Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTOR/ES:

Ronny Gonzalo Rocohano Ramos

Andres Alejandro Vallejo Zúñiga

Dennis Joel Diaz Campaña

TUTOR/ES:

Alejandro Cortés López

TEMA:

Implementación de un Sistema Automatizado de Respuesta a Incidentes de Seguridad Basado en Wazuh SIEM para la Mitigación Proactiva de Amenazas en Entornos

Quito - Ecuador

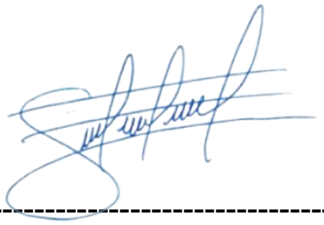
junio – 2025

REINVENTEMOS EL FUTURO

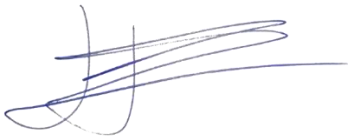
Certificación de autoría

Nosotros, **Ronny Gonzalo Rocohano Ramos, Andres Alejandro Vallejo Zúñiga y Dennis Joel Diaz Campaña,** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.



Firma del graduando
Ronny Gonzalo Rocohano Ramos



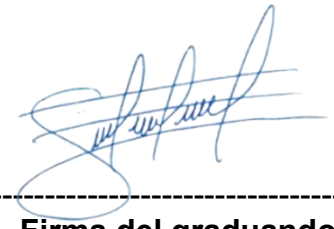
Firma del graduando
Andres Alejandro Vallejo Zúñiga

Firma del graduando
Dennis Joel Diaz Campaña

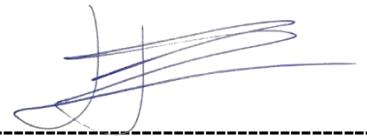
Autorización de Derechos de Propiedad Intelectual

Nosotros, **Ronny Gonzalo Rocohano Ramos, Andres Alejandro Vallejo Zúñiga y Dennis Joel Diaz Campaña,** en calidad de autores del trabajo de investigación titulado ***Implementación de un Sistema Automatizado de Respuesta a Incidentes de Seguridad Basado en Wazuh SIEM para la Mitigación Proactiva de Amenazas en Entornos Empresariales***, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, (Junio 2025)



Firma del graduando
Ronny Gonzalo Rocohano Ramos

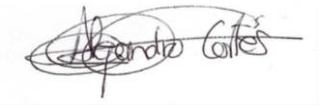


Firma del graduando
Andres Alejandro Vallejo Zúñiga

Firma del graduando
Dennis Joel Diaz Campaña

Aprobación de dirección y coordinación del programa

Nosotros, **Iván Reyes Ch. y Alejandro Cortés L.,** declaramos que: **Ronny Gonzalo Rocohano Ramos, Andres Alejandro Vallejo Zúñiga y Dennis Joel Diaz Campaña**, son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.



_____

Alejandro Cortés L.

Maestría en Ciberseguridad

_____

Iván Reyes Ch.

Maestría en Ciberseguridad

Dedicatoria

Este trabajo de fin de maestría está dedicado principalmente a Dios,

por darme la fuerza y perseverancia para cumplir con el objetivo de acabar mis estudios.

A mis amados padres Nelly, Gonzalo y a mi hermano Sebastián, por su sacrificio, trabajo y amor incondicional en este proceso de estudio, Su ejemplo de esfuerzo y compromiso ha sido mi mayor inspiración. Gracias a ustedes he logrado culminar esta importante etapa de mi vida.

A mi amada novia Selena, quien ha sido mi compañera incansable, mi confidente y mi mayor apoyo emocional. Gracias por tu paciencia, por creer en mí cuando yo dudaba, por tus palabras de aliento y por estar presente en cada paso de este camino.

A todas las personas que me han apoyado y me dieron la oportunidad de cumplir mis metas, en especial, a aquellos docentes y compañeros de curso que compartieron sus conocimientos.

Ronny Rocohano

El desarrollo de esta tesis esta principalmente dedicado a Dios padre y al enorme esfuerzo por parte de mis padres para que pueda desarrollarme dentro del ámbito profesional

Andrés Vallejo

Dedico esté presente trabajo a mi madre por ser mi mayor fuente de inspiración y amor; a mis abuelas que, desde niño me llenaron de amor y valores, siempre cuidándome y moldeándome para que no desviara mi camino.

A mis hermanos, esposo de mamá y demás familiares que me ayudaron siempre que se los pedí sin esperar nada a cambio.

A mis amigos que también fueron fundamental en este proceso brindándome su apoyo y a quienes alguna vez me inspiraron con una palabra, un libro o una mirada de confianza.

Este logro es tan mío como suyo.

Dennis Diaz

Agradecimiento

Agradezco principalmente a Dios por guiarme a lo largo de mi vida, bendecirme y permitirme haber llegado hasta este momento.

Mi profundo agradecimiento a mis padres Gonzalo y Nelly, y a mi hermano Sebastián, por ser ellos mi principal fuente de inspiración y los promotores de cumplir este sueño.

A mi novia Selena, por ser mi sostén emocional, mi motivación diaria y mi cómplice en cada reto superado. Gracias por tu paciencia, por confiar en mí y por estar presente en cada etapa de este camino.

Ronny Rocohano

Un enorme y gran agradecimiento a mis padres Lino Ramiro y Sofia Zúñiga por ser los ejes principales para haberme formado como profesional y ahora dar un paso adelante con mi formación académica.

De igual forma a las autoridades, docentes del área de Ciberseguridad de la maestría en la Universidad Internacional del Ecuador.

Andrés Vallejo

Mi más profundo agradecimiento a mi madre y a mis abuelas por inculcarme valores desde muy temprana edad, por su infinito amor, paciencia; para poder cumplir este logro, que sin ellas no hubiese podido hacerlo realidad.

A mi familia en general por creer en mí, y brindarme su apoyo; y a las demás personas que lamentablemente no están conmigo que también dejaron su granito de arena en este logro.

A mis amigos y compañeros del trabajo de titulación ya que han sido parte fundamental para el desarrollo de las tareas y he aprendido mucho de ellos, a los docentes, y al tutor de tesis; gracias a todos por sus consejos y compartir sus conocimientos, aporte de gran importancia para mi formación profesional.

Dennis Diaz

Índice de contenidos

Índice de tablas

Índice de Figuras

Resumen

El aumento sofisticado de las amenazas cibernéticas en entornos empresariales exige soluciones de Ciberseguridad cada vez más proactivas y sofisticadas que sean capaces de integrar capacidades de detección, respuesta y mitigación automatizada. Con el objetivo de proteger los activos digitales el presente Trabajo Final de Maestría (TFM) presenta la implementación de un Sistema Automatizado de Respuesta a Incidentes de Seguridad basado en Wazuh SIEM, en conjunto con el firewall de protección perimetral pfSense y el motor de detección y prevención de intrusos Suricata. La arquitectura está integrada por una topología de red en un entorno virtualizado con pfSense como el firewall perimetral, gestionado por las políticas internas y perimetral, uso de internet, y controlando el tráfico de la red. Además, Integra estaciones de trabajo Windows y Linux, los cuales son monitoreados por agentes de seguridad instalados en cada host. Los logs que fueron generados por pfSense y Suricata son enviados al servidor de Wazuh centralizado, donde son analizados para identificar eventos de seguridad, estos eventos generan alertas las cuales son enviadas al responsable de seguridad a través de correo electrónico Gmail, facilitando la respuesta temprana y coordinada. Este proyecto permite demostrar la efectividad de una arquitectura que combine la vigilancia, la detección de intrusiones en la red y la gestión de los logs, dando como resultado una reducción del tiempo de detección y las respuestas a incidentes, permitiendo fortalecer la seguridad de la empresa ante amenazas e incidentes.

- Palabras claves:
    - **CIBERSEGURIDAD**
    - **WAZUH SIEM**
    - **PFSENSE**
    - **SURICATA**
    - **RESPUESTA A INCIDENTES**

Abstract

The sophisticated increase in cyber threats in business environments requires increasingly proactive and sophisticated cybersecurity solutions that are capable of integrating automated detection, response and mitigation capabilities. With the aim of protecting digital assets, this Master's Final Project (TFM) presents the implementation of an Automated Security Incident Response System based on Wazuh SIEM, in conjunction with the pfSense perimeter protection firewall and the Suricata intrusion detection and prevention engine. The architecture is integrated by a network topology in a virtualized environment with pfSense as the perimeter firewall, managed by internal and perimeter policies, internet usage, and controlling network traffic. In addition, it integrates Windows and Linux workstations, which are monitored by security agents installed on each host. The logs that were generated by pfSense and Meerkat are sent to the centralized Wazuh server, where they are analyzed to identify security events. These events generate alerts, which are sent to the security officer via Gmail, facilitating an early and coordinated response. This project demonstrates the effectiveness of an architecture that combines surveillance, network intrusion detection, and log management, resulting in reduced incident detection and response times, strengthening the company's security against threats and incidents.

- Keywords:
    - **CYBERSECURITY**
    - **WAZUH SIEM**
    - **PFSENSE**
    - **SURICATA**
    - **INCIDENT RESPONSE**

Capítulo I

Introducción

Este capítulo tiene como propósito realizar la investigación y revisión del estado del proyecto. En esta sección se detallan los antecedentes del proyecto, los cuales se centran en la revisión de literatura de los seguridad informática, ataques informáticos y gestión de incidentes, el alcance del proyecto mediante la búsqueda de implementación de un sistema centralizado para recopilas logs y centralizarlo mediante un SIEM. La iniciación de este capítulo nos servirá como punto de partida para conocer los aspectos actuales de la Seguridad informática y prevención ante amenazas. Una vez revisados los antecedes, se pudo determinar la problemática existente y la dirección del proyecto de titulación.

Definición del proyecto

En el contexto actual de creciente digitalización, las organizaciones enfrentan un aumento sostenido de ciberataques cada vez más sofisticados, dirigidos y persistentes. Esta realidad pone en evidencia la insuficiencia de los mecanismos tradicionales de seguridad, que suelen ser reactivos y manuales, generando retrasos en la contención y mitigación de incidentes. Muchos entornos empresariales carecen de sistemas integrados que permitan una correlación eficaz de eventos, monitoreo en tiempo real y respuesta automatizada. La ausencia de un enfoque proactivo pone en riesgo la integridad, disponibilidad y confidencialidad de los activos digitales.

Aunque existen soluciones SIEM en el mercado, su implementación suele ser costosa o compleja. Wazuh, como plataforma de código abierto, representa una alternativa robusta y accesible. Sin embargo, su adopción aún es limitada en entornos empresariales medianos, principalmente por falta de conocimiento sobre su potencial en la automatización de respuestas a incidentes. Surge entonces la necesidad de evaluar, diseñar e implementar un sistema que integre capacidades automatizadas de detección, análisis y respuesta usando Wazuh, para elevar el nivel de resiliencia de las organizaciones.

Antecedentes

En la actualidad, la ciberseguridad se inclina a presentarse como un pilar esencial para las empresas, garantizando, protegiendo las operaciones y procesos principales ante ciberataques. Las organizaciones se encuentran enfrentando un aumento significativo en la cantidad de ciberataques. La detención de incidentes de seguridad se ha vuelto esencial para la protección de infraestructuras empresariales. No obstante, en su mayoría los sistemas de monitoreo tradiciones requiere intervención manual para poder mitigar las amenazas, lo que genera es un retraso ante la respuesta y aumenta el riesgo de daño hacia las empresas.

Hablar del tema de seguridad de la información es lo más común en las organizaciones, ya que los datos de una organización se convierten en un bien preciado para la empresa, basados en la premisa de que las organizaciones dependen mucho de la información que estas generan, tanto histórica como actualizada y que permite realizar planificación a futuro en un entorno empresarial.

Dentro del entorno empresarial en entidades públicas es mandatorio implementar el EGSI (Esquema Gubernamental de Seguridad de la Información) el cual está basado en la norma ISO 27001., 27002, 27005 y a partir de la versión 3 implementa medidas de ciberseguridad, así como lo indica en su Registro-Oficial-Acuerdo-Ministerial-No.-0003-2024-EGSI (Registro-Oficial-Acuerdo-Ministerial-No.-0003-2024-EGSI-version-3.0.pdf) pag 10.

En el entorno empresarial privado está regulado por la Ley Orgánica de Protección de Datos Personales (LOPD) y la Norma de control para la gestión del riesgo operativo de la Superintendencia de Bancos.

El artículo 26 de la norma de la Superintendencia de Bancos indica que las entidades financieras públicas y privadas deben establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.

Definición de la problemática

En la actualidad, las organizaciones enfrentan una situación de amenazas cibernéticas cada vez más frecuentes y sofisticadas, que pone en riesgo la confidencialidad, integridad y disponibilidad de los activos de información. Muchos entornos empresariales en especial los que tiene recursos limitados, no cuentan con sistemas automatizados y centralizados que puedan detectar, prevenir y responder de manera confiable y eficiente ante los incidentes de seguridad informática.

Uno de los principales problemas es la falta de alertas y visualización en tiempo real de los eventos de seguridad que ocurren tanto en perímetro de la red como en los sistemas internos. Esta ausencia de monitoreo, en conjunto con la falta de herramientas de correlación de eventos de varias fuentes, dificulta la respuesta eficiente frente amenazas como, accesos no autorizados, tráfico malicioso, escaneos de red y vulnerabilidades.

Basados en lo indicado anteriormente las organizaciones tanto privadas como públicas deberían utilizar herramientas que mejoren la seguridad de la información de una manera automatizada basado en las plataformas actuales y open source que nos permita mitigar los riesgos antes de que pase algún evento de seguridad de la información. Estas herramientas que ayudan en este contexto son los SIEM.

Por lo tanto, este proyecto permite identificar la necesidad de implementar una solución que combine capacidades de detección y respuestas a incidentes que además permita automatizar la gestión de logs, alertas y que facilite al personal de seguridad monitorizar en tiempo real los eventos de seguridad. En este contexto, tecnologías como Wazuh SIEM, pfSense, Suricata IDS/IPS permiten crear un sistema de defensa que es capaz de alertar, registrar y responder de manera automatizada a eventos o ataques en la red corporativa.

Justificación

El aumento de la frecuencia de los ataques cibernéticos representa una amenaza para las organizaciones sin importar su sector o tamaño. Para las organizaciones es importante optar por un enfoque preventivo y automatizado que ayude a las empresas anticiparse a los eventos de riesgos y responder de una manera temprana y oportuna a los incidentes de seguridad informática.

El aumento de ataques cibernéticos en el país hace que las instituciones implementen herramientas tecnológicas que ayuden a mitigar las mismas, como IPS(Sistema de Prevención de Intrusiones), IDS (Sistema de Detección de Intrusos), Firewalls , etc. Es por esto que la implementación de un sistema basado en Wazuh SIEM, complementado con pfSense y Suricata, proporciona una solución accesible en costo, recursos, robusta y escalable para monitorizar la infraestructura tecnológica, detectar comportamientos y generar alertas en tiempo real. Esta implementación permite fortalecer la seguridad de las organizaciones mediante una correlación de eventos que provienen de diversas fuentes como firewalls, endpoints y sistemas detecciones de intrusos.

Las herramientas firewall e IDS/IPS, generan registros que contienen información sobre las acciones que realizan los endpoint o los eventos en la red. Se justifica que la implementación de un SIEM (Security Information and Event Management) es una herramienta de ciberseguridad que ayuda a las organizaciones a detectar, responder a amenazas y notificar a los responsables lo que está sucediendo para una correcta toma de decisiones ante un posible evento de ciberataque.

Este trabajo de investigación y desarrollo busca aportar soluciones prácticas al desafío de la detección temprana y mitigación de amenazas mediante un enfoque automatizado. La implementación de un sistema de respuesta a incidentes basado en Wazuh no solo representa un avance técnico, sino también una oportunidad de democratizar la ciberseguridad mediante herramientas accesibles y eficientes. (Tomás Guerra, 2019)

Alcance

Este proyecto contempla la implementación de un sistema automatizado de respuesta a incidentes de seguridad informática. Utilizando herramientas de código abierto como Wazuh SIEM, pfSense y Suricata. La solución está enfocada en la recopilación de logs de diversas fuentes y él envió de alertas para detectar, alertar y responder de forma proactiva ante amenaza.

La topología de trabajo está bajo un entorno virtualizado en VirtualBox, integrada por un firewall pfSense con Suricata integrado, estaciones de trabajo Windows 10, 11 y Linux, y un servidor centralizado con Wazuh SIEM. Por medio de la instalación de agentes Wazuh y la composición de logs que provienen de las estaciones de trabajo, se habilita el monitoreo, la generación de alertas, y la automatización de acciones de respuestas ante eventos de seguridad, como accesos no autorizados y escaneos de red.

El proyecto incluye la definición de políticas de seguridad perimetral, uso de internet y monitoreo de endpoints, la personalización de reglas en Suricata para detección y bloqueo de amenazas, el envío de logs y eventos hacia Wazuh para el análisis y visualización en su dashboard y la generación de alertas por correo electrónico Gmail dirigidas hacia el personal de seguridad.

Objetivos

Objetivo General

Implementar un sistema automatizado de respuesta a incidentes de seguridad basado en Wazuh SIEM, integrado con Suricata IPS/IDS y pfSense, para mejorar la detección y mitigación proactiva de amenazas en un entorno empresarial virtualizado.

