DISEÑO DE UN SISTEMA DE SEGURIDAD PARA LA PROTECCIÓN Y PREVENCIÓN DE INTRUSOS IDS/IPS EN LA RED EMPRESARIAL DE PUNTOQOM MINIMIZANDO EL RIESGO Y ASEGURANDO LOS ACTIVOS DE INFORMACIÓN DE LA ORGANIZACIÓN

DIEGO ALEJANDRO CARDENAS RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2022

DISEÑO DE UN SISTEMA DE SEGURIDAD PARA LA PROTECCIÓN Y PREVENCIÓN DE INTRUSOS IDS/IPS EN LA RED EMPRESARIAL DE PUNTOQOM MINIMIZANDO EL RIESGO Y ASEGURANDO LOS ACTIVOS DE INFORMACIÓN DE LA ORGANIZACIÓN

DIEGO ALEJANDRO CARDENAS RODRIGUEZ

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

Edgar Mauricio Lopez Rojas
Director de Trabajo de Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 20 septiembre 2022

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

RED DATOS: Son aquellas implementadas para transmitir información a través de paquetes que son enviadas sobre infraestructura creada para tal fin dependiendo de la distancia sobre la cual se desea enviar la información.

VULNERABILIDADES: Son aquellas debilidades o falencias sobre un sistema y la cual puede llegar a ser utilizada en beneficio propio por un atacante con el fin de afectar, robar o dañar el sistema o información.

IPS: Sistema de prevención de intrusos, como su nombre lo indica es una herramienta de seguridad informática cuyo fin es el de proteger sistemas de información ante intentos de ataques e intentos de ingresos no autorizados, actuando en tiempo real cuando es detectado un comportamiento anómalo y bloqueándolo como medida de protección.

MALWARE: Es la definición dada a un programa de informática cuya finalidad es la de generar daño, con el objetivo de causar daño, robar o interceptar información de gran importancia para una organización.

FIREWALL: Es un dispositivo diseñado para proteger la seguridad de una red interna ante ingresos o conexiones no permitidas a través del bloqueo de las mismas, mediante el uso de reglas que permiten la entrada y salida del mismo siempre y cuando se cumpla con las condiciones establecidas.

IDS: Sistema de detección de intrusos, son herramientas utilizadas para monitorear el tráfico e identificar intentos no autorizados de ingreso a los sistemas, equipos o red de una organización, apoyado en una serie de firmas para identificar ataques ya conocidos.

POLITICAS SEGURIDAD: Se crean a partir del desarrollo de reglas, protocolos y normas que indican el actuar para garantizar la seguridad de la información de una organización, identificando los puntos que debe tener control no solo a elementos técnicos, también personas y procesos que tengan relación y que puedan ser susceptibles a vulnerabilidades.

SIEM: Es una herramienta utilizada para de manera centralizada recopilar eventos que serán analizados e interpretados con el fin de detectar comportamientos o patrones que afecten la seguridad de una organización

SNIFFER: Herramienta utilizada para capturas paquetes de datos dentro de una red informática con el fin de analizar la información, dependiendo de quien lo use se puede realizar de manera ética o que pueda afectar a la organización.

ATAQUES INFORMATICOS: Son aquellos intentos cuyo fin buscar aprovechar una vulnerabilidad, causando daño o robando información de un sistema de información o de una red.

RESUMEN

Los ataques en Latinoamérica se han incrementado y Colombia no es ajena a estos eventos, esto hace necesario que las empresas se protejan con sistemas que prevengan contra intentos de intrusión e incidentes que puedan afectar la empresa y esta empresa al prestar servicios hacia otras compañías con sistemas que contienen información sensible se convierte en blanco de posibles eventos de ciberseguridad.

Por lo cual se realizarán ajustes sobre la red de la empresa para que contengan sistemas IDS/IPS (Sistemas de detección de intrusos/Sistemas de prevención de intrusos), esto con el objetivo de protección de la red interna, servidores, redes para usuarios invitados, así como evitar posibles ataques desde internet o desde redes compartidas por conexiones con proveedores externos, ataques que pueden basarse en técnicas tales como:

- Geolocalización: Basado en ataques provenientes de países conocidos por sus altos riesgos de ataques los cuales serán bloqueados.
- Comportamiento: Accesos anormales por parte de los usuarios, los cuales indiquen un riesgo para la seguridad de la compañía.
- Firmas: Basado en eventos ya conocidos y que por su naturaleza deben se bloqueados.

Se genera un análisis de vulnerabilidades, de las instalaciones físicas, detección de eventos los cuales no son bloqueados, definición, aplicación y afinamiento de políticas de red.

ABSTRACT

Attacks in Latin America have increased and Colombia is no stranger to these events, this makes it necessary for companies to protect themselves with systems that prevent intrusion attempts and incidents that may affect the company and this company by providing services to other companies with systems. containing sensitive information becomes the target of potential cybersecurity events.

Therefore, adjustments will be made on the company's network so that they contain IDS / IPS systems (Intrusion detection systems / Intrusion prevention systems), this with the aim of protecting the internal network, servers, networks for guest users. , as well as avoiding possible attacks from the internet or from networks shared by connections with external providers, attacks that can be based on techniques such as:

• Geolocation: Based on proven attacks from countries known for their high risk of attacks which will be blocked.
• Behavior: Abnormal access by users, which indicates a risk to the security of the company.
• Signatures: Based on events already known and which by their nature must be blocked.

An analysis of vulnerabilities is generated, of the physical facilities, detection of events which are not blocked, definition, application and fine-tuning of network policies.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

PUNTOQOM es una empresa que tiene como actividad principal: Actividades de desarrollo de sistemas informáticos (planificación análisis diseño programación pruebas). A mediados del 2020 uno de los colaboradores de la empresa en su modalidad de trabajo en casa y haciendo uso de la red de internet de su hogar, expuso su sistema y toda la información de su equipo de trabajo, accediendo a un correo informativo sobre el COVID-19 el cual se trataba de un correo de phishing. Esto llevó a que la información de un gran proyecto que tenía en marcha la empresa se pusiera en riesgo y en manos de cibercriminales, trayendo como consecuencia la cancelación del servicio de uno de los clientes potenciales.
Esta situación deja ver que la empresa no cuenta con un sistema de protección ágil ante posibles amenazas, lo cual incrementa el riesgo de los activos que tiene la empresa en particular la información de sus clientes.

La empresa actualmente posee un sistema UTM que permite proteger la red y servicios, para lo cual se requiere mejorar la seguridad de la red con la implementación de una herramienta que permita prevenir ataques e intrusiones y reducir el alto riesgo de ataques al no estar protegida.

La implementación de sistemas de seguridad ayuda a reducir el riesgo de no tener protegida la información, la cual es sensible y más cuando se manipulan datos pertenecientes a clientes, la cual debe garantizarse su protección y evitar problemas legales ocasionados por perdidas de esta.

Mediante la implementación de sistemas de prevención ya sean comerciales o software OpenSource se podrá disminuir y mitigar este riesgo, lo cual permitirá bloquear las diferentes amenazas que se presenten e ir aplicando y afinando políticas de seguridad sobre la red.

Estadísticas indican que en Colombia los delitos informáticos se han incrementado con 31.058 casos[1].

De esta manera es que los cibercriminales incrementan su accionar para obtener ganancias logrando acceder y hurtar información relevante y de importancia para las organizaciones.

[1] CAMARA COLOMBIANA DE INFORMATICA Y TELECOMUNICACIONES, [sitio web], Colomiba: CCIT; Tendencias Cibercrimen Colombia 2019-2020. [Consulta: 12 junio 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué recursos tecnológicos son los más apropiados para diseñar un sistema de prevención de instrucciones IDS/IPS que permita monitorear y evitar ataques cibernéticos en la red y asegure los activos de información de la empresa PUNTOQOM?

2 JUSTIFICACIÓN

El desarrollo de este proyecto se ha escogido con el propósito de identificar la seguridad informática de la empresa PUNTOQOM y el objetivo de diseñar un sistema de seguridad para la red que le permitan minimizar el riesgo y las amenazas de cibercriminales. Esto le servirá a la empresa para definir políticas de seguridad informática y técnicas que aseguren los activos de información y de red de la empresa.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar un sistema de seguridad de protección y prevención para la red empresarial de PUNTOQOM que permita minimizar el riesgo de ataques por parte de cibercriminales y asegurar los activos de información de la empresa
.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar levantamiento del estado actual de la red de los equipos que facilitan la comunicación de la empresa y que soportan los sistemas de información, examinando los riesgos y fallas de seguridad
- Seleccionar un sistema de detección y prevención de intrusos para la seguridad informática, mejorando el monitoreo, corrección oportuna y garantizar una máxima seguridad.
- Proponer políticas de seguridad dentro del IDS/IPS que permitan el correcto funcionamiento e implementación del sistema de detección de intrusos
- Elaborar la documentación de la herramienta de prevención y detección seleccionada que sirva como manual de funcionamiento.

4 MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL Y TEÓRICO

Los Sistemas de prevención de intrusos (IPS), son utilizados para proteger la red y los sistemas internos ante posibles ataques o ingresos no autorizados, usado como herramienta de prevención analizando en tiempo real las conexiones que se van generando para determinar si se está presentando o se puede presentar la ocurrencia de un incidente mediante la identificación de patrones y la aplicación de políticas sobre el tráfico que se está analizando.[2]

Una característica de los sistemas de protección y que puede garantizar un alto porcentaje de cubrimiento de los posibles ataques externos es geolocalización, una empresa que requiere que sus servicios sean accedidos y consultados solo a nivel Colombia puede configurar el servicio para que solo se permita tráfico a nivel nacional, descartando todo lo que provenga desde otras ubicaciones geográficas garantizando un nivel de protección muy alto cuando se trate de ataques a nivel externo.

Con la adopción de estos sistemas se detectarán eventos de seguridad los cuales se podrán ir bloqueando e ir afinando políticas de seguridad sobre la red.

Para la adopción de las alternativas de sistemas de prevención a utilizar se puede elegir entre diferentes alternativas de mercado, existiendo herramientas comerciales con alto reconocimiento y posicionadas por su alto rendimiento.

- **ACCESO NO AUTORIZADO:** Consiste en ingresas si el debido permiso, en contra de la voluntad del propietario, administrador, o encargado a un sistema de información, mediante técnicas para encontrar, descifrar o vulnerar contraseñas o sistemas de seguridad.
- **ATAQUES INFORMÁTICOS**: Su objetivo primordial es afectar un sistema de información, mediante la vulneración de la confidencialidad, integridad y disponibilidad de los datos.
- **BITÁCORA**: Permite llevar registro de acciones y procedimientos
- **CONFIDENCIALIDAD**: Cualidad de la información que permite que solo sea vista por el personal autorizado.
- **DATOS**: parte mínima de la información
- **DIDS**: Sistema de detección de intrusos distribuido

[2] INSTITUTO NACIONAL DE CIBERSEGURIDAD, [sitio web], España: INCIBE, ¿Qué son y para qué sirven los SIEM, IDS e IPS? [Consulta: 08 junio 2021], Disponible en: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

- **DISPONIBILIDAD**: Cualidad de la información que sea accesible en el momento que se necesite
- **DOMINIO DE COLISIÓN**: Segmento físico presente en una red de computadores donde las tramas interfieren unas con otras.
- **FIREWALL**: Es un muro virtual que protege a los sistemas de información de acceso no autorizado.
- **HIDS**: Sistema de detección de intrusos basado en host
- **IDS**: Sistema de detección de intrusos
- **INFORMACIÓN**: Conjunto de datos procesados
- **INTEGRIDAD**: Cualidad de la información de mantener los datos sin cambios no autorizados
- **IPS**: Sistema de prevención de intrusos
- **LOGS**: son registros o bitácoras que almacenan datos de registro de un programa, Base de datos o sistema.
- **NIDS**: Sistema de detección de intrusos en red
- **NMAP**: Aplicación que permite el escaneo de puertos
- **PUERTOS**: Es una interfaz que permite la comunicación de aplicaciones a través de la red
- **SNIFFER**: Detecta cada paquete que viaja por una red para poder ser analizado.
- **VULNERABILIDADES**: Una debilidad o falencia en un sistema de información.
- **WEB**: Información que se encuentra en una red de internet mediante diferentes protocolos

4.2 MARCO GEOGRAFICO

La Empresa PUNTOQOM se encuentra ubicada en Colombia y la operación se realiza desde la ciudad de Bogotá, la atención a clientes se realiza a nivel nacional. El área estudio del proyecto corresponde a la ubicación geográfica de la empresa, la cual corresponde a la ciudad de Bogotá-Colombia, en la dirección Cra 6 # 14-74[3].

