UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERÍA
CARRERA DE TELECOMUNICACIONES

ESTUDIO COMPARATIVO DE SISTEMAS DE DETECCIÓN DE INTRUSIONES (IDS) EN SOFTWARE LIBRE E IMPLEMENTACIÓN EN LOS LABORATORIOS DE LA FACULTAD DE INGENIERÍA DE UNIVERSIDAD NACIONAL DE CHIMBORAZO

Trabajo de Titulación para optar al título de

Ingeniero en Telecomunicaciones

Autor:

Silva Marroquín Andrés Armando

Tutor:

Mgs. Alejandra Pozo Jara

Riobamba, Ecuador. ***2024***

DECLARATORIA DE AUTORIA

Yo, Andres Armando Silva Marroquín con cédula de ciudadanía 070536216-8, autor del trabajo de investigación titulado: **Estudio comparativo de Sistemas De Detección De Intrusiones (IDS) En software libre e implementación en los Laboratorios De La Facultad De Ingeniería de la Universidad Nacional De Chimborazo**, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

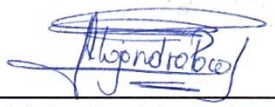
Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor de la obra referida será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

Andres Armando Silva Marroquín
C.I: 070536216-8

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, Alejandra del Pilar Pozo Jara catedrático adscrito a la Facultad de Ingeniería, por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación titulado: **Estudio comparativo de Sistemas De Detección De Intrusiones (IDS) En software libre e implementación en los Laboratorios De La Facultad De Ingeniería de la Universidad Nacional De Chimborazo**, bajo la autoría de Andres Armando Silva Marroquín; por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba, a los 27 días del mes de mayo de 2024



Mgs. Alejandra del Pilar Pozo Jara
TUTORA

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación: Estudio comparativo de Sistemas De Detección De Intrusiones (IDS) En software libre e implementación in los Laboratorios De La Facultad De Ingeniería de la Universidad Nacional De Chimborazo, presentado por Andrés Armando Silva Marroquín, con cédula de identidad número 070536216-8, bajo la tutoría de Mgs. Alejandra del Pilar Pozo Jara; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 31 de mayo de 2024.

PhD. Antonio Meneses
PRESIDENTE DEL TRIBUNAL DE GRADO

PhD. Leonardo Rentería
MIEMBRO DEL TRIBUNAL DE GRADO

Mgs. José Luis Jinez
MIEMBRO DEL TRIBUNAL DE GRADO

CERTIFICACIÓN

Que, **Silva Marroquín Andres Armando** con CC: **0705362168**, estudiante de la Carrera **Telecomunicaciones**, Facultad de **Ingeniería**; ha trabajado bajo mi tutoría el trabajo de investigación titulado "**ESTUDIO COMPARATIVO DE SISTEMAS DE DETECCIÓN DE INTRUSIONES (IDS) EN SOFTWARE LIBRE E IMPLEMENTACIÓN EN LOS LABORATORIOS DE LA FACULTAD DE INGENIERÍA DE UNIVERSIDAD NACIONAL DE CHIMBORAZO**", cumple con el 2 %, de acuerdo al reporte del sistema Anti plagio **TURNITIN**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 28 de mayo de 2024

Mgs. Alejandra Pozo Jara
TUTOR(A)

DEDICATORIA

Dedico el presente trabajo a Dios Todopoderoso, por ser la luz que ha guiado mis pasos y por darme la fortaleza para alcanzar mis metas.

Patricia Marroquín, mi madre, por ser mi fuente de inspiración constante. Gracias por creer en mí siempre, incluso cuando yo dudaba de mí mismo, a mi papá, Armando Silva, por enseñarme el valor del trabajo duro y la perseverancia. Gracias por ser mi ejemplo a seguir y por mostrarme siempre el camino correcto, a mis hermanos, por su amistad, su apoyo y por compartir conmigo los momentos más importantes de mi vida. Gracias por ser mi pilar fundamental y por estar siempre ahí para mí, así también a mis abuelos, por su amor incondicional y por sus sabios consejos. Gracias por ser parte de mi vida y por enseñarme valores importantes como la familia, la responsabilidad y el respeto.

AGRADECIMIENTO

La culminación de este trabajo de investigación representa un hito importante en mi vida personal y profesional, el cual no hubiera sido posible sin el apoyo incondicional y la colaboración de diversas personas e instituciones a quienes quiero expresar mi más profundo agradecimiento.

A mi madre, Patricia Marroquín, y a mi padre, Armando Silva, por su constante apoyo y motivación, inculcándome desde temprana edad el valor del esfuerzo y la perseverancia.

A la Universidad Nacional de Chimborazo, mi alma mater, por brindarme la oportunidad de formarme profesionalmente en un ambiente académico de excelencia. Agradezco a las autoridades, docentes y personal administrativo por su invaluable contribución a mi formación personal e intelectual.

De manera especial, a mi tutora de tesis, Mgs. Alejandra Pozo, por su invaluable guía, paciencia y dedicación durante el desarrollo de este trabajo. Su experticia, conocimiento y comentarios constructivos fueron fundamentales para la culminación satisfactoria de esta investigación.

ÍNDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

En la presente investigación se aborda la temática de la seguridad en redes, enfocándose en la evaluación y comparación de tres herramientas de Detección de Intrusiones (IDS) de Software Libre: Suricata, Snort y Zeek. El objetivo principal fue analizar las características, funcionalidades, rendimiento y eficiencia de estas herramientas en la detección de intrusiones en redes informáticas, con la finalidad de implementar una herramienta para evitar intrusiones maliciosas dentro de los Laboratorios de Ingeniería.

Se realizo un análisis con las herramientas Nessus y OpenVas, para el descubrimiento de las vulnerabilidades dentro de los Laboratorios. Finalmente, se demuestra que las vulnerabilidades encontradas son supervisadas y controladas por el IDS implementado.

Palabras claves: IDS, ciberseguridad, vulnerabilidades, Suricata, Snort, Zeek.

ABSTRACT

This research delves into the crucial realm of network security, with a specific focus on evaluating and comparing three free software Intrusion Detection Systems (IDS): Suricata, Snort, and Zeek. Our primary aim was to meticulously analyze these tools' features, functionalities, performance, and efficiency in detecting intrusions in computer networks. Furthermore, we sought to implement a tool that could effectively prevent malicious intrusions within the Engineering Laboratories, a significant step towards bolstering network security. Through a comprehensive analysis using the OpenVas and Nessus Tools, we successfully unearthed vulnerabilities within the Laboratories. Crucially, we were able to demonstrate that these vulnerabilities, once identified, were effectively monitored and controlled by the implemented IDS. This successful implementation underscores the robustness and reliability of these tools, marking a significant milestone in our ongoing efforts to enhance network security.

Keywords: IDS, cybersecurity, vulnerabilities, Suricata, Snort, Zeek

Reviewed by:
Mgs. Kerly Cabezas
ENGLISH PROFESSOR
C.C 0604042382

CAPÍTULO I

1.1 Introducción

En la última década, ha habido un crecimiento exponencial en el uso del internet, hasta prácticamente volverlo una necesidad, según un estudio de la Unión Internacional de Telecomunicaciones (UIT) nos menciona que más del 63% de la población mundial utilizan el servicio de internet[1]. Esta penetración de internet en la población ha ocasionado que las empresas de todos los tamaños sean dependientes del internet, lo que los vuelve blancos atractivos para los ciberdelincuentes.

Los ciberataques son acciones potencialmente peligrosas realizadas por organizaciones criminales con el objetivo de obtener información confidencial, provocar interrupciones de servicios o causar graves daños a los sistemas informáticos de las organizaciones atacadas[2].

Existen gran variedad de ataques en la actualidad, de los que se podría mencionar los más utilizados: el ataque distribuido de denegación de servicio (DDoS), Malwares, MITM, Exploits, phishing, etc. Para evitar estos ataques es sumamente importante tener medidas de seguridad para protegerse y garantizar la confidencialidad, integridad y disponibilidad de la información confidencial de la organización[2].

Los IDS son una de las formas más utilizadas para detectar y prevenir los ciberataques[2]. Sin embargo, es necesario mencionar aquí que estos sistemas IDS se han convertido en un medio eficaz para controlar las redes de comunicación debido a su capacidad para supervisar la red en tiempo real utilizando distintos métodos de detección de intrusiones[3].

En el presente Proyecto de Investigación se llevará a cabo un estudio comparativo sobre los diferentes Sistemas Detección de Intrusos (IDS) que se encuentran en el mercado, optando por los de código abierto, con el objetivo de evaluar cual de estos sistemas es el óptimo para su implementación dentro del Universidad Nacional de Chimborazo en los Laboratorios de la Facultad de Ingeniería.

1.2 Antecedentes

En los últimos años, la seguridad informática se ha convertido en un tema de gran importancia, debido a la creciente dependencia de la tecnología y la información digital[4]. Una de las herramientas más importantes para proteger los sistemas informáticos es un Sistema de Detección de Intrusos (IDS, por sus siglas en inglés)[5], además el Articulo: "Análisis integral de los IDS"[6], nos menciona como funcionan estos sistemas y como impactan en la protección de los datos .

Los Sistemas de Detección de Intrusos son un método efectivo para detectar actividad maliciosa en una red o sistema informático, y alertar al personal encargado de la seguridad sobre posibles intrusiones. Estos sistemas se pueden implementar a nivel de red, de host o de aplicación, y pueden usar una variedad de técnicas y algoritmos para detectar intrusiones [4].

A lo largo de los años, ha habido una tendencia hacia el uso de software libre (Open Source) para implementar sistemas de detección de intrusos [7]. Las vulnerabilidades también son un tema importante a tratar por este motivo el articulo "*An analysis of how many undiscovered vulnerabilities remain in information systems*" [8], trata de abordar todo lo relacionado a vulnerabilidades no descubiertas y como puede afectar.

Hablando de entornos educativos la Revista Tecnológica ESPOL [9], nos da una idea de las comparaciones de IDS en estos entornos. La Universidad Nacional de Chimborazo, dentro de la Facultad de Ingeniería cuenta con laboratorios de informática donde se realizan diversas actividades académicas y de investigación. Por este motivo es necesario que estos laboratorios dispongan de sistemas de detección de intrusiones que salvaguarden la información dentro de estos laboratorios.

En este contexto, se plantea la realización de un estudio comparativo entre varios sistemas de detección de intrusos (IDS) en software libre y su implementación en los laboratorios de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo. Esta investigación, permitirá determinar las características, fortalezas y debilidades de los diferentes IDS en software libre, y optar por el más adecuado para su implementación en los laboratorios de Ingeniería.

1.3 Planteamiento del Problema

Todas las instituciones u organizaciones tienen algo en común, que su activo más importante es la información que manejan de forma digitalizada, lo cual deja vulnerabilidades hacia ataques del tipo informático, que ponen en riesgo a las redes institucionales. Nuestro país se ha visto perjudicado por este tipo de ataques, en el año 2017, Ecuador quedó en tercer lugar de afectación en América Latina por el virus WannaCry, y para el 2019 toda la información de los 17 millones de ecuatorianos quedo expuesta por los hackers" [10].

Las Universidades y grandes Instituciones en sus inmediaciones ofrecen gran variedad de servicios lo cual implica tener redes de gran tamaño con distintos puntos de acceso al internet, por esta razón, muchas veces son blancos fáciles para distintos tipos de programas malignos, virus y hackers [11].

La Universidad Nacional de Chimborazo dentro de su infraestructura de red dispone de dispositivos de seguridad como Firewall, y antivirus, pero existen ataques que estos dispositivos de seguridad pudieran omitir en sus análisis.

El problema en el que se centrará esta investigación es comparar las diferentes alternativas de sistemas de IDS existentes de software Libre y determinar cuál es el más eficaz para detectar ataques informáticos en un entorno específico. Se pretende analizar las diferentes características de los sistemas de IDS y su capacidad para detectar ataques cibernéticos, y mediante un estudio comparativo, determinar cuál es el sistema de IDS recomendado para su implementación en los laboratorios de la Facultad de Ingeniería.

1.4 Justificación

En lo que respecta a la seguridad informática es de gran importancia en la actualidad, ya que el auge del internet y la creciente dependencia de la tecnología ha llevado a un aumento en los riesgos de seguridad informática. La implementación de sistemas de seguridad es fundamental para proteger los sistemas informáticos y las redes de comunicación de datos[7].

Entre las diversas herramientas de seguridad informática, los sistemas de detección de intrusiones (IDS) son una línea de protección adicional que pueden detectar actividades maliciosas en una red o sistema informático, y alertar al personal encargado de la seguridad sobre posibles intrusiones. Estos sistemas son capaces de detectar intrusiones tanto en la parte exterior como dentro de la red, y responder a los ataques en tiempo real, permitiendo la transmisión del tráfico no malicioso de la red [7].

Aunque existen sistemas IDS en el mercado, varios de ellos se encuentran licenciados y su precio es bastante elevado. Dado esto, los sistemas IDS en software libre es una alternativa maravillosa, ya que permite adaptarse a las necesidades específicas de cada organización. [7].

Tomando en cuenta esta información, se propone realizar un estudio comparando los IDS de Software Libre que existen en el mercado, donde se permita identificar las características, funcionalidades y rendimiento, y así seleccionar el más acorde a las necesidades para implementar en los Laboratorios de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo [7].

1.5 Objetivos

1.5.1 General

- Comparar los Sistemas de Detección de Intrusiones utilizando Software Libre y su implementación dentro de los laboratorios de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo.

1.5.2 Específicos

- Identificar las vulnerabilidades que existen en la Red de los Laboratorios de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo.
- Realizar un estudio comparativo de los IDS en Software Libre.
- Determinar el IDS que se implementará en función de las vulnerabilidades detectadas para un óptimo funcionamiento en la Red de los Laboratorios de la Facultad de Ingeniería.
- Evaluar el rendimiento y estabilidad del inicio de operación del Servidor IDS mediante pruebas de detección y rendimiento.

CAPÍTULO II

1.1 Marco Teórico

1.1.1 La Seguridad Informática

En el ámbito de la seguridad informática, la comprensión profunda de los fundamentos que la sustentan resulta indispensable para abordar con éxito las áreas más complejas de esta disciplina. Uno de estos fundamentos es el concepto de seguridad, el cual implica un estado de bienestar que se logra al eliminar el riesgo gracias a la confianza en algo o alguien. Si se aborda la seguridad desde el ámbito disciplinario, se la puede definir como una ciencia interdisciplinaria que se dedica a evaluar y gestionar los riesgos a los que se exponen las personas, los animales, el medio ambiente o los bienes[12].

La seguridad siempre busca la gestión de riesgos, esto quiere decir que se tenga siempre una forma de evitarlo o prevenirlo y que se pueda realizar ciertas acciones para evitar esas situaciones de la mejor forma[12]. Se definió que la seguridad podría ser catalogada como la ausencia de riesgo, la definición de este término involucra cuatro acciones que siempre están inmersas en cualquier asunto de seguridad como son:

- Prevención del riesgo
- Mitigar el riesgo
- Transferir el riesgo
- Aceptar el riesgo

Así que, cuando se está buscando hacer algo más seguro, estas acciones son algo que se debe de considerar sin importar el área, se aplica a cualquier intento de tener mejor o mayor seguridad en cualquier tema que se requiera[12].

1.1.2 Importancia de la Seguridad de la Red

La seguridad de la red es esencial para proteger los sistemas informáticos, los datos almacenados en ellos y los servicios en línea de las organizaciones. Es importante contar con medidas de seguridad adecuadas para protegerse de los ciberataques y garantizar la disponibilidad y confiabilidad de los servicios y aplicaciones en línea. Los ciberataques pueden tener graves consecuencias como la pérdida de datos confidenciales, interrupciones en los servicios y daños económicos. Por lo tanto, es crucial mantenerse

actualizado y contar con una estrategia de seguridad en red sólida y en constante evolución [13].

1.1.3 Ataques más comunes en una red de datos

Existen muchos tipos diferentes de ataques cibernéticos que pueden afectar a las redes de datos, pero algunos de los más comunes incluyen:

Ataques de malware: el malware es un software malicioso que se utiliza para dañar o controlar los sistemas informáticos. Los ataques de malware pueden incluir virus, troyanos, gusanos y ransomwares, entre otros [14].

Ataques de denegación de servicio (DoS): los ataques de DoS son una técnica utilizada para interrumpir o detener los servicios en línea mediante el envío de un gran volumen de tráfico a un servidor o red [14].

Ataques de inyección SQL: los ataques de inyección SQL son una técnica utilizada para obtener acceso no autorizado a bases de datos mediante la inyección de código malicioso en consultas SQL [14].

Ataques de fuerza bruta: los ataques de fuerza bruta son una técnica utilizada para descifrar contraseñas mediante el intento de adivinar la contraseña mediante la prueba de un gran número de combinaciones posibles [14].

Ataques de intrusión: Un ataque de intrusión es una forma de ataque cibernético en el cual un atacante logra acceso no autorizado a un sistema o red, pudiendo realizar cambios, extracción de información, propagación de malware, etc. [14].

1.2 Líneas de Defensa contra Ataques de Red

Existen varias líneas de defensa que se pueden implementar para proteger una red de ataques cibernéticos, algunas de las cuales incluyen:

Seguridad en la capa de red: se refiere a medidas de seguridad que se implementan en el nivel de la red, como firewalls, Routers de seguridad y dispositivos de detección de

intrusos (IDS). Estas medidas ayudan a controlar el tráfico de red y a detectar actividades sospechosas [15].

Autenticación y autorización: se refiere a medidas de seguridad que se utilizan para garantizar que solo los usuarios autorizados tengan acceso a los recursos de la red. Esto puede incluir la implementación de contraseñas seguras y la autenticación de dos factores [15].

Monitoreo y detección: se refiere a la implementación de medidas para monitorear y detectar actividades sospechosas en la red, como el uso de software de detección de intrusos y registros de seguridad [15].

1.3 Funcionamiento y características de los sistemas de detección de intrusiones (IDS)

1.3.1 Sistema de Detección de Intrusos

Un sistema de detección de intrusos es una herramienta fundamental para detectar y prevenir ataques informáticos no autorizados a sistemas, redes y dispositivos. Los proveedores de seguridad informática confirman que los sistemas de detección de intrusos son una de las mejores herramientas para combatir estas amenazas, y se encuentran entre los programas más utilizados y reconocidos en la actualidad. Conocido como IDS (sistema de detección de intrusiones, por sus siglas en inglés), este programa emplea sensores virtuales para recopilar datos externos, generalmente sobre el tráfico de red, y detectar así anomalías que puedan indicar la presencia de un ataque, evitando así falsas alarmas[16].

1.3.2 Funcionamiento de un IDS

Un IDS (Sistema de Detección de Intrusos) es un software que tiene como objetivo detectar y prevenir accesos no autorizados a un sistema, red o dispositivo. Su funcionamiento se basa en la captura y análisis del tráfico de red, identificando patrones y comportamientos anómalos que puedan ser indicativos de un intento de intrusión[17], [18].

Los IDS suelen contar con sensores virtuales que analizan el tráfico de red y envían alertas al núcleo del sistema cuando se detecta alguna anomalía. [17], [18].

El IDS es capaz de detectar diferentes tipos de ataques, como, por ejemplo: intentos de intrusión, escaneos de puertos, denegación de servicio (DoS), ataques de fuerza bruta y otros tipos de ataques [17], [18].

1.3.3 Características de los IDS

Los IDS tienen varias características importantes que los hacen una herramienta crucial en la protección de los sistemas informáticos. Según la investigación [19], algunas de las características más relevantes de los IDS son:

Monitoreo en tiempo real: Los IDS monitorean de manera continua los eventos que ocurren en el sistema y alertan de inmediato cuando detectan una actividad sospechosa.

