Revista Ciencia UNEMI
Vol. 15, N° 39, Mayo-Agosto 2022, pp. 44 - 53
ISSN 1390-4272 Impreso
ISSN 2528-7737 Electrónico
https://doi.org/10.29076/issn.2528-7737vol15iss39.2022pp44-53p

Suricata como detector de intrusos para la seguridad en redes de datos empresariales

Rudibel Perdigón-Llanes[1]

Resumen

El objetivo de esta investigación consiste en analizar la pertinencia y aplicabilidad de Suricata como sistema de detección de intrusiones para fortalecer la seguridad en las redes digitales de las pequeñas y medianas empresas. Se desarrolló una investigación de tipo descriptiva donde se emplearon como métodos científicos el analítico sintético y el experimental. Se evaluó el consumo de recursos de hardware de Suricata y su capacidad para la detección de intrusiones mediante el análisis basado en firmas en la red de una mediana empresa agroindustrial cubana. Se generó tráfico de red malicioso mediante la distribución Kali Linux para simular ataques de sondeo de redes, denegación de servicios y de fuerza bruta. Los resultados obtenidos evidenciaron que Suricata posee una buena efectividad para la detección de intrusiones mediante el análisis basado en firmas con un consumo eficiente de recursos de hardware. El uso de Suricata en las pequeñas y medianas empresas contribuirá a asegurar la confidencialidad, disponibilidad e integridad de sus recursos digitales.

Palabras claves: ciberseguridad, código abierto, sistemas de detección de intrusiones, telemática.

Suricata as intrusion detector for enterprise data network security

Abstract

The objective of this research is to analyze the relevance and applicability of Suricata as an intrusion detection system to strengthen security in digital networks of small and medium enterprises. A descriptive type of research was developed using synthetic analytical and experimental scientific methods. Suricata's hardware resource consumption and its intrusion detection capacity were evaluated through signature-based analysis in the network of a medium-sized Cuban agro-industrial company. Malicious network traffic was generated using Kali Linux distribution to simulate network probing, denial of service and brute force attacks. The results obtained showed that Suricata has a good effectiveness for intrusion detection through signature-based analysis with an efficient consumption of hardware resources. The use of Suricata in small and medium enterprises will contribute to ensure the confidentiality, availability and integrity of their digital resources.

Keywords: cybersecurity, open source, intrusion detection systems, telematics

Recibido: 17 de diciembre de 2021
Aceptado: 10 de marzo de 2022

[1] Ingeniero en Ciencias Informáticas. Universidad de Pinar del Río "Hermanos Saíz Montes de Oca" rperdigon90@gmail.com ORCID: https://orcid.org/0000-0001-7288-6224

I. INTRODUCCIÓN

La utilización de las tecnologías digitales en el sector empresarial contribuye a elevar la competitividad, productividad y el desarrollo económico de estas organizaciones (Perdigón y Pérez, 2020; Toala et al., 2021). En la actualidad, el uso de estas tecnologías constituye una alternativa efectiva para mantener la operatividad de las empresas ante la incidencia de crisis como la ocasionada por la pandemia COVID-19 (Medina, Ávila Y González, 2020). Sin embargo, su utilización ha incrementado los riesgos de seguridad en estas organizaciones debido al auge de los ataques informáticos y la ciberdelincuencia (Rafamantanantsoa y Rabetafika, 2018; Husák et al., 2021; Zuñiga, Jalón, Andrade y Giler 2021).

Según reportes de la compañía especializada en ciberseguridad Check Point Software Technologies Ltd., durante el primer semestre de 2021 los ciberataques se incrementaron un 29% a nivel mundial (Check Point, 2021). Según registros de Eset Security para Latinoamérica 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 (16%) y denegación de servicios (11%) (Eset Security, 2021).

Las pérdidas económicas generadas por los ciberataques impactan negativamente en las economías de las empresas, principalmente en pequeñas y medianas empresas (PYMES), que son incapaces de sostener sus negocios luego de sufrir un ciberataque de envergadura (Bustamante et al., 2020). Incrementar la seguridad de las redes digitales empresariales constituye una necesidad para garantizar la integridad y usabilidad de los recursos digitales en estas organizaciones (Tapia, Guijarro- Rodríguez y Viteri, 2018; Morales, Toapanta y Toasa, 2020).

