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

Evaluation of the functionalities of the intrusion detection systems based on the network of open source platforms using the anomaly detection technique

ARTICLE HISTORY

Received 26 April 2020
Accepted 06 June 2020

José Eduardo Arteaga Pucha
Quito, Ecuador
jeap_fer@yahoo.es

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

Evaluation of the functionalities of the intrusion detection systems based on the network of open source platforms using the anomaly detection technique

Arteaga Pucha José Eduardo
Quito, Ecuador
jeap_fer@yahoo.es

Resumen — El presente trabajo investigativo tiene por objeto evaluar las funcionalidades de los sistemas de detección de intrusos (IDS) basados en red de plataformas Open Source utilizando la técnica de detección de anomalías, definiendo varios conceptos acerca de los sistemas de detección de intrusos. Para la evaluación de los IDS se utilizó una metodología basada en la investigación aplicativa y cuasi-experimental, considerando los conocimientos existentes y la implementación de los casos de: aprendizaje, simulación de ataques y aplicativo, por medio escenarios virtuales, sobre los cuales se instalaron los IDS Snort, Suricata, Bro y las diferentes herramientas de Benchmark. La correlación de las alertas emitidas tanto por Snort y Suricata utilizando la técnica de detección de anomalías basada en datos estadísticos, permitió determinar los verdaderos positivos (VP) para las alertas efectivas y los falsos negativos (FN) para las anomalías.

Palabras clave — Tecnología y ciencias de la ingeniería, redes, Snort, seguridad informática, sistemas de información, Suricata (herramienta), Bro (herramienta), sistema de detección de intrusos (IDS), anomalías de sistemas de información.

Abstract *— The purpose of this research work is to evaluate the functionality of the intrusion detection systems (IDS) based on Open Source platforms using the anomalies detection technique, defining several concepts about intrusion detection systems. For the evaluation of the IDS a methodology based on the application and quasi-experimental research was used, considering the existing knowledge and the implementation of the cases of: learning, simulation of attacks and application by means of virtual scenarios, on which they were installed the Snort, Suricata and Bro IDS and the different Benchmark tools. The correlation of the alerts issued by both Snort and Suricata using the anomaly detection technique based on statistical data, allowed to determine the true positives (TP) for the effective alerts and the false negatives (FN) for the anomalies.*

Keywords — Technology and science of engineering, networks, Snort, computer security, information systems, Suricata (tool), Bro (tool), intrusion detection system (ids), anomalies of information systems.

ISSN: 1390 -9266 – 2020 LAJC

1 INTRODUCCIÓN

Los sistemas de detección de intrusos (IDS) constituyen una herramienta indispensable para la seguridad de la red de una institución o empresa. Los IDS de plataforma Open Source, que actualmente existen en el mercado son: Snort, Suricata, BRO IDS y Kismet, cada uno de ellos con su propia estructura de funcionalidad.

Para contribuir al uso de software libre, se planteó realizar una evaluación de los IDS de plataforma Open Source, con la finalidad de contar con un estudio comparativo, que sirva de base para seleccionar un sistema que se adapte a las necesidades de las instituciones y así reducir los tiempos de implementación.

Los sistemas informáticos pueden ser protegidos desde el ámbito lógico (con el desarrollo de software especializado) o físico (vinculado al mantenimiento eléctrico, por ejemplo).

Las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (virus) o llegar por vía remota (Hackers).

La cantidad de intentos de accesos no autorizados a la información que existe en Internet ha crecido durante estos últimos años, en la mayoría de las instituciones u organizaciones, estos intentos pueden ser o no detectados, debido a que al momento no han implementado mecanismos de seguridad en su infraestructura tecnológica.

Muchas empresas u organizaciones, normalmente por motivos de coste, han migrado información clave a Internet, exponiéndola hacia el exterior. Además, para comodidad de los trabajadores que solicitan teletrabajo, las compañías han tenido que "abrir sus puertas" para permitir la conexión a la intranet de la oficina desde su hogar. Desafortunadamente, cuando los atacantes comprometen los sistemas de entrada, ellos también tienen acceso a datos de la empresa u organización.

La incorporación de cortafuegos y redes privadas virtuales (VPNs) para permitir de forma segura que los usuarios externos se puedan comunicar con la intranet de la organización ha aliviado un poco el problema; un cortafuego con una política correcta puede minimizar el que muchas redes queden expuestas.

Sin embargo, los atacantes están evolucionando constantemente y aparecen nuevas técnicas como los troyanos, gusanos y escaneos silenciosos que atraviesan los cortafuegos mediante protocolos permitidos como HTTP, ICMP o DNS. Los atacantes buscan vulnerabilidades en los pocos servicios que el cortafuego permite y enmascaran sus ataques dentro de estos protocolos, quedando expuesta la red nuevamente.

La cantidad de mensajes publicados en listas de vulnerabilidades como BUGTRAQ ha aumentado de forma exagerada durante los últimos años. Las vulnerabilidades no solo afectan a sistemas tradicionalmente seguros, sino que afectan incluso a sistemas de seguridad: cortafuegos y sistemas de detección de intrusos o IDS (Intrusion Detection Systems). Esto se debe en parte a un crecimiento del número de auditorías que las empresas de software aplican a sus productos y por el aumento de interés en el campo de la seguridad por parte de los profesionales de la informática.

Los atacantes hoy en día también intentan sobrepasar los sistemas de detección de intrusos, ya sea saturándolos de tráfico o bien mediante herramientas que les proporcionan información falsa de lo que pasa por la red. El hecho de que los atacantes están incorporando técnicas anti-IDS a su arsenal, lo que les coloca en situación más ventajosa frente a organizaciones que ni siquiera disponen de un IDS.

Usualmente las instituciones, para el desarrollo de sus actividades cuenta con equipamiento tecnológico critico como son: servidores físicos y servidores virtuales, donde cada uno de ellos tiene diferente funcionalidad, como servidor puede ser: el alojamiento de la página web, correo electrónico institucional, respaldos de información, aplicaciones cliente servidor, impresiones, información técnica acorde al campo estratégico, entre otras. Se puede evidenciar la vulnerabilidad de la seguridad de información en diferentes instituciones del Ecuador.

En el año 2014 en el Ecuador, “las cifras de los ciberataques son alarmantes, según Daniel Molina, experto de la empresa Kaspersky, quien asegura que cerca del 16% de usuarios de la región son víctimas de fraudes informáticos, lo cual suma 60’090.173.” [1].