Objetivos Específicos

- Diseñar una topología de red virtualizado que simule un entorno empresarial, integrando firewall, Sistema detección y prevención de intrusos, sistema SIEM y estaciones de trabajo.
- Configurar el firewall pfSense con Suricata, aplicando políticas de seguridad perimetral y reglas personalizadas para la detección y bloqueo de tráfico malicioso.
- Instalar y configurar el servidor Wazuh SIEM, integrando agentes en los distintos equipos de la red para monitorear eventos y la recolección de logs.
- Establecer políticas de seguridad orientadas al monitoreo de endpoints, al uso de internet y a la detección de intrusiones dentro de la red.
- Automatizar la generación de reglas y notificaciones por correo electrónico, dirigidas al personal de seguridad, ante la detección de eventos críticos.
- Evaluar la eficacia del sistema implementado, mediante la simulación de escenarios de ataque y el análisis de la respuesta del sistema ante los incidentes.

Capítulo II

Revisión de Literatura

Estado del Arte

En los últimos años, el aumento exponencial de ciberataques ha impulsado el desarrollo y la adopción de sistemas de gestión de eventos e información de seguridad (SIEM), tecnologías esenciales para el monitoreo centralizado, la detección de amenazas y la respuesta ante incidentes. Según un informe de (Gartner, 2024)las soluciones SIEM se han consolidado como componentes estratégicos dentro de la arquitectura de ciberseguridad de las organizaciones modernas.

Los primeros sistemas SIEM se enfocaban exclusivamente en la recolección y centralización de logs, sin capacidades de análisis automatizado. Con el tiempo, estas soluciones evolucionaron para incorporar motores de correlación, análisis de comportamiento, inteligencia de amenazas y automatización de respuestas, dando paso a soluciones más robustas como Splunk, IBM QRadar, AlienVault OSSIM y, en el ámbito open-source, Wazuh.

Wazuh ha ganado relevancia como una alternativa poderosa de código abierto, al integrar funcionalidades de HIDS (Host-based Intrusion Detection System), SIEM, monitoreo de integridad, escaneo de vulnerabilidades y gestión de cumplimiento normativo. En estudios como el de (Reid, 2024) , se demostró que Wazuh no solo es competitivo frente a soluciones comerciales, sino que también es altamente personalizable y escalable para entornos empresariales.

La automatización en la respuesta a incidentes representa un cambio de paradigma en la gestión de ciberseguridad. En lugar de depender exclusivamente del análisis humano, se han empezado a aplicar técnicas de orquestación y ejecución de respuestas automatizadas mediante scripts, reglas de correlación y herramientas SOAR (Security Orchestration, Automation and Response). Investigaciones como la de (lazarus Alliance, 2024)muestran cómo la automatización reduce significativamente el tiempo de detección y mitigación de amenazas, mejorando la resiliencia organizacional.

En el ámbito académico y empresarial, diversos proyectos han explorado la integración de Wazuh con tecnologías como ElasticSearch y Kibana, facilitando visualizaciones intuitivas de eventos de seguridad. Por ejemplo, en el estudio de (Wazuh, 2024), una empresa financiera implementó Wazuh para la monitorización de endpoints, logrando detectar comportamientos anómalos en tiempo real y ejecutar respuestas automáticas a través de reglas personalizadas.

Sin embargo, a pesar de estas investigaciones, persiste un vacío en la aplicación práctica de Wazuh como plataforma completa de respuesta proactiva a incidentes en entornos empresariales de mediana escala, con enfoque en automatización de acciones correctivas y correlación avanzada. Es precisamente este vacío el que esta tesis pretende abordar, mediante la implementación real de una arquitectura automatizada basada en Wazuh, que demuestre su eficacia, aplicabilidad y ventajas frente a soluciones tradicionales o manuales

Marco Teórico

En esta sección del trabajo de titulación de desglosan la terminología y conceptos claves para el mejor entendimiento del proyecto estipulado.

Ciberseguridad

La ciberseguridad es el conjunto de prácticas, tecnologías, procesos y políticas diseñadas para proteger sistemas, redes, dispositivos y datos frente a accesos no autorizados, daños, interrupciones o destrucción. Abarca dimensiones como la seguridad de red, la seguridad de aplicaciones, la seguridad de la información, la continuidad del negocio y la recuperación ante desastres. La ciberseguridad es importante porque los ataques cibernéticos pueden causar consecuencias graves para organizaciones y/o personas. Los ataques cibernéticos exitosos conducen al robo de identidad, extorsión personal y corporativa, pérdida de información confidencial y datos críticos para el negocio, interrupciones temporales del negocio, pérdida de negocios y pérdida de clientes y, en algunos casos, cierres de negocios. (Perez, 2025)

Según (Nacher, 2024), la ciberseguridad se enfoca en proteger el ciberespacio, entendido como el entorno de interacción entre personas, software y servicios sobre internet o redes privadas. En contextos empresariales, la ciberseguridad busca garantizar la confidencialidad, integridad y disponibilidad de la información, conocida como la Tríada CID.

La ciberseguridad ya no se limita a la protección de infraestructuras críticas, sino que abarca la defensa de datos personales frente a amenazas como el phishing, ransomware y filtraciones masivas (Delgado, Muñoz, Padilla, & Quiñónez, 2025)

Gestión de Incidentes

La gestión de incidentes es un punto clave dentro de los pasos para detectar, analizar, contener, recuperar, aislar y erradicar novedades y/o eventos que se presenten y pongan en riesgo la seguridad de la información.

SIEM (Security Information and Event Management)

Son sistemas que permiten centralizar, almacenar, correlacionar y analizar grandes volúmenes de datos generados por diferentes dispositivos, sistemas operativos, aplicaciones y redes. Su objetivo es detectar patrones de ataque, generar alertas y proporcionar una visión integral de la postura desde la seguridad informática.

Un SIEM permite recopilar, analizar y gestionar los datos de seguridad generados por sistemas y aplicaciones en tiempo real. Estas herramientas no solo nos permiten detectar y responder de manera eficaz a los incidentes de seguridad, sino que también ser un fuerte de control centralizado y una correlación automatizada de sucesos, posicionándose como una solución integral frente a las ciber amenazas de los ciberdelincuentes.

Los Siem no solo automatizan la recolección y análisis de eventos, sino que también facilitan la respuesta a incidentes, lo que mejora la eficiencia y reduce los tiempos de reacción ante posibles

amenazas. Tal como explica (Lara, Miranda, Alejando, & Marcillo, 2024) existen diversas recomendaciones y mejores prácticas, como firewalls y sistemas de prevención, para mitigar amenazas cibernéticas, sin embargo, presentan desafíos importantes, como la gestión de múltiples interfaces, la acumulación masiva de registros de eventos que a menudo no son analizados de manera eficiente y la falta de personal capacitado para gestionar estos sistemas. Es por ello que las soluciones SIEM han surgido como herramientas esenciales para superar los desafíos al centralizar y correlacionar eventos de seguridad en una plataforma única.

Figura1

Solución de gestión de eventos e información de seguridad (SIEM)

Respuestas automatizadas

La automatización de respuestas a incidentes es una estrategia clave para mejorar la eficiencia y reducir el tiempo de reacción ante eventos de seguridad. Esta se ejecuta a través de **SOAR** (*Security Orchestration, Automation and Response*), lo que permite integrar herramientas, personas y procesos para responder de forma automática.

(Ricard, 2024) menciona que Los IDS/IPS como Suricata son herramientas clave para monitorear el tráfico de red y detectar comportamientos sospechosos, como intentos de escaneo de puertos o transferencias de datos inusuales, un IDS alerta al Blue Team sobre actividades potencialmente maliciosas, mientras que un IPS puede bloquear automáticamente ciertos tipos de tráfico, por ejemplo si detecta un intento de explotación de vulnerabilidad conocida, el IPS puede detener la conexión antes de que el atacante logre comprometer el sistema, protegiendo los activos críticos de la organización.

Wazuh

Es un SIEM que utiliza una plataforma de código abierto utilizada en la ciberseguridad y monitorización que combina las capacidades de (SIEM) y Extended Detection and Response (XDR). Su diseño es enfocado en la prevención, detección y respuesta automatizadas ante amenazas, análisis de logs, monitoreo de integridad de archivos, detección de vulnerabilidades, estableciendo herramientas clave para la ciberseguridad y la protección de los datos en un solo sistema. Una de las funcionalidades características de wazuh es su integración con Elastis Stack y kibana 16 que sirve para potenciar su capacidad analítica logrando un acceso rápido y eficiente en grandes volúmenes de datos. Es compatible con la mayoría de los sistemas operativos, aplicaciones, dispositivos y entornos virtuales. (Ruiz, 2025)

Entre sus principales características tenemos:

- Gestión de logs: Recopila, analiza y almacena automáticamente logs de diferentes endpoints y aplicaciones en tiempo real.
- Análisis de vulnerabilidades: Evalúa configuraciones y detecta posibles debilidades en los sistemas.
- Soporte Multiplataforma: Wazuh también es compatible con sistemas operativos basados en Linux, Windows y macOS

- Detección basada en HIDS: Identifica actividades sospechas y de índole maliciosas además de, detectar cambios y accesos no autorizados en los sistemas y endpoints.
- Cumplimiento normativo: Cumple con las normas PCI DSS, HIPAA y GDPR(ley europea)

Riesgos Cibernéticos

Son riesgos operativos para los activos tecnológicos y de información que tienen efectos que influyen en la confidencialidad, disponibilidad o integridad de la información o de los sistemas de información

La definición que ofrece la (ISO/IEC 27000, 2018) sobre el riesgo en el contexto de los sistemas de seguridad, este que este es un efecto previsto o negativo que recae sobre los sistemas de información. Esto está relacionado con la posibilidad de recibir un ataque, de manera que en caso de recibirlo se explotaran las vulnerabilidades que tengan los sistemas o las instalaciones de la organización, pero en el caso de que el riesgo sea asumido puede pasar de improvisto y no afectar a los sistemas, la información o las instalaciones de la organización. Existen diversos métodos de tratar los riesgos, estos se deben evaluar para saber el efecto negativo o esperado que tendrán dentro de la organización o del sistema de información y una vez analizados se deberán tomar decisiones para mitigarlos, mejorar la seguridad o definir si los riesgos serán asumidos (Park & Huh, 2020).

Capítulo III

Metodología

En este capítulo se detalla la metodología empleada para el desarrollo e implementación del Sistema automatizado de Respuesta a Incidentes de Seguridad basado en Wazuh SIEM, Suricata (IPS/IDS) y pfSense. El proceso esta seccionado en tres etapas claves: El diseño de la arquitectura de seguridad, la implementación técnica de las herramientas y la validación mediante pruebas controladas de detección y mitigación de amenazas.

Esta sección plantea dos objetivos principales:

- Implementar un entorno integrado de monitorización y respuesta automatizada, mediante la aplicación de políticas de seguridad perimetral (pfSense y Suricata) y de endpoints.
- Validad la capacidad para detectar y mitigar amenazas comunes en entornos empresariales

Para poder garantizar la eficacia del sistema, el primer paso es establecer reglas de detección personalizadas en Suricata y pfSense, estas reglas van a estar basadas en patrones de amenazas conocidas como las firmas de MITRE ATT&CK. Aunque la detección no cumple con los objetivos de mitigación, es crítico automatizar las respuestas y notificar al personal.

Tipo de investigación

La investigación del presente trabajo es de tipo aplicada y de desarrollo tecnológico porque busca resolver el problema de la insuficiencia detección y respuesta a incidentes mediante la implementación de una solución práctica. Es de desarrollo tecnológico porque los procesos ejecutados implican el diseño, construcción y pruebas de un sistema informático de seguridad funcional.

El enfoque es considerado descriptivo y explicativo, ya que describe las características del sistema de seguridad implementado y explica el funcionamiento correcto y por qué sus procesos son efectivos para lograr la mitigación temprana y proactiva de amenazas en el ciberespacio.

Fuente de datos

Para definir y encontrar una correlación entre Wazuh, pfSense y Suricata la fuente de datos incluye logs del firewall de pfSense, alertas de Suricata (detección e IPS), y eventos de seguridad generados y recolectados por los agentes de Wazuh instalados en los endpoints y en pfSense. Los datos generados por las herramientas de la implementación son la evidencia principal de la funcionalidad del sistema. Adicional se utilizó como fuentes externas los estándares de seguridad como la ISO 27001, la documentación oficial de Wazuh, Suricata y pfSense, que sirven como base teórica para el correcto diseño e implementación del sistema.

Planteamiento del diseño de la investigación

La implementación se basa en la simulación de escenario de amenazas reales mediante el uso de herramientas de software libre, permitiendo poder replicar condiciones similares y reales a las que presentan las empresas. A través de la configuración de un entorno virtual, conformado por una infraestructura con firewall pfSense más Suricata, estaciones de trabajo con Windows 10, 11 y Ubuntu, un servidor SIEM Wazuh, y un equipo Linux adicional con Kali. Se evalúa el comportamiento del sistema ante escaneo de puertos, tráfico malicioso y actividades anómalas.

El diseño contempla las siguientes fases:

1- Definir y crear las políticas que serán parte del sistema y regirán sobre los demás usuarios dentro de la red.
2- Establecer los equipos que formaran parte del entorno y que tendrá acceso a la red interna.

3- Modificar el firewall de pfSense a partir de las políticas establecidas para garantizar un control efectivo del tráfico.
4- Integrar el IPS/IDS Suricata para la detección y bloqueo de direcciones maliciosas.
5- Integrar de los agentes de Wazuh dentro de las maquinas establecidas para la gestión de eventos a tiempo real.
6- Incorporar de los logs de Suricata en Wazuh como nuevo agente.
7- Enviar los registros procesados por Wazuh vía correo electrónico.

Desarrollo de la implementación

En la fase inicial de la implementación del sistema, se establecieron políticas de seguridad que rigen el comportamiento de los usuarios, dispositivos y sistemas dentro del entorno de red. Estas reglas se diseñaron en base a buenas prácticas de ciberseguridad y están establecidas dentro de la Política general de seguridad de la información, la cual es detallada a continuación:

Políticas de general de seguridad informática

Objetivo

Establecer una política responsable en el uso de los sistemas de información, definiendo las normas para la seguridad y buen uso de equipos informáticos y de comunicación en la EMPRESA XYZ

Alcance

Esta política se aplica a todos los colaboradores, sin importar su nivel jerárquico, y a todos los equipos de cómputo y sistemas informáticos, independientemente del lugar físico donde se encuentren funcionando.

Definiciones

La EMPRESA XYZ proporciona a sus trabajadores y colaboradores distintas herramientas informáticas que deberán utilizarse para fines laborales. Cada usuario deberá tratar su equipo y sistema informático asignado de manera honesta y responsable, cuidando al máximo la información generada y siguiendo las políticas de seguridad y respeto a los acuerdos contractuales y licencias de uso.

Política de seguridad interna y perimetral de la red

Se Establece una política que garantice la protección de la red y los recursos de la EMPRESA XYZ. Esta política debe ser aplicada a todos los servicios, acceso y aplicaciones.

Proceso general

- Todo el tráfico de la red interna debe pasar por el Firewall.
- Se debe bloquear a usuarios y dispositivos no autorizados a la red.
- En el caso de alguna anomalía en la Red, el Oficial de Seguridad podrá tomar las acciones necesarias para detener la misma.
- Está prohibido el acceso a la red interna o corporativa de equipos o dispositivos personales.
- El acceso del Internet se deberá hacer por medio de Filtrado de Web (Categorizaciones) para bloquear acceso a páginas y aplicaciones no autorizadas.
- Todos los puertos o servicios no definidos estarán bloqueados.

Excepciones y su aprobación

La excepción a esta política debe ser autorizada por el Gerente TI.

Determinación de responsables

Es responsabilidad del oficial de seguridad mantener esta política actualizada en base a los estándares internacionales y mejores prácticas de seguridad, así como velar por el cumplimiento de esta.

Es responsabilidad de los gerentes garantizar que las personas que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la organización.

Es responsabilidad de los usuarios mantener la seguridad de información dentro de las actividades relacionadas con su trabajo y revisar periódicamente los cambios que se realicen a esta política para viabilizar la seguridad tecnológica de los recursos.

Prohibiciones

Los usuarios que no cumplan con las disposiciones a esta política deberán aceptar las sanciones por incumplimiento del mismo.

Política de uso de internet

Proceso general

Establecer una política clara sobre el uso aceptable de los recursos de Internet dentro de la EMPRESA XYZ, con el objetivo de prevenir el uso inadecuado que pueda comprometer la seguridad, productividad o imagen de la organización.

Lo que esta permitido

- Navegación en páginas de interés general que apoyen las labores asignadas.
- Consultas en sitios gubernamentales, bancarios y servicios relacionados con la empresa.
- Acceso a contenidos técnicos y profesionales directamente vinculados a las responsabilidades del puesto.

- Consulta de noticias generales que no interfieran con la productividad laboral.

Lo que no está permitido

- Acceso a páginas con contenido ilícito, violento, discriminatorio o que atente contra la dignidad humana.
- Participación en foros, blogs o chats no vinculados a la actividad profesional.
- Descarga de ficheros o programas que no hayan sido aprobados por el Departamento de TI.
- Uso de servicios de streaming (video, música) salvo que estén justificados por la labor y autorizados formalmente.

Excepciones y su aprobación

Cualquier excepción a esta política deberá contar con la autorización escrita de la Gerencia de TI, y deberá estar registrada mediante informe formal.

Determinación de responsables

- Oficial de Seguridad: Responsable de monitorear el cumplimiento de esta política y establecer alertas en Wazuh y Suricata para detectar accesos indebidos.
- Gerentes y supervisores: Deberán comunicar estas normas a su equipo y dar seguimiento a su cumplimiento.
- Usuarios: Deben actuar con responsabilidad y ética, respetando las condiciones establecidas para el uso de Internet corporativo.

Prohibiciones

El uso del servicio de Internet para fines personales, ilícitos o que puedan afectar el desempeño y la reputación de la empresa queda estrictamente prohibido.

Política de detección y prevención de intrusiones en la red

Establecer las directrices para el uso de Suricata como sistema de detección y prevención de intrusiones (IDS/IPS) para identificar amenazas en el tráfico de red de la empresa XYZ.

