DEFINICIÓN DE UN SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS EN UNA RED PARA EL CONTROL DE VULNERABILIDADES USANDO SOFTWARE LIBRE

JUAN PABLO ORTEGON CRIOLLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2020

DEFINICIÓN DE UN SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS EN UNA RED PARA EL CONTROL DE VULNERABILIDADES USANDO SOFTWARE LIBRE

JUAN PABLO ORTEGON CRIOLLO

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Director:
Ing. JOEL CARROLL VARGAS MSc

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 23 de diciembre de 2020

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

GLOSARIO

ATAQUE DE DENEGACIÓN DE SERVICIO (DOS): Un tipo de ataque destinado a inutilizar el sistema o la red objetivo, a menudo monopolizando los recursos del sistema. Por ejemplo, en febrero de 2000, un hacker dirigió miles de solicitudes al sitio web de eBay. El tráfico de la red inundó la conexión a Internet disponible para que ningún usuario pueda acceder a eBay durante algunas horas. Una denegación de servicio distribuida (DDoS) involucra muchos sistemas informáticos, posiblemente cientos, todos enviando tráfico a unos pocos destinos selectos. El término "Denegación de servicio" también se usa de manera imprecisa para referirse a cualquier condición inducida hacia el exterior que hace que una computadora sea inutilizable, por lo que "deniega el servicio" a su usuario legítimo.

AUTENTICACIÓN: El proceso de identificación de una persona, generalmente basado en un nombre de usuario y contraseña. La autenticación generalmente requiere algo que una persona tiene (como una llave, una credencial o un token), algo que una persona sabe (como una contraseña, número de identificación o el apellido de soltera de la madre) o algo que una persona (representada por una foto, huella digital) o escaneo de retina, etc). Cuando la autenticación requiere dos de esas tres cosas, se considera una autenticación fuerte.

AUTORIDAD DE CERTIFICACIÓN (CA): Un tercero de confianza (TTP) que verifica la identidad de una persona o entidad, luego emite certificados digitales que acreditan que varios atributos (por ejemplo, nombre, una clave pública dada) tienen una asociación válida con esa entidad.

AUTORIZACIÓN: Para transmitir el acceso oficial o poder legal a una persona o entidad.

CIFRADO: El proceso de disfrazar los datos para ocultar su contenido. Tal como se usa en un contexto de seguridad de red, el cifrado generalmente se realiza al colocar los datos a través de cualquiera de los algoritmos matemáticos establecidos desarrollados específicamente para este propósito.

CLIENTE: Un proceso informático que solicita un servicio de otro computador y acepta las respuestas del servidor.

CONTRASEÑA: Una secuencia secreta de caracteres o una palabra que un usuario envía a un sistema para fines de autenticación, validación o verificación. Se recomienda el uso de frases de contraseña en lugar de contraseñas

CRIPTOGRAFÍA: El arte y la ciencia de codificar y decodificar mensajes utilizando algoritmos matemáticos que utilizan una clave secreta. El concepto se ha ampliado para incluir la gestión de mensajes que tienen una combinación de: privacidad (al ser ilegibles para todos, excepto para el remitente y el destinatario); integridad (no modificada mientras está en ruta), y no repudio (firmada digitalmente de tal manera que el originador no pueda reclamar plausiblemente que no la originó).

DRIVER: Un programa de software que manipula un dispositivo (como una impresora, un teclado, un mouse o un disco duro). El controlador acepta comandos genéricos de un programa y luego los traduce en comandos especializados para el dispositivo.

FIREWALL Componentes de software o hardware que restringen el acceso entre una red protegida e Internet, o entre otros conjuntos de redes, para bloquear el uso o abuso no deseado.

GATEWAY Un sistema que proporciona acceso entre dos o más redes. Las puertas de enlace se utilizan normalmente para conectar redes que son diferentes. El Firebox a menudo sirve como puerta de enlace entre Internet y su red.

GESTIÓN DE CLAVES: El proceso y el procedimiento para almacenar y distribuir con seguridad claves criptográficas precisas; El proceso general de generación y distribución de claves criptográficas a destinatarios autorizados de manera segura.

IDS (SISTEMA DE DETECCIÓN DE INTRUSIÓN): Una clase de productos de redes dedicados a detectar ataques de hackers. Los sistemas de detección de intrusos basados en la red examinan el tráfico en una red en busca de signos de acceso no autorizado o ataques en curso, mientras que los sistemas basados en host observan los procesos que se ejecutan en una máquina local para determinar la actividad que un administrador ha definido como "incorrecto".

IP (PROTOCOLO DE INTERNET): Un conjunto fundamental de especificaciones detalladas que controla cómo se formatean los paquetes de datos y cómo se mueven de una computadora en red a otra

IP SPOOFING: El acto de insertar una dirección IP de la remitente falsa (pero de apariencia ordinaria) en el campo "Desde" del encabezado de una transmisión de Internet para ocultar el origen real de la transmisión. Existen pocas razones, si las hay, legítimas para realizar la falsificación de la propiedad intelectual; La técnica suele ser un aspecto de un ataque.

LAN (RED DE ÁREA LOCAL): Una red de computadores que abarca un área relativamente pequeña, generalmente limitada a un solo edificio o grupo de edificios.

NIDS: Sistema de detección de intrusos en la red.

PANEL DE CONTROL: El conjunto de programas de Microsoft Windows utilizados para cambiar el hardware, el software y la configuración del sistema.

PAQUETE: Una unidad de información formateada de acuerdo con protocolos específicos que permiten la transmisión precisa de datos de un nodo en una red a otro. También llamado datagrama o paquete de datos, contiene dos partes: un encabezado y una carga útil. El encabezado es como un sobre; La carga útil es el contenido. En el Protocolo de Internet, cualquier mensaje de más de 1.500 bytes se fragmenta en paquetes para su transmisión.

PUERTA DE ENLACE PREDETERMINADA: Cuando las máquinas individuales en un segmento de red envían paquetes de datos, verifican el destino del paquete para determinar si el destino es local (es decir, en el mismo segmento de red) o no. Si el destino del paquete no es local, la máquina lo reenvía a un nodo en la red que sirve como entrada a todas las demás redes. Este nodo se denomina puerta de enlace predeterminada y podría ser cualquier dispositivo de enrutamiento, como un enrutador o un dispositivo de firewall.

PUERTA TRASERA: Un fallo de diseño, planificado o accidental, que permite que la fuerza aparente del diseño sea evitada fácilmente por aquellos que conocen el truco.

SOMBRERO BLANCO: Una persona que investiga fallas en las medidas de seguridad de la red para fortalecerlas y evitar que las redes de computadoras sean invadidas. Cuando un investigador descubre nuevas fallas de seguridad, las reporta al proveedor apropiado para que las arregle, en lugar de usar el conocimiento de manera ilícita.

SOMBRERO NEGRO: Una persona con intenciones maliciosas que investiga, desarrolla y usa técnicas para vencer las medidas de seguridad e invadir las redes de computadoras.

SPAM: Correo electrónico comercial no solicitado enviado a muchos destinatarios, como una versión electrónica de correo no deseado.

TELNET: Un programa de control remoto que normalmente se encuentra en sistemas Unix en redes TCP / IP. Un cliente telnet se ejecuta en su PC y lo conecta a un servidor remoto en una red. Luego puede ingresar comandos a través del programa Telnet y se ejecutarán como si los estuviera ingresando directamente en la consola del servidor. Esto le permite controlar el servidor y comunicarse con otros servidores en esa red remota.

TOKEN: También se llama un token de seguridad o un token de autenticación. Algo que una persona tiene que evidencia validez, o identidad. Por lo general, es un dispositivo de hardware que se asemeja a una calculadora de mano, ya que a menudo tiene algún tipo de pantalla y quizás un teclado para ingresar números. Los tokens alcanzan el objetivo de la "autenticación de dos factores", que se considera un estándar de seguridad sólido al validar quién es un usuario, porque el acceso a una red que usa tokens requiere dos factores: algo que la persona sabe (una contraseña) y algo que la persona tiene (el token).

TOPOLOGÍA DEL BUS: Un tipo de diseño de red utilizado por todos los sistemas Ethernet, en el que todos los dispositivos están conectados a un cable central.

WIRESHARK: Programa para detectar el tráfico en una red.

RESUMEN

Una intrusión puede denominarse una entrada no autorizada a la propiedad o área de otra persona, pero en términos de seguridad Informática y de equipos de cómputo, son las actividades que comprometen los objetivos básicos de seguridad de una red que son. Confidencialidad, integridad y privacidad.

La detección de intrusos es el proceso de monitorear los eventos que ocurren en un sistema informático o red y analizarlos para detectar posibles incidentes de amenazas y violaciones de las prácticas de seguridad informática, políticas de uso aceptable o políticas de seguridad estándar. Uno de los objetivos que se presenta es el de Proteger de ataques e intrusiones a las redes de una empresa.

El sistema de detección de intrusos (IDS) es un componente de software o hardware que automatiza el proceso de detección de intrusos, está diseñado para monitorear los eventos que ocurren en un sistema y red de equipos y responde a los eventos con signos de posibles incidentes de violaciones de las políticas de seguridad. El Sistema de Prevención de Intrusiones (IPS), por otro lado, es la tecnología de detección de actividades de intrusión o amenaza y de tomar medidas preventivas para aprovecharlas. Combina el conocimiento de IDS de forma automatizada.

La intrusión en los sistemas produce daños y pérdidas económicas que pueden ser mitigadas con una implementación técnica de (IDS), por lo tanto, es de vital importancia blindar la redes para que se eviten estos ataques mediante la definición de un sistema de detección y prevención de intrusos en una red lo que permitirá el control de la vulnerabilidad todo esto apoyado por el uso de software libre.

PALABRAS CLAVE: Redes, Software Libre, (IDS)

ABSTRACT

An intrusion can be called an unauthorized entry to the property or area of another person, but in terms of IT security and computer equipment, they are the activities that compromise the basic security objectives of a network that they are. Confidentiality, integrity and privacy.

Intrusion detection is the process of monitoring events that occur on a computer system or network and analyzing them for potential threat incidents and violations of computer security practices, acceptable use policies, or standard security policies. One of the objectives presented is to protect a company's networks from attacks and intrusions.

The intrusion detection system (IDS) is a software or hardware component that automates the intrusion detection process, is designed to monitor events that occur in a system and equipment network and responds to events with signs of possible incidents of violations of security policies. The Intrusion Prevention System (IPS), on the other hand, is the technology for detecting intrusion or threat activities and taking preventive measures to take advantage of them. It combines the knowledge of IDS in an automated way.

The intrusion in the systems produces damages and economic losses that can be mitigated with a technical implementation of (IDS), therefore, it is of vital importance to shield the networks so that these attacks are avoided by defining a detection and prevention system of intruders in a network which will allow the control of the vulnerability all this supported by the use of free software.

KEY WORDS: Networks, Free Software, (IDS)

INTRODUCCIÓN

De la misma manera en que se desarrolla y evolucionan todas las áreas de la ciencia, de igual forma se van especializando las técnicas que se desarrollan para irrumpir de manera ilegal en las redes de telecomunicaciones.

Los ataques de los intrusos son cada vez más comunes y sofisticados, durante el último año se observaron ataques que buscaban no solo la captura de información sensible sino que pretendían la eliminación de los datos y sistemas que los contenían, de igual forma han desarrollado experiencia en la evasión de los controles mediante la utilización de servicios de la nube legítimos camuflando así su intencionalidades ilegitimas, el grado de avance de los atacantes ha mostrado la adopción de cifrados, y el aprovechamiento de las brechas que van apareciendo con la expansión del internet y sus servicios, según ciso 2018.

De manera ingenua los ciudadanos les restan valor a los incidentes reportados a nivel mundial por considerarse lejanos, es necesario que se reconozca la velocidad y avance de la amenaza. Lo que permitirá que se reconozca la vulnerabilidad de las redes de cómputo con la que se interactúa cotidianamente tanto en la vida social como laboral para de esta manera desarrollar mejoras en la seguridad.

Dentro de las organizaciones la vulnerabilidad está latente debido al desconocimiento de los avances que han desarrollado los atacantes para acceder de manera ilegitima al sistema, esta amenaza constituye un problema real de las organizaciones que es necesario resolver.

Por lo anterior surge la necesidad de contar con redes seguras, puesto que una intrusión que se presente puede acarrear un sinfín de problemas desde perdidas de los activos económicos y de infraestructura tecnológica hasta perdida de información sensible y vital para el funcionamiento de las empresas, así como los riesgos de inseguridad laboral junto con las implicaciones sociales que esto acarrearía. Es a causa de esta necesidad que se motiva el desarrollo de esta monografía, con el propósito de contribuir a la seguridad de las redes con el manejo

de herramientas y equipos que hagan una red más segura y así evitar contratiempos a futuro.

La definición de un Sistema de Detección y Prevención de Intrusos en una red mediante el uso de software libre permitirá que se pueda acceder a los servicios de seguridad por parte de las pequeñas empresas garantizando el control de su vulnerabilidad y la salvaguarda de su información.

Esta monografía es de carácter cualitativo descriptivo mediante la identificación de categorías y elementos que permiten definir el sistema de detección y prevención de intrusos utilizando software libre.

El desarrollo del trabajo inicia con el establecimiento de un marco teórico del cual partir para la identificación de la variables y categorías que abrirán paso a la definición del sistema de detección y prevención de intrusos.

Debido a que el desarrollo del sistema parte de la revisión bibliográfica y se desarrolla en simulación, dejando los aspectos de aplicación para fases posteriores de este proceso de investigación.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

A partir de la globalización de la economía el uso de las tecnologías de la información y la comunicación ha ido en aumento, los avances tecnológicos en la conformación de redes de computadoras han constituido un activo importante de las empresas para el desarrollo de sus actividades económicas, los que el uso de redes y servicios de conectividad, con este auge se han incrementado también los ataques a los sistemas mencionado en el informe Cisco[1], convirtiendo la seguridad de la información en un problema de vital importancia a solucionar.

En el mundo las empresas y organizaciones dependen del uso de redes internas o intranets para el manejo de su información corporativa, la interconexión ha facilitado la comunicación y el uso eficiente de los recursos de las empresas, la utilización de las redes informáticas se constituye en una actividad sensible y prioritaria dentro de la estructuras de negocio y convirtiéndose en muchos casos en soportes fundamentales del Core de la empresa, este hecho conduce a que se tenga un interés particular en la seguridad de la información que se transmita en estas redes sea confiable, integra y con disponibilidad tal como lo menciona Rivero[2], debido a que constituyen información sensible para el desarrollo del propósito empresarial.

De acuerdo con los datos los estadísticos el 43% de las pequeñas empresas son el blanco de los ataques cibernéticos, solo el 14% de la pequeñas empresas cuentan con la capacidad para mitigar los riesgos y ataques cibernéticos y el 60% de las pequeñas empresas cierran operaciones debido a un ataque cibernético como lo

[1] CISCO INC. Informe anual de seguridad de 2014
[2] RIVERO PÉREZ, J. L. Técnicas de aprendizaje automático para la detección de intrusos en redes de computadoras. Revista Cubana de Ciencias Informáticas,8(4), 52-73. 2014

indica Smallbussines trends[3], los usuarios en general desconoce las amenazas latentes que se ciernen sobre las redes que usa en su trabajo con lo cual expone su información a riegos de fugas de datos y vulnerabilidad de la información, que constituye un activo fundamental en las labores de la empresa, en este sentido la seguridad de redes se convierte en un asunto prioritario para los procesos empresariales.

Actualmente de manera recurrente se observa como los atacantes buscan eludir efectivamente casi cualquier sistema de detección de intrusos en la red o NIDS por su abreviatura en inglés. “Los actores maliciosos continúan innovando en maneras de explotar la confianza pública con el fin de provocar consecuencias dañinas”[4] Los hackers negros pueden ocultar un ataque de dos maneras fundamentales, primero, pueden cambiar la forma en que se realiza la intrusión, mediante una división del ataque en muchos paquetes de red y en segundo lugar, pueden alterar la carga útil del ataque para que ya no coincida con la firma NIDS, a través del uso de una codificación diferente para las URL.

A diferencia de los analistas de los protocolos de seguridad, que utilizan modelos formales de amenazas para evaluar la resistencia de un protocolo contra los ataques, los analistas del (NIDS) realizan su evaluación utilizando algunos métodos y herramientas externas, que permite que se estructure un modelo de amenaza formal que describa de manera exhaustiva cual es la capacidad que tienen los atacantes para eludir el sistema de detección de intrusos, el establecimiento de la capacidad del ataque, permite que se emita una alerta para el administrador del sistema cada vez que ese tipo de intrusión intente penetrar la red

[3] SMALL BUSINESS TREND. Cyber Security Statistics: Numbers Small Businesses Need to Know 2017
[4] CISCO INC. Informe anual de seguridad de 2014

Por lo anterior, cuando se realiza un uso indebido del (NIDS) se establecen unas categorías de ataques que se define a través de una tabla de firmas maliciosas, por lo tanto, si el intruso intenta penetrar la red y esta actividad coincide con las categorías y con una de las firmas maliciosas en la tabla, se genera un hecho de alarma y protección de sistema, en tal sentido el contar con un análisis de NIDS robusto permitirá que los administradores de estas redes corporativas personalicen la bases de datos de las firmas maliciosas, estableciendo una línea de defensa para la infraestructura de redes de la organización.

1.2 FORMULACIÓN DEL PROBLEMA

Considerando lo planteado es vital preguntarse ¿Cómo evitar los ataques cibernéticos a la red de una empresa?

2 JUSTIFICACIÓN

En la actualidad la seguridad de las redes es uno de los principales problemas de seguridad, el desarrollo de malware nuevo y específico para cada red constituye un aspecto de alarma, se puede identificar que algunas de la causas de la intensificación de los ataques tienen su origen en el crecimiento del tamaño de la redes, en la mayor capacidad de procesamiento de datos, el aumento de la conexión y acceso a internet, y por último el valor de la información que se encuentra en las redes, son atractivos para los intrusos, como lo menciona Villalba[5]. Confirmando que la intrusión y los ataques a las redes se constituyen en un problema contemporáneo.

A raíz de este como lo platea Romero[6] hecho los especialistas en seguridad informática han establecido sistemas soportados en reglas que identifican los ataques, a pesar de ello este sistema se han quedado corto al momento de identificar los nuevos ataques e intrusiones, debido a que los atacantes y desarrolladores de malware programan de manera disruptiva de modo que estos nuevos incidentes no compartan las características del malware ya conocido, lo cual lo deja por fuera de las reglas establecidas por el sistema convirtiéndolo en obsoleto e incapaz de detectarlo e identificarlo, debido a que para poder detectar el ataque es necesario contar con la definición de algunas características a partir de la cuales se pueda establecer una regla que lo identifique.

Los ataques cibernéticos que sufren las redes de una empresa son ocasionados por los denominados intrusos que se pueden catalogar en dos tipos, los intrusos externos que son aquellos que sin acceso autorizado realizan ataques al sistema y

[5] VILLALBA, L. J. G., OROZCO, A. L. S., & VIDAL, J. M. Anomaly-based network intrusion detection system. IEEE Latin America Transactions, 13(3), 850-855. 2015

[6] ROMERO CASTRO, Martha Irene, et al. Introducción a La Seguridad Informática y El Análisis de Vulnerabilidades. Alcoy (Alicante). info@3ciencias.com Primera edición: octubre 2018 ISBN: 978-84-949306-1-4 DOI: http://dx.doi.org/10.17993/IngyTec.2018.46

los intrusos internos que cuentan con acceso restringido a los sistemas como lo indica Rivero[7]

La intrusión se puede definir como “cualquier acción que atente y comprometa la integridad, confidencialidad o disponibilidad de un recurso” [8], en este sentido las intrusiones realizadas tanto por un intruso externo como interno deben ser considerados ataques cibernéticos que comprometen la seguridad de la red.

Como lo plantea Dong[9] es pertinente establecer una línea de defensa que proteja a la red de los ataques, es en este punto donde la detección de intrusos cobra un papel determínate constituyéndose en una barrera adicional que identifica y repele los ataques

Con el propósito de que se evite el hecho de identificar de manera tardía los ataques, se ha formulado el sistema de detección de intrusiones en red (Network Intrusión Detection Systems o NIDS). que se fundamenta en la comparación de algún modelo construido o en el establecimiento de filtros de reconocimiento que detecte el nuevo programa maligno desde el comienzo.

La solución al problema de los ataques cibernéticos a las redes de la empresa recae en los sombreros blancos que podemos llamar también diseñadores de NIDS, donde se establece un ataque A en una instancia de la red y una secuencia de paquetes para determinar si esa instancia es vulnerable. A partir de este propósito el uso de una herramienta que sea capaz de manejar ambos problemas, debe usar el modelo de derivación de ataque para generar instancias de ataque y alimentar estas instancias en el NIDS especifico, hasta que encuentre una que no se detecta. Para ello la herramienta o software usa el modelo para verificar si la instancia dada coincide con una de las instancias generadas.

---

[7] RIVERO PÉREZ, J. L. Técnicas de aprendizaje automático para la detección de intrusos en redes de computadoras. Revista Cubana de Ciencias Informáticas,8(4), 52-73. 2014

[8] HEADY, R., G. LUGER, A. MACCABE AND M. SERVILLA The architecture of a network-level intrusion detection system. Edition ed.: Department of Computer Science, College of Engineering, University of New Mexico, 1990

[9] DONG, G., J. GAO, R. DU, L. TIAN, et al., Robustness of network of networks under targeted attack. Physical Review E, 87(5), 052804. 2013

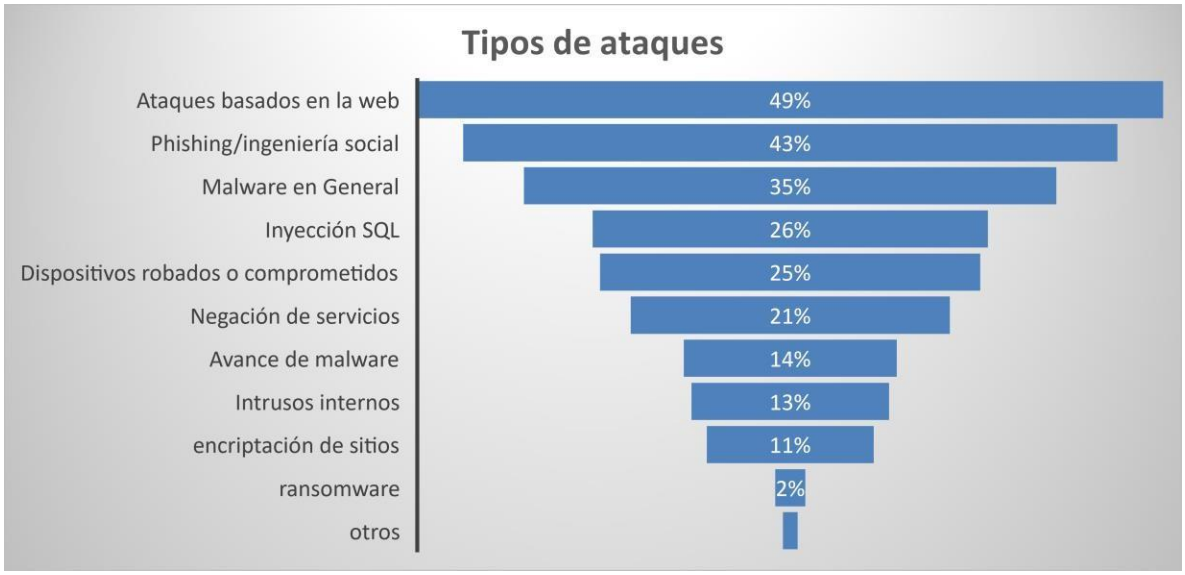
Una de las razones por las que se debe tener una prevención en las redes de una organización o empresa es la de evitar que se ocasionen daños irreparables y de impacto a esta, de igual manera nos ayuda a dimensionar el tamaño y estructura de la red favoreciendo su eficiencia, evitando que no se ralentice y sature, otra es la de saber qué elementos tiene nuestra red y de qué manera puedo asegurar que estos equipos los tengo controlados y asegurados de tal manera que nos evite incursiones e intrusiones peligrosas.

En lo social podemos establecer que el personal de la entidad este completamente seguro que no se van a presentar intrusiones ni ataques que pongan en riesgo la estabilidad laboral.

Lo cual es corroborado por las estadísticas de small business[10] que informan que como consecuencia de los incidentes las pequeñas compañías gastaron en promedio 879,582 debido a daños o robo de activos de TI, además la interrupción de las operaciones normales cuesto un promedio de US 955,429.

[10] SMALL BUSINESS TREND. Cyber Security Statistics: Numbers Small Businesses Need to Know 2017

Figura 1Tipos de Ataques



Fuente: SMALL BUSINESS TREND. Cyber Security Statistics: Numbers Small Business Need to Know 2017.

Dentro de los reportes realizados de los tipos de ataques se identifica que los ataques que ingresa vía web cupa un 49% de los casos, de allí se recoge el desarrollo de robo de identidades y la generación del programa maligno.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Definir un sistema de detección de intrusos a la red de una empresa, mediante el uso de software especializado y simulación, para evitar ataques de forma que se robustezca su seguridad, confiabilidad y eficiencia.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los tipos y formas en que los atacantes intervienen las redes.
- Establecer los puntos de control de acceso a la red.
- Determinar las herramientas para el análisis, control y regulación del tráfico de la red.

4 MARCO REFERENCIAL

4.1 MARCO TEORICO

4.1.1 **Definición de un sistema de detección y prevención de intrusos y su importancia dentro de una organización**. Para abordar un sistema de detección de intrusos se hace necesario abordar sus inicios, que parten de una necesidad de automatizar la revisión de eventos de seguridad realizada por James P. ANDERSON que abordo el concepto de Monitor de referencias en un informe que sería el precursor de los sistemas de detección de intrusos que se desarrolló para la fuerza aérea de estados unidos, en el año de 1980, el informe busca como propósito la eliminación e información relevante o redundante en el registro de sucesos[11]

Dentro de los avances que planteo Anderson estaba la clasificación entre los ataques internos y externos que apoyarían posteriormente el desarrollo de proceso de auditoria, su modelo permita recuperar el sistema de la intrusión a cuentas de usuario ilegítimos, lo cual se soportaban en un análisis de comportamiento y patrones de uso. Estableciendo las bases a sistemas posteriores de detección.[12]

Durante la década de los 80 se presentaron desarrollos en términos de modelo de detección de intrusos que permitía detecta actividades fuera de lo normal, en comportamiento, o en uso no adecuado o acorde con la naturaleza del trabajo del usuario lo cual se podía efectuar en tiempo real.[13]

---

[11] González Gómez, D. Sistema de Detección de intrusos. 2013 tomado de https://dgonzalez.net/papers/ids/ids_v1.0.pdf

[12] ANDERSON, James P. Computer SecurityThreat Monitoring and Surveillance. Fort Whashinton,PA: James P. ANDERSON Co.1980

[13] Denning Dorothy E. An intrusión Detection Model.Proceedings of the 1986 IEE Symposium on Secutity and Privacy, Oakland, CA, April 1986.

Se conto con el sistema Discovery que permitid detectar y evitar problemas en la base de datos de TRW, lo cual da un giro en el desarrollo porque este sistema trabaja sobre software[14].

Se encuentra el proyecto HAYSTACK, del centro criptológico de la fuerza aérea de los Estados Unidos, realizaba una revisión periodo de los datos, mediante dos fases de análisis[15].

Con este breve repaso de los ochenta se observa como los sistemas de detección de intrusos se basada en monitorear lo que sucede en las maquinas, pero el gusano de internet de 1988, contribuyo a que se buscaran soluciones de seguridad más optimas[16] buscando la unión de sistemas de seguridad basados en maquina y red, estableciendo el Distibuted Intrusion Detection System (DIDS)[17], que tenía como propósito brindar las herramientas que centraran el control y la publicación de los resultados desde un controlador central, este sistema podía rastrear los eventos y detectar la intrusión haciendo seguimiento del intruso y relacionar los eventos en diferentes niveles de la red.

La historia ha mostrado la importancia que tiene el desarrollo de sistema de identificación de intrusos, al que no solo se ven expuestas las grandes organizaciones sino cualquier empresa u organización que trabaja con redes y maneja información sensible[18], un hacker realiza una intrusión para sustraer, modificar, dañar o tener en su poder información que le proporcione algún tipo de

---

[14] SRI internacional. System Design Laboratory. Intrusión Detection [en línea] fecha no disponible. Disponible en internet en http://www.csl.sri.com/programs/intrusion/history.html

[15] SMAHA Steve E. An Intrusion Detection System for the Air Force. Proceedings of the Fourth Aurospace Conputer Security Aplications conference, Orlando FL, December 1998.

[16] SPAFFORD, Eugene H. The Internte Worm: Crisis and Aftermath; communications of the ACM; 32(6): 678-687, June 1989.

[17] SNAPP, S.R. et Al. DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early prototype, proceedings of the Fifteenthe National Computer Security Conference, Baltimore, MD, October 1992.

[18] SOLARTE MARTINEZ, G., Ocampo, C., & Castro Bermúdez, Y. Sistema de detección de intrusos en redes corporativas. 2017. *Scientia Et Technica*, *22*(1), 60-68. https://doi.org/10.22517/23447214.9105

ventaja, es en este punto que los sistema de detección de intrusos aparecen para controlar estos efectos negativos.

Dentro del sistema se establece una clasificación de claves por tipo de usuario y acceso a la información, pero a veces los sistemas son vulnerados por los mismos usuarios quienes prestas sus claves, permitiendo que un externo acceda a información dentro de las organizaciones y vulnerando la seguridad.

Los sistemas de detección de intrusos se utilizan en máquinas y en redes el éxito de su aplicación tiene relación con la eficiencia es decir cuál es el tiempo de respuesta de este al sistema, este tiempo permite establecer un espacio de ventaja para poder reaccionar al ataque[19]. Para ello podemos abordar la una tipología de acuerdo con sus funciones, desde el origen de los datos, del modo de detección y por el comportamiento, iniciemos con la primera tipología donde encontramos la siguiente clasificación de IDS.

4.1.1.1. Sistemas de Detección de intrusos basados en el Host. Estos sistemas se caracterizan por trabajar a través de la identificación de los ataques a través de un análisis que se realiza a las modificaciones en el sistema de archivos, en el registro de las aplicaciones y en las llamadas que se realice al sistema junto con el estado de Host. Su funcionamiento se soporta en un agente de software y aplicaciones; los análisis se pueden realizar mediante la herramienta honeypost.[20], con este sistema se puede realizar una revisión del origen de los datos, como se realizan los registros en el sistema y como se ejecuta el sistema operativo, su eficacia está ligada a la cantidad de logs que deba procesar y no realiza una analisis de comportamiento de red.

[19] SOLARTE MARTINEZ, G., Ocampo, C., & Castro Bermúdez, Y. Sistema de detección de intrusos en redes corporativas. 2017. *Scientia Et Technica*, *22*(1), 60-68. https://doi.org/10.22517/23447214.9105

[20] MAIRH, Abhishek, et al. Honeypot in network security: a survey. En *Proceedings of the 2011 international conference on communication, computing & security*. 2011. p. 600-605

4.1.1.2. Sistemas de detección de Intrusos basado en red (NIDS). Estos sistemas acceden al tráfico de red y de esta forma monitorea distintos hosts mediante un concentrador de red a un conmutador que está configurado para que de la duplicación de puertos. Los sensores se ubican en los límites de la red para que capturen el tráfico y pueda analizar cuál es el contenido, detectando el tráfico malicioso, las características de este tipo de sistema es que se maneja en lo nodos de la red, es capaz de detectar los ataques en tiempo real, lo que le permite rastrear el tiempo y la posición de acuerdo con la IP, lo cual se realizará solo en un segmento de red.

Los comportamientos que se analizan serian, el Tree-way handshake que hace referencia que el puerto que solicito el usuario y el servidor acepto la conexión en el puerto solicitado, si se considera que es el puerto habilitado o autorizado para tal fin, la transmisión de datos, la transmisión de los datos es decir que cuando se realiza el análisis de tráfico se verifica el número de bytes que se enviaron en la conexión y determinar quién inicia y finaliza la conexión.

4.1.1.3. IDS basado en firmas Este tipo de IDS busca la firma, patrones o identidad conocida de un evento especifico, lo que requiere que se cuente con una actualización periódica de las bases de datos que cuenta con las firmas e identidades del sistema, es decir que cuanto más actualizada las bases de datos más eficiente la detección[21]

4.1.1.4. IDS basado en Anomalías. Esta tipología se centra en identificar los ataques desconocido que los IDS firmas no detectan, este sistema se desarrolló mediante enfoque de aprendizaje automático que permite que se comparen los modelos de comportamiento confía con comportamientos nuevo y eso permitirá identifica que anomalías o comportamiento extraños se identifican. En este tipo de

[21] YADAV, Ajay. Network Design: Firewall, IDS/IPS. Infosec Institute, 2018, p. 5-9. Disponible en línea https://resources.infosecinstitute.com/topic/network-design-firewall-idsips/#gref

sistema los administradores tienen que realizar una revisión de las alarmas para descartar si es un falso positivo.

4.1.1.5. IDS de comportamiento Activo. los sistemas de detección de tipo activo o IPS (intrusión Prevention System)[22] combina el IDS y la respuesta cuando se detecta un ataque.

4.1.1.6. IDS de comportamiento pasivo: solo detecta la anomalía, pero no realizan ningún acción y respuesta al ataque.

4.1.1.7. La seguridad de la información como activo de la empresa. Realizada la identificación de los sistemas de identificación de intrusos sus clasificación y tipologías, es necesario determinar cuál es la importancia o relevancia del uso de estos sistemas para las empresas.

Dentro de las organizaciones se cuenta con activos que corresponden a bienes que son propiedad de la empresa y que pueden convertirse en dinero, dentro de los activos encontramos los tangibles que corresponden a la maquinaria, los bienes inmuebles

4.1.1.8. Un activo es un bien que la empresa posee y que puede convertirse en dinero u otros medios líquidos equivalentes. que son propiedad de la empresa que deben ser salvaguardados, estos activos son tangibles de bienes inmuebles, muebles. equipos informáticos, y los activos intangibles que incluyen marcas, permisos patentes y dentro de ello, la reputación, el conocimiento e información de la empresa[23].

[22] KENKRE, Poonam Sinai; PAI, Anusha; COLACO, Louella. Real time intrusion detection and prevention system. En Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014. Springer, Cham, 2015. p. 405-411.

[23] ROSIQUE, Antonio Sola; MÁRQUEZ, Adolfo Crespo. *Principios y marcos de referencia de la gestión de activos*. AENOR-Asociación Española de Normalización y Certificación, 2016

Considerando la importancia de los activos se hace necesario establecer la seguridad y salvaguarda de estos bienes, entrándonos en los activos que atañe a la seguridad informática se hace necesario determinar el ámbito de la seguridad de la información.

4.1.1.9. Seguridad de la información. De acuerdo con la norma ISO 27001 hace referencia al a preservación de la de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad[24]

Considerando el activo que se va a proteger en este acaso los sistemas de información que son indispensables para el eficaz funcionamiento de la empresa, y el tipo de acción de seguridad a implementar, para evitar los daños en el sistema o para minimizar estos daños[25].

4.1.2. Riegos y vulnerabilidades que se pueden llegar contrarrestar en un sistema de detección de intrusos. teniendo presente la importancia de un sistema de detección y prevención de intrusos, se hace necesario que se definan las vulnerabilidades que enfrentan para ello se establen las siguientes

4.1.2.1. Vulnerabilidades aún no conocidas por la empresa, pero que un ajeno puede detectar y aprovechar para cumplir su propósito de afectación a la empresa, este tipo de vulnerabilidad puede clasificarse como Critica porque permite la propagación de un gusano de internet; importante si pone en riegos la confidencialidad, integridad o disponibilidad de datos o recursos de procesamiento

[24] ICONTEC. Norma IEC 27001. Tecnología de información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.2013. Bogotá: Icontec

[25] SEOANE RUANO, C., SAIZ Herrero, A. B., FERNÁNDEZ ÁLVAREZ, E., & FERNÁNDEZ ARANDA, L. Seguridad informática. 2010. Madrid: McGraw-Hill/Interamericana de España, S.L.

del sistema; moderad cuando es fácil de manejar a partir de configuración por defecto y baja que es detecta con facilidad y no produce impacto.[26]

4.1.2.2. Vulnerabilidades conocidas de aplicaciones no instaladas pero que son de conocimiento de la industria que desarrolla el software

4.1.2.3. Vulnerabilidad conocida sobre aplicaciones instaladas que son conocidas por la empresa que las desarrolla y que establece una solución que se denomina parche.

4.1.2.4. Tipos de amenazas que enfrenta una organización son los robos de información, perdidas de información, perdida de la integridad de la información de la empresa, ataques de red, acceso no autorizado al sistema y contagio de virus informáticos. Que pueden ser operados por diferentes tipos de atacantes[27]:

- Hackers: persona con conocimiento informáticos y amplia curiosidad en identificar las vulnerabilidades del sistema peri sin motivación dañina
- Crackers: persona con conocimiento informáticos y amplia curiosidad en identificar las vulnerabilidades del sistema, pero con intensión dañina
- Phreaks: es un cracker telefónico, que altera el sistema de redes telefónicas para conseguir llamadas gratis.
- Sniffers: persona con conocimiento amplio en redes informáticas que realiza un análisis de tráfico y obtiene paquetes de información determinada.
- Ciber terroristas: personas con conocimiento amplio en informática e intrusiones de red que sirve a organizaciones de

[26] SEOANE RUANO, C., Saiz Herrero, A. B., FERNÁNDEZ ÁLVAREZ, E., & Fernández Aranda, L. Seguridad informática. 2010. Madrid: McGraw-Hill/Interamericana de España, S.L
[27] Ibid

contrainteligencia y para sabotear los sistemas con propósitos políticos y financieros.

- Programadores de virus: persona con amplio conocimiento en programación, sistemas y redes que desarrollan programas que atacan lo sistema produciendo efectos muchas veces catastróficos.
- Carders: personas que se dedican al estudio se la informática y los sistemas de cajeros automáticos

Tipos de interrupción • Un recurso del sistema o la red deja de estar disponible debido a un ataque

4.1.2.5. Los Tipos de ataques, son las formas en las cuales se ven amenazados los sistemas y se producen las intrusiones encontramos así[28]:

- Phishing: Suplantación de identidad a través de un sitio web
- Keyloggers: herramientas que espía al usuario y permite observar lo que digita y ejecuta en pantalla.
- Spoofing: suplantación de la identidad de una maquina
- Sniffing: monitorización del tráfico de red para robar paquetes de información.
- Ingeniería social: obtención de información personal y confidencial con fines de manipulación y uso indebido.
- Conexión no autorizada: se realiza una conexión a través de puertas traseras o vacíos de seguridad de un servidor o equipo

Teniendo conocimiento de la tipología de los ataques, las amenazas y los tipos de ataques se observa como in sistema de detección de intrusos, previene el desarrollo de las amenazas planteadas al sistema de una empresa.

[28] SEOANE RUANO, C., Saiz Herrero, A. B., FERNÁNDEZ ÁLVAREZ, E., & FERNÁNDEZ ARANDA, L. Seguridad informática. 2010. Madrid: McGraw-Hill/Interamericana de España, S.L

4.2 MARCO CONCEPTUAL

Desde que internet se hizo realidad en la década de los 70s, ha crecido de manera exponencial, de otra manera las soluciones para detectar la intrusión en la red están muy lejos, los impactos económicos de ataques maliciosos y la pérdida de ingresos para una empresa son bastante considerables.

Los IDS se clasifican en función del despliegue de sus sensores o método de análisis. Según la fuente de entrada, "el IDS puede clasificarse como Basado en el host, estos IDS implementan sensores para monitorear las características y comportamientos de un solo host; Basados en la red, estos IDS implementan sensores para recopilar tráfico de red para segmentos de red de interés o tráfico de red de hosts específicos; e IDS híbridos, que implementan sensores para recopilar tráfico de red, así como entradas de host de hosts monitoreados"[29]. Los IDS también se clasifican según el componente de análisis del IDS, es decir, según el procesamiento de los datos recopilados de los sensores[30] Esta distinción es importante, ya que, antes de la red inteligente, la visibilidad de la demanda era limitada. –La red lateral

La notificación[31] y los enfoques del sistema de respuesta manual [32] [33]son insuficientes e incapaces de responder a los ataques de alta velocidad debido a su

[29] LIU, A. X., & GOUDA, M. G. Diverse firewall design. IEEE Transactions on Parallel and Distributed Systems.2008

[30] SABAHI F. AND MOVAGHAR A. "Intrusion Detection: A Survey," in 2008 Third International Conference on Systems and Networks Communications, 2008, pp. 23-26.