4.3 ANTECEDENTES O ESTADO ACTUAL

Cada año se hace necesario realizar estudios de vulnerabilidades que permitan identificar los riesgos potenciales que puedan afectar la compañía, para esto se realizan análisis de los niveles de seguridad y como esto se ve reflejado en el retorno de inversión realizado.

Por tal razón se requiere redefinir el estado actual de la seguridad de la red con políticas acordes a los niveles actuales de incidentes y ataques.

[3] UNIVERSIDAD CATOLICA, [Sitio web]. Colombia, Marcos de Referencia, [Consulta: 15 junio 2021], Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/2967/10/parte2.pdf

4.4 MARCO CIENTÍFICO O TECNOLÓGICO

Para la adopción de las alternativas de sistemas de prevención a utilizar se puede elegir entre diferentes alternativas de mercado, existiendo herramientas comerciales con alto reconocimiento y posicionadas por su alto rendimiento.

Figura 1. Cuadro Garther de las diferentes herramientas comerciales y su posicionamiento en el mercado.

Fuente : TRENDMICRO; Global Threat Communications [Sitio web]. Disponible en: https://blog.trendmicro.com/trend-micro-named-leader-2018-gartner-magic-quadrant-intrusion-detection-prevention-systems-idps/

Ubicando productos comerciales de Cisco, Trend Micro, McAfee, como líderes de mercado.

Dentro de alternativas también se tiene herramientas OpenSource, las cuales tiene altos niveles de protección para implementación en empresas, algunas de estas herramientas son: [4]

- Snort
- Security Onion

[4] OPENWEBINARS, [sitio web] Las 8 mejores herramientas open source de detección de intrusión [Consulta: 15 junio 2021], Disponible en: https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/

- OpenWIPS-NG}
- Suricata
- BroIDS
- OSSEC
- AIDE

4.5 MARCO LEGAL

El proyecto se rige bajo algunas leyes colombianas correspondiente a delitos informáticos y el acceso a tipos de información:

Ley 1273 de 2009, el cual en su capítulo 1 estipula lo siguiente:

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

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Articulo 269G: Suplantación de sitios web para capturar datos personales: El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, tendrá una pena de prisión entre 4 a 8 años y multas entre 100 a 1000 SMLMV

Ley 1581 del 2012

Artículo 5. Datos Sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos. Artículo 9. Autorización del Titular. Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior

5 DISEÑO METODOLÓGICO

a. Tipo de investigación

El presente trabajo es de carácter descriptivo, va a manejar un enfoque cuantitativo y también cualitativo[5] para lo cual se realizará una previa investigación de los ataques más frecuentes sobre los servicios de la compañía PUNTOQOM y los sistemas, lo cual permitirá generar las reglas que se aplicaran como sistema de protección de bloqueo.

b. Diseño

Método observación: La recolección de datos validando cuales han sido las tendencias en vectores que ataques, con visita a la empresa PUNTOQOM, analizando su sistema de protección actual e identificar posibles huecos de seguridad, y levantamiento de diagrama de red.
Esta información permitirá realizar una comparación para proponer un sistema de seguridad perimetral.

El proyecto consta de siete etapas

1. Interpretativa: Se validarán los datos recolectados de seguridad y el mapa actual de red, junto con la validación en el mercado de las diferentes alternativas de prevención de intrusos ya se comercial o software libre.

2. Trabajo de campo: Visitas a la empresa para levantamiento de estado de la red, elementos de seguridad de red, conexión de internet, análisis de vulnerabilidades con herramienta de software libre como Vega, Kali linux con esto se tendrá un diagnóstico del estado actual de seguridad de la empresa PUNTOQOM.

3. Propuesta de solución: Se realizar la propuesta de implementación de la solución, la cual genere beneficios y minimice los riesgos de seguridad.

4. Pruebas: Validaciones de tráfico para afinar reglas de protección y aseguramiento.

5. Afinamiento: Depuración de reglas y políticas para determinar que no se estén bloqueando o restringiendo servicios requeridos.

[5] UNIVERSIDAD DE MEXICO, [sitio web], Mexico; Metodología De La Investigación cuantitativa Y Cualitativa [Consulta: 17 junio 2021], Disponible en: https://www.uv.mx/rmipe/files/2017/02/Guia-didactica-metodologia-de-la-investigacion.pdf

6. Fuentes de información

Basadas en internet de los sitios web de los fabricantes en caso de productos comerciales o de Las fuentes de información para productos software libre (OpenSource).

7. Equipamiento

Se determinarán los componentes físicos requeridos para la implementación de la solución.

6. REALIZAR LEVANTAMIENTO DEL ESTADO ACTUAL DE LA RED DE LOS EQUIPOS QUE FACILITAN LA COMUNICACIÓN DE LA EMPRESA Y QUE SOPORTAN LOS SISTEMAS DE INFORMACIÓN, EXAMINANDO LOS RIESGOS Y FALLAS DE SEGURIDAD

Conocer la infraestructura actual de comunicaciones permitirá identificar aquellos puntos que pueden ser vulnerables y sobre los cuales no se tiene conocimiento y control generando soluciones que eviten perdidas de información, elementos como servidores, switch, equipos de escritorio, software de seguridad entre otros son elementos que se deben identificar y conocer su funcionamiento dentro de la infraestructura general.

Levantamiento del estado actual de la infraestructura,

Tabla 1 Inventario Infraestructura TI actual de la empresa PUNTOQOM.

ELEMENTO	DESCRIPCION	UBICACION	RESPONSABLE	CANTIDAD
Servidores WEB	Dell PoweEdge Intel Xeon 3.3 Ghz (4 core), 32 GB RAM, 2 TB, WIN 2012 Server	Cuarto comunicaciones	Administrador Infraestructura	2
Servidores Active Directory	Dell PoweEdge Intel Xeon 3.3 Ghz (4 core), 16 GB RAM, 2 TB, WIN 2012 Server	Cuarto comunicaciones	Administrador Infraestructura	2
Servidor Impresión	Dell PoweEdge Intel Xeon 3.3 Ghz (4 core), 16 GB RAM, 2 TB, WIN 2012 Server	Cuarto comunicaciones	Administrador Infraestructura	2
Servidor DHCP	Dell PoweEdge Intel Xeon 3.3 Ghz (4 core), 16 GB RAM, 2 TB, WIN 2012 Server	Cuarto comunicaciones	Administrador Infraestructura	1
Equipos de escritorio	DELL OptiPlex GX620 (3.2Ghz), 2 GB de RAM, Win 10 pro	Puestos oficina empresa	Usuario	85
Switch	Cisco Catalyst 24 puertos	Cuarto comunicaciones	Administrador Infraestructura	8
Enlaces comunicaciones	Canal dedicado de 200 MB	Cuarto comunicaciones	Administrador Infraestructura	1
Impresoras Laser	Multifuncional HP	Instalaciones Empresa	Administrador Infraestructura	5
AP Wifi	TrendNet	Instalaciones Empresa	Administrador Infraestructura	10
Firewall	Linux	Cuarto comunicaciones	Administrador Infraestructura	1
Antivirus	kaspersky	Servidores y Equipos	Administrador Infraestructura	100
Proxy	Squid	Cuarto comunicaciones	Administrador Infraestructura	1
Share point	Almacenamiento información	Nube	Administrador Infraestructura	1

Fuente: Autor

Se describen los activos encontrados y la valoración realizada a cada uno

Tabla 2 Activos encontrados en la empresa PUNTOQOM y Valoración Cualitativa

No.	DATOS DEL ACTIVO DE INFORMACION		
	Nombre del activo de información	Proceso propietario del activo	Responsable
1	[www] Página Web	Departamento de Sistemas	Jefe Sistemas
2	[host] Servidor WEB Dell PoweEdge Intel	Departamento de Sistemas	Jefe Sistemas
3	[host] Servidor Active Directory Dell PoweEdge Intel	Departamento de Sistemas	Jefe Sistemas
4	[host] Servidor Impresión Dell PoweEdge Intel	Departamento de Sistemas	Jefe Sistemas
5	[print] Impresora Multifuncional HP	Departamento de Sistemas	Jefe Sistemas
6	[email] Correo en nube	Departamento de Sistemas	Jefe Sistemas
7	[host] Servidor DHCP Dell PoweEdge Intel	Departamento de Sistemas	Jefe Sistemas
8	[pc] Computadores usuarios (85)	Áreas usuarias	Jefes áreas
9	[firewall] LINUX	Departamento de Sistemas	Jefe Sistemas
10	Software Antivirus	Departamento de Sistemas	Jefe Sistemas
11	Proxy	Departamento de Sistemas	Jefe Sistemas
12	[wap] AP inalámbrico (10)	Departamento de Sistemas	Jefe Sistemas

13	[switch] cisco catalyst (8)	Departamento de Sistemas	Jefe Sistemas
14	[router] Puntos acceso internet (1)	Departamento de Sistemas	Jefe Sistemas
15	[vhost] Servidores virtuales	Departamento de Sistemas	Jefe Sistemas
16	Software operativo y aplicativo	Departamento de Sistemas	Jefe Sistemas
17	[std] Sistemas de informacion	Departamento de Sistemas	Jefe Sistemas
18	[backup] Copias de seguridad	Departamento de Sistemas	Jefe Sistemas
19	[os] Windows 10 pro (85)	Departamento de Sistemas	Jefe Sistemas

Fuente: Autor

Tabla 3 Valoración Cuantitativa de activos de la empresa PUNTOQOM

Nombre	Riesgo
[www] Página Web	CRITICO
[host] Servidor impresión Dell PoweEdge Intel	IMPORTANTE
[print] Impresora Multifuncional HP	APRECIABLE
[print] Impresora SMART M4370LX	APRECIABLE
[email] Correo en nube	CRITICO
[host] Servidor DHCP Dell PoweEdge Intel	IMPORTANTE
[pc] Computadores usuarios (85)	IMPORTANTE
[firewall] LINUX	CRITICO
[wap] AP inalámbrico (10)	IMPORTANTE
[switch] cisco catalyst (8)	IMPORTANTE
[router] Puntos acceso internet (1)	IMPORTANTE
[vhost] Servidores virtuales	IMPORTANTE
Software operativo y aplicativo	APRECIABLE
[std] Sistemas de información	IMPORTANTE
[backup] Copias de seguridad	IMPORTANTE
[os] Windows 10 pro (85)	APRECIABLE
[std] Software Antivirus	IMPORTANTE
[std] Proxy	IMPORTANTE

Fuente: Autor

Para el levantamiento del diagrama de red se hace uso de herramientas de escaneo de IP como advaced port scaner identificando dispositivos conectados en la red y mediante visita en sitio junto con levantamiento de datos con el administrador de infraestructura para conocer los elementos que se utilizan para prestar los servicios, se mostrarán algunos datos debido a que no se puede publicar información detallada, el segmento de red esta creado sobre una red clase C 192.168.x.x, con subredes a las cuales se les realizara los respectivos escaneos de red para identificar activos, puertos activos y vulnerabilidades sobre los mismos.

Identificar e instalar medidas para afrontar las amenazas y las vulnerabilidades a las cuales se encuentran expuestas las organizaciones hoy en día es posible mitigarlo, si se cuenta con un buen plan de análisis y gestión de los riesgos informáticos, esto no quiere decir que se va a lograr un 100% de la seguridad ya que llegar a ese nivel no es posible, no existe ningún entidad organización o experto en sistemas que pueda garantizar esta condición y adicional impedir que alguna situación se presente por más controles que se tenga, lo importante es generar un plan que permita reducir los posibles eventos.

Para ello es importante identificar todas las vulnerabilidades que se pueden encontrar en una organización relacionados con sus sistemas de información y recursos de TI, esto con el fin de llegar a generar un plan donde se gestionen esos riesgos informáticos a partir de los peligros y de las vulnerabilidades que se encuentren y las consecuencias que estas acarrean. Es importante tener el detalle de todos los elementos que se requieren para el funcionamiento y operación de una organización para así poder crear un mapa donde se evidenció todos aquellos puntos que puede generar un impacto para la operación.

Es importante mencionar las amenazas y tipos más comunes que se presenta para poder realizar un análisis de riesgos sobre los sistemas informáticos, entre ellos encontramos:
Exposición de información o fuga de datos, los riesgos generados a partir del uso de discos extraíbles, USB u otro elemento de almacenamiento que no estén cifrados, también el mal uso de documentos físicos los cuales no son almacenados debidamente o destruidos cuando no son requeridos.
Usuarios autorizados que tienen privilegios dentro de la organización y utilizan este nivel para filtrar información.
Accesos a la información no autorizados, que pueden llegar a materializarse a través de malware enviados dentro de correos o peligrosa que pueden estar de manera interna en una organización.