Proceso general

- Suricata debe estar instalado y funcionando en modo IPS dentro del pfSense, inspeccionando todo el tráfico LAN ↔ WAN.
- Las reglas de detección deben mantenerse actualizadas mediante fuentes oficiales como Emerging Threats.
- Se bloqueará automáticamente todo tráfico detectado como potencialmente malicioso, como escaneos de puertos, exploits, o conexiones no autorizadas.
- Todo evento generado por Suricata será logueado y correlacionado con Wazuh para análisis conjunto.
- El tráfico hacia servicios internos no autorizados será considerado como intento de intrusión.

Excepciones y su aprobación

Toda excepción relacionada con la desactivación de reglas o el bypass de tráfico debe ser documentada y aprobada por el Gerente de TI.

Determinación de responsables

- Oficial de Seguridad: Responsable de revisar y mantener las reglas activas de Suricata, así como analizar los eventos generados.
- Equipo de Infraestructura: Deberá asegurar que el motor Suricata se mantenga activo y actualizado dentro del firewall.
- Usuarios: No deben realizar acciones que generen tráfico sospechoso o malicioso dentro de la red.

Prohibiciones

- Está prohibido deshabilitar reglas del IDS sin una evaluación formal.
- No se permite el uso de herramientas de escaneo o ataque (como Nmap, Metasploit, etc.) dentro de la red empresarial sin autorización explícita.

Política de monitoreo y detección de eventos en sistemas endpoint

Establecer los lineamientos para la supervisión, detección y notificación de eventos de seguridad en los sistemas de la empresa Grupo2, mediante la implementación de la plataforma Wazuh.

Proceso general

- Todos los servidores y estaciones de trabajo deberán tener instalado el agente Wazuh.
- Se deben auditar logs del sistema, cambios de archivos críticos, intentos fallidos de acceso, ejecuciones de comandos sospechosos y elevaciones de privilegios.
- Los eventos críticos serán clasificados de acuerdo a su nivel de severidad y notificados al Oficial de Seguridad.
- El servidor de Wazuh mantendrá las reglas de detección actualizadas para responder ante nuevas amenazas.

- Se deben conservar los registros de eventos durante al menos 90 días, conforme a buenas prácticas de auditoría.

Excepciones y su aprobación

Cualquier excepción a la implementación o monitoreo deberá ser justificada y autorizada por la Gerencia de TI.

Determinación de responsables

- Oficial de Seguridad: Responsable de configurar las reglas de Wazuh, revisar los dashboards y gestionar las alertas.
- Equipo de TI: Responsable de asegurar que todos los endpoints tengan el agente activo y en comunicación con el servidor.
- Usuarios Finales: Deben informar cualquier comportamiento anómalo en sus dispositivos y no manipular el agente instalado.

Prohibiciones

- Está prohibido desinstalar o deshabilitar el agente de Wazuh sin autorización previa.
- Está prohibida la alteración de archivos de log o sistemas de auditoría del endpoint.

Estas políticas se diseñaron para la creación de reglas principales del Firewall para la simulación de un entorno empresarial. Estas reglas con determinadas por la necesidad de contar con normas para la protección.

Se integrará Suricata en Pfsense para monitorizar el tráfico y los dispositivos en busca de actividades que puedan resultar sospechosas o maliciosas, mediante suricata se bloqueara

automáticamente sitios web maliciosos o que no se encuentran contemplados dentro de las políticas de la empresa.

Únicamente se colocaron sitios de mensajería y otros referentes a entidades financieras que no representan una amenaza y son parte importante dentro de la empresa, dominios referentes a sitios relacionados con redes sociales y páginas de contenido inadecuado serán bloqueadas.

Para controlar en tiempo real la gestión de amenazas se requiere de Wazuh, este último juega un papel fundamental para la gestión de seguridad en el SIEM automatizado, nos permite detectar y monitorear en tiempo real las amenazas y analizar eventos de seguridad.

Wazuh nos permite recopilar y analizar logs, alerta sobre cambios críticos o modificaciones no autorizadas y es capaz de identificar debilidades y vulnerabilidades dentro de los agentes.

Existirán un total de 3 agentes dentro de Wazuh, un agente para la maquina Windows 11 con Ip 192.168.1.103, otro agente para la maquina Windows 10 con Ip 192.168.1.106 y el ultimo agente será integrado junto a Suricata para el procesamiento de alertas, esto último para una correlación más efectiva de eventos relacionados a la seguridad. La topología del sistema está conformada de la forma en la se muestra en la figura.

Figura 3

Topología principal de la red LAN implementada en Virtual Box

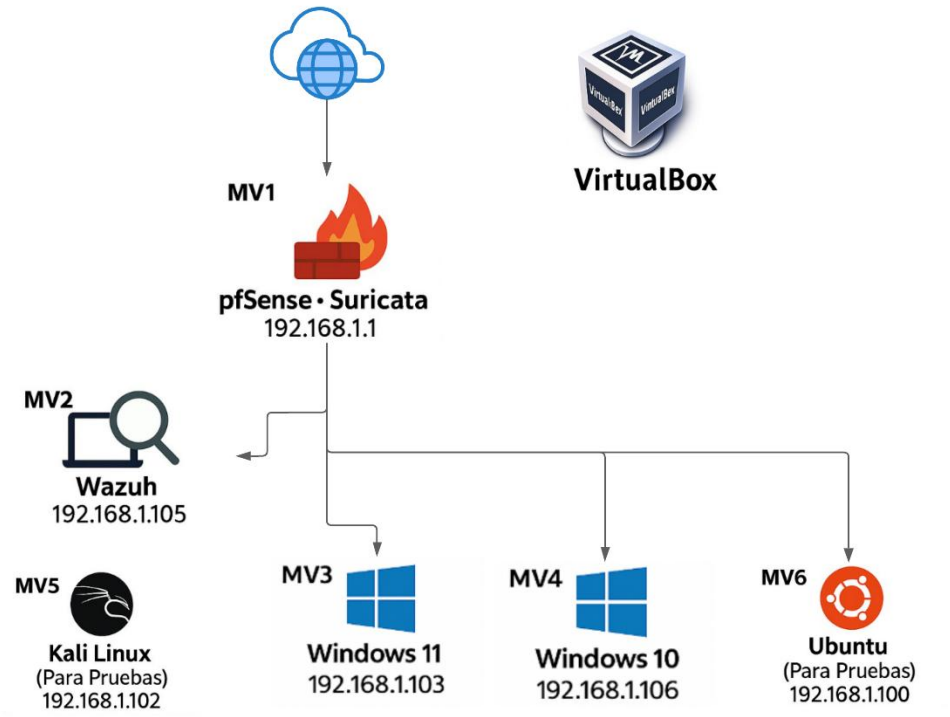


Tabla 1

Configuración topología de las maquinas con sus respectivas IP

Hipervisor Virtual Box		
MV1	Pfsense - Suricata	192.168.1.1
MV2	Wazuh	192.168.1.105
MV3	Windows 11	192.168.1.103
MV4	Windows 10	192.168.1.106
Mv5	Kali Linux	192.168.1.102
MV6	Ubuntu	192.168.1.100

La máquina referente a Kali Linux se utilizará como recurso para la realización de pruebas, tanto del firewall como de los agentes Wazuh.

Características de las máquinas virtuales

Para una detallada gestión y funcionamiento se presenta las características de las máquinas virtuales en función a su utilización.

Maquina Pfsense

La característica de la máquina del firewall es la siguiente:

- Memoria RAM: 4096 MB
- Adaptador 1: NAT para la conexión a internet
- Adaptador 2: Red interna para la conexión entre la red local
- Almacenamiento: 6GB

Figura 4

Maquina Pfsense y sus especificaciones

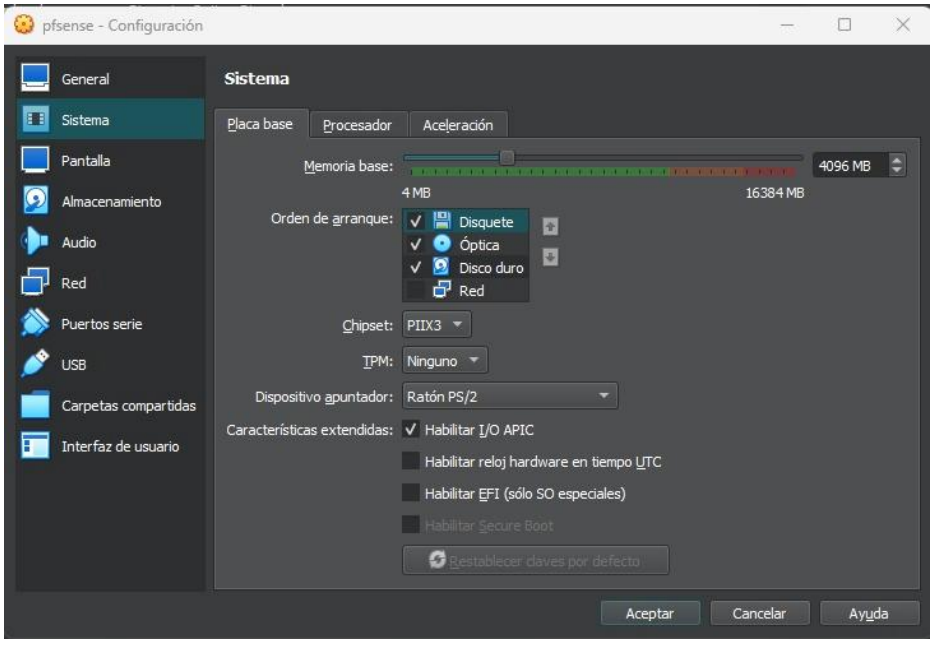


Figura 5

Pfsense Adaptador de Red 1 (Red NAT)

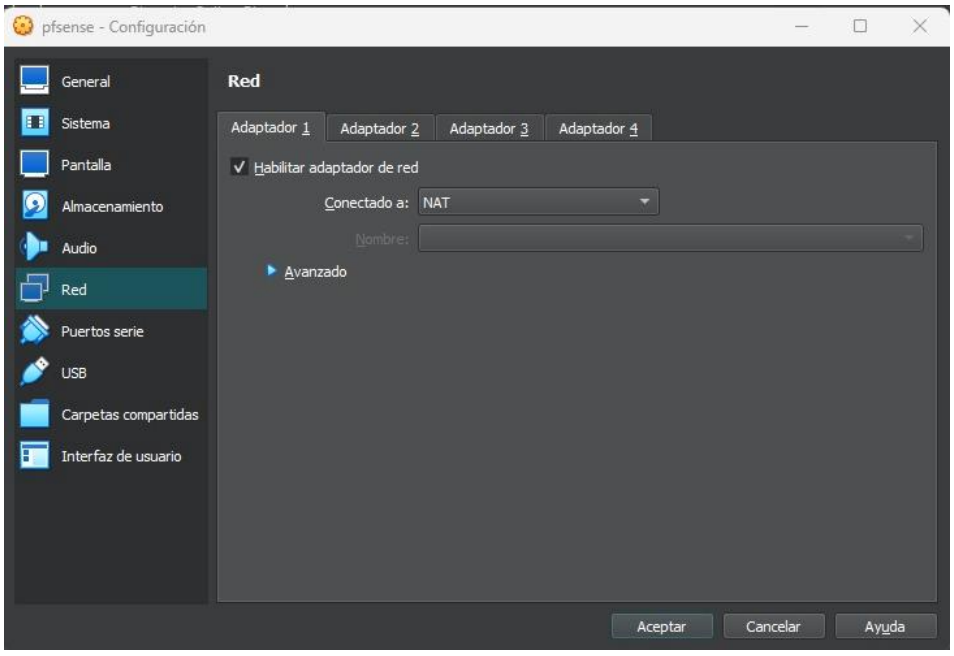
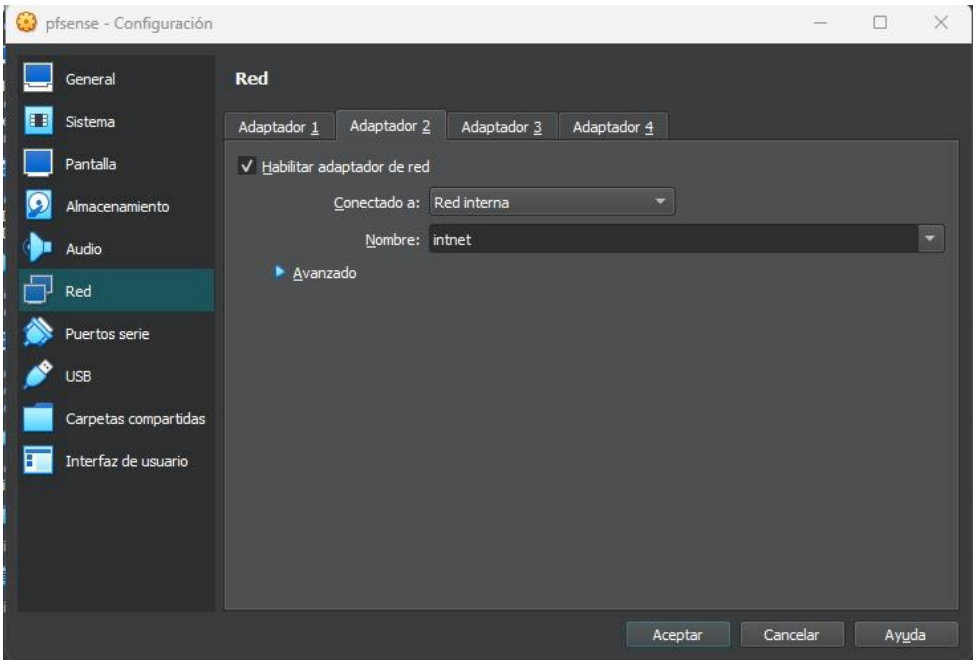


Figura 6

Pfsense Adaptador de Red 2 (Red Interna)



Maquina Servidor Wazuh

La característica de la máquina del servidor de wazuh es la siguiente:

- Memoria RAM: 8192 MB
- Adaptador 1: Red interna para la conexión entre la red local
- Almacenamiento: 6GB

Figura 7

Maquina Wazuh y sus especificaciones

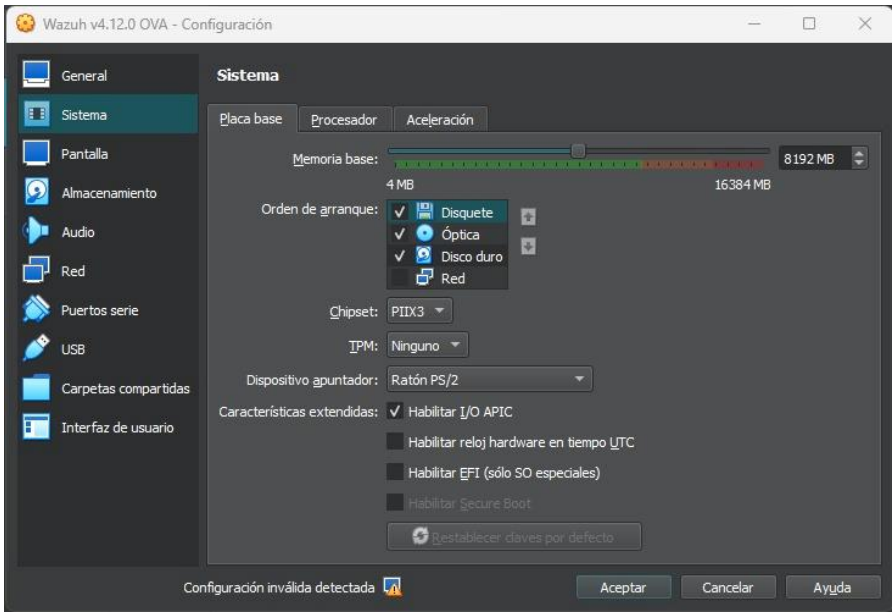
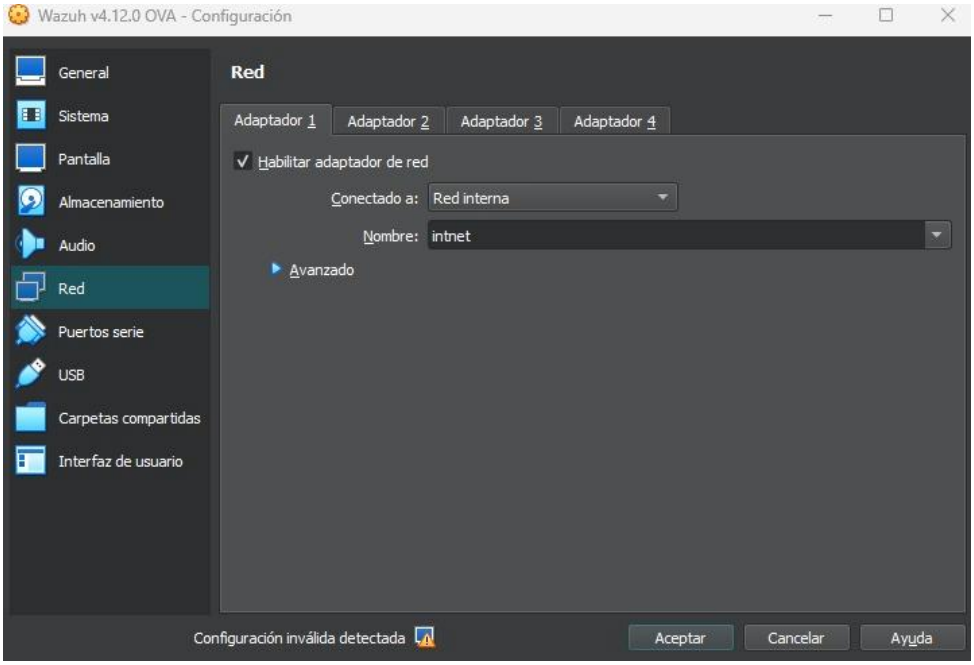