[31] PAXSON v, et al. Framework for IP Performance Metrics. IETF RFC2330. (1998.).

[32] TANACHAIWIWAT, Sapon; HWANG, Kai; CHEN, Yue. Adaptive intrusion response to minimize risk over multiple network attacks. *ACM Trans on Information and System Security*, 2002, vol. 19, no 1-30, p. 95-96.

[33] KRÜGEL, Christopher; TOTH, Thomas; KIRDA, Engin. Service specific anomaly detection for network intrusion detection. En *Proceedings of the 2002 ACM symposium on Applied computing*. 2002. p. 201-208.

inactividad naturaleza. Los enfoques antes mencionados dejan un espacio de tiempo de vulnerabilidad entre la primera respuesta y la intrusión detectada[34] [35] por lo tanto, se proponen sistemas de respuesta altamente automatizados para disminuir el tamaño de la ventana de vulnerabilidad.

DS (detección de intrusiones) se realiza a través de una red o sistema informático desde una serie de puntos clave en la recopilación de información y análisis, desde una red o sistema se encuentra en violación del comportamiento de la política de seguridad y signos de un ataque, mientras se responde. Como herramienta matemática, el análisis se ha utilizado ampliamente en análisis de señales, procesamiento de imágenes, análisis numérico, etc. se presenta el desarrollo del sistema de detección de intrusos basado en la red y propone el sistema de detección de intrusos basado en el algoritmo de red. Finalmente, el documento diseña un sistema de detección de intrusos de red[36] y verificado a través de experimentos de simulación de este sistema de detección de intrusos es factible.

Para este proyecto es importante contar con claridad en conceptos que se abordaran en su desarrollo. Iniciamos con la seguridad Informática que hace referencia a las medidas que se implemente para evitar que se realicen acciones no autorizadas en un sistema o de informática que cause daño o comprometa la confidencialidad, la autenticidad o la integridad de la información y disminuya la efectividad de los equipos que compone el sistema o la red[37].

---

[34] STAKHANOVA, Natalia; BASU, Samik; WONG, Johnny. A taxonomy of intrusion response systems. *International Journal of Information and Computer Security*, 2007, vol. 1, no 1-2, p. 169-184.

[35] LIAO, Hung-Jen, et al. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 2013, vol. 36, no 1, p. 16-24.

[36] GUANGXIAN. JI.The Development Of Intrusion Detection System Based On Wavelet Network. (2012). INTERNATIONAL JOURNAL ON Advances in Information Sciences and Service Sciences. 4. 261-268. 10.4156/aiss.vol4.issue9.32.

[37] VIEITES, Álvaro Gómez. *Enciclopedia de la seguridad informática*. Grupo Editorial RA-MA, 2011

Si se aborda la amenaza en este contexto se pude establecer que es un evento realizado de manera accidental o intencional que llegué a ocasionar daños en el sistema informática acareando pérdidas materiales, financieras o de otro tipo a la organización que lo sufre[38]

En este orden es pertinente abordar la vulnerabilidad como la debilidad que posee el sistema informático, que es ocasionado por las amenazas que puede ocasionar daños y perdidas[39],

De aquí se derivan los incidentes de seguridad que son eventos que pueden ocasionar la interrupción de los servicios del sistema y con ello perdida, es la manera en la que se materializa la amenaza[40].

Dentro de la seguridad informática es de vital importancia establecer los riesgos que tiene el sistema, entendido este como la probabilidad de que se materialice a causa de una vulnerabilidad una amenaza causando un incidente que genere impacto[41]
Un concepto que es importante conocer es el Hacking considerada una acción para obtener los privilegios que le permitan ingresar en un sistema informático mediante el uso de técnicas de programación y identificado las vulnerabilidades del sistema[42]

Con el propósito de contrarrestar las amenazas y vulnerabilidades se cuenta con herramientas como los IDS que es un sistema de detección de intrusos, que determina la existencia de comportamiento anómalos en los usuarios de la red y que pueden ser una amenaza para esta[43]

---

[38] VIEITES, Álvaro Gómez. *Enciclopedia de la seguridad informática*. Grupo Editorial RA-MA, 2011.
[39] Ibid
[40] Ibid
[41] Ibid
[42] STALLMAN, Richard. On hacking. *Retrieved April*, 2002, vol. 30, p. 2009.
[43] SABAHI F. AND MOVAGHAR A. “Intrusion Detection: A Survey,” in 2008 Third International Conference on Systems and Networks Communications, 2008, pp. 23-26

También se cuenta con sistema de detección de intrusos IPS que realiza acciones de control de acceso en una red para poder protegerla de ataques y amenazas [44]Software libre es un software de código abierto que permite a los usuarios ver libremente su código fuente, modificarlo, distribuirlo y utilizarlo sin ninguna restricción.[45]

[44] DITECH. Prevención de Intrusos. consultado en línea http://ditech.com.co/soluciones-integrales/seguridad-informatica-en-redes/prevencion-de-intrusos-ips-2/

[45] GONZÁLEZ Yolanda . ¿Qué es el software libre? Características y ventajas. Grupo Atico34. Consultado en línea https://protecciondatos-lopd.com/empresas/software-libre/

4.3 ANTECEDENTES

Para el desarrollo de este proyecto se han tenido en cuenta trabajos que presentan problemáticas similares a las abordadas en este trabajo de grado, en este sentido se describen algunos de estos proyectos que sirven de referencia frente a la temática abordada y al entorno de los modelos de detección de intrusos

Iniciamos con el proyecto desarrollado en la Universidad Regional Autónoma De Los Andes en Ambato Ecuador que desarrolla un sistema de detección y prevención de intrusos para el control de vulnerabilidades de la red corporativa de la universidad regional autónoma de los andes “UNIANDES” presentados por Byron Patricio Camacho Mera, quien propone un IDS que observa y verifica los paquetes de información que viajan por una o más líneas de la red corporativa, buscando identificar las actividades anómalas o maliciosas, para este desarrollo se aplica IDS snort con el firewall, para doblar la seguridad y monitorizar la comunicación y el tráfico de información con el exterior, se implementó un software IDS/IPS, en concordancia con la políticas de manejo de información de la universidad, perfilando la presencia de los funcionarios en la redes y proporcionado blogs que permitieron el bloqueo de IP de atacantes, el desarrollo del sistema se realiza con herramientas de código abierto, demostrado compatibilidad entre ellas, con lo cual se reducen las exposiciones al riesgo y la disminución de amenazas.

El segundo proyecto es un Detector de Intrusos Basado en Sistema Experto, presenta un modelo que aísla un equipo que haya sido atacado y que ese ataque compromete la seguridad e la red a través del control e instalación de código malicioso, en este caso hace la propuesta de un filtro de direcciones IP mediante la herramienta Fira, que aísla el equipo, el sistema propone una estrategia de distracción o engaño en el que dados los parámetros determinados, el atacante no detecta el aislamiento del equipo, lo que permite que el administrador de la red analice el ataque, actualice los protocolos y emita la alertas para salvaguardar el sistema. Este modelo lo propone la ingeniera Vanessa Gonzales Marques como

trabajo de grado de la maestría en Ciencias en Ingeniería de Cómputo con opción en Sistemas Digitales, del Instituto Politécnico Nacional de México

El tercer proyecto es un trabajo de Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia, este desarrollo plantea una propuesta para el desarrollo de un sistema automático para análisis el tráfico de la red que emite un reporte digital con la alertas de intrusiones diarias, con el propósito de identificar la respuesta que debe operar en cada llamada realizada, estableciendo así protocolos de acción a las maquinas, lo cual disminuye el riesgo de intrusiones a través de la utilización del software Snort gratuito, multiplataforma y de código abierto, este modelo es presentado por Emilio José Mira Alfaro.

4.4 MARCO LEGAL

Para establecer el marco legal en el ámbito de seguridad de la información, que acoge un sistema de detección y prevención de intrusos en la red es necesario precisar una jerarquía para uso y aplicación de la normatividad, en ese sentido y acogiéndose a orden de prelación de las normas jurídicas establecido por Kelsen46 encontramos los siguiente:

La constitución política de Colombia, dentro de su articulado presenta elementos que abordan la protección de la información de los ciudadanos en diferentes ámbitos el primero se encuentra en el artículo 15 presenta el derecho a la intimidad personal y familiar como aspectos fundamentales, de igual manera en el artículo 61 se presenta la garantiza y responsabilidad de protección de la propiedad intelectual por parte del estado.

Acogiendo lo dispuesto en la carta magna se expide la ley 527 de 1999 acerca del comercio electrónico, que presente la regulación fundamental acerca del acceso y

[46] KELSEN, Hans. Teoría general del derecho y del Estado. Unam, 1958.

uso de los mensajes de datos, el comercio electrónico y la firma digital estableciendo entidades de certificación de los procesos referidos en esta ley.

En el año 2000 el código penal tipifica la violación de la intimidad reserva e interceptación de comunicaciones en el capítulo VII y en lo artículos 192 a 197, donde acceso abusivo a un sistema informático, dando una connotación de delito a la violación de las redes informáticas.

La ley 1266 de 2008, dicta disposiciones acerca de habeas data y la regulación Enel manejo de la información que se encuentra consignada en las bases de datos personales, incluyendo la información financiera, crediticia, comercial, de servicios y la que sea proveniente de terceros, con lo que se regula la protección a la privacidad establecida en la constitución,

En el año 2009 se promulga la Ley 1273, la cual es una modificación al código penal que establece la inclusión de la protección de la información y de los datos con el fin de preservar de manera integral los sistemas que utilizan tecnologías de la información y la comunicación; esta ley presenta un hito importante en la normalización de los delitos informáticos, así como en la regulación y defensa de los derechos de privacidad y de propiedad intelectual consagrados ne la constitución.

La ley 1581 de 2012, se expide para la protección de los datos de los ciudadanos, se encuentra enmarcada por el derecho constitucional de los artículos 15, 20 y 21 sobe la intimidad, la privacidad, el conocimiento, actualización y rectificación de la información recogida en bases de datos o archivos.

El decreto 1377 reglamenta la ley 1581 de protección de datos, donde se abordan aspectos que atañen con el tratamiento de datos personales, las políticas de tratamiento de los responsables y encargado de la información, la transferencia de datos entre otros, sentando un precedente jurídico con respecto al manejo de información y de los datos.

Este marco jurídico establece ámbito de actuación y justifica la importancia de la seguridad informática, del manejo de la información y del tratamiento de los datos dando alcance a la relevancia en el diseño de sistemas de detección y prevención de intrusos controlando la vulnerabilidad de la rede informáticas, cumpliendo con la ley del estado colombianos y favoreciendo los derechos de los ciudadanos.

4.5 MARCO METODOLÓGICO

El proyecto es de carácter cualitativo y se desarrolla con un alcance descriptivo, mediante, el cual se propone definir un sistema de detección de intrusos en la red de una empresa, mediante el uso de software especializado y simulación, este desarrollo cobra importancia en el caso concreto de las pequeñas empresas que requiere de un control de sus vulnerabilidades y la garantía de la seguridad de la información, mediante el uso del software libre, lo cual a su vez favorece los costos de seguridad informática.

4.5.1. MÉTODO

El proyecto definirá la detección de intrusos que se realiza a una red con 5 equipos, en donde se cuenta con sistemas operativos montados en una máquina virtual desde donde se monitorea el funcionamiento de la red y la seguridad propuesta describiendo las fases que se realizan para la detección de la vulnerabilidad de la red a partir de los cual se analizaran las alternativas de solución y se llegara a una conclusión.

El método se aborda desde la perspectiva del esquema Pozas que incluye las siguientes etapas.

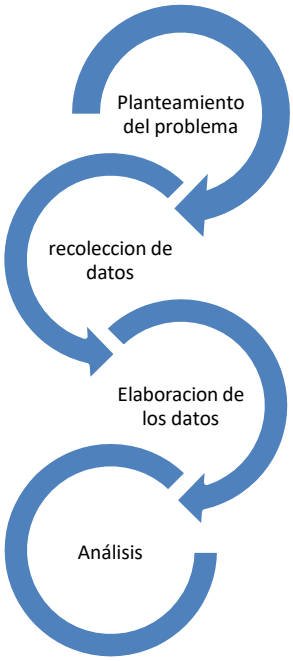
a) Planteamiento de la investigación: donde se realiza el proceso de información bibliográfica y descripción de la problemática y su visión

b) Recolección de datos: Establecimiento y definición de variables a relacionar con el problema

c) Elaboración de los datos: Elaboración de instrumentos de observación e identificación de variables.

d) Análisis: estudio de los datos de fuentes primarias y secundarias y desarrollo de la parte concluyente.

Figura 2 Perspectiva de investigación



Fuente: **POZAS, R. El desarrollo de comunidades técnicas de investigación social. 2 Ed. UNAM México. 1979**

4.5.1.1. FASES DE DESARROLLO

Fase 1: identificación de tipos y formas de ataques en las redes.

Actividades:

- Verificar que los protocolos de red sean adecuados para evitar por este lado vulnerabilidades y amenazas, y que se cumpla con las normas establecidas.
- Revisar que por la transmisión de los datos no se esté presentando derivaciones ni alteraciones que puedan ocasionar fuga de la información.
- Analizar que por los canales de la interfase se esté efectuando una transmisión acorde con las especificaciones.
- Estar completamente seguro de que en lo referente a la recuperación este bien establecido que si falla la señal ya sea por corriente o por otro aspecto, la información sea capaz de recuperarse y que no se pierda nada de la información emitida.
- Que la parte del formato de los datos garantice su emisión y recepción sin perdida alguna de este.
- De acuerdo con la repetición de la información si hay un error que se pueda garantizar la retrasmisión del mensaje hasta que este llegue sin errores.
- Efectuar un análisis concerniente al enrutamiento de la red, con, lo que se verifica tanto que el emisor como el receptor sean los autorizados.
- Identificación de acuerdo con las direcciones que lleguen los mensajes a su destino así no se encuentre el destinatario en la misma red.
- Analizar que el control de flujo no se sature evitando saturación de la red.

Fase 2 Establecimiento de puntos de control.
Actividades:

- Contraseñas seguras con mínimo 8 caracteres incluyendo letras, mayúsculas minúsculas, números y caracteres.
- Cifrado y autenticación de usuariosA

- Filtrado de direcciones IP, el cual es un método eficaz para conceder accesos específicos a la red.
- Actualización de Software, comprobación de configuraciones, verificar estándares en la seguridad de la empresa

Fase 3 Determinar las herramientas para el análisis, control y regulación del tráfico de la red.

Actividades:

- Escaneo para determinar clase de gravedad de la red, tarea con resultados en los hosts, informe para la clase de gravedad obtenido, reportes de estado
- Informe de la puntuación de las vulnerabilidades CVSS.
- Análisis de las vulnerabilidades en la nube, con resultados por sistema de puntuación de vulnerabilidad.
- Análisis SSH algoritmos de MAC débiles admitidos.
- OpenSSH vulnerabilidades de denegación de servicio y enumeración de usuarios
- Topología de los hosts
- Llaves y reportes.
- Estado de SO y gravedad de los sistemas.
- Sistemas operativos por CVSS
- Listado de los SO existentes en la red.
- Servicios de terminal virtual, clase de gravedad de estos.
- Porcentaje de vulnerabilidades posibles en los SO.

- Lenguajes de evaluación.
- Avisos de seguridad DFN.
- Informe de procesos y cargas de los sistemas, sistema de subida, de información, usos de CPU, usos de memorias físicas y de intercambio de información, uso del sistema de archivos, lectura de discos y operación de escritura, cargas y entradas de discos, interfaz del tráfico de la red, sensores de temperatura de los procesadores.

5 DESARROLLO DE LOS OBJETIVOS

5.1. FASE 1: IDENTIFICACION DE TIPOS Y FORMAS DE ATAQUES EN LA REDES

Cada violación de datos y ataque en línea parece involucrar algún tipo de intento de phishing para robar credenciales de contraseña, lanzar transacciones fraudulentas o engañar a alguien para que descargue malware. A principios de 2016, el 93 por ciento de los correos electrónicos de phishing entregaron ransomware, según las estadísticas de PhishMe .

Las empresas regularmente recuerdan a los usuarios que tengan cuidado con los ataques de phishing , pero muchos usuarios realmente no saben cómo reconocerlos. Una razón para esto es el hecho de que estos ataques pueden tomar muchas formas. "Los ataques de phishing se presentan en todas las formas y tamaños, dirigidos a individuos específicos dentro de una organización que tienen acceso a datos confidenciales", dice Shalabh Mohan de Area 1 Security.

Los usuarios tienden a ser malos para reconocer estafas. Según un informe de seguridad cibernética de VERIZON , un atacante que envía 10 correos electrónicos de phishing tiene un 90 por ciento de posibilidades de que una persona caiga en la trampa. Esto parece absurdo al principio, pero es razonable cuando se considera en el contexto de los usuarios fuera de la burbuja tecnológica, como los de la manufactura y la educación. Agregue el hecho de que no todas las estafas de phishing funcionan de la misma manera, algunas son explosiones genéricas de correo electrónico, mientras que otras están cuidadosamente diseñadas para dirigirse a un tipo muy específico de persona, y se hace más difícil capacitar a los usuarios para saber cuándo un mensaje parece

un poco extraño. Veamos los diferentes tipos de ataques de phishing y cómo reconocerlos

5.1.1. ¿Qué es el phishing? correos electrónicos del mercado masivo. La forma más común de phishing es el tipo general, enviado por correo masivo, donde alguien envía un correo electrónico simulando ser otra persona e intenta engañar al destinatario para que haga algo, generalmente iniciando sesión en un sitio web o descargando programa maligno. Los ataques con frecuencia dependen de la suplantación de identidad del correo electrónico, donde el encabezado del correo electrónico, el campo de, se falsifica para que el mensaje aparezca como si hubiera sido enviado por un remitente de confianza[47].

Sin embargo, los ataques de phishing no siempre se ven como un correo electrónico de notificación de entrega de UPS[48], un mensaje de advertencia de PayPal sobre el vencimiento de las contraseñas o un correo electrónico de Office 365 sobre las cuotas de almacenamiento. Algunos ataques están diseñados para apuntar específicamente a organizaciones e individuos, y otros dependen de métodos distintos al correo electrónico[49].

[47] RANGEL SOSA, Karen Irlanda, et al. Rastreo de correos electrónicos. 2017.
[48] CORTÉS HERNÁNDEZ, Andrés Mauricio. Ingenieria social Phishing y Baiting. 2019
[49] GIRALDO MARTÍNEZ, Jenny Paola, et al. Ingeniera social: Técnica de ataque Phishing y su impacto en las empresas colombianas.

5.1.2. ¿Qué es el spear phishing? Ir tras objetivos específicos Los ataques de phishing reciben su nombre de la noción de que los estafadores están buscando víctimas aleatorias mediante el uso de correo electrónico fraudulento o falso como cebo. Los ataques de spear phishing amplían la analogía de la pesca, ya que los atacantes apuntan específicamente a víctimas y organizaciones de alto valor[50]. En lugar de tratar de obtener credenciales bancarias para 1,000 consumidores, el atacante puede encontrar más lucrativo apuntar a un puñado de negocios. Un atacante de una nación-estado puede apuntar a un empleado que trabaja para otra agencia gubernamental, o un funcionario del gobierno, para robar secretos de estado.

Los ataques de spear phishing son extremadamente exitosos porque los atacantes pasan mucho tiempo elaborando información específica para el destinatario, como hacer referencia a una conferencia a la que el destinatario acaba de asistir o enviar un archivo adjunto malicioso donde el nombre de archivo hace referencia a un tema que le interesa al destinatario.

En una reciente campaña de phishing, el Grupo 74 (también conocido como Sofact, APT28, Fancy Bear[5152]) se dirigió a profesionales de la seguridad cibernética con un correo electrónico que pretendía estar relacionado con la conferencia Cyber Conflict US, un evento organizado por el Instituto Cibernético del Ejército de la Academia Militar de los Estados Unidos, la Cooperativa de la OTAN La Academia Militar Cibernética y el Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN. Si bien CyCon es una conferencia real, el archivo adjunto era en realidad un documento que contenía una macro maliciosa de Visual Basic para Aplicaciones (VBA) que descargaría y ejecutaría un programa maligno de reconocimiento llamado Seduploader.

---

[50] DOMINGUEZ, Antonio Hernández. Sistema para la detección de ataques PHISHING utilizando correo electrónico. *Telemática*, 2019, vol. 17, no 2, p. 60-70

[51] CALVET, Joan; CAMPOS, Jessy; DUPUY, Thomas. Visiting The Bear Den. *WeLiveSecurity Blog*, 2016.

[52] VAN DEN BERG, Jan. MODELING FANCY BEAR CYBER ATTACKS. 2017.

5.1.3. ¿Qué es la caza de ballenas? ir tras el grande. Diferentes víctimas, diferentes días de pago. Un ataque de phishing[53] dirigido específicamente a los altos ejecutivos de la empresa se llama caza de ballenas, ya que la víctima se considera de alto valor, y la información robada será más valiosa que la que puede ofrecer un empleado regular. Las credenciales de la cuenta que pertenecen a un CEO abrirán más puertas que un empleado de nivel de entrada. El objetivo es robar datos, información de empleados y dinero en efectivo.

La caza de ballenas también requiere investigación adicional porque el atacante necesita saber con quién se comunica la víctima prevista y el tipo de discusiones que tiene. Los ejemplos incluyen referencias a quejas de clientes, citaciones legales o incluso un problema en la suite ejecutiva. Los atacantes suelen comenzar con la ingeniería social para recopilar información sobre la víctima y la empresa antes de elaborar el mensaje de phishing que se utilizará en el ataque de la caza de ballenas.

5.1.4. ¿Qué es el compromiso comercial por correo electrónico (BEC)? Pretendiendo ser el CEO. Además de las campañas de phishing general distribuidas en masa, los delincuentes atacan a personas clave en los departamentos de finanzas y contabilidad a través de estafas de compromiso de correo electrónico comercial (BEC) y fraude de correo electrónico de CEO54. Al hacerse pasar por oficiales financieros y directores ejecutivos, estos delincuentes intentan engañar a las víctimas para que inicien transferencias de dinero en cuentas no autorizadas.

Por lo general, los atacantes comprometen la cuenta de correo electrónico de un alto ejecutivo o funcionario financiero al explotar una infección existente o

[53] BELISARIO MÉNDEZ, Aymara Noriley. *Análisis de métodos de ataques de Phishing*. 2014. Tesis Doctoral. Universidad de Buenos Aires. Facultad de Ciencias Económicas.
[54] FERRANDO GUILLEM, Anna Lourdes. La ciberseguridad como reto internacional: la protección frente a las ciberamenazas.

mediante un ataque de phishing. El atacante acecha y monitorea la actividad de correo electrónico del ejecutivo durante un período de tiempo para conocer los procesos y procedimientos dentro de la empresa. El ataque real toma la forma de un correo electrónico falso que parece provenir de la cuenta del ejecutivo comprometido que se envía a alguien que es un destinatario habitual. El correo electrónico parece ser importante y urgente, y solicita que el destinatario envíe una transferencia bancaria a una cuenta bancaria externa o desconocida. El dinero finalmente aterriza en la cuenta bancaria del atacante.

Según el Centro de Quejas de Delitos en Internet del FBI, las estafas de BEC han generado más de $ 4.5 mil millones en pérdidas reales e intentadas, y son un problema global masivo.

5.1.5. ¿Qué es el phishing de clones? Las copias son igual de efectivas. El phishing de clones[55] requiere que el atacante cree una réplica casi idéntica de un mensaje legítimo para engañar a la víctima para que piense que es real. El correo electrónico se envía desde una dirección que se asemeja al remitente legítimo, y el cuerpo del mensaje tiene el mismo aspecto que un mensaje anterior. La única diferencia es que el archivo adjunto o el enlace en el mensaje se ha cambiado por uno malicioso. El atacante puede decir algo parecido a tener que reenviar el original, o una versión actualizada, para explicar por qué la víctima estaba recibiendo el "mismo" mensaje nuevamente.

Este ataque se basa en un mensaje legítimo visto anteriormente, por lo que es más probable que los usuarios caigan en el ataque. Un atacante que ya ha infectado a un usuario puede usar esta técnica contra otra persona que también recibió el mensaje que se está clonando. En otra variación, el atacante puede crear un sitio web clonado con un dominio falso para engañar a la víctima.

[55] ABDELHAMID, Neda; AYESH, Aladdin; THABTAH, Fadi. Phishing detection based associative classification data mining. *Expert Systems with Applications*, 2014, vol. 41, no 13, p. 5948-5959.

5.1.6. ¿Qué es vishing? Phishing por teléfono. Vishing[56] significa "phishing de voz" e implica el uso del teléfono. Típicamente, la víctima recibe una llamada con un mensaje de voz disfrazado como una comunicación de una institución financiera. Por ejemplo, el mensaje puede pedirle al destinatario que llame a un número e ingrese su información de cuenta o PIN por seguridad u otros fines oficiales. Sin embargo, el número de teléfono suena directamente al atacante a través de un servicio de voz sobre IP.

Recientemente, los delincuentes han comenzado a llamar a las víctimas que fingen ser soporte técnico de Apple y proporcionan a los usuarios un número para llamar para resolver el "problema de seguridad". Al igual que la antigua estafa de soporte técnico de Windows, estas estafas aprovechan los temores de los usuarios de que sus dispositivos sean pirateados.

5.1.7. ¿Qué son raquetas de nieve? Difusión mensajes venenosos. Las raquetas de nieve[57], o spam "golpear y correr", requiere que los atacantes envíen mensajes a través de múltiples dominios y direcciones IP. Cada dirección IP envía un bajo volumen de mensajes, por lo que las tecnologías de filtrado de spam basadas en la reputación o el volumen no pueden reconocer y bloquear mensajes maliciosos de inmediato. Algunos de los mensajes llegan a las bandejas de entrada del correo electrónico antes de que los filtros aprendan a bloquearlos.

Las campañas de tormenta de granizo funcionan igual que las raquetas de nieve, excepto que los mensajes se envían en un período de tiempo extremadamente corto. Algunos ataques de granizo terminan justo cuando las herramientas

[56] GRIFFIN, Slade E.; RACKLEY, Casey C. Vishing. En *Proceedings of the 5th annual conference on Information security curriculum development*. 2008. p. 33-35.
[57] GARRIDO, Fabián Blanco; MOYANO, Eduardo Triana; CARRANZA, Juan Fernando Velásquez. TANATALOGÍA DIGITAL: MÁXIMA EXPRESIÓN DE LA SEGURIDAD INFORMÁTICA.

antispam se ponen al día y actualizan los filtros para bloquear mensajes futuros, pero los atacantes ya han pasado a la próxima campaña.

5.1.8. Como reconocer los diferentes tipos de phishing. Los usuarios no son buenos para comprender el impacto de caer en un ataque de phishing[58]. Un usuario razonablemente inteligente puede evaluar el riesgo de hacer clic en un enlace en un correo electrónico, ya que eso podría provocar una descarga de programa maligno o mensajes de estafa de seguimiento pidiendo dinero. Sin embargo, un usuario ingenuo puede pensar que no pasaría nada o terminar con anuncios de spam y ventanas emergentes. Solo los usuarios más expertos pueden estimar el daño potencial del robo de credenciales y el compromiso de la cuenta. Esta brecha en la evaluación de riesgos hace que sea más difícil para los usuarios comprender la seriedad de reconocer mensajes maliciosos."A pesar de la continua inversión, los correos electrónicos de phishing continúan eludiendo las tecnologías perimetrales para llegar a las bandejas de entrada de los empleados todos los días", dijo Rohyt Belani, cofundador y CEO de PhishMe.

Las organizaciones deben considerar las campañas de concienciación interna existentes y asegurarse de que los empleados reciban las herramientas para reconocer diferentes tipos de ataques. Las organizaciones también necesitan reforzar las defensas de seguridad, porque algunas de las herramientas tradicionales de seguridad de correo electrónico, como los filtros de spam, no son suficiente defensa contra algunos tipos de phishing. Por ejemplo, los filtros de spam no son útiles contra los ataques BEC.

[58] BELISARIO MÉNDEZ, Aymara Noriley. *Análisis de métodos de ataques de Phishing*. 2014. Tesis Doctoral. Universidad de Buenos Aires. Facultad de Ciencias Económicas

5.2. FASE 2 ESTABLECIMIENTO DE PUNTOS DE CONTROL

5.2.1. Procedimiento de Detección de Paquetes. La detección de paquetes tiene como propósito fundamental capturar todos los datos entrantes y el tráfico de red saliente, en este sentido la instalación de un rastreador de paquetes debe ser ubicado en los bordes de la red, para que ejerza la labor de revisión de todos los paquetes sospechosos que son recibidos por la red y de fama indiscriminada dentro de este ejercicio se debe contar con un módulo que elabore y analice los paquetes en bruto logrando la identificación de la firma del paquete de ataque, con base en el encabezado de este y en los detalles particulares como son, dirección IP de origen y destino, puertos, protocolos, encabezado, tamaño, tiempo de vida, marcas de bits utilizadas.

La Identificación de ataques implica la extracción de paquetes de trazas de información esencial, captar detalles y comprarlos con el analizador de paquetes en bruto para determinar cuál es el ataque real lanzado, desde este momento se realiza un reporte de los detalles del ataque, que soportan el proceso de decisión a ejecutar en el sistema como la aplicación, de reglas, alertas, acciones, eventos, verificación del estado de la red.

Al contar con la operación del cortafuegos combinado con el uso de NIDS, se busca la identificación de los paquetes sospechosos desconocidos, categorizados como privados o externos provenientes de una red no confiable, nos permite rastrear el funcionamiento eficiente o defectuoso del firewall, aspecto que permite suministrar información al administrador de la red que contenga los detalles del ataque, como la fuente, la víctima, las direcciones IP y se haga una marca de tiempo del ataque y el tipo de regla aspectos que le permitirán diseñar estrategias de seguridad para la red.

Es conocido que los paquetes pueden tener origen en una fuente privada o una red no confiable, en tal sentido si se piensa en el paquete [P] que se origina en una red no confiable y se lanza a una ataque lo primero que encuentra es el Switch LAN, este paquete [P] entonces se dirige al firewall donde su función principal es la de

hacer de filtro al tráfico y acorde con el conjunto de reglas que se hayan configurado, en este punto si el paquete se caen, se puede afirmar que su ciclo de vida termino, ahora si el paquete tiene alguna rasta sospechosa el sensor NIDS debe tener la capacidad de detectar y elaborar una copia de este paquete [PC],la cual debe ser desarrollada por el interruptor LAN, las características de estos paquetes deben ser entregadas y enviadas a una interfaz junto con la copia detectada del paquete, para efectuar un examen y análisis acorde con las reglas y políticas establecidas en la configuración inicial, posteriormente si en el análisis el sensor detecta que el paquete examinado como una amenaza y el firewall permite, se debe remitir al segundo conmutador de LAN donde nuevamente se cree una copia de paquete PC2 por si hay alguna sospecha entonces se envía al sensor maestro NIDS para examen y análisis según las reglas y políticas definidas en el inicio en la configuración del sensor NIDS, este procedimiento se realiza con el propósito del confirmar que el firewall realmente hace cumplir las reglas y políticas configuradas, de esta manera se validad la seguridad de la información que solicita acceso a red garantizando la confiabilidad de este paquete.

5.2.2. Detección de intrusión al sistema

5.2.2.1. Materiales y procedimientos. Un sistema de intrusión ideal debería abordar los temas independientemente del mecanismo en el que se basa, para defenderse de los ataques e intrusiones que a continuación, se describen de a curdo con Vinchurkar & Reshamwala[59] .

- El sistema debe poder ejecutarse continuamente sin supervisión humana, esto debe ser lo suficientemente confiable para ejecutarse en los antecedentes del sistema observado.
- No debe ser una "caja negra", lo que significa que su funcionamiento interno debe ser examinable desde afuera.

[59] VINCHURKAR, Deepika P.; RESHAMWALA, Alpa. A Review of Intrusion Detection System Using Neural Network and Machine Learning. 2012.

- Debe ser tolerante a fallos, lo que significa que debe sobrevivir a un fallo del sistema y no tener su base de datos reconstruida en el reinicio.
- Debe resistir la destrucción, el sistema puede monitorearse para asegurarse de que no ha sido explorado.
- Debe observar y registrar desviaciones de comportamiento normal.
- Se debe adaptar fácilmente al sistema, cada sistema tiene un patrón de uso diferente y el mecanismo de defensa debe adaptarse, se facilitan a estos patrones.
- Debe lidiar con el cambio de comportamiento del sistema, con el tiempo a medida que se van desarrollando nuevas aplicaciones adicionales.
- El sistema debe tener un falso muy bajo, una tasa positiva negativa y falsa.
- Dado que un IDS típico genera una gran cantidad de tráfico y eventos en sus registros, la clave es para el sistema y solo generar alertas sobre eventos de interés, el IDS efectivo tiene una tasa baja de falsos positivos y falsos negativos.

5.2.2.2. Clasificación de Intrusión. Se presenten sistemas de Detección y muchas maneras diferentes de clasificar los varios tipos de IDS en una red. Las clasificaciones no son mutuamente excluyentes. Por ejemplo, un IDS basado en red puede estar usando el enfoque basado en la firma para la detección y el seguimiento.

5.2.2.3. IDS Basados en Host. Un IDS basado en host (HIDS) es un IDS que generalmente opera dentro de un equipo, nodo o dispositivo su función principal es el monitoreo interno, aunque se han desarrollado muchas variantes de HIDS que pueden ser utilizadas para monitorear redes[60] principalmente, supervisa y analiza los aspectos internos de un equipo, nodo o dispositivo, un HIDS determina si un sistema ha sido comprometido y advierte a los administradores[61] Por ejemplo,

[60] RUIZ HOUSEHOLDER, Adrián; CANDIL VIZCAÍNO, Daniel; SÁNCHEZ-MARISCAL GONZÁLEZ, Guillermo. Detección de intrusos basada en Host (HIDS)-OSSEC. 2020.
[61] DE BOER, Pieter; PELS, Martin. Host-based intrusion detection systems. *Amsterdam University*, 2005.

puede detectar un programa sospechosos que accede a los recursos de un sistema de manera ilegal, o descubre que un programa ha modificado el registro de manera nociva los HIDS fueron los primeros tipos de intrusión en software de detección[62], a diferencia de los IDS basados en la red, un HIDS puede inspeccionar el flujo de comunicaciones completo, NIDS son técnicas de evasión, como los ataques de fragmentación o empalme de sesión, no se aplica porque el HIDS es capaz de inspeccionar la sesión totalmente recombinada como es presentado al sistema operativo[63].Las comunicaciones cifradas pueden ser monitoreadas porque una inspección de HIDS puede mirar el tráfico antes de que sea cifrado esto significa que las firmas de HIDS todavía son capaces de igualar contra ataques comunes y no ser cegados por el cifrado.

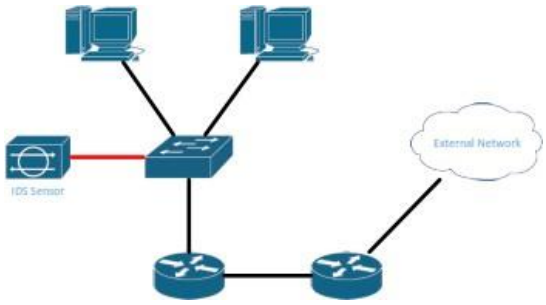
Un HIDS también es capaz de realizar, verificaciones adicionales a nivel del sistema que solo el software IDS instalado en una máquina host puede hacer, como archivo verificación de integridad, monitoreo de registro, análisis de registro,
detección de roots, y respuesta activa[64]

5.2.2.4. IDS Basados en Red. Un IDS basado en red (NIDS) [65]difiere de un HIDS en que generalmente se coloca a lo largo de una LAN, con lo que se Intenta descubrir personas no autorizadas y acceso malicioso a una LAN mediante el análisis de tráfico que atraviesa el cable a múltiples hosts. Hay muchos algoritmos para detectar tráfico malicioso, pero en general, leer los paquetes entrantes y salientes y buscar cualquier patrón sospechoso, cualquier alerta generada por un NIDS le permite notificar a los administradores o tomar las acciones activas, como

[62] SHARMA, Sanjay; GUPTA, R. K. Intrusion detection system: A review. *International Journal of Security and Its Applications*, 2015, vol. 9, no 5, p. 69-76.
[63] LÓPEZ, Julio Gómez. *Optimización de sistemas de detección de intrusos en red utilizando técnicas computacionales avanzadas*. Universidad Almería, 2009.
[64] RUIZ HOUSEHOLDER, Adrián; CANDIL VIZCAÍNO, Daniel; SÁNCHEZ-MARISCAL GONZÁLEZ, Guillermo. Detección de intrusos basada en Host (HIDS)-OSSEC. 2020.
[65] MARTINEZ, Guillermo Roberto Solarte; OCAMPO, Carlos Alberto; BERMÚDEZ, Yanci Viviana Castro. Sistema de detección de intrusos en redes corporativas. *Scientia et technica*, 2017, vol. 22, no 1, p. 60-68.

el bloqueo a la dirección IP de origen, las colocaciones más comunes de NIDS son conectándolo directamente a un conmutador que se extiende a un puerto, usando un toque de red, y conectado en línea.

Figura 3 Conexión a Interruptor

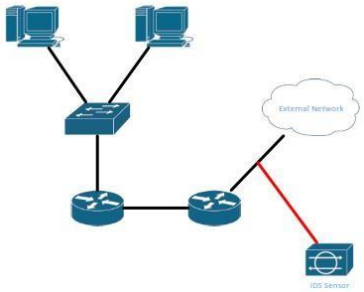


Fuente: **Programa Cisco Packet Tracer (Simulacion)**

La figura 1 muestra el IDS conectado a un interruptor que tiene la capacidad de configuración de puerto SPAN, en algunos switches gestionados, un puerto SPAN se puede configurar para enviar todos los paquetes en la red a ese puerto, así como su destino final [66]. En esta configuración, el conmutador copia todo el tráfico que recibe a la interfaz IDS que se está utilizando para controlar el tráfico, el mayor inconveniente de este método es que se incrementa el ancho de banda y el uso de recursos, ya que el interruptor debe funcionar el doble para entregar el tráfico, muy pocas LAN modernas usan hubs debido a la falta de seguridad. Los hubs permiten a los sistemas interceptar el tráfico no enviado intencionalmente a ellos, cuando se usa un concentrador o un conmutador con capacidades de puerto SPAN, los sistemas en la red interna no están en la IDS que tiene un fallo del sistema que trae la red descendente[67], haciendo uso del cambio del puerto SPAN que es un método común de conexión de sensores.

[66] BAKER, A. R., BEALE, J., CASWELL, B., & POOR, MSnort 2.1 Intrusion Detection. (2004). Second Edition. Rockland, MA: Syngress Publishing, Inc.
[67] PAPPAS, N. SANS Institute InfoSec Reading Room. (April, 2008). Network IDS & IPS deployment strategy [White paper]]

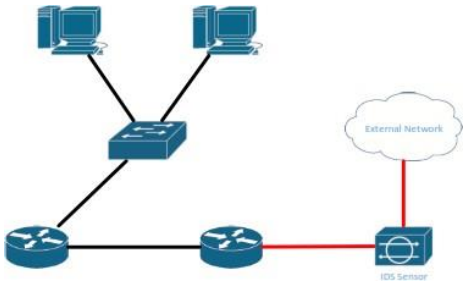
Figura 4. IDS



Fuente **Programa Cisco Packet Tracer (Simulacion)**

La Figura muestra un IDS usando un toque de red, que esencialmente replica datos pasados a través del cable. Los grifos de red no se encuentran comúnmente en redes informáticas típicas, pero se pueden adquirir [68]. Los grifos son útiles cuando una red de un administrador necesita configurar una supervisión apresurada, tal vez para solucionar un problema o implementar temporalmente un IDS "ibed"[69], en general, el toque de red es necesario cuando la red no lo hace, tener switches gestionados, cuando no se está utilizando hubs, o cuando se coloca un IDS en línea no es práctico.