Una de las soluciones más empleadas para alcanzar este propósito son los Sistemas de Detección de Intrusos (IDS, por sus siglas en inglés) que permiten identificar acciones y comportamientos malintencionados en una red digital mediante el análisis de los datos que por ella transitan (Karim et al., 2017; Raza & Issac, 2018; Maniriho et al., 2020; Perdigón y Orellana, 2021). Estos sistemas pueden identificar comportamientos anómalos o tipos de ataques específicos dirigidos a una red o un host en particular (Castellanos y García, 2020).

Los IDS pueden clasificarse según su enfoque de detección y por los sistemas que monitorean (Kumar & Singh, 2018; Arteaga, 2020; Cappo y Aceval, 2020). Según su enfoque de detección, se agrupan en: IDS de análisis de firmas (S-IDS) y de análisis de anomalías (A-IDS) (Macia-Fernández, et al., 2017). 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, 2020; Maniriho, et al., 2020; Alsoufi et al., 2021). 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 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 (Ashok & Manikrao, 2015; Macia-Fernández, et al., 2017; Ocampo, et al., 2017; Arteaga, 2020).

Aunque los IDS comerciales son reconocidos por su alto desempeño y efectividad, los costos 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 estas tecnologías (Janampa et al., 2021). Las PYMES poseen características organizativas y económicas que obstaculizan el despliegue de potentes infraestructuras de red en estas organizaciones (Logroño, 2017). Por tal motivo, estas empresas deben adoptar tecnologías confiables y eficientes que garanticen el correcto funcionamiento de sus recursos digitales con ahorro de costos.

Las herramientas basadas en software libre representan una solución tecnológica viable para las PYMES porque reducen costos y facilitan el despliegue de servicios digitales con un aprovechamiento óptimo de sus recursos de hardware (Perdigón y Ramírez, 2020). En este ámbito, los autores Perdigón y Orellana (2021) identificaron que Suricata constituye uno de los

Sistemas de Detección de Intrusos basados en código abierto más utilizado en la actualidad. Esta herramienta de utilización libre y gratuita permite detectar comportamientos anómalos e intrusiones en redes de datos con altos índices de efectividad mediante diferentes enfoques de detección (Park & Ahn, 2017; Murphy, 2019; Arteaga, 2020).

Los autores Janampa et al. (2021) identificaron que las PYMES carecen de sistemas de seguridad para enfrentar ataques dirigidos a sus redes digitales. Según el reporte de Eset Security para Latinoamérica, las empresas de la región apenas utilizan sistemas para la prevención de intrusiones en sus esquemas de ciberseguridad, elemento que atenta contra la confidencialidad, disponibilidad e integridad de sus sistemas digitales (Eset Security, 2021). El objetivo de esta investigación es analizar la pertinencia y aplicabilidad de Suricata como sistema de detección de intrusiones para fortalecer la seguridad en las redes digitales de las PYMES.

II. METODOLOGÍA

Se desarrolló una investigación de tipo descriptiva donde se utilizaron como métodos científicos el analítico sintético para el análisis de la literatura relacionada con el IDS Suricata y el método experimental para su implementación y evaluación práctica. Los autores Hernández-Sampieri y Mendoza (2018) determinaron que las investigaciones descriptivas permiten especificar propiedades y características de conceptos, fenómenos, variables o hechos en un contexto determinado. En este trabajo se refleja la implementación del IDS Suricata en la red de una mediana empresa agroindustrial cubana, se especifican propiedades relacionadas con su capacidad para detectar intrusiones y su consumo de recursos de hardware durante este proceso. Los indicadores anteriores constituyen aspectos relevantes para la evaluación de los IDS según los criterios de Karim et al., (2017) y Aludhilu y Rodríguez-Puente (2020).

Se desplegó la versión 6.0.4 de Suricata en un ordenador físico con las siguientes prestaciones: CPU: corei3-4160, HDD: 500 Gb, RAM: 2Gb DDR 3, NIC: 1 Gbit/s modelo TP-LINK TG-3269 y Ubuntu Server 20.04.3 como sistema operativo (SO) base. La Figura 1 describe la ubicación de la herramienta en la red de la institución.