Figura 8

Wazuh Adaptador de Red 1 (Red Interna)



Maquina Windows 11

La característica de la máquina de Windows 11 es la siguiente:

- Memoria RAM: 4096 MB
- Adaptador 1: Red interna para la conexión entre la red local
- Almacenamiento: 50 GB

Figura 9

Maquina Windows 11 con sus especificaciones

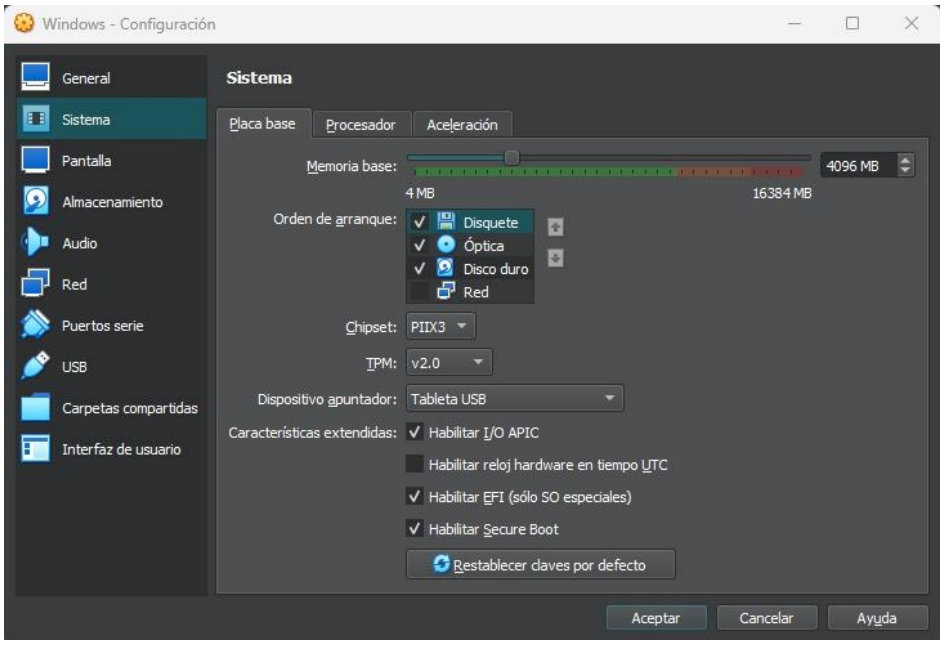
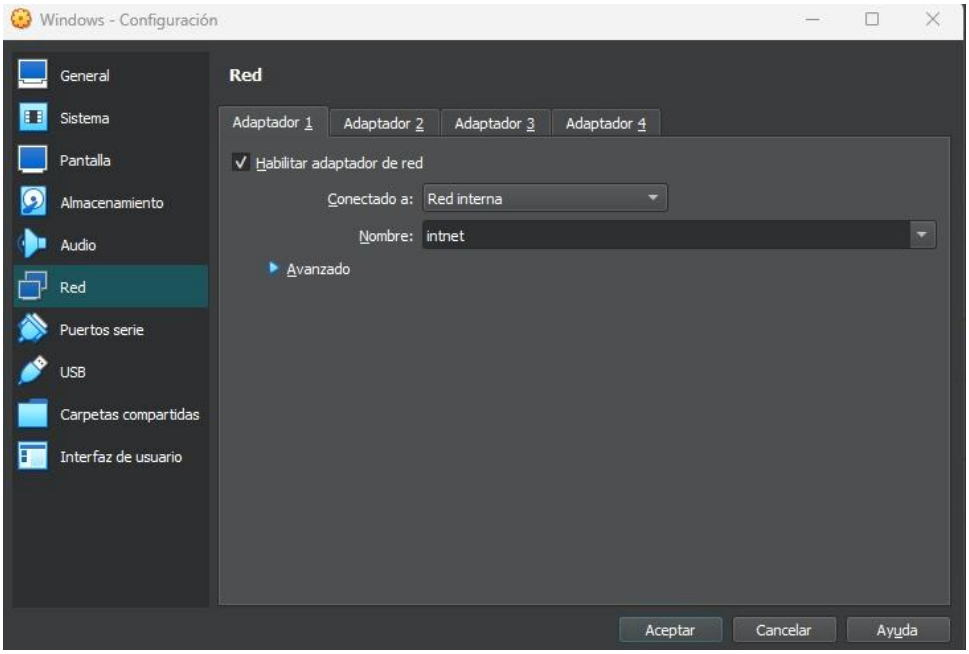


Figura 10

Windows 11 Adaptador de Red 1 (Red interna)



Maquina Windows 10

La característica de la máquina de Windows 10 es la siguiente:

- Memoria RAM: 2048 MB
- Adaptador 1: Red interna para la conexión entre la red local
- Almacenamiento: 6 GB

Figura 11

Maquina Windows 10 y sus especificaciones

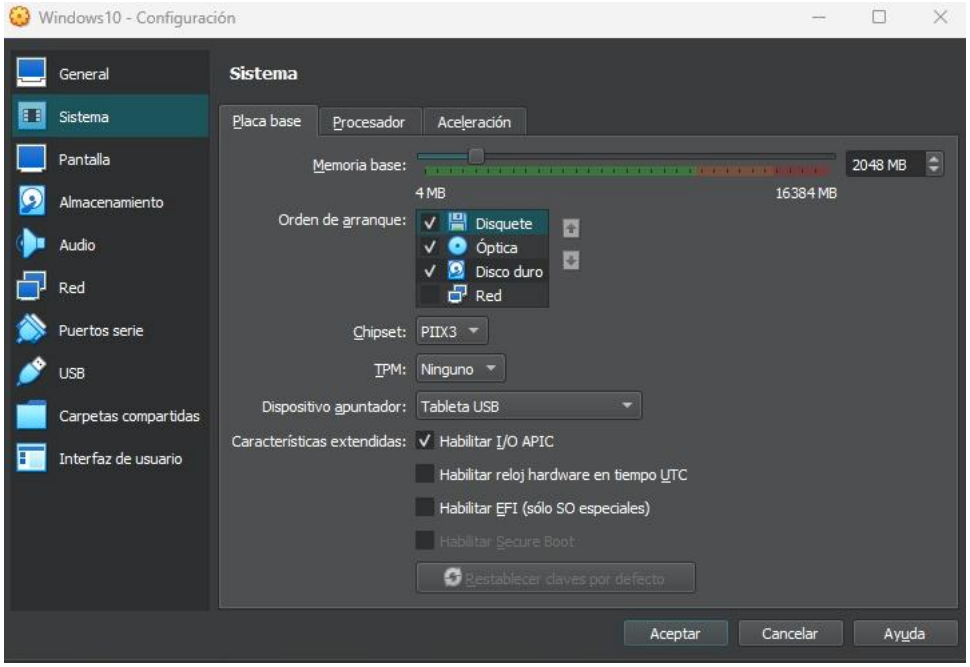
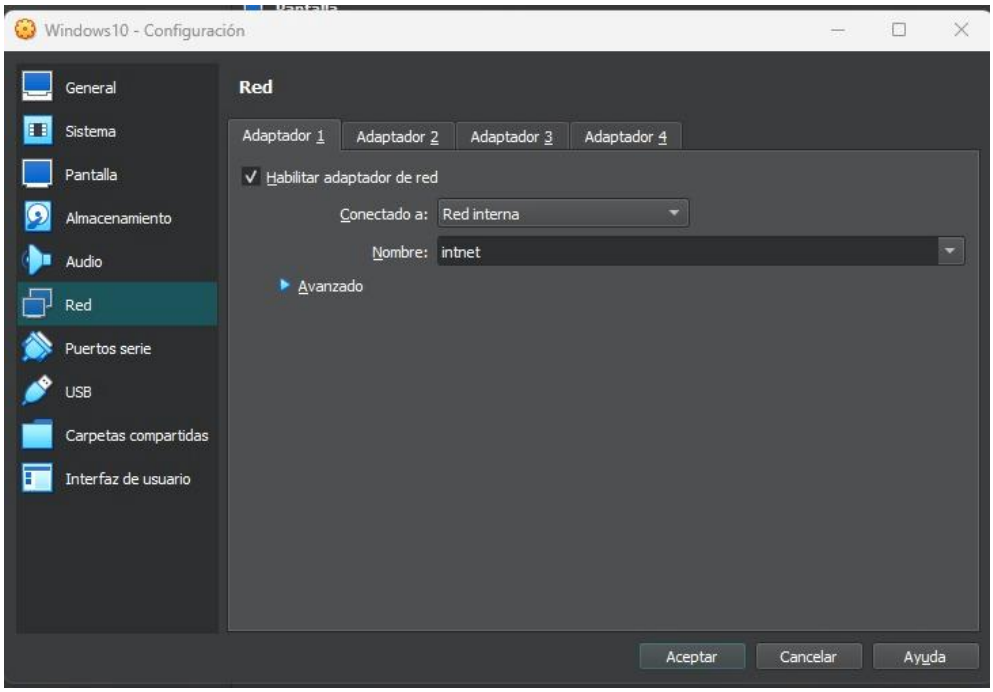


Figura 12

Windows 10 Adaptador de Red 1 (Red interna)



Maquina Kali Linux

La característica de la máquina de Kali Linux es la siguiente:

- Memoria RAM: 4096 MB
- Adaptador 1: Red interna para la conexión entre la red local
- Adaptador 1: Bridge/NAT realizando el cambio para hacer pruebas
- Almacenamiento: 6GB

Figura 13

Maquina Kali y sus especificaciones

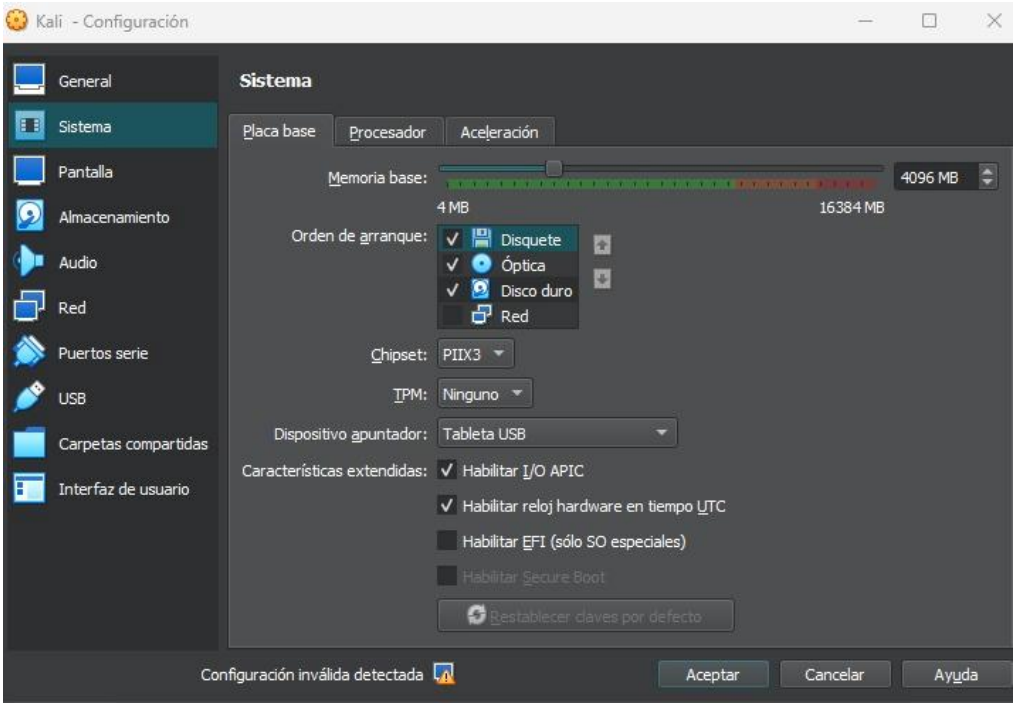
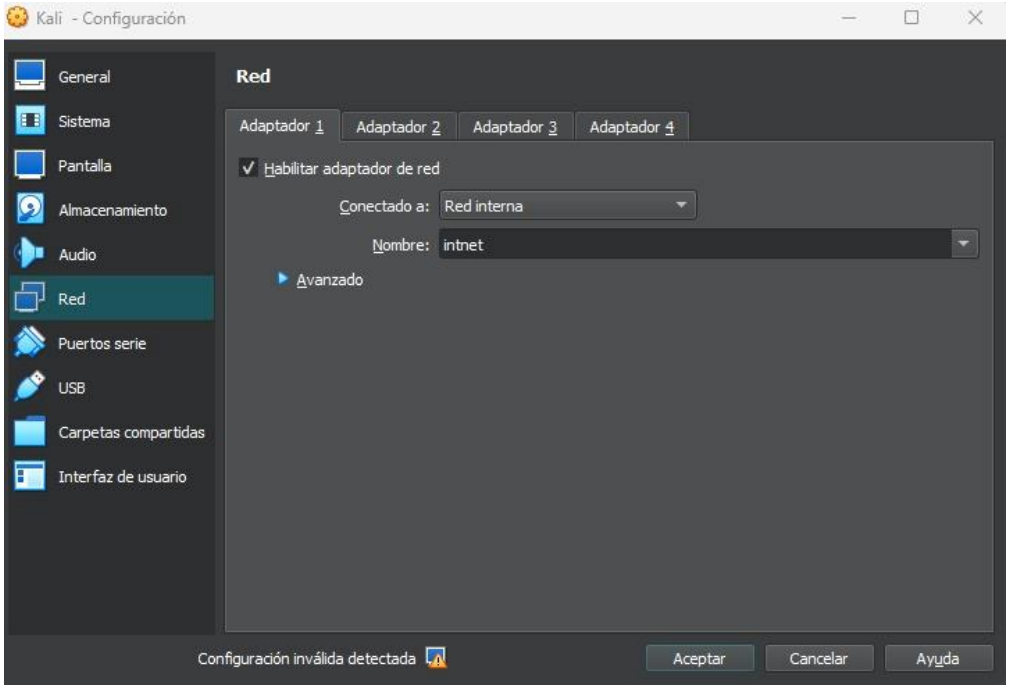


Figura 14

Kali Adaptador de Red 1 (Red interna)



Maquina Ubuntu

La característica de la máquina de Ubuntu es la siguiente:

- Memoria RAM: 4096 MB
- Adaptador 1: Red interna para la conexión entre la red local
- Almacenamiento: 5GB

Figura 15

Maquina Ubuntu y sus especificaciones

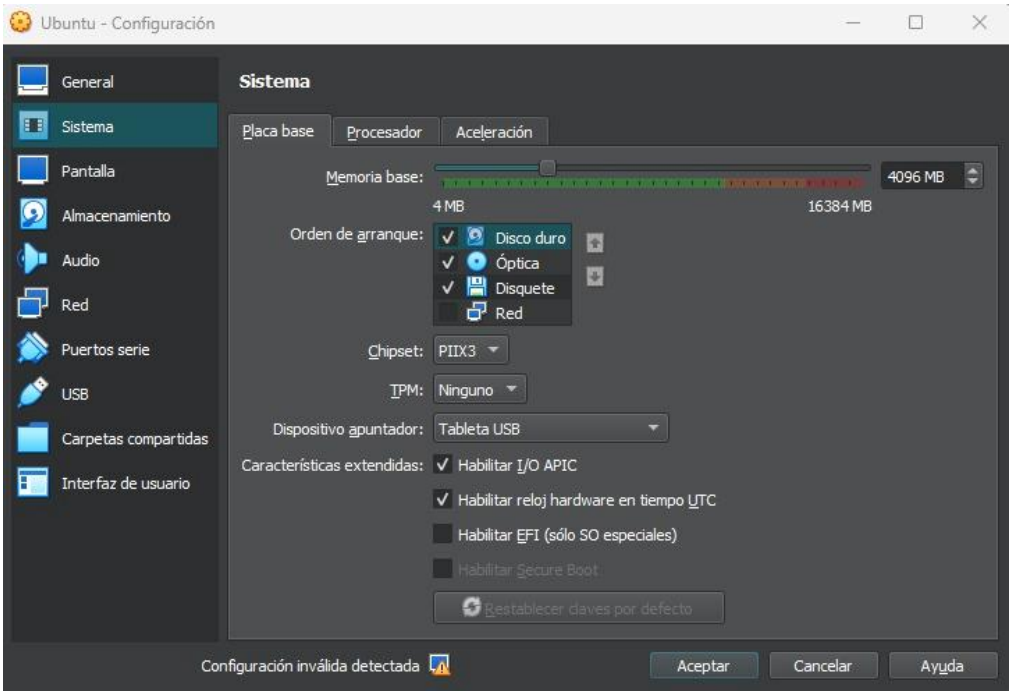
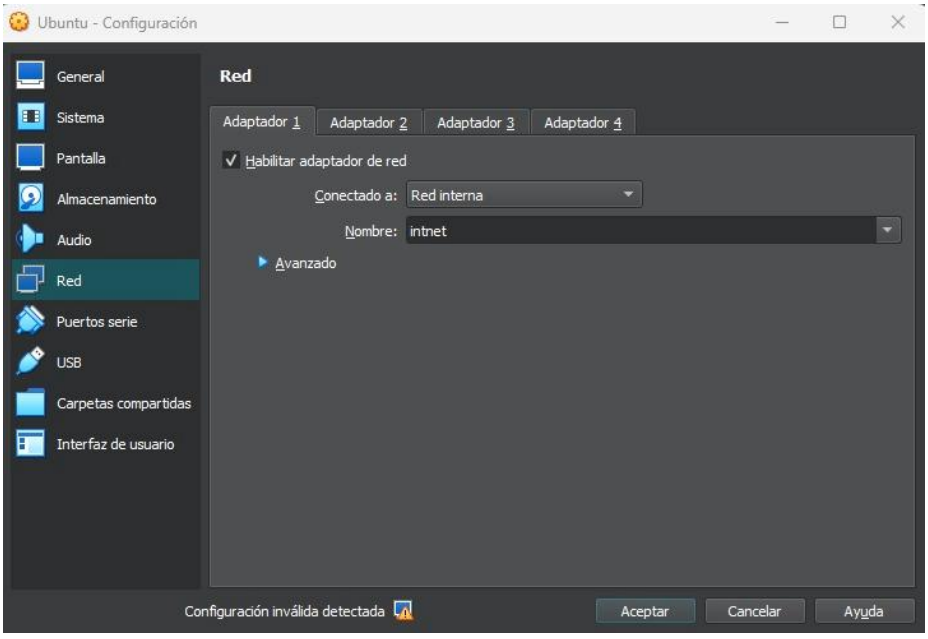


Figura 16

Ubuntu Adaptador de Red 1 (Red interna)



Firewall pfSense

La máquina virtual con Pfsense aparte de ser el firewall, posee integrado el IDS Suricata, este último cuenta con reglas las cuales fueron realizadas mediante un análisis y preparación de políticas de seguridad.

