UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES: Ing. Guarango Guacho Daniel Humberto

Ing. Morales Panta Wellington Xavier

Ing. Vallejo Pacheco Fabricio Andrés

Ing. Zuñiga Vivanco Luis Alberto

TUTOR: Ing. Ronie Stalin Martínez Gordon, Mtr

Desarrollo de un entorno controlado de laboratorio en Máquinas Virtuales (Windows / Linux) para la detección y mitigación de vulnerabilidades en servicios de Banca Online desarrollados en .NET utilizando SIEM basados en herramientas Open Source para monitorizar y responder a incidentes en tiempo real.

Aprobación del Tutor

Yo, Ronie Stalin Martínez Gordon, certifico que conozco los autores del presente trabajo siendo la responsable exclusiva tanto de su originalidad y autenticidad, como de su contenido.

Ing. Ronie Stalin Martínez Gordon, Mtr

DIRECTOR DE TESIS

Declaración de Autoría del Trabajo de Titulación

Nosotros, Guarango Guacho Daniel Humberto, Morales Panta Wellington Xavier, Vallejo Pacheco Fabricio Andrés, Zuñiga Vivanco Luis Alberto 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, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Ing. Guarango Guacho Daniel Humberto

Ing. Morales Panta Wellington Xavier

Ing. Vallejo Pacheco Fabricio Andrés

Ing. Zuñiga Vivanco Luis Alberto

Dedicatoria

Principalmente dedico mi tesis a mis hermanas y sobrinos que son el pilar fundamental de mi vida como Rosy, Myriam, Emy, Pame, Dome, Paúl y especialmente a Christian que con su apoyo y confianza me motivaron para poder lograr terminar esta etapa importante de mi vida profesional.

Daniel Humberto Guarango Guacho

Dedicatoria

A Dios, por ser mi guía y fortaleza en cada paso de este camino. A mi abuela (Carmen), quien es como una madre para mí, y a mi madre (Maribel) y padre (Eduardo), por su amor incondicional y apoyo inquebrantable, por su cuidado y guía desde cada propósito y proyecto de mi vida. A mis hermanos (Priscila, Edu) y sobrinos (Xander, Jissel), por ser una fuente constante de inspiración y alegría.

Y especialmente, al amor de mi vida (Paola), por darme la fuerza y el impulso para seguir mejorando cada día sin su ayuda y apoyo no hubiera llegado a este objetivo.

Morales Panta Wellington Xavier

Dedicatoria

Dedico mi tesis principalmente a Dios, por darme la fuerza necesaria para culminar esta meta. A mi esposa por no soltar mi mano en ningún momento y darme ánimos durante este camino. A mis hijas que son la fuente de inspiración y el motor para seguir avanzando y poder generar orgullo en ellas. A mis padres y suegros, por todo su amor y ayuda, por motivarme a seguir hacia adelante. También a mis hermanos, por brindarme su apoyo moral y espero les sirva de ejemplo de que todo se puede lograr. Y, finalmente, a los que creyeron en mí, familia, tíos, primos, abuelita, que fueron fuente de impulso para lograr este objetivo.

Vallejo Pacheco Fabricio Andrés

Dedicatoria

A mis padres y mi hermano quienes han sido mi fortaleza para seguir siempre adelante.

Luis Alberto Zuñiga Vivanco

Agradecimiento

Agradezco principalmente a Dios, a mis hermanas y sobrinos que para llegar hasta esta etapa no ha sido nada fácil, y les doy gracias a todos por ser mi soporte y así poder superar todos los obstáculos presentados.

Daniel Humberto Guarango Guacho

Agradecimiento

Quiero expresar mi más profundo agradecimiento al amor de mi vida, Paola, por ser mi apoyo incondicional. Su impulso constante me ha motivado a seguir preparándome, y en esta travesía llena de retos y desafíos, ha sido mi fuerza cuando la carga se volvió pesada. Sin su ayuda y apoyo, no habría alcanzado este objetivo.

Agradezco también a mi familia, quienes han confiado en mí y han puesto toda su fe en que seguiré mejorando. Gracias a su amor y apoyo, he podido crecer tanto profesional como personalmente. Su confianza en mi capacidad para superar obstáculos y su aliento continuo han sido fundamentales para mi éxito.

Morales Panta Wellington Xavier

Agradecimiento

En primer lugar agradezco a Dios que me ha dado fuerza, tiempo, salud, trabajo, amor, ganas de superación y generó todas las posibilidades para poder emprender este viaje que en este momento está finalizando, por darme una gran esposa (Estefanía) que es mi fortaleza mi apoyo y que nunca me soltó de la mano, por tener cerca a mis hijas (Andreith, Andreina, Ariana) que son el equilibrio que se requiere para nivelar estudios, trabajo, familia, que son la alegría y mi fuente de inspiración, por tener vivos a mis padres y suegros que son un apoyo y ayuda día a día que siempre están cuando los necesito, por tener cerca a mis hermanos, abuelita, tíos, primos, por rodearme de gente maravillosa que cree en mí.

A todos mis docentes por su empeño y esfuerzo en enseñarme día a día y transmitir los conocimientos necesarios para poder emprender este camino con ganas y dedicación por aprender más y superarme a mí mismo.

Vallejo Pacheco Fabricio Andrés

Agradecimiento

A mis padres por los valores inculcados que han sido la base de la persona que soy ahora.

Luis Alberto Zuñiga Vivanco

Resumen

La ciberseguridad se ha convertido en una preocupación primordial en la era digital, especialmente con la creciente dependencia de los servicios en línea para operaciones críticas lo que ha elevado la banca en línea a un componente esencial de la vida cotidiana, facilitando transacciones financieras a millones de usuarios globalmente. Sin embargo, esta comodidad viene acompañada de vulnerabilidades. La banca en línea, desarrollada predominantemente en plataformas robustas como .NET, se enfrenta constantemente a amenazas cibernéticas que evolucionan rápidamente, desde ataques de phishing hasta violaciones más sofisticadas. Esta dinámica presenta un desafío único para la ciberseguridad, a partir de esto nos preguntamos ¿Cómo podemos defender efectivamente los servicios esenciales en este entorno hostil y en constante cambio?, ante este panorama, la implementación de Sistemas de Información de Gestión de Eventos de Seguridad (SIEM) surge como un enfoque para la monitorización y respuesta a incidentes de seguridad en tiempo real. En este contexto, el presente estudio se enfoca en el desarrollo de un entorno controlado de laboratorio utilizando Máquinas Virtuales Windows y Linux para simular ataques cibernéticos dirigidos a servicios de banca en línea desarrollados en .NET. Este enfoque metodológico permite una investigación sobre la efectividad de los SIEM basados en herramientas Open Source para detectar, monitorizar y responder a ataques en tiempo real, ofreciendo una perspectiva única sobre su capacidad para proteger infraestructuras críticas en el sector financiero.

Palabras clave: Ciberseguridad, SIEM, banca en línea, firewall.

Abstract

Cybersecurity has become a paramount concern in the digital age, especially with the growing reliance on online services for critical operations, which has elevated online banking to an essential component of daily life, facilitating financial transactions for millions of users globally. However, this convenience comes with vulnerabilities. Online banking, predominantly developed on robust platforms like .NET, constantly faces rapidly evolving cyber threats, ranging from phishing attacks to more sophisticated breaches. This dynamic presents a unique challenge for cybersecurity, prompting the question: How can we effectively defend essential services in this hostile and ever-changing environment? In this scenario, the implementation of Security Information and Event Management (SIEM) systems emerges as an approach for real-time security incident monitoring and response. In this context, the present study focuses on developing a controlled laboratory environment using Windows and Linux Virtual Machines to simulate cyber-attacks targeting online banking services developed in .NET. This methodological approach allows for an investigation into the effectiveness of SIEM systems based on open-source tools to detect, monitor, and respond to attacks in real-time, offering a unique perspective on their capability to protect critical infrastructures in the financial sector.

Keywords: Cybersecurity, SIEM, online banking, firewall.

Tabla De Contenido

Lista de Figuras

Lista de Figuras Apéndice A

Lista de Figuras Apéndice B

Lista de Tablas

Lista de Tablas Apéndice A

Lista de Tablas Apéndice B

CAPÍTULO 1

Introducción

La ciberseguridad se ha convertido en una preocupación primordial en la era digital, especialmente con la creciente dependencia de los servicios en línea para operaciones críticas como la banca. La transformación digital ha elevado la banca en línea a un componente esencial de la vida cotidiana, facilitando transacciones financieras a millones de usuarios globalmente. Sin embargo, esta comodidad viene acompañada de vulnerabilidades significativas. La banca en línea, desarrollada predominantemente en plataformas robustas como .NET, se enfrenta constantemente a amenazas cibernéticas que evolucionan rápidamente, desde ataques de phishing hasta violaciones de datos sofisticadas. Esta dinámica presenta un desafío único para la ciberseguridad: ¿Cómo podemos defender efectivamente los servicios esenciales en este entorno hostil y en constante cambio?

Ante este panorama, la implementación de Sistemas de Información de Gestión de Eventos de Seguridad (SIEM) surge como un enfoque proactivo para la monitorización y respuesta a incidentes de seguridad en tiempo real. Los SIEM, especialmente aquellos basados en soluciones Open Source, ofrecen una plataforma integrada para la detección, documentación y contramedida de amenazas, aprovechando la inteligencia artificial y el aprendizaje automático para adaptarse a las tácticas en evolución de los actores maliciosos. Aunque la adopción de tecnologías SIEM en el ámbito de la banca online promete mejorar la postura de seguridad, su implementación y eficacia práctica aún se encuentran bajo escrutinio.

En este contexto, el presente estudio se enfoca en el uso de Wazuh, una plataforma SIEM Open Source, para la monitorización y gestión de la seguridad en servicios de banca en línea. En lugar de simular ataques cibernéticos completos, el estudio se centrará en tres áreas críticas de seguridad: el monitoreo de integridad de archivos, la detección de vulnerabilidades y la integración con VirusTotal para el análisis de archivos sospechosos. Estas áreas fueron seleccionadas debido a su relevancia en la detección y mitigación de amenazas cibernéticas comunes en entornos bancarios.

Monitoreo De Integridad De Archivos. El monitoreo de integridad de archivos es esencial para detectar cambios no autorizados en archivos críticos del sistema. Utilizando Wazuh FIM (File Integrity Monitoring), se pueden generar alertas cuando se detecten modificaciones, eliminaciones o creaciones de archivos, proporcionando una capa de seguridad adicional contra posibles compromisos del sistema.

Detección De Vulnerabilidades. La detección de vulnerabilidades es una función clave para identificar y alertar sobre debilidades en el sistema que podrían ser explotadas por atacantes. Wazuh Vulnerability Detector permite escanear el sistema en busca de vulnerabilidades conocidas, generando informes y recomendaciones para su mitigación.

Integración Con Virus Total. La integración con Virus Total añade una capacidad crítica para analizar archivos sospechosos utilizando la base de datos de Virus Total. Esto permite verificar la integridad de los archivos y detectar posibles amenazas, aumentando la capacidad de respuesta ante incidentes de seguridad.

Este enfoque metodológico permitirá una investigación detallada sobre la efectividad de Wazuh en la monitorización y gestión de la seguridad en tiempo real, ofreciendo una perspectiva única sobre su capacidad para proteger infraestructuras críticas en el sector financiero.

Caso de Estudio / Problema de Investigación

Preguntas de Investigación

Las preguntas de investigación que guían este estudio son:

1. **Monitoreo de Integridad de Archivos:**

   ¿Cómo puede el monitoreo de integridad de archivos con Wazuh detectar y alertar sobre cambios no autorizados en archivos críticos del sistema? ¿Qué impacto tiene el monitoreo de integridad de archivos en la postura de seguridad de una institución bancaria?

2. **Detección de Vulnerabilidades:**

   ¿Cómo puede Wazuh identificar y alertar sobre vulnerabilidades presentes en el sistema? ¿Qué efectividad tiene Wazuh en la mitigación de vulnerabilidades críticas en un entorno bancario?

3. **Integración con VirusTotal:**

   ¿Cómo puede la integración de Wazuh con VirusTotal ayudar a detectar y analizar archivos sospechosos en tiempo real? ¿Qué beneficios aporta la integración con VirusTotal para la seguridad de los servicios de banca en línea?

Este estudio aborda estas preguntas mediante una investigación empírica y teórica, combinando la construcción de un entorno de laboratorio específico con el análisis de datos de ataques simulados. Se explorará el potencial de los SIEM Open Source para transformar la seguridad cibernética en la banca online, con el objetivo de proporcionar recomendaciones concretas para su implementación efectiva y mejorar las prácticas de seguridad en un sector crítico para la economía global.

Alcance Del Proyecto

El presente proyecto de titulación se fundamenta en la investigación y práctica del uso de Wazuh para la detección y mitigación de vulnerabilidades en un entorno bancario. El proyecto se desarrolla de acuerdo con la siguiente estructura:

Monitoreo de Integridad de Archivos. Implementación del monitoreo de integridad de archivos utilizando Wazuh para detectar y alertar sobre cambios no autorizados en archivos críticos. Evaluación del impacto del monitoreo de integridad de archivos en la postura de seguridad de una institución bancaria.

Detección de Vulnerabilidades: Configuración de Wazuh para identificar y alertar sobre vulnerabilidades presentes en el sistema. Análisis de la efectividad de Wazuh en la detección y mitigación de vulnerabilidades críticas.

Integración con VirusTotal. Integración de Wazuh con VirusTotal para detectar y analizar archivos sospechosos en tiempo real. Evaluación de los beneficios de la integración con VirusTotal para la seguridad de los servicios de banca en línea.

Entorno Bancario. El prototipo de servicio de banca online será básico, enfocado en demostrar la viabilidad del entorno de simulación más que en replicar completamente un sistema bancario en línea existente.

Límites y Exclusiones

Tabla 1

Límites y exclusiones del proyecto

Límites	Exclusiones
El proyecto se centrará únicamente en la implementación y evaluación de Wazuh para las tres áreas específicas mencionadas (monitoreo de integridad de archivos, detección de vulnerabilidades e integración con Virus Total).	No se incluirá la simulación de ataques cibernéticos complejos ni la exploración de vulnerabilidades desconocidas o de día cero en los sistemas utilizados.
La aplicación de banca online desarrollada será un prototipo con funcionalidades limitadas, diseñado únicamente para fines de este proyecto y no para un uso real en producción.	

Casos de Usos

Realizar pruebas de diferentes escenarios de vulnerabilidades y monitoreo en los servicios de banca online, determinando los siguientes escenarios:

Tabla 2:

Casos de Uso para la Implementación y Evaluación de Wazuh en Servicios de Banca Online

Casos de Uso	Objetivo	Métodos	Herramientas SIEM a Utilizar	Resultados Esperados

Caso de Uso 1: Monitoreo de Integridad de Archivos	Detectar cambios no autorizados en archivos críticos del sistema.	Implementar el monitoreo de integridad de archivos utilizando Wazuh para rastrear modificaciones, creaciones y eliminaciones de archivos en tiempo real.	Wazuh FIM (File Integrity Monitoring).	Generación de alertas sobre cualquier cambio no autorizado en archivos críticos, mejorando la capacidad de respuesta ante posibles compromisos de seguridad.
Caso de Uso 2: Detección de Vulnerabilidades	Identificar y alertar sobre vulnerabilidades presentes en el sistema.	Configurar Wazuh para realizar escaneos periódicos de vulnerabilidades, proporcionando informes detallados y recomendaciones para la mitigación.	Wazuh Vulnerability Detector	Detección temprana de vulnerabilidades críticas, permitiendo su mitigación antes de que puedan ser explotadas por actores maliciosos.
Caso de Uso 3: Integración con VirusTotal	Detectar y analizar archivos sospechosos utilizando la base de datos de VirusTotal.	Integrar Wazuh con VirusTotal para escanear archivos sospechosos en tiempo real, proporcionando análisis detallados y alertas sobre posibles amenazas.	Wazuh Integration with VirusTotal	Identificación y análisis de archivos maliciosos, mejorando la capacidad de respuesta ante posibles amenazas y reduciendo el riesgo de infecciones en el sistema.

Objetivos

Objetivo General

- Desarrollar un entorno controlado de laboratorio utilizando Wazuh para evaluar la efectividad en la mejora de la seguridad de los servicios de banca en línea mediante el monitoreo de integridad de archivos, la detección de vulnerabilidades y la integración con VirusTotal.

Objetivos Específicos

- Simular la arquitectura del servicio de banca web para obtener logs de eventos de los componentes de red, aplicación y seguridad, a fin de demostrar la efectividad del SIEM en la correlación y notificación de los eventos de seguridad.
- Desarrollar o configurar herramientas/scripts para simular los ataques definidos contra el servicio de banca online.
- Integrar las herramientas SIEM seleccionadas para el monitoreo en tiempo real del entorno y la detección de ataques.
- Realizar pruebas de ataque en el entorno para evaluar la efectividad de las herramientas SIEM en la detección y respuesta.

Contexto de la Ciberseguridad en la Banca Online.

La industria financiera, enfrenta desafíos adicionales como el robo de credenciales e identidades, el cual se ha acelerado especialmente en el contexto de la pandemia. La rápida

adaptación de las operaciones financieras al entorno digital ha sido aprovechada por los ciberdelincuentes, resultando en un aumento significativo de malwares móviles capaces de robar credenciales de instituciones financieras. Además, el robo de identidad ha experimentado un crecimiento, en parte debido a la implementación de programas de ayuda financiera por gobiernos e instituciones financieras, ofreciendo a los ciberdelincuentes nuevas oportunidades para el fraude (ITware Latam, 2022).

Estas tendencias destacan la importancia de una estrategia de seguridad cibernética adaptativa y proactiva, capaz de anticiparse a las tácticas en evolución de los ciberdelincuentes para proteger efectivamente la infraestructura crítica de la banca online. La colaboración intersectorial y el intercambio de inteligencia sobre amenazas son fundamentales para mejorar la eficacia en la respuesta a potenciales ataques (ITware Latam, 2022).

El análisis del artículo de SentinelOne sobre ataques cibernéticos internos en instituciones financieras destaca la relevancia de los sistemas SIEM como herramientas complementarias en la ciberseguridad. Sin presentar el SIEM como una solución definitiva, el estudio propone su uso como parte integral de una estrategia de seguridad más amplia y multidimensional, capaz de mejorar la detección temprana de actividades fraudulentas y proteger los activos financieros. (SentinelOne, 2022).

Simulación de la Arquitectura de Servicios de Banca Web y Evaluación de la Efectividad de SIEM.

Las plataformas SIEM integran y analizan datos de eventos de seguridad y registros de sistemas, redes y computadoras, convirtiéndolos en información de seguridad accionable. Estas

plataformas son fundamentales para detectar amenazas que los sistemas de seguridad individuales podrían pasar por alto, utilizando inteligencia de amenazas, análisis de comportamiento con aprendizaje automático y análisis del comportamiento de usuarios y entidades (UEBA) para mejorar la precisión de las alertas y detectar nuevas amenazas Exabeam. (2024).

Mejores Prácticas Operativas para SIEM.

Implementar un SIEM requiere seguir las mejores prácticas operativas, incluyendo el desarrollo de un plan de respuesta a incidentes y la integración del sistema SIEM con otras herramientas de seguridad. Esto optimiza las operaciones de seguridad y mejora la eficiencia en la respuesta a incidentes (Amsat, 2024.).

Arquitectura del Laboratorio de Simulación para Entidad Financiera.

Este laboratorio está diseñado para simular un entorno operativo de una entidad financiera, utilizando un conjunto de máquinas virtuales (VM) para modelar distintos componentes clave de la infraestructura TI detallados en la Tabla 1. La configuración incluye:

Tabla 3

Tabla de Componentes del Entorno de Simulación

COMPONENTE	DESCRIPCIÓN
SERVIDOR DE APLICACIONES	Una VM con Windows Server 2016 actúa como el servidor de aplicaciones, alojando el portal web de la entidad

	financiera, simulando el punto de acceso para los usuarios a los servicios financieros online.
SERVIDOR DE BASE DE DATOS	Otra VM con Windows Server 2016 se dedica a gestionar la Base de Datos en SQL Server, almacenando información crítica de la entidad como transacciones, cuentas de usuarios y datos financieros.
FIREWALL	Se emplea pfSense como solución de firewall para proteger el entorno simulado, configurado para controlar el tráfico de red y prevenir accesos no autorizados.
SIEM - WAZUH	Se integra Wazuh como el sistema SIEM para monitorear y gestionar la seguridad del laboratorio, recopilando y analizando datos para detectar y responder a incidentes de seguridad.

La interconexión de estos componentes permite crear un escenario realista para evaluar la eficacia de Wazuh en la detección de amenazas y la gestión de incidentes de seguridad dentro de un contexto financiero.

pfSense es un software de firewall y router de código abierto que se basa en FreeBSD, destacándose por su versatilidad y robustez en la creación de redes seguras. Ofrece amplias

funcionalidades como control de tráfico, VPN y seguridad de capa de aplicación, facilitando su gestión a través de una interfaz web accesible (Netgate, 2023).

Wazuh se posiciona como una plataforma integral de gestión de información y eventos de seguridad (SIEM) que combina funcionalidades de detección y respuesta extendida (XDR), ofreciendo un enfoque proactivo hacia la seguridad en TI. Dicha plataforma es capaz de recolectar, agregar y analizar datos de eventos en tiempo real para detectar amenazas y asegurar el cumplimiento de normativas, lo que la hace adecuada para una amplia cobertura de seguridad. La solución de Wazuh incluye análisis de logs de seguridad, detección de vulnerabilidades, evaluación de configuraciones de seguridad y ayuda para cumplir con regulaciones como PCI DSS, NIST 800-53, GDPR, entre otras (Wazuh, 2024). Además de sus capacidades como SIEM, Wazuh extiende su funcionalidad con herramientas de XDR para gestionar de forma proactiva las amenazas de seguridad, diferenciándose de las soluciones SIEM tradicionales al permitir una búsqueda activa de amenazas antes de que estas sean detectadas (Devoteam, 2024). La licencia de código abierto y su modelo de implementación en la nube hacen que Wazuh sea accesible para empresas de todos los tamaños, incluyendo PYMEs y organizaciones con departamentos de TI limitados (Devoteam, 2024.).