Figura 5. IDS Conectado en Línea



Fuente **Programa Cisco Packet Tracer (Simulacion)**

La figura ilustra un IDS conectado en línea, esta instancia incluye dos conexiones, que se muestran en rojo, con uno conectado al puerto de enlace ascendente del conmutador y el segundo conectado a la red externa, en la mayoría de los casos,

[68] PAPPAS, N. SANS Institute InfoSec Reading Room. (April, 2008). Network IDS & IPS deployment strategy [White paper]]
[69] Ibid

este no es el mejor método para usar porque algún fallo del sistema del IDS evitará que los sistemas en la red interna se comuniquen con los sistemas externos[70] sin embargo esta configuración es una garantía de que todos los paquetes serán vistos por el IDS, los paquetes están sujetos a ser perdidos cuando un IDS está conectado a un puerto SPAN de conmutador, especialmente cuando este interruptor está ocupado o procesando una gran ráfaga de tráfico, el tráfico perdido se puede perder para siempre si no fueron capturados por una red de rastreo o protocolo, dependiendo de la capacidad de un online IDS, una explosión similar puede conducir a la congestión del rendimiento de la red, aunque un NIDS es un poderoso sistema de monitoreo de tráfico de red, hay varias desventajas[71] NIDS las técnicas comunes de evasión como los ataques de fragmentación, el empalme de sesión, e incluso la denegación del servicio (DoS) los ataques se pueden usar para omitir un NIDS, representándolo inútil, si las comunicaciones entre hosts son de cifrado, un NIDS pasivo no tiene la capacidad para desencriptar un mensaje en transición.

5.2.2.5. Detección Basada en Firmas. En el enfoque basado en firmas, un IDS usa paquetes y los compara con reglas predefinidas o patrones conocidos como firmas que se definen en la base de datos, estas firmas de ataque pasan el tráfico específico o una actividad que se basa en actividades intrusivas conocidas[72], la principal ventaja de esta técnica es el procesamiento simple y eficiente de los datos de auditoría, los enfoques basados en firmas tienen una tasa mucho más baja de los falsos positivos, por otro lado, la misma naturaleza de detección basada en la firma significa que el enfoque es ineficaz contra los ataques de día cero, para que no pueda haber un conjunto de reglas o descubrir un método de ataque, estableciendo el ritmo de los nuevos ataques y actividades maliciosas cada hora, el

[70] PAPPAS, N. SANS Institute InfoSec Reading Room. (April, 2008). Network IDS & IPS deployment strategy [White paper]
[71] HAY, A., & CID, D.. OSSEC host-based intrusion detection guide. (2008) Burlington, Mass.: Syngress Pub
[72] GUPTA, M. Hybrid Intrusion Detection System: Technology and Development. (2015). International Journal of Computer Applications IJCA, 5-8

IDS basado en firmas es tan bueno como lo último de su base de datos de firmas y sus conjuntos de reglas.

5.2.2.6. Detección Basada en Anomalías. El IDS basado en anomalías funciona identificando patrones de usuarios o grupos de usuarios ya definido este enfoque busca variaciones y desviaciones de un comportamiento de base establecido lo que podría indicar malicia, implica un aumento en la cantidad de procesamiento que se utiliza por anomalía, detectado para estudiar el comportamiento del sistema desde sus auditorías[73], la línea de base, primero debe ser creado del sistema, red o actividad del programa, esta línea de base es el perfil de lo que un escenario normal usa el ancho de banda o comportamiento, se vería como en un entorno de red específico, a partir de entonces, cualquier actividad que se desvíe de la línea de base se trata como una posible intrusión[74] y se generaría una alerta, la mayor ventaja de la anomalía basada en enfoque es su capacidad para detectar ataques de día cero, ya que no depende de una firma establecida si no de bases de datos o simplemente con desviaciones de una base establecida, el comportamiento de cada sistema de destino o la red es única, por lo tanto basada en anomalías estos enfoques utilizan perfiles personalizados que a su vez hacen que sea difícil para un atacante saber con certeza qué actividad se puede llevar sin establecer una alarma, por otro lado, los IDS basados en anomalías tienen una alta tasa de falsos positivos, también requieren tiempo para establecer un comportamiento de línea de base cuando se coloca por primera vez en un nuevo entorno de red o dispositivo host, los sistemas también son más complejos y la dificultad de asociando a una alarma con el evento específico que activó esta alarma[75]

[73] CANNADY, James, et al. A comparative analysis of current intrusion detection technologies. En *Proceedings of the Fourth Technology for Information Security Conference*. 1996.
[74] GANGWAR, A.; SAHU, S. A survey on anomaly and signature based intrusion detection system (IDS). *Int. Journal of Engineering Research and Applications*, 2014, vol. 4, no 4.
[75] GUPTA, M. Hybrid Intrusion Detection System: Technology and Development. (2015). International Journal of Computer Applications IJCA, 5-8

5.2.2.7. IDS Pasivos y Activos. Al clasificar IDSs, también podemos categorizarlos por la forma en que los IDS responden durante un ataque, un IDS pasivo se limita a los registros, análisis y alertas de un administrador, sobre la posibilidad de un ataque en términos de colocación, los IDS pasivos son generalmente los que se colocan a un lado en una red, un IDS activo puede tomar acciones cuando detecta una posible intrusión, como el bloqueo adicional el tráfico de una fuente de red específica o bloqueo abajo del sistema con modo seguro, en la seguridad moderna de los sistemas, un IDS activo también se conoce como Intrusión Sistema de Prevención (IPS). IPS que se coloca en línea en una red.

5.2.2.8. Sistemas de Prevención de Intrusiones (IPS). La función principal de un IPS es intervenir en casos de sospecha de atentados, en general, un IPS es esencialmente una combinación de dispositivos de control de acceso tales como cortafuegos y enrutadores - e IDSs en otras palabras, un IPS es un IDS con control de acceso con capacidades o métodos de respuesta activa al igual que los IDS, un IPS puede estar basado en host o basado en la red, y utiliza detección basada en anomalías (prevención) o una firma o conjunto de reglas basado en enfoque las siguientes son contramedidas comunes implementado por IPSs:

- Negar el tráfico, este es el más simple, método, donde el sistema de intrusión bloquea las direcciones IP y los puertos involucrados – ambos fuente y destino, la desventaja de esto es el método, es que muchos dispositivos en el global las redes están ocultas detrás de una dirección global, el bloqueo de esa dirección también bloqueará otros tráficos legítimos que pueden estar ubicados detrás esa dirección.

- Registro activo, aunque el registro es una característica compartida por IDSs, un IPS puede aumentar la usabilidad de un registro, por ejemplo, exportando automáticamente los registros de tráfico para cumplir ciertos criterios a la red externa utilizando un software de análisis como el Wireshark.
- Comunicarse con un dispositivo separado con capacidades de control de acceso, modernos como IDSs y IPSs también complementan las operaciones de una LAN mediante la comunicación, con un firewall o enrutador externo, o separado,que tienen capacidades de control de acceso en el evento de una intrusión, un IDS / IPS puede enviar una alerta o solicitud a un cortafuegos o enrutador, el firewall o enrutador tomará las acciones necesarias para hacer frente a la intrusión, como dejar caer los paquetes o bloqueando más tráfico de esa fuente.
- Envío de un reset TCP[76], si el ataque es un ataque basado en TCP, un IPS puede enviar una señal de reinicio al atacante protocolo el cual cerraría la sesión actual, y puede repetirse con frecuencia según sea necesario.
- Configuración de una captura SNMP[77] Cuando se dispara una alarma, el sistema de intrusión enviará una trampa SNMP para indicar a un sistema de gestión SNMP que una red o dispositivo está bajo ataque los sistemas de gestión pueden optar por tomar una acción basada en el evento, como sondeo al agente directamente, o encuestando a otros asociados y el agente de dispositivos para asi obtener una mejor comprensión del evento.

5.2.2.9. IPS O IDS?. “Aunque la tendencia del mercado se centra en IPS en lugar de IDS con el avance de DDoS ataques”[78] hay razones para elegir entre un

[76] CARTER, Michael. *A Review of Transport Protocols as Candidates for use in a Tactical Environment*. DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURG (AUSTRALIA) INFORMATION NETWORKS DIV, 2005.
[77] Burns, D., Adesina, O., & Barker, K. (2012). CCNP Security IPS 642-627 official cert guide. S.l.: Cisco Press.
[78] FUCHSBERGER, A. Sistema de detección de intrusiones y sistemas de prevención de intrusiones. Informe técnico de seguridad de la información 2005 pp 34, 134-139

IPS y un IDS. IDS rara vez causa latencia en el tráfico de la red, ya que generalmente está apagado (a menos que se coloque en línea) y todo el tráfico es simplemente copiado al sensor, un IPS, por otro lado, puede causar pequeños retrasos en el tráfico debido a la colocación en línea esto significa que cada paquete tiene que ser inspeccionado y analizado antes de ser enviado a su destino.

Si un sistema de intrusión está deshabilitado, por ejemplo, por accidente o corte de energía, un IDS no causa denegación de servicio por su posicionamiento, un IPS, que tendría que estar conectado en línea, sería para negar la disponibilidad de los recursos de la red, moderna.

Los IPS tienen mecanismos preventivos como el fallo, la tolerancia o potencia de respaldo para minimizar la interrupción de actividades de la red si el costo es un problema, muchos enrutadores como los routers Cisco® permiten módulos o firmware específicos para ser instalados en la parte superior de los enrutadores existentes para proporcionar capacidades de detección y prevención de intrusos.

5.2.3. Técnicas de Detección. A partir de diferentes fuentes, sistemas como el basado en reglas, sistemas expertos, análisis de transición de estado, y los algoritmos genéticos son formas directas y eficientes de implementar la detección de firmas, secuencial inductiva patrones, redes neuronales artificiales, análisis estadístico. y métodos de minería de datos se han utilizado en la anomalía y detección, hay diferentes tipos de marcos se utiliza para la detección basada en anomalías, esta sección presenta un extenso estudio sobre las diversas técnicas clasificadoras de detección de intrusiones y técnicas de detección híbrida algunos propuestos los métodos podrían ser descritos como sigue.

5.2.3.1. Redes Bayesianas. Las redes bayesianas son probabilísticos modelos gráficos que representan conjuntos de variables y sus probabilísticas independencias de la teoría bayesiana esta nombrada así por su desarrollador Thomas Bayes esta teoría puede ser explicada de la siguiente manera:

Si los eventos A1, A 2, ... y A constituir una partición del espacio muestral S tal que P (A k) ≠ 0 para k = 1,2, n, luego para cualquier evento B tal que P (B) ≠0:

Figura 6. Formula Teoría Bayesiana

$$P(A_i \backslash B) = \frac{P(A_i \cap B}{P(B)} = \frac{P(A_i)P(B\backslash A_i)}{\sum_{k=1}^{n} P(A_k)P(B\backslash A_k} = \frac{P(A_i)P(B\backslash A_i}{P(B)}$$

Fuente: **DARWICHE, Adnan. Bayesian networks. Communications of the ACM, 2010, vol. 53, no 12, p. 80-90**

Darwiche [79], estipuló que las redes bayesianas se han utilizado en muchos equipos como campos de la ciencia, tales como filtros de correo no deseado, voz, reconocimiento y reconocimiento de patrones, debido a su capacidad de construir resultados coherentes mediante el uso probabilístico esta información específica de las redes bayesianas son dirigidas acíclicas, lo gráficos donde los nodos se representan, las variables y cuyos bordes codifican dependencias condicionales entre esas variables[80] estos se aplican a la detección de anomalías de tantas formas; por ejemplo ha desarrollado un sistema de detección de anomalías,[81] , que emplea Bayes, que es una red bayesiana de dos capas que asume total independencia entre los nodos.

5.2.3.2. Algoritmo Genético (GA). Es una técnica de búsqueda que se utiliza para encontrar una solución adecuada para buscar problemas genéticos se han aplicado algoritmos en la detección de anomalías de muchas maneras, ya que son flexibles y una poderosa búsqueda el método de detección de intrusión en la red los

[79] DARWICHE, Adnan. Bayesian networks. *Communications of the ACM*, 2010, vol. 53, no 12, p. 80-90.
[80] HECKERMAN, David. A tutorial on learning with bayesian networks. Microsoft Research. 1995.
[81] JAVITZ, Harold S., et al. The SRI IDES Statistical Anomaly Detector. En *IEEE Symposium on Security and Privacy*. 1991. p. 316-326.

enfoques han utilizado algoritmos genéticos para la clasificación de instancias, mientras que a otros les gusta un borroso enfoque de minería de datos se ha aplicado esta técnica para la selección de características para enumerar una ventaja de GA, se selecciona la mejor característica y así tener mejor eficiencia pero su método es un poco complejo.

5.2.3.3. Algoritmos de Generación de Reglas Inductivos. Estos algoritmos son una de las más famosas técnicas utilizadas[82], en esta técnica; tenemos un modelo de árbol de decisión predictivo que mapea las observaciones. de un artículo, el árbol de decisión (DT) es muy poderoso y el Algoritmo de minería de datos popular para la toma de decisiones y problemas de clasificación, también se usa en muchas aplicaciones de la vida real como diagnóstico médico, radares. clasificación de señales, predicción del tiempo, aprobación de crédito y detección de fraudes.

Este árbol de decisión puede ser construido a partir de un gran volumen de datos con muchos atributos, porque el tamaño del árbol es independiente del tamaño del conjunto de datos, se puede procesar tanto de manera numérica como de datos categóricos, los árboles creados a partir de números y los conjuntos de datos pueden ser complejos en su construcción de inductivos, los algoritmos de generación de reglas pueden no requerir ningún conocimiento del dominio y pueden manejar alta dimensionalidad, los datos y la representación son fáciles de entender[83] de todos modos, eso está limitado a un atributo de salida de árbol de decisión, los algoritmos son inestables y la mayoría de los árboles de decisión y los métodos de construcción no son retrógrados.

[82] JIMÉNEZ, Gonzalo Ramos; MUÑOZ, Javier López. ALGORITMO DE APRENDIZAJE INDUCTIVO BORROSO.

[83] PATEL, R. THAKKAR A AND. GANATRA; A. A Survey and Comparative Analysis of Data Mining Techniques for Network Intrusion Detection Systems, International Journal of Soft Computing and Engineering (2012).

5.2.3.4. Detección de Valores Atípicos. Enfoque de detección de valores atípicos se basa en la idea de aprendizaje semi-supervisado en el que el sistema aprendería una base de datos, y consideraría cualquier instancia que no encaje en el perfil de datos normal como una anomalía la mayoría de los algoritmos de detección de anomalías requieren un conjunto de datos de referencia para enfrentar el modelo y asumen que las anomalías pueden ser tratadas como patrones, nunca observados antes dado que un valor atípico se define como punto de datos que es muy diferente del resto de los datos, por lo tanto, en cierta medida, empleamos varios esquemas de detección de valores atípicos para ver qué tan eficientemente funciona, los esquemas pueden tratar los problemas de anomalía de detección en la detección de valores atípicos basados en estadísticas, las técnicas, los puntos de datos se modelan utilizando un distribución estocástica y estos puntos son determinados a ser atípicos en función de su relación con este modelo.

5.2.3.5. Agrupamiento. Esta técnica se basa en dos importantes supuestos[84], primero, la mayoría de las conexiones de red representan tráfico normal y solo un muy pequeño porcentaje de ese tráfico es malicioso y segundo el tráfico malicioso es estadísticamente diferente de lo normal del tráfico, se detectarán anomalías en función de su tamaño del grupo, es decir, los grupos grandes están destinados a ser datos de referencia, y el resto corresponden a maliciosos, los ataques y la agrupación es el aprendizaje no supervisado y se etiquetan los datos y los patrones naturales en los datos se extraen y no requieren el uso de un conjunto de datos etiquetados para la formación.

5.2.3.6. Redes Neuronales. Las redes neuronales son redes de unidades computacionales que implementan conjuntamente complejas funciones de mapeo

[84] PORTNOY, L. ESKIN, E. and STOLFO. S.J. Intrusion detection with unlabeled data using clustering. In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA2001), pages 76–105. Philadelphia, PA, 2001.

en primer lugar, las redes están capacitadas con un conjunto de datos etiquetando las instancias de prueba, son luego alimentadas en la red para ser clasificadas como normales o anómalas, un ejemplo de la red neuronal técnica ampliamente utilizada en la detección de anomalías son las máquinas de vectores de soporte (SVM) [85]

Este método sería efectivo si las características del ataque ya son conocidas sin embargo, estas intrusiones están cambiando constantemente debido a los enfoques individuales tomadas por los atacantes y los cambios regulares realizados en el software y hardware de los sistemas de destino debido a la gran variedad de ataques y atacantes a pesar de su esfuerzo dedicado a actualizar constantemente la base de reglas de un sistema, nunca puede esperar con precisión Identificar la variedad de intrusiones por estas naturalezas en constante cambio en estos ataques de red. Requerimos una defensiva flexible del sistema que puede analizar estas enormes cantidades de tráfico de red de una manera, que es menos estructurada que los sistemas basados en reglas por ejemplo, un neuronal, el sistema de detección de firmas basado en la red podría potencialmente abordar muchos de los problemas que son encontrados en sistemas basados en reglas, la velocidad inherente de las redes neuronales son otro beneficio de este enfoque, ya que requiere una identificación oportuna de los ataques y la velocidad de procesamiento de las redes neuronales podría permitir respuestas de intrusión que se llevarán a cabo antes o se podría causar daño irreversible al sistema, esto tiene una alta relación señal-ruido y requiere más tiempo y más fase de entrenamiento de la muestra.

5.2.3.7. Lógica Difusa. La lógica difusa se inicia y se basa en un conjunto de reglas del lenguaje humano proporcionadas por el usuario los sistemas convierten estas reglas en su matemática equivalentes esto simplifica el trabajo del sistema diseñador y el equipo los resultados son una gran representación más precisa en la

[85] MUKKAMALA, S., JANOSKI, G., AND SUNG, A.. Intrusion detection using neural networks and support vector machines. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), volume 2, 2002

forma en que los sistemas se comportan en el mundo, la lógica difusa también es simple y flexible puede manejar problemas derivados de datos imprecisos e incompletos, y modelo no lineal de funciones de las complejidades arbitrarias, en la lógica difusa se han empleado técnicas en el campo de la seguridad desde principios de los 90[86] la capacidad de modelar sistemas complejos lo hace válido.

La alternativa en el campo de la seguridad informática para analizar fuentes continuas de datos e incluso procesos desconocidos o procesos imprecisos "[87]." la lógica difusa tiene el potencial en la intrusión del campo de detección en comparación con los sistemas que utilizan firma estricta basada en la coincidencia o patrón clásico, la detección de desviaciones puentes y estado de Vaughn [88] dice que el concepto de seguridad en sí mismo es confuso y en otras palabras, el concepto de borrosidad ayuda a suavizar la abrupta separación del comportamiento normal del comportamiento anormal, esto significa un punto de datos por fuera de un intervalo de referencia definido, esto será considerado anómalo al mismo grado de independiente de su distancia del intervalo, la lógica difusa tiene una capacidad para representar formas imprecisas de razonamiento en áreas donde se deben tomar decisiones firmes en entornos indefinidos como la detección de intrusiones. Dokas [89]sugirió un modelo que trabaja construyendo modelos de predicción de clases raras para identificar intrusiones conocidas y sus variaciones al igual que esquemas de detección de anomalías / valores atípicos para la detección y novedosos ataques cuya naturaleza es desconocida, los investigadores proponen técnicas para generar clasificadores difusos utilizando algoritmos genéticos que pueden detectar anomalías y algunas intrusiones específicas la idea principal era

[86] HOSMER, H. Security is fuzzy: applying the fuzzy logic paradigm to the multipolicy paradigm (1993). Proceedings of 1992-1993 Workshop on New Security Paradigms, 175-184, Little Compton
[87] Ibid
[88] BRIDGES, Susan M., et al. Fuzzy data mining and genetic algorithms applied to intrusion detection. En *Proceedings of 12th Annual Canadian Information Technology Security Symposium*. 2000. p. 109-122.
[89] DOKAS, Paul, et al. Data mining for network intrusion detection. En *Proc. NSF Workshop on Next Generation Data Mining*. 2002. p. 21-30.

evolucionar dos reglas; una para lo clase normal y otra para la clase anormal usando un conjunto de datos de perfil de línea de base.

5.3. FASE 3 DETERMINAR LAS HERRAMIENTAS PARA EL ANÁLISIS, CONTROL Y REGULACIÓN DEL TRÁFICO DE LA RED

5.3.1. Redes Seguras. Para mantener una red segura se parte de la estructuración de aspectos y remisas que favorezca esta condición, es necesario tener en cuenta los siguiente:

5.3.1.1. Instalar y Mantener una Configuración de firewall para proteger los datos del usuario.

Los cortafuegos son dispositivos informáticos que controlan el tráfico informático permitido dentro y fuera de la red de una empresa, así como el tráfico hacia áreas más sensibles dentro la red interna de una empresa.

Un firewall examina todo tráfico de red y bloquea esas transmisiones que no cumple con los criterios de seguridad especificados.

Todos los sistemas deben estar protegidos contra el acceso no autorizado desde Internet, ya sea que ingresen al sistema como comercio electrónico, acceso basado en Internet de los empleados a través de navegadores de escritorio o correo electrónico de los empleados acceso, a menudo, caminos aparentemente insignificantes hacia y desde Internet puede proporcionar vías desprotegidas en sistemas clave, los firewalls son un mecanismo de protección clave para cualquier red de computadoras.

5.3.1.2. Establecer Soporte de Configuración de Firewall ARDS (Automatic Recovery of Database Structure). El soporte de configuración de firewall[90] hace necesario que se cuente con un proceso formal para aprobar y probar todas las conexiones y cambios de red externa a la configuración del firewall, para este propósito es necesario que se establezca un diagrama de red actual con todas las conexiones a los datos del titular de la tarjeta, incluida cualquier conexión inalámbrica.

Los cortafuegos deben presentar características diferenciadoras que permitan identificar cada conexión a Internet y entre cualquier zona desmilitarizada (DMZ) y la zona de red interna.

Describir los grupos, roles y responsabilidades, entidades para la gestión lógica de la red, componentes.

Lista documentada de servicios y puertos necesarios para los negocios.

Justificación y documentación para cualquier protocolo disponible además de la transferencia de hipertexto protocolo (HTTP) y capa de sockets seguros (SSL), shell seguro (SSH) y virtual privado red (VPN).

Justificación y documentación, para cualquier protocolo arriesgado permitido (por ejemplo, transferencia de archivos protocolo (FTP), que incluye razones para uso de protocolo y funciones de seguridad implementado.

Revisión trimestral de conjuntos de reglas de firewall y enrutador.

[90] CHESWICK, William Roberts; WHITTEN, Edward G. *Firewall security method and apparatus*. U.S. Patent Application No 09/047,207, 6 Feb. 2001.

Estándares de configuración para enrutadores.

Crear una configuración de firewall que niega todo el tráfico de redes y hosts "no confiables", excepto protocolos necesarios para el entorno de datos del titular de la tarjeta.

Crear una configuración de firewall[91] que restrinja conexiones entre servidores de acceso público y cualquier almacenamiento de componentes del sistema datos del titular de la tarjeta, incluidas las conexiones inalámbricas y redes esta configuración de firewall debe incluir lo siguiente:

Restricción del tráfico entrante de Internet a Internet y direcciones de protocolo de red (IP) dentro de la DMZ (filtros de ingreso).

No permitir que las direcciones internas pass de Internet a la DMZ.

Implementación de inspección con estado, también conocida como filtrado dinámico de paquetes (es decir, solo las conexiones "establecidas" están permitidas en la red).
Colocación de la base de datos en una zona de red interna, segregada de la DMZ.

Restringir el tráfico entrante y saliente al que sea necesario para el titular de la tarjeta entorno de datos.

Asegurar y sincronizar los archivos de configuración del enrutador, por ejemplo, ejecutando la configuración de archivos para el funcionamiento normal de la ruta de las especificaciones de los requisitos del sistema- ERS y configuración de inicio,

[91] LYU, Michael R.; LAU, Lorrien KY. Firewall security: Policies, testing and performance evaluation. En *Proceedings 24th Annual International Computer Software and Applications Conference. COMPSAC2000*. IEEE, 2000. p. 116-121.

archivos (cuando las máquinas se reinician) deben tener la misma configuración segura.

Estándar de seguridad de datos de la industria de tarjetas de pago (PCI)

Negar todo el tráfico entrante y saliente no permitido específicamente

Instalación de firewalls perimetrales entre cualquier red inalámbrica y los datos del titular de la tarjeta, entorno y configuración de estos firewalls para negar cualquier tráfico de la red inalámbrica, entorno o de controlar cualquier tráfico (si dicho tráfico es necesario para los propósitos)

Instalación de software de firewall personal en cualquier computador móvil y propiedad de los empleados con conectividad directa a Internet (por ejemplo, computadores portátiles utilizados por los empleados), que son utilizados para acceder a la red de la entidad.

Prohibir el acceso público directo entre redes externas cualquier sistema o componente que almacene datos del titular de la tarjeta (por ejemplo, bases de datos, registros, archivos de rastreo).

Implemente una DMZ[92] para filtrar todo el tráfico y prohibir rutas directas de entrada y tráfico saliente de Internet

Restringir el tráfico saliente desde las aplicaciones de tarjetas de pago a las direcciones IP dentro de la DMZ.

Implementar enmascaramiento de IP para evitar direcciones finales de ser traducidas y reveladas en Internet, usar tecnologías que implementen espacios de

[92] ISKANDAR, Akbar; VIRMA, Elisabet; AHMAR, Ansari Saleh. Implementing DMZ in improving network security of web testing in STMIK AKBA. *arXiv preprint arXiv:1901.04081*, 2019.

direcciones, como la dirección del puerto traducción (PAT) o traducción de direcciones de red (NAT).

5.3.2. Herramientas de software para tener una red segura. La red es un término extenso en el mundo de la tecnología, la red se conoce como la columna vertebral del sistema de telecomunicaciones que se utiliza para compartir datos y recursos mediante el enlace de datos.

El siguiente término que entra en el marco es Seguridad de red, la seguridad de la red consiste en un conjunto de reglas, políticas e instrucciones que se aceptan para monitorear y prevenir el uso indebido y la manipulación no autorizada de una red.

El escaneo de la red trata con la Seguridad de la red y esta es una actividad que identifica las vulnerabilidades de esta y las lagunas para proteger su red de comportamientos no deseados e inusuales que pueden dañar el sistema, puede dañar incluso la información personal y la confidencialidad.

5.3.2.1. ¿Qué es el Escaneo en Red? El escaneo en red[93] es un proceso que se puede definir de muchas maneras, identifica los hosts activos (clientes y servidores) en una red y sus actividades para atacar una red. Los atacantes también lo están utilizando para hackear el sistema.

Este procedimiento se utiliza para el mantenimiento del sistema y la evaluación de seguridad de una red. En resumen, el proceso de escaneo en red incluye:

- Identificar sistemas de filtrado entre dos hosts activos en una red.
- Ejecución de servicios de red UDP y TCP.
- Detecta el número de secuencia TCP de ambos hosts.

La exploración de red también se refiere a la exploración de puertos en la que los paquetes de datos se envían a un número de puerto especificado.

[93] TESAVIS, Carl; BERNSTEIN, Lawrence; OLIVER, James. *Network scanner interface*. U.S. Patent Application No 10/834,452, 3 Nov. 2005.

5.3.2.2. Establecer los Puntos de Control de Acceso a La Red. Se debe determinar cómo integrar el nivel correcto de acceso seguro a las personas que lo necesitan. Si la red ha utilizado con éxito el mismo sistema de control de acceso durante años, se debe considerar implementar un sistema o ha habido un evento (por ejemplo, fusión, ubicación o incidente de seguridad) que justifica un cambio, ahora es el momento adecuado para evaluar el control de acceso al sistema y procedimientos, y si no tiene ninguno, se debe considerar incluirlo en su plan de seguridad.

Se debe mantener seguros los activos al tener un plan y tecnología para proporcionar acceso seguro a las personas adecuadas en las áreas correctas de la empresa.

5.3.2.3. Integración de Control de Acceso.Es importante comprender que el control de acceso es una parte de un plan de seguridad completo agrupando los sistemas y operaciones de seguridad complementarios y capacitación para los trabajadores[94].

No importa en qué parte de su plan o sistema se encuentre, hay seis cosas clave para tener en cuenta cuando se busca fortalecer el sistema de control de acceso.

- Las características de su sistema de control de acceso

¿Qué se necesita en el sistema de control de acceso? ¿Qué configuración actual se tiene? Muchos administradores de las redes cambiarán la apariencia de un sistema y la información, pero realmente no profundizarán en las características específicas que enfrentan los desafíos cotidianos que se enfrentan.

[94] PULIDO VELANDIA, Giovanni Andrés. Sistema de control de acceso para la administración y seguridad de equipos de red. 2016.

Para ello es necesario que se simplifique el control de acceso con teléfonos inteligentes, no solo elija un sistema basado en su aspecto, sino en las características que tiene, Al elegir un sistema de control de acceso, considere:

- Las áreas donde se necesita un sistema
- Veces que se utilizará para obtener acceso
- ¿Cuántas personas tendrán niveles de acceso separados?
- Cómo encaja en cualquier otro componente que ya tenga instalado

El acceso se trata de conveniencia. Más seguro no es conveniente, se quiere fomentar un entorno para autenticar el acceso a la red y dejar ingresar a las personas adecuadas en los momentos adecuados.

5.3.2.4. Determinar los niveles de acceso. No todos necesitan acceso a toda la red de la empresa, antes de decidir quién debe tener acceso, miramos la empresa, los trabajadores de esta en sí para determinar qué áreas necesitan diferentes niveles de acceso[95].

Se debe tener mapa de la red desglosarlo haciendo que ciertas zonas tengan diferentes colores según el nivel de acceso o seguridad que se necesite, a partir de ahí, se decide a qué nivel de acceso requerirá y si existen restricciones de tiempo o fecha para ciertos participantes o trabajadores.

El constante monitoreo del ingreso de los empleados no significa un espionaje ni una intromisión en la privacidad de estas, puesto que se define la actividad laboral como un punto apartado, ya que está en riesgo la fuga de la información y el normal desarrollo de una entidad

[95] VARGAS, IGNACIO ALVAREZ; SIEMENS, S. Seguridad en Redes Industriales. 2013.

Al configurar un sistema de control de acceso, debe asegurarse que todos tengan el nivel de acceso adecuado para sus necesidades, es importante tener un proceso y un protocolo establecido.

La determinación del nivel correcto de acceso para diferentes partes de la red y los empleados depende de los gerentes de las instalaciones y los supervisores de los empleados.

La validación por medio antropométrico o con claves es una alternativa eficaz para los casos de ingreso a una red con lo que se valida y se controla el uso de esta.
También alienta a automatizar el proceso conectando el sistema de control de acceso a una base de datos de recursos humanos de terceros para que cuando el empleado renuncie o sea despedido, el acceso sea revocado simultáneamente.

5.3.2.5. Principales Herramientas de Escaneo en Red (IP y escáner de red).Las mejores herramientas de escáner de red que se utilizan ampliamente para detectar vulnerabilidades de red y que son condigo libre se enuncian a continuación Acunetix, OpenVAS, Wireshark, Nikto, Angry IP Scanner, Advanced IP Scanner, Qualys Frescan, SoftPerfect Network Scanner, Retina Network Security Scanner, Nmap, Nessus, Metasploit Framework, Snort, Open SSH, Nexpose, MyLanVlewer Network/IP Scanner.

Acunetix incluye una herramienta de escaneo de red totalmente automatizada que detecta e informa sobre más de 50,000 vulnerabilidades y configuraciones incorrectas de red conocidas.
Descubre puertos abiertos y servicios en ejecución; evalúa la seguridad de enrutadores, firewalls, conmutadores y equilibradores de carga; prueba contraseñas débiles, transferencia de zona DNS, servidores proxy mal configurados, cadenas de comunidad SNMP débiles y cifrados TLS / SSL, entre otros. Se integra con Acunetix

Online para proporcionar una auditoría integral de seguridad de la red perimetral además de la auditoría de la aplicación web Acunetix.

- *Escanear servicios de red perimetral*

Las redes perimetrales inseguras siguen siendo la causa de la mayoría de las infracciones de datos y una de las áreas más importantes de la red para proteger contra vulnerabilidades, configuración incorrecta y otras amenazas que podrían comprometer la seguridad o la disponibilidad de los servicios de red.

- *Prueba de vulnerabilidades de red*

Acunetix escanea la red en busca de vulnerabilidades y presenta resultados dentro del panel, desde donde se puede generar fácilmente un informe de seguridad de la red.

Evalúa la seguridad de enrutadores, firewalls, conmutadores y equilibradores de carga, pruebas de contraseñas débiles en FTP, IMAP, servidores de bases de datos, POP3, Socks, SSH y Telnet, pruebas para transferencia de zona DNS, DNS recursivo abierto y ataques de envenenamiento de caché DNS

Detecta configuraciones incorrectas de seguridad de red

Este software puede detectar una amplia gama de configuraciones incorrectas de seguridad de la red que podrían conducir a la divulgación de datos confidenciales, la denegación de servicio o incluso el compromiso de los hosts, realizando pruebas para:

- Acceso FTP anónimo y directorios grabables a través de FTP
- Servidores proxy mal configurados
- Cadenas de comunidad SNMP débiles
- Cifrados TLS / SSL débiles

- *Control de acceso a la red (NAC)*

El Control de acceso a la red o NAC controla qué personas puedan acceder a su red y cuáles no le permite identificar diferentes usuarios y dispositivos, y descubrir si personal no autorizado está tratando de obtener acceso a la red, por lo tanto, puede aplicar diferentes políticas de seguridad para bloquear dispositivos y controlar lo que puede suceder en su red.

También puede configurar herramientas de análisis de comportamiento, que lo ayudan a identificar comportamientos anormales en su red, de modo que reciba una notificación cuando alguien actúe de manera anormal en su red.

- *Seguridad de la aplicación*

También puede aprovechar la seguridad de las aplicaciones, que está diseñada para ofrecer una protección completa a estas, es importante, garantizar que las aplicaciones con fallas en ellas no sean atacadas y aprovechadas por los piratas informáticos. Básicamente protege su red de la amenaza y que sus aplicaciones sean pirateadas, por lo que definitivamente es una herramienta de seguridad de red esencial que debe tener.

- *Software Antivirus y Antimalware*

Definitivamente debe usar software antivirus y antimalware para proteger su red de spyware, phishing, troyanos y virus. El programa maligno es como una enfermedad para su red, y no solo permanecerá dentro de su red, sino que provocará ataques y provocará un mal funcionamiento de sus sistemas.

El software antivirus y antimalware le permite detectar fácilmente programa maligno y otras amenazas de virus, ya que explorarán continuamente la red en busca de programa maligno oculto.

5.3.2.6. Seguridad del Correo Electrónico. Es importante que también se le dé importancia a la seguridad del correo electrónico, especialmente si se tiene un negocio que utiliza muchos correos electrónicos. Los ataques de suplantación de identidad (phishing) pueden comprometer gravemente sus operaciones comerciales, por lo que es imprescindible invertir en seguridad de correos electrónicos de última generación.

Si los piratas informáticos pueden obtener información personal o financiera, pueden recurrir al chantaje y también comenzarán a engañar a sus clientes robando su información personal y enviándoles programa maligno. Es por eso por lo que la seguridad del correo electrónico debe ser una prioridad para todas las empresas que se ejecutan hoy.

5.3.2.7. Seguridad Inalámbrica. Otro tipo de seguridad de red en el que se debe invertir es la seguridad inalámbrica, las empresas realizan más negocios en la nube, y esto significa redes inalámbricas y puntos de acceso, el gran problema aquí es que las redes inalámbricas no son muy seguras y pueden ser atacadas fácilmente por piratas informáticos, con lo que su seguridad inalámbrica debe ser de primera categoría.

5.3.2.8. La Importancia de la Seguridad de la Red. Las organizaciones y las empresas de hoy necesitan comprender la importancia de la seguridad de la red, no importa si se trata de una organización gubernamental, una pequeña empresa o una multinacional, la seguridad de la red debe tener el mismo nivel de importancia para ellos, una brecha en la seguridad de la red puede resultar en todo tipo de daños irreparables, razón por la cual las organizaciones necesitan ser educadas sobre la importancia de la seguridad de la red, por qué deberían protegerla.

Las organizaciones necesitan actualizar sus sistemas regularmente, especialmente porque los piratas informáticos están descubriendo nuevas fallas en las redes de

seguridad y están presentando nuevos métodos para obtener acceso a redes no autorizadas.

5.3.2.9. Enfoque de Seguridad. Si tiene la tarea de administrar la seguridad de la red de su organización, hay ciertas acciones en las que debe centrarse, las que se describen a continuación:

- Determinar: Educar a las personas y disuadirlas de entrar en redes por razones maliciosas o ilegales.
- Prevenir: Hay que presentar nuevas medidas para garantizar la prevención del acceso no autorizado a las redes, se puede hacer creando un acceso especial, actualizando los sistemas de seguridad y encriptando la comunicación.
- Detectar: Aprenda a reconocer las brechas de seguridad y mantenga un registro de todas las personas que tienen acceso a la red.
- Corregir: Implemente nuevas soluciones en el diseño de una seguridad de red después de descubrir fallas. Intente corregir las violaciones de seguridad anteriores implementando nuevas medidas para evitar que eso vuelva a suceder.

5.3.2.10. Ataques de Seguridad. Realmente necesita vigilar los ataques de seguridad, ya que existen diferentes tipos de ataques que pueden ocurrir en la red de sus equipos, los piratas informáticos y los ciberdelincuentes saben exactamente cómo conectar determinados tipos de red, por lo que también debe saber sobre el tipo de ataques de seguridad que existen. Su red informática puede ser vulnerable a los siguientes ataques de seguridad:

- Interrupción

Un ataque de interrupción apunta a la disponibilidad de un DOS o un ataque de denegación de servicio, el objetivo principal de este tipo de ataque es garantizar que los servicios no estén disponibles.

- Intercepción

Este ataque se basa en obtener acceso no autorizado a una red, se puede poner en práctica mediante la adquisición de información valiosa o sensible.

- Modificación

Un ataque de modificación se basa en la manipulación de recursos, y generalmente cambiará la información que se comunica entre las partes, podría estar enviando información incorrecta a una de las partes para causar una falta de comunicación.

- Fabricación

El ataque de fabricación se conoce comúnmente como falsificación, y generalmente se usa para evitar las pruebas de autenticidad, personificando información o imitando, este ataque toma nueva información y los registra en un archivo, y se utiliza principalmente para acceder a un servicio o datos.

Estos son los principales tipos de ataques de seguridad que pueden comprometer la seguridad de la red, los principales tipos de ataques a los que la red será vulnerable son los ataques pasivos y los ataques activos, es importante buscar protección contra ambos tipos de ataques para garantizar una seguridad de red excepcional.

5.3.2.11. OpenVAS - Escáner de Evaluación de Vulnerabilidad Abierta. OpenVAS[96] es un escáner de vulnerabilidades con todas las funciones, sus capacidades incluyen pruebas no autenticadas, pruebas autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para escaneos a gran escala y un potente lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad.

[96] AKSU, M. Ugur; ALTUNCU, Enes; BICAKCI, Kemal. A First Look at the Usability of OpenVAS Vulnerability Scanner. En *Workshop on Usable Security (USEC) 2019*. NDSS, 2019.

El escáner se acompaña de un feed de pruebas de vulnerabilidad con un largo historial y actualizaciones diarias, este feed comunitario de Greenbone incluye más de 50,000 pruebas de vulnerabilidad.

El escáner es desarrollado y mantenido por Greenbone Networks desde 2009, los trabajos son aportados como Código Abierto a la comunidad bajo la Licencia Pública General de GNU (GNU GPL).

