Artículo de revisión

Sistemas para la detección de intrusiones en redes de datos de instituciones de salud

Intrusion-Detection Systems for Healthcare Institutions' Data Networks

M.Sc. Rudibel Perdigón Llanes[1 *] 0000-0001-7288-6224
Dr.C. Arturo Orellana García[2] 0000-0002-3652-969X

[1] Empresa Comercializadora "Frutas Selectas", Pinar del Río, Cuba.

[2] Universidad de las Ciencias Informáticas. Centro de Informática Médica, La Habana, Cuba.

[*] Autor para correspondencia: rperdigon90@gmail.com

RESUMEN

El empleo de las tecnologías digitales en instituciones médicas permite mejorar la calidad en la prestación de servicios de salud. Sin embargo, su utilización incrementa las vulnerabilidades y los riesgos de seguridad en estas organizaciones. En la actualidad los sistemas digitales en el sector de la salud representan un objetivo atractivo para los ciberdelicuentes porque constituyen fuentes de información valiosa deficientemente protegida. El estudio de la literatura permitió identificar una carencia de investigaciones orientadas a elevar la seguridad en redes de datos de instituciones de salud. La presente investigación tiene como objetivo realizar una revisión bibliográfica sobre los principales Sistemas de Detección de Intrusiones de código abierto existentes en la actualidad para contribuir a fortalecer la seguridad en las redes de datos de estas organizaciones. Se identificó la superioridad de Snort y Suricata como herramientas de código abierto para la detección de intrusiones en redes de datos.

Palabras clave: IDS; seguridad computacional; sistemas de computación; redes de comunicación de computadores.

ABSTRACT

The use of digital technologies in medical institutions allows to improve the quality of health services. However, its use increases the vulnerabilities and security risks of these organizations. Currently, digital systems in the health sector represent an attractive target for cyber-criminals because they constitute poorly protected sources of valuable information. The study of the literature made it possible to identify a lack of research aimed at increasing security in health institutions data networks. The

objective of this research is to carry out a literature review on the main open source Intrusion Detection Systems currently existing to strengthen security in the data networks of these organizations. The superiority of Snort and Suricata as open source tools for intrusion detection in data networks was identified.

Keywords: IDS; computer security; computer systems; computer communication networks.

Recibido: 24/03/2021
Aprobado: 30/06/2021

Introducción

La aplicación de las Tecnologías de la Información y las Comunicaciones (TIC) en la medicina ha marcado un cambio de paradigma dentro de este sector [(1)]. El empleo de las tecnologías digitales en la atención médica permite agilizar los trámites, la atención a los pacientes, apoyar los diagnósticos, facilitar el control de los procesos administrativos y garantizar la calidad de los servicios de salud [(2)]. Además, contribuye a elevar la eficiencia y la reducción de errores en el tratamiento y monitoreo de enfermedades crónicas sin necesidad de aplicar procedimientos invasivos [(3)]. En este ámbito, las redes de datos constituyen medios de comunicación fundamentales para la integración y el intercambio de información entre los diferentes equipos médicos [(1)].

Las redes de datos en instituciones de salud aunque se asemejan a las redes digitales empresariales en términos de arquitectura y configuración, denotan características singulares que imponen mayores riesgos de seguridad [(1)]. Estos riesgos están relacionados con las terribles consecuencias que ocasionan los ciberataques en el bienestar de los pacientes [(4)].

Los sistemas de salud representan un objetivo atractivo para los ciberdelicuentes porque son una fuente de información valiosa deficientemente protegida. [(3), (5-9)] Esta información puede ser explotada mediante el robo, la suplantación de identidad y el fraude con el fin de adquirir sustancias médicas controladas. [(1)] Las intrusiones en redes digitales y las afectaciones en el acceso a sistemas e informaciones de entidades sanitarias constituyen amenazas que producen graves problemas de seguridad e impactan negativamente en el tratamiento de los pacientes. [(8), (10)]

Los ciberataques en el sector de la salud se han incrementado en un 125% durante los últimos cinco años. [(7)] Estas transgresiones ocupan la octava posición de los fenómenos con mayor impacto a nivel mundial durante 2020. [(11)] Su repercusión económica en organizaciones de atención médica es significativamente mayor a las pérdidas que ocasionan en organizaciones de otros sectores. [(7), (9)] Entre los ciberataques más comunes se encuentran: Probing (sondeo de redes), Spoofing (suplantación de

identidad), *DoS* (Denegación de Servicios), Brute Force Attack (ataque de fuerza bruta) y SQL Injections (inyecciones SQL). [1], [8], [9]