CAPÍTULO 2

Metodología

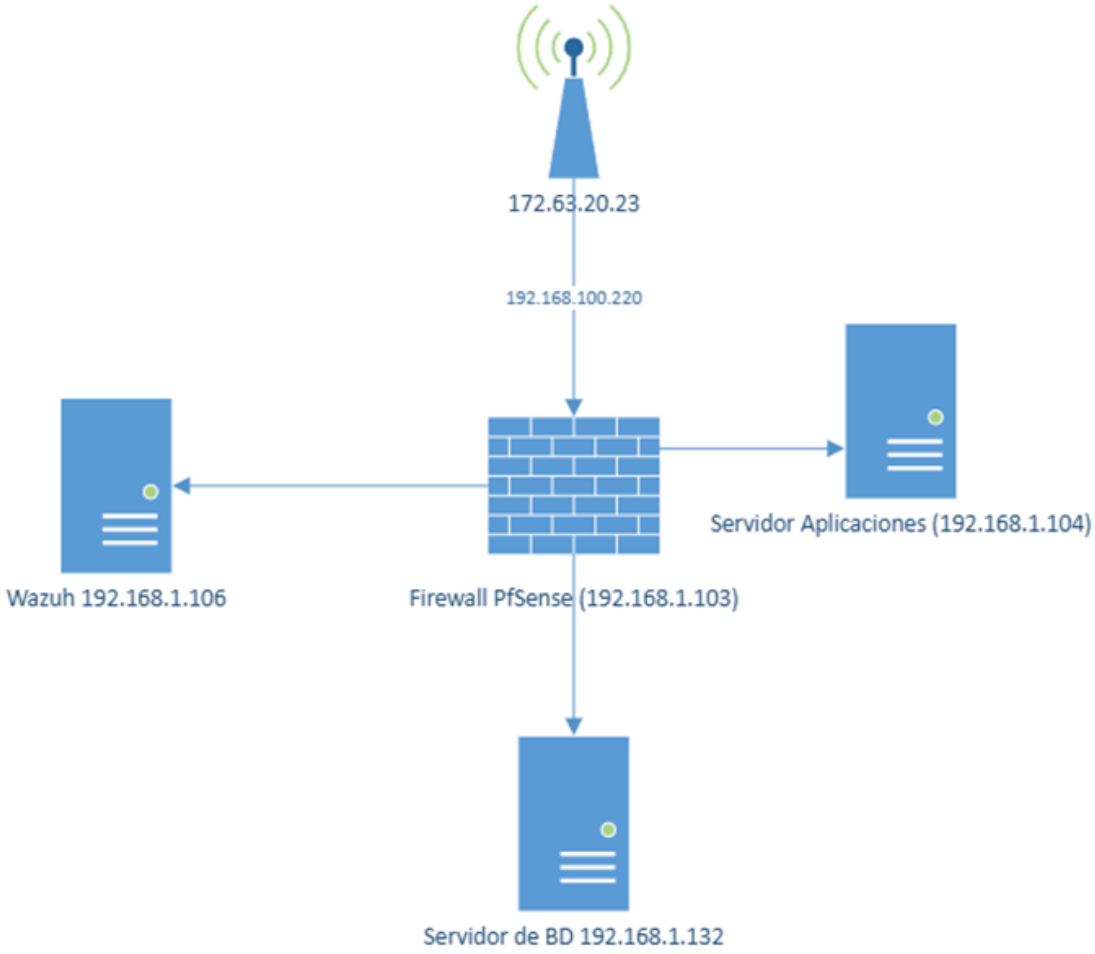
Preparación del Laboratorio.

Descripción General: La infraestructura se compone de un servidor de aplicaciones .NET para la banca online, un servidor de bases de datos SQL Server, un firewall pfSense para la seguridad perimetral, y un servidor Ubuntu con Wazuh para la monitorización de seguridad.

Diagrama de Arquitectura: Se incluye un diagrama que ilustra la conexión entre el servidor de aplicaciones, el servidor de base de datos, el firewall, y el sistema de monitorización, destacando las zonas de red protegidas por pfSense y la cobertura de monitorización de Wazuh (ver Figura 1)

Figura 1

Diagrama de Red del Laboratorio Controlado



Configuración del Servidor de Banca Online y SQL Server.

Se ajustó el servidor Windows para optimizar el rendimiento, aplicando configuraciones específicas de seguridad como la desactivación de servicios innecesarios y la configuración de políticas de grupo para reforzar el acceso. En la Tabla 2 se detalla las características de las máquinas virtuales del servidor de aplicación y base de datos

Tabla 4

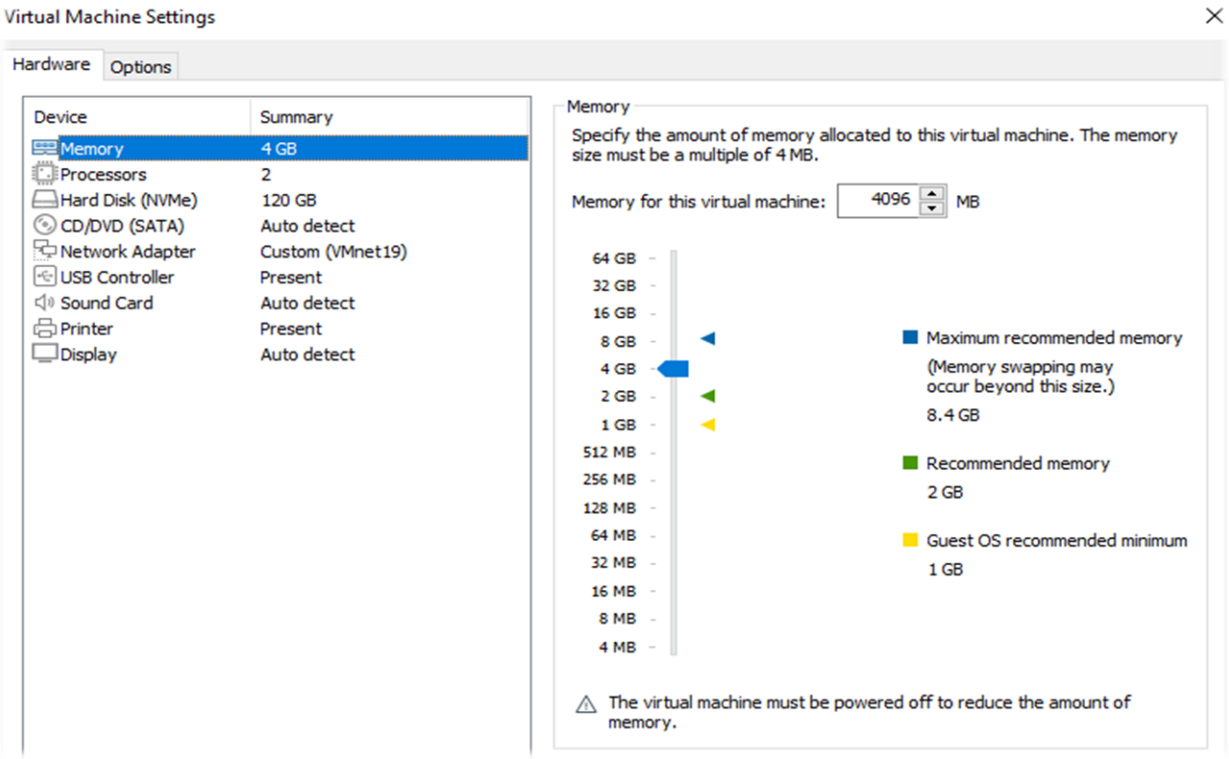
Característica de Máquinas Virtuales

Tipo de Servidor	Sistema Operativo	Características
Servidor de Aplicación	Windows Server Estándar 2016	Máquina Virtual para la publicación de la aplicación Web con la característica del Internet Information Services
Servidor de Base de Datos	Windows Server Estándar 2016	Máquina Virtual dedicada a gestionar la Base de Datos en SQL Server

En la Figura 2 se observa las características establecidas para la máquina virtual del servidor de aplicación de la banca online.

Figura 2.

Característica del Servidor Aplicación de la Banca Online

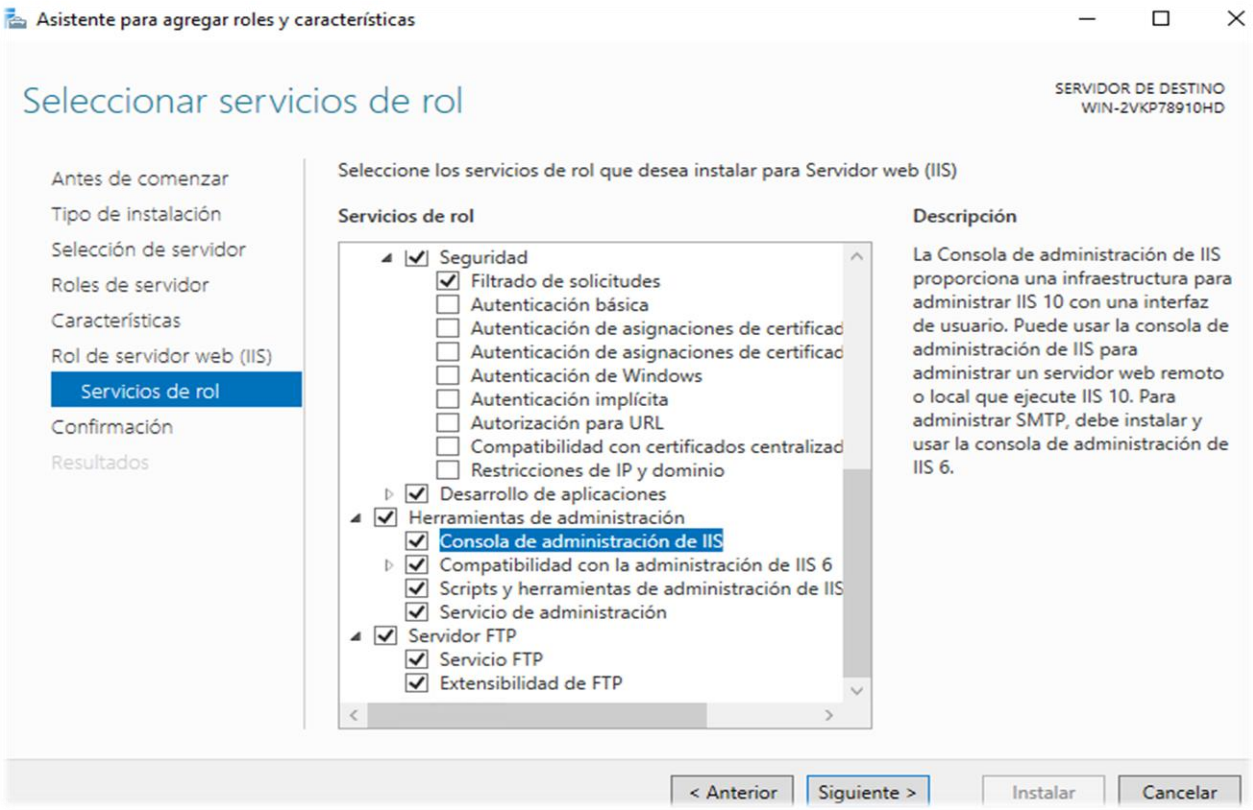


Configuración del Servidor IIS para la Aplicación Bancaria Online

Instalación y Configuración Básica. Se procedió a la instalación del Internet Information Services (IIS) en un servidor Windows dedicado para alojar la aplicación de banca en línea desarrollada en .NET (ver Figura 3). Esta configuración inicial incluyó la instalación de los roles necesarios de IIS a través del Administrador de Servidores de Windows, asegurando que los componentes esenciales como .NET Framework, servicios de autenticación y el módulo HTTP Redirection estuvieran habilitados.

Figura 3

Instalación del IIS en el servidor



Configuración de Pool de Aplicaciones Para optimizar el rendimiento y la seguridad de la aplicación, se creó un pool de aplicaciones dedicado específicamente para la banca en línea como se observa en la Figura 4. Este pool de aplicaciones se configuró con las siguientes características:

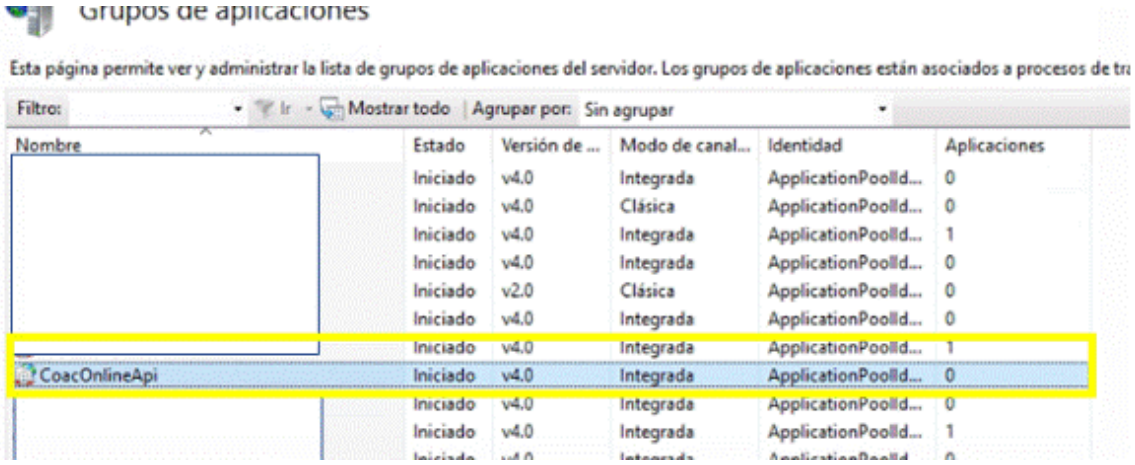
Modo de Pipeline: Integrado, para aprovechar las funcionalidades avanzadas de procesamiento de ASP.NET.

Identidad del Pool: Se utilizó una cuenta de servicio personalizada con permisos mínimos necesarios para ejecutar la aplicación, reduciendo así la superficie de ataque potencial.

Configuración de Reciclaje: Establecido para reciclar periódicamente los procesos del pool para liberar recursos y mejorar la estabilidad.

Figura 4.

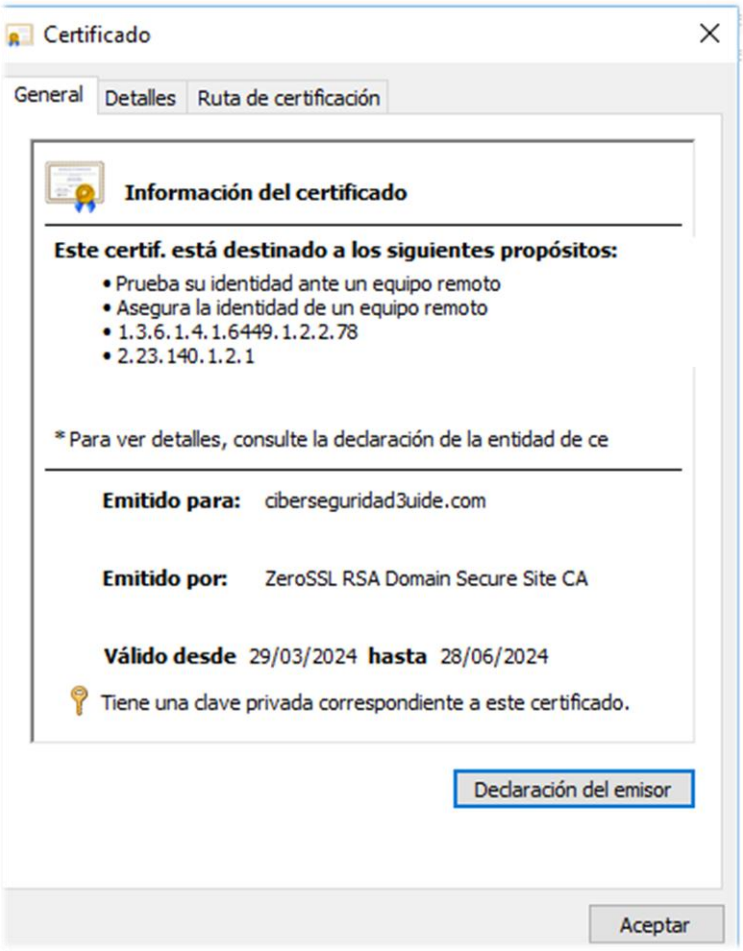
Creación del Pool de Aplicaciones



Implementación de Certificados SSL. Para asegurar que todas las transacciones y comunicaciones a través de la aplicación sean seguras, se implementaron certificados SSL/TLS. Esto se realizó mediante la adquisición de Certificado Se obtuvo un certificado SSL de una autoridad certificadora reconocida (ver Figura 5).

Figura 5

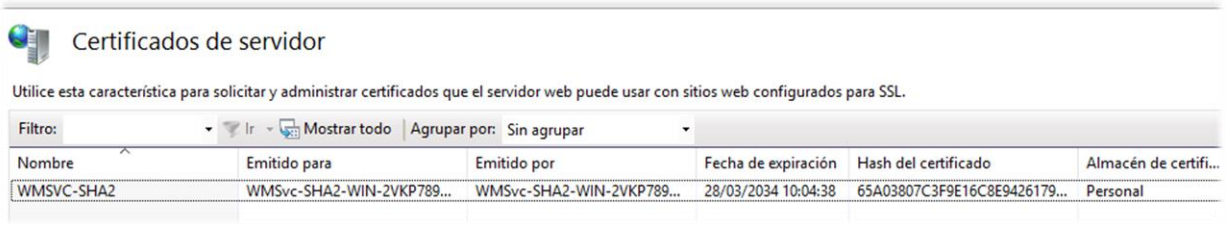
Descripción del Certificado con el dominio ciberseguridad3uide.com



Instalación del Certificado: El certificado se instaló en el servidor IIS a través del administrador de certificados de Windows como se puede evidenciar en la Figura 6.

Figura 6

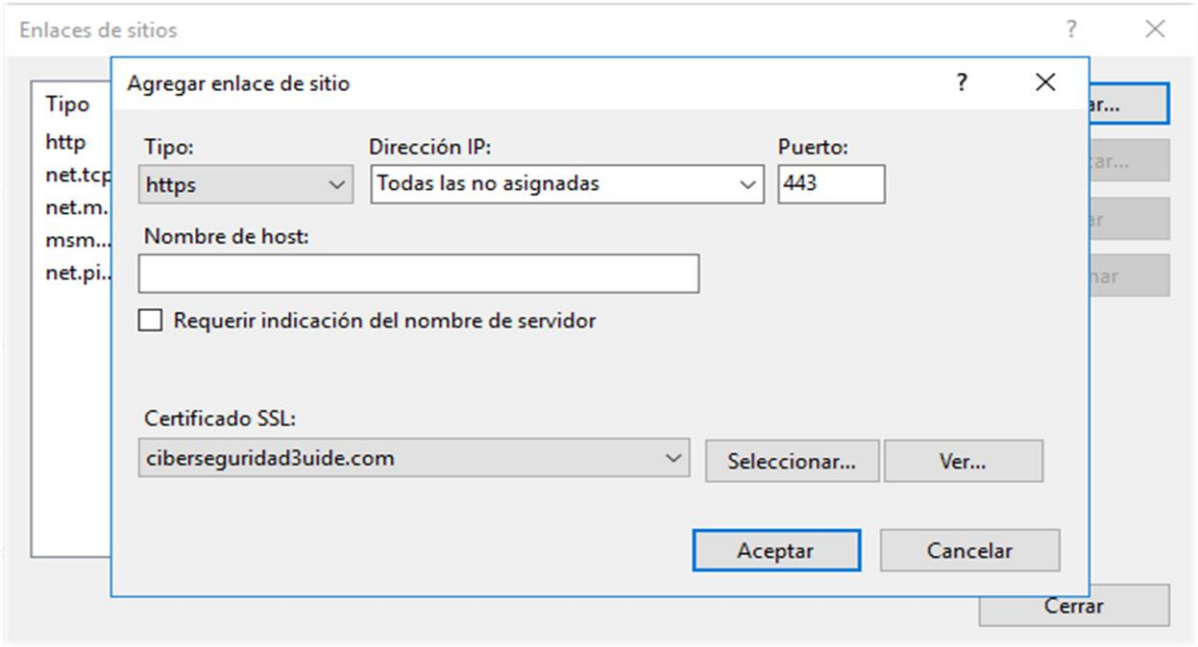
Instalación del Certificado (ciberseguridad3uide.com)



Asignación Al Sitio Web: El certificado se asignó al sitio web de la aplicación bancaria, configurando el enlace HTTPS y especificando el puerto seguro 443 (ver Figura 7).

Figura 7

Asignación del certificado a la Aplicación creada

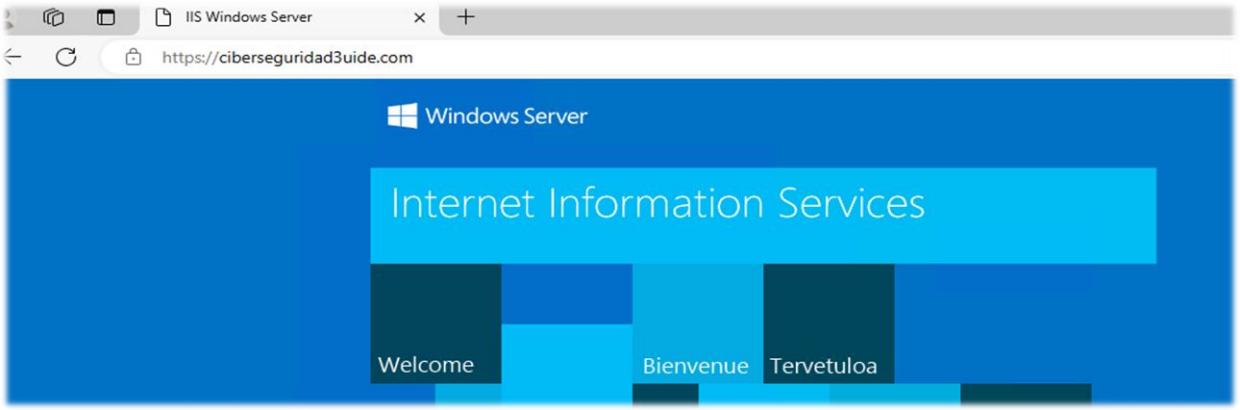


Pruebas Y Validación. Finalmente, se realizaron pruebas exhaustivas para validar la configuración. Cabe indicar que para llegar a esta prueba se tuve que realizar configuraciones que se detallaran en el apartado de (configuración del Firewall) pero para objeto de la Aplicación Web publicada en la nube esto incluyó pruebas de:

Conectividad Segura. En la Figura 8 se visualiza la Verificación del protocolo HTTPS mediante navegadores web y herramientas de diagnóstico de red para asegurar una encriptación adecuada.

Figura 8

Verificación de protocolo y acceso por el puerto seguro

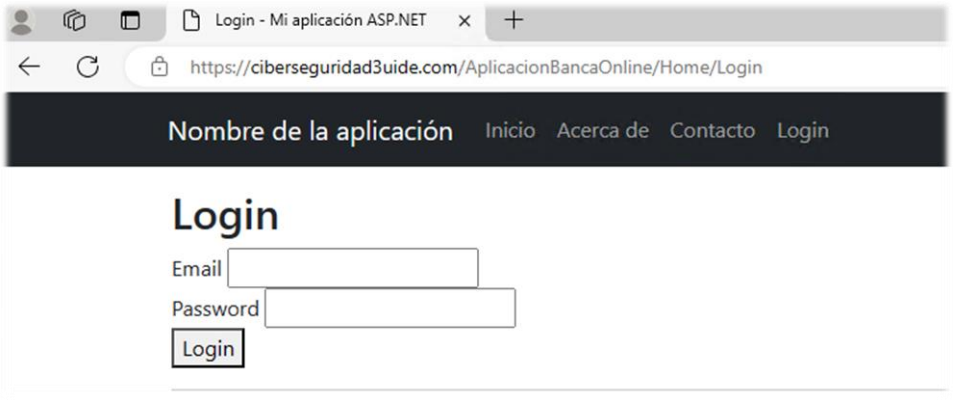


Funcionalidad De La Aplicación: Pruebas de las funcionalidades críticas de la aplicación para asegurar que operan correctamente bajo el pool de aplicaciones y la configuración SSL (ver Figura 9).

URL: https://ciberseguridad3uide.com/AplicacionBancaOnline/Home/Login

Figura 9

Pruebas de Funcionabilidad de la Aplicación

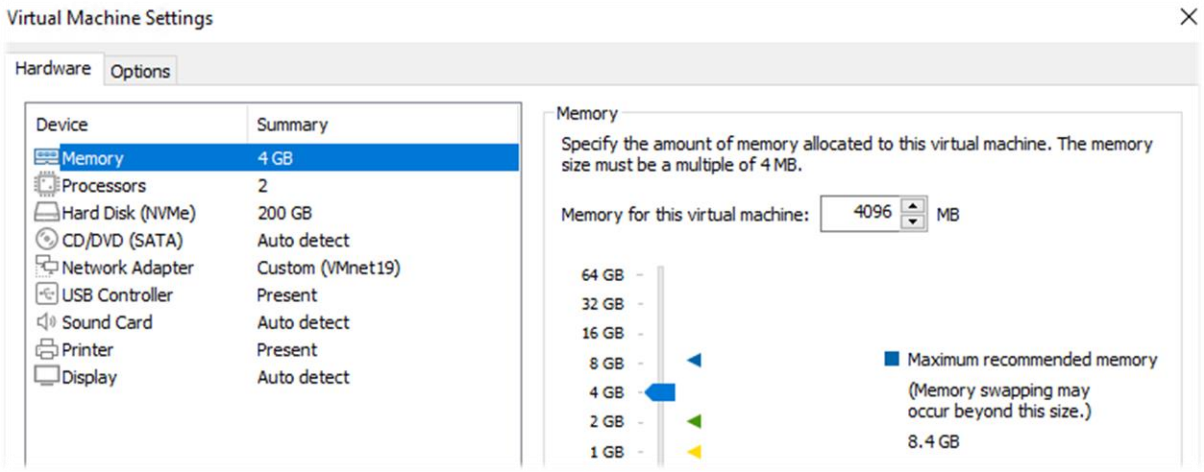


Configuración del Servidor de Base de Datos.

