UNIVERSIDAD NACIONAL DE SAN MARTIN

RCSI
https://revistas.unsm.edu.pe/index.php/rcsi
e-ISSN: 2709-992X

Artículo original
Original article
Jul-Dic, 2022

Evaluación de Snort y Suricata para la detección de sondeos de redes y ataques de denegación de servicio

Evaluation of Snort and Suricata for detection of network probes and denial of service attacks

Perdigón-Llanes, Rudibel[1*]

[1]COPEXTEL S.A. División Pinar del Río: Pinar del Río, Cuba

Recibido: 04 May. 2022 | **Aceptado:** 22 Jun. 2022 | **Publicado:** 20 Jul. 2022

Autor de correspondencia*: rperdigon90@gmail.com

Como citar este artículo: Perdigón-Llanes, R. (2022). 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*(2), e363. https://doi.org/10.51252/rcsi.v2i2.363

RESUMEN

Los sistemas de detección de intrusiones constituyen una de las herramientas más utilizadas para identificar ataques o intrusiones en redes de datos en aras de asegurar la confidencialidad, disponibilidad e integridad de la información que por ellas se transmite. Debido a la complejidad de su aplicación en los esquemas de ciberseguridad de las empresas es necesario realizar una evaluación objetiva de estas soluciones con el propósito de seleccionar la herramienta que mejor se ajuste a los requerimientos de estas organizaciones. El objetivo de la presente investigación consiste en comparar cuantitativamente el rendimiento de Snort y Suricata para la detección de sondeos de redes y ataques de denegación de servicio. Se utilizó la herramienta htop para comprobar el rendimiento de Snort y Suricata ante sondeos de redes y ataques de denegación de servicio simulados con diferentes aplicaciones de Kali Linux. Se identificó que Snort posee un consumo de CPU inferior a Suricata durante la detección de intrusiones mediante análisis de firmas, sin embargo, Suri-cata evidenció mejores índices de efectividad. Los resultados obtenidos contribuyen a la toma de decisiones en relación a la selección, despliegue e implementación de sistemas de detección de intrusiones en redes de datos empresariales.

Palabras clave: ciberseguridad; pentest; rendimientos; sistemas de detección de intrusiones.

ABSTRACT

Intrusion detection systems are one of the most widely used tools to identify attacks or intrusions in data networks in order to ensure the confidentiality, availability and integrity of the information transmitted through them. Due to the complexity of its application in companies' cybersecurity schemes, it is necessary to carry out an objective evaluation of these solutions in order to select the tool that best suits the requirements of these organizations. The objective of this research is to quantitatively compare the performance of Snort and Suricata for the detection of network probes and denial of service attacks. The htop tool was used to test the performance of Snort and Suricata against network probes and denial of service attacks simulated with different Kali Linux applications. It was identified that Snort has a lower CPU consumption than Suricata during intrusion detection through signature analysis, however, Suricata showed better effectiveness rates. The results obtained contribute to decision making in relation to the selection, deployment and implementation of intrusion detection systems in business data networks.

Keywords: cybersecurity; pentest; performance; intrusion detection systems

1. INTRODUCCIÓN

La aplicación de las tecnologías digitales en los procesos de negocio del sector empresarial mundial denota marcados beneficios económicos para estas organizaciones (Perdigón Llanes & Pérez Pino, 2020). Sin embargo, el uso acelerado de las tecnologías digitales ha ocasionado un crecimiento de los ataques informáticos, los cuales ocupan la octava posición de los fenómenos con mayor impacto económico a nivel mundial (World Economic Forum, 2020).

Datos de Eset Security para Latinoamérica reflejan que durante 2020 las empresas de la región sufrieron ataques vinculados fundamentalmente a la infección por malware (34%), ataques de ingeniería social (20%), acceso indebido a aplicaciones e información (18%) y denegación de servicios (11%) (Eset Security, 2021). Registros de la compañía Fortinet aseveran que durante el primer semestre de 2020 en América Latina se produjeron más de 15 mil millones de intentos de ciberataques (Fortinet, 2020). Las pérdidas económicas generadas por estos delitos impactan negativamente en las economías de las organizaciones, principalmente en las pequeñas y medianas empresas (PYME), que son incapaces de sostener sus negocios luego de sufrir un ciberataque de envergadura (Bustamante Garcia et al., 2020).

