ESTUDIO SOBRE LA IMPORTANCIA DE LOS SISTEMAS DE MONITOREO DE REDES DE DATOS EN LAS EMPRESAS

JONHATAN ALEXANDER SUESCUN PINEDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA

MEDELLIN 2019

ESTUDIO SOBRE LA IMPORTANCIA DE LOS SISTEMAS DE MONITOREO DE REDES DE DATOS EN LAS EMPRESAS

JONHATAN ALEXANDER SUESCUN PINEDA

Monografía presentada(o) como requisito parcial para optar al título de:
Especialista en seguridad informática

Director (a):
Ingeniera Yolima Esther Mercado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA

MEDELLIN 2019

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

DEDICATORIA

Esta Monografía va dedicada a mis padres, gracias a ellos por formarme como persona y como profesional. No me quiero imaginar que sería de mí sin la ayuda y el apoyo incondicional que ellos me ofrecieron siempre.

Muchas Gracias:

Padre, Carlos Alberto Suescun tascon

Madre, Ana Isabel pineda Jaramillo.

CONTENIDO

Pág

LISTA DE FIGURAS

Pág

LISTA DE TABLAS

Pag

LISTA DE ANEXOS

Pag

TITULO

ESTUDIO SOBRE LA IMPORTANCIA DE LOS SISTEMAS DE MONITOREO DE REDES DE DATOS EN LAS EMPRESAS

INTRODUCCION

A medida que vamos evolucionando tecnológicamente, la tecnología va tomando un crecimiento el cual busca simplificarle actividades o procedimientos a los seres humanos, como por ejemplo la interconexión con otras personas sin importar la distancia, educación a distancia y transacciones bancarias. Actividades que anteriormente el ser humano no gozaba de las actividades mencionadas.

En el siguiente documento vamos hacer referencia a la importancia de los sistemas de monitoreo en las empresas, definiendo el tipo de ataques informáticos que afectan directamente las redes en el mundo informático, con el fin de dar a conocer al lector una corta definición de los respectivos ataques.

Además de dar definiciones, en el documento encontramos un resumen de ataques informáticos que afectan directamente las redes y la prestación del servicio de las empresas. Tanto a nivel global y regional (Colombia), con el fin de dar a conocer que los ataques informáticos a las redes empresariales, es una problemática que también toca nuestro país y que las empresas colombianas no están exentas de algún tipo de ataque informático a su infraestructura.

De acuerdo a diversos ataques hacía las redes de las empresas, en el documento vamos a encontrar una serie de tablas; las cuales nos muestra un historial de ataques informáticos con su respectiva ubicación geográfica y las pérdidas económicas ocasionadas por intrusiones, virus o denegación de servicios.

Por último, se muestra en el documento, una variedad de software de monitoreo tanto licenciados como libres existentes en el mercado, con el fin de que el lector conozca las diversas alternativas en el tema de software de monitoreo que podrían ser implementados en las empresas con el fin de disminuir la probabilidad de sufrir ataques informáticos como virus, posibles intrusiones y denegación de servicios. Convirtiéndose en una empresa sólida en el tema de seguridad informática.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCION

Para entrar en sintonía con el tema, un sistema de monitoreo es la combinación de hardware y software encargado de analizar todo el tráfico que circula por una red empresarial compuesta por diferentes dispositivos de red aplicando el término de gestión de red.

Los sistemas de monitoreo implementado en una empresa, sirve para realizar constante seguimiento al tráfico que circula en la empresa, teniendo la ventaja de detectar tráfico malicioso que pueda ocasionar diferentes desastres tecnológicos perjudiciales al normal funcionamiento de la infraestructura.

Según un artículo del periódico el tiempo[1], Es un problema que Colombia sea el tercer país de la región con más ataques cibernéticos en donde el sector financiero registró en 2014 el 14,34 por ciento de los ataques realizados en Latinoamérica, se manifiestan para el año 2015 la cifra se incrementó hasta 75,29 por ciento; es decir, más de seis millones de ataques por día; en segundo lugar se encuentra el sector gubernamental con un total de 925.000 ataques por día, representando el 10,56 por ciento de las arremetidas cibernéticas, seguido por el sector de comunicaciones que representa el 8,41 por ciento equivalente a 737.200 ataques por día que se manifiestan al interior de los departamentos de IT de la empresa, porcentajes los cuales podrían disminuir siempre y cuando las empresas tengan un sistema de monitoreo implementado en su infraestructura.

Así entonces, es necesario indagar lo importante que es un sistema de monitoreo en las empresas, con el fin de analizar, reducir y prevenir las vulnerabilidades en la infraestructura tecnológica de la industria. Cuyas características surgen de la interacción del usuario final frente a las infraestructuras tecnológicas, ya que el

[1]A diario se registran 542.465 ataques informáticos en Colombia (online) El tiempo, Bogotá, 27 de septiembre 2017 Citado(20/09/2018) Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

usuario final es el factor más vulnerable donde el atacante lo clasifica como el eslabón más débil de la infraestructura.

1.1 FORMULACION DEL PROBLEMA

¿Cuál es la importancia de los sistemas de monitoreo de redes al interior de las empresas?

2. JUSTIFICACION

Los sistemas de monitoreo son importantes por el hecho de que están centrados en dar vigilancia y seguimiento a la red, como lo sabemos la red es el recurso más importante a nivel tecnológico, pues se encarga de interconectar dispositivos los cuales permiten optimizar todos los procesos y servicios que ofrece una empresa, como sabemos, si una red se cae puede parar las actividades o producciones de esta misma. Ahora bien, un sistema de monitoreo dentro las empresas permite que el administrador de la plataforma pueda hacer seguimiento del tráfico y funcionamiento de la red, garantizando el 100 % de rendimiento y prestación del servicio, tratando de tener un paso más adelante de posibles atacantes o fallas que puedan afectar la prestación del servicio generando pérdidas económicas.

Es importante recopilar toda la información necesaria para crear una sensibilización empresarial frente a las diversas amenazas que acechan nuestra información, tratando de dar una orientación de cómo y con qué medios se puede hacer una monitorización de nuestras infraestructuras tecnológicas.

Mostrando algunas cifras de ataques que afectan directamente el funcionamiento de las empresas como virus, ataques de intrusión, Ramsoware y Denegación de servicios Con su respectiva pérdida económica, se puede empezar a fomentar el uso de un sistema de monitoreo, Dando a conocer los diferentes softwares en el mercado para dichas actividades y dar una implementación en las determinadas empresas, Realizando un comparativo de cómo está preparada la empresa para realizar un monitoreo a un posible ataque que pueda afectar la prestación del servicio y rendimiento de la red.

Con este trabajo estamos contribuyendo a que las empresas conozcan de la existencia de los sistemas de monitoreo de redes, mostrando los beneficios de tener una herramienta como esta en la empresa, ya que actualmente el software de monitoreo tiene la capacidad de analizar el estado del sistema informático en tiempo real, detección del origen de cualquier incidente, darle seguimiento a los activos informáticos más relevantes de la empresa, mejorar el rendimiento y eficacia de la red, mostrar inventariado de la infraestructura con su respectivo mapa.

Es un estado actual realmente completo de los sistemas de monitoreo. En donde una empresa no dudaría en la implementación de esta.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un estudio que resalte la importancia de los sistemas de monitoreo de redes de datos al interior de las empresas y sus diversas amenazas.

3.2 OBJETIVOS ESPECIFICOS

1. Documentar la información relacionada con los sistemas de monitoreo de redes existentes en el mercado, y así se plantea el concepto de gestión de red como base de los sistemas de monitoreo.

2. Identificar los diferentes ataques orientados a redes de datos que puedan afectar el funcionamiento de las empresas.

3. Revisar con base a fuentes periodísticas, los sucesos y ataques a diferentes empresas, a nivel regional e internacional.

4. Ofrecer al personal responsable de administrar infraestructura de red de las empresas, argumentos de índole técnico para la selección de herramientas de monitoreo de red.

4. MARCO DE REFERENCIA

4.1 MARCO TEORICO

Los sistemas de monitoreo a redes de datos, son sistemas con la función de brindar un monitoreo de todo el tráfico de una red determinada. En busca de componentes defectuosos o lentos para dar información a los administradores de la red.

De acuerdo a los ataques orientados a la red, se puede mostrar la importancia y el impacto que tiene el uso de sistemas de monitoreo a las empresas, en donde la mayor problemática actual es que las empresas no tienen implementado un sistema de monitoreo de red, las empresas no están concientizadas de la importancia de estos sistemas de monitoreo, no dimensionan la problemática y las pérdidas que puede ocasionar un ataque informático.

Entonces con esta Investigación se busca tapar esa brecha que tiene la mayoría de empresas con el uso de los sistemas de monitoreo, mostrar lo importante que es tener implementado en la empresa un sistema de monitoreo de acuerdo a los ataques orientados a la red consultados en dicho trabajo y algunos eventos o ataques tanto nacionales e internacionales, mostrando el tipo de ataque ejecutado y su cifra de pérdida económica.

Gracias a la gestión de red, se puede identificar todos los dispositivos que interactúan con la red, se determinan los puertos por el cual los dispositivos están trasmitiendo datos. En donde los sistemas de monitoreo sacan provecho a la gestión de red, ya que se puede realizar trazas de paquetes no identificados y la cantidad de ataques los cuales se pueden evitar mediante el constante monitoreo por los administradores de la red.

Analizando la ubicación geográfica (Colombia), según el periódico el tiempo en Colombia se efectúan 542465 ataques a diario[2], donde el impacto de los delitos

[2] A diario se registran 542.465 ataques informáticos en Colombia (online) El tiempo, Bogota, 27 de septiembre 2017 Citado(20/09/2018) Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

informáticos ha generado pérdidas por 6179 millones de dólares en el país, Para no ser parte de estas cifras de ataques diarios en Colombia, se debe de contar con un sistema de monitoreo en la empresa, estos sistemas ayudaran a mitigar muchos tipos de ataques a nivel de red e intrusiones , dificultando a los ciberdelincuentes a las hora de realizar un ataque contra una empresa que está protegida y constantemente monitoreada.

En Colombia el sector más afectado por los constantes ataques según digiware, es el sector financiero con 214600 ataques por día, seguido el sector de comunicaciones con 138329, gobierno con 83756 e industria con 51263 casos.

Ahora a nivel internacional los ataques más relevantes son la denegación de servicio, Ataques que por medio de un sistema de monitoreo se puede mitigar y reaccionar de forma inmediata, según el artículo de karpesky[3] sobre los ataques de denegación de servicio, nos plasma que los mencionados ataques en el tercer trimestre de 2017, han aumentado en china, corea del sur, EE.UU. y Rusia. Donde se refleja un aumento de ataques con botnet, donde en el sector australiano hubo un brusco reporte en el número de ataques (más de 450 por día) y su potencia(hasta 15.5 millones de paquetes por segundo).contando con un sistema de monitoreo, se puede detectar el host el cual este generando demasiado tráfico en la red intentando realizar la denegación de servicios, el sistema permite hacerle un exhaustivo seguimiento al posible ataque de denegación de servicios desde donde empieza hasta que se mitiga.

De acuerdo al material consultado sobre los sistemas de monitoreo, ataques informáticos orientados a la red y el cuadro de pérdidas económicas por ataques informáticos, se puede mostrar el impacto el cual genera estos resultados en contra de los beneficios de las empresas los cuales no cuentan con un sistema de monitoreo. El mensaje que se quiere compartir con esta monografía es la importancia que tiene un sistema de monitoreo en la empresa, no esperar a que la empresa sea víctima de un ciber ataque y tenga pérdidas millonarias, en donde este dinero se puede invertir en la seguridad de la empresa y en un sistema de monitoreo. Es muy triste que las empresas realicen una inversión en la seguridad informática

[3] Los Ataques DDos en el tercer trimestre de 2017 (online), Karpesky,usa,6 de noviembre del 2017 citado(26/09/2018) Disponible en: https://securelist.lat/ddos-attacks-in-q3-2017/85669/

cuando ya fueron víctimas de un ataque cibernético.

La investigación busca crear una concientización a las empresas, sobre lo importante que es implementar un sistema de monitoreo, conocer los diferentes sistemas en el mercado tano licenciados como libres. Tratar de mitigar los ataques orientados a la red que puedan intervenir con la prestación de servicio de las infraestructuras empresariales.

Esta Investigación está orientada a brindar concientización a toda empresa la cual posea una red interna de trabajo, no importa el tipo de sector el cual se desempeñe la empresa, lo importante es que las empresas gocen de un software de monitoreo en su infraestructura tecnológica garantizando un porcentaje alto de seguridad a su información.

En la siguiente sección, se va a presentar algunos trabajos de investigación que hacen referencia al tema de sistemas de monitoreo de redes:

BAYAS,Johnny Israel, estudiante de la universidad Técnica de Ambato ecuador, realiza un proyecto de investigación sobre la implementación de un sistema de monitoreo[4] para una empresa de su país, donde manifiesta que el principal problema que presentaba la empresa era la falta de monitoreo constante y tener control sobre los dispositivos de red. Efectivamente el estudiante implementa un servidor para monitorear la red y tener un control sobre los dispositivos utilizando recursos ya existentes dentro de la misma empresa, Realiza la implementación sin obtener equipos nuevos, ni equipos que son diseñados para ese tipo de labores. Esta investigación nos aporta que indirectamente está resaltando la importancia de la implementación de un sistema de monitoreo para las empresas en general, Resaltando que, para realizar la implementación, no necesita de muchos recursos y podría utilizar los equipos que tiene la empresa en la actualidad, en pocas palabras puede reutilizar equipos que cumpla los requerimientos y cubra el rendimiento que necesita la implementación de acuerdo a la infraestructura tecnológica de la

[4] BAYAS, Johnny Israel. Servidor de control de dispositivos y servicios mediante protocolo smtp Trabajo de grado, Ingeniero electrónico, Ambato : Universidad Técnica de Ambato, Facultad de ingeniería en electrónica,2015,184p.

empresa.

El estudiante ECHEVERRIA, Francisco de Borja, su trabajo de grado[5] es muy interesante, ya que su nivel de dificultad es alto por el hecho de implementar y crear su propio sistema de monitoreo a nivel de hardware y software, el cual tiene como función recolectar la respectiva información de tráfico ip proveniente de diferentes redes, con el fin de analizar comportamientos anormales los cuales se pueden presentar en la red por casos de infección de virus y malware. Este trabajo de grado nos enseña que un sistema de monitoreo también puede ser creado de acuerdo a la necesidad puntual del administrador de la red. Que, por el hecho de ser un software sencillo y no avalado empresarialmente, no va a dejar de ser importante para la empresa contar con un sistema de monitoreo.

En la universidad nacional autónoma de México, los estudiantes DELGADILLO, José Luis y GARCIA, Daniel, presentan un trabajo de grado el cual tiene como objetivo crear un sistema para monitorear el desempeño de la red y servidores utilizados en la institución educativa a la cual pertenecen[6], Donde la idea principal de la implementación, es que les permita llevar un registro y conteo de los datos que son transportados hacia los servidores por medio de los swtiches de acceso. Además, quieren que su sistema sea multifuncional, con la capacidad de estar generando alertas y reportes. Lo que nos aporta este trabajo de grado a nuestro estudio, es que involucra varios dispositivos de red los cuales son componentes muy poco mencionados a comparación de los otros trabajos de grado. Resalta estos dispositivos de red a su nivel de importancia, señalando que todo tráfico saliente de ellos, serán almacenados y reportados para un mayor seguimiento mostrando el objetivo principal y el funcionamiento que tiene un software de monitoreo en la empresa.

En Colombia, los estudiantes de la universidad javeriana, MENDIVELSO, John Jairo y NEVA, Iván Gerardo, desarrollan una aplicación para la administración de redes

[5] ECHEVERRIA, Francisco de Borja Implementación y evaluación de sistema de monitoreo de seguridad basado en flujos de paquetes, Trabajo de grado, Ingeniero civil en computación, Santiago de chile, Universidad de Chile, Facultad de ciencias Físicas y Matemáticas, 2008, 126p.

[6] DELGADILLO, José Luis y GARCIA, Daniel, Monitorización de servicios de red y servidores, Trabajo de grado, Ingeniero en Computación, México DF, Universidad Nacional Autónoma de México, Facultad de Ingenieria,2010, 141p.

distribuidas, orientada a conexiones con dispositivos móviles a través de redes inalámbricas[7], Donde el objetivo de la aplicación es poder tener la administración de la red desde dispositivos móviles, dándole un manejo versátil y a la mano desde cualquier ubicación geográfica, además, la aplicación tendrá la característica de monitorear la red y el estado de sus componentes, gestionar las alertas generadas por alguna anormalidad en la red. El aporte que nos deja este trabajo de grado, es mostrar que una red también puede ser monitoreada remotamente por medio de dispositivos móviles, Además de que no está limitando el alcance que puede tener un sistema de monitoreo independientemente del medio por el cual se transporte los datos(cable utp, fibra óptica, coaxial o inalámbrica).

En la siguiente monografía, el estudiante GONZALEZ, Víctor Rafael de la universidad santo tomas, realiza la propuesta de implementar un sistema de monitoreo de red para una determinada empresa[8], con el objetivo de registrar y almacenar el funcionamiento de la red y sus respectivos servicios, con el fin de estar al tanto del comportamiento de la red para poder tomar acciones inmediatas de acuerdo a las alarmas generadas por el sistema de monitoreo. Este trabajo de grado nos aporta, las acciones que debería de realizar un sistema de monitoreo de red y el debido tratamiento de la información levantada por la constante monitorización de la infraestructura tecnológica. Resaltando el análisis periódico del comportamiento que puede presentar la red la cual se está custodiando.

Observando los diferentes trabajos de grado sobre los sistemas de monitoreo de red, todos se basan en elaboración e implementación, ninguno busca resaltar la importancia que tienen estos sistemas implementados directamente en una empresa, ¿qué beneficios trae la implementación?, ¿A que amenaza están expuestos los datos e infraestructuras tecnológicas?, Estos trabajos de grado no dan una respuesta directa del por qué es importante contar con un sistema de monitoreo a nivel empresarial. Teniendo en cuenta los ataques existentes orientados a la red, ni hechos que muestran las pérdidas económicas que han generado dichos ataques.

[7] MENDIVELSO, John Jairo y NEVA, Iván Gerardo, Administrador distribuido de redes orientado a dispositivos móviles, Trabajo de grado, Ingeniero de sistemas, Bogotá DC, Universidad Javeriana, Facultad de ingeniería, 2015,122p.

[8] GONZALEZ, Víctor Rafael, Diseño e Implementación de un sistema de monitoreo basado en snmp para la red, Trabajo de grado, Ingeniero en telecomunicaciones, Bogotá DC, Universidad Santo Tomas, Facultad de Ingeniería y Telecomunicaciones,2014,86p.

4.2 MARCO CONCEPTUAL

AMENAZA: palabra que hace referencia a los riesgos que están expuestas las diferentes infraestructuras tecnológicas.

- Amenazas más comunes en las redes:

  - ✓ Malware: Software malicioso, creado para infectar y dañar los sistemas. Puede infectar páginas web.
  - ✓ Intercepción: Ocurre cuando un atacante captura datos que envían las victimas por la red, y los utiliza para su beneficio propio.
  - ✓ Ataque DOS: ataque con el fin de interrumpir los servicios que presta un servidor como tal o servicios de red.
  - ✓ Configuración incorrecta: es considerada la vulnerabilidad más riesgosa, ya que, con una configuración incorrecta, la brecha de seguridad es demasiado extensa.
  - ✓ Virus; software malicioso con el fin de infectar los diferentes sistemas con el fin de volverlos vulnerables o dañarlos definitivamente.

PROTOCOLOS: es un conjunto de reglas, que autorregula el intercambio de datos entre dispositivos de red y host.

- Protocolos de red:
  - ✓ Ip: encargado del direccionamiento y enrutamiento.
  - ✓ Arp: da resolución de direcciones ip.
  - ✓ Ndp: resolución para direcciones ip v6.
  - ✓ Icmp: intercambio de información y de errores.
  - ✓ Sna: conecta los dispositivos a sus recursos de red.
  - ✓ Nbf: comunica con la capa de presentación.
  - ✓ Ipx: enrutamiento y direccionamiento.
  - ✓ Ddp: enrutamiento y direccionamiento.
  - ✓ Ospf: optimiza el routing en costes de trasmisión.

- Protocolos de transporte:
  - ✓ Tcp: protocolo de control de trasmisión; encargado de proporcionar trasmisión confiable de paquetes de datos sobre redes.

- ✓ Udp: es el encargado en el intercambio de datagramas, permite él envió de datagramas en la red sin que se haya establecido una conexión.

DISPOSITIVOS DE RED: dispositivos encargados de brindar la intercomunicación y tránsito de datos entre host. A continuación, se definen los diferentes tipos de dispositivos de red existentes:

- Switch: dispositivo encargado de la segmentación de la red, con el fin de intercomunicar computadores y periféricos entre si. Evitando inundaciones de broadcast en las redes.

- Router: dispositivo encargado de enrutar los paquetes en una determinada red.

- Access point: dispositivo encargado de brindar conectividad inalámbrica a los demás dispositivos.

CONFINDENCIALIDAD: se encarga de garantizar que los datos, objetos y recursos puedan ser leídos por los verdaderos destinatarios; por ejemplo, los datos pueden ser almacenados físicamente en (disco duro, CD-ROM, memoria) o pueden transitar a través de una red. En donde en ambos escenarios los datos y recursos necesitan controles de seguridad.

Los ataques más comunes que atentan contra la confidencialidad:

- El acceso no autorizado a bases de datos: comúnmente los delincuentes se concentran en explotar los errores de configuración o fallos en las interfaces que interactúa el usuario y las bases de datos, en donde finalmente se logra el acceso ilegal a la confidencialidad de la información almacenada en la base de datos.
- Accesos no autorizados a los archivos: cuando no hay una previa configuración de controlar los accesos a los recursos, personas sin ninguna autorización pueden tener acceso a la información.
- Sniffer de red: este software tiene la capacidad de capturar el tráfico que transita por la red, si la información no tiene una previa configuración de cifrado, esta será vulnerada por cualquier atacante.

Métodos para salvaguardar la confidencialidad:

- Cifrado de datos: se encarga de que la información no sea tangible para los atacantes, transforma el texto claro en texto cifrado. existen algunos métodos de encriptación como lo son: AES,DES,Triple,RC4,RC5. En donde se puede utilizar una clave de lado a lado clasificadas en claves públicas y privadas.
- Autenticación de usuarios: identifica los usuarios autorizados para acceder a un tipo de recurso o información, existen algunos métodos de autenticación como lo son: comunicación o inicios de sesión en aplicaciones o terminales por medio de contraseñas, biometría (identificación de retina, huellas dactilares), tarjetas inteligentes de microchip o banda magnética.
- Autorización de usuario: cuando la persona sea identificada correctamente, obtiene privilegios para poder operar en el ámbito de los datos, objetos y los diferentes recursos ofrecidos por la red.
- Clasificación de los datos: los datos se deben de clasificar por niveles de sensibilidad, la clasificación ayuda a determinar cuánto dinero y recursos se deben destinar para proteger los datos existentes asignándole control a su acceso.

SEGURIDAD FISICA: La seguridad física es el aspecto el cual los profesionales no le dan mucha importancia, ya que en pensamientos erróneos cedemos todo el peso de responsabilidad a el área de vigilancia de la infraestructura física (edificio, casa, fabrica) en definición, al personal encargado de la seguridad del establecimiento.