La ciberseguridad en instituciones de salud es un tema de interés para la comunidad científica internacional. [12] Sin embargo, las investigaciones orientadas a fortalecer la seguridad de las redes de datos de estas organizaciones son escasas. [8], [9], [13], [14]

Los Sistemas de Detección de Intrusiones (IDS, por sus siglas en inglés) constituyen una de las herramientas más utilizadas para garantizar la seguridad de las redes de datos porque detectan actividades sospechosas mediante el análisis y monitoreo del tráfico de paquetes de red. [15], [16-18] Estas herramientas permiten detectar ataques y violaciones de seguridad, implementar diferentes controles de supervisión, prevenir problemas de comportamiento y abusos en los sistemas interconectados a la red. [16]

Los IDS pueden emplearse para proteger una red o un equipo en particular y en correspondencia al enfoque que utilicen pueden detectar comportamientos anómalos o ataques específicos. [19] Debido a la complejidad de los IDS y su aplicación en las arquitecturas de seguridad, es necesario realizar una evaluación objetiva de estas herramientas, con el propósito de seleccionar adecuadamente la solución que mejor se ajuste a los requerimientos de las organizaciones. [20] Existe una carencia de investigaciones donde se desarrolle un análisis crítico de las tendencias actuales de estas herramientas para contribuir a facilitar su selección e implementación. [17]

La presente investigación tiene como objetivo realizar una revisión de la literatura relacionada con los principales IDS de código abierto existentes en la actualidad para contribuir a fortalecer la seguridad en redes de datos de organizaciones de salud. Se seleccionaron herramientas libres de código abierto porque constituyen soluciones efectivas de bajo costo para mejorar la ciberseguridad en las organizaciones. [21] Además, estas soluciones permiten enfrentar las restricciones económicas internacionales que dificultan la adquisición de tecnologías de avanzada en Cuba y contribuyen a alcanzar la soberanía tecnológica en el país. [22]

Métodos

En esta investigación se desarrolló una revisión de la literatura donde se aplicó como metodología de investigación el enfoque de la vigilancia tecnológica. Esta metodología constituye un proceso informativo-documental-selectivo que recopila y organiza información relevante sobre un área de conocimiento concreta para contribuir a la toma de decisiones. [23] Se adoptó este enfoque por su relación con la innovación tecnológica en las organizaciones, elemento estrechamente relacionado con la aplicación de las TIC en instituciones de salud.

Para la búsqueda y captación de información se utilizaron los motores de búsqueda Google Scholar, Scielo y Science Direct, por ser herramientas gratuitas que abarcan un cúmulo considerable de artículos académicos. Se examinaron las fuentes bibliográficas disponibles durante el período 2013-2020, que permitieron su consulta íntegra y

gratuita. Para el análisis y tratamiento de las fuentes obtenidas se emplearon como métodos científicos el analítico-sintético, el histórico-lógico y la triangulación teórica, lo que permitió disminuir el sesgo en la investigación y transformar la información adquirida en conocimiento útil para obtener conclusiones sobre el objeto de estudio.

Desarrollo

Arquitectura y clasificación de los IDS

Los IDS están integrados por varios módulos [24], como se muestra en la Figura 1. Estos módulos se encargan de la obtención de datos, de su adaptación, preprocesamiento, análisis para determinar la existencia de intrusiones o comportamientos sospechosos y de la generación de alertas para su visualización por operadores y administradores de red. [24]

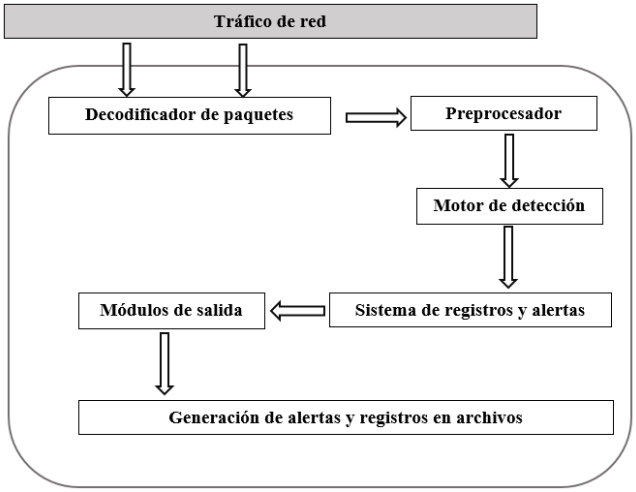

Fig. 1- Arquitectura de los IDS. (Elaboración propia).