Tabla 2

Políticas de seguridad Implementadas

Políticas de seguridad
Políticas de Seguridad Interna y Perimetral de la red
Política de uso de internet
Política de monitoreo y detección de eventos de sistemas endpoints
Política de detección y prevención de intrusiones en la red

Las reglas del firewall detallan:

1- Anti-Lockout Rule es una regla que se crea automáticamente para evitar que el administrador se bloquee así mismo fuera de la interfaz web de administración del firewall.

2- Permitir dispositivos autorizados es una regla que permite ingresar el rango de direcciones IP que van a poder tener conexión a internet, siendo las IP de la red interna.

3- Bloquear dispositivos no autorizados es una regla de bloqueo que agrupa a las IP que fuera que no va a poder acceder a los recursos de la red interna y a internet.

4- Bloquear escaneo o tráfico de puertos maliciosos es una regla que permite bloquear las IP que realicen tráfico malicioso hacia la red interna.

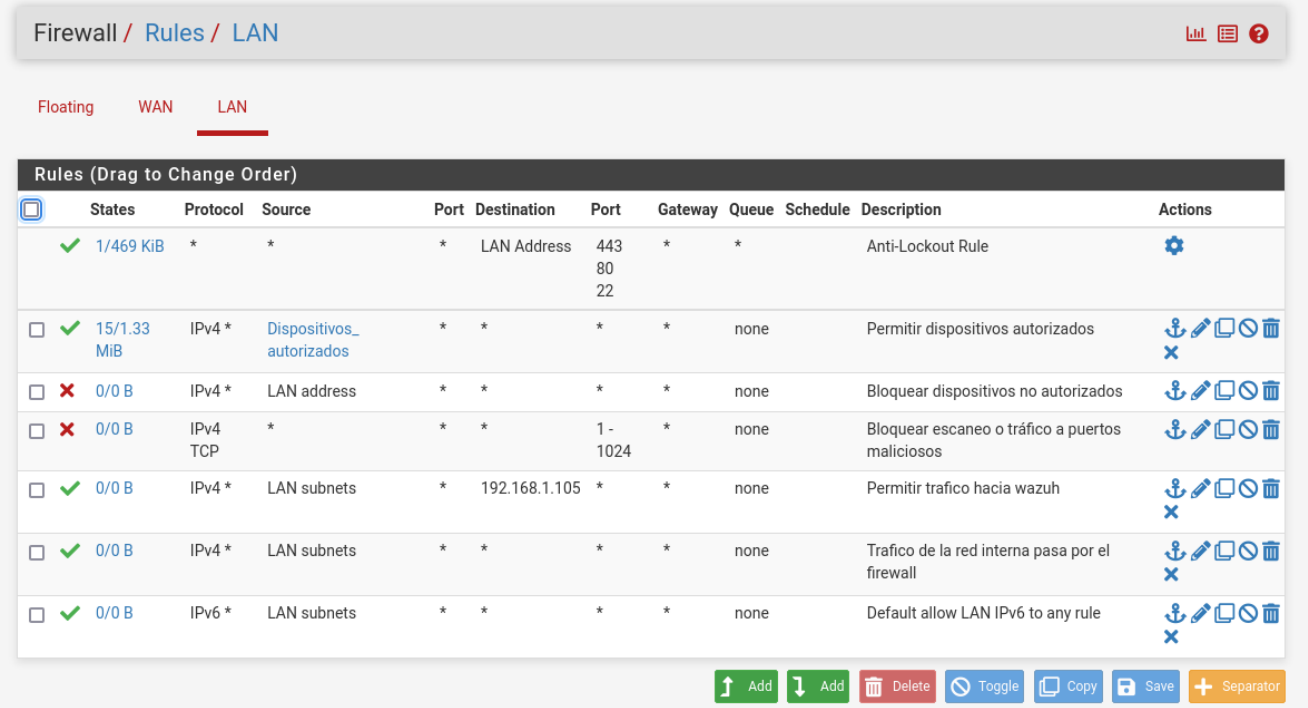
5- Permitir tráfico hacia Wazuh es una regla que va permitir la conexión de pfSense con Wazuh y va permitir el envio de logs

6- Tráfico de la red interna para por el firewall es una regla que permite que los equipos de la red interna pasen por el firewall para salida a internet

7- Default allow LAN IPv6 to any rule es una regla automática que se crea para las conexiones entre los equipos de la red interna con el firewall.

Figura 17

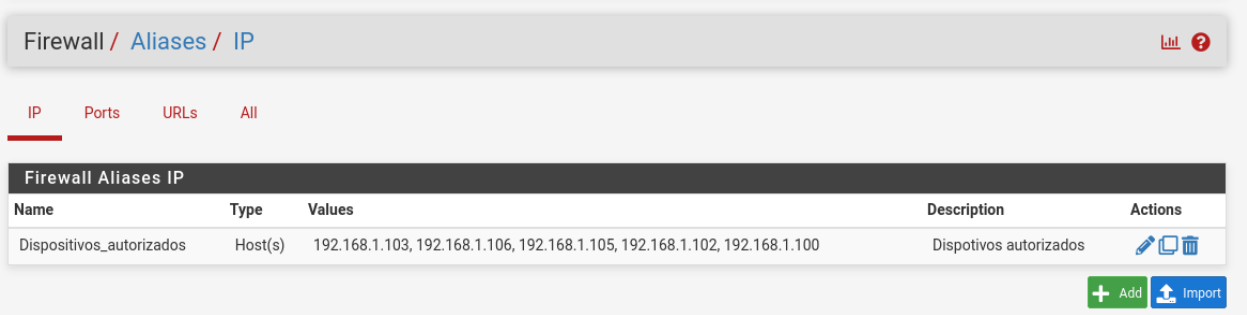
Reglas implementadas en el Firewall



En base a las reglas tenemos como resultado que unicamente las maquinas autorizadas podrán acceder a la red, en este caso los maquinas con Windows 11 y Windows 10 respectivamente, y las maquinas Ubuntu y Kali Linux para pruebas y acceso a los paneles de administración del firewall y Wazuh.

Figura 18

Direcciones IP reconocidas por el Firewall

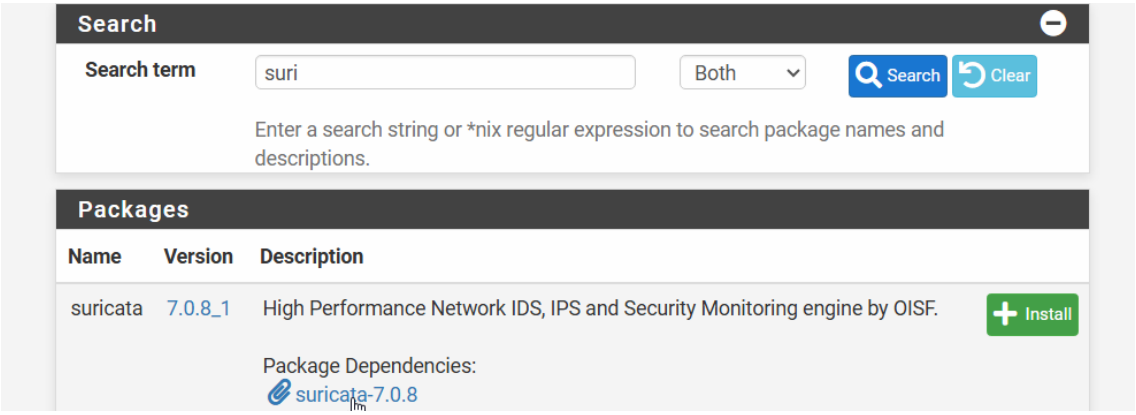


Suricata IDS

Para integrar Suricata dentro del firewall debemos instalarlo dentro de la sección de instalación de paquetes.

Figura 19

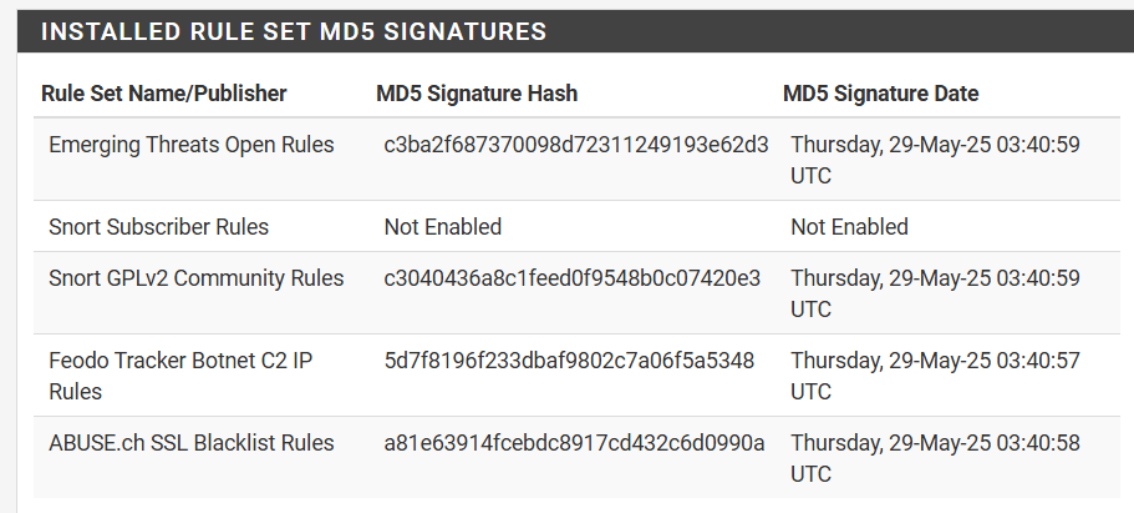
Primer paso para la instalación de Suricata



Adicional se deben descargar y colocar las reglas que pertenecen al IDS

Figura 20

Reglas implementadas en Suricata y su previsualización



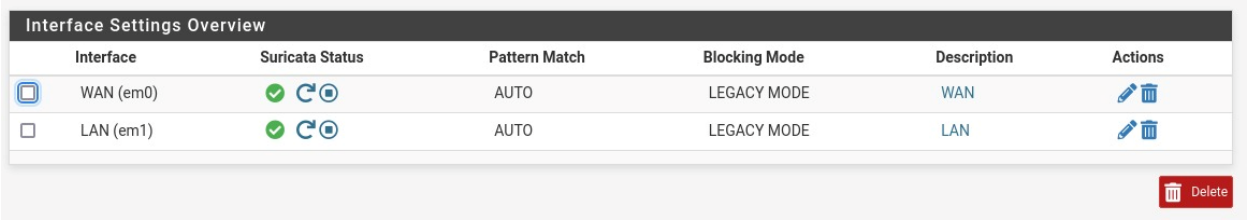
INSTALLED RULE SET MD5 SIGNATURES

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	c3ba2f687370098d72311249193e62d3	Thursday, 29-May-25 03:40:59 UTC
Snort Subscriber Rules	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	c3040436a8c1feed0f9548b0c07420e3	Thursday, 29-May-25 03:40:59 UTC
Feodo Tracker Botnet C2 IP Rules	5d7f8196f233dbaf9802c7a06f5a5348	Thursday, 29-May-25 03:40:57 UTC
ABUSE.ch SSL Blacklist Rules	a81e63914fcebdc8917cd432c6d0990a	Thursday, 29-May-25 03:40:58 UTC

Se crean dos interfaces, una es correspondientes a la red WAN para la conexión a internet y la otra es correspondiente a la red LAN, donde se encuentras las maquinas que forman parte de la red empresarial. La opción de ¨Legacy Mod¨ en el apartado Blocking Mode permite que el IDS bloquee automáticamente sitios maliciosos o que no van de acuerdo con las políticas establecidas.

Figura 21

Configuración de las interfaces de Suricata en Legacy Mode

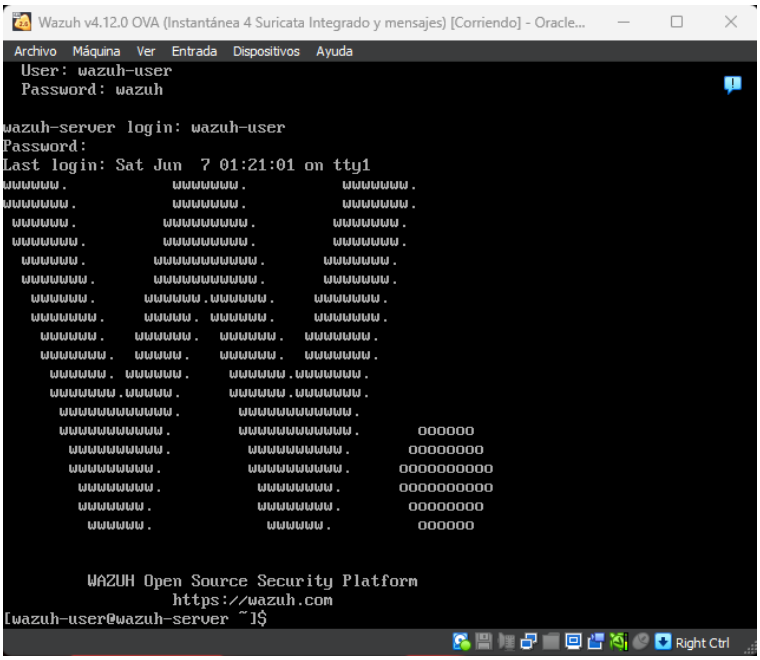


Agentes Wazuh

Wazuh Manager se encuentra instalado en la red interna, permitiendo el monitoreo a tiempo real de las amenazas, será integrado con las dos máquinas Windows 10 y 11.

Figura 22

Wazuh desplegado en Máquina Virtual

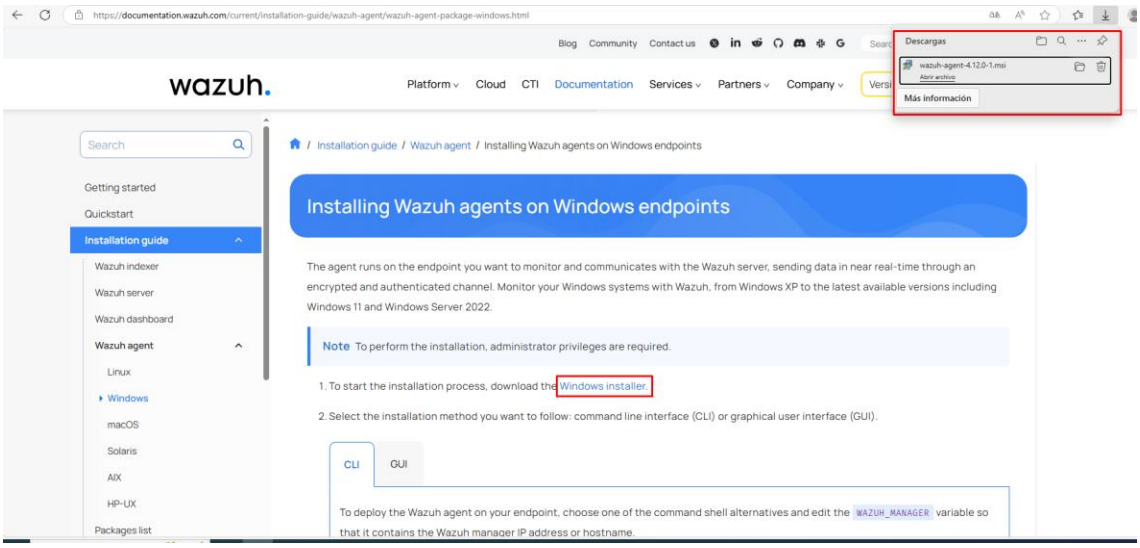


Instalación de agentes

Para instalar los agentes en Windows necesitamos ingresar https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html y procedemos a descargar el archivo del instalador del agente.