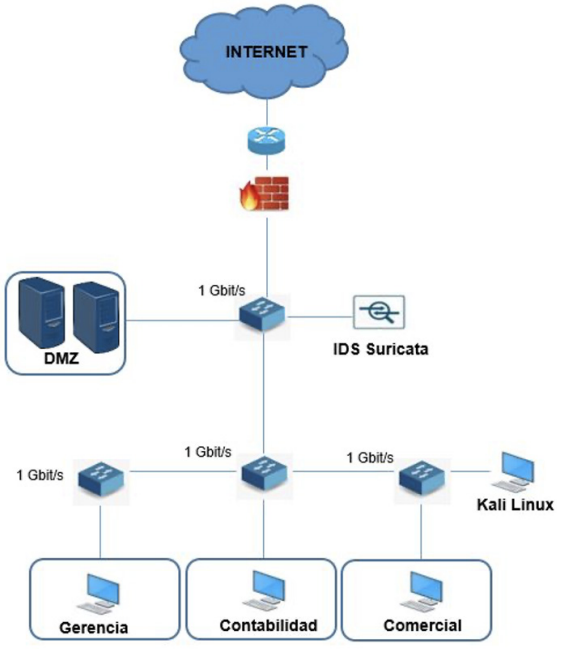


Figura 1. Ubicación del IDS en la red de la organización

La localización de Suricata detrás del firewall frontera permitirá monitorear el flujo de paquetes de red entrante y saliente de la organización. Para medir el consumo de recursos de hardware de Suricata se empleó la herramienta htop. El uso de las herramientas nmap, hping3 e hydra recogidas en la distribución Kali Linux permitió simular ataques de tipo Probing (Sondeo de redes), DoS (denegación de servicios) y de fuerza bruta, respectivamente; estos ataques son muy comunes en la actualidad y emplean un conjunto de técnicas orientadas a evadir los IDS (Bouziani et al., 2019; Perdigón y Orellana, 2021). Suricata fue desplegado en modo S-IDS empleando la base de reglas Emerging Threats Open Rules con fecha del 13 de diciembre de 2021. Estas reglas son gratuitas, disponibles en internet y poseen una estructura similar a las utilizadas por Snort por lo que también son compatibles con este IDS.

III. DESARROLLO Y DISCUSIÓN

Funcionamiento e instalación de Suricata

La arquitectura y el funcionamiento de Suricata es muy similar a Snort, sin embargo, Suricata posee mayor capacidad para analizar paquetes de red porque implementa una arquitectura de procesamiento multi-hilo (Park y Ahn, 2017). La Figura 2 describe la arquitectura de Suricata.

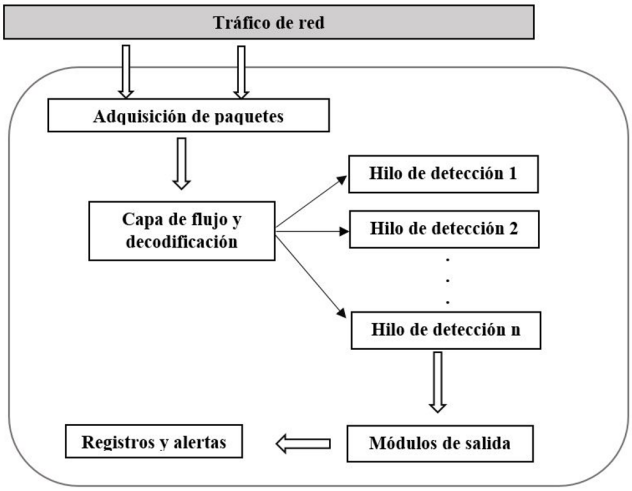


Figura 2. Arquitectura de Suricata

En este estudio no se pretende realizar una descripción exhaustiva del proceso de instalación y configuración del IDS Suricata en Ubuntu Server 20.04.3, sin embargo, es necesario resaltar algunos elementos que inciden en el correcto funcionamiento de esta solución y a la vez facilitan la reproducibilidad de este trabajo:

1. Configurar correctamente la fecha y hora del SO para visualizar de forma coherente las alertas arrojadas por Suricata durante su funcionamiento.
2. Añadir el repositorio oficial de Suricata (ppa:oisf/suricata-stable) a la lista de repositorios de Ubuntu Server.
3. Actualizar los paquetes del SO e instalar el IDS Suricata mediante los comandos del gestor de paquetes de Ubuntu (apt-get).
4. Configurar los parámetros: HOME_NET, default-log-dir, interface, default-rule-path y rules-files en el fichero de configuración suricata.yaml. Estos parámetros permiten establecer respectivamente, la subred a monitorear, la dirección de los ficheros logs, la interfaz de red por donde se capturarán los paquetes, la dirección y el nombre de los ficheros que contendrán las reglas de detección.

