REVISTA INCAING
ISSN 2448 9131

Breve análisis comparativo de Snort y Suricata.

José Antonio Morales Flores[1], Jorge Yussel Nuñez Peña[2], Luis Antonio Pereda Jimenez[3], José Arturo Bustamante Lazcano[4]

[1,3,4] TecNM/I.T.S. de la Sierra Negra de Ajalpan, División de Ingeniería en Sistemas Computacionales.

[2]Estudiante del TecNM/I.T.S. de la Sierra Negra de Ajalpan

Ajalpan, México
prof_joseantoniomorales@ajalpan.tecnm.mx

Resumen.

La presente investigación está enfocada en la importancia de estudiar la evaluación de Snort y Suricata para la detección de sondeos de redes y ataques de denegación de servicio, el motivo principal, está en definir cuál de estas redes de detección de intrusos es la mejor, además de demostrar las ventajas y desventajas que disponen cada una de ellas.

Además de esto, hasta el momento se ha observado una gran diferencia del uno al otro, esto debido al tipo de industria al cual le da sus debidas actualizaciones a cada una de sus reglas de sondeo contra intrusos, por lo que existe una gran controversia por saber cuál es el mejor, además de que uno de estos es más sofisticado que el otro, por el año en el que fue desarrollado y la empresa que le da sus debidas actualizaciones, pero no olvidemos que, aunque más sofisticado que este, sino cumple con lo propuesto, se tendrán dificultades.

Por lo que el presente trabajo, mediante una exhaustiva búsqueda de información y comparando cada una de las reglas y formas en las que opera cada uno de estos softwares, pretende determinar un panorama simple, como primer acercamiento a estos conceptos.

Palabras claves: Detección de intrusos, Reglas de sondeo, Empresa desarrolladora.

BRIEF COMPARATIVE ANALYSIS OF SNORT AND SURICATA.

Abstract

This research is focused on the importance of studying the evaluation of Snort and Suricata for the detection of network probing and denial of service attacks, the main reason is to define which of these intrusion detection networks is the best, in addition to demonstrating the advantages and disadvantages of each of them.

In addition to this, so far a great difference has been observed from one to the other, this due to the type of industry to which it gives its due updates to each of its probing rules against intruders, so there is a great controversy for know which is the best, in addition to the fact that one of these is more sophisticated than the other, because of the year in which it was developed and the company that gives it its due updates, but let's not forget that, although more sophisticated than this one, it does not comply with what is proposed, there will be difficulties.

Therefore, the present work, through an exhaustive search for information and comparing each of the rules and ways in which each of these software operates, aims to determine a simple panorama, as a first approach to these concepts.

Keywords: Intrusion detection, Probing rules, Developer company.

I. INTRODUCCIÓN.

El uso de la tecnología digital en los negocios del sector empresarial global, traen grandes beneficios económicos para estas organizaciones. Sin embargo, el rápido uso de la tecnología digital ha provocado un aumento de los ataques informáticos, que forma una de las grandes amenazas para la información privada.

Por eso es importante saber qué tipo de seguridad es más viable usar en este tipo de organizaciones, mediante análisis rigurosos teniendo en cuenta ciertas normas. Las pruebas de rendimiento (benchmark) facilitan la toma de decisiones para la selección de sistemas digitales basados en un conjunto de parámetros. Este método se emplea para comprobar el desempeño de los IDS seleccionados mediante la realización de pruebas de rendimiento.

Los IDS consta de varios módulos, estos módulos son responsables de recopilar datos, procesarlos, verificar si hay intervención o comportamiento sospechoso y crear recordatorios para que los muestren los usuarios y administradores de la red. Es decir que bloquean de manera automática los ataques sospechosos sin la necesidad de la supervisión o interferencia humana.

II. DESARROLLO DE CONTENIDOS

1. Planteamiento del problema

Este tipo de software constituyen una de las herramientas de seguridad más utilizadas en negocios del sector empresarial y de salud, es decir que usar diferentes formas de supervisión ayudan a prevenir problemas.

Determinar la eficiencia y efectividad de estos programas facilita la adaptación de acuerdo a las necesidades que cada empresa o institución presente. La eficiencia de los IDS se determina por el consumo de recursos de hardware durante su funcionamiento y su efectividad, esta última característica se evalúa mediante indicadores como las tasas de falsos positivos, falsos negativos y verdaderos positivos [1]. Este tipo de estudios ayudan a decidir qué tipo de programa es mejor que otra, además de ver que beneficios y fallos tiene cada uno de ellos.

La adopción de medidas de prevención, monitoreo y mitigación ayudan a las diferentes instituciones a mantener protegida su información en todo momento, en este aspecto, los IDS desempeñan un rol fundamental porque son herramientas que ayudan a implementar medidas para prevenir intrusiones en las redes de datos.

De igual manera se emplean ciertas herramientas y programas para poder comprobar la eficacia de cada uno de estos. Para determinar la eficacia de los IDS analizados se empleó la herramienta Kali Linux. Para simular el ambiente de una red empresarial se utilizó la herramienta Ostinato 0.9[2]. Este tipo de pruebas además de darnos una noción de cómo funciona cada uno de los sistemas para la detección de intrusiones en redes de datos, también nos indica cual es la efectividad de cada uno.

El empleo de Snort y Suricata en los esquemas de ciberseguridad de las instituciones y empresas contribuye a disminuir el riesgo de intrusiones y ataques cibernéticos. Al emplear Snort y Suricata está mejorando su seguridad, su privacidad para prevenir actividades sospechosas o maliciosas, ya que de esta manera los programas IDS serán capaces de mantenerlo seguro de ataques cibernéticos [1].

Se habla mucho de la eficacia que tienen los programas IDS en la protección contra los ataques cibernéticos.

La especialidad de estos dos sistemas de seguridad es la prevención y la seguridad de la información, se especializan en descubrir nuevas amenazas y en dar respuesta a las vulnerabilidades y malware más actuales. De esta manera se encarga de mantener el conjunto de reglas de Snort y Suricata más actualizado ante nuevos ataques [3]. Son dos sistemas de seguridad muy efectivas con una constante series de actualizaciones para su mayor desempeño.

2. *Justificación*

Es importante saber que los ataques cibernéticos han evolucionado de tal manera que han encontrado nuevas formas de hacer dichos ataques, los ataques evolucionan, apareciendo versiones de ataques anteriores, o ataques novedosos, es muy importante mantener actualizado y bien configurado este conjunto. Suricata y Snort usan la misma sintaxis para definir reglas [3]. Así mismo la relevancia de mantenerse informado sobre estas situaciones es de suma importancia, y esto es correcto, y que sin estos la información seria vulnerable ante cualquier ataque.

3. Marco conceptual:

En este trabajo se propone determinar cuál es el mejor software para la detección de intrusos, esto a través de las descripciones en torno al comportamiento y la capacidad para poder analizar cada uno de los archivos que pasan a través de este, por lo cual se rescatan los conceptos siguientes que se deben conocer para entender porque Suricata es mejor que Snort.

Hardware: El hardware son aquellos elementos físicos o materiales que constituyen una computadora o un sistema informático. Es decir, son aquellas partes físicas de un sistema operativo tales como sus componentes eléctricos, electrónicos, electromecánicos, mecánicos y cualquier elemento físico que esté involucrado [4].

Mitigación: Forman parte de las tareas del RC, o Responsable de Cumplimiento, y son todas aquellas acciones que se desarrollan en forma de medidas para minimizar o eliminar un riesgo [5].

IDS: Un sistema de detección de intrusiones (o IDS de sus siglas en inglés intrusión Detection System) es un programa de detección de accesos no autorizados a un computador o a una red [6].

Malware: El término "malware" hace referencia al software malicioso, e incluye cualquier sistema de software que afecte los intereses del usuario. No solo pueden afectar a la computadora o al dispositivo infectado, sino también a cualquier otro con el que este se comunique [7].

4. *Marco Teórico*

Snort es uno de los IDPS más viejos en el mercado el cual ya ha recorrido un largo trayecto en las diferentes áreas de seguridad. Snort es un IDPS de código abierto creado en 1998 por Martin Roesch, fundador de Sourcefir. En 2013, Cisco compró Sourcefire y se hizo cargo del desarrollo de Snort [3]. Por lo que hoy en día es uno de los que más empleados en empresas, aunque no cuente con muchas funciones como los actuales de hoy en día.

En Snort uno de los componentes fundamentales que lo conforman es el procesador, ya que este se encarga de realizar un funcionamiento super importante que el de procesar datos antes de que lleguen al motor de detección. De esta manera, Snort puede detectar posibles ataques que no se ajusten al modelo de patrones. Por ejemplo, ataques fragmentados en los que el ataque se divide en diferentes paquetes de un flujo TCP [3]. Es decir que de esta manera se pueden añadir procesadores de forma modular.

Pero una de las diferencias más importantes que ambos IDS presentan, es que Snort dispone de un grupo llamado Talos, que son lo que se encargan de dar solución a las amenazas que aparecen día con día. Talos se encarga de mantener el conjunto de reglas de Snort actualizado ante nuevos ataques. Cuenta con una suscripción de pago por la que proporcionan las últimas actualizaciones en el conjunto de reglas [3]. Porque, cada vez que se presente algún problema ellos son los encargados de solucionarlos.

En cambio, Suricata, las reglas lo actualizan una compañía llamada Emerging Threats de Proofpoint, quienes se encargan de la ciberseguridad. La misma empresa también genera una versión del conjunto de reglas específico para Snort. También es posible usar el conjunto de reglas de Talos. No obstante, estas son creadas específicamente para Snort [3]. Para que Talos pueda darle solución a algunas amenazas que presenta Suricata es necesario adoptar algunos parámetros para que estos puedan ser compatibles.

Por otro lado, Suricata dispone de una de más funciones, aunque su documentación no sea muy extensa como lo es Snort. Suricata permite el multiprocesamiento, por lo que puede aprovechar los procesadores multi-núcleo y multi-hilo. Sin embargo, Snort se ejecuta en un solo hilo. Debido a esto, Suricata tiene ventaja respecto a Snort en el rendimiento [3]. Pero esto no le quita méritos a Snort porque este dispone de mucha más información en cuanto a su funcionamiento y con una mayor cantidad de usuarios.

La especialidad de estos dos sistemas de seguridad es la prevención y la seguridad de la información. Se especializan en descubrir nuevas amenazas y en dar respuesta a las vulnerabilidades y malware más actuales. De esta manera se encarga de mantener el conjunto de reglas de Snort actualizado ante nuevos ataques [3]. Son dos sistemas de seguridad muy efectivas con una constante series de actualizaciones para su mayor desempeño.

Este software dispone de tres modos de trabajo, cada uno con una característica diferente en cual nos centraremos en primer lugar del modo Sniffer, que tiene como objetivo monitorear y mostrarnos todo el tráfico de red. Este modo se caracteriza por monitorizar los paquetes que pasan por la red y mostrárnoslos en pantalla. Gracias a su funcionamiento disponemos de información sobre todo el tráfico que fluye por nuestra organización [8]. Se puede decir que este modo de trabajo funciona igual que otras herramientas conocidas en el mercado.

El modo log de paquetes, se encargar de almacenar todos los paquetes de red, es decir que Snort lo va recolectando y almacenado en el disco duro del ordenador para tener un registro controlado de la información recolectado. Este modo será necesario en caso de querer almacenar los paquetes en nuestro disco. Durante su ejecución, Snort va recogiendo todos los paquetes de red y agrupándolos jerárquicamente mediante la dirección IP de cada datagrama [8]. Este modo de suma importancia porque además de recolectar dicha información, lo va almacenado jerárquicamente para tener un fácil acceso a ellos.

El modo NIDS, es el que se encarga de escanear todo el tráfico de red, de igual forma lo compara con reglas ya predefinidas, almacena a información y también puede ejecutar alguna acción dependiendo del tipo de detención. Esta modalidad se caracteriza principalmente por aplicar el conjunto de reglas al tráfico de red para la detección de alertas. Siendo más específicos, en el caso de Snort el fichero de configuración de las reglas se denomina snort.conf [8]. Es decir que pueden fácilmente monitorear mapeos de puertos, ataques conocidos, además de sustituciones de direcciones ip.

Aunque comparta algunas características similares a la que cuenta Snort, Suricata posee mayores ventajas, esto debido a que cuenta con una mayor cantidad de reglas de protocolos de seguridad. Una de las principales diferencias respecto a otro NIDS,

es que se encuentra preparado para multihilos y para aplicar automáticamente balanceo de carga entre estos hilos [8]. Debido a esta característica peculiar con la que cuenta este software, nos ofrece la posibilidad de entrar a entornos más sofisticados, que con Snort no podríamos lograr tan fácilmente.

El funcionamiento de Suricata es casi parecido al de Snort, esto porque fue desarrollado en base a este, pero con una gran cantidad de mejores y con un desarrollo más sofisticado. El funcionamiento de Suricata es similar al de Snort puesto que su desarrollo se ha realizado basándose en el que emplea Snort. En el caso de Suricata se divide en 4 módulos [8]. Cada uno de estos módulos se encarga de una terea diferente, para que este pueda tener un óptimo desarrollo durante el proceso de detección de amenazas en cada uno de los paquetes recibidos.

III: RESULTADOS

TABLA I

EN LA SIGUIENTE TABLA MOSTRAMOS LAS CARACTERÍSTICAS MÁS RESALTANTES DE CADA SOFTWARE.

Snort

VENTAJAS	DESVENTAJAS
Multiplataforma	Dificultad de aprendizaje
Gratuito	No disponible de GUI
Manual y comunidad de soporte	Configuración especial para falsos positivos
Reglas actualizadas y customizables	Saturación de información debido a una base de datos de reglas muy amplia
Bajos requisitos necesarios	No enfocado a entornos de gran tamaño
Disponibilidad de interfaz web	No diseñado para infraestructuras modernas No soporta IPV6, multithread o velocidades altas de red

Tabla 1.1: Ventajas y desventajas Snort

Suricata

VENTAJAS	DESVENTAJAS
Multiplataforma	Mayor uso de recursos (CPU, RAM)
Gratuito	Obtención de mayor numero de falsos positivos
Manual de usuario y para desarrollo	Posibilidad de positivos grises
Reglas actualizadas y customizables	
Mayor precisión que otros IDS	
Escalabilidad	

Tabla 1.1: Ventajas y desventajas Suricata

IV: CONCLUSIONES

En base a los resultados de la tabla anterior se obtienen las siguientes conclusiones.

Cabe decir que el análisis de los resultados de cada uno de estos sistemas facilita la selección de cuál es el mejor y porque emplearlo. El uso de Suricata como IDS en PYMES contribuirá a fortalecer la seguridad de la información, ante ataques y accesos no autorizados con un uso óptimo de los recursos de hardware [2]. Se puede decir que Suricata supero a Snort por el rendimiento más optimo que mostro durante las pruebas.

A partir de esta exhaustiva investigación con diferentes autores, he llegado a la conclusión de que el mejor software, para detectar archivos e intrusos maliciosos es Suricata, esto es como ya lo había mencionado antes por su optimo desempeño a la hora de resolver este tipo de problemas, además de que este programa puede desempeñar un papel muy importante en empresas de gran prestigio, que el cual Snort no puede lograr, por su poca capacidad de recolección de paquetes.

En conclusión, el uso de algún tipo de seguridad para proteger los datos personales ya sea para una empresa o institución pública son de vital importancia para mantener protegida la información, que en estas manejen ante los ataques cibernéticos de una

forma más automatizado y con una menor intervención humana.

REFERENCIAS:

[1] Perdigón-Llanes, R «Evaluación de Snort y Suricata para la detección de sondeos de redes y ataques de denegación de servicio». Revista Científica de Sistemas e Informática, 2 21, e363, 2022. [En línea]. Available: https://doi.org/10.51252/rcsi.v2i2.363

[2] Perdigón Llanes, R. «Suricata como detector de intrusos para la seguridad en redes de datos empresariales». CIENCIA UNEMI, 15(39), 44-53, 2022. [En línea]. Available: https://doi.org/10.29076/issn.2528-7737vol15iss39.2022pp44-53p

[3] Veramendi Pérez, Ainhoa «Evaluación de sistemas de detección de amenazas: Snort y Suricata» Facultad de Informática Grado en Ingeniería Informática, 1.3, 2021. [En línea]. Available: http://hdl.handle.net/10810/53353

[4] «Glosario» Apen Informatica [En línea]. Available: https://apen.es/glosario-de-informatica/hardware/ [Último acceso: 29 noviembre 2022].

[5] «Glosario» Grupo Cibernos [En línea]. Available: https://www.grupocibernos.com/blog/que-son-los-controles-de-mitigacion-y-como-garantizarla [Último acceso: 29 noviembre 2022].

[6] «Concepto» Grupo Cibernos [En línea]. Available: https://www.grupocibernos.com/blog/que-son-los-controles-de-mitigacion-y-como-garantizarla [Último acceso: 29 noviembre 2022].

[7] «Concepto» Red Hat [En línea]. Available: https://www.redhat.com/es/topics/security/what-is-malware [Último acceso: 29 noviembre 2022].

[8] Alonso Frutos, Alberto «Diseño e Implementación de una Plataforma de detección de amenazas de red» Grado en Ingeniería Informática Mención Tecnologías de la Información, 2021. [En línea]. Available: https://uvadoc.uva.es/bitstream/handle/10324/50089/TFG-G5229