En enero de 2016, una red de hackers accedió a los sistemas informáticos de universidades privadas del Ecuador para registrar como alumnos a personas que nunca cursaron estudios superiores. Este delito incluyó a una lista de 366 personas que habrían inscrito ilegalmente sus títulos falsos en la base de datos de la Senescyt. [1].

El 17 de febrero del 2016, GMS, empresa ecuatoriana con más de 35 años de experiencia en seguridad de la información, realiza un análisis sobre los riesgos cibernéticos a los que se exponen las instituciones educativas, a propósito del reciente suceso ocurrido en enero de 2016 donde una red de hackers vulneró información de universidades privadas para ingresar ilegalmente 366 títulos falsos en la base de datos de la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (Senescyt). Este hecho ha permitido constatar las vulnerabilidades que presenta en la red y la importancia que implica para las universidades el protegerse de manera adecuada ante la inminente amenaza de ataques avanzados [1].

Carlos López, Consultor de Tecnologías de la Información de GMS, señala que existen páginas donde un cibernauta puede encontrar datos no solo de universidades sino de empresas en general. Explica que luego de hallar esta información conocida como "huella digital" los ciber delincuentes penetran las defensas perimetrales, siendo los usuarios atacados al acceder a correos maliciosos o con ayuda de algún infiltrado. Finalmente, cuando el delincuente ya está en la red, la información es manipulada sin dejar huellas, e incluso burlando los sistemas de seguridad de las universidades que no son lo necesariamente robustos o completos [1].

En varios proyectos y estudios se evidencia la utilización de sistemas de detección de intrusos de plataformas Open Source:

En el proyecto "Sistema para la correlación de alertas NIDS basados en anomalías", con el objeto de llevar a cabo un diseño capaz de correlacionar las alertas emitidas por NIDS basados en anomalías que analizan la carga útil del tráfico de la red, en busca malware. Los principales objetivos han sido la identificación de los falsos positivos, la valoración cualitativa de la probabilidad de que una anomalía sea efectivamente una amenaza y una clasificación cuantitativa que muestre el tipo concreto de amenaza detectada. Snort fue utilizado en este estudio [2].

En el artículo científico acerca de la "comparación de algoritmos para detección de intrusos en entornos estacionarios y de flujo de dato", concluyen que la detección de intrusos bajo el enfoque de aprendizaje automático tiene varias deficiencias dada la naturaleza de la propia aplicación. A pesar de ello los investigadores continúan trabajando en lograr soluciones que permitan cubrir las mismas, el despliegue de estas soluciones es lograr que cada red, como sistema autónomo, haga la construcción de su propio conjunto de datos, lo cual debe actualizarse periódicamente debido a la diversidad de aplicaciones y al emergente crecimiento de estas [3].

En otros casos el desconocimiento de la funcionalidad de los sistemas de detección de intrusos ocasiona que los administradores de servidores o de red lo instalen a modo de prueba para realizar los testeos correspondientes a fin de probar sus funcionamiento, ocasionando pérdidas tiempo y recursos, debido a estos inconvenientes no lo utilizan y prefieren utilizar otras alternativas de seguridad o software propietario.

Por unas causas u otras, las instituciones tanto privadas como públicas carecen parcialmente o tiene deficientes mecanismos de seguridad de la información que hagan frente al aumento del número de ataques que se producen en Internet, como una medida para mitigar los ataques informáticos es utilizar un sistema de detección de intrusos que alerte a los administradores de los servidores y red, cuando un intruso o eventos anormales se presenten en la red.

Actualmente la mayoría de instituciones del Ecuador no tienen instalado un sistema de detección de intrusos, debido a que no existen evaluaciones de funcionalidad o cuadro comparativos de ventajas y desventajas de los sistemas de detección de intrusos de plataformas Open Source que les permita elegir de manera eficiente y segura un sistema acorde a la infraestructura tecnológica con la que cuentan.

El presente trabajo de investigación tiene como finalidad realizar la evaluación de funcionalidades de los sistemas de detección de intrusos de plataformas Open Source, debido a que, en los estudios citados anteriormente solo se enfocan en uno solo como es el caso de Snort, por lo que se ha visto la necesidad de evaluar el resto de sistemas como son: Bro y Suricata utilizando la técnica de detección de anomalías, con el objeto de dar a conocer el mejor sistema de detección de intrusos en plataformas Open Source, debido a que en la actualidad, en el país existe el decreto 1073, emito el 12 de junio del 2020, que en su artículo 11 establece los lineamientos para la "Evaluación de factibilidad y plan de migración a tecnologías libres digitales libres" [4].

Al finalizar el trabajo de investigación se presentará un manual de buenas prácticas de los sistemas de detección de intrusos de plataformas Open Source lo que permitirá a los administradores de servidores o de red, elegir un IDS, conociendo sus ventajas y desventajas y que puede ser adaptable al entorno de trabajo con el fin de garantizar la seguridad de la información de las diferentes unidades a su cargo, ya que en su mayor parte poseen información confidencial y de uso gubernamental para la toma de decisiones, en los diferentes campos de desarrollo del país.

1.1 Preguntas de Investigación

Las preguntas de investigación definidas para este estudio son las siguientes: 1) ¿La evaluación de funcionalidades de un sistema de detección de intrusos (IDS) de plataformas Open Source utilizando la técnica de anomalías permitirá determinar al mejor IDS, al momento de realizar la detección de amenazas?; 2) ¿Cuáles son los sistemas de detección de intrusos de plataformas Open Source que se utilizan para la seguridad de la información a nivel de red?; 3) ¿Cuál es el segmento de red que garantiza una mayor cantidad de detecciones de amenazas por parte de un IDS basado en la red?; 4) ¿Cómo medir el rendimiento de los IDS basados en la red?; 5) ¿Cuál es la técnica que mejor evalúa el funcionamiento adecuado de un IDS?

1.2 Objetivo General

El objetivo principal es evaluar las funcionalidades de los sistemas de detección de intrusos basados en red de plataformas Open Source utilizando la técnica de detección de anomalías.