Greenbone desarrolla OpenVAS como parte de su familia de productos de gestión de vulnerabilidad comercial "Greenbone Security Manager" (GSM). OpenVAS es un elemento en una arquitectura más grande, en combinación con módulos adicionales de código abierto, forma la solución Greenbone Vulnerability Management. En base a esto, los dispositivos GSM utilizan una alimentación más extensa que cubre las necesidades de la empresa, un GVM con características adicionales, administración de dispositivos y un acuerdo de nivel de servicio.

El año 2017 marcó el comienzo de una nueva era: en primer lugar, Greenbone se hizo visible como la fuerza impulsora detrás de OpenVAS, reduciendo la confusión de la marca. esto incluyó varias actividades, la más esencial es el cambio de nombre del "marco OpenVAS" a "Greenbone Vulnerability Management" (GVM), de los cuales OpenVAS Scanner es uno de los muchos módulos, también condujo a "GVM-10" como el sucesor de "OpenVAS-9", no se produjeron cambios de licencia, todos los módulos permanecieron de código abierto.

El segundo gran cambio en 2017 fue sobre el servicio de alimentación, además de la confusión de la marca, varias compañías estaban integrando la tecnología y la alimentación y haciéndola pasar por su trabajo o afirmando ser una alternativa al producto de Greenbone a un mejor precio, solo una minoría de ellos cumplió adecuadamente con las licencias GPL. Ninguno de ellos coopera comercialmente con Greenbone, para lograr una mejor visibilidad, menos malentendidos y una mejor distinción de otros productos basados en OpenVAS, el feed público pasó a llamarse "Greenbone Community Feed" y el desarrollo del feed se internalizó, además, el esquema de lanzamiento cambió de una demora de 14 días a una publicación diaria

sin demora donde ahora ya no se incluyen las pruebas de vulnerabilidad para productos empresariales.
El tercer gran cambio hacia la nueva era fue la transición a una infraestructura moderna, a saber, GitHub y un foro comunitario, toda la transición se completó en 2018 y aumentó la productividad y la actividad comunitaria.

En 2019 se completó la separación de la marca. OpenVAS ahora representa el escáner de vulnerabilidad real como lo hizo originalmente y la "S" en "OpenVAS" ahora significa "Escáner" en lugar de "Sistema". Estos cambios van acompañados de un logotipo actualizado de OpenVAS, el marco donde se integra OpenVAS es la Gestión de Vulnerabilidad de Greenbone (GVM).
OpenVAS lanzado con GVM-10 recibe numerosas optimizaciones de rendimiento para abordar el desafío de un número creciente de pruebas de vulnerabilidad, escaneando redes objetivo de tamaño y heterogeneidad crecientes.
OpenVAS lanzado con GVM-11 introduce cambios arquitectónicos sustanciales: el antiguo servicio "openvassd" se convierte en una herramienta de línea de comandos "OpenVAS". Está controlado por la capa de servicio ospd-openvas, este concepto reemplaza esencialmente el antiguo OTP con estado, permanente y patentado (Protocolo de transferencia OpenVAS) por el nuevo OSP genérico (Protocolo de escáner abierto) sin estado, basado en solicitud y respuesta XML.
Demostración en vivo de Greenbone: la gestión de vulnerabilidad consta de un administrador de seguridad de Greenbone y una serie de sistemas de destino que presentan diversas vulnerabilidades.
Se inicia con un usuario y una contraseña Esta información básica antes de comenzar: La demostración ofrece derechos extendidos y datos de ejemplo para escaneos y otras configuraciones, en comparación con el portal, si se desea escanear activamente, se puede descargar el GCE o solicitar pruebas gratuitas para un dispositivo ilimitado, compartirá el mismo sistema de demostración con otros usuarios, por lo tanto, el rendimiento puede variar según la cantidad de usuarios concurrentes, se ejecuta GSM en una máquina virtual, no en el hardware real del

dispositivo GSM, por lo tanto, la descripción general del rendimiento muestra menos CPU, menos espacio en disco y menos interfaces, ofrece acceso a la interfaz del cliente web, la interfaz de la consola de línea de comandos no es accesible. Cualquier actividad es monitoreada y registrada.

5.3.2.12. Desarrollo de la Aplicación Concerniente al Escaneo y Detección de Elementos de la Red. En el Software de exploración y aplicación Acunetix[97], al efectuar su maniobrabilidad en la red escogida, se efectúa el escaneo total de la red para ver, detectar y corregir las vulnerabilidades de esta, al igual que las características, reflejadas con lo que se encuentra en su proceso, nos envía resultados en tablas de informe del estado.

Nos coloca tableros en los que indica,

- Las tareas por clase de gravedad
- La tarea por estado
- Vulnerabilidades y exposiciones comunes (CVE) por tiempo de creación
- Servicio de terminal virtual de red (NVTs) por clase de gravedad

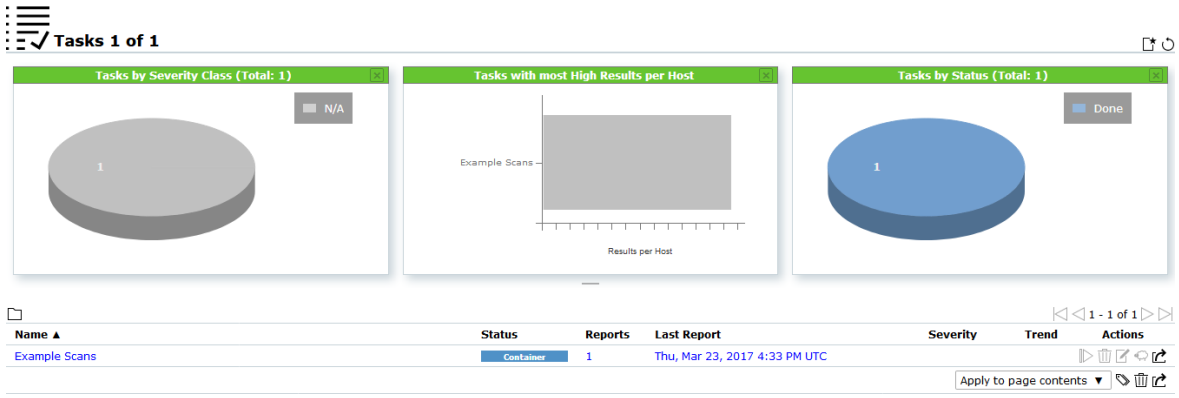
Figura 7. Vulnerabilidades y exposiciones

Fuente: Elaboración Propia

[97] WIRYAWAN, Drajad, et al. Implementation of the Acunetix for Testing the Banking Website (Owned by the government and non-government in Indonesia). *International Information Institute (Tokyo). Information*, 2016, vol. 19, no 6A, p. 1785.

En esta gráfica vemos que la vulnerabilidad del sistema alta es del 33% al igual que la media

Figura 8. Tarea Por Estado



Fuente: Elaboración Propia

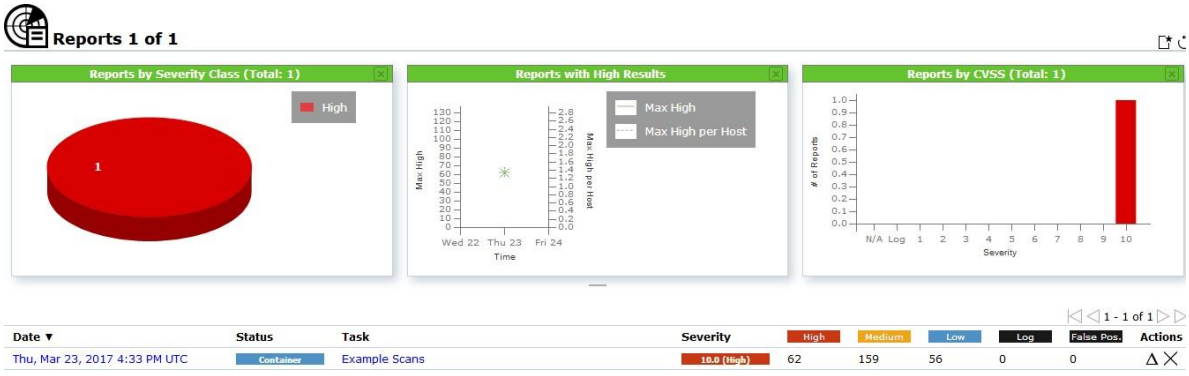
Tarea por clase de gravedad

Tarea con resultados más altos por host

Tarea por estado

Los hosts del sistema presentan una optimo desarrollo, pero igualmente deben ser tratados para no llegar a tener problemas ni riesgos de vulnerabilidades .

Figura 9. Clase de Gravedad



Fuente: Elaboración Propia

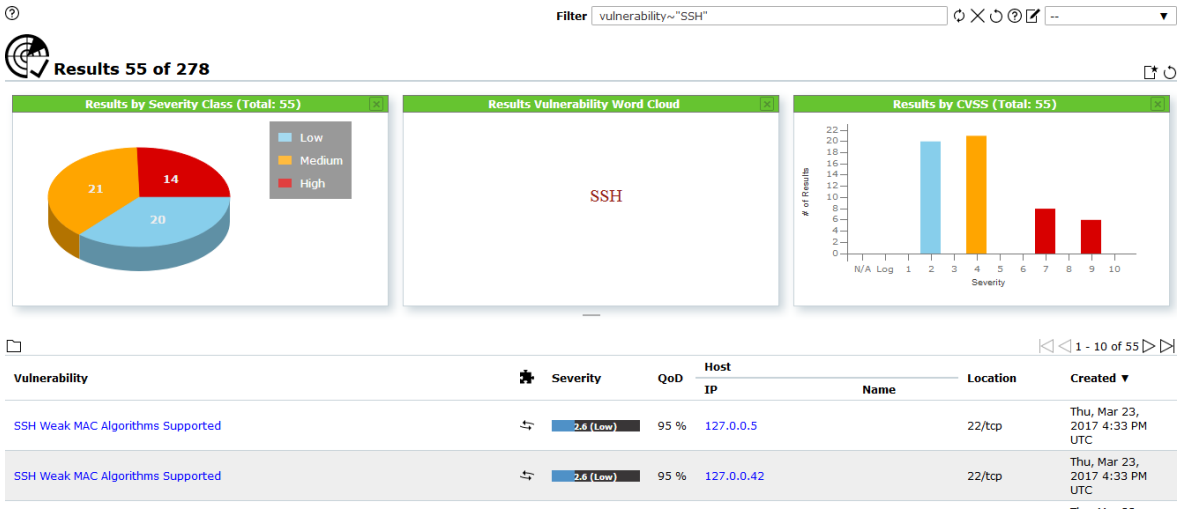
Informes por clase de gravedad

Reportes con altos resultados

Informes de Sistema de puntuación de vulnerabilidad común (CVSS).

Las vulnerabilidades expresadas en esta gráfica son preocupante con lo que se trata, solucionar el problema con planes de contingencia y desarrollo de herramientas para poder contrarrestar los riesgos plasmados

Figura 10. Vulnerabilidad



Fuente: Elaboración Propia

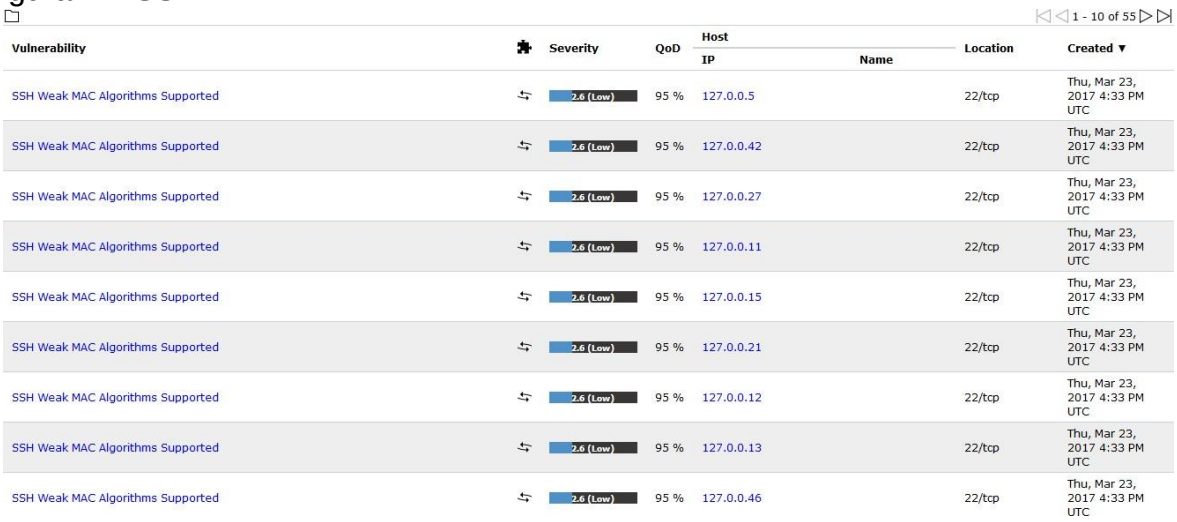
Informes por clase de gravedad

Reportes con altos resultados

Informes de Sistema de puntuación de vulnerabilidad común (CVSS)

Las vulnerabilidades se solucionan implementando pasos específicos que reducen en gran porcentaje los problemas presentados inicialmente.

Figura 11. SSH



1 - 10 of 55

Vulnerability	Severity	QoD	Host IP	Host Name	Location	Created ▼
SSH Weak MAC Algorithms Supported	2.6 (Low)	95 %	127.0.0.5		22/tcp	Thu, Mar 23, 2017 4:33 PM UTC
SSH Weak MAC Algorithms Supported	2.6 (Low)	95 %	127.0.0.42		22/tcp	Thu, Mar 23, 2017 4:33 PM UTC
SSH Weak MAC Algorithms Supported	2.6 (Low)	95 %	127.0.0.27		22/tcp	Thu, Mar 23, 2017 4:33 PM UTC
SSH Weak MAC Algorithms Supported	2.6 (Low)	95 %	127.0.0.11		22/tcp	Thu, Mar 23, 2017 4:33 PM UTC
SSH Weak MAC Algorithms Supported	2.6 (Low)	95 %	127.0.0.15		22/tcp	Thu, Mar 23, 2017 4:33 PM UTC
SSH Weak MAC Algorithms Supported	2.6 (Low)	95 %	127.0.0.21		22/tcp	Thu, Mar 23, 2017 4:33 PM UTC
SSH Weak MAC Algorithms Supported	2.6 (Low)	95 %	127.0.0.12		22/tcp	Thu, Mar 23, 2017 4:33 PM UTC
SSH Weak MAC Algorithms Supported	2.6 (Low)	95 %	127.0.0.13		22/tcp	Thu, Mar 23, 2017 4:33 PM UTC
SSH Weak MAC Algorithms Supported	2.6 (Low)	95 %	127.0.0.46		22/tcp	Thu, Mar 23, 2017 4:33 PM UTC

Fuente: Elaboración Propia

Al desarrollar ssh se puede reducir los porcentajes de riesgos, intimidaciones y vulnerabilidades del sistema

OpenSSH Vulnerabilidades de denegación de servicio y enumeración de usuarios (Windows)

Resumen, este host se instala con openssh y es propenso a la denegación de servicio y vulnerabilidades de enumeración de usuarios.

5.3.2.13. Resultado de Detección.

La vulnerabilidad se detectó de acuerdo con el Método de detección.Visión existen múltiples fallas debido a La función auth_password en el script 'auth-passwd.c' no limita la contraseña longitudes para la autenticación de contraseña.

El sshd en OpenSSH, cuando se utilizan SHA256 o SHA512 para el hash de contraseña de usuario.

usa BLOWFISH hashing en una contraseña estática cuando el nombre de usuario no existe y toma mucho más tiempo calcular el hash SHA256 / SHA512 que el hash BLOWFISH.

Método de detección

Comprueba si hay una versión vulnerable en el host de destino.

Detalles:

Vulnerabilidades de denegación de servicio de OpenSSH y enumeración de usuarios (Ventana ...OID: 1.3.6.1.4.1.25623.1.0.809121

Versión utilizada:

$ Revisión: 5083 $ Software / SO afectado versiones de OpenSSH anteriores a 7.3 en Windows.

Impacto. explotar con éxito este problema permite atacantes remotos para causar una denegación de servicio (consumo de CPU de la cripta) y para enumerar usuarios aprovechando la diferencia de tiempo entre las respuestas cuando se proporciona una contraseña grande.

Solución

Tipo de solución:

Vendorfix

Actualice a OpenSSH versión 7.3 o posterior referencias CVE

CVE-2016-6515CVE-2016-6210

OFERTA92212CERT

CB-K18 / 0041CB-K17 / 2219CB-K17 / 2112CB-K17 / 1753CB-K17 / 1349CB-K17 / 1292CB-K17 / 0055CB-K16 / 1837CB-K16 / 1629CB-K16 / 1487CB-K16 / 1485CB-K16 / 1252CB K16 / 1221CB-K16 / 1082DFN-CERT-2019-1408DFN-CERT-2018-1828DFN-CERT-2018-1070DFN-CERT-2018-0046DFN-CERT-2017-2320DFN-CERT-2017-2208DFN-CERT-2017-1831DFN- CERT-2017-1407DFN-CERT-2017-1340DFN-CERT-2017-0060DFN-CERT-2016-1943DFN-CERT-2016-1729DFN-CERT-2016-1576DFN-CERT-2016-1574DFN-CERT-2016-1331DFN-CERT- 2016-1243DFN-CERT-2016-1149.

Bienes

Figura 12. Topología de Hosts

Fuente: Elaboración Propia

El listado de equipos que tiene la red al igual que la topología de estas siendo de mucho valor esto para la persona que va a ejecutar el análisis del estado de la red.

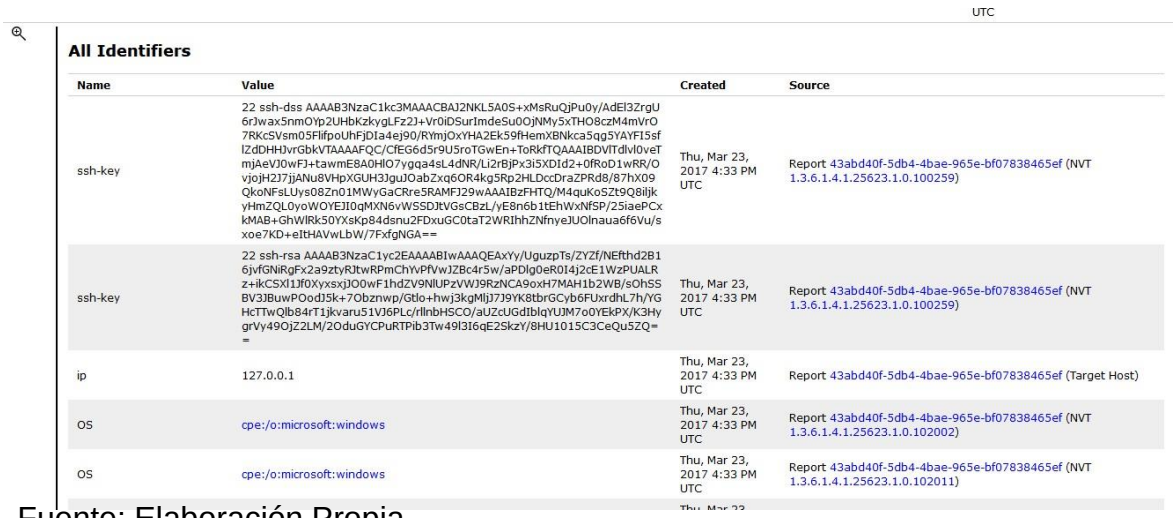
Anfitriones por clase de gravedad total 46

Topología de hosts

hosts por modificación

Llaves y reportes

Figura 13. Llaves



All Identifiers

Name	Value	Created	Source
ssh-key	22 ssh-dss AAAAB3NzaC1kc3MAAACBAJ2NKL5A0S+xMsRuQjPu0y/AdEl3ZrgU 6rJwax5nmOYp2UHbKzkygLFz2J+Vr0iDSurImdeSu0OjNMy5xTHO8czM4mVrO 7RKcSVsm05FlifpoUhFjDIa4ej90/RYmjOxYHA2Ek59fHemXBNkca5qg5YAYFI5sf lZdDHHJvrGbkVTAAAAFQC/CfEG6d5r9U5roTGwEn+ToRkfTQAAAIBDVlTdlvl0veT mjAeVJ0wFJ+tawmE8A0HlO7ygqa4sL4dNR/Li2rBjPx3i5XDId2+0fRoD1wRR/O vjojH2J7jjANu8VHpXGUH3JguJOabZxq6OR4kg5Rp2HLDccDraZPRd8/87hX09 QkoNFsLUys08Zn01MWyGaCRre5RAMFJ29wAAAIBzFHTQ/M4quKo5Zt9Q8iljk yHmZQL0yoWOYEJI0qMXN6vWSSDJtVGsCBzL/yE8n6b1tEhWxNfSP/25iaePCx kMAB+GhWlRk50YXsKp84dsnu2FDxuGC0taT2WRIhhZNfnyeJUOlnaua6f6Vu/s xoe7KD+eItHAVwLbW/7FxfgNGA==	Thu, Mar 23, 2017 4:33 PM UTC	Report 43abd40f-5db4-4bae-965e-bf07838465ef (NVT 1.3.6.1.4.1.25623.1.0.100259)
ssh-key	22 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAxYy/UguzpTs/ZYZf/NEfthd2B1 6jvfGNiRgFx2a9ztyRJtwRPmChYvPfvWJZBc4r5w/aPDlg0eR0I4j2cE1WzPUALR z+ikCSXl1Jf0XyxsxjJO0wF1hdZV9NlUPzVWJ9RzNCA9oxH7MAH1b2WB/sOhSS BV3JBuwPOodJ5k+7Obznwp/Gtlo+hwj3kgMlj7J9YK8tbrGCyb6FUxrdhL7h/YG HcTTwQlb84rT1jkvaru51VJ6PLc/rllnbHSCO/aUZcUGd1blqYUJM7o0YEkPX/K3Hy grVy49OjZ2LM/2OduGYCPuRTPib3Tw49l3I6qE2SkzY/8HU1015C3CeQu5ZQ= =	Thu, Mar 23, 2017 4:33 PM UTC	Report 43abd40f-5db4-4bae-965e-bf07838465ef (NVT 1.3.6.1.4.1.25623.1.0.100259)
ip	127.0.0.1	Thu, Mar 23, 2017 4:33 PM UTC	Report 43abd40f-5db4-4bae-965e-bf07838465ef (Target Host)
OS	cpe:/o:microsoft:windows	Thu, Mar 23, 2017 4:33 PM UTC	Report 43abd40f-5db4-4bae-965e-bf07838465ef (NVT 1.3.6.1.4.1.25623.1.0.102002)
OS	cpe:/o:microsoft:windows	Thu, Mar 23, 2017 4:33 PM UTC	Report 43abd40f-5db4-4bae-965e-bf07838465ef (NVT 1.3.6.1.4.1.25623.1.0.102011)

Fuente: Elaboración Propia

El control de llaves es importante en los archivos para tener la absoluta seguridad de tener la información salvaguardad y de manera encriptada

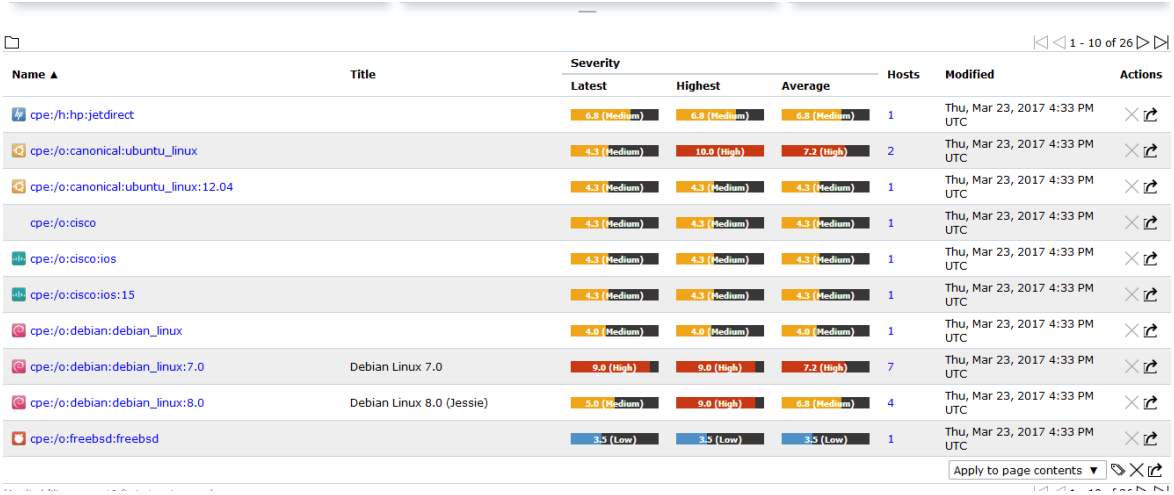
Figura 14 Sistemas Operativos

Fuente: Elaboración Propia

- Sistemas operativos por clase de gravedad
- Sistemas operativos más vulnerables
- Sistemas operativos por CVSS

Listado de los sistemas operativos y sus debidas vulnerabilidades y soluciones

Figura 15. Vulnerabilidad y Soluciones



1 - 10 of 26

Name ▲	Title	Severity			Hosts	Modified	Actions
		Latest	Highest	Average			
cpe:/h:hp:jetdirect		6.8 (Medium)	6.8 (Medium)	6.8 (Medium)	1	Thu, Mar 23, 2017 4:33 PM UTC	
cpe:/o:canonical:ubuntu_linux		4.3 (Medium)	10.0 (High)	7.2 (High)	2	Thu, Mar 23, 2017 4:33 PM UTC	
cpe:/o:canonical:ubuntu_linux:12.04		4.3 (Medium)	4.3 (Medium)	4.3 (Medium)	1	Thu, Mar 23, 2017 4:33 PM UTC	
cpe:/o:cisco		4.3 (Medium)	4.3 (Medium)	4.3 (Medium)	1	Thu, Mar 23, 2017 4:33 PM UTC	
cpe:/o:cisco:ios		4.3 (Medium)	4.3 (Medium)	4.3 (Medium)	1	Thu, Mar 23, 2017 4:33 PM UTC	
cpe:/o:cisco:ios:15		4.3 (Medium)	4.3 (Medium)	4.3 (Medium)	1	Thu, Mar 23, 2017 4:33 PM UTC	
cpe:/o:debian:debian_linux		4.0 (Medium)	4.0 (Medium)	4.0 (Medium)	1	Thu, Mar 23, 2017 4:33 PM UTC	
cpe:/o:debian:debian_linux:7.0	Debian Linux 7.0	9.0 (High)	9.0 (High)	7.2 (High)	7	Thu, Mar 23, 2017 4:33 PM UTC	
cpe:/o:debian:debian_linux:8.0	Debian Linux 8.0 (Jessie)	5.0 (Medium)	9.0 (High)	6.8 (Medium)	4	Thu, Mar 23, 2017 4:33 PM UTC	
cpe:/o:freebsd:freebsd		3.5 (Low)	3.5 (Low)	3.5 (Low)	1	Thu, Mar 23, 2017 4:33 PM UTC	

Apply to page contents ▼

Fuente: Elaboración Propia

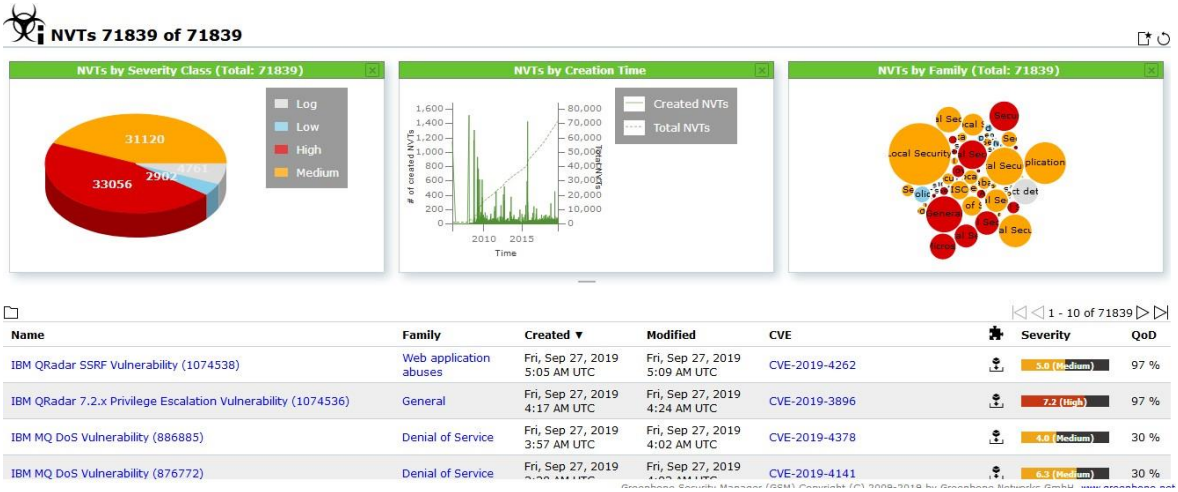
Servicio de terminal virtual de red (NVTs)

Clase de gravedad de NVT

NVT por tiempo de creación

NVT por familia

Figura 16. Gravedad NVT



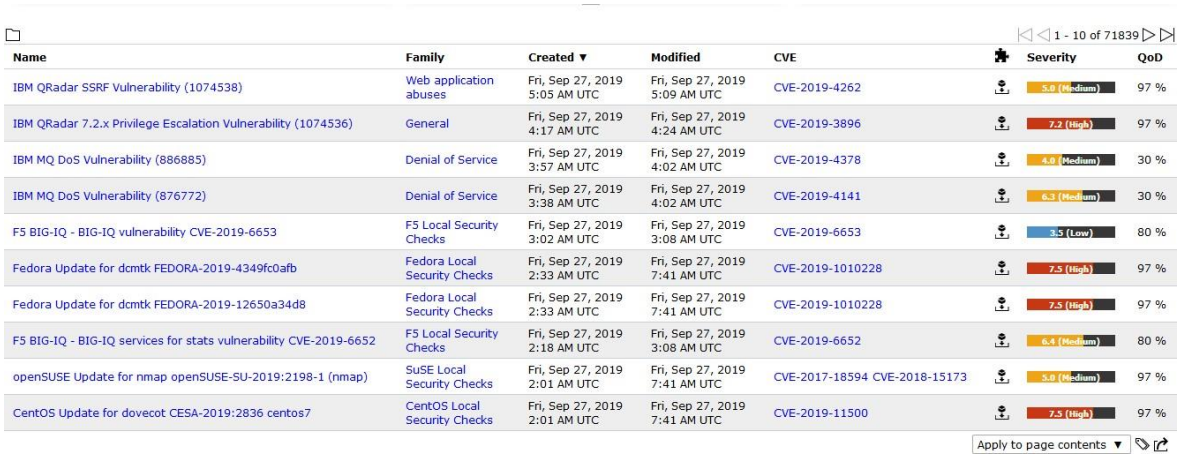
1 - 10 of 71839

Name	Family	Created ▼	Modified	CVE	Severity	QoD
IBM QRadar SSRF Vulnerability (1074538)	Web application abuses	Fri, Sep 27, 2019 5:05 AM UTC	Fri, Sep 27, 2019 5:09 AM UTC	CVE-2019-4262	5.0 (Medium)	97 %
IBM QRadar 7.2.x Privilege Escalation Vulnerability (1074536)	General	Fri, Sep 27, 2019 4:17 AM UTC	Fri, Sep 27, 2019 4:24 AM UTC	CVE-2019-3896	7.2 (High)	97 %
IBM MQ DoS Vulnerability (886885)	Denial of Service	Fri, Sep 27, 2019 3:57 AM UTC	Fri, Sep 27, 2019 4:02 AM UTC	CVE-2019-4378	4.0 (Medium)	30 %
IBM MQ DoS Vulnerability (876772)	Denial of Service	Fri, Sep 27, 2019	Fri, Sep 27, 2019	CVE-2019-4141	6.3 (Medium)	30 %

Fuente: Elaboración Propia

Listado de sistemas operativos con porcentaje de vulnerabilidades

Figura 17. Listado de SO



1 - 10 of 71839

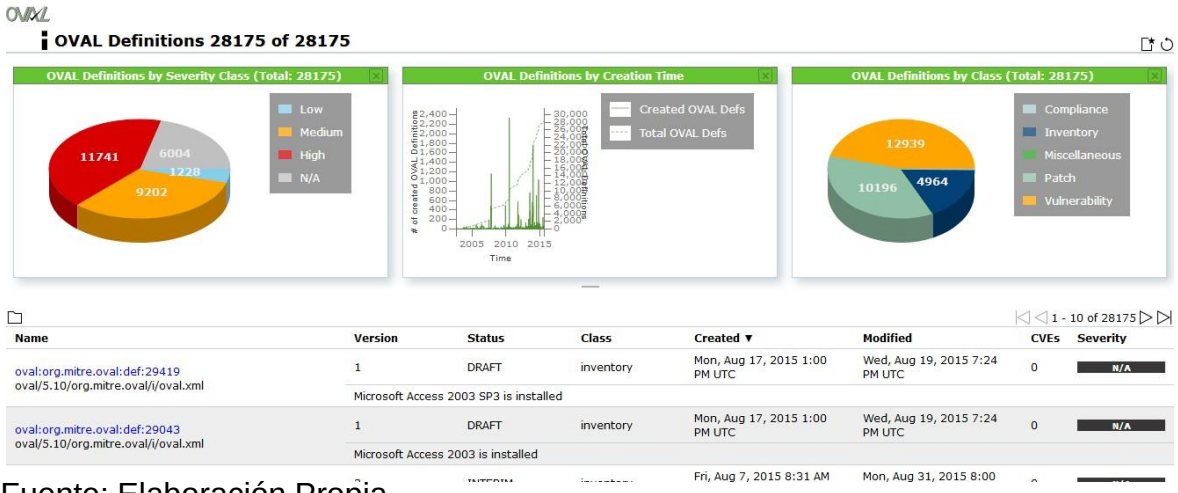
Name	Family	Created ▼	Modified	CVE	Severity	QoD
IBM QRadar SSRF Vulnerability (1074538)	Web application abuses	Fri, Sep 27, 2019 5:05 AM UTC	Fri, Sep 27, 2019 5:09 AM UTC	CVE-2019-4262	5.0 (Medium)	97 %
IBM QRadar 7.2.x Privilege Escalation Vulnerability (1074536)	General	Fri, Sep 27, 2019 4:17 AM UTC	Fri, Sep 27, 2019 4:24 AM UTC	CVE-2019-3896	7.2 (High)	97 %
IBM MQ DoS Vulnerability (886885)	Denial of Service	Fri, Sep 27, 2019 3:57 AM UTC	Fri, Sep 27, 2019 4:02 AM UTC	CVE-2019-4378	4.0 (Medium)	30 %
IBM MQ DoS Vulnerability (876772)	Denial of Service	Fri, Sep 27, 2019 3:38 AM UTC	Fri, Sep 27, 2019 4:02 AM UTC	CVE-2019-4141	6.3 (Medium)	30 %
F5 BIG-IQ - BIG-IQ vulnerability CVE-2019-6653	F5 Local Security Checks	Fri, Sep 27, 2019 3:02 AM UTC	Fri, Sep 27, 2019 3:08 AM UTC	CVE-2019-6653	3.5 (Low)	80 %
Fedora Update for dcmtk FEDORA-2019-4349fc0afb	Fedora Local Security Checks	Fri, Sep 27, 2019 2:33 AM UTC	Fri, Sep 27, 2019 7:41 AM UTC	CVE-2019-1010228	7.5 (High)	97 %
Fedora Update for dcmtk FEDORA-2019-12650a34d8	Fedora Local Security Checks	Fri, Sep 27, 2019 2:33 AM UTC	Fri, Sep 27, 2019 7:41 AM UTC	CVE-2019-1010228	7.5 (High)	97 %
F5 BIG-IQ - BIG-IQ services for stats vulnerability CVE-2019-6652	F5 Local Security Checks	Fri, Sep 27, 2019 2:18 AM UTC	Fri, Sep 27, 2019 3:08 AM UTC	CVE-2019-6652	6.4 (Medium)	80 %
openSUSE Update for nmap openSUSE-SU-2019:2198-1 (nmap)	SuSE Local Security Checks	Fri, Sep 27, 2019 2:01 AM UTC	Fri, Sep 27, 2019 7:41 AM UTC	CVE-2017-18594 CVE-2018-15173	5.0 (Medium)	97 %
CentOS Update for dovecot CESA-2019:2836 centos7	CentOS Local Security Checks	Fri, Sep 27, 2019 2:01 AM UTC	Fri, Sep 27, 2019 7:41 AM UTC	CVE-2019-11500	7.5 (High)	97 %

Apply to page contents ▼

Fuente: Elaboración Propia

OVAL: lenguaje de evaluación y vulnerabilidad abierta

Figura 18. Vulnerabilidad abierta



1 - 10 of 28175

Name	Version	Status	Class	Created ▼	Modified	CVEs	Severity
oval:org.mitre.oval:def:29419 oval/5.10/org.mitre.oval/i/oval.xml	1	DRAFT	inventory	Mon, Aug 17, 2015 1:00 PM UTC	Wed, Aug 19, 2015 7:24 PM UTC	0	N/A
	Microsoft Access 2003 SP3 is installed						
oval:org.mitre.oval:def:29043 oval/5.10/org.mitre.oval/i/oval.xml	1	DRAFT	inventory	Mon, Aug 17, 2015 1:00 PM UTC	Wed, Aug 19, 2015 7:24 PM UTC	0	N/A
	Microsoft Access 2003 is installed						
				Fri, Aug 7, 2015 8:31 AM	Mon, Aug 31, 2015 8:00		

Fuente: Elaboración Propia

Avisos del CERT Bund por clase de gravedad

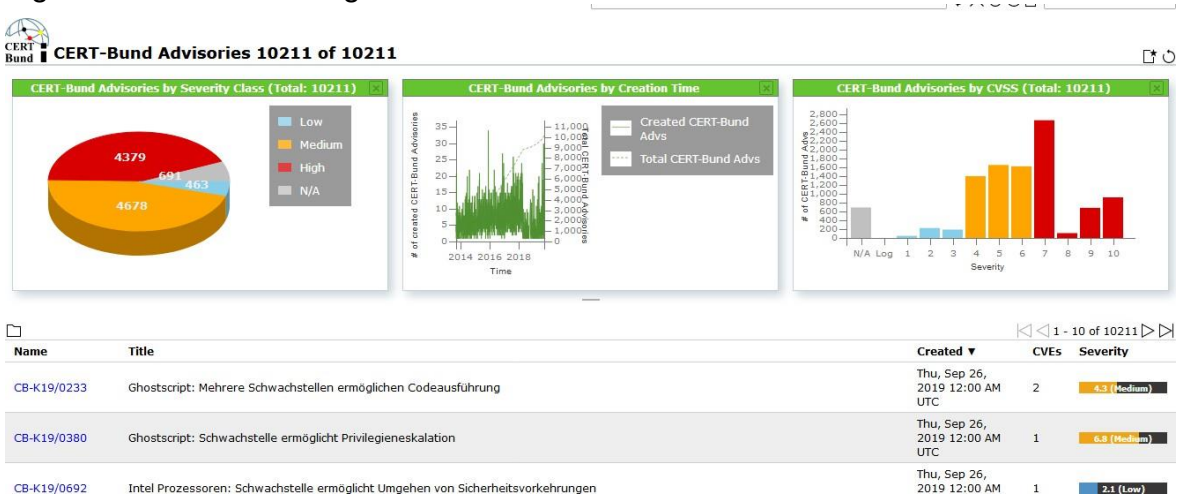
Avisos del paquete CERT por hora de creación