La clasificación de los IDS se realiza según su enfoque, comportamiento ante las intrusiones y los tipos de sistemas que monitorean. [25], [26] Según su enfoque, se clasifican en: IDS de análisis de anomalías (A-IDS) y de análisis de firmas (S-IDS). [24] Los A-IDS diferencian patrones de tráfico normal del tráfico sospechoso, incluso aquellos de los que no han tenido conocimiento con anterioridad mediante el empleo de técnicas de machine learning. [17], [18] Los S-IDS detectan intrusiones analizando coincidencias exactas del tráfico de red con firmas de ataques conocidos. [17], [25], [27]

En relación a su comportamiento, los IDS se clasifican en pasivos y activos. [26] Los IDS pasivos monitorean y analizan las actividades del tráfico de red para generar alertas dirigidas a operadores y administradores de las TIC; estas soluciones no realizan acciones de protección o corrección por sí mismas. [26] Los IDS activos, también conocidos como Sistemas de Prevención de Intrusos (IPS, por sus siglas en inglés), bloquean automáticamente los ataques sospechosos sin necesidad de supervisión o

interferencia humana, proporcionando acciones de corrección en tiempo real ante los ataques. [26]

Según los sistemas que monitorean, los IDS se clasifican en: Sistemas de Detección de Intrusiones de Red (NIDS, por sus siglas en inglés) y Sistemas de Detección de Intrusiones en Equipos (HIDS, por sus siglas en inglés). [25] Los NIDS realizan la detección y el análisis del tráfico de red garantizando la seguridad dentro de esta y los HIDS permiten garantizar la seguridad en un equipo específico. [24], [25], [28], [29] A continuación (Fig.2) se muestran las posibles ubicaciones de los IDS en una red de computadoras. [30]

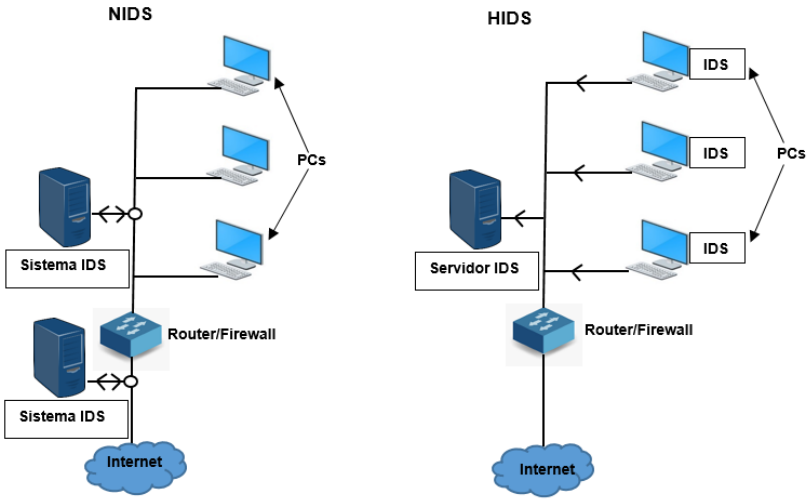

Fig. 2- Localización de los IDS. Fuente: [30]

Determinar la eficiencia y efectividad de estas soluciones facilita su adecuación a las necesidades de las organizaciones. [18], [21] Según los autores anteriores la eficiencia de los IDS se determina por el consumo de recursos de hardware durante su funcionamiento y su efectividad por la capacidad para identificar comportamientos maliciosos y actividades de intrusión. Esta última característica se evalúa mediante indicadores como las tasas de falsos positivos, falsos negativos y verdaderos positivos que son obtenidos durante el proceso de detección. [31]