Figura 23

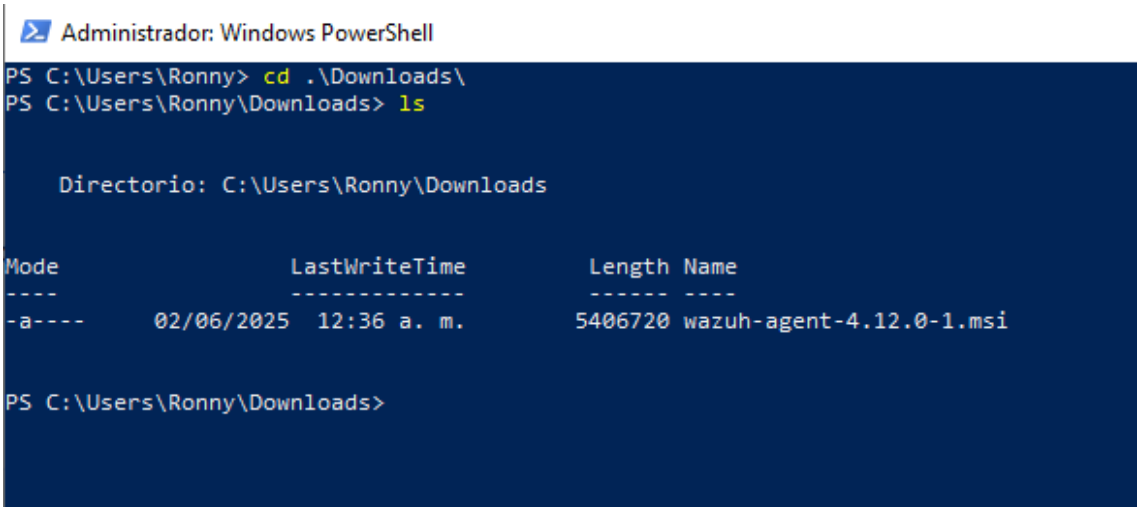
Documentación provista por parte de Wazuh



Ahora abrimos una consola powershell con permisos de administrador y nos dirigimos al directorio donde se descargó el archivo del agente

Figura 24

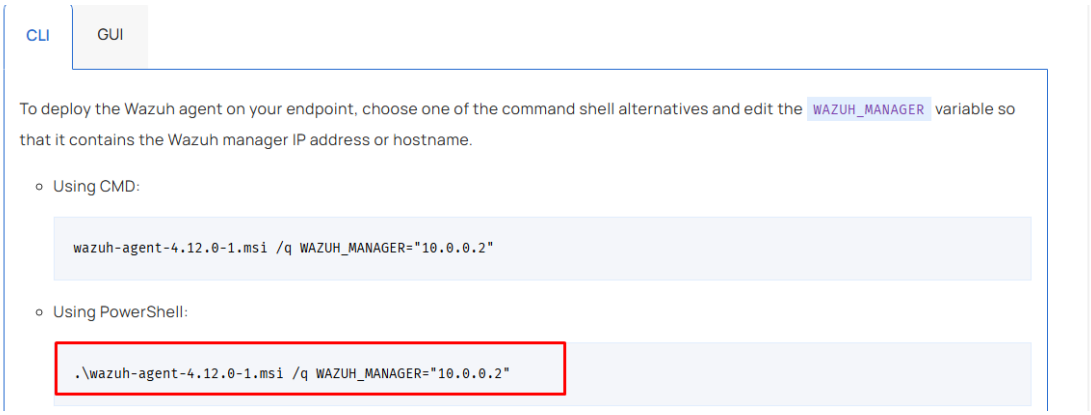
Directorio o ubicación donde se encuentra el agente



Ahora como nos menciona el sitio de Wazuh nos piden ingresar este comando .\wazuh-agent-4.12.0-1.msi /q WAZUH_MANAGER="Dirección IP del servidor Wazuh"

Figura 25

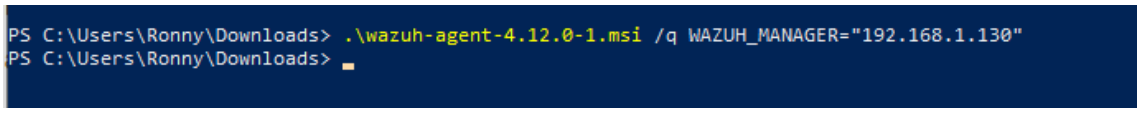
Despliegue de Wazuh a través de consola



Por motivo de ejemplificación de la instalación del agente Wazuh de uso la dirección 192.168.1.130 para el servidor Wazuh

Figura 26

Uso de la IP designada por motivo de ejemplificación



Ahora procedemos ejecutar el instalador el cual se encuentra en la dirección: C:\Program Files (x86)\ossec-agent, ahí ejecutamos agent-auth.exe -m y la IP del wazuh que es la 192.168.1.130

Figura 27

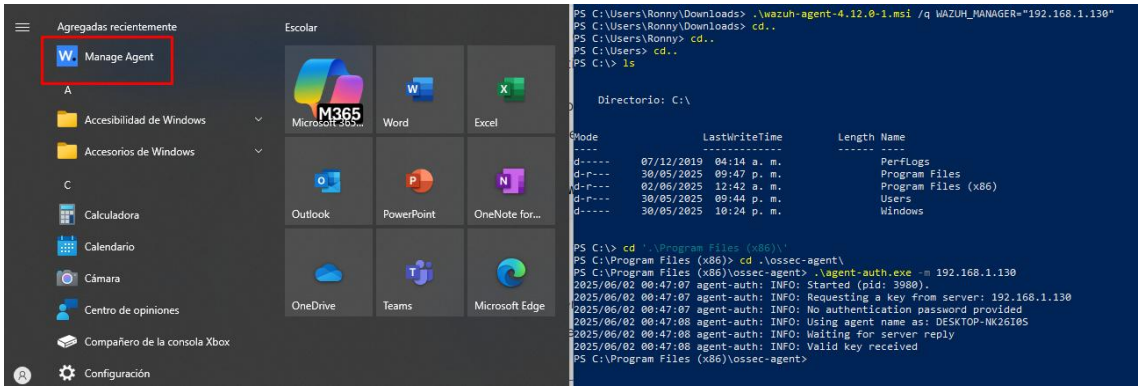
Instalación del agente mediante el siguiente comando

```
PS C:\> cd '.\Program Files (x86)\'
PS C:\Program Files (x86)> cd .\ossec-agent\
PS C:\Program Files (x86)\ossec-agent> .\agent-auth.exe -m 192.168.1.130
```

Una vez que este valida la clave, procedemos a ejecutar la aplicación Manage Agent

Figura 28

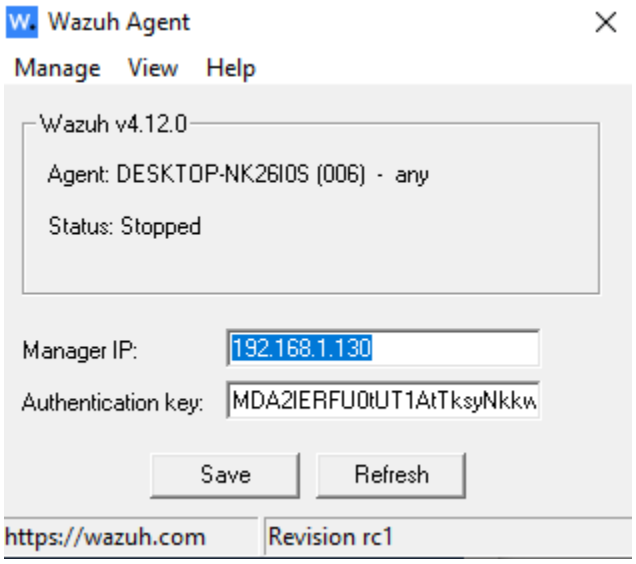
Despliegue de Manage Agent para visualizar la instalación



Donde al ejecutar nos dará ya el panel con la Ip del wazuh y la clave valida, donde le daremos en guardar.

Figura 29

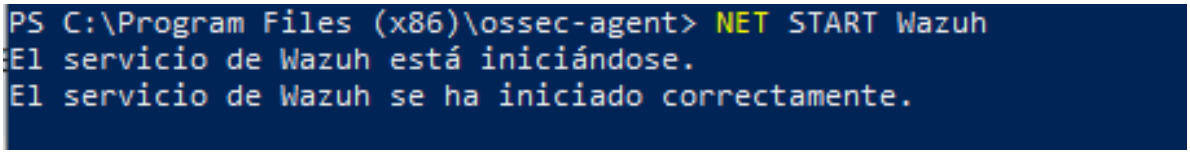
Ingreso de clave de autentificación del agente



Ahora ejecutamos el comando NET START Wazuh y nos sale que este iniciado correctamente

Figura 30

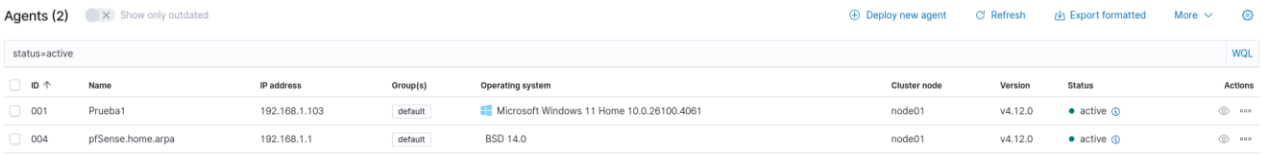
Comando para verificar que el agente se ejecuta de manera correcta



Los agentes se distribuyen como Endpoints en los equipos que componen el sistema, en este caso por cuestiones de memoria, se muestra una de las maquinas Windows y en este caso la integración de los logs de Suricata en el panel de control de Wazuh.

Figura 31

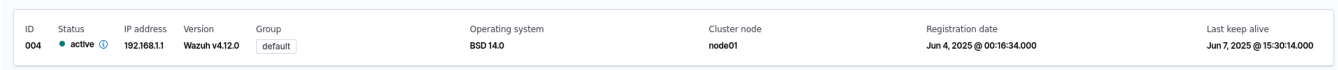
Endpoints correspondientes a Windows 11 y Pfsense



Al integrarse los logs de Suricata dentro Wazuh, podremos observar que aparece listado como un nuevo agente dentro del panel de control.

Figura 32

Visualización de la integración de Suricata con Wazuh

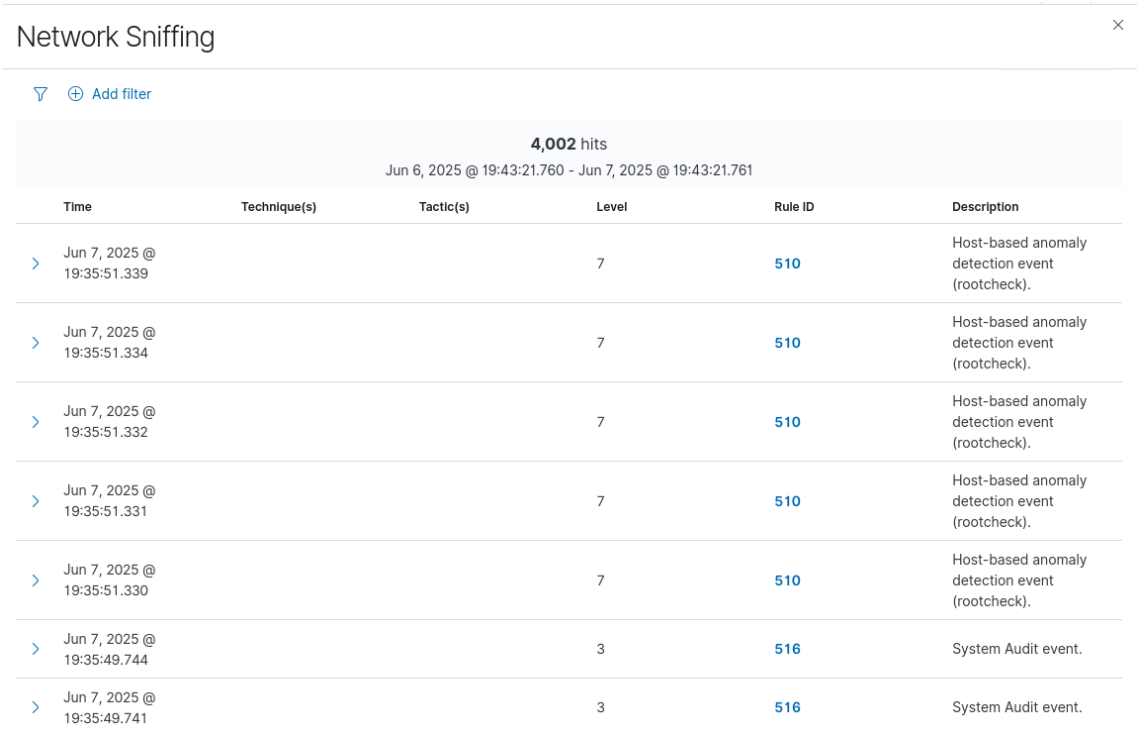


La ventaja que nos brinda Wazuh es que se adaptar a múltiples entornos, pasando por pequeñas hasta grandes y complejas infraestructuras empresariales.

Adicional complementa la seguridad brindada tanto de PfSense y de Suricata, desarrollando un sistema de defensa integral.

Figura 33

Logs comunes dentro de la interfaz de Wazuh



Para habilitar la visualización de logs de Suricata es necesario activar la opción de creación de logs en el panel de control de Suricata y modificar el archivo de configuración de Wazuh con las siguientes líneas. Para ellos nos dirigimos a la dirección /Var/ossec/etc/ossec.conf y configuramos la etiqueta de ossec_config

Figura 34

Archivo de configuración donde se agregan una dirección para almacenar logs de suricata

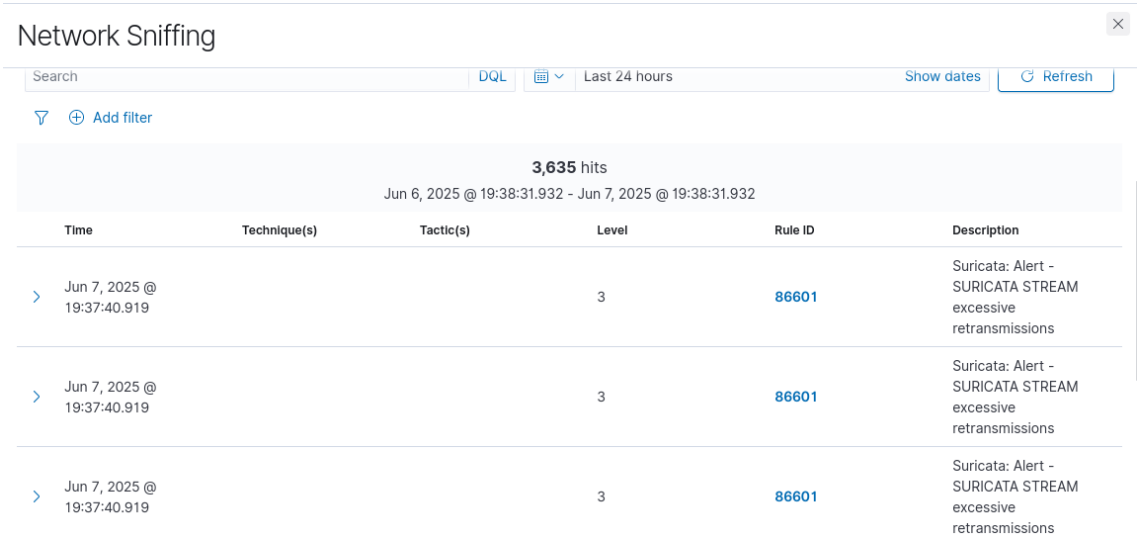
```
<ossec_config>
  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>
</ossec_config>
```

De esta manera los logs generados por Suricata serán visibles dentro de la interfaz del panel de control de los agentes. Por lo tanto, el IDS identifica el tráfico sospechoso mientras Wazuh procesos esos eventos para la creación de alertas más detalladas.

Y por supuesto facilitar la administración de seguridad desde una interfaz más proactiva, además de ayudar a cumplir con los estándares de seguridad en respuesta a incidentes.

Figura 35

Logs de Suricata visibles dentro del panel de control de Wazuh



Notificaciones por correo

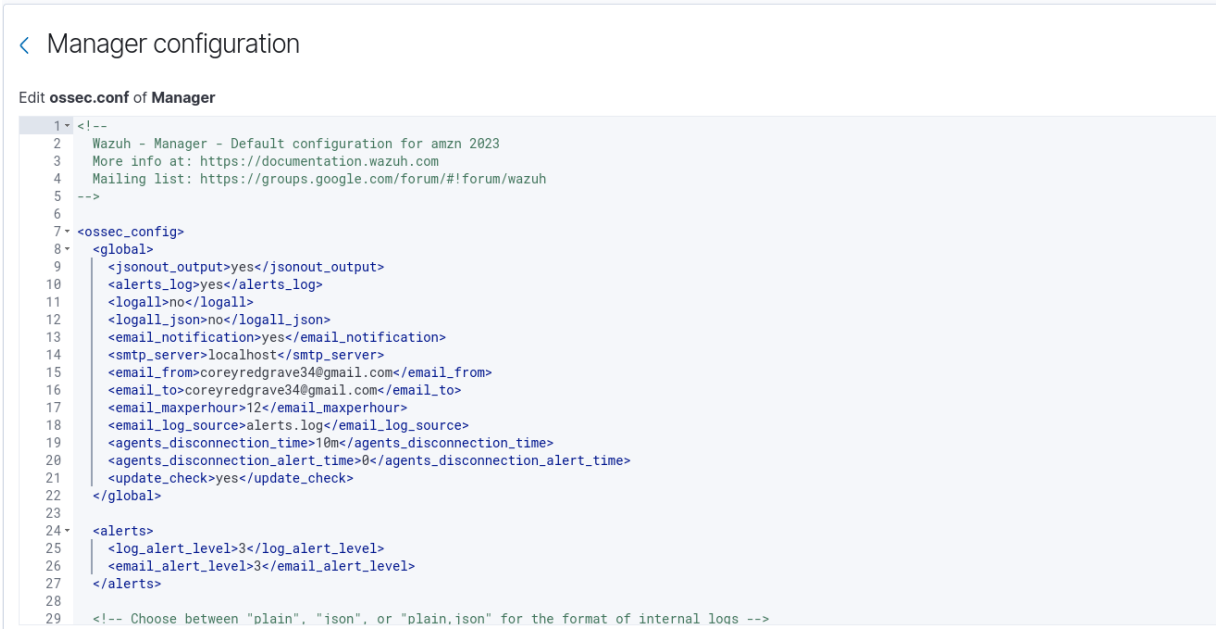
Finalmente se ha configurado el agente Wazuh para que sea capaz de enviar notificaciones en base a las alertas, esto permite recibir alertas desde cualquier lugar, sin necesidad de acceder directamente al SIEM.

Permite obtener un historial de eventos, esto resulta útil para las auditorias y posteriores revisiones.