Avisos del paquete CERT por CVSS

Equipo informático de respuesta a emergencias

Avisos de seguridad - DFN-CERT

Figura 19. Avisos de Seguridad

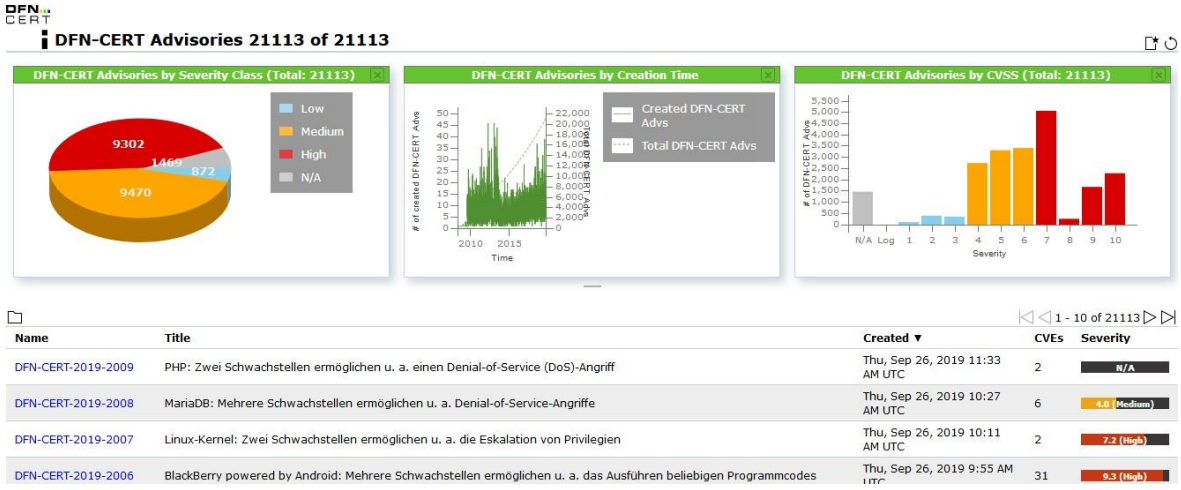


Name	Title	Created ▼	CVEs	Severity
CB-K19/0233	Ghostscript: Mehrere Schwachstellen ermöglichen Codeausführung	Thu, Sep 26, 2019 12:00 AM UTC	2	4.3 (Medium)
CB-K19/0380	Ghostscript: Schwachstelle ermöglicht Privilegieneskalation	Thu, Sep 26, 2019 12:00 AM UTC	1	6.8 (Medium)
CB-K19/0692	Intel Prozessoren: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen	Thu, Sep 26, 2019 12:00 AM	1	2.1 (Low)

Fuente: Elaboración Propia

Avisos de seguridad - DFN-CERT

Figura 20. Avisos de Seguridad DFN-CERT



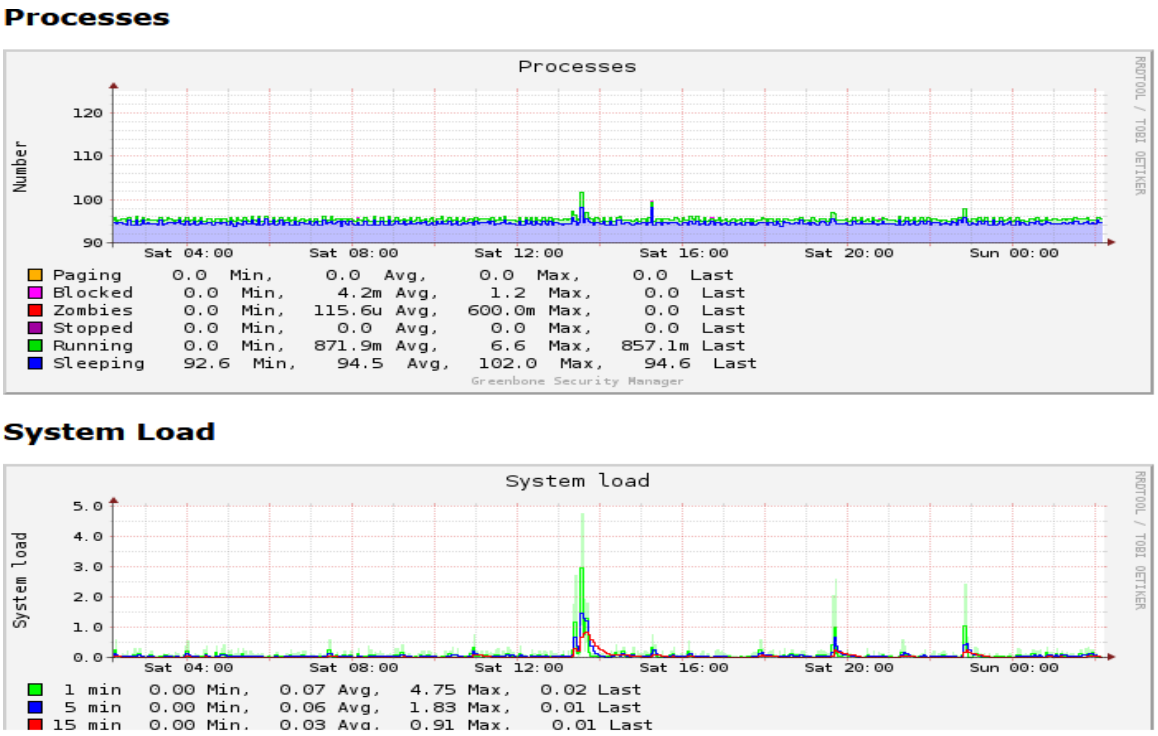
Name	Title	Created ▼	CVEs	Severity
DFN-CERT-2019-2009	PHP: Zwei Schwachstellen ermöglichen u. a. einen Denial-of-Service (DoS)-Angriff	Thu, Sep 26, 2019 11:33 AM UTC	2	N/A
DFN-CERT-2019-2008	MariaDB: Mehrere Schwachstellen ermöglichen u. a. Denial-of-Service-Angriffe	Thu, Sep 26, 2019 10:27 AM UTC	6	4.0 (Medium)
DFN-CERT-2019-2007	Linux-Kernel: Zwei Schwachstellen ermöglichen u. a. die Eskalation von Privilegien	Thu, Sep 26, 2019 10:11 AM UTC	2	7.2 (High)
DFN-CERT-2019-2006	BlackBerry powered by Android: Mehrere Schwachstellen ermöglichen u. a. das Ausführen beliebigen Programmcodes	Thu, Sep 26, 2019 9:55 AM UTC	31	9.3 (High)

Fuente: Elaboración Propia

En esta imagen vemos un alto riesgo, la tarea debe ser equilibrar estas vulnerabilidades haciendo uso del software y la configuración de las herramientas, para poder corregir estos porcentajes que si bien se ven en su mayoría no son graves

Informe de procesos y Carga del sistema

Figura 21. Procesos y Carga

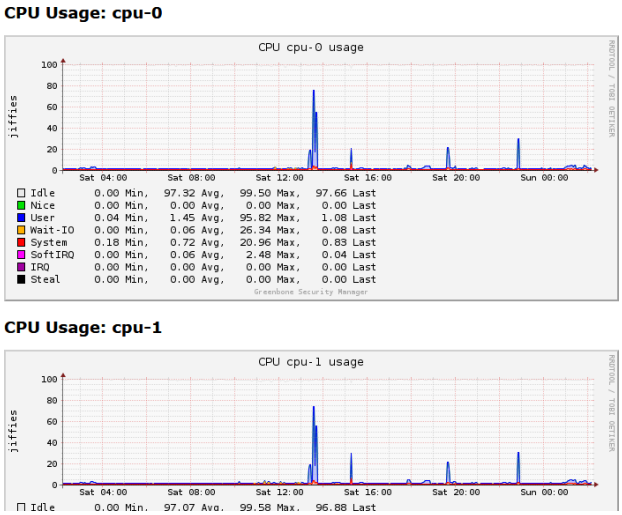


Fuente: Elaboración Propia

El sistema de carga presenta una condición optima y dentro de los rangos normales de funcionamiento.

Uso de CPU 0 y 1

Figura 22. Uso de CPU



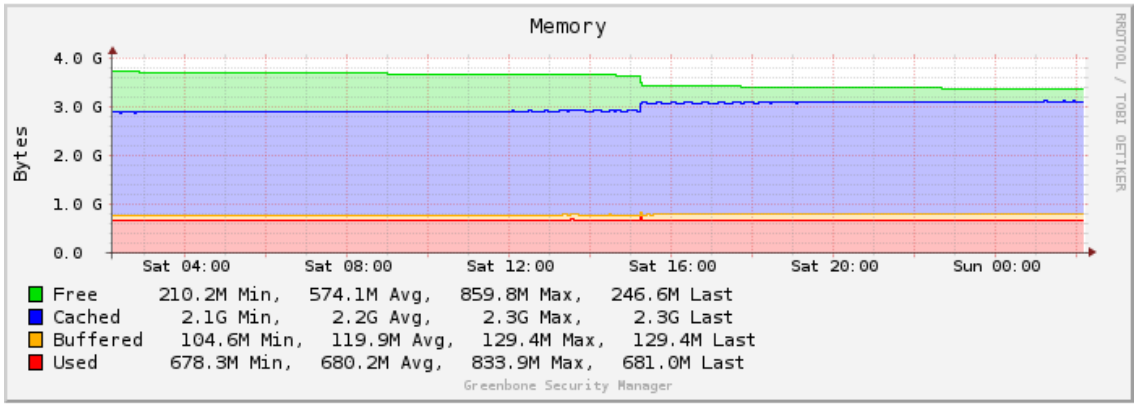
Fuente: Elaboración Propia

El uso de la memoria de los sistemas en estudio presenta las condiciones básicas para no tener problemas, sin embargo, se puede optimizar el sistema para que tenga un mejor desempeño.

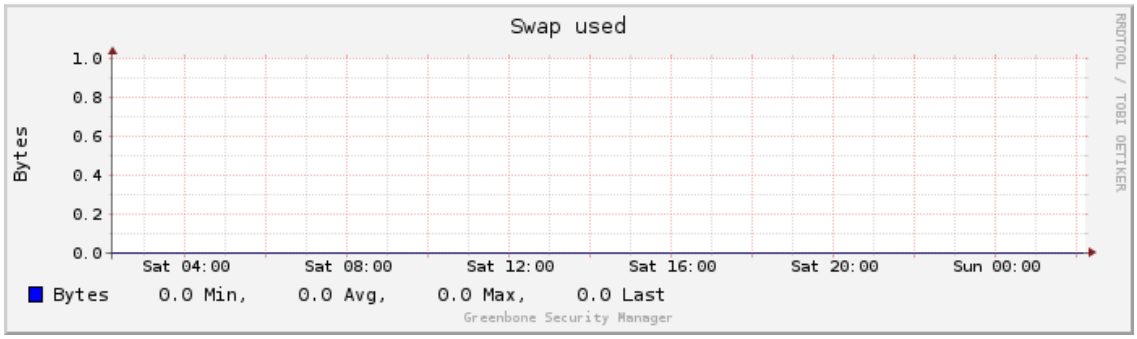
Uso de memoria y uso de intercambio

Figura 23 Intercambio y Uso de Memoria

Memory Usage



Swap Usage



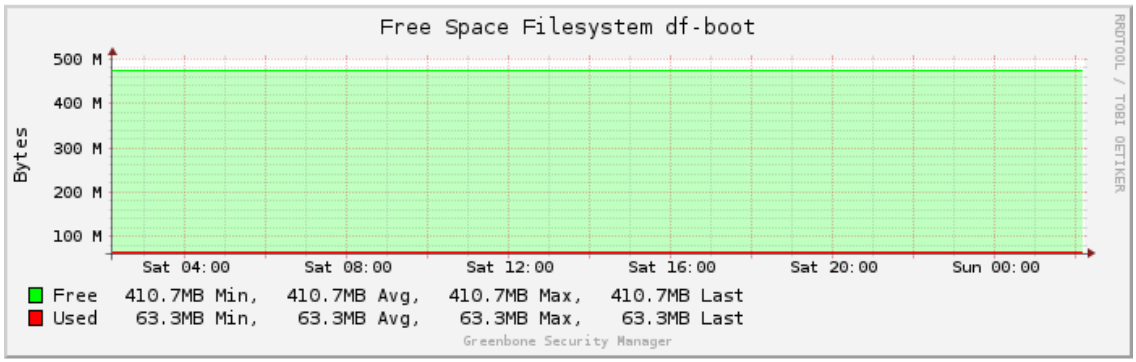
Fuente: Elaboración Propia

La memoria de este sistema funciona en su máximo tope, se debe proponer que se implemente una memoria de más capacidad para así mismo tener un desempeño acorde con el funcionamiento general del sistema

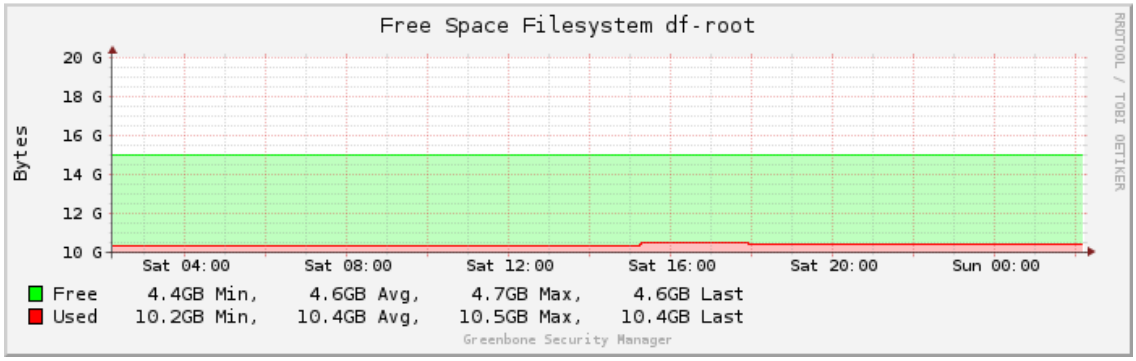
Uso de sistemas de archivos boot y de raiz

Figura 24. Raíz y Archivos del Sistema

File System Usage df-boot



File System Usage df-root

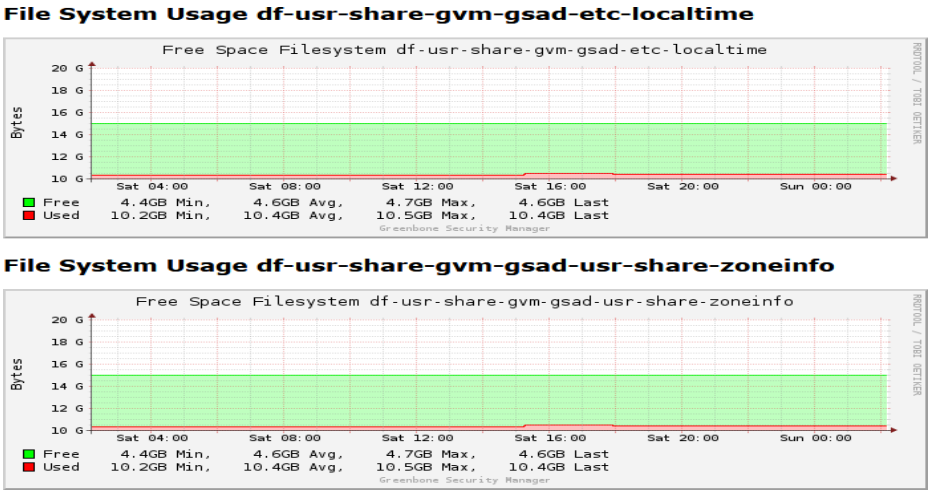


Fuente: Elaboración Propia

Los archivos de estos equipos están debidamente organizados con lo que el sistema maneja una información ordenada.

Uso del sistema de archivos

Figura 25. Sistemas de Archivos en Uso

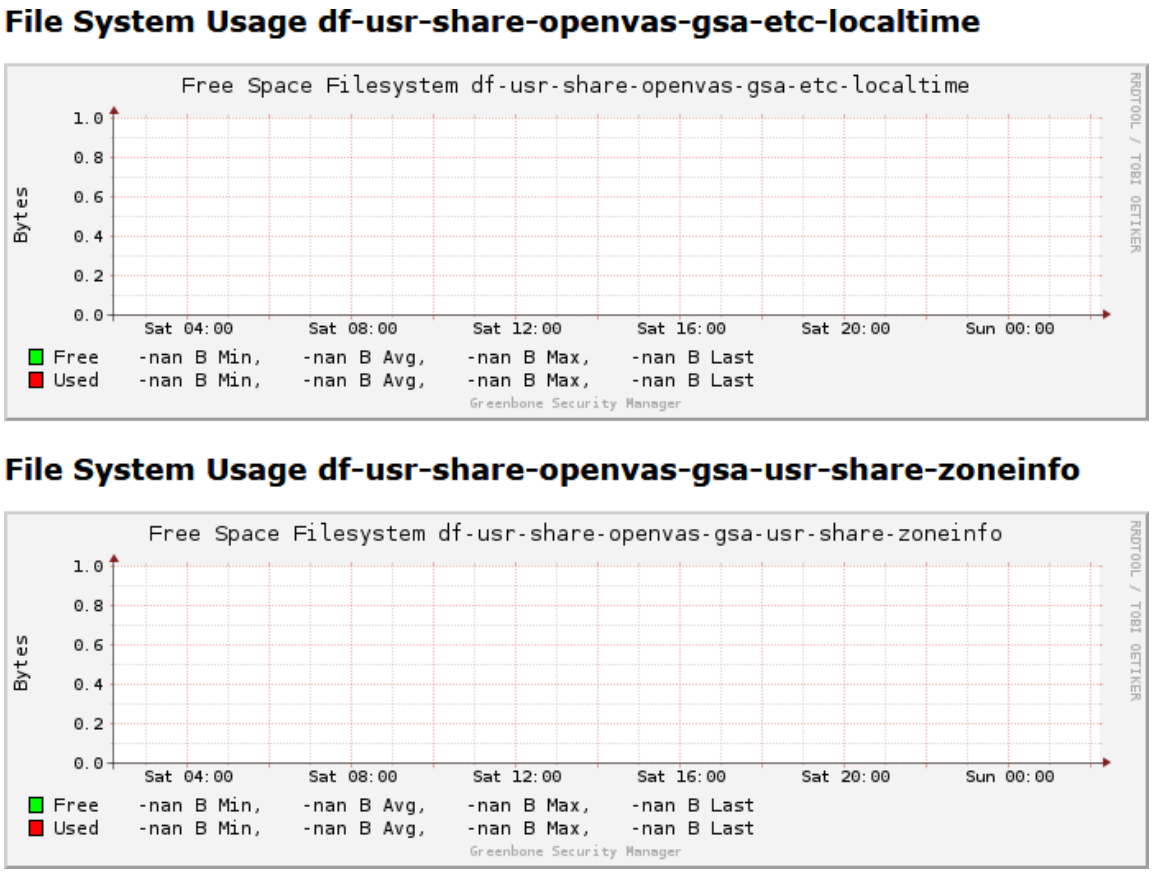


Fuente: Elaboración Propia

En la anterior figura nos expresa y nos indica que el equipo posee un nivel óptimo en su uso

Uso del sistema de archivos de usuario

Figura 26. Archivos de Usuario

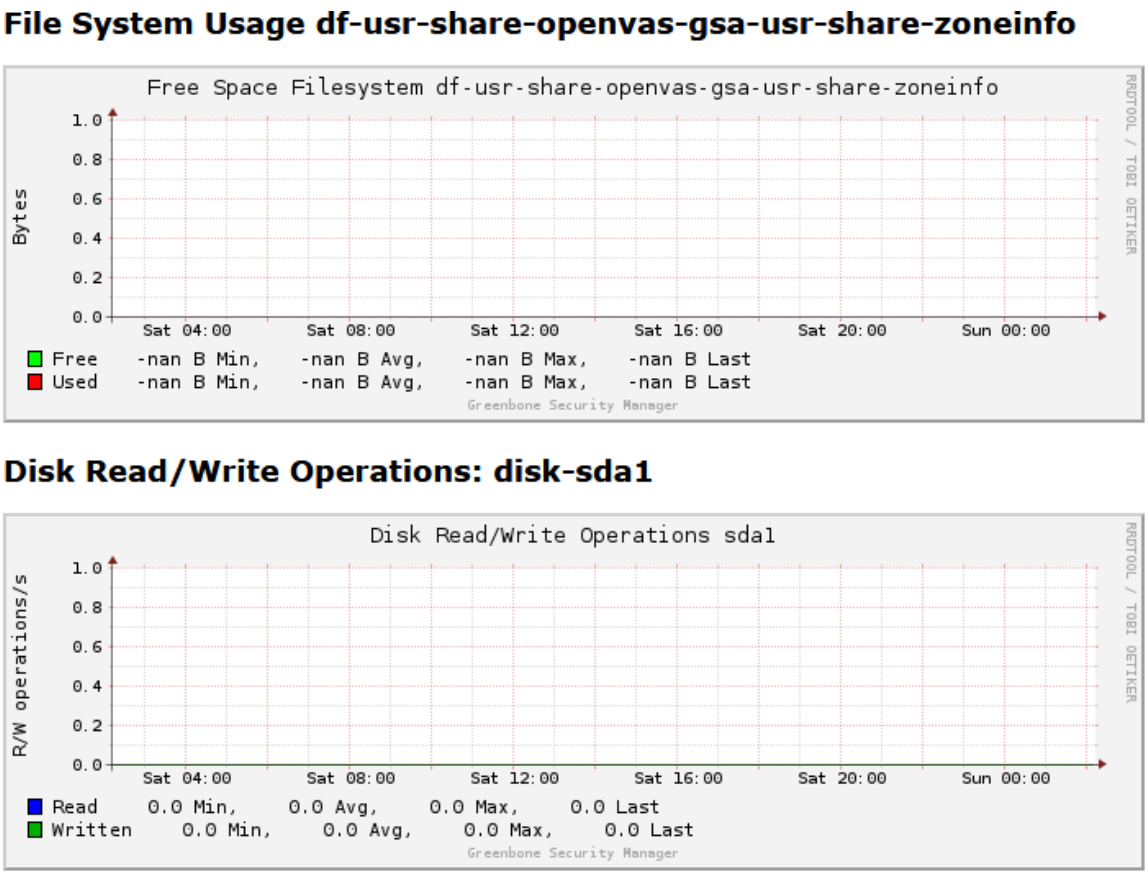


Fuente: Elaboración Propia

Si los archivos tuvieran algún tipo de infección o vulnerabilidad nos expresaría algunos Bytes dispersados con lo que nos indicaría alguna intromisión o riesgo de este

Lectura de disco y operación de escritura

Figura 27. Lectura de Disco

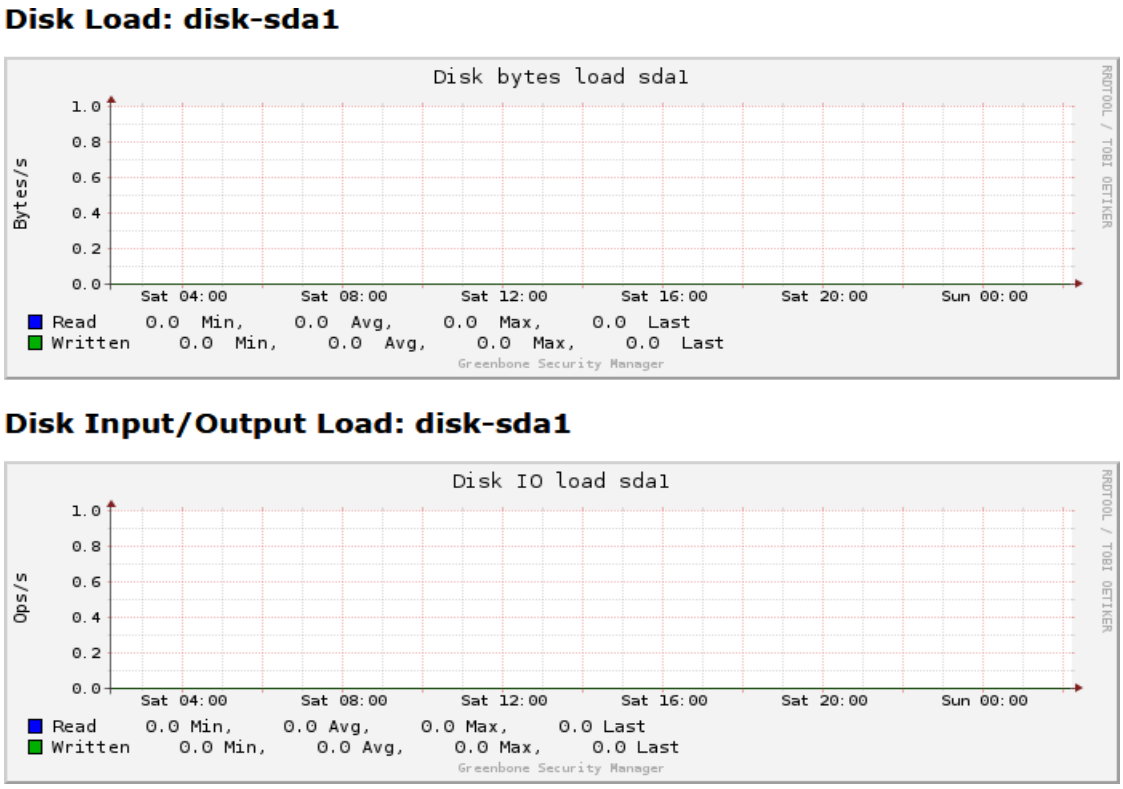


Fuente: Elaboración Propia

Los discos tanto en su lectura como escritura, nos avisa si presenta algún problema el sistema para así mismo poner correctivos al respecto

Carga de disco y entrada de disco

Figura 28. Entrada de Disco

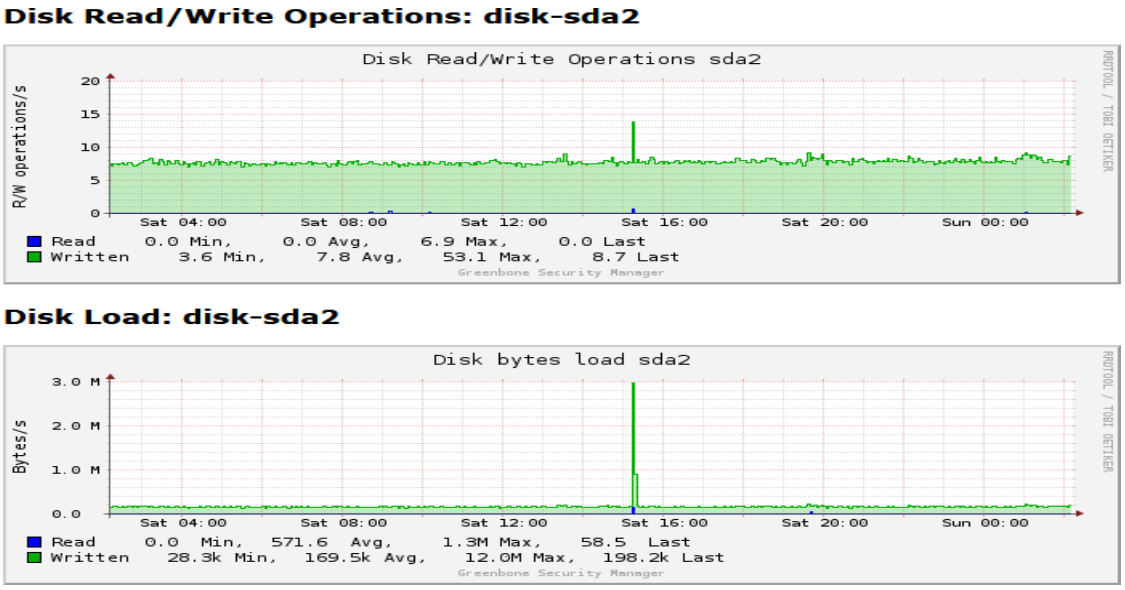


Fuente: Elaboración Propia

Tanto la carga de los discos como la entrada de estos, debe ser estable para mantener un sistema fácil de analizar, el tiempo de respuesta y de carga, depende del nivel óptimo de configuración si presentara alguna vulnerabilidad se expresaría un pico

Operaciones de lectura y escritura de disco/ carga de disco

Figura 29. Lectura de Disco



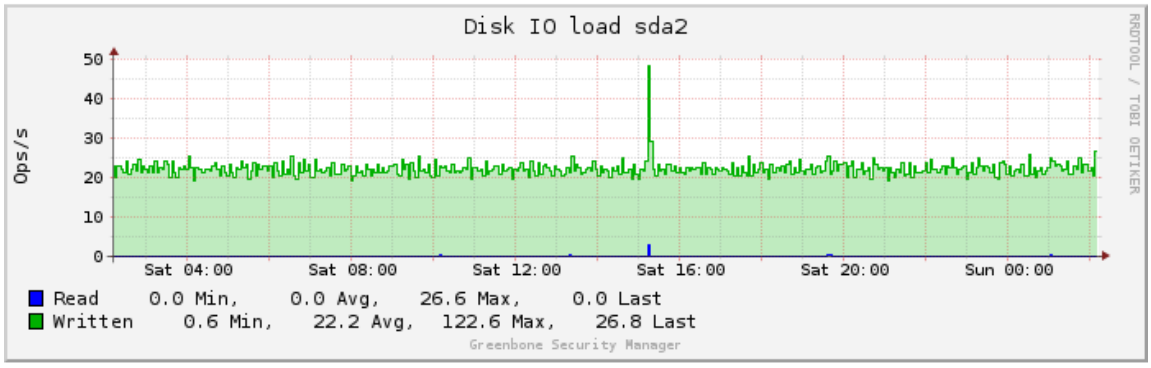
Fuente: Elaboración Propia

La operación de lectura de los discos posee un nivel acorde, esto debido a la correcta configuración de los equipos, presentando picos estables

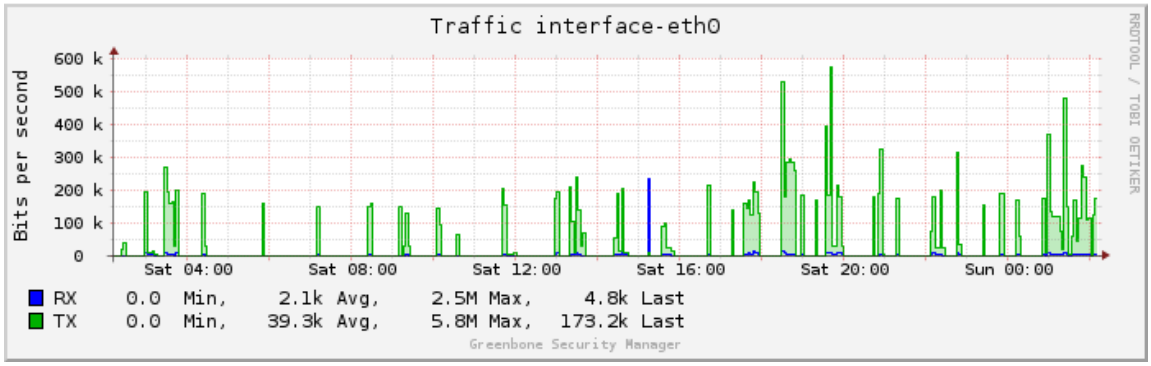
Salida de entrada de disco / interfaz de trafico de red

Figura 30. Trafico de Red

Disk Input/Output Load: disk-sda2



Network Traffic: interface-eth0



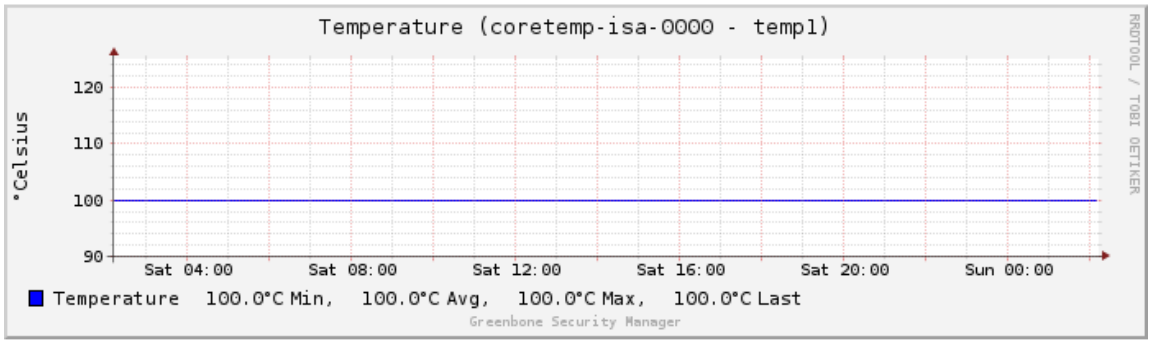
Fuente: Elaboración Propia

El tráfico circundante en la red es otor factor importante que incide en constantes amenazas a los sistemas es por eso tener mucha atención con los sitios web a los que se ingrese, en este caso tenemos diferente tráfico en la red, pero con una navegación segura.

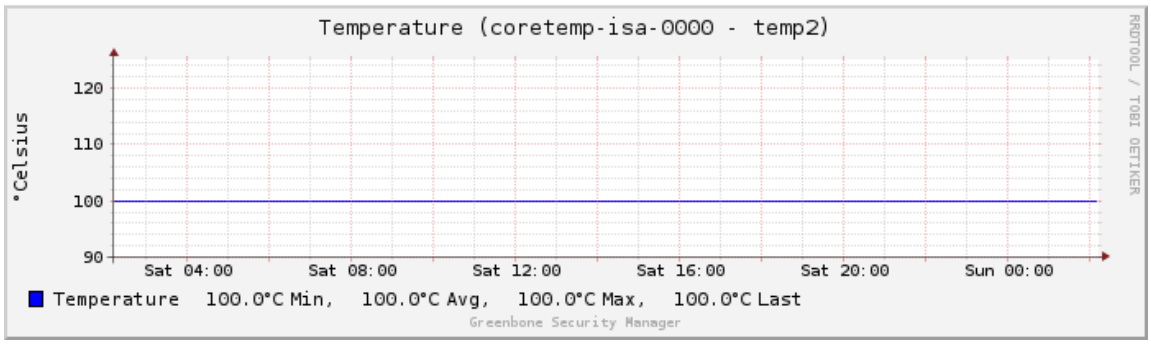
Sensores de temperatura

Figura 31. Temperatura

Temperature: sensors-coretemp-isa-0000 temperature-temp1



Temperature: sensors-coretemp-isa-0000 temperature-temp2



Fuente: Elaboración Propia

Mantener una correcta temperatura de los equipos es fundamental para evitar sobrecalentamiento de los procesadores y así mismo evitar perdida de datos y mal funcionamiento del sistema, en esta lectura se analizan los sensores de temperatura, los cuales son estables para este sistema.

5.3.2.14. Aplicación de Herramientas de Software Libre. Para efectuar de manera eficiente el uso de Software libre en este ejercicio, a continuación, se tiene que conocer cómo se configuran las herramientas que ayudaran en la labor de mantener la red libre de vulnerabilidades, riesgos y amenazas, para eso deben mencionar que algunas de estas herramientas se pueden trabajar directamente en el SO Windows y otros bajo Linux u otros SO que se manejan de manera fácil, económica y segura bajo Máquinas virtuales.

Bajo estos parámetros se logra que los equipos se mantengan en óptimas condiciones de seguridad y están listo para el uso eficiente de la red, para así mismo poder entrelazar la información con toda la seguridad del caso.

5.3.2.15. Supervisión de la Seguridad de los Servidores. Utilice OSSEC HIDS para monitorear los registros y la integridad del sistema de archivos de los servidores y correlacionar.

- Eventos.

Asegurar un servidor no termina con el bloqueo hacia abajo. Los servidores deben ser monitoreados constantemente los sistemas tienen un valor incalculable para alertar sobre posibles ataques contra cualquier número de sistemas de la red, deben realmente sólo ser considerados como sistemas de alerta temprana, en última instancia, tendrá que supervisar cada uno de sus sistemas con mayor detalle, esto implica mantener un ojo en muchas piezas diferentes de información para cada sistema, ver multitudes de diferentes registros archivos en busca de evidencia de los ataques, y la inspección de los binarios importantes para los signos de manipulación, aunque se puede usar una variedad de herramientas para registros agregados de múltiples sistemas , alerta automática en ciertas cadenas y comprobación de los archivos estas herramientas carecen de integración y, al final,

se convierten en sólo cosas que necesitan ser monitoreados, afortunadamente, una herramienta puede realizar todas estas tareas y más: OSSEC HIDS [98].

Esto conduce a una especie de sinergia que no es alcanzable con los sistemas de seguimiento separadas sin trabajo de integración adicional. Por ejemplo, OSSEC puede correlacionar eventos a través de los diferentes archivos de registro para activar alertas especializadas, también puede desplegar OSSEC en una arquitectura cliente / servidor y de fácil escalarlo para supervisar los servidores adicionales a medida que se agregan a su infraestructura. Y OSSEC está disponible tanto para los sistemas Windows y Unix, lo que le permite controlar la integridad de todos sus sistemas con una sola herramienta.

- Instalación

Primeros pasos con OSSEC es fácil, para instalarlo, se descarga el archivo rar desde el sitio web OSSEC HIDS y se descomprime, posteriormente se cambia el directorio que se ha creado (por ejemplo, ossec-hids-0.8) y ejecutar el install-. después de preguntar qué idioma usar para la instalación, verá un mensaje similar a este:

- ¿Qué instalación necesita el servidor, agente local o ayuda?

Para instalar OSSEC en un solo equipo, seleccione la opción local, de lo contrario se configura cliente OSSEC o un servidor, seleccionar agente o servidor, respectivamente.

Después de seleccionar el tipo de instalación a realizar, el script preguntará dónde instalarlo y dónde enviar alertas de correo electrónico, en este punto, se puede elegir si instalar la integridad del sistema comprobación y componentes de detección de rootkits y si es convienente que las respuestas activas, esta característica permite reaccionar a los eventos de forma automática a medida que ocurren, por lo que puede prevenir las intrusiones de tener éxito, si se realiza una instalación local, se configura OSSEC., para hacer una instalación cliente / servidor, primero, se

[98] OSSEC, [sitio web] [Consultado julio 22 de 2020] disponible en: https://www.ossec.net/

realiza la instalación en el servidor o en una máquina, paso seguido se realzara instalación en uno o más huéspedes, al seleccionar un agente al instalar, obtendrá este mensaje adicional:

- ¿Qué dirección IP tenemos del servidor OSSEC HIDS?: para ellos es necesario digitar la dirección IP del equipo donde se efectuó la instalación, el resto de las indicaciones serán las mismas, el proceso que realiza, remoted-ossec, utiliza el puerto UDP 1514, por lo que debe asegurar que las reglas del cortafuegos le permitirán el tráfico de los agentes lleguen a él, agregar agentes después de haber instalado un agente, vaya al sistema en el que haya instalado el servidor y agrega el agente:

/ var / ossec / bin / manage_agents

****

* Administrador de Agent v0.8 OSSEC HIDS.

*

* Las siguientes opciones están disponibles: *

****

(A) dd un agente (A).

Tecla (E) Xtract para un agente (E).

(L) ist ya se ha agregado agentes (L).

(R) emueva un agente (R).

(Q) uit.

Elija sus acciones: A, E, L, R o Q: un - adición de un nuevo agente (use '\" para volver al menú principal), por favor, proporcione la siguiente:

* Un nombre para el nuevo agente: spek

* La dirección IP para el nuevo agente: 192.168.0.62

* Una identificación para el nuevo agente [001]:

Información Agente:

ID: 001

Nombre: spek

Dirección IP: 192.168.0.62

? Confirme agregarlo (y / n): y

Alta.

A continuación, tendrás que extraer la clave que se ha generado para el agente y la importación en el propio agente, de modo que pueda comunicarse con el servidor, para ello, mediante la ejecución de manage_agents nuevo y escribiendo en el indicador: ... Elija sus acciones: A, E, L, R o Q: en agentes disponibles:

ID: 001, Nombre: spek, IP: 192.168.0.62

Proporcione el ID del agente para extraer la clave (o '\" para dejar): 1 agente de información clave para '001 'es:

MDAxIHNwZWsgMTkyLjE2OC4wLjYyIDhhNzVmNGY1ZjBmNTIzNzI5NzAzMTRjMTFmNGVlOWZhZDEzY2QxZWY1ODQyZDEyMmFjYjM2

** Pulse ENTER para volver al menú principal.

Ahora, vaya a la agente y haga lo siguiente:

/ var / ossec / bin / manage_agents

****

* Administrador de Agent v0.8 OSSEC HIDS.

*

* Las siguientes opciones están disponibles: *

****

Clave (I) mport para el servidor (I), (Q) uit. elija sus acciones: I o Q: i

* Proporcionar la clave generada por el servidor.

* El mejor enfoque consiste en cortar y pegar.

*** OBS: No incluya espacios o nuevas líneas.

Pegue aquí (o '\" para dejar):

MDAxIHNwZWsgMTkyLjE2OC4wLjYyIDhhNzVmNGY1ZjBmNTIzNzI5NzAzMTRjMTFmNGVlOWZ

hZDEzY2QxZWY1ODQyZDEyMmFjYjM2YzVmY2JmYTg5OGM =

Información Agente:

ID: 001

Nombre: spek

Dirección IP: 192.168.0.62

? Confirme agregarlo (y / n): y

Alta.

** Pulse ENTER para volver al menú principal.

A continuación, iniciar el servidor:

/ var / ossec / bin / puesta en el control ossec

A partir OSSEC HIDS v0.8 ...

Iniciado ossec-maild ...

Iniciado ossec-execd ...

Iniciado ossec-analysisd ...

Iniciado ossec-logcollector ...

-Remoted ossec Iniciado ...

Iniciado ossec-syscheckd ...

Completado.

Por último, iniciar los agentes:

/ var / ossec / bin / puesta en el control ossec

A partir OSSEC HIDS v0.8 ...

Iniciado ossec-execd ...

Iniciado ossec-AgentD ...

Iniciado ossec-logcollector ...

Iniciado ossec-syscheckd ...

Completado.

Por desgracia, el servidor no proporcionará ninguna indicación de que el cliente puede o se ha conectado a él hasta se genera una alerta, por lo que querrá probarlo intentando generar una alerta. Por ejemplo, si se está ejecutando un demonio SSH en el sistema de agente, usted podría tratar de ssh para la cuenta root (Con suerte, de haber conexiones como root deshabilitado, por lo que este será inocuo), si ha elegido la opción predeterminada la ubicación de instalación para el servidor, usted debería ser capaz de encontrar las alertas en / var / ossec / logs / alertas.

Las alertas se organizan en directorios por año y mes con archivos separados para cada día (por ejemplo, 2019/Jun/ossec-alerts-01.log).

Compruebe el archivo de alertas adecuado, y usted debería ver algo similar a esto:

** Alerta 1149663466.1082:

2019 01 de junio 01:53:28 (spek) 192.168.0.62-> / var / log / messages

Regla: 401 (nivel 5) -> 'error de autenticación del usuario.' Src IP: (ninguno)

Usuario: (ninguno)

sshd (pam_unix) [7917]: error de autenticación; logname = uid = 0 = 0 euid tty = ssh ruser =

rhost = kryten.nnc user = root

** Alerta 1149663468.1362:

2019 01 de junio 01:53:30 (spek) 192.168.0.62-> / var / log / secure

Regla: 1.516 (Nivel 5) -> 'autenticación SSHD falló.' Src IP: 192.168.0.60

Usuario: root

sshd [7917]: error de contraseña para el usuario root desde 192.168.0.60 puerto 64206 ssh2

** Alerta 1149663480.1604: correo

2019 01 de junio 00:54:00 (spek) 192.168.0.62-> / var / log / messages

Regla: 402 (nivel 10) -> 'El usuario se perdió la contraseña más de una vez'

Src IP: (ninguno)

Usuario: (ninguno)

sshd (pam_unix) [7917]: 2 más los errores de autenticación; logname = uid = 0 = 0 euid tty = ssh ruser = rhost = kryten.nnc user = root

Usted también debería recibir comunicación vía email que se especifica en el servidor durante el proceso de instalación, la instalación de un agente de Windows la versión para Windows de OSSEC sólo admite la instalación del agente, que se puede configurar con sólo descargar el instalador y ejecutarla, cuando se inicia, se le preguntará dónde instalar los archivos y luego ejecutar el manage_agents programa, aquí, usted puede importar la clave que ha generado para de la misma manera que lo hizo para la versión Unix del agente, después de haber introducido

la llave y salir del programa de gestión de agente, el instalador le presentará la información que está en OSSEC ossec.conf y que queda almacenado en el directorio en el que ha decidido instalar el agente, desafortunadamente, el instalador de Windows no está tan automatizado como el Unix instalar guion es, por lo que tendrá que escribir la dirección IP de su servidor OSSEC manualmente, busque la línea que tiene este aspecto:

<Server- abcd </ server-ip>

y reemplazar abcd con la dirección IP de su servidor, después que la instalación se haya completado, vaya al panel de control del applet Servicios, busque el servicio OSSEC HIDS, y arrancarlo. mientras está en ello, probablemente querrá también se configura para que sea iniciado al encender el sistema, ahora usted puede probarlo con un enfoque similar al previamente utilizado para poner a prueba el agente Unix, si usted tiene cuenta de inicio de sesión de auditoría habilitadas para el sistema, se puede tratar de iniciar sesión en una cuenta con una contraseña incorrecta, lo que debería crear algo como esto en el archivo de registro actual en su OSSEC servidor:

** Alerta 1149742916,124085:

2019 02 de junio 23:01:56 (mirlo) 192.168.0.67-> WinEvtLogRegla: 8.005 (Nivel 4) -> 'evento de fallo de la auditoría de Windows. "

Src IP: (ninguno) usuario: sistema

WinEvtLog: Seguridad: AUDIT_FAILURE (680): Seguridad: SISTEMA: NT AUTHORITY: BLACKBIRD: partida de arranque

intento por: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0

Cuenta al iniciar: Andrew Fuente

Puesto de ejecución: BLACKBIRD Código de error: 0xC000006A

Configuración

Archivo de configuración por defecto de OSSEC está formateado en XML y ubicado en / var / ossec / etc / ossec.conf (en Windows, este archivo estará en el directorio en el que ha decidido instalar OSSEC), secciones de particular interés para los servidores es <syscheck>,<localfile>,<alerts>, Y <Global> secciones, la sección

define qué archivos y directorios OSSEC debe comprobar si hay signos de deterioro, <syscheck> etiqueta especifica la frecuencia para realizar la comprobación: <frecuencia> <frecuencia> 7200 </ frecuencia> 7200 segundos (cada dos horas) es el valor predeterminado, si utiliza los servicios que están agotado para el subsistema de disco, puede que desee incrementar este valor, ya que los archivos de suma de control pueden ser bastante de E / S intensiva, especifica los directorios que se consulte con el <directories> tag, el valor predeterminado es realizar todos los controles de los archivos de cada uno de los directorios cerrados dentro de la etiqueta en una lista delimitada por comas, esto sígnica que OSSEC comparará Suma de control MD5 de cada archivo a los valores anteriores, así como su tamaño, propietario, grupo, y los permisos, los cheques de archivos de configuración por defecto en los siguientes directorios:

<directorios check_all="yes"> / etc, / usr / bin, / usr / sbin </ directorios> <directorios check_all="yes"> / bin, / sbin </ directorios> girar cheques individuales o fuera sustituyendo el check_all atributo con cualquier combinación de check_sum, check_size, check_owner, check_group, O check_perm y estableciendo su valor a ya sea sí o no, si desea ignorar un archivo o directorio en particular, encerrarlo entre <omitir> tags: <omitir> / etc / mtab </ ignore> cambiando de tema, <localfile> secciones se utilizan para especificar los archivos de registro para monitorear, dentro de ellas, se puede utilizar la <location> etiqueta para especificar la ruta completa al archivo de registro, especificar el formato del archivo con <log_format> tag. Los valores válidos para el formato son syslog, snort-completo, snort-rápido, calamar, o apache.

Además, los usuarios de Windows se encuentran el iis y eventlog formatos que consideren de especial interés, porque permiten OSSEC para analizar su IIS y registros de eventos, cuando se dispara una alerta, OSSEC asocia un nivel de gravedad con él (de 1 a 16), puede utilizar <alerts> sección para establecer el umbral en el que registre una alerta o generar un correo electrónico. Aquí están los valores predeterminados para estas opciones: <alerts> <log_alert_level> 1 </ log_alert_level> <email_alert_level> 7 </ email_alert_level> </ Alertas>

Por último, utilice el <globals> sección para definir diversas opciones que afectan OSSEC en su conjunto, por ejemplo, puede manipular el acceso al e-mail que el script de instalación configura para esta sección, aquí es también donde se puede utilizar el <white_list> etiqueta para especificar los hosts que nunca deben ser bloqueadas con respuestas activas, por ejemplo, para asegurarse de que 10.0.0.123 nunca se bloquea, agregue una línea como ésta al <globals> sección: <white_list> 10.0.0.123 </ white_list> ahora, echemos un vistazo a cómo configurar respuestas activas.

- Las Respuestas Activas

Respuestas activas pueden variar de bloqueo anfitriones a través de servidores de seguridad para desactivar automáticamente las cuentas de usuario, esta es una característica de gran alcance, pero tenga especial cuidado al usarlo, una respuesta activa que pueda causar inadvertidamente DOS sí mismo o proporcionar un medio fácil para un atacante para hacerlo, es por eso que OSSEC proporciona una función de lista blanca, para asegurarse de que las reglas del cortafuegos añadidos dinámicamente no se bloquean confianza anfitriones. Respuestas activas en OSSEC funcionan mediante la vinculación de un comando a un nivel de alerta y cualquier número de identificadores de regla, la respuesta activa se dispara cuando se genera una alerta para una de las reglas que especifica su nivel y si cumple o excede lo especificado, cuando la creación de una respuesta activa, primero debe definir el comando para ejecutar sus parámetros, dentro de un <comando> bloque, definir un nombre para el comando que se ejecutará cuando el comando es asociada con una o más reglas en un <active-response> bloque, he aquí un ejemplo del archivo de configuración por defecto de OSSEC, los siguientes bloqueos de mandato de un usuario cuenta que está asociada con una alerta: <comando> <nombre> desactivar la cuenta </ name> <ejecutable> disable-account.sh </ ejecutable> usuario <expect> </ esperar> <timeout_allowed> sí </ timeout_allowed> </ Command> más tarde, puede hacer referencia a este <comando> bloquear en un <active-response> bloquear, así: <active-response>

<comando> deshabilitar la cuenta </ command> <location> locales </ location> <nivel> 10 </ nivel> <rules_id> 402 </ rules_id> <timeout> 900 </ timeout> </ Respuesta activa> esta respuesta hará que las cuentas que desencadenan 'El usuario se perdió la contraseña de más de un tiempo " alertar mostrado anteriormente se bloquee durante 15 minutos. Una cosa para destacar en este ejemplo es la <location> tag, esta etiqueta permite especificar el lugar donde quiere la respuesta que se active. Uso local hará que la respuesta a ser activada en la máquina que generó la alerta, mientras que análisis servidor hará que se active en el servidor, alternativamente, puede utilizar todo o agente definido a provocar la respuesta que se activará en todos los sistemas o un agente específico, respectivamente, en este último caso de que también tendrá que utilizar el <agent_id> etiqueta para especifica el agente para desencadenar la respuesta, cuando se desencadena una respuesta, una entrada aparecerá en / var/ossec/active-response/ossec-hidsresponses.log, por ejemplo, cuando se activa la respuesta se muestra más arriba, algo similar a esto aparecerá: Jue 02 de junio 05:18 :26 MDT 2019 .. /active-response/bin/disable-account.sh añadir Andrew como puede ver, la función de respuesta activa de OSSEC puede ser muy poderoso, usted puede incluso escribir su propios guiones de respuesta activa, que le da un número ilimitado de posibilidades literalmente en forma automática reaccionar a los ataques, esto y muchas otras características de OSSEC puede ser replicado por la combinación de otras herramientas, sin embargo, OSSEC les ofrece de manera integrada y le ahorra el tiempo dedicado a pegar juntos con su lenguaje de script favorito de tiempo que puede pasar frente a real problemas de seguridad.

5.3.2.16. Seguimiento y Tendencias

Si bien la importancia de los registros del sistema confiable no puede ser sobrestimada, los registros sólo cuentan parte de la historia de lo que está sucediendo en su red, cuando algo fuera de lo normal ocurre, el evento es debidamente registran en el archivo correspondiente, donde se espera a un ser

humano para darse cuenta y tomar la acción apropiada, pero registros son valiosos sólo si alguien realmente los lee, cuando los archivos de registro, simplemente se suman a la avalancha de información que la mayoría de los administradores de red deben vadear a través de cada día, podrían ser puestos a un lado e ir sin leer durante días o semanas, esta situación se agrava cuando los archivos de registro están obstruidos con información irrelevante, por ejemplo, una llamada de auxilio de un servidor de correo sobrecargado puede ser fácilmente pierde si está rodeado de entradas inocuas sobre los intentos de spam que han fallado, con demasiada frecuencia, los registros se utilizan como un recurso para averiguar lo que pasó cuando los sistemas fallan, y no como una guía de lo que está sucediendo ahora, otro aspecto importante de las entradas de registro es que sólo proporcionan un "control sobre el terreno" de su sistema en un momento particular, sin una historia del normal desempeño parece, puede ser difícil decirla diferencia entre el tráfico normal de red, un (DoS) ataque de denegación de servicio, y una visita de los lectores de Slashdot, mientras que usted puede construir fácilmente un informe de la cantidad de veces que el / var llena partición arriba, ¿cómo se puede realizar un seguimiento de lo que el uso normal se parece a lo largo del tiempo? ¿Es la cola de correo obstruye debido a un usuario desconsiderado, o es parte de un ataque de un adversario? ¿O es simplemente una tendencia general que es el resultado de tratar de servir a muchos usuarios en demasiado pequeño de un disco? Se describe un número de métodos para el seguimiento de la disponibilidad de servicios y recursos con el tiempo, en lugar de tener que mirar los registros del sistema de forma manual, por lo general es mucho mejor tener los sistemas que notifiquen cuando hay un problema-y sólo cuando hay un problema, se dan una serie de sugerencias sobre cómo reconocer las tendencias en el tráfico de red de monitoreo flujos y gráficos los resultados en gráficos, claro, usted puede ser que sepa lo que su saliente de Internet promedie el tráfico que aparece, pero ¿cuánto de ese tráfico se compone de HTTP frente peticiones SMTP? usted puede saber más o menos la porción de datos de cada servidor que genera en la red, pero si usted quiere romper es el tráfico por protocolo? Los hackers le mostrarán cómo.

- Monitorear la Disponibilidad

Nagios es utilizada para mantener un control sobre la red, Exploits remotos a menudo pueden bloquear el servicio romperlo o causar mal funcionamiento de CPU, por lo que es esencial controlar los servicios que se ejecutan en la red, sólo en busca de un puerto abierto (usando una herramienta como Nma no es suficiente, la máquina puede ser capaz de responder a una solicitud de conexión TCP, pero el servicio puede ser incapaz de responder (o peor, podría ser sustituido por un programa completamente diferente!), una herramienta que puede ayudarle a verificar sus servicios es Nagios (http://www.nagios.org).

Nagios es una aplicación de red de monitoreo que controla no sólo servicios presentes en los equipos y en la red, sino también los recursos en cada host, tales como el uso de CPU, espacio en disco, uso de memoria, los procesos en ejecución, archivos de registro, y mucho más, en el advenimiento de un problema, se le puede notificar a través del correo electrónico, un smartphone , o cualquier otro método que defina, y que puede comprobar el estado de la red en utilizando la interfaz web, Nagios también es fácilmente extensible a través de su API plug-in.

- Instalación de Nagios

Para instalar Nagios, descargue la distribución de código fuente de la página web de Nagios. Luego, descomprimir la fuente de distribución y se va al directorio que crea:

$ tar xfz nagios-1.1.tar.gz

$ nagios-1.1 cd

Crear un usuario y un grupo para Nagios para funcionar como (por ejemplo, nagios), y ejecute el configure script:

$. / configure

- With-nagios-user = nagios - with-nagios-grp = nagios

Esto instala en Nagios / / local / nagios usr . Como de costumbre, puede modificar este comportamiento a través de la

- Prefix cambiar, después de la configuración de la escritura termina, compilar Nagios ejecutando todo.

Entonces, hágase root y corre make install para instalarlo, opcionalmente, puede instalar scripts de inicialización de Nagios ejecutando hacer init a instalar

Si nos fijamos en el usr / local / local / nagios directorio en este punto, verá cuatro directorios, la papelera y directorio contiene nagios , que es el núcleo del paquete, esta aplicación hace el real

Monitoreo, el sbin directorio contiene los scripts CGI que se utilizarán en la interfaz basada en web, dentro de la cuota de directorio, usted encontrará los archivos HTML y la documentación. por último, la var directorio es donde Nagios almacena su información una vez que se pone en marcha, antes de poder utilizar Nagios, tendrá que ejecutar el siguiente comando:

$ make install-config

Este comando crea un etc directorio poblado con una copia de muestra de cada archivo de configuración requerida por Nagios, vamos a ver cómo configurar los archivos, la instalación de Nagios ha finalizado, sin embargo, no es muy útil en su estado actual, porque carece de las aplicaciones de monitoreo reales, estas aplicaciones, que comprueban si un particular,

servicio supervisado está funcionando correctamente, son llamados plug-ins . Nagios viene con un conjunto predeterminado de

plug-ins, pero deben ser descargados e instalados por separado. Instalar plug-ins

Descargue la última versión de Nagios Plugins paquete y descomprimirlo, usted tendrá que ejecutar la configurar prevista script para preparar el paquete para la compilación en su sistema. Usted encontrará que los plug-ins están instalados de una manera similar al programa real de Nagios, para compilar los plug-ins, ejecute los siguientes comandos:

$. / configure - prefix = / usr / local / nagios \

- With-nagios-user = nagios - with-nagios-group = nagios

$ marcar

Usted puede obtener notificaciones acerca de que faltan programas o módulos de Perl, mientras que el script se está ejecutando, estos son en su mayoría muy bien, a menos que necesite específicamente las aplicaciones mencionadas para controlar

un servicio, una vez finalizado la compilación, la raíz y ejecutar convertido make install para instalar los plug-ins, los plug-ins
se instalará en el libexec directorio de su directorio base Nagios (por ejemplo, / usr / local / nagios / libexec).
Hay algunas opciones que todos los plug-ins de Nagios debe implementar, lo que hace que sean adecuadas para su uso por Nagios, cada plug-in proporciona una
- Help
opción que muestra información sobre el plug-in y la forma en que funciona, esta característica es útil cuando usted está tratando de monitorear un nuevo servicio mediante un plug-in que no ha usado antes, por ejemplo, para aprender la
check_ssh
plug-in de trabajos, ejecute el siguiente comando:
$ / usr / local / nagios / libexec / check_ssh
check_ssh (nagios-plugins 1.4.3) 1.27
<nagiosplug-devel@lists.sourceforge.net>
Trate de conectarse a un servidor SSH en el servidor y el puerto especificado
Uso: check_ssh [-46] [-t <timeout>] [-r <remote version>] [-p <puerto>] <host>
Valores:
-H, - help
Impresión en detalle de pantalla de ayuda
-V, - version
Datos de la versión
-H, - hostname = DIRECCIÓN
Nombre, dirección IP o socket Unix Anfitrión (debe ser una ruta absoluta)
-P, - port = INTEGER
Número de puerto (por defecto: 22)
-4, - Use-ipv4
Usar conexión IPv4
-6, - Use-ipv6
Usar conexión IPv6

-T, - timeout = INTEGER

Segundos antes de los tiempos de conexión hacia fuera (por defecto: 10)

-R, - versión remota = STRING

Advertir si la cadena no coincide con la versión del servidor esperado (por ejemplo: OpenSSH_3.9p1)

-V, - verbose

Se visualizan los detalles para la depuración de línea en los comandos (Nagios puede truncar la salida) enviar email a nagios-users@lists.sourceforge.net si tiene preguntas relacionadas con la utilización de este software, para enviar parches o sugerir mejoras, envíelo a la nagiosplug-devel@lists.sourceforge.net, ahora que tanto Nagios y los plug-ins instalados, ya está casi listo para empezar el monitoreo de servidores. Sin embargo, Nagios ni siquiera comenzar antes de que este configurado correctamente.

Configuración de Nagios

Configuración de Nagios puede ser una tarea ardua, pero los archivos de configuración de ejemplo proporcionar un buen punto de partida:

$ cd / usr / local / nagios / etc

$ ls -1

bigger.cfg-muestra

cgi.cfg-muestra

checkcommands.cfg-muestra

minimal.cfg-muestra

misccommands.cfg-muestra

nagios.cfg-muestra

resource.cfg-muestra

Como se trata de archivos de ejemplo: los autores de Nagios añadieron una. cfg-muestra sufijo a cada archivo, primeramente, necesitará copiar o cambiar el nombre de cada uno para terminar en. cfg, por lo que el software puede utilizar de manera adecuada.

Si usted no cambia las extensiones de archivo, Nagios no será capaz de encontrar los archivos de configuración, se puede cambiar el nombre de cada archivo de forma manual o utilizar el siguiente comando para cuidar todos a la vez:

for i in * cfg-muestra.; hacer $ mv i \ Qbasename $ i cfg-sample \ Q.cfg.; hecho;

Para obtener Nagios funcionando, debe modificar todos, pero algunos de los archivos de configuración de ejemplo, al inicio, está el archivo principal que se configuro, nagios.cfg, puede dejar casi todo como está aquí; el Nagios en el proceso de instalación se asegurará de que las rutas de archivos utilizados en el fichero de configuración sean correctos, hay una opción, sin embargo, que es posible que desee cambiar:

check_external_commands , Que se fija para 0 por predeterminado, si desea ejecutar comandos directamente a través de la interfaz web, ponga esto en dependiendo del entorno de red, esto puede o no puede ser un riesgo de seguridad aceptable, ya que permite esta opción y permite la ejecución de scripts desde la interfaz web, otras opciones que necesita para poner en cgi.cfg configure que se permiten nombres de usuario para ejecutar comandos externos. Configuración de Nagios para supervisar los servidores no es tan difícil como parece, para ayudarle, puede utilizar el modo detallado del binario Nagios al ejecutar:

/ usr / local / nagios / bin / nagios-v / usr / local / nagios / etc / nagios.cfg locales

Esto va a través de los archivos de configuración y los informes de errores. Iniciar la fijación de los errores uno por uno, ejecutar el comando de nuevo para encontrar el siguiente error.

Adición de hosts para monitorear usted primero necesita agregar su definición del host y configurar algunas opciones para ese host, puede añadir muchos anfitriones como usted quiera, pero aquí vamos a seguir con uno por el bien de la simplicidad. Estos son los contenidos de hosts.cfg :

Plantilla genérica definición de equipo

definir el sistema principal {# El nombre de esta plantilla de acogida - que se hace referencia en otras definiciones de equipos,

Utilizado para la plantilla de la recursividad / resolución

nombre
generic-host
Notificaciones de host están activados
notifications_enabled
1
Controlador de eventos Host está activada
event_handler_enabled
1
Detección # Flap está habilitado
flap_detection_enabled
1
Datos de rendimiento de proceso #
process_perf_data
1
Mantener la información de estado en los reinicios del programa
retain_status_information
1
Retener información no estado en los reinicios del programa
retain_nonstatus_information
1
DONT REGISTRAR ESTA DEFINICIÓN - que no es un verdadero anfitrión,
SOLO UNA PLANTILLA!
registrar
0
contact_groups
FLCD-admins
}
# Host Definición
definir el sistema principal {
# Nombre de la plantilla de host para utilizar

utilizar
generic-host
nombre_de_equipo
freelinuxcd.org
alias
Libre de Project Server CD de Linux
dirección
www.freelinuxcd.org
check_command
check-host-vivo
max_check_attempts
10
notification_interval
120
notification_period
24x7
notification_options
D, U, R
}
Asegúrese de quitar las líneas que comienzan con
#
al crear su hosts.cfg ; de lo contrario, recibirá
errores.
El primer host definido no es un anfitrión real, sino una plantilla a partir de la cual se derivan otras definiciones de acogida.
Este mecanismo se utiliza en otros archivos de configuración, así y hace que la configuración basada en un conjunto predefinido de valores predeterminados de una brisa. Con esta configuración, estamos monitoreando solo host, www.freelinuxcd.org, para ver si está vivo, el

nombre_de_equipo parámetro es importante porque otros archivos de configuración se referirán a este servidor por este nombre, una vez que haya terminado de editar hosts.cfg , elimine la línea que lo incluye en nagios.cfg :
Cfg_file = / usr / local / nagios / etc / hosts.cfg

5.3.2.17. Creación de grupos de hosts

Ahora que usted tiene una gran cantidad de supervisar, tiene que ser añadido a un hostgroup, de manera que la aplicación sabe que el contacto de grupo para enviar notificaciones a, esto el hostgroups.cfg parece:
definir hostgroup {hostgroup_name FLCD servidores alias los servidores gratuitos de Proyecto de CD de Linux contact_groups-admins FLCD miembros freelinuxcd.org}
Esto define un nuevo hostgroup y asocia el FLCD-admins contact_group con ella. Al igual que con hosts.cfg, tendrá que editar nagios.cfg e incluir su hostgroups.cfg :
Cfg_file = / usr / local / nagios / etc / hostgroups.cfg
Creación de contactos al igual que grupos de los mismos
Ahora, tendrá que definir el FLCD-admins grupo de contacto en contactgroups.cfg :
definir:
contactgroup {contactgroup_name FLCD-admins alias FreeLinuxCD.org Administradores
miembros oktay, verty} aquí, este se define con dos miembros, oktay y verty , esta configuración asegura que tanto los usuarios serán notificados cuando algo va mal con un servidor que FLCD-admins es responsable el siguiente paso es configurar las preferencias de información de contacto y notificación de estos los usuarios.
Estas son las definiciones de esos dos miembros en contacts.cfg :
definir el contacto {
contact_name
oktay
alias

Oktay Altunergil
service_notification_period
24x7
host_notification_period
24x7
service_notification_options
W, U, C, R
host_notification_options
D, U, R
service_notification_commands
notifique por correo electrónico, notifique por epager
host_notification_commands
acoger a notificar por correo electrónico, host-notify-por-epager
email oktay@freelinuxcd.org smartphone dummypagenagios-admin@localhost.localdomain
}
definir el contacto {
contact_name
verty
alias
David 'Verty' Ky
service_notification_period
24x7
host_notification_period
24x7
service_notification_options
W, U, C, R
host_notification_options
D, U, R
service_notification_commands

notifique por correo electrónico, notifique por epager
host_notification_commands
Aloja a notificar por correo electrónico
email
verty@flcd.org
}
Además de proporcionar información de contacto para un usuario en particular, la contact_name
en el contacts.cfg archivo
también es utilizado por los scripts CGI (es decir, la interfaz web) para determinar si un usuario en particular es permitido acceder a un recurso particular, configuración de los servicios de monitor de ahora que sus anfitriones y los contactos están configurados, usted puede comenzar a configurar la supervisión para el individuo los servicios en el servidor,esto se hace en services.cfg (eliminar los comentarios que al crear el tuyo):
# Plantilla genérica definición de servicio
define service {
# El 'nombre' de esta plantilla de servicio, referencia en otras definiciones de servicio
nombre generic-service
cheques de servicio activos están habilitados
active_checks_enabled 1
cheques servicio pasivo se habilitan / aceptadas
passive_checks_enabled 1
cheques de servicio activas deben ser paralelizados
(Deshabilitar esto puede dar lugar a importantes problemas de rendimiento)
parallelize_check 1
Hay que obsesionarse con este servicio (si es necesario)
obsess_over_service 1
Por defecto es no comprobar el servicio "frescura"
check_freshness

0
Notificaciones de servicio se activan
notifications_enabled 1
Controlador de eventos # servicio está habilitado
event_handler_enabled 1
Detección # Flap está habilitado
flap_detection_enabled 1
Datos de rendimiento de proceso #
process_perf_data 1
Mantener la información de estado en los reinicios del programa
retain_status_information 1
Retener información no estado en los reinicios del programa
retain_nonstatus_information 1
DONT REGISTRAR ESTA DEFINICIÓN - que no es un verdadero servicio, SOLO UNA PLANTILLA!
registrar0 }
Definición # Servicio
define service {
# Nombre de la plantilla de servicio a utilizar
utilizar generic-service
nombre_de_equipofreelinuxcd.org
service_description HTTP
is_volatile
0
check_period
24x7
max_check_attempts 3
normal_check_interval 5
retry_check_interval 1
contact_groups

FLCD-admins
notification_interval 120
24x7 notification_period
notification_options w, u, c, r
check_command
check_http
}
Definición # Servicio
define service {
# Nombre de la plantilla de servicio a utilizar
utilizar generic-service
nombre_de_equipofreelinuxcd.org
PING service_description
is_volatile
0
check_period
24x7
max_check_attempts 3
normal_check_interval 5
retry_check_interval 1
contact_groups
FLCD-admins
notification_interval 120
24x7 notification_period
notification_options c, r
check_command
check_ping! 100.0,20%! 500.0,60%
}
Esta configuración establece la supervisión de los dos servicios, la primera definición de servicio, que ha sido llamado HTTP, controla si el servidor web está

en marcha y le avisa si hay un problema, la segunda definición monitorea las estadísticas de ping desde el servidor y le notifica si el tiempo de respuesta o de paquetes de pérdida llega a ser demasiado alta, los comandos que se utilizan son
check_http
y
check_ping
Que se instalaron en la libexec directorio durante la instalación de plug-in, por favor, tómese su tiempo para familiarizarse con todos los otros plug-ins disponibles y configurarlos de manera similar a las definiciones de ejemplo anteriores, definición de períodos de tiempo ahora, tendrá que definir los períodos de tiempo que usted ha estado utilizando en el periodo de notificación y directivas mediante la creación de un timeperiods.cfg archivo, los ejemplos anteriores utilizan un periodo de tiempo, aquí hay una definición de lo que se puede poner en su timeperiods.cfg :
definir periodo de tiempo { timeperiod_name 24 horas y 7 dias alias 24x7 Lunes 01:18 18:00 lunes 12:16 -24:00 martes 12:16-24:00 miércoles 12:16-24:00 jueves 12:16-24:00 viernes 12:16-24:00 sábado 12:16-24:00 }
Ahora, todo lo que tiene que hacer es incluir cada uno de estos archivos dentro de su principal nagios.conf utilizando el cfg_file, esta directiva la muestra nagios.cfg contiene una directiva para cargar todos los archivos de configuración mencionados aquí, se buscan las entradas ejecute Nagios con el
-V
cambiar una vez más para asegurarse de que todo va bien, a continuación, ejecutarlo como demonio mediante el
-D
cambiar:
/ usr / local / nagios / bin / nagios-d / usr / local / nagios / etc / nagios.cfg
Después de que usted haya conseguido Nagios en funcionamiento, coloque el servidor web favorita de Nagios sbin directorio
(Contiene los scripts CGI) y reinícielo. Eso es todo lo que hay que hacer. Dale Nagios un par de minutos para

generar algunos datos, y luego dirija su navegador a la máquina y mirar la advertencia servicio bastante
luces.

5.3.2.18. Tendencias Gráficas. Se utiliza RRDtool para generar de forma sencilla los gráficos para casi cualquier cosa. Al estar familiarizado con el uso del ancho de graficar con herramientas como MRTG. A partir de una seguridad punto de vista, el uso de ancho de banda de graficos es útil porque puede ayudar a detectar comportamientos anómalos.

Tener un historial de uso típico ancho de banda que ofrece una línea de base a la actividad juez. Esto puede hacer más más fácil determinar si alguien está realizando un ataque DoS en su sitio, o si la máquina en la red está actuando como Warez depósito. RRDtool (http://people.ee.ethz.ch/oetiker/webtools/rrdtool/) Proporciona una funcionalidad similar a MRTG, pero es mucho más flexible. RRDtool es básicamente una pieza que guarda datos en una de propósito general base de datos que nunca crecerá en tamaño. RRD representa la base de datos de todos contra todos, que en los datos mantiene un número fijo de entradas: la entrada más antigua constantemente está siendo sustituida por los nuevos datos. RRDtool también tiene la capacidad de generar gráficos de dato en la base de datos.

El uso más común de RRDtool es hacer gráficos bastante ancho de banda, lo que se hace fácilmente con RRDtool y snmpget , una utilidad que realiza consultas a los dispositivos gestionados con SNMP, en primer lugar, usted tendrá que crear una base de datos de todos contra todos mediante la ejecución de un comando similar a éste:

$ rrdtool crear zul.rrd - start N \ DS: de0_in: CONTADOR: 600: U: U \ DS: de0_out: CONTADOR: 600: U: U
\ RRA: PROMEDIO: 0.5:1:600 \ RRA: PROMEDIO: 0.5:6:700 \ RRA: PROMEDIO: 0.5:24:775

\ RRA: PROMEDIO: 0.5:288:797 \ RRA: MAX: 0.5:1:600 \ RRA: MAX: 0.5:6:700 \ RRA: MAX: 0.5:24:775
\ RRA: MAX: 0.5:288:797
Este comando crea una base con entradas para los dos contadores independientes:
de0_in
y
de0_out

Estas muestras almacenan entradas de estadísticas de la interfaz recogen cada cinco minutos de un daemon SNMP en un router. Además, la base de datos contiene varios campos para el mantenimiento automático de funcionamiento promedios. Puede rellenar la base de datos mediante la ejecución de un comando como este:
$ rrdtool actualización zul.rrd N: \ \ public zul Qsnmpget-Oqv
interfaces. ifTable.ifEntry. ifInOctets.4 \ Q: \ public zul \ Qsnmpget-Oqv
interfaces. ifTable.ifEntry. ifOutOctets.4 \ Q
Este comando consulta las estadísticas de entrada y salida para el de0 interfaz en un equipo denominado zul .
Para programarlo para que se ejecute cada cinco minutos, se puede hacer una entrada crontab similar al siguiente:
Actualización rrdtool 0-55/5 **** / home / andrew / rrdbs / zul.rrd N: \ public zul Qsnmpget-Oqv
interfaces. ifTable.ifEntry. ifInOctets.4 \ Q: \ public zul Qsnmpget-Oqv
interfaces. ifTable.ifEntry. ifOutOctets.4 \ Q
Sin embargo, puede utilizar cualquier método que desea recopilar los datos. Para generar los gráficos por hora de la
datos, puede ejecutar un comando como este:
$ gráfico rrdtool zul_de0-hourly.png-t "de ancho de banda por hora" - comienzan -3600 \
DEF: inoctets = zul.rrd: de0_in: AVERAGE \

DEF: outoctets = zul.rrd: de0_out: AVERAGE \

ÁREA: inoctets # 00FF00: "de0 En" \

LÍNEA 1: outoctets # 0000FF: "de0 Out"

La -3600 en el comando le dice

Rrdtool que desea graficar los datos recogidos durante la última hora (Hay 3.600 segundos en una hora). Del mismo modo, si desea crear un gráfico en el transcurso de un día, utilizar -86,400. pero eso es sólo el comienzo, tras la recogida de múltiples fuentes de datos, puede combinarlos todos en un único gráfico que le da una gran cantidad de información de un vistazo, el uso de salida de varios servidores a la vez, con la media total para todos los servidores justo debajo de él. si bien esta cifra es en escala de grises, la gráfica actual utiliza un color diferente para cada servidor, por lo que es fácil saber de un vistazo lo que uno está acaparando todo el ancho de banda.

RRDtool es una herramienta flexible, todo lo que necesitas hacer es decir que la cantidad de datos que desea almacenar y luego establecer algún método para recopilar los datos en un intervalo regular, entonces, usted puede fácilmente generar un gráfico de los datos siempre que lo desee.

5.3.2.19. Consiga en Tiempo Real Estadísticas de la Red

Ver quién está haciendo qué en la red a través del tiempo con ntop. Si usted está buscando para las estadísticas de la red en tiempo real, echa un vistazo a la excelente ntop herramienta(http://www.ntop.org), Un analizador de protocolos con todas las funciones con una interfaz web, con SSL y apoyo de gráficas. ntop no es precisamente ligero (la cantidad exacta de recursos que se requieren depende del tamaño de la red y el volumen de tráfico de la red), pero se le puede dar una muy buena imagen en su red, ntop necesita para funcionar inicialmente como root, a tirar las interfaces en modo promiscuo y empezar a capturar paquetes, pero luego la libera de sus privilegios a un usuario que se especifique, si decide ejecutar ntop por mucho períodos de tiempo, es probable que sea más feliz corriendo en una caja de

monitoreo dedicado (con algunos otros servicios que se ejecutan en él, por razones de seguridad y de rendimiento). Aquí hay una referencia rápida sobre cómo conseguir ntop en marcha y funcionando, en primer lugar, crear un ntop de usuarios y grupos:

groupadd ntop

useradd-c "usuario ntop"-d / usr / local / etc / ntop-s / bin / true-g ntop ntop

Entonces, desempaquetar y construir ntop según las instrucciones en docs / BUILD-NTOP.txt. después que ntop ha terminado compilar, instalarlo ejecutando make install como root, durante el proceso de instalación, un directorio para ntop para almacenar sus bases de datos en el se creará. Si usted no ha utilizado el - Prefix opción cuando se ejecuta:

configurar, este directorio debe ser / usr / local / var / ntop. Se creó como root durante la instalación, por lo que usted tendrá que cambiar su dueño al usuario se le ejecuta ntop como para que ntop para poder escribir en él, ntop también debe copiar un certificado auto-firmado a / usr / local / etc / ntop / ntop-cert.pem locales como parte de la instalación proceso, por lo que se puede acceder de forma segura su interfaz web, tenga en cuenta que la clave SSL por defecto no será construido con el nombre de host correcto para su servidor, por lo que es probable que desee para generar su propio SSL certificado y par de claves, ahora, usted necesita establecer una contraseña de administración para ser utilizado al configurar ntop a través de su interfaz:

ntop-A-u ntop

Vie 05 de mayo 2019 22:03:27 NOTA: merge Interface activada por defecto

¡Vie 05 de mayo 2019 22:03:27 Iniciando bases de datos GDBM inicio ntop - a la espera de la respuesta del usuario! por favor, introduzca la contraseña para el usuario admin: por favor, introduzca la contraseña de nuevo: Vie 05 de mayo 2019 22:03:31 admin contraseña de usuario se ha configurado finalmente, ejecute ntop como demonio, e iniciar el servidor SSL en el puerto favorito (4242, por ejemplo):

ntop-u ntop-W4242-d

Por defecto, ntop también dirige un servidor HTTP de serie en el puerto 3000, usted debería considerar seriamente el bloqueo por el acceso a estos puertos, ya sea en el servidor de seguridad o mediante el uso de la línea de comandos iptables reglas, deje ntop funcionar durante un rato, y luego conectarse a https://your.server.here:4242/, usted puede encontrar todo tipo de detalles sobre lo que el tráfico se ha visto en la red.

Mientras que las herramientas como tcpdump y Ethereal le dan los análisis detallados e interactivos de tráfico de red, ntop ofrece una gran cantidad de información estadística en una interfaz web muy elegante y fácil de usar. ¿Cuándo correctamente instalado y bloqueado, que probablemente se convierta en una herramienta favorita en su herramienta de análisis de redes?