Tendencias actuales de los IDS

El estudio de las tendencias actuales de los IDS se realizó en dos pasos fundamentales y sobre la premisa de que fueran IDS de código abierto. En un primer momento se investigaron las soluciones más populares en el mercado, en la Figura 3 se muestran los IDS que durante 2020 lideran el mercado mundial según datos del sitio *G2 Crowd, Inc*. [32] Algunas soluciones como AlienVault, MacAfee Network Security Plataform y Palo Alto Networks Next-Generation Firewall son ampliamente reconocidas por su efectividad pero poseen como inconveniente que son herramientas con licencias privativas y limitan sus funcionalidades en versiones libres de pago. Además, se plantea que las versiones comerciales de los IDS generalmente no brindan el

rendimiento ideal que anuncian y podrían comprometer la seguridad de las redes informáticas. [31]

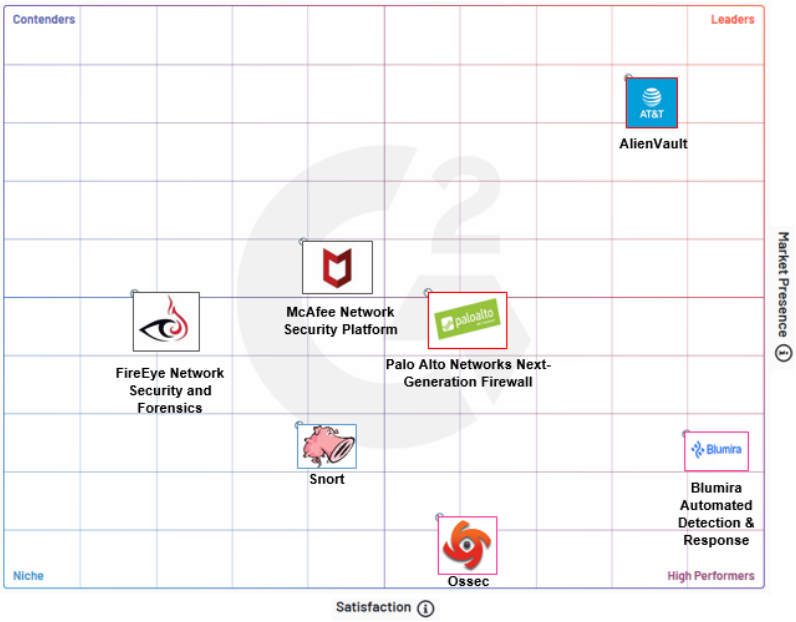

Fig. 3- IDS líderes del mercado en 2020. Fuente: [32]

En un segundo momento se realizó un análisis de la literatura publicada durante el período comprendido entre 2013 y 2020 para identificar los IDS de código abierto más estudiados por los diferentes autores consultados. En la Tabla 1 se muestran los resultados obtenidos.

Tabla 1- IDS de código abierto identificados en la literatura.

Autores	IDS
(20, 21, 25, 28 - 31, 33-37)	Snort
(19, 21, 25, 28, 31, 34-37)	Suricata
(24,28, 34-38)	Zeek (antiguamente Bro)
(20)	Ourmon
(20)	Samhain
(34, 37)	Ossec
(37)	Tripwire

El enfoque de los IDS, su comportamiento, soporte técnico, compatibilidad con diferentes estándares de interconexión de redes basados en internet y sistemas operativos, fueron aspectos considerados para su selección y análisis. Estos datos fueron extraídos de los sitios oficiales de los fabricantes de las herramientas. Se realizó una triangulación de los resultados obtenidos y se determinó que los IDS Snort y Suricata cumplen con los criterios de selección establecidos (Tabla 2).

Tabla 2- Características de los IDS seleccionados.

IDS	Licencia	Compatibilidad	Estándares de interconexión	Enfoque	Soporte técnico	IPS	Tipo
AlienVault	Propietaria/ Libre	Linux y Windows	IPv4/IPv6	S-IDS	Sí	No	HIDS
MacAfee Network Security Plataform	Propietaria	Linux y Windows	IPv4/IPv6	A-IDS, S-IDS	Sí	Sí	NIDS
Palo Alto Networks Next-Generation Firewall	Propietaria	PAN-OS	IPv4/IPv6	A-IDS, S-IDS	Sí	Sí	NIDS
Snort	Libre	Linux, FreeBSD, Windows, MacOS	IPv4/IPv6	A-IDS, S-IDS	Sí	Sí	NIDS
Suricata	Libre	Linux, FreeBSD, Windows, MacOS	IPv4/IPv6	A-IDS, S-IDS	Sí	Sí	NIDS
Zeek	Libre	Linux, FreeBSD, MacOS	IPv4/IPv6	A-IDS, S-IDS	Sí	No	NIDS
Ourmon	Libre	Linux, FreeBSD	IPv4	A-IDS	No	No	NIDS
Samhain	Libre	Unix, Linux, Cygwin/Windows	IPv4/IPv6	S-IDS	Sí	No	HIDS
Ossec	Libre	Linux, FreeBSD, Windows, MacOS	IPv4/IPv6	S-IDS	Sí	No	HIDS
Tripwire	Libre	Linux, Windows	IPv4/IPv6	S-IDS	Sí	No	HIDS