1.3 Objetivos Específicos

Para este estudio de investigación se han definido los siguientes objetivos específicos: 1) Estudiar los diferentes IDS basados en red de plataformas Open Source para determinar su funcionalidad; 2) Diseñar un esquema de red para la implementación de los sistemas de detección de intrusos (IDS) de plataformas Open Source; 3) Definir el Benchmark para determinar el rendimiento de los IDS frente a los ataques; 4) Elaborar un manual de buenas prácticas de los sistemas de detección de intrusos de plataformas Open Source para aportar en la implementación de un IDS de forma óptima; 5) Implementar un IDS basado en red de plataforma Open Source utilizando la técnica de detección de anomalías, en un escenario de prueba en la red de datos de una institución para mejorar la seguridad de la información.

1.4 Hipótesis

Se plantea como hipótesis que la implementación de un sistema de detección de intrusos, basado en la red de plataforma Open Source, utilizando la técnica de detección de anomalías mejorará la seguridad de la información que viaja por la red.

2 SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

La detección de intrusiones es la práctica de utilizar herramientas inteligentes y automáticas para detectar intentos de intrusión en tiempo real. Dichas herramientas se llaman Sistemas de Detección de Instrucciones (Intrusion Detection Systems, IDS).

2.1 Clasificación de los IDS

Los sistemas de detección de intrusos pueden clasificarse en función de los sistemas que vigilan (Secciones 2.1.1 y 2.1.2); y en función de cómo actúan (Secciones 2.1.3 y 2.1.4); a continuación se describe cada uno de ellos.

2.1.1 Sistemas de detección de intrusos de red (NIDS)

Garantizan la seguridad dentro de la red, por lo que necesitan un hardware exclusivo donde se implementa el sistema para que pueda verificar los paquetes de información que viajan por una o más líneas de la red. Esto se realiza con el objetivo de descubrir si se ha producido alguna actividad maliciosa o anormal.

El NIDS pone uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo.

ISSN: 1390 -9266 – 2020 LAJC

Éste es una especie de modo "invisible" en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados. Es común encontrar diversos IDS en diferentes partes de la red.

Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través del firewall o que se han realizado desde dentro [5].

2.1.2 Sistema de detección de intrusiones en el host (HIDS)

Garantizan la seguridad en el host, cubren una amplia gama de sistemas operativos como Windows, Solaris, Linux, HP-UX, Aix, etc.

El HIDS actúa como un daemon o servicio estándar en el sistema de un host. Tradicionalmente, el H-IDS analiza la información particular almacenada en registros (como registros de sistema, mensajes, lastlogs y wtmp) y también captura paquetes de la red que se introducen/salen del host para poder verificar las señales de intrusión (como ataques por denegación de servicio, puertas traseras, troyanos, intentos de acceso no autorizado, ejecución de códigos malignos o ataques de desbordamiento de búfer) [5].

2.1.3 Detección de anomalías

Desde que en 1980 James P. Anderson propusiera la detección de anomalías como un método válido para detectar intrusiones en sistemas informáticos, la línea de investigación más activa (esto es, la más estudiada, pero no por ello la más extendida en entornos reales) es la denominada Anomaly Detection IDS, IDS basados en la detección de anomalías. Estos modelos de detección conocen lo que es “normal” en nuestra red o nuestras máquinas a lo largo del tiempo, desarrollando y actualizando conjuntos de patrones contra los que comparar los eventos que se producen en los sistemas. Si uno de esos eventos (por ejemplo, una trama procedente de una máquina desconocida) se sale del conjunto de normalidad, automáticamente se cataloga como sospechoso [6].

Los IDS basados en detección de anomalías se basan en la premisa de que cualquier ataque o intento de ataque implica un uso anormal de los sistemas, Pero ¿cómo puede un sistema conocer lo que es y lo que no es “normal” en nuestro entorno de trabajo? [6]. Para conseguirlo, existen dos grandes aproximaciones: o es el sistema el que es capaz de aprenderlo por sí mismo (basándose por ejemplo en el comportamiento de los usuarios, de sus procesos, del tráfico de nuestra red) o bien se le especifica al sistema dicho comportamiento mediante un conjunto de reglas. La primera de estas aproximaciones utiliza básicamente métodos estadísticos (medias, varianzas, entre otros), aunque también existen modelos en los que se aplican algoritmos de aprendizaje automático; la segunda aproximación consiste en especificar mediante un conjunto de reglas los perfiles de comportamiento habitual basándose en determinados parámetros de los sistemas (con la dificultad añadida de decidir cuáles de esos parámetros que con mayor precisión delimitan los comportamientos intrusivos) [6].

En el primer caso (el basado en métodos estadísticos), el detector observa las actividades de los elementos del sistema, activos - sujetos -, pasivos - objetos - o ambos, y genera para cada uno de ellos un perfil que define su comportamiento; dicho perfil es almacenado en el sistema, y se actualiza con determinada frecuencia envejeciendo la información más antigua y priorizando la más fresca. El comportamiento del usuario en un determinado momento se guarda temporalmente en otro perfil, denominado ‘perfil actual’ (current profile), y a intervalos regulares se compara con el almacenado previamente en busca de desviaciones que puedan indicar una anomalía [6].

2.1.4 Detección de usos indebidos

El funcionamiento de los IDS basados en la detección de usos indebidos supone que podemos establecer patrones para los diferentes ataques conocidos y algunas de sus variaciones; mientras que la detección de anomalías conoce lo normal (en ocasiones se dice que tienen un 'conocimiento positivo', positive knowledge) y detecta lo que no lo es, este esquema se limita a conocer lo anormal para poderlo detectar (conocimiento negativo, negative knowledge) [6].

2.2 Sistemas de detección de intrusos plataformas Open Source

Dentro del proyecto de investigación se usaron los siguientes sistemas de detección de intrusos basados en la red de plataforma Open Source, ver Fig. 1, considerando que Kismet es un sistema de detección de intrusiones para redes inalámbricas 802.11, no fue analizado debido que su campo de aplicación es distinto al resto de los IDS, y no se podrían establecer cuadros comparativos al respecto.

ISSN: 1390 -9266 – 2020 LAJC

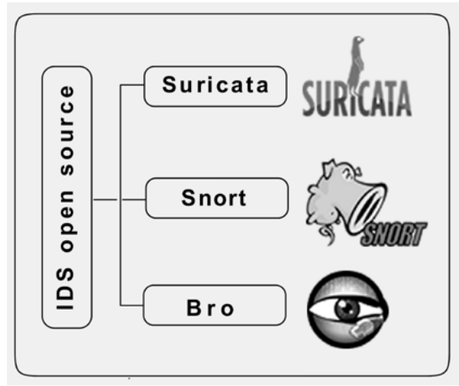

Fig. 1. IDSes de plataformas Open Source.