Los profesionales de seguridad informática, así no tengan la competencia en el área de seguridad física, deben tener claro, el hecho de colocar obstáculos físicos y evitar la manipulación a los equipos relacionados con la red corporativa, eliminando las vulnerabilidades físicas posibles.
Enfatizando que el atacante al tener acceso físico a los equipos que estén conectados en la red, puede apoderarse de estos y ejecutar diversos ataques orientados a las redes. Evadiendo los múltiples controles de seguridad e inclusive la desactivación de firewall, antivirus o sistema de monitoreo de red.

En este segmento se menciona algunos ejercicios de seguridad física:

- Sistemas de control de acceso (clave de ingreso,biométricos,personal)
- Cuartos de cableado con control de acceso o cerradura de seguridad
- Cableado cubierto por estructura metálica (tubería mt o canastilla transportadora de cableado)
- Ubicación estratégica de dispositivos (altura de los access point)
- Respectiva configuración de seguridad de puertos (aplicable a los swicth de Acceso)
- Autenticación con servidor Radius.
- Políticas de ingreso al Data Center.
- Refrigeración del Data center.
- Ups con total cobertura en el data center

Propósitos de la seguridad Física:

- Garantizar la adecuación ambiental, que reduzcan los riesgos por falla o mal funcionamiento de los equipos.
- Clasificar y registrar el ingreso de personal a la manipulación de equipos (ingreso a data center)
- Preservar y garantizar la supervivencia de la infraestructura tecnológica, en todo tipo de circunstancia donde se vea amenazada.
- Reducir fallas y perdidas, tener contingencia en caso de recuperación.
- Cubrir las amenazas ocasionadas por el hombre o estados ambientales

CONTROLES EN LA SEGURIDAD INFORMATICA: Comúnmente en todos los entornos existentes, siempre deben existir reglas y deberes los cuales regulen un debido control al entorno, con estas implementaciones se busca en dar una orden, sea para una mejor evolución o prevención de inconvenientes que pueda afectar el entorno. En este caso nos referimos al entorno de la red y sus amenazas.

Entonces por la razón de la existencia de varias amenazas en la red, se debe de dar un control a este gran recurso, El control se implementa para minimizar ataques al sistema, donde se deben establecer políticas y procedimientos

especiales en el diseño e implementación de la seguridad informática como tal.

El control se basa en métodos, políticas y procedimientos que aseguran la protección de los activos de la empresa, la exactitud y confiabilidad de sus registros y el apego de sus operaciones a los estándares que definan la administración. Recordemos que el éxito es fácil de alcanzar de acuerdo a la buena administración, seguimiento de procedimientos y normas. Todo de la mano del buen orden que ponga el encargado de administrar los controles establecidos.

Controles Generales:

- Establece un marco de trabajo para controlar el diseño, la seguridad y usos de software a lo largo de la organización. (políticas sobre usos de programas no licenciados y no permitidos por la organización). en este aspecto las empresas deben de blindarse, ya que los empleados pueden crear brechas en la seguridad de la red ejecutando programas desconocidos y de dudosa procedencia, donde estos como contenido pueden desatar gusanos o abrir puertas para ingreso a la red. Para este tipo de eventualidades el administrador del antivirus crea una serie de reglas o políticas del antivirus para evitar que los usuarios hagan una ejecución de estos archivos ejecutables.

Controles de aplicaciones:

- Controles específicos únicos para cada aplicación computarizada. (control y registro de todas las aplicaciones que funcionan en la red empresarial)

Tipos de controles:

- Controles preventivos: Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones; Por ejemplo, los sistemas de claves de acceso.

- Controles Detectivos: Son aquellos que no evitan que ocurran las causas del riesgo si no que los detecta luego de ser ocurridos, son los

más importante para el auditor, De cierta manera sirven para evaluar la eficiencia de los controles preventivos. Por ejemplo, la infección de un virus en la red, que nos damos cuenta ya cuando el sistema o la red está infectada por este.

- Controles correctivos: Ayuda en la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a nuevos errores.

- Controles disuasivos: Reducen la probabilidad de un ataque deliberado

HACKER: persona de alto coeficiente en el medio de la tecnología lo cual busca sacar provecho de su conocimiento usándolo a beneficio propio (económica e intelectualmente)

- Tipos de hacker:

  - ✓ Black hat: Denominados como los delincuentes, se caracterizan por apoderarse de sistemas con el fin de secuestrar información o eliminarla.
  - ✓ White hat: Persona la cual actúa cumpliendo con las leyes establecidas con ética profesional.
  - ✓ Grey hat: Es una persona intermedia, a veces actúa bajo la legalidad y otras veces en la ilegalidad.
  - ✓ Crackers: Personas totalmente destructivas, su finalidad es destruir sistemas.
  - ✓ Carder: Personas enfocadas al fraude con tarjetas de crédito.
  - ✓ Pharmer: se dedican a realizar ataques de phishing.
  - ✓ War driver: Especialistas en hackeo de tecnologías móviles.
  - ✓ Defacer: buscan vulnerabilidades de sitios web para realizar una intrusión.
  - ✓ Spammer: especialistas en crear spywares.
  - ✓ Scrip-kiddie: Personas que solo se limitan a recolectar información.
  - ✓ Wizard: especialista en sistemas informáticos, sabe cómo funcionan y el por qué.
  - ✓ Lammer: persona inicialista en el mundo del hacking.

NORMA 27001: DEL 2013 EN LAS EMPRESAS: La seguridad informática es un conjunto de seguridad de Información, ya que protege la Información de manera digital, mientras que la seguridad de la Información es un concepto mucho más amplio y abarca mucha más Información acerca de este protegiendo la Información en cualquier medio de comunicación.

La mayoría de las empresas reconocen que la seguridad de la Información hace parte de su gestión de riesgos, el objetivo es disminuir los riesgos que atenten contra el bienestar de la empresa.

La ISO 27001:2013 se le realizaron algunas modificaciones en su estructura como lo fueron en los temas de:

- Contexto de la organización: En este contexto se encuentra consignado el conocimiento de la organización, comprensión y estudios de necesidades de la empresa, la determinación del alcance del sistema (hacia donde tiende a ir, ciclo de vida, capacidades de reacción frente a un desastre tecnológico), y el objetivo del sistema de gestión de seguridad implementado en la empresa.

- Liderazgo: Resalta el liderazgo que implementan los ingenieros de seguridad al hacerse responsables de velar por la integridad de los datos y de la red empresarial, implementación de políticas internas, asignación de roles, responsabilidades y autoridades en la organización.

- Planificación: Se centra en las acciones para tratar los riesgos y oportunidades, planifica los objeticos de seguridad de la Información y planes para lograrlos.

- Soporte: Hace referencia a los recursos con los que se cuenta, Información documentada y toma de conciencia frente a las situaciones posibles de suceder.

- Operación: Se valoran los riesgos de la seguridad de la información, se plantea el tratamiento de riesgos de la seguridad de la Información.

- Evaluación del desempeño: Se realiza el seguimiento, medición, análisis y evaluación de la seguridad implementada.

- Mejora: Análisis de no conformidades y acciones correctivas referente al sistema de seguridad. Procurando darle mejoras continúas.

ISO 27002:2013 EN LA EMPRESA: La modificación de la ISO respecto a la anterior, amplia los campos de cobertura, cubre más temática, procurando en expandir la base del conocimiento que contienen las normas ISO.

Temas Incorporados:

- Cifrado: Implementación de controles criptográficos y políticas de su uso.

- Seguridad física y ambiental: Hace referencia a las áreas seguras (ubicaciones estratégicas de los equipos) controles físicos de entrada, seguridad de oficinas, despachos y recursos.

    - Seguridad de los equipos, mantenimientos, instalaciones y configuraciones.
    - Seguridad de cableado, reutilización de recursos y equipos.

- Seguridad ligada a recursos humanos: Investigación de antecedentes, velar cumplimiento de términos y condiciones de contratación.

- Seguridad en telecomunicaciones: Hace gestión de la seguridad de la red (controles de red, mecanismos de seguridad asociados a los servicios de red).

- Intercambio de Información con partes externas (políticas y procedimientos de intercambio, acuerdos de intercambio, acuerdos de confidencialidad y secreto.)

SERVICIOS TI Y LA IMPORTANCIA EN LA ORGANIZACIÓN:

Las organizaciones se volvieron muy dependientes de los servicios que ofrece TI, por medio de este, las organizaciones tienen el privilegio de compartir Información, estar en contacto con otras dependencias, ciudades o países. Estas interconexiones benefician demasiado a las organizaciones,

ya que pueden conectarse o expandirse a otras partes fuera de las instalaciones.

Hay que tener en cuenta que para disfrutar de los beneficios que nos ofrece la tecnología, debemos tener conocimientos de esta, su funcionamiento, las amenazas que nos acecha por medio de esta.

Por eso las organizaciones crean un SGSI para dar control y administración a este tipo de servicios ofrecidos por la tecnología, procurando dar protección tanto a la Información de la organización y al personal que labora en esta.

Los SGSI implementan un procedimiento de seguridad aplicando la normatividad vigente de la seguridad informática (ISO 27002:2013), tratando de abarcar todos los aspectos posibles, tratando de opacar todo tipo de evento el cual se podría considerar como una amenaza.

Esta normatividad veo que es muy completa a comparación de las anteriores.

La norma abarca desde la contratación de una persona, hasta la instalación y ubicación de los equipos tecnológicos. La normatividad trata de cubrir hasta el último detalle, desconfiando que por más pequeña e importante que sea la acción sea catalogada como una posible vulnerabilidad. Esto es lo que comúnmente llamamos precavidos.

En los casos de precaución hay puntos de la normatividad lo cual hace alusión a la investigación y análisis para adelantarse a ciertos hechos y así evitar catástrofes tecnológicas, procurando a seguir un plan previamente planeado como contingencia en casos de ataques o pérdidas de Información y denegación de servicios.

El éxito y la armonía de la tecnología en la empresa, es basarse y tratar de cumplir la normatividad vigente al pie de la letra, implementar educación a

los usuarios finales, crearles conciencia de los peligros que corren las personas y las empresas por medio del mal uso de la tecnología y la no confidencialidad de los empleados

4.3 MARCO LEGAL

Como lo sabemos; la ley que regula la seguridad de la información es la 1273 del 2009, A continuación, vamos a explicar algunas leyes que se relacionan directamente con el contenido de la monografía:

- Artículo 269A acceso abusivo a un sistema informático: El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

El articulo hace referencia al acceso abusivo a cualquier sistema informático, como lo sabemos esto se puede lograr por medio de ataques informáticos orientados a la red como infección de virus, instalación de troyanos o backdoors. Técnicas que conllevan a la violación de dicho artículo, permitiendo al atacante acceder al sistema informático de cualquier empresa sin una previa autorización por parte de un superior de la entidad, logrando tener acceso a información sensible para la empresa. En pocas palabras el tener accesos a un sistema informático de una empresa es tener el poder informático sobre ella, tomar decisiones que pueden poner en riesgo la integridad de los datos y el funcionamiento de ella misma.

- 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.

Cuando se habla de obstaculización de sistema informático o red, nos estamos refiriendo a los ataques que interfieren con la transferencia de datos o

intercomunicaciones de unos equipos a otros, afectando el tránsito de información o prestación de servicios informáticos, el artículo se incurre por medio de ataques orientados a la red como lo es el ataque de denegación de servicio e inundaciones flood y tráfico. Logrando una saturación en el transporte de datos logrando así la obstaculización del servicio que presta una determinada empresa. Ataques los cuales pueden ser detectados por un software de monitoreo de red identificando el aumento notable del tráfico que es inspeccionado por este software.

- 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 trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Para lograr una interceptación de datos informáticos, se debe también incurrir en el Artículo 269ª el cual nos habla de un acceso abusivo al sistema, en donde se debe de tener acceso al sistema informático y hacer instalación de software o códigos maliciosos los cuales permitan hacer capturas de todo el tráfico de datos que transita por la red empresarial. Actividad la cual es perjudicial para cualquier empresa, ya que el atacante tiene la habilidad de capturar información vital y podría divulgarla o venderla a las diferentes competencias. O peor aún obtener información sobre la infraestructura tecnológica y ejecutar diversos ataques que puedan afectar con el funcionamiento de la empresa como tal y la prestación del servicio.

- 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 1000 salarios mínimos legales mensuales vigentes.

Los daños informáticos pueden ser tanto físicos y lógicos, en este caso nos vamos a referir a los daños lógicos producido por ataques orientados a la red, como se dijo en el artículo anterior, para que un atacante pueda lograr el daño informático, primero debe de incurrir con el artículo 269ª,en nuestro caso el atacante debe de acceder al sistema informático ilegalmente e instalar código malicioso, virus que se encarguen de eliminar información o lograr una afectación en los sistemas operativos, logrando dañar el funcionamiento de las maquinas a nivel de hardware. Cuando hablamos de los daños causados, nos referimos a formateo de máquinas, saboteo de los sistemas operativos ocasionando que el sistema no siga sus parámetros de funcionamiento.

El papel del sistema de monitoreo de redes, nos mostraría el extraño comportamiento del tráfico de las maquinas afectadas o el estado en el que se encuentra dicho artefacto, si el ataque afecto como tal, el funcionamiento de hardware y software (bloqueos o apagados) el sistema nos arroja la alerta que los equipos han dejado de funcionar. En caso de que S.O este fallando, el sistema de monitoreo simplemente alerta, dependiendo del ataque, el comportamiento del tráfico generado por estos equipos (virus o modificaciones en el funcionamiento del sistema operativo.

- Artículo 269e uso de software malicioso: El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, 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.

El artículo hace alusión a cualquier tipo de software malicioso que pueda afectar el rendimiento o funcionamiento de los sistemas informáticos a nivel de software y redes. Para realizar cualquier tipo de ataque se deben ejecutar software malicioso. Software con intensiones puntuales sobre la seguridad e integridad de infraestructuras tecnológicas y la información.

Un sistema de monitoreo de redes puede detectar las acciones de estos softwares maliciosos, en algunos casos puede mitigar el daño que puede causar dicho software. Inclusive en la mayoría de casos, alerta sobre el comportamiento de la red causado por este software malicioso.

- 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 p 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.

A mi parecer, este articulo acobija a todos los demás en nuestro caso, pues para poder violar los datos personales, lo primero que debe de hacer el atacante es acceder a un sistema informático (artículo 269ª), para lograr el acceso al sistema debe de ejecutar ciertos programas maliciosos (artículo 269e) que permitan que el atacante tenga acceso al sistema informático y tenga el privilegio de tener toda la información a la mano.

Ya con el sistema vulnerado el atacante puede hacer lo que quiera con la información confidencial de determinada empresa, incurriendo con el artículo de violación de datos personales, modificando, divulgando o vendiendo. Legalmente a un atacante le pueden aplicar el número de artículos que haya violado. Y a mi parecer para realizar ataques que estén orientados a las redes debe de incurrir con la mayoría de artículos de la ley 1273 del 2019 de la república de Colombia.

En conclusión, todos los artículos de la ley 1273, el sistema de monitoreo de redes está involucrado directamente con ellos, pues el sistema se encarga de custodiar todo el tráfico que se mueve por las redes de las diferentes empresas o negocios involucrados con la tecnología. En donde las acciones que componen los artículos pueden ser detectados por dicho sistema de monitoreo o peor aún, el sistema de monitoreo también podría ser afectado en la falta de los artículos que componen la ley 1273.

5. DISEÑO METODOLOGICO

La monografía está compuesta por 4 fases, en donde la primera fase damos una breve introducción al concepto de gestión de redes, tema central y esencial para comprender con facilidad el funcionamiento de un sistema de monitoreo de redes. Luego de dar el concepto de gestión de redes, mencionamos los diferentes tipos de sistemas de monitoreo de redes existentes en el mercado; tanto licenciados como Open Source. Se realiza un cuadro comparativo de las características de alguno de ellos. Lo que se pretende con la primera fase es dar a conocer el concepto de gestión de redes y mostrar algunas alternativas de software de monitoreo de redes, con el fin de mostrar al lector alternativas en las cuales, dependiendo del estado financiero de la empresa, pueda implementar un software de monitoreo.

En la fase número dos, damos a conocer una variedad de ataques los cuales van orientados a las redes. Además de dar una pequeña definición de estos, se realizan dos ataques para mostrar el funcionamiento y el caos que puede provocar un tipo de ataque como los experimentados, la idea de esta fase es dar a conocer los ataques que puede sufrir una empresa a nivel de red.

Ahora, en la fase número tres, mostramos los ciberataques más destacados en la historia, tanto a nivel nacional e internacional, con el fin de crear conciencia de que ninguna empresa está libre de un ciberataque orientado a la red, no importa si es pequeña, mediana o grande, o su ubicación geográfica.

Por último, la fase cuatro se realiza un análisis de las fases anteriores para llegar a la conclusión del por qué es importante tener un sistema de monitoreo de red al interior de las empresas.

6.SISTEMAS DE MONITOREO

En este capítulo vamos a conocer el término de la gestión de red, en donde dicho termino es la base para poder entender el funcionamiento de los sistemas de monitoreo de redes, además del término de gestión de red, conoceremos los diferentes softwares de monitoreo que existen el mercado de la tecnología con sus respectivas características.

6.1. GESTIÓN DE RED

La gestión de red consiste en las acciones de analizar, configurar, monitorizar y controlar los diferentes recursos de red con el objetivo de transmitir información por medio de dispositivos de red que interactúan para que dicha información transite libremente por una infraestructura tecnológica. Permitiendo el compartimiento, distribución y almacenamiento de la información. En donde el hardware, software y el recurso humano trabajan de la mano para brindar y soportar las interacciones con las redes.

Un sistema de gestión ofrece una interfaz que tiene la capacidad de ejecutar múltiples tareas de gestión, en donde la combinación de hardware y software nos permite realizar actividades de monitoreo y la capacidad de generación de reportes de acuerdo al tráfico de una red en específico.

El sistema de gestión está elaborado para mostrar una infraestructura en un reporte unificado. Compuesto por direcciones lógicas y un inventario de activos tecnológicos los cuales cumplen una tarea determinada y hacen parte esencial de la red.

6.1.1 Composición de la gestión de red

Está compuesta por entidad de gestión de red y la aplicación de gestión de red; los cuales se caracterizan por sus diferentes actividades; en donde la combinación de estos términos facilita la recolección de información obedeciendo a una serie de comandos previamente configurados por el proveedor de los dispositivos de red.

6.1.1.1 Entidad de gestión de red

Realiza presencia en todos los nodos, cuya función es capturar y almacenar a nivel local las estadísticas de las actividades y variaciones que se presentan en la red. Además, obedece a comandos ejecutados desde la administración o centro de control de la red.

6.1.1.2 Aplicación de gestión de red

Lista información generada por comandos o peticiones a la entidad de gestión de red por medio de la red dando respuesta a los comandos ejecutados por la administración. Posee una interfaz en donde usuarios autorizados y el administrador tengan una interacción con la gestión de la red.

6.1.2 Estructura de la gestión de red

Base de datos de la información de Administración (MIB); define variables utilizadas por el protocolo de transporte SNMP para monitorear y administrar todo lo que compone una red, como switches y enrutadores.

6.1.3 Tipos de información

En los tipos de información, vamos a encontrar la caracterización que se le da a la información en la gestión de redes, cada tipo de información está centrada en diferentes temas y definiciones, en donde esta información es recolectada por los diferentes dispositivos y son centralizados en una estación de control encargada de almacenar dicha información y a la vez permitir la gestión sobre los demás dispositivos que interactúan en la red.

6.1.3.1 Información estática

Información por la cual se resalta la configuración actual, y los elementos de red que hacen parte de una determinada infraestructura tecnológica. Por ejemplo, la identificación de los puertos, los cuales estén activos en la red realizando múltiples tareas de transmisión de diferentes paquetes y conexiones con otros dispositivos de red o host que estén localizados por fuera de la red interna (internet o una red wan dependiendo de la infraestructura tecnológica de la empresa). En resumidas cuentas, identifica todos los puertos activos que estén realizando trasmisiones.

6.1.3.2 Información Dinámica

Información sobre los eventos presentados en una red. En donde se analiza todos los paquetes que están transitando en la red, dado que dichos paquetes contienen información la cual puede afectar la conectividad y crear eventos los cuales son almacenados y monitoreados en una estación central con el fin de tener una traza y registro de los diferentes paquetes transitados en la red.

6.1.3.3 Información Estadística:

Información recolectada de acuerdo a la cantidad y el tiempo de los paquetes en la red. En donde el número de paquetes trasmitidos es medido por unidad de tiempo por los diferentes elementos que se encuentran interconectados en la misma red (dispositivos de interconexión). Información por la cual podemos medir la estabilidad de trasmisión de datos y detectar tempranamente fallos de conexión y trasmisión.

6.1.4 Elementos de la gestión de red

Es el conjunto de elementos; los cuales por medio de sus funciones permiten la gestión de red en todos los ámbitos; a nivel de comunicación se encuentran los agentes, a nivel de administración, se desempeña el sistema de gestión como tal, y a nivel de base de datos se encuentra la base de gestión; la cual se encarga del almacenamiento de datos de conexión.

6.1.4.1 Agentes

Realiza reportes del estado de los elementos que componen la red los cuales son administrados para garantizar su funcionamiento correcto, los agentes reciben comandos desde la administración para tomar diversas acciones frente a los acontecimientos que se puedan presentar con una red de datos y su debida transferencia y transporte de los datos.

6.1.4.2 Sistema de gestión de redes (NMS)

Dirige y administra las diferentes operaciones que realiza los agentes. buscando la interconexión entre los dispositivos para facilitar el transporte exitoso de los datos, por medio de comandos administrativos transportados por los mencionados agentes.

6.1.4.3 Base de datos de gestión (MIB)

Base de datos a disposición de los agentes y el sistema de gestión de redes alimentando la información sobre el funcionamiento de la red. Almacenando el estado de los dispositivos de red que componen la infraestructura, almacenamiento de posibles fallas en los diferentes dispositivos de red. Para tener una reacción rápida frente a una posible falla de conexión.

6.1.5 Tipos de gestión de red

En el siguiente punto, vamos a dar a conocer las diferentes gestiones que componen como tal el término de la gestión de redes de datos:

6.1.5.1 Gestión de configuraciones

Detecta y controla el funcionamiento de la red en el ámbito de configuraciones físicas y lógicas.

6.1.5.1.1 Estado de la red

Hace referencia al estado actual de la red a nivel de hardware y software. En donde el estado de la red se compone por el registro de la topología que se divide en dos clases que son:

- Estático:
  - ✓ Lo que está instalado (dispositivos a nivel de hardware y aplicaciones a nivel de software)
  - ✓ En donde se encuentra instalado
  - ✓ Qué tipo de conexión posee
  - ✓ Responsable en cada área
  - ✓ Como contactar el responsable de cada área

- Dinámico:
  - ✓ Estado del funcionamiento de los dispositivos que conforman la red.

6.1.5.2 Gestión de inventario

Hace referencia del inventario a nivel de software y recolección de datos que se almacenan en las diferentes bases de datos que componen la red.

- Base de datos de los dispositivos de la red.
- Histórico de los cambios y conflictos de los activos.