Análisis de comportamiento: Los IDS analizan el comportamiento normal del sistema y generan alertas cuando detectan actividades que no se ajustan a ese patrón.

Detección de anomalías: Los IDS utilizan técnicas avanzadas de detección de anomalías para identificar patrones de tráfico que pueden ser indicativos de actividades maliciosas.

Automatización: Los IDS utilizan técnicas de automatización para gestionar y procesar grandes cantidades de datos en tiempo real.

Flexibilidad: Los IDS pueden ser configurados y personalizados para satisfacer las necesidades específicas de cada organización.

Escalabilidad: Los IDS son capaces de manejar grandes volúmenes de tráfico y son escalables para adaptarse a redes de cualquier tamaño.

1.4 Tipos de sistemas de detección de intrusiones (IDS)

Existen dos tipos de sistemas de detección de intrusos: basados en red y basados en host[20].

Los sistemas de detección de intrusos basados en red (NIDS) analizan todos los paquetes de datos que pasan por la red y generan alertas basadas en el contenido, lo que los hace más distribuidos que los IDS basados en host[20].

Por otro lado, ***los IDS basados en host (HIDS)*** analizan el comportamiento de cada sistema y son más versátiles que los NIDS, pudiendo instalarse en cualquier sistema, desde un PC de escritorio hasta un servidor. Además de detectar actividades internas no autorizadas, son eficaces para detectar modificaciones no autorizadas de archivos [20].

1.5 Arquitectura de los sistemas IDS

Hoy en día, las arquitecturas utilizadas para desarrollar herramientas IDS se basan en dos principios fundamentales: el uso de agentes autónomos que recopilan información por separado y la exploración de datos en tiempo real. También existen arquitecturas híbridas que buscan la mejor solución posible[21].

Arquitectura basada en la Exploración en Tiempo Real

La arquitectura basada en Agentes Autónomos se basa en tres componentes esenciales: agentes, transceivers y monitores [21].

Los agentes envían sus resultados a un transceivers que envía los resultados globales del host a uno o más monitores[21].

Un transceivers es la interfaz de comunicación externa de un host que recibe informes de varios agentes y construye un mapa de estado del host. Tiene funciones de control y procesamiento de datos[21].

El monitor es la entidad de más alto nivel. Tiene funciones parecidas a las del transceivers, la principal diferencia es que un monitor puede controlar entidades que están ejecutándose en diferentes hosts[21].

1.6 Evaluación de sistemas IDS

La evaluación de los Sistemas de Detección de Intrusiones (IDS, por sus siglas en inglés) es un proceso crítico para evaluar la efectividad y el rendimiento de estos sistemas en la

detección y respuesta a actividades maliciosas. La evaluación tiene como objetivo medir la precisión, eficiencia y robustez de los IDS en la identificación y alerta sobre posibles intrusiones.

Se utilizan varios métodos comunes para la evaluación de los IDS:

Evaluación basada en entorno de pruebas: Este enfoque implica establecer un entorno controlado o entorno de pruebas donde se despliega el IDS. Se simulan varios tipos de ataques y escenarios de intrusión, y se evalúa la capacidad del IDS para detectar y responder a estos ataques[22].

Evaluación basada en métricas: Se definen métricas específicas para evaluar el rendimiento de un IDS. Estas métricas incluyen la tasa de detección, la tasa de falsos positivos, el tiempo de respuesta, la utilización de recursos y la escalabilidad. Se prueba el IDS con respecto a estas métricas para medir su efectividad y eficiencia en la detección y respuesta a intrusiones [22].

1.7 Herramientas de software libre para la detección de intrusiones

Las herramientas de software libre para la detección de intrusiones son ampliamente utilizadas en la industria de la seguridad informática. A continuación, se presenta una descripción de algunas de estas herramientas junto con sus características, ventajas y desventajas:

Suricata: es un sistema de detección de intrusos de red de código abierto desarrollado por la ***Open Information Security Foundation*** **(OISF)**. Es rápido, robusto y capaz de detectar intrusos en tiempo real, prevenir intrusiones en línea y monitorear la seguridad de la red. Utiliza reglas y firmas para identificar patrones maliciosos en el tráfico de red[23], [24], [25], [26].

Ventajas:

- Soporta multithreading, lo que permite aprovechar mejor los recursos del sistema.

- Puede analizar el tráfico cifrado, como los certificados TLS/SSL, las solicitudes HTTP y las peticiones DNS.

Desventajas:

- Requiere más recursos que Snort, especialmente en términos de memoria y procesamiento.
- Tiene una curva de aprendizaje más alta que Snort, debido a su mayor complejidad y variedad de opciones.

Snort: es otro sistema de detección de intrusos de red de código abierto ampliamente utilizado. Es conocido por su capacidad de análisis en tiempo real y su amplia comunidad de usuarios y desarrolladores. Snort utiliza reglas y firmas para detectar patrones de tráfico malicioso y generar alertas. - Snort es un sistema de detección de intrusos (IDS) basado en red y de código abierto [23], [24], [25], [26].

Ventajas:

- Es gratuito y flexible.
- Tiene una gran comunidad de usuarios.
- Permite un control y análisis detallado del tráfico de red.

Desventajas:

- Requiere una configuración y administración cuidadosa y compleja.
- Puede generar FP o FN si las reglas no están bien ajustadas.
- Puede consumir muchos recursos del sistema.

Bro-IDS (ahora conocido como Zeek): Bro (Zeek) es un sistema de detección de intrusiones de red de código abierto que combina técnicas basadas en firmas y anomalías. Utiliza capturas de paquetes para generar eventos y analizar el tráfico de red en busca de comportamientos sospechosos [23], [24], [25], [26].

Ventajas:

- Es flexible y extensible, se puede adaptar a diferentes escenarios y necesidades.

- Tiene una comunidad activa que desarrolla y mantiene scripts, paquetes y herramientas para Bro (Zeek).
- Genera registros de alto nivel que facilitan el análisis forense y la detección de anomalías.

Desventajas:

- Requiere un alto rendimiento y capacidad de procesamiento para analizar grandes volúmenes de tráfico.
- Tiene una curva de aprendizaje elevada para dominar su lenguaje de scripting y su arquitectura.
- Puede generar falsos positivos o falsos negativos si no se configura adecuadamente.

Es importante tener en cuenta que existen muchas otras herramientas de IDS disponibles, cada una con sus propias características, ventajas y desventajas.

1.8 Herramientas para analizar el funcionamiento de IDS

Dentro de las herramientas que se pueden utilizar para analizar el funcionamiento de los IDS o IPS podemos contar los siguientes:

Wireshark: es una herramienta de análisis de tráfico de red de código abierto que permite a los administradores de red capturar y analizar el tráfico en sus redes. Wireshark utiliza el protocolo de pcap para capturar paquetes y los muestra en una interfaz fácil de usar, permitiendo a los administradores ver detalles como direcciones IP, puertos y protocolos utilizados[27].

CAPÍTULO III

2.1 Metodología

2.1.1 Proceso de la Metodología de la Investigación

Figura I Proceso de la Metodología de la Investigación

Fuente: El Autor

2.1.1.1 Fase 1 – Revisión bibliográfica sobre los IDS

Realizar una revisión íntegra de la literatura existente sobre los sistemas de detección de intrusos (IDS) con la finalidad de lograr una comprensión profunda de los conceptos, principios y técnicas fundamentales en este campo y los principales IDS gratuitos en la red, llegando a la conclusión de que los IDS más populares son Snort, Suricata y Zeek.

2.1.1.2 Fase 2 – Realización de Simulaciones para comprobar el rendimiento de los IDS seleccionados

En esta etapa se evaluará el rendimiento de los IDS seleccionados mediante simulaciones controladas, utilizando esta simulación se podrá identificar el IDS más adecuado para proteger los laboratorios de la Facultad de Ingeniería.

2.1.1.3 Fase 3 – Determinar las vulnerabilidades de los laboratorios de la Facultad de Ingeniería

Dentro de esta fase se utilizarán distintas herramientas para identificar y evaluar las vulnerabilidades existentes en los laboratorios de la Facultad de Ingeniería, con el fin de comprender los puntos débiles que podrían ser utilizados por hackers.

2.1.1.4 Fase 4 – Elección del mejor IDS según las vulnerabilidades encontradas

Para esta fase se seleccionará el IDS más adecuado para proteger los laboratorios de la Facultad de Ingeniería, tomando en cuenta las vulnerabilidades identificadas y los requisitos de seguridad establecidos.

2.1.1.5 Fase 5 – Implementación del IDS de acuerdo a las necesidades

En esta fase se procederá a la implementación del IDS seleccionado en la fase 4 en los Laboratorios de la Facultad de Ingeniería. La implementación se llevará a cabo siguiendo las mejores prácticas de seguridad para este tipo de despliegue, asegurando una integración fluida con el entorno existente.

2.1.1.6 Fase 6 – Verificación de la funcionalidad del IDS

Comprobar que la implementación de IDS en la fase 5 funciona de manera óptima y cumple con los objetivos establecidos de seguridad. Para esta verificación se debe incluir los siguientes aspectos: La detección de ataques, la tasa de falsos positivos y el rendimiento.

2.1.2 Enfoque de la Investigación

El presente trabajo de investigación se basa en un enfoque metodológico mixto, el cual combina estrategias de investigación tanto cualitativa como cuantitativa. Este enfoque permite abordar el problema de investigación desde diferentes perspectivas.

2.1.3 Tipo de Investigación

Para la elaboración del Marco Teórico se utilizó *la* ***investigación bibliográfica*** ya que el internet es la principal fuente de información, donde se pueden encontrar documentos, informes, artículos científicos y tesis de grados de distintas universidades con información relacionada con el tema propuesto. ***La investigación cuasiexperimental***, se utilizó debido que no se utiliza ningún tipo de selección aleatoria; además es *Aplicada*, porque se analizó las diferentes vulnerabilidades encontradas; con esto se determinó que IDS tiene más ventajas con respecto a los demás; por otro lado, también se utilizó la ***investigación descriptiva*** y la ***correlacional*** porque estas nos permiten tener un análisis de los IDS, sus requerimientos, reglas, etc. y realizar un análisis crítico para seleccionar el óptimo, mientras que el otro tipo de investigación nos permite conocer la compatibilidad de la variable independiente con la dependiente.

2.2 Población y Muestra

2.2.1 Población

La población de este estudio está conformada por los datos de rendimiento de tres herramientas de Sistemas de Detección de Intrusiones (IDS): Suricata, Snort y Zeek. Estos datos se obtuvieron mediante la ejecución de cuatro ataques simulados contra las tres herramientas, con el objetivo de evaluar su efectividad en la detección de intrusiones. La toma de datos se realizó durante un periodo de 6 semanas.

2.2.2 Muestra

En este estudio, la variable dependiente de interés es el rendimiento. Para determinar el tamaño muestral adecuado, se aplicará la siguiente ecuación, válida para una población infinita:

$$n = \frac{Z\alpha^2 * p * q}{e^2}$$

Donde
n: Tamaño de la muestra
Zα: Unidad de desviación estándar con un nivel de confianza del 99% = 2.58
p: Probabilidad de que ocurra el evento estudiado = 50% = 0.5
q: Probabilidad de que no ocurra el evento estudiado (1-p) = 50% = 0.5

e: error máximo permitido =1% = 0.01
Reemplazando los valores anteriores en la formula en mención tendremos:

$$n = \frac{2.58^2 * 0.5 * 0.5}{0.01^2}$$

$$n = 16441$$

Se ha especificado el tamaño de la muestra para proporcionar un control adecuado en las pruebas para una recopilación de datos fiable, se tomarán 33 registros de cada día que se realizó las pruebas dando un total de 16632 registros. La distribución de la muestra se ha diseñado de la siguiente manera:

División por herramientas: De la muestra total calculada, para tener igual cantidad de registros a cada una de las tres herramientas IDS analizadas (Suricata, Snort y Zeek), se distribuirá de forma equitativa entre las tres (5544).

División por ataques: La porción de la muestra que se asigna a cada herramienta se dividirá en cuatro subgrupos, correspondiendo a un tipo particular de ataque (ataques de prueba de conectividad de host ICMP (1386), ataques de escaneo de puertos(1386), ataques de fuerza bruta SSH(1386) y ataques DDoS(1386)).

2.2.3 Métodos y Técnicas

Para el desarrollo del Proyecto de Investigación se utilizó las siguientes técnicas:

- Observación
- Recopilación de Información
- Pruebas

2.3 Operacionalización de las Variables

2.3.1 Variable Independiente: IDS - Sistema de detección de Intrusiones.

Tabla 1 Variable Independiente: Sistema de Detección de Intrusiones

Concepto	Categorías	Indicadores

Los IDS (Sistema de Detección de Intrusos) es una aplicación de software destinado a la detección, en dispositivos o en una red, de accesos no autorizados.	• Suricata • Snort • Zeek (BroIDS)	• Características • Funcionalidades

2.3.2 Variable Dependiente

- ***Vulnerabilidades en los Laboratorios de la Facultad.***

Tabla 2 Operacionalización de Variable: Vulnerabilidades en los Laboratorios de la Facultad

Concepto	Categorías	Indicadores
Vulnerabilidades son debilidades o agujeros de seguridad en un sistema o software que pueden ser explotados por un atacante para obtener acceso no autorizado o causar daños.	• Gravedad	• Crítico • Alta • Media • Baja • Info
	• Vulnerabilidades Encontradas	• 0-999

- ***Rendimiento.***

Tabla 3 Operacionalización de Variable: Rendimiento

Concepto	Categorías	Indicadores
Rendimiento hace referencia a la eficiencia y efectividad de un IDS en la detección de posibles intrusiones en una red	• Tasa de detección	Tasa de detección = (Intrusiones detectadas / Intrusiones totales) x 100
	• Tasa de falsos positivos	Tasa de falsos positivos = (Alertas falsas / Alertas totales) x 100
	• Tiempo de respuesta	• Milisegundos

2.4 Procedimientos

En este apartado se inicia el proceso de evaluación comparativa entre las herramientas IDS Suricata, Snort y Zeek. Para ello, se han simulado infraestructuras de red que permiten ejecutar cada una de las herramientas y obtener datos para su posterior comparación. A continuación, se procederá al análisis de las vulnerabilidades presentes

en los laboratorios de la Facultad de Ingeniería. Finalmente, se seleccionará la herramienta IDS que mejor se ajuste a las necesidades específicas del entorno.

2.4.1 Instrumentos

Para la recopilación de información en este estudio se emplearon las siguientes herramientas y técnicas:

- **Herramientas de captura de tráfico:** Estas herramientas permiten registrar el tráfico de red que circula por la infraestructura objetivo.
- **Herramientas de generación de ataques:** Estas herramientas permiten generar diferentes tipos de ataques informáticos para evaluar la efectividad de las medidas de seguridad implementadas.
- **Técnica de observación:** Esta técnica consiste en observar el comportamiento de la red y los sistemas durante la ejecución de los ataques para identificar posibles vulnerabilidades o comportamientos anómalos.

Para la captura de Tráfico

Dentro de las herramientas que se usaron para capturar el tráfico de datos se listan las siguientes:

- ***Wireshark:*** es una aplicación con interfaz gráfica de usuario intuitiva para capturar, filtrar, analizar y visualizar el tráfico de red, proporcionando información detallada sobre los protocolos, direcciones IP, puertos, contenido de los paquetes y otros datos relevantes.[28]

Para la realización de los ataques

Para esto se utilizaron algunas herramientas disponibles en Kali Linux que es una distribución de Linux optimizada para pruebas de penetración e informática forense, utilizada para encontrar vulnerabilidades y evaluación de medidas de seguridad actuales[29].

Las herramientas utilizadas para realizar los ataques son:

Hping3 es una herramienta que sirve para la generación de paquetes IP, similar al comando "ping", pero teniendo más funcionalidades. Permite él envió de diferentes tipos de paquetes como lo son: TCP, UDP, ICMP, entre otros y verificar las respuestas recibidas[30].

Nmap es una herramienta esencial para administradores de redes, investigadores de seguridad y profesionales de TI que necesitan mapear sus redes, identificar hosts vulnerables, detectar malware y realizar pruebas de penetración[31].

Hydra se utiliza para probar la seguridad de los sistemas y servicios, identificando cuentas débiles o configuraciones incorrectas de autenticación. Es una herramienta poderosa que debe utilizarse con precaución y solo con fines de prueba de seguridad autorizada[32].

2.4.2 Procedimientos para la obtención de la información.

Dentro de este proceso está la creación de un ambiente virtual (simulación) como escenario de pruebas y obtención de la información pertinente. Con el fin de que en este escenario se retransmita el tráfico de datos y poner a prueba los IDS de software libre que se procura investigar.

2.4.2.1 Creación del ambiente de pruebas

El escenario de pruebas establecido tiene como finalidad la ejecución de los IDS para la detección de los ataques realizado por las herramientas ya mencionadas.

Dicho escenario se crea a partir de la aplicación Virtual Box, las características del ordenador anfitrión son las siguientes:

Tabla 4 Características del equipo anfitrión

Procesador	AMD Ryzen 5600X 3.7GHz
Memoria RAM	16 GB
Tarjeta de Red	Realtek® RTL8111H 1000 base T (Full Duplex)
Almacenamiento	4 TB
SO	Windows 11 64 bits

La infraestructura realizada para la simulación consta de una red interna (LAN), y la red externa (WAN), además de contar con un dispositivo que hace de Router y los dispositivos utilizados para Suricata, Snort y Zeek.

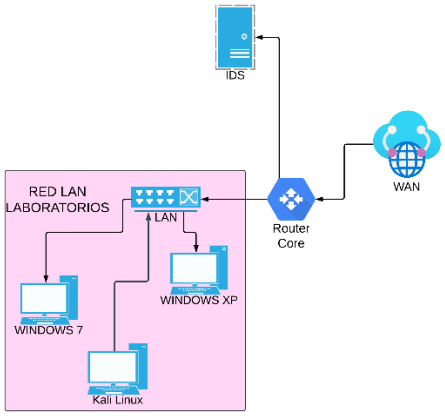


Figura II Esquema del escenario de simulación

En la siguiente table se lista los dispositivos y las características de cada uno:

Tabla 5 Características de los equipos utilizados

Descripción	Conexión de red	Características
Router	WAN Red LAN	S.O.: Other Linux Memoria RAM: 32 MB Tarjeta de red disponible: 2
IDS Suricata, Snort, Zeek	Red LAN	S.O.: Ubuntu 20.04 Memoria RAM: 8GB Almacenamiento: 50GB Procesador: Ryzen 5600X 2 núcleos Tarjeta de red disponible: 1
Switch		Dentro de Virtual Box, se generó 1 red interna nombrad: LAN

Red LAN:

Dentro de esta red están usuarios legales que ejecutan distintos sistemas operativos.

Además, existe un dispositivo (Kali Linux) introducido que simulará los ataques desde el interior.

Dispositivos IDS:

Se crearon 3 dispositivos con las exactamente las mismas especificaciones para realizar las funciones de los IDS, donde el primer dispositivo tiene instalado la herramienta Suricata, el segundo la herramienta Snort y el último dispone de la herramienta Zeek (BroIDS).

Estos dispositivos estarán ubicados detrás del dispositivo Router, que interconecta la red LAN.