Identificar eventos internos que se pueda presentar dentro una organización también es importante para la gestión de riesgos, saber a qué ese puede llegar a enfrentar, tales como un daño sobre equipos físicos por parte de los empleados, principalmente sobre servidores que es donde se de instalan aplicaciones o se almacena información, así como robos, inundaciones o incendios, fallas en la infraestructura que soportar la organización tales como caídas de internet o canales de comunicaciones que afectan la continuidad de la operación del negocio y fallas humanas que también deben contemplarse y

determinar cómo se actuará ante estas.
Apoyarse de un tercero para identificar las vulnerabilidades y los riesgos es una buena opción dado que son expertos en la materia y pueden ayudar a identificar lo que al interior de una organización no se está evidenciando, todo esto dependiendo del tipo de organización y los recursos económicos que se contemplen para ello. Dentro de todo este proceso es importante que el personal de la organización conozca el plan que se está gestando ya que ellos serán los que al final cumplan con las normas y reglas que se generen o deriven para garantizar que los riesgos encontrados no se materialicen.

Todo este proceso al final derivará en un gran beneficio para la organización ya que a menor cantidad de eventos que se presenten y de vulnerabilidades corregidas la calidad y seguridad a la información será mejor.

Por último generar un ambiente de seguridad informática y cultura, creando sentido de responsabilidad sobre acatar y cumplir con las políticas que defina la organización en esta materia, debe hacer parte del día a día de todos los que componen la organización, lograr llegar a los colaboradores para que tomen esto no como una imposición sino como una mejora para el bienestar general, iniciando con el ejemplo desde la alta gerencia quienes apoyan las políticas que se generen sobre seguridad informática.

PUNOQOM, en su continua evolución y prestaciones de servicios, requiere realizar un análisis de riesgos informáticos mediante el uso de la metodología MAGERIT para determinar que procedimientos de seguridad se deben adoptar, implementando controles y políticas para mitigar eventos de seguridad que puedan impactar la continuidad de sus servicios, se identificarán las siguientes etapas:

- Identificación de activos
- Identificación de amenazas
- Establecimiento de salvaguardas
- Estimación el impacto y riesgo.

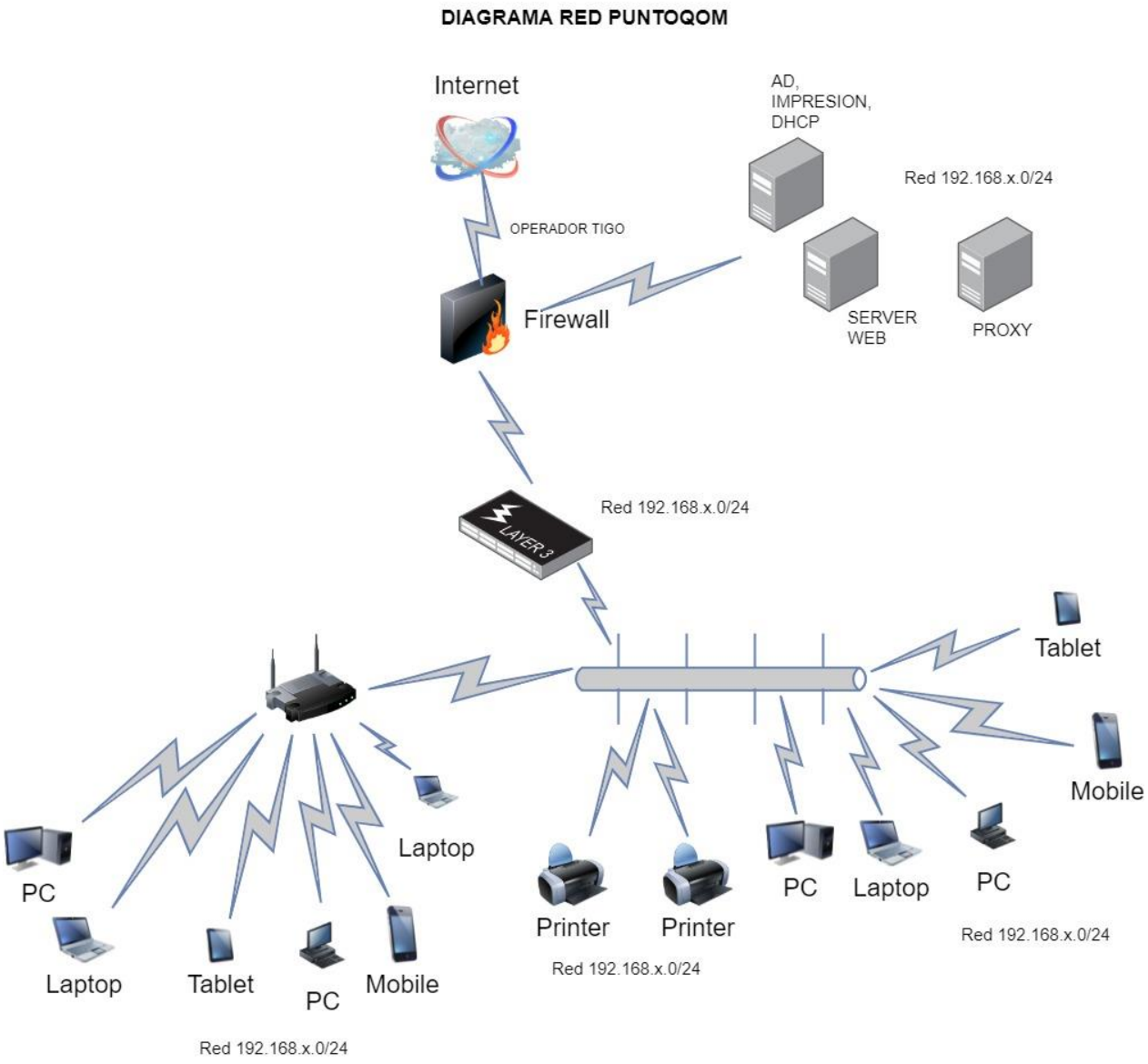
Tabla 4 Seguridad Actual activos informáticos empresa PUNTOQOM

ACTIVOS	TIPO	RIESGOS	VULNERABILIDADES
Portal WEB, aplicaciones financieras, aplicaciones internas, terceros	Datos	Fuga de información, alteración de datos, ataque sitios WEB	No existe control de accesos, Logs de monitoreo de eventos no se tiene, información no se encuentra protegida por métodos de cifrado
Servidores Active Directory	Hardware	Permisos privilegiados a usuarios comunes	No existe control sobre permisos de administración a usuarios, riesgo de escalamiento de privilegios
Equipos de escritorio	Hardware	Actualizaciones no controladas	Equipos vulnerables por parche no actualizados
Switch	Comunicaciones	Acceso físico sin control ni protección, Administracion sin controles	Accesibles por cualquier usuario, administración de equipos con contraseñas débiles y sin ACL de control de acceso
Firewall	Aplicaciones	Administracion sin control, políticas débiles	Acceso por parte de usuarios sin conocimiento, políticas con niveles bajos de protección a los recursos permitiendo puertos o servicios con riesgos
Proxy	Aplicaciones	Políticas Débiles	Bajo control de acceso a internet, permitiendo accesos con peligro potencial

Fuente: Autor

La Figura 2 muestra los componentes de red y seguridad identificados durante el levantamiento de información.

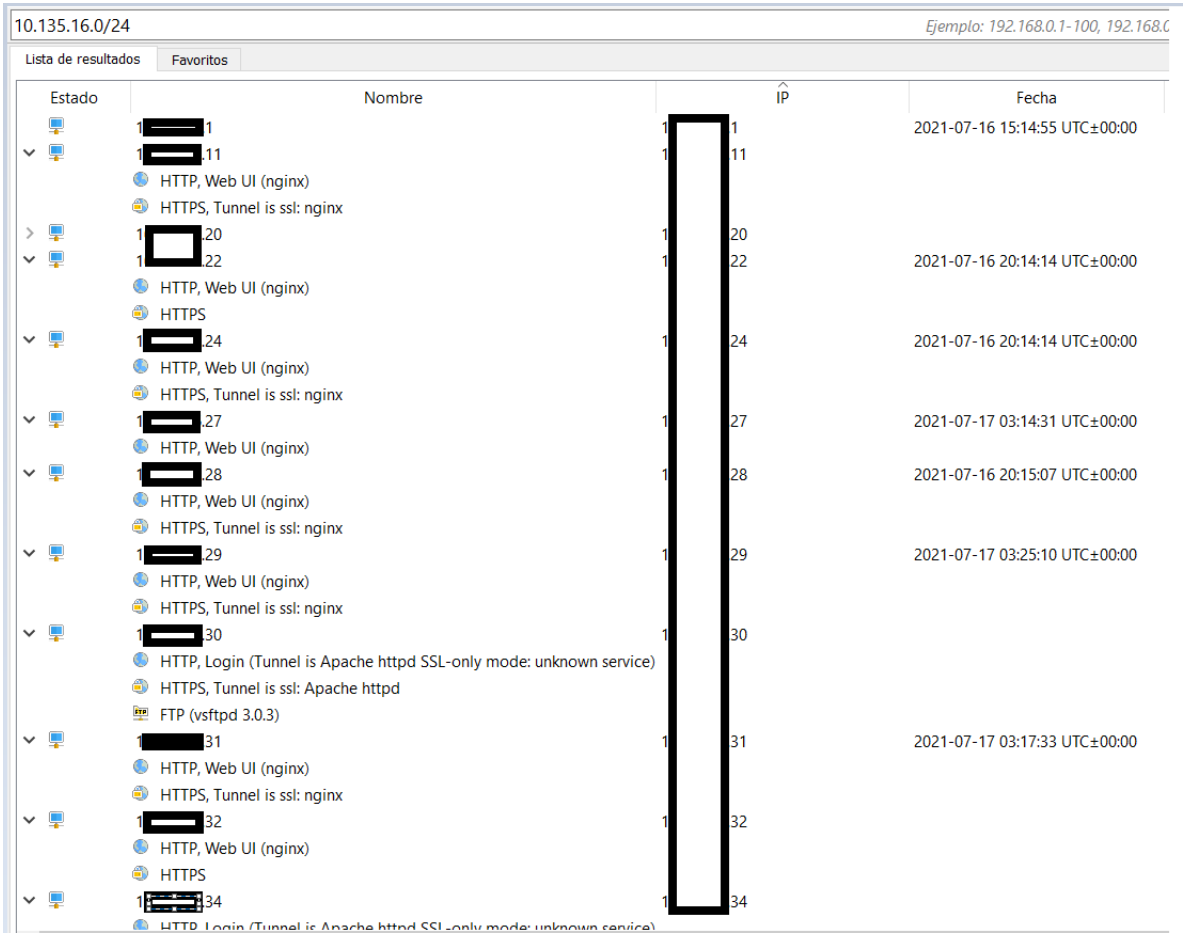
Figura 2 Diagrama de Red levantamiento información componentes red



Fuente: Autor

La Figura 3 muestra el escaneo de la red para validar equipos encontrados, para esto se utilizó la herramienta QUALYS, la cual permite analizar elementos basados en plantillas de vulnerabilidades.

Figura 3 Escaneo de red para identificación vulnerabilidades



Fuente: Autor

La Figura 4, muestra el análisis de vulnerabilidades y cumplimento con la herramienta QUALYS la cual cuenta con templates para tipos de productos y cumplimientos de seguridad.