6.1.5.3 Control operacional de la red

Hace referencia a todas las funciones que pueden ser aplicadas administrativamente:

- Inicia y detiene los componentes individuales.
- Modificar las configuraciones de los dispositivos.
- Actualizar el HD y SW
- Métodos de acceso
- SNMP
- Fuera de banda

6.1.5.4 Gestión del rendimiento:

Análisis de los eventos presentados en el tráfico de la red; en donde se realiza las siguientes actividades administrativas:

- Garantizar el 100% de rendimiento de la red.
- estadísticas de las operaciones de las interfaces.
- Trafico
- Alertas de errores
- Disponibilidad
- Análisis, mediciones y pronósticos.
- Niveles de rendimiento.
- Análisis de la capacidad y sus instalaciones.
- Resolución de incidentes
- Planes a largo plazo
- Mediciones activas y pasivas.
- Herramientas de gestión y estadística

6.1.5.5 Gestión de fallas

identificación y seguimiento de las fallas presentadas en la red; de acuerdo a las siguientes actividades:

- Caracterización de la falla
- Sondeo de los activos de la red.
- Diagnóstico de los activos de la red
- Reacción a la falla
- Analizar las prioridades.
- Procedimiento técnico y de gestión
- Resolución de la falla

6.1.5.6 Detección y gestión de fallas

Comandos o acciones ejecutadas por la administración de la red, utilidades que traen por defecto los dispositivos:

- Traceroute
- Ping
- Ethereal
- Snmp

6.1.5.7 Gestión de seguridad:

Establecimiento de políticas y normas en la utilización del recurso de red

- Control de recursos y políticas de red.
- Herramientas para analizar el debido uso de la red.

6.1.5.8 Áreas funcionales

Las áreas funcionales están compuestas por una serie de gestiones que se definen a continuación:

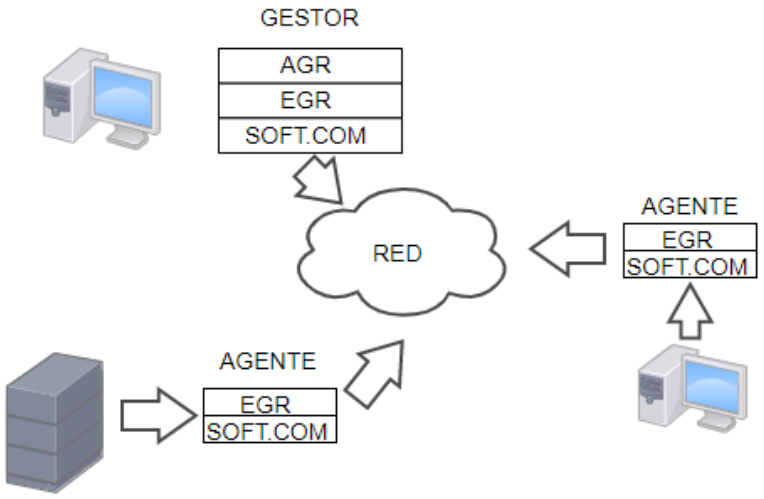
- Gestión de fallos: Identificación de problemas en la red, y su respectivo mantenimiento, recuperación.
- Gestión de contabilidad: Monitoreo del uso de recursos de red por parte de un grupo de usuarios.
- Gestión de configuración: Inicialización (start t-up) y desconexión (shut-down) ordenada de la red o de parte de ella. Mantenimiento y adicción de componentes, y actualización de componentes (reconfiguraciones).
- Gestión de prestaciones: Garantizar la Calidad del funcionamiento. asegurar que las capacidades de la red correspondan con las necesidades de usuarios finales.
- Gestión de seguridad: Control de acceso a la información contenida en los elementos de la red, protección ante fallos intencionados o accidentales, accesos no autorizados, etc

Como lo hemos mencionado anteriormente; la gestión de la contabilidad se encarga de monitorear el uso de los recursos de la red, por un usuario en específico o grupo de usuarios; En la ilustración 1 podemos observar que los host trabajan sobre unos elementos como lo son los EGR (Entidad de gestión de red) los cuales están presentes en cada nodo de la red, encargada de recolectar las estadísticas de la actividad de la red y llevarlos a la estación de control. Ahora bien; para que la

estación de control pueda monitorear las actividades de la red y sus componentes, lo realiza por medio del AGR (Aplicación de gestión de red) la cual permite mostrar información y generar comandos administrativos sobre los componentes de la red.

Entonces en la ilustración 1 vemos un conjunto de host y dispositivos de red, interconectados con una estación de control la cual por medio de los EGR y los AGR puede centralizar la información que se recolecta por estos elementos de la gestión de redes.

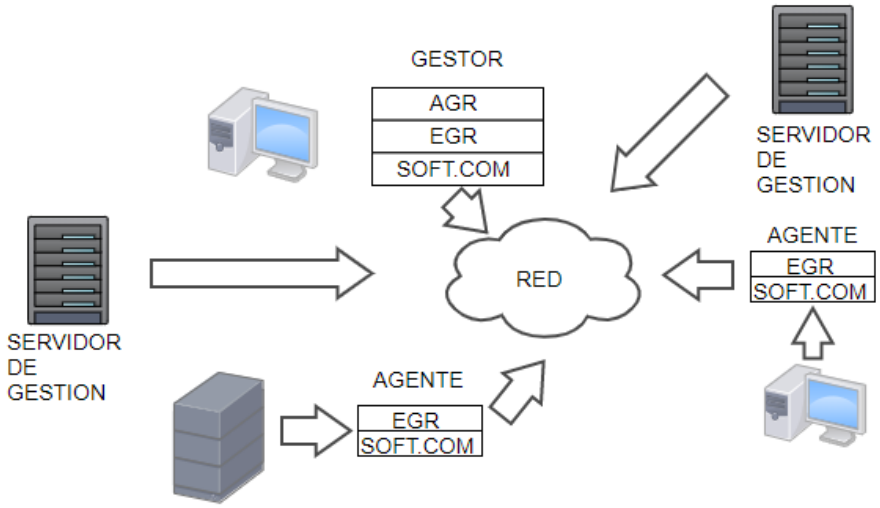
Ilustración 1 Gestión de contabilidad



Fuente: https://www.tamps.cinvestav.mx/~vjsosa/clases/redes/GestionRedes.pdf

La gestión de fallos; localiza los problemas y fallas en la red, como observamos en la ilustración 2, la cual nos muestra una red compuesta por una estación de control (encargada de la administración de la red) Dos servidores de gestión; los cuales están configurados para permitir las gestiones de los diferentes dispositivos de la red. Por medio de los AGR y los EGR la estación de trabajo tiene la capacidad de identificar las fallas y por medio de los servidores de gestión, reaccionar ante las fallas presentadas en la red.

Ilustración 2 Gestión de fallos



Fuente: https://www.tamps.cinvestav.mx/~vjsosa/clases/redes/GestionRedes.pdf

6.2. TIPOS DE SOFTWARE EN EL MERCADO

En el siguiente capítulo vamos a conocer los diferentes softwares de monitoreo de redes existentes en el mercado; tanto licenciados como open source, con el fin de conocer las características de cada uno y así tener un amplio conocimiento sobre estos softwares a la hora de una posible implementación en la empresa.

6.2.1 Software de monitoreo Open Source

Gracias a la gestión de red[9], podemos monitorizar nuestras redes empresariales con el objetivo de saber cuál es el tráfico que circula por nuestra red, para alguna empresa ha sido un reto la implementación de estas ayudas, ya que todas no tienen la capacidad económica para realizar dicha implementación, por motivo de que los software licenciados tiene un costo demasiado alto más el mantenimiento y soporte de este.

Ahora bien, esto ya no es una excusa de no implementar un sistema de monitorización, A continuación, vamos a listar algunos softwares los cuales son de licenciamiento libre (Llamados open source) herramientas gratuitas la cuales

[9] Que es la gestión de red(online) Cuba, Citado (31/09/2018) Disponible en: https://www.ecured.cu/Gesti%C3%B3n_de_Redes

cumplen las funciones que las licenciadas, pero un poco menos robustas en utilidades como las licenciadas.

6.2.1.1 Naggios

Es el software de monitorización de red más popular del software open sources, se diseñó para soportar originalmente Linux, proporciona monitorización de los servicios de red (smtp, pop3, http, nntp, icmp, snmp, ftp, ssh), recursos de host como (carga de procesador, uso de disco, registros del sistema) la administración remota es a través de túneles SSH o SSL cifrado. Para detectar equipos que están shutdown o inalcanzables, nagios permite definir jerarquía de la red de acogida con los host padre, cuando los servicios presentan dificultades, la notificación es enviada al administrador a través del correo electrónico o sms, tal y como este configurado el medio de alerta.

6.2.1.2 Zabbix

Monitorea y da seguimiento de la situación de los diferentes tipos de servicios de red, servidores y otro hardware de red. Zabbix tiene grandes funcionalidades de visualización incluidas las vistas definidas por el usuario, zoom, y la cartografía. Tiene un método de comunicación versátil que permite una configuración rápida y sencilla de los diferentes tipos de notificaciones de eventos predefinidos. Cuenta con tres módulos principales: el servidor, los agentes, y el usuario. Para almacenar los datos de seguimiento, puede utilizar MySQL, PostgreSQL, Oracle o SQLite como base de datos. Sin necesidad de instalar ningún software en el host de seguimiento, Zabbix permite a los usuarios comprobar la disponibilidad y capacidad de respuesta de los servicios estándar, como SMTP o HTTP. Para supervisar las estadísticas, tales como carga de la CPU, utilización de la red y espacio en disco, un agente de Zabbix debe estar instalado en la máquina host. Zabbix incluye soporte para el monitoreo a través de SNMP, TCP y controles ICMP, IPMI y parámetros personalizados como una opción para instalar un agente en los hosts.

6.2.1.3 Zennos

Basado en zope y escrito en python,zennos es un servidor y la plataforma de gestión de red que combina la programación y varios proyectos de código abierto para integrar el almacenamiento de datos y los procesos de recopilación a través de la interfaz de usuario basada en la web, permite revisar la disponibilidad, inventario, configuración, desempeño y acontecimientos, Supervisa la disponibilidad mediante SNMP,SSH,WMI, servicios de red (http,pop3,nntp,snmp,ftp)

6.2.1.4 Munin

Al igual que los Cacti, Munin utiliza RRDtool para presentar resultados en gráficos a través de una interfaz web. Cuenta con una arquitectura de maestro/nodo en el que el maestro enlaza a todos los nodos a intervalos regulares y que solicita los datos. Usando Munin, puedes rápida y fácilmente para supervisar el rendimiento de sus equipos, redes, redes SAN, y las aplicaciones. Esto hace que sea sencillo para detectar el problema cuando se produce un problema de rendimiento y ver claramente cómo lo está haciendo de la capacidad racional de todos los recursos restringidos. Para el plugin Munin, su prioridad principal es la arquitectura plug and play. Tiene un montón de plugins de control disponibles que fácilmente funcionarán sin una gran cantidad de modificaciones.

6.2.2 Software de monitoreo licenciado

Es importante que una empresa pueda contar con la posibilidad de adquirir un sistema licenciado, pues tiene la ventaja de soporte técnico en caso de falla por parte de su respectivo proveedor, garantía por la cual no corre un sistema gpl.

6.2.2.1 Pandora fmc

Es un conjunto de herramientas que permitirá a los administradores de red a sacar el máximo rendimiento de las infraestructuras que gestione.

- Descubre todos los host que hacen parte de la infraestructura
- Localice cuellos de botella y rediseñe su red.
- Controlé que cantidad de ancho de banda utilizan sus aplicativos y actué en base a sus rendimientos.
- Localice geográficamente todos sus componentes.
- Permite añadir panales de monitorización, sistemas, servidores, aplicaciones y procesos de negocio.
- Monitoriza hasta 100.000 agentes usando un solo servidor.

Crea su propia arquitectura desde cero, el cual permite escalar en entornos grandes, ya que tiene la capacidad comprobada de monitorizar más de 100.00 nodos sin problemas de rendimiento. Es amigable con la tecnología de dispositivos móviles, desde ellos se puede acceder a la administración y también hacen parte del monitoreo.

6.2.2.2 Groundwork

GroundWork Monitor reúne sus infraestructuras física, virtual y basada en la nube en una sola plataforma.

Donde quiera que sus aplicaciones publiquen datos, puede recopilarlos en GroundWork y seguir el estado de la aplicación. Coloque todos los datos clave de rendimiento de las aplicaciones en un solo lugar para la sintonización y la resolución de problemas. Reciba alertas de degradación del rendimiento Ver la pila de aplicaciones, el dispositivo y los datos de red juntos para la resolución de problemas Administre los SLA y mida el rendimiento de su servicio comercial

Los servidores monitoreados virtuales y físicos son el corazón del negocio. Monitoree cada máquina virtual interconectada, servidor, contenedor y más. Implementar automáticamente la monitorización con cada evento de escalado.

Gráficos completos e historial para sus hipervisores, máquinas virtuales y redes.

Amplia cobertura del dispositivo para servidores monitoreados y tipos de máquinas virtuales.

Con una supervisión inteligente y unificada que comprende su red, puede conocer los problemas de la red antes que nadie. El descubrimiento automático y el mapeo de topología pueden sofocar las tormentas de alarma. Con monitoreo unificado, toda la información que se necesita para mejorar la red está en un solo lugar. Las notificaciones y la correlación avanzadas lo ayudan a atravesar los miles de eventos y llegar al meollo del asunto.

Monitorear métricas detalladas y agregar Autodescubrimiento y mantenimiento de red y dispositivos La comprensión de la topología suprime las alarmas que no necesita

Recopila datos a través de SNMP, CPD, LLDP, IPMI y mucho más Admite OpenDaylight SDNs

6.2.2.3 Monitis

Está enfocada en pequeñas y medianas empresas. Cubre con todas las necesidades que puede tener una empresa con una infraestructura no muy robusta. Esta aplicación incluye monitoreo de transacciones web, monitoriza sistemas de aplicaciones en la nube como Racks pace y Amazon. Posee una interfaz gráfica y personalizable.

Las únicas desventajas es que está enfocada a Linux y Windows, no tiene mayor cobertura en las diferentes distribuciones. Es una herramienta licenciada y es difícil de añadir monitorizaciones ad-hoc.

6.2.2.4 Icinga

Realizada en base del core Nagios, el cual le mejoraron la interfaz gráfica, tiene la capacidad de integrarse con varios tipos de bases de datos, es amigable con para integrarse con otras aplicaciones, se enfoca principalmente a redes complejas y la monitorización de protocolos, recurso de los host y servidores de la infraestructura.

Es una herramienta con diferentes módulos, diseñados paras las diferentes necesidades de las empresas y tipo de infraestructura.

6.2.2.5 Manage Engine/opmanager

Es una de las herramientas con más demanda en el mercado, es fácil de instalar, su calidad de grafico son excepcionales, ofrece gran variedad de funcionalidades a cubrir.

Las desventajas del aplicativo es que es sus configuraciones son muy complejas ya que tienen demasiada documentación. Solo es instalable en plataforma Windows y Linux, carece de inventario y la correlación de los eventos.

6.2.2.6 Observium

Software de monitorización enfocado a Linux, Unix, hp, sus graficas se destacan por su gran detalle y diseño, para mostrar información a nivel gerencial.

La interfaz es muy amigable con la vista y muy práctica para su uso, tiene la capacidad de monitorizar grandes infraestructuras.

6.2.2.7 Op5 monitor

Principalmente se centra en la monitorización de hardware, tráfico y servicios de red. También está basada en Nagios.

Es capaz de monitorizar múltiples plataformas, sistemas en la nube y entornos virtuales.

Es fácil de usar y tiene un buen sistema de balanceo de cargas.

6.2.2.8 Opsview

Herramienta especializada en la monitorización de red y de aplicaciones, de igual manera a otros aplicativos también se empezó a trabajar a partir de Nagios.

Su demanda es similar al op5 monitor.

Sus desventajas es que su panel de monitorización es muy rígido, los informes son limitados sin la opción de ser exportados.

6.2.2.9 Prtg network monitor

Solución de monitorización para entornos completos de tecnología, desde ambientes virtualizadas, hardware, tráfico de datos y aplicaciones. Realiza monitoreo de disponibilidad y el desempeño de los mismos.

Este aplicativo es multiplataforma, permite mostrar informes en tiempo real.

Su interfaz gráfica es agradable y amigable para su manipulación, tiene la posibilidad de ingresar administrativamente desde dispositivos móviles. Su sistema de alertas es robusto y tiene la capacidad de generar informes en pdf y html.

6.2.2.10 Solarwinds

Es una herramienta realmente robusta, se destaca por su mapeo de redes automáticos, su interfaz gráfica es amigable y robusta en el que se puede ver fácilmente la topología de red y su estado. Tiene la falibilidad de monitorear máquinas virtuales, algunas de sus ventajas es su entorno gráfico, y el acceso administrativo desde dispositivos móviles.

Algunos de sus defectos es que no se familiariza con aplicativos de la nube estilo Amazon, la generación de informes no es de muy buena presentación. Cada módulo es una licencia diferente.

6.2.2.11 Whatsup gold

Excelente herramienta para la monitorización, una de las mejores en balancear cargas, es totalmente automática, reacciona frente algunos eventos ocurridos. Tiene la capacidad de auto descubrir las topologías como pandora y solarwinds.

Se pueden integrar otras aplicaciones o servicios de monitorización. Tiene la capacidad de monitorear entornos en la nube que incluye amazon web services y los servidores azure, monitorea, informa y alerta sobre los estados y los rendimientos de cada métrica que en la nube se recopila.

Permite monitorear las redes inalámbricas con más detalle, monitores tipo radio para un mejor diagnóstico, actualiza la superposición inalámbrica con una visualización más clara de los SSID activos de cada ap.

6.2.2.12 Microsoft network monitor

Su principal función es analizar protocolos y tener una supervisión del tráfico de red. permite a los usuarios a capturar los paquetes de la red local en tiempo real, lista y analiza el tráfico según el protocolo de transporte, nos permite realizar varias sesiones al tiempo que pueden ser en tiempo real desde servidores azure, powershell o bases de datos. Tiene la capacidad de establecer filtros de manera que se evita capturar paquetes innecesarios. Tiene la opción de monitorizar tarjetas de red locales, servidores, vpn, tarjetas de red remotas.

6.2.3 Comparativos de monitores de red

En la siguiente tabla encontramos los comparativos de cada uno los programas de monitorización, evaluando el tipo de protocolo, gráficos y sus diferentes módulos que componen los softwares.

Tabla 1, Comparativo de sistemas de monitoreo

Software	**Graficas**	**Agentes**	**Snmp**	**Syslog**	**Alertas**	**App web**	**Licencia**	**Mapas**
Nagios	Si	Si	Si	Si	Si	Si	Free	Si
Pandora	Si	Si	Si	Si	Si	Si	Si	Si
Op5	Si	Si	Si	Si	Si	Si	Si	Si
Munin	Si	Si	Si	Si	Si	Si	Gpl	No
Zennos	Si	Si	Si	Si	Si	Si	Gpl	Si
Solarwind	Si	Si	Si	Si	Si	Si	Si	Si
Ground	Si	Si	Si	Si	Si	Si	Gpl	No
Opmanager	Si	Si	Si	Si	Si	Si	Si	Si
Zabbix	Si	Si	Si	Si	Si	Si	Gpl	Si
Monitis	Si	Si	Si	Si	Si	Si	Si	Si
Icinga	Si	Si	Si	Si	Si	Si	Si	Si
Opmanager	Si	Si	Si	Si	Si	Si	Si	Si
Observium	Si	Si	Si	Si	Si	Si	Si	No
Ops view	Si	Si	Si	Si	Si	Si	Si	Si
Prtg	Si	Si	Si	Si	Si	Si	Si	Si
Whatssapgold	Si	Si	Si	Si	Si	Si	Si	No
Microsoft network	Si	Si	Si	Si	Si	Si	Si	Si

Fuente: El autor.

7. ATAQUES ORIENTADOS A REDES DE DATOS.

Como es de conocimiento; en el mundo informático hay miles de ataques cibernéticos, pero en este capítulo solo vamos hacer énfasis a los ataques orientados a la red, en donde se vea involucrado las acciones de un software de monitoreo de redes. No es nada coherente que mencionemos ataques que no tengan ninguna afectación con la red.

7.1. TIPOS DE ATAQUES

A continuación, vamos a conocer los diferentes ataques informáticos orientados a la red. Ataques que afectan directamente con el desarrollo de las empresas.

7.1.2 Denegación de servicios (DOS)

Ataque hacia un conjunto de host o redes, que suspende el servicio o recursos que prestan otros dispositivos haciéndolos inaccesibles. Comúnmente ocasiona perdida de conectividad por el aumento de consumo del ancho de banda o la sobrecarga de recursos de los sistemas que prestan el servicio.

El ataque provoca la saturación en los puertos con altos flujos de información. Provocando que los servidores se sobrecarguen y no tenga la capacidad de seguir transportando la información y prestando el debido servicio. Evitando que el servidor no de abasto con las conexiones simultaneas.

EL ataque de denegación de servicios tiene diferentes maneras de ejecutarlas:

7.1.3 Inundación de SYN (SYN Flood)

Se envía una serie de paquetes tcp/syn, casualmente con las direcciones ip de origen falsificadas, todos los paquetes enviados son recibidos como peticiones de conexión. Provocando que el server intente restablecer las conexiones al responder con paquetes de respuesta TCP/ACK. Entonces debido a que la dirección ip es falsa las respuestas nunca van a llegar. Estos paquetes consumen los recursos y limitan

la cantidad de conexiones al servidor. Evitando que el servidor pueda responder a las direcciones legitimas.

7.1.4 Inundación de ICMP (ICMP flood)

El objetivo de este ataque es consumirse todo el ancho de banda de la víctima, empieza a enviar paquetes de forma continua (paquetes ICMP) de un tamaño considerable. En donde la victima responde con ICMP (pong) lo que ejecuta una sobrecarga en el sistema de la víctima y de la red por la cual transita.

7.1.5 Inundación UDP (UDP flood)

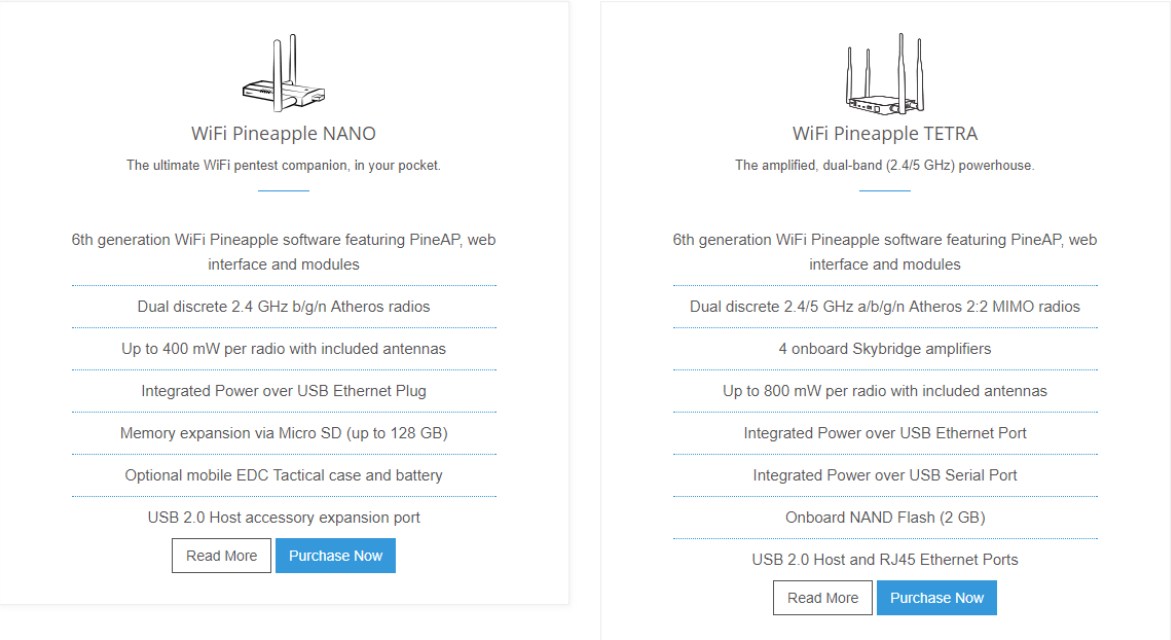
Este ataque consiste en enviar muchos paquetes udp a las víctimas, casualmente el ataque se realiza contra equipos que utilizan el servicio echo generando que los mensajes echo aumenten su tamaño.