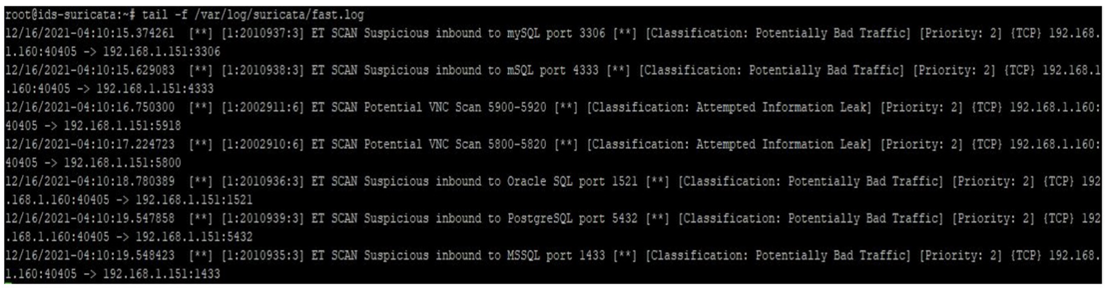
Detección de Intrusiones con Suricata en modo S-IDS

El uso de Kali Linux posibilitó evaluar la capacidad de Suricata para detectar ataques y comportamientos maliciosos en la red. Inicialmente se ejecutó la herramienta nmap para escanear los

65535 puertos de un equipo servidor ubicado en la red DMZ, mediante el siguiente comando:

>> nmap -sS -p- Dirección_IP_Servidor_DMZ

Suricata fue capaz de detectar la intrusión y arrojó las alertas descritas en la Figura 3.



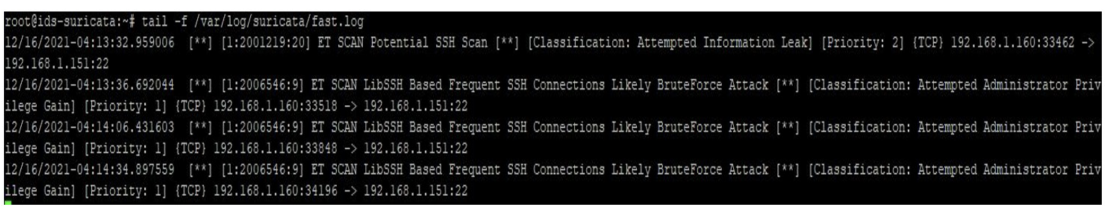
```
root@ids-suricata:~# tail -f /var/log/suricata/fast.log
12/16/2021-04:10:15.374261  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.160:40405 -> 192.168.1.151:3306
12/16/2021-04:10:15.629083  [**] [1:2010938:3] ET SCAN Suspicious inbound to mSQL port 4333 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.160:40405 -> 192.168.1.151:4333
12/16/2021-04:10:16.750300  [**] [1:2002911:6] ET SCAN Potential VNC Scan 5900-5920 [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.160:40405 -> 192.168.1.151:5918
12/16/2021-04:10:17.224723  [**] [1:2002910:6] ET SCAN Potential VNC Scan 5800-5820 [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.160:40405 -> 192.168.1.151:5800
12/16/2021-04:10:18.780389  [**] [1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.160:40405 -> 192.168.1.151:1521
12/16/2021-04:10:19.547858  [**] [1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.160:40405 -> 192.168.1.151:5432
12/16/2021-04:10:19.548423  [**] [1:2010935:3] ET SCAN Suspicious inbound to MSSQL port 1433 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.160:40405 -> 192.168.1.151:1433
```

Figura 3. Alertas de Suricata ante ataque de escaneo de puertos

Posteriormente se realizó un ataque de fuerza bruta mediante hydra al servicio SSH alojado en un servidor de la DMZ:

>> hydra -L /directorio/lista/nombre/usuarios.txt -P /directorio/lista/contraseñas.txt Dirección_IP_Servidor_DMZ ssh

Suricata también identificó el comportamiento malicioso en la red, la Figura 4 muestra las alertas arrojadas por el IDS.



```
root@ids-suricata:~# tail -f /var/log/suricata/fast.log
12/16/2021-04:13:32.959006  [**] [1:2001219:20] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.160:33462 -> 192.168.1.151:22
12/16/2021-04:13:36.692044  [**] [1:2006546:9] ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.160:33518 -> 192.168.1.151:22
12/16/2021-04:14:06.431603  [**] [1:2006546:9] ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.160:33848 -> 192.168.1.151:22
12/16/2021-04:14:34.897559  [**] [1:2006546:9] ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.160:34196 -> 192.168.1.151:22
```