Con el objetivo de minimizar la incidencia de estas transgresiones, las organizaciones emplean diferentes herramientas digitales para preservar la confidencialidad, disponibilidad e integridad de sus recursos informáticos (AlYousef & Abdelmajeed, 2019). Los Sistemas de Detección de Intrusiones (IDS, por sus siglas en inglés) representan una de las soluciones más utilizadas para este propósito porque permiten identificar acciones y comportamientos malintencionados en una red de computadoras mediante el análisis de los datos que por ella transitan ((Karim et al., 2017); (Syed Ali Raza Shah, 2018); (Maniriho et al., 2020); (Perdigón Llanes & Orellana García, 2021). Estos sistemas pueden detectar comportamientos anómalos o ataques específicos dirigidos a una red o un host en particular (Olia Castellanos & Milton García, 2020).

Según los autores Kumar & Singh (2018) y Arteaga Pucha (2020) los IDS se clasifican según su enfoque de detección, su comportamiento ante las intrusiones y los tipos de sistemas que monitorean. Maciá-Fernández et al. (2017) establecen que, en correspondencia con su enfoque de detección los IDS se clasifican en: IDS de análisis de firmas (S-IDS) y de análisis de anomalías (A-IDS). Los S-IDS comparan el tráfico de red con firmas de ataques conocidos, por su parte, los A-IDS distinguen patrones de tráfico malicioso del tráfico normal mediante la aplicación de técnicas de inteligencia artificial (Divekar et al., 2018); (Arteaga Pucha, 2020); (Maniriho et al., 2020).

En relación a su comportamiento ante las intrusiones, los autores Kumar & Singh (2018) catalogan a los IDS en pasivos y activos. Los IDS pasivos no realizan acciones de protección por sí mismos, estas soluciones solo generan alertas dirigidas a operadores y administradores de las TIC durante la detección de comportamientos anómalos e intrusiones, por su parte, los IDS activos poseen la capacidad de bloquear automáticamente los comportamientos sospechosos sin necesidad de supervisión o interferencia humana, proporcionando acciones de corrección en tiempo real ante los ataques (Kumar & Singh, 2018).

En correspondencia con los sistemas que monitorean, los IDS se catalogan en: Sistemas de Detección de Intrusiones de Red (NIDS, por sus siglas en inglés) y Sistemas de Detección de Intrusiones en el Host (HIDS, por sus siglas en inglés). Los autores Ashok & Manikrao (2015); Maciá-Fernández et al. (2017); Solarte Martinez et al. (2017) y Arteaga Pucha (2020) establecen que los NIDS efectúan la detección de tráfico malicioso en una red fortaleciendo la seguridad de esta y los HIDS contribuyen a elevar la seguridad de un equipo específico.

Debido a la complejidad del despliegue y aplicación de los IDS en las arquitecturas de ciberseguridad de las empresas, es necesario realizar una evaluación objetiva de estos sistemas, con el propósito de seleccionar adecuadamente la solución que mejor se ajuste a los requerimientos de estas organizaciones (Wang et al., 2013). Aunque los IDS comerciales son reconocidos por su alto desempeño y efectividad, los cos-tos

asociados a su implementación en los esquemas de seguridad limitan su utilización en organizaciones como las PYMES, que carecen de recursos económicos y financieros para adquirir tecnologías de avanzada (Janampa Patilla et al., 2021). Por tal motivo, estas organizaciones deben adoptar alternativas tecnológicas confiables y eficientes para minimizar fallas y garantizar el correcto funcionamiento de sus recursos digitales con ahorro de costos.

Las herramientas de código abierto representan una solución viable para las PYMES porque facilitan el despliegue de servicios digitales con un aprovechamiento óptimo de los recursos de hardware (Perdigón & Ramírez, 2020) y (Perdigón-Llanes, 2022). Los autores Perdigón Llanes & Orellana García (2021) identificaron que Snort y Suricata constituyen los IDS de código abierto más utilizados en la actualidad para la detección de intrusiones en redes de datos. Sin embargo, en la literatura consultada no se evidenció un consenso sobre cuál de estas soluciones posee mejores índices de desempeño (Syed Ali Raza Shah, 2018); (Murphy, 2019); (Bouziani et al., 2019); (Arteaga Pucha, 2020); (Perdigón Llanes & Orellana García, 2021). Además, según Arteaga Pucha (2020) son escasas las investigaciones orientadas a comparar el rendimiento de estas herramientas ante ciberataques dirigidos a redes de pequeñas y medianas empresas.