7.1.6 Wifi pine-apple

Dispositivo con la función de buscar vulnerabilidades en las redes WIFI o inalámbricas, Buscando si existe alguna debilidad que permita a cuál intruso a incadir nuestra red poniendo en peligro la infraestructura tecnológica y todos los datos que viajan y se almacenan en esta.

Como lo sabemos la gente utiliza estas herramientas para fines ilegales, con esta herramienta se pueden realizar ataques de DNS spoofing, Tener acceso a páginas navegadas de cualquier dispositivo que haga parte de la red, Ataques de MINM (man in the middle) hombre en el medio, permitiendo espiar todo el tráfico que corre en la infraestructura, herramienta la cual permite intrusiones a redes de datos por medio inalámbrico tal y como se observa en la ilustración 3.

Ilustración 3. Dispositivo Wifi pine-apple



Fuente: https://www.redeszone.net/2017/06/28/wi-fi-pineapple-hacking-etico/

7.1.7 Malware

Software malicioso o código malicioso, donde su objetivo es dañar un sistema o causar un mal funcionamiento.

Incluye virus, gusanos y caballos de Troya.

El malware accede a su dispositivo a través de internet y del correo electrónico, aunque también puede conseguir acceder a través de sitios web hackeados, demos de juegos, archivos de música, barras de herramientas, software, suscripciones gratuitas o cualquier descargue de internet en un dispositivo que no esté protegido con software antimalware

7.1.8 Spear phising

Es un ataque de suplantación de correo electrónico, dirigido a una organización o individuo especifico que busca acceso no autorizado a información confidencial.

Los intentos de suplantación de identidad no suelen ser iniciados por piratas informáticos al azar, pero es más probable que sean víctimas por piratas para obtener ganancias financieras, secretos comerciales o información militar.

7.1.9 Clickjacking

Es un nuevo método de ataque realizado a través del navegador de internet, donde su objetivo es engañar a las víctimas con una capa transparente colocada delante de un enlace o cuadro de dialogo, lo que permite que el usuario pulse un enlace sin percatarse de dicha acción.

Por lo tanto, es similar al ataque de CSRF (cross-site request forgery)

- Realizar acciones no deseadas en páginas en las que estemos autenticados, como por ejemplo modificar parámetros de configuraciones de privacidad/seguridad de un perfil de MySpaceo enviar información privada al atacante.
- Creación de sitios de phishing más creíbles utilizando la página del banco auténtica como fondo.
- Obtención de beneficio económico mediante fraude en publicidad basada en número de clicks.
- Fraude en votaciones

7.1.10 Ataque de WannaCry

Este es una derivación de un ransomware, el cual ataca secuestrando al información del usuario en su equipo de cómputo o cualquier almacenamiento que encuentre en la red, basado en sistemas operativos Windows, este ataque, solo deja habilitados dos archivos dentro de la máquina del usuario, los cuales hacen referencia a las instrucciones de recuperación de información y el wanna Decryptor, el cual al abrirlo, supone la liberación de los archivos, los cuales solo se logra pagando un rescate según las instrucciones del usuario.

7.1.11 Petya

Es un malware, el cual , apareció poco después simulando ataques de tipo WannaCry o Ransomware, principalmente en sistemas operativos Windows, los

cuales no habían instalado una actualización de seguridad para sanear, un problema expuesto de sistemas operativos Windows, el cual, como lo hicieron sus otros derivados de Ransomware, exploto efectivamente la vulnerabilidad causando diversos problemas en empresa de todo el mundo, este al igual que los demás tipo ransomware, alcanza a dejar inservible el sistema, al realizar un ataque directo al MBR y dejarlo inservible.

7.1.12 Ramsonware

Describe un ataque informático, muy común durante 2017 en diferentes partes de mundo, el cual, se encarga de tomar control de los equipos e computo bloqueando sus accesos a la información, hasta tanto el usuario final o propietario de la información, haga pagos exigidos por el atacante, normalmente, se utilizó la modalidad de pago con Bitcoins, dado que se transaba la información con esta moneda digital

7.1.13 DDos Botnet Mirai

Este ataque fue recordado por su afectación a las plataformas Play Stations y Twitter, las cuales sufrieron caídas de varios de sus servicios durante el ataque de DDoS, este ataque fue materializado, usando la Botnet Miari, esta Botnet, está desarrollada para atacar dispositivos, enmarcados en los nuevos procesos de IoT, por eso, ha afectado principalmente, Routers, Cámaras de seguridad con funciones de IP y reproductores de video principalmente. Este ataque dejo sin servicio de mensajería a millones de personas en todo el mundo por varios minutos y afecto los procesos online de las plataformas de Play Stations.

Para la detección de este tipo de ataques, es importante contar con algún IDS e IPS los cuales, puedan realizar bloqueos al detectar alguna anormalidad tratando de entrar a nuestra red, estos sistemas, tienen prestaciones proactivas, que pueden impedir la materialización de ataques de este tipo.

7.1.14 Spy.Agent.NZD Troyano

Este es un tipo de troyano, que afecto empresas principalmente de mensajería instantánea en estados unidos, los cuales, lograron que, al materializar sus ataques, las empresas suspendieran la prestación del servicio.

Estos troyanos son de tratamiento principalmente a nivel de Anti Spam y seguridad perimetral con firewall, son unos ataques enfocados la reproducción dentro de la red de algún tipo de software mal intencionado, normalmente en su materialización, compromete múltiples equipos e información.

7.1.15 El Phishing

Esta es una de las modalidades de ataques informáticos más escuchadas y aunque lleva mucho tiempo en el mundo del cibercrimen, aún es usada con bastante frecuencia dentro de entorno reciente, de esta afirmación podemos recordar los múltiples correos electrónico falsos, con encabezados de La Fiscalía general de la nación , del ICBF entre otras muchas entidades, principalmente del estado y bancos, los cuales, insertan en estos viejos trucos de Phishing para tratar de vulnerar la seguridad de la información de las empresas y personas.

Aquí, es fundamental, capacitar a las personas en cómo identificar este tipo de amenazas, esto, se puede complementar con servicios antispam, filtros de correo alternativos y seguridad perimetral, cada uno de estos, realizando tareas, en pro de la detección temprana y deshecho de este tipo de ataques.

7.1.16 Virus informático

Programas o Ficheros que se cargan en los equipos sin el consentimiento del usuario. Son archivos totalmente molestos, destructivos, diseñados para infectar y tomar control de los sistemas que se muestran vulnerables. Los virus se pueden propagar a través de redes y equipos, realizando una reproducción masiva o realizando copias de sí mismo. De la misma manera de los virus biológicos que se transmiten entre las personas.

Normalmente los virus se esconden en programas comunes, como puede ser en juegos o documentos, se puede recibir archivos infectados adjuntos en correos o archivos que se descaran desde los sitios web. En cuanto se ejecuta el archivo, el virus se activa automáticamente y empieza a realizar los procedimientos a los cuales este fue elaborado, como duplicarse y realizar cambios notorios en el sistema operativo, provocando serios daños en este.

7.1.17 Adware

Software o fichero que se instala de forma oculta, con el propósito de colocar y mostrar varios anuncios en los navegadores de internet o sitios en los que antes no se exhibían. Además de hacer uso indeseado de los recursos de funcionamiento (reduciendo el rendimiento de la memoria RAM) en donde el ataque va ofreciendo publicidad basada en el historial de nuestros navegadores con el registro de visitas o búsquedas que se realiza.

7.1.18 Spyware

Software espía que recopila la información de los equipos, transmitiéndolos a otra entidad sin que los propietarios de la información se den cuenta, Es un ataque que resulta peligrosa para las empresas ya que se puede filtrar información sensible a otras empresas que pueden ser la competencia directa de la nuestra. Además, la información hurtada puede convertirse en otro tipo de ataques, como chantajes y extorsión a las víctimas

7.1.19 Gusanos

Se multiplican en Diferentes sistemas, por medio de envío masivo de copias de sí mismo vía email u otras vías de contacto, como redes domésticas y de WiFi. Por esto es importantísimo tener especial cuidado con los datos que insertamos cuando estamos conectados a redes inalámbricas de acceso público.

7.1.20 Caballo de Troya o troyano

Tipo de malware que a Siempre se disfraza de software legítimo. Los cibercriminales y hackers pueden utilizar troyanos para tratar de acceder a los sistemas de los usuarios. Generalmente, los usuarios son engañados por alguna forma de ingeniería social para que carguen y ejecuten troyanos en sus sistemas. Una vez activados, los troyanos permiten a los cibercriminales espiarte, robar tu información confidencial y obtener acceso de puerta trasera a tu sistema. Estas acciones pueden incluir:

- Borrar datos
- Bloquear datos
- Modificar datos
- Copiar datos
- Interrumpir el funcionamiento de PC o redes de diferentes dispositivos.

A diferencia de virus y gusanos, los troyanos no son capaces de auto replicarse.

Los troyanos se clasifican según el tipo de acciones que pueden realizar en tu computadora:

- Backdoor
  Un troyano backdoor (puerta trasera) ofrece a los usuarios maliciosos control a distancia de la computadora infectada. Permiten que el autor haga cualquier cosa que desee en la computadora infectada, como enviar, recibir, ejecutar y borrar archivos, mostrar datos y reiniciar la computadora. Los troyanos backdoor a menudo se usan para crear un grupo de computadoras víctimas y formar una red botnet o zombi que puede usarse para fines delictivos.
- Exploit
  Los exploits son programas que contienen datos o códigos que aprovechan una vulnerabilidad del software de aplicaciones que se ejecutan en la computadora.
- Rootkit
  Los rootkits están diseñados para ocultar ciertos objetos o actividades en tu sistema. A menudo su propósito principal es evitar la detección de programas maliciosos para ampliar el período en el que pueden ejecutarse en una computadora infectada.
- Trojan-Banker
  El objetivo de los programas Trojan-Banker es robar los datos de cuentas de sistemas de banca en línea, sistemas de pago electrónico y tarjetas de crédito y débito.
- Trojan-DDoS
  Estos programas realizan ataques DoS (denegación de servicio) contra una dirección web dirigida. Mediante el envío de numerosas solicitudes (desde tu computadora y desde varias otras computadoras infectadas), el ataque puede desbordar la dirección objetivo y provocar una denegación del servicio.
- Trojan-Downloader
  Los Trojan-Downloaders pueden descargar e instalar nuevas versiones de programas maliciosos en tu computadora, incluso troyanos y adware.
- Trojan-Dropper
  Los hackers utilizan estos programas con el fin de instalar troyanos o virus, o evitar la detección de programas maliciosos. No todos los programas

antivirus son capaces de examinar la totalidad de componentes que incluye este tipo de troyano.

- Trojan-FakeAV
  Los programas Trojan-FakeAV simulan la actividad del software antivirus. Se han diseñado para extorsionarte (a cambio de la detección y eliminación de amenazas, aun cuando en realidad no existan).
- Trojan-GameThief
  Este tipo de programa roba información de la cuenta de usuario de jugadores en línea.
- Trojan-IM
  Los programas Trojan-IM roban credenciales de inicio de sesión y contraseñas de programas de mensajería instantánea, como ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype y muchos otros.
- Trojan-Ransom
  Este tipo de troyano puede modificar datos en tu computadora, para alterar su correcto funcionamiento o para que no te deje usar datos específicos. El delincuente solo restaurará tu computadora a su estado de funcionamiento normal o desbloqueará tus datos cuando le hayas pagado el rescate exigido.
- Trojan-SMS
  Estos programas envían mensajes de texto desde tu dispositivo móvil a números de teléfono de tarifa prémium y pueden salirte caros.
- Trojan-Spy
  Los programas Trojan-Spy pueden espiar cómo usas tu computadora; por ejemplo, a través del seguimiento de los datos que ingresas con el teclado, de capturas de pantalla o de una lista de las aplicaciones en ejecución.
- Trojan-Mailfinder
  Estos programas pueden recolectar direcciones de correo electrónico desde tu computadora.

7.2. ATAQUE MAN IN THE MIDDLE

Para realizar este ataque se montó un ambiente controlado, para evitar afectar a diferentes empresas o personas y por ética profesional no incurrir con la ley 1273 del 2009 referente a la seguridad informática de la república de Colombia.

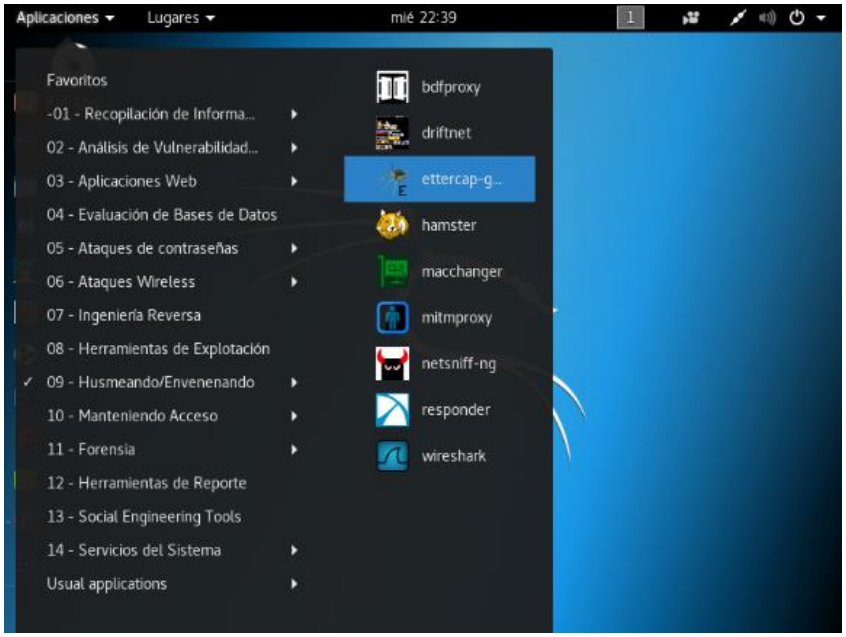
Para ejecutar dicho ataque se necesitó de un computador origen en el cual se crean unas máquinas virtuales por medio de un software de virtualización.

En la maquina origen se crean dos máquinas virtuales que son; el sistema operativo kali Linux cuya función es hacer la auditoria o ataque, y un sistema operativo Windows 7 cuyo papel es ser la víctima del ataque.

Ahora si vamos a explicar el procedimiento del ataque:

Iniciamos con el sistema operativo kali Linux y buscamos el aplicativo ethercap ubicado en aplicaciones en la sección 09 husmeando/envenenado.

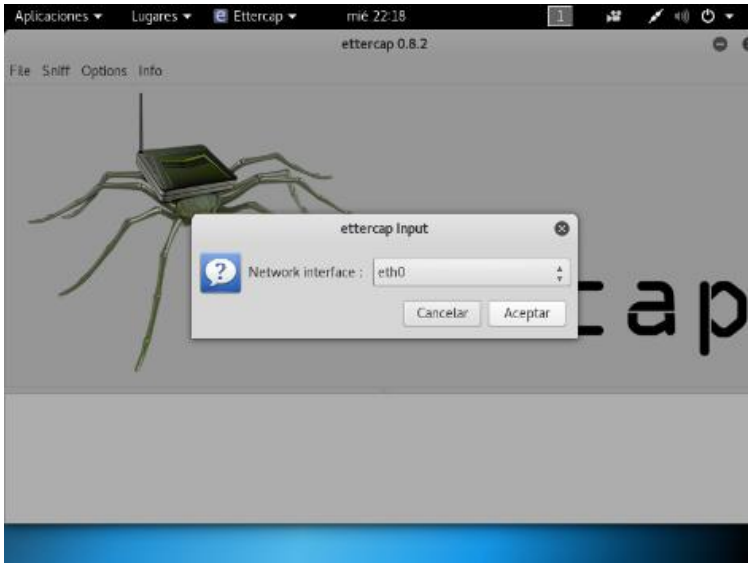
Ilustración 4. Inicio de ethercap



Fuente: El autor.

Luego de abrir el ethercap, seleccionamos la interfaz por la cual vamos a escuchar todo el tráfico.

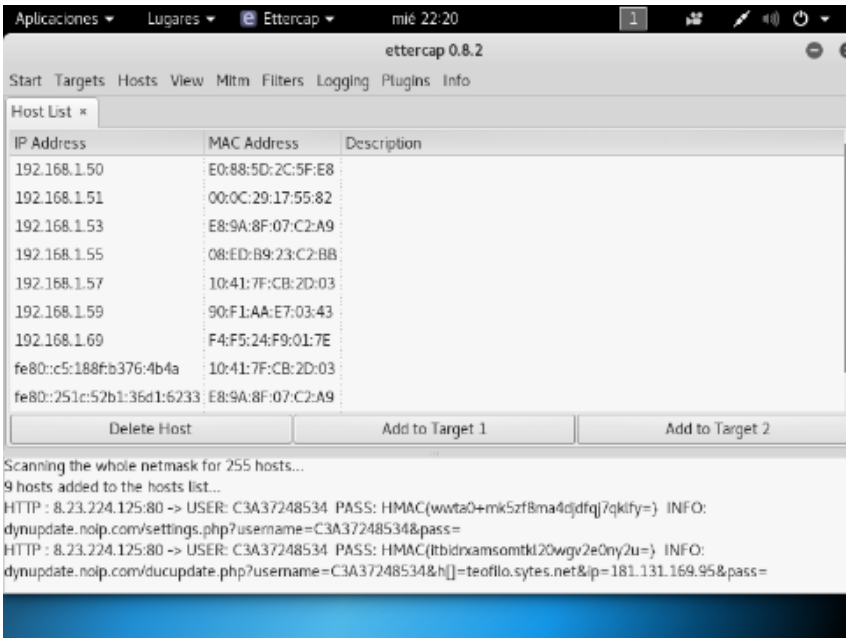
Ilustración 5. Selección de interfaz



Fuente: El autor

Luego de seleccionar la interfaz, vamos a listar todos los hosts que están conectados bajo la misma red en la opción host y presionamos en list host.

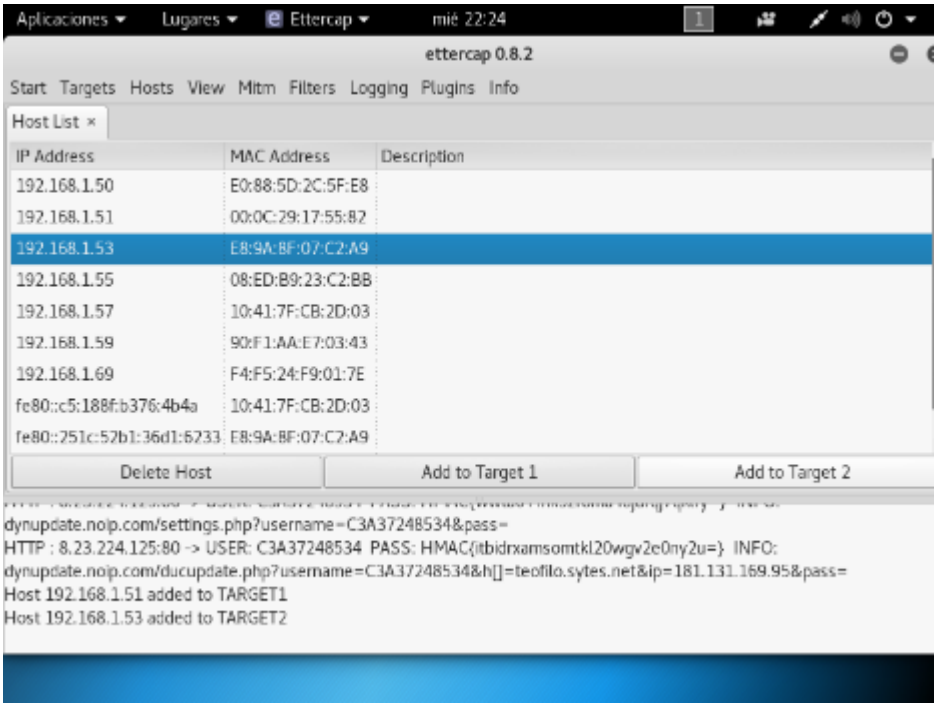
Ilustración 6. Listar los host



Fuente: El autor

Ahora que tenemos la lista de host, identificamos las ip de las víctimas, en este caso como es un ambiente controlado ya tenemos la claridad de cuáles son las víctimas. Seleccionamos el host víctima y presionamos el botón add to target1, de igual manera seleccionamos la segunda víctima y presionamos el botón add to target 2.

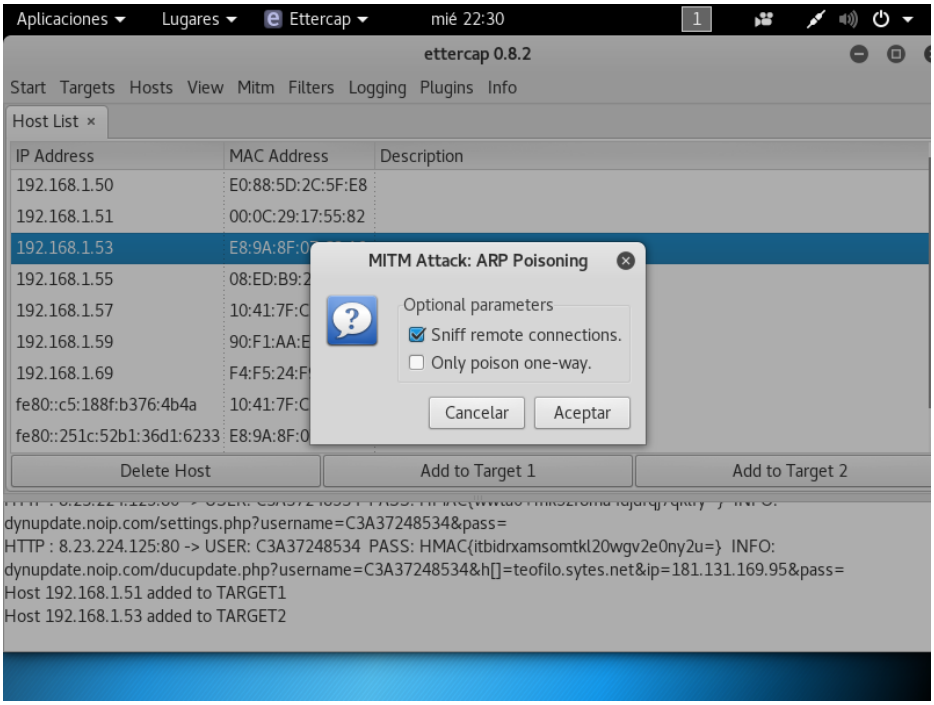
Ilustración 7. Selección de victimas



Fuente: el Autor

Ya con las victimas asignadas, vamos a presionar el botón start para iniciar la captura y el envenenamiento arp, el envenenamiento arp hacen que los host envíen la información al atacante creyendo que este es el enrutador. Luego elegimos la opción snift remote conection e inicia el procedimiento.