Figura 4 Análisis Vulnerabilidades componentes de red indentificados

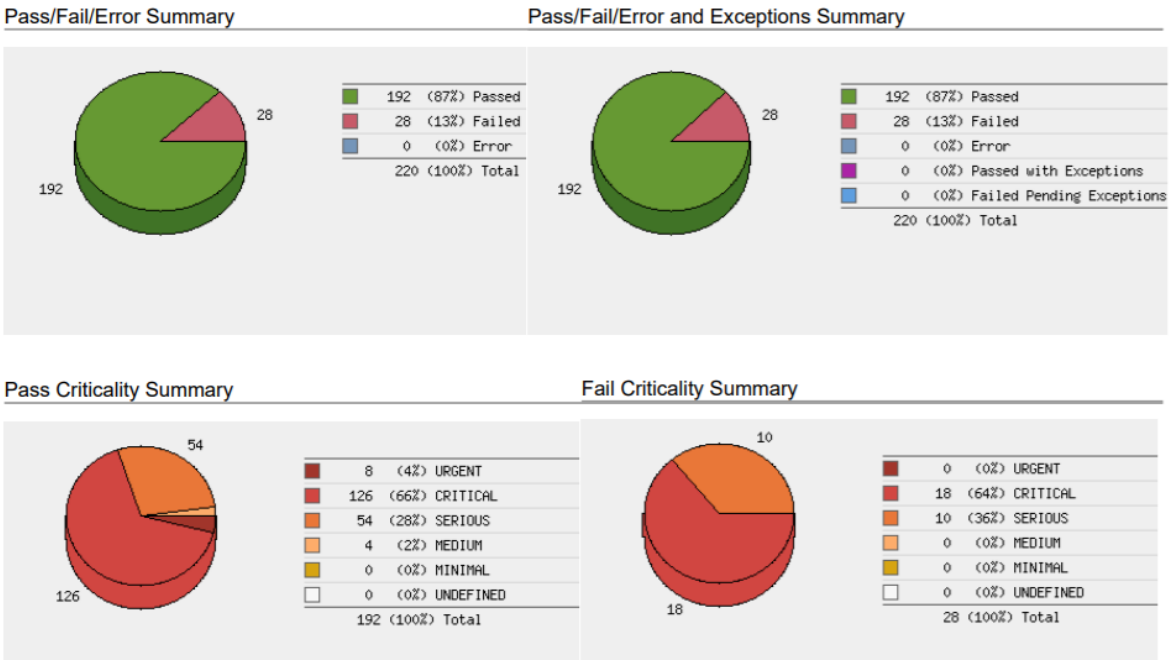
Report Summary

Policy:	[redacted]
Policy Locking:	Locked - [redacted]
Template:	Policy Report Template
Asset Groups:	[redacted]
Ips:	N/A
Asset Tags:	N/A
PC Agent IPs:	No
[redacted]	
Controls:	55
Technologies:	1 (Cisco IOS XE)
Total Control Instances:	220
Total Passed:	192 (87.27%)
Total Failed:	28 (12.73%)
Total Error:	0
Approved Exceptions:	0
Pending Exceptions:	0
Policy Modified:	05/26/2020 at 13:03:41 (GMT-0500)
Policy Last Evaluated:	07/15/2021 at 22:22:31 (GMT-0500)

Fuente: Autor

La Figura 5 muestra el cumplimiento y controles aprobados y no aprobados.

Figura 5 Análisis Vulnerabilidades 2 componentes de red



Fuente: Autor

La Figura 6, muestra los controles de vulnerabilidades en equipos de comunicaciones

Figura 6 Listado Vulnerabilidades componentes de red

Order	Control ID	Statement
1.1	4357	Status of the 'aaa new-model' configuration command on the device
1.2	4358	Status of the 'aaa authentication login' configuration command on the device
1.3	4359	Status of the 'aaa authentication enable' configuration command on the device
1.4	4361	Status of the 'login authentication' configuration command for 'line con' on the device
1.5	4362	Status of the 'login authentication' configuration command for 'line tty' on the device
1.6	4363	Status of the 'login authentication' configuration command for 'line vty' on the device
1.7	4397	Status of the 'ip http secure-server' configuration command on the device
1.8	17805	Status of the 'ip http authentication' global config command
1.9	4364	Status of the existence of at least one (1) 'local user account' on the device
1.10	4370	Status of the 'transport input' configuration command for 'line vty'
1.11	4374	Status of the 'no exec' configuration command for 'line aux'
1.12	17883	List of Line VTY in which ACL is applied
1.13	17884	List of Line VTY in which ACL is NOT applied
1.14	8344	Require VTY Access Control
1.15	4371	Status of the 'exec-timeout' configuration command for 'line aux'
1.16	4372	Status of the timeout configuration for local console
1.17	4373	Status of the 'exec-timeout' configuration command for 'line tty'
1.18	4433	Status of the timeout configuration for vty console
1.19	4375	Status of the 'transport input' configuration command for 'line aux'
1.22	4376	Status of the 'banner exec' configuration command on the device
1.23	4377	Status of the 'banner login' configuration command on the device
1.24	4378	Status of the 'banner motd' configuration command on the device
1.25	17808	Status of the 'ip admission auth-proxy-banner' global config command
1.26	4379	Status of the 'enable secret' configuration command on the device
1.27	4380	Status of the 'service password-encryption' configuration command on the device
1.28	4385	Status of the '[username] passwords' being set on the device
1.29	4390	Status of the 'SNMP-server community' configuration command on the device
1.30	4386	Status of the 'snmp-server community private' configuration command on the device
1.31	4387	Status of the 'snmp-server community public' configuration command on the device
1.32	17809	List of SNMP rw communities
1.33	17881	List of SNMP Communities in which ACL is applied and applied ACL is present in the system
1.34	17882	List of SNMP Communities in which ACL is NOT applied or applied ACL is not present in the system
1.35	8550	Status of the 'SNMP Trap Server / receivers' setting
1.36	9183	Status of the SNMP type trap messages

Fuente: Autor

7. SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS PARA LA SEGURIDAD INFORMÁTICA, MEJORANDO EL MONITOREO, CORRECCIÓN OPORTUNA Y GARANTIZAR UNA MÁXIMA SEGURIDAD

Un sistema de detección de intrusos es una herramienta de seguridad que permite observar tráfico, analizándolo, detectándolo y bloqueando accesos no autorizados a la infraestructura de una organización que pueden generar consecuencias como perdida y robo de información vital para la operación de esta.

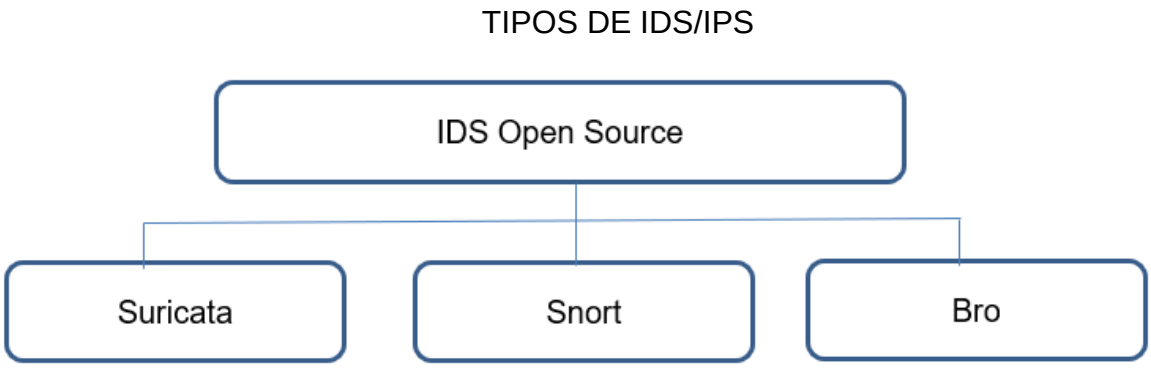
Su funcionamiento se basa en una base de datos la cual contiene firmas de ataques los cuales compara con el tráfico que está analizando y de acuerdo con el resultado determina si realiza bloqueos clasificándolos por el tipo detectado.

Teniendo en cuenta las alternativas, se validan las herramientas que existen en el mercado tanto comerciales como OpenSource, por lo cual se determina que la herramienta a implementar se basara en OpenSource por representar menos costo económico en cuanto a tema de licenciamiento.

Para esto se analizan diversos productos que existen los cuales son:

Suricata, Snort, Bro

Figura 7 Tipos de IDS software libre disponibles en el mercado



Fuente: Autor

7.1. Suricata

Es un sistema de detección y prevención de código abierto, el cual monitorea el tráfico de red, generando alertas cuando se detectan eventos anómalos, se basa en muti-hilos lo cual permitirá balancear entre los procesadores disponibles la carga, lo cual permite

una mayor velocidad y más eficiente durante el análisis de tráfico[6], identifica los principales protocolos de red, controlando el tráfico ante posibles amenazas de malware.

Se basa en conjuntos de reglas, las cuales supervisan el tráfico que se encuentra en la red, generando alertas para los administradores al momento de detectar eventos sospechosos.

Dentro de sus características más importantes se tiene[7]:

- IP reputation, GeoIP, IP list support
- Graphic Cards Acceleration
- Fast IP matching
- Network Security Monitoring
- Network Intrusion Prevention (IPS - Intrusion Prevention System)

Se instala bajo Linux y su gestión y administración se encuentra bajo consola CLI, comandos que pueden generar problemas a la hora de administrar si el encargado no tiene experticia con Linux.

7.2. Snort

Está basado en red (N-IDS) y es opensource, permite la creación de reglas que se utilizaran para monitoreo, cuenta con un set de reglas y filtros predefinidos que se pueden ajustar en el momento de su instalación.

Durante su funcionamiento la herramienta analiza los paquetes y cuando coincide con las reglas se registra el evento de cuando, donde y como se generó el ataque, con inspección basada en firmas, en los protocolos y posibles anomalías, realizando análisis de alto nivel sobre el tráfico que pasa a través de él[8].

Esta herramienta se ha empezado a incorporar en NGFW (Firewall de última generación) como Palo alto.

---

[6] UBUNLOG, [Sitio web], Detecta intrusos y supervisa el trafico de la red, [Consulta: 22 junio 2021], Disponible en: https://ubunlog.com/suricata-4-0-supervisa-el-trafico-de-la-red/

.

[7] SURICATA, [Sitio web], IDS/IPS Suricata [Consulta: 22 junio 2021], Disponible en: https://blog.elhacker.net/ids-ips-suricata-reglas-rules

[8] REDES ZONE, [Sitio web], Snort 3 ya es oficial [Consulta 22 junio 2021]. Disponible en: https://www.redeszone.net/noticias/seguridad/snort-3-oficial-caracteristicas-sistema-prevencion-intrusiones/

Dentro de sus características más importantes se tiene[9]:

- Soporte procesando los paquetes en múltiples hilos.
- Configuración compartida y tabla de atributos.
- Generación de reglas más fácil
- Soporte de multiplataforma.

Cuenta con una interfaz gráfica, la cual lo hace más amigable para la gestión y administración de la herramienta.

7.3. Bro

Sistema de detección de intrusos OpenSource, se basa en anomalías y en firmas, a través de una serie de scripts o políticas en lenguaje nativo se describen se determina el tráfico que será catalogado como sospechoso.

Dentro de sus características más importantes se tiene:

- Gran capacidad de análisis a nivel de protocolo.
- Alto nivel de trafico
- Generación de logs de acuerdo con las necesidades.
- Con los scripts o políticas se pueden determinar el tipo de eventos a monitorear y detectar.

Se gestión y administración se base en consola CLI mediante comandos, lo cual puede ocasionar problemas al momento de gestión y administración si no se cuenta con conocimientos de Linux.

[9] REDES ZONE, [Sitio web], Snort 3 ya es oficial [Consulta 22 junio 2021]. Disponible en: https://www.redeszone.net/noticias/seguridad/snort-3-oficial-caracteristicas-sistema-prevencion-intrusiones/

7.4. SELECCIÓN HERRAMIENTA

Una vez conocidas las características de los 3 IDS, basado en su alta efectividad y ser una herramienta de gran uso a nivel mundial, contando con gran cantidad de documentación de referencia y soporte en internet y su gestión más amigable mediante interfaz gráfica se optó por implementar (SNORT), como solución de prevención y detección.

Tabla 5 Cuadro comparativo herramientas IDS/IPS para uso empresa PUNTOQOM

HERRAMIENTA	ADMINISTRACION	RENDIMIENTO	CARACTERISTICAS
SURICATA	Comandos por CLI	Multi-hilos sobre varios procesadores	Fast IP matching Network Security Monitoring Network Intrusion Prevention (IPS - Intrusion Prevention System)
SNORT	Interfaz Grafica	Multi-hilos, uso en NGFW	Soporte procesando los paquetes en múltiples hilos. Configuración compartida y tabla de atributos. Generación de reglas más fácil Soporte de multiplataforma.
BRO	Comandos, Script	Análisis de paquetes	Gran capacidad de análisis a nivel de protocolo. Alto nivel de trafico Generación de logs de acuerdo con las necesidades. Con los scripts o políticas se pueden determinar el tipo de eventos a monitorear y detectar.

8. PROPONER POLÍTICAS DE SEGURIDAD DENTRO DEL IDS/IPS QUE PERMITAN EL CORRECTO FUNCIONAMIENTO E IMPLEMENTACIÓN DEL SISTEMA DE DETECCION DE INTRUSOS

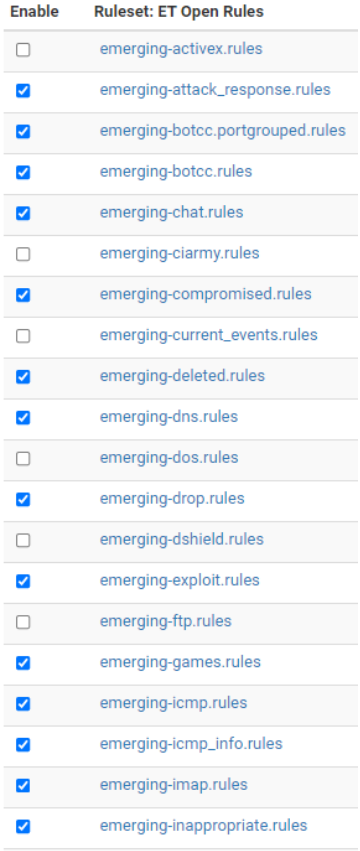
Una correcta selección de políticas dentro de la herramienta permitirá un mejor control del tráfico que se analiza y que llegará a ser bloqueado en el análisis que se realice de este y pueda afectar o comprometer la seguridad.

