UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS “ESPOG”

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021-CES

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del artículo
ANÁLISIS DE SISTEMAS DE DETECCIÓN DE INTRUSOS CON HERRAMIENTAS OPEN SOURCE
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Autora:
SELENE PAOLA ORTEGA RENDON
Tutor:
MSc. Pablo Recalde

Quito – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, Pablo Marcel Recalde Varela con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: ANÁLISIS DE SISTEMAS DE DETECCIÓN DE INTRUSOS CON HERRAMIENTAS OPEN SOURCE.

Elaborado por: **SELENE PAOLA ORTEGA RENDON**, de C.I: 0940799059, estudiante de la Maestría: SEGURIDAD INFORMÁTICA, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M. septiembre de 2022

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Ortega Rendon Selene Paola con C.I: 0940799059, autora del proyecto de titulación denominado: ANÁLISIS DE SISTEMAS DE DETECCIÓN DE INTRUSOS CON HERRAMIENTAS OPEN SOURCE.

Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autora del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M. septiembre de 2022

Selene Ortega K.

ORCID: 0000-0002-5486-7422

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Actualmente todos los sistemas y redes se pueden ver comprometidos frente a vulnerabilidades de seguridad, es por eso que el concepto de seguridad informática en los últimos años se ha popularizado.

La seguridad informática realiza la protección de todos los sistemas y redes para evitar que estos sean manipulados para causar daños a la información. Entre los cuales es importante contar con un sistema de detección de intrusos para la prevención de intrusiones. (¿Qué es la Seguridad Informática?, s. f.)

Según indica (Ortiz, 2021). El último informe anual de Kaspersky indica que en Ecuador la tasa de crecimiento de los ataques informáticos es del 75%, lo que equivale a unos 89 ataques por minuto. Según indican los expertos, esto no solo es relevante para grandes empresas o los bancos, como antes, sino que en la actualidad existe más interés por la información de medianas y pequeñas empresas (pymes).

La mayoría de las empresas pequeñas destinan poca inversión a la seguridad de sus sistemas o redes de comunicación porque suelen pensar que al ser pequeñas nunca les va a suceder, en la actualidad vemos como cualquier tipo de empresa y personas son atacadas por hacker de todo el mundo que simplemente se encuentran en la búsqueda de algún agujero de seguridad para ingresar y aprovechar la situación para robar información; y luego solicitar rescate para su liberación.

En 2020 debido al confinamiento provocado por el virus SARS-COV-2 muchas empresas se vieron en la necesidad de migrar sus sistemas a cloud o a su vez dar accesos externos a sus colaboradores para realizar teletrabajo, ya sea por medio de una Red Virtual Privada (VPN) o de aplicaciones de control remoto. Con esto la seguridad se vio mucho más afectada, en la mayoría de los casos las migraciones fueron tan rápidas que pasaron por alto temas de seguridad de los sistemas y de la información. (Ecuador: Políticas en el teletrabajo y seguridad de la información, 2021)

Este trabajo de titulación promueve la innovación de infraestructuras de seguridad informática de manera que toda empresa pueda brindar confidencialidad, integridad, disponibilidad y autenticación de la información a los usuarios finales. Cabe recalcar que los sistemas de seguridad que se analizan en este trabajo son de código abierto y se pretende dar una solución más viable a las empresas que están surgiendo y luchan por posicionar su marca en el mercado.

El presente trabajo de investigación abarca el siguiente Objetivo de Desarrollo Sostenible (ODS) de la ONU:

- Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación. (ODS, 2017)

Problema de investigación

Las redes y sistemas de información siempre están en constante peligro de infiltración, convirtiéndose en un problema diario para las organizaciones y los departamentos de TI. Es por eso que los sistemas de detección de intrusos del idioma inglés Intrusion Detection Systems (IDS) son una solución a dicha problemática que se presenta en la mayoría de las organizaciones, estos sistemas se encargan de prevenir la infiltración y alertar o a su vez realizar alguna acción cuando detectan alguna anomalía.

Según indica (Ciberpyme, 2022). El gran problema de la falta de recursos en materia de ciberseguridad es que, en caso de existir un ataque, o un problema en la seguridad del sistema, puede tardar en ser detectado y subsanado. Durante ese periodo, se podría haber perdido información muy sensible de la organización, y las consecuencias, a niveles económicos podrían ser fatales.

¿Con el uso de herramientas open source de monitoreo se puede minimizar los riesgos de seguridad de las redes?

Objetivo general

Realizar una comparativa de los IDS Snort y Suricata para recomendar su posterior implementación en la Empresa Tracape S.A.

Objetivos específicos

- Contextualizar los fundamentos teóricos sobre los Sistemas de detección de intrusos (IDS).
- Analizar las herramientas Open Source Snort y Suricata y los beneficios que cada una posee.
- Recomendar la herramienta que mejor se adapte para una futura implementación, tomando en cuenta la guía de referencia NIST 800-94.
- Validar el impacto que puede causar la implementación.

Vinculación con la sociedad y beneficiarios directos:

Este trabajo de investigación muestra a la comunidad y a la empresa para la cual se está realizando el análisis, que existen herramientas Open Source que son de fácil acceso y no es necesario una gran inversión económica para proteger sus sistemas o redes de comunicación.