El objetivo de la presente investigación consiste en comparar cuantitativamente el rendimiento de Snort y Suricata para la detección de ataques de tipo Probing (Sondeo de redes) y DoS (Denegación de Servicios). Se evaluaron ambas herramientas ante estos tipos de ataques porque según los autores Bouziani et al. (2019); López-Avila et al. (2020) y Arteaga Pucha (2020) son muy utilizados por los ciberdelincuentes en la actualidad, fundamentalmente dirigidos a las redes digitales de empresas que brindan sus servicios en internet.

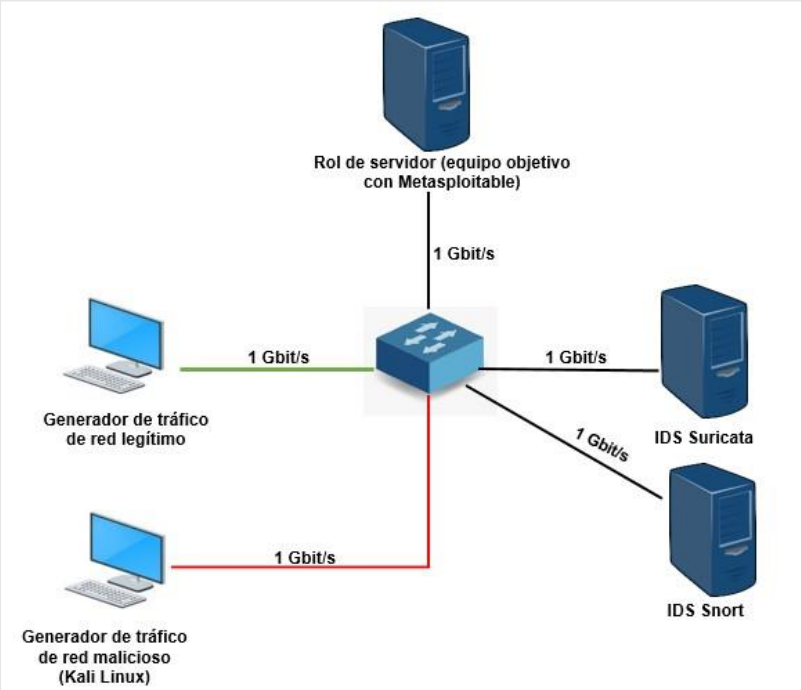
2. MATERIALES Y MÉTODOS

En esta investigación se utilizaron como métodos científicos el analítico-sintético y el experimental. El método analítico-sintético posibilitó el análisis de la literatura existente relacionada con los IDS. Para la búsqueda de información se emplearon las bases de datos Google Scholar y ScienceDirect que son herramientas gratuitas y abarcan un número considerable de fuentes académicas. El método experimental se empleó para comprobar el desempeño de los IDS seleccionados mediante la realización de pruebas de rendimiento.

Las pruebas de rendimiento (benchmark) facilitan la toma de decisiones para la selección de sistemas digitales basados en un conjunto de parámetros (Perdigón Llanes & Ramírez Alonso, 2020). Estas pruebas permiten evaluar el funcionamiento de los IDS y determinar si su desempeño se ajusta a los requerimientos tecnológicos de las organizaciones (Arteaga Pucha, 2020).

El desempeño de los IDS es influenciado en gran medida por las prestaciones de hardware del equipo donde operan (Siddiqi, 2016); (Karim et al., 2017) y (Caro Moreno, 2020). Con el objetivo de obtener resultados fiables durante las pruebas benchmark, los autores de la presente investigación instalaron los IDS a evaluar en ordenadores físicos con similares prestaciones; CPU: core-i3 4160; RAM: 4Gb DDR3; HDD: 500Gb, NIC: 1Gbit/s modelo TP-LINK TG-3269 y Ubuntu Server 20.04 como sistema operativo. La tarjeta de red en estos equipos fue configurada en modo promiscuo y se deshabilitaron sus mecanismos de segmentación (offload) para evitar el rechazo de paquetes de red. La Figura 1 describe el entorno donde se desarrollaron las pruebas.