Se procederá con la instalación basada en SNORT, a partir de este se definirán políticas que ayudarán con el análisis y bloqueo de tráfico, divididas en los siguientes tipos de reglas:

8.1. Reglas IPS

Esta sección (Figura 8), permitirá seleccionar el tipo de tráfico que se analizará y bloqueara, con el objetivo de prevenir la penetración de intrusos, esto mediante el análisis de firmas y de las vulnerabilidades que ya son conocidas.

Figura 8 Reglas IPS sobre SNORT para análisis de trafico



Fuente: Autor

La sintaxis de las reglas que genera la herramienta y las cuales se pueden seleccionar como se observa en la (Figura 8) define la interface por la cual va a analizar el tráfico, tipo de puerto y los parámetros de análisis de la regla junto con tipo de origen y tipo de ataque.

#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Sony ImageStation (SonyISUpload.cab 1.0.0.38) ActiveX Buffer Overflow Exploit"; flow:to_client,established; content:"0x40000"; nocase; content:"E9A7F56F-C40F-4928-8C6F-7A72F2A25222"; nocase; content:"SetLogging"; nocase; reference:url,www.milw0rm.com/exploits/5086; reference:url,www.milw0rm.com/exploits/5100; reference:url,doc.emergingthreats.net/bin/view/Main/2007847; classtype:web-application-attack; sid:2007847; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag ActiveX, updated_at 2016_07_01;)

alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Adobe browser document ActiveX DoS Function call Attempt"; flow:from_server,established; file_data; content:"ActiveXObject"; nocase; distance:0; content:"AcroPDFLib.AcroPDF"; distance:0; nocase; content:"src"; nocase; distance:0; reference:url,www.packetstormsecurity.nl/0911-exploits/acropdf-dos.txt; reference:url,doc.emergingthreats.net/2010705; classtype:attempted-user; sid:2010705; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag ActiveX, updated_at 2019_09_27;)

alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Adobe browser document ActiveX DoS Attempt"; flow:established,to_client; file_data; content:"clsid"; nocase; distance:0; content:"CA8A9780-280D-11CF-A24D-444553540000"; nocase; distance:0; content:"src"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*CA8A9780-280D-11CF-A24D-444553540000/si"; reference:url,www.packetstormsecurity.nl/0911-exploits/acropdf-dos.txt; reference:url,doc.emergingthreats.net/2010726; classtype:attempted-user; sid:2010726; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag ActiveX, updated_at 2019_09_27;)

#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Liquid XML Studio 2010 OpenFile Method Remote Heap Overflow Attempt"; flow:established,to_client; file_data; content:"clsid"; nocase; content:"E68E401C-7DB0-4F3A-88E1-159882468A79"; nocase; distance:0; content:"OpenFile"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*E68E401C-7DB0-4F3A-88E1-159882468A79/si"; reference:url,exploit-db.com/exploits/11750; reference:url,doc.emergingthreats.net/2011050; classtype:attempted-user; sid:2011050; rev:4; metadata:created_at 2010_07_30, updated_at 2010_07_30;)

La parte inicial muestra la acción que se ejecutara, protocolo, direcciones IP origen, destino, máscaras de red, puertos origen-destino. Las opciones de reglas tienen mensajes sobre alertas y la información de las partes de los paquetes que se deben inspeccionar

Ejemplo:

alert tcp any any -> 192.168.0.0/24 80 \ (content:"|00 00 00 00|"; depth: 8; \ msg:"Error de bytes nulos"; sid:4885)

Estas reglas pueden aplicarse a encabezados en la capa de red y transporte tales como (TCP, UDP, IP, ICMP) también a los encabezados en la capa de aplicación (HTTP, FTP, etc.).

Reglas formadas por dos componentes, parte inicial o encabezado, indicando la acción a tomar cuando ésta presente una coincidencia ya sea (TCP, UDP, etc.),

con las IP de origen y destino y sus respectivos puertos; seguido de las opciones de la regla, validando el contenido marcando los paquetes que coincidan

8.2. Reglas por Malware

Esta sección (Figura 9) analizara dentro del tráfico que se está generando posibles malware o software malicioso que se pueda estar presentando y que puedan llegar a equipos internos afectando y comprometiendo la seguridad de la información.

Figura 9 Reglas Malware para análisis de trafico

Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
⚠	1	105	tcp	$HOME_NET	2589	$EXTERNAL_NET	any	MALWARE-BACKDOOR - Dagger_1.4.0
⚠	1	108	tcp	$EXTERNAL_NET	any	$HOME_NET	7597	MALWARE-BACKDOOR QAZ Worm Client Login access
⚠	1	110	tcp	$EXTERNAL_NET	any	$HOME_NET	12345:12346	MALWARE-BACKDOOR netbus getinfo
⚠	1	115	tcp	$HOME_NET	20034	$EXTERNAL_NET	any	MALWARE-BACKDOOR NetBus Pro 2.0 connection established
⚠	1	117	tcp	$HOME_NET	any	$EXTERNAL_NET	any	MALWARE-BACKDOOR Infector.1.x
⚠	1	118	tcp	$HOME_NET	666	$EXTERNAL_NET	any	MALWARE-BACKDOOR SatansBackdoor.2.0.Beta
⚠	1	119	tcp	$HOME_NET	6789	$EXTERNAL_NET	any	MALWARE-BACKDOOR Doly 2.0 access
⚠	1	121	tcp	$EXTERNAL_NET	1000:1300	$HOME_NET	146	MALWARE-BACKDOOR Infector 1.6 Client to Server Connection Request
⚠	1	141	tcp	$HOME_NET	31785	$EXTERNAL_NET	any	MALWARE-BACKDOOR HackAttack 1.20 Connect
⚠	1	144	tcp	$EXTERNAL_NET	any	$HOME_NET	21	PROTOCOL-FTP ADMw0rm ftp login attempt
⚠	1	146	tcp	$HOME_NET	30100:30102	$EXTERNAL_NET	any	MALWARE-BACKDOOR NetSphere access
⚠	1	147	tcp	$HOME_NET	6969	$EXTERNAL_NET	any	MALWARE-BACKDOOR GateCrasher
⚠	1	152	tcp	$HOME_NET	5401:5402	$EXTERNAL_NET	any	MALWARE-BACKDOOR BackConstruction 2.1 Connection
⚠	1	157	tcp	$EXTERNAL_NET	any	$HOME_NET	666	MALWARE-BACKDOOR BackConstruction 2.1 Client FTP Open Request

Fuente: Autor

8.3. Reglas de inspección de trafico

Su objetivo principal (Figura 10), es detectar en un nivel más detallado el tráfico anómalo tal como tramas inconsistentes paquetes de datos con problemas, ingresos por puertas traseras o vulnerabilidades que pueden ser explotadas sin darnos cuenta y aprovechadas para ingresar a la red y robar información.

Figura 10 Reglas Inspección Trafico con análisis más detallado del trafico

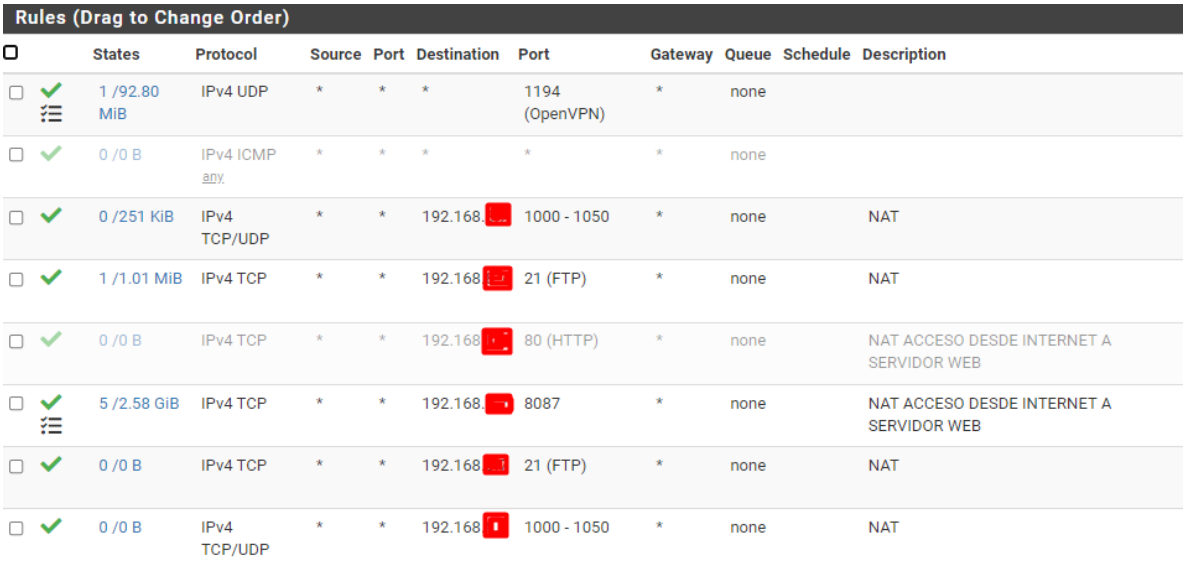
Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
⚠	1	2010371	tcp	$EXTERNAL_NET	any	$HOME_NET	any	ET SCAN Amap TCP Service Scan Detected
⚠	1	2002973	tcp	$HOME_NET	any	$EXTERNAL_NET	3127	ET SCAN Behavioral Unusual Port 3127 traffic, Potential Scan or Backdoor
⚠	1	2010642	tcp	$EXTERNAL_NET	any	$HOME_NET	21	ET SCAN Multiple FTP Root Login Attempts from Single Source - Possible Brute Force Attempt
⚠	1	2010643	tcp	$EXTERNAL_NET	any	$HOME_NET	21	ET SCAN Multiple FTP Administrator Login Attempts from Single Source - Possible Brute Force Attempt
⚠	1	2008560	udp	$EXTERNAL_NET	any	$HOME_NET	1434	ET SCAN NNG MS02-039 Exploit False Positive Generator - May Conceal A Genuine Attack
⚠	1	2001906	tcp	$EXTERNAL_NET	any	$SQL_SERVERS	3306	ET SCAN MYSQL 4.0 brute force root login attempt
⚠	1	2002842	tcp	$EXTERNAL_NET	any	$SQL_SERVERS	3306	ET SCAN MYSQL 4.1 brute force root login attempt
⚠	1	2010493	tcp	$HOME_NET	3306	any	any	ET SCAN Non-Allowed Host Tried to Connect to MySQL Server
⚠	1	2000537	tcp	$EXTERNAL_NET	any	$HOME_NET	any	ET SCAN NMAP -sS window 2048
⚠	1	2000536	ip	$EXTERNAL_NET	any	$HOME_NET	any	ET SCAN NMAP -sO
⚠	1	2000538	tcp	$EXTERNAL_NET	any	$HOME_NET	any	ET SCAN NMAP -sA (1)
⚠	1	2000540	tcp	$EXTERNAL_NET	any	$HOME_NET	any	ET SCAN NMAP -sA (2)
⚠	1	2000543	tcp	$EXTERNAL_NET	any	$HOME_NET	any	ET SCAN NMAP -f -sF
⚠	1	2000544	tcp	$EXTERNAL_NET	any	$HOME_NET	any	ET SCAN NMAP -f -sN

Fuente: Autor

8.4. Firewall

Dentro de esta sección (Figura 11), se controla el tráfico que se expondrá hacia internet permitiendo o no servicios a través de reglas con las IP, puertos, orígenes y destinos, es importante ser muy explícito en lo que se permitirá y no crear reglas muy generales ya que esto puede exponer la seguridad, es recomendable uso de reglas explicitas lo más restrictivas pero que no afecten el servicio que se quiere exponer hacia internet.