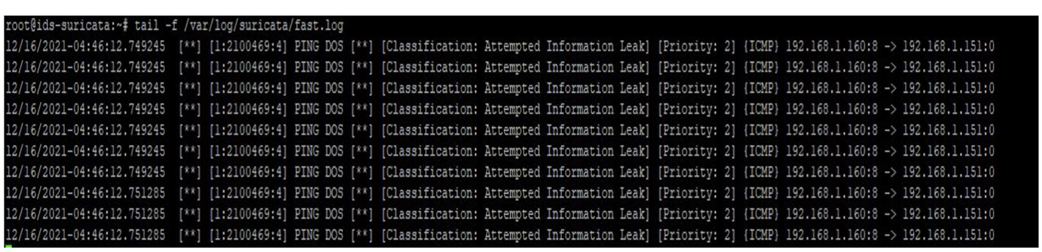
Figura 4. Alertas de Suricata ante ataques de fuerza bruta

Se generaron ataques DoS de tipo PING Flood, SYN Flood y UDP Flood y se utilizó la opción --rand-source para evadir el IDS.

PING Flood:

>> hping3 --rand-source -c 1000 --icmp Dirección_IP_Servidor_DMZ --faster

La Figura 5 muestra las alertas generadas por Suricata ante el tráfico malicioso generado.



```
root@ids-suricata:~# tail -f /var/log/suricata/fast.log
12/16/2021-04:46:12.749245  [**] [1:2100469:4] PING DOS [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.160:8 -> 192.168.1.151:0
12/16/2021-04:46:12.749245  [**] [1:2100469:4] PING DOS [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.160:8 -> 192.168.1.151:0
12/16/2021-04:46:12.749245  [**] [1:2100469:4] PING DOS [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.160:8 -> 192.168.1.151:0
12/16/2021-04:46:12.749245  [**] [1:2100469:4] PING DOS [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.160:8 -> 192.168.1.151:0
12/16/2021-04:46:12.749245  [**] [1:2100469:4] PING DOS [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.160:8 -> 192.168.1.151:0
12/16/2021-04:46:12.749245  [**] [1:2100469:4] PING DOS [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.160:8 -> 192.168.1.151:0
12/16/2021-04:46:12.749245  [**] [1:2100469:4] PING DOS [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.160:8 -> 192.168.1.151:0
12/16/2021-04:46:12.751285  [**] [1:2100469:4] PING DOS [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.160:8 -> 192.168.1.151:0
12/16/2021-04:46:12.751285  [**] [1:2100469:4] PING DOS [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.160:8 -> 192.168.1.151:0
12/16/2021-04:46:12.751285  [**] [1:2100469:4] PING DOS [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.160:8 -> 192.168.1.151:0
```

Figura 5. Alertas de Suricata ante ataque PING Flood

SYN Flood y UDP Flood:

>> hping3 --rand-source -c 1000 Dirección_IP_Servidor_DMZ -p 80 --faster

>> hping3 --rand-source -c 1000 --udp Dirección_IP_Servidor_DMZ -p 53 --faster

Se identificó que Suricata no fue capaz de detectar los ataques DoS de tipo SYN Flood y UDP Flood. Sin embargo, este IDS permite efectuar el análisis del tráfico de red mediante reglas personalizadas, lo cual posibilita elevar la efectividad de la herramienta ante las intrusiones. Estas reglas están conformadas por un encabezado y diferentes opciones (Janampa et al., 2021). La Figura 6 describe la sintaxis de las reglas de detección empleadas por Suricata.

<Acción> <Protocolo> <IP-origen> <Puerto-Origen> <dirección> <IP-Destino> <Puerto-Destino> [(<Opción-1>;...<Opción-n>;)]

Figura 6. Sintaxis de las reglas de detección de Suricata

El encabezado posee la acción que debe ejecutar el IDS (alert, drop, reject) y recoge una descripción de la comunicación establecida, definida por los parámetros: IP de origen, puerto de origen, IP de destino y puerto de destino. Las opciones de la regla recogen diferentes características y estados de conexión que, de coincidir con el paquete de red analizado, se ejecuta la acción establecida en el encabezado de la regla. La tabla 1 describe la sintaxis de las reglas creadas para incrementar la efectividad de Suricata ante los ataques generados.

Table 1. Descripción de reglas personalizadas para detectar ataques SYN Flood y UDP Flood

Ataque	Protocolo	IP-Origen	IP-Destino	Puerto-Origen	Puerto-Destino	Cuerpo de la regla
SYN Flood	TCP	any	HOME_NET	any	80	flags: S; msg: "Posible ataque DoS SYN flood detectado"; flow: to_server; detection_filter: track by_src, count 50, seconds 1; sid:100000001; rev:001;
UDP Flood	UDP	any	HOME_NET	any	53	msg: "Posible ataque DoS UDP detectado"; detection_filter: track by_src, count 50, seconds 1; sid:100000002; rev:001;

Una vez reiniciado el servicio en el servidor, Suricata fue capaz de identificar el tráfico malicioso. Las Figuras 7 y 8 muestran respectivamente la respuesta de Suricata ante los ataques SYN Flood y UDP Flood generados con la herramienta hping3

Figura 7. Respuesta de Suricata ante ataque SYN Flood

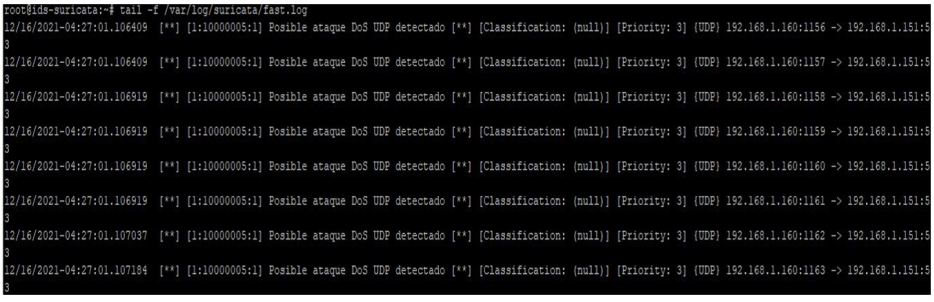


Figura 8. Respuesta de Suricata ante ataque UDP Flood

La efectividad de Suricata para la detección de intrusiones en modo S-IDS se corresponde en gran medida con la exactitud y la actualización periódica de la base de firma que utiliza. Los resultados anteriores evidencian la capacidad de Suricata para identificar ataques Probing, DoS y de fuerza bruta en una red mediante el análisis de firmas prestablecidas y reglas de detección personalizadas.

Consumo de hardware de Suricata durante la detección de intrusiones

Para comprobar el consumo de recursos de hardware del IDS Suricata se utilizó la herramienta htop durante la simulación de pruebas de intrusión. Esta evaluación se realizó durante un período de 20 minutos, las Figuras 9 y 10 describen el rendimiento de CPU y memoria RAM de Suricata durante los ataques simulados.

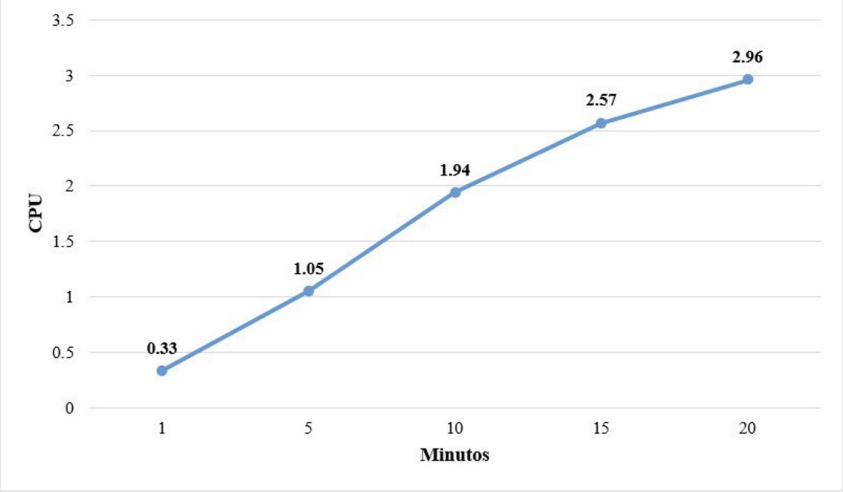


Figura 9. Consumo CPU

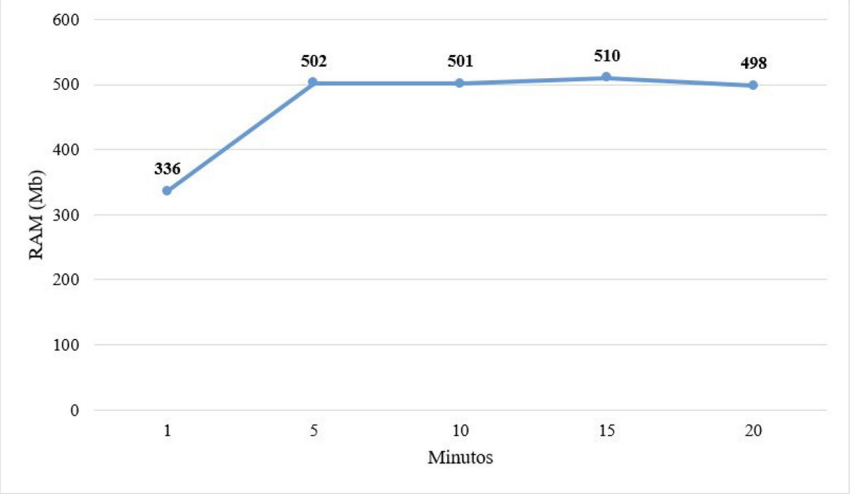


Figura 10. Consumo memoria RAM

Los resultados obtenidos permitieron identificar que el consumo de memoria RAM de Suricata no superó el 25% de la RAM disponible en el ordenador donde fue implementado. Aunque no se evidenció una sobreexplotación del CPU, se identificó un consumo considerable del mismo durante la detección de intrusiones. Esto se debe a la arquitectura de procesamiento multi-hilo que emplea la herramienta para la detección de intrusiones. De manera general se evidenció que durante su funcionamiento Suricata mantiene un consumo eficiente de los recursos de hardware.

En sus investigaciones Park y Ahn (2017); Murphy (2019) y Arteaga (2020) identificaron que Suricata posee altos índices de eficiencia y efectividad para la detección de tráfico malicioso en redes digitales. En correspondencia con estos criterios en el presente trabajo de identificó que este IDS representa una herramienta viable y efectiva para detectar tráfico malicioso en redes de

datos de PYMES.

CONCLUSIONES

En esta investigación se evaluó la pertinencia y la aplicabilidad de Suricata como sistema para la detección de intrusiones en una mediana empresa agroindustrial cubana. Se comprobó la capacidad de esta herramienta para detectar ataques de tipo Probing, DoS y de fuerza bruta y su consumo de recursos computacionales durante su funcionamiento en modo S-IDS.

Los resultados obtenidos evidenciaron que Suricata posee una buena efectividad para la detección de intrusiones utilizando reglas de detección personalizadas y la base de firmas Emerging Threats Open Rules. Asimismo, se identificó que Suricata mantiene un consumo eficiente de los recursos de hardware del ordenador donde opera durante su funcionamiento en modo S-IDS. La implementación de Suricata como IDS en los esquemas de seguridad informática de las PYMES contribuirá a identificar comportamientos maliciosos e intrusiones en sus redes digitales con un consumo eficiente de sus recursos de cómputo. El uso de esta herramienta permitirá incrementar las capacidades de las PYMES para combatir los ciberataques y sostener sus negocios en la economía digital actual.

REFERENCIAS BIBLIOGRÁFICAS

Alsoufi, M.A.; Razak, S.; Siraj, M.M.; Nafea, I.; Ghaleb, F.A.; Saeed, F.; Nasser, M. (2021) Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review, *Applied Science*, 11, 8383. doi: https://doi.org/10.3390/app1118838

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

Arteaga, 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 (LAJC)*, 7(1), 49-64. doi: https://doi.org/10.5281/zenodo.5730299

Ashok, D., y Manikrao, V. (2015). Comparative Study and Analysis of Network Intrusion Detection Tools. International Conference on Applied and Theoretical Computing and Communication Technology. Conferencia llevada a cabo en Davangere. doi: https://doi.org/10.1109/ICATCCT.2015.7456901

Bustamante, S.; Valles, M. A.; Levano, D. (2020). Factores que contribuyen en la pérdida de información en las organizaciones, *Revista Cubana de Ciencias Informáticas*, 14(3), 148-164. Recuperado de http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2227-18992020000300148

Bouziani, O., Benaboud, H., Samir Chamkar, A., 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. Conferencia llevada a cabo en Rabat. doi: https://doi.org/10.1145/3320326.3320383

Cappo, C. R., Aceval, C. R. (2020). Evaluación Heurística de Usabilidad utilizando Indicadores Cualitativos para Sistemas Detectores de Intrusión, *Entre Ciencia e Ingeniería*, 14(28), 46-51. doi: https://doi.org/10.31908/19098367.2015

Castellanos, O.; García, M. (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. Recuperado de https://publicaciones.uci.cu/index.php/serie/article/view/558

Check Point. (2021). Cyber attack trends 2021 mid year report. Recuperado de https://pages.checkpoint.com/cyber-attack-2021-trends.html

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).

Conferencia llevada a cabo en Kathmandu. doi: https://doi.org/10.1109/CCCS.2018.8586840

Eset Security. (2021). Eset Security Report Latinoamérica 2021. Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

Hernández-Sampieri, R., y Mendoza, C.P (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*. México, McGraw Hill Education.

Husák, M.., Komárková, J., Bou-Harb, E., y Čeleda, P. (2019). Survey of Attack Projection, Prediction, and Forecasting in Cyber Security, *IEEE Communications Surveys & Tutorials*, 21(1), 640-660. doi: https://doi.org/10.1109/COMST.2018.2871866

Janampa, H.; Huamani, H. L.; Meneses, 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. Recuperado de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992021000300055

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), 1-15. https://doi.org/10.3390/computers6010006

Kumar, D.; Singh, R. (2018). A Comprehensive Review on Intrusion Detection System and Techniques. International Conference on Contemporary Technological Solutions towards fulfilment of Social Needs. Conferencia llevada a cabo en RKDF University, India.

Logroño, E. (2017). Análisis de los servicios Cloud Computing para una gestión empresarial eficaz, (tesis de maestría). Pontificia Universidad Católica de Ecuador.

Macia-Fernández, G.; Camacho, J.; Magan-Carrión, R.; Fuentes-García, M.; García-Teodoro, P. (2017). UGR'16: Un nuevo conjunto de datos para la evaluacion de IDS de red. XIII Jornadas de Ingeniería Telemática. Evento llevado a cabo en Valencia: Polytechnic University of Valencia. doi: http://dx.doi.org/10.4995/JITEL2017.2017.6520

Maniriho, P., Jovial, L., Niyigaba, E., Bizimana, Z., y Ahmad, T. (2020). Detecting Intrusions in Computer Network Traffic with Machine Learning Approaches, *International Journal of Intelligent Engineering and Systems*, 13(3), 433-445. doi: https://doi.org/10.22266/ijies2020.0630.39

Medina, A., Ávila, A. y González, Y. F. (2020). Teletrabajo en condiciones de COVID-19. Ventajas, retos y recomendaciones, *Revista Cubana de Salud y Trabajo*, 21(3), 59-63. Recuperado de http://revsaludtrabajo.sld.cu/index.php/revsyt/article%20/view/168

Morales, F., Toapanta, S., y Toasa, R. M. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información, *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E27), 553-565. Recuperado de https://www.proquest.com/openview/35d3af032ceee8d79daf8a813e2c7967/1?pq-origsite=gscholar&cbl=1006393

Murphy, B. (2019). Comparing the performance of intrusion detection systems: snort and suricata, (tesis de doctorado). Colorado Technical University.

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

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

Perdigón, R., y Orellana, A. (2021). Sistemas para la detección de Intrusiones en redes de datos de instituciones de salud, *Revista Cubana de Informática Médica*, 13(2), e440. Recuperado de http://www.revinformatica.sld.cu/index.php/rcim/article/view/440

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

Perdigón, R., y Ramírez, 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. Recuperado de http://scielo.sld.cu/scielo.php?pid=S2227-18992020000100040&script=sci_arttext&tlng=es

Rafamantanantsoa, F., y Rabetafika, H. L. (2018). Performance Comparison and Simulink Model of Firewall Free BSD and Linux, *Communications and Network*, 10(4), 180-195. doi: https://doi.org/10.4236/cn.2018.104015

Raza, S. A., y Issac, B. (2018). Performance comparison of intrusion detection systems and application of machine learning to Snort system, *Future Generation Computer Systems*, 80, 157-170. doi: https://doi.org/10.1016/j.future.2017.10.016

Tapia, J. H., Guijarro- Rodríguez, A. A., y Viteri, X. O. (2018). Práctica de aplicación de seguridad y distribución de Lan Corporativa, *Revista Universidad y Sociedad*, 10(1), 41-45. Recuperado de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202018000100041&lng=es&tlng=es.

Toala, F.J., Maldonado, K., Toala, M.M., y Álava, J. E. (2021). Impacto del intranet y extranet en el desarrollo empresarial. *Serie Científica de la Universidad de las Ciencias Informáticas*, 14(9), 28-21. Recuperado de https://publicaciones.uci.cu/index.php/serie/article/view/936/792

Zuñiga, A. R., Jalón, E. J., Andrade, M. E., y Giler, J. L. (2021). Análisis de seguridad informática en entornos virtuales de la universidad Regional Autónoma de Los Andes extensión Quevedo en tiempos de Covid-19, *Universidad Y Sociedad*, 13(3), 454-459. Recuperado de https://rus.ucf.edu.cu/index.php/rus/article/view/2120