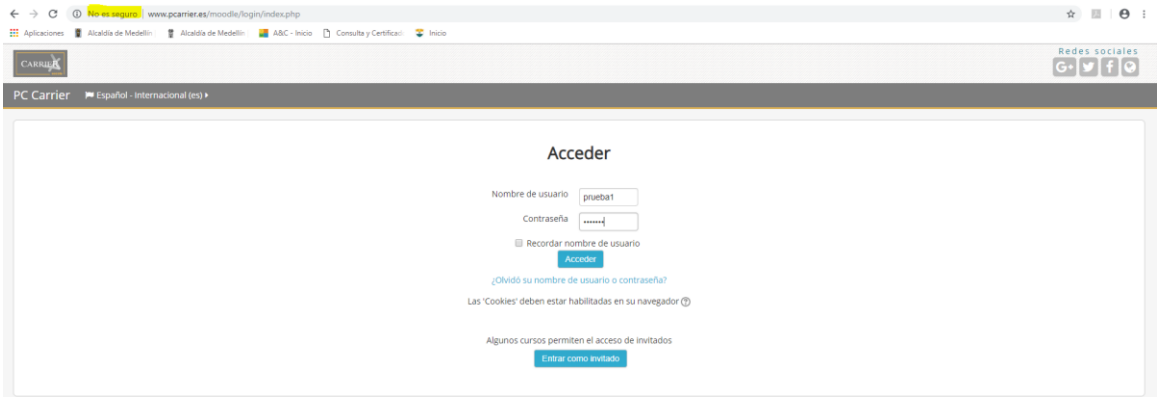
Ilustración 8. Inicio de la captura y envenenamiento



Fuente: El autor.

Ahora vamos a un pc víctima y nos vamos a loguear en una página la cual no tenga el protocolo https habilitado.

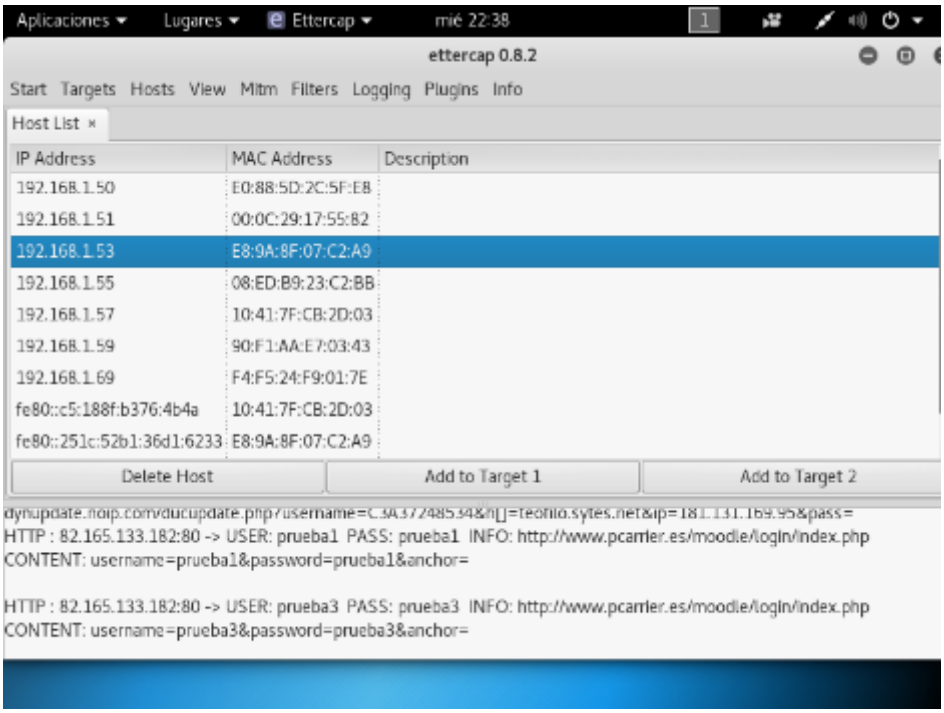
Ilustración 9. interfaz de la victima



Fuente: El autor.

Luego de ingresar las credenciales, Abrimos el ethercap y podemos darnos cuenta; que el ataque fue exitoso y los datos ingresados fueron capturados.

Ilustración 10. Captura de los datos



Fuente: El autor

Como podemos observar en la ilustración 10, Captura de los datos, se captura varias informaciones como lo son: protocolo, dirección ip, nombre de usuario y contraseña.

Nota: Cabe aclarar que el ataque ha sido en un ambiente controlado y dirigido a la red interna capturando todos los datos que viajan a través de ella y nuestro router, en ningún momento se está realizando ataques a la página la cual estamos colocando como ejemplo.

Aquí finaliza el ataque man in the middle, donde nos muestra que, si estuviera operando un sistema de monitoreo de red, este ataque no sería exitoso, ya que el

sistema de monitoreo lanza las alertas de actividades anormales en el tráfico o en su defecto podría mitigar el ataque de inmediato.

7.3. ATAQUE DE DENEGACION DE SERVICIOS

Para realizar este ataque se montó un ambiente controlado, para evitar afectar a diferentes empresas o personas y por ética profesional no incurrir con la ley 1273 del 2009 referente a la seguridad informática de la república de Colombia.

Para ejecutar dicho ataque se necesitó de un computador origen en el cual se crean unas máquinas virtuales por medio de un software de virtualización.

En la maquina origen se crean dos máquinas virtuales que son; el sistema operativo kali Linux cuya función es hacer la auditoria o ataque, y un sistema operativo metaspoitable el cual es un servidor web vulnerable cuyo papel es ser la víctima del ataque.

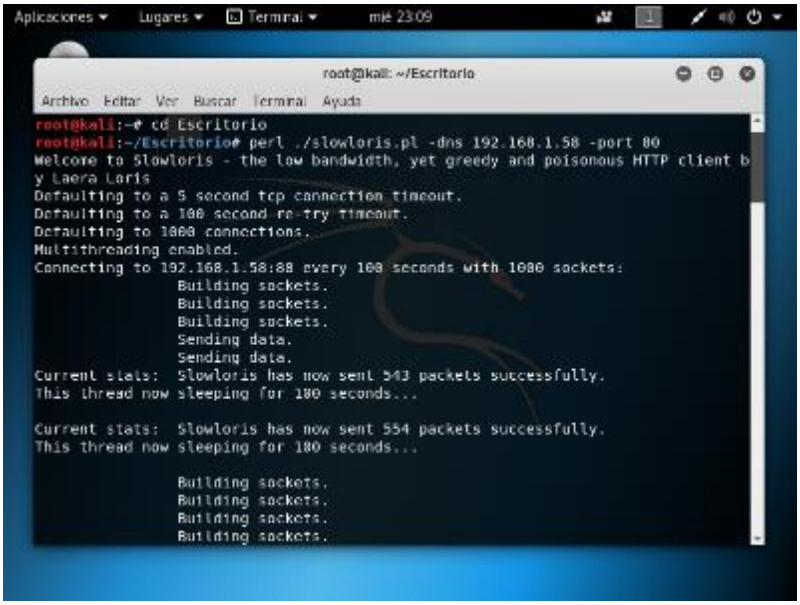
Ahora si vamos a explicar el procedimiento del ataque:

Para iniciar el ataque; ingresamos a la máquina virtual en la que está instalado el sistema operativo kali Linux. Luego de estar en el sistema vamos a utilizar la línea de comando invocando un archivo el cual es la configuración del ataque reprogramado previamente.

Iniciamos la línea de comandos y escribimos:

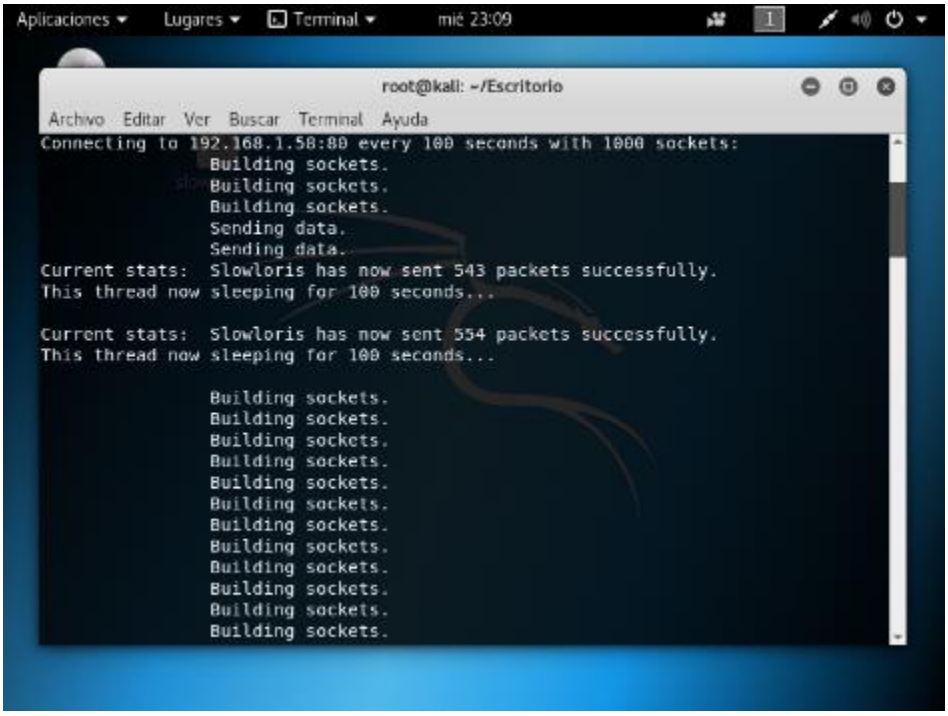
```
perl ./slowloris.pl -dns 192.168.1.58 -port 80
```

Ilustración 11. Ataque dos



Fuente: el autor

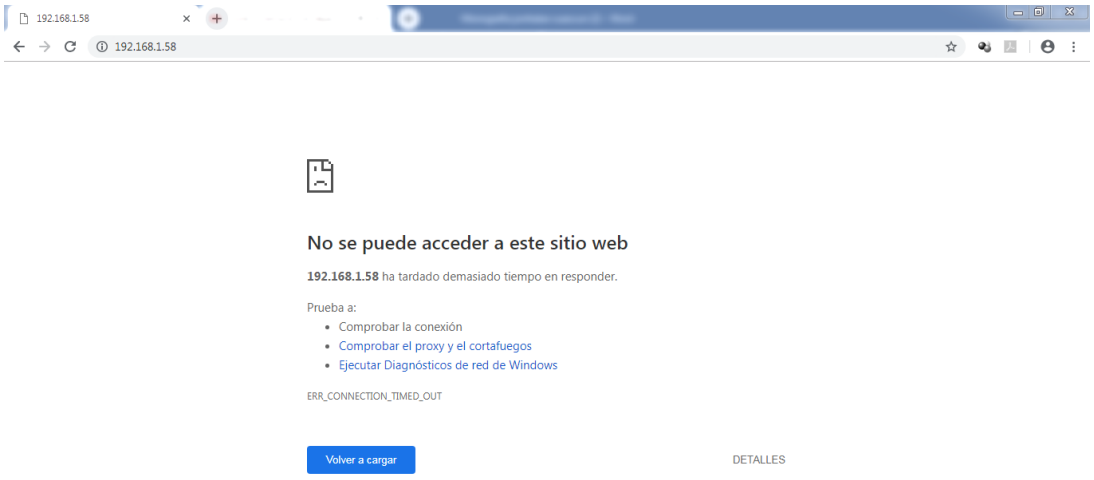
Ilustración 12. Proceso Ataque Dos



Fuente: el autor

Cuando validamos que el procedimiento está en proceso, vamos al explorador del equipo origen e intentamos ingresar a la página la cual estamos atacando en donde nos vamos a dar cuenta que el ataque está dando resultado.

Ilustración 13. Página caída



Fuente: El autor

8. CASOS DE ATAQUES A NIVEL EMPRESARIAL.

En este capítulo vamos a conocer por medio de referencias periodísticas, varios sucesos que han marcado la historia informática, de los ataques más sobresalientes a nivel empresarial. Tanto nacional e internacionalmente, con el fin de mostrar que los ataques cibernéticos no tienen limitación alguna por su ubicación geográfica.

8.1. HISTÓRICO DE ATAQUES INFORMÁTICOS MÁS SOBRESALIENTES A NIVEL INTERNACIONAL

Para poder saber a qué estamos expuestos, debemos conocer un poco de la historia de los ataques existentes en el medio, en el siguiente bloque vamos a mencionar los ataques más sobresalientes en la historia de la informática, con el objetivo de conocer los tipos de ataques y el número de afectados por cada ataque, buscando concientizar al lector sobre la seguridad informática y las consecuencias, perdidas que generan estos ataques informáticos.

8.1.2 El gran hack de eeuu 160 millones de usuarios

Afecto a una larga lista de personas, el ataque[10] se inició desde el 2005, los hackers intervenían las redes de más de una docena de empresas, robando y vendiendo información de identificación personal.

Los hackers tenían como blanco las tiendas minoristas relacionadas con transacciones financieras o trasmisión de datos financieros, donde hurtaron nombres de usuarios, contraseñas, medios de identificación. Números de tarjetas de crédito, débito.

[10] EEUU, desarticula una banda que hackeo 160 millones de tarjeta de crédito (online)Cnn, Usa, 25 de julio del 2013 Citado(31/09/2018) Disponible en: http://cnnespanol.cnn.com/2013/07/25/ee-uu-desarticula-una-banda-que-hackeo-160-millones-de-tarjeta-de-credito/

Este ataque produjo cientos de millones de dólares en pérdidas, los hackers ofrecían servicios de alojamiento web para esconder sus identidades y así poder vender la información hurtada.

La venta de números de tarjeta de crédito estadounidense estaba alrededor de10 dólares, las europeas cobraban 50 dólares y las canadienses costaban 15 dólares.

Las personas que compraban al por mayor obtenían descuentos por sus compras.

8.1.3 Adobe: 152 millones de usuarios

La empresa adobe sufrió un ataque[11] informático, donde los crackers tuvieron acceso a información de 2.9 millones de clientes y al código fuente de algunos productos de adobe.

Los crackers tuvieron acceso a identificación y contraseñas de los usuarios, asi como sus nombres, números encriptados de tarjetas de crédito y débito y su respectiva fecha de caducidad de las tarjetas.

8.1.4 Ebay 145 millones de usuarios

El ataque[12] que sufre ebay, no comprometió datos financieros de los usuarios como números de cuentas y tarjetas de crédito, al contrario, vulneraron una base de datos con los nombres de usuarios sus respectivas contraseñas encriptada, cuentas de correo electrónico, teléfono y fecha de nacimiento, solo datos personales las cuales no tuvieron relación con la parte financiera del usuario.

---

[11] Adobe sufre ciberataque y roban datos de 2.9 millones de clientes (online) RTVE,España, 04 de octubre del 2013, Citado (31/09/2018) Disponible en: http://www.rtve.es/noticias/20131004/adobe-sufre-ciberataque-roban-datos-29-millones-clientes/757880.shtml

[12]Ebay obliga a cambiar las contraseñas a sus usuarios a cambiar sus contraseñas (online)diario la Nación, Argentina, 21 de mayo del 2014, citado (31/09/2018) Disponible en: https://www.lanacion.com.ar/1693243-un-ataque-informatico-a-ebay-obliga-a-los-usuaris-a-cambiar-su-contrasena

8.1.5 Heartland 130 millones de usuarios

Un cracker de 28 años de edad, hackeo más de 130 millones de números de tarjetas de crédito y débito[13], invadieron las bases de datos de 5 compañías, los números fueron adquiridos de heartland payment, sistema de procesamiento de pagos con tarjetas. El cracker empezó a explorar las páginas web de las compañías para identificar sus brechas de seguridad. Identificaron el tipo de máquinas de pago que usaban los establecimientos.

Luego se idearon un ataque sql injection[14] para entrar en sus redes y robar los datos de las tarjetas de crédito y débito. Replicaron estos datos a un servidor localizado en california,Illinois,letonia,Holanda y ucrania.

Dicen las autoridades que es el mayor caso de hackeo y robo de identidades juzgado por el departamento de justicia de los estados unidos.

8.1.6 Tjx 45,7 millones de usuarios

La empresa Txj sufrio un ataque, en el cual se robaron 45.7 millones de tarjetas de crédito[15], en el cual un grupo de hackers accedieron a las bases de datos de clientes de la compañía y extrajeron todos los datos financieros. La empresa asegura que aproximadamente dos terceras partes de las tarjetas habían caducado en el momento del ataque, hubo un primer asalto en el cual solo robaron información sobre las transacciones, luego a los 3 meses sustrajeron los datos de los 45 millones de tarjetas.

---

[13] Un Cracker de 28 año, acusado de robar datos de 130 millones de tarjetas de credito (online),El mundo, EEuu, 17 de agosto del 2009, Citado (31/09/2018) Disponible en: http://www.elmundo.es/elmundo/2009/08/17/navegante/1250535175.html

[14] Que es Sql injection(online)Open webinars,Sevilla,12 de octubre del 2017, Citado(31/09/2018) Disponible en: https://openwebinars.net/blog/que-es-sql-injection/

[15] Txj denuncia el robo de información de 47.5 millones de tarjetas de crédito de clientes (online)Europa press, Nueva york, 29 de marzo del 2007, Citado(31/09/2018) Disponible en: http://www.europapress.es/internacional/noticia-eeuu-tjx-denuncia-robo-informacion-457-millones-tarjetas-credito-clientes-20070329192659.html

8.1.7 Aol 92 millones de usuarios

Según los medios el ataque fue ejecutado por un ex empleado de la compañía, el cual robo un listado de clientes con sus respectivas direcciones de correo electrónico y tipo de tarjeta de crédito, el implicado vendió la información a otro sujeto, el cual la utilizo para enviar publicidad por medio de correo electrónico, las autoridades estadounidenses lograron las capturas de los dos implicados.

8.1.8 Sony play station 77 millones de usuarios

La empresa sony descubrió que estaban ejecutando unos accesos autorizados en el cual estaban extrayendo algunos datos de los usuarios como: el nombre, dirección de residencia, correo electrónico datos de tarjetas de créditos entre otros. La empresa aún no sabe cómo el atacante hizo para acceder de forma no autorizada a las bases de datos de play station. Dícese que los responsables de este ataque es el grupo activista anonymous.

8.1.9 Veteranos de EEUU 76 millones de usuarios

La organización envió un disco duro a un servicio técnico, en donde extrajeron 76 millones de fichas personales de veteranos de guerra estadounidenses, incluyendo datos sobre la seguridad social de los veteranos.

8.1.10 target 70 millones de usuarios

Los hackers se infiltraron en las redes informáticas de target y robaron millones de números de tarjetas de crédito y débito. En la serie de infiltraciones se robaron más de 70 millones de datos, entre ellos números de tarjetas de crédito. Target declaro que las infiltraciones fueron realizadas en época navideña.

8.1.11 Evernote 50 millones de usuario

El ataque tuvo comienzos el 28 de febrero del 2013, cuando el equipo de evernote detecto una actividad sospechosa y maliciosa, de acuerdo a la acción, los hackers lograron el acceso a nombres, cuentas de correo y claves de acceso de los usuarios. Aunque las claves se encontraban encriptados.

8.1.12 Pánico en corea del sur

Un empleado de una empresa de corea, se robaba la información personal de la clientela de las empresas emisoras de tarjetas de crédito cuando trabaja para ellos como consultor, luego de recolectar dicha información, vendía la información a empresas de marketing telefónico.

8.1.13 Tabla ilustrativa de víctimas

En la Tabla 2, se ha realizado en base al número de víctimas, que está citado en el punto anterior de los ataques más relevantes a nivel histórico.

Tabla 2, Numero de victimas

Nombre del ataque	**Victimas**
Gran hack eeuu	160.000.000
Adobe	152.000.000
Ebay	145.000.000
Heartland	130.000.000
Tjx	45.700.000
Aol	92.000.000
Sony play Station	77.000.000
Veteranos eeuu	76.000.000
Target	70.000.000
Evernote	50.000.000
Panico corea del sur	20.000.000
Total, de victimas	1.017.700.000

Fuente: el autor

8.2. HISTÓRICO DE ATAQUES EN COLOMBIA

Es importante conocer históricamente los ataques locales más sobresalientes, con el fin de demostrar que los ataques orientados a redes no tienen limitación regional. Como suelen pasar en EEUU también puede suceder en Colombia.

8.2.1 Ataque a la Registraduría Civil de Colombia

‘Oroboruo’, el Hacker de los más de 3.000 ataques a dominios del gobierno

A sus 27 años, ‘Oroboruo’, nombre en el mundo cibernético de la persona que atacó la página web de la Registraduría previo a las votaciones del plebiscito, vulneró en 3.196 oportunidades a 1.374 dominios, muchos de ellos del gobierno, a los que les inyectaba códigos maliciosos, realizando cambios en las bases de datos declarando las personas como fallecidas.

La guarida desde donde ‘Oroboruo’ realizaba sus ataques cibernéticos era su casa, en el barrio Buenas Aires, en Medellín, donde llegaron las autoridades de la Policía para capturarlo.[16]

8.2.2 700 millones fueron trasferidos desde una sucursal de Bogotá

Funcionaria de entidad bancaria conecto memoria usb con software malicioso logrando la vulnerabilidad del sistema de seguridad (virus) y de esta forma transferir dinero a cuentas donde sus “socios” retiraban el dinero, donde se identificaron 22 personas pertenecientes a la red de cibercriminales. La policía realizo un seguimiento por seis meses,[17]

8.2.3 Vulneración de sistema de información y falsificación

Favorecimiento a un condenado, por medio de la corrupción y del sistema manejaban beneficios, Se trata de José Henry Torres Mariño, juez 12 de Ejecución de Penas de Bogotá, y Justo Reinaldo Arias Humaña, ingeniero de sistemas, quienes habrían favorecido a un narcotraficante[18]

8.2.4 Ataques constantes hacia la Registraduría el día de elecciones

El día de elecciones, varios medios de comunicación reportaban fallos constantes en el portal de la Registraduría nacional, impidiendo así el acceso a la información, no solo para los ciudadanos sino para todos los medios que deseaban informar a la población, explican los expertos que los fallos se debieron a un ataque informático, por esto contrataron una empresa llamada “Adalid” para investigar el caso y llegaron

[16] A la cárcel el hacker señalado de infiltrar la página de la registraduria(online)Blu radio, Bogotá, 05 de octubre del 2016; Citado (31/09/2018) Disponible en: https://www.bluradio.com/nacion/la-carcel-el-hacker-senalado-de-infiltrar-la-pagina-de-la-registraduria-118605

[17] Autoridades rastrearon durante seis meses a asaltantes virtuales(online),El tiempo, Bogota, 26 de octubre del 2017, Citado (31/09/2018) Disponible en: http://www.eltiempo.com/bogota/rastreo-de-seis-meses-a-asaltantes-virtuales-de-una-sucursal-bancaria-en-bogota-145250

[18] Vulneración de sistema de información; https://www.rcnradio.com/judicial/ordenan-detencion-domiciliaria-juez-capturado-por-presunta-corrupcion

a la conclusión que se trataba de un ataque de denegación de servicios (DoS) y afirman que “casos como estos normalmente no son obra de un hacker, sino son obra de una empresa de delincuentes que está tratando de tumbar un servicio como el de la Registraduría o como el de la información”.[19]

8.2.5 Ataques de phising en Colombia

En el año 2017 se presentó en Colombia un caso de Phishing, este se vio reflejado a los usuarios de la entidad bancaria Bancolombia, la investigación arrojo, que el engaño comenzó con un correo electrónico de la cuenta informacion@bancolombia.com.co los cuales eran enviados los usuarios de este banco, allí se le indicaba a estos que por motivos de seguridad los servicios contratados por este habían sido suspendidos temporalmente y que para volver a hacer uso de estos canales virtuales debían hacer clic en un enlace adjunto al cuerpo del correo. Una vez el cliente ingresaba a la página fraudulenta, se le solicitaba que ingresara los datos correspondientes al usuario, contraseña y preguntas de seguridad con el fin de obtener en una base de datos toda la información necesaria a la hora de realizar una transferencia de dinero. Para darles sensación de seguridad a los usuarios, los delincuentes diseñaron el teclado virtual que usa realmente el banco y hacían que para ingresar la contraseña solo se pudiera por medio de este teclado virtual. Así, el cliente no sospechaba que estaba entregándoles información valiosa a personas sin escrúpulos.