Para realizar la configuración correcta, se debe

Figura 36

Habilitar las notificaciones por email (línea 13)

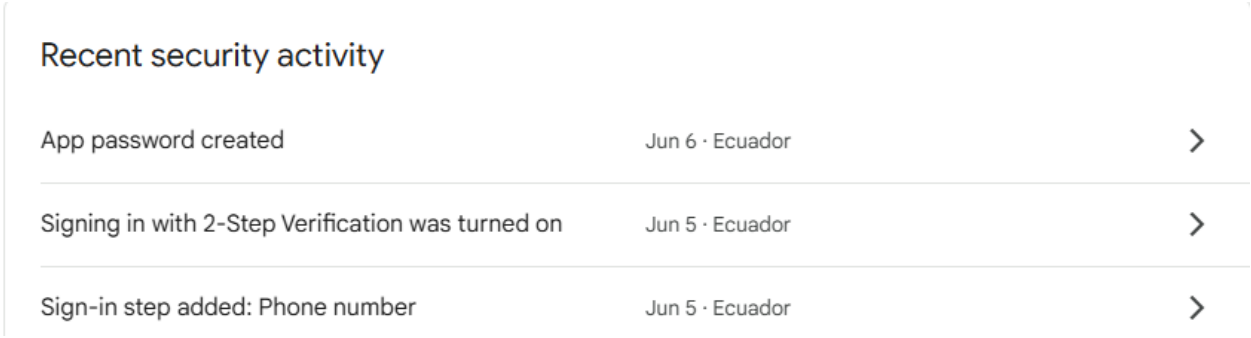


El servidor SMTP deberá configurarse de acuerdo a las políticas de correo electrónico en cuestión, estas pueden variar dependiendo si se trata de Gmail, Outlook, Yahoo etc.

Dispondremos de localhost ya que haremos uso de Postfix como servidor de transmisión dentro del administrador.

Figura 37

Creación de la contraseña de app dentro del correo (verificación en dos pasos requerida)



Iniciamos la instalación de Postfix.

Figura 38

Comando para la instalación de Postfix en la consola de Wazuh

Debemos verificar que el archivo de configuración que se encuentra en la ruta /etc/postfix/main.cf contenga la información correcta del servidor.

Figura 39

Verificar que los datos dentro del archivo de configuración sean correctos

```
relayhost = [smtp.gmail.com]:587
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
smtp_tls_CAfile = /etc/ssl/certs/thawte_Primary_Root_CA.pem
smtp_use_tls = yes
compatibility_level = 2
```

Al verificar que la información esta correcta, debemos lanzar los siguientes comandos en la consola, en la sección mypassword debemos colocar la contraseña que fue provista por la app del correo electrónico.

Figura 40

Comandos para ingresar en la consola de Wazuh y activar las alertas por correo

```
# echo [smtp.gmail.com]:587 wazuhtest@testserver.com:mypassword > /etc/postfix/sasl_passwc
# postmap /etc/postfix/sasl_passwd
# chmod 400 /etc/postfix/sasl_passwd

# chown root:root /etc/postfix/sasl_passwd /etc/postfix/sasl_passwd.db
# chmod 0600 /etc/postfix/sasl_passwd /etc/postfix/sasl_passwd.db

# systemctl restart postfix
```

De esta manera obtenemos la siguiente estructura de comandos que debemos implementar y por último reiniciar el agente para que los cambios sean visibles.

De esta manera los mensajes de alerta llegaran vía correo electrónico.

Figura 41

Comandos adaptados para la configuración del correo designado

```
echo [smtp.gmail.com]:587 coreyredgrave34@gmail.com:exaxbnhdijxhjpit > /etc/postfix/sasl_passwd
postmap /etc/postfix/sasl_passwd
chmod 400 /etc/postfix/sasl_passwd
```

Figura 42

Servidor Localhost y correo designado en la configuración de alertas de Wazuh

Capítulo IV

Análisis de resultados

Pruebas de concepto

Para realizar la evaluación del SIEM automatizado, se realizó diversas pruebas que permitirán evaluar tanto el rendimiento, precisión y la eficacia de las respuestas ante diferentes políticas de seguridad planteadas. Esto tiene por objetivo comprobar la integración de herramientas de pfSense, Suricata y Wazuh.

Se analizó los resultados obtenidos en el panel de control de Wazuh, para verificar la capacidad de gestionar eventos de seguridad, la correlación de registros y las gráficas detalladas.

Se ejecutará una prueba de escaneo de puertos, se evaluó cómo se comporta Suricata al identificar este evento y como Wazuh es capaz de procesar la alerta.

Se verifico la capacidad de bloqueo automático por parte de Suricata, mediante las reglas de filtrado y como el sistema no tiene acceso a esos sitios.

Estas pruebas permiten demostrar el funcionamiento del sistema en un entorno controlado y medir la eficacia de las herramientas configuradas, asegurando un monitoreo proactivo.

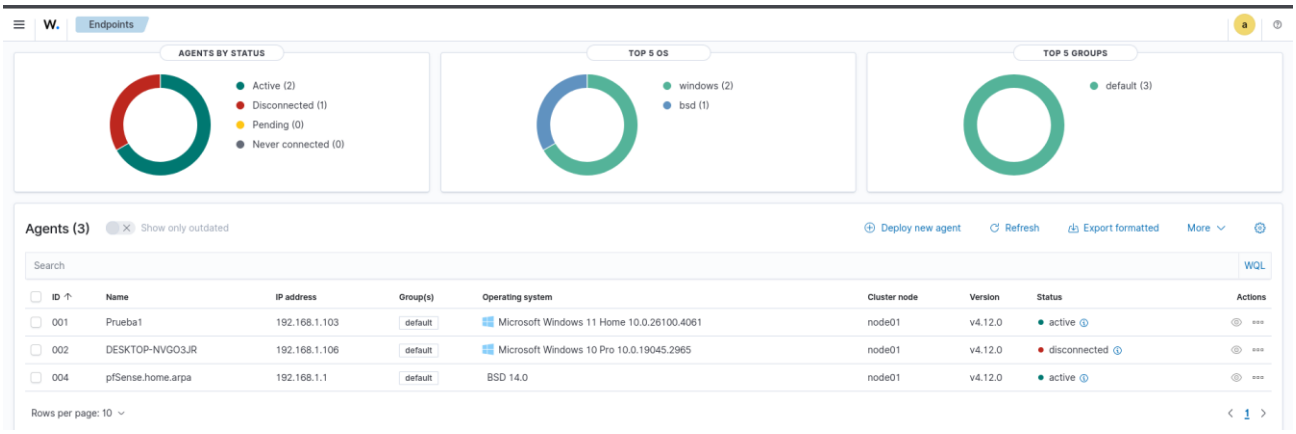
Panel de control de Wazuh

En esta prueba verifico el funcionamiento del panel de control de Wazuh, evaluando su capacidad para monitorear eventos de seguridad a tiempo real. Se explorarán varios módulos y sus respectivas gráficas, su correlación de eventos y su respectiva integración con Suricata y como los logs aparecen dentro de la interfaz.

En la gráfica observamos que dos agentes se encuentran activos, el agente por parte de pfsense y el agente de Windows 11, se muestra el otro agente de la máquina de Windows 10 aunque esta desconectada.

Figura 43

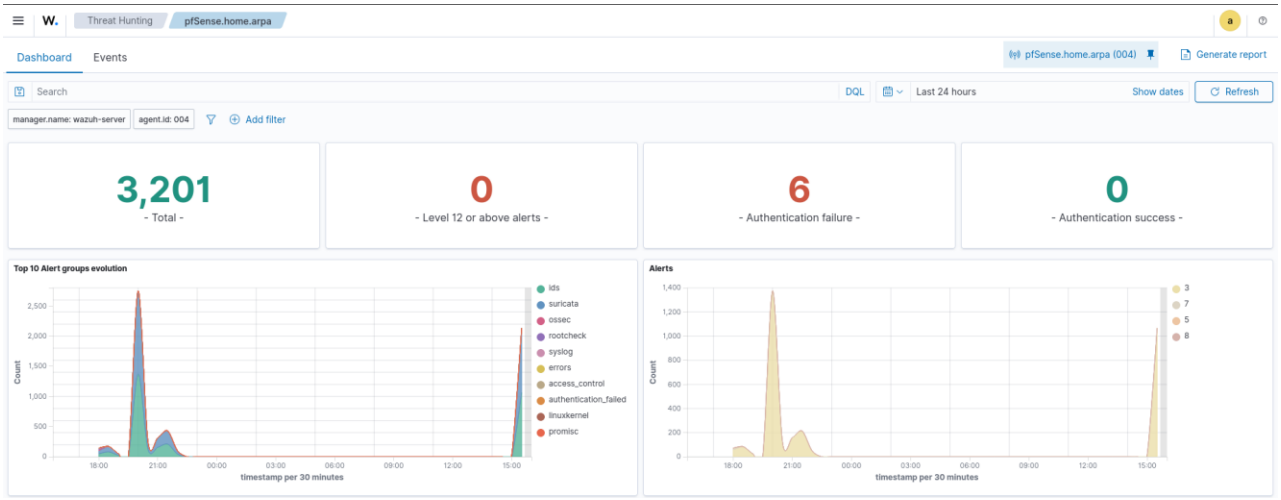
Panel principal de Wazuh desplegado



Esta grafica nos muestra la distribución de los logs y de su procedencia, también destaca varias autentificaciones fallidas, lo cual es muy útil para detectar posibles intentos de obtención de credenciales y accesos no autorizados.

Figura 44

Autentificaciones fallidas captadas por Wazuh



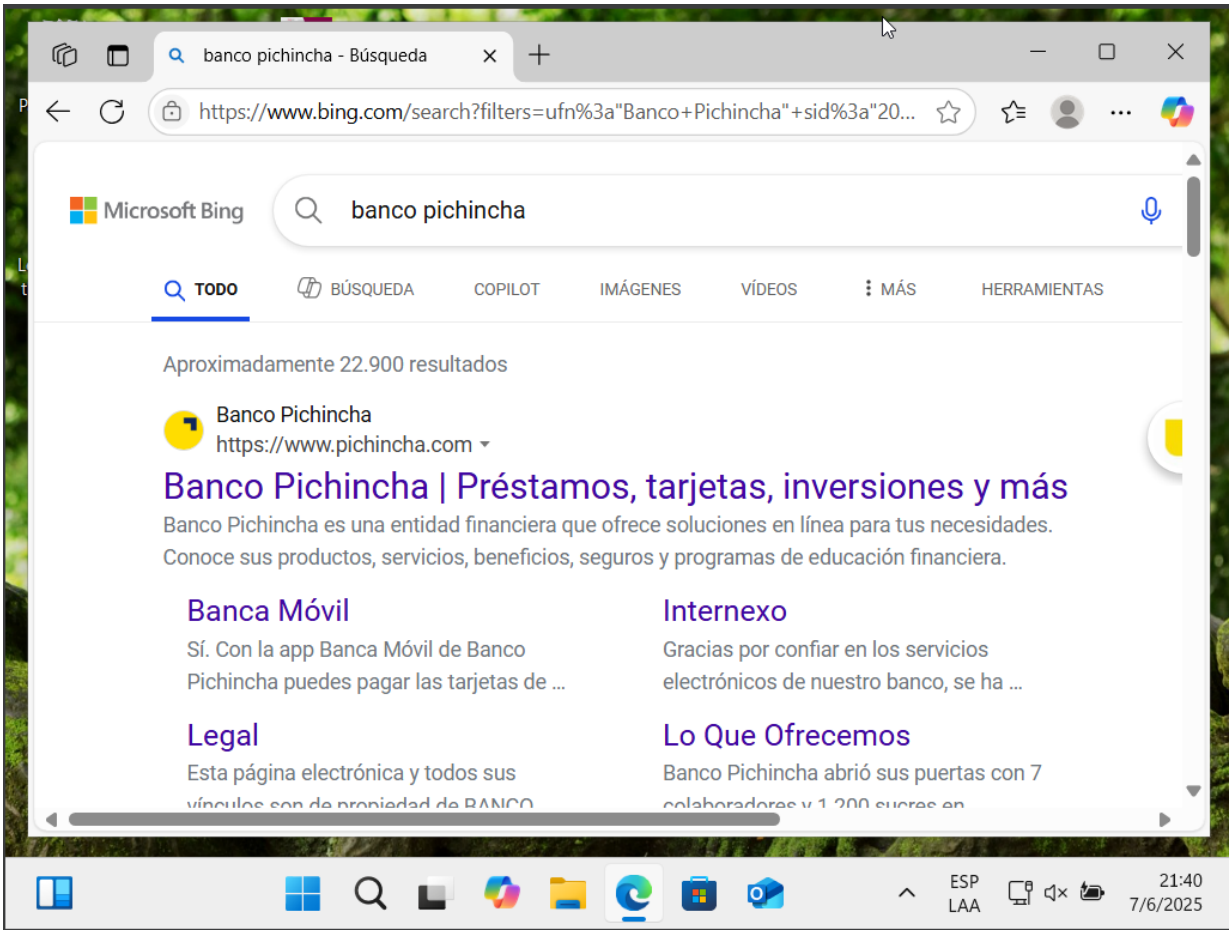
Bloqueo de equipos no perteneciente a la red

Se realizó pruebas para garantizar que el firewall de pfSense, de la mano con Wazuh pueda identificar y bloquear equipos no autorizados a la red. Mediante las políticas implementadas se restringirá el acceso a equipos con direcciones IP no registradas y la respuesta del sistema antes intentos de conexión de dispositivos externos.

Se hizo uso de dos equipos para comprobar este punto, en primero se encuentra la maquina con Windows 11 con IP 192.168.1.103, esta última se encuentra registrada dentro del firewall como parte de la red y se puede acceder a internet y navegar libremente.

Figura 45

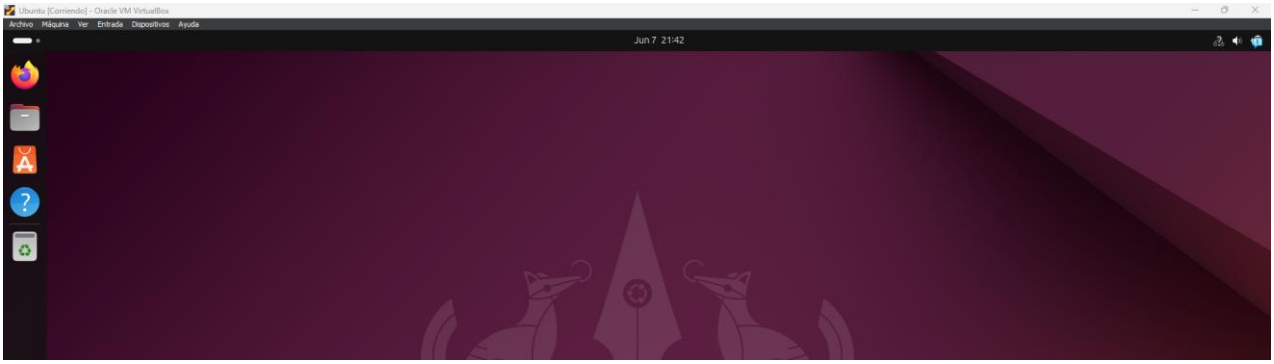
Navegación de la maquina Windows con IP reconocida por el Firewall



Por otro lado, la maquina Ubuntu con IP 192.168.1.100 ha sido eliminada de los equipos reconocidos en el firewall, y como tal ha perdido acceso a internet y por lo tanto no tiene conectividad y no se puede navegar.

Figura 46

Navegación por la maquina Ubuntu sin conexión a red al no estar reconocida en el Firewall



Pruebas de escaneo de puertos

Se ejecutará un escaneo de puertos mediante el comando Nmap, esto último con el propósito de verificar la detección del sistema de seguridad, la manera de como Suricata es capaz de registrar estos eventos en sus logs y como aparecen en Wazuh.

Desde la máquina de Kali Linux podemos realizar un escaneo de puertos.

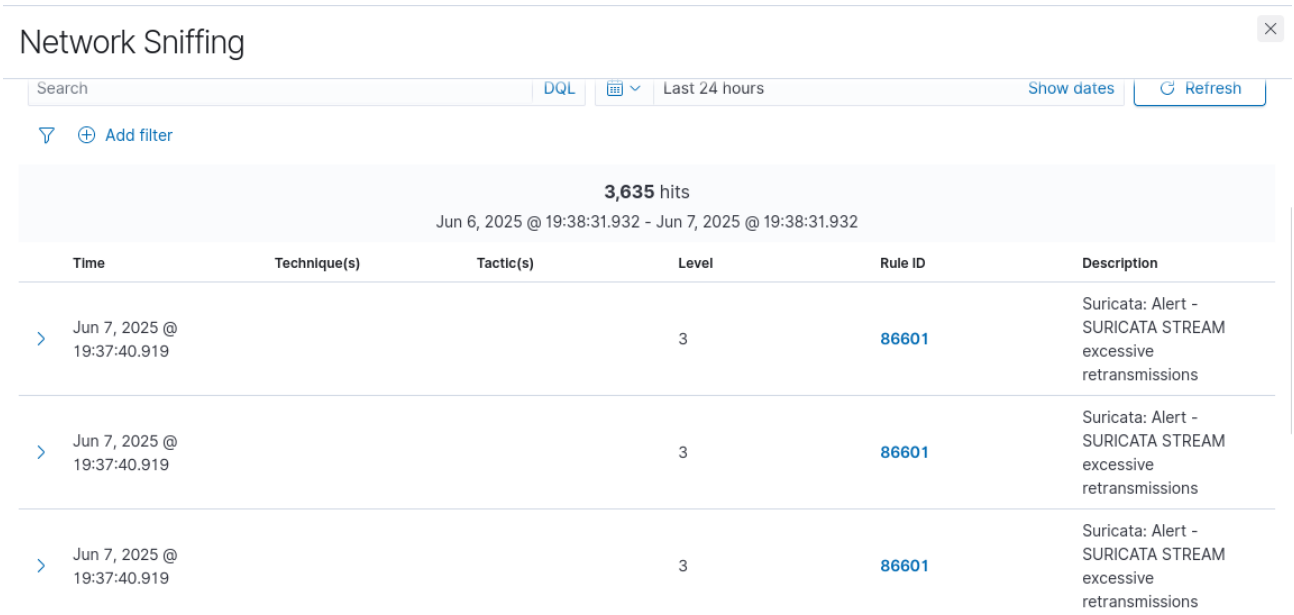
Figura 47

Escaneo de puertos desde la maquina Kali Linux

Y como observamos en la parte de logs que llegan a través de Suricata, el escaneo es visible dentro del panel de control de Wazuh.