2.2.1 Snort

Snort es un Sistema de Detección de Intrusos (IDS) basado en red (N-IDS) Open Source. Cuenta con un lenguaje de creación de reglas en el que se pueden definir los patrones que se utilizarán a la hora de monitorizar el sistema. Además, ofrece una serie de reglas y filtros ya predefinidos que se pueden ajustar durante su instalación y configuración para que se adapte lo máximo posible a lo que deseamos, su última versión estable es de diciembre de 2016 (v.2.9.9.0) [7]. Snort puede ser configurado a modo de sniffer, packet logger y NIDS (Network Intrusion Detection System).

Entre sus ventajas más importantes están que: 1) Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, se registran sus datos. Así se sabe cuándo, de dónde y cómo se produjo el ataque hacia un equipo terminal; 2) Snort utiliza un lenguaje de descripción de reglas sencillo y ligero que es flexible y bastante potente [8].

2.2.2 Suricata

Suricata es una herramienta escalable. Este monitor de seguridad hace uso de las funciones multi-hilo de manera que solo con ejecutarse en una instancia el monitor balanceará su carga entre todos los procesadores disponibles, evitando incluso alguno de ellos si así lo especificamos. Gracias a ello, esta herramienta es capaz de procesar un ancho de banda de hasta 10 gigabits por segundo sin que ello repercuta sobre el rendimiento [9].

Esta herramienta también es capaz de identificar los principales protocolos de red, siendo capaz de controlar en todo momento todo el tráfico que se genera en el sistema y controlando posibles amenazas de malware.

Suricata trabaja actualmente de acuerdo con los avances tecnológicos actuales, se planteó contribuir con dos aspectos fundamentales faltantes: una interfaz de administración, que facilite su gestión como solución empresarial y un módulo de detección de anomalías [10].

Entre sus principales características tenemos:

• Network Intrusion Prevention (IPS - Intrusion Prevention System).
• Network Security Monitoring.
• Detección de Protocolos automáticos.
• IP Reputation, GeoIP, IP list support.
• JSON event and alert outputs – Logstache

2.2.3 Bro

Bro es un sistema de detección de intrusiones para UNIX/Linux Open Source, algo distinto a Snort y Suricata. En cierto modo, Bro es tanto un IDS basado en anomalías como en firmas. El tráfico capturado generará una serie de eventos.

Bro dispone de una serie de scripts o políticas escritos en un lenguaje nativo de Bro. Estas políticas describen qué tipo de actividades se consideran sospechosas. En base a esto, disponemos de una gran cantidad de políticas para la detección de las actividades sospechosas más comunes.

Entre sus ventajas más representativas pueden ser:

• Gran capacidad de análisis a nivel de protocolo y las políticas especializadas y configurables y la capacidad de ser una herramienta de análisis forense.
• Es de elevado rendimiento y capacidad para gestionar grandes volúmenes de tráfico.
• Sus alertas pueden ser configuradas para generar eventos de log, alertas en tiempo real y hasta ejecución de comandos de sistema.
• Las políticas, además de generar logs por actividad sospechosa, pueden generar logs de actividad normal dependiente de las configuraciones dadas.
• A través del lenguaje de scripts de políticas o policies, se pueden crear políticas específicas para un entorno de red o una actividad concreta que deseemos detectar.

3 BENCHMARK

Para realizar la evaluación de funcionalidades de los NIDS, previa investigación se procedió a instalar en diferentes entornos, obteniéndose los siguientes resultados, ver Tabla I.

TABLA I. COMPARACIÓN DE CARACTERÍSTICAS DE LOS NIDS

Características	Bro	Snort	Suricata
Multi-Threading	No	No	Si
Detección automática de protocolos	Si	No	Si
Aceleración de GNU	No	No	Si
GeoIP	Si	No	Si
Detección de alertas basa en reglas	No	Si	Si
Detección de alertas basada en scripts	Si	No	No

Como el objetivo del trabajo de investigación tiene que ver con la evaluación de los NIDS utilizando la técnica de detección de anomalías, se tomará en cuenta a los NIDS que utilicen la misma técnica para detección de alertas, en este caso: Snort y Suricata están basados en firmas o reglas y su funcionalidad se basa en el conocimiento sobre malwares y utilizan el mismo conjunto de reglas; por otro lado, Bro IDS se basa en el comportamiento y mantiene una estructura basada en la interpretación de políticas, plugins y scripts que son cargados al momento de su instalación, razón por la cual dentro del proceso de investigación realizado, se descarta la comparación de Bro IDS, debido a que su arquitectura a evaluar difiere con las características de Snort y Suricata y no se podrían establecer parámetros de igual similitud [9].

Los Benchmarks pueden ser un modo importante de averiguar cómo funciona un Sistema de Detección de Intrusos frente a los ataques, para cerciorarse de que el IDS, funciona correctamente y se ajusta a los requerimientos de la institución u organización.

Para la detección de los ataques por parte de los IDS, se utilizó la técnica de detección de anomalías basado en datos estadísticos, para lo cual se utilizaron casos de entrenamiento y simulación de ataques, mediante los cuales se analizó el tráfico de la red, con la finalidad de evaluar el comportamiento de los eventos generados y su clasificación, ya sea como un verdadero negativo, falso positivo y verdadero positivo, sus definiciones se pueden encontrar en la sección 5 Evaluación de un IDS;

Con la finalidad de comprobar la hipótesis de la investigación se realizó un caso aplicativo de evaluación de tráfico real de una institución, utilizando los escenarios virtuales.

4 DONDE COLOCAR UN IDS

Un IDS puede ser colocado en diferentes puntos de la red:

A. Delante de contrafuegos externo
B. Detrás de cortafuegos externo
C. Redes principales
D. Subredes de valor crítico
E. Máquinas

Dentro del proyecto de investigación para el proceso de evaluación de los IDS, se consideró el punto B, ya que ofrece varias ventajas al respecto como son: 1) Se monitorizan intrusiones que logran atravesar el firewall principal; 2) Detección de ataques a servidores que ofrecen servicios públicos; 3) En caso de no detectar ataques con éxito, puede reconocer algunas consecuencias de estos, como intentos de conexiones salientes, realizadas desde servidores comprometidos; 4) Identificación de los ataques y escaneos más comunes permite mejorar la configuración de los cortafuegos; 5) Monitoreo de la red LAN, ya que muchas amenazas son provocadas por usuarios internos al momento de ingresar a páginas web maliciosas o al insertar medios extraíbles contaminados en sus equipos informáticos.