Figura 11 Reglas de Firewall para acceso a bloqueos de servicios



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓	1 /92.80 MiB	IPv4 UDP	*	*	*	1194 (OpenVPN)	*	none		
✓	0 /0 B	IPv4 ICMP any	*	*	*	*	*	none		
✓	0 /251 KiB	IPv4 TCP/UDP	*	*	192.168.	1000 - 1050	*	none		NAT
✓	1 /1.01 MiB	IPv4 TCP	*	*	192.168	21 (FTP)	*	none		NAT
✓	0 /0 B	IPv4 TCP	*	*	192.168	80 (HTTP)	*	none		NAT ACCESO DESDE INTERNET A SERVIDOR WEB
✓	5 /2.58 GiB	IPv4 TCP	*	*	192.168.	8087	*	none		NAT ACCESO DESDE INTERNET A SERVIDOR WEB
✓	0 /0 B	IPv4 TCP	*	*	192.168	21 (FTP)	*	none		NAT
✓	0 /0 B	IPv4 TCP/UDP	*	*	192.168	1000 - 1050	*	none		NAT

Fuente: Autor

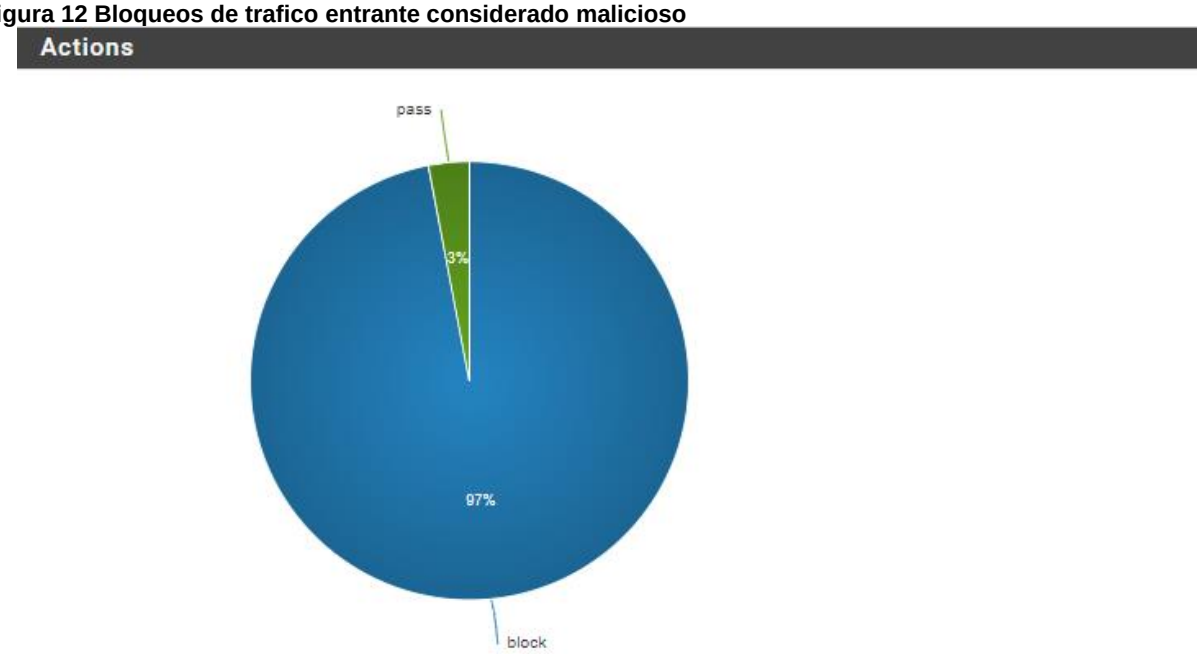
9. ELABORAR LA DOCUMENTACIÓN DE LA HERRAMIENTA DE PREVENCIÓN Y DETECCIÓN SELECCIONADA QUE SIRVA COMO MANUAL DE FUNCIONAMIENTO

Snort como herramienta IDS/IPS seleccionada en el punto 7.4, detectara intrusos sobre la red, a través de sus sensores realizara análisis con un alto nivel, permitiendo detectar spam y phishing, bloqueando el tráfico desde orígenes que pueden ser potenciales riesgos para la seguridad.

9.1. Tendencia de ataques bloqueados

Mediante vistas graficas (Figura 12), se observan los bloqueos realizados al tráfico origen desde internet hacia la IP pública donde se encuentran los servicios que se exponen para ser utilizados por los usuarios.

Figura 12 Bloqueos de trafico entrante considerado malicioso



Actions	Data points
block	9546
pass	296

Fuente: Autor

9.2. Log de bloqueos hacia servicio WEB

Dentro de sus características (Figura 13), se pueden ver las conexiones que son analizadas por la herramienta de detección y prevención de intrusos, conociendo el detalle del tipo y clasificación del tráfico y el detalle de este para conocer su clasificación.

Figura 13 Logs bloqueos tráfico malicioso entrante

Alert Log View Filter

Most Recent 500 Entries from Active Log

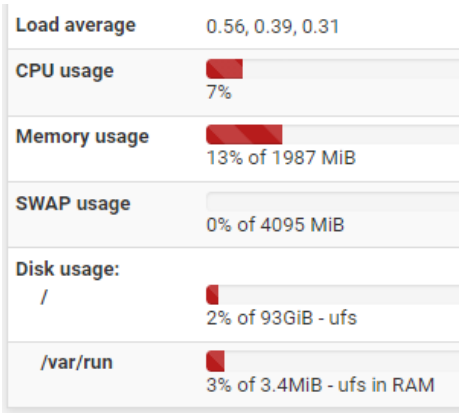
Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2021-08-30 19:06:01		2	TCP	Misc Attack	209.141.61.155	38262	192.168[redacted]	81	1:2500096	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 49
2021-08-30 19:00:25		2	TCP	Misc Attack	46.101.2.225	61000	192.16[redacted]	22	1:2500114	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 58
2021-08-30 18:57:22		2	TCP	Misc Attack	165.22.84.144	42742	192.1[redacted]	8700	1:2500060	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 31
2021-08-30 18:57:07		2	TCP	Misc Attack	45.61.188.118	26645	192.16[redacted]	22	1:2500114	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 58
2021-08-30 18:43:04		2	UDP	Attempted Information Leak	45.143.223.110	5217	192.16[redacted]	5060	1:2008578	ET SCAN Sipvicious Scan
2021-08-30 18:43:04		2	UDP	Attempted Information Leak	45.143.223.110	5217	192.16[redacted]	5060	1:2011716	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
2021-08-30 18:24:36		2	TCP	Misc Attack	209.141.61.155	35930	192.16[redacted]	81	1:2500096	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 49
2021-08-30 18:18:26		2	UDP	Attempted Information Leak	147.135.70.167	5159	192.1[redacted]	5060	1:2008578	ET SCAN Sipvicious Scan
2021-08-30 18:18:26		2	UDP	Attempted Information Leak	147.135.70.167	5159	192.16[redacted]	5060	1:2011716	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
2021-08-30 17:56:48		2	TCP	Potentially Bad Traffic	91.185.216.4	58542	192.16[redacted]	1433	1:2010935	ET SCAN Suspicious inbound to MSSQL port 1433
2021-08-30 17:48:17		2	TCP	Misc Attack	209.141.35.244	9326	192.16[redacted]	22	1:2500094	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 48
2021-08-30 17:23:53		2	TCP	Misc Attack	165.22.84.144	57135	192.168[redacted]	8600	1:2500060	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 31
2021-08-30 17:19:27		2	UDP	Attempted Information Leak	45.95.147.4	5295	192.168[redacted]	5060	1:2008578	ET SCAN Sipvicious Scan
2021-08-30 17:19:27		2	UDP	Attempted Information Leak	45.95.147.4	5295	192.168[redacted]	5060	1:2011716	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)

Fuente: Autor

9.3. Reporte de recursos de servidor

Característica que nos permite conocer en tiempo real (Figura 14), el consumo de recursos utilizado por el servicio de herramientas IDS/IPS sobre el servidor, permitiendo conocer si presenta sobrecargas y la disponibilidad para ejecutar las tareas**.**

Figura 14 Recursos usados por los servicios del sistema

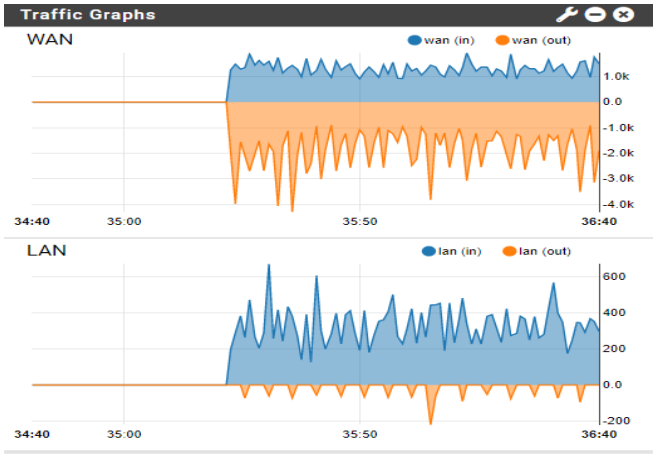


Fuente: Autor

9.4. Trafico de red

EL monitoreo (Figura 15), del tráfico de red entrante y saliente desde internet hacia los servicios WEB publicados, permitirá conocer y determinar si se están presentando anomalías cuando se presenten altos consumos que no sean normales al tráfico que generalmente se presenta con el consumo de los servicios.

Figura 15 Consumo tráfico sobre las interfaces de red

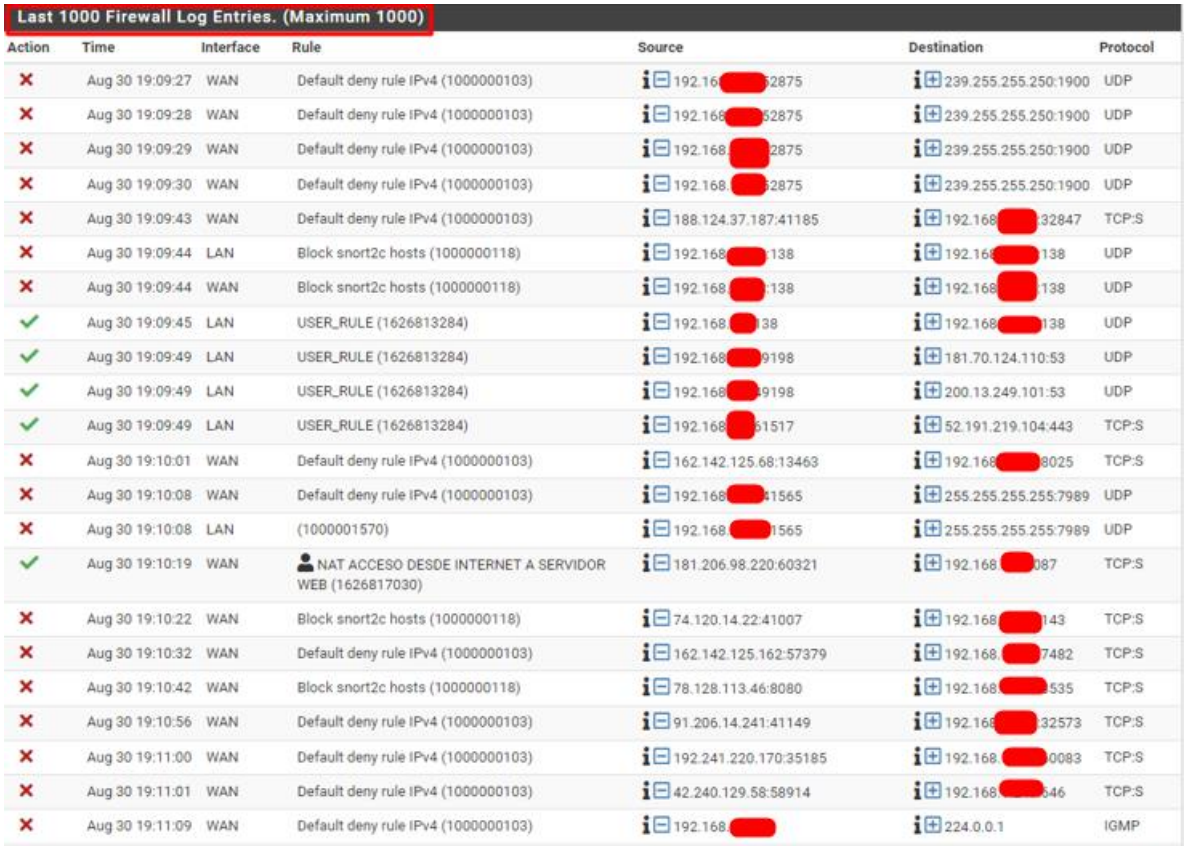


Fuente: Autor

9.5. Conexiones Internet

El registro de conexiones entrantes (Figura 16), que son analizadas para permitir o negar tráfico, se puede visualizar a través de los logs que son registrados para proteger los servicios WEB expuesto hacia internet. (Muestra de log de eventos ya que es muy grande).

