Identificación de origen del Ataque:

Ataque Interno:

a. Si el ataque es de origen interno, procede con el bloqueo de la ip identificada, para ello se debe proceder en realizar el cambio de reglas en el Firewall.
b. Realizar el cambio de puerto usando SFTP y emplear password más robustos.

Ataque Externo:

a. Es necesario al igual que se identificó en el ataque interno utilizar el protocolo seguro SFTP.
b. Si se observa reiterados ataques desde una misma ip realizar bloqueo por regla de firewall.
c. Evitar el empleo de usuarios anónimos sobre el servicio SFTP.

Se debe realzar los mismos pasos para los demás servicios identificados, se debe validar y analizar cada acción. Para ello es necesario que el área de sistemas apoye en cada una de las mismas.

Arquitectura propuesta para la red de honeynet:

En el proyecto se definió la posible arquitectura del honeynet dentro de la red en las PYMES. Empleando las mejores prácticas de seguridad para su puesta en marcha.

Es importante definir que el ambiente del honeynet debe interactuar con otras herramientas las cuales le van a permitir trabajar de una forma más optima y segura, entre estas herramientas se encuentran IDS, Antivirus y herramientas de monitoreo de red como wireshark o sniffers a si mismo con el soporte indiscutible de firewalls y proxys todas estas conformando un ambiente de seguridad perimetral óptimo.

Clasificación de Perfiles Criminalísticos:

Con la información suministrada por la red de honeynet, los esquemas, procedimientos e instructivos construidos durante el proceso de implementación, puesta en marcha y mantenimiento del honeynet se cuanta, con el insumo para la creación de los documentos de perfiles criminalísticos, los cuales serán de apoyo para identificar las herramientas y modus operandi de los atacantes.

17. GLOSARIO

HECKERS: Individuo que por manejar un amplio conocimiento en el área de sistemas e informática cuenta con un desempeño sobresaliente sobre el tema y tiene la capacidad de realizar todo tipo de actividades que lo pongan a prueba e ilícitas sobre los computadores.

BOTS: Programa informático que ejecuta tareas automáticas

CIBERSEGURIDAD: Área afín con la información y telemática dirigida a la seguridad de la información e infraestructura computacional

HONEYNET: Son arquitectura o software especial de un Honeypot de alta interacción que actúa en la red como señuelo

HONEYBOT: Honeypot de baja interacción basado en sistemas Windows

KASPERSKY LAB: Compañía Rusa en la cual se desarrollan software para el análisis y detección de virus

NMAP: Programa open source que permite efectuar rastreos de los puertos en un sistema de cómputo o red

LANCE SPITNER: Creador del modelo HoneyPot, experto en seguridad en investigación de amenazas cibernéticas, arquitectura de seguridad y conciencia y capacitación

PHISHING: Método de ingeniería social que emplean los delincuentes para obtener información de carácter confidencial, como nombres de usuarios, contraseñas bancarias o de correos entre otra

PYMES: Empresa pequeña o mediana

RANSOMWARE: Tipo de programa maligno que impide que los usuarios puedan acceder a sus sistemas o archivos personales y que exige un pago por su rescate.

SPEAR PHISHING: Tipo de estafa de correo electrónico dirigida que obtiene acceso no autorizado a los datos confidenciales

SERVICIO WEB: Tecnología basada en un conjunto de protocolos y estándares que permiten el intercambio de información entre aplicaciones

SERVICIO FTP: Servicio que permite la transferencia de datos

SPAM: Se refiere a correo basura, donde se difunde en la mayoría información de carácter publicitario enviado de manera masiva

TELNET: Comando que permite acceder a otra máquina para manejar de forma remota mediante el protocolo de red por el puerto 23.

PYME: Sigla que indica pequeña y mediana empresa, de acuerdo con la ley; en Colombia se entiende por micro donde se incluyen las famiempresas pequeñas y mediana empresas, toda unidad de explotación económica, realizada por persona natural o jurídica, en actividades empresariales, agropecuaria e industriales con un máximo de 200 empleados.

WIRESHARK: Software que ayuda en el análisis de protocolos de red, como es bajo licenciamiento GPL, existen muchos desarrolladores que lo están mejorando constantemente.

IDS: Software que permite la detección de intrusos a la red, funcionan automatizando procesos de monitorización de eventos que ocurren en una redo en un sistema. Luego dichos eventos son analizados, con el fin de detectar problemas de seguridad.

FIREWALL: Son sistemas de seguridad que conforman una parte vital de una red corporativa, están diseñados para denegar o permitir el acceso, en base a reglas que son configuradas en ellos a si mismo hace uso de otros criterios predefinidos.

ZENMAP: Herramienta de redes que permite el descubrimiento de puertos y servicios de un servidor o de cualquier dispositivo en la red.

18. BIBLIOGRAFÍA O REFERENCIAS

AGUDELO ACOSTA, Eibin Fabian, CHAPARRO MENDIVELSO, Miguel Ángel. Diseño e implementación de un HoneyPot para la empresa solocontrucciones SAS. Bogotá, 2013, 144p. Proyecto de grado (especialización en seguridad informática). Universidad Piloto de Colombia. Ingeniería.

Almeroth K., Puigjaner R., Shen S., Black J.P. (eds) NETWORKING 2005. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems. NETWORKING 2005. Lecture Notes in Computer Science, vol 3462. Springer, Berlin, Heidelberg.

Alexandria, Feb. 11 -- United States Patent for automated honeypot provisioning system has been issued to Level 3 Communications. This invention was developed by Bingham Skyler J and Shirley Mark R. The patent application number is 15/428,977. The International Patent Classification code is H04L 29/06 (20060101). Cooperative.

AMAYA GUTIÉRREZ, Camilo. Honeypots: alternativas para analizar códigos maliciosos. {En línea}. {21 enero 2013}.. Disponible en: (https://www.welivesecurity.com/la-es/2013/01/21/honeypots-alternativas-analizar-codigos-maliciosos/)

BOLAÑOS BOTINA, Jesús. Diseño de la arquitectura de seguridad perimetral de la red informática en la industria de licares del valle. 2018, p199. Proyecto de grado para optar el título de maestría en ingeniería. Universidad Autónoma de Occidente

BMCSOFTWARE ACTIVATE BUSINESS WHITH THE POWER OF I.T.. ITIL para las pymes. P8

CABALLERO QUEZADA, Alonso Eduardo. Hacking con Kali Linux Una perspectiva práctica. {En línea}. {Julio del 2019} disponible en: (http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf)

CALDERÓN GARCÉS, Andrés Mauricio, MARÍN VÉLEZ, juan Carlos. Modelo de gestión integral de TIC en procesos de producción de educación virtual. Santiago de Cali, 2011, 215p. Trabajo de grado para optar al título de magister en gestión de informática y telecomunicaciones. Universidad ICESI. facultad de Ingeniería Maestría en gestión de informática y telecomunicaciones.