La compatibilidad de Snort y Suricata con múltiples sistemas operativos facilita su implementación por parte de los administradores de red en las organizaciones. Ambas soluciones combinan distintos enfoques para la detección de intrusiones y operan con las mismas bases de firmas, elemento que agiliza su actualización ante la aparición de nuevos tipos de amenazas e intrusiones. La capacidad de estas herramientas para operar en modo IPS les brinda autonomía y fortalece la seguridad de los sistemas que monitorean.

Desventajas de los IDS

La principal desventaja de los IDS radica en sus índices de eficiencia y efectividad, fundamentalmente en redes con grandes flujos de datos. [26], [31], [39] Si el tráfico de red excede la capacidad de análisis del IDS ya sea por el tamaño de los paquetes, su velocidad, o por limitaciones del *hardware* donde opera la herramienta, esta puede rechazarlos sin realizar su análisis, situación que repercute negativamente en la seguridad del sistema porque los paquetes rechazados pueden ser producto de una intrusión o tráfico malicioso. En estos casos el IDS pierde efectividad y la seguridad de la red será comprometida.

Los autores de la presente investigación no identificaron un consenso en la literatura consultada sobre el IDS de código abierto con mejores índices de eficiencia y

efectividad. Sin embargo, se determinó que los criterios de los autores consultados están divididos en tres soluciones respectivamente: Snort [20, 21, 30, 31, 33], Suricata [24, 36, 40] y Zeek. [35, 36]

Discusión

La adopción de medidas de prevención, monitoreo y mitigación constituye una vía efectiva para evitar ataques cibernéticos y elevar la seguridad en instituciones de salud [41]. En este aspecto, los IDS desempeñan un rol fundamental porque son herramientas de monitoreo que contribuyen a implementar medidas para prevenir intrusiones en las redes de datos.

Los resultados obtenidos en este trabajo evidencian que los IDS Snort y Suricata constituyen potentes soluciones de código abierto capaces de monitorear las redes de datos y prevenir posibles ataques cibernéticos. En la presente investigación se determinó que ambas soluciones ofrecen rendimientos de seguridad superiores a sus similares en el mercado, en lo que se concuerda con otros autores. [31], [33], [36], [40]

Sin embargo, para mantener un desempeño óptimo, los IDS requieren al igual que cualquier sistema informático de actualizaciones sistemáticas. Además, aunque estas herramientas disminuyen la ocurrencia de posibles intrusiones y ataques informáticos a las redes de datos, no garantizan la invulnerabilidad de estos medios. Por esta razón, es recomendable su integración con diferentes herramientas de seguridad como los firewalls.

Conclusiones

Se identificó que Snort y Suricata constituyen los IDS de código abierto más estudiados en la literatura durante el período 2013-2020. La compatibilidad de estas soluciones con los protocolos IPv4/IPv6, su capacidad de análisis mediante el uso firmas y detección de anomalías y su funcionamiento en modo IPS constituyen elementos que resaltan su desempeño respecto a otras herramientas de detección de intrusiones. Además, la integración con diferentes sistemas operativos facilita su implementación y despliegue en las organizaciones.

El empleo de Snort y Suricata en los esquemas de ciberseguridad de las instituciones médicas contribuirá a disminuir el riesgo de intrusiones y ataques cibernéticos. Los autores de este trabajo proponen como tema para futuras investigaciones evaluar la eficiencia y efectividad de Snort y Suricata en el ambiente real de una institución de salud cubana.