Para alojar la base de datos de la aplicación de banca online, se optó por instalar Windows Server Data Center como sistema operativo en un servidor dedicado, aprovechando sus capacidades avanzadas de manejo y seguridad de datos a gran escala. Posteriormente, se procedió a instalar SQL Server 2018, seleccionando este sistema de gestión de base de datos por su robustez, capacidad de integración con aplicaciones .NET y soporte extensivo de transacciones seguras. En la Figura 10 se puede observar las características físicas de la máquina virtual

Figura 10

Característica de la Maquina de Base de Datos.



Configuración de SQL Server

Una vez instalado SQL Server, se realizaron las siguientes configuraciones clave para asegurar el rendimiento óptimo y la seguridad (ver Figura 11):

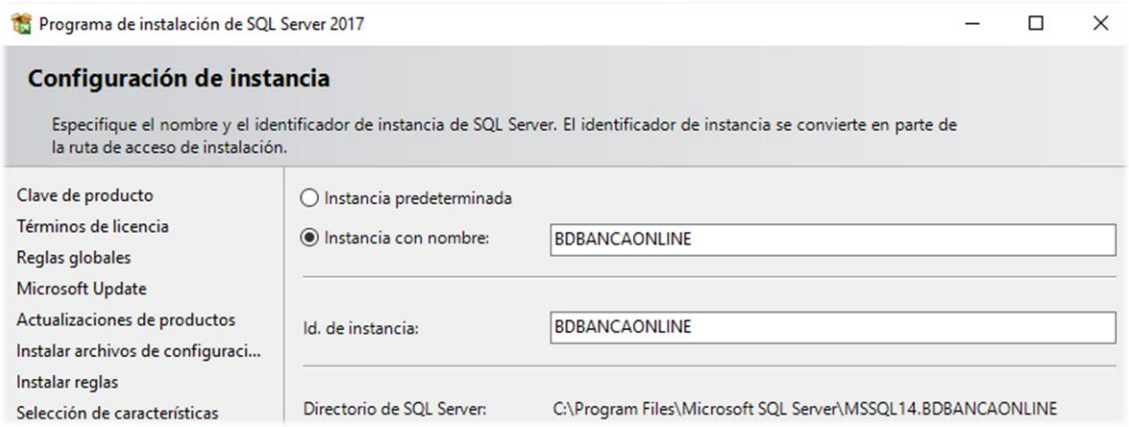
Creación De Instancia Dedicada. Se configuró una instancia dedicada de SQL Server para la aplicación bancaria, aislándola de otras aplicaciones y mejorando así la seguridad y el manejo de recursos.

Configuración De Red Y Firewall. Se establecieron reglas específicas en el firewall para permitir únicamente las conexiones entrantes al SQL Server desde la dirección IP del servidor IIS, reforzando la seguridad al limitar el acceso solo al entorno de la aplicación.

Cadenas de Conexión Seguras. Las cadenas de conexión utilizadas por la aplicación .NET para acceder al SQL Server están cifradas y configuran de manera segura los parámetros de conexión, incluyendo el nombre de la instancia, credenciales y el protocolo de cifrado utilizado.

Figura 11

Instalación del SQL SERVER



Desarrollo de la Aplicación de Banca Online

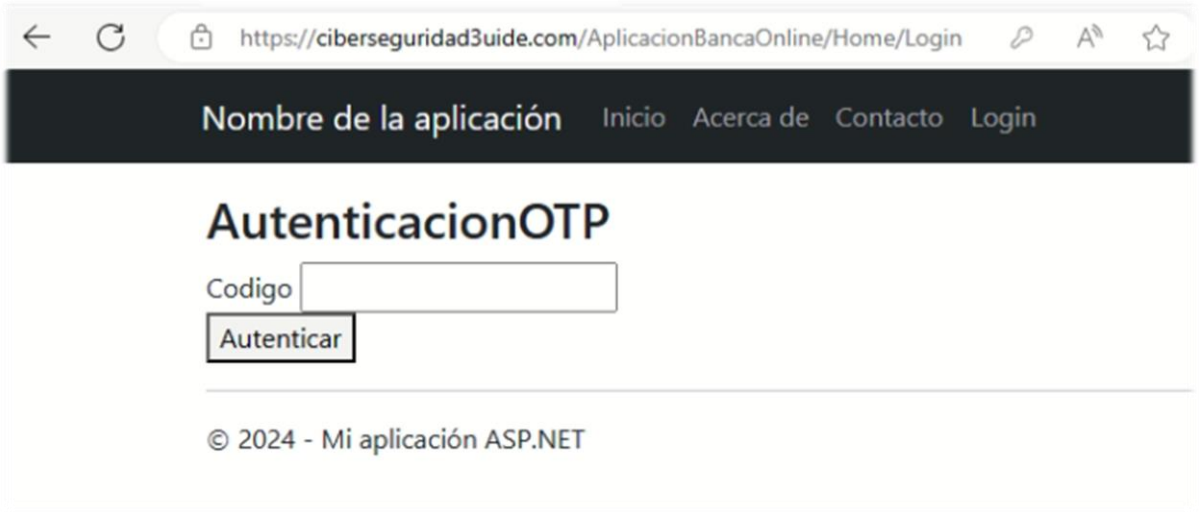
Se desarrolló una aplicación de banca online basada en .NET, diseñada para proporcionar a los usuarios un entorno seguro para realizar operaciones financieras a través de Internet. La aplicación se aloja en un entorno controlado de servidor IIS, con configuraciones detalladas previamente para optimizar seguridad y rendimiento. A continuación, se describen los componentes clave de la interfaz y funcionalidad de la aplicación:

Pantalla De Inicio. La aplicación inicia con una pantalla de Inicio, donde se solicita al usuario que ingrese su nombre de usuario y contraseña. Esta primera capa de autenticación ayuda a verificar la identidad del usuario mediante credenciales establecidas (ver Figura 9).

Autenticación De Dos Factores. Después de la autenticación inicial, el sistema implementa un segundo nivel de seguridad mediante un código de verificación OTP (One-Time Password) (ver Figura 12).

Figura 12

Pantalla de código de verificación

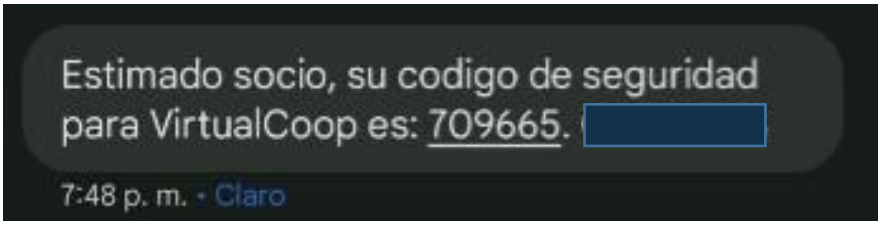


Este código se genera automáticamente y se envía al usuario a través de dos canales simultáneamente:

Mensaje de Texto (SMS): El código OTP se envía al número de teléfono móvil registrado del usuario, asegurando que solo el titular de la cuenta pueda acceder al código (ver Figura 13).

Figura 13

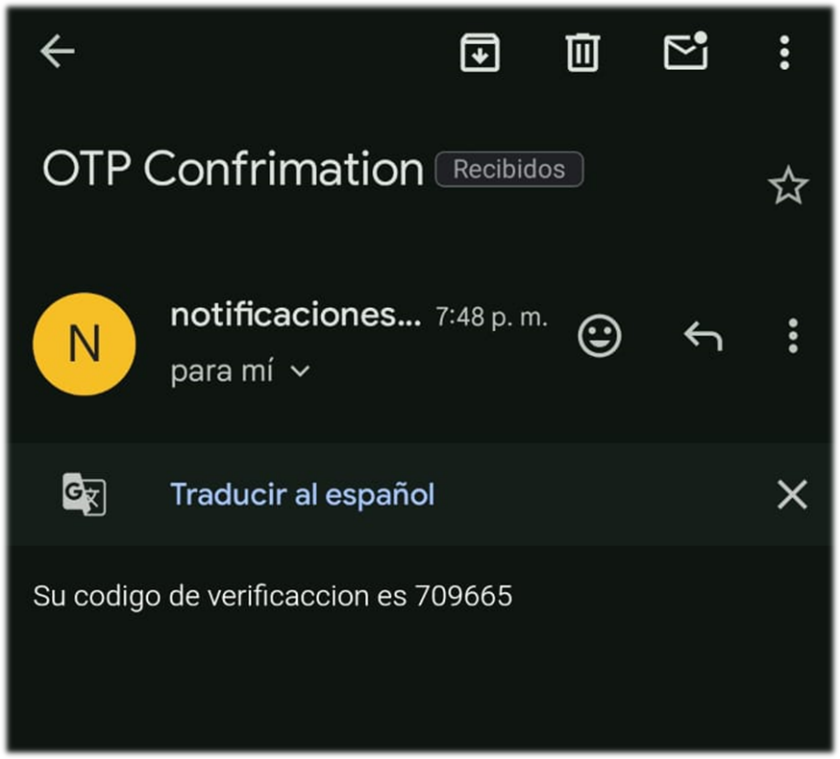
Código generado enviado por mensaje de texto



Correo Electrónico: Paralelamente, se envía una copia del código OTP al correo electrónico asociado con la cuenta del usuario para proporcionar un método de recuperación alternativo (ver Figura 14).

Figura 14

Código OTP recibido desde el correo electrónico



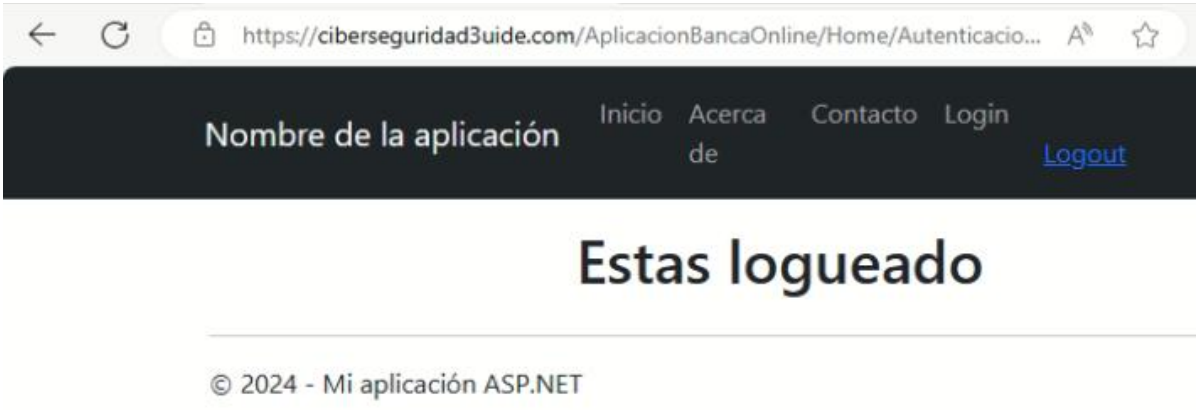
Esta metodología de autenticación de dos factores (2FA) añade una capa adicional de seguridad, protegiendo contra el acceso no autorizado y mitigando el riesgo de ataques como el phishing.

Pantalla Principal. Una vez completada la autenticación de dos factores, el usuario es dirigido a la pantalla principal de la aplicación, que confirma que ha iniciado sesión

correctamente. Esta pantalla principal puede mostrar información relevante para el usuario, como saldos de cuentas, mensajes recientes del banco, y enlaces a diferentes servicios y operaciones financieras disponibles (ver Figura 15).

Figura 15

Pantalla una vez registrada el código OTP



Configuración del Firewall pfSense

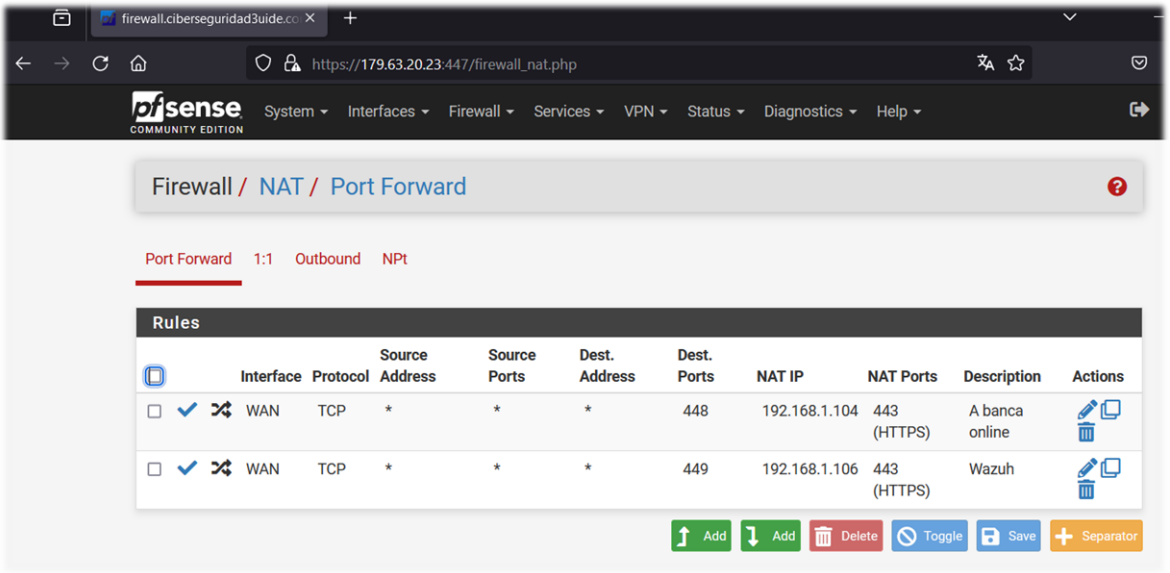
Se procede con la instalación de un firewall en una máquina virtual para realizar el control y redireccionamiento hacia los servicios interno para ello se siguen las instrucciones de la siguiente página de GitHub (Zuñiga & Guarango, 2024)

Principios de Configuración: Se adoptó un enfoque de mínima exposición, donde solo se permiten los servicios estrictamente necesarios, configurando reglas de firewall para bloquear todo el tráfico no solicitado.

Reglas de Firewall: Se establecieron reglas específicas para permitir únicamente el tráfico HTTPS hacia el servidor de la aplicación, además de reglas para la gestión remota segura de pfSense por medio de un redireccionamiento de puertos. (ver figura 16).

Figura 16

Redireccionamiento de puertos de la IP pública a IPs LAN del aplicativo web y wazuh.



En la Figura 17 y 18 se detallan las políticas de acceso a nivel de red WAN y LAN en la que se establecen políticas de seguridad de autorización de ingreso y salida de tráfico del redireccionamiento de puertos que se está realizando.

Figura 17

Políticas de acceso a equipos de red interna con publicación de puerto 443 desde el internet

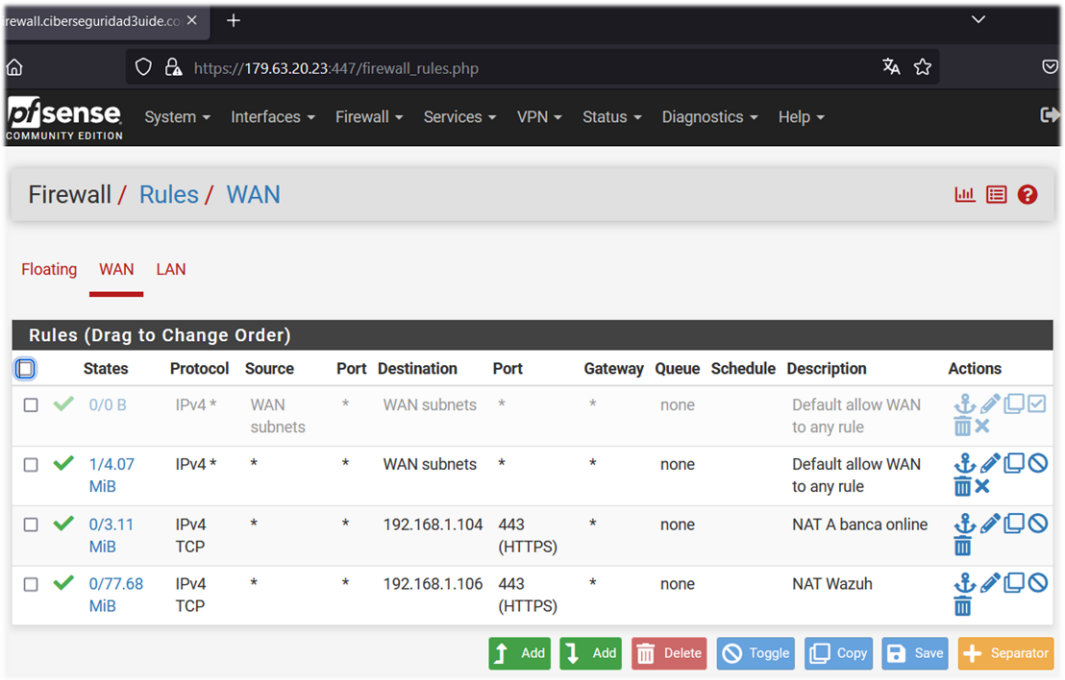
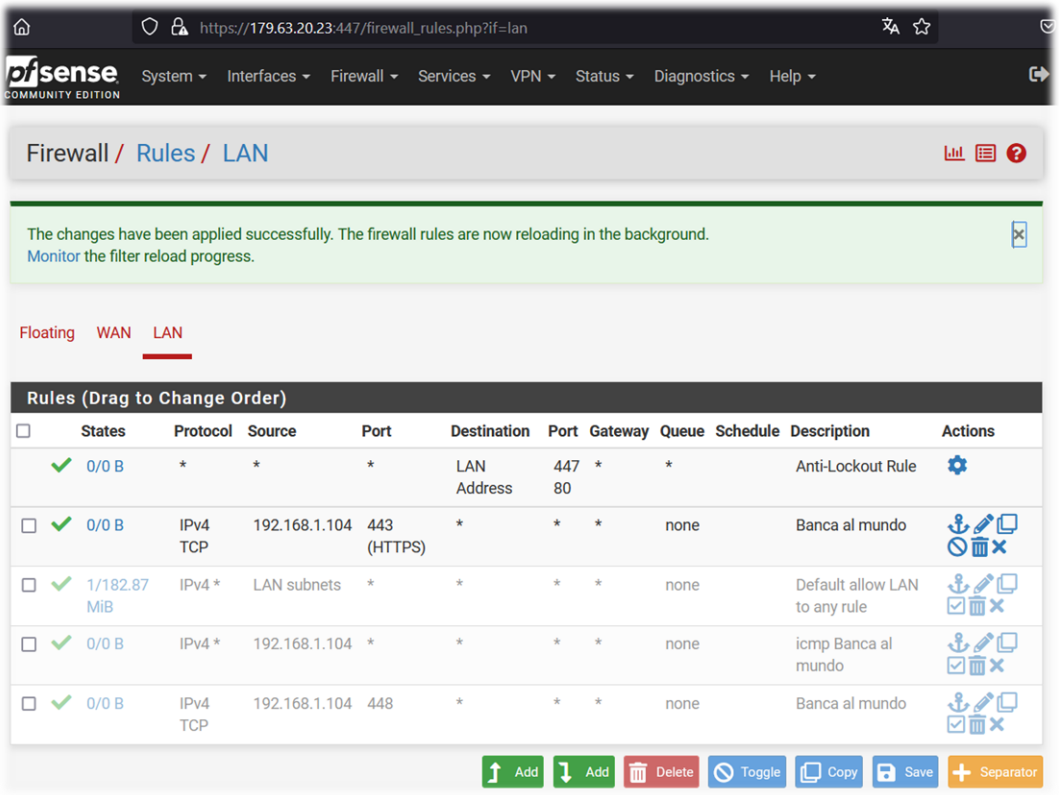


Figura 18

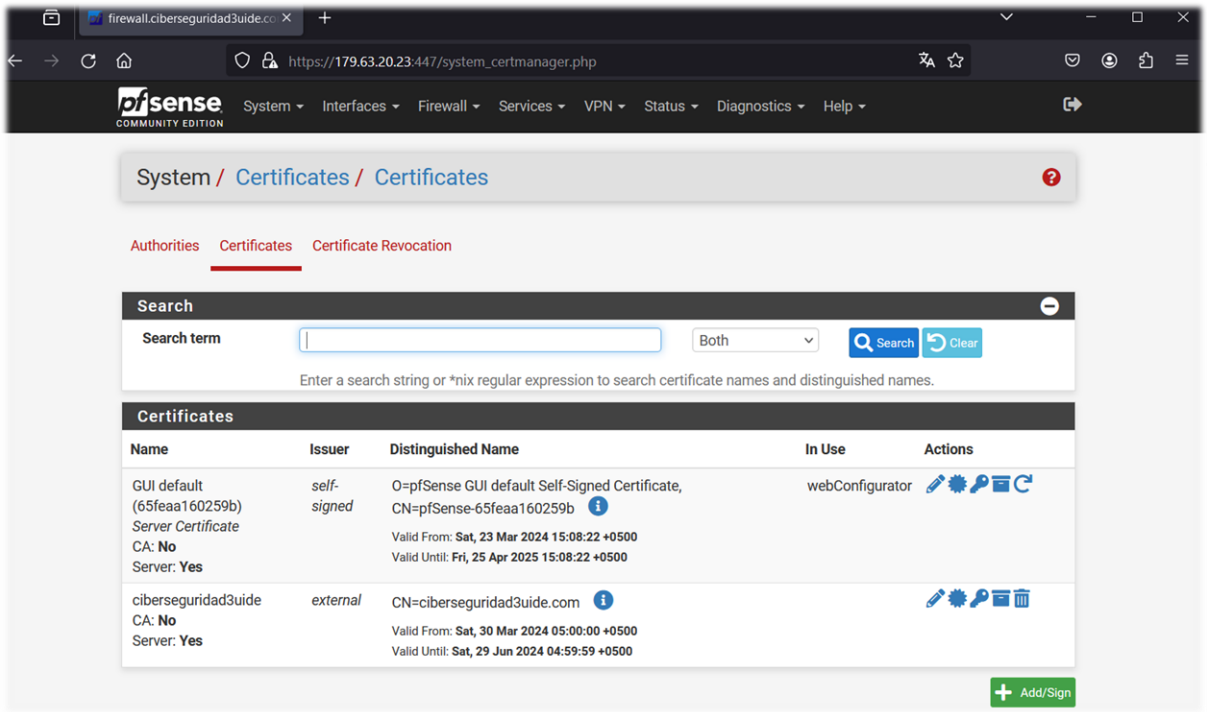
Políticas de salida al mundo de banca web



En la Figura 19 se agrega el certificado SSL dentro del Firewall para publicación de dominios internos para el acceso por URL desde el mundo.

Figura 19

Configuración de certificado SSL en firewall



Implementación de Wazuh como Herramienta SIEM

Dentro del entorno controlado desarrollado para simular ataques cibernéticos a servicios de banca online, se eligió Wazuh como la herramienta SIEM clave para la monitorización en tiempo real y la detección de amenazas.