CANO MARTÍNEZ, Jeimy J. Computación Forense Descubriendo los rastros informáticos. México: AlfaOmega, 2009. 329p.

Ceron, João Marcelo; Steding-Jessen, Klaus; Hoepers, Cristine; Lisandro Zambenedetti Granville; Cíntia Borges Margi.Sensors.Improving IoT Botnet Investigation Using an Adaptive Network Layer.; Basel Tomo 19, N.º 3, (Jan 2019).

Ciber incidentes | centro cibernético policial. {En línea}. {2019} disponible en: (https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico).

Colombia en Latinoamérica es el sexto país en ciberataques | tecnología | caracol radio. (En línea). {25 de octubre del 2019}. Disponible en: (https://caracol.com.co/radio/2018/04/11/tecnologia/1523464449_167083.html).

Data Center Security: Honey Pots and the Art of Deceiving Hackers. SQL Server Pro; Chicago (Nov 22, 2017).

Elempleo.com. Pymes, la base del mercado laboral. {En línea}. {9 de febrero 2018}. Disponible en: (https://www.elempleo.com/co/noticias/investigacion-laboral/pymes-la-base-del-mercado-laboral-5510).

¿Eres una pyme? Te enfrentas a estos riesgos de ciberseguridad. {En línea}. {2019} disponible en: (https://seguridad.prestigia.es/riesgos-de-ciberseguridad-en-pymes/).

ESTRELLA QUIJIJE, Gustavo Daniel. Diseño del prototipo de una HoneyPot virtual que permitirá mejorar el esquema de seguridad en las redes de la carrera de ingeniería en sistemas computacionales y networking. 2011 p370. Tesis de grado (Ingeniería en sistemas computacionales). Universidad de Guayaquil. Facultad de ciencias matemáticas y físicas.

FONSECA AMADO, Leidy Yulieth, LACOUTURE PLATA, Oscar Oscar. Plan de continuidad del negocio para pequeñas y medianas empresas decall center que usan la plataforma mitrol en Colombia – ARS Technology SAS. Bogotá, 2013, 143p. Trabajo de grado para optar al título de especialización en seguridad informática. Universidad Piloto de Colombia. Facultad de ingeniería . Programa Ingeniería de Sistemas.

F-Secure Corporation; Patent Application Titled "Detection of Coordinated Cyber-Attacks" Published Online (USPTO 20170180402). Computer Weekly News; Atlanta [Atlanta]12 July 2017: 1280p.

GÓMEZ FERNÁNDEZ, Luis. FERNÁNDEZ RIVERO, Pedro Pablo. Como implementar un SGSI según ISO/IEC 27001 y su aplicación en el esquema nacional de seguridad. Bogotá: AlfaOmega, 2019. 163p.

Hassan, Sharif; Guha, Ratan. Honeypots and the Attackers Bias..International Conference on Cyber Warfare and Security; Reading, (2018).

HEREDIA TERÁN, Carlos Mauricio. Diseño e implementación de una honeynet para la red de datos de la Universidad Nacional de Loja, utilizando software Libre. Ecuador. 2015, 108p. Tesis de grado. Universidad Nacional de Loja, Ecuador, Loja.

Honeypot. {En línea}. {19 de julio 2019}. Disponible en: (https://es.wikipedia.org/wiki/Honeypot)

Importancia de la seguridad informática en las pymes, Informática para empresas. {En línea}. {17 de Julio de 2018} Disponible en: (https://www.gadae.com/blog/seguridad-informatica-en-las-pymes/).

Endicott-Popovsky B., Narvaez J., Seifert C., Frincke D.A., O'Neil L.R., Aval C. (2009) Use of Deception to Improve Client Honeypot Detection of Drive-by-Download Attacks. In: Schmorrow D.D., Estabrooke I.V., Grootjen M. (eds) Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience. FAC 2009. Lecture Notes in Computer Science, vol 5638. Springer, Berlin, Heidelberg.

Ingeniería social: técnicas utilizadas por los ciberdelincuentes y como protegerse. {En línea }. {2019} Disponible en: (https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse).

Indian Applicants File Patent Application for Data Traffic Analysis Based Iot Detection Using Honeynet Da Classification Technique. Indian Patents News; New Delhi [New Delhi]25 Nov 2019.

Information Technology - Information Security; Study Findings from University of Ostrava Provide New Insights into Information Security (Causal Analysis of Attacks Against Honeypots Based On Properties of Countries).Computer Technology Journal; Atlanta [Atlanta]05 Sep 2019: 935p.

Kapil, Gayatri; Agrawal, Alka; Attaallah, Abdulaziz; Algarni, Abdullah; Kumar, Rajeev. Attribute based honey encryption algorithm for securing big data: Hadoop distributed file system perspective. et al .PeerJ Computer Science; San Diego (Feb 17, 2020). 259p.

LABERIS, Bill. Informática forense Colombia, 20 estadísticas reveladoras de cibercrimen. {En línea}. {12 de diciembre del 2017} Disponible en: (https://www.informaticaforense.com.co/20-estadisticas-reveladoras-de-cibercrimen/).

LEÓN CUERVO, Camilo Andrés. BONILLA DIAZ, María Alejandra. Análisis de ataques informáticos mediante Honeypots para el apoyo de actividades académicas en la universidad distrital Francisco José de Caldas. Bogotá, 2017, 84p. Proyecto de grado (optar por el título de ingeniero telemática). Universidad Distrital Francisco José de Caldas. Facultad Tecnológica Ingeniería en Telemática.

Lance Spitzner Joins the Attivo Networks® Advisory Board.Business Wire; New York [New York]29 Jan 2019.

LARA ROCHA, Miguel Ángel, LÓPEZ CANTE, Diana Carolina. Honeypot virtualizado para ambientes académicos y de investigación. Bogotá, 2013, 148p. Documento de proyecto de grado para optar por el título de especialista en seguridad informática. Universidad Piloto de Colombia Facultad de Ingeniería de Sistemas.

Las 5 herramientas más utilizadas por los crackers. {En línea}. {2019}. Disponible en: (https://hackerslatinos.com/las-5-herramientas-mas-utilizadas-por-los-cracker/)

LEXANDRIA, Va., Feb. 12 -- Level 3 Communications, Broomfield, Colorado, has been assigned a patent (No. 10,560,434, initially filed Feb. 9, 2017) developed by two co-inventors for an "automated honeypot provisioning system." The co-inventors are Skyler J. Bingham, Superior, Colorado, and Mark R. Shirley, Louisville, Colorado.

Ling, Xing; Rho, Yeonwoo; Ten, Chee-Woo. Predicting Global Trend of Cybersecurity on Continental Honeynets Using Vector Autoregression..The Institute of Electrical and Electronics Engineers, Inc. (IEEE) Conference Proceedings; Piscataway, (2019).