Figura 48

Escaneo siendo visible dentro de la interfaz de Wazuh



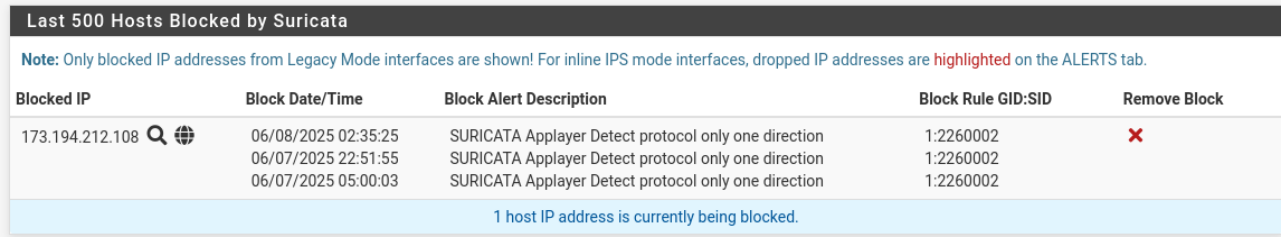
Bloqueo automático de sitios por parte de Suricata

En esta prueba se ejecutará una simulación de tráfico hacia direcciones previamente identificas como amenazas o que no van de acuerdo con las políticas implementadas.

Suricata bloqueara automática sitios maliciosos o que no se encuentren en una lista de paso, esto último en base a las políticas implementadas en el proyecto.

Figura 49

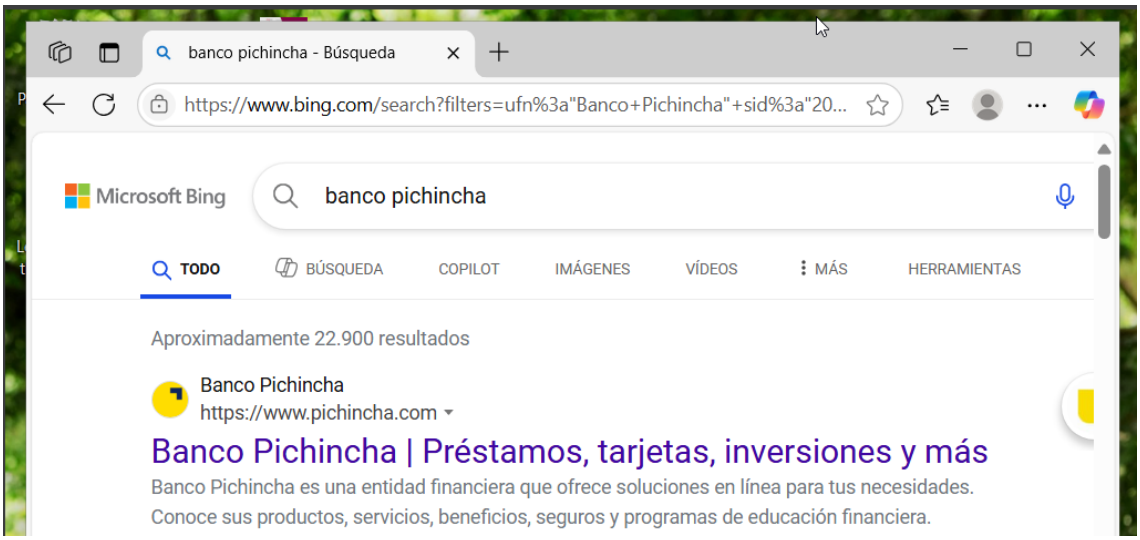
Detección y bloqueo automático de sitios por parte de Suricata



Sitios web como entidades bancarias, a los propios navegadores Bing, Google o Mozilla se encuentra habilitados.

Figura 50

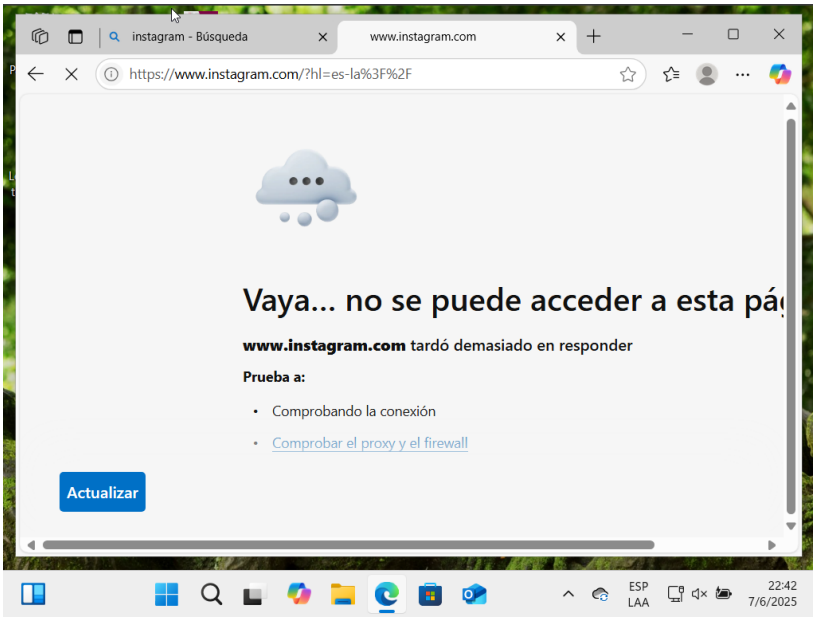
Navegación correcta desde los diferentes equipos



No obstante redes sociales tales como Instagram se encuentran bloqueadas y no es posible acceder a ellas.

Figura 51

Redes sociales se encuentran bloqueadas según las políticas planteadas



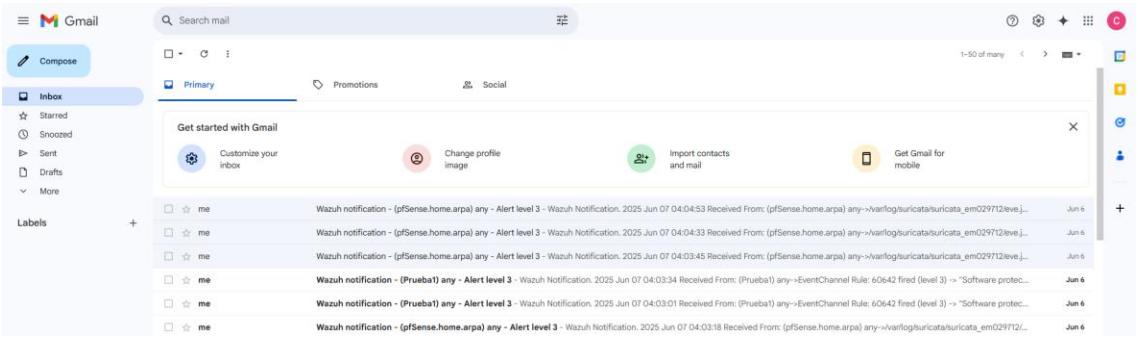
Notificaciones por correo

Esta prueba garantizara que el sistema pueda notificar a los responsables de seguridad de manera eficiente y efectiva, facilitando la gestión de incidentes y fortaleciendo el entorno monitoreado.

Las alertas llegan al correo designado para las pruebas.

Figura52

Alertas y notificaciones llegan mediante correo electrónico



Capítulo V

Conclusiones, Trabajo Futuro y Recomendaciones

Conclusiones

Se logró diseñar una topología de red virtualizada que simula en entorno empresarial rea, se lo realizo integrando un firewall, en conjunto con sistema de detección y prevención de intrusos (IDS/IPS), SIEM y estaciones de trabajos, esto permitió generar un entorno controlado. La implementación de Wazuh como SIEM automatizado demostró ser una solución efectiva y viable para entornos empresariales, al proporcionar monitoreo continuo, detección temprana de amenazas y respuesta automatizada ante incidentes. Su naturaleza open-source lo convierte en una alternativa económica sin comprometer funcionalidad.

El firewall pfSense fue configurado de manera correcta con Suricata, permitiendo establecer políticas y reglas de seguridad perimetral efectivas y personalizadas que demuestran una capacidad óptima para detectar y bloquear el tráfico malicioso en tiempo real. La automatización de la respuesta a incidentes contribuye significativamente a la reducción del tiempo de detección (MTTD) y respuesta (MTTR). Esto minimiza el impacto de las amenazas y fortalece la resiliencia operativa de la organización frente a ciberataques.

La instalación y configuración del servidor Wazuh SIEM, en conjunto con la integración de agentes en los equipos de la red, permitió una recolección de logs y el monitoreo centralizado de los eventos de seguridad interna, mejorando la capacidad de respuesta ante posibles intrusiones. Wazuh facilita el cumplimiento de normativas internacionales de seguridad, como ISO/IEC 27001, PCI DSS y NIST, al integrar módulos de control, auditoría, correlación de eventos y gestión de logs, aspectos fundamentales en auditorías y gestión del riesgo.

Se establecieron políticas de seguridad orientas al monitoreo de endpoints y al control del uso de internet, lo cual fortaleció el área de seguridad interna de la red y mejoro la capacidad de respuesta a intrusiones.

Se automatizo la generación de reglas y notificaciones correctamente, estas notificaciones son dirigidas al personal de seguridad, lo que agiliza el proceso de detección temprana de eventos críticos, disminuyendo tiempos de reacción ante incidentes.

Se evaluó el sistema implementado, donde concluimos que la implementación del sistema mejora la detección, análisis y respuesta ante incidentes de seguridad informática en un entorno empresarial. La respuesta proactiva mediante scripts personalizados y políticas automatizadas eleva el nivel de madurez del área de seguridad informática, permitiendo mitigar amenazas antes de que generen daño y elevando el estándar de protección digital empresarial.

Recomendaciones

Capacitar continuamente al personal encargado de la seguridad de la información, no solo en el uso y administración de Wazuh, sino también en metodologías de gestión de incidentes, análisis forense y normativas de cumplimiento.

Realizar pruebas periódicas de intrusión (pentesting) y simulaciones de incidentes que permitan validar la efectividad de las reglas de correlación, los mecanismos de alerta y las respuestas automatizadas configuradas en Wazuh.

Mantener actualizada la base de firmas, reglas y scripts de respuesta del sistema, con el fin de adaptarse a las nuevas amenazas cibernéticas emergentes. Se recomienda apoyarse en fuentes como MITRE ATT&CK y feeds de amenazas para enriquecer la inteligencia del sistema.

Ampliar la implementación del sistema a todos los activos críticos de la empresa, incluyendo endpoints, servidores, redes y dispositivos IoT, asegurando una cobertura integral y homogénea del monitoreo.

Integrar Wazuh con plataformas suricata permitió fortalecer la orquestación de incidentes complejos, optimizando la escalabilidad y la automatización en tiempo real.

Evaluar periódicamente los indicadores clave de rendimiento (KPIs) como el tiempo promedio de respuesta, número de incidentes detectados, falsos positivos, y eficiencia en contención, a fin de medir el retorno de inversión (ROI) y mejorar el sistema continuamente.

Fomentar una cultura organizacional de ciberseguridad, involucrando no solo al área técnica sino también a usuarios finales, a través de políticas claras, simulacros de seguridad, campañas de concienciación y protocolos internos bien definidos.

Bibliografía

Delgado, J. C., Muñoz, G. F., Padilla, B. A., & Quiñónez, V. H. (2025). Ciberseguridad y Protección de Datos Personales: Desafíos y Perspectivas. Obtenido de Revista Cientifica GADE: https://revista.redgade.com/index.php/Gade/article/view/642

Gartner. (08 de 05 de 2024). Magic Quadrant for Security Information and Event Management. Obtenido de Gartner: https://www.gartner.com/reviews/market/security-information-event-management

Lara, F. R., Miranda, M. F., Alejando, S. B., & Marcillo, J. L. (27 de 11 de 2024). Polo de Conocimiento. Obtenido de http://polodelconocimiento.com/ojs/index.php/esPol. Con. (Edición núm. 102) Vol. 10, No 1Enero2025, pp. 2233-2250ISSN: 2550 -682XDOI: https://doi.org/10.23857/pc.v10i1.8807Análisis del rendimiento de soluciones SIEM de código abierto: https://polodelconocimiento.com/ojs/index.php/es/article/view/8807/pdf

lazarus Alliance. (11 de 12 de 2024). Obtenido de La importancia de SOAR para el cumplimiento en ecosistemas de ciberseguridad avanzados: https://lazarusalliance.com/es/the-importance-of-soar-for-compliance-in-advanced-cybersecurity-ecosystems/

Nacher, J. D. (13 de 03 de 2024). gesdataconsulting. Obtenido de ISO 27032 directrices para la ciberseguridad: https://gesdataconsulting.es/iso-27032#:~:text=La%20ISO%20IEC%2027032%20no%20solo%20se%20centra%20en%20la,operativa%20en%20entornos%20digitales%20desafiantes.

Perez, M. J. (04 de 02 de 2025). Universidad Politecnica de Catalunya . Obtenido de Sistema de Gestión de Incidentes de Ciberseguridad: https://upcommons.upc.edu/handle/2117/427314

Reid, C. (2024). Magic Quadrant for Security Information and Event Management. Obtenido de Splunk.

Ricard, A. C. (01 de 12 de 2024). Universidad Nacional Abierta y a Distancia UNAD. Obtenido de Capacidades técnicas, legales y de gestión para equipos blue team y red team: https://repository.unad.edu.co/bitstream/handle/10596/68713/Capacidades_Tecnicas_legales_y_de_gestion_de_equipos_para_blueteam_y_readteam_.pdf?sequence=1&isAllowed=y

Ruiz, J. M. (2025). IMPLEMENTACIÓN DE UN SOC MODULAR. Obtenido de https://openaccess.uoc.edu/server/api/core/bitstreams/1b630697-7e88-40d9-bbf3-0f353d3400fa/content

Suarez, D., & Avila, A. (10 de 2021). ista de Una forma de interpretar la seguridad informática. Obtenido de http://repository.lasallista.edu.co:8080/ojs/index.php/jet/article/view/1015/1072

Tomás Guerra, J. (2019). Monitorización de seguridad con Wazuh. Obtenido de http://hdl.handle.net/10609/107166

Torres, G. (2021). ¿Qué es un virus informático? Obtenido de Guía sobre virus informáticos: https://www.avg.com/es/signal/what-is-a-computer-virus

Wazuh. (2024). Security Information and Event Management. Obtenido de https://wazuh.com/platform/siem/

Ö‡ütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016a). Analysis of personal information security behavior and awareness. Computers and Security, 56, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Ö‡ütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016b). Analysis of personal information security behavior and awareness. Computers and Security, 56, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Park, J.-Y., & Huh, E.-N. (2020). A Cost-Optimization Scheme Using Security Vulnerability Measurement for Efficient Security Enhancement. https://doi.org/10.3745/JIPS.02.0128

Quiroz, S., & Macias, D. (2017). Seguridad en informática: consideraciones Computer security: considerations. 3(5), 676–688. https://doi.org/10.23857/dom.cien.pocaip.2017.3.5.agos.676-688

Rodriguez Rincón, E. Y., & García Valdés, Á. M. (2018). Metodologías de Ingeniería Social. 65.

Soriano, M. (n.d.). Seguridad en redes y seguridad de la información. Retrieved July 12, 2021, from http://improvet.cvut.cz

Suárez, D., & Ávila, A. (2015, September 10). Vista de Una forma de interpretar la seguridad informática. http://repository.lasallista.edu.co:8080/ojs/index.php/jet/article/view/1015/1072

Torres, G. (2021, May 6). ¿Qué es un virus informático? | Guía sobre virus informáticos | AVG. https://www.avg.com/es/signal/what-is-a-computer-virus

Warikoo, A. (2014). Proposed Methodology for Cyber Criminal Profiling. Information Security Journal, 23, 172–178. https://doi.org/10.1080/19393555.2014.931491

Wilcox, H., & Bhattacharya, M. (2016). A framework to mitigate social engineering through social media within the enterprise. Proceedings of the 2016 IEEE 11th Conference on Industrial Electronics and Applications, ICIEA 2016, 1039–1044. https://doi.org/10.1109/ICIEA.2016.7603735

Ye, Z., Guo, Y., Ju, A., Wei, F., Zhang, R., & Ma, J. (2020). A risk analysis framework for social engineering attack based on user profiling. Journal of Organizational and End User Computing, 32(3), 37–49. https://doi.org/10.4018/JOEUC.2020070104

Zhou, Q., Shahidehpour, M., Alabdulwahab, A., & Abusorrah, A. (2020). A Cyber-Attack Resilient Distributed Control Strategy in Islanded Microgrids. IEEE Transactions on Smart Grid, 11(5), 3690–3701. https://doi.org/10.1109/TSG.2020.2979160

Apéndices

Acceso a los archivos (Ova)

Para la respectiva revisión y comprobación de la implementación de Sistema de detección se adjunta el siguiente link para obtener las máquinas virtuales:

https://drive.google.com/drive/folders/1KIxXDM_2Ku8oTgxqymjB3EQwAvb9j50P?usp=sharing