Wazuh es una plataforma de seguridad integral que proporciona detección de intrusiones, monitorización de cumplimiento, respuesta a incidentes y análisis de seguridad. Para ello se sigue las instrucciones de lo desarrollado de GitHub (Zuñiga, Guarango, Morales, & Vallejo, GitHub, 2024)

Descripción General de Wazuh. Wazuh contribuye a fortalecer la seguridad de los sistemas informáticos al detectar comportamientos maliciosos en tiempo real y responder a

ellos. Utiliza tecnología de análisis de log y monitorización de integridad de archivos para proporcionar visibilidad sobre el estado de seguridad de la infraestructura de TI.

Instalación de Wazuh. La instalación detallada de Wazuh se ha realizado siguiendo las mejores prácticas y configuraciones recomendadas por los desarrolladores de la herramienta. Dado que los detalles técnicos y procedimientos específicos de la instalación son extensos, estos se han documentado por completo en el Apéndice A, el cual proporciona una guía paso a paso sobre cómo configurar Wazuh en el entorno diseñado para este proyecto. Este anexo es esencial para cualquier administrador de sistemas o investigador interesado en replicar o entender la instalación en profundidad.

Configuración de Wazuh. En este capítulo, nos centraremos en explicar la configuración específica de Wazuh adaptada a nuestras necesidades de simulación y monitorización de ataques cibernéticos. Abordaremos cómo se han establecido las políticas de seguridad, las reglas de detección de intrusiones y los mecanismos de respuesta a incidentes para maximizar la efectividad de Wazuh en nuestro entorno simulado.

Además, discutiremos cómo la integración de Wazuh con otras herramientas y sistemas contribuye a una arquitectura de seguridad robusta y cohesiva. Ingresamos a la página principal de wazuh para validar el acceso.

En el marco de este proyecto, se ha procedido a la instalación de Wazuh en dos servidores Windows Server, específicamente configurados para gestionar y monitorizar la seguridad del entorno de banca online simulado. Wazuh se utiliza para la detección de

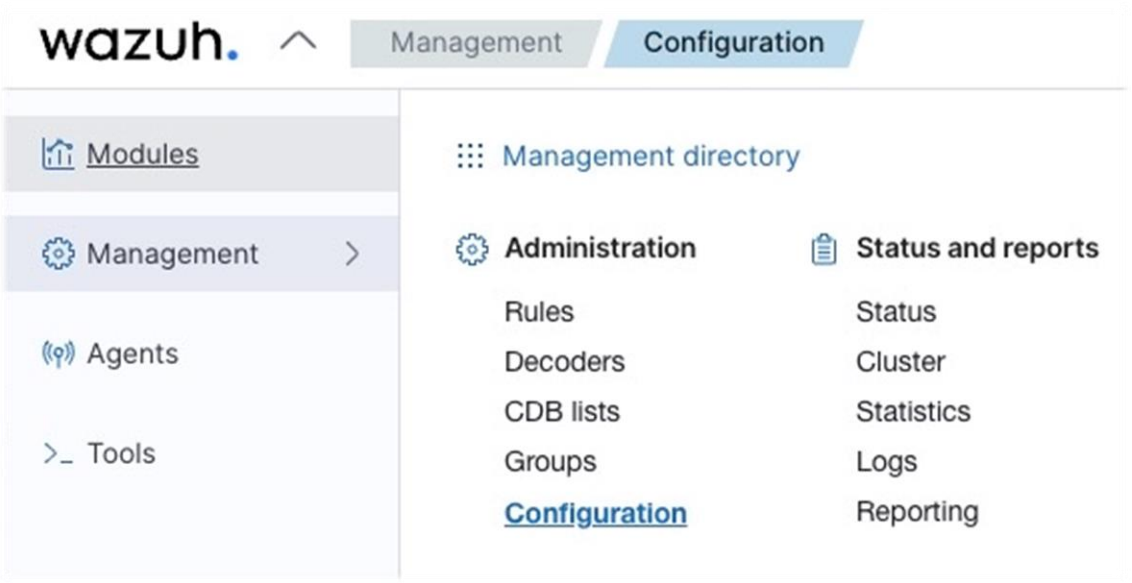
intrusiones, monitorización de cumplimiento y respuesta a incidentes, elementos cruciales para la protección de infraestructuras críticas. A continuación, se detalla el proceso de instalación, apoyado por capturas de pantalla que ilustran cada paso significativo.

El primer ajuste que se realizará es la activación del sensor de vulnerabilidades en Wazuh. Para llevar a cabo este procedimiento, se deben seguir los siguientes pasos (ver Figura 20):

1. Acceso al Menú de Wazuh: Haga clic en la flecha hacia abajo ubicada al lado derecho de la palabra "Wazuh" en la interfaz de usuario.
2. Navegación a la Gestión: Seleccione la opción "Management" en el menú desplegable.
3. Configuración del Sistema: Dentro del menú de gestión, haga clic en "Configuration" para acceder a las configuraciones del sistema.

Figura 20

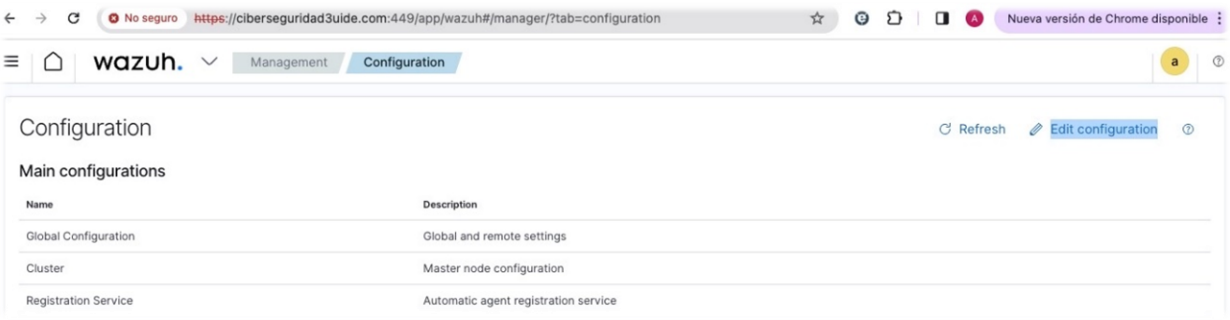
Pantalla configuración Wazuh



En la Figura 21 se observa la ventana de configuración de Wazuh.

Figura 21

Pantalla de edición de configuración.



Presionamos CTRL+ F para que nos de la opción de buscar dentro de la configuración y buscamos “vulnerability-detector”, en nuestro caso se encuentra en la línea 104 (ver figura 22).

Figura 22

Pantalla de configuración de Wazuh en formato XML – opción buscar

Buscamos la línea 105 que tiene la etiqueta enable y cambiamos el valor de “no” por “yes” (ver Figura 23)

Figura 23

Activación de módulo de detección de vulnerabilidades

En la figura 24 se encuentra el boto de SAVE para guardar la configuración y confirmación de los cambios realizados

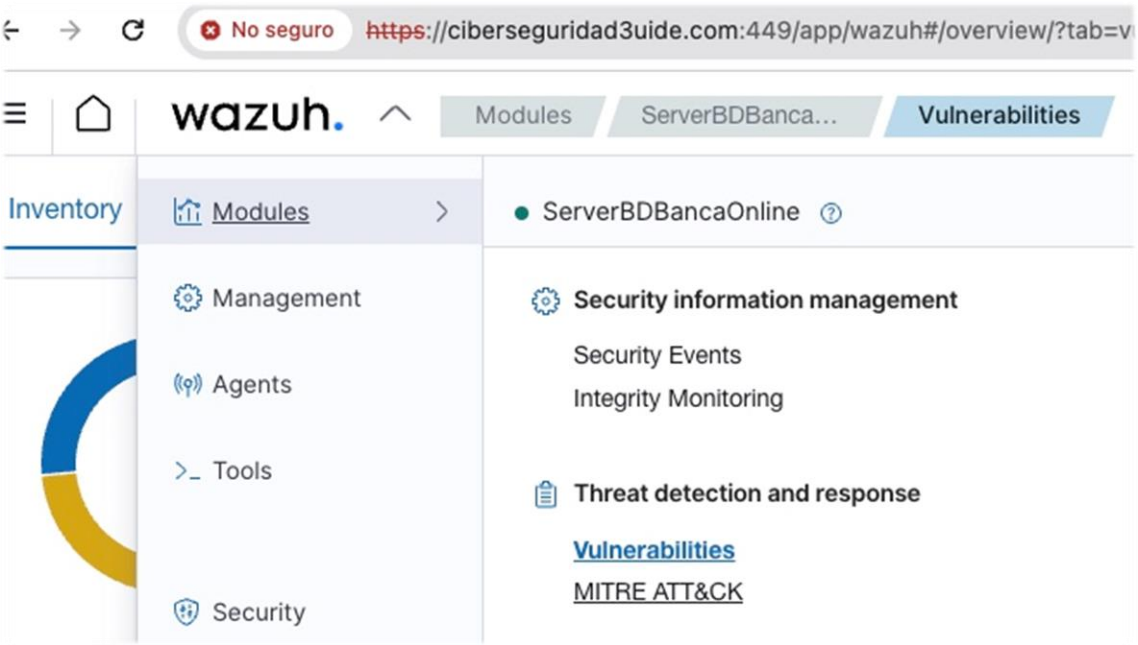
Figura 24

Botón guardar configuración

Para poder ver si tenemos vulnerabilidades en el equipo con agente, damos clic en la flecha a la derecha de wazuh y luego en Vulnerabilities (ver Figura 25).

Figura 25

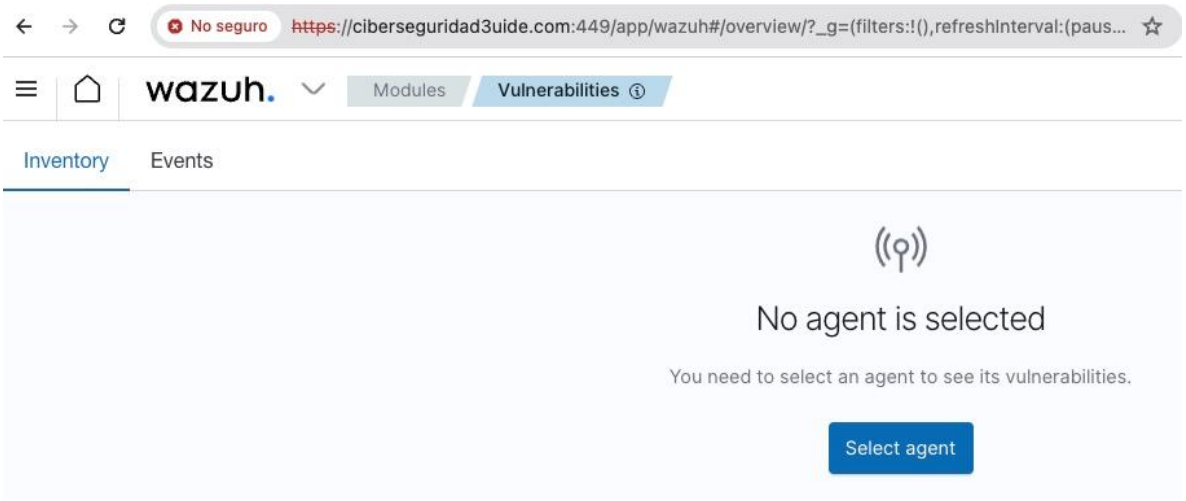
Ubicación módulo de vulnerabilidades



Nos aparece la siguiente pantalla (ver Figura 26) en la cual debemos dar clic en Select agent.

Figura 26

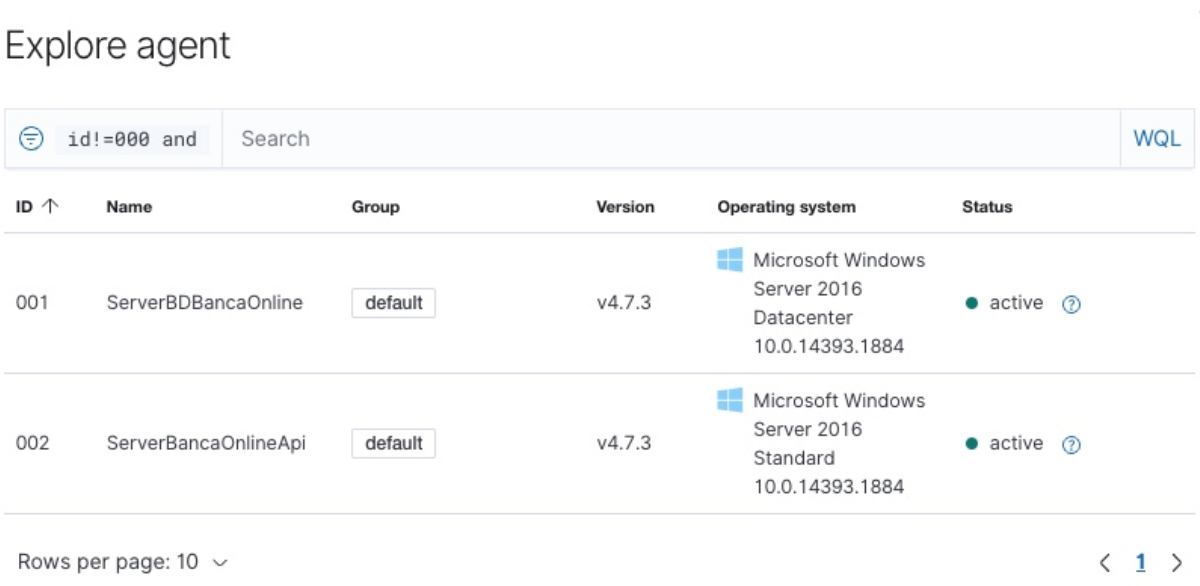
Módulo de vulnerabilidades – selección de agente.



Seleccionamos uno de los 2 equipos en los cuales instalamos el agente. En este caso ServerBancaOnlineApi (ver Figura 27).

Figura 27

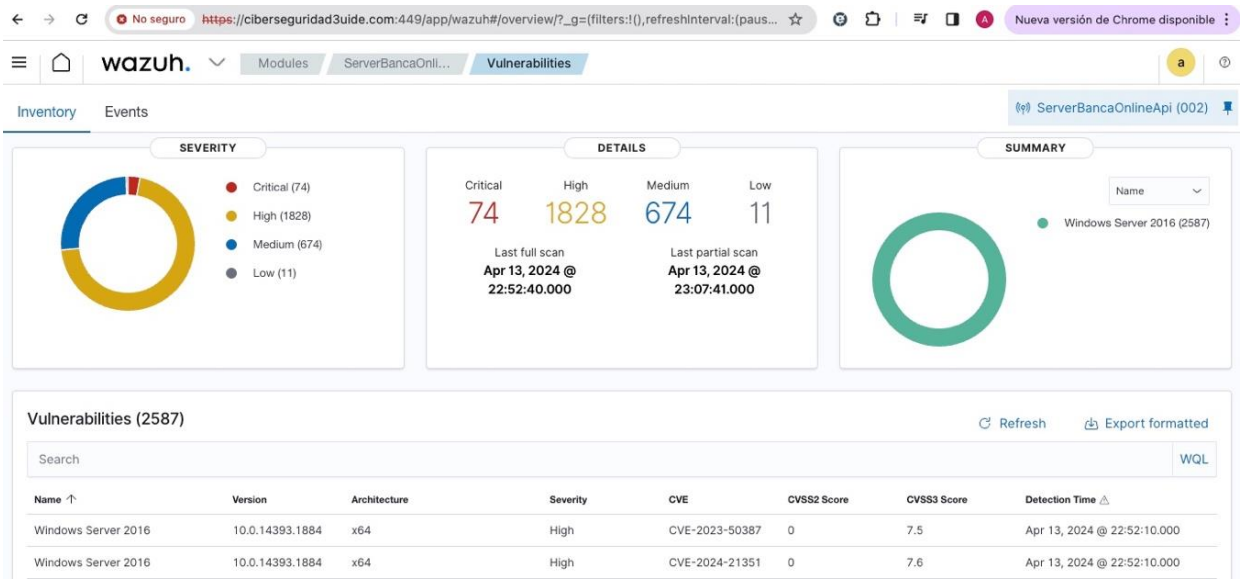
Listado de servidores con agente para verificar vulnerabilidades



Podemos observar la siguiente página nos muestra un resumen de las vulnerabilidades encontradas de ese agente (ver Figura 28).

Figura 28

Visualización de vulnerabilidades por agente



Cambiamos de agente en el módulo de vulnerabilidades, dando click en el nombre del servidor actual nos presenta la siguiente pantalla donde podemos observar todos los agentes instalados y seleccionamos el ServerBDBancaOnline que en nuestro caso es el server que contiene la base de datos de nuestra aplicación (ver Figura 28).

CAPÍTULO 3

Implementación de Casos de Uso. La implementación de casos de uso en una plataforma SIEM como Wazuh es crucial para la detección y respuesta efectiva a incidentes de seguridad. En nuestro estudio, nos enfocamos en tres vulnerabilidades principales que fueron explotadas utilizando Wazuh (ver Tabla 3, 4 y 5):

- Monitoreo de Integridad de Archivos
- Detección de Vulnerabilidades
- Integración con VirusTotal

Estos casos de uso se seleccionaron debido a su relevancia en el sector financiero y su potencial para mejorar significativamente la postura de seguridad de una institución bancaria.

Caso de Uso 1: Monitoreo de Integridad de Archivos

Tabla 5

Monitoreo de Integridad de Archivos

Aspecto	Descripción
Objetivo	Detectar cambios no autorizados en archivos críticos del sistema.
Metodología	Configuración de Wazuh para monitorear directorios específicos y archivos críticos. Implementación de reglas de monitoreo en tiempo

	real para detectar modificaciones, creaciones y eliminaciones de archivos.
Resultados	Detección de Cambios: Se configuró Wazuh para monitorear archivos en los directorios críticos. Se detectaron y registraron todas las modificaciones, creaciones y eliminaciones de archivos en tiempo real. Alertas Generadas: Wazuh generó alertas instantáneas para cada cambio detectado, notificando al equipo de seguridad a través del correo electrónico y registrando los eventos en el panel de control de Wazuh.
Impacto	El monitoreo de integridad de archivos con Wazuh mejoró significativamente la capacidad de la institución para detectar y responder a cambios no autorizados en archivos críticos, proporcionando una capa adicional de seguridad.

Proceso Detallado

Para un análisis detallado del proceso de detección de vulnerabilidades y ejemplos específicos, consulte el Apéndice A: Monitoreo de Integridad de Archivo

Configuración de Monitoreo de integridad:

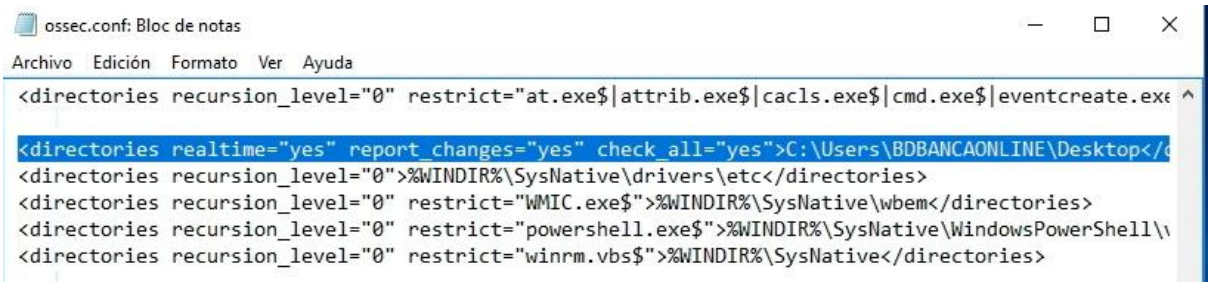
Tabla 6

Configuración del Archivo ossec.conf para el Endpoint

Elemento	Detalle
Ubicación del archivo de configuración local del endpoint	C://Program Files(x86)/ossec-agent/
Nombre del archivo de configuración a modificar	ossec.conf
Editor de archivo de configuración	Bloc de notas
Línea que se debe agregar o modificar	<directories realtime="yes" report_changes="yes" check_all="yes"> C:\Users\BDBANCAONLINE\Desktop </directories>
Descripción de lo ingresado en cada instrucción	
realtime="yes"	Activa la detección en tiempo real, permitiendo que el sistema identifique y registre cambios tan pronto como ocurren.
report_changes="yes"	Habilita el reporte de cambios, lo que significa que cualquier modificación en los archivos dentro del directorio será documentada.
check_all="yes"	Establece la revisión completa del directorio, asegurando que todos los archivos sean monitoreados.

Figura 29

Directorio de archivos monitoreados.

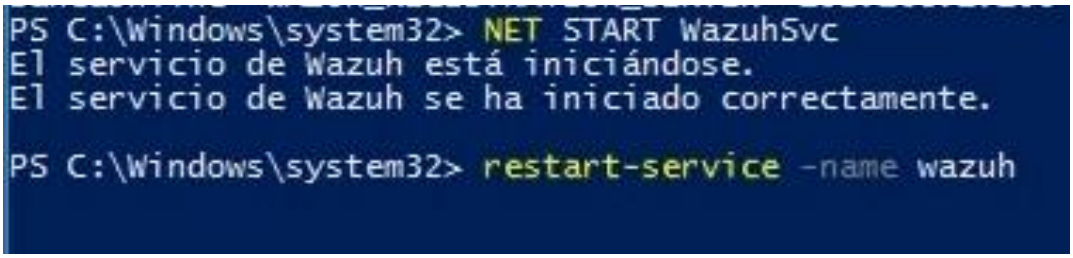


Al especificar el directorio del escritorio de la cuenta BDBANCAONLINE de la Figura 29, se configura Wazuh para registrar todos los cambios que ocurran en esta ubicación.

Es necesario reiniciar el servicio del agente de Wazuh (ver Figura 30) para que los cambios surjan efecto. Para lo cual en modo admin abrimos el Windows PowerShell y ejecutamos el siguiente comando. Restart-service -name wazuh

Figura 30

Reiniciar el servicio.



Caso de Uso 2: Detección de Vulnerabilidades

Tabla 7

Detección de Vulnerabilidades

Aspecto	Descripción
Objetivo	Identificar y alertar sobre vulnerabilidades presentes en el sistema.
Metodología	Configuración de Wazuh para realizar escaneos periódicos de vulnerabilidades. Generación de informes detallados sobre vulnerabilidades encontradas y recomendaciones para su mitigación.

Resultados	Identificación de Vulnerabilidades: Wazuh identificó múltiples vulnerabilidades críticas en el sistema, clasificándolas según su nivel de riesgo. Alertas Generadas: Se generaron alertas para cada vulnerabilidad detectada, proporcionando detalles específicos y recomendaciones para su mitigación.
Impacto	La detección de vulnerabilidades con Wazuh permitió a la institución identificar y mitigar vulnerabilidades críticas de manera oportuna, reduciendo el riesgo de explotación por parte de actores maliciosos.

Proceso Detallado

Para un análisis detallado del proceso de detección de vulnerabilidades y ejemplos específicos, consulte el Apéndice B: Caso de Análisis de Vulnerabilidades.

Configuración de detección de vulnerabilidades:

Ubicación de archivo de configuración en webservice de Wazuh, página principal: Wazuh – Management – Configuration – Edit configuration.

Nombre del archivo de configuración a modificar:ossec.conf

Editor de archivo de configuración: Management configuration – webservice (ver Figura 31).

Figura 31

Módulo de configuración.