LOPEZCANO, George. Nuevo diccionario de la microcomputación. Impreso en Colombia, 1998. 747p

MARTÍNEZ CONTRERAS, Kevin David. Honeypot, hacia un protocolo de seguridad más eficiente y competitivo. 2018, 67p. Proyecto de grado (especialización en seguridad informática). Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería.

Mayorga, Franklin; Vargas, Javier; Alvarez, Edison; Martinez, H David. Honeypot Network Configuration through Cyberattack Patterns..The Institute of Electrical and Electronics Engineers, Inc. (IEEE) Conference Proceedings; Piscataway, (2019).

Noaman, Ahmed; Abdel-Hamid, Ayman; Eskaf, Khalid. A Novel Honeynet Architecture using Software Agents.The Institute of Electrical and Electronics Engineers, Inc. (IEEE) Conference Proceedings; Piscataway, (2019).

Novikova, Evgenia Elena,. Attacker Behaviour Forecasting Using Methods of Intelligent Data Analysis: A Comparative Review and Prospects. Doynikova,; Kotenko, Igor.Information; Basel Tomo 11, N.º 3, (2020): 168p.

Parra, Leonard David Lobo; Rico-Bautista, Dewar; Medina-Cárdenas, Yurley; Sanchez-Ortiz, Edgar Antonio. Alternate title: Defining of a practical methodology for the acquisition and analysis of digital evidence in the context of a research post mortem..Revista Ibérica de Sistemas e Tecnologias de Informação; Lousada N.º E18, (Feb 2019).

PAZMIÑO Mayra, AVILÉS Jorge, ABAD ROBALINO Cristina Lucia. Diseño preliminar de una honeynet para estudiar patrones de ataques en las redes de datos de la ESPOL. 2009, 4p. Ensayo (Grupo de visualización científica y sistemas distribuidos). Facultar de ingeniería en electricidad y computación. Escuela superior politécnica del litoral. Campus Gustavo Galindo.

Pymes, La base del mercado laboral | noticias elempleo.com. {En línea}. {2018}. Disponible en: (https://www.elempleo.com/co/noticias/nvestigación-laboral/pymes-la-base-del-mercado-laboral-5510).

¿Qué es ciberseguridad? | definición de ciberseguridad. {En línea}. {2016}. Disponible en: (https://www.economiasimple.net/glosario/ciberseguridad).

RAMOS VARÓN, Antonio ángel. BARBERO MUÑOZ, Carlos A. GONZÁLEZ CAÑAS, Juan M. PI COUTO RAMOS, Fernando. SERRANO APARICIO, Enrique. Seguridad perimetral, monitorización y ataques en redes. Bogotá: Ra-ma, 2015. 204p.

RAMOS VARÓN, Antonio Ángel. BARBERO MUÑOZ, Carlos A. GRIJALBA GONZÁLEZ, Jacinto. OCHOA, Martin Ángel. LÓPEZ BRO, Santiago. LAZO CANAZAS, Gabriel. Hacking practico en internet y redes de ordenadores. Bogotá: Ra-ma, 2015. 291p.

Repositorio Institucional Universidad de Oviedo. {En línea}. {2018}. Disponible en: (http://digibuo.uniovi.es/dspace/bitstream).

Revista Científica Dominio de las Ciencias. Las Tics en las empresas. {En línea}. {5 de enero 2018} disponible en: (https://dialnet.unirioja.es/descarga/articulo/6313252.pdf)

Riverbed Technology {En línea}. {2018}. Disponible en: (https://www.winpcap.org/)

Redwood O., Lawrence J., Burmester M. A Symbolic Honeynet Framework for SCADA System Threat Intelligence. In: Rice M., Shenoi S. (eds) Critical Infrastructure Protection IX. ICCIP 2015. IFIP Advances in Information and Communication Technology, vol 466. Springer, Cham.

Riebach S., Rathgeb E.P., Toedtmann B. (2005) Efficient Deployment of Honeynets for Statistical and Forensic Analysis of Attacks from the Internet. In: Boutaba R.,

Ren, Jianguo; Xu. A compartmental model to explore the interplay between virus epidemics and honeynet potency., Yonghong.Applied Mathematical Modelling; New York Tomo 59, (Jul 2018): 86p.

Rashidi, Bahman; Fung, Carol; Hamlen, Kevin W; Kamisinski, Andrzej. HoneyV: A virtualized honeynet system based on network softwarization..The Institute of Electrical and Electronics Engineers, Inc. (IEEE) Conference Proceedings; Piscataway, (2018).

SALINAS LA ROSA, Alberto. Inteligencia de negocio. Auditoría y control. Prototipo de herramienta de calidad de datos. Proyecto Fin de Carrera. Departamento de informatica. Universidad Carlos III de Madrid. 2010

SEIDLER, Oswald Kai, VOGELGESANG, Kay. {En línea}. {2020} disponible en: (https://www.apachefriends.org/es/index.html)

Sokol, P., Míšek, J. & Husák, M. Honeypots and honeynets: issues of privacy. EURASIP J. on Info. Security 2017, 4 (2017). https://doi.org/10.1186/s13635-017-0057-4.

Science - Applied Sciences; Findings from University of Brasilia Yields New Findings on Applied Sciences (Cybersecurity and Network Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection). Science Letter; Atlanta [Atlanta]01 Dec 2017: 692p.

TORREZ PEDRAZA, Julián Alejandro. Análisis de la influencia del fenómeno del ciberterrorismo en las dinámicas de seguridad de la unión europea. Bogotá, 2014, 55p. Proyecto de monografía (título de internacionalista en la facultad de relaciones internacionales). Universidad Colegio Mayor de Nuestra Señora del Rosario.

Triantopoulou, Stamatia; Papanikas, Dimitrios; Kotzanikolaou. An Experimental Analysis of Current DDoS attacks Based on a Provider Edge Router Honeynet., Panayiotis.The Institute of Electrical and Electronics Engineers, Inc. (IEEE) Conference Proceedings; Piscataway, (2019).

Turek, Tomislav; Kišasondi, Tonimir; Schatten, Markus. Domain Specific Honeytokens Based on Natural Language Processing – A Conceptual Model..Central European Conference on Information and Intelligent Systems; Varazdin : 207-211. Varazdin: Faculty of Organization and Informatics Varazdin. (2018).

V Kalpana, Sobhana Munnaneni and M Senbagavalli. Intellectual Property India Publishes Patent Application for 'Data Traffic Analysis Based Iot Detection Using Honeynet Da Classification Technique' Filed by. US Fed News Service, Including US State News; Washington, D.C. [Washington, D.C]30 Nov 2019.