Referencias

1. Ioana D, Dumitrache I. Cyber Security in Healthcare Networks. 6th IEEE International Conference on E-Health and Bioengineering - EHB 2017 [Internet]. Sinaia, Romania:

IEEE, 2017 [citado 15 Nov 2020], p. 414-417. Disponible en: https://doi.org/10.1109/EHB.2017.7995449
2. Rodríguez A, Vidal MJ, Cuellar A, Martínez BD, Cabrera YM. Desarrollo de la informatización en Hospitales. INFODIR [Internet]. 2015 [citado 15 Nov 2020]; 21:3-15. Disponible en: http://www.revinfodir.sld.cu/index.php/infodir/article/view/121/177
3. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas [Internet]. 2018 [citado 12 Nov 2020]; 113: 48-52. Disponible en: https://doi.org/10.1016/j.maturitas.2018.04.008
4. García G, Vidal MJ. La informática y la seguridad. Un tema de importancia para el directivo. INFODIR [Internet]. 2016 [citado 15 Nov 2020]; 22:47-58. Disponible en: http://www.revinfodir.sld.cu/index.php/infodir/article/view/177
5. Jalali MS, Kaiser JP. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. Journal of Medical Internet Research [Internet]. 2018 [citado 13 Nov 2020]; 20(5): e10059. Disponible en: https://doi.org/10.2196/10059
6. Ahmed M, Barkat A. False Data Injection Attacks in Healthcare. En: Data Mining. AusDM 2017. Communications in Computer and Information Science [Internet]. Singapore: Boo Y., Stirling D., Chi L., Liu L., Ong KL., Williams G. (eds), Springer, 2018 [citado 17 Nov 2020], 845, p. 192-202. Disponible en: https://doi.org/10.1007/978-981-13-0292-3_12
7. Abraham C, Chatterjee D, Sims R. Muddling through cybersecurity: Insights from the U.S. healthcare industry. Business Horizons [Internet]. 2019 [citado 19 Nov 2020]; 62: 539-548. Disponible en: https://doi.org/10.1016/j.bushor.2019.03.010
8. Barad M. Linking Cyber Security Improvement Actions in Healthcare Systems to Their Strategic Improvement Needs. Procedia Manufacturing [Internet]. 2019 [citado 9 Nov 2020]; 39: 279-286. Disponible en: https://doi.org/10.1016/j.promfg.2020.01.335
9. Bhuyan SS, Kabir U, Escareno JM, Ector K, Palakodeti S, Wyant D, et al. Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. Journal of Medical Systems [Internet]. 2020 [citado 19 Nov 2020]; 44(98): 1-9. Disponible en: https://doi.org/10.1007/s10916-019-1507-y
10. Sánchez-Henarejos, A.; Fernández-Alemán, J. L.; Toval, A.; Hernández-Hernández; I.; Sánchez-García AB; Carrillo de Gea, J. M. Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. Atención Primaria [Internet]. 2014 [citado 15 Nov 2020]; 46(4):214-222. Disponible en: http://dx.doi.org/10.1016/j.aprim.2013.10.008
11. World Economic Forum. (2020). The Global Risks Report 2020 15th Edition [Internet] [citado 30 Oct 2020]. Disponible en: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
12. Sethuraman SC, Vijayakumar V, Walczak S. Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles. Journal of Medical Systems [Internet]. 2020 [citado 14 Nov 2020]; 44(29): 1-10. Disponible en: https://doi.org/10.1007/s10916-019-1489-9
13. Jalali MS, Razak S, Gordon W, Perakslis E, Madnick S. Health Care and Cybersecurity: Bibliometric Analysis of the Literature. Journal of Medical Internet Research [Internet]. 2019 [citado 11 Nov 2020]; 21(2): e12644. Disponible en: https://doi.org/10.2196/12644
14. Guerrero J. Diseño e implementación de un sistema de monitoreo a la red de datos de entidad prestadora del servicio de salud [tesis de maestría]. Colombia: Universidad