Figura 32

Editar el archivo el detector de vulnerabilidad

```
104  <vulnerability-detector>
105    <enabled>yes</enabled>
106    <interval>5m</interval>
107    <min_full_scan_interval>6h</min_full_scan_interval>
108    <run_on_start>yes</run_on_start>
```

Figura 33

Editar el archivo provider

```
183    <!-- Windows OS vulnerabilities -->
184    <provider name="msu">
185      <enabled>yes</enabled>
186      <update_interval>1h</update_interval>
187    </provider>
```

Tabla 8

Configuración del Detector de Vulnerabilidades en Wazuh

Descripción de lo ingresado en cada instrucción	Detalle
<enabled>yes</enabled>	Activa la detección del módulo de vulnerabilidades en los equipos con agentes.
<interval>30m</interval>	Intervalo de escaneo de vulnerabilidades parciales.
<min_full_scan_interval>2h</min_full_scan_interval>	Intervalo de escaneo de vulnerabilidades completo.
<!-- Windows OS vulnerabilities -->	Comentario para las vulnerabilidades del sistema operativo Windows.
<enabled>yes</enabled>	Activa la detección de vulnerabilidades para los sistemas operativos Windows que tengan agentes de Wazuh.

Proceso de Guardado de Información

1. **Guardado de la configuración**:

   - Guardamos la configuración al dar click en SAVE.
   - Si todo está bien configurado, se mostrará un mensaje indicando que todo fue guardado correctamente.

2. **Restaurar el servicio**:

   - Procedemos a restaurar el servicio dando click en Restart Manager.

Visualización de Vulnerabilidades de los Agentes

1. **Ubicación**:

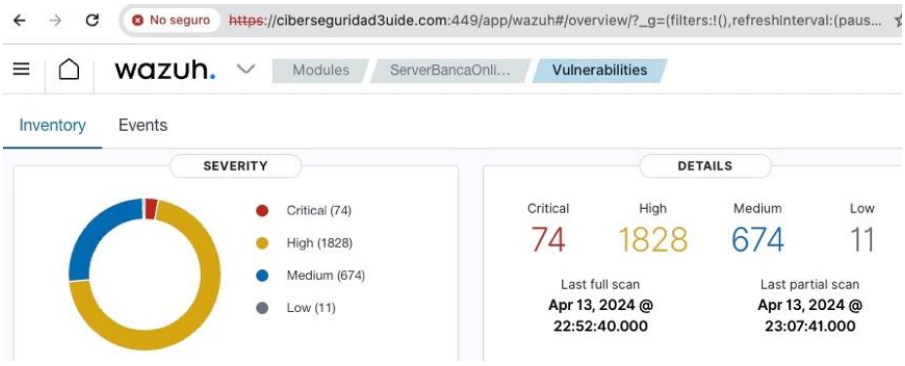
- Wazuh – Modules – Vulnerabilities.

2. **Proceso:**

- Seleccionamos el agente y visualizamos las vulnerabilidades del equipo (ver Figura 34).

Figura 34

Vulnerabilidades



Caso de Uso 3: Integración con VirusTotal

Tabla 9

Integración con VirusTotal

Aspecto	**Descripción**
Objetivo	Detectar y analizar archivos sospechosos utilizando la base de datos de VirusTotal.

Metodología	Integración de Wazuh con VirusTotal para escanear archivos sospechosos en tiempo real. Configuración de reglas para enviar archivos a VirusTotal automáticamente y analizar los resultados.
Resultados	Análisis de Archivos: Wazuh envió archivos sospechosos a VirusTotal para su análisis. VirusTotal proporcionó un análisis detallado y una clasificación de amenazas para cada archivo. Alertas Generadas: Wazuh generó alertas basadas en los resultados del análisis de VirusTotal, notificando al equipo de seguridad sobre archivos maliciosos detectados.
Impacto	La integración de Wazuh con VirusTotal mejoró la capacidad de la institución para detectar y analizar archivos sospechosos en tiempo real, proporcionando información crítica para la respuesta a incidentes.

Proceso Detallado

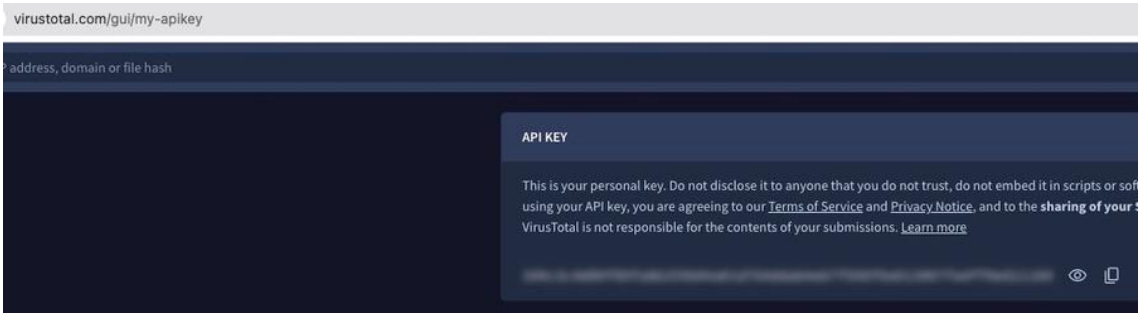
Para un análisis detallado del proceso de detección de vulnerabilidades y ejemplos específicos, consulte el Apéndice C: Caso de Análisis de Vulnerabilidades.

Configuración de detección e integración con VirusTotal:

Prerrequisito: Registrarse en la página de VirusTotal y obtener una cuenta gratuita, copiar el código API desde la página autenticada de VirusTotal y tenerlo respaldado para la configuración de Wazuh. (ver Figura 35).

Figura 35

Registrar en la página de VirusTotal.



Ubicación de archivo de configuración en webservice de Wazuh, página principal:

Wazuh – Management – Configuration – Edit configuration.

Nombre del archivo de configuración a modificar de la Figura 36: ossec.conf

Editor de archivo de configuración: Management configuration – webservice

Figura 36

Editar el archivo ossec.conf

Línea que se debe agregar o modificar (ver Figura 37 y 38):

<integration>

<name>virustotal</name>

<api_key>349c3c4d00f09255b04a01d764ddab4eb7f508f8aff0e621160</api_key> <!- - Replace with your VirusTotal API key -->

<group>syscheck</group>

<alert_format>json</alert_format>

</integration>

Figura 37

Editar el archivo la integración

```
<!-- Integracion Virus_Total -->

<integration>
<name>virustotal</name>
<api_key>349c3c4d00f09fa8b255b04a01d764ddab4eb7f50
<group>syscheck</group>
<alert_format>json</alert_format>
</integration>
```

<syscheck>

<directories check_all="yes" realtime="yes">c:|virustotal</directories>

</syscheck>

Figura 38

Editar el archivo la verificación del sistema.

```
<syscheck>
<directories check_all="yes" realtime="yes">c:\virustotal</directories>
</syscheck>
```

La siguiente tabla detalla las configuraciones y procesos necesarios para integrar y configurar el monitoreo de archivos en tiempo real utilizando la API de VirusTotal y el sistema Wazuh. Cada entrada de la tabla explica los elementos clave y las instrucciones para su correcta implementación.

Tabla 10

Configuraciones VirusTotal en Wazuh

Elemento	Descripción
`<api_key>XXX</api_key>`	Las X deben ser reemplazadas por la cadena de conexión de la API de VirusTotal.
`<group>syscheck</group>`	Nombre del grupo para identificar a los endpoints pertenecientes al grupo.
`<alert_format>json</alert_format>`	Formato para la alerta de VirusTotal.
`realtime="yes"`	Activa la detección en tiempo real, permitiendo que el sistema identifique y registre cambios tan pronto como ocurren.

`check_all="yes"`	Establece la revisión completa del directorio, asegurando que todos los archivos sean monitoreados.
`<directories>c:\virustotal</directories>`	Directorio para monitorear.
Proceso de guardado de información	**Descripción**
Guardado de configuración	Guardamos la configuración al dar click en SAVE. Si todo está bien configurado, nos dará un mensaje de que todo fue guardado y procedemos a restaurar el servicio dando click en Restart Manager.
Ubicación de archivo de configuración local de endpoint	**Descripción**
Ruta de archivo	C://Program Files(x86)/ossec-agent/
Nombre del archivo	ossec.conf
Editor de archivo	Bloc de notas
Línea que se debe agregar o modificar (ver Figura 39)	`<directories realtime="yes">C:\virustotal</directories>`
Descripción de lo ingresado en cada instrucción	**Descripción**
`realtime="yes"`	Activa la detección en tiempo real, permitiendo que el sistema identifique y registre cambios tan pronto como ocurren.
`<directories>C:\virustotal</directories>`	Directorio que debe ser monitoreado.

Figura 39

Activación la detención en tiempo real.

```
    <disabled>no</disabled>

<directories realtime="yes">C:\virustotal</directories>

    <!-- Frequency that syscheck is executed default every 12
```

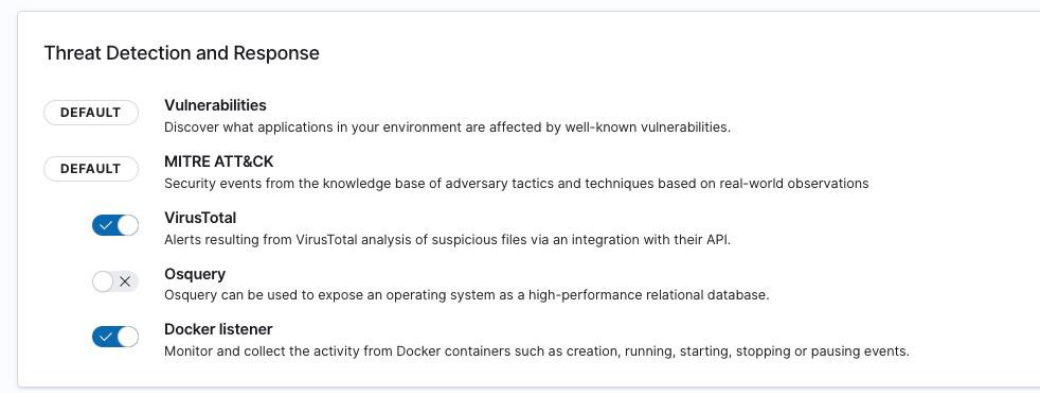
Al especificar el directorio c:\virustotal, se configura Wazuh para registrar y enviar muestras o hash de todos los archivos de ese directorio hacia virustotal con esto podemos observar en tiempo real si se colocan archivos maliciosos en el directorio.

Es necesario reiniciar el servicio del agente de Wazuh como se observa en la Figura 30 para que los cambios surjan efecto

Activación módulo de VirusTotal: Wazuh – Settings – Modules – habilitar VirusTotal (ver Figura 40)

Figura 40

Activación módulo de VirusTotal



Visualización de módulo de VirusTotal:

Ubicación: Wazuh – Modules – VirusTotal – seleccionamos el agente y visualizamos en tiempo real cuando se coloque un archivo en él directorio configurado (ver Figura 41).

Figura 41

Visualización de módulos, administración y herramientas

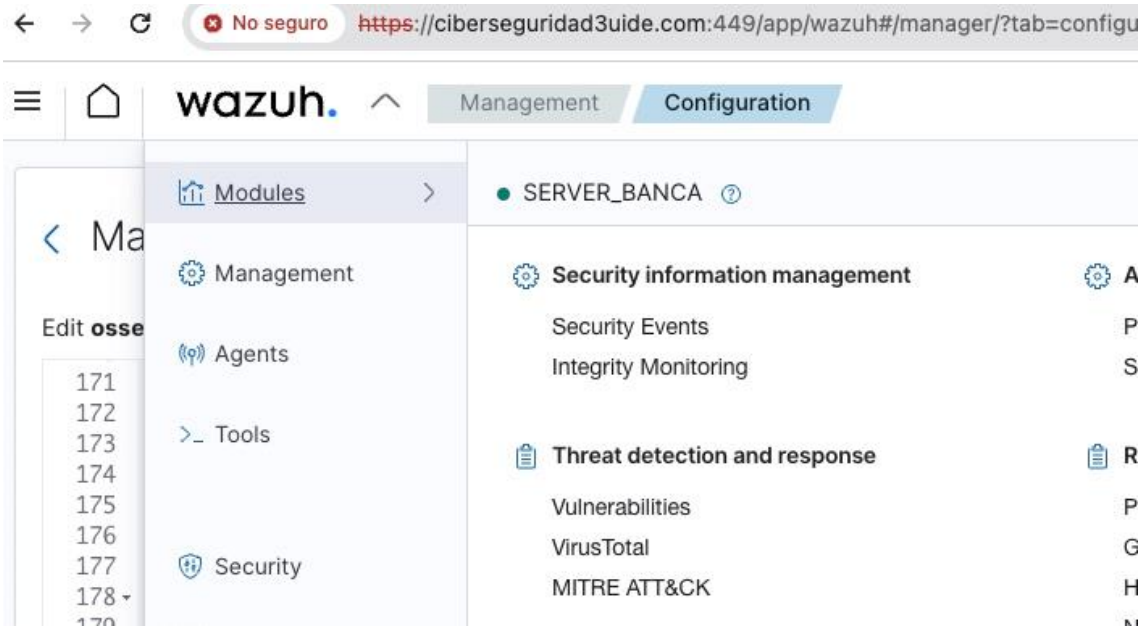
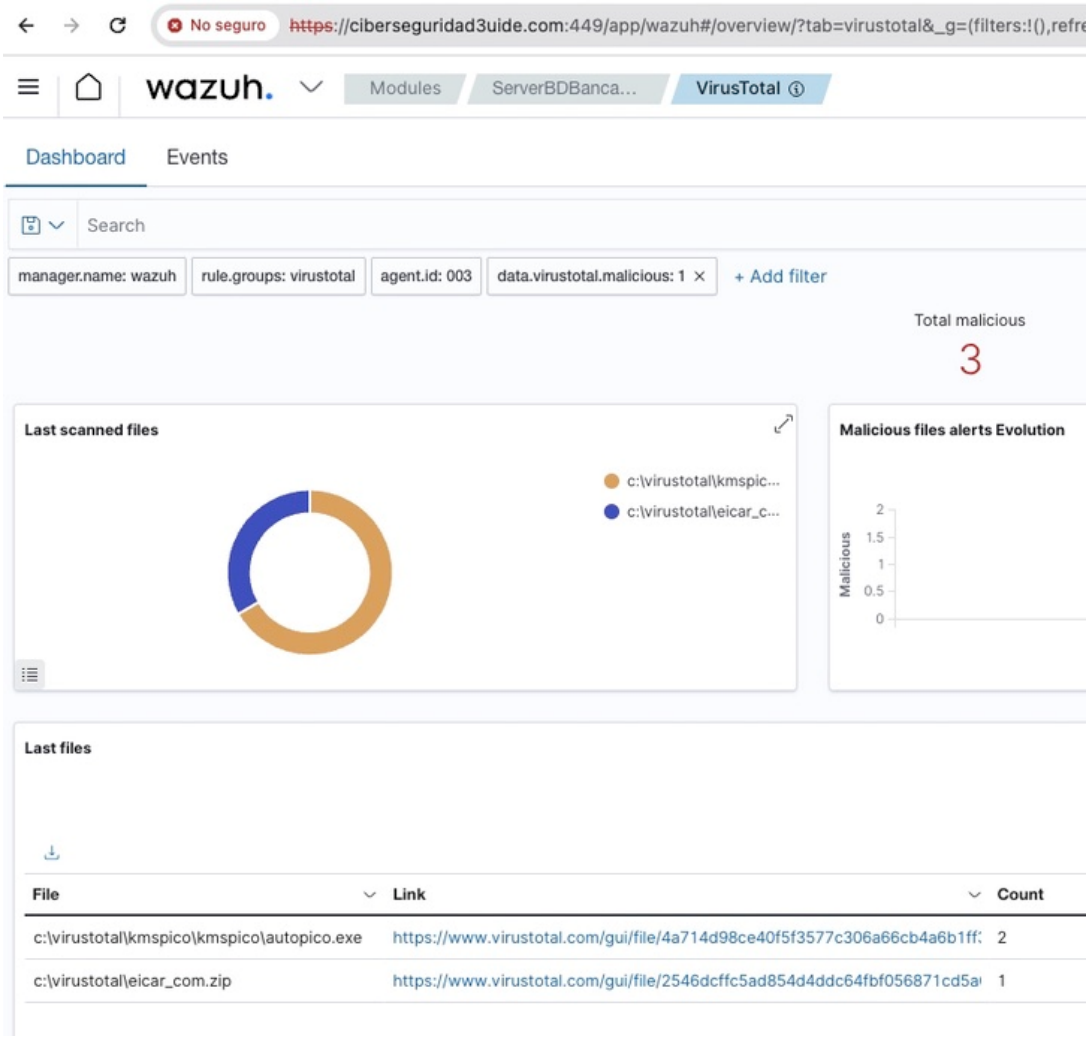


Figura 42

Visualización de módulo de VirusTotal en Dashboard



Pruebas de integración de VirusTotal con Wazuh

Para nuestras pruebas vamos a descargar 2 archivos que son conocidos como virus, uno es el KMSPICO y el otro es EICAR.

- KMSPICO se utiliza para activaciones de Windows y de Office, pero tiene alertas conocidas.

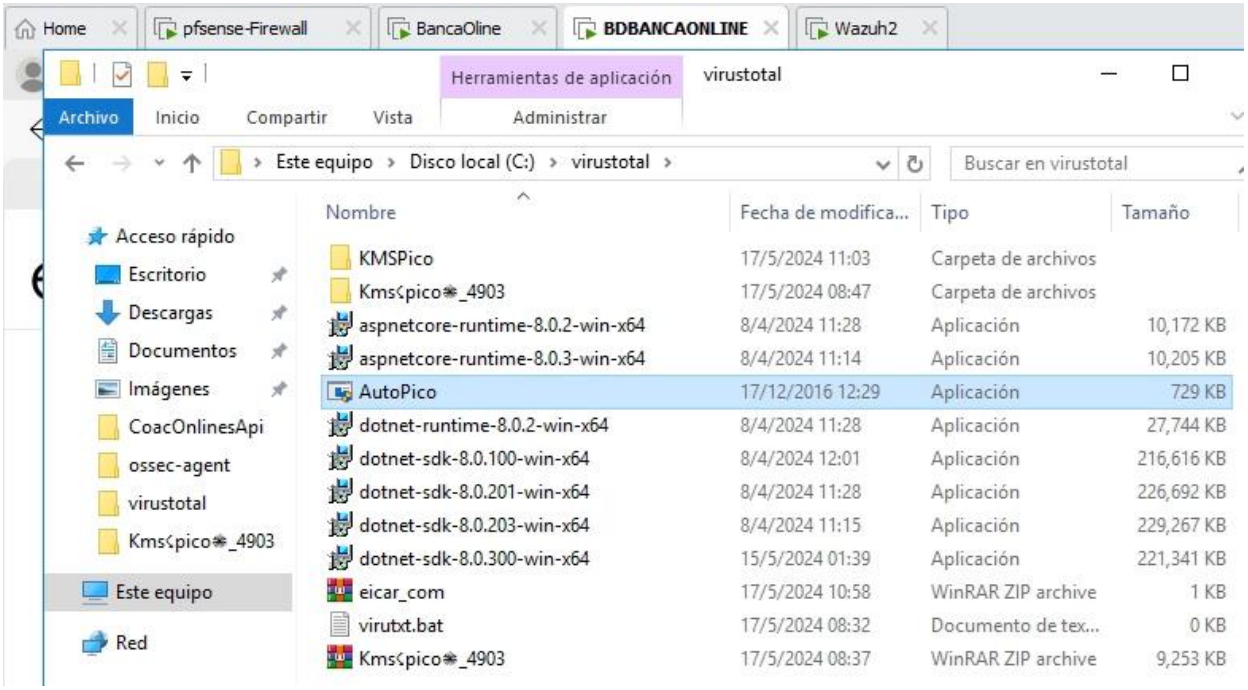
- EICAR es una página web que nos permite descargar un archivo detectado como virus por varios sensores por lo tanto procedemos con la descarga de este. Como podemos

ver en la siguiente imagen agregamos varios archivos para confirmar que se detectan y cuáles no.

- Eicar por seguridad lo deje comprimido para ver si se detecta sin descomprimir.

Figura 43

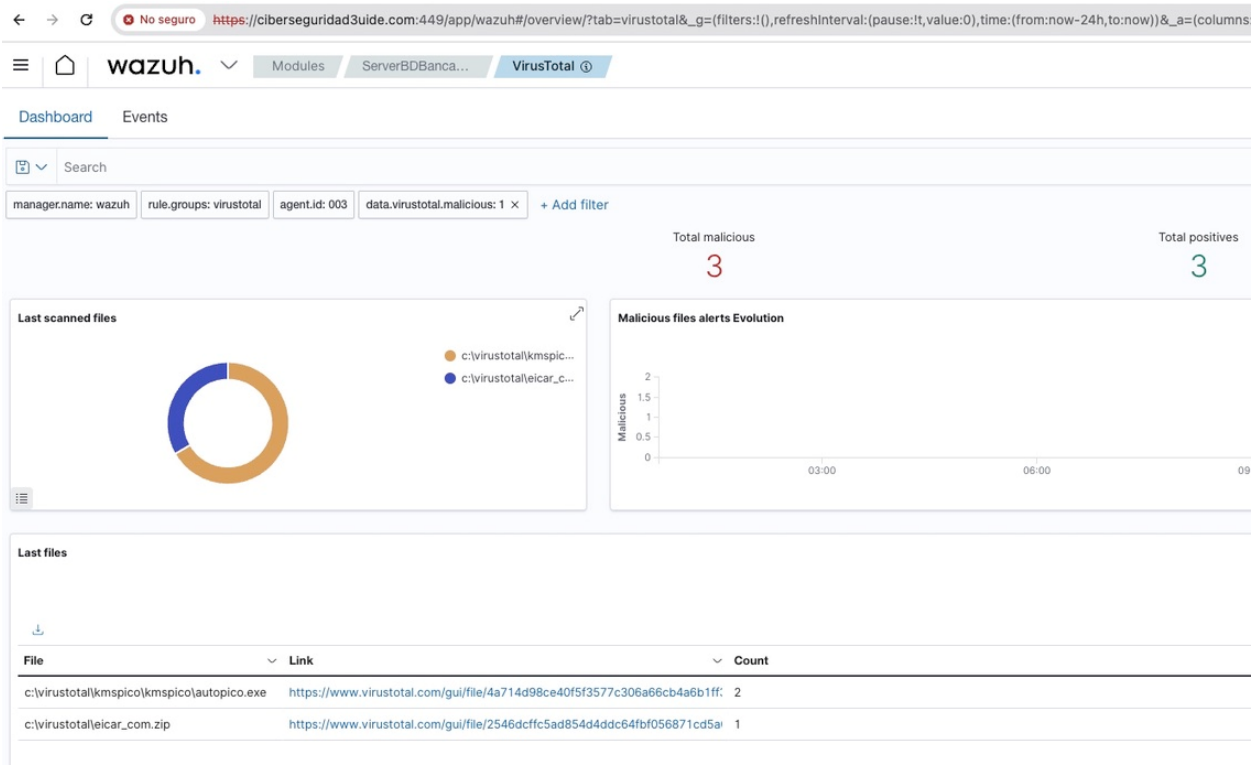
Ubicación en el EndPoint de los archivos infectados para análisis de VirusTotal.



Damos clic a refrescar en VirusTotal para actualizar el escaneo en tiempo real y podemos observar que tenemos 3 vulnerabilidades, Autopico lo detecta 2 veces y Eicar 1 solo vez, lo detecta enseguida como archivo malicioso y nos da un enlace directo a VirusTotal para poder revisar de que se trata la amenaza.

Figura 44

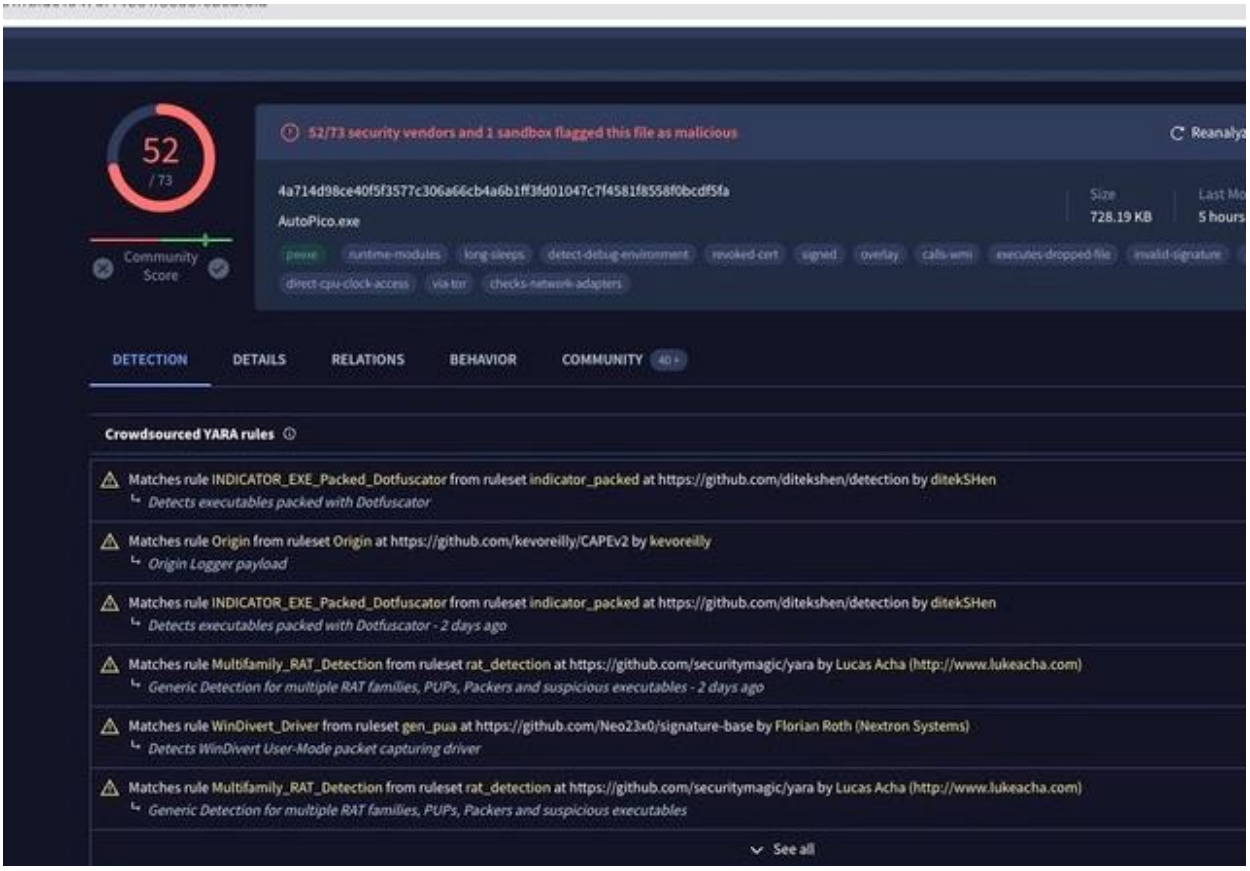
Wazuh Server – VirusTotal, archivos detectados peligrosos.



Damos clic al primer link y observamos lo siguiente.

Figura 45

Pantalla de VirusTotal con información de la vulnerabilidad KMS detectada.

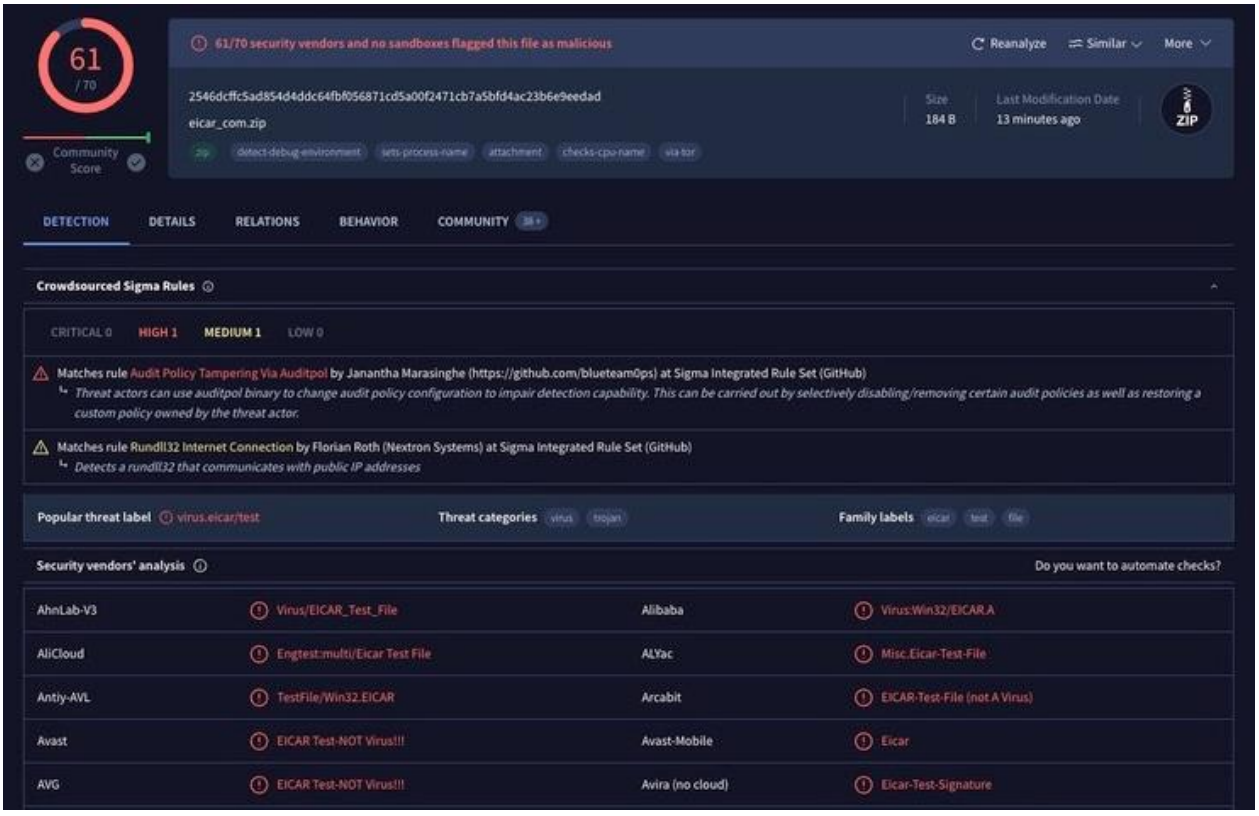


Nos indica que el archivo AutoPico.exe fue detectado como software malicioso en 52 de 73 detectores de virus, por lo tanto, pudimos validar que la integración está funcionando con VirusTotal.

Como segundo punto procedemos a dar clic en el segundo enlace y nos presenta lo siguiente.

Figura 46

Pantalla de VirusTotal con información de la vulnerabilidad EICAR detectada.



Nos indica que el archivo eicar_com.zip si presenta una amenaza y fue alertada por 61 de 70 revisores de virus.

Con esta prueba podemos definir que la configuración del API con VirusTotal, como la configuración del Endpoint y la configuración del Server Wazuh está integrada de manera correcta y al momento se encuentra analizando archivos en el directorio determinado.

Conclusiones

El presente estudio ha demostrado que el uso de Wazuh como plataforma SIEM en un entorno controlado de laboratorio es efectivo para mejorar la seguridad de los servicios de banca en línea. A través de la implementación de monitoreo de integridad de archivos, detección de vulnerabilidades e integración con VirusTotal, se ha logrado una detección y respuesta rápida a incidentes de seguridad.

Los principales hallazgos incluyen:

Monitoreo de Integridad de Archivos: La implementación de Wazuh FIM (File Integrity Monitoring) ha permitido detectar cambios no autorizados en archivos críticos del sistema, lo cual es esencial para prevenir compromisos del sistema.

Detección de Vulnerabilidades: Wazuh ha demostrado ser efectivo en la identificación de vulnerabilidades críticas, proporcionando informes detallados y recomendaciones para su mitigación.

Integración con VirusTotal: La integración con VirusTotal ha añadido una capa adicional de análisis de archivos sospechosos, mejorando la capacidad de respuesta ante posibles amenazas.

A lo largo del desarrollo de este proyecto de titulación, hemos aplicado gran parte de los conocimientos adquiridos durante la maestría, desde la configuración, implementación y evaluación de sistemas avanzados de seguridad. Este proyecto no solo resalta la importancia de

los sistemas SIEM en la banca en línea, sino también la necesidad de una configuración y monitoreo cuidadosos para maximizar su efectividad.

Recomendaciones

Para maximizar la efectividad de los sistemas SIEM en la banca en línea, se recomienda:

Personalización y Configuración Detallada: Realizar una configuración detallada y personalizada de los sistemas SIEM para adaptarse a las necesidades específicas de cada institución financiera.

Monitoreo Continuo: Implementar un monitoreo continuo y ajustes periódicos de las políticas de seguridad para responder a nuevas amenazas emergentes.

Capacitación Continua: Fomentar la capacitación continua del personal de TI en el uso y gestión de herramientas SIEM como Wazuh.

Integración de Herramientas: Considerar la integración de Wazuh con otros sistemas de detección y respuesta a incidentes para una cobertura de seguridad más amplia y robusta.

Evaluaciones Periódicas: Realizar evaluaciones periódicas del entorno de seguridad para identificar posibles mejoras y ajustar las estrategias de seguridad según sea necesario.

Trabajos Futuros

El presente estudio abre varias direcciones para futuras investigaciones:

Comparación de Herramientas SIEM: Explorar la efectividad de otras herramientas SIEM Open Source en diferentes entornos financieros y comparar sus resultados con los obtenidos con Wazuh.

Integración con Otros Sistemas: Investigar la integración de Wazuh con otros sistemas de detección y respuesta a incidentes para evaluar posibles mejoras en la capacidad de respuesta.

Capacitaciones y Efectividad: Evaluar la eficacia de las capacitaciones periódicas en seguridad cibernética para el personal de TI en la mejora del uso de sistemas SIEM.

Nuevas Aplicaciones y Mejoras: Proponer y probar nuevas aplicaciones o mejoras tecnológicas basadas en los hallazgos de este estudio para fortalecer la seguridad en la banca en línea.

Hacking Ético: Realizar un hacking ético para probar las herramientas configuradas y su actualización.

Referencias

AMSAT. (2024). *SIEM Architecture and Best Operational Practices for Modern Security Operations*. Recuperado el 17 de abril de 2024, de https://amsat.ai/siem-architecture-and-best-operational-practices-for-modern-security-operations/

Devoteam. (2024, febrero 2). *Enhancing Cybersecurity with Wazuh: The Open Source XDR & SIEM Platform*. Recuperado el 15 de abril de 2024, de https://www.devoteam.com

Exabeam. (2024). *SIEM Architecture: Technology, Process and Data*. Recuperado el 15 de abril de 2024, de https://www.exabeam.com/siem-guide/siem-architecture/

Halfond, W. G. J., Viegas, J., & Orso, A. (2006). *A Classification of SQL Injection Attacks and Countermeasures*. En Proceedings of the IEEE International Symposium on Secure Software Engineering (pp. 13-15). Recuperado de https://sites.cc.gatech.edu/home/orso/papers/halfond.viegas.orso.ISSSE06.pdf

ITware Latam. (2022). *Las 6 tendencias de la industria financiera en ciberseguridad*. Recuperado de https://www.itwarelatam.com

Netgate. (2023). *pfSense®: Your Next-Generation Firewall*. Recuperado de https://www.pfsense.org

SentinelOne. (2022). *Financial Cyber Threats: 10 Cases of Insider Bank Attacks*. Recuperado de https://www.sentinelone.com

Wazuh. (2024). *Documentation*. Recuperado el 15 de abril de 2024, de https://documentation.wazuh.com/

Zuñiga, L., Guarango, D., Morales, W., & Vallejo, F. (2024, mayo 28). GitHub. Obtenido de *pfsense-maestria-grupo-3*: https://github.com/lazuniga03/pfsense-maestria-grupo3.git

Zuñiga, L., Guarango, D., Morales, W., & Vallejo, F. (2024, mayo 28). GitHub. Obtenido de *Wazuh-maestria-grupo3*: https://github.com/lazuniga03/Wazuh-maestria-grupo3.git

Apéndice A: Monitoreo de Integridad de Archivos

Objetivo: Implementar y configurar el monitoreo de integridad de archivos utilizando Wazuh para detectar y registrar cambios en archivos y directorios específicos en el servidor ServerBDBancaOnline.

Segmentación del Análisis

Como parte del segundo módulo de control de Wazuh, se detalla a continuación el proceso para activar el control de cambios por carpeta o directorio en uno de los servidores con agente Wazuh instalado, específicamente en el servidor ServerBDBancaOnline.

Localización del Archivo de Configuración

Acceso al Directorio del Agente: Inicialmente, acceda al directorio donde se encuentra instalado el agente de Wazuh en el servidor, navegando a la ruta C://Program Files(x86)/ossec-agent/ (ver Figura A1).

Edición del Archivo de Configuración: Localice el archivo ossec.conf dentro de este directorio. Este archivo contiene la configuración central del agente de Wazuh y es crucial para la implementación del control de cambios.

Modificación del Archivo de Configuración

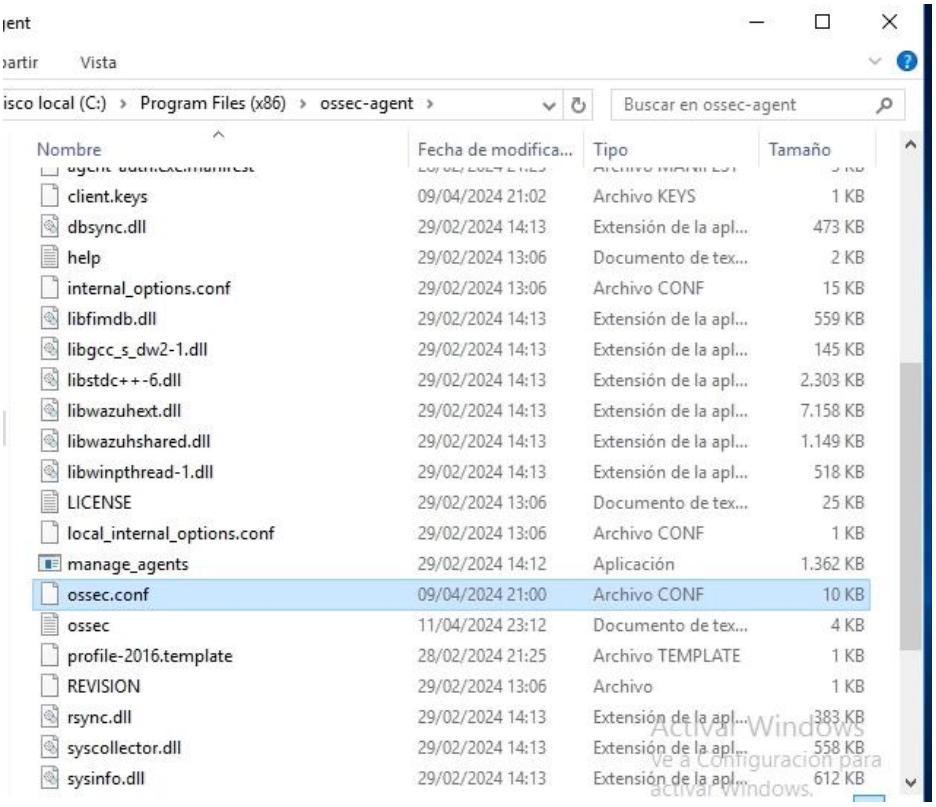
Abrir como Administrador: Para modificar el archivo ossec.conf, es necesario abrirlo con privilegios de administrador para evitar restricciones de permisos. Esto se puede hacer

utilizando un editor de texto como Notepad. Haga clic derecho sobre Notepad y seleccione "Ejecutar como administrador", luego abra el archivo desde el editor.

Realizar Cambios: Una vez abierto el archivo en el editor, proceda a realizar las configuraciones necesarias para activar el control de cambios en los directorios específicos que desee monitorear.

Figura A1

Directorio de agente de Wazuh en servidor.



Después de abrir el archivo ossec.conf con privilegios de administrador, se procede a configurar el monitoreo de directorios específicos en el servidor ServerBDBancaOnline. A continuación, se detallan los pasos para realizar esta configuración:

Búsqueda del Parámetro de Directorios. Búsqueda en el Archivo: Presione Ctrl + F para abrir la función de búsqueda en el editor de texto. Escriba "directories" en el cuadro de búsqueda para localizar rápidamente las líneas donde se configuran los directorios a monitorizar.

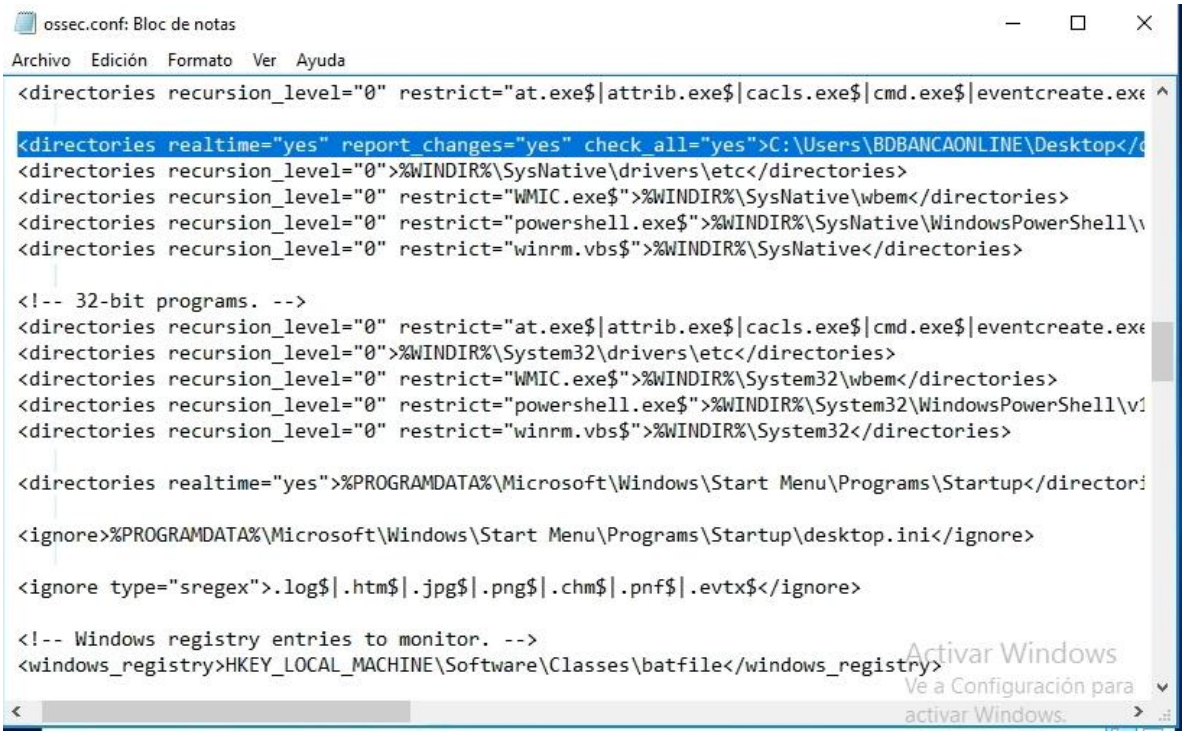
Tabla A1

Configuración de Monitoreo de Directorios en Wazuh

Paso	Descripción
Agregando el Directorio a Monitorear	Una vez localizadas las líneas pertinentes en el archivo de configuración, agregue la siguiente línea para especificar el directorio que desea monitorear: `<directories realtime="yes" report_changes="yes" check_all="yes">C:\Users\BDBANCAONLINE\Desktop</directories>`
Configuración de Parámetros	- `realtime="yes"`: Activa la detección en tiempo real, permitiendo que el sistema identifique y registre cambios tan pronto como ocurren. `report_changes="yes"`: Habilita el reporte de cambios, documentando cualquier modificación en los archivos dentro del directorio. `check_all="yes"`: Establece la revisión completa del directorio, asegurando que todos los archivos sean monitoreados.
Especificación del Directorio	Al especificar el directorio del escritorio de la cuenta BDBANCAONLINE, se configura Wazuh para registrar todos los cambios que ocurran en esta ubicación (ver Figura A2).
Guardando los Cambios	Para aplicar los cambios realizados, diríjase a la opción "Archivo" en el menú del editor de texto y seleccione "Guardar". Esto asegurará que todas las modificaciones en la configuración sean efectivas.

Figura A2

Archivo de configuración de Wazuh en servidor



Es necesario reiniciar el servicio del agente de Wazuh (ver Figura 39) para que los cambios surgan efecto. Para lo cual en modo admin abrimos el Windows PowerShell y ejecutamos el siguiente comando. Restart-service -name wazuh

Realizamos pruebas. En el server creamos el TXT “prueba de cambios wazuh” como se observa en la Figura A3.

Figura A3

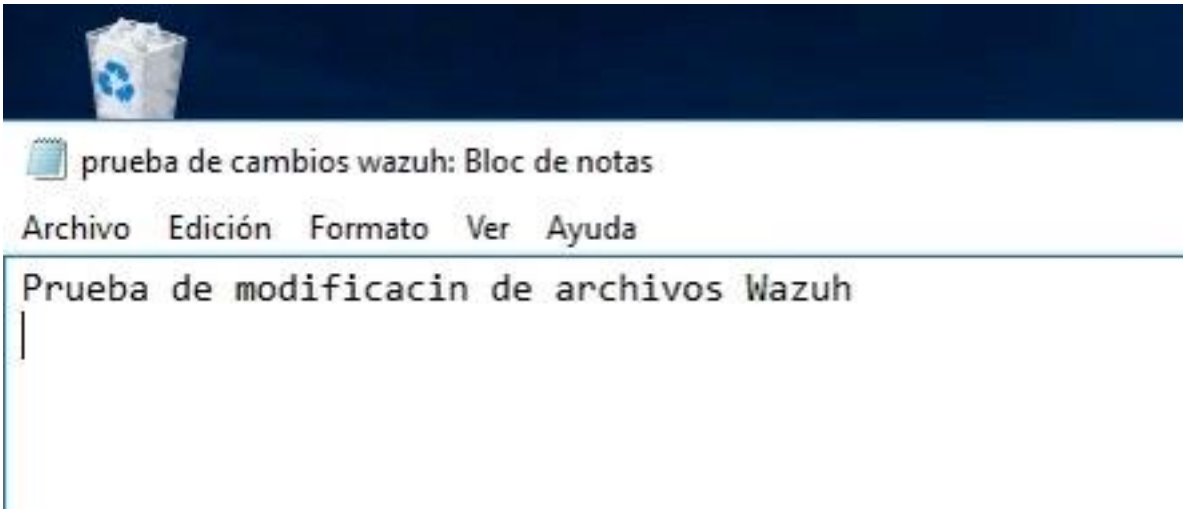
Escritorio de ServerBDBancaOnline

Luego modificamos el archivo y escribimos lo siguiente. “Prueba de modificación wazuh”

Damos click en archivo y en guardar (ver Imagen 4).

Figura A4

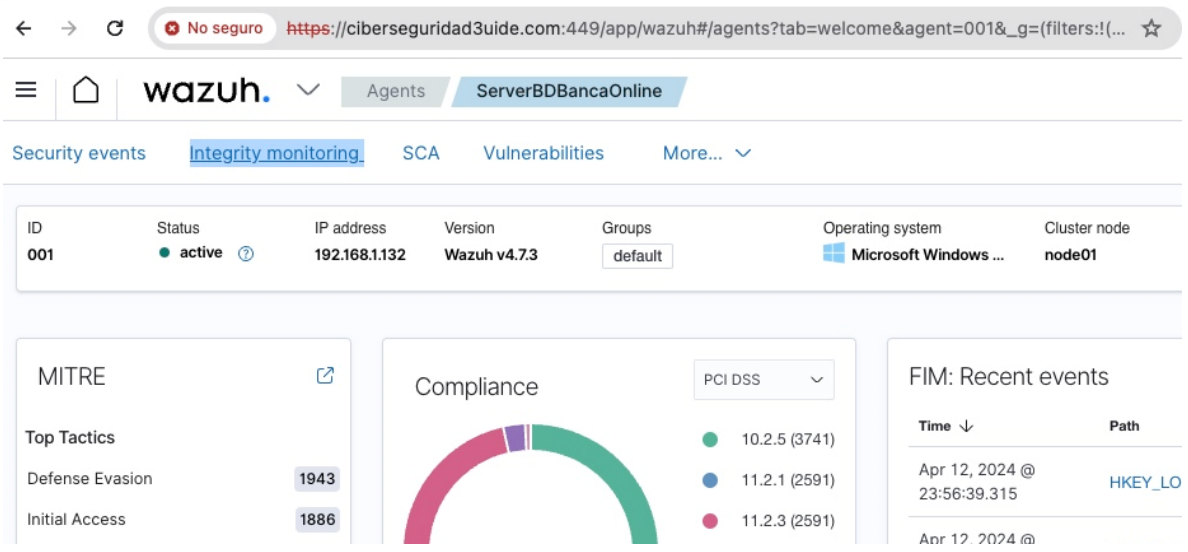
Visualización de modificación de archivo TXT



Vamos a ingresar a SERVER de Wazuh (ver Figura A5). Seleccionamos el ServerBDBancaOnline y damos click en Integrity monitoring.

Figura A5

Acceso a monitor de integridad



Una vez configurado el monitoreo del directorio, es crucial verificar que los eventos se estén registrando correctamente en Wazuh. Para ello, se procede de la siguiente manera:

Acceso a los Eventos. Navegación a Eventos: En la interfaz de usuario de Wazuh, haga clic en la opción "Events" para acceder al registro de eventos. Esto permite visualizar todas las actividades monitorizadas por el sistema.

Búsqueda de Eventos Específicos. Localización de la Auditoría: Busque en la lista hasta encontrar la línea que muestra la auditoría del documento creado. Esta línea proporcionará detalles básicos sobre la acción auditada (ver Figura A6).

Análisis de los Logs

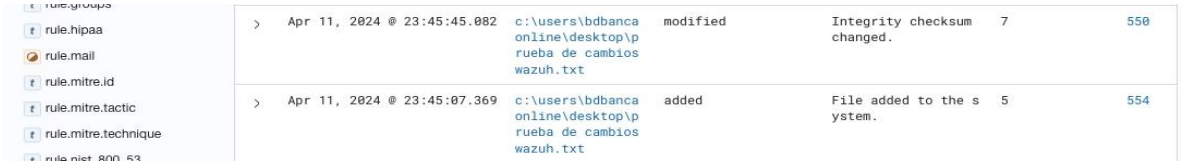
Detalles en los Logs: En los registros se puede observar que el sistema ya está generando logs correspondientes a las creaciones, modificaciones y eliminaciones de archivos en el directorio especificado.

Información Detallada: Cada log incluye información crucial como la fecha del evento, la ruta y el nombre del archivo afectado, así como la naturaleza de la acción realizada (creación, modificación, o eliminación) y un identificador único (ID).

Consulta de Más Información: Al hacer clic sobre un log específico, se puede acceder a información más detallada sobre el evento. Esto puede incluir detalles técnicos adicionales que son fundamentales para un análisis más profundo o para la resolución de problemas.

Figura A6

Visualización de cambios realizados en el monitor de integración



Realizamos una segunda prueba. Para lo cual creamos el archivo wazuh seguimiento 3 en el escritorio. Abrimos el archivo y escribimos lo siguiente “Texto nuevo de Wazuh 3”

Figura A7

Escritorio de ServerBDBancaOnline

Abrimos el Server para verificar la creación y la modificación. Observamos los siguientes estados (ver Figura A8).

- Id 554 se crea un documento TXT con nombre wazuh seguimiento 3.
- Id 553 se modifica el archivo TXT con nombre wazuh seguimiento 3.

Figura A8

Visualización de cambios realizados en el monitor de integración

	Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
›	Apr 12, 2024 @ 00:05:05.507	c:\users\bdbancaonline\desktop\wazuh seguimiento 3.txt	modified	Integrity checksum changed.	7	550
›	Apr 12, 2024 @ 00:01:11.253	c:\users\bdbancaonline\desktop\wazuh seguimiento 3.txt	added	File added to the system.	5	554

Para ver mayor detalle del cambio realizado en el documento damos click sobre la línea del log modificado y observamos lo siguiente en la Figura A9.

Figura A9

Visualización detallada de cambios realizados detectados por el monitor de integración.

t _index	wazuh-alerts-4.x-2024.04.12
t agent.id	001
t agent.ip	192.168.1.132
t agent.name	ServerBDBancaOnline
t decoder.name	syscheck_integrity_changed
t full_log	› File 'c:\users\bdbancaonline\desktop\wazuh seguimiento 3.txt' modified Mode: realtime Changed attributes: size,mtime,md5,sha1,sha256 Size changed from '0' to '24' Old modification time was: '1712898064', now it is '1712898305' Old md5sum was: 'd41d8cd98f00b204e9800998ecf8427e' New md5sum is : '51fa512efed16a3af8a69c3f52028d8c'

En la Figura A10 buscamos la línea syscheck.diff y podemos observar el texto que se modificó que es “Texto nuevo de wazuh 3” Podemos observar otra información importante como la fecha de creación y la fecha del cambio.

Figura A10

Visualización detallada de cambios realizados detectados por el monitor de integración.

Apéndice B: Caso de Análisis de Vulnerabilidades

Objetivo: Evaluar y mitigar la vulnerabilidad CVE-2024-21386 en el entorno de laboratorio utilizando las capacidades de detección de vulnerabilidades de Wazuh.

Segmentación del Análisis:

1. Identificación de la Vulnerabilidad:
    - Descripción y detalles de la vulnerabilidad CVE-2024-21386.
    - Fecha de publicación: 13 de febrero de 2024
    - Tipo de vulnerabilidad: Denegación de servicio bajo .NET
2. Proceso de Análisis:
    - Pasos para acceder a la información de la vulnerabilidad en Wazuh.
    - Visualización de la vulnerabilidad específica y detalles obtenidos.
3. Remediación de la Vulnerabilidad:
    - Procedimiento para actualizar los servidores Windows y remediar la vulnerabilidad.
    - Verificación de la efectividad de la remediación utilizando Wazuh.
4. Resultados:
    - Estado de las vulnerabilidades antes y después de la remediación.

- Evaluación de la efectividad del sistema de detección de vulnerabilidades de Wazuh.

Proceso Detallado

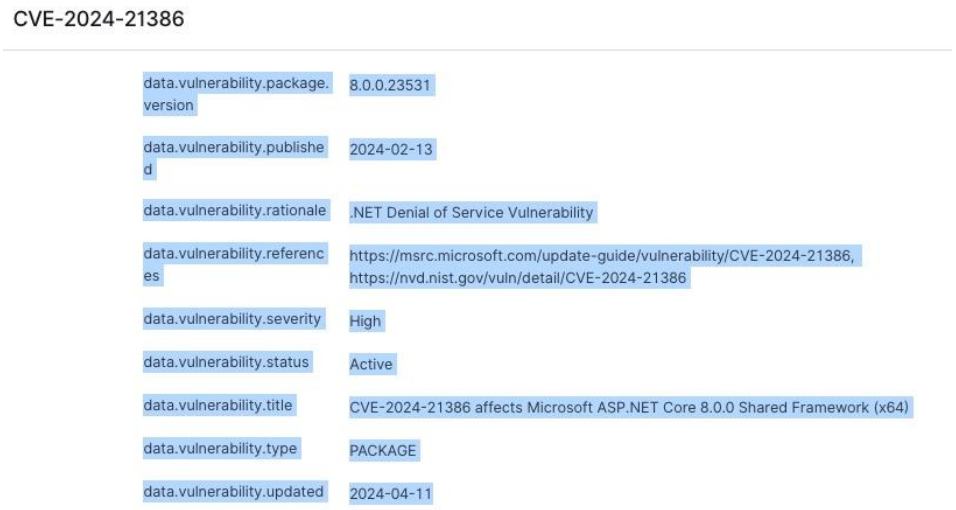
1. Identificación de la Vulnerabilidad:

Fecha de Publicación: La vulnerabilidad fue reportada el 13 de febrero de 2024 como se muestra en el campo data.vulnerability.published de la Figura B1.

Tipo de Vulnerabilidad: Esta también es clasificada como una vulnerabilidad de denegación de servicio bajo .NET detallada en el sistema bajo data.vulnerability.rationale como ".NET Denial of Service Vulnerability".

Figura B1

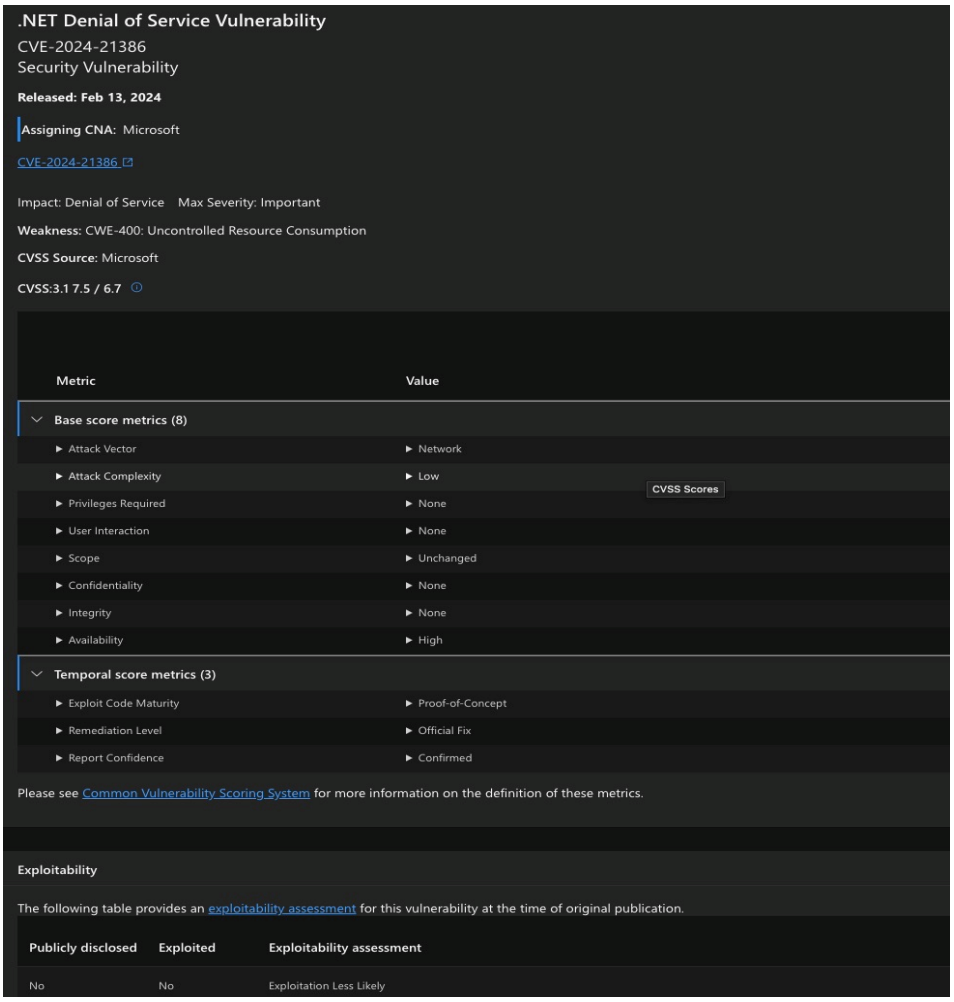
Tipo de vulnerabilidad



Damos click en el enlace acerca de la información de la vulnerabilidad. Podemos observar lo siguiente en la Figura B2.

Figura B2

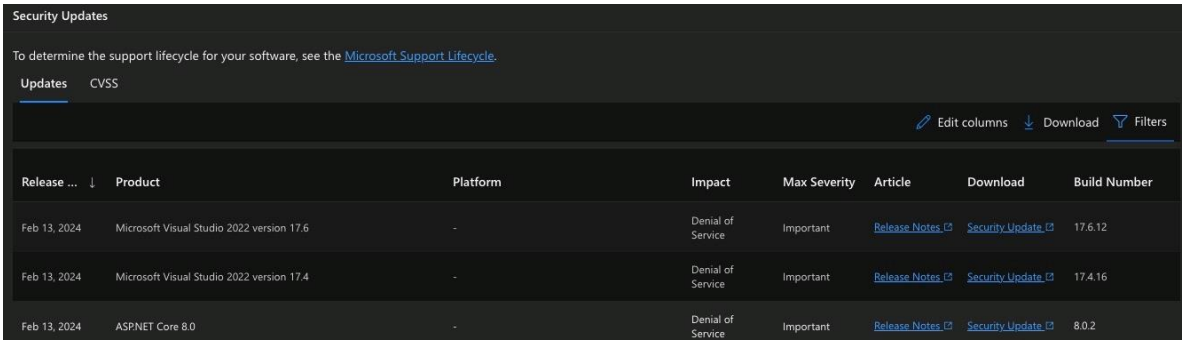
Información de vulnerabilidad.



En este caso no se pudo encontrar ninguna mitigación para la vulnerabilidad en la página oficial, pero buscando observamos el apartado Security Updates, en la cual vemos la página del componente ASP y Visual Studio donde podemos descargar las actualizaciones y volver a escanear para validar si al actualizar los componentes la vulnerabilidad queda mitigada.

Figura B3

Mitigación de vulnerabilidad.



Remediación de la Vulnerabilidad:

Para poder remediar las vulnerabilidades detectadas es importante actualizar nuestros servidores Windows ejecutando Windows Update en cada uno de ellos (ver Figura B4).

Tabla B1

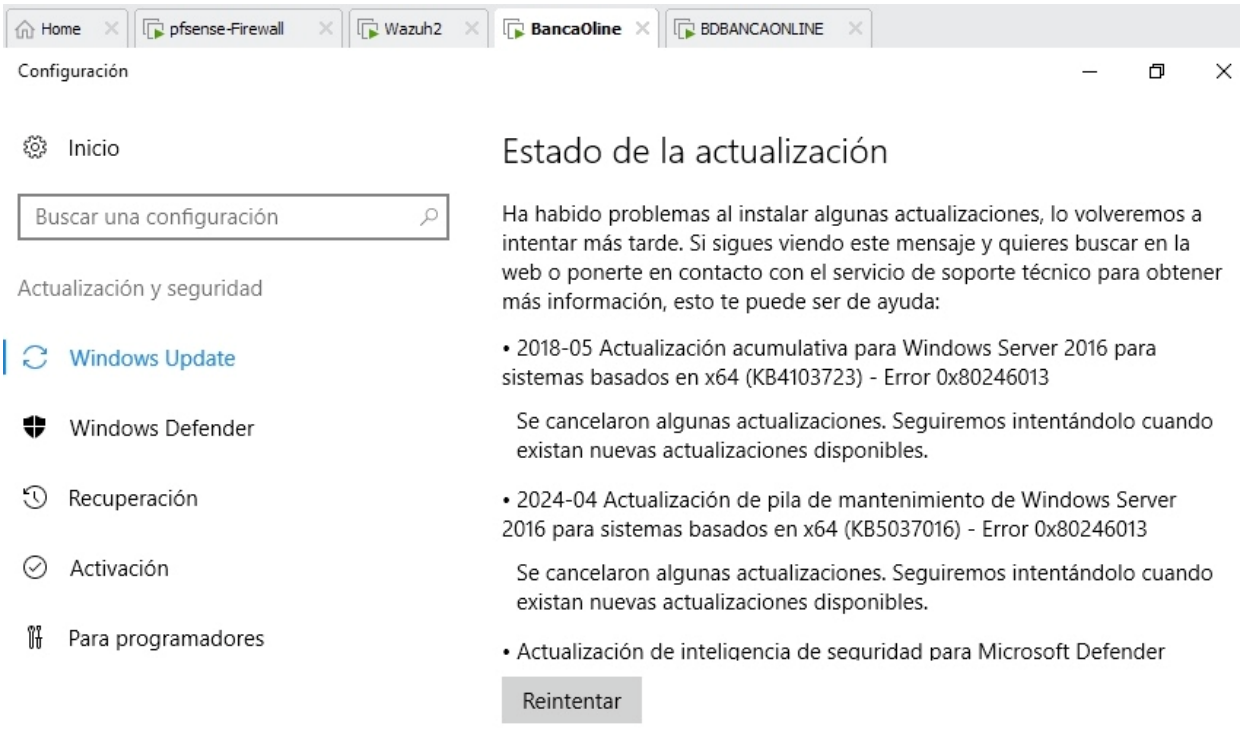
Tabla de Mitigación de vulnerabilidades

Proceso	Descripción
Actualizaciones Pendientes	Actualizaciones pendientes en los servidores Windows.
Actualizaciones Instaladas	Lista de actualizaciones que ya han sido instaladas.
Actualización Server BDBancaOnline en Curso	Proceso de actualización en el servidor BDBancaOnline.
Actualización Server BancaOnline en Curso	Proceso de actualización en el servidor BancaOnline.
Historial de Actualizaciones BDBANCAONLINE	Registro de actualizaciones aplicadas en BDBancaOnline.
Actualizaciones Acumulativas 2021-2023 en BancaOnline	Resumen de actualizaciones aplicadas durante 2021-2023.
Estado de Actualización de Equipo BancaOnline	Estado del dispositivo BancaOnline después de las actualizaciones.
Estado de Actualización de Equipo BDBancaOnline	Estado del dispositivo BDBancaOnline después de las actualizaciones.

Verificación de Historial de Actualizaciones BancaOnline a mayo 2024	Confirmación del estado de las actualizaciones en BancaOnline a mayo de 2024.
Verificación de Historial de Actualizaciones BDBancaOnline a mayo 2024	Confirmación del estado de las actualizaciones en BDBancaOnline a mayo de 2024.
Configuración del Escaneo de Vulnerabilidades en ossec.conf	Configuración del periodo de escaneo parcial cada 30 minutos y de escaneo total cada 2 horas.

Figura B4

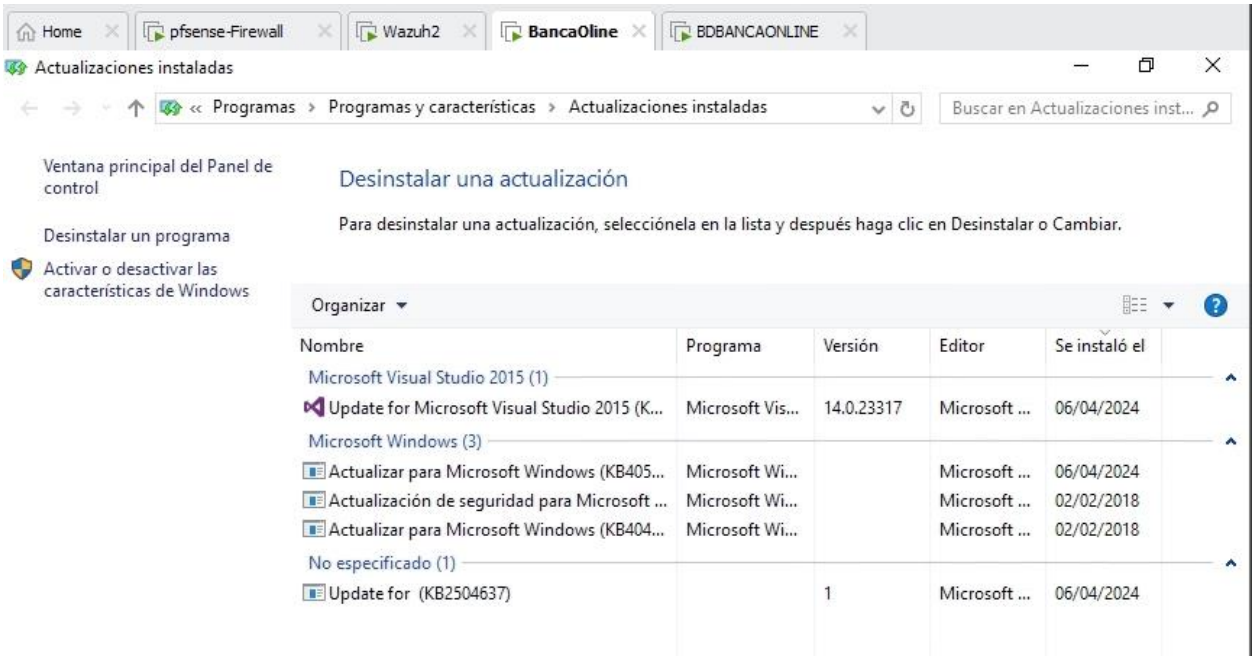
Remediación de vulnerabilidad.



- Actualizaciones pendientes (ver Figura B5).

Figura B5

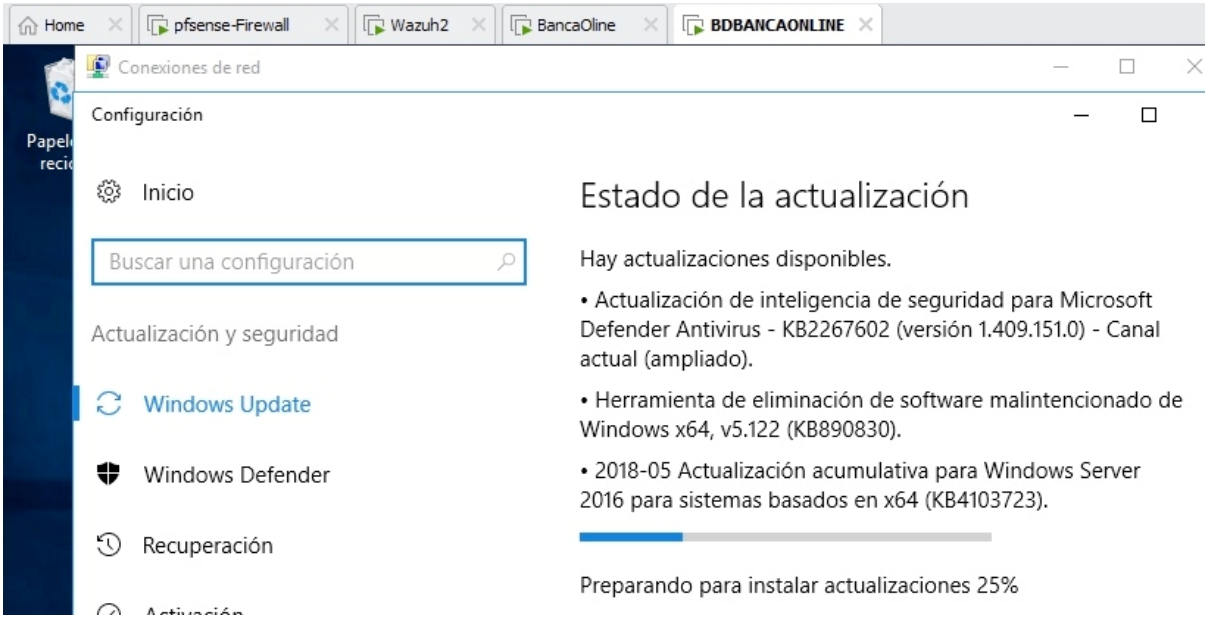
Actualizaciones pendientes.



- Actualizaciones instaladas (ver Figura B6).

Figura B6

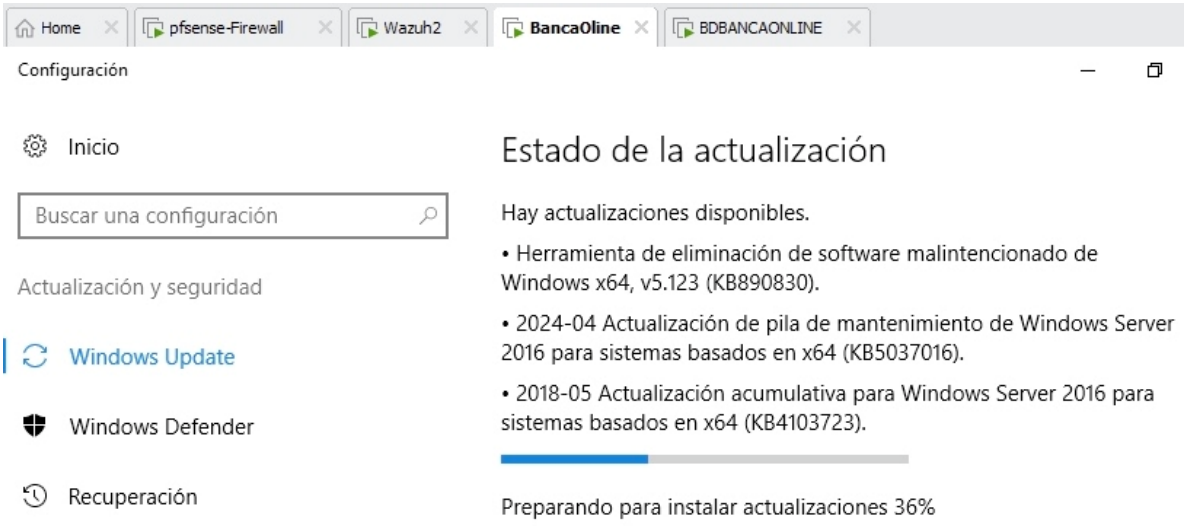
Actualizaciones instaladas.



- Actualización Server BDBancaOnline en curso (ver Figura B7).

Figura B7

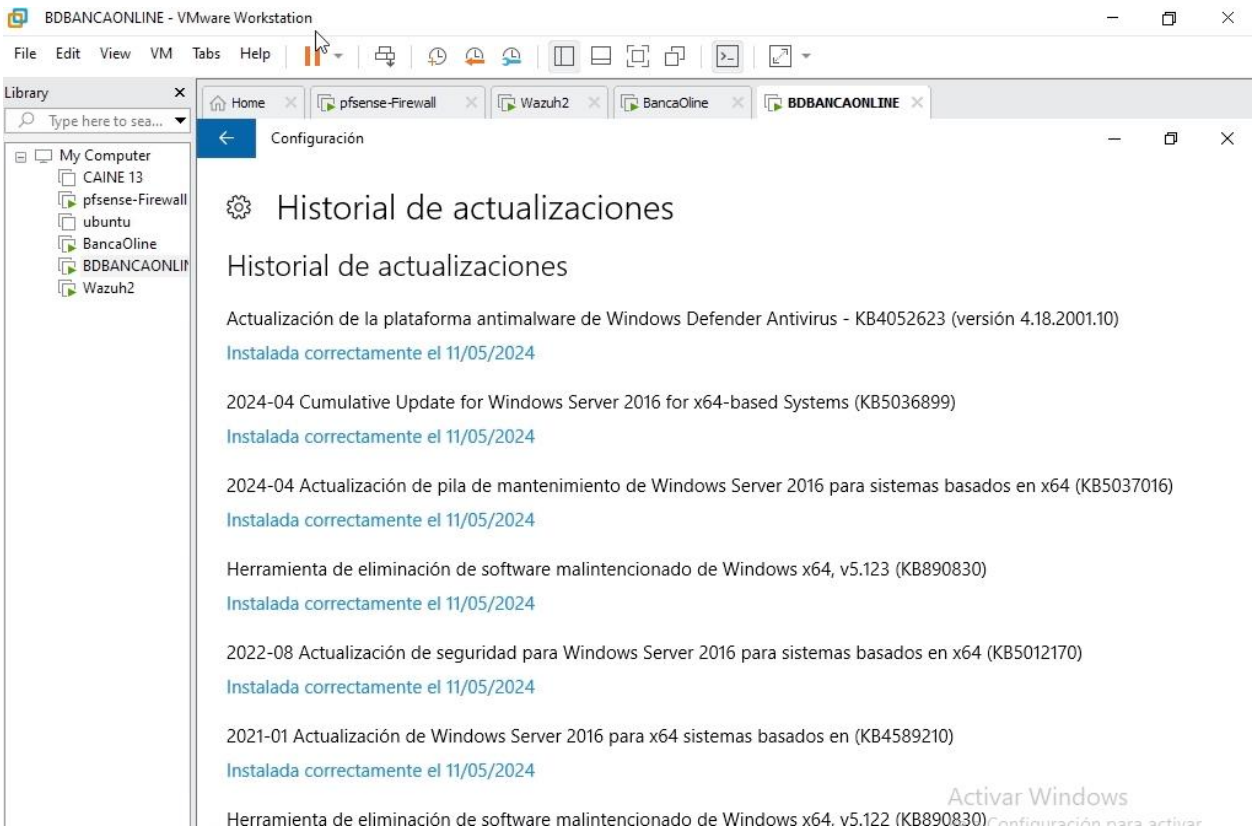
Actualizaciones instaladas.



- Actualización Server BancaOnline en curso (ver Figura B8).

Figura B8

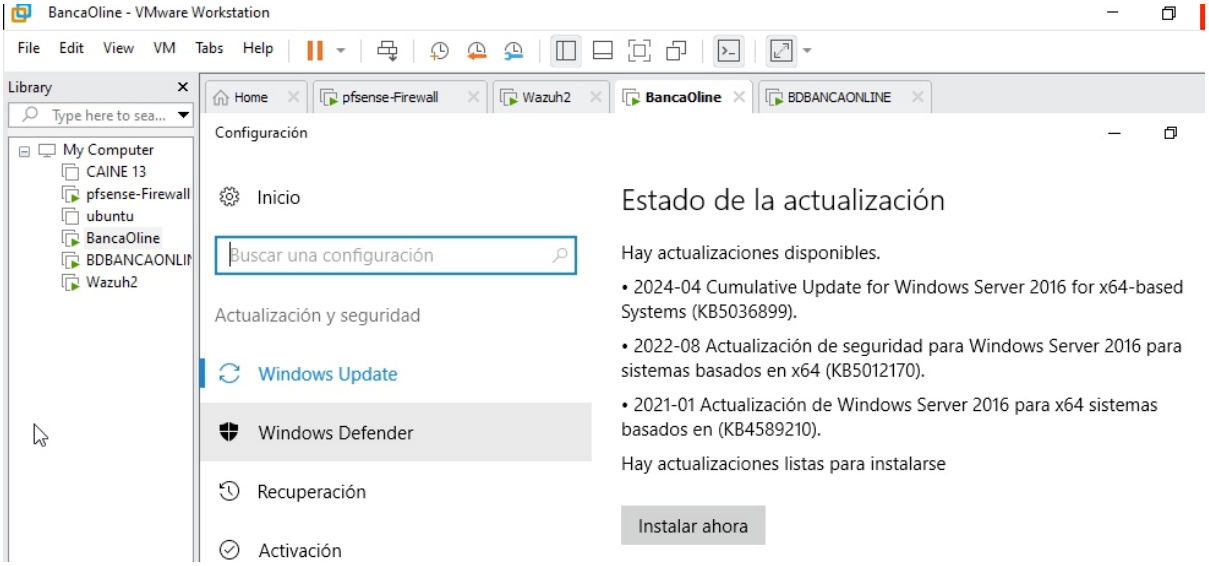
Historial de actualizaciones server.



- Historial de actualizaciones BDBANCAONLINE (ver Figura B9)

Figura B9

Historial y estado de actualizaciones server.



- Actualizaciones acumulativas 2021, 2022, 2023 en BancaOnline (ver Figura B10).

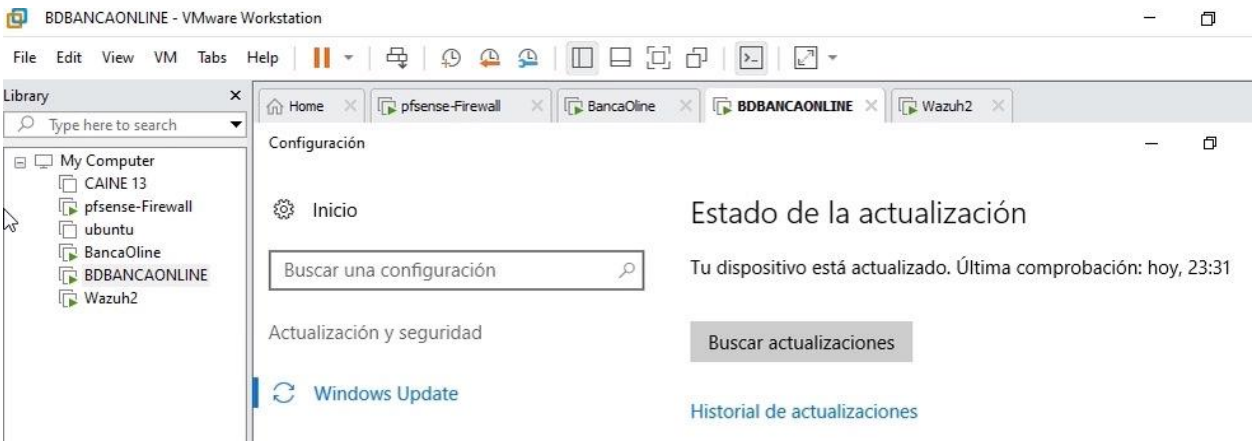
Figura B10

Actualizaciones acumulativas.

- Estado de actualización de equipo, BancaOnline, Dispositivo actualizado (ver Figura B11).

Figura B11

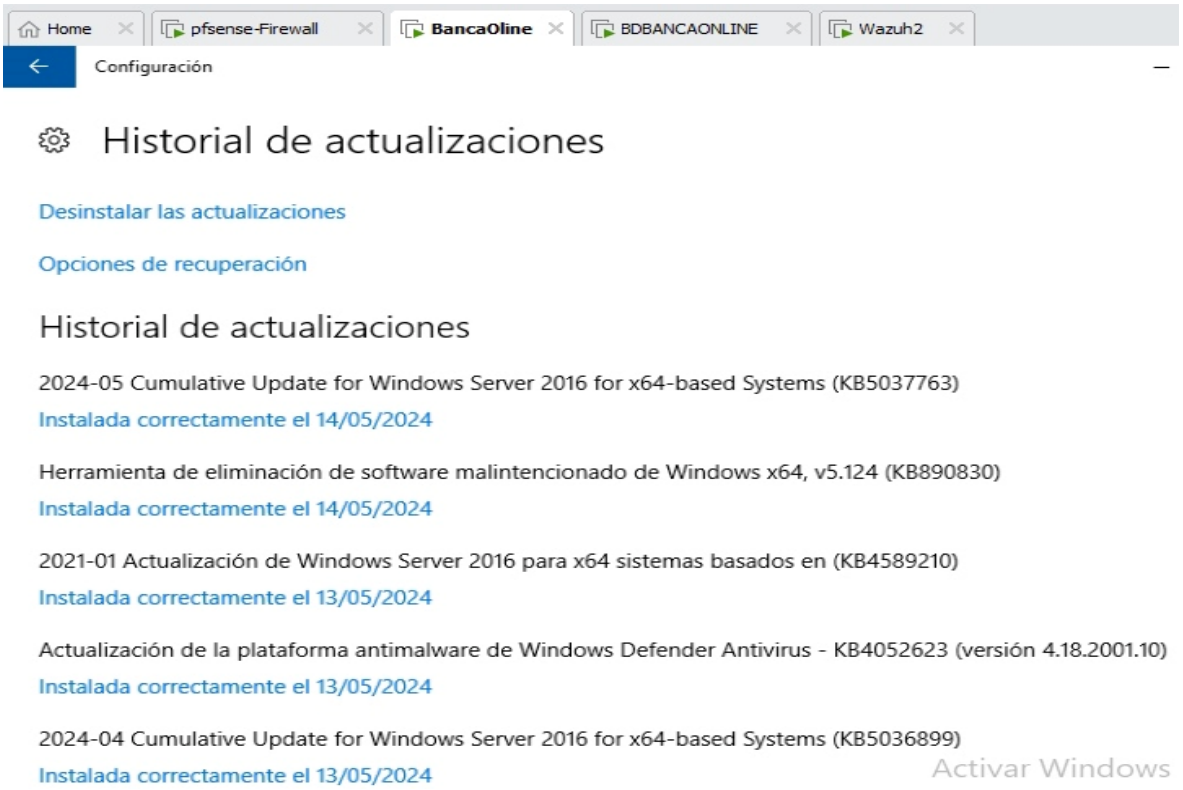
Estado de actualizaciones del equipo.



- Estado de actualización de equipo, BDBancaOnline, Dispositivo actualizado (ver Figura B12).

Figura B12

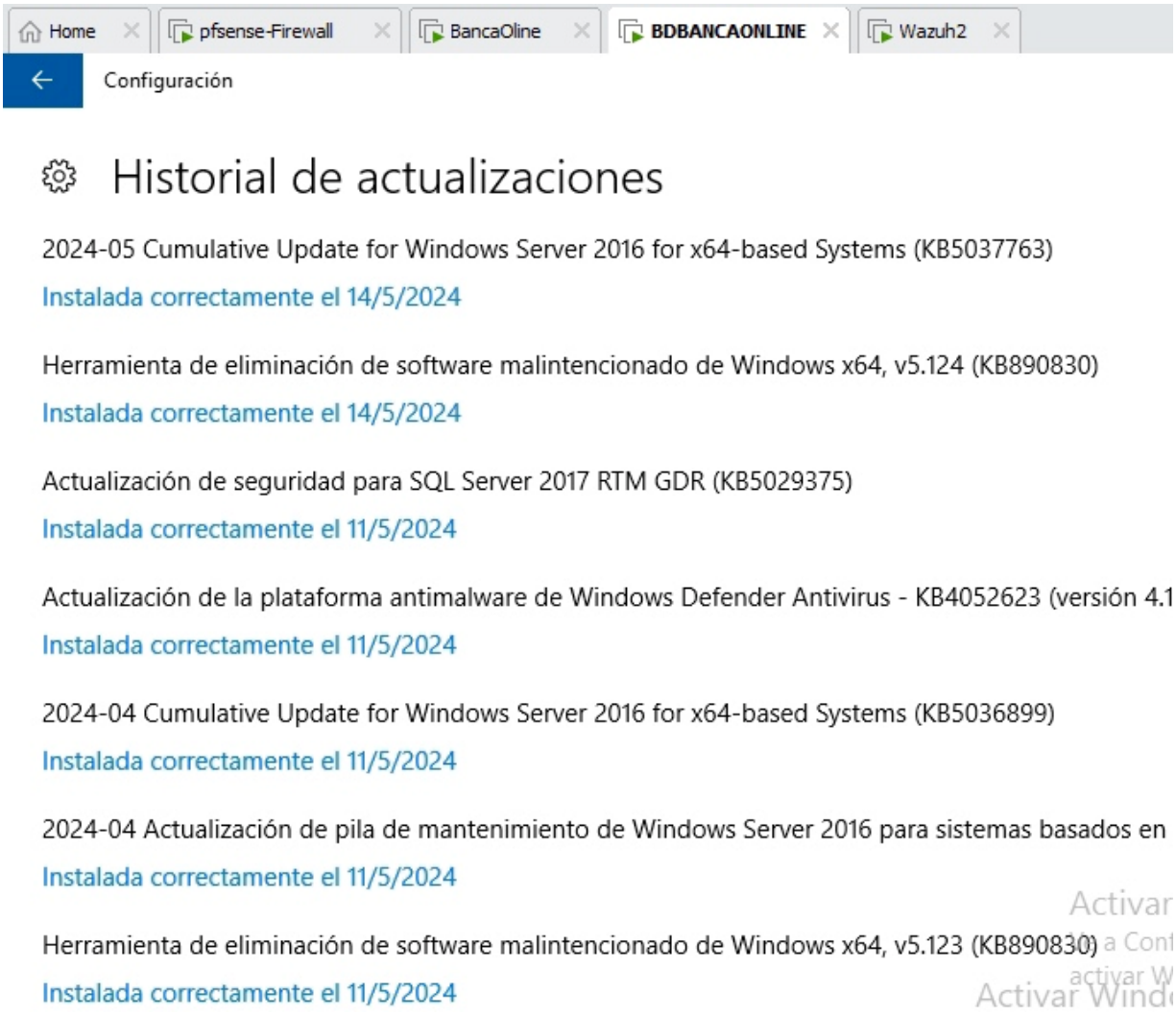
Historial y estado de todas las actualizaciones.



- Verificación de historial de actualizaciones BancaOnline a mayo del 2024 (ver Figura B13).

Figura B13

Historial de todas las actualizaciones.



Verificamos la confirguración del escaneo de vulnerabilidades en el archivo ossec.conf para determinar el periodo de escaneo parcial cada 30 minutos y de escaneo total cada 2 horas solo para nuestra demostración como se observa en la Figura B14.

Figura B14

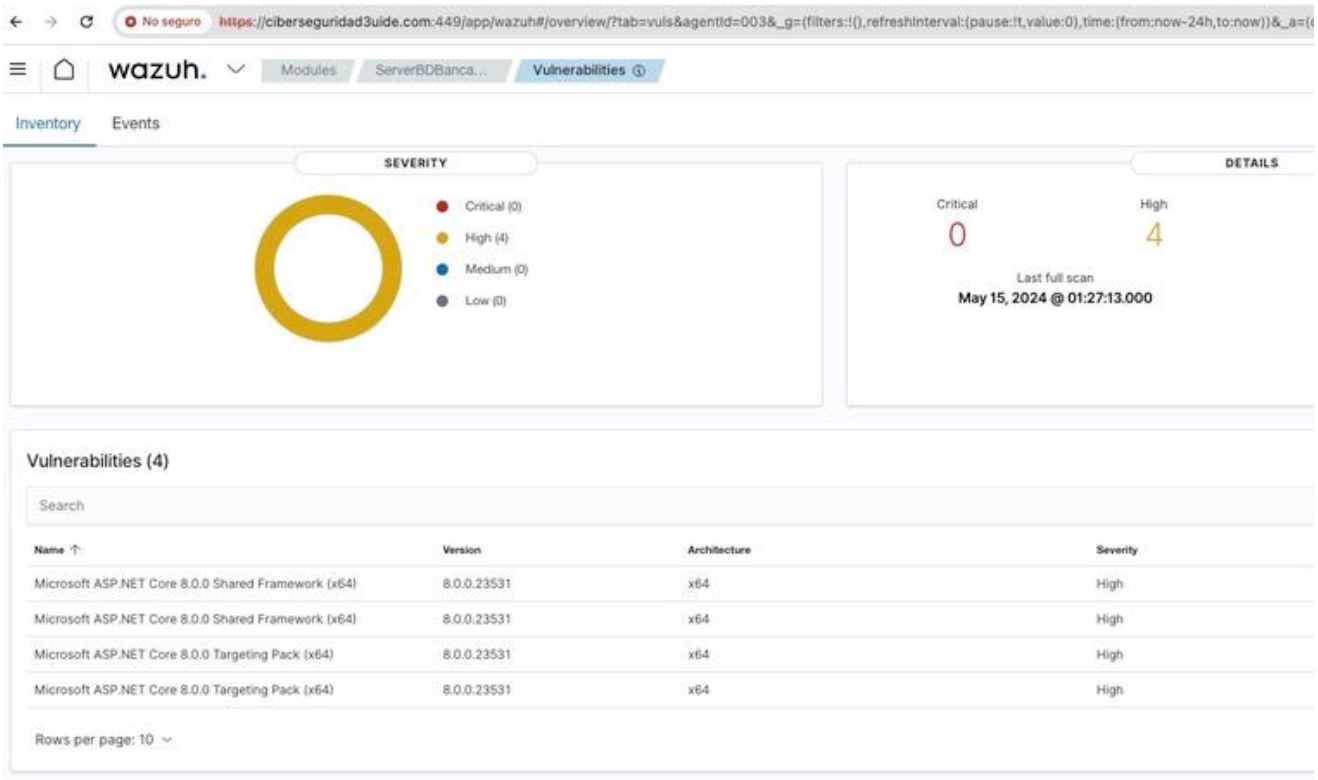
Intervalo de detección de vulnerabilidad.

```
<vulnerability-detector>
  <enabled>yes</enabled>
  <interval>30m</interval>
  <min_full_scan_interval>2h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>
```

Para poder verificar si las vulnerabilidades están solventadas, abrimos la web del wazuh e ingresamos al módulo de vulnerabilidades (ver Figura B15).

Figura B15

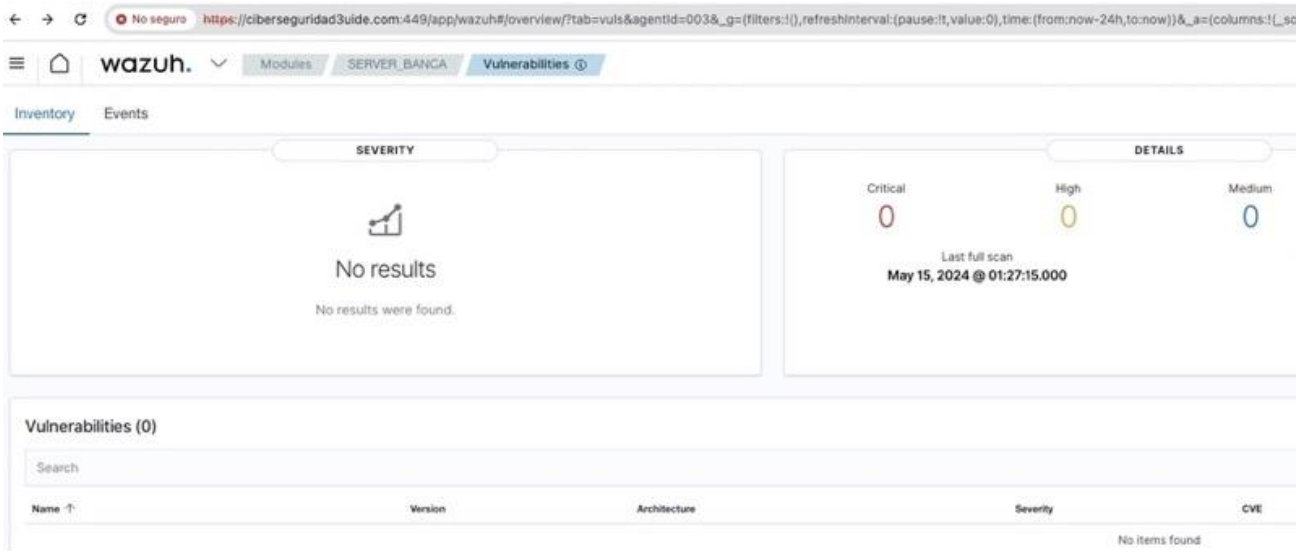
Vulnerabilidades solventadas



Esperamos el periodo de actualización de las vulnerabilidades configuradas en Wazuh y podemos observar en la Figura 69 que las vulnerabilidades detectadas en el servidor BDBancaOnline bajaron de 2591 a 4 vulnerabilidades las cuales hacen referencia a .NET

Figura B16

Actualización de Vulnerabilidades configuradas.



Una vez transcurrido el periodo de configuración de escaneo de vulnerabilidades observamos el segundo servidor BancaOnline el cual ya no detecta vulnerabilidades en Wazuh.

Como conclusión podemos definir que el sistema de detección de vulnerabilidades de Wazuh se encuentra trabajando de manera efectiva en el ambiente y en caso de presentar nuevas vulnerabilidades conocidas se va a presentar por pantalla.