Figura 16 Log de conexiones desde internet hacia servicios internos



Last 1000 Firewall Log Entries. (Maximum 1000)

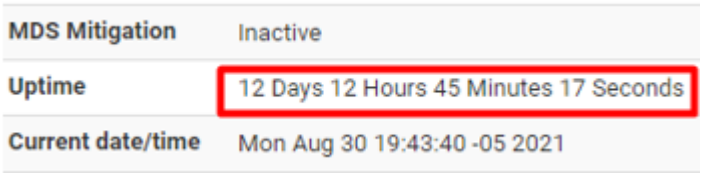
Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Aug 30 19:09:27	WAN	Default deny rule IPv4 (1000000103)	192.16[redacted]2875	239.255.255.250:1900	UDP
✗	Aug 30 19:09:28	WAN	Default deny rule IPv4 (1000000103)	192.168[redacted]2875	239.255.255.250:1900	UDP
✗	Aug 30 19:09:29	WAN	Default deny rule IPv4 (1000000103)	192.168.[redacted]2875	239.255.255.250:1900	UDP
✗	Aug 30 19:09:30	WAN	Default deny rule IPv4 (1000000103)	192.168.[redacted]2875	239.255.255.250:1900	UDP
✗	Aug 30 19:09:43	WAN	Default deny rule IPv4 (1000000103)	188.124.37.187:41185	192.168[redacted]32847	TCP:S
✗	Aug 30 19:09:44	LAN	Block snort2c hosts (1000000118)	192.168[redacted]138	192.168[redacted]138	UDP
✗	Aug 30 19:09:44	WAN	Block snort2c hosts (1000000118)	192.168.[redacted]138	192.168[redacted]138	UDP
✓	Aug 30 19:09:45	LAN	USER_RULE (1626813284)	192.168.[redacted]138	192.168[redacted]138	UDP
✓	Aug 30 19:09:49	LAN	USER_RULE (1626813284)	192.168[redacted]9198	181.70.124.110:53	UDP
✓	Aug 30 19:09:49	LAN	USER_RULE (1626813284)	192.168[redacted]9198	200.13.249.101:53	UDP
✓	Aug 30 19:09:49	LAN	USER_RULE (1626813284)	192.168[redacted]61517	52.191.219.104:443	TCP:S
✗	Aug 30 19:10:01	WAN	Default deny rule IPv4 (1000000103)	162.142.125.68:13463	192.168[redacted]8025	TCP:S
✗	Aug 30 19:10:08	WAN	Default deny rule IPv4 (1000000103)	192.168[redacted]41565	255.255.255.255:7989	UDP
✗	Aug 30 19:10:08	LAN	(1000001570)	192.168.[redacted]1565	255.255.255.255:7989	UDP
✓	Aug 30 19:10:19	WAN	NAT ACCESO DESDE INTERNET A SERVIDOR WEB (1626817030)	181.206.98.220:60321	192.168[redacted]087	TCP:S
✗	Aug 30 19:10:22	WAN	Block snort2c hosts (1000000118)	74.120.14.22:41007	192.168[redacted]143	TCP:S
✗	Aug 30 19:10:32	WAN	Default deny rule IPv4 (1000000103)	162.142.125.162:57379	192.168.[redacted]7482	TCP:S
✗	Aug 30 19:10:42	WAN	Block snort2c hosts (1000000118)	78.128.113.46:8080	192.168[redacted]535	TCP:S
✗	Aug 30 19:10:56	WAN	Default deny rule IPv4 (1000000103)	91.206.14.241:41149	192.168[redacted]32573	TCP:S
✗	Aug 30 19:11:00	WAN	Default deny rule IPv4 (1000000103)	192.241.220.170:35185	192.168.[redacted]0083	TCP:S
✗	Aug 30 19:11:01	WAN	Default deny rule IPv4 (1000000103)	42.240.129.58:58914	192.168[redacted]546	TCP:S
✗	Aug 30 19:11:09	WAN	Default deny rule IPv4 (1000000103)	192.168.[redacted]	224.0.0.1	IGMP

Fuente: Autor

9.6. Disponibilidad del servicio

Característica que permite conocer (Figura 17), el tiempo que el sistema se encuentra activo y en operación después de algún evento de tipo eléctrico o falla no controlada (UPTIME).

Figura 17 Tiempo de disponibilidad del sistema sin caídas



Fuente: Autor

9.7. Reporte detección de intrusos

Sección que permitirá (Figura 18), conocer mediante el proceso de detección y bloqueo todas las IP sospechosas y que la herramienta IDS/IPS no permite conectar hacia los servicios WEB expuestos**.**

Figura 18 Log detección intrusos hacia servicios

Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove
1	185.162.192.32	ET SCAN Suspicious inbound to MSSQL port 1433 -- 2021-08-24 01:07:14	✕
2	211.155.128.203	ET SCAN Suspicious inbound to MSSQL port 1433 -- 2021-08-24 05:33:19	✕
3	185.53.90.85	GPL DNS named version attempt -- 2021-08-24 15:43:53	✕
4	209.141.47.35	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 66 -- 2021-08-21 13:55:20 ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 67 -- 2021-08-07 21:40:43 ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 58 -- 2021-08-28 15:58:34 ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 48 -- 2021-08-30 15:29:49	✕
5	192.241.219.67	ET SCAN Suspicious inbound to MSSQL port 1433 -- 2021-07-21 00:32:18 ET SCAN Suspicious inbound to mySQL port 3306 -- 2021-08-25 02:45:36	✕
6	167.248.133.31	ET SCAN Suspicious inbound to MSSQL port 1433 -- 2021-08-18 15:14:43 ET SCAN Suspicious inbound to PostgreSQL port 5432 -- 2021-08-17 21:33:58	✕
7	5.77.254.236	ET SCAN Suspicious inbound to MSSQL port 1433 -- 2021-08-20 23:00:26	✕
8	74.120.14.21	ET SCAN Suspicious inbound to Oracle SQL port 1521 -- 2021-08-25 10:44:35 ET SCAN Suspicious inbound to MSSQL port 1433 -- 2021-08-25 09:04:26	✕
9	146.88.240.4	GPL RPC portmap listing UDP 111 -- 2021-08-29 22:35:50	✕
10	205.185.125.109	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 64 -- 2021-08-21 23:02:57 ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 65 -- 2021-08-07 23:22:30 ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 57 -- 2021-08-23 21:51:43	✕
11	192.241.218.69	ET SCAN Suspicious inbound to PostgreSQL port 5432 -- 2021-07-21 05:48:09 (spp_sip) Content length mismatch -- 2021-08-29 10:48:51	✕
12	162.142.125.25	ET SCAN Suspicious inbound to PostgreSQL port 5432 -- 2021-08-03 08:31:44 ET SCAN Suspicious inbound to Oracle SQL port 1521 -- 2021-08-19 15:14:14 ET SCAN Suspicious inbound to mySQL port 3306 -- 2021-08-30 02:29:50	✕
13	167.248.133.18	ET SCAN Suspicious inbound to mySQL port 3306 -- 2021-07-21 09:08:23 ET SCAN Suspicious inbound to MSSQL port 1433 -- 2021-08-09 22:59:35 ET SCAN Suspicious inbound to PostgreSQL port 5432 -- 2021-08-11 15:05:20 ET SCAN Suspicious inbound to Oracle SQL port 1521 -- 2021-08-27 16:45:24	✕
14	14.1.112.177	GPL RPC portmap listing UDP 111 -- 2021-08-26 04:38:22	✕
15	219.150.218.243	ET SCAN Suspicious inbound to MSSQL port 1433 -- 2021-08-30 06:48:45	✕

Fuente: Autor

10. CONCLUSIONES

El análisis realizado a la red de PUNTOQOM, permitió conocer los riesgos a los cuales se encuentra expuesto y la necesidad de aumentar el nivel de seguridad con el uso de una herramienta IDS/IPS la cual detecte y prevenga ataques e intrusiones la cual apoyara al firewall sobre el tráfico que se expone hacia internet y mantener la disponibilidad de los servicios expuestos.

Conocer las características de cada una de las herramientas IDS/IPS analizadas, permite determinar la que se implementó (SNORT), conociendo sus funcionalidades, ventajas ante sus competidores, facilidad de configuración y uso, bajo costo de implementación y adaptándose a las necesidades y desarrollo del proyecto.

El uso de software OPEN SOURCE permite que las empresas acceden a soluciones igual de confiables a las herramientas de costo por licencia, teniendo un amplio margen de soporte a nivel mundial con el desarrollo y aporte de comunidades que se dedican día a día a mejorar las herramientas.

Es importante que los administradores de infraestructura realicen un monitoreo constante de las alertas y logs que genera la herramienta, para identificar que se está bloqueando y las causas, con el fin de tener control y seguimiento del funcionamiento de la herramienta.

11. RECOMENDACIONES

Mantener las actualizaciones de la herramienta permitirá que esta actúe día a día contra el tráfico malicioso nuevo que se genere en internet, junto con el backup de las configuraciones ante cualquier evento que interrumpa el servicio.

El monitoreo del tráfico permitirá la generación de nuevas reglas que se requieran de acuerdo con el patrón que se identifique, teniendo un control constante y evitar intrusiones no deseables que afecten la infraestructura.

Analizar nuevos ataques con sus patrones con el objetivo de ir creando nuevas reglas que permitan mantener la base de reglas actualizadas.

Mantener un constante flujo de recomendaciones e instrucciones a los usuarios finales, ayudara en los riesgos informáticos que se pueden generar, concientizarlos de la importancia que tiene las acciones que estos realizan y que pueden llegar a comprometer la seguridad, con el uso de software no deseado, correos de dudosa procedencia, uso de dispositivos de almacenamiento, siendo esto una de las principales causas de fallas de seguridad.

Generar un cronograma con pruebas de seguridad, en un tiempo no mayor a 3 meses, que permita fortalecer los esquemas de seguridad y reforzar lo implementado.

BIBLIOGRAFÍA

ALONSO PALLARES, Federico. Implementación de un sistema de detección de intrusos IDS mediante la inspección del tráfico a través de la red. 2021.

AVILA MALDONADO, Dayannara Cindy; TORRES URRESTO, Joel Anthony. Modelo de detección de intrusos para detectar y evitar la inserción de Malware en una red, basado en técnicas de aprendizaje automático. 2021. Tesis de Licenciatura. Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Sistemas Computacionales.

AVILA-TORRES, Remigio Alfredo; CUENCA-TAPIA, Juan Pablo. Análisis y evaluación de riesgos: aplicado a EMAPAL-EP, basado en la metodología de MAGERIT versión 3.0. Dominio de las Ciencias, 2021, vol. 7, no 4, p. 363-376.

CAMPOS ROPERO, Adrián, et al. Sistema de generación de reglas para la detección y análisis de ataques en red. 2022.

CAMARA COLOMBIANA DE INFORMATICA Y TELECOMUNICACIONES, [sitio web] Colombia: CCIT; Tendencias Cibercrimen Colombia 2019-2020. [Consulta: 12 junio 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

CANDO-SEGOVIA, Mauricio Rodrigo; CHICAIZA, Ricardo Patricio Medina. Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. 3 c TIC: cuadernos de desarrollo aplicados a las TIC, 2021, vol. 10, no 1, p. 17-41.

CASTELLANOS-RODRIGUEZ, Cindy Paola; GARCIA-SUAREZ, Nelson Javier. Entrenamiento de un sistema de detección de intrusos. 2021.

CASTILLO, Jessica Nataly, et al. Modelo para la reducción de riesgos de seguridad informática en servicios web. Cumbres, 2018, vol. 4, no 2, p. 19-30.

CATANZARO, María Elena Tasa, et al. Análisis de información de la gestión de incidentes de seguridad en organizaciones. PURIQ, 2022, vol. 4, no 1, p. 14-30.

CHIQUE VELASQUEZ, Wilson Freddy. Prueba de penetración en la seguridad de la información de la empresa Electro Puno SAA. 2021.

COYLA JARITA, Yony. Implementación de un sistema de detección y prevención de intrusos (IDS/IPS), basado en la norma ISO 27001, para el monitoreo perimetral de la seguridad informática, en la red de la Universidad Peruana Unión–Filial Juliaca. 2019.
DUSSAN CLAVIJO, Ciro Antonio. Políticas de seguridad informática. 2006.

EL CONFIDENCIAl, [sitio web], España, Las pymes del futuro que no cuenten con un experto en ciberseguridad morirán, [Consulta: 12 mayo 2021] Disponible en: https://www.elconfidencial.com/empresas/2019-09-30/pymes-ciberseguridad-informatica-bra_2253931/

FARÍAS ZAMBRANO, Jessica Katiuska; YÉPEZ SALAS, Oscar Eduardo. Diseño de un sistema de detección de intrusos usando SNORT a través del análisis de tráfico en tiempo real y el análisis de protocolos. 2022. Tesis Doctoral. Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones.

GONZÁLEZ BRITO, Henry Raúl; MONTESINO PERURENA, Raydel; GAINZA REYES, Dainys. Riesgos de Seguridad en Pruebas de Penetración Web. 2021.