Figura 1. Entorno de pruebas



La generación de tráfico de red malicioso se realizó mediante la distribución Kali Linux que constituye una solución ampliamente empleada para pruebas de penetración y contiene las herramientas nmap y hping3. Se dispuso un equipo con Metasploitable 2 para simular el rol de un servidor empresarial que provee servicios web, base de datos y compartición de ficheros. Este equipo constituyó el objetivo de los ataques y pruebas de penetración realizadas. Snort y Suricata operan con similares bases de firmas, por tal motivo, estas fueron descargadas en la misma fecha para garantizar similares condiciones de detección durante las pruebas benchmark. Se utilizaron las bases de firmas Emerging Threats del 6 de enero de 2022 que son de libre acceso y se encuentran disponibles en internet.

La diversidad de servicios y aplicaciones digitales que utilizan las empresas incrementan significativamente el tráfico de datos en sus redes informáticas (Syed Ali Raza Shah, 2018). Para simular el tráfico de una red empresarial y comprobar el rendimiento de los IDS seleccionados, los autores de este trabajo se apoyaron en los criterios de (Karim et al., 2017), mediante el uso de la herramienta Ostinato. Según Karim et al. (2017), el tráfico de una red con grandes flujos de datos puede simularse combinando la cantidad de paquetes enviados, sus dimensiones e intervalos de tiempo entre cada envío. En correspondencia con los criterios de (Karim et al., 2017), en esta investigación se realizó el envío de 10000 paquetes de red de 128 y 3072 bytes respectivamente, cada 1 segundo mediante el protocolo TCP para simular el tráfico de una red empresarial.

3. RESULTADOS Y DISCUSIÓN

Los autores Murphy (2019) y Aludhilu & Rodríguez-Puente (2020) consideran que la eficiencia y efectividad de los IDS constituyen aspectos relevantes para su evaluación. Estas características se relacionan respectivamente, con su consumo de recursos de hardware y con su capacidad para identificar comportamientos maliciosos y actividades de intrusión (Murphy, 2019) y (Aludhilu & Rodríguez-Puente, 2020). Para determinar la eficiencia de los IDS analizados se empleó la herramienta htop y para comprobar su efectividad se simularon pruebas de intrusión mediante la distribución Kali Linux. Con el propósito de generar tráfico de red para simular el ambiente de una red empresarial se utilizó la herramienta Ostinato

0.9. Se seleccionaron las últimas versiones estables disponibles de Snort y Suricata hasta la fecha en que se realizó este estudio: Snort 2.9.18.1 y Suricata 6.0.4.

Según los criterios de Aludhilu & Rodríguez-Puente (2020) los IDS son efectivos si arrojan bajos índices de falsas alarmas. Los autores Bijone (2016) y Syed Ali Raza Shah (2018) consideran que las tasas de falsos positivos (FPR, por sus siglas en inglés), tasas de falsos negativos (FNR, por sus siglas en inglés) y tasas de verdaderos posi-tivos (TPR, por sus siglas en inglés) constituyen indicadores fiables para medir la efectividad de los IDS. Según estos autores, FPR: denota la probabilidad de que un IDS emita una alerta cuando no existe intrusión, FNR: representa la probabilidad de que un IDS no emita una alerta cuando sí existe una intrusión y TPR: determina la probabilidad de que un IDS emita una alerta ante una intrusión. Estos indicadores se determinan según las siguientes fórmulas (Bijone, 2016); (Syed Ali Raza Shah, 2018); (Kumar & Singh, 2018):

$$FPR = FP / (FP + TN) * 100 \quad (1)$$

$$FNR = FN / (FN + TP) * 100 \quad (2)$$

$$TPR = TP / (TP + FN) * 100 \quad (3)$$

Donde:

Verdadero negativo (TN, por sus siglas en inglés): El tráfico de red inofensivo es identificado como tal por el IDS.

Verdadero positivo (TP, por sus siglas en inglés): El tráfico de red malicioso es identificado como tal por el IDS.

Falso positivo (FP, por sus siglas en inglés): El tráfico de red inofensivo es identificado como tráfico malicioso por el IDS.

Falso negativo (FN, por sus siglas en inglés): El tráfico de red malicioso es identificado como como tráfico de red inofensivo por el IDS.

Se comprobó en un primer momento la efectividad de los IDS para manejar el tráfico de red inofensivo. Posteriormente y de forma simultánea al tráfico de red inofensivo, fue generado secuencialmente el tráfico de red malicioso mediante las herramientas nmap y hping3. El empleo de estas herramientas permitió simular ataques de tipo sondeo de redes y DoS. Se generaron ataques DoS de tipo SYN Flood, UDP Flood y PING Flood y se utilizó la opción randsource para evadir los IDS utilizados.