Direccionamiento de red general:

LAN 10.0.2.0/24 Puerta de Enlace (10.0.2.1)

WAN 192.168.3.0/24 Puerta de Enlace (192.168.3.1)

RED	Descripción	Sistema Operativo	Dirección IP
LAN	Ordenador Usuario 1	Windows 7	10.0.2.4
	Ordenador Usuario 2	Windows XP	10.0.2.3
	Ordenador Atacante	Kali Linux	10.0.2.5
WAN	Salida a internet		192.168.3.6
Router		Other Linux	10.0.2.1 (LAN) 192.168.3.1 (Salida a internet)

Descripción de los servicios simulados:

Router

El dispositivo que funciona como Router dispone de 2 tarjetas de red; donde eth0 es de tipo bridge (que se conecta a la tarjeta de red del equipo anfitrión), eth1 se conecta a la red LAN. Se ha configurado el equipo para que todo el tráfico de datos sea visible por todos los dispositivos.

IDS Suricata, Snort y Zeek

Las terminales utilizadas para funcionar como IDS se hallan de manera individual instalados con las siguientes características que permiten la visualización y la gestión de las alertas generadas.

Tabla 6 Características de Hardware de los IDS Simulados

Procesador	AMD Ryzen 5600X 3.7GHz
Memoria RAM	8 GB
Tarjeta de Red	Intel PRO/1000 MT Desktop
Almacenamiento	50 GB
SO	Ubuntu Server 20.04

2.5 Procesamiento de datos y Análisis de los mismos

2.5.1 Procesamiento y análisis de los indicadores de la variable independiente

Para el análisis de la variable independiente que son las herramientas IDS de software libre. En esta sección procederemos a analizar las herramientas en función de cada indicador los cuales contienen algunos parámetros a evaluar.

Cabe destacar que para este estudio se utilizó la versión 7.0.3 de Suricata, la 2.9.7.0 de Snort y por último la versión 6.0.3 de Zeek (BroIDS). Para el objetivo de analizar se realizó una tabla de estimación para evaluar los valores porcentuales.

2.5.1.1 Indicador 1: Características

Para la evaluación de este indicador se considera la escala de Likert[33] , en la que se crea valores graduales en una escala de 1 a 5 puntos. Cada valor de la tabla se representa por su valoración cualitativa y porcentual.

Tabla 7 Tabla de ponderación

Calificación cualitativa	Valor asignado	Porcentaje
Excelente	5	100%
Muy bueno	4	61% - 80%
Bueno	3	41% - 60%
Deficiente	2	21% - 40%
No Disponible	1	0% - 20%

Se presenta a continuación una explicación detallada de la tabla elaborada previamente.

No Disponible: esta calificación cualitativa está representada por la calificación cuantitativa de 1 y el valor porcentual de 0%, dicha calificación será otorgada a las herramientas que no dispongan o cumplan de manera muy deficiente con el criterio objetivo.

Deficiente: esta calificación cualitativa cuyo valor cuantitativo es 2 y valor porcentual es 40%, se asignará a las herramientas que cumplan el criterio seleccionado de manera deficiente.

Bueno: esta calificación cualitativa cuyo valor cuantitativo es 3 y valor porcentual es 60%, se asignará a las herramientas que cumplan el criterio parcialmente.

Muy bueno: esta calificación cualitativa cuyo valor cuantitativo es 4 y valor porcentual es 80%, se asignará a las herramientas que cumplan el criterio seleccionado casi en su totalidad.

Excelente: esta calificación cualitativa cuyo valor cuantitativo es 5 y valor porcentual es 100%, se asignará a las herramientas que cumplan el criterio seleccionado en su totalidad.

Comparación de las características presentadas por las herramientas IDS:

Detección de intrusiones en tiempo real: capacidad para detectar intrusiones en tiempo real y generar alertas para notificar a los administradores de seguridad sobre actividades ilícitas. Esta capacidad permite acelerar las respuestas ante amenazas potenciales.[17], [18], [19], [26], [34], [35], [36]

Soporte para múltiples protocolos: capacidad de soporte con una amplia gama de protocolos de red, incluyendo TCP, UDP, ICMP, HTTP, FTP y DNS. Esto responde a una amplia cobertura de las comunicaciones de red y la detección de diferentes ataques independiente del protocolo utilizado. [17], [18], [19], [26], [34], [35], [36]

Análisis de flujo de red: capacidad de identificar patrones de tráfico sospechosos y comportamientos anómalos. Dicha capacidad permite la detección de ataques que no se basan en firmas conocidas, como ataques de día cero o ataques de baja firma. [17], [18], [19], [26], [34], [35], [36]

Generación de registros detallados: este criterio es tomado en cuenta ya que la generación de registros detallados puede ser utilizados para la investigación de incidentes. Estos registros proporcionan información valiosa para entender la naturaleza de un ataque, identificar su origen y determinar el impacto en la red. [17], [18], [19], [26], [34], [35], [36]

Escalabilidad: característica de los IDS que se utiliza para proteger redes de diferentes tamaños. Esto sirve para que las herramientas puedan adaptarse a las distintas necesidades sean estas pequeñas empresas, grandes empresas u organizaciones o entornos en la nube. [17], [18], [19], [26], [34], [35], [36]

Facilidad de uso: Característica que indica que tanto facilitan las herramientas su implementación, configuración y operación. [17], [18], [19], [26], [34], [35], [36]

Detección de intrusiones en tiempo real:

Suricata y Snort: Ambos IDS ofrecen detección de intrusiones en tiempo real con un alto rendimiento y precisión.

Zeek: La detección de intrusiones en tiempo real de Zeek es menos eficiente que la de Suricata y Snort, pero aún puede ser efectiva para identificar amenazas.

Soporte para múltiples protocolos:

Suricata, Snort y Zeek: Los tres IDS soportan una amplia gama de protocolos de red, incluyendo TCP, UDP, ICMP, HTTP, FTP y DNS.

Análisis de flujo de red:

Zeek: se destaca en el análisis de flujo de red, proporcionando información detallada sobre el comportamiento del tráfico y la detección de anomalías.

Suricata: también ofrece análisis de flujo de red, pero con menos funcionalidades que Zeek.

Snort: El análisis de flujo de red de Snort es menos robusto que el de Suricata y Zeek.

Generación de registros detallados:

Zeek: genera registros detallados y enriquecidos con información contextual, ideal para análisis forense e investigación de incidentes.

Suricata y Snort: Ambos IDS generan registros detallados, pero con menos información contextual que Zeek.

Escalabilidad:

Suricata, Snort y Zeek: Los tres IDS son escalables y pueden adaptarse a redes de diferentes tamaños.

Facilidad de uso:

Snort: tiene una interfaz de usuario intuitiva y una amplia documentación, lo que lo hace fácil de usar para principiantes.

Suricata: tiene una interfaz de usuario amigable y herramientas de administración que facilitan su uso.

Zeek: tiene una curva de aprendizaje más pronunciada debido a su enfoque en el análisis de flujo de red y la generación de registros detallados.

2.5.1.2 Resultados de las evaluaciones del indicador Características

Dentro de este apartado se realiza la presentación de los resultados de la comparativa que se muestran en una tabla de manera resumida los criterios que se evaluaron con su respectiva calificación.

Tabla 8 Resultados del Indicador Características

Característica	Suricata		Snort		Zeek	
	Evaluación		Evaluación		Evaluación	
Detección de intrusiones en tiempo real	Excelente	5	Excelente	5	Muy bueno	4
Soporte para múltiples protocolos	Excelente	5	Excelente	5	Excelente	5

Análisis de flujo de red	Muy bueno	4	Bueno	3	Excelente	5
Generación de registros detallados	Muy bueno	4	Muy bueno	4	Excelente	5
Escalabilidad	Excelente	5	Excelente	5	Muy bueno	4
Facilidad de uso	Muy bueno	4	Excelente	5	Bueno	3
Promedio		4.5		4.5		4.33

2.5.1.3 Indicador 2: Funcionalidades

Este indicador se menciona las funcionalidades disponibles en los IDS que se están comparando, las funcionalidades en mención son las siguientes:

- Automatización de detección de Protocolos de Red
- Gestión de distintos Módulos de Registros
- Soporte IPV6
- Aplicaciones Extendidas
- Aceleración con GPU
- Reputación IP
- Geolocalización IP

Automatización de detección de Protocolos de Red

Suricata: dispone de los siguientes protocolos que utilizan palabras claves: TCP, UDP, ICMP, IP, HTTP, FTP, TLS, SMB, DNS, DHCP, SSH, SMTP, IMAP, RDP, IMAP, NFS, RFB, NFS.[34] Lo cual da un total de 18 protocolos.

Snort: dispone de los siguientes protocolos que utilizan palabras claves: IP, ICMP, TCP, UDP, SSL, TLS, HTTP, SMTP, FTP, SSH[35]. Lo cual da un total de 10 protocolos.

Zeek: dispone de los siguientes protocolos que utilizan palabras claves: IP, IP6, TCP, UDP, ICMP, ICMP6[36]. Esto da un total de 6 protocolos.

Para valorar esta función de manera cuantitativa, se toma el valor más significativo como 100% en este caso seria 18. Dado este valor significativo realizamos una regla de tres para evaluar el resto de IDS.

$$\frac{18}{10} = \frac{100\%}{x} => \frac{10 * 100}{18} = 55.56\%$$

$$\frac{18}{6} = \frac{100\%}{x} => \frac{6 * 100}{18} = 33.33\%$$

La valoración cuantitativa de Suricata para este parámetro es de 5 correspondiente a la valoración cualitativa de Excelente, para Snort la calificación cuantitativa es de 3 con una valoración cualitativa de Bueno, y por último Zeek (BroIDS) tiene una calificación de Deficiente o valor numérico de 2.

Gestión de distintos Módulos de Registros:

Suricata: Utiliza los siguientes archivos de registros: Registro de alerta por líneas **FAST** (fast.log), Formato de Eventos extensibles **EVE** (eve.json), salida de registros usando Barnyarnd **UNIFIED-LOG** (unified.log), salida de Alertas utilizando Barnyarnd **UNIFIED-ALERT** (unified.alert), registro de las alertas utilizando Barnyarnd **UNIFIED2-ALERT** (unified2.alert), registro de las peticiones HTTP **HTTP-LOG** (http.log), registro de las consultas DNS y las respuestas obtenidas **DNS-LOG** (dns.log), Registro de los paquetes **PCAP-LOG** (log.pcap), Registro de las estadísticas y rendimiento de Suricata **STATS** (stats.log), Registro detallado de las alertas que sirve para la investigación de falsos positivos **ALERT-DEBUG** (alert-debug.log). Dando un total de 10 Módulos de Salida.[34]

Snort: Snort utiliza los siguientes módulos de registro: **ALERT_SYSLOG, ALERT_FAST, ALERT_FULL, ALERT_UNIXSOCK, LOG_TCPDUMP, CSV, UNIFIED 2.**[35] La suma de estos módulos da un total de 7.

Zeek: Dispone de los siguientes módulos de registro: **CONN.LOG, DNS.LOG, HTTP.LOG, FILES.LOG, FTP.LOG, SSL.LOG, TRACEROUTE.LOG, TUNNEL.LOG, DHCP.LOG, NTP.LOG, CAPTURE_LOSS.LOG, REPORTER.LOG.**[36] Dando un total de 12 módulos.

Realizando una regla de 3 tomando como valor más significativo 12 como el 100% tenemos los siguientes valores.

$$\frac{12}{7} = \frac{100\%}{x} => \frac{7 * 100}{12} = 58.33\%$$

$$\frac{12}{10} = \frac{100\%}{x} => \frac{10 * 100}{12} = 83.33\%$$

Tenemos las siguientes calificaciones Zeek obtuvo una calificación de 5 equivalente a Excelente, le sigue Suricata con una calificación de 5 equivalente a Excelente y por último Snort con una calificación cualitativa de Bueno equivalente a 3.

Soporte IPV6: Las 3 herramientas comparadas disponen de manera nativa el soporte de IPV6. Por esta razón cumplen de manera Excelente con este indicador.

Aplicaciones Extendidas:

Los IDS con funciones bastante completas, pero para tener un control exhaustivo de las alertas se acoplan a distintas herramientas entre las que se puede nombrar: Security onion (NMS)[37][38], AlientVault OSSIM (SIEM)[39], Prelude (SIM)[40], Aanval (SIEM)[41], Cisco ISE (SIEM)[42], USM Anywhere (SIEM)[43], Splunk(SIEM)[44] y openIDS (NMS). Las herramientas Cisco ISE y Splunk son herramientas comerciales, las demás herramientas mencionadas son open source.

Para tener una idea más clara podemos mencionar que SIEM (información de seguridad y gestión de eventos), sirve para la detección rápida, su pronta respuesta y neutralización de amenazas. SIM (gestión de información de seguridad) se utiliza para recopilar los datos a largo plazo para luego proceder al análisis de la información. [45]

Suricata y Snort es posible la integración con todas las herramientas mencionadas anterior mente por lo que obtienen una calificación de 5 equivalente a Excelente. En cambio, Zeek no es posible la integración directa de 2 herramientas siendo esta Cisco ISE y USM Anywhere por lo cual obtiene una calificación de 4 equivalente a Muy Bueno[34], [35], [36].

Aceleración con GPU:

Suricata: ofrece soporte para aceleración por GPU a través del proyecto Suricata-IDS-GPU. Este proyecto utiliza la biblioteca CUDA de NVIDIA para optimizar el rendimiento del análisis de tráfico en GPUs [46].

Snort: no ofrece soporte nativo para aceleración por GPU[35].

Zeek: no ofrece soporte nativo para aceleración por GPU[36].

Obteniendo una calificación de 5 para Suricata y de 1 para Snort y Zeek.

Reputación IP:

Suricata: ofrece soporte nativo para la integración con listas negras de IP y servicios de reputación IP.[34]

Snort: ofrece soporte nativo para la integración con listas negras de IP y servicios de reputación IP.[35]

Zeek: no ofrece soporte nativo para la integración con listas negras de IP o servicios de reputación IP. Sin embargo, mediante scripts de terceros permite implementar dicha función.[36]

En este apartado Suricata y Snort reciben una calificación de 5 equivalente a Excelente y Zeek una calificación de 3 equivalente a Bueno.

Geolocalización IP:

Las tres herramientas comparadas si disponen de la función de Geolocalización IP, Suricata mediante la keyword "geoip" para habilitar el uso de GeoIP2 de MaxMind [47], mientras que Snort utiliza el Preprocesador GeoIP [48] y por último Zeek utiliza la librería GeoIp library para este fin [49].

Dado esta información los tres IDS reciben una calificación de 5 equivalente a Excelente.

2.5.1.4 Resultados de las evaluaciones del indicador Funciones

Tabla 9 Resultado del indicador Funciones

Funciones	Suricata	Snort	Zeek
	Evaluación	Evaluación	Evaluación

Automatización de detección de Protocolos de Red	Excelente	5	Bueno	3	Deficiente	2
Gestión de distintos Módulos de Registros	Excelente	5	Bueno	3	Excelente	5
Soporte IPV6	Excelente	5	Excelente	5	Excelente	5
Aplicaciones Extendidas	Excelente	5	Excelente	5	Muy bueno	4
Aceleración con GPU	Excelente	5	No Disp.	1	No Disp.	1
Reputación IP	Excelente	5	Excelente	5	Bueno	3
Geolocalización IP	Excelente	5	Excelente	5	Excelente	5
Promedio		5		3.86		3.57

2.5.2 Procesamiento y análisis de los indicadores de las variables dependientes

Las variables dependientes en esta investigación vienen siendo el Rendimiento de los IDS y las vulnerabilidades encontradas dentro los laboratorios de la Facultad de Ingeniería.

2.5.2.1 Variable Rendimiento

Dentro de esta variable tenemos varias categorías las cuales son: Tasa de Detección, Tasa de Falsos Positivos, Tiempo de Respuesta.

Escenario Simulado

Los IDS Suricata, Snort y Zeek fueron evaluados durante 42 días, con las siguientes pruebas: Comprobación Conexión al Host, Verificación de los puertos Abiertos, Ataque de Fuerza Bruta por SSH y Ataque de Denegación de Servicios, todos los ataques fueron realizados a una maquina objetivo dentro de la misma red.

El tiempo de los ataques se detalla a continuación: 1 hora con un intervalo entre ataque de 10 segundos, 1 hora y 30 minutos con un intervalo de ataque de 20 segundos, 4 horas con un intervalo de ataque de 3 minutos, 3 horas con un intervalo de ataque de 20 segundos, respectivamente.

Los archivos de salida para cada IDS son los siguientes: fast.log para Suricata, output.csv para Snort y conn.log para Zeek, dentro de estos archivos se registraron la hora (timestamp), además de las IP’s y todas las detecciones de los IDS.

Dentro de la configuración de los IDS se utilizaron reglas personalizadas para una evaluación más eficiente de los parámetros ya seleccionados

Interpretación de reglas activadas

Dentro de los IDS Suricata, Snort y Zeek se activaron 4 alertas una para cada evento o ataque realizado. En este apartado se detallan las reglas que se utilizaron para evaluar los IDS.

Reglas activadas para Suricata

Detección de Ping

- alert icmp any -> $HOME_NET any (msg:"ICMP Ping detectado"; sid:1000001)

Detección del escaneo de puertos

- alert tcp any -> $HOME_NET any (msg:"Escaneo de puertos TCP detectado"; sid:1000002; rev:1;)
- alert udp any -> $HOME_NET any (msg:"Escaneo de puertos UDP detectado"; sid:1000003; rev:1;)

Detección de Ataques de Fuerza Bruta SSH

- alert tcp any -> $HOME_NET 22 (msg:"Ataque de fuerza bruta SSH detectado"; threshold: type threshold, track by_src, seconds 10, count 5; classtype:attempted-admin; sid:1000004;)

Detección de Ataques DDoS

- alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Ataque DDoS Interno Detectado"; flow:to_server; flags: S,12; threshold: type both, track by_dst, count 5000, seconds 5; classtype:misc-activity; sid:1000005;)

- alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Ataque DDoS Externo Detectado"; flow:to_server; flags: S,12; threshold: type both, track by_dst, count 5000, seconds 5; classtype:misc-activity; sid:1000006;)

En este ejemplo definimos las partes de la regla que son la acción en color rojo, la cabecera en color verde y las opciones de regla en color azul.

alert tcp any → $HOME_NET 22 (msg:"Ataque de fuerza bruta SSH detectado"; threshold: type threshold, track by_src, seconds 10, count 5; classtype:attempted-admin; sid:1000004;)

Acción: Indica la acción que ejecutara la regla ya sea (alert, drop, pass, reject) que para este caso es una regla de alerta (alert).[50]

Cabecera: dentro de este apartado se encuentra el protocolo “tcp”, además de él origen “$EXTERNAL_NET” y destino “$HOME_NET” que deben ser configurados en la configuración inicial de las herramientas o configurar las direcciones IP manualmente dentro de la regla. También se hace mención de los puertos que se deben analizar en el origen “any” y el destino “22”, además de la dirección “→” en la que trabajaría la regla.[50]

Opciones de Regla: en este apartado se encuentran varias opciones separadas por “ ; ”, una de las primeras opciones es “msg” que muestra un mensaje en la alerta que se detecta, “threshold: type threshold, track by_src, seconds 10, count 5” define el umbral de detección. En este caso, se activa la alerta si se detectan 5 intentos de conexión fallidos al puerto 22 en un intervalo de 10 segundos desde la misma dirección IP de origen, “classtype:attempted-admin” clasifica la alerta como un intento de ataque administrativo.[50]

Alertas detectadas por Suricata

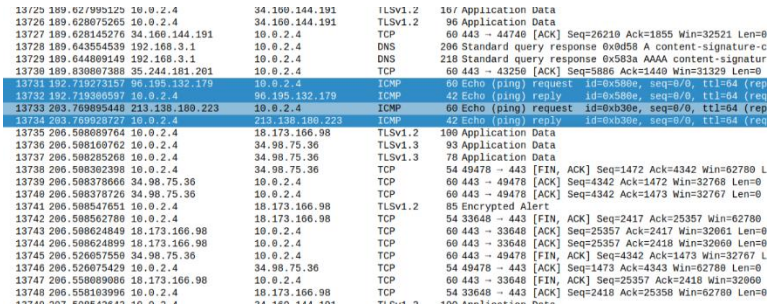


Figura III Análisis del Tráfico de datos a través de WireShark

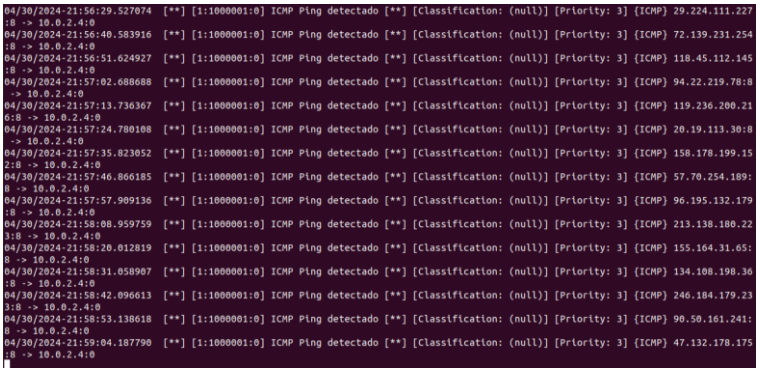


Figura IV Registro de alertas ICMP por parte de Suricata

Reglas activadas para Snort

Detección de Ping

- alert icmp any any -> $HOME_NET any (msg:"ICMP Ping detectado"; sid:1000001;)

Detección del escaneo de puertos

- alert tcp any any -> any any (flags:S; msg:"Escaneo de puertos TCP detectado"; sid:1000002;)
- alert udp any any -> any any (msg:"Escaneo de puertos UDP detectado"; sid:1000003;)

Detección de Ataques de Fuerza Bruta SSH

- alert tcp any any -> any 22 (msg:"Ataque de fuerza bruta SSH detectado"; sid:1000004; threshold: track by_src, seconds 10, count 5; classtype:attempted-admin;)

Detección de Ataques DDoS

- alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (threshold: type threshold, track by_dst, count 5000, seconds 5; msg: “Ataque DDoS Externo Detectado”; sid: 10000009; rev: 1;)
- alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (threshold: type threshold, track by_dst, count 5000, seconds 5; msg: “Ataque DDoS Interno Detectado”; sid: 10000009; rev: 1;)

Las reglas que ejecuta Suricata son compatibles con las de Snort, salvo algunos cambios menores por ende la estructura de la regla es la misma que se detalló en el apartado de las “reglas de Suricata”.[51]

Alertas detectadas por Snort

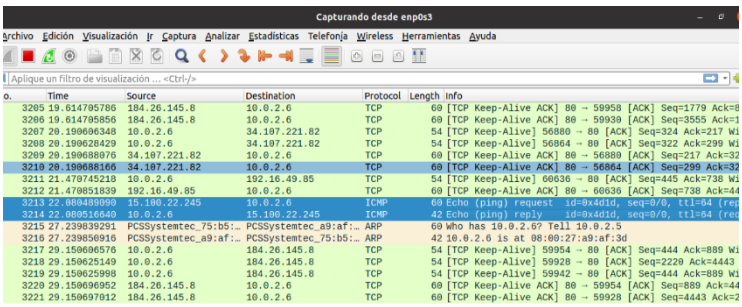


Figura V Análisis del Tráfico de datos a través de WireShark

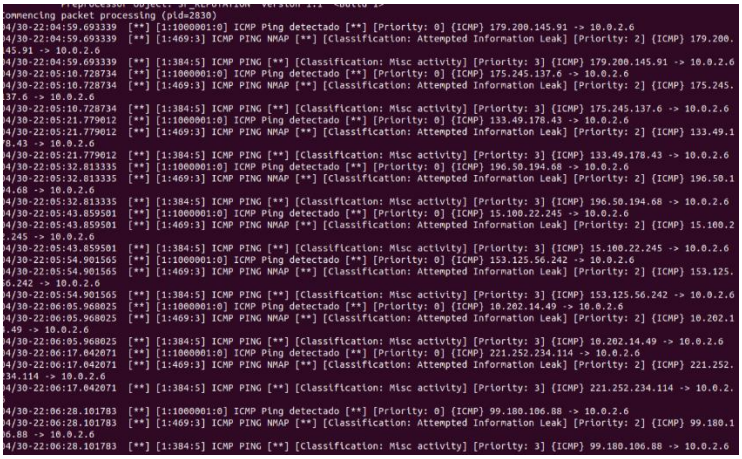


Figura VI Registro de alertas ICMP por parte de Snort

<u>Reglas activadas para Zeek</u>

- ***Detección de Ping***

```
event icmp_packet(c: connection, p: icmp_packet)
        {
        if ( p$type == ICMP_Echo_Request )
                {
                print fmt("ICMP Ping detectado desde %s hacia %s", c$id$orig_h, c$id$resp_h);
                }
        }
```

- ***Detección del escaneo de puertos***

```
event tcp_packet(c: connection, p: tcp_packet)
    {
    if ( c$id$resp_p == 22 )
            {
            print fmt("Escaneo de puertos TCP detectado desde %s hacia %s en el puerto %d", c$id$orig_h, c$id$resp_h, c$id$resp_p);
            }
    }
event udp_packet(c: connection, p: udp_packet)
    {
    print fmt("Escaneo de puertos UDP detectado desde %s hacia %s en el puerto %d", c$id$orig_h, c$id$resp_h, c$id$resp_p);
    }
```

- ***Detección de Ataques de Fuerza Bruta SSH***

```
global ssh_attempts: table[addr] of count &default=0;
event ssh_login_attempt(c: connection, username: string, success: bool)
    {
    if ( c$id$resp_p == 22 && !success )
            {
            ssh_attempts[c$id$orig_h]++;
            if ( ssh_attempts[c$id$orig_h] > 5 )
                    {
```

```
                print fmt("Ataque de fuerza bruta SSH detectado desde %s hacia %s", c$id$orig_h, c$id$resp_h);
                }
        }
    }
```

- ***Detección de Ataques DDoS***

```
global internal_ddos_counter: counter &default=0;
event ddos_internal_attack(c: connection, p: tcp_packet)
    {
    internal_ddos_counter += 1;
    if ( internal_ddos_counter > 5000 )
        {
        print fmt("Ataque DDoS Interno Detectado hacia %s", c$id$resp_h);
        }
    }
global external_ddos_counter: counter &default=0;
event ddos_external_attack(c: connection, p: tcp_packet)
    {
    external_ddos_counter += 1;
    if ( external_ddos_counter > 5000 )
        {
        print fmt("Ataque DDoS Externo Detectado desde %s hacia %s", c$id$orig_h, c$id$resp_h);
        }
    }
```

Alertas detectadas por Zeek

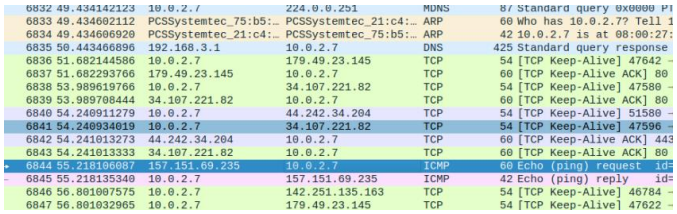


Figura VII Análisis del Tráfico de datos a través de WireShark

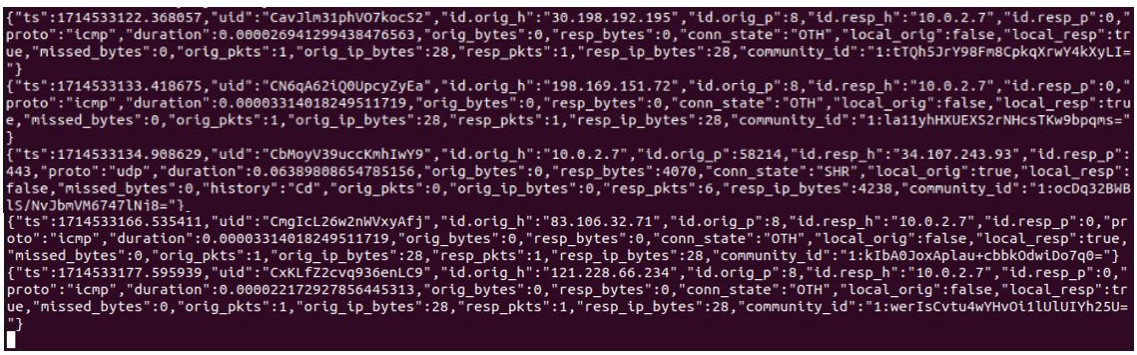


Figura VIII Registro de alertas ICMP por parte de Zeek

Tasa de Detección.

Dentro de este indicador se calcula el porcentaje de detección de ataques detectados. La simulación del escenario es el detallado en la Figura II, para esta investigación se utilizó la interfaz por defecto de todas las herramientas utilizadas.

Los registros obtenidos de la muestra seleccionada para la cantidad de detecciones registradas se encuentran en la sección de anexos.

Tasa de Falsos Positivos

Utilizando la misma simulación anterior se obtuvo además de las detecciones de los ataques realizados, existen una serie de alertas que pueden ser catalogadas como falsos positivos, dichas alertas se determinaron mediante un examen minucioso de los registros comparándolos con los registros de los ataques que se realizaron, y determinando que existían alertas que no coincidían con los ataques tomándolas como falsos positivos.

La tabla donde se puede observar las cantidades se encuentra en la sección de anexos.

Tiempo de Respuesta

Con el mismo escenario se obtuvieron los tiempos de Respuestas en base a los ataques realizados los cuales se ven tabulados en las tablas que se ubican en la sección de anexos.

CAPÍTULO IV

3.1 Resultados

3.1.1 Comparativas de los Sistemas de Detección de Intrusiones de Software Libre

3.1.1.1 Análisis de los resultados obtenidos

Este proceso se realizará tanto para las variables dependientes como la independiente, con la variable independiente que concierne a las características y funcionalidades que disponen las tres herramientas IDS, tenemos los siguientes resultados.

INDICADOR 1: Características

Los siguientes resultados fueron obtenidos de la evaluación teórica y se presentan en el siguiente gráfico.

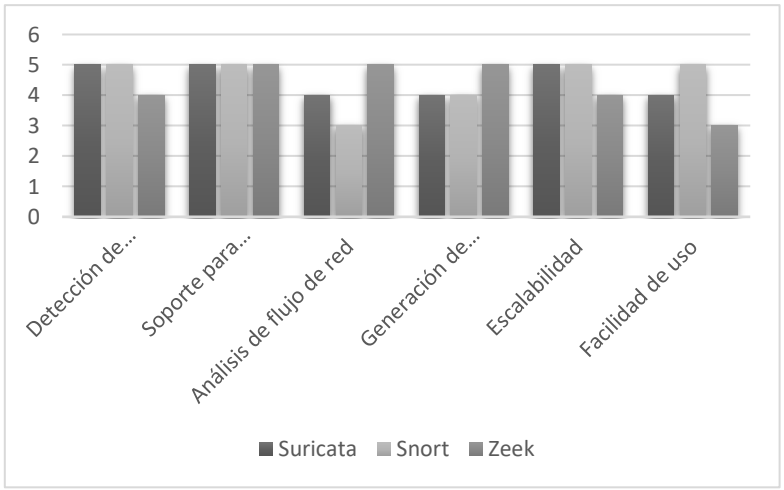


Figura IX Resumen evaluación del Indicador Características

El promedio de la evaluación es: 4.5 puntos para Suricata, 4.5 para Snort y 4.33 para Zeek.

Cabe destacar que es una comparativa teórica, teniendo como base la documentación oficial de las herramientas IDS de Software Libre.

La evaluación en términos porcentuales obtenidos en función de las seis características para los tres Sistemas de Detección de Intrusiones se detalla a continuación: Suricata tiene un porcentaje total de 90%, en cambio Snort dispone de un porcentaje de 90% y por último Zeek tiene un porcentaje de 86.60%.

INDICADOR 2: Funcionalidades

Los siguientes resultados fueron obtenidos de la evaluación teórica y se presentan en el siguiente gráfico.

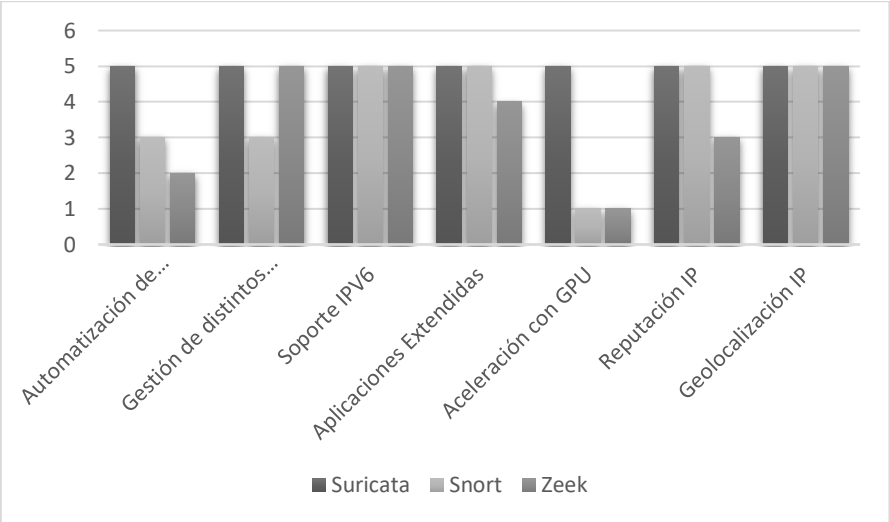


Figura X Resumen evaluación del Indicador Funcionalidades

El promedio de la valoración es: 5 puntos para Suricata, 3.86 para Snort y 3.57 para Zeek.

Se presenta la evaluación comparativa de las funcionalidades de tres Sistemas de Detección de Intrusiones (IDS): Suricata, Snort y Zeek, en base a seis funciones. El análisis se realiza en términos porcentuales, considerando el desempeño de cada sistema en cada característica.

Los resultados obtenidos indican que Suricata se ubica como el sistema con mayor rendimiento general, al alcanzar un porcentaje total del 100%. En segundo lugar, se encuentra Snort, con un porcentaje del 77.20%, mientras que Zeek presenta un porcentaje total del 71.40%.

El análisis de los indicadores nos revela que Suricata se perfila como una solución prometedora en materia de detección de intrusiones. Su rendimiento promedio, expresado en términos porcentuales, alcanza el 95%, superando significativamente a Snort (83.6%) y Zeek (79%).

Variable Dependiente: Rendimiento

Tasa de Detección

Los promedios de detecciones para las tres herramientas fueron los siguientes:

Tabla 10 Resumen Tasa de Detección

Número total de Intrusiones detectadas			
	Snort	Suricata	Zeek
ICMP	1355	1371	1344
NMAP	1322	1339	1339
SSH	1356	1364	1347
DDoS	1329	1351	1334
Total	5362	5425	5364
Ataques Totales	5364	5426	5367
Porcentaje	99.9627%	99.9816%	99.9441%

La evaluación de las tasas de detección de los Sistemas de Detección de Intrusiones (IDS) Snort, Suricata y Zeek arroja resultados con pequeñas diferencias. Suricata presenta una tasa de detección ligeramente superior al 99.9816%, mientras que Snort se mantiene cercana con un 99.9627%. En contraste, Zeek se ubica por debajo del 99.9441%.

Tasa de Falsos Positivos

La cantidad de alerta catalogadas como falsos positivos se detallan a continuación:

Tabla 11 Resumen Tasa de Falsos Positivos

Número total de Falsos Positivos			
	Snort	Suricata	Zeek
ICMP	31	15	42
NMAP	64	47	47
SSH	30	22	39
DDoS	57	35	52
Total	182	119	180
Porcentaje	3.3929%	2.1931%	3.3538%

La evaluación de las tasas de Falsos Positivos (FP) en los Sistemas de Detección de Intrusiones (IDS) Snort, Suricata y Zeek revela diferencias notables. Suricata presenta la tasa de FP más baja, con un 2.1931% del total de alertas detectadas. Zeek se ubica en segundo lugar, con un 3.3538%, mientras que Snort registra una tasa de FP de un 3.3929% del total de alertas registradas por cada IDS.

Tiempo de Respuesta

Las herramientas IDS se toman un tiempo para detectar alguna intrusión o alerta a esto le llamamos tiempo de respuesta, dentro del escenario propuesto se obtuvo los siguientes resultados:

Tabla 12 Resumen Tiempo de Respuesta

	SNORT (ms)	SURICATA (ms)	ZEEK (ms)
ICMP	499.051	396.732	1801.903
NMAP	351.585	275.753	1919.079
SSH	478.342	479.918	2344.163
DDoS	472.118	488.423	2184.396
TIEMPO DE RESPUESTA	450.274	410.207	2062.385

La evaluación del Tiempo de Respuesta (TR) en los Sistemas de Detección de Intrusiones (IDS) Snort, Suricata y Zeek evidenció diferencias significativas. Suricata presenta el TR más bajo, con un promedio de 410.207 ms. Snort se ubica en segundo lugar, con un promedio de 450.274 ms, mientras que Zeek registra el TR más alto, alcanzando una media de 2062.385 ms.

3.1.1.2 Análisis Estadístico de los resultados obtenidos

INDICADOR: TASA DE DETECCIÓN

Para poder avanzar con el análisis estadístico se debe tomar en cuenta si los datos que se van a trabajar son normalmente distribuidos o no, para esto se realizó el test de Normalidad de Shapiro-Wilk.

Tabla 13 Cuadro resumen de Pruebas de normalidad para las detecciones

Establecer hipótesis nula y alternativa. **H_0:** La cantidad de detecciones de Snort, Zeek y Suricata se distribuye normalmente **H_a:** La cantidad de detecciones de Snort, Zeek y Suricata no se distribuye normalmente			
Nivel de significancia	$\alpha = 0.05$		
PRUEBA	**IDS**	**Estadistico (W)**	**p-valor**
ICMP	SNORT	0.79622	0.0000036830
	SURICATA	0.6068	0.0000000022
	ZEEK	0.83909	0.0000337200
NMAP	SNORT	0.88931	0.0007000000
	SURICATA	0.81167	0.0000079280
	ZEEK	0.82394	0.0000149500
SSH	SNORT	0.79622	0.0000036830
	SURICATA	0.6068	0.0000000022
	ZEEK	0.83903	0.0000337200
DDOS	SNORT	0.88931	0.0007000000
	SURICATA	0.81167	0.0000079280
	ZEEK	0.82394	0.0000149500
Tomar la decisión Se puede observar que el ***p-valor*** para todas las pruebas es menor que el ***nivel de significancia α***. Se rechaza la hipótesis nula ***La cantidad de detecciones de Snort, Zeek y Suricata se distribuye normalmente*** con un nivel de confianza del 95%			

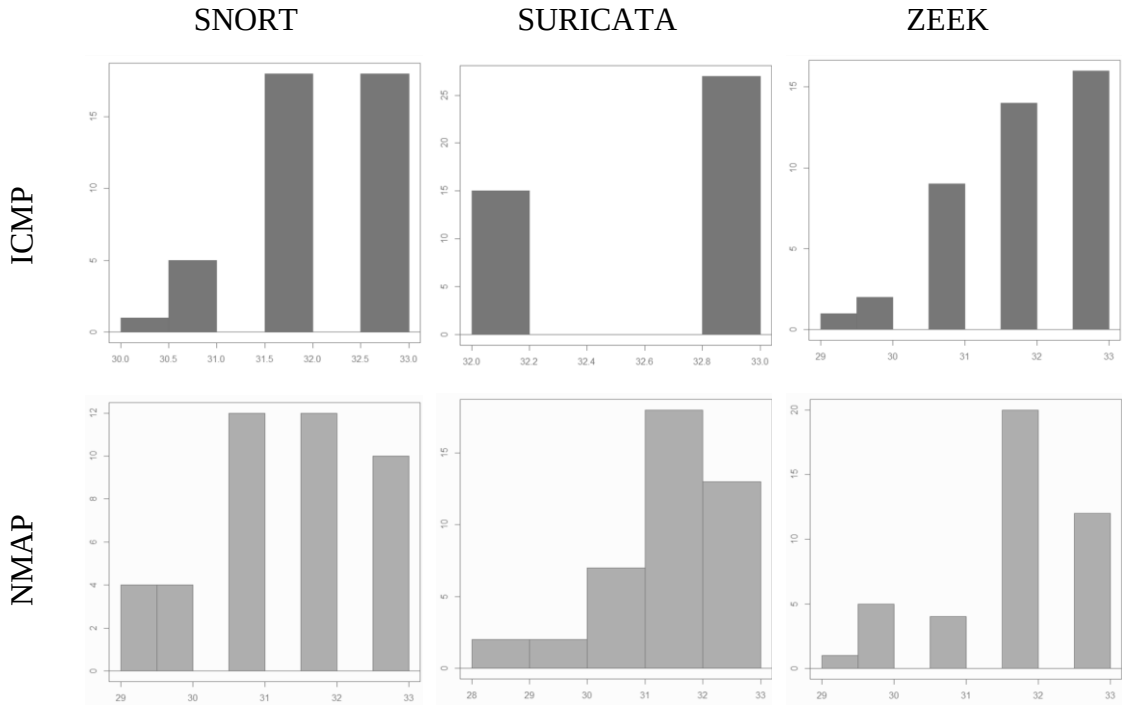


Figura XI Histogramas para las Pruebas de Normalidad para las detecciones – Parte 1

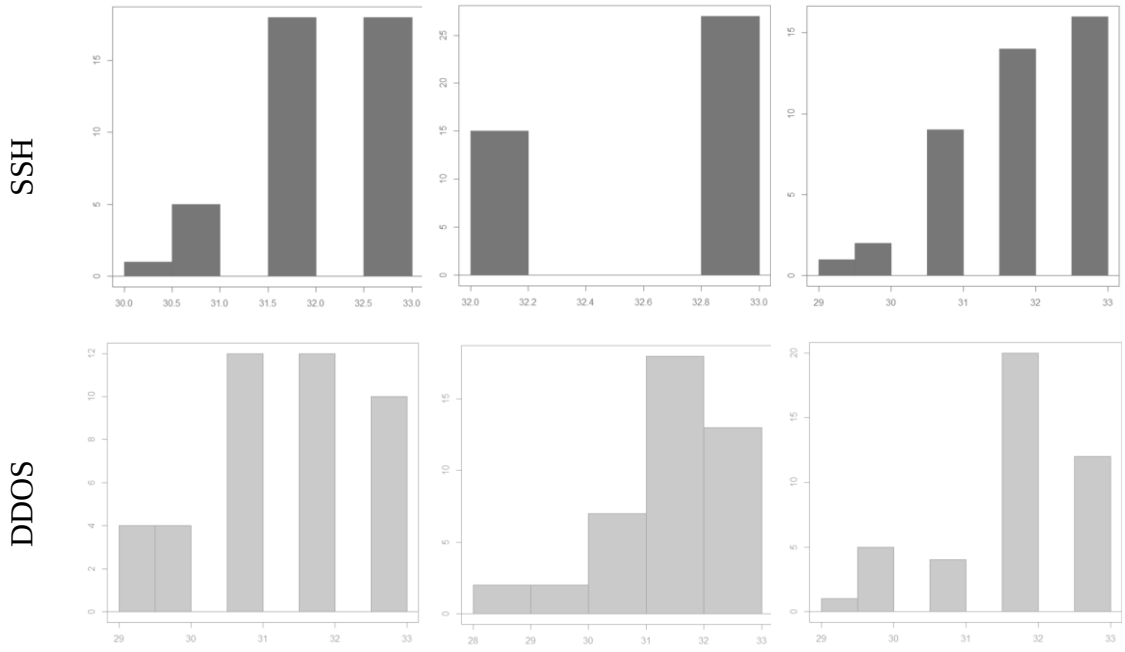


Figura XII Histogramas para las Pruebas de Normalidad para las detecciones – Parte 2

Considerando las pruebas de normalidad a la tasa de detecciones, se evidencian la no distribución normal de los datos, se opta por emplear pruebas no paramétricas. Se recurre al Test de Suma de Rangos de Friedman para el análisis en cuestión.

Hipótesis Nula: No existe diferencias significativas entre *SNORT, SURICATA y ZEEK.*

Hipótesis alternativa: Existe una diferencia significativa entre *SNORT, SURICATA y ZEEK.*

Tabla 14 Resultados de Prueba de Friedman

Ataques	*MEDIANAS*			*Test de Sumas de Friedman*	
	SNORT	SURICATA	ZEEK	Friedman Chi-Squared	p-valor
ICMP	32	33	32	6.25	0.044
NMAP	32	32	32	2.3	0.317
SSH	32	33	32	4.33	0.115
DDOS	33	32	32	2.25	0.325

Se puede observar que en los registros de los ataques para NMAP, SSH y DDOS ***no existe diferencias significativas entre SNORT, SURICATA y ZEEK,*** para los registros de ICMP se acepta la hipótesis alternativa ***Existiendo una diferencia significativa entre SNORT, SURICATA y ZEEK.***

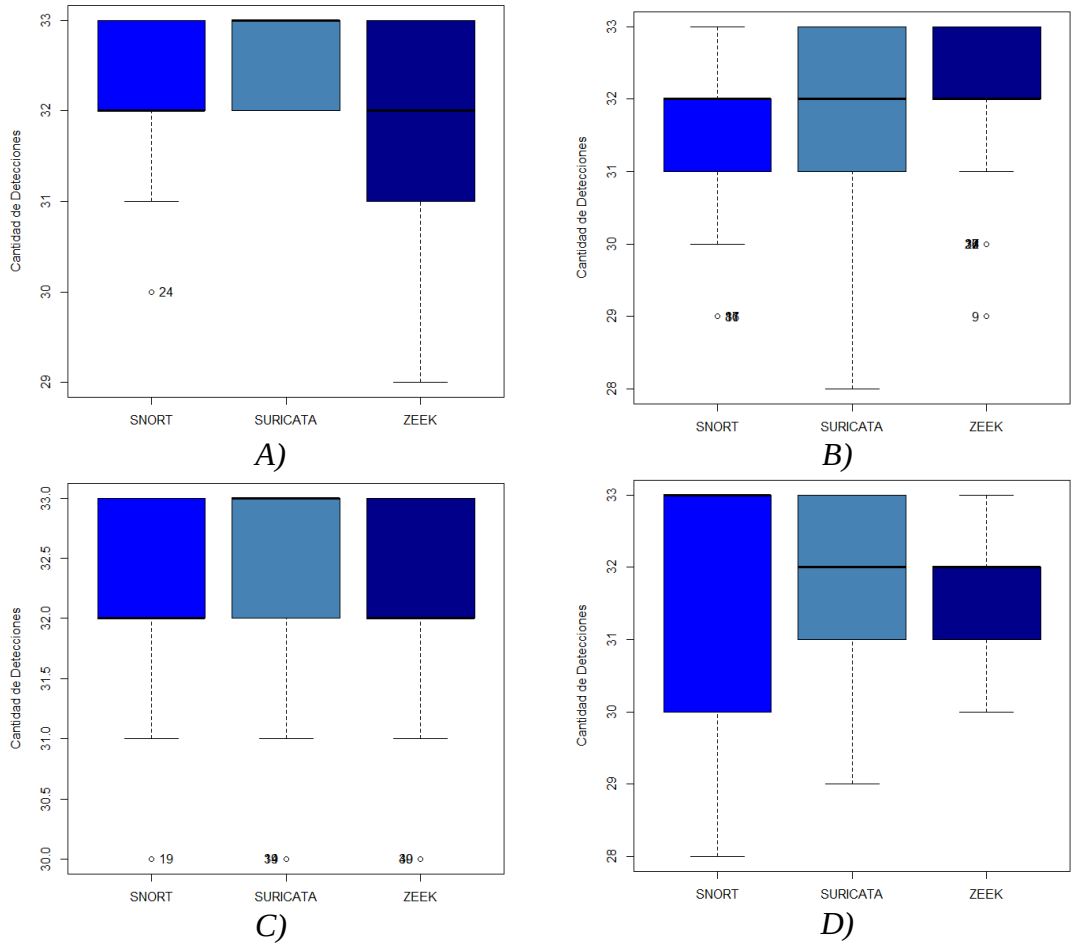


Figura XIII Gráficos de Caja para las Pruebas de Friedman de la Tasa de Detección

En el diagrama de caja A) de la Figura XIII podemos observar que Suricata y Snort no tienen una diferencia notable en la cantidad de detecciones, a su vez donde existen mayor diferencia en la cantidad de detecciones es para Zeek. El los diagramas de caja B), C), D) de la Figura XIII se observa que no hay una diferencia muy relevante.

Considerando que una mayor cantidad de detecciones de intrusiones indica un mejor rendimiento de la herramienta IDS, se observa que SURICATA detecta en promedio más intrusiones, seguido de SNORT y finalmente ZEEK.

INDICADOR: TASA DE FALSOS POSITIVOS

Tabla 15 Cuadro resumen de Pruebas de normalidad para los falsos positivos

Establecer hipótesis nula y alternativa. **H_0:** La cantidad de falsos positivos de Snort, Zeek y Suricata se distribuye normalmente **H_a:** La cantidad de falsos positivos de Snort, Zeek y Suricata no se distribuye normalmente

Nivel de significancia	$\alpha = 0.05$		
PRUEBA	**IDS**	**Estadistico (W)**	**p-valor**
ICMP	SNORT	0.78983	0.0000027070
	SURICATA	0.67349	0.0000000215
	ZEEK	0.834	0.0000256100
NMAP	SNORT	0.7578	0.0000006254
	SURICATA	0.78163	0.0000018390
	ZEEK	0.84868	0.0000579400
SSH	SNORT	0.79622	0.0000036830
	SURICATA	0.6068	0.0000000022
	ZEEK	0.83909	0.0000337200
DDOS	SNORT	0.7578	0.0000006254
	SURICATA	0.78163	0.0000018390
	ZEEK	0.84868	0.0000579400

Tomar la decisión

Se puede observar que el **p-valor** para todas las pruebas es menor que el **nivel de significancia α**.

Se rechaza la hipótesis nula **la cantidad de falsos positivos de Snort, Zeek y Suricata se distribuye normalmente** con un nivel de confianza del 95%

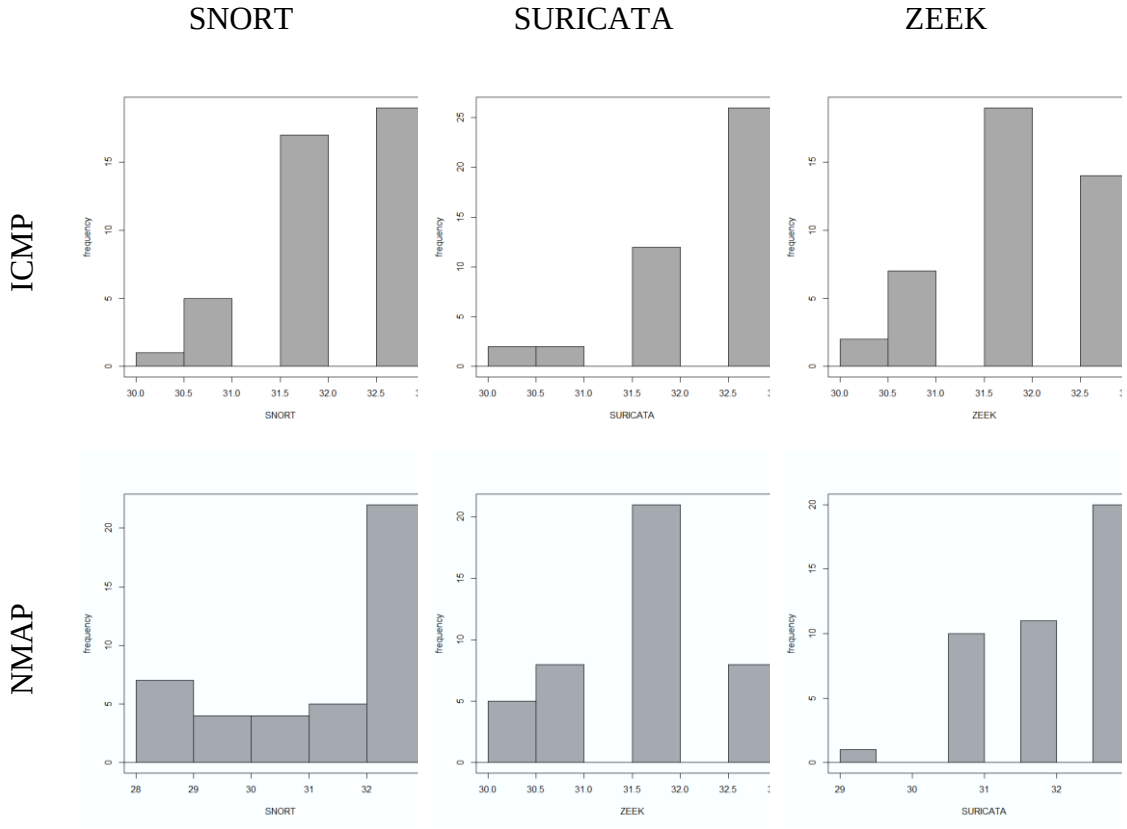


Figura XIV Histogramas para las Pruebas de Normalidad de falsos positivos – Parte 1

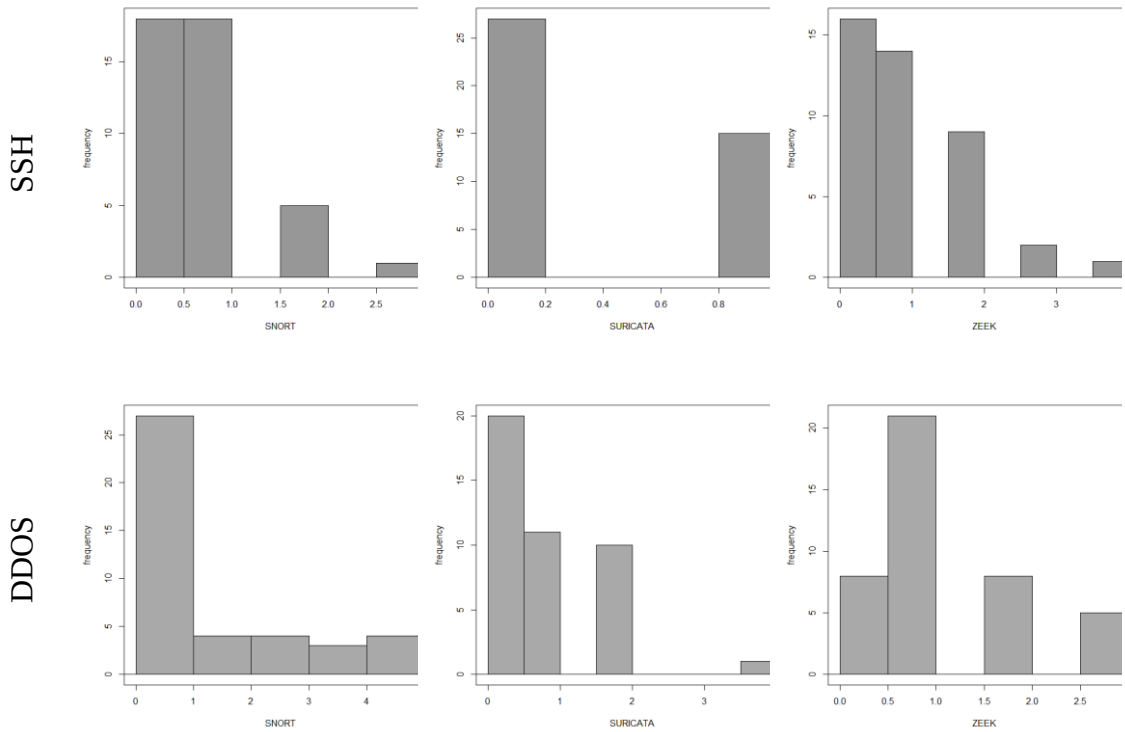


Figura XV Histogramas para las Pruebas de Normalidad de falsos positivos – Parte 2

Con base en las pruebas anteriores a la tasa de falsos positivos, podemos notar que no existen una distribución normal de los datos, se opta por emplear pruebas no paramétricas. Al igual que el indicador anterior, se selecciona el Test de Suma de Rangos de Friedman como la herramienta estadística adecuada.

Hipótesis Nula: No existe diferencias significativas entre *SNORT, SURICATA y ZEEK.*

Hipótesis alternativa: Existe una diferencia significativa entre *SNORT, SURICATA y ZEEK.*

Tabla 16 Resultados Prueba de Friedman para la Tasa de Detección

Ataques	*MEDIANAS*			*Test de Sumas de Friedman*	
	SNORT	SURICATA	ZEEK	Friedman Chi-Squared	p-valor
ICMP	1	0	1	8.8983	0.01169
NMAP	1	1	1	3.0394	0.2188
SSH	1	0	1	3.0394	0.2188
DDOS	0	1	1	2.7	0.2592

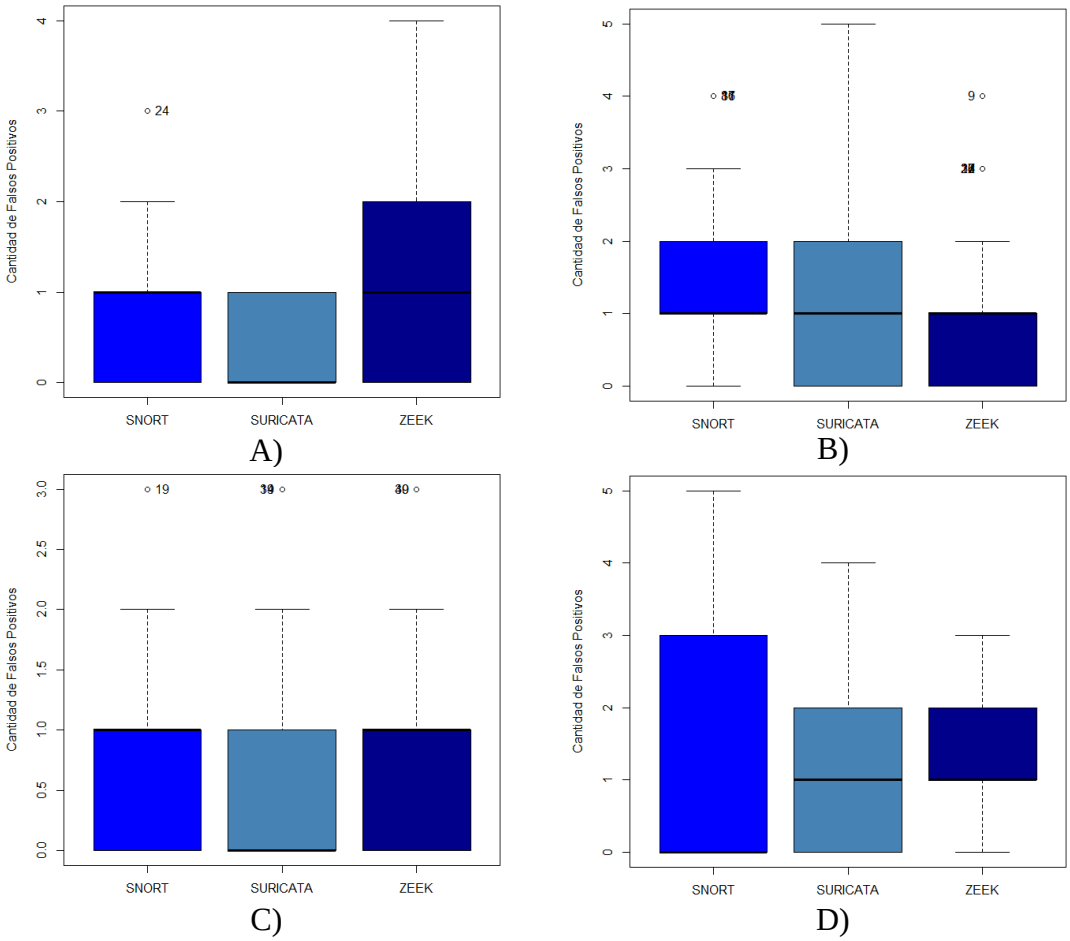


Figura XVI Gráficos de Caja para la Tasa de Falsos positivos utilizando el Test de Friedman

El diagrama de caja A) de la Figura XVI permite apreciar que la cantidad de falsos positivos que registraron Suricata y Snort no presentan diferencias notables. En cambio el promedio de falsos positivos en superior para la herramienta Zeek. Por otra parte, los diagramas de caja B), C) y D) de la Figura XIII evidencian que no existe una diferencia relevante en cuanto a la cantidad de detecciones entre las tres herramientas analizadas.

Considerando que una menor cantidad de falsos positivos indica un alto rendimiento de la herramienta IDS, SURICATA registra en promedio menos falsos positivos, seguido de SNORT y finalmente ZEEK.

INDICADOR: TIEMPO DE RESPUESTA

Tabla 17 Cuadro resumen Pruebas de normalidad de Tiempos de Respuesta

Establecer hipótesis nula y alternativa. **H_0:** Los tiempos de respuesta de Snort, Zeek y Suricata se distribuye normalmente **H_a:** Los tiempos de respuesta de Snort, Zeek y Suricata no se distribuye normalmente
Nivel de significancia $\alpha = 0.05$

PRUEBA	IDS	Estadistico (W)	p-valor
ICMP	SNORT	0.98168	0.7264
	SURICATA	0.96163	0.1689
	ZEEK	0.97423	0.4528
NMAP	SNORT	0.97955	0.6441
	SURICATA	0.97998	0.6609
	ZEEK	0.97602	0.5132
SSH	SNORT	0.98127	0.7104
	SURICATA	0.98866	0.9467
	ZEEK	0.97503	0.4794
DDOS	SNORT	0.98906	0.9544
	SURICATA	0.96587	0.2383
	ZEEK	0.97313	0.4181

Tomar la decisión

Se puede observar que el ***p-valor*** para todas las pruebas es mayor que el ***nivel de significancia α***.

Se acepta la hipótesis nula ***los tiempos de respuesta de Snort, Zeek y Suricata se distribuye normalmente*** con un nivel de confianza del 95%

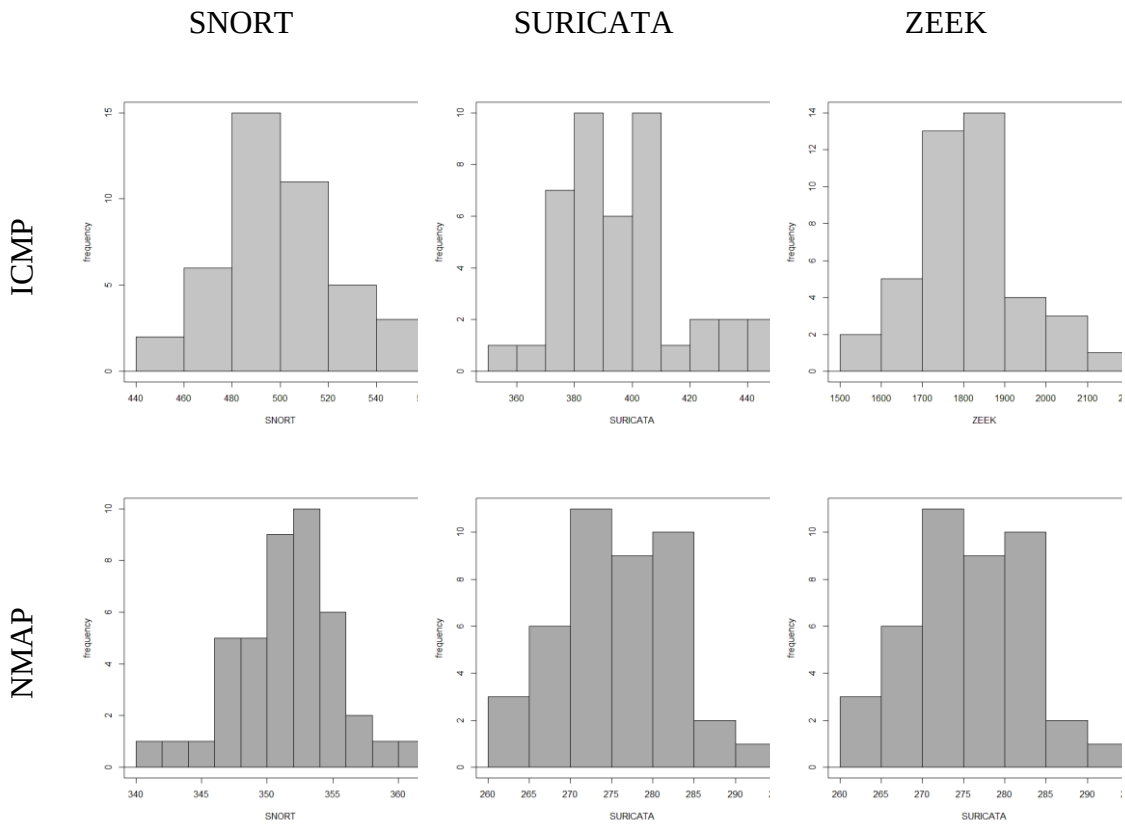


Figura XVII Histogramas para Pruebas de normalidad para Tiempos de respuesta - Parte 1

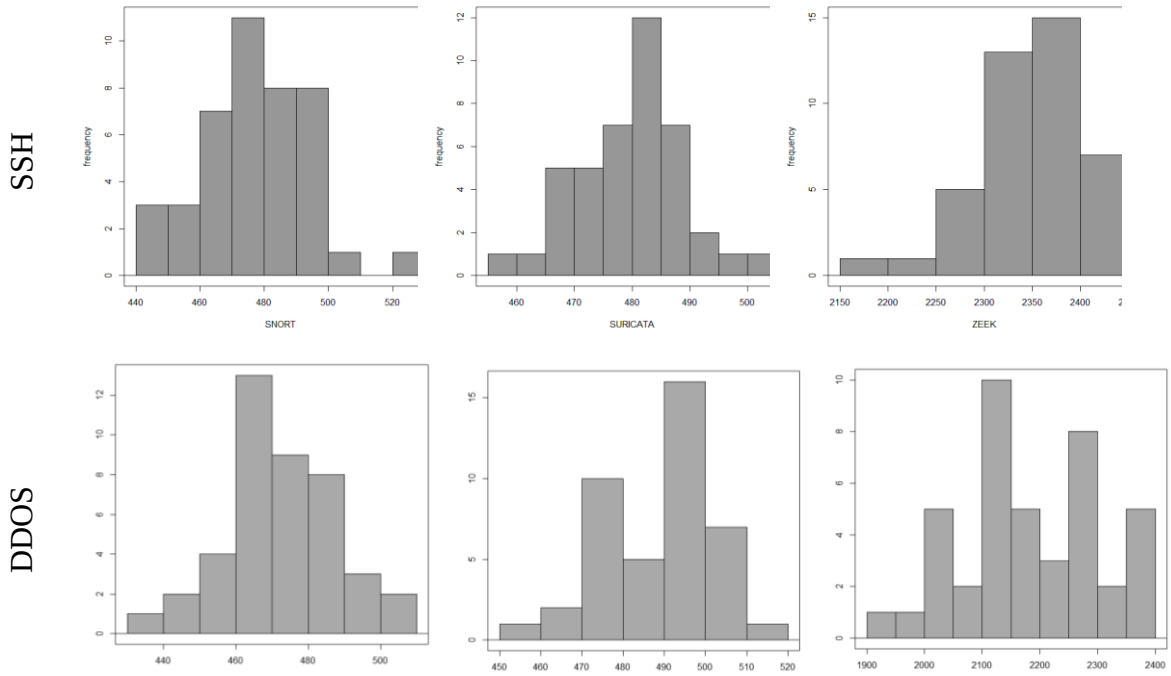


Figura XVIII Histogramas para Pruebas de normalidad para Tiempos de respuesta - Parte 2

Hipótesis Nula: No existe diferencia significativa entre los grupos de IDS en relación con el TIEMPO.

Hipótesis alternativa: *E*xiste diferencia significativa entre los grupos de IDS en relación con el TIEMPO.

Tabla 18 Resultados Test ANOVA para Múltiples factores

	Type III Sum of Squares	*df*	*Mean Squares*	*F*	*p*	η^2_p
IDS	298491404.1	2	149245702.05	33961.04	<.001	0.99
ATAQUE	5401211.88	3	1800403.96	409.68	<.001	0.71
IDS x ATAQUE	4061159.52	6	676859.92	154.02	<.001	0.65
Error	2162150.73	492	4394.62			

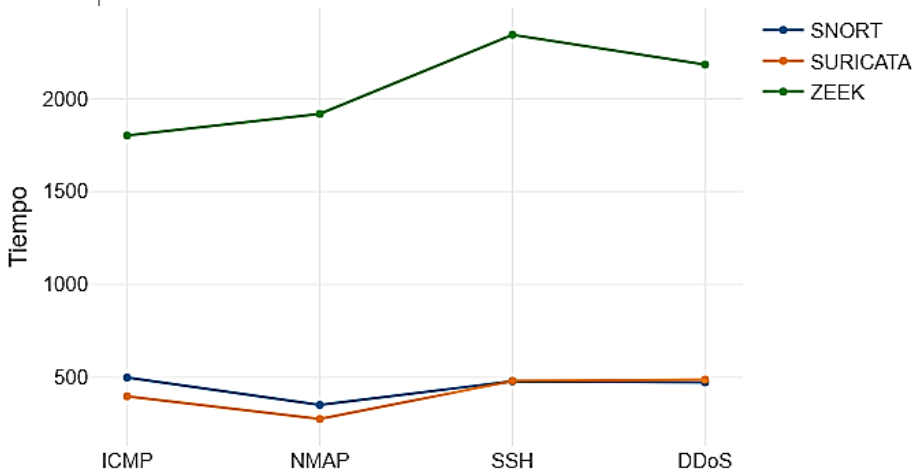


Figura XIX Diagrama de Líneas de la Prueba ANOVA

Tabla 19 Prueba Post-hoc Bonferroni - IDS

		Mean Difference	*SE*	*t*	*p*
SNORT	SURICATA	40.07	7.233	5.54	<.001
SNORT	ZEEK	-1612.11	7.233	-222.88	<.001
SURICATA	ZEEK	-1652.18	7.233	-228.42	<.001

El análisis de varianza ANOVA mostró que ***existe una diferencia significativa entre los grupos de IDS en relación con el TIEMPO p=<.001***, al realizar el test Post-hoc o comparación por pares, vemos que el tiempo de respuesta entre las tres herramientas poseen diferencias significativas.

Un factor crucial para la elección de la herramienta IDS es el tiempo de respuesta a las amenazas mientras; menor sea este parámetro la herramienta tendrá un mejor rendimiento. Después de haber analizado con pruebas estadísticas SURICATA es una opción muy viable, ya que su promedio de tiempo de respuesta es menor al de SNORT y ZEEK.

3.1.2 Análisis de Vulnerabilidades en los Laboratorios de Ingeniería

Para comprobar las vulnerabilidades dentro de los laboratorios de Ingeniería se obtuvo las VLAN disponibles en la Facultad de Ingeniería que se detallan en la tabla y se procedió a realizar el escaneo de los equipos dentro de la red para tener una idea clara de los equipos.

Tabla 20 Descripción de las VLAN de la Facultad de Ingeniería

VLAN	*Descripción*	*Dirección del Switch en la VLAN*	*Dirección IP de Gateway*	*Conexión del Gateway*	*Mascara de red*
2	Vlan_Fi_Administrativo	172.30.2.1	172.30.2.1	Switch Core	/24
3	Vlan_Fi_LabsSistemas	172.30.3.1	172.30.3.1	Switch Core	/24
4	Vlan_Fi_Electronica	172.30.4.1	172.30.4.1	Switch Core	/24
5	Vlan_Fi_SalasDocentes	172.30.5.1	172.30.5.1	Switch Core	/24
6	Vlan_Fi_LabIdiomasIngenieria	172.30.6.1	172.30.6.1	Switch Core	/24
7	Vlan_Fi_Agro	172.30.7.1	172.30.7.1	Switch Core	/24
8	Vlan_Fi_Civil	172.30.8.1	172.30.8.1	Switch Core	/24
9	Vlan_Fi_LabTurismo	172.30.9.1	172.30.9.1	Switch Core	/24
10	Vlan_Fi_AulasMultimedia/Auditorio	172.30.10.1	172.30.10.1	Switch Core	/24

Para este fin se utilizó la herramienta Nessus. Dentro de este escaneo se trabajó con la VLAN 4 que corresponde a los laboratorios de Electrónica y los primeros equipos que fueron escaneados son el SWITCH ya que este puede contener diversas vulnerabilidades, estos resultados se muestran en la siguiente tabla:

Tabla 21 Tabla de Vulnerabilidades Encontradas

Equipo	**Reporte Nessus**				
	Crítico	Alto	Medio	Bajo	Info
SWITCH	-	-	7	2	22
Cámara Web	-	-	-	1	12
Cliente Windows	-	-	-	1	4

Descripción de las vulnerabilidades encontradas

Tabla 22 Descripción de las Vulnerabilidades encontradas en los Laboratorios de la Facultad de Ingeniería

Ítem	**Vulnerabilidad**	**Riesgo**	**Descripción**
1	CVE-1999-0511	Medio	Esta vulnerabilidad puede permitir a un atacante remoto redirigir el tráfico de red a través de la máquina vulnerable. Esto podría permitir al atacante interceptar o modificar el tráfico, o incluso lanzar ataques de denegación de servicio[52].
2	CVE-2019-6110		Actualizar el software NTP a una versión que no sea vulnerable [52].
3	CVE-2023-51385		Esta vulnerabilidad puede permitir a un atacante remoto ejecutar código arbitrario en un servidor DHCP vulnerable [52].
4	CVE-2023-48795		Esta vulnerabilidad puede permitir a un atacante remoto causar una denegación de servicio (DoS) en un servidor DHCP vulnerable [52].
5	CVE-2018-15473		Esta vulnerabilidad puede permitir a un atacante remoto ejecutar código arbitrario en un servidor DHCP vulnerable [52].

6	Network Time Protocol (NTP) Mode 6 Scanner		El servidor NTP remoto responde a las consultas de modo 6. Los dispositivos que responden a estas consultas tienen el potencial de ser utilizados en ataques de amplificación NTP. Un atacante remoto no autenticado podría explotar esto, a través de una consulta de modo 6 especialmente diseñada, para causar una denegación de servicio reflejada [52].
7	CVE-2017-15906		Esta vulnerabilidad puede permitir a un atacante remoto causar una denegación de servicio (DoS) en un servidor DHCP vulnerable [52].
8	DHCP Server Detection	Bajo	Esta vulnerabilidad puede permitir a un atacante remoto detectar la presencia de servidores DHCP en una red [52].
9	CVE-1999-0524		El host remoto responde a una solicitud de marca de tiempo ICMP. Esto permite a un atacante conocer la fecha que se establece en la máquina objetivo, lo que puede ayudar a un atacante remoto no autenticado a derrotar protocolos de autenticación basados en la hora [52].

3.1.3 Proceso de Creación de reglas específicas para las Vulnerabilidades encontradas.

Una vez identificadas las vulnerabilidades que serán objeto de tratamiento, se propone un proceso de creación de reglas personalizadas para mitigar cada una de ellas.

CVE-1999-0511

- **Regla:** `alert tcp $EXTERNAL_NET -> $INTERNAL_NET 256 (msg:"IP forwarding enabled on non-router/firewall"; flow:established).`

Esta regla alerta sobre el tráfico TCP que se origina en una red externa y se destina a una red interna en el puerto 256. El flujo debe estar establecido, lo que significa que la conexión ya se ha establecido. Esto puede indicar que IP forwarding está habilitado en una máquina que no es un router o firewall.

CVE-2019-6110

- Regla: `alert udp $EXTERNAL_NET -> $INTERNAL_NET 123 (msg:"NTP buffer overflow"; sid:1000001; flow:established).`

Esta regla alerta sobre el tráfico UDP que se origina en una red externa y se destina a una red interna en el puerto 123. El flujo debe estar establecido, lo que significa que la conexión ya se ha establecido. Esto puede indicar un desbordamiento de búfer en el protocolo NTP.

CVE-2019-6110, CVE-2023-51385, CVE-2023-48795, CVE-2018-15473, CVE-2017-15906, DHCP Server Detection, CVE-1999-0524

- Regla: `alert udp $EXTERNAL_NET -> $INTERNAL_NET 67 (msg:"DHCP server buffer overflow"; sid:1000005; flow:established).`

Esta regla alerta sobre el tráfico UDP que se origina en una red externa y se destina a una red interna en el puerto 67. El flujo debe estar establecido, lo que significa que la conexión ya se ha establecido. Esto puede indicar un desbordamiento de búfer en el servidor DHCP, también una vulnerabilidad RCE en el servidor DHCP, además de un intento de falsificación de direcciones MAC en el protocolo DHCP .

3.1.4 Implementación de IDS

Para la Implementación se habló con el Ingeniero Javier Montalvo, el cual nos dio acceso a una máquina servidor con las siguientes características:

Tabla 23 Características del Servidor IDS facilitado por DTIC

Procesador	1 núcleos
Memoria RAM	4 GB
Almacenamiento	25 GB
SO	Ubuntu 20.04

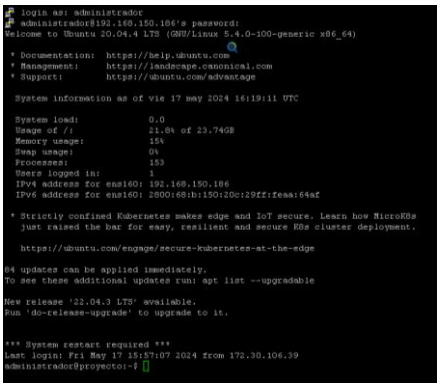


Figura XX Ingreso a la Maquina que servirá de Servidor IDS

El primer paso es la instalación del IDS que hemos seleccionado, para esta implementación será la herramienta SURICATA.

```
administrador@proyecto:~$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.5 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 1
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Warning: detect-classtype: signature sid:1000001 uses unknown classtype: "icmp-cust
om-event", using default priority 3. This message won't be shown again for this cla
sstype
Info: detect: 2 rule files processed. 37545 rules successfully loaded, 0 rules fail
ed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 37548 signatures processed. 1120 are IP-only rules, 4872 are inspecti
ng packet payload, 31343 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
administrador@proyecto:~$
```

Figura XXI Instalación de Suricata

Luego de haber instalado la herramienta procederemos a realizar una pequeña prueba de funcionamiento, verificando si las reglas que trae por defecto SURICATA están funcionando a la perfección.

```
administrador@proyecto:~$ curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
administrador@proyecto:~$ grep 2100498 /var/log/suricata/fast.log
05/17/2024-16:51:49.123464  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returne
d root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 18.64.174
.31:80 -> 192.168.150.186:58682
```

Figura XXII Prueba de Intrusiones para Suricata.

Posterior a esto se procederá a agregar las reglas personalizadas creadas para mitigar las vulnerabilidades encontradas.

```
 GNU nano 4.8                  /var/lib/suricata/rules/misreglas.rules                Modificado
alert tcp $EXTERNAL_NET -> $HOME_NET 256 (msg: "IP forwarding enbale on non-router/firewall"; flow:>
alert udp $EXTERNAL_NET -> $HOME_NET 123 (msg: "NTP buffer overflow"; sid:1000001; flow:establised)
alert udp $EXTERNAL_NET -> $HOME_NET 67 (msg: "DHCP server is attacking"; sid: 1000002; flow:establ>
```

Figura XXIII Inclusión de las reglas personalizadas

Comprobamos el funcionamiento de las nuevas reglas mediante un NSM ElasticSearch.

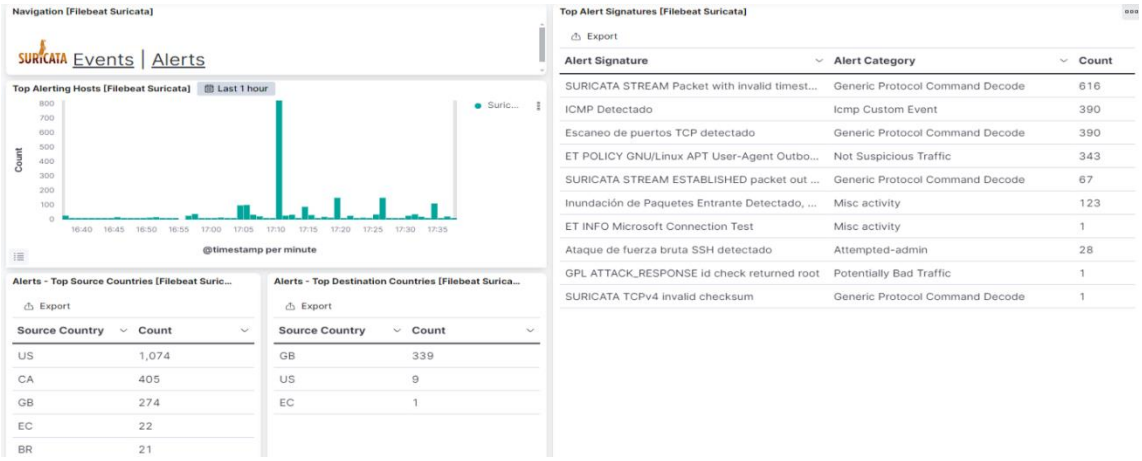


Figura XXIV Interfaz de Elasticsearch

Podemos verificar como el Servidor IDS detecta gran variedad de eventos, y distintos tipos de alertas entre las cuales podemos notar las reglas personalizadas de los ataques dirigidos(ICMP, NMAP, DDoS, SSH) que implementamos en SURICATA

Top Alert Signatures [Filebeat Suricata]

Export

Alert Signature	Alert Category	Count
SURICATA STREAM Packet with invalid timest...	Generic Protocol Command Decode	616
ICMP Detectado	Icmp Custom Event	390
Escaneo de puertos TCP detectado	Generic Protocol Command Decode	390
ET POLICY GNU/Linux APT User-Agent Outbo...	Not Suspicious Traffic	343
SURICATA STREAM ESTABLISHED packet out ...	Generic Protocol Command Decode	67
Inundación de Paquetes Entrante Detectado, ...	Misc activity	123
ET INFO Microsoft Connection Test	Misc activity	1
Ataque de fuerza bruta SSH detectado	Attempted-admin	28
GPL ATTACK_RESPONSE id check returned root	Potentially Bad Traffic	1
SURICATA TCPv4 invalid checksum	Generic Protocol Command Decode	1

Figura XXV Alertas Detectadas por Suricata

3.2 Discusión

Cuando se habla de la metodología empleada en el estudio, se destaca su enfoque sistemático y su adaptación a las necesidades específicas del entorno de los laboratorios de la Facultad de Ingeniería. El proceso de la metodología de investigación, detallado en la Figura I, permitió seguir una secuencia estructurada para alcanzar los objetivos planteados. Además, la operacionalización de las variables, tal como se muestra en las Tabla 1, Tabla 2, Tabla 3, facilitó la medición y análisis de los indicadores relevantes para evaluar el rendimiento de los IDS.

En el marco de la presente investigación, se realizó una evaluación de tres Sistemas de Detección de Intrusiones (IDS) de Software Libre ampliamente utilizados en el ámbito de la seguridad informática: Suricata, Snort y Zeek. El objetivo principal de este estudio fue comparar sus características, funcionalidades, rendimiento y eficiencia en la detección de intrusiones en redes informáticas, los detalles de las comparaciones se presentan a continuación:

En cuanto al primer objetivo, la identificación de las vulnerabilidades en la red de los Laboratorios de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo, los resultados muestran que se encontraron diversas vulnerabilidades detalladas en la Tabla 21. Esto permite concluir que es necesario implementar un sistema de detección de intrusiones (IDS) para monitorizar y proteger la red de estos laboratorios.

Para el segundo objetivo, el estudio comparativo de los IDS en software libre, se analizaron los indicadores de rendimiento como la detección de ataques, la tasa de falsos positivos y el tiempo de respuesta. Los resultados de las pruebas estadísticas realizadas, como las pruebas de normalidad y la prueba de Friedman, permitieron identificar diferencias significativas entre los tres IDS evaluados. Esto sugiere que la selección del IDS más adecuado dependerá de las prioridades y requisitos de seguridad de la red.

Y tercer objetivo, la determinación del IDS a implementar en función de las vulnerabilidades detectadas, el análisis de los resultados permitió concluir que el IDS más apropiado para proteger los laboratorios de la Facultad de Ingeniería es aquel que logre un equilibrio entre una alta tasa de detección de ataques, una baja tasa de falsos positivos

y un tiempo de respuesta adecuado. Esto se determinó tomando en cuenta las necesidades de seguridad y las vulnerabilidades identificadas en la red.

Sin embargo, una debilidad identificada en la metodología es la limitación en el tamaño de IDS seleccionados, ya que solo se evaluaron tres IDS en software libre. Una cantidad mayor de IDS podría proporcionar resultados más generalizables. Además, la implementación y pruebas se realizaron en un entorno simulado, por lo que sería recomendable validar los resultados en un entorno real de producción.

CAPITULO V

4.1 CONCLUSIONES

El estudio comparativo entre los IDS de Software Libre, Suricata, Snort y Zeek, reveló sus respectivas características, funcionalidades, rendimiento y eficiencia en la detección de intrusiones en redes informáticas. Este análisis permitió determinar las fortalezas y debilidades de cada sistema, brindando una visión clara de sus capacidades en entornos específicos como los laboratorios de la Facultad de Ingeniería.

Tras realizar un análisis con herramientas como Nessus, se identificó y documentó las vulnerabilidades presentes en la red de los laboratorios. Estas vulnerabilidades, una vez detectadas, fueron supervisadas y controladas por el IDS implementado, garantizando así la seguridad de la información manejada en dichos entornos.

Después del escaneo de vulnerabilidades y el estudio comparativo de los IDS, se seleccionó el sistema más adecuado para su implementación en los laboratorios. Esta elección se fundamentó en la capacidad del IDS para abordar las vulnerabilidades específicas detectadas, asegurando un funcionamiento óptimo y una protección efectiva de la red de los laboratorios. El IDS que se seleccionó fue SURICATA.

Se llevaron a cabo pruebas exhaustivas de detección, rendimiento, falsos positivos y penetración en el servidor IDS implementado. Estas pruebas permitieron evaluar de manera precisa la eficacia del sistema en la detección de intrusiones, su capacidad de respuesta ante amenazas y su estabilidad operativa en el entorno de los laboratorios de la Facultad de Ingeniería.

El presente trabajo contribuye al avance del conocimiento en el ámbito de la seguridad de redes al ofrecer una comparativa de tres herramientas IDS de Software Libre de uso extendido. Se prevé que los resultados obtenidos sirvan como cimiento para futuros estudios más amplios y profundos enfocados principalmente en los sistemas de detección y prevención de intrusiones (IDPS).

4.2 RECOMENDACIONES

La configuración adecuada del IDS es fundamental para reducir al máximo la tasa de falsos positivos y optimizar su rendimiento. A continuación, se detallan algunas recomendaciones:

Habilitación selectiva de reglas: Se recomienda habilitar únicamente las reglas pertinentes a los servicios u objetivos que se pretenden proteger. Esto evita saturar el sistema con firmas de seguridad irrelevantes y mejora la eficiencia del análisis.

Listas blancas: Si la red monitorizada incluye servicios que no se desea analizar, es recomendable crear listas de confianza (listas blancas). Estas listas informan al IDS que los eventos de red dirigidos hacia las direcciones IP o rangos IP especificados son confiables y no deben generar alertas.

Actualización periódica de firmas: Es crucial realizar comprobaciones y actualizaciones periódicas de las firmas de seguridad implementadas en el IDS. Esto permite eliminar reglas obsoletas de la base de datos de intrusiones y maximizar la efectividad del sistema frente a las amenazas más recientes.

Bloqueo de direcciones IP maliciosas: La utilización de plugins adicionales que permitan bloquear activamente las direcciones IP que registran alertas de mayor severidad puede contribuir a mitigar el riesgo de intrusiones y reducir la carga de trabajo del equipo de seguridad.

Para fortalecer la seguridad de la red de la Universidad y maximizar las capacidades del sistema IDS implementado, se recomienda la futura implementación de un Sistema de Detección y Prevención de Intrusos (IDPS). Un IDPS complementa al firewall existente, proporcionando la capacidad de bloquear ataques en tiempo real sin necesidad de intervención manual por parte de un administrador de red.

BIBLIOGRAFIA

[1] J. A. Astudillo Herrera, A. A. Jimenez Macias, y F. M. Ortiz Flores, "ADAPTACIÓN DEL IDS/IPS SURICATA PARA QUE SE PUEDA CONVERTIR EN UNA SOLUCIÓN EMPRESARIAL", Escuela Superior Politecnica del Litoral, Guayaquil, 2011. Consultado: el 13 de noviembre de 2022. [En línea]. Disponible en: http://www.dspace.espol.edu.ec/handle/123456789/19502

[2] J. Miranda Mejia, F. A. Peralta Mtz., y M. A. Muñoz Mata, "Next generation systems — Scope and application of intrusion detection and prevention systems (IDPS) a systematic literature review", en *12th Iberian Conference on Information Systems and Technologies (CISTI)*, Lisbon, jun. 2017, pp. 2–5. doi: 10.23919/CISTI.2017.7975925.

[3] J. E. Alvarado Chang, "ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR", *Revista Científica Aristas*, vol. 2, núm. 1, Daule, 2020.

[4] INTERPOL, "CIBERDELINCUENCIA: AGOSTO DE 2020", Lyon, 2020. [En línea]. Disponible en: www.interpol.int

[5] Telecommunication Union International, *Measuring digital development - Facts and figures 2021*. Geneva: ITU, 2021.

[6] J. R. Enciso Suárez, J. E. Portilla Rodriguez, y A. C. Mendoza de los Santos, "Análisis integral de los sistemas de detección de intrusos y sus algoritmos asociados en la seguridad de la información", *INGENIERÍA INVESTIGA*, vol. 5, nov. 2023, doi: 10.47796/ing.v5i0.840.

[7] J. A. Lorenzo, "La gran mayoría de redes son vulnerables a ataques informáticos", RZ. Redes Zone. Consultado: el 17 de noviembre de 2022. [En línea]. Disponible en: https://www.redeszone.net/noticias/seguridad/mayoria-redes-vulnerables-ataques-informaticos/

[8] J. M. Spring, “An analysis of how many undiscovered vulnerabilities remain in information systems”, *Comput Secur*, vol. 131, p. 103191, ago. 2023, doi: 10.1016/j.cose.2023.103191.

[9] A. E. Caizapanta González, “Análisis comparativo de Sistemas de Detección de Intrusos (IDS) en entornos universitarios”, *Revista Tecnológica - ESPOL*, vol. 34, núm. 3, pp. 118–138, nov. 2022, doi: 10.37815/rte.v34n3.955.

[10] AdminIberoBlogs, “La importancia de la Seguridad de la Información”. Consultado: el 17 de noviembre de 2022. [En línea]. Disponible en: https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/

[11] MINTEL, “ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR. Retos y oportunidades para la ciberseguridad”, ago. 2022. Consultado: el 17 de noviembre de 2022. [En línea]. Disponible en: https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

[12] M. I. Romero Castro *et al.*, *Introducción a la seguridad informática y el análisis de vulnerabilidades*. Editorial Científica 3Ciencias, 2018. doi: 10.17993/IngyTec.2018.46.

[13] IBM.com, “¿Qué es la seguridad de red?” Consultado: el 11 de enero de 2023. [En línea]. Disponible en: https://www.ibm.com/es-es/topics/network-security#:~:text=La%20seguridad%20de%20red%20protege,dentro%20del%20entorno%20de%20TI.

[14] M. M. Jiménez, “Ataques cibernéticos: causas, tipos y consecuencias”. Consultado: el 11 de enero de 2023. [En línea]. Disponible en: https://www.piranirisk.com/es/blog/ataques-ciberneticos-causas-y-consecuencias

[15] Logitek, “Estrategia de Defensa en profundidad en ciberseguridad industrial.” Consultado: el 11 de enero de 2023. [En línea]. Disponible en: https://www.ciberseguridadlogitek.com/estrategia-de-defensa-en-profundidad-en-ciberseguridad-industrial/

[16] Euronnova, “Qué son los sistemas de detección de intrusos”.

[17] R. G. Bace, P. Mell, y others, “Intrusion detection systems”, 2001.

[18] D. A. Kumar y S. R. Venugopalan, “INTRUSION DETECTION SYSTEMS: A REVIEW.”, *International Journal of Advanced Research in Computer Science*, vol. 8, núm. 8, 2017.

[19] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, y K.-Y. Tung, “Intrusion detection system: A comprehensive review”, *Journal of Network and Computer Applications*, vol. 36, núm. 1, pp. 16–24, 2013.

[20] P. Gómez, “¿Qué es un Sistema de Detención de Intrusiones?”

[21] J. M. Saura Martín, “Implantación de seguridad en entornos Web”, Cartagena, 2006.

[22] C. A. Navarrete Rodríguez, “Aplicación y Metodología para evaluación de Sistemas de Detección de Intrusos”, Universidad de los Andres, Bogota, 2003.

[23] J. E. Arteaga Pucha, “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”, jun. 2020.

[24] Pathak Amrita, “8 herramientas IDS e IPS para una mejor seguridad y conocimiento de la red”. Consultado: el 16 de mayo de 2023. [En línea]. Disponible en: https://geekflare.com/es/best-ids-and-ips-tools/

[25] Fruhlinger Josh, “12 principales herramientas de IDS/IPS”. Consultado: el 16 de mayo de 2023. [En línea]. Disponible en: https://cioperu.pe/articulo/29982/12-principales-herramientas-de-idsips/?p=3

[26] el-brujo, “IDS/IPS Suricata”. Consultado: el 15 de mayo de 2023. [En línea]. Disponible en: https://blog.elhacker.net/2017/04/ids-ips-suricata-reglas-rules.html

[27] S. De Luz, “Aprende a usar Wireshark para capturar y analizar el tráfico de red”. Consultado: el 12 de enero de 2023. [En línea]. Disponible en: https://www.redeszone.net/tutoriales/redes-cable/wireshark-capturar-analizar-trafico-red/

[28] M. Sohail, “Wireshark: A Beginner’s Guide to Network Traffic Analysis”. Consultado: el 15 de febrero de 2024. [En línea]. Disponible en: https://www.linkedin.com/pulse/wireshark-beginners-guide-network-traffic-analysis-sohail-%D1%85%D0%B0%D0%BA%D0%B5%D1%80--svtzf

[29] “¿Qué es Kali Linux?”, Digital Guide IONOS. Consultado: el 15 de febrero de 2024. [En línea]. Disponible en: https://www.ionos.es/digitalguide/servidores/configuracion/kali-linux/#:~:text=Kali%20Linux%20es%20un%20sistema,distribuci%C3%B3n%20no%20carece%20de%20pol%C3%A9mica.

[30] P. Carrasco, “Manual práctico de hping”. Consultado: el 16 de febrero de 2024. [En línea]. Disponible en: https://www.pedrocarrasco.org/manual-practico-de-hping/

[31] “Chapter 15. Nmap Reference Guide”. Consultado: el 16 de febrero de 2024. [En línea]. Disponible en: https://nmap.org/book/man.html

[32] J. Flores, “HYDRA - HERRAMIENTA DE FUERZA BRUTA”. Consultado: el 16 de febrero de 2024. [En línea]. Disponible en: https://www.kolibers.com/blog/hydra-herramienta-de-fuerza-bruta.html

[33] M. Hammond, “Escala de Likert: qué es y cómo utilizarla (incluye ejemplos)”. Consultado: el 18 de febrero de 2024. [En línea]. Disponible en: https://blog.hubspot.es/service/escala-likert

[34] “Suricata”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://suricata.io/

[35] “Snort”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://www.snort.org/

[36] “Zeek”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://zeek.org/

[37] “Security Onion”, feb. 2022, Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://docs.securityonion.net/en/2.3/faq.html#ids-engines

[38] “Security Onion”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://github.com/Security-Onion-Solutions/securityonion

[39] “AlienVault OSSIM”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://cybersecurity.att.com/products/ossim

[40] “Prelude”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://www.prelude-siem.com/en/

[41] “Aanval”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://en.wikipedia.org/wiki/Aanval

[42] “Cisco ISE”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://www.cisco.com/site/us/en/products/security/identity-services-engine/index.html

[43] “USM Anywhere”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://cybersecurity.att.com/products/usm-anywhere

[44] “Splunk”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://www.splunk.com/

[45] C. Polanco, “SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://sofecom.com/que-es-un-siem/

[46] M. Gonen, “Accelerating the Suricata IDS/IPS with NVIDIA BlueField DPUs”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://developer.nvidia.com/blog/accelerating-the-suricata-ids-ips-with-nvidia-bluefield-dpus/

[47] Suricata, “geoip”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://docs.suricata.io/en/suricata-6.0.14/rules/header-keywords.html#:~:text=8.-,geoip,the%20GeoIP2%20API%20of%20MaxMind.&text=One%20of%20the%20directions%20has,the%20given%20geoip(s).

[48] Snort, “GeoIP patch to enhance Snort Reputation Preprocessor”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://github.com/redBorder/Snort_GeoIP

[49] Zeek, “GeoLocationℑ”. Consultado: el 28 de febrero de 2024. [En línea]. Disponible en: https://docs.zeek.org/en/lts/frameworks/geoip.html

[50] Suricata, “6.1. Rules Format”. Consultado: el 29 de enero de 2024. [En línea]. Disponible en: https://docs.suricata.io/en/suricata-6.0.9/rules/intro.html

[51] Snort, “Writing Snort Rules”. Consultado: el 29 de enero de 2024. [En línea]. Disponible en: https://paginas.fe.up.pt/~mgi98020/pgr/writing_snort_rules.htm#:~:text=Snort%20rules%20are%20divided%20into,source%20and%20destination%20ports%20information.

[52] tenable, “CVEs”. Consultado: el 21 de abril de 2024. [En línea]. Disponible en: https://www.tenable.com/cve

ANEXOS

Anexo 1: Alertas detectadas mediante pruebas de ICMP, NMAP, SSH, DDoS para las tres Herramientas

FECHA	CANTIDAD DE DETECCIONES											
	SURICATA				SNORT				ZEEK			
	ICMP	NMAP	SSH	DDoS	ICMP	NMAP	SSH	DDoS	ICMP	NMAP	SSH	DDoS
01/15/2024	31	33	32	32	33	33	33	31	31	32	33	32
01/16/2024	32	32	33	28	33	32	32	31	32	32	32	30
01/17/2024	31	31	32	29	33	33	33	32	32	32	32	33
01/18/2024	32	33	32	30	33	31	33	29	33	30	33	31
01/19/2024	33	32	33	29	32	33	32	32	33	33	31	31
01/20/2024	32	31	33	33	33	31	32	32	29	33	33	32
01/21/2024	31	32	31	33	33	31	33	32	31	30	33	32
01/22/2024	33	29	31	31	32	30	33	31	33	33	32	32
01/23/2024	33	31	31	33	32	33	33	33	33	29	32	32
01/24/2024	31	31	33	33	33	33	33	33	32	31	32	32
01/25/2024	33	29	32	33	32	32	33	33	33	32	32	30
01/26/2024	32	32	33	33	32	32	33	33	31	30	33	32
01/27/2024	33	32	33	33	32	33	33	33	30	32	32	31
01/28/2024	33	31	33	32	32	31	33	31	33	32	33	32
01/29/2024	32	33	32	30	33	33	33	33	32	32	31	33
01/30/2024	32	31	33	32	32	29	32	33	31	32	32	32
01/31/2024	33	29	33	28	33	32	33	31	31	33	33	33
02/01/2024	33	33	33	28	33	32	32	31	33	32	33	32
02/03/2024	32	31	30	31	33	32	30	33	32	32	33	32
02/05/2024	32	33	32	33	33	32	33	32	32	33	33	33
02/07/2024	33	33	31	33	33	33	33	33	33	33	31	30
02/09/2024	32	32	33	33	33	32	33	32	31	33	32	30
02/11/2024	32	31	32	33	33	32	33	33	33	32	32	31
02/13/2024	30	32	33	33	33	33	33	31	33	32	32	32
02/15/2024	33	32	33	33	33	32	33	33	32	33	32	32
02/17/2024	33	31	32	33	33	32	33	33	33	33	32	31
02/19/2024	33	32	32	33	33	33	33	32	32	30	33	32
02/21/2024	31	32	33	33	33	30	32	33	31	31	32	32
02/23/2024	33	33	32	31	33	33	33	33	32	33	31	32
02/25/2024	32	33	32	28	32	31	33	32	33	31	31	32
02/27/2024	32	31	32	33	33	31	32	32	32	33	32	33
02/29/2024	33	30	33	30	32	32	33	31	32	32	31	31

03/02/2024	33	31	31	33	33	32	31	32	33	32	33	32
03/04/2024	33	30	32	33	32	33	30	31	31	32	32	30
03/06/2024	33	32	32	33	32	32	32	32	31	32	33	31
03/08/2024	32	29	32	33	32	33	31	33	33	30	32	31
03/10/2024	32	31	33	33	33	32	33	33	33	32	32	32
03/12/2024	32	30	33	32	32	32	32	33	33	32	32	32
03/14/2024	32	33	32	31	32	32	32	33	32	32	30	32
03/16/2024	32	33	33	32	33	32	32	31	32	32	30	33
03/18/2024	33	32	32	30	33	31	32	33	30	31	33	33
03/20/2024	32	30	33	29	33	28	33	33	32	33	31	33

Anexo 2: Cantidad de Falsos Positivos detectados en las pruebas hacia las tres herramientas.

FECHA	CANTIDAD DE FALSOS POSITIVOS											
	SURICATA				SNORT				ZEEK			
	ICMP	NMAP	SSH	DDoS	ICMP	NMAP	SSH	DDoS	ICMP	NMAP	SSH	DDoS
01/15/2024	2	0	1	1	0	0	0	2	2	1	0	1
01/16/2024	1	1	0	5	0	1	1	2	1	1	1	3
01/17/2024	2	2	1	4	0	0	0	1	1	1	1	0
01/18/2024	1	0	1	3	0	2	0	4	0	3	0	2
01/19/2024	0	1	0	4	1	0	1	1	0	0	2	2
01/20/2024	1	2	0	0	0	2	1	1	4	0	0	1
01/21/2024	2	1	2	0	0	2	0	1	2	3	0	1
01/22/2024	0	4	2	2	1	3	0	2	0	0	1	1
01/23/2024	0	2	2	0	1	0	0	0	0	4	1	1
01/24/2024	2	2	0	0	0	0	0	0	1	2	1	1
01/25/2024	0	4	1	0	1	1	0	0	0	1	1	3
01/26/2024	1	1	0	0	1	1	0	0	2	3	0	1
01/27/2024	0	1	0	0	1	0	0	0	3	1	1	2
01/28/2024	0	2	0	1	1	2	0	2	0	1	0	1
01/29/2024	1	0	1	3	0	0	0	0	1	1	2	0
01/30/2024	1	2	0	1	1	4	1	0	2	1	1	1
01/31/2024	0	4	0	5	0	1	0	2	2	0	0	0
02/01/2024	0	0	0	5	0	1	1	2	0	1	0	1
02/03/2024	1	2	3	2	0	1	3	0	1	1	0	1
02/05/2024	1	0	1	0	0	1	0	1	1	0	0	0
02/07/2024	0	0	2	0	0	0	0	0	0	0	2	3
02/09/2024	1	1	0	0	0	1	0	1	2	0	1	3
02/11/2024	1	2	1	0	0	1	0	0	0	1	1	2
02/13/2024	3	1	0	0	0	0	0	2	0	1	1	1
02/15/2024	0	1	0	0	0	1	0	0	1	0	1	1
02/17/2024	0	2	1	0	0	1	0	0	0	0	1	2
02/19/2024	0	1	1	0	0	0	0	1	1	3	0	1
02/21/2024	2	1	0	0	0	3	1	0	2	2	1	1
02/23/2024	0	0	1	2	0	0	0	0	1	0	2	1
02/25/2024	1	0	1	5	1	2	0	1	0	2	2	1
02/27/2024	1	2	1	0	0	2	1	1	1	0	1	0
02/29/2024	0	3	0	3	1	1	0	2	1	1	2	2
03/02/2024	0	2	2	0	0	1	2	1	0	1	0	1
03/04/2024	0	3	1	0	1	0	3	2	2	1	1	3
03/06/2024	0	1	1	0	1	1	1	1	2	1	0	2
03/08/2024	1	4	1	0	1	0	2	0	0	3	1	2

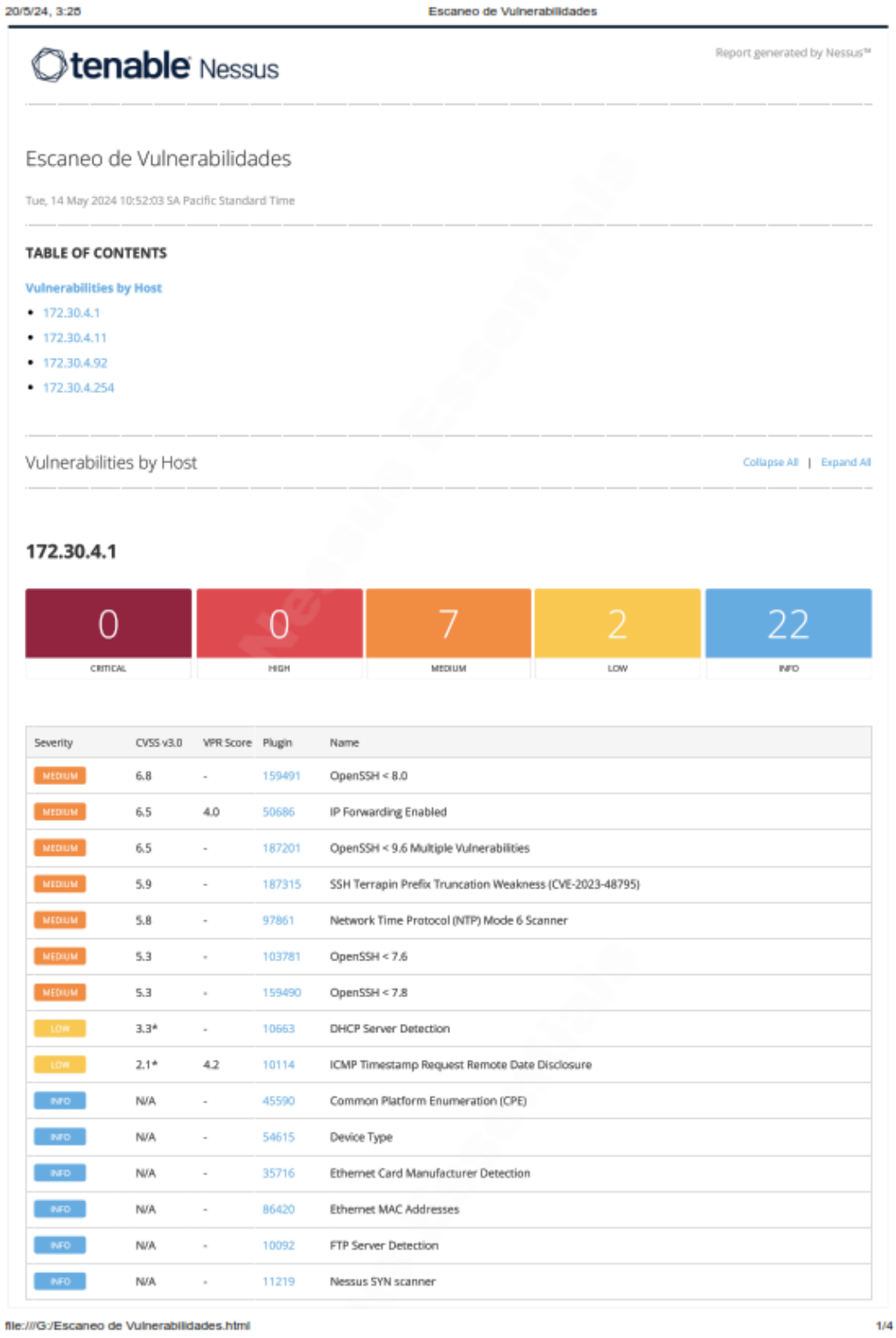
03/10/2024	1	2	0	0	0	1	0	0	0	1	1	1
03/12/2024	1	3	0	1	1	1	1	0	0	1	1	1
03/14/2024	1	0	1	2	1	1	1	0	1	1	3	1
03/16/2024	1	0	0	1	0	1	1	2	1	1	3	0
03/18/2024	0	1	1	3	0	2	1	0	3	2	0	0
03/20/2024	1	3	0	4	0	5	0	0	1	0	2	0

Anexo 3: Tiempos de Respuestas durante las pruebas expresados en milisegundos (ms)

FECHA	TIEMPOS DE RESPUESTA											
	SURICATA				SNORT				ZEEK			
	ICMP	NMAP	SSH	DDoS	ICMP	NMAP	SSH	DDoS	ICMP	NMAP	SSH	DDoS
01/15/2024	507.965	354.756	523.121	475.125	389.906	271.927	473.038	476.933	1719.265	1865.806	2448.720	2286.524
01/16/2024	496.396	350.367	471.285	489.437	408.055	271.962	489.653	476.528	1780.038	1997.687	2355.570	2041.031
01/17/2024	477.773	351.185	493.221	465.165	386.404	264.523	471.560	476.643	1741.662	1748.202	2316.815	2264.713
01/18/2024	476.631	351.874	493.878	451.471	375.419	283.000	481.512	499.504	1687.303	1833.781	2304.023	2323.418
01/19/2024	485.616	347.926	464.176	457.167	382.493	268.654	458.406	511.682	1845.635	1810.644	2253.977	2161.787
01/20/2024	486.310	342.611	488.662	487.236	398.115	275.963	468.083	481.450	1890.488	1927.379	2331.969	2353.011
01/21/2024	443.083	349.432	483.788	445.110	381.229	270.816	482.895	504.553	2077.051	2006.641	2275.049	2203.937
01/22/2024	471.335	353.918	495.804	461.977	386.441	276.932	475.828	491.383	1837.902	1859.161	2368.476	2124.760
01/23/2024	529.988	357.278	487.491	477.671	383.525	279.057	478.745	491.988	1830.300	1823.239	2354.658	2103.752
01/24/2024	481.353	352.817	471.050	481.094	374.300	285.148	479.001	491.310	1647.186	2167.707	2358.257	2395.218
01/25/2024	532.305	347.980	471.852	463.491	420.528	279.243	479.619	492.049	1713.522	1935.255	2411.097	2108.703
01/26/2024	503.199	354.725	508.902	490.804	401.774	266.681	486.023	489.606	1759.275	2038.945	2428.570	2178.515
01/27/2024	484.063	353.868	477.884	472.255	399.372	265.971	485.963	498.915	1833.729	2058.593	2342.587	2135.679
01/28/2024	520.257	360.666	469.878	457.800	378.588	291.497	471.568	467.861	1749.715	2161.918	2320.969	2296.016
01/29/2024	507.424	345.878	495.235	477.432	423.882	282.830	470.482	469.737	1757.628	1865.903	2411.169	2013.482
01/30/2024	497.601	351.616	475.905	486.000	372.818	284.887	482.150	502.260	1810.213	1800.995	2351.468	2142.282
01/31/2024	495.223	346.781	483.852	462.360	355.072	265.896	483.218	474.866	1760.726	1730.154	2285.467	2044.361
02/01/2024	510.765	356.028	453.958	460.381	369.299	273.863	481.714	454.110	1837.766	1858.987	2358.016	2143.458
02/03/2024	487.189	354.521	475.215	476.879	407.756	284.552	493.592	496.662	1815.305	1859.424	2395.382	2275.440
02/05/2024	524.203	352.214	448.423	445.764	387.487	277.925	481.874	490.343	1716.720	1932.415	2310.017	2375.165
02/07/2024	501.972	354.164	485.615	484.207	399.653	276.526	481.997	498.636	1901.127	2056.589	2375.747	2113.203

02/09/2024	496.412	352.475	468.958	469.959	401.038	282.135	488.676	494.104	1863.722	1817.673	2345.020	2120.008
02/11/2024	486.168	349.673	467.139	494.278	406.747	271.023	485.279	491.587	1803.298	1907.559	2324.810	2210.369
02/13/2024	449.124	358.139	465.489	465.126	407.517	282.199	469.329	486.448	1906.461	1910.614	2407.096	2192.954
02/15/2024	495.936	353.845	470.603	468.131	379.399	272.287	477.060	480.324	2021.963	2002.978	2298.393	2286.394
02/17/2024	514.290	346.281	499.471	472.358	393.354	271.826	496.399	507.342	2104.765	2117.412	2319.083	2038.345
02/19/2024	559.811	352.927	487.574	431.813	387.789	275.944	480.970	476.817	2042.459	2101.843	2378.926	2116.957
02/21/2024	461.115	349.725	488.869	467.066	408.006	281.215	483.081	495.235	1612.924	1975.674	2387.304	2321.387
02/23/2024	532.139	350.420	473.371	484.726	382.773	289.488	475.394	500.560	1789.401	1743.210	2346.543	2297.833
02/25/2024	477.159	349.833	494.334	461.123	409.401	278.845	484.062	476.890	1521.934	1727.316	2239.747	2162.109
02/27/2024	549.859	350.575	459.277	470.636	396.854	271.245	473.102	497.552	1622.738	2059.064	2312.505	2355.016
02/29/2024	472.805	354.915	464.169	484.644	373.286	284.592	477.772	490.710	1847.413	2045.255	2361.863	2091.828
03/02/2024	543.991	347.813	469.996	507.011	432.654	273.623	467.432	470.240	1731.558	2106.049	2380.457	2243.911
03/04/2024	504.153	349.088	496.359	468.817	376.393	274.559	484.835	501.151	1904.867	1983.424	2387.627	2298.729
03/06/2024	485.196	341.818	445.945	503.064	431.594	275.431	494.187	506.957	1530.668	1648.698	2351.964	2003.052
03/08/2024	497.210	351.978	478.544	464.994	412.022	267.182	469.514	480.940	1754.664	1899.829	2403.934	1959.336
03/10/2024	487.414	352.540	454.816	458.694	398.973	261.673	489.591	477.283	1794.893	1794.956	2303.842	1928.880
03/12/2024	518.669	355.148	492.594	470.489	403.859	281.828	482.825	493.862	1829.786	1917.382	2292.540	2054.643
03/14/2024	494.259	353.012	449.967	466.819	382.545	264.313	468.200	493.297	1940.859	2047.089	2182.577	2183.279
03/16/2024	504.914	351.955	488.829	490.490	402.953	269.297	462.715	478.685	1803.743	1865.855	2302.727	2148.300
03/18/2024	502.527	353.331	475.499	477.175	449.095	283.383	488.494	473.507	1885.924	1849.831	2407.057	2380.626
03/20/2024	506.342	350.466	479.384	482.696	444.391	271.688	500.735	503.247	1653.328	1740.185	2362.839	2266.237

Anexo 4: Informe de Vulnerabilidades Encontradas



tenable Nessus

Report generated by Nessus™

Escaneo de Vulnerabilidades

Tue, 14 May 2024 10:52:03 SA Pacific Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

172.30.4.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	7	2	22

Severity	CVSS v3.0	VPR Score	Plugin	Name
MEDIUM	6.8	-	159491	OpenSSH < 8.0
MEDIUM	6.5	4.0	50686	IP Forwarding Enabled
MEDIUM	6.5	-	187201	OpenSSH < 9.6 Multiple Vulnerabilities
MEDIUM	5.9	-	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.8	-	97861	Network Time Protocol (NTP) Mode 6 Scanner
MEDIUM	5.3	-	103781	OpenSSH < 7.6
MEDIUM	5.3	-	159490	OpenSSH < 7.8
LOW	3.3*	-	10663	DHCP Server Detection
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	11219	Nessus SYN scanner

INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	185519	SNMP Server Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Hide

172.30.4.11

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	1	12

Severity	CVSS v3.0	VPR Score	Plugin	Name
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	33523	Network Camera Web Server Detection
INFO	N/A	-	11936	OS Identification

INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

Hide

172.30.4.92

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	16

Severity	CVSS v3.0	VPR Score	Plugin	Name
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	11239	Web Server Crafted Request Vendor/Version Information Disclosure
INFO	N/A	-	72427	Web Site Client Access Policy File Detection
INFO	N/A	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

Hide

172.30.4.254

0	0	0	1	4
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	Plugin	Name
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Hide