Wang, Yu; Guo, Yi; Zhang, Liancheng; Peng . SWIM: An Effective Method to Perceive Cyberspace Situation from Honeynet., Tianqiang.The Arabian Journal for Science and Engineering. Section B, Engineering; Heidelberg Tomo 43, N.º 12, (2018).

Xuan Dau Hoang; Nguyen, Quynh Chi. Botnet Detection Based On Machine Learning Techniques Using DNS Query Data..Future Internet; Basel Tomo 10, N.º 5, (2018): 43. DOI:Future Internet 2018, 10(5), 43p.

Yang, Li; Shi, Leyi; Feng, Haijie A Game-Theoretic Analysis for Distributed Honeypots..Future Internet; Basel Tomo 11, N.º 3, (Mar 2019).

Zhuge J., Holz T., Han X., Song C., Zou W. (2007) Collecting Autonomous Spreading Malware Using High-Interaction Honeypots. In: Qing S., Imai H., Wang G. (eds) Information and Communications Security. ICICS 2007. Lecture Notes in Computer Science, vol 4861. Springer, Berlin, Heidelberg.

ANEXO A

Tabla 2. Plantilla de Indicadores

Objetivo		
Métrica		
Indicador		
Frecuencia		
Formula		
Mediciones	Fecha:	Valor:
	Fecha:	Valor:
	Fecha:	Valor
	Fecha:	Valor

Fuente: GÓMEZ FERNÁNDEZ, Luis. FERNÁNDEZ RIVERO, Pedro Pablo. Como implementar un SGSI según ISO/IEC 27001 y su aplicación en el esquema nacional de seguridad. Bogotá: AlfaOmega, 2019. 163p

ANEXO B

Indicador de la incidencia

Fecha de notificación: __/__/__/

Tipo de incidencia/vulnerabilidad

Información afectada:

Descripción detallada de la incidencia /vulnerabilidad

Fecha y hora en que se produjo la incidencia/vulnerabilidad

Lugar en que se produjo la incidencia / vulnerabilidad

Persona que realizo la comunicación

Fdo.: _____ Departamento: _____

A completa por el responsable del sistema

Efectos que puede producir

Acciones para tomar:

Acciones realizadas:

Fecha de resolución de la incidencia o vulnerabilidad:

Fdo.: _____ Fecha.: _____

ANEXO C

Tabla 3. Control de modificaciones

Rev. Nr.	Fecha	Modificaciones a la versión
0		
1		
2		
3		
4		

Contenido

1. Objetivo

Indicar las instrucciones, políticas y normas respecto a las mejores prácticas para el uso de servicios web, así como la implementación.

2. Alcance

Lograr establecer las normas, políticas e instrucciones para la buena implementación de servicios web, así como el uso de estos u otros servicios que se requieran emplear en la PYME.

3. Definiciones

Software: Programas para computadoras. Son las instrucciones responsables de que el hardware realice su tarea hablando propiamente del pc.

Hardware: Conjunto de componentes de carácter físico que componen la parte de una computadora tanto interna como externa.

Protocolos de Red: Clase de estructura o sistema que cuenta con un patrón determinado

Puertos de Red: Un puerto de red es un punto final a una conexión lógica y el medio por el que un programa cliente se comunica con un programa específico en una computadora o una red.

Firewall: Sistema diseñado para prevenir el acceso no autorizado y permitir comunicaciones autorizadas.

Virus: "Programa de computación diseñado como broma o sabotaje que se copia a sí mismo, para lo cual se adjunta a otros programas y lleva a cabo operaciones indeseables y en ocasiones dañinas"[29].

Antivirus: Herramienta para detector o eliminar virus informáticos.

Incidente: Se refiere a cualquier suceso que no forma parte de la operación básica de un servicio y que causa, o puede ocasionar, una fluctuación o una reducción de calidad en la operación del servicio[30].

Interrupción no planificada de un Servicio de infraestructura o reducción en la Calidad de un Servicio de infraestructura. También lo es el Fallo de un Elemento de Configuración que no ha impactado todavía en el Servicio[23].

Cambio: Adición, modificación o eliminación de algo que podría afectar a los Servicios de infraestructura, el cual debería incluir todos los Servicios de infraestructura, Elementos de Configuración, Procesos, Documentación etc.[31].

Problema: Causa subyacente, aún no identificada, de una serie de incidentes o un incidente aislado de importancia significativa[32].

Requerimiento: Una declaración o solicitud formal de un servicio el cual no interrumpe la operación y que no afecta el proceso que lo requiere.

Integridad: Se relaciona con la precisión y completitud de la información, así

---

[29] LOPEZCANO, George. Nuevo diccionario de la microcomputación. Impreso en Colombia, 1998. 691p

[30] BMCSOFTWARE ACTIVATE BUSINESS WHITH THE POWER OF I.T.. ITIL para las pymes. P8

[31] BMCSOFTWARE ACTIVATE BUSINESS WHITH THE POWER OF I.T.. ITIL para las pymes. P8

[32] BMCSOFTWARE ACTIVATE BUSINESS WHITH THE POWER OF I.T.. ITIL para las pymes. P8

como a su validez de acuerdo con los valores y expectativas del negocio.

Disponibilidad: Se refiera a que la información esté disponible cuando sea requerida por los clientes o procesos del negocio en cualquier momento.

4. Metodología

4.1. Roles y Responsabilidades.

Esta sección lista los roles involucrados en este proceso y las responsabilidades asociadas a estos teniendo en cuenta:

- Las responsabilidades incluyen, pero no se limitan a aquellas descritas para cada rol.
- Los roles son entendidos como agrupaciones de ejecutores de actividades, no como cargos puntuales dentro de la organización del equipo de trabajo establecida.
- Un rol puede ser desempeñado entre varios funcionarios.
- Un funcionario puede desempeñarse o verse involucrado en varios roles.

Desarrollador.

Es la persona o grupo encargado del desarrollo in-house de los servicios web.

Analista de Infraestructura.

Es el encargado de administrar y operar la infraestructura de los Data Center como servidores, equipos de comunicaciones garantizando su correcto funcionamiento.

Adicionalmente será la persona que recibirá y analizará los requerimientos para la implementación de los servicios web sobre los servidores. Deberá garantizar las buenas prácticas en temas de seguridad, así como selección de mejores estándares para implementaciones web.

Usuarios Internos: Son cada uno de los colaboradores que conforma la compañía.

4.2. Políticas

Uso Puertos de red seguros.

Dentro de la operación de infraestructura las políticas de buenas prácticas para la implementación y configuración de los servicios web son las siguientes:

Selección de puertos seguros:

Puertos HTTPS: De acuerdo con los análisis determinados por la red de honeynet, se identificó que el puerto http es vulnerable a todo tipo de ataques como scripts meta exploits, ataque de denegación de servicios entre otros. Para contrarrestar esta vulnerabilidad se recomienda el empleo de puertos seguros como https.

Puertos innecesarios: Es importante validar que puertos no son requeridos en los servidores y desactivarlos o bloquearlos mediante el uso de reglas en el firewall, algunos de estos puertos pueden ser:

Configuración de puertos de red y servicios web/uso de internet:

1. Identificar los puertos seguros tales como https, sftp, ssh, para las conexiones terminal se recomienda emplear el servicio de terminal server.

2. Para la implementación de los servicios web sobre IIS (Internet Information Services). Se recomienda usar las últimas versiones, aplicar mejores prácticas para la configuración de los sitios:

    a. A nivel de desarrollo, es necesarios que de esta área se apliquen las mejores prácticas de seguridad en cuanto al manejo del código, para la implementación del IIS se recomienda la siguiente parametrización:

        i. Estructura de sitios

            1. Crear la carpeta WEBSITES: dentro de esta se tendrán todos los sitios a crear.

            2. Crear carpeta WEBSERVICES: Aquí se encontrarán los sitios solo-referentes a servicios web.

            3. Luego de tener los sitios y webservices definidos se procede con la creación estructural del sitio:

                a. Manejar siempre los sitios por nombre, para ello en el DNS se deberá crear, el nombre del sitio de igual manera será creado el host con la ip interna del sitio para que este sea llamado directamente al nombre.

b. Configurar el sitio para que trabaje sobre el puerto https, para ello se selecciona el puerto en la configuración del sitio y se despliega la selección del certificado valido SSH.

c. Purgar los pools de aplicaciones, y programarlos para que estos se refresquen cada cierto tiempo.

d. Los pools de aplicaciones deben estar siempre con el framework actualizado.

e. Configurar la cache de los sitios para que estos sean óptimos al cargar, esto se hace en las propias configuraciones del IIS

3. **Configuración de reglas en el firewall:** Se debe prestar cuidado a la hora de establecer las reglas pertinentes en el firewall corporativo. Para ello se debe:

    a. Realizar la correcta configuración de las zonas en los firewalls o el firewall.

    b. Identificar los puertos a bloquear y a permitir. Esto depende del servicio a consumir o a consultar.

    c. Creación de grupos de servicios, segmentos de red entre otros, esto con el fin de optimizar el uso de las reglas y mejorar la creación de estas.

    d. Configuración de filtrado de contenido en el servicio de proxy, esto es importante para el control de la navegación de los usuarios.

5. Distribución

Este instructivo deberá estar sujeto a las regulaciones La distribución de este instructivo deberá estar regulada en los correspondientes procedimientos que maneje el SGS de cada PYME - Control de Información Documentada.

ANEXO D

Tabla 4. Algunos tipos de atacantes y sus motivaciones

Motivaciones	Ciberterrorista	Script Kiddies	Crackers	Desarrolladores De virus	Atacante interno
Reto				X	X
Ego		X	X	X	
Espionaje				X	X
Ideología	X				
Dinero			X	X	X
Venganza	X	X		x	X

Algunos tipos de atacantes y sus motivaciones. Adoptado de: Furnell, S. 202, p. 55

1. Crear los diferentes tipos de escenarios en el software KF Sensor
2. Configurar los diferentes servicios según el posible perfil del atacante
3. Verificar las alertas por la red honeynet
4. Identificar que escenario tiene el más alto número de ataques e identificar el perfil correspondiente
5. Aplicar las acciones necesarias para evitar los ataques con la información obtenida.

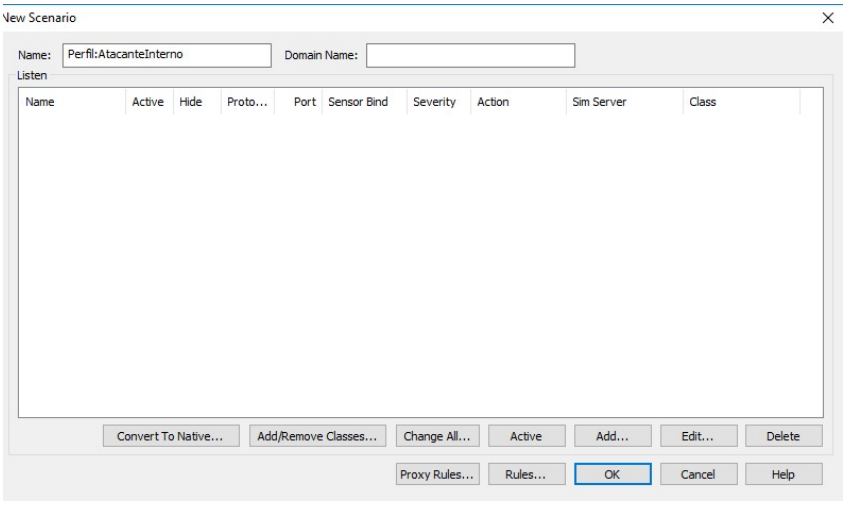
A continuación, se realizar un ejemplo de cómo realizar la caracterización del perfil del atacante.

Ejemplo perfil atacante interno:

1. Crear el escenario para el perfil seleccionado en este caso perfil Atacante Interno
2. Crear los servicios y asignación de puertos para identificación del perfil
3. Revisión del sensor de eventos e identificación del ataque.

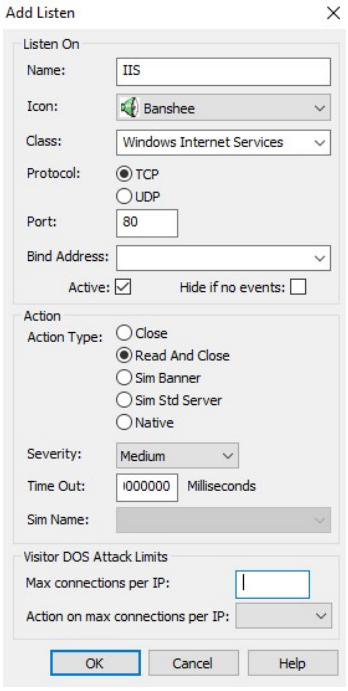
A continuación, se indica el soporte fotográfico de las acciones anteriores, en la fig. 28, 29, 30, 31, 32, 33 y 34.

Figura 28. Creación de Escenario Perfil atacante



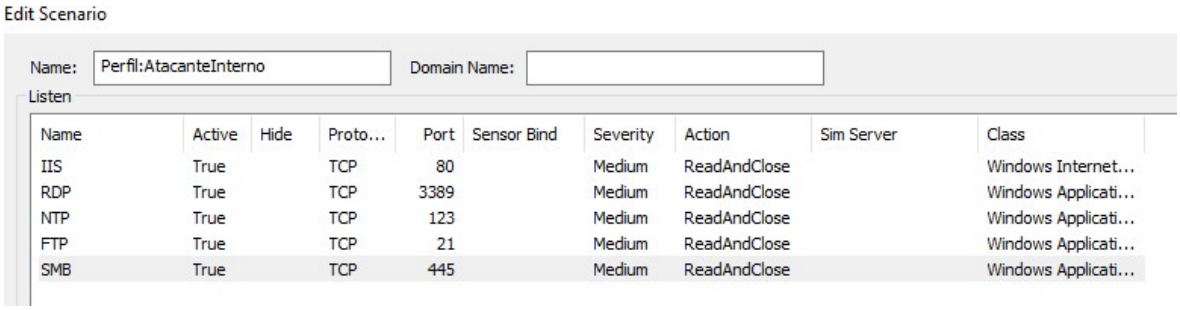
Fuente el autor

Figura 29. Creación de servicios y puertos para el escenario y perfil indicado



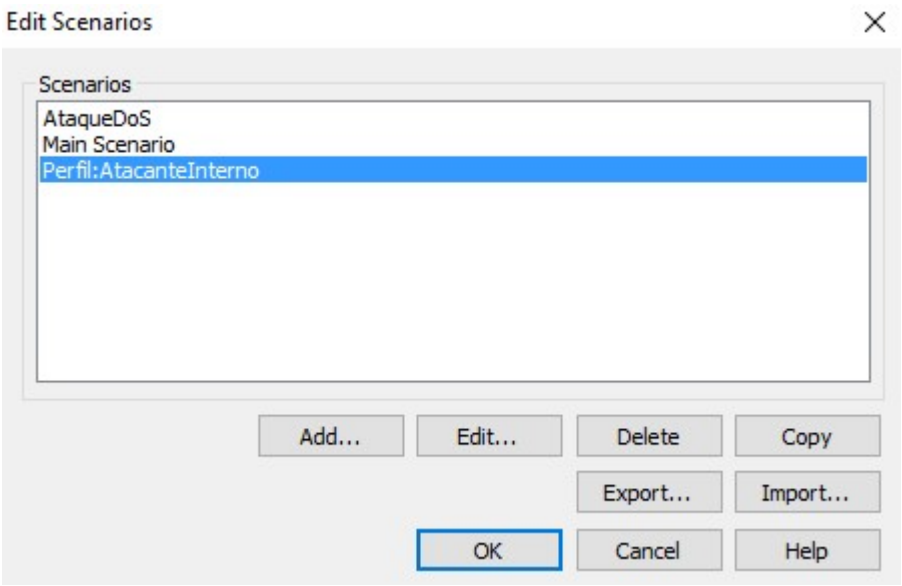
Fuente el autor

Figura 30. Servicios y puertos creados para el perfil Atacante Interno



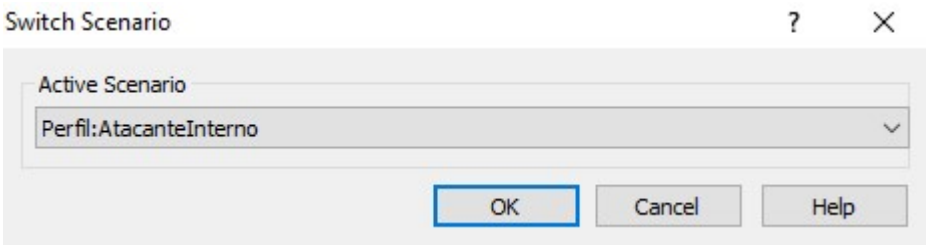
Fuente el autor

Figura 31. Escenario finalizado - Perfil Atacante Interno



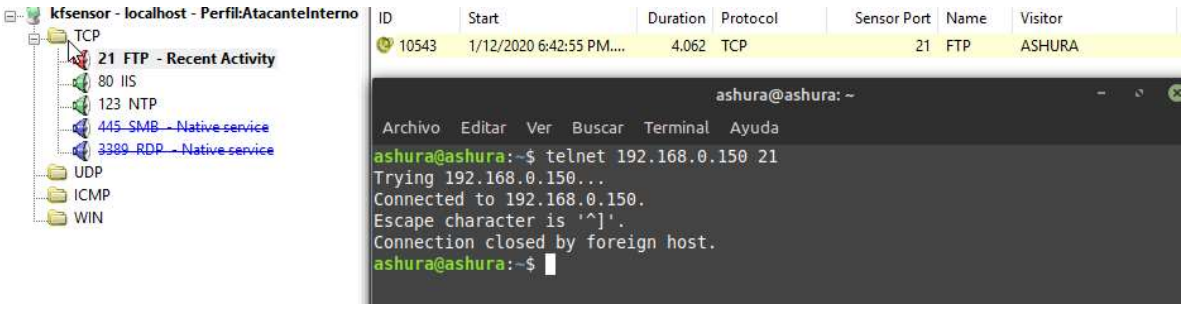
Fuente el autor

Figura 32. Cambio al perfil Atacante Interno



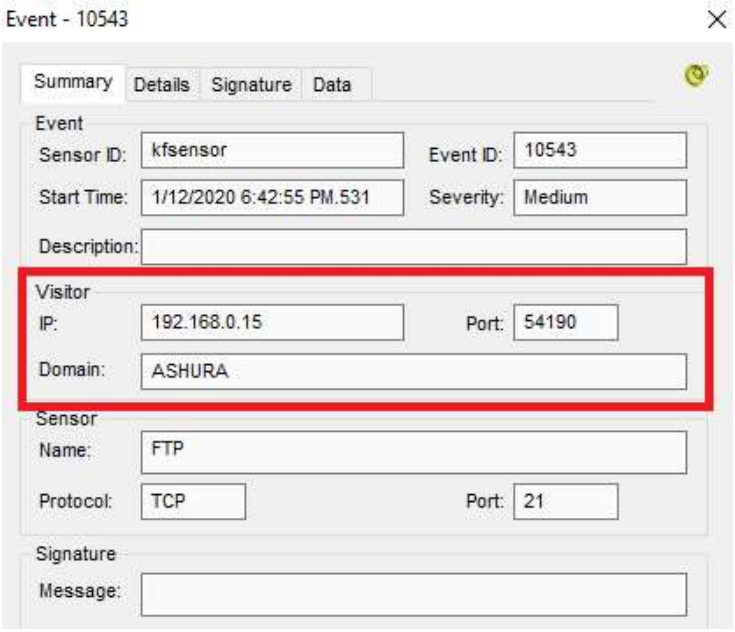
Fuente el autor

Figura 33. Simulación de ataque para generación de eventos



Fuente el autor

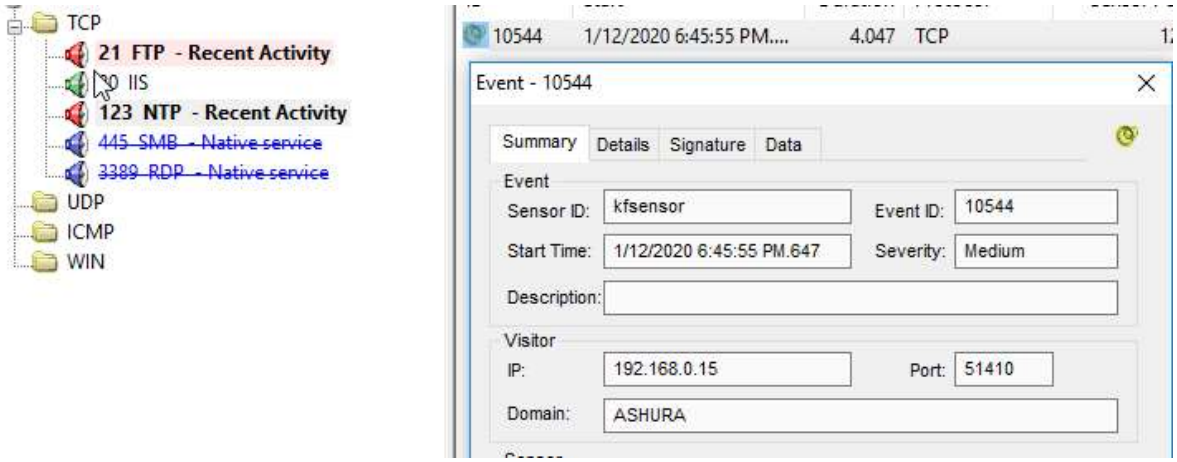
Figura 34. Revisión del evento e identificación si se trata de un ataque interno



Fuente el autor

Para identificar si se trata de un ataque interno se verifica la ip origen, en este caso se puede saber que el ataque en efecto provino de un pc de la misma red, como se observa en la fig. 35.

Figura 35. Identificación del origen



Fuente el autor

ANEXO E

Tabla 5. Control de modificaciones

Rev. Nr.	Fecha	Modificaciones a la versión
0		Aprobación del documento.
1		Inclusión de incidente, cambio y requerimiento en el glosario de términos.

Contenido

1. Objetivo y Alcance

2. Conceptos y Abreviaturas

3. Responsabilidad y Funciones

4. Descripción - Metodología

5. Distribución

6. Referencias

1. Objetivo y Alcance

Reglamentar los procedimientos necesarios para determinar y proporcionar la infraestructura tecnológica con las respectivas medidas de seguridad para la red de la compañía.

Toda la infraestructura tecnológica de la empresa que se relacione con el cumplimiento de los requisitos que afecten la conformidad con los requisitos del servicio.

2. Conceptos y Abreviaturas

Cambio: adición, modificación o eliminación de algo que podría afectar a los servicios de infraestructura. El Alcance debería incluir todos los Servicios de infraestructura, Elementos de Configuración, Procesos, Documentación etc.[33].

[33] BMCSOFTWARE ACTIVATE BUSINESS WHITH THE POWER OF I.T.. ITIL para las pymes. P8

Cumplimiento: tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas[34].

Data Center: centro de cómputo, centro de proceso de datos, es una instalación empleada para albergar los sistemas de información y sus componentes asociados, como las telecomunicaciones sistemas de almacenamiento e infraestructura en general[35].

Disponibilidad: se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas[36].

Efectividad: Esta se relaciona a la relevancia de la información y pertinente a los procesos del negocio, y se proporcione de una manera acertada, correcta, consistente y disponible.

Eficiencia: Reside en que la información sea formada con el óptimo (más productivo y económico) uso de los recursos.

Equipo activo: Dispositivo físico que hace parte de la infraestructura tecnológica de la compañía.

HelpDesk: soporte para los usuarios mediante una atención eficaz y personalizada. Incluye actividades de capacitación, formación, suministros y atención de requerimientos o incidentes informáticos tanto hardware como software.