Se identificó que ambas soluciones fueron incapaces de detectar los ataques DoS SYN Flood y UDP Flood simulados, por lo que se crearon 2 reglas personalizadas para identificar este tipo de transgresiones. Las reglas creadas se estructuraron según las especificaciones realizadas por Janampa Patilla et al. (2021) para estos tipos de ataques:

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (flags: S; msg: "Posible ataque DoS SYN flood detectado"; flow: to_server; detection_filter: track by_src, count 50, seconds 1; sid:10000004; rev:001;)

alert udp $EXTERNAL_NET any -> $HOME_NET any (msg: "Posible ataque DoS UDP flood detectado"; detection_filter: track by_src, count 50, seconds 1; sid:10000005; rev:001;)

La Tabla 1 muestra la efectividad de los IDS analizados según los indicadores descritos en las fórmulas 1, 2 y 3 respectivamente.

Tabla 1. *Efectividad de Snort y Suricata ante sondeos de red y ataques DoS*

Tráfico de red legítimo generado	Tráfico de red malicioso generado	Snort			Suricata		
		FPR	FNR	TPR	FPR	FNR	TPR
Tráfico de paquetes de 128 bytes		0	0	0	0	0	0
Tráfico de paquetes de 3072 bytes		0	0	0	0	0	0
Tráfico de paquetes de 128 bytes	nmap -sS -p- ip_Metasploitable	0	99,98	0,02	0	99,96	0,04
	SYN Flood: hping3 --rand-source -c 1000 ip_Metasploitable -p 80 --faster	0	1	99	0	1	99
	UDP Flood: hping3 --rand-source -c 1000 --udp ip_Metasploitable -p 53 --faster	0	97,9	2,1	0,005	0	100
	PING Flood: hping3 --rand-source -c 1000 --icmp ip_Metasploitable --faster	0	0	100	0	0	100
Tráfico de paquetes de 3072 bytes	nmap -sS -p- ip_Metasploitable	0	99,98	0,02	0	99,98	0,02
	SYN Flood: hping3 --rand-source -c 1000 ip_Metasploitable -p 80 --faster	0	22,1	77,9	0,0048	0	100
	UDP Flood: hping3 --rand-source -c 1000 --udp ip_Metasploitable -p 53 --faster	0	35,5	64,5	0,0168	0	100
	PING Flood: hping3 --rand-source -c 1000 --icmp ip_Metasploitable --faster	0	19,0	81,0	0	46,4	53,6

Ambos IDS mostraron tasas de detección inefectivas ante los ataques Probing generados con nmap. Se identificó que Snort no arrojó falsos positivos durante las pruebas de penetración realizadas, sin embargo, demostró elevadas tasas de falsos negativos (FNR), elemento que incide negativamente en la seguridad de la red. De forma general Suricata evidenció índices de efectividad superiores a Snort para la detección de intrusiones en el ambiente de pruebas utilizado.

Durante el período de tiempo que demoraron las pruebas realizadas se monitoreó la carga de CPU y el uso de memoria RAM de ambos IDS. Las Figuras 2 y 3 muestran respectivamente, los resultados obtenidos.