Nacional Abierta y a Distancia; 2020. [citado 16 Nov 2020]; 100 p. Disponible en: https://repository.unad.edu.co/handle/10596/34999
15. Mahamat S, Flauzac O, Nolot F, Rabat C, Gonzalez C. Secure Exchanges Activity in Function of Event Detection with the SDN. En: e-Infrastructure and e-Services for Developing Countries. AFRICOMM 2018, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering [Internet]. Dakar, Senegal: Mendy G., Ouya S., Dioum I., Thiaré O. (eds), Springer, 2019 [citado 17 Nov 2020], 275, p. 315-324. Disponible en: https://doi.org/10.1007/978-3-030-16042-5_28
16. Socarrás HE, Santana I. Ciberseguridad del Sistema de Control Industrial de la Planta Cloro-Sosa ELQUIM. Revista Ibérica de Sistemas y Tecnologías de Información [Internet]. 2019 [citado 17 Nov 2020]; 32: 83-96. Disponible en: http://dx.doi.org/10.17013/risti.32.83-96
17. Maniriho P, Jovial L, Niyigaba E, Bizimana Z, Ahmad T. Detecting Intrusions in Computer Network Traffic with Machine Learning Approaches. International Journal of Intelligent Engineering and Systems, 2020, 13(3): 433-445. Disponibe en: https://doi.org/10.22266/ijies2020.0630.39
18. Aludhilu H, Rodríguez-Puente RA. Systematic Literature Review on Intrusion Detection Approaches. Revista Cubana de Ciencias Informáticas [Internet]. 2020 [citado 20 Nov 2020]; 14(1): p. 58-78. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2227-18992020000100058&lng=es&nrm=iso&tlng=en
19. Castellanos O, García M. Análisis y caracterización de conjuntos de datos para detección de intrusiones. Serie Científica de la Universidad de las Ciencias Informáticas [Internet]. 2020 [citado 16 Nov 2020]; 13(4): 39-52. Disponible en: https://publicaciones.uci.cu/index.php/serie/article/view/558
20. Wang X, Kordas A, Hu L, Gaedke M, Smith D. Administrative Evaluation of Intrusion Detection System. En: 2nd Annual Conference on Research in Information Technology [Internet]. Florida, USA: Association for Computing Machinery, 2013 [citado 17 Nov 2020], p. 47–52. Disponible en: https://doi.org/10.1145/2512209.2512216
21. Murphy B. Comparing the performance of intrusion detection systems: snort and suricata [tesis de doctorado]. EEUU: Colorado Technical University; 2019.
22. Perdigón R, Ramírez R. Plataformas de software libre para la virtualización de servidores en pequeñas y medianas empresas cubanas. Revista Cubana de Ciencias Informáticas [Internet]. 2020 [citado 18 Nov 2020]; 14(1): 40-57. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992020000100040&lng=es&nrm=iso&tlng=es
23. Perdigón R, Pérez MT. Análisis holístico del impacto social de los negocios electrónicos en América Latina, de 2014 a 2019. Paakat: Revista de Tecnología y Sociedad [Internet]. 2020 [citado 27 Nov 2020]; 10(18). Disponible en: http://dx.doi.org/10.32870/Pk.a10n18.459
24.Macia-Fernández G, Camacho J, Magan-Carrión R, Fuentes-García M, García-Teodoro P. UGR'16: Un nuevo conjunto de datos para la evaluación de IDS de red. En: XIII Jornadas de Ingeniería Telemática [Internet]. Valencia, España: Editorial Universidad Politécnica de Valencia, 2017 [citado 18 Nov 2020], p. 71-78. Disponible en: http://dx.doi.org/10.4995/JITEL2017.2017.6520