8.2.6 hacker señalado de cometer hurto por más de $1.400 millones

Persona con alias “El Ministro” es señalado de cometer hurto por medios informáticos, con prontuario desde el 2010. Cae ‘El Ministro’, hacker señalado de cometer hurto por más de $1.400 millones.[20]

8.2.7 Millonario fraude al BBVA

En este caso, un ex empleado de la entidad bbva, logra realizar un gran desfalco, manipulando el software encargado del control de los cajeros electrónicos del

---

[19] Se han registrado cuatro ataques para tumbar la página de la registraduria(online),El espectador, Bogota,08 de marzo del 2018, Citado(31/09/2018) Disponible en: https://www.elespectador.com/economia/se-han-registrado-cuatro-intentos-para-tumbar-la-pagina-de-la-registraduria-mindefensa-articulo-743295

[20] Cae ‘el ministro’, hacker señalado de cometer Hurto por más de 1400 millones(online)El heraldo,Barranquilla,15 de mayo del 2017, Citado (31/09/2018) Disponible en: https://www.elheraldo.co/cesar/cae-el-ministro-hacker-senalado-de-cometer-hurto-por-mas-de-1400-millones-361761

BBVA, permitiendo y eliminando todo tipo de registro relacionados con las altas transacciones el cual se realizaban simultáneamente en diferentes partes del país.

El atacante tenía acceso al software de administración en el cual tenía potestad de controlar el sistema a su antojo.[21]

8.2.8 Wanna cry en Colombia

37 casos reportados a la Dijín; por el ataque del virus Wannacry, ataque que ha secuestrado la información de más de 200.000 sistemas en empresas, entidades gubernamentales, hospitales, bancos y universidades de 120 países, donde piden un rescate de maso menos US$300 para recuperarla. Según el coronel Fredy Bautista, el programa maligno, principalmente, llegó de forma masiva a Colombia a través de un correo sospechoso que tenía como asunto “Transferencia banca en línea” y como remitente tenía una entidad financiera mexicana.[22]

8.3. PÉRDIDAS ECONÓMICAS GENERADAS POR ATAQUES A LAS EMPRESAS

En la tabla 3, se recopila una serie de ataques en donde mostramos las pérdidas económicas generadas por alguno de estos. En donde especificamos; la empresa que fue víctima; país de la empresa, tipo de ataque el cual sufrió, pérdida económica y su respectiva fuente.

[21]El Millonario Fraude al bbva(online)El espectador, Bogota,29 de octubre del 2014,Citado (31/09/2018) Disponible en: https://www.elespectador.com/noticias/judicial/el-millonario-fraude-al-bbva-articulo-524960

[22]Así llego Wannacry a Colombia(online) El espectador, Bogotá, 17 de mayo del 2017, Citado(31/09/2018) Disponible en: https://www.elespectador.com/noticias/judicial/asi-llego-wannacry-colombia-articulo-694262

Tabla 3, Pérdidas económicas

Empresa Afectada	Tipo de Ataque	País	Perdida en Dinero	Fuente
Equifax	User Exploit	Usa	300 millones USD	https://blog.cheapism.com/major-data-breaches-17580/#image=3
U.S. Office of Personnel Management	Server Exploit	Usa	1 billón USD	https://blog.cheapism.com/major-data-breaches-17580/#image=4
Ashley Madison	Server Exploit	Usa	11.2 millones USD	https://blog.cheapism.com/major-data-breaches-17580/#image=5
Anthem	Server Exploit	Usa	115 millones USD	https://blog.cheapism.com/major-data-breaches-17580/#image=6
Sony	Server Exploit	Usa	1 billón USD	https://blog.cheapism.com/major-data-breaches-17580/#image=7
Home depot	Phishing	Usa	179 millones USD	https://blog.cheapism.com/major-data-breaches-17580/#image=9
Yahoo	Server Exploit	Europa	350 millones USD	https://blog.cheapism.com/major-data-breaches-17580/#image=10

Continuación Tabla 3				
Empresa Afectada	**Tipo de Ataque**	**País**	**Perdida en Dinero**	**Fuente**
Global (NotPetya)	Ransomware	Global	300 millones USD	https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#7040ef184f9a
Bancos chilenos	Phishing	Chile	10 millones USD	https://www.eleconomista.com.mx/sectorfinanciero/En-ataque-a-banco-chileno-hackers-robaron-10-millones-de-dolares-20180610-0047.html
Bancos mexicanos	Phishing	Mexico	300 millones de pesos MXP	https://www.forbes.com.mx/hackers-roban-de-300-a-400-mdp-con-ataque-a-sistema-de-bancos/
Global (Wanna Cry)	Ransomware	Global	4 Billones USD	https://www.lbmcinformationsecurity.com/blog/4-of-the-most-expensive-cyber-attacks-of-2017-and-how-they-could-have-been-prevented
Washington State University	Server Exploit	Usa	630.000 USD	https://www.lbmcinformationsecurity.com/blog/4-of-the-most-expensive-cyber-attacks-of-
Heartland Payment Systems	Server Exploit	Usa	140 millones USD	https://www.firmex.com/thedealroom/the-10-most-expensive-data-breaches-in-corporate-history/
TJ Maxx	Phishing	Usa	162 millones USD	https://www.firmex.com/thedealroom/the-10-most-expensive-data-breaches-in-corporate-history/

Continuación Tabla 3				
Empresa Afectada	**Tipo de Ataque**	**País**	**Perdida en Dinero**	**Fuente**
Target	Phishing	Usa	162 millones USD	https://www.firmex.com/thedealroom/the-10-most-expensive-data-breaches-in-corporate-history/
Hannaford Bros	Malware	Usa	252 millones US	https://www.firmex.com/thedealroom/the-10-most-expensive-data-breaches-in-corporate-history/
Veterans Administration Epsilon	SQL INJECTION Server Exploit	Usa Usa	500 millones USD 4 billones USD	https://www.firmex.com/thedealroom/the-10-most-expensive-data-breaches-in-corporate-history/ https://www.firmex.com/thedealroom/the-10-most-expensive-data-breaches-in-corporate-history/
Linked in	Server Exploit	Usa	4 millones USD	https://www.securityweek.com/linkedin-breach-cost-1m-says-2-3-million-security-upgrades-coming
Dyn Dns	DDOS	Usa	Cientos de billones USD	https://www.quora.com/How-much-monetary-damage-was-done-during-the-Oct-21-2016-DDOS-of-DynDNS
Leoni and Bangladesh Bank	Business Email Compromise (BEC)	Bangladesh	81 millones USD	https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/a-rundown-of-the-biggest-cybersecurity-incidents-of-2016#LeoniAndBangladeshBank

Continuación Tabla 3				
Empresa Afectada	**Tipo de Ataque**	**País**	**Perdida en Dinero**	**Fuente**
Swift	Business Email Compromise (BEC)	Ecuador	12 millones USD	https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/ecuadorean-bank-loses-12m-via-swift
Adult Friend Finder	Server Exploit	Usa	239 millones USD	https://blog.primefactors.com/famous-data-breaches-what-they-cost
My space	Server Exploit	Usa	209 millones USD	https://blog.primefactors.com/famous-data-breaches-what-they-cost
Linked in	Server Exploit	Usa	96 millones USD	https://blog.primefactors.com/famous-data-breaches-what-they-cost
Target stores	Phishing	Usa	64 millones USD	https://blog.primefactors.com/famous-data-breaches-what-they-cost
SFI Logistic Company	Phising	Pakistán	36271 Euros	https://elpais.com/politica/2018/06/18/actualidad/1529343443_062238.html?rel=mas
Linksys, microtik	Malware	Global	Sin calcular	https://www.abc.es/tecnologia/abci-temor-mundial-nuevo-ciberataque-detectarse-mas-500000-routers-infectados-malware-201805242129_video.html

Continuación Tabla 3				
Empresa Afectada	**Tipo de Ataque**	**País**	**Perdida en Dinero**	**Fuente**
Apple	Backdoor	Usa	Sin perdidas	https://www.abc.es/tecnologia/redes/abci-joven-16-anos-logro-hackear-servidores-internos-apple-201808171517_noticia.html

Fuente: El autor.

8.4. CANTIDAD DE INFORMACIÓN AFECTADA POR EL CIBER ATAQUE

A comparación de la Tabla 3, pérdidas económicas, en la Tabla 4, vamos a mencionar la cantidad de información afectada por medio de algunos ciber ataques.

Tabla 4, cantidad de información afectada

Empresa Afectada	**Tipo de Ataque**	**País**	**Perdida en #Datos**	**Fuente**
Facebook	Server Exploit	Usa	50 millones	https://www.portafolio.co/internacional/hackean-50-millones-de-cuentas-de-facebook-521728
Huazhu Hotels Group	Server Exploit	China	130 millones	https://technode.com/2018/08/28/huazhu-hotels-data-leak/
Brazilian Crypto Arbitrage Platform	Phishing	Brasil	264.000	https://www.cryptoglobe.com/latest/2018/08/hacked-brazilian-atlas-user-data-leaked-funds-reportedly-not-stolen/

Continuación Tabla 4				
Empresa Afectada	**Tipo de Ataque**	**País**	**Perdida en #Datos**	**Fuente**
Apcce	Server Exploit	India	60.000	https://www.databreaches.net/aadhaar-details-of-over-60k-students-on-apcce-website/
Babysitting-booking app	Public Database LINK MONGO DB	Mexico	2.4 Millones	https://nakedsecurity.sophos.com/2018/08/23/babysitting-app-suffers-temporary-data-breach-of-93000-users/
Tmobile	Server Exploit	Usa	2.3 Millones	https://www.tmonews.com/2018/08/t-mobile-data-breach-august-20/
Melbourne	Error Humano	Usa	300	https://www.theguardian.com/australia-news/2018/aug/22/melbourne-student-health-records-posted-online-in-appalling-privacy-breach
Superdrug	Server Exploit	Usa	20.000	
Ryde Hospital	Error Humano	Usa	1	https://www.9news.com.au/2018/08/21/14/58/ryde-hospital-patient-records-privacy-breach-investigation

Continuación Tabla 4				
Empresa Afectada	**Tipo de Ataque**	**País**	**Perdida en #Datos**	**Fuente**
Legacy Health	Email SCAM	Usa	38.000	https://www.oregonlive.com/business/index.ssf/2018/08/legacy_health_email_breach_mig.html
Augusta university	Server Intrusion	Usa	417.000	https://www.ajc.com/news/state--regional/university-breach-risks-health-personal-information-417-000/nPuUSV8qqvQXTQjY0ML8wN/
Adams County	Manipulate computer system	Usa	250.000	https://www.databreaches.net/wi-adams-county-clerk-suspected-in-connection-with-data-breach/
Gomo app	Server Exploit	Mundial	50 Millones	https://www.databreaches.net/50553664-gomo-app-users-information-exposed-researcher/
Butlins	Phishing	Usa	34.000	https://www.itgovernance.co.uk/blog/butlins-hacked-34000-customers-affected/

Continuación Tabla 4				
Empresa Afectada	**Tipo de Ataque**	**País**	**Perdida en #Datos**	**Fuente**
MedSpring	Phishing	Usa	13.000	https://www.databreaches.net/tx-medspring-urgent-care-notifies-13000-patients-after-phishing-attack/
Comcast	Server Exploit	Usa	25 Millones	https://boingboing.net/2018/08/09/most-hated-cable-operator.html
Telemedicine	Server Exploit	Mexico	2 millones	https://www.databreaches.net/telemedicine-company-exposed-data-of-more-than-2-millions-patients-in-mexico/
US Military	Server Exploit	Usa	850.000	https://www.databreaches.net/forum-post-claims-breach-of-850k-users-information-leak-from-recruitmilitary-com/

Fuente: el autor

9.ANALISIS SOBRE LOS SISTEMAS DE MONITOREO DE REDES

En el siguiente capítulo se conocerá algunas pautas las cuales los administradores de infraestructuras tecnológicas deben de conocer y así tomar una decisión sabia sobre la implementación de estos sistemas, resaltando sus respectivas ventajas y sus características como tal, además se mostrará los módulos más sobresalientes que puede tener un sistema de monitoreo de red, en este caso mostraremos el software prtg.

9.1 VENTAJAS DE UN SISTEMA DE MONITOREO EN LA EMPRESA

- La optimización del rendimiento de los dispositivos
- Reducción de errores en el transporte de datos
- Ahorro de tiempo, a la hora de encontrar una falla.
- Reducción de costos
- Máximo aprovechamiento a nivel de hardware.
- Control total de todos los dispositivos de la red.
- Facilita la toma de decisiones a la hora de la adquisición de nuevos equipos.
- Recolecta y centraliza toda la información sobre los dispositivos que hacen parte de la infraestructura.
- Registro de incidencias y sus respectivas soluciones que permite agilizar el proceso de resolución de problemas.
- Prevención de incidentes
- Temprana detección de problemas
- Mejora la atención a los clientes
- Acceso en tiempo real al estado de los sistemas informáticos.
- Detección del origen de los incidentes.
- Chequeo de los activos informáticos más críticos
- Mejoría en la eficiencia en los mantenimientos de los sistemas.
- Inventario de los activos informáticos de la empresa.
- Diseño de mapas de la infraestructura
- Planificación del crecimiento de la infraestructura.
- Configuración de alarmas y eventos.
- Fácil adaptación a la interfaz gráfica.
- Facilita la interpretación de los datos estadísticos que se reflejan de acuerdo al funcionamiento y consumo de red de la determinada infraestructura tecnológica.

- Hace menos vulnerable la empresa en sufrir ataques relacionados con los servicios de red.

9.2 ASPECTOS A TENER EN CUENTA EN LA IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO.

Es obvio que, a la hora de realizar cualquier tipo de implementación de nuevas tecnologías en las empresas, se deben de tener en cuenta unas pautas para su respectiva implementación. Se debe tener presente muchos aspectos como, por ejemplo, el estado actual de la infraestructura, de acuerdo a este aspecto se desglosan unas preguntas importantísimas como los son:

- ¿Mi red tiene la capacidad de soportar un sistema de monitoreo?,
- ¿Qué nivel de compatibilidad tiene mi red con los sistemas de monitoreo?

A continuación, se mencionan los aspectos más importantes a la hora de implementar el sistema de monitoreo:

- Capacidad de generar Syslogs, es importante tener une herramienta donde se pueda realizar trazabilidad de todos los movimientos ejecutados por la administración de la red o personas ajenas a esta.
- Tener una banda ancha amplia, que cubra con todas las necesidades de los activos informáticos de las empresas.
- La manera en que el sistema de monitoreo reporte las diferentes alertas.
- Validar que el sistema de monitoreo pueda integrarse con servidores externos de la red local.
- El sistema de monitoreo debe de tener la capacidad de incluir en el inventario general todo lo relacionado con hardware y software de la empresa.
- Integraciones con diferentes motores de bases de datos.
- Cobertura en el mayor número de protocolos posibles.
- Interfaz amigable para los usuarios del sistema de monitoreo.
- Medios de presentación de los datos en el panel.
- La capacidad para integrarse con máquinas virtuales.
- Brindar accesos desde sistemas externos.
- Escalado de incidentes con el proveedor del sistema de monitoreo.
- La capacidad de detectar automáticamente los dispositivos.
- Nivel de seguridad.
- Capacidad de ser compatible con varios dispositivos.
- Geolocalización.

9.3 DEMOSTRACIÓN DE UN SISTEMA DE MONITOREO.

A continuación, se dará a conocer algunas de las funciones más relevantes que tiene un sistema de monitoreo de redes, con el objetivo que un administrador de red pueda tener una idea del funcionamiento como tal del mencionado software.

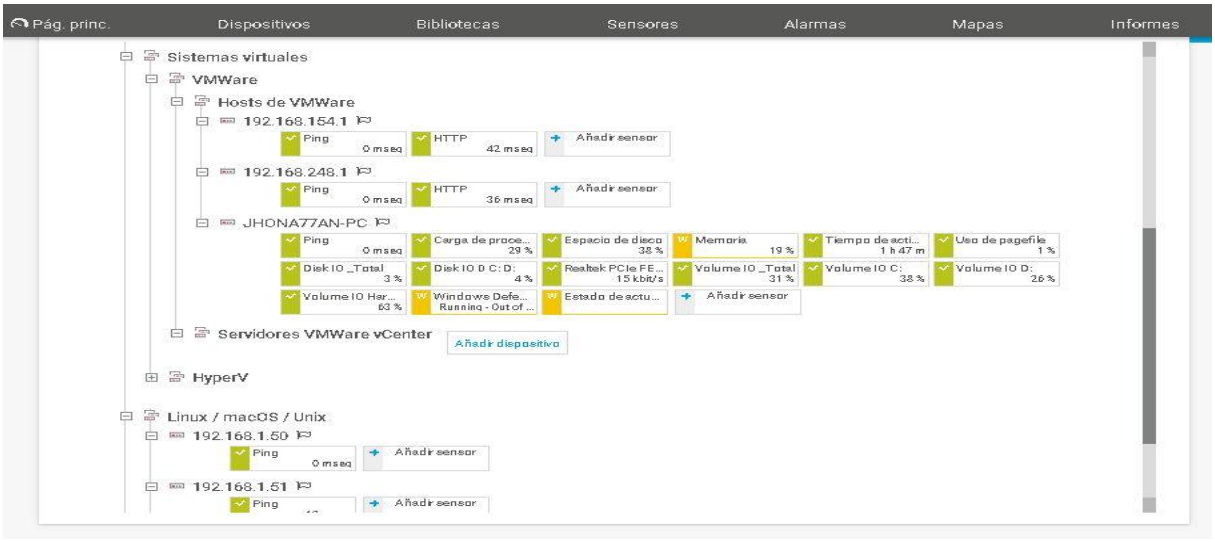
En la ilustración 14, observamos que, en el inicio del software del sistema de monitoreo, nos trae el porcentaje de los sensores y las alarmas generadas en lo corrido de su ejecución. El sistema estará constantemente enviando alertas, sea en ventanas emergentes o al correo electrónico del administrador de la red, previamente configurado en el sistema.

Ilustración 14. Menú principal

Fuente el autor.

En la ilustración 15, se observa que el sistema nos lista todo tipo de dispositivos que se encuentran dentro de la infraestructura tecnológica, en donde tenemos la posibilidad de identificar su dirección ip, tipo de máquina, protocolos en ejecución, sistema operativo, antivirus instalado, espacio en disco de los diferentes dispositivos, consumo de ancho de banda, consumo de memoria ram entre otras utilidades.

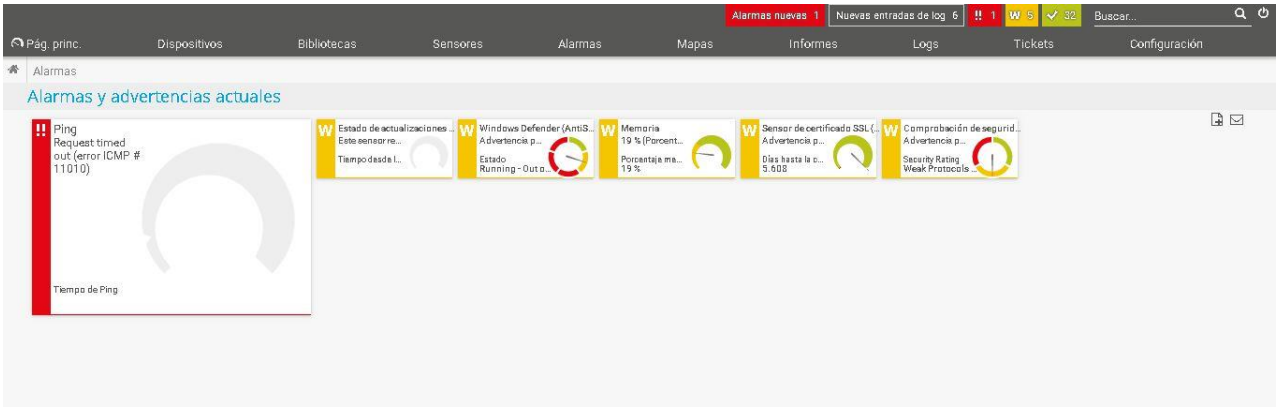
Ilustración 15. Monitoreo Dispositivos



Fuente el autor.

En la ilustración 16, se puede observar que es una alarma generada, en donde el sistema permite darle seguimiento a fondo, identificando que es una alarma de un ping perdido. Las que están marcadas de amarillas son advertencias en diferentes aspectos de la infraestructura como tal a nivel de hardware y software.

Ilustración 16. Alarmas



Fuente el autor.