GRUPO GARATU CLOUD COMPUTING, [sitio web], La Seguridad de tu empresa es innegociable, [Consulta: 27 mayo 2021] Disponible en: https://garatucloud.com/seguridad-informatica-empresa/

GUINEA CABRERA, Miguel Angel. Implementación de un Sistema de Detección de Intrusos (IDS) mediante la inspección de tráfico de la red.

INFO SECURITY MEMO; Gartner Magic Quadrant For Intrusion Detection And Prevention Systems. [Sitio web]. Bogotá: INFO SECURITY MEMO [Consulta: 30 septiembe 2021] Disponible en: https://www.51sec.org/2018/11/10/gartner-magic-quadrant-for-intrusion-detection-and-pre

INSTITUTO NACIONAL DE CIBERSEGURIDAD, [sitio web], España: INCIBE, ¿Qué son y para qué sirven los SIEM, IDS e IPS? [Consulta: 08 junio 2021], Disponible en: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

LEAL RODRÍGUEZ, Yennyfer Paola, et al. Buenas prácticas de seguridad informática aplicado al comercio electrónico para las Pymes colombianas asociada a la norma ISO 27001: 2013 Anexo A. 2021.

LEÓN GUDIÑO, Marcelo Wladimir. Diseño de un sistema de detección de intrusos a través de redes definidas por software para identificar tráfico malicioso. 2021. Tesis de Maestría.

LEYVA, Nelly Victoria Ley, et al. Eficacia y eficiencia de la seguridad de las redes LAN. Cantón Pasaje. Sociedad & Tecnología, 2021, vol. 4, no 2, 205-222 p.

LÓPEZ RAMÍREZ, Marxela. Análisis de riesgos en un sistema de gestión de seguridad informática (SGSI) con metodologías complementarias. 2018. Tesis de Licenciatura. Universidad Piloto de Colombia.

LLANES, Rudibel PerdigÃ³n. Sistemas para la detecciÃ³n de intrusiones en redes de datos de instituciones de salud. Revista Cubana de Informática MÃ© dica, 2021, vol. 13, no 2, p. 440.

MÉNDEZ MORALES, Nelson Enrique, et al. Diseño e implementación del sistema de detección de intrusos en el grupo empresarial Grodco utilizando herramientas de software libre. 2021.

MOHANTA, Abhijit; SALDANHA, Anoop. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware. Apress, 2020.

MOHANTA, Abhijit; SALDANHA, Anoop. IDS/IPS and Snort/Suricata Rule Writing. En Malware Analysis and Detection Engineering. Apress, Berkeley, CA, 2020. p. 819-850.

MOSQUERA MAZACON, María Brigitte. Análisis comparativo sobre las herramientas de Seguridad Informática Open Source: Nessus y Snort. 2022. Tesis de Licenciatura. Babahoyo: UTB-FAFI. 2022.

NUÑEZ NOBOA, Jose Vicente; PERDOMO CORDOVA, Jaime Eduardo. Propuesta de mejora para la gestión de seguridad perimetral de la empresa Fasako SA, Guayaquil–2020. 2021.

OPENWEBINARS, [sitio web] Las 8 mejores herramientas open source de detección de intrusión [Consulta: 15 junio 2021], Disponible en: https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/

ORTEGON CRIOLLO, Juan Pablo, et al. Definición de un sistema de detección y prevención de intrusos en una red para el control de vulnerabilidades usando software libre.

PÁEZ GONZÁLEZ, D. D. Propuesta de metodología de evaluación de seguridad informática, aplicada a proveedores de servicios de pequeñas y medianas empresas (pyme), que accedan a información de personas físicas en el municipio de Toluca, estado de México.

RANGEL MENDEZ, Joel Asunción, et al. Sistemas de detección de intrusiones y gestión de eventos e información de seguridad basados en nuevas tecnologías de código abierto. 2021.

REDES ZONE, [Sitio web], Snort 3 ya es oficial [Consulta 22 junio 2021]. Disponible en: https://www.redeszone.net/noticias/seguridad/snort-3-oficial-caracteristicas-sistema-prevencion-intrusiones/

RESELLER, [Sitio web], Una de cada cinco pymes ha sufrido un ataque en los últimos 12 meses, [Consulta: 15 septiembre 2021] Disponible en: https://www.itreseller.es/seguridad/2020/01/una-de-cada-cinco-pymes-ha-sufrido-un-ataque-en-los-ultimos-12-meses

RODRÍGUEZ CHANG, Leobel; GONZÁLES BRITO, Henry Raúl; PÉREZ FERNÁNDEZ, Dayana. Automatización de pruebas de seguridad a servidores web. 2021.
RODRIGUEZ, O. J. S., de Lema, D. G. P., & García, J. J. B. El sistema de información y los mecanismos de seguridad informática en la pyme. Punto de vista, 7(11), 2016, 79-98.

SAMPER, Juan José Candelario; BOLAÑO, Moisés Rodríguez. Seguridad informática en el siglo XX: una perspectiva jurídica tecnológica enfocada hacia las organizaciones nacionales y mundiales. Publicaciones e Investigación, 2015, vol. 9, p. 153-162.

SÁNCHEZ-SÁNCHEZ, Paola A., et al. "Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia." Información tecnológica 32.5 (2021): 121-128 p.

Seguridad de la información en PyMES, [Sitio web] [Consulta: 29 mayo 2021] Disponible en: http://logopoliskpo.com/2018/06/21/seguridad-de-la-informacion-en-pymes/

SOUCASE IRANZO, Adrián. Implementación de un Sistema de Prevención de Intrusiones (IPS) en un modelo de red industrial. 2021. Tesis Doctoral. Universitat Politècnica de València.

SURICATA, [Sitio web], IDS/IPS Suricata [Consulta: 22 junio 2021], Disponible en: https://blog.elhacker.net/ids-ips-suricata-reglas-rules
UBUNLOG, [Sitio web], Detecta intrusos y supervisa el trafico de la red, [Consulta: 22 junio 2021], Disponible en: https://ubunlog.com/suricata-4-0-supervisa-el-trafico-de-la-red/

UNIVERSIDAD CATOLICA, [Sitio web]. Colombia, Marcos de Referencia, [Consulta: 15 junio 2021], Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/2967/10/parte2.pdf

UNIVERSIDAD DE MEXICO, [sitio web], Mexico; Metodología De La Investigación cuantitativa Y Cualitativa [Consulta: 17 junio 2021], Disponible en: https://www.uv.mx/rmipe/files/2017/02/Guia-didactica-metodologia-de-la-investigacion.pdf

URBINA, Gabriel Baca. Introducción a la seguridad informática. Grupo editorial PATRIA, 2016.

ANEXO A

Resumen Analítica Especializado - RAE

Fecha de Realización:	11/07/2022
Programa:	Especialización Seguridad Informática
Línea de Investigación:	Administración de Tecnologia
Título:	Especialista en Seguridad Informática
Autor(es):	Cardenas Rodriguez Diego Alejandro
Palabras Claves:	IPS, IDS, FIREWALL, MALWARE
Descripción:	Diseñar un sistema de seguridad para la protección y prevención de intrusos ids/ips en la red empresarial de puntoqom, para lo cual se realizan análisis de vulnerabilidades con herramientas de software libre como Kali Linux, Vega y apoyo con software especializado como QUALYS; el resultado de los análisis se convierte en el inicio para la definición de políticas a implementar y el análisis de herramientas finales como solución. Por costos se enfoca en herramientas de software libre donde se analizan varias alternativas y el resultado es la implementación de SNORT. Con la herramienta ya seleccionada se procede a la implementación de SNORT realizando análisis del tráfico para generar políticas y reglas que permitan proteger los servicios.

Fuentes bibliográficas destacadas:

AVILA MALDONADO, Dayannara Cindy; TORRES URRESTO, Joel Anthony. Modelo de detección de intrusos para detectar y evitar la inserción de Malware en una red, basado en técnicas de aprendizaje automático. 2021. Tesis de Licenciatura. Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Sistemas Computacionales.

INSTITUTO NACIONAL DE CIBERSEGURIDAD, [sitio web], España: INCIBE, ¿Qué son y para qué sirven los SIEM, IDS e IPS? [Consulta: 08 junio 2021], Disponible en: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

FARÍAS ZAMBRANO, Jessica Katiuska; YÉPEZ SALAS, Oscar Eduardo. Diseño de un sistema de detección de intrusos usando SNORT a

<table>
<tr><td colspan="2">través del análisis de tráfico en tiempo real y el análisis de protocolos. 2022. Tesis Doctoral. Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones

MOSQUERA MAZACON, María Brigitte. Análisis comparativo sobre las herramientas de Seguridad Informática Open Source: Nessus y Snort. 2022. Tesis de Licenciatura. Babahoyo: UTB-FAFI. 2022.
SOUCASE IRANZO, Adrián. Implementación de un Sistema de Prevención de Intrusiones (IPS) en un modelo de red industrial. 2021. Tesis Doctoral. Universitat Politècnica de València.</td></tr>
<tr><td>Contenido del documento:</td><td>1. DEFINICIÓN DEL PROBLEMA
1.1 ANTECEDENTES DEL PROBLEMA
1.2 FORMULACIÓN DEL PROBLEMA
2 JUSTIFICACIÓN
3 OBJETIVOS
3.1 OBJETIVOS GENERAL
3.2 OBJETIVOS ESPECÍFICOS
4 MARCO REFERENCIAL
4.1 MARCO CONCEPTUAL Y TEÓRICO
4.2 MARCO geografico
4.3 ANTECEDENTES O ESTADO ACTUAL
4.4 MARCO CIENTÍFICO O TECNOLÓGICO
4.5 MARCO LEGAL
5 DISEÑO METODOLÓGICO
6. Realizar levantamiento del estado actual de la red de los equipos que facilitan la comunicación de la empresa y que soportan los sistemas de información, examinando los riesgos y fallas de seguridad
7. Sistema de detección y prevención de intrusos para la seguridad informática, mejorando el monitoreo, corrección oportuna y garantizar una máxima seguridad
7.1 Suricata
7.2 Snort
7.3 Bro
7.4 SELECCIÓN HERRAMIENTA
8. Proponer políticas de seguridad dentro del ids/IPS que permitan el correcto funcionamiento e implementación del sistema de deteccion de intrusos
8.1 Reglas IPS
8.2 Reglas por Malware
8.3 Reglas de inspección de trafico
8.4 Firewall</td></tr>
</table>

	9. Elaborar la documentación de la herramienta de prevención y detección seleccionada que sirva como manual de funcionamiento 9.1 Tendencia de ataques bloqueados 9.2 Log de bloqueos hacia servicio WEB 9.3 Reporte de recursos de servidor 9.4 Trafico de red 9.5 Conexiones Internet 9.6 Disponibilidad del servicio 9.7 Reporte detección de intrusos 10. CONCLUSIONES 11. RECOMENDACIONES BIBLIOGRAFÍA
Marco Metodológico:	El presente trabajo es de carácter descriptivo, va a manejar un enfoque cuantitativo y también cualitativo para lo cual se realizará una previa investigación de los ataques más frecuentes sobre los servicios de la compañía PUNTOQOM y los sistemas, lo cual permitirá generar las reglas que se aplicaran como sistema de protección de bloqueo.
Conceptos adquiridos:	**DOMINIO DE COLISIÓN**: Segmento físico presente en una red de computadores donde las tramas interfieren unas con otras **IPS**: Sistema de prevención de intrusos **NIDS**: Sistema de detección de intrusos en red **DIDS**: Sistema de detección de intrusos distribuido **SIEM**: Es una herramienta utilizada para de manera centralizada recopilar eventos que serán analizados e interpretados con el fin de detectar comportamientos o patrones que afecten la seguridad de una organización
Conclusiones:	El análisis realizado a la red de PUNTOQOM, permitió conocer los riesgos a los cuales se encuentra expuesto y la necesidad de aumentar el nivel de seguridad con el uso de una herramienta IDS/IPS la cual detecte y prevenga ataques e intrusiones la cual apoyara al firewall sobre el tráfico que se expone hacia internet y mantener la disponibilidad de los servicios expuestos. Conocer las características de cada una de las herramientas IDS/IPS analizadas, permite determinar la que se implementó (SNORT), conociendo sus funcionalidades, ventajas ante sus competidores, facilidad de configuración y uso, bajo costo de

	implementación y adaptándose a las necesidades y desarrollo del proyecto. El uso de software OPEN SOURCE permite que las empresas acceden a soluciones igual de confiables a las herramientas de costo por licencia, teniendo un amplio margen de soporte a nivel mundial con el desarrollo y aporte de comunidades que se dedican día a día a mejorar las herramientas. Es importante que los administradores de infraestructura realicen un monitoreo constante de las alertas y logs que genera la herramienta, para identificar que se está bloqueando y las causas, con el fin de tener control y seguimiento del funcionamiento de la herramienta.