Recopilar Estadísticas con las Reglas del Cortafuegos

Haga su conjunto de reglas de firewall haga el trabajo cuando se quiere recoger estadísticas. si quieres empezar a recopilar estadísticas sobre el tráfico de su red, pero teme la creación de SNMP, no lo hace no tienen por qué preocuparse, usted puede utilizar el código del cortafuegos de su sistema operativo para recopilar estadísticas para usted, por ejemplo, si está usando Linux, puede utilizar iptables comandos similares a la siguiente para mantener pista de ancho de banda consumido por una máquina especial que pasa el tráfico a través del firewall:

```
# iptables-N kryten && iptables-A kryten-j ACCEPT
# iptables-N KRYTEN_IN && iptables-A KRYTEN_IN-j kryten
# iptables-N KRYTEN_OUT && iptables-A KRYTEN_OUT-j kryten
# iptables-A FORWARD-s 192.168.0.60
-J KRYTEN_OUT
# iptables-A FORWARD-d 192.168.0.60-j KRYTEN_IN
```

Este enfoque aprovecha los contadores de bytes y paquetes asociados con cada iptables para proporcionar entrada y salida de las estadísticas de ancho de banda para el tráfico remitidas a través del firewall, funciona primero la definición de una cadena llamado Kryten , que lleva el nombre del host en el que se recogerán las estadísticas, esta cadena contiene una regla de aceptar incondicional, y se utiliza

para agregar rápidamente el total del ancho de banda que kryten consume, para calcular el ancho de banda descendente kryten está utilizando, otra cadena llamada KRYTEN_IN del mismo modo, para calcular el ancho de banda de salida kryten está utilizando, una cadena llamada KRYTEN_OUT se crea, cada una de estas cadenas contiene una sola regla, que salta sin condiciones a Kryten cadena, esta permite que el ancho de banda de salida que se añade al ancho de banda de entrada de ser consumido por último, las normas se añaden a la cadena que dirige cada paquete a la cadena correcta, dependiendo de si es procedente o con destino a Kryten después de la aplicación de estas reglas, se puede ver el ancho de banda total (entrante y saliente) consumida por Kryten ejecutando un comando como éste:
iptables-vx-L kryten
Kryten Chain (2 referencias) pkts bytes de destino prot opt in fuera fuente destino 442 46340 ACEPTAR todo – cualquier lugar usted puede analizar fácilmente bytes del campo, y así generar gráficos con RRDtool, usando un comando como el siguiente:
iptables-vx-L kryten | egrep-v 'Chain | pkts "| awk' {print $ 2} '
Para obtener la cantidad de ancho de banda de entrada o de salida consumida, basta con sustituir
Kryten con KRYTEN_IN o , respectivamente por supuesto, usted no tiene que limitar sus criterios de recopilación de estadísticas a poco KRYTEN_OUT por el equipo de ancho de banda se puede recoger estadísticas sobre cualquier cosa que se puede crear con iptables entre determinados puertos, direcciones MAC, o casi cualquier otra cosa que pasa a través de su puerta de enlace, también puede hacer algo similar para los sistemas que utilizan Packetfilter de OpenBSD para todas las reglas, PF realiza un seguimiento del número de veces que ha sido evaluado, cuántos paquetes han provocado la regla, ¿cuántos bytes se encontraban en esos paquetes, y cuántos estados se han creado (en el caso de stateful reglas). El problema está en los datos se puede ver las estadísticas de reglas mediante la ejecución pfctl-s de reglas -Vv , pero los datos no están en una forma fácilmente analizable:

@ 3 inet pase desde 192.168.0.60 a cualquier
[Evaluaciones: 125 los paquetes: 60 Bytes: 4976 unidos: 0] [Insertado: uid 0 pid 15815]
@ 4 inet pase de cualquier a 192.168.0.60
[Evaluaciones: 128 los paquetes: 65 Bytes: 7748 Unidos: 0]
[Insertado: uid 0 pid 15815]
Sin embargo, puede agregar la etiqueta palabra clave al final de cada regla, para que se lean como sigue:
pasar inet de 192.168.0.60 a cualquier etiqueta "KRYTEN_OUT"
pasar inet de cualquier a 192.168.0.60 etiqueta "KRYTEN_IN"
Entonces, usted puede obtener las estadísticas sobre las normas mediante la ejecución
pfctl-s etiquetas:
KRYTEN_OUT 175 77 6660 77 6660 0 0
KRYTEN_IN 176 93 1166 8 0 0 93 11 668
No sólo son las estadísticas más fáciles de analizar, pero también dan más de ellos, los números de arriba, de izquierda a derecha, representan el número de evaluaciones, los paquetes totales, el total de bytes, paquetes salientes, el total de bytes salientes, los paquetes entrantes, y los bytes entrantes totales, al igual que con iptables, puede obtener estadísticas sobre cualquier cosa por la que puede crear una regla.

5.3.2.20. Análisis de Forma Remota. Para realizar un control de redes de manera remota se utiliza rpcapd. El control de tráfico de la red y de cualquier otro segmento utilizado protocolos gráficos y de analizadores como etéreo acarrea mucho tiempo, en este sentido es necesario que sé que capturen los datos, e identificar la estación de trabajo donde se está ejecutando el analizador, y cargar el archivo en el propio analizador, esto crea un problema real debido a que aumenta el tiempo entre la realización de un experimento y los resultados, lo que genera que el diagnostico y la solución de problemas de red tarden mucho más tiempo de lo

que debería, para dar solución a este incovenite se utilizar la rpcapd , un programa incluido con WinPcap (http://winpcap.polito.it). rpcapd es un agente eficiente que monitoriza las interfaces de red en modo promiscuo y envía los datos que recoge de nuevo a un sniffer que se ejecuta en una máquina remota, puede ejecutar rpcapd ya sea desde la línea de comandos o como un servicio para iniciar rpcapd , es probable que desee utilizar el -N bandera, que le dice agente para utilizar la autenticación usando esta opción, usted será capaz de controlar el flujo de datos que rpcapd produce con cualquier programa que utiliza la interfaz de captura WinPcap. de lo contrario, tendrá que agregar código especial con el programa que está utilizando para permitir que se autentique con rpcapd. desde el -N opción que permite que cualquiera pueda conectarse al demonio, también querrá utilizar el -L opción, que le permite especificar una lista separada por comas que se pueden conectar. Por lo tanto, para ejecutar rpcapd desde la línea de comandos, utilice un comando similar al siguiente.

5.3.2.21. Túneles Seguros. Las Redes informáticas no son de confianza (como Internet y las redes inalámbricas públicas) pueden ser ambientes hostiles, pero pueden ser domesticados en algún grado se debe configurar y codificar la comunicación y asegurarlas a través de redes que no sean completamente de confianza, algunos de los hacks centrarán principalmente en proporcionar un mecanismo de transporte seguro y cifrado, mientras que otros discuten cómo crear una red privada virtual (VPN). Como verás aquí, mediante el aprovechamiento de cifrado y algunos trucos de encapsulación se puede construir redes más confiable en la cima de una red insegura, incluso si esta última está llena de sinvergüenzas que tratan de espiar o manipular los datos pero cómo configurar enlaces cifrados basados en IPsec en varias operaciones de sistemas, cómo crear interfaces de red virtuales que se pueden tunneled a través de un cifrado de conexión, y cómo reenviar conexiones TCP a través de un canal cifrado. Además, aprenderá cómo configurar una solución VPN multiplataforma. la belleza de la mayoría de estos hacks es que después de leerlos, usted puede mezclar y emparejar la capa de

transporte soluciones de cifrado con cualquier enfoque virtual orientada a la red que le conviene más, de esta manera, se puede construir con seguridad grandes y poderosas redes privadas el aprovechamiento de la Internet pública como la infraestructura que Usted pueda utilizar estas técnicas para cualquier cosa de conectar de forma segura con dos oficinas remotas para la construcción de una red empresarial privada completamente derrotando el hackeo

Configuración de IPsec En Linux

Asegure su tráfico en Linux con Openswan.

La manera más popular de configurar conexiones IPsec en Linux es utilizando el Openswan (http://www.openswan.org.)

Paquete Openswan está formado por dos componentes: plutón y, opcionalmente, Kernel de seguridad IP (KLIPS). Desde la versión 2.6, el kernel de Linux incluye soporte para IPsec, pero KLIPS pueden utilizarse en lugar de algunas características adicionales. Plutón es el demonio de espacio de usuario que controla negociación de Internet Key Exchange (IKE). para comenzar, descargue la última fuente para las herramientas Openswan desde el sitio web del proyecto y desempaquete el árbol de código fuente, a continuación, cambie al directorio que se extrajo y construirlo:

$ tar xfz openswan-2.4.6rc3.tar.gz

$ cd openswan-2.4.6rc3

$ realizar programas

Después que termine la compilación, convertirse en root y ejecute make install si usted quiere probar el soporte de encriptación oportunista de en lugar de utilizar KLIPS soporte IPsec nativa en el kernel. Para ello, descargue el parche apropiado desde el Openswan descargar la página. Aplique el parche a las fuentes del núcleo con los siguientes comandos:

cd / usr/src/kernels/linux-2.6.14.6

zcat / tmp/openswan-2.4.6rc3.kernel-2.6-klips.patch.gz | patch-p1

Si ha configurado el código fuente del núcleo antes de aplicar el parche, lo puede activar de forma rápida y sencilla KLIPS ejecutando make oldconfig
. Estas son las opciones que necesitas tener:
Openswan IPsec (KLIPS26) (KLIPS) [N / m / y /?] (NEW) m*
* Opciones Klips *
Carga de seguridad encapsuladora - ESP ("VPN") (KLIPS_ESP) [Y / n /?] (NEW)
¿Cabecera de Autenticación - [? N / y /] AH (KLIPS_AH) (NEW) y
Algoritmo de autenticación HMAC-MD5 (KLIPS_AUTH_HMAC_MD5) [Y / n /?] (NEW)
Algoritmo de autenticación HMAC-SHA1 (KLIPS_AUTH_HMAC_SHA1) [Y / n /?] (NEW)
Interfaz algoritmo CryptoAPI (KLIPS_ENC_CRYPTOAPI) [N / y /?] (NEW)
Algoritmo de cifrado 3DES (KLIPS_ENC_3DES) [Y / n /?] (NEW)
Algoritmo de cifrado AES (KLIPS_ENC_AES) [Y / n /?] (NEW)
Compresión IP (KLIPS_IPCOMP) [Y / n /?] (NEW)
IPsec depuración (KLIPS_DEBUG) [Y / n /?] (NEW)
Esta salida muestra KLIPS configurado para ser compilado como un módulo; sin embargo, puede vincular en el kernel estáticamente, si lo prefiere.
Si el kernel parcheado para KLIPS, se reconstruye y reinicia con ella, la próxima vez que arranque, el ipsec el servicio se iniciará automáticamente, si decide utilizar una función de IPsec apoyo del núcleo, puede ir adelante y comenzar ahora: # / etc / init.d / inicio ipsec ipsec_setup: comenzando Openswan IPsec 2.4.6rc3 ...
ipsec_setup: insmod / lib/modules/2.6.16-1.2115_FC4/kernel/net/key/af_key.ko
ipsec_setup: insmod / lib/modules/2.6.16-1.2115_FC4/kernel/net/ipv4/ah4.ko
ipsec_setup: insmod / lib/modules/2.6.16-1.2115_FC4/kernel/net/ipv4/esp4.ko
ipsec_setup: insmod / lib/modules/2.6.16-1.2115_FC4/kernel/net/ipv4/ipcomp.ko
ipsec_setup: insmod / lib/modules/2.6.16-1.2115_FC4/kernel/net/ipv4/xfrm4_tunnel.ko
ipsec_setup: insmod / lib/modules/2.6.16-1.2115_FC4/kernel/crypto/des.ko
ipsec_setup: insmod / lib/modules/2.6.16-1.2115_FC4/kernel/crypto/aes.ko

Ahora, compruebe que la configuración del sistema están configurados correctamente para utilizar IPsec:

/ usr / local / sbin / ipsec verificar

Comprobar su sistema para ver si IPsec quedó instalado correctamente:

Comprobación de la versión y el ipsec-path

[Aceptar]

Linux Openswan U2.4.6rc3/K2.6.16-1.2115_FC4 (NetKey)

Comprobar la compatibilidad IPsec en el kernel

[Aceptar]

NETKEY detecta, pruebas para discapacitados send_redirects ICMP

[FAILED]

Por favor, desactivar / proc/sys/net/ipv4/conf / * / send_redirects

o NETKEY hará que el envío de las redirecciones ICMP falsos!

NETKEY detecta, pruebas para discapacitados accept_redirects ICMP

[FAILED]

Por favor, desactivar / proc/sys/net/ipv4/conf / * / accept_redirects

o NETKEY aceptará redirecciones ICMP falsos!

Comprobación de clave privada RSA (/ etc / ipsec.secrets)

[Aceptar]

Comprobación de que Plutón se está ejecutando

[Aceptar]

Dos o más interfaces encontraron, comprobando el reenvío de IP

[FAILED]

Comprobación de comando 'ip'

[Aceptar]

Comprobación de comando 'iptables'

[Aceptar]

Soporte de cifrado oportunista

[Disabled]

Asegúrese de investigar cualquier elemento que aparece como

FALLIDO

. El ejemplo anterior muestra que usted necesitará

deshabilita el paso al igual que aceptar el redireccionamiento de ICMP y activar el reenvío IP. Para deshabilitar las redirecciones ICMP,

ejecute los siguientes comandos:

for f in / proc/sys/net/ipv4/conf / * / accept_redirects; hacer echo 0> $ f; hecho

for f in / proc/sys/net/ipv4/conf / * / send_redirects; hacer echo 0> $ f; hecho

Para desactivar el reenvío IP, ejecute la siguiente:

echo 1> / proc/sys/net/ipv4/ip_forward

Ahora, compruebe la configuración de nuevo para asegurarse de que todo se muestra como

Bueno

:

/ usr / local / sbin / ipsec verificar

Comprobar su sistema para ver si IPsec quedó instalado e iniciado correctamente:

Comprobación de la versión y el ipsec-path

[Aceptar]

Linux Openswan U2.4.6rc3/K2.6.16-1.2115_FC4 (NetKey)

Comprobar la compatibilidad IPsec en el kernel

[Aceptar]

NETKEY detecta, pruebas para discapacitados send_redirects ICMP

[Aceptar]

NETKEY detecta, pruebas para discapacitados accept_redirects ICMP

[Aceptar]

Comprobación de clave privada RSA (/ etc / ipsec.secrets)

[Aceptar]

Comprobación de que Plutón se está ejecutando

[Aceptar]

Dos o más interfaces encontraron, comprobando el reenvío de IP

[Aceptar]

Comprobación de NAT y MASQUERADEing
[N / A]
Comprobación de comando 'ip'
[Aceptar]
Comprobación de comando 'iptables'
[Aceptar]
Soporte de cifrado oportunista
[Disabled]
Ahora, usted puede seguir adelante con la tarea de configurar Openswan. de Openswan se controla la configuración por dos archivos de configuración: / etc / ipsec.conf y / etc / ipsec.secrets . El ipsec.conf archivo rompe una VPN conexión en segmentos derecho e izquierdo, Esto es simplemente una división lógica el segmento de la izquierda puede ser la interna o la red externa; esto permite que el mismo archivo de configuración que se utilizará para ambos extremos de un túnel de red-a-red VPN, ahora, comience con una sencilla ipsec.conf para probar Openswan. Adición de una entrada como esta crea un túnel cifrado entre dos:
conn-host-to-host
izquierda = 192.168.0.64
leftid = @ colossus.nnc
# Leftnexthop =% defaultroute
derecha = 192.168.0.62
rightid = @ spek.nnc
# Rightnexthop =% defaultroute
auto = añadir
Esto funcionará si los hosts están ambos en la misma red si no lo son, puede desconectar la
Leftnexthop y rightnexthop entradas para propósitos de autenticación, esta conexión utiliza RSA
firmas, que se obtienen mediante la ejecución
/ Usr / local / sbin / ipsec showhostkey

en ambos ejércitos inicie sesión en el host que ha especificado para izquierda, ejecute el comando siguiente y, a continuación, pega el resultado en su archivo de configuración:

/ usr / local / sbin / ipsec showhostkey - izquierda
RSA 2192 bits de
colossus.nnc
Jue Jul 13 20:48:58 2019
leftrsasigkey =
0sAQNpOndA2SO5aQnEmxqlM5c3JerA9cMwGB0wPE9PshVFBgY44
Ml8Lw7usdMzZTMNaSeXu3 80
fK7aXWqBGVXWpIEw2EAFlGcbg1mrEoAVpLwbpM7ZmZPr6Cl0A
dFyTFxFK4k52y702h6xsdSoeTWabs2vkzPLDR8QqvlzIzPkDHE + MQG4q / F +
fVUkn/TNeGL7ax
xfVkepqTHI1nwbNsLdPXdWGKL9c28ho8TTSgmVMgr9jVLYMNwWjN/BgKMF5J/g
lALr6kjy19u
NEpPFpcq9d0onjTMOts1xyfj0bst2 + + IMufX21ePuCRDkWuYsfcTMlo7o7Cu
alW0AP4mZHz8Z
e8PzRm9h3oGrUMmwCoLWzMeruud

Ahora, la clave para pegar en el derecho acoger al ingresar en él y ejecutar el mismo comando, este tiempo de reemplazar – Izquierda con - A la derecha, copie el archivo de configuración para ambos anfitriones y reinicie el ipsec servicio en ambos sistemas:

/ / init.d / ipsec etc
ipsec_setup: Detener Openswan IPsec ...
ipsec_setup: Comenzando Openswan IPsec 2.4.6rc3 ...
ipsec_setup: insmod / lib/modules/2.6.16-1.2115_FC4/kernel/net/key/af_key.ko
ipsec_setup: insmod / lib/modules/2.6.16-1.2115_FC4/kernel/net/ipv4/xfrm4_tunnel.ko

A continuación, cree la conexión IPsec, ejecute el comando siguiente en uno de los ejércitos;

/ usr / local / sbin / auto ipsec locales - hasta host-to-host

Página 307

104 # "host-to-host" 6: STATE_MAIN_I1: iniciar

003 # "host-to-host" 6: recibida la carga útil ID de proveedor [Openswan (esta versión) 2.4.6rc3

X.509-1.5.4 PLUTO_SENDS_VENDORID PLUTO_USES_KEYRR]

003 # "host-to-host" 6: recibida la carga útil ID de proveedor [Dead Peer Detection]

003 # "host-to-host" 6: Método de carga útil recibida Vendor ID [RFC 3947] ajustado = 110

106 # "host-to-host" 6: STATE_MAIN_I2: envió MI2, esperando MR2

03 # "host-to-host" 6: NAT-Traversal: Resultado usando 3: no NAT detectado

108 # "host-to-host" 6: STATE_MAIN_I3: envió MI3, esperando MR3

04 "host-to-host" # 6: STATE_MAIN_I4: ISAKMP SA establecida {auth = OAKLEY_RSA_SIG

cipher = oakley_3des_cbc_192 prf = oakley_md5 grupo = modp1536}

117 # "host-to-host" 7: STATE_QUICK_I1: iniciar

004 # "host-to-host" 7: STATE_QUICK_I2: enviado QI2, IPsec SA establecida {ESP => 0x070009a9

<0xca6c0796 xfrm = AES_0-HMAC_SHA1 NATD = ninguno DPD = none}

Si quieres poner a prueba tu conexión, ping-uno de los anfitriones en el túnel de la otra:

$ ping-spek.nnc

(192.168.0.62) 56 (84) bytes PING spek.nnc de datos.

64 bytes de spek.nnc (192.168.0.62): icmp_seq = 0 ttl = 64 tiempo = 3,56 ms

64 bytes de spek.nnc (192.168.0.62): icmp_seq = 1 ttl = 64 time = 0.975 ms

64 bytes de spek.nnc (192.168.0.62): icmp_seq = 2 ttl = 64 tiempo = 1,73 ms

64 bytes de spek.nnc (192.168.0.62): icmp_seq = 3 ttl = 64 tiempo = 2,29 ms

...

Ahora, comience tcpdump en el otro host:

/ usr / sbin / tcpdump-n-i eth0

tcpdump: salida detallada suprimido, uso-v o-vv para decodificar protocolo completo escucha en eth0, link-type EN10MB (Ethernet), el tamaño de captura de 96 bytes
23:57:35.280722 IP 192.168.0.43> 192.168.0.62: ESP (spi = 0x070009a9, ss = 0x18)
23:57:35.280893 IP 192.168.0.43> 192.168.0.62: icmp 64: echo solicitud ss 19
23:57:35.280963 IP 192.168.0.62> 192.168.0.43: ESP (spi = 0xca6c0796, ss = 0x18)
23:57:36.267451 IP 192.168.0.43> 192.168.0.62: ESP (spi = 0x070009a9, ss = 0x19)
23:57:36.267451 IP 192.168.0.43> 192.168.0.62: icmp 64: echo solicitud ss 20
23:57:36.269713 IP 192.168.0.62> 192.168.0.43: ESP (spi = 0xca6c0796, ss = 0x19)

Observe los paquetes ESP en la salida el contenido de estos paquetes está cifrados utilizando Ipsec carga de seguridad encapsulada no hay que preocuparse por el eco ICMP (ping) los paquetes que se ve, sin embargo, se presentan porque la pila IPsec de núcleo utiliza la misma interfaz de cifrado y descifrado de paquetes, en lugar de utilizar una interfaz virtual para los paquetes descifrados, si usted es capaz de ver los paquetes procedentes de un tercer huésped, usted verá solamente los ESP. ¡Felicitaciones! todo el tráfico entre los dos ejércitos se han configurado ahora será encriptada sin problemas sin embargo, Openswan tiene muchas configuraciones posibles, tales como red-a-red y host-totúneles de la red, así como el cifrado oportunista sin fisuras, para obtener más información, echa un vistazo a la ipsec.conf página de manual (hombre ipsec.conf), así como los ejemplos en la / etc / ipsec.d / Ejemplos de directorios y en el doc / ejemplos de archivos distribuidos con la fuente Openswan código.

Configuración de IPsec en FreeBSD

Utilice soporte incorporado de IPsec de FreeBSD para asegurar su tráfico.

El uso de IPsec con IKE en FreeBSD necesita habilitar IPsec en el kernel y la instalación de un espacio de usuario programa, mapache, para manejar las

negociaciones IKE. asegúrese de que el núcleo ha sido compilado con las opciones siguientes:

Opciones IPSEC Seguridad IP # Opciones IPSEC_ESP Seguridad # IP (cripto, definir w / IPSEC)

Opciones IPSEC_DEBUG # Debug para la seguridad IP si no es así, tendrá que definirlos y luego reconstruir e instalar el kernel, después de que hacer esto, reiniciar el sistema para comprobar que funciona, puede instalar mapache utilizando la sección de red de la colección de ports o descargándolo de ftp://ftp.kame.net/pub/kame/misc/. Instale mapache según las instrucciones proporcionadas con la distribución en el cliente, primero debe configurar mapache modificando este ejemplo racoon.conf archivo para adaptarse a sus necesidades:

ruta include "/ usr / local / etc / racoon";

ruta pre_shared_key "/ usr / local / etc / racoon / psk.txt"; anónimo remoto {

exchange_mode agresivo, principal;

my_identifier user_fqdn "user1@domain.com";

tiempo de vida de 1 hora;

initial_contact en; propuesta {3des encryption_algorithm; sha1 hash_algorithm; authentication_method pre_shared_key; dh_group 2; } } sainfo anónimo { pfs_group 1; tiempo de vida útil 30 min; 3des encryption_algorithm; hmac_sha1 authentication_algorithm; desinflado compression_algorithm; } en la configuración del cortafuegos, asegúrese que permite conexiones IKE a su máquina (puerto UDP 500), debe configurar mapache para iniciar en tiempo de arranque.

5.3.2.22. Configuración del cliente. El directorio / usr / local / etc / racoon / psk.txt archivo contiene sus credenciales, este fichero debe ser legible por root solamente, si los permisos no se establecen correctamente, mapache no funcionará, para un IPsec compartida secreta conexión, el archivo contiene su identificación (en este caso, el dato del e-mail y clave, en este formato: user1@domain.com supersecret ahora, configure la política de seguridad, el uso de la setkey utilidad para añadir

entradas a la Política de Seguridad kernel Database (SPD), crear un client.spd archivo para setkey para cargar, con entradas como la siguiente:

spdadd 192.168.0.104/32 0.0.0.0 / 0 any-P fuera ipsec \
esp/tunnel/192.168.0.104-192.168.0.1/require;
spdadd 0.0.0.0 / 0 192.168.0.104/32 cualquier-P en ipsec \
esp/tunnel/192.168.0.1-192.168.0.104/require;

Para esta configuración, la estación IP es 192.168.0.104 y la puerta de enlace es 192.168.0.1. La primera entrada se crea una política de seguridad que envía todo el tráfico hacia el punto final de VPN. La segunda entrada se crea una política de seguridad que permite que todo el tráfico de vuelta desde el punto final de VPN.
En esta configuración, el cliente no es capaz de hablar con cualquier host en la subred local, a excepción de la puerta de enlace de VPN, en una red inalámbrica en la que el cliente es un objetivo de primer orden para el ataque, esta es probablemente una buena cosa para su estación de trabajo, cargue el SPD ejecutando el siguiente comando:
setkey-f client.spd
La puerta de enlace racoon.conf es el mismo que el archivo para el lado del cliente, esto permite que cualquier cliente se conecte, el psk.txt archivo debe contener las identificaciones y los secretos compartidos de todos los clientes que se pueden conectar: user1@domain.com supersecret user2@domain.com evenmoresecret user3@domain.com notsosecret

5.3.2.23. Configuración de puerta de enlace. Es neesaesario que se asegure que el psk.txt es legible por sólo root, comience mapache y asegúrese de que no hay errores, por último, establecer un gateway.spd archivo que crea un SPD para cada cliente, el siguiente ejemplo asume sus clientes están en 192.168.0.10 [4-6]:

spdadd 0.0.0.0 / 0 192.168.0.104/32 cualquier-P fuera ipsec \
esp/tunnel/192.168.0.1-192.168.0.104/require;
spdadd 192.168.0.104/32 0.0.0.0 / 0 any-P en ipsec \

esp/tunnel/192.168.0.104-192.168.0.1/require;
spdadd 0.0.0.0 / 0 192.168.0.105/32 cualquier-P en ipsec \
esp/tunnel/192.168.0.1-192.168.0.105/require;
spdadd 192.168.0.105/32 0.0.0.0 / 0 any-P out \
ipsec esp/tunnel/192.168.0.105-192.168.0.1/require;
spdadd 0.0.0.0 / 0 192.168.0.106/32 cualquier-P en ipsec \
esp/tunnel/192.168.0.1-192.168.0.106/require;
spdadd 192.168.0.106/32 0.0.0.0 / 0 any-P fuera ipsec \
esp/tunnel/192.168.0.106-192.168.0.1/require;
Cargue el SPD mediante la emisión de setkey-f gateway.spd
Verifique las entradas SPD utilizando el spddump mando en setkey , en este punto, usted debería ser capaz de hacer ping a un cliente de la puerta de enlace, puede ser que tome un paquete o dos para la negociación VPN para completar, pero la conexión debe ser sólida después de eso si usted no puede hacer ping, examine su syslog salida de errores y advertencias.
Uso de certificado X.509 puede utilizar este certificado con lo que puede realizar autenticación en lugar de una clave previamente compartida, pero si usted es va a hacer esto, primero necesita configurar una entidad emisora de certificados (CA) después de haber hecho modificar su racoon.conf archivo a tener este aspecto: path certificate "/ etc / ssl"; anónimo remoto {exchange_mode principal; tiempo de vida de 1 hora; certificate_type x509 "cletus.crt" "cletus.key"; verify_cert en;
asn1dn my_identifier;
peers_identifier asn1dn;
propuesta {3des encryption_algorithm;
sha1 hash_algorithm;
authentication_method rsasig;
dh_group 2;
}
}
sainfo anónimo

{
pfs_group 1;
tiempo de vida útil 30 min;
3des encryption_algorithm;
hmac_sha1 authentication_algorithm;
desinflado compression_algorithm;
}
Con esta configuración, racoon espera encontrar los certificados X.509 en / etc / ssl, por lo que una copia de su certificado / par de claves (cletus.crt y cletus.key) a la ubicación que decida utilizar, en el resto de sistemas, modificar el archivo de configuración en consecuencia, en sustitución del certificado y los nombres de fichero clave para cada sistema, copie el certificado de la CA en el directorio de certificados, esto será utilizado para verificar que su CA tiene firmado los certificados en cada sistema, si es así, estarán autorizadas a conectarse, se dará cuenta que el certificado de CA no se especifica en cualquier parte del archivo de configuración, esto es porque racoon lo busca en un nombre de archivo el nombre de un hash de la misma para activar mapache para encontrar el certificado CA, ejecute un comando similar al siguiente:
ln-s CA.crt \ Qopenssl x509-noout-hash <CA.crt \ Q.0
El comando anterior supone que se ha copiado su certificado CA a / etc / ssl y la llamó CA.crt.
Reinicie mapache ejecutando / Usr / local / etc / rc.d / reinicio mapache locales. ahora, usted puede comprobarlo haciendo que el host ping entre sí, a continuación, ejecute tcpdump en uno de sus sistemas, debe comenzar a ver ESP paquetes: # tcpdump-n tcpdump: salida detallada suprimido, uso-v o-vv para decodificar protocolo completo escuchando en lnc0, enlace de tipo EN10MB (Ethernet), el tamaño de captura de 96 bytes
03:35:57.481254 IP 192.168.0.40> 192.168.0.41: ESP (spi = 0x05d628a3, ss = 0xd)
03:35:57.483451 IP 192.168.0.41> 192.168.0.40: ESP (spi = 0x0c53fadb, ss = 0xd)
03:35:58.490287 IP 192.168.0.40> 192.168.0.41: ESP (spi = 0x05d628a3, ss = 0xe)

03:35:58.491160 IP 192.168.0.41> 192.168.0.40: ESP (spi = 0x0c53fadb, ss = 0xe)
03:35:59.500509 IP 192.168.0.40> 192.168.0.41: ESP (spi = 0x05d628a3, ss = 0xf)
03:35:59.501289 IP 192.168.0.41> 192.168.0.40: ESP (spi = 0x0c53fadb, ss = 0xf)
Estos son los paquetes de ping en forma encriptada.
Configuración de IPsec en OpenBSD
Utilizar IPsec el camino OpenBSD.
Configuración de IPsec en OpenBSD es bastante fácil, ya que está compilado en el kernel que se incluye con cada
liberar y está activado por defecto. Todo lo que queda por hacer es crear el apropiado
/ Etc / isakmpd / isakmpd.conf y / etc / isakmpd / isakmpd.policy archivos y empezar a isakmpd (la clave IPsecdemonio de administración) esto puede sonar desalentador, pero la configuración de documentación y ejemplo sobresaliente de OpenBSD archivos que sea más fácil de lo que se piensa

5.3.2.24. Autenticación de contraseña. En primer lugar, establecer una contraseña a utilizar para la conexión IPsec, tendrá que poner estas líneas en su / Etc / isakmpd / isakmpd.policy :KeyNote-Version: 2

Autorizador: "POLÍTICA"
Los licenciatarios: "passphrase: squeamishossifrage"
Condiciones: app_domain == "directiva IPsec" &&
esp_present == "sí" &&
esp_enc_alg == "aes" &&
esp_auth_alg == "HMAC-SHA" -> "true";
Ahora, edite el / etc / isakmpd / isakmpd.conf archivo para que contenga las siguientes líneas:
[General]
= Listen-on
10.1.0.11

Compartida SADB =
Definido
Política-File =
/ Etc / isakmpd / isakmpd.policy
[Phase 1]
10.1.0.11 =
ISAKMP-par-oeste
10.1.0.12 =
ISAKMP-peer-este
De fábrica =
ISAKMP-peer-este-agresiva
[Phase 2]
Conexiones =
IPsec-oeste-este
[ISAKMP-peer-al este]
= Fase
1
Dirección local =
10.1.0.11
= Dirección
10.1.0.12
= Configuración
-Main-El modo por defecto
= Autenticación
squeamishossifrage
[ISAKMP-par-oeste]
= Fase
1
Dirección local =
10.1.0.12

= Dirección
10.1.0.11
= Configuración
-Main-El modo por defecto
= Autenticación
squeamishossifrage
[ISAKMP-peer-este-agresivo]
= Fase
1
Dirección local =
10.1.0.11
= Dirección
10.1.0.12
= Configuración
-Agresiva-El modo por defecto = Autenticación squeamishossifrage
[ISAKMP-par-oeste-agresivo] = Fase 1
Dirección local = 10.1.0.12 = Dirección 10.1.0.11 = Configuración -Agresiva-El modo por defecto = Autenticación
squeamishossifrage
[IPsec-este-oeste]
= Fase
2
ISAKMP-par =
ISAKMP-par-oeste
= Configuración
-Quick-El modo por defecto
Local-ID =
Host-este
Remote-ID =
Host-oeste

[IPsec-este-oeste]
= Fase
2
ISAKMP-par =
ISAKMP-peer-este
= Configuración
-Quick-El modo por defecto
Local-ID =
Host-oeste
Remote-ID =
Host-este
[Host-oeste]
ID-type =
IPV4_ADDR
= Dirección
10.1.0.11
[Host-este]
ID-type =
IPV4_ADDR
= Dirección
10.1.0.12
[-Principal del modo predeterminado]
EXCHANGE_TYPE =
ID_PROT
Transforma =
3DES-SHA
[-Agresiva-El modo por defecto]
EXCHANGE_TYPE =
AGRESIVO
Transforma =

3DES-SHA-RSA
[-Quick-mode defecto]
DOI =
IPSEC
EXCHANGE_TYPE =
QUICK_MODE
Suites =
QM-ESP-AES-SHA-PFS-SUITE
El mismo archivo de configuración se puede usar en ambos extremos del túnel, con sólo unos pocos cambios.
En primer lugar, la configuración del ejemplo anterior es para uso en una máquina con una dirección IP de 10.1.0.11.
Usted puede modificarlo para trabajar en el otro extremo (10.1.0.12) cambiando la dirección IP especificada en
:
Escuchar-en
= Listen-on
10.1.0.12
A continuación, cambie el
Defecto
línea a la siguiente:
De fábrica =
ISAKMP-par-oeste-agresiva
Por último, cambiar el
Conexiones
line:
Conexiones =
IPsec-este-oeste
Después de editar los archivos de configuración, puede iniciar isakmpd ejecutando este comando:

/ sbin / isakmpd

A continuación, utilice un host en su túnel de ping al otro host, mientras hace esto, empezar cpdump en uno de los sistemas, debe ver a algunos paquetes ESP:

tcpdump-n

tcpdump: escucha en pcn0, enlace de tipo EN10MB

21:19:38.920316 esp 10.1.0.11> 10.1.0.12 spi 0xB9C862E7 seq 1 len 132

21:19:38.921420 esp 10.1.0.12> 10.1.0.11 spi 0xBC4069F4 seq 1 len 132

21:19:39.926389 esp 10.1.0.11> 10.1.0.12 spi 0xB9C862E7 siguientes 2 len 132

21:19:39.927216 esp 10.1.0.12> 10.1.0.11 spi 0xBC4069F4 siguientes 2 len 132

21:19:40.940115 esp 10.1.0.11> 10.1.0.12 spi 0xB9C862E7 siguientes 3 len 132

21:19:40.940711 esp 10.1.0.12> 10.1.0.11 spi 0xBC4069F4 siguientes 3 len 132

Si desea ver el contenido del paquete descifrado, puede usar tcpdump para supervisar el ENC0 interfaz:

tcpdump-n-i ENC0

tcpdump: ADVERTENCIA: ENC0: ninguna dirección IPv4 asignada

tcpdump: escucha en ENC0, enlace de tipo ENC

21:21:53.281316 (auténtico, confidencial): SPI 0xb9c862e7: 10.1.0.11> 10.1.0.12: icmp:

solicitud de eco (encap)

21:21:53.281480 (auténtico, confidencial): SPI 0xbc4069f4: 10.1.0.12> 10.1.0.11: icmp:

echo reply (encap)

21:21:54.240855 (auténtico, confidencial): SPI 0xb9c862e7: 10.1.0.11> 10.1.0.12: icmp:

solicitud de eco (encap)

21:21:54.241059 (auténtico, confidencial): SPI 0xbc4069f4: 10.1.0.12> 10.1.0.11: icmp:

echo reply (encap)

5.3.2.25. Autenticación de Certificados

La configuración que se muestra en la sección anterior permite que cualquiera pueda conectarse con la contraseña squeamishossifrage, pero lo que se desea utilizar certificados X.509 para la autenticación, para lograr este propósito es necesario establecer una autoridad de certificación (CA) , posteriormente se debe asegurar que cada uno de los certificados tiene un subjectAltName , para que isakmpd pueda identificar lo que el certificado a utilizar para la conexión, si se usan la versión de OpenBSD antes de 3.8, usted puede hacer esto fácilmente con la certpatch herramienta, de lo contrario, tendrá que regenerar los certificados para cada punto final de su firma de certificado peticiones.

Usando certpatch es fácil; usted indica el certificado de modificar, la dirección IP o el dominio completo

nombre (FQDN), y la clave de la CA requerida para firmar el certificado modificado. Si desea modificar un certificado para incluir una dirección IP en el subjectAltName campo, el uso

certpatch de esta manera:

$ certpatch-i 10.1.0.11-k ca.key 10.1.0.11.crt 10.1.0.11.crt

Lectura ssleay creado certificado 10.1.0.11.crt y modificarlo

Ingrese frase PEM:

Creación de Firma: PKEY_TYPE = RSA: X509_sign: 128 OKAY

Escribir nuevo certificado para 10.1.0.11.crt si desea utilizar el nombre completo, ejecutar algo como esto:

$ certpatch-t fqdn-i hinchados-k ca.key puffy.crt puffy.crt

Lectura ssleay creado certificado asdf.crt y modificarlo

Ingrese frase PEM:

Creación de Firma: PKEY_TYPE = RSA: X509_sign: 128 OKAY

Escribir nuevo certificado para puffy.crt para agregar el subjectAltName campo al firmar un certificado, añada -EXTFILE / etc/ssl/x509v3.cnf extensiones x509v3_IPAddr al openssl comando que se utiliza para firmar sus certificados.

Si desea utilizar un nombre de dominio completo en lugar de una dirección IP, reemplace x509v3_IPAddr con x509v3_FQDN. si su CA reside en un sistema no

OpenBSD, tendrá que copiar / etc/ssl/x509v3.cnf a él desde un sistema OpenBSD una vez que haya terminado de añadir el subjectAltName campo, copia de su certificado de CA de / etc / isakmpd / ca a continuación, copie los certificados a / etc / isakmpd / certs en su host correspondiente, del mismo modo, tendrá que copiar las llaves a / etc / isakmpd / private / local.key , después de que haya recibido el certificado de negocio es el momento para modificar su isakmpd.conf y isakmpd.policy archivos en primer lugar, eliminar todo y autenticar líneas en el isakmpd.conf archivo, a continuación, busque las transformaciones línea en la -Main-El modo por defecto sección y cambiarlo para leer 3DES-SHA-RSA_SIG. isakmpd para utilizar los certificados X.509 para la autenticación, a decir isakmpd para permitir que sólo los sistemas que utilizan certificados firmados por el CA para conectar, isakmpd.policy y decirle que el nombre completo (DN) del certificado de CA:

$ openssl x509-sujeto-noout en ca / CA.crt

subject = / C = GB / ST = Berkshire / L = Newbury / O = Mi Company Ltd / CN = CA Root

Luego, vuelva a colocar la linea en su isakmpd.policy :

KeyNote-Version: 2

Comentario: Esta política acepta ESP SA de hosts con certs suscritos por nuestro CA

Autorizador: "POLÍTICA"

Los licenciatarios: "DN: / C = GB / ST = Berkshire / L = Newbury / O = Mi Company Ltd / CN = CA Root"

Condiciones: app_domain == "directiva IPsec" &&

esp_present == "sí" &&

! esp_enc_alg = "null" -> "true";

Finalmente, para tener isakmpd iniciará con cada inicio del sistema, edite el / etc / rc.conf archivo (o crear uno

si no existe) y poner la siguiente línea en él:

isakmpd_flags = ""

Eso debería bastar. Como siempre, verifique sus registros del sistema si su túnel tiene problemas para conectarse.

Cifrar Tráfico Automáticamente con Openswan

Utilice los registros DNS TXT Openswan y crear automáticamente las conexiones cifradas entre
máquinas.

Una característica particularmente fresca apoyado por Openswan es el cifrado oportunista con
otros hosts corriendo Openswan. Esto permite Openswan para cifrar el tráfico de forma transparente entre todos
anfitriones que también soportan encriptación oportunista. Para que esto funcione, cada host debe tener una clave pública
generada a utilizar con Openswan. Esta clave puede entonces ser almacenado en un DNS
TXT
registrar para ese host. Cuándo un host que está configurado para el cifrado oportunista quiere iniciar una conexión cifrada con otro anfitrión, busca la clave pública del host a través de DNS y lo utiliza para iniciar la conexión.

ADVERTENCIA

Antes de empezar, si usted está utilizando un núcleo Linux 2.6.x, asegúrese de que ha instalado Openswan con KLIPS [Hack # 92]
en lugar de apoyar IPsec nativa de Linux. El soporte nativo en el kernel no funciona correctamente con el cifrado oportunista.

Tendrá que generar una clave para cada host con el que se desea utilizar esta función. Por lo general, Openswan crea una clave para usted cuando lo instale. Usted puede comprobar si tiene uno ejecutando el
siguiente comando:

```
# / usr / local / sbin / ipsec showhostkey - izquierda
```

Si usted ve la siguiente salida, tendrá que crear una:

```
showhostkey ipsec: ninguna tecla predeterminada en "/ etc / ipsec.secrets"
```

Usted puede hacer que al ejecutar este comando:

/ usr / local / sbin / ipsec newhostkey - salida - >> / etc / ipsec.secrets

Después, usted necesita para generar un

TXT

registro para poner en su zona DNS, usando un comando como el siguiente:

/ usr / local / sbin / ipsec showhostkey - txt @ colossus.nnc

; RSA 2192 bits de

Coloso Lun Jul 13 03:02:07 2019 IN TXT "X-IPsec-Server (10) = @ colossus.nnc" "

AQOR7rM7ZMBXu2ej/1vtzhNnMayZO1jwVHUyAIubTKpd /

PyTMogJBAdbb3I0xzGLaxadPGfiqPN2AQn76zLIsYFMJnoMbBTDY/2xK1X /

pWFRUUIHzJUqCBIijVWEMLNrIhdZbei1s5 /

MgYIPaX20UL +

yAdxV4RUU3JJQhV7adVzQqEmdaNUnCjZOvZG6m4zv6dGROrVEZmJFP54v6W

hckYf

qSkQu3zkctfFgzJ/rMTB6Y38yObyBg2HuWZMtWI "

"8VrTQqi7IGGHK + +

wSoXer3iFD7JxRTzPOxLk6ihAJMibtKna3j7QP9ZHG0nm7NZ MWK /

L5M9VpK + + Rfe evUUMUTfAtSdlpus2BIeXGWcPfz6rw305H9 "

Añadir este disco a su zona (asegúrese de agregar el nombre de host para el inicio de la grabación) y vuelva a cargarlo por defecto, está desactivado el soporte de encriptación oportunist, para habilitarlo, abierto / etc / ipsec.conf y comente la siguiente línea: include / etc / ipsec.d / examples / no_oe.conf guarde el archivo y, a continuación, reinicie el ipsec servicio ejecutando

/ Etc / init.d / ipsec.

Compruebe que DNS funciona correctamente ejecutando el siguiente comando:

/ usr / local / sbin / ipsec verificar

Comprobar su sistema para ver si IPsec quedó instalado e iniciado correctamente

Comprobación de la versión y el ipsec-path

[Aceptar]

Comprobar la compatibilidad KLIPS en el kernel

[Aceptar]

Comprobación de clave privada RSA (/ etc / ipsec.secrets)

[Aceptar]

Comprobación de que Plutón se está ejecutando

[Aceptar]

Cheques DNS.

Buscando TXT en un mapa a seguir: coloso

[Aceptar]

¿La máquina tiene al menos una dirección que no es privado

[Aceptar]

Ahora, sólo tienes que reiniciar Openswan:

/ / init.d / ipsec etc

Ahora debería ser capaz de conectarse a cualquier otro host que admite el cifrado oportunista. Pero lo que, si otros anfitriones quieren conectar para permitir esto, se tiene que crear un TXT registro para su máquina en la zona DNS inversa: # ipsec showhostkey - txt 192.168.0.64; RSA 2192 bits de coloso

Mar 06 de enero 2019 12:24:27 IN TXT

"X-IPsec-Server (10) = 192.168.0.64" "

AQOR7rM7ZMBXu2ej/1vtzhNnMayZO1jwVHUyAIubTKpd /

PyTMogJBAdbb3I0xzGLaxadPGfiqPN2AQn76zLIsYFMJnoMbBTDY/2xK1X /

pWFRUUIHzJUqCBIijVWEMLNrIhdZbei1s5 /

MgYIPaX20UL +

yAdxV4RUU3JJQhV7adVzQqEmdaNUnCjZOvZG6m4zv6dGROrVEZmJFP54v6W

hckYf

qSkQu3zkctfFgzJ/rMTB6Y38yObyBg2HuWZMtWI "

"8VrTQqi7IGGHK + +

wSoXer3iFD7JxRTzPOxLk6ihAJMibtKna3j7QP9ZHG0nm7NZ MWK /

L5M9VpK + + Rfe evUUMUTfAtSdlpus2BIeXGWcPfz6rw305H9 "

Añadir este registro a la zona inversa para su subred, y otras máquinas serán capaces de iniciar

conexiones con la máquina de cifrado. Con el cifrado oportunista en uso, todo el tráfico entre
los anfitriones serán cifrados automáticamente, protegiendo todos los servicios de forma simultánea. Con buena pinta, ¿no?

Adelantar y Cifrar el Tráfico con SSH

Mantenga el tráfico de red a los puertos arbitrarios seguras con el reenvío de puerto SSH.

Además de proporcionar acceso a una consola remota y la ejecución de comandos, OpenSSH puede reenviar arbitraria
Puertos TCP al otro extremo de la conexión. Esto puede ser extremadamente útil para la protección de correo electrónico, web, o cualquier otro tipo de tráfico que usted necesita para mantener en privado (por lo menos, todo el camino hasta el otro extremo del túnel), SSH lleva a cabo el reenvío de locales mediante la unión a un puerto local, la realización de cifrado, el envío de la cifrado de datos para el extremo remoto de la SSH conexión, y luego descifrar y de enviarlo a la host remoto y puerto especificado, inicie un ssh túnel con el -L (Abreviatura de "local") Interruptor: # ssh-f-N-L 110: mailhost: 110 usuario @ mailhost naturalmente, sustituto usuario con su nombre de usuario y mailhost con e-mail al igual que le servidor IP dirección, tenga presente que tendrá que ser root para este ejemplo, ya que va a enlazar puerto (110, el puerto POP3), también debe deshabilitar cualquier daemon POP3 se ejecuta localmente (busque en / Etc / inetd.conf); de lo contrario, se pondrá en el camino.

Ahora, para cifrar todo su tráfico POP3, configurar el cliente de correo para conectarse a localhost puerto 110 se estará feliz de hablar con mailhost como si estuviera conectado directamente, a excepción de que toda la conversación sera cifrada, alternativamente, usted podría decirle a ssh para que escuche en un puerto por encima de 1024 y eliminar la necesidad de ejecutarlo como root; sin embargo, usted tendría que configurar su cliente de correo electrónico que utilice también este puerto, en lugar de puerto 110, -F horquillas ssh a un segundo plano, y -N dice que no se ejecute en realidad un comando en el extremo remoto, pero sólo para hacer

el envío, una característica interesante cuando se utiliza el -N interruptor es que todavía se puede avanzar un puerto, incluso si usted no tiene un shell de entrada válida en el servidor remoto. Sin embargo, para que esto funcione que necesitará para configurar la autenticación de clave pública con la cuenta de antemano, si el ssh del servidor lo admite, también puede probar el -C cambiar a activar la compresión y reducir significativamente el tiempo que se tarda en descargar el correo electrónico, para acelerar las conexiones aún más, trate de usar el sistema de cifrado Blowfish, que es generalmente más rápido que 3des (por defecto), para utilizar el sistema de cifrado Blowfish, tipo -C pez globo. Puede especificar hasta -L líneas como desee al establecer la conexión. Para también hacia adelante tráfico de correo electrónico saliente, intente lo siguiente: # ssh-f-N-L 110: mailhost: 110-L 25: mailhost: 25 usuario@mailhost Ahora, configure su servidor de correo electrónico saliente a localhost, y el tráfico de correo electrónico se cifrará en cuanto a mailhost . Generalmente, esto es útil sólo si el correo electrónico se dirige a un host interno o si no se puede confiar su conexión de red local (como es el caso con la mayoría de las redes inalámbricas). Obviamente, una vez que su email deja mailhost , que se transmitirá en el claro, a menos que se ha cifrado el mensaje con una herramienta como PGP o GPG.

Si ya está conectado a un host remoto y necesita reenviar un puerto rápido, intente lo siguiente:

1. Pulse Intro.
2. Tipo

C

(No echo).

3. Usted debe estar en un ssh> rápidos; entrar en -L

línea como lo haría desde la línea de comandos.

Por ejemplo:

rob @ catlin: $

rob @ catlin: $ C

ssh> -L8000: localhost: 80

El reenvío de puertos.

Su shell actual entonces delantero portuario local de 8000 a cambio puerto 's 80, como si hubiera entrado en el primer lugar, también puede permitir a otros clientes (a distancia) para conectar a su puerto reenviado, con el -G cambiar, si está conectado a una puerta de enlace remota que sirve como un traductor de direcciones de red para una red privada, utilice un comando como este:

$ ssh-f-g-N-L8000: localhost: 80 10.42.4.6 esto envía todas las conexiones desde un puerto de la pasarela 8000 al puerto host interno 10.42.4.6 's 80. si la puerta de entrada tiene una dirección de Internet en vivo, esto permite que cualquier persona de la red pueda conectar con el servidor web en 10.42.4.6 como si se estuviera ejecutando en el puerto 8000 de la puerta de enlace, un último punto a destacar es que el anfitrión remitido no tiene por qué ser localhost ; puede ser cualquier anfitrión que la máquina que se está conectando puede acceder directamente, por ejemplo, para reenviar puerto local 5150 a un servidor web en cualquier sitio en una red interna, intente lo siguiente: $ ssh-f-N-L5150: intranet.insider.nocat: 80 gateway.nocat.net suponiendo que usted está funcionando en un dominio privado llamado . nocat, y que gateway.nocat.net también tiene una conexión a la red privada, todo el tráfico en el puerto 5150 de la máquina remota será complaciente remitido a intranet.insider.nocat: 80 , la dirección intranet.insider.nocat no tiene que resolver en DNS al host remoto; no se levantó hasta qe la conexión se realiza a Gateway.nocat.net , y luego que es la puerta de enlace que hace la consulta. Para navegar con seguridad que el sitio del host remoto intente conectarse a http://localhost:5150/.

6. CONCLUSIONES

Mediante el desarrollo del trabajo de grado se identificaron formas y tipologías mediante las cuales los atacantes intervienen las redes, lo que permite apreciar un panorama claro de la realidad en la vulnerabilidad de las redes, identificando la forma y manera de establecer herramientas de código abierto que ayuden a conocer, proteger y evitar vulnerabilidades de las redes.

En el proceso de aseguramiento se establecieron 8 puntos de acceso a la red, los cuales cumplían las siguientes características (Ejecución sin participación humana, Fácil acceso remoto, Tener una tolerancia a fallos, Adaptación fácil al SO, debe permitir actualizaciones, Generación de alertas con baja tasa de falsos positivos y falsos negativos).

Para establecer la herramientas más útiles para el análisis y la regulación del tráfico en la red, se evaluó la posibilidad de utiliza Snort o suricata que son utilizadas en el desarrollo de estos modelos, pero estas presentan algunas desventajas, en el caso de snort por ser muy conocida, los atacantes ya se encuentran familiarizados y prevenidos, el análisis en el sistema genera alta notificacion de falsos positivos, en la red lo que puede favorecer que el atacante se camufle con tanto falso positivo realizando un ataque dirigido, en el caso de Suricata presenta inestabilidad en la conexión inalámbrica lo cual se traduce en una vulnerabilidad para la red, en ese sentido se determinó que las herramientas más útiles para el análisis, control y regulación del tráfico de red son (Acunetix, OpenVAS, Wireshark, Nikto, Angry IP Scanner, Advanced IP Scanner, Qualys Frescan, SoftPerfect Network Scanner), debido a que son de carácter libre y de código abierto permitiendo una manejo de información confiable, etc (Evalúan la seguridad de enrutadores, al igual que el escaneo total de la red),

El trabajo con el software (Acunetix) permitió la formulación de protocolos (tales como escaneo de la red, corrección de vulnerabilidades e informe de resultados) que permitieron que se realizara un tránsito completo y seguro en la red.

7. RECOMENDACIONES

Mediante el conocimiento de las diferentes tipologías de ataque se pueden desarrollar protocolos de seguridad informática organizacional en la que cada uno de los colaboradores actúen en la acción de identificación y prevención de los riesgos.

Es de vital importancia que las organizaciones establezcan acciones de aseguramiento informático acorde con su estructura, para establecer los puntos de acceso y vulnerabilidad y de esta manera establecer las acciones de seguridad de la red.

Las organizaciones desde su área de IT pueden hacer uso de herramientas libres de código abierto para el manejo de la información, siempre tomado como base el analisis diagnóstico de la red de la empresa y las necesidades de seguridad requeridos.

Es necesario que a partir del proceso de aseguramiento informático de la organización a partir de la herramienta que para el caso fue el software (Acunetix), se formulen los protocolos que permitan garantizar una red segura que no permita la vulnerabilidad de la información que es el activo más importante de la empresa.

BIBLIOGRAFÍA

ABDELHAMID, Neda; AYESH, Aladdin; THABTAH, Fadi. Phishing detection based associative classification data mining. *Expert Systems with Applications*, 2014, vol. 41, no 13, p. 5948-5959.

ALFARO, Emilio José Mira. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. *Ingeniería Informatica*, 2002.

Anderson, James P. Computer SecurityThreat Monitoring and Surveillance. Fort Whashinton,PA: James P. Anderson Co.1980

AKSU, M. Ugur; ALTUNCU, Enes; BICAKCI, Kemal. A First Look at the Usability of OpenVAS Vulnerability Scanner. En *Workshop on Usable Security (USEC) 2019*. NDSS, 2019.

ALMQUIST, P., & KASTENHOLZ, P. Towards Requirements for IP Routers. Rfc 1716. 1994. [Consultado julio 7 de 2020]. Disponible en: https://doi.org/10.17487/RFC1716

ÁLVAREZ MARAÑÓN, Gonzalo; Pérez García, Pedro Pablo; Seguridad informática para empresas y particulares; McGraw-Hill/ Interamericana, Madrid España. 2014

ARMAS, A. G. De. Malware_Virus Informáticos. Introducción a La Computación. 2008

BARABÁSI, A. L. Network science. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 2013. [Consultado julio 7 de 2020]. Disponible en: https://doi.org/10.1098/rsta.2012.0375.

BARAN, N. Redes Inalámbricas. Redes. 2012

BELISARIO MÉNDEZ, Aymara Noriley. *Análisis de métodos de ataques de Phishing*. 2014. Tesis Doctoral. Universidad de Buenos Aires. Facultad de Ciencias Económicas.

BELLIDO QUINTERO, Enrique. Instalación y configuración de aplicaciones Informáticas Editorial CEP S.L. Madrid España. 2014

BAKER, A. R., BEALE, J., CASWELL, B., & POOR, MSnort 2.1 Intrusion Detection. (2004). Second Edition. Rockland, MA: Syngress Publishing, Inc

BRIDGES, Susan M., et al. Fuzzy data mining and genetic algorithms applied to intrusion detection. En *Proceedings of 12th Annual Canadian Information Technology Security Symposium*. 2000. p. 109-122.

CAMACHO MERA, Byron Patricio. *Sistemas de detección y prevención de intrusos para el control de vulnerabilidades de la red corporativa de la Universidad Regional Autónoma de Los Andes Uniandes*. 2017. Tesis de Licenciatura.

CANNADY, James, et al. A comparative analysis of current intrusion detection technologies. En *Proceedings of the Fourth Technology for Information Security Conference*. 1996.

CALVET, Joan; CAMPOS, Jessy; DUPUY, Thomas. Visiting The Bear Den. *WeLiveSecurity Blog*, 2016.

CARTER, Michael. *A Review of Transport Protocols as Candidates for use in a Tactical Environment*. DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURG (AUSTRALIA) INFORMATION NETWORKS DIV, 2005.

CISCO INC. Informe anual de seguridad de 2014

CISCO INC. Informe anual de seguridad de 2018

CHESWICK, William Roberts; WHITTEN, Edward G. *Firewall security method and apparatus*. U.S. Patent Application No 09/047,207, 6 Feb. 2001.

CHICANO TEJADA, Ester; Gestión de incidentes de seguridad informática. IC Editorial. Antequera Málaga. 2014

CHUANG, S.-T., KESLASSY, I., YU, K., SOLGAARD, O., HOROWITZ, M., MCKEOWN, N., & MILLER, D. Scaling internet routers using optics. 2003 [Consultado julio 7 de 2020]. Disponible en: https://doi.org/10.1145/863977.863978

CORONA, I., ARIU,D. & GIACINTO,G. “HMM-Web: A framework for the detection of attacks against web applications,” in Proceedings of the 2009 IEEE International Conference on Communications, ICC'09, pp. 1–6, IEEE. 2009

CORTÉS HERNÁNDEZ, Andrés Mauricio. Ingenieria social Phishing y Baiting. 2019.

DARWICHE, Adnan. Bayesian networks. *Communications of the ACM*, 2010, vol. 53, no 12, p. 80-90.

DEBORAH REYES Roig Guía de implementación de la seguridad en redes de núcleos MPLS La Habana Cuba. 2010

DEERING, S. E., & CHERITON, D. R. Multicast routing in datagram internetworks and extended LANs. ACM Transactions on Computer Systems 2002. [Consultado julio 7 de 2020]. Disponible en: https://doi.org/10.1145/78952.78953

Denning Dorothy E. An intrusión Detection Model.Proceedings of the 1986 IEE Symposium on Secutity and Privacy, Oakland, CA, April 1986

DE LA HOZ FRANCO, E., DE LA HOZ CORREA, E. M., ORTIZ, A., & ORTEGA, J. Modelo de detección de intrusiones en sistemas de red, realizando selección de características con FDR y entrenamiento y clasificación con SOM. INGE CUC. 2012.

Díaz Vizcaíno, L.M. (2005). Sistemas de Detección de Intrusos. Tomado de. Universidad Carlos III de Madrid. Sitio Web: http://www.it.uc3m.es/~lmiguel/ids2.pdf

DOMINGUEZ, Antonio Hernández. Sistema para la detección de ataques PHISHING utilizando correo electrónico. *Telemática*, 2019, vol. 17, no 2, p. 60-70.

DONG, G., J. GAO, R. DU, L. TIAN, et al., Robustness of network of networks under targeted attack. Physical Review E, 87(5), 052804. 2013

DONGO QUINTANA, A. D. relación entre los virus informáticos (malware) y ataques en países vulnerables de seguridad en informática utilizando análisis de componentes principales (Acp). Logos 2017. [Consultado julio 7 de 2020]. Disponible en: https://doi.org/10.21503/log.v6i1.1316

DOKAS, Paul, et al. Data mining for network intrusion detection. En *Proc. NSF Workshop on Next Generation Data Mining*. 2002. p. 21-30.

ESCRIVÁ GASCO, Gema; ROMERO SERRANO, Rosa María; Rama Introducción a la Seguridad Informática. Editorial Macmillan Iberia, S.A Madrid España. 2015

FERRANDO GUILLEM, Anna Lourdes. La ciberseguridad como reto internacional: la protección frente a las ciberamenazas.

FERNÁNDEZ REGALADO, Raúl. El teorema de Bayes y su utilización en la interpretación de las pruebas diagnósticas en el laboratorio clínico. *Revista cubana de investigaciones biomédicas*, 2009, vol. 28, no 3, p. 158-165.

FUCHSBERGER, A. Sistema de detección de intrusiones y sistemas de prevención de intrusiones. Informe técnico de seguridad de la información 2005 pp 34, 134-139

FULP, E. W. Firewalls. In Managing Information Security: Second Edition. 2013. [Consultado julio 13 de 2020]. Disponible en: https://doi.org/10.1016/B978-0-12-416688-2.00006-4

GARRIDO, Fabián Blanco; MOYANO, Eduardo Triana; CARRANZA, Juan Fernando Velásquez. TANATALOGÍA DIGITAL: MÁXIMA EXPRESIÓN DE LA SEGURIDAD INFORMÁTICA.

González Gómez, D. Sistema de Detección de intrusos. 2013 tomado de https://dgonzalez.net/papers/ids/ids_v1.0.pdf

GIMÉNEZ ALBACETE, José Francisco; Seguridad en equipos informáticos. IC Editorial, Málaga España. 2014

GIMENEZ GARCIA, M. I. Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral. Vasa. 2008

GIRALDO MARTÍNEZ, Jenny Paola, et al. Ingeniera social: Técnica de ataque Phishing y su impacto en las empresas colombianas.

GOLLMANN, D. "Securing Web applications," Information Security Technical Report, vol. 13, no. 1, pp. 1–9, View at Publisher. 2008

GOLLAKOTA, S., PERLI, S. D., & KATABI, D. Interference alignment and cancellation. ACM SIGCOMM Computer Communication Review 2009. [Consultado julio 13 de 2020]. Disponible en: https://doi.org/10.1145/1594977.1592588

GÓMEZ VIEITES, Álvaro; Gestión de incidentes de seguridad informática. Editorial RA_MA, Madrid España. 2014

GÓMEZ VIEITES, Álvaro; Seguridad en equipos informáticos. Editorial RA_MA, Madrid España. 2014

GRIFFIN, Slade E.; RACKLEY, Casey C. Vishing. En *Proceedings of the 5th annual conference on Information security curriculum development*. 2008. p. 33-35.

GUPTA, M. Hybrid Intrusion Detection System: Technology and Development. (2015). International Journal of Computer Applications IJCA, 5-8

GUANGXIAN. JI.The Development Of Intrusion Detection System Based On Wavelet Network. (2012). INTERNATIONAL JOURNAL ON Advances in Information Sciences and Service Sciences. 4. 261-268. 10.4156/aiss.vol4.issue9.32.

GUANGXIAN, Ji. A Novel SIP Protocol Stack for IMS Network [J]. *Telecommunications Science*, 2012, vol. 28, no 4, p. 90-98.

HAY, A., & CID, D.. OSSEC host-based intrusion detection guide. (2008) Burlington, Mass.: Syngress Pub.

HECKERMAN, David. A tutorial on learning with bayesian networks. Microsoft Research. 1995.

HEADY, R., G. LUGER, A. MACCABE AND M. SERVILLA The architecture of a network-level intrusion detection system. Edtion ed.: Department of Computer Science, College of Engineering, University of New Mexico, 1990

HOSMER, H. Security is fuzzy: applying the fuzzy logic paradigm to the multipolicy paradigm (1993). Proceedings of 1992-1993 Workshop on New Security Paradigms, 175-184, Little Compton

HU, H., MYERS, S., COLIZZA, V., & VESPIGNANI, A. WiFi networks and malware epidemiology. Proceedings of the National Academy of Sciences. 2009. [Consultado Agosto 8 de 2020]. Disponible en: https://doi.org/10.1073/pnas.0811973106.

ICONTEC. Norma IEC 27001. Tecnología de información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.2013. Bogotá: Icontec

INEC. Tecnologías de la Información y Comunicaciones. Educación 2014. [Consultado agosto 8 de 2020]. Disponible en: https://doi.org/10.4321/S1575-18132004000200004.

IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016. [Consultado agosto 8 de 2020]. Disponible en: https://doi.org/10.1109/WiSPNET.2016.7566486

ISKANDAR, Akbar; VIRMA, Elisabet; AHMAR, Ansari Saleh. Implementing DMZ in improving network security of web testing in STMIK AKBA. *arXiv preprint arXiv:1901.04081*, 2019.

JAIN, L. C. Intelligent biometric techniques in fingerprint and face recognition. CRC Press. 1999. [Consultado agosto 8 de 2020]. Disponible en: https://www.researchgate.net/publication/28222432_Aplicacion_del_NFIS_Nist_Fingerprint_Image_Software_para_la_extraccion_de_caracteristicas_de_huellas_dactilares

JAVITZ, Harold S., et al. The SRI IDES Statistical Anomaly Detector. En *IEEE Symposium on Security and Privacy*. 1991. p. 316-326.

JIMÉNEZ, Gonzalo Ramos; MUÑOZ, Javier López. ALGORITMO DE APRENDIZAJE INDUCTIVO BORROSO.

KELSEN, Hans. *Teoría general del derecho y del Estado*. Unam, 1958.

KENKRE, Poonam Sinai; PAI, Anusha; COLACO, Louella. Real time intrusion detection and prevention system. En *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*. Springer, Cham, 2015. p. 405-411.

KARTHIKA, K. C. Wireless mesh network: A survey. In Proceedings of the 2016

KRÜGEL, Christopher; TOTH, Thomas; KIRDA, Engin. Service specific anomaly detection for network intrusion detection. En *Proceedings of the 2002 ACM symposium on Applied computing*. 2002. p. 201-208.

LIAO, Hung-Jen, et al. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 2013, vol. 36, no 1, p. 16-24.

LIU, A. X., & GOUDA, M. G. Firewall policy queries. IEEE Transactions on Parallel and Distributed Systems. 2009. [Consultado agosto 8 de 2020]. Disponible en: https://doi.org/10.1109/TPDS.2008.263

LIU, A. X., & GOUDA, M. G. Diverse firewall design. IEEE Transactions on Parallel and Distributed Systems.2008. [Consultado agosto 8 de 2020]. Disponible en: https://doi.org/10.1109/TPDS.2007.70802

LYU, Michael R.; LAU, Lorrien KY. Firewall security: Policies, testing and performance evaluation. En *Proceedings 24th Annual International Computer Software and Applications Conference. COMPSAC2000*. IEEE, 2000. p. 116-121.

LÓPEZ, Julio Gómez. *Optimización de sistemas de detección de intrusos en red utilizando técnicas computacionales avanzadas*. Universidad Almería, 2009.

MAIRH, Abhishek, et al. Honeypot in network security: a survey. En *Proceedings of the 2011 international conference on communication, computing & security*. 2011. p. 600-605

MARTÍNEZ., Evelio Topologías de red 2007.

MARTINEZ, Guillermo Roberto Solarte; OCAMPO, Carlos Alberto; BERMÚDEZ, Yanci Viviana Castro. Sistema de detección de intrusos en redes corporativas. *Scientia et technica*, 2017, vol. 22, no 1, p. 60-68.

MUKKAMALA, S., JANOSKI, G., AND SUNG, A.. Intrusion detection using neural networks and support vector machines. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), volume 2, 2002

NET OPTICS, INC.: “Fiber Tap singlemode and multimode Gigabit”, 2002. [Consultado agosto 18 de 2020]. Disponible en: http://www.netoptics.com/11.html,

OBAIDAT, M. S., PAPADIMITRIOU, G. I., & OBEIDAT, S. Wireless LANs. In Handbook of Computer Networks 2011. [Consultado agosto 18 de 2020]. Disponible en: https://doi.org/10.1002/9781118256114.ch57

OCAMPO, C. A., VIVIANA, BERMÚDEZ, C., & SOLARTE MARTÍNEZ, G. R. Sistema de detección de intrusos en redes corporativas Intrusion Detection System in Corporate Networks. Scientia et Technica Año XXII. 2017

OSSEC, [sitio web] [Consultado julio 22 de 2020] disponible en: https://www.ossec.net/

PAPPAS, N. SANS Institute InfoSec Reading Room. (April, 2008). Network IDS & IPS deployment strategy [White paper]]

PATEL, R. THAKKAR A AND. GANATRA; A. A Survey and Comparative Analysis of Data Mining Techniques for Network Intrusion Detection Systems, International Journal of Soft Computing and Engineering (2012).

PAXSON v, et al. Framework for IP Performance Metrics. IETF RFC2330. (1998.).

POZAS, R. El desarrollo de comunidades técnicas de investigación social. 2 Ed. UNAM México. 1979

PRASITHSANGAREE, P., KRISHNAMURTHY, P., & CHRYSANTHIS, P. K. On indoor position location with wireless lans. In IEEE International Symposium on PERSONAL, Indoor and Mobile Radio Communications, PIMRC. 2002. [Consultado agosto 18 de 2020]. Disponible en: https://doi.org/10.1109/PIMRC.2002.1047316

PTACEK, T.H., NEWSHAM, T.N.: “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection”. Secure Networks, Inc. 1998.

PORTNOY, L. ESKIN, E. and STOLFO. S.J. Intrusion detection with unlabeled data using clustering. In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA2001), pages 76–105. Philadelphia, PA, 2001.

PULIDO VELANDIA, Giovanni Andrés. Sistema de control de acceso para la administración y seguridad de equipos de red. 2016.

RAMAKRISHNAN, K., & FLOYD, S.. A Proposal to add Explicit Congestion Notification (ECN) to IP 1999. Rfc. [Consultado agosto 18 de 2020]. Disponible en: https://doi.org/10.17487/rfc2481

RANGEL SOSA, Karen Irlanda, et al. Rastreo de correos electrónicos. 2017.

RIVERO PÉREZ, J. L. Técnicas de aprendizaje automático para la detección de intrusos en redes de computadoras. Revista Cubana de Ciencias Informáticas,8(4), 52-73. 2014

ROMERO CASTRO, V. F., MURILLO QUIMIZ, L. R., CAMPOZANO PILAY, Y. H., AZÚA MENÉNDEZ, M. D. J., REGALADO JALCA, J. J., PARRALES ANZÚLES, G. R., & PIN PIN, Á. L. Redes de computadoras. 2018. [Consultado agosto 18 de 2020]. Disponible en: https://doi.org/10.17993/ingytec.2018.32

ROSIQUE, Antonio Sola; MÁRQUEZ, Adolfo Crespo. *Principios y marcos de referencia de la gestión de activos*. AENOR-Asociación Española de Normalización y Certificación, 2016.

RUBIO NAVARRO, Antonio Maria. Aspectos prácticos de la protección de datos de las personas físicas. Barcelona J.M. Bosh editor. 2004

RUEDA, F. ¿Qué es la computación en la nube? Sistemas.2009

RUIZ HOUSEHOLDER, Adrián; CANDIL VIZCAÍNO, Daniel; SÁNCHEZ-MARISCAL GONZÁLEZ, Guillermo. Detección de intrusos basada en Host (HIDS)-OSSEC. 2020.

SABAHI F. AND MOVAGHAR A. “Intrusion Detection: A Survey,” in 2008 Third International Conference on Systems and Networks Communications, 2008, pp. 23-26.

SANTOS GONZALES, Manuel. Diseño de redes telemáticas Editorial RA-MA. Madrid España. 2014.

SAN MARTIN GONZALES, Enrique, Salvaguarda y seguridad de los datos administración de bases de datos Editorial IC. Málaga España. 2014

SAUNDERS, G., HITCHENS, M. & VARADHARAJAN, V. “Role-based access control and the access control matrix,” ACM SIGOPS Operating Systems Review, vol. 35, no. 4, pp. 6–20, .2001

SHARMA, Sanjay; GUPTA, R. K. Intrusion detection system: A review. *International Journal of Security and Its Applications*, 2015, vol. 9, no 5, p. 69-76.

SENDIN ESCALONA, Albert. Fundamentos de los sistemas de comunicaciones. McGraw-Hill. 2014

SHIRALI-SHAHREZA, S., & GANJALI, Y. FLEXAM: flexible sampling extension for monitoring and security applications in openflow. of the Second ACM SIGCOMM Workshop 2013. [Consultado agosto 25 de 2020]. Disponible en: https://doi.org/10.1145/2491185.2491215

SMALL BUSINESS TREND. Cyber Security Statistics: Numbers Small Businesses Need to Know 2017. . [Consultado agosto 18 de 2020]. Disponible en: https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

Smaha Steve E. An Intrusion Detection System for the Air Force. Proceedings of the Fourth Aurospace Conputer Security Aplications conference, Orlando FL, December 1998.

Snapp, S.R. et Al. DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early prototype, proceedings of the Fifteenthe National Computer Security Conference, Baltimore, MD, October 1992.

Solarte Martinez, G., Ocampo, C., & Castro Bermúdez, Y. Sistema de detección de intrusos en redes corporativas. 2017. *Scientia Et Technica*, *22*(1), 60-68. https://doi.org/10.22517/23447214.9105

SRI internacional. System Design Laboratory. Intrusión Detection [en línea] fecha no disponible. Disponible en internet en http://www.csl.sri.com/programs/intrusion/history.html

Spafford, Eugene H. The Internte Worm: Crisis and Aftermath; communications of the ACM; 32(6): 678-687, June 1989.

STALLMAN, Richard. On hacking. *Retrieved April*, 2002, vol. 30, p. 2009.

STANEK, William R. SQL Server Manual del Administrador McGraw-Hill Ciudad de México. 2007

STAKHANOVA, Natalia; BASU, Samik; WONG, Johnny. A taxonomy of intrusion response systems. *International Journal of Information and Computer Security*, 2007, vol. 1, no 1-2, p. 169-184.

STALLINGS, William. Comunicaciones y Redes de Computadores. Pearson Prentice Hall. 2004.

STALLINGS, William. Redes de ocomunicación: Topología y enlaces. Creative Commons. 2013. Consultado agosto 25 de 2020]. Disponible en: https://doi.org/10.1017/CBO9781107415324.004.

TANACHAIWIWAT, Sapon; HWANG, Kai; CHEN, Yue. Adaptive intrusion response to minimize risk over multiple network attacks. *ACM Trans on Information and System Security*, 2002, vol. 19, no 1-30, p. 95-96.

TOMBINI,E., DEBAR,H., MÉ, L.,et al., “A serial combination of anomaly and misuse IDSes applied to HTTP traffic,” in Proceedings of the 20th Annual Computer Security Applications Conference, pp. 428–437, IEEE, 2004.

TESAVIS, Carl; BERNSTEIN, Lawrence; OLIVER, James. *Network scanner interface*. U.S. Patent Application No 10/834,452, 3 Nov. 2005.

VAN DEN BERG, Jan. MODELING FANCY BEAR CYBER ATTACKS. 2017.

VARGAS, IGNACIO ALVAREZ; SIEMENS, S. Seguridad en Redes Industriales. 2013.

VIEITES, Álvaro Gómez. *Enciclopedia de la seguridad informática*. Grupo Editorial RA-MA, 2011.

VELTE, Toby J & VELTE, Anthony T. Manual de Cisco McGraw-Hill/Osborne. 2012

VILLALBA, L. J. G., OROZCO, A. L. S., & VIDAL, J. M. Anomaly-based network intrusion detection system. IEEE Latin America Transactions, 13(3), 850-855. 2015

WIRYAWAN, Drajad, et al. Implementation of the Acunetix for Testing the Banking Website (Owned by the government and non-government in Indonesia). *International Information Institute (Tokyo). Information*, 2016, vol. 19, no 6A, p. 1785.

YADAV, Ajay. Network Design: Firewall, IDS/IPS. Infosec Institute, 2018, p. 5-9. Disponible en línea https://resources.infosecinstitute.com/topic/network-design-firewall-idsips/#gref

YING, Lin & Yan, Zhang & Yang-jia, Ou. (2010). The Design and Implementation of Host-Based Intrusion Detection System. 3rd International Symposium on Intelligent Information Technology and Security Informatics, IITSI 2010. 595 - 598. 10.1109/IITSI.2010.127.

ZELST, A. VAN. MIMO OFDM for Wireless LANs. Geboren Te Waalwijk.2004.

ANEXOS

ANEXO A. RAE

Fecha de Realización:	23/12/2020
Programa:	Especialización en seguridad informática
Línea de Investigación:	Infraestructura tecnológica y seguridad de redes
Título:	Definición de un sistema de detección y prevención de intrusos en una red para el control de vulnerabilidades usando software libre.
Autor(es):	Juan Pablo Ortegón Criollo
Palabras Claves:	Software, DDoS, CEO, IDS, IPS, IPSEC, SSH.
Descripción:	Lograr una red segura no es tarea fácil, implica le usos de recursos económicos, humanos y tecnológicos, en ese sentido se realiza el estudio del uso de Software Libre para el análisis e implementación de la seguridad en una red. Se analizan alternativas de uso de diferentes programas que en su conjunto hacen una red segura, con seguridad robusta por que se abarcando aspectos puntuales, dificultando el acceso a los intrusos y diseñando estrategias para prevenir, eliminar o contrarrestar la intrusión, las herramientas que se estudiaron para el análisis, control y regulación del tráfico de red son Acunetix, OpenVAS, Wireshark, Nikto, Angry IP Scanner, Advanced IP Scanner, Qualys Frescan, SoftPerfect Network Scanner, debido a que son de carácter libre y de código abierto permitiendo una manejo de información confiable.
Fuentes bibliográficas destacadas: ÁLVAREZ MARAÑÓN, Gonzalo; Pérez García, Pedro Pablo; Seguridad informática para empresas y particulares; McGraw-Hill/ Interamericana, Madrid España. 2014 BELISARIO MÉNDEZ, Aymara Noriley. Análisis de métodos de ataques de Phishing. 2014. Tesis Doctoral. Universidad de Buenos Aires. Facultad de Ciencias Económicas. CISCO INC. Informe anual de seguridad de 2018	

DE LA HOZ FRANCO, E., DE LA HOZ CORREA, E. M., ORTIZ, A., & ORTEGA, J. Modelo de detección de intrusiones en sistemas de red, realizando selección de características con FDR y entrenamiento y clasificación con SOM. INGE CUC. 2012.
DOMINGUEZ, Antonio Hernández. Sistema para la detección de ataques PHISHING utilizando correo electrónico. Telemática, 2019, vol. 17, no 2, p. 60-70.
GIMENEZ GARCIA, M. I. Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral. Vasa. 2008
GÓMEZ VIEITES, Álvaro; Gestión de incidentes de seguridad informática. Editorial RA_MA, Madrid España. 2014
GÓMEZ VIEITES, Álvaro; Seguridad en equipos informáticos. Editorial RA_MA, Madrid España. 2014
OCAMPO, C. A., VIVIANA, BERMÚDEZ, C., & SOLARTE MARTÍNEZ, G. R. Sistema de detección de intrusos en redes corporativas Intrusion Detection System in Corporate Networks. Scientia et Technica Año XXII. 2017
OSSEC, [sitio web] [Consultado julio 22 de 2020] disponible en: https://www.ossec.net/
SMALL BUSINESS TREND. Cyber Security Statistics: Numbers Small Businesses Need to Know 2017.[Consultado agosto 18 de 2020]. Disponible en: https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

Contenido del documento:	El trabajo se compone de 7 partes. Las tres primeras partes abordar la formulación y justificación del problema junto con los objetivos a desarrollar en el estudio. La cuarta parte está conformada por le marco referencia que contiene marco teórico, conceptual, Antecedentes, marco legal y un marco metodológico. En la quinta parte se inicia el desarrollo de los objetivos del estudio realizando los analisis correspondientes a las herramientas seleccionadas. La sexta y séptima partes aborda la recomendación y conclusiones del estudio.
Conceptos adquiridos:	Conocimiento de las diferentes tipologías de ataque que permite el desarrollo de protocolos de seguridad informática en las organizaciones Identificar las acciones de aseguramiento informático en relación con la estructura de red, estableciendo puntos de control, acceso y vulnerabilidad.

	Es posible establecer sistemas de detección de intrusiones con el uso de herramientas libres y de condigo abierto generando una red robusta con seguridad informática.
Conclusiones:	Identificación de tipologías y formas en que son atacadas las redes Definición de un proceso de aseguramiento de 8 puntos de acceso a la red, los cuales cumplían las siguientes características (Ejecución sin participación humana, Fácil acceso remoto, Tener una tolerancia a fallos, Adaptación fácil al SO, debe permitir actualizaciones, Generación de alertas con baja tasa de falsos positivos y falsos negativos). Definición del uso de la herramienta para el análisis, control y regulación del tráfico de red como Acunetix, OpenVAS, Wireshark, Nikto, Angry IP Scanner, Advanced IP Scanner, Qualys Frescan, SoftPerfect Network Scanner, debido a que son de carácter libre y de código abierto permitiendo un manejo de información confiable, Evalúan la seguridad de enrutadores, al igual que el escaneo total de la red El trabajo con el software (Acunetix) permitió la formulación de protocolos tales como escaneo de la red, corrección de vulnerabilidades e informe de resultados, que permitieron que se realizara un tránsito completo y seguro en la red.