Teniendo en cuenta los Objetivos de Desarrollo Sostenible de la ONU, el presente trabajo se encuentra dentro del objetivo nueve “Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación”.

El ODS nueve tiene como objetivo contar con una infraestructura sostenible, robusta y de calidad para todos en 2030, promover una industria sostenible que utilice tecnologías y procesos industriales limpios y eco amigables con el medio ambiente, promover la tecnología, la innovación y la investigación, para lograr el acceso al conocimiento y la información, a través de Internet. («9 Industria innovación e infraestructura», s. f.)

La innovación y el progreso tecnológico son la clave para aportar soluciones duraderas a los retos económicos y medioambientales. A nivel mundial, la inversión en investigación y desarrollo (I+D), como porcentaje del PIB, aumentó del 1,5 % en 2000 al 1,7 % en 2015, y se mantuvo casi al mismo nivel en 2017. Sin embargo, en las regiones en desarrollo fue inferior al 1 %. (ODS, 2017)

Las infraestructuras de comunicaciones han aumentado en los últimos años, hoy en día la mitad de población a nivel mundial se encuentra conectada y casi toda la población global se encuentra asentada en áreas que cuentan con cobertura móvil. (ODS, 2017)

Según (Pathak, 2022). El uso de soluciones IDS permite automatizar las tareas de seguridad. Ya no se necesita monitorear y configurar todo de forma manual; los sistemas IDS permiten automatizar estas tareas para liberar el tiempo en el crecimiento de los negocios. Con esto no solo reduce el esfuerzo, sino que también ahorra costos.

CAPÍTULO I: DESCRIPCIÓN DEL ARTÍCULO PROFESIONAL

1.1. Contextualización general del estado del arte

Sistemas de Detección de Intrusos (IDS)

La detección de intrusos se refiere al monitoreo de eventos que pueden ocurrir en un sistema informático e informar a los administradores de seguridad de manera automatizada; además se pueden utilizar para otros fines, como identificar problemas con las políticas de seguridad, documentar las amenazas existentes. Los IDS son herramientas necesarias para la infraestructura de seguridad de casi todas las organizaciones. (Scarfone y Mell, 2007)

Los sistemas detectores de intrusiones del idioma inglés Intrusion Detection Systems se ubican sobre los sistemas que desean ser protegerse, pero sin realizar ninguna otra tarea se servicio aparente al cliente, por lo que puede preguntarse cuál es su verdadera función. Como se ha indicado anteriormente, su principal misión radica en el pilar básico de la detección de ataques a la seguridad del sistema, que es un eslabón más en la cadena de la seguridad, al igual que otros sistemas como los cortafuegos se centran en la prevención o como las copias de seguridad se centran en la recuperación. (Álvarez y Marañón, 2004)

Tipos de IDS

- **Basado en el host (HIDS)**

Este sistema monitorea las características de un solo host y los eventos que ocurren dentro ese host, con la misión de identificar actividades sospechosas. (Guías NIST: un sustento metodológico para los analistas de ciberseguridad, 2022).

- **Basado en la red (NIDS)**

Supervisa el tráfico de red en busca de determinados dispositivos o segmentos de la red y analiza la actividad de la red y aplicaciones para identificar actividades sospechosas. (Guías NIST: un sustento metodológico para los analistas de ciberseguridad, 2022).

Comparación de tipos de tecnologías IDS

Tabla 1.
Comparación de tipos de tecnología IDS NIST 800-94

Tecnología IDS	Actividad detectada	Alcance por sensor o agente	Fortalezas
Basado en la red (NIDS)	Actividad de la capa TCP/IP de red, transporte y aplicación	Múltiples subredes y grupos de hosts	Capaz de analizar la más amplia gama de protocolos de aplicación
Basado en el host (HIDS)	Actividad del sistema operativo (SO) y de host de aplicación; actividad de la capa TCP/IP de red, transporte y aplicación	Host individual	Puede analizar la actividad que se transfirió en comunicaciones cifradas de extremo a extremo

Nota: Scarfone y Mell (2007, p. 8-1)

Componentes de los IDS

- **Sensores o agentes:** se encargan de monitorear y analizar la actividad.
- **Servidor de gestión:** equipo centralizado que recibe información de los sensores o agentes y los gestiona.
- **Servidor de base de datos:** almacena información de los eventos registrados por los sensores, agentes o servidores de administración.
- **Consola:** interfaz para los usuarios y administradores de los IDS.

Metodologías de detección comunes

- **Detección basada en firmas:** es el método más simple, consiste en comparar firmas con eventos observados para identificar posibles incidentes, es eficaz para detectar amenazas conocidas.
- **Detección basada en anomalías:** puede ser muy efectivo para detectar amenazas desconocidas, consiste en comparar que actividades se consideran normales con los eventos observados para identificar amenazas
- **Análisis de protocolo con estado:** compara perfiles ya establecidos de definiciones que siempre son aceptadas de actividad de protocolo benigna en cada estado de

protocolo con los eventos observados para identificar desviaciones. (Scarfone y Mell, 2007)

Sistemas IDS open source

Existen varios IDS open source, pero para el presente estudio se analizará Snort y Suricata ambos son sistemas IDS basados en red (NIDS).

Snort

Snort es un sistema Open Source de detección de intrusos basado en red, implementa un motor de detección de ataques que permite registrar, alertar y responder ante anomalías en tiempo real. Snort revisa registros de paquetes en tiempo real, analiza el tráfico, los protocolos y el contenido. Colecciona información de muchos recursos del sistema y de la red, su función principal es capturar paquetes de datos según lo determinado por la pila de protocolos TCP/IP. Un IDS utilice la metodología de detección basada en firmas genera una alerta para informar a los administradores siempre que encuentre datos que concuerdan con el contenido encontrado en una firma. (Janampa et al., 2021)

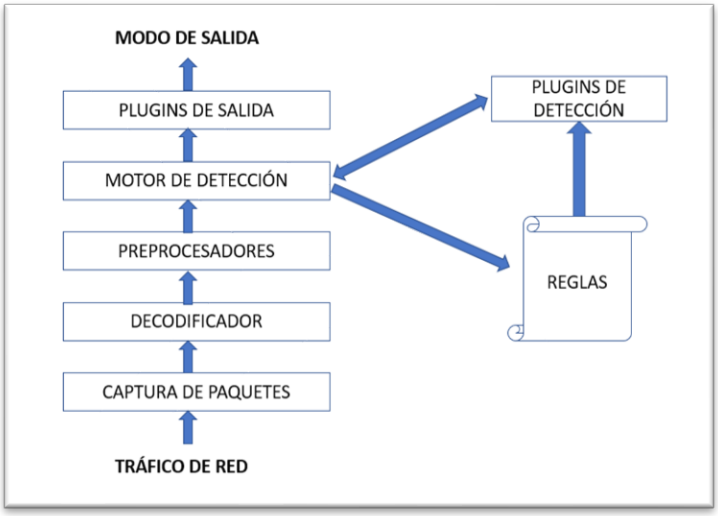
Características de Snort

- Monitoreo de tráfico en tiempo real.
- Creación de registros.
- Registro de paquetes.
- Reglas fáciles de implementar.
- Análisis de protocolo.
- Instalable en cualquier entorno de red.
- Código abierto.

Arquitectura

La arquitectura de Snort basa en simplicidad, flexibilidad y rendimiento. Se divide en tres subsistemas, es decir, el subsistema de alertas y registros, decodificador de paquetes y el motor de detección. Estos módulos o plugins se encuentran por encima de la librería de captura de paquetes libpcap, lo que proporciona a Snort de las funciones necesarias para un sniffer de paquetes, mediante el uso de una interfaz de red configurada en modo promiscuo. La configuración de las reglas, del programa y la creación de las estructuras de datosse realizan antes de que se inicie la parte del sniffer, lo que hace que el procesamiento mínimo por paquete aumente al realizar funciones básicas del programa. (Arquitectura de Snort - Introducción a los Sistemas de Detección de Intrusos, s. f.)

Figura 1.
Arquitectura de Snort



Nota: tomado de SNORT. (2013, diciembre 10). SNORT. https://snortudenar.wordpress.com/snort-2/

Detalle del análisis de paquetes en Snort

Decodificador de paquetes: toma los paquetes de la interfaz de red y los prepara para su posterior procesamiento.

Reprocesadores: preparan cada paquete para simplificar la tarea de análisis.

Motor de detección: es el núcleo del IDS. Es el encargado de evaluar si un paquete concreto supone un riesgo.

Módulo de alerta: genera una alarma en caso de que un paquete viole la política de seguridad.

Módulo de salida: se encarga de enviar las alarmas al personal o al sistema de gestión previsto. (Ortega, 2021)

Suricata

Es un IDS basado en red libre y gratuito, su característica principal es la capacidad de analizar certificados TLS/SSL, solicitudes HTTPS y DNS. También se basa en reglas para detectar intrusiones para su posterior bloqueo por parte del firewall. (Ortega, 2021)

Suricata ofrece compatibilidad con las reglas de Snort, además que es multi-aplicación con subprocesos. Funciona en Linux, FreeBSD, Open BSC, Mac y Windows.

Características de Suricata

- Suricata es una herramienta de detección de intrusos en la red completa, rápida y potente, gratuita y de código abierto.
- Esta herramienta es capaz de detección de intrusiones en tiempo real (IDS), sistema de monitoreo de seguridad de red (NSM) y manejo de pcap fuera de línea.
- Soporta formatos de entrada y salida estándar como JSON y YAML, se integra con herramientas como SIEM, Splunk, OSSIM, SIEMonster, Logstash/ElasitcSearch, Kibana.
- Detección automática de protocolos.
- Soporta Script en Lua para la detección de amenazas.

Tabla de comparación Snort vs Suricata

Tabla 2.
Tabla de comparación Snort vs Suricata

Parámetro	Snort	Suricata
Multiproceso	No.	Si.
Sistema Operativo	Todos.	Todos.
Desarrollador	Sourcefire.	Open Information Security Foundation.
Reglas	Reglas VRT Snort, reglas SO, reglas de preprocesador, reglas emergentes de amenazas.	Reglas de amenazas emergentes, VRT reglas de.
Instalación	Manual o utilizando paquetes.	Manual o utilizando paquetes.
Documentación	Proporciona soluciones a problemas comunes.	No está documentado.
Costo	Libre.	Libre.
GUI	Compatible con gran número de GUIs.	Muy pocos.

Nota: tomado de Singh, P. K., Kar, A. K., Singh, Y., Kolekar, M. H., y Tanwar, S. (2019). *Proceedings of ICRIC 2019: Recent Innovations in Computing*. Springer Nature.

Normativa NIST

El Instituto Nacional de Estándares y Tecnología (NIST) es una organización pública de Estados Unidos dedicada a crear conocimiento, desarrollar recursos y organizar programas de capacitación en muchas áreas. (Guías NIST: un sustento metodológico para los analistas de ciberseguridad, 2022)

El marco NIST brinda una variedad de buenas prácticas en muchas áreas de ciberseguridad. Desde la gestión de riesgo, hasta el sistema de gobierno de ciberseguridad. abarcan la realización de pentesting o la gestión de incidentes. (Guías NIST: un sustento metodológico para los analistas de ciberseguridad, 2022)

Recomendaciones de NIST para elección IDS

La guía NIST 800-94 aporta con una serie de recomendaciones al momento de elegir una herramienta IDS, a continuación (Scarfone y Mell, 2007) detalla las principales recomendaciones:

- **Requisitos generales**
  - **Entorno de sistema de red:** conocer las características de los sistemas y red de las empresas para seleccionar el IDS adecuado.
  - **Metas y objetivos:** que se desean alcanzar con la implementación.
  - **Seguridad y otras políticas de TI:** en caso de existir políticas se deben revisar, ya que son especificaciones de las características que deben tener los productos IDS.
  - **Requisitos externos:** requisitos de seguridad por ley establecidos, requisitos de auditoría para mejores prácticas de seguridad o diligencia, requisitos de acreditación de los sistemas, requisitos para la investigación policial o resolución de incidentes de seguridad, requisitos para adquirir productos evaluados a través de un proceso independiente y requisitos de criptografía.
  - **Restricciones de recursos:** se debe considerar el presupuesto para la adquisición y el soporte del hardware, software e infraestructura.
- **Requisitos de capacidad de seguridad**
  - **Capacidades de recopilación de información:** identificar la capacidad de recopilación necesarias de información de detección y evaluación de cada IDS por la capacidad que ofrece.
  - **Capacidades de registro**: evaluar de cada IDS la capacidad de registro, calidad del registro; desde la integridad hasta la precisión, ya que ambas afectan la capacidad para realizar un análisis.

- **Capacidades de detección**: entre los factores que se deben considerar están los siguientes: actividades de forma integral y parcial, los tipos de incidentes que puede identificar, alcance de la detección, configuración inicial predeterminada debe ser razonables, efectividad para detectar ataques maliciosos conocidos o desconocidos, mecanismos de respuesta que ofrecen, personalización de las capacidades de detección por firmas, política y otros por medio de los administradores.
- **Capacidades de prevención**: determinar si el IDS necesitará o no acciones de prevención presentes y futuras, además de evaluar las capacidades actuales de prevención.

- **Requisitos de rendimiento:** va a depender mucho de la configuración y ajuste de cada producto.
- **Requisitos de gestión:** muy importante para que el producto se utilice eficazmente.
  - **Diseño e implementación**
    - **Confiabilidad:** para que se cumpla la confiabilidad se debe considerar qué tipo de hardware redundante incluye o están disponibles por separado, características de redundancia y si el producto puede utilizar varios servidores de administración e implementar múltiples sensores.
    - **Interoperabilidad**: todos los sistemas deben interoperar de manera adecuada, entre ellos fuentes de entrada de datos, software de gestión y análisis de registros, sistemas de reconfiguración.
    - **Escalabilidad:** considerar necesidades actuales y futuras, entre las cuales se pueden considerar: cantidad de sensores o agentes, variedad de dispositivos disponibles, cuantas redes se puede monitorear simultáneamente, mejoras de capacidades de almacenamiento.
    - **Seguridad:** proteger los datos almacenados, funciones de autenticación, control de acceso y auditoría para el uso y administración.
    - **Operación y mantenimiento:**
      - **Uso diario:** como se debe realizar el monitoreo diario, reportes de alertas, estado de usuarios y administradores sea fácil de analizar, notificaciones sobre eventos, cuanta información respalda, formatos de informe que ofrecen.

- **Mantenimiento:** se debe considerar los mecanismos de mantenimiento local y remoto, protecciones de seguridad, como se pueden respaldar y restaurar los ajustes de configuración.
- **Actualizaciones:** considerar la frecuencia que tienen actualizaciones, tipos de actualizaciones que requieren reinicios, cómo distribuir las actualizaciones a todos los componentes, además de evaluar como las actualizaciones pueden afectar a las configuraciones existentes.

  - **Capacitación, documentación y soporte técnico:** las empresas deben considerar tener recursos disponibles para que los administradores y usuarios conozcan todas las funcionalidades y características del IDS, así también tener toda la documentación como por ejemplo guías de instalación, usuarios, administrador.

- **Costos de ciclo de vida:** determinar costos estimados, entre los cuales se puede identificar costos iniciales que incluyen hardware y software, costos de instalación y configuración, costos de personalización.
- **Evaluación de productos:** entre las recomendaciones se puede encontrar laboratorio de pruebas o pruebas en ambientes reales, experiencia previa en organizaciones o individuos, información proporcionada por el proveedor como manuales, documentos técnicos.

  - **Desafíos de las pruebas de IDS:** las organizaciones que puedan realizar prácticas reales de los productos IDS tendrán datos precisos de sobre como funcionará el IDS en su organización, sin embargo, no es tan fácil lograr debido los recursos que se necesitan para realizar pruebas, en caso de que una empresa realice pruebas debe crear sus propias metodologías ya que no existen ningún modelo de metodología ya establecido.
  - **Recomendaciones para realizar evaluaciones IDS:** realizar pruebas puede resultar muy útil para evaluar si se cumplen los requisitos que la organización estableció al inicio acerca de capacidades de seguridad, rendimiento, mantenimiento y operación de los sistemas IDS. Durante las pruebas no se debe interrumpir las operaciones de la organización.

1.2. Proceso investigativo metodológico

Enfoque de la investigación

Se utilizará el enfoque cualitativo, el cual sirve para investigar causas, emociones y valores subyacentes, antes de desarrollar una hipótesis. El propósito de los estudios cualitativos es

descubrir y explicar porque ocurre un fenómeno o comportamiento. («Diferencia entre investigación cualitativa y cuantitativa», 2017)

Tipo de investigación

La investigación que se realizo es documental y comparativo, que se puede definir según (Uriarte, 2020) como: Una estrategia para comprender y analizar la realidad teórica o empírica a través de la revisión, cotejo, comparación o comprensión de diferentes tipos de fuentes que tratan de un tema en particular, a través de un enfoque sistemático y organizado.

Población y muestra

En el presente trabajo de investigación se considera como población al departamento de TI de la empresa Tracape, se pueden realizar futuras comparaciones con otras empresas pymes para realizar validaciones de los resultados obtenidos en el presente trabajo.

Métodos

Método inductivo

Permite extraer conclusiones generales a partir de premisas particulares, es decir, basa su estudio en la observación y en la experimentación de diversos hechos para obtener una conclusión que involucre el conjunto de casos estudiados. (Pereyra, 2020)

Con la aplicación del método inductivo se pudo determinar cuál de las dos herramientas analizadas de detección de intrusos se adapta mejor para una futura implementación.

Método deductivo

Es el estudio de un fenómeno particular basándose en uno general, es decir, se particularizan los resultados. El método deductivo tiene la característica de que las conclusiones de la deducción son verdaderas, si las premisas también lo son. Entonces, si un fenómeno se ha verificado para un determinado grupo de personas, se puede inferir que este se aplica a uno de estos individuos. (Pereyra, 2020)

El método deductivo se utilizó para analizar conceptos fundamentales de la guía NIST y aplicar en los sistemas de detección de intrusos analizados en el presente trabajo de investigación.

1.3. Análisis de resultados

Luego de realizar el análisis de los sistemas de detección de intrusos con las herramientas open source Snort y Suricata se pudo identificar que si bien ambos son sistemas libres es necesario inversión adicional para realizar la implementación.

Snort se encarga de observar el tráfico que coincide con sus reglas y alerta sobre la posible intrusión, pero así mismo snort no puede ejecutar múltiples subprocesos.

Por su parte Suricata es un sistema más actual, es un detector de intrusiones robusto y rápido, que a diferencia de Snort soporta múltiples subprocesos, además que soporta las reglas de la capa de aplicación de Snort.

Según el estudio realizado por (Singh et al., 2019) indica que hicieron una comparación del rendimiento de Suricata con Snort basada en la escalabilidad y el rendimiento, realizaron 8600 pruebas diferentes sobre la cantidad de núcleos utilizados (1-24 núcleos) el conjunto de las reglas utilizados para la comparación de firmas, la carga de trabajo utilizada para obtener los resultados y la configuración tanto del IDS. Las métricas que utilizaron para la comparación fueron paquetes por segundo (PPS) procesada por cada IDS, la cantidad de memoria utilizada por cada proceso IDS y el uso de la CPU. Los resultados indicaron que tanto Snort como Suricata eran escalables, pero Suricata superó a Snort en casi todas las pruebas. Suricata también mostró un uso de memoria promedio más bajo y uso de CPU promedio más bajo.

Luego del análisis anterior se puede recomendar para la empresa Tracape la implementación de la herramienta Suricata, para esto se debe trabajar con el departamento de TI de la organización.

Después de realizar el análisis de las herramientas open source Snort y Suricata se puede determinar que, si pueden minimizar los riesgos de seguridad de las redes de las organizaciones, esto va a depender de que la implementación se realice siguiendo los parámetros adecuados y necesarios para la organización.

ANÁLISIS DE SISTEMAS DE DETECCIÓN DE INTRUSOS CON HERRAMIENTAS OPEN SOURCE

ANALYSIS OF INTRUSION DETECTION SYSTEMS WITH OPEN SOURCE TOOLS

1.1. Resumen

Actualmente todos los sistemas y redes se pueden ver comprometidos frente a vulnerabilidades de seguridad, es por eso que el concepto de seguridad informática se ha popularizado en los últimos años.

El presente trabajo de investigación tiene como objetivo realizar el análisis de los IDS open source Snort y Suricata, para su posterior implementación aplicando recomendaciones de la guía NIST 800-94 que proporciona conceptos básicos sobre la detección de intrusos, las metodologías generales de detección de intrusiones y una serie de recomendaciones de implementación, operación y selección de IDS.

El tipo de investigación utilizada fue comparativa y documental, además de utilizarse el método inductivo y deductivo.

a. **Palabras clave:** IDS, snort, suricata, NIST

1.2. Abstract

Currently all systems and networks can be compromised by security vulnerabilities, which is why the concept of computer security has become popular in recent years.

The objective of this research work is to carry out the analysis of the open source IDS Snort and Suricata, for its subsequent implementation by applying recommendations of the NIST 800-94 framework that provides us with basic concepts on intrusion detection, general intrusion detection methodologies and a series of recommendations for the implementation, operation and selection of IDS.

The type of research used was comparative and documentary, in addition to using the inductive and deductive method.

a. **Keywords**: IDS, snort, suricata, NIST

1.3. Introducción

Las redes y sistemas de información siempre están en constante peligro de infiltración, convirtiéndose en un problema diario para las organizaciones y los departamentos de TI. Es por eso que los sistemas IDS son una solución a dicha problemática que se presenta en la

mayoría de las organizaciones, estos sistemas se encargan de prevenir la infiltración y alertar o a su vez realizar alguna acción cuando detectan alguna anomalía.

Según (Ciberpyme, 2022). El gran problema de la falta de recursos en materia de ciberseguridad es que, en caso de existir un ataque, o un problema en la seguridad del sistema, puede tardar en ser detectado y subsanado. Durante ese periodo, se podría haber perdido información muy sensible de la organización, y las consecuencias, a niveles económicos podrían ser fatales.

La mayoría de las empresas pequeñas destinan poca inversión a la seguridad de sus sistemas o redes de comunicación porque se suelen pensar que al ser pequeñas nunca les va a suceder, en la actualidad vemos como cualquier tipo de empresa y personas son atacadas por hacker de todo el mundo que simplemente se encuentran en la búsqueda de algún agujero de seguridad para ingresar y aprovechar la situación para robar información; y luego solicitar rescate para su liberación.

Los sistemas de detección de intrusos del idioma inglés Intrusion Detection Systems (IDS) es un software que se encarga de detectar posibles incidentes o intrusiones en los sistemas o redes, además de registrar información para luego ser analizada por los administradores, pueden ser utilizados también para identificar problemas con las políticas de seguridad.

Existen dos tipos de IDS; los basados en red (NIDS) que se encargan de supervisar el tráfico de red en busca de determinados dispositivos o segmentos de la red y analiza la actividad de la red y aplicaciones para identificar actividades sospechosas. (Guías NIST: un sustento metodológico para los analistas de ciberseguridad, 2022).

También existen los basado en host (HIDS), como indica (Guías NIST: un sustento metodológico para los analistas de ciberseguridad, 2022) se encargan de monitorear las características de un solo host y los eventos que ocurren dentro ese host, con la misión de identificar actividades sospechosas.

Entre los componentes de los IDS están los sensores o agentes que se encargan de monitorear y analizar las actividades, servidor de gestión que es el equipo centralizado que recibe información de los sensores o agentes y los gestiona, servidor de base de datos que almacena información de los eventos registrados por los sensores, agentes o servidores de administración y consola que es la interfaz para los usuarios y administradores de los IDS.

El presente trabajo de investigación utilizara Snort y Suricata para revisar sus diferencias y determinar cuál sería la mejor opción para implementar en la empresa Tracape S.A.

Snort

Snort es un sistema Open Source de detección de intrusos basado en red, implementa un motor de detección de ataques que permite registrar, alertar y responder ante anomalías en tiempo real. Snort revisa registros de paquetes en tiempo real, analiza el tráfico, los protocolos y el contenido. Colecciona información de muchos recursos del sistema y de la red, su función principal es capturar paquetes de datos según lo determinado por la pila de protocolos TCP/IP. Un IDS utilice la metodología de detección basada en firmas genera una alerta para informar a los administradores siempre que encuentre datos que concuerdan con el contenido encontrado en una firma. (Janampa et al., 2021)

Características de Snort

- Monitoreo de tráfico en tiempo real.
- Creación de registros.
- Registro de paquetes.
- Reglas fáciles de implementar.
- Análisis de protocolo.
- Instalable en cualquier entorno de red.
- Código abierto.

Detalle del análisis de paquetes en Snort

- **Decodificador de paquetes:** toma los paquetes de la interfaz de red y los prepara para su posterior procesamiento.
- **Reprocesadores:** preparan cada paquete para simplificar la tarea de análisis.
- **Motor de detección:** es el núcleo del IDS. Es el encargado de evaluar si un paquete concreto supone un riesgo.
- **Módulo de alerta:** genera una alarma en caso de que un paquete viole la política de seguridad.
- **Módulo de salida:** se encarga de enviar las alarmas al personal o al sistema de gestión previsto. (Ortega, 2021)

Suricata

Es un IDS basado en red libre y gratuito, su característica principal es la capacidad de analizar certificados TLS/SSL, solicitudes HTTPS y DNS. También se basa en reglas para detectar intrusiones para su posterior bloqueo por parte del firewall. (Ortega, 2021)

Suricata ofrece compatibilidad con las reglas de Snort, además que es multi-aplicación con subprocesos. Funciona en Linux, FreeBSD, Open BSC, Mac y Windows.

Características de Suricata

- Suricata es una herramienta de detección de intrusos en la red completa, rápida y potente, gratuita y de código abierto.
- Esta herramienta es capaz de detección de intrusiones en tiempo real (IDS), sistema de monitoreo de seguridad de red (NSM) y manejo de pcap fuera de línea.
- Soporta formatos de entrada y salida estándar como JSON y YAML, se integra con herramientas como SIEM, Splunk, OSSIM, SIEMonster, Logstash/ElasitcSearch, Kibana.
- Detección automática de protocolos.
- Soporta Script en Lua para la detección de amenazas.

1.4. Metodología

La metodología utilizada para el presente trabajo de investigación es el método inductivo que se utilizó para determinar cuál de las dos herramientas analizadas de detección de intrusos se adapta mejor para una futura implementación.

El método deductivo se utilizó para analizar conceptos fundamentales de la guía NIST y aplicar en los sistemas de detección de intrusos analizados en el presente trabajo de investigación.

Además de utilizar la investigación documental y comparativo que se puede definir según (Uriarte, 2020) como: Una estrategia para comprender y analizar la realidad teórica o empírica a través de la revisión, cotejo, comparación o comprensión de diferentes tipos de fuentes que tratan de un tema en particular, a través de un enfoque sistemático y organizado.

1.5. Resultados – Discusión

Luego de realizar el análisis de los sistemas de detección de intrusos con las herramientas open source Snort y Suricata se pudo identificar que si bien ambos son sistemas libres es necesario inversión adicional para realizar la implementación.

Snort se encarga de observar el tráfico que coincide con sus reglas y alerta sobre la posible intrusión, pero así mismo snort no puede ejecutar múltiples subprocesos.

Por su parte Suricata es un sistema más actual, es un detector de intrusiones robusto y rápido, que a diferencia de Snort soporta múltiples subprocesos, además que soporta las reglas de la capa de aplicación de Snort.

Según el estudio realizado por (Singh et al., 2019) indica que realizó la comparación del desempeño de Suricata con Snort sobre la base de escalabilidad y el rendimiento, realizaron 8600 pruebas variando el número de núcleos utilizados (1-24 núcleos) los conjuntos de reglas utilizados para la comparación de firmas, la carga de trabajo utilizada para obtener resultados y la configuración tanto del IDS. Las métricas utilizadas para la comparación fueron paquetes por segundo (PPS) procesada por cada IDS, la cantidad de memoria utilizada por cada proceso IDS y la utilización de la CPU. Los resultados mostraron que tanto Snort como Suricata eran escalables, pero Suricata superó a Snort en casi todos los escenarios de prueba. Suricata también exhibió uso de memoria promedio más bajo y uso de CPU promedio más bajo.

Luego del análisis anterior se puede recomendar para la empresa Tracape la implementación de la herramienta Suricata, para esto se debe trabajar con el departamento de TI de la organización.

Después de realizar el análisis de las herramientas open source Snort y Suricata se puede determinar que, si pueden minimizar los riesgos de seguridad de las redes de las organizaciones, esto va a depender de que la implementación se realice siguiendo los parámetros adecuados y necesarios para la organización.

CONCLUSIONES

Luego de realizar la comparativa entre los IDS Snort y Suricata se puede concluir que, si bien no existe entre las dos una herramienta mejor o peor ya que ambas son de código abierto, además que se podrían configurar en ambientes de pruebas, la elección del producto va a depender de las necesidades de la organización.

Los sistemas de detección de intrusos no solo se utilizan para detectar accesos no deseados, sino también son útiles para corregir errores de configuración además de actuar a tiempo frente a un ataque, para esto es necesario tener usuarios con privilegios limitados, nodos con acceso limitado, y por supuesto tener segmentada la red de la organización en varias subredes.

Los IDS open source ofrecen varios beneficios entre los que se puede mencionar que a pesar de tener mucho tiempo en el mercado siguen siendo funcionales muy utilizados, han sido probados y comparados en muchos estudios.

Luego de analizar la guía de referencia NIST 800-94 sobre la detección de intrusos en la sección nueve donde proporciona características o recomendaciones al momento de seleccionar un sistema de detección de intrusos, la herramienta que mejor se adapta para la implementación es Suricata porque posee más funcionalidades entre las que se puede mencionar detección de protocolos en cualquier puerto, ejecutar varios procesos al mismo tiempo, logs más detallados, entre otras.

El impacto que puede causar en la organización la implementación de un sistema IDS es fuerte, esto se debe a que en la actualidad no cuenta con procedimientos establecidos en temas de seguridad, los servicios con lo que cuenta son subcontratados.

RECOMENDACIONES

Luego del estudio realizado es recomendable para la futura implementación de una herramienta de IDS seguir las indicaciones con las que aporta la guía NIST 800-94 sobre implantación y funcionamiento en la sección número tres de la guía.

Con el fin de asegurar la funcionalidad de los sistemas IDS y aprovechar las demás funcionalidades que pueden tener es recomendable antes de la implementación realizar un estudio de la situación actual de la organización en materia de seguridad, donde se establezcan políticas de seguridad y se dejen documentados todos los procesos.

Utilizar la guía de referencia NIST 800-94 la cual ofrece recomendaciones para ayudar a las organizaciones a comprender las tecnologías de detección de intrusos, además de diseñar, implementar, monitorear y administrar estos sistemas.

Este trabajo de investigación recomienda la implementación del IDS Suricata para la empresa Tracape S.A. porque posee más funcionalidades entre las que se puede mencionar detección de protocolos en cualquier puerto, puede ejecutar varios procesos al mismo tiempo, logs más detallados, extracción de archivos, entre otras.

Se recomienda realizar capacitación al personal de TI para adquirir los conocimientos necesarios para la implementación y administración del IDS seleccionado.

Los dos sistemas de detección de intrusos analizados alertan sobre posibles amenazas, pero así mismo pueden actuar como un sistema de prevención de intrusos, es decir se puede decidir que hacer luego de detectar la amenaza, por eso se recomienda para futuras investigaciones que deseen apoyarse en este trabajo realizar un análisis para determinar la factibilidad de implementación completa con el sistema de prevención de intrusos.

BIBLIOGRAFÍA

Álvarez Marañón, G. (2004). *Seguridad informática para empresas y particulares*. McGraw-Hill España. https://elibro.net/es/lc/uisrael/titulos/50050

Arquitectura de Snort—Introducción a los Sistemas de Detección de Intrusos. (s. f.). Recuperado 12 de agosto de 2022, de https://1library.co/article/arquitectura-snort-introducci%C3%B3n-sistemas-detecci%C3%B3n-intrusos.yd7x7x6y

Ciberpyme. (2022, abril 7). La importancia de la ciberseguridad en las pymes. *Revista de Ciberseguridad y Seguridad de la Información para Empresas y Organismos Públicos.* https://www.ciberseguridadpyme.es/actualidad/importancia-ciberseguridad-pymes/

Gamez, M. J. (s. f.). Objetivos y metas de desarrollo sostenible. *Desarrollo Sostenible*. Recuperado 8 de julio de 2022, de https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

Gómez Vieites, Á. (2015). *Gestión de incidentes de seguridad informática*. RA-MA Editorial. https://elibro.net/es/ereader/uisrael/62467

Guías NIST: un sustento metodológico para los analistas de ciberseguridad. (2022, 14 de junio). Tarlogic Security. https://www.tarlogic.com/es/blog/guias-nist-sustento-metodologico-para-ciberseguridad/

Industria innovación e infraestructura. (s. f.). *Pacto Mundial*. Recuperado 12 de agosto de 2022, de https://www.pactomundial.org/ods/9-industria-innovacion-e-infraestructura/

Janampa Patilla, H., Huamani Santiago, H. L., Meneses Conislla, Y., Janampa Patilla, H., Huamani Santiago, H. L., y Meneses Conislla, Y. (2021). Snort Open Source como detección de intrusos para la seguridad de la infraestructura de red. *Revista Cubana de Ciencias Informáticas*, *15*(3), 55-73.

Niubox (2021, 9 noviembre). Ecuador: Políticas en el teletrabajo y seguridad de la información. Niubox. https://niubox.legal/teletrabajo-y-ciberseguridad/

Ortega Candel, J. M. (2021). *Ciberseguridad. Manual práctico*. Editorial Paraninfo.

Ortiz, D. (2021, septiembre 3). *Los ataques informáticos a pymes crecen en el Ecuador*. El Comercio. https://www.elcomercio.com/tendencias/tecnologia/ataques-informaticos-pymes-crecen-ecuador.html

Pathak, A. (2022, febrero 14). *8 herramientas IDS e IPS para una mejor seguridad y conocimiento de la red*. Geekflare. https://geekflare.com/es/best-ids-and-ips-tools/

Pereyra, L. E. (2020). *Metodología de la investigación*. Klik.

¿Qué es la Seguridad Informática? | *UNIR Ecuador*. (s. f.). Universidad Virtual. | UNIR Ecuador - Maestrías y Grados virtuales. Recuperado 9 de agosto de 2022, de https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/

Scarfone, K. A., y Mell, P. M. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)* (NIST SP 800-94; 0 ed., p. NIST SP 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

Singh, P. K., Kar, A. K., Singh, Y., Kolekar, M. H., y Tanwar, S. (2019). *Proceedings of ICRIC 2019: Recent Innovations in Computing*. Springer Nature.