En la Fig. 2. se muestra los puntos principales de ubicación de un IDS.

ISSN: 1390 -9266 – 2020 LAJC

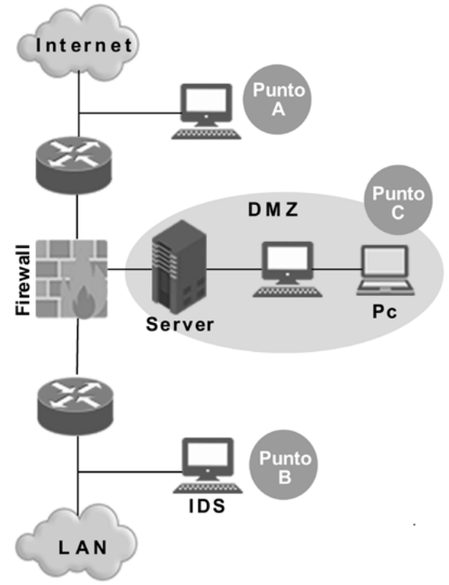

Fig. 2. Colocación de un IDS

5 EVALUACIÓN DE UN IDS

Para detectar los ataques en los diferentes escenarios se utilizará la técnica de detección de anomalías.

En los IDS basados en anomalías consiste en analizar el tráfico de la red para ver si el comportamiento de los usuarios se clasifica como ataque. Para ello, el IDS genera un autómata en el que asocia las comunicaciones a un determinado estado, y dependiendo de la actividad va cambiando la comunicación de estado hasta que se termine la comunicación o que llegue a un estado que se considera como ataque [11].

La detección de anomalías permite dar flexibilidad al sistema y detectar ataques conocidos a partir de la información del sistema. En el momento que un IDS toma una decisión, éste puede tomarla de forma correcta o incorrecta, ver Fig. 3. De acuerdo con los cuatro posibles estados [8]:

Verdadero positivo. Ataque detectado correctamente.

Verdadero negativo. Eventos inofensivos que se etiquetan como tráfico normal.

Falso positivo. También se conoce como falsa alarma y corresponde a tráfico inofensivo que se considera como ataque.

Falso negativo. Ataque que no detecta el IDS.

Fig. 3. Posibles estados en los IDS [8]

Para la evaluación de Snort y Suricata, se desarrollaron tres casos: entrenamiento, simulación y aplicativo:

Para el caso de entrenamiento se utilizaron los conjuntos de datos de DARPA 99, que contiene 2 semanas de tráfico normal y una semana de tráfico anormal, los mismos que permitieron establecer la línea base para verificación anomalías al momento de generar alertas por parte de Snort y Suricata; Para el caso de simulación a través de herramientas polivalentes como son: Hydra, Nmap, Nikto2, Hping3 y otras, se generaron ataques a hacia equipos servidores y host que eran parte de los escenarios de Snort y Suricata respectivamente; Para el caso aplicativo, se realizó el análisis de tráfico de la red de datos de una institución con la finalidad de verificar si existían alertas a nivel red y determinar si un IDS podría ser un complemento para mejorar la seguridad de la red.

Con el fin de efectuar la evaluación de Snort y Suricata, se utiliza el método de evaluación sumaria escala de Likert y para ello se crea la siguiente Tabla II, con las ponderaciones de evaluación cualitativamente, cuantitativamente y en una escala porcentual. La escala gradual es de 0 a 5 puntos de acuerdo con el cumplimiento de los indicadores expuestos.

TABLA II. PONDERACIÓN DE EVALUACIÓN DE LOS IDS

Calificación cualitativa	Valor asignado	Porcentaje
No existe	*0*	*0%*
Malo	*1*	*20%*
Regular	*2*	*40%*
Bueno	*3*	*60%*
Muy bueno	*4*	*80%*
Excelente	*5*	*100%*

Dentro del proceso de evaluación de Snort y Suricata, se definieron 3 indicadores como son: funciones, desempeño y seguridad, a continuación, se muestran los resultados obtenidos.

5.1 Indicador 1: Funciones

Con el fin de proceder con la evaluación del indicador de funciones, se consideró los valores definidos en la siguiente Tabla III, fundamentada en el método de evaluaciones sumarias (escala de Likert), en la que se crea una escala con valores graduales de 0 a 5 puntos, de acuerdo con el cumplimiento de los criterios expuestos. Además, cada valor está representado por su respectiva valoración cualitativa y porcentual.

TABLA III. PONDERACIÓN DE EVALUACIÓN DEL INDICADOR 1

Calificación cualitativa	Valor asignado	%	Descripción
No existe (N/A)	*0*	*0%*	*No aplicable para la asignación de un valor cuantitativo o no posee ese indicador o característica evaluada.*
Deficiente	*1*	*20%*	*Esta cualidad cuyo equivalente cuantitativo es igual a 1, será otorgada a las herramientas que no cumplan o cumplan de manera deficiente con el objetivo del indicador.*
Regular	*2*	*40%*	*Esta cualidad cuyo equivalente cuantitativo es 2, será otorgado a la herramienta que cumpla de manera insuficiente el indicador.*
Bueno	*3*	*60%*	*Esta cualidad cuyo equivalente cuantitativo es 3, será otorgado a la herramienta que cumpla parcialmente el indicador.*
Muy bueno	*4*	*80%*	*Esta cualidad cuyo equivalente cuantitativo es 4, será otorgado a la herramienta que cumpla casi en su totalidad el indicador.*
Satisfactorio	*5*	*100%*	*Esta cualidad cuyo equivalente cuantitativo es 5, será otorgado a la herramienta que cumpla en su totalidad el indicador.*

Para realizar la comparación de funciones que inciden directamente con la detección de intrusiones de los IDS, se compararon los criterios descritos en la Tabla IV.

ISSN: 1390 -9266 – 2020 LAJC

TABLA IV. EVALUACIÓN DEL INDICADOR 1

Criterios	Snort	Suricata
Escalabilidad	*4*	*5*
Protocolos de red	*4*	*5*
Gestiona distintos módulos salida	*3*	*4*
Soporte IPV6	*5*	*5*
Aplicaciones extendidas	*5*	*5*
Subherramientas para respuestas activas	*5*	*4*
Reputación IP	*5*	*5*
GeoIP	*5*	*5*
Promedio	4,50	4.75

El promedio del resultado de la evaluación del indicador 1 es de: 4,50 puntos para Snort y 4,75 para Suricata. Cabe indicar que esta evaluación está sustentada principalmente por búsqueda de información en sitios web oficiales de las herramientas NIDS Open Source.

Finalmente, de acuerdo con los resultados porcentuales obtenidos de acuerdo a los 8 criterios del indicador funciones de los IDS, se estipula que: Suricata es la solución más prometedora con un porcentaje total de 95 % frente a 90 % de Snort. La diferencia de los resultados obtenidos entre Suricata y Snort es sutil.

5.2 Indicador 2: Desempeño

Para la evaluación del desempeño de los sistemas de detección de intrusos, se utilizaron los paquetes de entrada y salida de DARPA 99, que corresponden a 2 semanas de entrenamiento con paquetes libre de amenazas y 1 una semana a paquetes que contiene amenazas. Con la finalidad de evaluar este indicador se hace uso de los datos de la etapa de entrenamiento, para lo cual se utilizó 44894776 (100%) paquetes divididos en 30 archivos de extensión (.pcap).

Una vez analizados los archivos correspondientes por los sistemas de detección intrusos Snort y Suricata respectivamente, se obtienen los siguientes resultados.

Se puede evidenciar, que Suricata para analizar 44894776 paquetes segmentados en 30 archivos, toma un tiempo promedio de 16,13 segundos, en cambio Snort lo realiza en un tiempo promedio de 36,20 segundos, cabe indicar que Suricata posee cierta ventaja respecto a Snort, debido a que es multihilo por lo que puede equilibrar sus procesos.

Respecto a la cantidad de alertas emitidas al momento del entrenamiento tanto con tráfico normal como anormal, se obtienen los siguientes datos al respecto, Snort emite un total de 593786 alertas, y por otra parte Suricata emite 225924 alertas, de esta manera se evidencia que Snort emite mayor cantidad de alertas al respecto.

También se pudo verificar al momento de analizar 44894776 paquetes que Suricata no tiene perdidas de paquetes y por otro lado Snort tiene una pérdida de 593786 paquetes equivalente al 1,32%. Por lo que se puede concluir que Suricata tiene un mejor desempeño respecto a Snort ya que sus tiempos son cortos a relación de Snort y no genera pérdidas de paquetes.

Para la valoración del indicador 2 se consideraron los datos de la etapa de entrenamiento, la valoración del indicador 2, se describe en la siguiente Tabla V.

TABLA V. RESUMEN DE LA EVALUACIÓN DEL INDICADOR 2

Criterio	Suricata	Snort
Tiempo de respuesta	*5*	*3*
Paquetes perdidos	*5*	*3*

5.3 Indicador 3: Seguridad

Con la finalidad de evaluar este indicador, se procedió a cuantificar el total de alertas detectadas por los sistemas de detección de intrusos, en los diferentes casos de estudio, ver Tabla VI., las mismas que serán correlacionadas a fin de obtener los valores de: verdaderos negativos (VN), verdaderos positivos (VP), falsos positivos (FP) y falsos negativos (FN).

TABLA VI. CANTIDAD DE ALERTAS EMITIDAS POR LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

Casos	Snort	Suricata
Entrenamiento	*232363*	*26975*
Simulación	*276*	*75050*
Aplicativo	*2652*	*38525*
Totales	*235291*	*140550*

En la Fig. 4, se muestra de forma gráfica la representación de las alertas emitidas por Snort y Suricata, en los diferentes casos de evaluación propuestos en el proyecto de investigación.

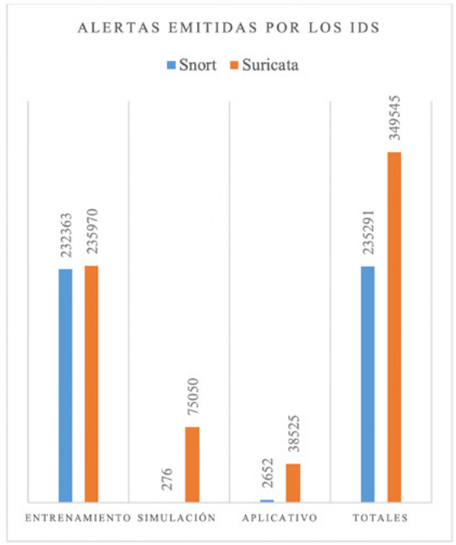

Fig. 4. Distribución del total de las alertas emitidas por los IDS

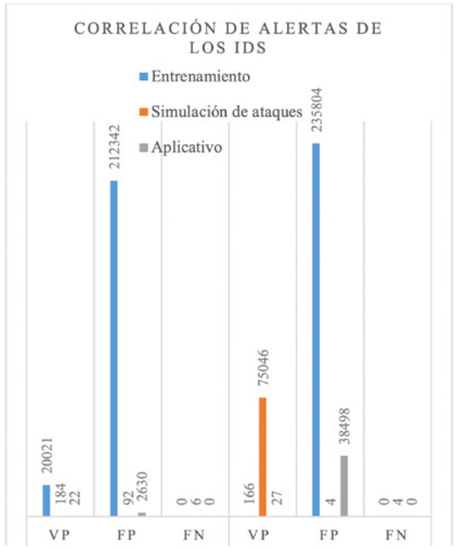

Fig. 5. Correlación de las alertas emitidas por los IDS

Una vez realizada la correlación de las alertas emitidas por Snort y Suricata con los datos estadísticos de la etapa de entrenamiento, se obtienen clasificación de los datos respecto a: VP, FP y FN, ver Tabla VII, a fin de determinar los ataques y falsas alertas (sección V. EVALUACIÓN DE UN IDS).

TABLA VII. CORRELACIÓN DE LAS ALERTAS EMITIDAS POR LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

Caso	Snort			Suricata		
	VP	FP	FN	VP	FP	FN
Entrenamiento	*20021*	*212342*	*0*	*166*	*235804*	*0*
Simulación de ataques	*184*	*92*	*6*	*75046*	*4*	*4*
Aplicativo	*22*	*2630*	*0*	*27*	*38498*	*0*
Totales	20227	215064	6	75239	274306	4

En la Fig. 5, se muestra de forma gráfica la representación de la correlación de las alertas como VP, FP y FN emitidas por Snort y Suricata, en los diferentes casos de evaluación propuestos en el proyecto de investigación.

Cabe indicar que, los falsos negativos (FN), se los consideraron en el caso simulación, debido a que los sistemas de detección de intrusos no emitieron ninguna alerta al momento de generar ataques a través de Nmap, Hydra, Nikto, Hping3 y otros, razón por la cual, por cada intrusión no detectada se otorgó un valor de la unidad que correspondería a una alerta no detectada, considerando que se desconoce la cantidad de alertas que pudiesen generar al respecto, tanto Snort como Suricata.

El valor de la precisión está determinado con la posibilidad de predecir amenazas (VP) en relación a todos los casos que el IDS detecta como positivos, y se determina por la división entre el número total de VP y la sumatoria de VP + FP (falsos positivos). El valor será un valor menor a 1, que multiplicado por 100 es el valor porcentual. Mientras el valor sea más cercano a 1, la herramienta se aproxima a un valor sensible de 100%, ver tabla VIII.

$$P = \frac{\Sigma\, VP}{\Sigma\,(VP+FP)} * 100\ \%$$

Nomenclatura:

P = Precisión
VP = Verdaderos positivos
FN = Falsos negativos

ISSN: 1390 -9266 – 2020 LAJC

TABLA VIII. CÁLCULO DE LA PRECISIÓN DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

Indicador	Snort	Suricata
Caso entrenamiento	*8.61%*	*0.07%*
Caso Simulación	*66.67%*	*99.99%*
Caso aplicativo	*0.82%*	*0.07%*
Valor promedio	**25.37%**	**33.37%**

De acuerdo a los resultados obtenidos se puede concluir que: Suricata tiene una precisión de un valor promedio de 33.37 % y por otro lado Snort tiene un valor promedio de 25.37%, estos valores son obtenidos de acuerdos a los casos de estudio del proyecto de investigación

6 MANUAL DE BUENAS PRÁCTICAS

En la actualidad las instituciones tanto privadas como públicas carecen parcialmente o tiene deficientes mecanismos de seguridad de la información que hagan frente al aumento del número de ataques que se producen en Internet.

Como una medida para mitigar los ataques informáticos es utilizar un sistema de detección de intrusos que alerte a los administradores de los servidores y red, cuando un intruso o eventos anormales se presenten en la red.

Actualmente la mayoría de instituciones del Ecuador no tienen instalado un sistema de detección de intrusos de plataforma open source, debido a que no existen evaluaciones de funcionalidad o cuadro comparativos de ventajas y desventajas de los sistemas de detección de intrusos de plataformas Open Source, que les permita elegir de manera eficiente y de forma segura un sistema acorde a la infraestructura tecnológica con la que cuentan.

En el manual de buenas prácticas de los sistemas de detección de intrusos de plataforma de software libre, se describen los pasos necesarios para su implementación y los resultados de la evaluación de sus funcionalidades, con la finalidad de reducir los tiempos al momento de elegir un IDS que se adapte a las necesidades de la institución y su proceso de instalación.

6.1 Los pasos para una implementación adecuada y eficiente de Suricata.

Para implementar Suricata de forma eficiente, se deben considerar los siguientes pasos de acuerdo con la Fig. 6.

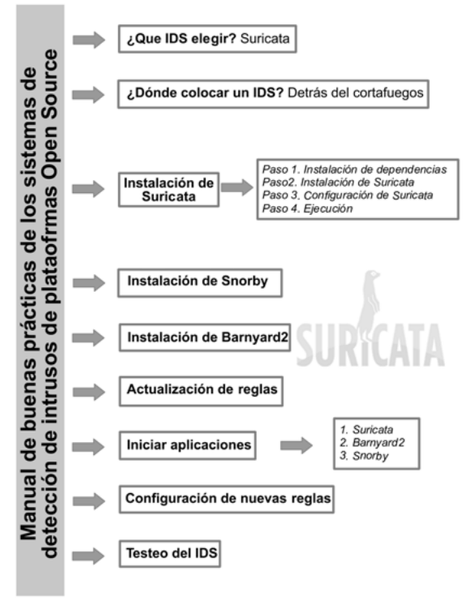

Fig. 6. Manual de buenas prácticas de implementación de un IDS de plataforma Open Source

Para un correcto funcionamiento de Suricata es necesario instalar las siguientes aplicaciones en conjunto como son: 1) Snorby que es una aplicación web (front-end), que interactúa con un IDS para monitorizar gráficamente la seguridad de la red; 2) Barnyard2 es un intérprete de las alertas que va recopilando Suricata.

Para iniciar Suricata, Snorby y Barnyard2, utilizar la siguiente secuencia, haciendo uso de 3 terminales o consolas:

Terminal 1: Iniciar Suricata
sudo suricata -c /etc/suricata/suricata.yaml -i enp0s3 -D

Nota: Cabe indicar que el nombre de la tarjeta de red puede variar dependiendo de la configuración o versión del sistema base.

Terminal 2: Iniciar Barnyard2
sudo barnyard2 -c /etc/suricata/barnyard2.conf -d /var/log/suricata -f unified2.alert -w /var/log/suricata/suricata.waldo –D

Terminal 3: Iniciar Snorby
cd /var/www/html/snorby
bundle exec rails server –e production

7 CONCLUSIONES

En el proyecto de investigación se realizó la implementación de los IDS de plataforma Open Source, que utilizan la técnica de detección de anomalías, como son Bro IDS, Snort y Suricata, en diferentes escenarios, considerando que Snort y Suricata mantienen una estructura basada en firmas de conocimiento y por otra parte BRO IDS se basa en una estructura de políticas de scripts (comportamiento), razón por la cual no se considera al momento de la evaluación de los indicadores propuestos, debido que su esquema de funcionalidad es distinto y por ende sus resultados serían discordantes.

Luego del análisis se concluyó que: en cuanto a la funcionalidad Suricata es un 5% mejor que Snort; en cuanto al desempeño se determinó que: Suricata al momento de analizar el conjunto de datos de DARPA 99 que consta de 44894776 paquetes tiene un 0% de paquetes perdidos, con respecto a Snort que tiene un 7.6 %; referente a los tiempos de respuesta utilizando el mismo conjunto de datos se evidencia que Suricata emplea un tiempo de 484 segundos y por otra parte a Snort lo toma realizar el análisis en un tiempo de 1086 segundos; y respecto a la seguridad Suricata ofrece una precisión del 3.37% respecto a Snort del 25.37%. Luego del análisis estadístico inferencial mediante la prueba Z, con la utilización de los datos del caso aplicativo se establece que Suricata ofrece una mejor seguridad que Snort.