Figura 2. Consumo de CPU

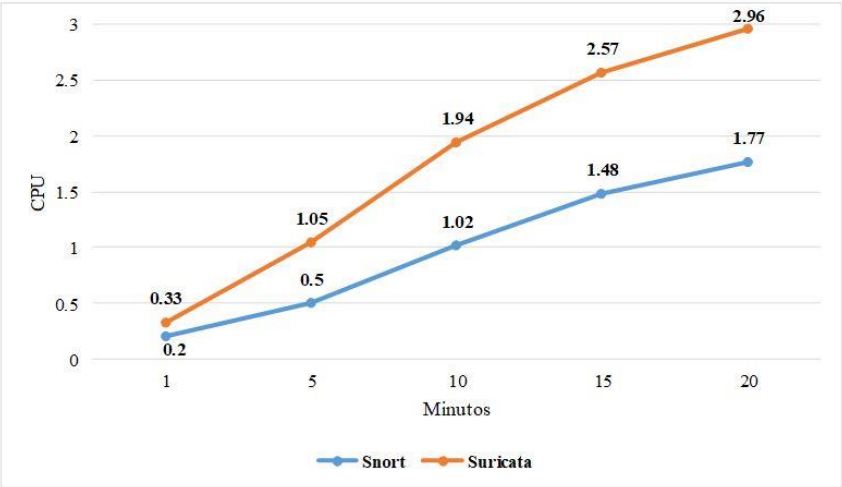
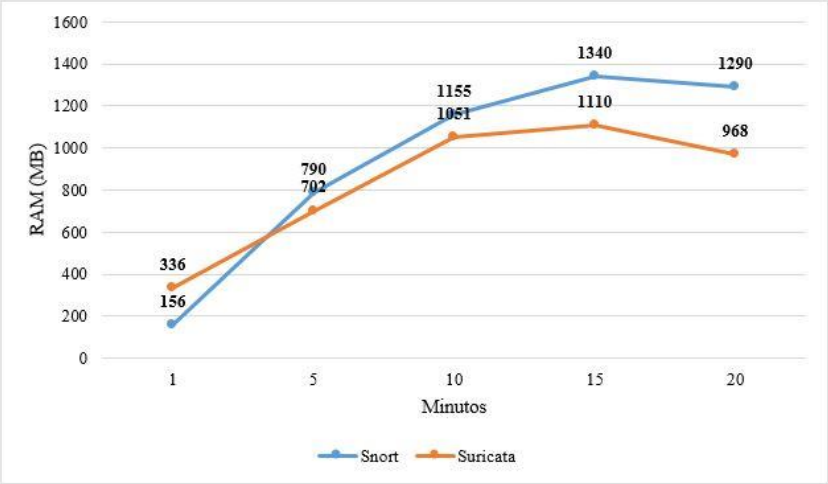


Figura 3. Consumo memoria RAM



Los resultados anteriores permitieron identificar que ambos IDS mantuvieron un consumo eficiente de los recursos de hardware durante las pruebas realizadas, pues no se evidenció sobreexplotación del CPU y el consumo de memoria RAM no sobrepasó el 33% de la memoria disponible. No obstante, Snort demostró mejores resultados en relación a la carga del CPU, aunque su consumo de memoria RAM fue ligeramente superior a Suricata.

En su investigación Park & Ahn (2017) determinaron que Snort posee mayor eficiencia respecto a Suricata en relación al consumo de CPU. Sin embargo, según estos autores, Suricata posee índices de efectividad superiores para la detección de intrusiones.

Syed Ali Raza Shah (2018) comprobaron los rendimientos de Snort y Suricata para la detección de intrusiones en redes de 10 Gbits/s. Los resultados obtenidos por Syed Ali Raza Shah (2018) evidenciaron que Snort posee mayor eficiencia que Suricata respecto al consumo de recursos de hardware (CPU y RAM) durante el análisis del tráfico en redes de 10 Gbits/s. Según estos autores, aunque ambos IDS demostraron altos índices de falsos positivos, Snort obtuvo mejores indicadores de efectividad para la detección de intrusiones en redes de altas velocidades.

Los autores Bouziani et al. (2019) evaluaron el funcionamiento de Snort y Suricata en modo S-IDS e identificaron que, aunque ambas soluciones emplean similares bases de firmas, sus índices de detección suelen ser diferentes. Estos autores determinaron que Snort obtuvo mejores resultados que Suricata ante ataques de evasión.

En su tesis Murphy (2019) identificó que, aunque Snort consume menos memoria RAM que Suricata, éste último posee tasas de detección superiores.

El autor Arteaga Pucha (2020) evaluó los rendimientos de Snort y Suricata en modo A-IDS e identificó que Suricata es un 5% mejor que Snort en relación a sus funcionalidades, posee una menor tasa de pérdida de paquetes y una precisión para la detección de anomalías un 8% superior a Snort.

En concordancia con los resultados obtenidos por Park & Ahn (2017), en la presente investigación se identificó que Snort posee un consumo de CPU inferior a Suricata para la detección de ataques Probing y DoS mediante el análisis de firmas, sin embargo, Suricata mantiene mejores índices de efectividad respecto a Snort para la detección de estos ataques en redes de datos con velocidades de 1 Gbits/s.

4. CONCLUSIONES

En esta investigación se realizó un análisis comparativo de la eficiencia y efectividad de Snort y Suricata para la detección de sondeos de redes y ataques DoS en redes de datos mediante el análisis de firmas. Los resultados obtenidos evidenciaron que, aunque ambos IDS operan con similares bases de firmas, existen marcadas diferencias en relación a su efectividad para la detección de estos ataques. Snort evidenció un consumo de CPU inferior a Suricata, sin embargo, ambas soluciones realizaron la detección de intrusiones con una alta eficiencia respecto al consumo de recursos de hardware. Las pruebas de intrusión simuladas permitieron identificar que Suricata posee mayor efectividad que Snort para la detección de ataques de tipo Probing y DoS en redes de datos con velocidades de 1 Gbits/s.