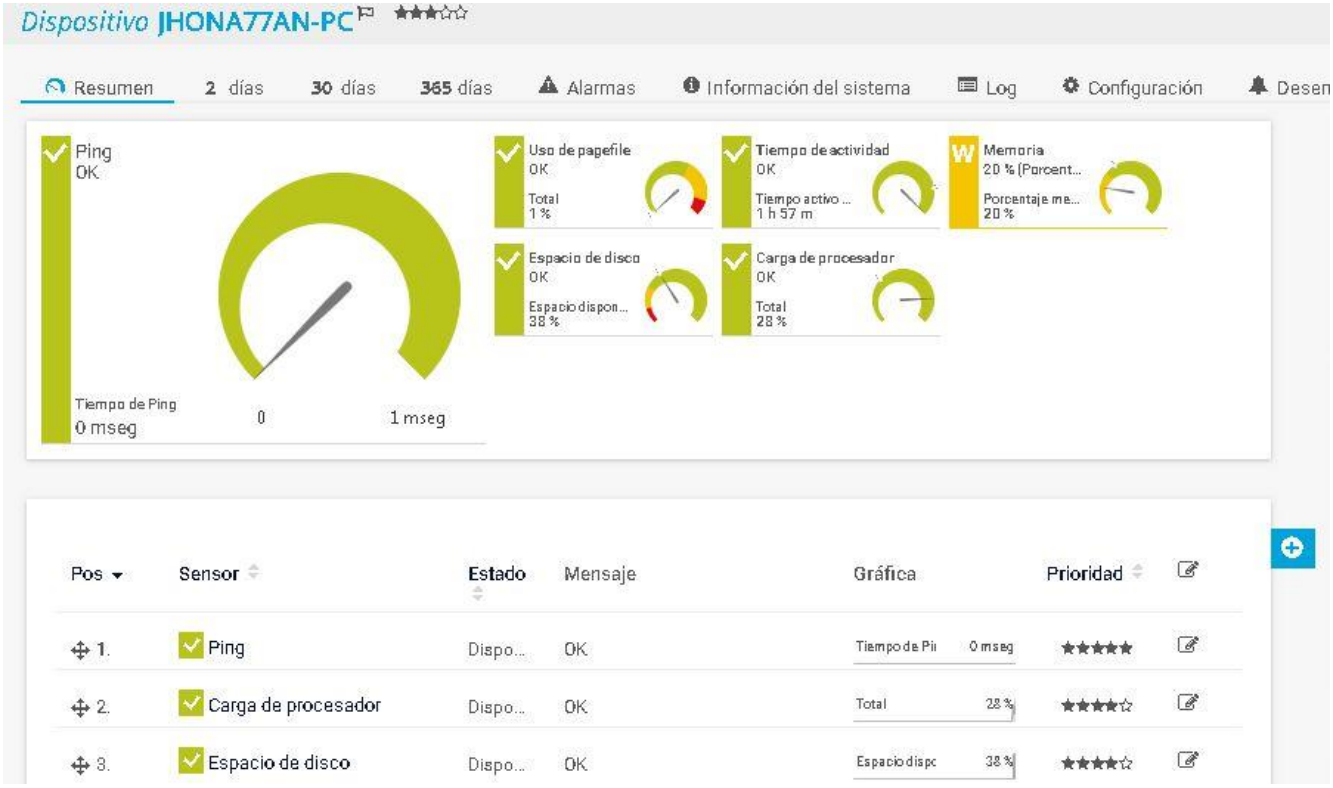
La ilustración 17 nos muestra el medidor en tiempo real del consumo de ancho de banda que tiene la infraestructura, donde se puede evidenciar los picos más altos y los picos más bajos de la red, las horas y el tipo de sensor medido.

Ilustración 17. Medidor ancho de banda

Fuente el autor.

La ilustración 18, hace referencia a la función de monitoreo de un dispositivo en específico, en donde nos muestra toda la información referente al estado de hardware y algunos componentes de software como lo son: disco duro, memoria ram y comportamiento de las tarjetas de red.

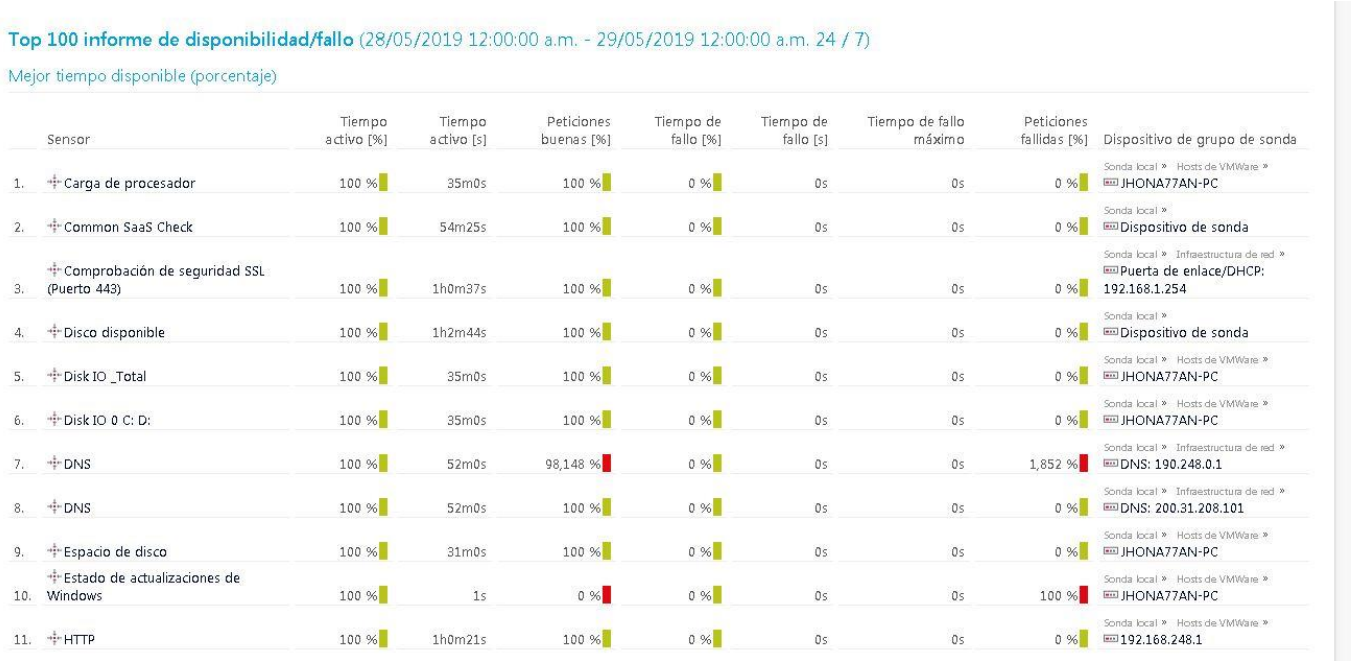
Ilustración 18. Monitoreo general equipo



Fuente el autor.

En la ilustración 19, se muestra uno de los informes que puede generar el sistema de monitoreo de red, Dejando en claro que el sistema puede generar informes de acuerdo a las necesidades o pautas que el administrador de red desee, en este caso estamos generando un reporte de disponibilidad y fallo de la red.

Ilustración 19. Informes



Top 100 informe de disponibilidad/fallo (28/05/2019 12:00:00 a.m. - 29/05/2019 12:00:00 a.m. 24 / 7)

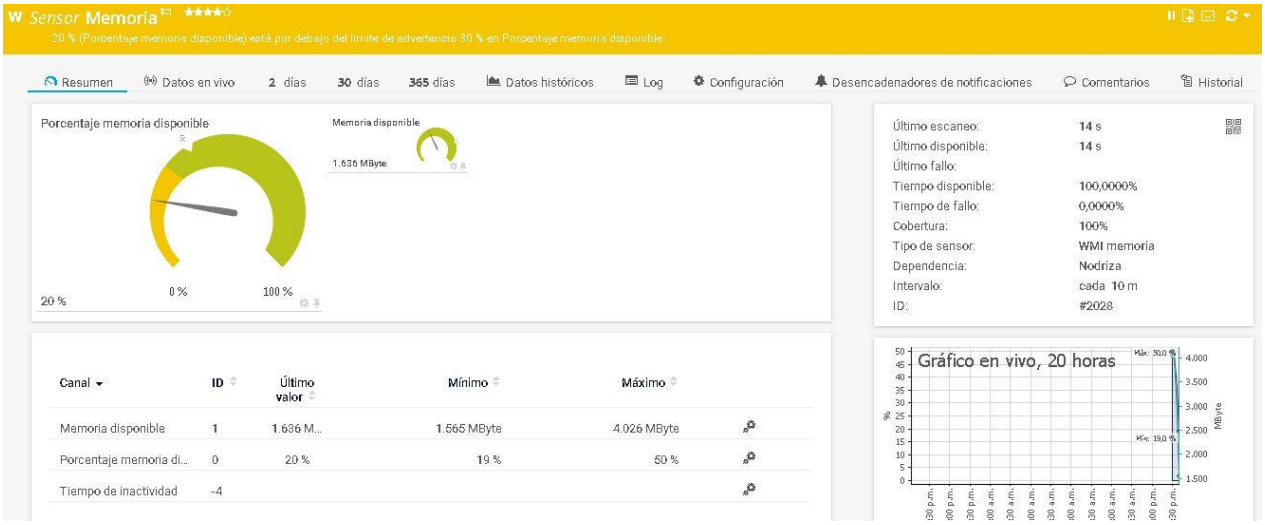
Mejor tiempo disponible (porcentaje)

	Sensor	Tiempo activo [%]	Tiempo activo [s]	Peticiones buenas [%]	Tiempo de fallo [%]	Tiempo de fallo [s]	Tiempo de fallo máximo	Peticiones fallidas [%]	Dispositivo de grupo de sonda
1.	Carga de procesador	100 %	35m0s	100 %	0 %	0s	0s	0 %	Sonda local » Hosts de VMWare » JHONA77AN-PC
2.	Common SaaS Check	100 %	54m25s	100 %	0 %	0s	0s	0 %	Sonda local » Dispositivo de sonda
3.	Comprobación de seguridad SSL (Puerto 443)	100 %	1h0m37s	100 %	0 %	0s	0s	0 %	Sonda local » Infraestructura de red » Puerta de enlace/DHCP: 192.168.1.254
4.	Disco disponible	100 %	1h2m44s	100 %	0 %	0s	0s	0 %	Sonda local » Dispositivo de sonda
5.	Disk IO _Total	100 %	35m0s	100 %	0 %	0s	0s	0 %	Sonda local » Hosts de VMWare » JHONA77AN-PC
6.	Disk IO 0 C: D:	100 %	35m0s	100 %	0 %	0s	0s	0 %	Sonda local » Hosts de VMWare » JHONA77AN-PC
7.	DNS	100 %	52m0s	98,148 %	0 %	0s	0s	1,852 %	Sonda local » Infraestructura de red » DNS: 190.248.0.1
8.	DNS	100 %	52m0s	100 %	0 %	0s	0s	0 %	Sonda local » Infraestructura de red » DNS: 200.31.208.101
9.	Espacio de disco	100 %	31m0s	100 %	0 %	0s	0s	0 %	Sonda local » Hosts de VMWare » JHONA77AN-PC
10.	Estado de actualizaciones de Windows	100 %	1s	0 %	0 %	0s	0s	100 %	Sonda local » Hosts de VMWare » JHONA77AN-PC
11.	HTTP	100 %	1h0m21s	100 %	0 %	0s	0s	0 %	Sonda local » Hosts de VMWare » 192.168.248.1

Fuente el autor.

Lo interesante de los monitores de red, es que también hacen énfasis en el consumo de memoria de los diferentes dispositivos, en la ilustración 20, se puede observar un sensor previamente configurado para poder ver los múltiples comportamientos los cuales pueda tener dicha memoria. Mide el consumo en porcentaje de la memoria y muestra gráficamente el funcionamiento en un intervalo de tiempo.

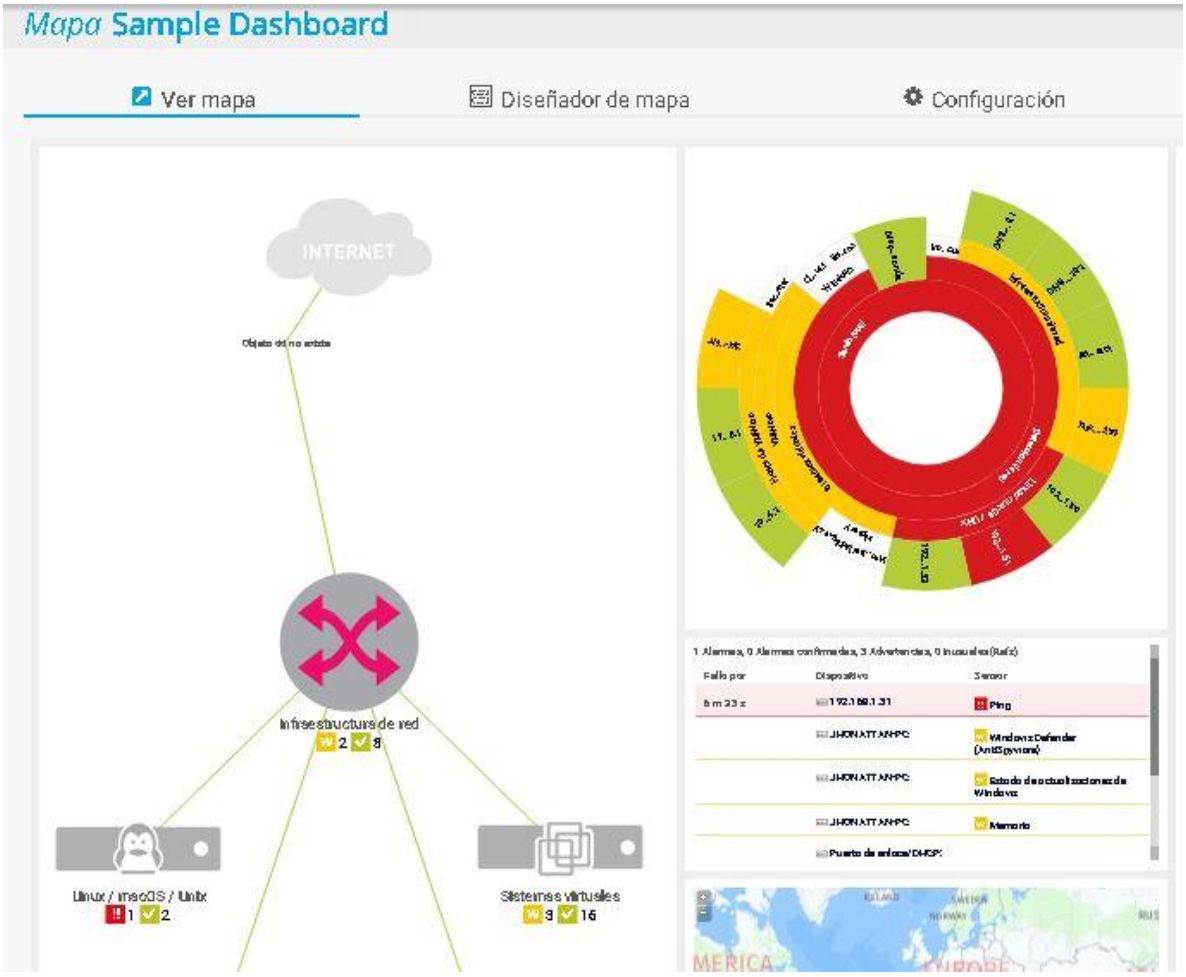
Ilustración 20. Sensores memoria



Fuente el autor.

Lo que no debe de faltar en un sistema de monitoreo de red, es el respectivo mapa lógico y físico, en la ilustración 21, se puede ver la variedad de mapas que puede implementar en dicho sistema, es de conocimiento general que en un mapa grafico podemos realizar de inmediato las ubicaciones de los diferentes activos informáticos de la infraestructura, en caso de una emergencia llegar de manera inmediata a dicho dispositivo.

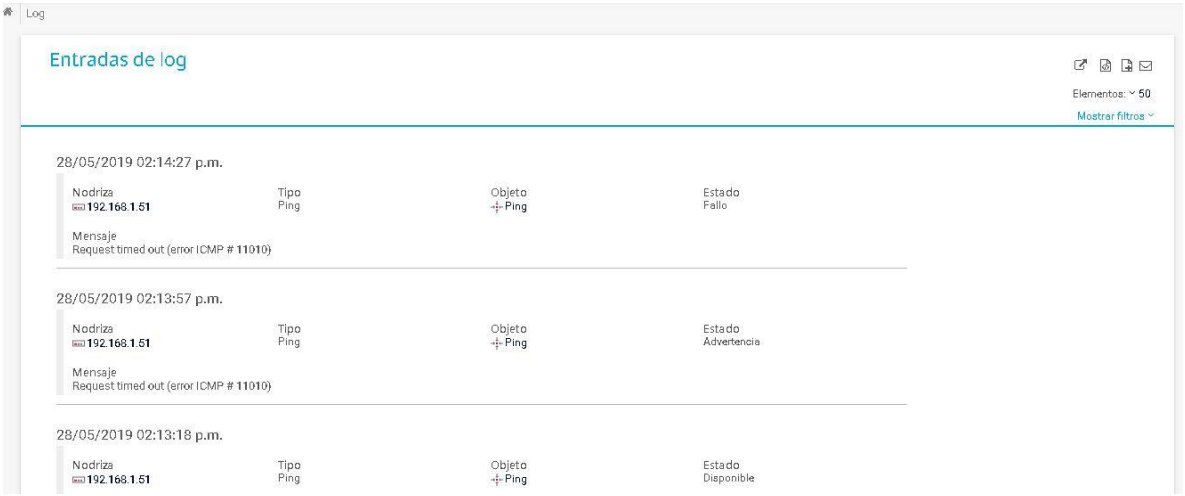
Ilustración 21. Mapas de red



Fuente el autor.

En la ilustración 22, se puede observar el módulo de los logs, uno de los módulos más importante en un sistema de monitoreo, es de mucha importancia para los administradores de red realizar seguimiento a todos los sucesos capturados por el sistema de monitoreo, con el fin de esclarecer cualquier eventualidad en la infraestructura tecnológica.

Ilustración 22. Servidor logs



Fuente el autor.

10. CONCLUSIONES

En la actualidad, estamos viviendo en un mundo en donde existen grandes empresas, las cuales están compuestas por miles de computadores conectados entre sí, una gran cantidad de información moviéndose por la red, y el acceso a determinadas aplicaciones que son utilizadas por la empresa para su propio desarrollo. Conectándose con infinidades de empresas o personas para el compartimiento de información. Es inconcebible que la seguridad no sea tenida en cuenta posteriormente, solo es tenida en cuenta cuando en alguna ocasión las empresas son víctimas de un ataque informático y es ahí donde la empresa se da cuenta de lo importante que es la seguridad informática en las redes y comunicaciones.

Ahora bien, de acuerdo a la información recolectada sobre el termino de gestión de red, se concluye que estamos logrando Transmitir a las personas encargadas de administrar una infraestructura de red de una determinada empresa, tenga el conocimiento base para el manejo y el entendimiento de los sistemas de monitoreo de redes. Ya teniendo el termino de gestión de red como base, pasamos a dar a conocer los sistemas de monitoreo de red existentes en el mercado, tanto licenciados y gpl. Concluyo que combinando el termino de gestión de red con la información de los diferentes sistemas de monitoreo de red, estamos facilitando el entendimiento del tema a la hora de una implementación de un sistema de monitoreo en la empresa por parte del personal encargado de la infraestructura.

Luego de conocer los tipos de software de monitoreo existentes en el mercado, se muestra los tipos de ataques informáticos orientados a las redes, definiéndolos y mostrando por medio de un laboratorio en un ambiente controlado el funcionamiento de los ataques más comunes que sufren las empresas. donde concluyo que las personas deben de conocer la mayoría de ataques orientados a la red y sus consecuencias, logrando que las personas tomen la conciencia de lo importante que es la implementación de un sistema de monitoreo de red, ya que por medio de este sistema se puede prevenir diversos ataques e inclusive la mitigación de estos.

A medida que vamos aprendiendo sobre la seguridad informática, se realiza una recopilación periodística acerca de los ataques más sobresalientes en grandes empresas. Empresas que se vieron afectadas en su prestación del servicio. Cabe notar que la recopilación abarca tanto lo regional como lo internacional. Es de suma importancia que las personas puedan notar el alcance geográfico que tienen estos ciber ataques, concluyendo que es bueno que las personas vean que los ataques orientados a la red no tienen límites geográficos; ni tampoco se limita por el hecho de que el país sea potencia mundial o no. Recordemos que el servicio de internet fue diseñado para intercomunicar “cortar distancias”. En donde esto facilita que personas inescrupulosas puedan tener acceso a informaciones vitales sin la necesidad de salir de su casa o por decirlo asi, de su país. Sin importar las afectaciones a empresas que se sostienen prestando servicios por medio de la red.

Lo positivo de los objetivos de la monografía, es que nos muestra los puntos más vitales que se deben tener en cuenta para tomar una decisión sabia acerca de la implementación de un sistema de monitoreo en sus respectivas empresas, capacitando al lector desde la base (gestión de red), pretendiendo que la persona al interactuar con un sistema de monitoreo, conozca el funcionamiento del sistema desde la raíz. Ya conociendo la base del funcionamiento del sistema de monitoreo, se adiciona la definición de algunos ataques orientados a la red y mostrando por medio de laboratorio los efectos de los ataques más relevantes. Por último, se realiza una recolección periodística de los ataques más sobresalientes en la historia. Con el fin de que las personas encargadas de administrar las infraestructuras tecnológicas conozcan la importancia que tienen los sistemas de monitoreo de redes en las empresas.

De acuerdo a los cuatro capítulos tratados en la monografía concluyo que los sistemas de monitoreo de redes son importantes al interior de la empresa, las empresas deben de mentalizarse que la implementación de estos sistemas es de alta importancia, recordemos que está en riesgo la seguridad de la información y la prestación del servicio de la mayoría de empresas que se encarga de prestar servicios a la comunidad. Las empresas no pueden estar a la expectativa de que les pueda pasar algún ataque informático y generar numerosas pérdidas, al contrario, debe de estar prevenido y a un paso más adelante de los ciberdelincuentes. Creería que la mejor inversión en tecnología es la seguridad informática, es claro que son inversiones altas, pero creo que sería más caro reponerse de un ataque informático.

11. RECOMENDACIONES

Teniendo en cuenta toda la temática presentada en la monografía, Hay ciertas pautas que debe de tener en cuenta el administrador de una red a la hora de dar manejo a la infraestructura tecnológica.

El administrador debe de identificar las vulnerabilidades más comunes que tenga la empresa, sin tanto rodeo todos los profesionales de la seguridad informática sabemos que el usuario final es una vulnerabilidad la cual puede ser tomada como una bomba de tiempo. Por esta razón lo primero que debe de hacer el administrador es capacitar al usuario final sobre la seguridad informática, sobre el manejo correcto de los recursos de red y el manejo del pc como tal. Dar a conocer los peligros a los cuales está expuesto y las consecuencias que puede crear el mal manejo de los recursos brindados por la infraestructura. Dar a conocer los tipos de ataques existentes (ataques orientados a la red, previamente mencionadas en el capitulo1).

Luego de centrarse en el usuario final, ahora entra en juego la evaluación del estado actual de la infraestructura tecnológica, validando que la infraestructura posea por obligación un SGSI (sistema de gestión de seguridad informática). luego validar el equipamiento entre hardware y software que posea la empresa para el taponamiento de brechas de la seguridad de la infraestructura.

Es de suma importancia que la empresa posea un sistema de monitoreo de redes de datos al interior de la empresas, ya que es una herramienta muy completa, la cual mantiene la red en constante monitoreo y estudio del comportamiento del tráfico como tal, logrando descubrir de acuerdo al comportamiento de la red posibles ataques informáticos orientados a la red como lo pueden ser virus, gusanos o ataques de denegación del servicio, lo cual puede ocasionar perdidas de información o la negación del servicio si se trata de empresas que ofrecen servicios a la comunidad como tal.

En la monografía se dan a conocer unos puntos clave para que el administrador de una infraestructura conozca la base por la cual funciona un sistema de monitoreo

refiriéndonos al termino de gestión de red, se dan a conocer algunos ataques informáticos orientados a las redes, Además se mencionan algunos monitores de red existentes en el mercado tanto libres y licenciados, con el fin de mostrar la variedad existente y que se acomode a la necesidad y el tamaño de determinada empresa. Es bueno que los administradores conozcan un poco de historia sobre los diferentes ataques informáticos más relevantes a nivel empresarial, por eso se dedica un capítulo de la monografía a la recopilación de datos estadísticos sobre los ataques informáticos y una gran variedad de noticias sobre ataques informáticos tomados de referencias periodísticas.