Con la finalidad de garantizar que un IDS pueda analizar todo el tráfico que viaja en una red datos es necesario su implementación delante del firewall para que nos permita realizar una monitorización de las intrusiones que logran atravesar el firewall principal, detectar ataques a servidores que ofrecen servicios públicos, intentos de conexiones salientes e identificar los ataques y escaneos más comunes que pudiesen ocurrir.

Para poder cuantificar las alertas que emite los IDS, se emplearon diferentes herramientas polivalentes como son: Hydra, Nmap, Nikto, Hping, entre otras, cabe indicar que cada una estas herramientas tienen un objetivo específico sobre las máquinas que están siendo atacadas.

La elaboración del manual de buenas prácticas de los sistemas de detección de intrusos de plataformas Open Source, sistematiza los pasos necesarios para la implementación de un sistema de IDS, los mismos que están verificados al 2017, y de acuerdo con las versiones propuestas, ya que al momento de realizar este manual en conjunto con la implementación de los laboratorios, se encontraron que ciertos pasos descritos en manuales y documentación de la WEB, estaban obsoletos e incompletos, causando muchas molestias al momento de instalar, por lo que este trabajo servirá de base para realizar la implementación de Suricata de forma óptima, eficiente y segura, y de esta manera ser un complemento más, para aportar a la seguridad de la información que viaja por la red.

ISSN: 1390 -9266 – 2020 LAJC

8 RECOMENDACIONES

Mantener actualizado las reglas del sistema de detección de intrusos con periodicidad, permitirá que el sistema alerte sobre nuevas amenazas que viajan por la red, ya sea esta externa o interna que pueden vulnerar la seguridad de la información.

Un sistema de detección de intrusos alerta sobre nuevas amenazas, por lo que es importante complementarlo con un sistema de prevención de intrusos, con la finalidad de saber que acción se debe tomar al respecto, como puede ser denegar el servicio o permitir el acceso, de acuerdo con las reglas establecidas.

Utilizar el manual de buenas prácticas permitirá implementar un sistema de detección de intrusos de plataforma Open Source por parte de los administradores de servidores y redes de manera eficiente y segura, ya que los pasos descritos en el manual corresponden a laboratorios de casos prácticos dentro de los casos de estudios de los IDS.

La ubicación de un IDS debe estar priorizado hacia los servicios del Core de la institución u organización, ya que serán el centro de ataques de terceros con la finalidad de detener servicios tecnológicos o robar información, cabe indicar que el IDS solo alerta de amenazas porque es muy importante fusionar con otras herramientas para denegar los servicios requeridos por los intrusos o atacantes de la red.

Considerando la importancia de la seguridad de la información dentro de las instituciones se recomienda que se realice un análisis de la usabilidad de las herramientas de análisis del tráfico, con finalidad de que se determine el grado de uso de las herramientas de plataforma Open Source y su eficiencia.

REFERENCIAS

[1] GMS, "Gms presento recomendaciones para prevenir ataques ciberneticos en instituciones educativas," [Online]. Available: https://tinyurl.com/y9dul7ks [Accessed: Apr.18, 2020].

[2] J. Maestre, "Sistema para la correlación de alertas de NIDS basados en anomalías," Universidad Complutense, Madrid, 2013.

[3] J. Rivero, B. Ribiero and K. Ortiz, "Comparación de algoritmos para detección de intrusos en entornos estacionarios y de flujo de datos," [Online]. Available: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202016000400004. [Accessed: Apr.18, 2020].

[4] L. Moreno, "Plataforma presidencial," [Online]. Available: https://minka.presidencia.gob.ec/portal/usuarios_externos.jsf. [Accessed: Jun. 12, 2020].

[5] V. Carlos, "CCM sistema de deteccion de intrusiones," [Online]. Available: http://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones. [Accessed: Apr.18, 2020].

[6] Rediris, "Sistemas de detección de intrusos," [Online]. Available: https://www.rediris.es/cert/doc/unixsec/node26.html. [Accessed: 18 April 2020].

[7] D. Ortego, "Snort: Primeros pasos," [Online]. Available: https://openwebinars.net/blog/que-es-snort/. [Accessed: Apr.18, 2020].

[8] J. Gómez, "Optimizacion de sistemas de deteccion de intrusos en red utilizando tecnicas computacionales avanzadas," [Online]. Available: https://tinyurl.com/yctjb9oo. [Accessed: Apr.18, 2020].

[9] IDS/IPS, "Descripción y características de Suricata," [Online]. Available: https://blog.elhacker.net/2017/04/ids-ips-suricata-reglas-rules.html. [Accessed: Apr.18, 2020].

[10] J. A. Astudillo Herrera, A. A. Jimenez Macias and F. M. Ortiz Flores, "Adaptación del ids/ips suricata para que se pueda convertir en una solución empresarial," [Online]. Available: http://www.dspace.espol.edu.ec/xmlui/handle/123456789/19502. [Accessed: Apr.18, 2020].

[11] G. M. I. Giménez, "Utilización de Sistemas de Detección de Intrusos como elemento de Seguridad Perimetral," [Online]. Available: www.adminso.es/recursos/Proyectos/PFC/PFC_marisa.pdf. [Accessed: Apr.18, 2020].

ISSN: 1390 -9266 – 2020 LAJC

AUTOR

EDUARDO ARTEAGA

Nacido en San Miguel de Bolívar el 18 de marzo de 1987; Graduado como Ingeniero en Sistemas Computacionales en la Universidad Estatal de Bolívar en el año 2011; Magister en Interconectividad de Redes en la Escuela Politécnica del Chimborazo en el año 2018; Entre los principales cursos aprobados: Gestión de proyectos, Empoderamiento y eficacia personal con orientación a lineamientos estratégicos, Control de gestión pública, Programación web, CCNA1, CCNA2, CCNA3; Principales cargados ocupados Administrador de Base de Datos en el Instituto Geográfico Militar, Asistente de Tecnologías de la Información en el CACES, Director de Tecnologías de la Información y Comunicaciones en la Secretaría de Hidrocarburos (2016-2017), Docente y Programador de Sistemas en la Universidad Estatal de Bolívar. Asistente Administrativo y Tecnológico en la Fundación Natividad de los Andes.

J. Arteaga, "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), vol. 7, no. 1, 2020.