Los resultados alcanzados en este trabajo facilitan la toma de decisiones en relación a la selección, despliegue e implementación de sistemas para la detección de intrusiones en redes de datos empresariales. El uso de Suricata como IDS en PYMES contribuirá a fortalecer la seguridad de la información en estas organizaciones ante ataques y accesos no autorizados con un uso óptimo de sus recursos de hardware. Los autores de futuros estudios pueden enriquecer esta investigación mediante el análisis de nuevas versiones de los IDS abordados y su rendimiento para la detección de anomalías.

FINANCIAMIENTO

Ninguno.

CONFLICTO DE INTERESES

No existe ningún tipo de conflicto de interés relacionado con la materia del trabajo.

CONTRIBUCIÓN DE LOS AUTORES

Conceptualización, curación de datos, análisis formal, investigación, metodología, supervisión, validación, redacción - borrador original, redacción - revisión y edición: Perdigón-Llanes, R.

REFERENCIAS BIBLIOGRÁFICAS

Aludhilu, H., & Rodríguez-Puente, R. (2020). A Systematic Literature Review on Intrusion Detection Approaches. *Revista Cubana de Ciencias Informáticas*, *14*(1), 58–78. http://scielo.sld.cu/scielo.php?pid=S2227-18992020000100058&script=sci_abstract&tlng=en

AlYousef, M. Y., & Abdelmajeed, N. T. (2019). Dynamically Detecting Security Threats and Updating a Signature-Based Intrusion Detection System's Database. *Procedia Computer Science*, *159*, 1507–1516. https://doi.org/10.1016/j.procs.2019.09.321

Arteaga Pucha, J. E. (2020). Evaluación de las funcionalidades de los sistemas de detección de intrusos basados en la red de plataformas open source utilizando la técnica de detección de anomalías. *Latin-American Journal of Computing*, *7*(1), 49–64. https://doi.org/10.1016/j.procs.2019.09.321

Ashok, D., & Manikrao, V. (2015). Comparative study and analysis of network intrusion detection tools. *International Conference on Applied and Theoretical Computing and Communication Technology. Davangere: IEEE*, 312–315. https://doi.org/10.1109/ICATCCT.2015.7456901

Bijone, M. (2016). A Survey on Secure Network: Intrusion Detection & Prevention Approaches. *American Journal of Information Systems*, *4*(3), 69–88. https://doi.org/10.12691/ajis-4-3-2

Bouziani, O., Benaboud, H., Chamkar, A. S., & Lazaar, S. (2019). A Comparative study of Open Source IDSs

according to their Ability to Detect Attacks. *2nd International Conference on Networking, Information Systems & Security. Rabat: ACM*, 1–5. https://doi.org/10.1145/3320326.3320383

Bustamante Garcia, S., Valles Coral, M. A., & Levano Rodriguez, D. (2020). Factores que contribuyen en la pérdida de información en las organizaciones. *Revista Cubana de Ciencias Informáticas*, *14*(3), 148–165. https://rcci.uci.cu/?journal=rcci&page=article&op=view&path%5B%5D=1948&path%5B%5D=818

Caro Moreno, R. (2020). *Despliegue y explotación de herramientas Open Source para la monitorización y gestión de eventos en un entorno virtualizado* [Universidad de Cádiz]. http://hdl.handle.net/10498/23447

Divekar, A., Parekh, M., Savla, V., Mishra, R., & Shirole, M. (2018). Benchmarking datasets for Anomaly based Network Intrusion Detection: KDD CUP 99 alternatives. *3rd International Conference on Computing, Communication and Security (ICCCS)*, 1–8. https://doi.org/10.1109/CCCS.2018.8586840

Eset Security. (2021). *Eset Security Report Latinoamérica 2021* (pp. 1–29). https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

Fortinet. (2020). *Threat Intelligence Insider Latin America 2020*. https://www.fortinetthreatinsiderlat.com/en/Q2-2020/BR/html/trends#trends_position

Janampa Patilla, H., Huamani Santiago, H., & 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. https://rcci.uci.cu/?journal=rcci&page=article&op=view&path%5B%5D=2042