Mi recomendación a nivel en general es que los administradores conozcan el término de gestión de red para poder entender el funcionamiento de los diferentes monitores de redes ofrecidos por el mercado, ahora bien, conocer las múltiples opciones que ofrece el mercado con estos monitores y de lo que realmente estos ofrecen como funcionalidad. Y así realizar la implementación de un sistema de monitoreo de redes a gusto de sus necesidades y tamaño de la infraestructura.

Es bueno que el administrador sepa un poco de historia y de cifras que han dejado los ataques informáticos orientados a la red, lo cual puede utilizar como argumento a la hora de implementar un sistema de monitoreo de redes en su respectiva empresa, sabiendo que la adquisición de un sistema de monitoreo debe de ser aprobado por un gerente o por un comité ejecutivo. La mejor manera de convencer estas personas claves es señalándoles la necesidad para el buen desarrollo de la empresa, mostrando las posibles pérdidas tanto informáticas como económicas que esta puede tener por el hecho de no poseer un sistema de monitoreo de redes.

BIBLIOGRAFIA

A diario se registran 542.465 ataques informáticos en Colombia (online) El tiempo, Bogotá, 27 de septiembre 2017 Citado (20/09/2018) Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

Adobe sufre ciberataque y roban datos de 2.9 millones de clientes (online) RTVE, España, 04 de octubre del 2013, Citado (31/09/2018) Disponible en: http://www.rtve.es/noticias/20131004/adobe-sufre-ciberataque-roban-datos-29-millones-clientes/757880.shtml

Así llego Wannacry a Colombia (online) El espectador, Bogotá, 17 de mayo del 2017, Citado (31/09/2018) Disponible en: https://www.elespectador.com/noticias/judicial/asi-llego-wannacry-colombia-articulo-694262

Ataque de denegación de servicios (online) Cuba: Autor desconocido, ecured, Foro. (s.f.), Fecha desconocida – (citado 9 de julio, 2018), Disponible en internet: https://www.ecured.cu/Ataque_de_denegaci%C3%B3n_de_servicio

Ataques informáticos (online) México: Cyberseguridad. Net, Mayo 2015-(citado 9 de julio, 2018), Disponible en internet: https://cyberseguridad.net/index.php/ataques-informaticos

Autoridades rastrearon durante seis meses a asaltantes virtuales (online),El tiempo, Bogotá, 26 de octubre del 2017, Citado (31/09/2018) Disponible en: http://www.eltiempo.com/bogota/rastreo-de-seis-meses-a-asaltantes-virtuales-de-una-sucursal-bancaria-en-bogota-145250

Berná Galiano, J. A., Pérez Polo, M., & Crespo Martínez, L. M. (2002). Redes de computadores para ingenieros en informática. [Alicante]: Digitalia. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=318062&lang=es&site=ehost-live

Cae ‘el ministro’, hacker señalado de cometer Hurto por más de 1400 millones (online) El heraldo, Barranquilla, 15 de mayo del 2017, Citado (31/09/2018) Disponible en: https://www.elheraldo.co/cesar/cae-el-ministro-hacker-senalado-de-cometer-hurto-por-mas-de-1400-millones-361761

Comprehensive Security Mechanism for Defending Cyber Attacks based upon Spoofing and Poisoning. Pandey, A. a., & Saini, J. s. (2016). Comprehensive Security Mechanism for Defending Cyber Attacks based upon Spoofing and Poisoning. BVICAM's International Journal of Information Technology, 8(2), 1011-1016.Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=122681957&lang=es&site=ehost-live

Desarrollo de las amenazas informáticas en el tercer trimestre del 2017 (online) Rusia: Román UNUCHEK, Karpesky, Noviembre 2017 – (citado 9 de julio, 2018) Disponible en internet: https://securelist.lat/it-threat-evolution-q3-2017-statistics/85714/

EBay obliga a cambiar las contraseñas a sus usuarios a cambiar sus contraseñas (online) diario la Nación, Argentina, 21 de mayo del 2014, citado (31/09/2018) Disponible en: https://www.lanacion.com.ar/1693243-un-ataque-informatico-a-ebay-obliga-a-los-usuaris-a-cambiar-su-contrasena

EEUU, desarticula una banda que hackeo 160 millones de tarjeta de crédito (online) Cnn, Usa, 25 de julio del 2013 Citado(31/09/2018) Disponible en: http://cnnespanol.cnn.com/2013/07/25/ee-uu-desarticula-una-banda-que-hackeo-160-millones-de-tarjeta-de-credito/

El Millonario Fraude al bbva (online) El espectador, Bogotá, 29 de octubre del 2014,Citado (31/09/2018) Disponible en: https://www.elespectador.com/noticias/judicial/el-millonario-fraude-al-bbva-articulo-524960

El Tiempo, T. (22 de Septiembre de 2015). El Tiempo. Recuperado el Diciembre de 2017, de http://www.eltiempo.com/archivo/documento/CMS-16383752

El tiempo. (27 de 09 de 2017). Periódico El Tiempo. Obtenido de Periódico El Tiempo: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

Gestión de redes (online) Cuba: ecured, Foro. (s.f.). ciberseguridad.net, Abril 2013 – (citado 9 de julio, 2018), Disponible en internet: https://www.ecured.cu/Gesti%C3%B3n_de_Redes

Guette, G. g. (2009). Automating trusted key rollover in DNSSEC. Journal Of Computer Security, 17(6), 839-854.Recuperado de http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=45435093&lang=es&site=ehost-live

Internet security threat report 2018 (online) EE.UU.: Sin autor, Symantec, Abril 2017 – (citado 9 de julio 2018).Disponible en internet: https://resource.elq.symantec.com/LP=3980?cid=70138000001BjppAAC&mc=202671&ot=wp&tt=sw&inid=symc_threat-report_regular_to_leadgen_form_LP-3980_ISTR22-report-main

Ip Spoofing Rengarajan, A., Sugumar, R., & Jayakumar, C. (2016). Secure Verification Technique for Defending IP Spoofing Attacks. International Arab Journal of Information Technology (IAJIT), 13(2), 302-309. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=114270555&lang=es&site=ehost-live

Kakarountas, A. k., Michail, H. h., Milidonis, A. m., Goutis, C. g., & Theodoridis, G. t. (2006). High-Speed FPGA Implementation of Secure Hash Algorithm for IPsec and VPN Applications. Journal of Supercomputing, 37(2), 179-195. Recuperado de http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=aci&AN=21436644&lang=es&site=ehost-live

La piña Wifi (online) México: Autor desconocido, Dragonjar, Fecha desconocida – (citado 9 de julio, 2018) Disponible en internet: https://www.dragonjar.org/la-pina-wifi-o-wifi-pineapple-mark-iv-en-espanol.xhtml

Los ataques DDos en el tercer trimestre de 2017 (online). Rusia: Alexander KHALIMONENKO, Karpesky, Noviembre 2017 – (citado 9 de julio, 2018). Disponible en internet: https://securelist.lat/ddos-attacks-in-q3-2017/85669/

Los Ataques DDos en el tercer trimestre de 2017 (online), Karpesky, Rusia, 6 de noviembre del 2017 citado (26/09/2018) Disponible en: https://securelist.lat/ddos-attacks-in-q3-2017/85669/

Los 5 mejores software de monitoreo (online) España: Valeria MAGONI, Enero 2018-(citado 9 de julio, 2018), Disponible en internet: https://es.tanaza.com/los-5-mejores-software-de-monitoreo-de-red-en-el-2017/

Los 9 tipos de ramsoware habituales (online) España: Autor desconocido, Diagonal informática, Fecha desconocida – (Citado 9 de julio 2018) Disponible en internet: http://docente.ucol.mx/al950441/public_html/osi1hec_B.htm

Que es el sniffing (online) (sin lugar), (autor desconocido) Noviembre 2002 – (citado 9 de julio, 2018) Disponible en internet: http://www.internetmania.net/int0/int93.htm

Que es la gestión de red (online) Cuba, Citado (31/09/2018) Disponible en: https://www.ecured.cu/Gesti%C3%B3n_de_Redes

Que es SQL injection (online) Open webinars, Sevilla, 12 de octubre del 2017, Citado (31/09/2018) Disponible en: https://openwebinars.net/blog/que-es-sql-injection/

Que es un ataque man in the middle (online), Rusia: Serge MALENKOVICH, Karpesky, Abril 2013 – (citado 9 de julio, 2018) Disponible en internet: http://repository.unilibre.edu.co/handle/10901/8811

Que es un ataque man in the middle (online), Lugar desconocido: Gabriela González, Hipertextual, Junio 2014 – (citado 9 de julio, 2018) Disponible en internet: http://www.delitosinformaticos.com/especial/seguridad/pgp.shtml

Que es un sniffer (online). México: Mundo cisco, agosto 2009 – (citado 9 de julio, 2018).Disponible en internet: http://www.mundocisco.com/2009/08/que-es-un-sniffer.html

Se han registrado cuatro ataques para tumbar la página de la registraduria (online), El espectador, Bogotá, 08 de marzo del 2018, Citado(31/09/2018) Disponible en: https://www.elespectador.com/economia/se-han-registrado-cuatro-intentos-para-tumbar-la-pagina-de-la-registraduria-mindefensa-articulo-743295

Study of Vulnerabilities of ARP Spoofing and its detection using SNORT. Bijral, R. K., Gupta, A., & Sharma, L. S. (2017). Study of Vulnerabilities of ARP Spoofing and its detection using SNORT. International Journal of Advanced Research in Computer Science, 8(5), 2074-2077. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=124636718&lang=es&site=ehost-live

Tipos de ataques informáticos y como protegerse (online), Noé REYES, Technodyan, Mayo 2014 – (Citado 9 de julio, 2018), Disponible en internet: https://www.technodyan.com/tipos-de-ataques-informaticos-i-malware/

Tipos de ataque y cómo prevenirlos (online) Colombia: Jonatán URREGO, Colombiadigital, Mayo 2013 – (citado 9 de julio, 2018). Disponible en internet: https://colombiadigital.net/actualidad/articulos-informativos/item/4801-tipos-de-ataque-y-como-prevenirlos.html

Top 16 best network monitoring tools (online). España: Sin autor, PandoraFms, Enero 2017 – (citado 9 de julio, 2018) Disponible en internet: https://blog.pandorafms.org/network-monitoring-tools/

Un Cracker de 28 año, acusado de robar datos de 130 millones de tarjetas de crédito (online), El mundo, EE.UU., 17 de agosto del 2009, Citado (31/09/2018) Disponible en: http://www.elmundo.es/elmundo/2009/08/17/navegante/1250535175.html

Vulneración de sistema de información; https://www.rcnradio.com/judicial/ordenan-detencion-domiciliaria-juez-capturado-por-presunta-corrupcion

Windows Microsoft network Architecture and the osi model (online). EE.UU.: Colaboradores, Microsoft, Abril 2017- (citado 9 de julio, 2018) Disponible en internet: https://support.microsoft.com/es-co/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained

ANEXOS

Anexo A Formato RAE

Fecha de Realización: 18/10/2019
Título: ESTUDIO SOBRE LA IMPORTANCIA DE LOS SISTEMAS DE MONITOREO DE REDES DE DATOS EN LAS EMPRESAS
Autor: SUESCUN PINEDA, Jonhatan Alexander
Palabras Claves: Ataques informáticos Infraestructura Redes de datos Sistemas de monitoreo Software licenciado Software libre Activos informáticos Datos Perdidas Usuarios Servidores Gestión de redes Intrusiones Fraude Empresa Informacion
Descripción: La monografía trata de mostrar la importancia que tiene los sistemas de monitoreo dentro de las empresas, para mostrar esta importancia se han elaborado 4 etapas con las cuales se busca crear conciencia basado en la recolección de información que se encuentra depositados en las etapas mencionadas. Empezando por el concepto de gestión de redes, tema el cual se debe de tener conocimiento para comprender el funcionamiento de dichos sistemas de monitoreo, Luego de tener este conocimiento como base, se da a conocer los diferentes softwares de monitoreo existentes en el mercado. Seguido, se consulta sobre los ataques existentes orientado a las redes de datos. Con el fin de que las personas conozcan el funcionamiento de cada ataque. Ahora, para poner en realidad dichos ataques se realiza una consulta periodística de los ataques más destacados a nivel empresarial enfatizando la ubicación geográfica(Colombia) y abarcando a nivel mundial.

Luego de comprender toda la información mencionada anteriormente, se finaliza con la demostración y descripción de un monitor de red.

Fuentes:

Para la realización de la monografía, se apoyó con 40 citas bibliográficas, las cuales son referencias electrónicas. A continuación, se listará las mencionadas citas:

A diario se registran 542.465 ataques informáticos en Colombia (online) El tiempo, Bogotá, 27 de septiembre 2017 Citado (20/09/2018) Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

Adobe sufre ciberataque y roban datos de 2.9 millones de clientes (online) RTVE, España, 04 de octubre del 2013, Citado (31/09/2018) Disponible en: http://www.rtve.es/noticias/20131004/adobe-sufre-ciberataque-roban-datos-29-millones-clientes/757880.shtml

Así llego Wannacry a Colombia (online) El espectador, Bogotá, 17 de mayo del 2017, Citado (31/09/2018) Disponible en: https://www.elespectador.com/noticias/judicial/asi-llego-wannacry-colombia-articulo-694262

Ataque de denegación de servicios (online) Cuba: Autor desconocido, ecured, Foro. (s.f.), Fecha desconocida – (citado 9 de julio, 2018), Disponible en internet: https://www.ecured.cu/Ataque_de_denegaci%C3%B3n_de_servicio

Ataques informáticos (online) México: Cyberseguridad. Net, Mayo 2015-(citado 9 de julio, 2018), Disponible en internet: https://cyberseguridad.net/index.php/ataques-informaticos

Autoridades rastrearon durante seis meses a asaltantes virtuales (online),El tiempo, Bogotá, 26 de octubre del 2017, Citado (31/09/2018) Disponible en: http://www.eltiempo.com/bogota/rastreo-de-seis-meses-a-asaltantes-virtuales-de-una-sucursal-bancaria-en-bogota-145250

Berná Galiano, J. A., Pérez Polo, M., & Crespo Martínez, L. M. (2002). Redes de computadores para ingenieros en informática. [Alicante]: Digitalia. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=318062&lang=es&site=ehost-live

Cae ‘el ministro’, hacker señalado de cometer Hurto por más de 1400 millones (online) El heraldo, Barranquilla, 15 de mayo del 2017, Citado (31/09/2018)

Disponible en: https://www.elheraldo.co/cesar/cae-el-ministro-hacker-senalado-de-cometer-hurto-por-mas-de-1400-millones-361761

Comprehensive Security Mechanism for Defending Cyber Attacks based upon Spoofing and Poisoning. Pandey, A. a., & Saini, J. s. (2016). Comprehensive Security Mechanism for Defending Cyber Attacks based upon Spoofing and Poisoning. BVICAM's International Journal of Information Technology, 8(2), 1011-1016.Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=122681957&lang=es&site=ehost-live

Desarrollo de las amenazas informáticas en el tercer trimestre del 2017 (online) Rusia: Román UNUCHEK, Karpesky, Noviembre 2017 – (citado 9 de julio, 2018) Disponible en internet: https://securelist.lat/it-threat-evolution-q3-2017-statistics/85714/

EBay obliga a cambiar las contraseñas a sus usuarios a cambiar sus contraseñas (online) diario la Nación, Argentina, 21 de mayo del 2014, citado (31/09/2018) Disponible en: https://www.lanacion.com.ar/1693243-un-ataque-informatico-a-ebay-obliga-a-los-usuaris-a-cambiar-su-contrasena

EEUU, desarticula una banda que hackeo 160 millones de tarjeta de crédito (online) Cnn, Usa, 25 de julio del 2013 Citado(31/09/2018) Disponible en: http://cnnespanol.cnn.com/2013/07/25/ee-uu-desarticula-una-banda-que-hackeo-160-millones-de-tarjeta-de-credito/

El Millonario Fraude al bbva (online) El espectador, Bogotá, 29 de octubre del 2014,Citado (31/09/2018) Disponible en: https://www.elespectador.com/noticias/judicial/el-millonario-fraude-al-bbva-articulo-524960

El Tiempo, T. (22 de Septiembre de 2015). El Tiempo. Recuperado el Diciembre de 2017, de http://www.eltiempo.com/archivo/documento/CMS-16383752

El tiempo. (27 de 09 de 2017). Periódico El Tiempo. Obtenido de Periódico El Tiempo: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

Gestión de redes (online) Cuba: ecured, Foro. (s.f.). ciberseguridad.net, Abril 2013 – (citado 9 de julio, 2018), Disponible en internet: https://www.ecured.cu/Gesti%C3%B3n_de_Redes

Guette, G. g. (2009). Automating trusted key rollover in DNSSEC. Journal Of Computer Security, 17(6), 839-854.Recuperado de

http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=45435093&lang=es&site=ehost-live

Internet security threat report 2018 (online) EE.UU.: Sin autor, Symantec, Abril 2017 – (citado 9 de julio 2018).Disponible en internet: https://resource.elq.symantec.com/LP=3980?cid=70138000001BjppAAC&mc=202671&ot=wp&tt=sw&inid=symc_threat-report_regular_to_leadgen_form_LP-3980_ISTR22-report-main

Ip Spoofing Rengarajan, A., Sugumar, R., & Jayakumar, C. (2016). Secure Verification Technique for Defending IP Spoofing Attacks. International Arab Journal of Information Technology (IAJIT), 13(2), 302-309. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=114270555&lang=es&site=ehost-live

Kakarountas, A. k., Michail, H. h., Milidonis, A. m., Goutis, C. g., & Theodoridis, G. t. (2006). High-Speed FPGA Implementation of Secure Hash Algorithm for IPsec and VPN Applications. Journal of Supercomputing, 37(2), 179-195. Recuperado de http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=aci&AN=21436644&lang=es&site=ehost-live

La piña Wifi (online) México: Autor desconocido, Dragonjar, Fecha desconocida – (citado 9 de julio, 2018) Disponible en internet: https://www.dragonjar.org/la-pina-wifi-o-wifi-pineapple-mark-iv-en-espanol.xhtml

Los ataques DDos en el tercer trimestre de 2017 (online). Rusia: Alexander KHALIMONENKO, Karpesky, Noviembre 2017 – (citado 9 de julio, 2018). Disponible en internet: https://securelist.lat/ddos-attacks-in-q3-2017/85669/

Los Ataques DDos en el tercer trimestre de 2017 (online), Karpesky, Rusia, 6 de noviembre del 2017 citado (26/09/2018) Disponible en: https://securelist.lat/ddos-attacks-in-q3-2017/85669/

Los 5 mejores software de monitoreo (online) España: Valeria MAGONI, Enero 2018-(citado 9 de julio, 2018), Disponible en internet: https://es.tanaza.com/los-5-mejores-software-de-monitoreo-de-red-en-el-2017/

Los 9 tipos de ramsoware habituales (online) España: Autor desconocido, Diagonal informática, Fecha desconocida – (Citado 9 de julio 2018) Disponible en internet: http://docente.ucol.mx/al950441/public_html/osi1hec_B.htm

Que es el sniffing (online) (sin lugar), (autor desconocido) Noviembre 2002 – (citado 9 de julio, 2018) Disponible en internet: http://www.internetmania.net/int0/int93.htm

Que es la gestión de red (online) Cuba, Citado (31/09/2018) Disponible en: https://www.ecured.cu/Gesti%C3%B3n_de_Redes

Que es SQL injection (online) Open webinars, Sevilla, 12 de octubre del 2017, Citado (31/09/2018) Disponible en: https://openwebinars.net/blog/que-es-sql-injection/

Que es un ataque man in the middle (online), Rusia: Serge MALENKOVICH, Karpesky, Abril 2013 – (citado 9 de julio, 2018) Disponible en internet: http://repository.unilibre.edu.co/handle/10901/8811

Que es un ataque man in the middle (online), Lugar desconocido: Gabriela González, Hipertextual, Junio 2014 – (citado 9 de julio, 2018) Disponible en internet: http://www.delitosinformaticos.com/especial/seguridad/pgp.shtml

Que es un sniffer (online). México: Mundo cisco, agosto 2009 – (citado 9 de julio, 2018).Disponible en internet: http://www.mundocisco.com/2009/08/que-es-un-sniffer.html

Se han registrado cuatro ataques para tumbar la página de la registraduria (online), El espectador, Bogotá, 08 de marzo del 2018, Citado(31/09/2018) Disponible en: https://www.elespectador.com/economia/se-han-registrado-cuatro-intentos-para-tumbar-la-pagina-de-la-registraduria-mindefensa-articulo-743295

Study of Vulnerabilities of ARP Spoofing and its detection using SNORT. Bijral, R. K., Gupta, A., & Sharma, L. S. (2017). Study of Vulnerabilities of ARP Spoofing and its detection using SNORT. International Journal of Advanced Research in Computer Science, 8(5), 2074-2077. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=124636718&lang=es&site=ehost-live

Tipos de ataques informáticos y como protegerse (online), Noé REYES, Technodyan, Mayo 2014 – (Citado 9 de julio, 2018), Disponible en internet: https://www.technodyan.com/tipos-de-ataques-informaticos-i-malware/

Tipos de ataque y cómo prevenirlos (online) Colombia: Jonatán URREGO, Colombiadigital, Mayo 2013 – (citado 9 de julio, 2018). Disponible en internet:

https://colombiadigital.net/actualidad/articulos-informativos/item/4801-tipos-de-ataque-y-como-prevenirlos.html

Top 16 best network monitoring tools (online). España: Sin autor, PandoraFms, Enero 2017 – (citado 9 de julio, 2018) Disponible en internet: https://blog.pandorafms.org/network-monitoring-tools/

Un Cracker de 28 año, acusado de robar datos de 130 millones de tarjetas de crédito (online), El mundo, EE.UU., 17 de agosto del 2009, Citado (31/09/2018) Disponible en: http://www.elmundo.es/elmundo/2009/08/17/navegante/1250535175.html

Vulneración de sistema de información; https://www.rcnradio.com/judicial/ordenan-detencion-domiciliaria-juez-capturado-por-presunta-corrupcion

Windows Microsoft network Architecture and the osi model (online). EE.UU.: Colaboradores, Microsoft, Abril 2017- (citado 9 de julio, 2018) Disponible en internet: https://support.microsoft.com/es-co/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained

Contenido del documento:

- Conclusiones

Metodología:

De acuerdo a que el escrito es una monografía, por lo general no tiene una metodología especifica. En este caso se elaboró una metodología la cual está compuesta por 4 etapas que están netamente relacionadas y basadas en los objetivos específicos de la monografía, con base a estas 4 etapas damos la respuesta a la pregunta formulada en el planteamiento del problema.

Conceptos nuevos:

- Gestión de redes
- Tipos de troyanos
- Perdidas económicas en las empresas
- Numero de información perdida en las empresas
- Monitores de red existentes en el mercado
- Características de un monitor de red
- Ataques más comunes a nivel empresarial

- **Conclusiones:**
- Aprendiendo la gestión de redes como base, da la capacidad de conocer el funcionamiento de un sistema de monitoreo de red.
- Se conocen varias alternativas de software de monitoreo de red, de acuerdo a la Necesidad y capacidad de cada empresa o tipo de infraestructura
- Se identifican los tipos de ataques existentes enfocado a las redes y sus posibles consecuencias.
- Los ataques informáticos no tienen una ubicación geográfica como tal.
- Es mejor prevenir ataques informáticos que reparar daños ocasionados por uno de ellos, incluso es más costosa la reparación.

AUTOR: JOHNATAN ALEXANDER SUESCUN PINEDA.