Incidente: Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad en la operación del servicio.

---

[34] Repositorio Institucional Universidad de Oviedo. {En línea}. {2018}. Disponible en: (http://digibuo.uniovi.es/dspace/bitstream)

[35] FONSECA AMADO, Leidy Yulieth, LACOUTURE PLATA, Oscar Oscar. Plan de continuidad del negocio para pequeñas y medianas empresas decall center que usan la plataforma mitrol en Colombia – ARS Technology SAS. Bogotá, 2013, 143p. Trabajo de grado para optar al título de especialización en seguridad informática. Universidad Piloto de Colombia. Facultad de ingeniería . Programa Ingeniería de Sistemas

[36] CALDERÓN GARCÉS, Andrés Mauricio, MARÍN VÉLEZ, juan Carlos. Modelo de gestión integral de TIC en procesos de producción de educación virtual. Santiago de Cali, 2011, 215p. Trabajo de grado para optar al título de magister en gestión de informática y telecomunicaciones. Universidad ICESI. facultad de Ingeniería Maestría en gestión de informática y telecomunicaciones.

Interrupción no planificada de un servicio de infraestructura o reducción en la Calidad de un Servicio de infraestructura. También lo es el Fallo de un Elemento de Configuración que no ha impactado todavía en el servicio.

Integridad: "Engloba los conceptos de completitud, exactitud y celeridad para asegurar que los datos son completos, correctos y oportunos"[37]

Intranet: Sistema de información WEB Interno.

Red corporativa: Conjunto de dispositivos activos y pasivos destinados para la comunicación y transferencia de información en un área local establecida.

Router: Dispositivo de Red que permite interconectar redes o diferentes segmentos de red (Vlan) de una misma área local.

Servidor: Equipo de cómputo con características robustas capaz de administrar y gestionar servicios de equipos clientes en una red corporativa.

Storage: Servidor de almacenamiento masivo de información

Switch: Dispositivo de red que permite interconectar los hosts finales mediante direccionamiento físico.

Vlan: Red de área local virtual, utilizado para segmentar una red de área local y crear redes lógicamente independientes.

[37] SALINAS LA ROSA, Alberto. Inteligencia de negocio. Auditoría y control. Prototipo de herramienta de calidad de datos. Proyecto Fin de Carrera. Departamento de informatica. Universidad Carlos III de Madrid. 2010 p135

3. Responsabilidad y Funciones

Tabla 6. Responsabilidad y Funciones

GG	Gerente General
JI	Jefe de Infraestructura
PROV	Proveedor de Servicios
HD	Helpdesk
F	Cualquier funcionario

R	Responsabilidad principal
A	Autoriza
E	Elabora / Ejecuta
I	Es informado
Fuente: el autor	

Es responsabilidad del Jefe de Infraestructura con la debida autorización de Gerencia General gestionar, planear y proporcionar la infraestructura tecnológica necesaria para el cumplimiento de las necesidades de los clientes y de los objetivos del negocio según las directrices corporativas establecidas bajo los lineamientos de la dirección de infraestructura y soporte.

El Jefe de Infraestructura debe autorizar y delegar funciones al grupo de trabajo para realizar revisiones y programación de los mantenimientos preventivos a la infraestructura tecnológica, garantizando y controlando la funcionalidad y estabilidad de los elementos tecnológicos de la compañía.

Así mismo es responsabilidad del Jefe de Infraestructura gestionar todos “los equipos activos que hacen parte de la infraestructura tecnológica”[38] delegando y autorizando

[38] BOLAÑOS BOTINA, Jesús. Diseño de la arquitectura de seguridad perimetral de la red informática en la industria de licares del valle. 2018, p199. Proyecto de grado para optar el título de maestría en ingeniería. Universidad Autónoma de Occidente

funciones para realizar las actividades de configuración, actualización, seguridad y atención de solicitudes; como se contempla en el presente documento.

4. Descripción - Metodología

Tabla 7. Descripción - Metodología

RESPONSABILIDAD				ACTIVIDAD
R	**A**	**E**	**I**	**GESTIÓN Y PLANEACIÓN DE INFRAESTRUCTURA TECNOLÓGICA**
JI	GG	JI	GG	El jefe de infraestructura teniendo en cuenta las directrices corporativas y las indicaciones de la dirección de infraestructura planteara la infraestructura tecnológica necesaria para garantizar la satisfacción del cliente y los objetivos de negocio necesarios para una buena alineación estratégica así mismo como velar y garantizar la seguridad informática tanto dentro de la compañía como por fuera.
JI	GG	JI	GG JI AI HD	El jefe de infraestructura teniendo en cuenta las directrices corporativas y las indicaciones de la dirección de infraestructura, proporcionaran los recursos necesarios para la administración de la infraestructura tecnológica, garantizando la conformidad con los requisitos del cliente y el soporte necesario a todos los Core business de la compañía. La planeación de la infraestructura tecnológica se tendrá alineada a los siguientes aspectos: • Infraestructura central DataCenter (servidores, equipos de comunicaciones, etc.). • Soporte eléctrico (ups, planta eléctrica). • Hardware (computadores de operación, impresoras, etc.). • Servicios compartidos (licenciamiento antivirus, seguridad perimetral, soportes de fábrica, licenciamientos office, etc.). • Seguridad en los sistemas, redes y software Dentro la planeación de infraestructura los criterios a evaluar en cada uno de los anteriores aspectos son: 1. Crecimiento organización.

				2. Disponibilidad. 3. Escalabilidad. 4. Renovación tecnológica. 5. Nuevos Servicios.
R	**A**	**E**	**I**	**REVISIONES PROGRAMADAS**
JI	JI	JI AI HD	JI AI HD	Dentro de las actividades para mantener la infraestructura tecnológica, se realizan revisiones periódicas que permiten controlar el buen funcionamiento y estabilidad del sistema físico y tecnológico de la compañía.
R	**A**	**E**	**I**	**Revisión de servicio web**
JI AI	JI	F	JI AI HD F	La revisión de buenas prácticas para el uso de los servicios web debe ser manejada en conjunto del área de tecnología y de desarrollo, con el fin de aplicar las mejores formas de implementación tanto del desarrollo web como de la parte de tecnología e infraestructura, con el objetivo de mantener una seguridad estable y congruente con los servicios. Se deben implementar todos los protocolos seguros sobre cada servicio, esto será tenido en cuenta de acuerdo a los resultados obtenidos por el honeynet, ya que según el tipo de ataque se podrá identificar que protocolo fue comprometido.
R	**A**	**E**	**I**	**Revisión reglas de firewall**
AI HD	JI	HD AI	JI AI HD	En atención a lo determinado o detectado por el honeynet, se debe mejorar o actualizar las reglas en los firewalls de la compañía, así mismo realizar siempre la documentación de estas con el fin de identificar para que fueron creadas, para que servicios y cuáles fueron los objetivos para aplicarlas
R	**A**	**E**	**I**	**MANTENIMIENTOS SERVICIOS WEB**
JI AI	JI	JI AI	JI AI HD	El jefe de infraestructura o a quien delegue, programara los mantenimientos preventivos necesarios para mantener la infraestructura tecnológica en conformidad con los requisitos del servicio y la producción, según se

				dispone en el MED CO-FO-INF-0045 Cronograma de actividades de Infraestructura.
R	**A**	**E**	**I**	
R	**A**	**E**	**I**	
AI HD	JI	AI HD PROV	JI AI HD	
R	**A**	**E**	**I**	**GESTIÓN EQUIPOS ACTIVOS** **Equipos Activos de infraestructura tecnológica**
JI AI	JI	JI AI HD	JI AI HD	El jefe de infraestructura o quien delegue, deberá gestionar todos los equipos activos que hacen parte de la infraestructura tecnológica, contemplando los siguientes aspectos: • Características del equipo activo • Periodicidad de cambio de contraseñas (cuando aplique). • Control de cambios. • Reporte de incidentes. • Mantenimientos preventivos. • Mantenimientos correctivos. • Responsable del equipo. • Observaciones generales.
R	**A**	**E**	**I**	**Configuración Equipos**
HD	JI	HD	JI AI HD F	El asistente HelpDesk será el encargado de la preparación y configuración de los equipos, y portátiles teniendo en cuenta lo establecido en los documentos de implementación.
R	**A**	**E**	**I**	**Instalación de Aplicaciones**
AI	JI	HD	JI	Todo software instalado en los equipos de cómputo de la empresa debe estar relacionado en el documento Matriz

HD		AI	AI HD F	de Rol de Usuarios, el cual debe contar con la aprobación del director de área de cada unidad de negocio.
R	**A**	**E**	**I**	**Control de actualizaciones**
HD	JI	AI HD	JI AI HD F	Todas las actualizaciones en los equipos de cómputo deberán estar deshabilitadas, asegurando la disponibilidad de la información, y únicamente en cada mantenimiento preventivo se deberán actualizar, validando su funcionamiento con el usuario final.
R	**A**	**E**	**I**	**Seguridad Perimetral y Antivirus**
JI AI	JI	AI	JI AI HD	Los equipos de cómputo deben contar con software de antivirus con la última actualización de seguridad que permita prevenir y eliminar cualquier malware. Este realiza análisis diariamente buscando vulnerabilidades y detectando anomalías que puedan afectar la seguridad.
JI AI	JI	AI	JI AI	Se cuenta con un firewall físico que monitorea el tráfico de red y en el cual se define políticas de acceso mediante reglas de seguridad.
R	**A**	**E**	**I**	**ATENCIÓN DE INCIDENTES DE SEGURIDAD**
JI AI HD	JI	JI AI HD F	JI AI HD F	Todo evento o incidente que afecte la integridad, disponibilidad y seguridad de la información deberá quedar registrado en la plataforma en la plataforma para tal fin, en la cual se deberá mantener el detalle y solución de esta.