25. Arteaga JE. 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 [tesis de maestría]. Ecuador: Escuela Superior Politécnica de Chimborazo; 2018. [citado 3 Nov 2020]; 162 p. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/8748
26. Kumar D, Singh RA. Comprehensive Review on Intrusion Detection System and Techniques. En: International Conference on Contemporary Technological Solutions towards fulfilment of Social Needs [Internet]. India: SHODH SANGAM, 2018 [citado 21 Nov 2020]; p. 133-137. Disponible en: http://www.shodhsangam.rkdf.ac.in/papers/suvenir/133-137-Dharmendra.pdf
27. Divekar A, Parekh M, Savla V, Mishra R, Shirole M. Benchmarking datasets for Anomaly-based Network Intrusion Detection: KDD CUP 99 alternatives. En: 3rd International Conference on Computing, Communication and Security (ICCCS) [Internet]. Kathmandu, Nepal: IEEE, 2018 [citado 9 Nov 2020], p. 1-8. Disponible en: https://doi.org/10.1109/CCCS.2018.8586840
28. Ashok D, Manikrao V. Comparative Study and Analysis of Network Intrusion Detection Tools. En: International Conference on Applied and Theoretical Computing and Communication Technology [Internet]. Davangere, India: IEEE, 2015 [citado 9 Nov 2020], p. 312-315. Disponible en: https://doi.org/10.1109/ICATCCT.2015.7456901
29. Ocampo CA, Castro YV; Solarte Martínez GR. Sistema de detección de intrusos en redes corporativas. Scientia et Technica [Internet]. 2017 [citado 4 Nov 2020]; 22(1): 60-68. Disponible en: https://doi.org/10.22517/23447214.9105
30. Park W, Ahn S. Performance Comparison and Detection Analysis in Snort and Suricata Environment. Wireless Pers Commun [Internet]. 2017 [citado 21 Nov 2020]; 94, 241–252. Disponible en: https://doi.org/10.1007/s11277-016-3209-9
31. Raza SA, Issac B Performance comparison of intrusion detection systems and application of machine learning to Snort system. Future Generation Computer Systems [Internet]. 2018 [citado 20 Nov 2020]; 80: 157-170. Disponible en: https://doi.org/10.1016/j.future.2017.10.016
32. G2 Crowd.com [página Web en Internet]. Best Intrusion Detection and Prevention Systems (IDPS), 2020. <https://www.g2.com/categories/intrusion-detection-and-prevention-systems-idps?utf8=%E2%9C%93&selected_view=grid#grid> [consultado 21 Nov 2020]
33. Karim I, Vien QT, Anh Le T, Mapp G. A Comparative Experimental Design and Performance Analysis of Snort-Based Intrusion Detection System in Practical Computer networks. Computers [Internet]. 2017 [citado 21 Nov 2020]; 6(1): 1-15. Disponible en: https://doi.org/10.3390/computers6010006
34. Uvidia LA. Evaluación de herramientas de generación de tráfico malicioso aplicadas a una red ip virtualizada [tesis de maestría]. España: Universidad Politécnica de Valencia; 2017. [citado 21 Nov 2020]; 40 p.
35. Bouziani O, Benaboud H, Samir Chamkar A, Lazaar SA. Comparative study of Open Source IDSs according to their Ability to Detect Attacks. En: 2nd International Conference on Networking, Information Systems & Security [Internet]. Rabat, Marruecos: Association for Computing Machinery, 2019 [citado 21 Nov 2020]; p. 1-5. Disponible en: https://doi.org/10.1145/3320326.3320383

36. Alsakran F, Bendiab G, Shiaeles S, Kolokotronis N. (2020) Intrusion Detection Systems for Smart Home IoT Devices: Experimental Comparison Study. En: Security in Computing and Communications 2019 [Internet]. Singapore: Thampi S., Martinez Perez G., Ko R., Rawat D. (eds), Springer, 2020 [citado 21 Nov 2020]; 1208. Disponible en: https://doi.org/10.1007/978-981-15-4825-3_7
37. Caro R. Despligue y explotación de herramientas Open Source para la monitorización y gestión de eventos en un entorno virtualizado [tesis de maestría]. España: Universidad de Cádiz; 2020. [citado 21 Nov 2020]; 382 p.
38. Farré X. Desplegar la herramienta "ZeekIDS" y su posterior explotación para el análisis de actividades sospechosas en la red [tesis de maestría]. España: Universitat Oberta de Catalunya; 2019. [citado 21 Nov 2020]; 124 p.
39. Alyousef MY; Abdelmajeed NT Dynamically Detecting Security Threats and Updating a Signature Based Intrusion Detection System's Database. Procedia Computer Science [Internet]. 2019 [citado 22 Nov 2020]; 159: 1507–1516. Disponible en: https://doi.org/10.1016/j.procs.2019.09.321
40. Hänninen, M. Open source intrusion detection systems evaluation for small and medium-sized enterprise environments [tesis de maestría]. Finlandia: JAMK University of Applied Sciences; 2019. [citado 22 Nov 2020]; 77 p.
41. Interpol.int [página Web en Internet]. Cybercriminals targeting critical healthcare institutions with ransomware, 2020 <https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware> [consultado 18 Nov 2020].

Conflicto de interés

Los autores declaran que no existe conflicto de intereses.

Declaración de autoría

M.Sc. Rudibel Perdigón Llanes. Dirigió el proyecto, aplicó métodos científicos para la búsqueda y recolección de información, elaboró y aprobó el manuscrito final.

Dr.C. Arturo Orellana García. Realizó análisis y arribó a conclusiones de importancia para la investigación, elaboró el manuscrito final.