Karim, I., Vien, Q.-T., Anh Le, T., & Mapp, G. (2017). A Comparative Experimental Design and Performance Analysis of Snort-Based Intrusion Detection System in Practical Computer Networks. *Computers*, *6*(1). https://doi.org/10.3390/computers6010006

Kumar, D., & Singh, R. (2018). Comprehensive Review: Intrusion Detection System and Techniques. *IOSR Journal of Computer Engineering*, *18*(4), 20–25. https://doi.org/10.9790/0661-1804032025

López-Avila, L., Acosta-Mendoza, N., & Gago-Alonso, A. (2020). Detección de anomalías basada en aprendizaje profundo: Revisión. *Revista Cubana de Ciencias Informáticas*, *13*(3), 107–123. https://rcci.uci.cu/?journal=rcci&page=article&op=view&path%5B%5D=1874&path%5B%5D=779

Maciá-Fernández, G., Camacho, J., Magán-Carrión, R., Fuentes-García, M., García-Teodoro, P., & Theron, R. (2017). UGR'16: Un nuevo conjunto de datos para la evaluación de IDS de red. *Jornadas de Ingeniería Telemática*, 71–78. https://doi.org/10.4995/jitel2017.2017.6520

Maniriho, P., Mahoro, L. J., Niyigaba, E., Bizimana, Z., & Ahmad, T. (2020). Detecting Intrusions in Computer Network Traffic with Machine Learning Approaches. *International Journal of Intelligent Engineering and Systems*, *13*(3), 433–445. https://doi.org/10.22266/IJIES2020.0630.39

Murphy, B. R. (2019). *Comparing the performance of intrusion detection systems: snort and suricata* [Colorado Technical University]. https://www.proquest.com/openview/885ab9a9d8f5c1b92d177780fbe81699/1?pq-origsite=gscholar&cbl=18750&diss=y

Olia Castellanos, L., & Milton García, B. (2020). Análisis y caracterización de conjuntos de datos para detección de intrusiones. *Serie Científica de La Universidad de Las Ciencias Informáticas*, *13*(4), 39–52. https://publicaciones.uci.cu/index.php/serie/article/view/558

Park, W., & Ahn, S. (2017). Performance Comparison and Detection Analysis in Snort and Suricata Environment. *Wireless Pers Commun*, *94*, 241–252. https://doi.org/10.1007/s11277-016-3209-9

Perdigón-Llanes, R. (2022). Suricata como detector de intrusos para la seguridad en redes de datos empresariales. *Revista Ciencia UNEMI*, *15*(39), 44–53. https://doi.org/10.29076/issn.2528-7737vol15iss39.2022pp44-53p

Perdigón Llanes, R., & Orellana García, A. (2021). Sistemas para la detección de intrusiones en redes de datos de instituciones de salud. *Revista Cubana de Informática Médica*, *13*(2). http://www.revinformatica.sld.cu/index.php/rcim/article/view/440

Perdigón Llanes, R., & Pérez Pino, T. M. (2020). Análisis holístico del impacto social de los negocios electrónicos en América Latina, de 2014 a 2019. *Revista de Tecnología y Sociedad*, *10*(18). https://doi.org/10.32870/Pk.a10n18.459

Perdigón Llanes, R., & Ramírez Alonso, R. (2020). Plataformas de software libre para la virtualización de servidores en pequeñas y medianas empresas cubanas. *Revista Cubana de Ciencias Informáticas*, *14*(1), 40–57. https://rcci.uci.cu/?journal=rcci&page=article&op=view&path%5B%5D=1901

Siddiqi, A. (2016). *Performance Analysis of Open Source IDPS in Virtual Computing Environment* [Northcentral University]. https://www.proquest.com/openview/decad1264757e8ac0c572441d0572fe9/1?cbl=18750&pq-origsite=gscholar

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

Syed Ali Raza Shah, B. I. (2018). Performance comparison of intrusion detection systems and application of machine learning to Snort system. *Future Generation Computer Systems*, *80*, 157–170. https://doi.org/10.1016/j.future.2017.10.016

Wang, X., Kordas, A., Hu, L., Gaedke, M., & Derrick. (2013). Administrative Evaluation of Intrusion Detection System. *2nd Annual Conference on Research in Information Technology*, 47–52. https://doi.org/10.1145/2512209.2512216

World Economic Forum. (2020). *The Global Risks Report 2020* (15th ed.). http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf