Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTORES:

AGUAGUIÑA ACONDA ANGEL ERIK

BONILLA ASIPUELA JORGE ANDRES

CASTRO RODRIGUEZ ROMINA ARLLEY

TUTORES:

Paulina Vizcaíno

Juan Fernando López

TEMA

Diseño y despliegue de un SIEM All-in-One para la detección y correlación de eventos de seguridad en entornos controlados.

Quito - Ecuador

Junio – 20206

REINVENTEMOS EL FUTURO

Certificación de autoría

Nosotros, ANGEL ERIK AGUAGUIÑA ACONDA, JORGE ANDRÉS BONILLA ASIPUELA, ROMINA ARLLEY CASTRO RODRIGUEZ**,** 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.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ANGEL ERIK AGUAGUINA ACONDA

Firma
ANGEL ERIK AGUAGUIÑA ACONDA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JORGE ANDRES BONILLA ASIPUELA

Firma
JORGE ANDRÉS BONILLA ASIPUELA

ROMINA ARLLEY CASTRO RODRIGUEZ
Firmado digitalmente por ROMINA ARLLEY CASTRO RODRIGUEZ
Fecha: 2026.07.24 18:46:08 -05'00'

Firma
ROMINA ARLLEY CASTRO RODRIGUEZ

Autorización de Derechos de Propiedad Intelectual

Nosotros, ANGEL ERIK AGUAGUIÑA ACONDA, JORGE ANDRÉS BONILLA ASIPUELA, ROMINA ARLLEY CASTRO RODRIGUEZ, en calidad de autores del trabajo de investigación titulado ***"Diseño y despliegue de un SIEM All-in-One para la detección y correlación de eventos de seguridad en entornos controlados"***, 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, 08 /2026

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ANGEL ERIK AGUAGUIÑA ACONDA

Firma
ANGEL ERIK AGUAGUIÑA ACONDA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JORGE ANDRES BONILLA ASIPUELA

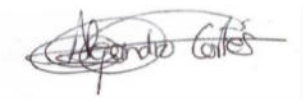
Firma
JORGE ANDRÉS BONILLA ASIPUELA

ROMINA ARLLEY CASTRO RODRIGUEZ
Firmado digitalmente por ROMINA ARLLEY CASTRO RODRIGUEZ
Fecha: 2026.07.24 18:46:22 -05'00'

Firma
ROMINA ARLLEY CASTRO RODRIGUEZ

APROBACIÓN DE DIRECCIÓN Y COORDINACIÓN DEL PROGRAMA

Nosotros, Alejandro Cortés López e Iván Galo Reyes Chacón, declaramos que: ANGEL ERIK AGUAGUIÑA ACONDA, JORGE ANDRÉS BONILLA ASIPUELA, ROMINA ARLLEY CASTRO RODRIGUEZ, son los autores exclusivos de la presente investigación y que esta es original, auténtica y personal de ellos.



Alejandro Cortés
Director/a de la
Maestría en Ciberseguridad

Iván Reyes
Coordinador/a de la
Maestría en Ciberseguridad

DEDICATORIA

Dedicamos este trabajo a nuestras familias, por su apoyo, comprensión y motivación durante cada etapa de nuestra formación académica.

A quienes nos acompañaron en este proceso, brindándonos palabras de aliento, confianza y respaldo en los momentos de mayor esfuerzo.

También dedicamos este proyecto a todas las personas que, de una u otra manera, contribuyeron a que esta meta pudiera alcanzarse.

AGRADECIMIENTOS

Expresamos nuestro agradecimiento a nuestras familias, por el apoyo, la paciencia y la motivación brindada a lo largo de nuestra formación profesional.

Agradecemos también a nuestros docentes y tutores, quienes, mediante sus conocimientos, observaciones y orientación, contribuyeron al desarrollo académico, técnico y metodológico de este proyecto.

De igual manera, extendemos nuestro agradecimiento a todas las personas que nos acompañaron durante este proceso, aportando su tiempo, apoyo y confianza para la culminación de esta etapa académica.

RESUMEN

En la actualidad muchas empresas u organizaciones enfrentan un incremento sostenido en la sofisticación de los ciberataques, y ante ello se exigen soluciones de monitoreo de seguridad accesibles y eficientes. Al tratarse de implementaciones de un sistema SIEM, estos carecen de una validación cuantitativa de su desempeño frente a técnicas de ataque documentadas.

El presente trabajo propone el diseño, despliegue y evaluación experimental de un sistema SIEM de código abierto basado en Elastic Stack, con el objetivo de detectar eventos de seguridad en un entorno de laboratorio virtualizado mediante reglas de correlación mapeadas al framework MITRE ATT&CK.

El desarrollo del proyecto se basó en tres fases: primero, el despliegue de la infraestructura virtualizada sobre la plataforma Virtual Box

Con segmentación por VLANs utilizando pfSense como firewall perimetral; segundo, la configuración del stack tecnológico conformado por ElasticSearch, Logstash, Kibana y Suricata, integrado con fuentes de información de Logs, como sistemas operativos Windows y Linux; añadiendo un equipo cliente Windows 10; tercero, el diseño de ocho reglas de correlación usando EQL, y la ejecución controlada de seis escenarios de ataque desde Kali Linux empleando herramientas como Hydra, Nmap, sqlmap, y Metasploit, cubriendo las técnicas T1110, T1046, T1059, T1190, T1021 y T1078 del framework MITRE ATT&CK.

Palabras clave. SIEM, Elastic Stack, MITRE ATT&CK, detección de intrusiones, Suricata, correlación de eventos, ciberseguridad, casos de uso.

ABSTRACT

Today, many companies and organizations face a sustained increase in the sophistication of cyberattacks, which demands accessible and efficient security monitoring solutions. Current SIEM system implementations lack quantitative validation of their performance against documented attack techniques.

This work proposes the design, deployment, and experimental evaluation of an open-source SIEM system based on Elastic Stack, with the objective of detecting security events in a virtualized laboratory environment through correlation rules mapped to the MITRE ATT&CK framework.

The process consisted of three phases: first, the deployment of the virtualized infrastructure on Virtual Box Versión 7.2.12 with VLAN segmentation using pfSense as the perimeter firewall; second, the configuration of the technology stack composed of Elasticsearch, Logstash, Kibana, and Suricata, integrated with log sources from Windows Server and Linux operating systems, including a Windows 10 client machine; third, the design of eight correlation rules using EQL and the controlled execution of six attack scenarios from Kali Linux using tools such as Hydra, Nmap, sqlmap, and Metasploit, covering techniques T1110, T1046, T1059, T1190, T1021, and T1078 of the MITRE ATT&CK framework.

Keywords: SIEM, Elastic Stack, MITRE ATT&CK, intrusion detection, Suricata, event correlation, cybersecurity, use cases.

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE FIGURAS

CAPITULO 1

1. INTRODUCCIÓN

La creciente dependencia de las organizaciones hacia las tecnologías de la información ha incrementado significativamente la exposición a amenazas cibernéticas capaces de comprometer la confidencialidad, integridad y disponibilidad de los activos de información. En este contexto, la detección temprana de incidentes de seguridad y la capacidad de correlacionar eventos provenientes de múltiples fuentes tecnológicas se han convertido en elementos fundamentales para fortalecer las estrategias de ciberseguridad organizacional. (IBM Security, 2023)

Los sistemas de gestión de información y eventos de seguridad (SIEM) surgen como una solución que permite centralizar la recolección, procesamiento y análisis de registros generados por servidores, dispositivos de red, aplicaciones y herramientas de seguridad, facilitando la identificación de comportamientos anómalos y posibles amenazas. Sin embargo, muchas organizaciones enfrentan limitaciones económicas y técnicas para implementar soluciones comerciales de alto costo, lo que ha impulsado el uso de tecnologías de código abierto como alternativa viable para el monitoreo de seguridad.

En este marco, el presente proyecto propone el diseño, despliegue y evaluación de un SIEM de tipo All-in-One basado en tecnologías open source, integrando herramientas como Elastic Stack y Suricata dentro de un entorno de laboratorio virtualizado. El propósito es analizar la capacidad de la solución para detectar, correlacionar y alertar sobre eventos de seguridad generados mediante escenarios de ataque controlados alineados con el framework MITRE ATT&CK.

Este capítulo presenta la definición del proyecto, su justificación, alcance y objetivos, estableciendo las bases conceptuales y metodológicas que orientan el desarrollo de la investigación.

1.1.Definición del proyecto

El proyecto consiste en diseñar, desplegar y evaluar un sistema de gestión de información y eventos de seguridad (SIEM) de tipo All-in-One, orientado a la detección, correlación y análisis centralizado de eventos de seguridad provenientes de una infraestructura tecnológica. La solución integra en una única plataforma los componentes encargados de la recepción, procesamiento, almacenamiento, correlación y visualización de eventos, permitiendo concentrar las capacidades operativas del SIEM en un único servidor. Esta característica la diferencia de las arquitecturas distribuidas, donde dichas funciones se encuentran separadas en múltiples nodos o servidores especializados. La solución propuesta incorpora capacidades de recolección de logs, normalización de eventos, correlación en tiempo real, generación de alertas y visualización de anomalías e incidentes de seguridad mediante una consola centralizada.

El stack tecnológico seleccionado está conformado por Elasticsearch, Logstash, Kibana, Elastic Security, Filebeat y Suricata, debido a que estas herramientas proporcionan de forma integrada las capacidades necesarias para cumplir los objetivos del proyecto relacionados con la recolección, normalización, correlación, análisis y visualización de eventos de seguridad. Elasticsearch actúa como motor de almacenamiento, indexación y búsqueda de eventos, permitiendo gestionar grandes volúmenes de información en tiempo real. Logstash facilita el procesamiento y normalización de registros provenientes de múltiples fuentes heterogéneas, mientras que Filebeat permite la recolección eficiente de logs desde los sistemas monitoreados. Por su parte, Kibana y el módulo Elastic Security proporcionan las funcionalidades de

visualización, análisis, gestión de alertas y correlación de eventos alineadas con el framework MITRE ATT&CK. Finalmente, Suricata complementa la solución mediante la detección de amenazas a nivel de red, generando eventos de seguridad que pueden ser centralizados y analizados por el SIEM.

La selección de este stack tecnológico responde además a criterios de integración nativa entre sus componentes, disponibilidad de funcionalidades SIEM de nivel empresarial, flexibilidad para la creación de reglas de detección personalizadas, amplia documentación técnica y condición de software de código abierto. Estas características permiten construir una solución funcional dentro de un entorno de laboratorio, reduciendo costos de implementación y facilitando la evaluación de la capacidad del sistema para detectar y correlacionar eventos de seguridad generados durante los escenarios de ataque controlados definidos en la investigación.

La construcción de las reglas de detección tomará como referencia el framework MITRE ATT&CK, una base de conocimiento desarrollada por MITRE Corporation que documenta tácticas, técnicas y procedimientos (TTPs) utilizados por adversarios reales durante las diferentes etapas de un ciberataque (MITRE Corporation, 2018). Este framework proporciona una clasificación estandarizada de comportamientos maliciosos y es ampliamente utilizado en actividades de monitoreo, detección de amenazas y evaluación de capacidades defensivas. Dentro del presente proyecto, MITRE ATT&CK será utilizado como guía para el diseño de reglas de correlación y detección, estableciendo una correspondencia directa entre los eventos de seguridad generados en el laboratorio y técnicas específicas de ataque. En particular, se trabajará con las técnicas T1110 (Brute Force), T1046 (Network Service Scanning), T1059 (Command and Scripting Interpreter) y T1190 (Exploit Public-Facing Application), permitiendo clasificar y documentar las detecciones bajo un estándar reconocido internacionalmente.

El proyecto será desplegado en un entorno de laboratorio virtualizado, utilizando máquinas virtuales que simulan una infraestructura tecnológica organizacional compuesta por servidores

Windows, servidores Linux, servicios web y un firewall. Sobre esta infraestructura se ejecutarán escenarios de ataque controlados alineados a las técnicas seleccionadas de MITRE ATT&CK, con el propósito de generar eventos de seguridad reales que permitan validar la capacidad del SIEM para recolectar, correlacionar, detectar y generar alertas frente a actividades potencialmente maliciosas.

El enfoque del proyecto no se limita a la implementación técnica del SIEM, sino que busca evaluar su efectividad mediante la correlación de eventos y su capacidad para identificar comportamientos maliciosos. Para ello, las detecciones serán mapeadas a nivel de tácticas y técnicas del framework MITRE ATT&CK, permitiendo relacionar los eventos observados con comportamientos adversarios documentados bajo un estándar reconocido internacionalmente. Este mapeo facilitará la clasificación de alertas, la validación de las reglas de detección implementadas y la evaluación de la cobertura de seguridad alcanzada por el SIEM frente a los escenarios de ataque controlados definidos en la investigación.

1.2.Justificación e importancia del trabajo de investigación

El incremento de ciberataques a nivel global ha elevado la frecuencia de los incidentes de seguridad y la complejidad de los vectores de ataque utilizados por actores maliciosos. Esta evolución exige que las organizaciones cuenten con mecanismos de visibilidad centralizada que permitan detectar comportamientos anómalos, correlacionar eventos provenientes de activos de información, y validar la efectividad de sus controles de seguridad en tiempo real. La ausencia de estas capacidades genera puntos ciegos que prolongan el tiempo de exposición ante amenazas activas y dificultan la respuesta oportuna ante incidentes.

Según el informe Cost of a Data Breach Report 2023 de IBM Security, el tiempo promedio requerido para identificar y contener una brecha de seguridad alcanza los 277 días, lo que evidencia limitaciones importantes en las capacidades de detección y respuesta de las

organizaciones. Esta problemática puede tener un impacto mayor en pequeñas y medianas empresas de Latinoamérica, debido a las restricciones económicas, técnicas y operativas asociadas con la adopción de soluciones SIEM empresariales.

En este contexto, la presente investigación realizará una comparación entre una solución SIEM basada en herramientas de código abierto y plataformas empresariales como Splunk Enterprise, IBM QRadar y Microsoft Sentinel. La evaluación considerará criterios como costos de licenciamiento e implementación, requerimientos de infraestructura, capacidad de integración de fuentes de eventos, cobertura de detección, consumo de recursos, tiempo medio de detección y generación de falsos positivos. Para garantizar una comparación objetiva, se establecerán escenarios de prueba controlados, fuentes de datos equivalentes y métricas previamente definidas, complementando los resultados experimentales con información técnica y comercial publicada por los fabricantes.

Frente a este escenario, el proyecto se justifica desde tres dimensiones. Desde la perspectiva del problema de investigación, persiste una falta de evidencia experimental sistemática sobre la capacidad real de detección y correlación de arquitecturas SIEM construidas con herramientas de código abierto, dado que la mayoría de las implementaciones documentadas se limitan a describir la instalación de componentes sin medir su desempeño frente a ataques reales.

Desde la perspectiva técnica, el framework MITRE ATT&CK ofrece una taxonomía estandarizada de tácticas, técnicas y procedimientos que permite diseñar reglas de correlación con fundamento empírico, mapear los eventos detectados a comportamientos adversarios documentados y establecer una metodología reproducible de evaluación. Adicionalmente, el uso de un stack tecnológico de código abierto como Elastic Stack y Suricata permite explorar si es posible construir una solución de detección robusta y funcionalmente comparable a plataformas comerciales, sin que ello implique necesariamente una reducción en la calidad de la correlación o en la cobertura de detección alcanzada. Desde la perspectiva del aporte académico, el proyecto

contribuye con evidencia cuantitativa sobre la efectividad de un modelo de detección y correlación específico, midiendo su tasa de detección, su tasa de falsos positivos y su tiempo medio de detección frente a escenarios de ataque controlados y alineados a técnicas MITRE ATT&CK, lo que permite no solo validar la solución implementada sino también identificar sus limitaciones y establecer una línea base medible para investigaciones futuras sobre arquitecturas de detección similares.

1.3.Alcance

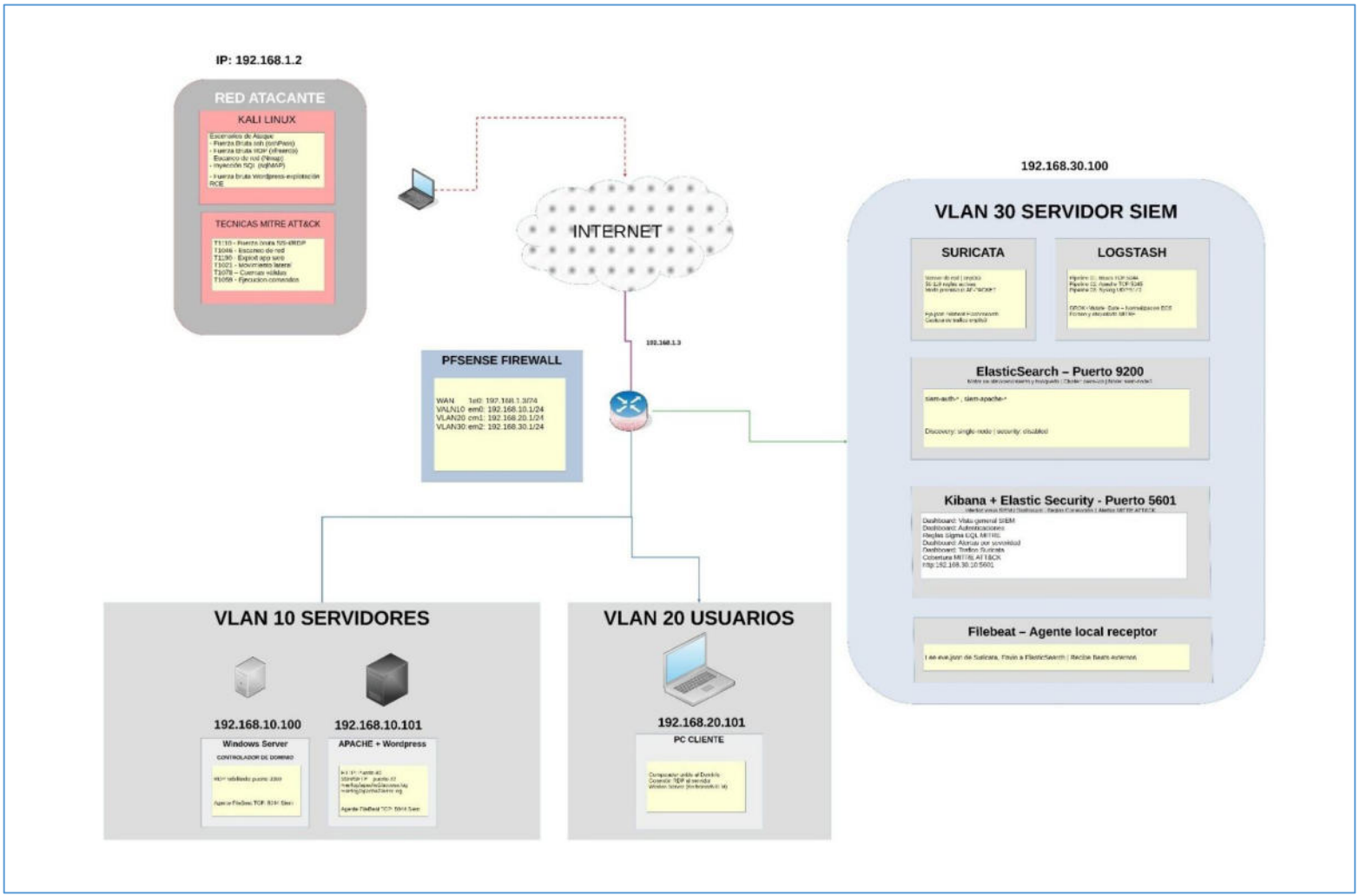
El presente proyecto abarca el diseño, implementación y evaluación de un SIEM All-in-One dentro de un entorno de laboratorio virtualizado desplegado sobre Virtual Box Versión 7.2.12, que simula una infraestructura organizacional segmentada mediante VLANs. El alcance está estructurado en tres componentes que le otorgan valor investigativo al trabajo: la definición y despliegue de la arquitectura tecnológica del laboratorio, el diseño y ejecución de escenarios de ataque controlados alineados al framework MITRE ATT&CK, y la evaluación cuantitativa del desempeño del sistema mediante métricas de detección definidas. Las condiciones operativas de evaluación comprenden la ejecución de seis escenarios de ataque reproducibles, cada uno generando un mínimo de cincuenta eventos de seguridad sobre las fuentes de logs definidas, con un criterio de éxito basado en la generación de al menos una alerta correcta por escenario dentro de un tiempo máximo de cinco minutos desde el inicio del ataque. El volumen esperado de eventos procesados por el SIEM durante las pruebas es de aproximadamente tres mil registros distribuidos entre los índices de autenticación, tráfico web, firewall y alertas de red. A continuación, se detallan los elementos específicos que comprende cada componente.

Arquitectura del laboratorio virtualizado. El entorno de laboratorio estará compuesto por seis máquinas virtuales desplegadas sobre Virtual Box Versión 7.2.12: un servidor Windows Server que actúa como controlador de dominio, configurado con Active Directory y como objetivo

de ataques de autenticación mediante RDP; un servidor Ubuntu Server con servicio SSH activo y un servidor web Apache con WordPress en versión desactualizada configurado con vulnerabilidades controladas; un equipo cliente Windows incorporado al dominio gestionado por el controlador de dominio, simulando un endpoint corporativo desde el cual se generan eventos de autenticación de dominio y se ejecutan escenarios de movimiento lateral utilizando credenciales de usuario válidas; un firewall pfSense encargado de gestionar la segmentación de red mediante VLANs y de generar registros de tráfico enviados al SIEM; el servidor SIEM central con Suricata integrado como sensor de detección de intrusiones en red; y una máquina atacante con Kali Linux desde donde se ejecutarán los escenarios de ataque. La arquitectura implementa segmentación lógica mediante VLANs que separan los servidores monitoreados, los equipos cliente, la red de gestión del SIEM y la red externa desde donde opera el atacante, replicando la separación entre zonas que existe en una infraestructura organizacional real.

El flujo de eventos está definido desde las fuentes de datos hacia el SIEM mediante el agente Filebeat instalado en cada sistema monitoreado, el cual envía los registros hacia Logstash para su procesamiento, parseo y normalización. Los eventos normalizados son almacenados en Elasticsearch, donde quedan disponibles para su consulta, correlación y visualización mediante Kibana y el módulo Elastic Security. De manera paralela, Suricata opera como sensor de red dentro del servidor SIEM, analizando el tráfico que atraviesa la infraestructura y generando alertas que son incorporadas al mismo flujo de almacenamiento y visualización. La arquitectura completa, incluyendo las fuentes de datos, los flujos de logs, el sensor de red y la posición de la máquina atacante respecto a la infraestructura monitoreada, se presenta en la Figura.

Figura 1
Infraestructura de red implementada



Nota: Elaboración propia.

Reglas de correlación y escenarios de ataque. El proyecto contempla el diseño de ocho reglas de correlación alineadas al framework MITRE ATT&CK, organizadas sobre cuatro técnicas base que cubren las principales fases de un ciclo de ataque: T1110 Fuerza Bruta, T1046 Escaneo de Red, T1059 Ejecución Remota de Comandos y T1190 Explotación de Servicios Web. Cada técnica base sustenta dos reglas de correlación específicas que distinguen variantes del mismo comportamiento adversario, permitiendo alcanzar el mínimo de ocho reglas documentadas establecido en los objetivos. Sobre T1110 se diseñarán reglas diferenciadas para fuerza bruta SSH sobre el servidor Linux y fuerza bruta RDP sobre el controlador de dominio, dado que los campos evaluados, las fuentes de logs y los umbrales de activación son distintos en cada caso. Sobre T1190 se diseñarán reglas diferenciadas para inyección SQL en formularios web y para explotación de plugins vulnerables en WordPress, considerando los patrones de tráfico específicos que cada técnica genera en los registros de Apache. Adicionalmente, la incorporación del equipo cliente unido al dominio permite extender la cobertura del framework hacia las técnicas T1021 (Remote Services) y T1078 (Valid Accounts), mediante escenarios ejecutados con credenciales de usuario válidas obtenidas previamente.

Se implementarán seis escenarios de ataque controlados que generarán incidentes de eventos reales sobre la infraestructura: ataques de fuerza bruta vía SSH y RDP ejecutados con Hydra, escaneos de red con Nmap, fuerza bruta contra el panel de administración de WordPress con WPScan, inyección SQL con sqlmap, y un escenario de movimiento lateral desde el equipo cliente comprometido hacia el controlador de dominio utilizando credenciales válidas.

Evaluación de desempeño. Se evaluará el desempeño del SIEM mediante tres métricas cuantitativas calculadas sobre los resultados de los seis escenarios de ataque ejecutados. La tasa de detección se calculará como el cociente entre el número de alertas correctas generadas y el número total de ataques ejecutados, multiplicado por cien. La tasa de falsos positivos se calculará como el cociente entre el número de alertas generadas sobre actividad legítima previamente definida y el

número total de actividades legítimas ejecutadas durante las pruebas de comportamiento normal, multiplicado por cien. El tiempo medio de detección se calculará como el promedio de los tiempos transcurridos entre el inicio documentado de cada ataque y la generación de la primera alerta correspondiente en Kibana. El criterio de validación de una alerta será la correspondencia entre la regla activada, la técnica MITRE ATT&CK asociada y el escenario de ataque ejecutado, verificada mediante la revisión de los campos de evento almacenados en Elasticsearch.

Fuera del alcance de este proyecto quedan la integración con entornos de producción reales, el desarrollo de reglas de machine learning para detección de anomalías, la implementación de un SOC completo con personal dedicado, y la integración con plataformas de inteligencia artificial externas.

1.4. Objetivos

1.4. Objetivo General

Diseñar e implementar un sistema SIEM de tipo All-in-One en un entorno de laboratorio virtualizado, capaz de recolectar, normalizar, correlacionar y analizar eventos de seguridad provenientes de múltiples fuentes tecnológicas heterogéneas, validando su efectividad mediante la simulación de escenarios de ataque controlados mapeados al framework MITRE ATT&CK y la medición de métricas cuantitativas de tasa de detección, tasa de falsos positivos y tiempo medio de detección.

1.4. Objetivos Específicos

Diseñar la arquitectura lógica y física del SIEM All-in-One, definiendo los componentes tecnológicos, flujos de datos y mecanismos de ingesta, procesamiento y almacenamiento de eventos de seguridad.

Desplegar e integrar el stack tecnológico del SIEM mediante la configuración de Filebeat, Logstash, Elasticsearch y Kibana con el módulo Elastic Security y Suricata como sensor de detección de intrusiones de red.

Diseñar e implementar un mínimo de seis reglas de correlación y detección en Elastic Security, estableciendo una correspondencia directa con las tácticas y técnicas T1110, T1046, T1059, T1190, T1021 y T1078 del framework MITRE ATT&CK, y documentando para cada regla su lógica de detección, fuente de datos, campos evaluados, condición de activación, nivel de severidad y escenario de ataque utilizado para su validación.

Diseñar, documentar y ejecutar seis escenarios de ataque controlados desde un entorno Kali Linux sobre la infraestructura de laboratorio, incluyendo fuerza bruta SSH y RDP, escaneo de red, fuerza bruta y explotación de WordPress, e inyección SQL, así como un escenario de movimiento lateral desde el equipo cliente del dominio hacia el controlador de dominio, verificando la capacidad del SIEM para detectar, correlacionar y alertar sobre los eventos generados en tiempo real.

El análisis de falsos positivos se realizará de manera cualitativa mediante la revisión de las alertas generadas durante la operación normal del laboratorio y que no se encuentren relacionadas con los escenarios de ataque ejecutados. Para esta revisión se considerarán principalmente las alertas de baja prioridad registradas por Suricata durante actividades legítimas observadas, como la actualización de paquetes del sistema. La clasificación se verificará mediante la comparación de la hora del evento, las direcciones de origen y destino, la firma activada, su categoría y la actividad que se encontraba en ejecución. Debido a que no se estableció un conjunto controlado y cuantificable de actividades legítimas, no se calculará una tasa porcentual de falsos positivos.

CAPITULO 2

2. REVISIÓN DE LITERATURA

2.1.Estado de Arte

La transformación digital y el crecimiento acelerado de las infraestructuras tecnológicas han incrementado significativamente la superficie de ataque de las organizaciones, este factor se

debe a la incorporación de entornos híbridos, servicios en la nube, aplicativos webs, dispositivos perimetrales de red y múltiples fuentes de generación de eventos. Generando la necesidad de implementar mecanismos avanzados de monitoreo, correlación y respuesta frente a incidentes de seguridad informática.

Los primeros enfoques de monitoreo de seguridad se centraban en la recopilación y revisión aislada de registros generados por sistemas operativos, aplicaciones, servidores de autenticación y dispositivos perimetrales. Sin embargo, esta gestión descentralizada dificultaba la identificación oportuna de ataques complejos que involucraban múltiples fuentes de información y diferentes etapas dentro de la infraestructura tecnológica (Kent & Souppaya, 2006).

En la actualidad, las organizaciones se enfrentan a amenazas cibernéticas cada vez más complejas. Estas son definidas por ataques persistentes y avanzados, el aprovechamiento de debilidades en la web, desplazamientos laterales en la red y métodos de evasión diseñados para eludir los mecanismos convencionales de detección.

En los últimos años, el comportamiento de los actores de amenaza ha evidenciado una evolución significativa, dejando atrás los ataques individuales y muy técnicos para adoptar campañas más organizadas, automatizadas y dirigidas a la utilización abusiva de tecnologías legítimas empleadas por las organizaciones. Según el informe Threat Detection Report 2025 de Red Canary, se revisaron aproximadamente 93.000 amenazas confirmadas en ambientes de identidad, endpoints, recursos en la nube y aplicaciones SaaS durante 2024. Se detectó un aumento significativo en los ataques de robo de información, abuso de VPN, compromiso del correo electrónico corporativo, así como amenazas en la nube y ataques con base en identidad (2025 Threat Detection Report, 2025). Estos descubrimientos demuestran que los atacantes no se apoyan solamente en malware clásico, sino que también emplean credenciales válidas, servicios de la empresa, herramientas administrativas y métodos propios de las plataformas corporativas para llevar a cabo sus operaciones. Una de las tendencias más importantes que sobresale es la

explotación de identidades digitales y cuentas en la nube. De hecho, tres de las diez estrategias MITRE ATT&CK más destacadas en 2024 estaban vinculadas a técnicas nativas de la nube habilitadas por identidad, incluyendo el empleo de cuentas en la nube, reglas para reenviar correos electrónicos y ocultar mensajes (2025 Threat Detection Report, 2025). Una de las tendencias más importantes que sobresale es la explotación de identidades digitales y cuentas en la nube. Esto demuestra que las credenciales, los tokens de acceso y las plataformas de identidad se han convertido en objetivos prioritarios para los adversarios, permitiéndoles acceder a múltiples servicios sin comprometer directamente un endpoint y facilitando actividades posteriores como reconocimiento, persistencia, evasión, movimiento lateral o acceso a información sensible. Asimismo, se ha observado un incremento en técnicas orientadas a engañar al usuario mediante señuelos web, falsas verificaciones CAPTCHA, descargas simuladas o instrucciones que inducen a ejecutar comandos en el sistema, permitiendo que amenazas como LummaC2, NetSupport Manager, HijackLoader o el abuso de Mshta sean utilizadas como mecanismos de acceso inicial, ejecución o despliegue de cargas maliciosas. De igual manera, el uso de herramientas legítimas como PowerShell, Windows Command Shell, Windows Management Instrumentation y servicios de administración remota refleja una tendencia hacia ataques de tipo “living off the land”, en los cuales los adversarios emplean componentes propios del sistema operativo para reducir la probabilidad de detección. Otro aspecto corresponde al abuso de reglas de correo electrónico, particularmente las reglas de ocultamiento de mensajes, utilizadas para mover, marcar como leídos, eliminar u ocultar correos relacionados con actividad sospechosa, phishing o incidentes de seguridad, dificultando la respuesta del usuario y del equipo de seguridad y convirtiéndose en una técnica especialmente relevante para el monitoreo de entornos Microsoft 365 (Red Canary, 2025).

En este contexto, los sistemas de Gestión de Información y Eventos de Seguridad, conocidos como SIEM por sus siglas en inglés, se han consolidado como herramientas esenciales para la gestión centralizada de registros, eventos y alertas de seguridad dentro de las

organizaciones de todos los activos que se encuentren integrados dentro del monitoreo de la infraestructura. (González-Granadillo, González-Zarzosa , & Diaz, 2021)

Estos escenarios evidencian la necesidad de implementar soluciones SIEM capaces de integrar y correlacionar eventos de múltiples fuentes, identificando patrones que, de forma aislada, podrían parecer legítimos, pero en conjunto pueden revelar una cadena de ataque. Asimismo, la alineación de los casos de uso con MITRE ATT&CK hace más fácil describir el comportamiento adversario a través de tácticas y técnicas vistas en situaciones reales, mientras que marcos como NIST Cybersecurity Framework posibilitan organizar las habilidades de detección, reacción, recuperación, identificación, protección y gobernanza ante incidentes cibernéticos (MITRE Corporation, 2018).

Entre los SIEM comerciales más utilizados se encuentran ArcSight, Microsoft Sentinel, IBM QRadar y Splunk Enterprise Security. Aunque implican costos de licenciamiento, infraestructura y almacenamiento, ofrecen capacidades avanzadas de análisis, correlación, integración y gestión de incidentes. Por ejemplo, Splunk Enterprise Security usa esquemas de licencia relacionados con sus soluciones de seguridad y necesita contacto comercial para cálculos concretos; IBM QRadar SIEM ofrece licencias por suscripción o perpetuas que incluyen indicadores como eventos por segundo, flujos por minuto o Managed Virtual Servers; y Microsoft Sentinel utiliza un modelo que se basa sobre todo en el análisis e ingesta de datos por GB en Azure (IBM, 2023; Microsoft, 2026; Kidd, 2025).

En los últimos años han crecido las soluciones SIEM open source, como Elastic Stack, Wazuh, Graylog y Security Onion. Estas herramientas reducen costos y permiten personalizar reglas de detección, integrar fuentes de datos, crear tableros y adaptar casos de uso. Wazuh combina funciones SIEM y XDR; Elastic Security centraliza y analiza eventos; Graylog gestiona logs y alertas; y Security Onion se enfoca en monitoreo de red, detección de intrusiones y caza de amenazas.

Tabla 1
Comparación de soluciones SIEM comerciales y open source.

Criterio	Splunk Enterprise Security	IBM QRadar	Microsoft Sentinel	Elastic Stack / Elastic Security	Wazuh	Graylog	Security Onion
Tipo de solución	SIEM comercial empresarial con capacidades de analítica, correlación, inteligencia de amenazas y respuesta.	SIEM comercial empresarial orientado a correlación, análisis de eventos, flujos de red y gestión de amenazas.	SIEM/SOAR cloud nativo de Microsoft Azure.	Plataforma de búsqueda, análisis y seguridad basada en Elastic Stack.	Plataforma open source que integra capacidades SIEM y XDR.	Plataforma de gestión centralizada de logs con capacidades SIEM y alertamiento.	Plataforma abierta para monitoreo de seguridad, threat hunting, IDS, gestión de logs y casos.
Costo	Alto; depende del licenciamiento de Splunk Enterprise o Splunk Cloud, volumen de indexación o uso de recursos.	Alto; depende del modelo de licenciamiento, eventos por segundo, flujos por minuto y tipo de despliegue.	Variable; depende principalmente de la ingesta, análisis y retención de datos en Azure.	Menor costo inicial si se usa la distribución básica; puede aumentar con características empresariales o soporte comercial.	Bajo costo inicial; gratuito y open source, aunque requiere infraestructura y administración técnica.	Bajo a medio; cuenta con opciones open source y versiones comerciales.	Bajo costo inicial; gratuito y abierto, aunque demanda recursos de hardware y conocimiento técnico.
Licencia	Comercial.	Comercial.	Comercial bajo modelo cloud por consumo.	Licencia con componentes gratuitos y opciones comerciales según funcionalidades.	Open source.	Open source con opciones empresariales.	Gratuita y abierta.
Integración de fuentes	Alta integración con múltiples fuentes empresariales, EDR, firewalls, sistemas cloud, identidad y aplicaciones.	Alta integración con logs, eventos de red, flujos, appliances, endpoints y servicios empresariales.	Alta integración con servicios Microsoft, Azure, Microsoft 365, Defender y conectores externos.	Integración flexible mediante Elastic Agent, Beats, Logstash, APIs, conectores y fuentes externas.	Integración mediante agentes, syslog, decoders, APIs, módulos cloud y monitoreo de endpoints.	Integración mediante syslog, agentes, APIs, extractores, pipelines y entradas configurables.	Integración de herramientas como Suricata, Zeek, Elastic Stack, osquery y sensores de red.

Criterio	Splunk Enterprise Security	IBM QRadar	Microsoft Sentinel	Elastic Stack / Elastic Security	Wazuh	Graylog	Security Onion
Reglas de detección	Reglas y contenido de seguridad preconstruido, correlación avanzada y búsquedas en SPL.	Reglas de correlación, ofensas, analítica de eventos y consultas mediante AQL.	Reglas analíticas, hunting queries en KQL, playbooks e integración con automatización.	Reglas de detección, consultas KQL/EQL, machine learning y dashboards personalizables.	Reglas propias, decoders, integración con MITRE ATT&CK, FIM, vulnerabilidades y respuesta activa.	Alertas, correlaciones, pipelines, dashboards y búsquedas personalizadas.	Reglas IDS/NSM, detecciones de red, hunting, alertas, casos y análisis de tráfico.
Escalabilidad	Adecuada para grandes organizaciones, aunque requiere arquitectura y licenciamiento adecuados.	Orientada a entornos empresariales con grandes volúmenes de eventos y flujos.	Al estar basado en Azure y escalar según consumo cloud.	Dependiendo del diseño del clúster, nodos, almacenamiento e ingesta.	Depende de arquitectura, número de agentes, indexadores y recursos disponibles.	Depende de arquitectura, almacenamiento y volumen de logs.	Dependiendo de sensores, nodos, almacenamiento y tráfico monitoreado.
Facilidad de despliegue	Media; requiere planificación, licenciamiento, configuración y personal especializado.	Media; puede requerir appliances, arquitectura empresarial y conocimiento especializado.	Media a alta en entornos Microsoft/Azure; requiere configuración de conectores, costos y reglas.	Media; requiere configurar ingesta, almacenamiento, índices, agentes y reglas.	Media; instalación accesible, pero requiere ajuste de agentes, reglas, decoders y fuentes.	Media; despliegue relativamente flexible, con configuración de entradas, parsing y alertas.	Media; útil para laboratorio, pero requiere recursos suficientes y comprensión de sensores/red.
Pertinencia académica	Permite estudiar un SIEM empresarial, pero su costo limita la implementación completa en laboratorio.	Útil para comprender correlación empresarial, pero menos accesible por licenciamiento.	útil para estudiar SIEM cloud, especialmente con ecosistema Microsoft, pero depende de Azure y costos de ingesta.	Permite comprender ingesta, indexación, búsqueda, visualización, reglas y dashboards.	Adecuada para laboratorios académicos por su enfoque open source, reglas, agentes y mapeo MITRE ATT&CK.	Útil para comprender gestión de logs, parsing, pipelines, búsqueda y alertamiento.	Adecuada para laboratorios de monitoreo, IDS, threat hunting, análisis de red y correlación de eventos.

A partir de la comparación anterior, se evidencia que las soluciones comerciales ofrecen capacidades robustas para entornos empresariales de gran escala; sin embargo, su implementación puede verse condicionada por costos de licenciamiento, dependencia del proveedor y requerimientos de infraestructura especializada. En contraste, las soluciones open source presentan una mayor pertinencia para entornos académicos, ya que permiten implementar laboratorios controlados, comprender el funcionamiento interno de un SIEM, integrar múltiples fuentes de datos, crear reglas personalizadas y analizar eventos de seguridad sin depender de licencias comerciales de alto costo. Por esta razón, el uso de tecnologías como Elastic Stack, Wazuh, Graylog o Security Onion resulta adecuado para proyectos de investigación aplicada orientados a la implementación, correlación y evaluación de eventos de seguridad informática.

Elastic Stack y Suricata fueron seleccionados como componentes principales del proyecto debido a su pertinencia técnica, académica y metodológica frente a otras alternativas SIEM. A diferencia de soluciones comerciales como Splunk Enterprise Security, IBM QRadar o Microsoft Sentinel, estas herramientas permiten implementar un entorno de monitoreo y detección sin depender de licencias de alto costo, consumo cloud o infraestructura propietaria.

Elastic Stack resulta preferible debido a su arquitectura flexible para la ingesta, indexación, búsqueda, análisis y visualización de grandes volúmenes de datos de seguridad. Además, Elastic Security incorpora un motor de detección que permite evaluar eventos mediante reglas, generar alertas cuando se cumplen determinados criterios y correlacionar eventos entre distintas fuentes de datos, lo cual facilita la identificación de amenazas que podrían no ser evidentes al analizar cada registro de forma aislada (Elastic, 2026). Asimismo, Elastic mantiene reglas de detección preconstruidas alineadas con MITRE ATT&CK, lo que permite relacionar los eventos del laboratorio con tácticas y técnicas adversarias observadas en escenarios reales (Elastic, 2026).

Suricata fue elegido debido a que es un motor IDS/IPS/NSM de código abierto, consolidado y comúnmente empleado para la inspección de tráfico en redes. Su habilidad para analizar el tráfico en tiempo real, implementar reglas de detección, reconocer patrones maliciosos y generar eventos en formato EVE JSON facilita su integración con plataformas SIEM. Este formato permite registrar alertas, eventos HTTP, DNS, TLS, archivos y otros metadatos relacionados con la red, proporcionando una mayor visibilidad sobre la actividad en el entorno monitoreado (Suritcata, 2026). Además, Elastic cuenta con una integración nativa para Suricata, diseñada para recolectar y procesar los registros generados por este motor IDS/IPS, lo que simplifica la integración entre ambas herramientas (Elastic, 2026).

En comparación con otras opciones de código abierto como Wazuh, Graylog o Security Onion, la combinación de Elastic Stack y Suricata presenta una ventaja significativa para los objetivos de este proyecto: permite crear una arquitectura modular, comprensible y adaptable, donde cada elemento desempeña un rol específico dentro del proceso de monitoreo. Elastic Stack funciona como una plataforma para el almacenamiento, búsqueda, visualización y correlación de datos; mientras que Suricata proporciona la capacidad de detección basada en el análisis del tráfico de red. Aunque Wazuh ofrece funcionalidades SIEM/XDR enfocadas sobre todo en el monitoreo de endpoints, Graylog se centra en la gestión centralizada de logs y Security Onion incorpora múltiples herramientas de seguridad en una distribución más integral, la combinación de Elastic Stack y Suricata brinda un mayor control sobre la arquitectura implementada, facilitando el aprendizaje técnico, la personalización de reglas y la evaluación individual de cada fase del proceso de detección.

Por esta razón, la elección de Elastic Stack y Suricata se considera apropiada para el proyecto actual, ya que permite establecer un laboratorio SIEM operativo, adaptable y replicable, centrado en la detección de amenazas en la red, el análisis de eventos, la creación de paneles y la correlación de alertas. Además, esta integración promueve la alineación de los casos de uso con

MITRE ATT&CK y refuerza el enfoque académico de la investigación, al poder demostrar de manera práctica cómo los eventos generados por un IDS/IPS pueden ser recolectados, procesados, visualizados y analizados en el contexto de una plataforma SIEM.

Tabla 2
Justificación de selección de Elastic Stack y Suricata

Criterio	Elastic Stack	Suricata	Pertinencia para el proyecto
Costo	Puede implementarse con componentes gratuitos y flexibles.	Herramienta open source.	Permite construir un laboratorio académico sin depender de licencias comerciales de alto costo.
Función principal	Ingesta, indexación, búsqueda, análisis, visualización y correlación de eventos.	Detección e inspección de tráfico de red como IDS/IPS/NSM.	Cubre dos necesidades clave del SIEM: análisis centralizado y detección de amenazas de red.
Integración	Compatible con agentes, Beats, Logstash, APIs, conectores e integraciones.	Genera eventos en formato EVE JSON compatibles con pipelines SIEM.	Facilita el envío de alertas de red hacia Elastic para su análisis y visualización.
Reglas de detección	Permite reglas de detección, correlación de eventos, consultas KQL/EQL y reglas alineadas con MITRE ATT&CK.	Utiliza reglas y firmas para identificar tráfico sospechoso o malicioso.	Permite construir casos de uso de detección y relacionarlos con técnicas adversarias.
Visualización	Kibana permite dashboards, búsquedas, alertas y análisis interactivo.	No es una herramienta de visualización; genera eventos para ser analizados por plataformas externas.	Elastic complementa a Suricata al transformar eventos de red en información visual y accionable.
Escalabilidad	Escalable mediante arquitectura distribuida, nodos e índices.	Escalable según sensores, interfaces monitoreadas y capacidad de procesamiento.	Permite iniciar con un laboratorio pequeño y crecer hacia arquitecturas más complejas.
Facilidad académica	Permite comprender cómo se recolectan, normalizan, indexan y consultan los eventos.	Permite comprender cómo se detectan amenazas a nivel de red.	Favorece el aprendizaje práctico del ciclo completo de monitoreo y detección.

Varios estudios han evidenciado la efectividad de los SIEM de código abierto para identificar ataques comunes como fuerza bruta, escaneo de puertos, explotación de servicios web, inyección SQL y ataques de denegación de servicio. Sin embargo, algunos de estos estudios se han

centrado principalmente en la implementación técnica, la integración de herramientas y la validación funcional de alertas, sin realizar un análisis cuantitativo exhaustivo utilizando métricas como tasa de falsos positivos, tasa de falsos negativos, precisión, recall, F1-score o tiempo promedio de detección.

Por ejemplo, Setiawan y Sulistyo (2023) propusieron un modelo SIEM para la detección de amenazas utilizando Suricata, EveBox y Elastic Stack. La solución fue evaluada mediante escenarios de escaneo de puertos, fuerza bruta, inyección SQL y denegación de servicio. Los resultados demostraron que el sistema permitió detectar los ataques ejecutados y visualizar los eventos mediante Elastic Stack; sin embargo, el estudio se concentró en la validación funcional de la arquitectura y no presentó métricas cuantitativas como la tasa de falsos positivos, la tasa de falsos negativos o el tiempo medio de detección.

De manera similar, Ramli y Soewito (2023) desarrollaron una implementación SIEM de código abierto integrada con pfSense y Suricata en modo IPS. Los autores determinaron que el sistema cumplió el 84 % de los requerimientos inicialmente establecidos y permitió realizar funciones de monitoreo, evaluación, detección y generación de alertas. No obstante, la evaluación se orientó principalmente al cumplimiento de funcionalidades y no al análisis de indicadores operativos de desempeño, como el tiempo medio de detección o la tasa de falsos positivos.

Además, Bhavana et al. (2025) propusieron una estructura de integración SIEM/SOAR que se fundamenta en pfSense, Suricata, Filebeat, Elasticsearch, Shuffle SOAR y Kibana. El análisis sostiene que la integración disminuye el tiempo promedio de detección y respuesta, así como los falsos positivos mediante correlación y automatización; no obstante, no proporciona un cálculo numérico pormenorizado de estas métricas, ni una matriz de evaluación para contrastar resultados entre diferentes escenarios de ataque. Por otro lado, estudios más actuales como el de Lisnevskyi et al. (2026) sí incluyen una evaluación cuantitativa con métricas como los positivos verdaderos, los falsos negativos, los falsos positivos, la precisión, el recall, el F1-score y el tiempo que se tarda

en entregar las notificaciones. Esto pone de manifiesto lo importante que es combinar la implementación técnica con mediciones objetivas del rendimiento del sistema.

Asimismo, la adopción del framework MITRE ATT&CK dentro de los procesos de monitoreo de seguridad ha permitido estandarizar la clasificación de tácticas y técnicas utilizadas por los atacantes. Este marco de referencia facilita la construcción de reglas de correlación más precisas y proporciona un lenguaje común para documentar comportamientos maliciosos observados dentro de una infraestructura tecnológica.

Dentro de este marco, el proyecto actual tiene como objetivo ayudar al campo de la investigación a través de la concepción y puesta en marcha de un SIEM "All-in-One" que emplea tecnologías de código abierto, incorporando Elastic Stack y Suricata en un ambiente virtualizado. La propuesta se enfoca en un ambiente académico replicable, asequible y flexible, donde se pueda entender de manera práctica el ciclo completo de monitoreo de seguridad: creación de eventos, recopilación de registros, normalización, indexación, visualización, correlación y análisis de alertas. Esto contrasta con soluciones comerciales como Splunk Enterprise Security o Microsoft Sentinel.

Además, este proyecto se distingue de otras investigaciones anteriores porque no se restringe solamente a la integración o instalación técnica de las herramientas, sino que incluye una validación experimental a través de escenarios de ataque controlados. Estos escenarios incluyen acciones como escaneo de puertos, fuerza bruta, explotación de servicios web y ejecución remota de comandos. Estas acciones se vincularán con estrategias y técnicas del marco MITRE ATT&CK. Así, la investigación no solo evidencia que el SIEM produce alertas, sino también que posibilita la interpretación de esas alertas en una cadena de comportamiento adverso.

La inclusión de métricas cuantitativas para medir el rendimiento del sistema es otra distinción importante. Este proyecto incluye el estudio de indicadores tales como la inclusión de métricas para evaluar el rendimiento del sistema constituyen otra característica relevante del

proyecto. La evaluación considera dos métricas cuantitativas: la tasa de detección y el tiempo medio de detección. Para calcular la tasa de detección, los resultados de cada escenario serán clasificados como verdaderos positivos cuando el SIEM genere correctamente una alerta asociada con el ataque ejecutado, o como falsos negativos cuando el escenario no sea detectado. Adicionalmente, se realizará un análisis cualitativo de las posibles alertas generadas sobre tráfico legítimo observado durante la operación del laboratorio. Esta metodología permite evaluar la eficacia de la solución a partir de los escenarios controlados y de la evidencia registrada, sin incorporar métricas como precisión o F1-score, cuyo cálculo requeriría un conjunto controlado y cuantificable de actividades legítimas.

La propuesta, se caracteriza por su enfoque educativo, porque une la arquitectura SIEM, la identificación de amenazas de red, el alineamiento con MITRE ATT&CK, la simulación de ataques, la creación de paneles de control y el análisis a través de métricas del rendimiento. Esta integración posibilita que el laboratorio sirva no solo como una solución de monitoreo, sino también como un espacio de aprendizaje, análisis y validaciones para futuras investigaciones en temas de detección de incidentes, optimización de soluciones SIEM de código abierto y ciberseguridad defensiva.

2.2.Marco Teórico

2.2. Ciberseguridad

La ciberseguridad incluye una serie de políticas, tecnologías, procesos y controles que tienen como objetivo salvaguardar redes, aplicaciones, sistemas informáticos y datos contra accesos no autorizados, interrupciones del servicio, ataques cibernéticos o daños. Su meta primordial es asegurar la confidencialidad, la integridad y el acceso a la información, al tiempo que disminuye el efecto de posibles amenazas que puedan perjudicar el funcionamiento normal de una entidad.

En el contexto del presente proyecto, la ciberseguridad constituye el marco general que fundamenta el diseño y despliegue de un SIEM All-in-One dentro de un entorno controlado. La solución propuesta centraliza, procesa y analiza eventos de seguridad provenientes de diferentes componentes de la infraestructura, con el propósito de facilitar la detección temprana de comportamientos anómalos o potencialmente maliciosos. Para ello, Elastic Security permite evaluar los datos recolectados mediante reglas de detección y generar alertas cuando se cumplen las condiciones establecidas, mientras que Suricata proporciona visibilidad sobre la actividad de red mediante la generación de alertas, anomalías y registros en formato EVE JSON (Elastic, 2026; Open Information Security Foundation [OISF], 2026).

Para entender la solución sugerida, este concepto es relevante porque el diseño y la puesta en marcha de un SIEM "All-in-One" son una respuesta directa a la demanda de robustecer las habilidades cibernéticas en un ambiente controlado. La solución que se propone posibilita la recopilación, centralización, correlación y análisis de eventos de seguridad producidos por diversos elementos de la infraestructura, lo que favorece la identificación precoz de conductas maliciosas o sospechosas. Por lo tanto, la ciberseguridad es el marco general que justifica el uso de herramientas como Elastic Stack y Suricata para supervisar, examinar y responder a posibles incidentes.

2.2. Seguridad de la información

La seguridad de la información se enfoca en proteger los activos de información independientemente del medio donde se encuentren almacenados o procesados. Se fundamenta en tres principios conocidos como la triada CIA:

Confidencialidad: Garantiza que la información solo sea accesible para usuarios autorizados.

Integridad: Asegura que los datos no sean modificados de forma no autorizada.

Disponibilidad: Permite que los sistemas y la información estén accesibles cuando sean requeridos. Dentro de los entornos tecnológicos actuales, la seguridad de la información requiere mecanismos de monitoreo continuo que permitan detectar actividades anómalas o incidentes de seguridad oportunamente.

De acuerdo con los conceptos planteados, el SIEM posibilita la supervisión de eventos que pueden poner en peligro la confidencialidad, integridad y disponibilidad de los datos. En este proyecto, Suricata se encarga de identificar tráfico malicioso o sospechoso en la red, mientras que Elastic Stack posibilita la centralización y visualización de los eventos de seguridad. La combinación de las dos herramientas ayuda a detectar conductas que podrían dañar los activos informáticos y posibilita el análisis de alertas, la correlación de eventos y la evaluación del sistema ante situaciones de ataque controladas.

2.2. SIEM (Security Information and Event Management)

La plataforma tecnológica conocida como SIEM, que en inglés significa Security Information and Event Management, tiene el propósito de recoger, unificar, guardar, normalizar, correlacionar y examinar eventos de seguridad que provengan de diversas fuentes en una infraestructura tecnológica. Según Gartner, un SIEM puede definirse como un sistema de registro configurable que recolecta, combina y examina información de eventos de seguridad procedentes de diversos activos tecnológicos (Gartner, 2026). Su objetivo es ayudar a identificar, investigar y reaccionar frente a riesgos. NIST, de manera complementaria, determina que una gestión apropiada de los registros (logs) tiene que posibilitar la recopilación, el análisis, la protección, la revisión y la preservación de los registros producidos por sistemas, aplicaciones y dispositivos de red. Esto se debe a que dichos registros son una fuente esencial para detectar incidentes y realizar auditorías (Kent & Souppaya, 2006).

Históricamente, los SIEM surgen de la integración de dos enfoques: SIM (Security Information Management) y SEM (Security Event Management). El componente SIM se orienta al

almacenamiento, consulta y análisis histórico de registros, lo cual permite revisar eventos pasados, apoyar procesos de auditoría y reconstruir actividades ocurridas dentro de un sistema. Por su parte, el componente SEM se enfoca en el monitoreo en tiempo real, la correlación de eventos y la generación de alertas ante comportamientos sospechosos o potencialmente maliciosos. La combinación de ambos enfoques permite que un SIEM proporcione tanto visibilidad histórica como capacidad de detección operativa.

Las funciones principales de un SIEM incluyen la recolección centralizada de logs, normalización de eventos, correlación de registros, generación automática de alertas, visualización mediante dashboards, retención de información, soporte para auditoría, investigación de incidentes y cumplimiento normativo. Estas capacidades son importantes porque los eventos de seguridad suelen generarse de forma distribuida en diferentes componentes, como servidores, estaciones de trabajo, firewalls, aplicaciones, sistemas de autenticación, servicios en la nube e IDS/IPS.

En el presente proyecto, el concepto de SIEM se vincula directamente con la arquitectura propuesta, ya que Elastic Stack será utilizado como plataforma central para la ingesta, indexación, búsqueda, análisis y visualización de eventos de seguridad. Elasticsearch permitirá almacenar e indexar los datos recolectados; Kibana facilitará la construcción de dashboards, búsquedas y visualizaciones; y Elastic Security permitirá administrar reglas de detección, alertas e investigaciones dentro del entorno de laboratorio. Elastic Security también permite trabajar con reglas preconstruidas y personalizadas, así como visualizar cobertura relacionada con tácticas y técnicas del marco MITRE ATT&CK, lo cual fortalece el análisis de los escenarios de ataque evaluados (Elastic, 2026).

De esta manera, la solución SIEM “All-in-One” propuesta integra los principios teóricos del SIEM con componentes prácticos de código abierto. Suricata genera eventos relacionados con posibles amenazas de red; Elastic Stack centraliza, almacena, procesa y visualiza dichos eventos; y Elastic Security permite crear reglas, gestionar alertas y analizar los resultados obtenidos en los

escenarios de ataque controlados. Esta integración permite evaluar la efectividad del sistema frente a actividades como escaneo de puertos, fuerza bruta, explotación de servicios web y ejecución remota de comandos, relacionando los eventos generados con técnicas MITRE ATT&CK y métricas de desempeño como verdaderos positivos, falsos positivos, falsos negativos, precisión y tiempo medio de detección.

2.2. Arquitectura SIEM "All-in-One"

Una arquitectura SIEM "All-in-One" integra en un único entorno los componentes necesarios para la recolección, procesamiento, almacenamiento, correlación y visualización de eventos de seguridad. A diferencia de una arquitectura distribuida, donde los servicios se separan en diferentes nodos o servidores especializados, el enfoque All-in-One concentra los servicios principales dentro de una sola plataforma o servidor. Esto simplifica la administración, reduce los requerimientos de infraestructura y facilita la implementación inicial del sistema.

La arquitectura propuesta en este proyecto está compuesta por los siguientes elementos: Filebeat, como agente encargado de recolectar logs desde diferentes sistemas; Logstash, como herramienta utilizada para procesar, transformar y normalizar eventos; Elasticsearch, como motor de indexación y búsqueda de datos; Kibana, como plataforma de visualización y análisis; Elastic Security, como módulo especializado para detección y gestión de eventos de seguridad; y Suricata, como sistema IDS/IPS para el monitoreo de tráfico de red. Esta integración permite centralizar información proveniente de servidores, dispositivos de red y sensores de seguridad en una única plataforma de análisis.

No obstante, una arquitectura All-in-One también presenta limitaciones importantes. Al centralizar todos los servicios en un mismo servidor, los recursos de procesamiento, memoria, almacenamiento y red son compartidos por todos los componentes, lo que puede generar degradación del rendimiento cuando aumenta el volumen de eventos. Además, este tipo de

arquitectura representa un único punto de falla, ya que una interrupción del servidor principal podría afectar simultáneamente la recolección, procesamiento, almacenamiento, visualización y análisis de eventos. También puede presentar limitaciones de escalabilidad, debido a que el crecimiento del sistema depende principalmente de la capacidad del servidor donde se encuentran instalados todos los servicios.

En contraste, una arquitectura SIEM distribuida separa los componentes principales en distintos servidores o nodos especializados. Por ejemplo, puede contar con nodos dedicados para ingesta de datos, procesamiento, almacenamiento, búsqueda, visualización y sensores de red. Este enfoque permite mayor escalabilidad, tolerancia a fallos y rendimiento en entornos empresariales con grandes volúmenes de eventos. Sin embargo, también requiere mayor inversión en infraestructura, administración más compleja, conocimientos avanzados de arquitectura, monitoreo de nodos, balanceo de carga, respaldo, alta disponibilidad y mantenimiento.

Para el presente proyecto, la arquitectura All-in-One resulta pertinente debido a que el objetivo principal no es desplegar una solución SIEM empresarial de alta disponibilidad, sino implementar un laboratorio académico funcional, controlado y replicable. Este enfoque permite comprender de forma práctica el flujo completo de los eventos de seguridad, desde su generación hasta su visualización y análisis. Además, facilita la evaluación de escenarios de ataque controlados, la creación de reglas de detección, el análisis de alertas y la medición de métricas de desempeño sin requerir una infraestructura extensa o costos elevados.

Por lo tanto, aunque una arquitectura distribuida sería más adecuada para un entorno productivo con alta demanda de procesamiento, disponibilidad y escalabilidad, la arquitectura All-in-One es apropiada para fines académicos y experimentales. Su principal ventaja radica en que permite integrar todos los componentes esenciales de un SIEM en un solo entorno, favoreciendo el aprendizaje, la implementación progresiva, la reducción de costos y la validación técnica de la solución propuesta

Tabla 3
Comparación conceptual entre arquitectura SIEM All-in-One y arquitectura distribuida.

Criterio	Arquitectura All-in-One	Arquitectura distribuida
Distribución de componentes	Los servicios principales del SIEM se concentran en un solo servidor o entorno.	Los servicios se separan en diferentes nodos o servidores especializados.
Complejidad de implementación	Menor complejidad, adecuada para laboratorios, pruebas de concepto y aprendizaje.	Mayor complejidad, requiere diseño de arquitectura, comunicación entre nodos y administración avanzada.
Requerimientos de infraestructura	Requiere menos servidores y menor inversión inicial.	Requiere mayor cantidad de recursos, servidores, almacenamiento y capacidad de red.
Escalabilidad	Limitada por la capacidad del servidor principal.	Mayor escalabilidad, ya que permite agregar nodos de ingesta, procesamiento o almacenamiento.
Rendimiento	Puede verse afectado si aumenta el volumen de eventos o si todos los servicios consumen recursos simultáneamente.	Mejor rendimiento en entornos de alta carga, al distribuir procesos entre varios nodos.
Tolerancia a fallos	Presenta un único punto de falla; si el servidor principal falla, se afecta toda la solución.	Puede ofrecer mayor disponibilidad si se implementan redundancia, balanceo y alta disponibilidad.
Administración	Más sencilla, ya que todos los componentes se gestionan desde un mismo entorno.	Más compleja, porque requiere administrar múltiples nodos y servicios interconectados.
Costo	Menor costo inicial, especialmente en entornos académicos.	Mayor costo por infraestructura, mantenimiento y recursos especializados.

2.2. Elastic Stack

Elastic Stack es un conjunto de herramientas orientadas a la ingesta, procesamiento, almacenamiento, búsqueda, análisis y visualización de grandes volúmenes de datos. En el contexto de ciberseguridad, Elastic Stack permite construir soluciones SIEM personalizadas, ya que facilita la centralización de eventos provenientes de distintas fuentes, su normalización, indexación, consulta y representación visual mediante dashboards. Está conformado principalmente por Elasticsearch, Logstash y Kibana, aunque en entornos de seguridad también se complementa con Beats, Elastic Agent y Elastic Security.

Dentro del presente proyecto, Elastic Stack cumple un rol central en el flujo de detección y correlación de eventos. Suricata genera eventos de seguridad relacionados con el tráfico de red;

Filebeat o Elastic Agent recolecta dichos eventos; Logstash puede procesarlos, transformarlos y normalizarlos; Elasticsearch los almacena e indexa; Kibana permite visualizarlos mediante dashboards; y Elastic Security facilita la creación de reglas de detección, administración de alertas y análisis de eventos asociados a posibles incidentes.

2.2. Elasticsearch

Es un motor de búsqueda y análisis distribuido basado en Apache Lucene. Permite indexar grandes volúmenes de información y realizar búsquedas rápidas sobre eventos y registros de seguridad.

Entre sus características principales destacan:

- Escalabilidad.
- Indexación distribuida.
- Búsquedas en tiempo real.
- Almacenamiento estructurado de eventos.

Elasticsearch actuaría como el repositorio central donde se conservan los eventos de seguridad. Esto permite consultar registros históricos, identificar patrones, filtrar eventos por dirección IP, puerto, protocolo, tipo de alerta, severidad o técnica asociada, y apoyar la correlación de actividades sospechosas. Por ejemplo, si Suricata detecta múltiples intentos de conexión hacia distintos puertos, Elasticsearch permite almacenar esos eventos y facilitar su análisis posterior para determinar si corresponden a un escaneo de puertos.

2.2. Logstash

Es una herramienta de procesamiento de datos encargada de recibir eventos desde múltiples fuentes, transformarlos y enviarlos hacia diferentes destinos.

Sus funciones incluyen:

- Filtrado de eventos.
- Normalización de logs.
- Conversión de formatos.

- Enriquecimiento de información.

Esto permitiría preparar los datos para que puedan ser interpretados de forma adecuada por el SIEM. Por ejemplo, puede convertir formatos de logs, extraer campos relevantes, agregar información contextual, clasificar eventos o adaptar los registros generados por sensores de seguridad. Esta etapa es importante porque la correlación depende de que los eventos se encuentren correctamente estructurados y normalizados

2.2. Kibana

Kibana proporciona una interfaz gráfica para la visualización y análisis de información almacenada en Elasticsearch.

Permite:

- Crear dashboards interactivos.
- Visualizar alertas.
- Analizar eventos de seguridad.
- Generar reportes.

Kibana permite transformar los registros técnicos en información comprensible. A través de dashboards, gráficos y tablas, es posible observar tendencias, cantidad de alertas, direcciones IP involucradas, protocolos utilizados, tipos de ataques detectados y comportamiento temporal de los eventos. Esto facilita la interpretación de los resultados y apoya la evaluación del desempeño del SIEM.

2.2. Elastic Security

Elastic Security es un módulo especializado de Elastic Stack orientado a operaciones de seguridad. Proporciona capacidades SIEM y análisis de endpoints dentro de la plataforma Elastic.

Entre sus principales funcionalidades se encuentran:

- Detección de amenazas.
- Gestión de alertas.

- Timeline de eventos.
- Integración con MITRE ATT&CK.
- Dashboards de seguridad.
- Correlación avanzada de eventos.

Elastic Security facilita la creación de reglas de detección basadas en consultas EQL (Elastic Query Language) y la clasificación de eventos según tácticas y técnicas de ataque.

Elastic Security cumple un papel fundamental, ya que permite evaluar los eventos almacenados en Elasticsearch mediante reglas predefinidas o personalizadas. Por ejemplo, una regla puede generar una alerta cuando se detectan múltiples intentos de conexión fallidos, tráfico asociado a explotación web o patrones compatibles con reconocimiento de red. De esta manera, Elastic Security no solo permite visualizar eventos, sino también convertirlos en alertas útiles para el análisis de incidentes.

2.2. Filebeat

Filebeat es un agente ligero de recolección de logs desarrollado por Elastic. Su función principal consiste en monitorear archivos de registro y enviar eventos hacia Logstash o Elasticsearch.

Entre sus ventajas destacan:

- Bajo consumo de recursos.
- Compatibilidad con múltiples sistemas operativos.
- Envío seguro de eventos.
- Integración nativa con Elastic Stack.

En este proyecto, Filebeat será utilizado para recolectar eventos desde servidores Windows, Linux y servicios web.

2.2. Suricata

Suricata es un sistema IDS/IPS de código abierto diseñado para detectar amenazas mediante inspección profunda de paquetes de red.

Sus principales características incluyen:

- Detección basada en firmas.
- Inspección de protocolos.
- Análisis de tráfico en tiempo real.
- Generación de alertas de seguridad.
- Compatibilidad con reglas Snort.

Suricata permite detectar actividades maliciosas como escaneo de puertos, ataques web, malware y tráfico sospechoso dentro de la red.

La capacidad de crear eventos en formato EVE JSON es una de las propiedades más destacadas de Suricata para su integración con plataformas SIEM. Suricata utiliza el formato de salida EVE como principal para registrar eventos de red en estructura JSON. Esto posibilita que cada evento tenga campos estructurados, incluyendo la dirección IP de origen y destino, los puertos, la fecha y hora, el protocolo, el tipo y la gravedad del evento, el identificador de flujo, la firma detectada, la categoría de alerta y metadatos relacionados. Según la documentación oficial de Suricata, la salida EVE posibilita la generación de anomalías, alertas, metadatos, datos de archivos y registros específicos de protocolos en formato JSON (Suricata, 2026).

El archivo eve.json no solo registra alertas de seguridad, sino también distintos tipos de eventos de red que aportan contexto para el análisis. Entre estos se incluyen eventos HTTP, DNS, TLS, flujo de red, archivos, estadísticas y anomalías. Por ejemplo, un evento de tipo alert puede indicar que una regla de detección fue activada por tráfico sospechoso; un evento dns puede registrar consultas y respuestas de nombres de dominio; un evento http puede incluir información sobre métodos, códigos de respuesta, URL o agentes de usuario; un evento tls puede registrar

metadatos de certificados o conexiones cifradas; y un evento flow puede describir la comunicación entre dos extremos de red. Esta variedad de eventos permite que el SIEM no dependa únicamente de una alerta aislada, sino que pueda analizar el contexto completo del tráfico observado.

Dentro del presente proyecto, Suricata cumple la función de sensor de red encargado de inspeccionar el tráfico generado durante los escenarios de ataque controlados. Cuando se ejecutan actividades como escaneo de puertos, fuerza bruta, explotación de servicios web o intentos de ejecución remota de comandos, Suricata analiza los paquetes de red y genera eventos en eve.json cuando identifica coincidencias con reglas configuradas o comportamientos relevantes. Estos eventos constituyen la fuente principal de información para alimentar el pipeline de Elastic.

La integración con Elastic se realiza mediante un flujo de ingesta en el que los eventos generados por Suricata son recolectados por Filebeat o Elastic Agent, procesados y posteriormente enviados hacia Elasticsearch. Elastic cuenta con una integración específica para Suricata, la cual permite recolectar logs generados por este IDS/IPS/NSM y procesar eventos en formato EVE JSON. Asimismo, el módulo de Suricata para Filebeat está diseñado para interpretar logs EVE JSON y preparar los datos para su almacenamiento y análisis dentro de Elastic Stack (Elastic, 2026).

En el pipeline de Elastic, los eventos de Suricata pueden ser normalizados, enriquecidos y almacenados en índices de Elasticsearch. Posteriormente, Kibana permite visualizar dichos eventos mediante dashboards, tablas, filtros y gráficos; mientras que Elastic Security puede utilizar los datos recolectados para generar alertas, ejecutar reglas de detección, apoyar investigaciones y relacionar eventos con tácticas y técnicas del marco MITRE ATT&CK. De esta manera, Suricata no funciona de forma aislada, sino como un componente generador de eventos que alimenta el SIEM y permite transformar el tráfico de red en información útil para la detección y análisis de amenazas.

Por lo tanto, Suricata cumple un rol fundamental dentro de la arquitectura propuesta, ya que proporciona visibilidad sobre el tráfico de red y genera evidencia técnica de posibles ataques. Su salida en formato EVE JSON facilita la integración con Elastic Stack, permitiendo que los eventos detectados sean recolectados, procesados, indexados, visualizados y correlacionados dentro del SIEM. Esta integración fortalece la capacidad del proyecto para evaluar escenarios de ataque controlados y medir la efectividad del sistema mediante métricas como verdaderos positivos, falsos positivos, falsos negativos y tiempo medio de detección.

Tabla 4
Tipos de eventos generados por Suricata y su utilidad dentro del SIEM.

Tipo de evento en Suricata	Descripción	Utilidad dentro del pipeline de Elastic
alert	Evento generado cuando una regla de Suricata detecta tráfico sospechoso o malicioso.	Permite generar alertas de seguridad, identificar firmas activadas y analizar severidad, categoría e IPs involucradas.
flow	Registra información sobre comunicaciones entre origen y destino, incluyendo protocolo, puertos y estado del flujo.	Aporta contexto para correlacionar conexiones, identificar patrones de comunicación y analizar actividad de red.
dns	Registra consultas y respuestas DNS observadas en la red.	Permite analizar dominios consultados, detectar posibles comunicaciones sospechosas o apoyar investigaciones de malware.
http	Registra información de tráfico web, como método, host, URL, agente de usuario y códigos de respuesta.	Ayuda a identificar intentos de explotación web, navegación sospechosa o patrones asociados a reconocimiento.
tls	Registra metadatos de conexiones cifradas, certificados y parámetros TLS.	Permite analizar conexiones seguras, certificados anómalos o comunicaciones cifradas sospechosas.
fileinfo	Registra información de archivos observados durante transferencias de red.	Permite identificar descargas, tipos de archivos, hashes y posibles transferencias maliciosas.
anomaly	Registra comportamientos anómalos o inconsistencias detectadas en protocolos o tráfico.	Ayuda a detectar comportamientos fuera de lo esperado que podrían complementar una investigación.

Tipo de evento en Suricata	Descripción	Utilidad dentro del pipeline de Elastic
stats	Registra estadísticas de funcionamiento del motor Suricata.	Permite monitorear rendimiento, volumen de eventos, paquetes procesados y posibles pérdidas.

Tabla 5
Integración de Suricata con el pipeline de Elastic

Etapa del pipeline	Componente	Función dentro del proyecto
Inspección de tráfico	Suricata	Analiza el tráfico de red y aplica reglas de detección sobre los paquetes observados.
Generación de eventos	Suricata EVE JSON	Registra alertas y eventos de red en formato estructurado JSON.
Recolección	Filebeat / Elastic Agent	Lee el archivo eve.json y envía los eventos hacia Elastic Stack.
Procesamiento	Filebeat module / Elastic integration / Logstash	Interpreta, normaliza o transforma los campos de Suricata para facilitar su análisis.
Almacenamiento	Elasticsearch	Indexa los eventos de Suricata para búsquedas, consultas y análisis histórico.
Visualización	Kibana	Presenta los eventos mediante dashboards, gráficos, filtros y tablas.
Detección y correlación	Elastic Security	Permite generar alertas, investigar eventos y relacionarlos con escenarios de ataque y MITRE ATT&CK.

2.2. Logs y eventos de seguridad

Los logs son registros generados por sistemas operativos, aplicaciones, dispositivos de red y herramientas de seguridad que documentan actividades realizadas dentro de una infraestructura tecnológica.

Los eventos de seguridad representan acciones relevantes relacionadas con autenticaciones, conexiones, errores, accesos no autorizados o actividades potencialmente maliciosas.

La centralización y análisis de logs permiten:

- Detectar anomalías.
- Investigar incidentes.

- Realizar auditorías.
- Correlacionar eventos.
- Generar alertas tempranas.

A continuación, se detallan las diferencias entre evento, log, alerta e incidente:

Tabla 6
Diferencias conceptuales entre log, evento, alerta e incidente

Concepto	Definición	Ejemplo en el proyecto	Relación con la evaluación
Log	Registro técnico generado por un activo.	Línea registrada en eve.json de Suricata o log generado.	Es la fuente primaria de información para el SIEM.
Evento	Acción identificada a partir de uno o varios logs.	Conexión TCP, petición HTTP, intento de autenticación o tráfico detectado.	Permite analizar comportamientos dentro del entorno monitoreado.
Alerta	Notificación generada por una regla de detección.	Alerta por escaneo de puertos, explotación o tráfico sospechoso.	Se clasifica como verdadero positivo, falso positivo o falso negativo según el escenario evaluado.
Incidente	Situación confirmada o altamente probable que representa una amenaza.	Fuerza bruta con autenticación exitosa no autorizada o explotación web confirmada en el laboratorio.	Permite valorar la efectividad del SIEM para apoyar el análisis y respuesta ante amenazas.

2.2. Correlación de eventos

La correlación de eventos es el proceso mediante el cual un SIEM analiza múltiples registros provenientes de distintas fuentes para identificar patrones asociados a comportamientos maliciosos.

Este proceso permite transformar eventos aislados en alertas significativas, reduciendo el ruido generado por grandes volúmenes de información.

Un evento aislado se convierte en una alerta relevante cuando cumple una condición previamente definida en una regla de detección o correlación. Esta condición puede estar basada en la repetición de eventos dentro de un periodo determinado, la coincidencia con una firma de ataque, la relación entre diferentes fuentes de logs, la presencia de indicadores de compromiso, el comportamiento anómalo de un usuario o la ejecución de una secuencia de acciones asociada a

una técnica adversaria. Por lo tanto, no todo evento registrado por el SIEM representa una alerta; únicamente se genera una alerta cuando el evento cumple criterios que aumentan su relevancia desde el punto de vista de seguridad.

Las reglas de correlación pueden basarse en:

- Umbrales.
- Secuencia temporal de eventos.
- Direcciones IP.
- Usuarios.
- Firmas de ataque.
- Patrones de comportamiento.

Por ejemplo, un único intento fallido de autenticación puede considerarse un evento común; sin embargo, múltiples intentos fallidos desde una misma dirección IP hacia un mismo servicio en un corto periodo de tiempo pueden convertirse en una alerta de posible ataque de fuerza bruta. De igual manera, una conexión hacia un puerto específico puede ser normal, pero múltiples conexiones consecutivas hacia varios puertos de un servidor pueden indicar un posible escaneo de puertos.

En el presente proyecto, la correlación de eventos permitirá evaluar los escenarios de ataque controlados ejecutados dentro del laboratorio. Los eventos generados por Suricata serán recolectados e indexados en Elastic Stack, donde podrán ser analizados mediante reglas, consultas, filtros y dashboards. Cuando dichos eventos cumplan condiciones definidas, como número de intentos, coincidencia con firmas de Suricata, comportamiento repetitivo, relación entre IP origen y destino o alineación con una técnica MITRE ATT&CK, serán considerados alertas relevantes para el análisis.

De esta forma, la correlación permite diferenciar entre actividad normal, eventos informativos y posibles amenazas. Su importancia dentro del SIEM radica en que ayuda a

priorizar la información, reducir el ruido operativo y enfocar el análisis en aquellos eventos que presentan mayor probabilidad de estar relacionados con una actividad maliciosa.

2.2. MITRE ATT&CK

MITRE ATT&CK es un framework de conocimiento que documenta tácticas, técnicas y procedimientos utilizados por atacantes reales durante distintas fases de una intrusión.

Este marco proporciona una clasificación estructurada de comportamientos adversarios y es ampliamente utilizado en ciberseguridad para:

- Diseño de reglas de detección.
- Simulación de ataques.
- Cacería de amenazas.
- Evaluación de cobertura defensiva.

Dentro del presente proyecto se utilizarán técnicas como:

Tabla 7
Criterios de selección de técnicas MITRE ATT&CK para el laboratorio.

Técnica MITRE ATT&CK	Táctica asociada	Criterio de selección	Evidencia esperada en el SIEM
T1046 – Network Service Scanning	Discovery	Representa una fase común de reconocimiento y puede simularse de forma controlada con herramientas como Nmap.	Conexiones hacia múltiples puertos, alertas IDS/IPS, eventos de red y patrones de escaneo.
T1110 – Brute Force	Credential Access	Permite evaluar intentos repetidos de autenticación contra servicios expuestos.	Múltiples intentos fallidos, eventos de autenticación, tráfico repetitivo hacia servicios como SSH o HTTP.
T1190 – Exploit Public-Facing Application	Initial Access	Permite simular explotación de servicios o aplicaciones web vulnerables dentro del laboratorio.	Alertas de Suricata, solicitudes HTTP sospechosas, patrones de explotación y eventos asociados a servicios expuestos.
T1059 – Command and Scripting Interpreter	Execution	Permite representar la ejecución de comandos o scripts tras una explotación o acceso inicial.	Comandos ejecutados, tráfico relacionado, eventos del sistema o evidencia de actividad posterior al compromiso.

Técnica MITRE ATT&CK	Táctica asociada	Criterio de selección	Evidencia esperada en el SIEM
T1021 – REMOTE SERVICES	Lateral Movement	Permite simular movimiento lateral desde el equipo cliente del dominio hacia el controlador de dominio mediante RDP con credenciales válidas previamente obtenidas.	EventID 4624 desde VLAN20, conexión RDP entre segmentos, registros de autenticación del controlador de dominio.
T1078 – VALID ACCOUNTS	Defense Evasion - Persistenc	Permite evaluar el uso de credenciales legítimas en un contexto anómalo, simulando un escenario de assumed breach desde el equipo cliente.	EventID 4624 con logon_type inusual, autenticación exitosa desde segmento de usuarios hacia servidores.

Por lo tanto, estas técnicas fueron seleccionadas porque cubren distintas etapas de una posible cadena de ataque dentro de un entorno controlado: reconocimiento, acceso inicial, ejecución y abuso de credenciales. Además, son técnicas técnicamente viables para el laboratorio, generan eventos detectables por las herramientas implementadas y permiten evaluar la efectividad del SIEM mediante métricas cuantitativas.

Los escenarios implementados permiten evaluar actividades asociadas con acceso a credenciales mediante T1110, descubrimiento de servicios de red mediante T1046, acceso inicial mediante T1190 y movimiento lateral mediante T1021 y T1078. Cada escenario genera registros que pueden ser recolectados, correlacionados y analizados por el SIEM, permitiendo evaluar su capacidad de detección mediante la tasa de detección y el tiempo medio de detección, complementados con un análisis cualitativo de posibles falsos positivos.

2.2. Reglas Sigma

Sigma es un formato abierto y genérico utilizado para describir reglas de detección de eventos de seguridad de manera independiente de la plataforma SIEM utilizada.

Las reglas Sigma permiten:

- Estandarizar detecciones.

- Compartir reglas entre plataformas.
- Facilitar conversiones hacia otros lenguajes como EQL o SPL.

Una regla Sigma normalmente contiene:

- Nombre de la detección.
- Descripción.
- Fuente de logs.
- Condiciones de detección.
- Nivel de severidad.
- Referencia MITRE ATT&CK.

2.2. Elastic Query Language (EQL)

Elastic Query Language es un lenguaje de consulta desarrollado por Elastic para detectar secuencias de eventos y patrones complejos dentro de los datos almacenados en Elasticsearch.

EQL permite:

- Crear reglas de correlación.
- Detectar comportamientos sospechosos.
- Analizar secuencias temporales.
- Identificar actividades anómalas.

EQL permite crear reglas de correlación, detectar comportamientos sospechosos, analizar secuencias temporales e identificar actividades anómalas. En Elastic Security, este lenguaje se utiliza principalmente para construir reglas de detección y correlación de eventos. Estas reglas pueden identificar eventos individuales con condiciones específicas, secuencias ordenadas de eventos o incluso la ausencia de eventos esperados. De esta manera, EQL facilita la detección de comportamientos que no siempre pueden identificarse mediante el análisis de un único evento aislado.

Dentro del presente proyecto, EQL será considerado como un mecanismo de apoyo para la detección y correlación de eventos generados en el laboratorio virtualizado. Su aplicación estará orientada a los escenarios de ataque definidos para la evaluación del SIEM, específicamente fuerza bruta, escaneo web, escaneo o ataque a puertos de servidores web y ataques dirigidos contra Active Directory. Estos escenarios generan múltiples eventos que, al analizarse de forma aislada, pueden parecer actividades comunes; sin embargo, al relacionarse temporalmente pueden evidenciar un comportamiento sospechoso o malicioso.

Por ejemplo, en un escenario de fuerza bruta, un único intento fallido de autenticación puede no representar una amenaza relevante; sin embargo, múltiples intentos fallidos contra una misma cuenta, servicio o servidor dentro de un periodo corto pueden convertirse en una alerta significativa. En un escenario de escaneo web, varias solicitudes hacia rutas inexistentes, directorios sensibles, archivos comunes o endpoints administrativos desde una misma dirección IP podrían indicar una actividad de reconocimiento. De igual manera, en un ataque a puertos de servidores web, conexiones sucesivas hacia distintos puertos o servicios expuestos pueden representar una técnica de descubrimiento de servicios. En el caso de Active Directory, múltiples fallos de autenticación, intentos contra diferentes cuentas de dominio o patrones anómalos relacionados con usuarios y servicios de autenticación podrían ser utilizados como indicadores para generar alertas de seguridad.

En el presente proyecto, las reglas de detección serán implementadas directamente en Elastic Security mediante los mecanismos de consulta y activación que resulten más adecuados para cada escenario. Para aquellas detecciones que requieran filtrar, agrupar y contabilizar eventos se podrá utilizar Elasticsearch Query Language, mientras que en otros casos se emplearán consultas personalizadas, condiciones de umbral u otros tipos de reglas disponibles en la plataforma. Por lo tanto, no se establece el uso obligatorio de EQL para todas las reglas implementadas. Cada regla será documentada de acuerdo con su configuración real, incluyendo la

fuente de datos, los campos evaluados, la consulta o condición utilizada, el umbral de activación, el intervalo de ejecución, el nivel de severidad y la técnica MITRE ATT&CK asociada..

El uso de EQL dentro de la solución propuesta se justifica porque permite transformar eventos individuales en alertas más relevantes mediante reglas de correlación. Esto fortalece la capacidad del SIEM para identificar patrones asociados a técnicas MITRE ATT&CK, tales como T1110 – Brute Force, T1046 – Network Service Scanning, T1190 – Exploit Public-Facing Application y técnicas relacionadas con ataques contra servicios de autenticación o entornos de dominio. Por lo tanto, EQL contribuye a que Elastic Security no solo almacene y visualice eventos, sino que también permita analizar comportamientos relacionados con los escenarios ofensivos definidos en el laboratorio.Su integración con Elastic Security facilita la construcción de reglas de detección avanzadas alineadas a MITRE ATT&CK.

Tabla 8
Aplicación conceptual de EQL en los escenarios del laboratorio

Escenario del laboratorio	Patrón que podría analizarse con EQL	Fuente de eventos esperada	Propósito dentro del SIEM
Fuerza bruta	Múltiples intentos fallidos de autenticación desde una misma IP, usuario o servicio dentro de una ventana temporal.	Logs de autenticación, eventos de servidor, registros de Active Directory o servicios expuestos.	Identificar intentos repetitivos de acceso no autorizado y generar alertas correlacionadas.
Escaneo web	Solicitudes repetitivas hacia rutas inexistentes, paneles administrativos, archivos sensibles o endpoints comunes.	Logs del servidor web, eventos HTTP de Suricata y registros indexados en Elastic.	Detectar actividades de reconocimiento contra aplicaciones o servicios web.
Escaneo o ataque a puertos de servidores web	Conexiones sucesivas hacia múltiples puertos o servicios expuestos desde una misma IP origen.	Eventos de red generados por Suricata y registros del servidor monitoreado.	Identificar comportamiento compatible con descubrimiento de servicios o reconocimiento de red.

Escenario del laboratorio	Patrón que podría analizarse con EQL	Fuente de eventos esperada	Propósito dentro del SIEM
Ataque al Active Directory	Fallos de autenticación repetidos, intentos contra múltiples cuentas, accesos anómalos o eventos asociados a servicios de dominio.	Eventos de Windows, logs de autenticación, registros del controlador de dominio y eventos enviados a Elastic.	Correlacionar actividad sospechosa relacionada con cuentas, credenciales y servicios de autenticación.
Correlación entre fuentes	Relación temporal entre eventos de Suricata, logs web, eventos de autenticación y alertas de Elastic Security.	Suricata, servidores web, Active Directory y Elastic Security.	Convertir múltiples eventos aislados en alertas relevantes para el análisis del laboratorio.

2.2. IDS e IPS

Un IDS, por sus siglas en inglés Intrusion Detection System, es un sistema encargado de monitorear el tráfico de red o la actividad de un sistema con el objetivo de identificar comportamientos sospechosos, anómalos o potencialmente maliciosos. Su función principal es detectar posibles amenazas y generar alertas para que puedan ser analizadas por un administrador, analista de seguridad o plataforma SIEM.

Un IPS, por sus siglas en inglés Intrusion Prevention System, cumple una función similar al IDS en cuanto a la detección de amenazas; sin embargo, incorpora además la capacidad de prevenir o bloquear automáticamente determinadas actividades maliciosas. Para ello, el IPS suele operar en línea dentro del flujo de tráfico, de manera que puede inspeccionar paquetes y tomar acciones como descartar conexiones, bloquear direcciones IP o impedir que una comunicación sospechosa continúe.

La diferencia principal entre ambos enfoques radica en su modo de operación. Un IDS trabaja de forma pasiva o fuera de línea respecto al tráfico, observando los eventos y generando alertas sin intervenir directamente en la comunicación. En cambio, un IPS opera de forma activa o

en línea, ya que se ubica dentro del camino del tráfico y puede aplicar medidas de bloqueo o prevención en tiempo real.

Dentro del presente proyecto, Suricata será utilizado principalmente en modo IDS/NSM, es decir, como sensor de monitoreo y detección de tráfico de red. Su función será inspeccionar el tráfico generado durante los escenarios controlados del laboratorio, identificar coincidencias con reglas de detección y generar eventos de seguridad en formato EVE JSON. Estos eventos serán enviados posteriormente hacia Elastic Stack para su almacenamiento, visualización, análisis y correlación dentro del SIEM.

Por lo tanto, aunque Suricata posee capacidades tanto IDS como IPS, en este proyecto no se utilizará como mecanismo de bloqueo activo de tráfico. Su operación estará orientada a la detección y generación de alertas, permitiendo observar ataques como fuerza bruta, escaneo web, escaneo o ataque a puertos de servidores web y actividades dirigidas contra Active Directory. Esta decisión responde al enfoque académico del laboratorio, cuyo objetivo principal es evaluar la capacidad de detección, correlación y análisis del SIEM, más que implementar medidas automáticas de prevención o contención.

La utilización de Suricata en modo IDS/NSM permite reducir riesgos dentro del entorno de pruebas, ya que no altera ni bloquea el tráfico generado por los escenarios de ataque. Esto facilita la recolección completa de evidencia, el análisis posterior de eventos y la medición de métricas de desempeño como verdaderos positivos, falsos positivos, falsos negativos y tiempo medio de detección. En consecuencia, Suricata actuará como una fuente generadora de eventos de seguridad, mientras que Elastic Stack y Elastic Security serán responsables de centralizar, visualizar y correlacionar dichos eventos dentro de la arquitectura SIEM propuesta

Tabla 9
Diferencia conceptual entre IDS, IPS y modo utilizado en el proyecto

Concepto	Modo de operación	Acción principal	Uso dentro del proyecto
IDS	Pasivo o fuera de línea respecto al tráfico.	Detectar actividad sospechosa y generar alertas.	Suricata será utilizado bajo este enfoque para monitorear tráfico y generar eventos hacia Elastic Stack.
IPS	Activo o en línea dentro del flujo de tráfico.	Detectar y bloquear tráfico malicioso automáticamente.	No será utilizado como modo principal, ya que el proyecto no busca bloquear tráfico, sino evaluar detección y correlación.

2.2. Virtualización

La virtualización es una tecnología que permite ejecutar múltiples sistemas operativos dentro de una misma infraestructura física mediante máquinas virtuales.

Su utilización en entornos de laboratorio permite:

- Simular infraestructuras reales.
- Ejecutar escenarios de ataque controlados.
- Reducir costos de implementación.
- Aislar ambientes de prueba.

En entornos académicos y de ciberseguridad, la virtualización resulta especialmente útil porque permite simular infraestructuras reales sin necesidad de contar con múltiples equipos físicos. Además, facilita la ejecución de escenarios de ataque controlados, reduce costos de implementación, permite restaurar máquinas mediante snapshots y contribuye al aislamiento de ambientes de prueba.

En el presente proyecto, la virtualización permitirá construir un entorno seguro y controlado para validar la efectividad del SIEM implementado en la plataforma de virtualización Virtual Box Versión 7.2.12, debido a que permite crear y administrar máquinas virtuales de forma local, configurar redes virtuales, asignar recursos por máquina y aislar el laboratorio del entorno físico principal.

La arquitectura virtual del laboratorio estará compuesta por máquinas destinadas a cumplir roles específicos dentro del escenario de análisis. Entre ellas se consideran una máquina atacante, basada en Kali Linux; un servidor SIEM All-in-One con Elastic Stack, Elastic Security y Suricata; servidores web vulnerables o servicios expuestos para pruebas controladas; y un entorno Windows/Active Directory para evaluar eventos relacionados con autenticación, usuarios y servicios de dominio. Esta distribución permite representar una infraestructura básica donde se puedan ejecutar ataques de fuerza bruta, escaneo web, escaneo o ataque a puertos de servidores web y actividades dirigidas contra Active Directory.

A nivel de red, se utilizará una red virtual interna o segmentada, configurada dentro de Virtual Box, con el objetivo de que las máquinas del laboratorio puedan comunicarse entre sí sin exponer directamente los servicios vulnerables hacia redes externas o productivas. Esta red virtual permitirá simular la comunicación entre atacante, servidores monitoreados, controlador de dominio y SIEM, manteniendo controlado el tráfico generado durante las pruebas. Dependiendo del escenario, se podrá utilizar una red tipo Host-Only para mantener el laboratorio aislado del exterior, o una red NAT únicamente cuando sea necesario descargar actualizaciones, paquetes o reglas de detección, evitando publicar servicios vulnerables hacia Internet.

El aislamiento del laboratorio constituye una consideración fundamental de seguridad. Al tratarse de un entorno donde se ejecutarán ataques simulados y pruebas ofensivas controladas, las máquinas virtuales no deberán interactuar con sistemas productivos ni con redes corporativas reales. Asimismo, se recomienda limitar el acceso a Internet de las máquinas vulnerables, evitar el uso de credenciales reales, deshabilitar carpetas compartidas innecesarias entre el host y las máquinas virtuales, y utilizar snapshots antes de ejecutar pruebas que puedan modificar el estado del sistema.

Como medida adicional, el tráfico generado por los escenarios de ataque será monitoreado dentro de la red virtual mediante Suricata, mientras que los eventos recolectados serán enviados

hacia Elastic Stack para su almacenamiento, visualización y análisis. Esta configuración permite observar el comportamiento de los ataques en un entorno seguro, reproducible y controlado, sin afectar infraestructuras externas.

Por lo tanto, la virtualización no solo permite desplegar los componentes técnicos del proyecto, sino que también proporciona las condiciones necesarias para realizar pruebas de seguridad de manera segura, aislada y repetible. Su uso es pertinente para el laboratorio académico, ya que permite validar la detección de eventos, la correlación de alertas y el análisis de métricas de desempeño del SIEM sin requerir infraestructura física dedicada ni exponer activos reales a riesgos innecesarios.

Tabla 10
Consideraciones de virtualización para el laboratorio SIEM

Elemento	Descripción dentro del proyecto
Plataforma de virtualización	Virtual Box Versión 7.2.12
Tipo de entorno	Laboratorio virtualizado local, controlado y replicable.
Máquina atacante	Kali Linux, utilizada para ejecutar pruebas de fuerza bruta, escaneo web, escaneo de puertos y ataques controlados.
Servidor SIEM	Máquina virtual con Elastic Stack, Elastic Security y Suricata para recolección, análisis, visualización y correlación de eventos.
Servidores monitoreados	Servidores web, servicios expuestos y entorno Windows/Active Directory utilizados como objetivos controlados.
Red virtual	Red Segmentación mediante VLANs (VLAN10, VLAN20, VLAN30) gestionadas por pfSense como firewall perimetral.
Aislamiento	Separación del entorno físico y redes productivas para evitar exposición de servicios vulnerables o tráfico ofensivo fuera del laboratorio.
Monitoreo	Suricata inspecciona el tráfico de red generado en el laboratorio y Elastic Stack centraliza los eventos para análisis.
Pertinencia académica	Permite simular una infraestructura real, ejecutar ataques controlados, repetir pruebas y medir la efectividad del SIEM sin afectar sistemas productivos.

2.2. Métricas de evaluación de desempeño del SIEM

La evaluación de desempeño de un SIEM permite determinar qué tan efectiva es la solución para detectar, clasificar y alertar sobre actividades sospechosas o maliciosas dentro de un entorno monitoreado. Para que dicha evaluación sea objetiva, es necesario definir previamente las

métricas que serán utilizadas, así como los criterios que permitirán diferenciar entre una detección correcta, una alerta incorrecta o una actividad maliciosa no detectada.

En el contexto de este proyecto, las métricas de evaluación serán aplicadas sobre los escenarios de ataque controlados ejecutados en el laboratorio, tales como fuerza bruta, escaneo web, escaneo o ataque a puertos de servidores web y ataques dirigidos contra Active Directory. Estas pruebas permitirán comparar los eventos realmente ejecutados durante el laboratorio con las alertas generadas por el SIEM, estableciendo así una base de verdad o ground truth para determinar el desempeño del sistema.

El ground truth corresponde al registro de referencia de las actividades ejecutadas durante cada escenario de prueba. En el presente proyecto, esta información se documenta en la sección 3.8.1, Matriz de referencia de los escenarios de ataque, donde se especifican la máquina de origen, el sistema objetivo, la técnica MITRE ATT&CK asociada, las herramientas o comandos utilizados y el resultado esperado. Las evidencias de ejecución, los eventos detectados y las alertas generadas por Elastic Security y Suricata se presentan en la sección 4.1, Pruebas de concepto, mientras que la clasificación consolidada de los resultados se incluye en la sección 4.2, Análisis de resultados. Esta documentación permite contrastar las actividades ejecutadas con las detecciones obtenidas y determinar si cada escenario corresponde a un verdadero positivo o a un falso negativo.

Un verdadero positivo, o True Positive (TP), se produce cuando el SIEM genera una alerta ante una actividad maliciosa o sospechosa que realmente ocurrió dentro del laboratorio. Por ejemplo, si se ejecuta un ataque de fuerza bruta contra un servicio o cuenta de Active Directory y el SIEM genera una alerta relacionada con múltiples intentos fallidos de autenticación, dicha detección será considerada un verdadero positivo.

Un falso positivo, o False Positive (FP), ocurre cuando el SIEM genera una alerta sobre una actividad que no corresponde a un ataque real o que forma parte del comportamiento normal del entorno. Por ejemplo, si una navegación legítima o una prueba administrativa controlada es

clasificada como ataque web sin que exista una actividad maliciosa, esa alerta será considerada un falso positivo. Esta métrica es importante porque un número elevado de falsos positivos puede generar ruido operativo, fatiga de alertas y pérdida de confianza en el sistema de detección.

Un falso negativo, o False Negative (FN), se presenta cuando ocurre una actividad maliciosa dentro del laboratorio, pero el SIEM no genera ninguna alerta relacionada. Por ejemplo, si se ejecuta un escaneo de puertos contra un servidor web y Suricata o Elastic Security no registran una alerta correspondiente, el caso será considerado un falso negativo. Esta métrica permite identificar brechas de visibilidad, reglas insuficientes o limitaciones en la configuración del sistema.

Un verdadero negativo, o True Negative (TN), se produce cuando una actividad benigna no genera alertas de seguridad. Aunque esta métrica puede ser más difícil de cuantificar en entornos SIEM debido al alto volumen de eventos normales, resulta útil para validar que el sistema no clasifique como maliciosa toda actividad legítima. Por ejemplo, una consulta web normal, una autenticación válida o una conexión esperada que no genere alerta puede considerarse un verdadero negativo dentro del escenario definido.

La tasa de detección representa la capacidad del SIEM para identificar correctamente las actividades maliciosas ejecutadas durante las pruebas. Esta métrica puede calcularse relacionando la cantidad de ataques detectados correctamente con el total de ataques ejecutados en el laboratorio. Una tasa de detección alta indica que el sistema logró identificar la mayoría de los escenarios ofensivos definidos.

La precisión permite medir qué proporción de las alertas generadas por el SIEM corresponden realmente a actividades maliciosas. Esta métrica es importante porque permite evaluar la calidad de las alertas. Un sistema puede generar muchas alertas, pero si una parte considerable corresponde a falsos positivos, su utilidad operativa disminuye.

El recall o sensibilidad permite medir qué proporción de las actividades maliciosas ejecutadas fueron detectadas por el SIEM. Esta métrica es útil para evaluar si el sistema está dejando pasar ataques sin generar alertas. En el contexto del laboratorio, permitirá determinar si los escenarios de fuerza bruta, escaneo web, ataque a puertos de servidores web y ataques al Active Directory fueron detectados adecuadamente.

El tiempo medio de detección, o MTTD por sus siglas en inglés Mean Time To Detect, representa el tiempo promedio transcurrido entre la ejecución de una actividad maliciosa y la generación de una alerta por parte del SIEM. Esta métrica es relevante porque no solo importa que el sistema detecte un ataque, sino también que lo haga de manera oportuna. En este proyecto, el MTTD podrá calcularse comparando la hora documentada de ejecución del ataque en el ground truth con la hora de generación de la alerta en Elastic Security o del evento relevante en Elasticsearch.

La evaluación de desempeño del SIEM propuesto se realizará mediante la comparación entre el ground truth de cada escenario y las alertas generadas por la solución. Para cada prueba se registrará si el ataque fue detectado, qué alerta se generó, qué fuente produjo el evento, qué técnica MITRE ATT&CK se relaciona con la actividad y cuánto tiempo transcurrió hasta la detección. Este enfoque permitirá evaluar la efectividad del SIEM no solo desde una perspectiva funcional, sino también cuantitativa, considerando la calidad, oportunidad y exactitud de las alertas generadas.

CAPITULO 3

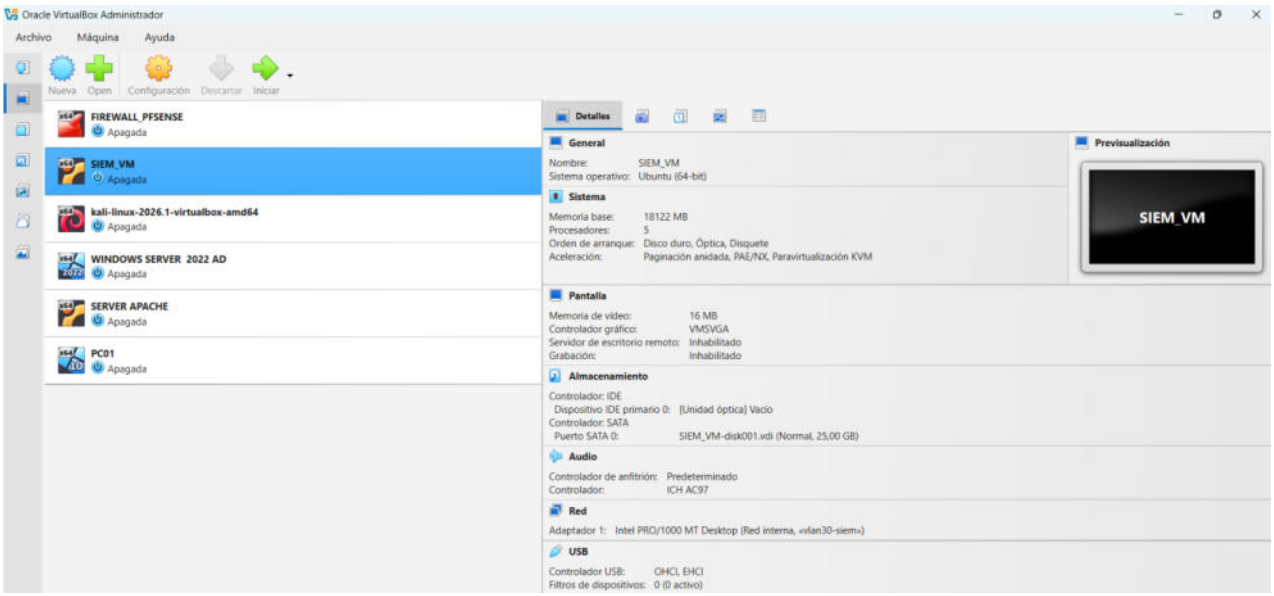
3. DESARROLLO

3.1.Arquitectura de red implementada

Para el desarrollo del laboratorio se integraron los servidores en Virtual Box, siendo base de la infraestructura de red simulado, junto con equipos adicionales que se conectarían

directamente a la red doméstica del router del proveedor de red, siendo estas la máquina atacante Kali Limux y, también, el servidor SIEM quien centralizará los eventos de cada activo de la infraestructura. El router ISP tendrá asignada la red 192.168.1.10/24 y constituye el único acceso del laboratorio a internet. En la **¡Error! No se encuentra el origen de la referencia.**, se observa la configuración del firewall dentro de VirtualBox.

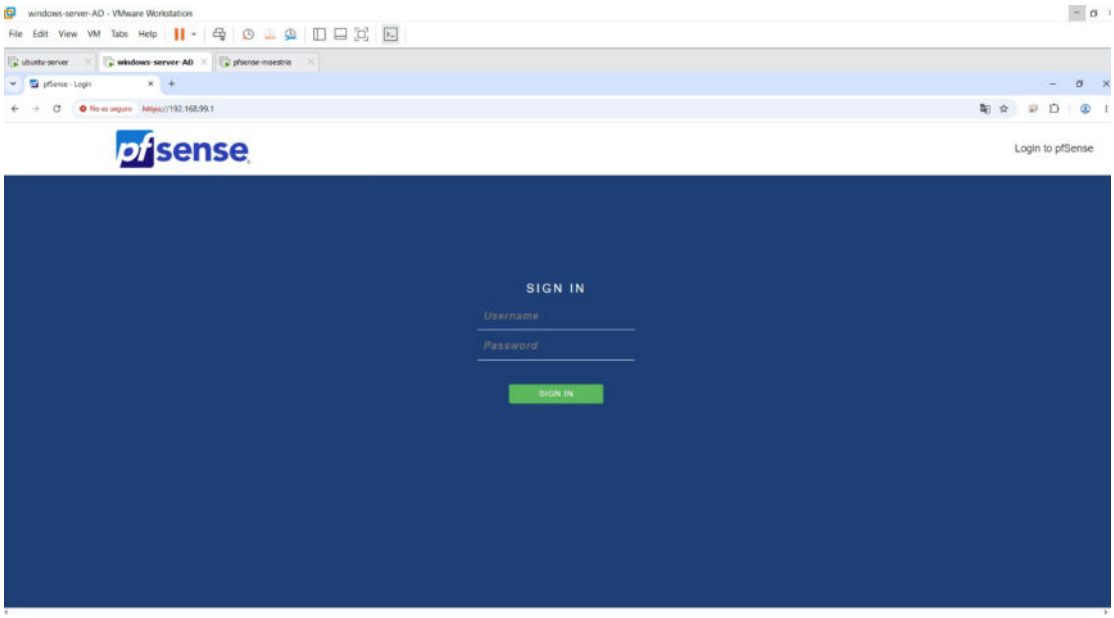
Figura 2
Configuración de máquina virtual PFSENSE en VIRTUAL BOX



Nota: Elaboración propia.

El activo que contiene Kali Linux se conecta en la red externa, el cual lanzará los ataques contra los otros activos (Servidores) y la interfaz WAN de pfSense con IP 192.168.1.9, siendo este la conexión hacia toda la infraestructura interna; lo que conlleva a que el tráfico correspondiente a la máquina atacante pase obligatoriamente por la seguridad perimetral (firewall), antes de establecer conexión a los activos internos, simulando un ataque desde un activo externo tratando de comprometer la infraestructura de red real de una organización.

Figura 3
Interfaz gráfica del Firewall pfSense



Nota: Elaboración propia.

PfSense actúa como el firewall del entorno simulado, adicionalmente, permite el enrutamiento entre las VLANs. La interfaz WAN (192.168.1.5) establecerá una conexión con la red del router mientras que la interfaz LAN (192.168.99.1) actúa como enlace troncal identificándose como VLAN 4095, que, en otras palabras, se establece como el tráfico entre varias VLANs.

Deste ese enlace, se crean las tres VLANs con su respectivo propósito en el entorno:

Tabla 11
LANs de los servidores

VLAN	Nombre VLAN	Interfaz de red	Activos
10	SERVIDORES_VLAN10	192.168.10.0/24	Directorio activo Ubuntu web Apache, WordPress
20	USUARIOS_VLAN20	192.168.20.0/24	Usuarios
30	SIEM_VLAN30	192.168.30.0/24	Servidor Siem

- Servidores (VLAN 10): En esta VLAN se encuentran los servidores victimas del equipo atacante, pertenecientes a la interfaz de red 192.168.10.0/24. En este segmento se encuentra el Directorio activo y el servidor web Ubuntu con Apache,

WordPress.

- Usuarios (VLAN 20): En esta VLAN se encuentran los equipos de usuario que serán usados para establecer movimiento lateral, con uso de credenciales válidas de usuarios correspondientes al dominio del controlados, perteneciente al segmento de red 192.168.20.0/24.

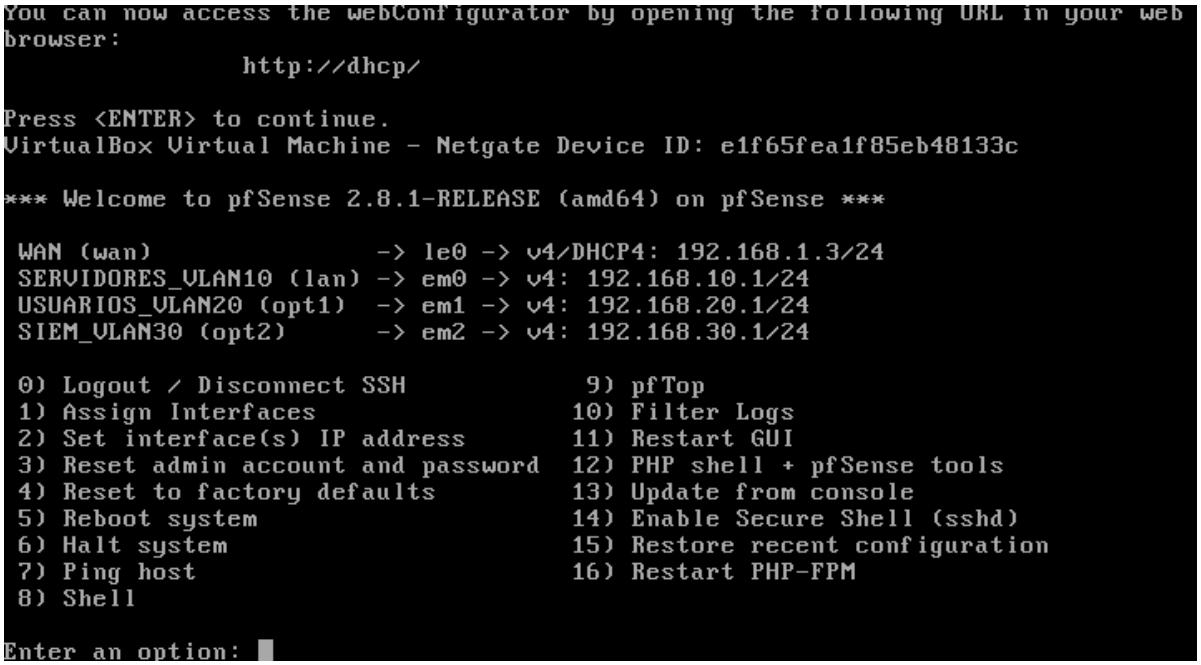
El SIEM se posiciona en la interfaz de red 192.168.30.0/24 y es el encargado de recibir, normalizar, correlacionar, almacenar y mostrar todos los eventos o actividad de seguridad que se generan en el entorno simulado.

Con esta estructura de red, se mantiene la separación de servidores víctimas, equipos de usuarios y servidor de monitoreo, dando como resultado que el tráfico pase por pfSense considerando las reglas definidas. La configuración de reglas está basada en que tanto el atacante como los usuarios puedan ser visibles para el SIEM, quien permitirá la centralización de aquellos eventos sospechosos dentro del entorno controlado.

3.2 Configuración de la segmentación de red (PFSENSE Y VLANS)

Una vez definidas las tres VLANs sobre el enlace troncal de pfSense, el siguiente paso fue configurar las interfaces correspondientes y las reglas de firewall que controlan el tráfico entre ellas. Esta configuración es la que realmente le da sentido a la segmentación, porque sin reglas claras, tener VLANs separadas no aportaría ningún control de seguridad real.

Figura 4
Interfaces configurados en pfSense.



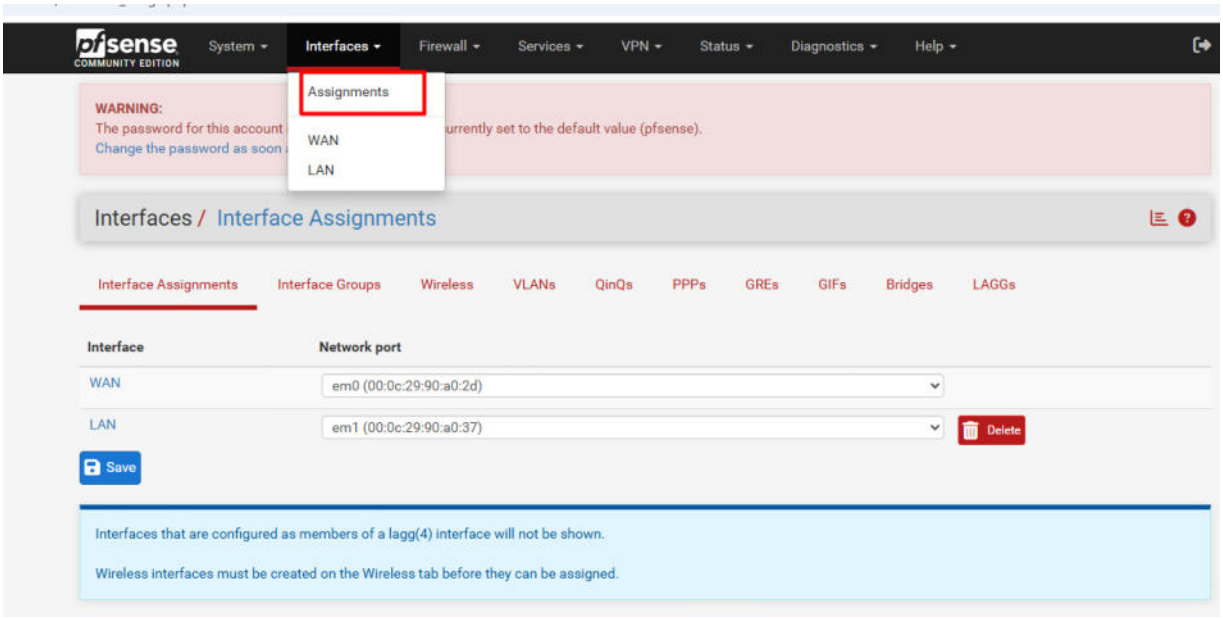
Nota: Elaboración propia.

Tabla 12
Configuración de interfaces en pfSense, VLAN , IP

Interfaz	VLAN	IP GATEWAY	RED
Em0	10	192.168.10.1	192.168.10.0/24
Em1	20	192.168.20.1	192.168.20.0/24
Em2	30	192.168.30.1	192.168.30.0/24

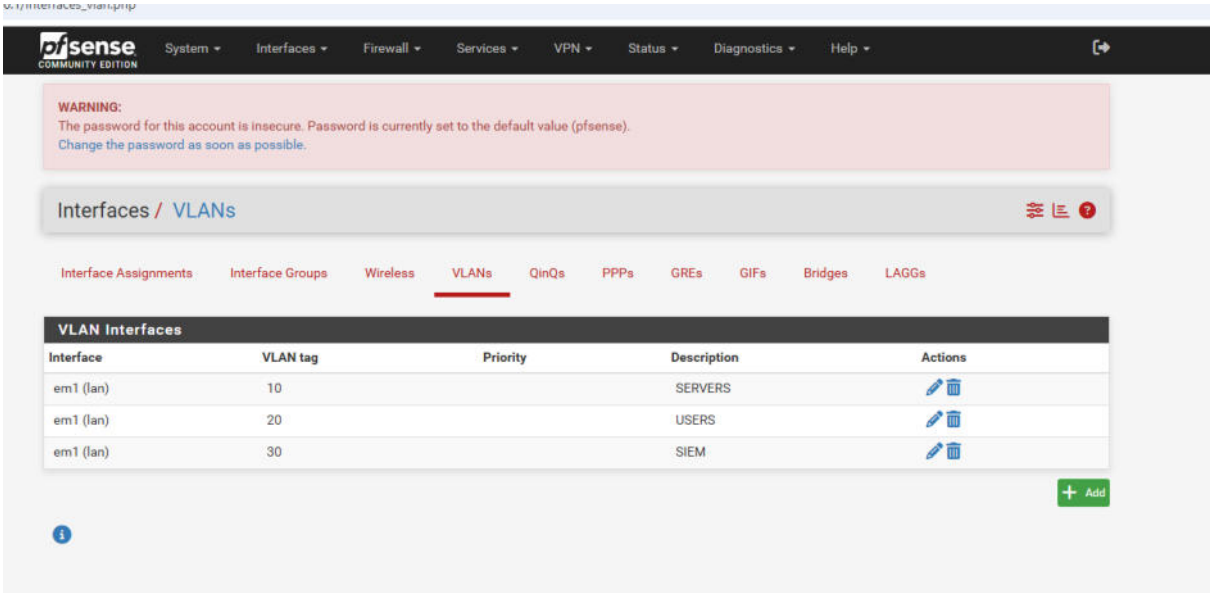
Cada una de estas interfaces se configuró con su propio servidor DHCP cuando fue necesario, aunque en la práctica las máquinas críticas del laboratorio (Windows Server, Ubuntu Web, PC cliente y SIEM) se configuraron con IP estática para mantener consistencia en los logs y en las reglas de firewall a lo largo de todas las pruebas.

Figura 5
Interfaces LAN Y WAN configurados en el Firewall pfSense



Nota: Elaboración propia.

Figura 6
Configuración de VLAN en pfSense

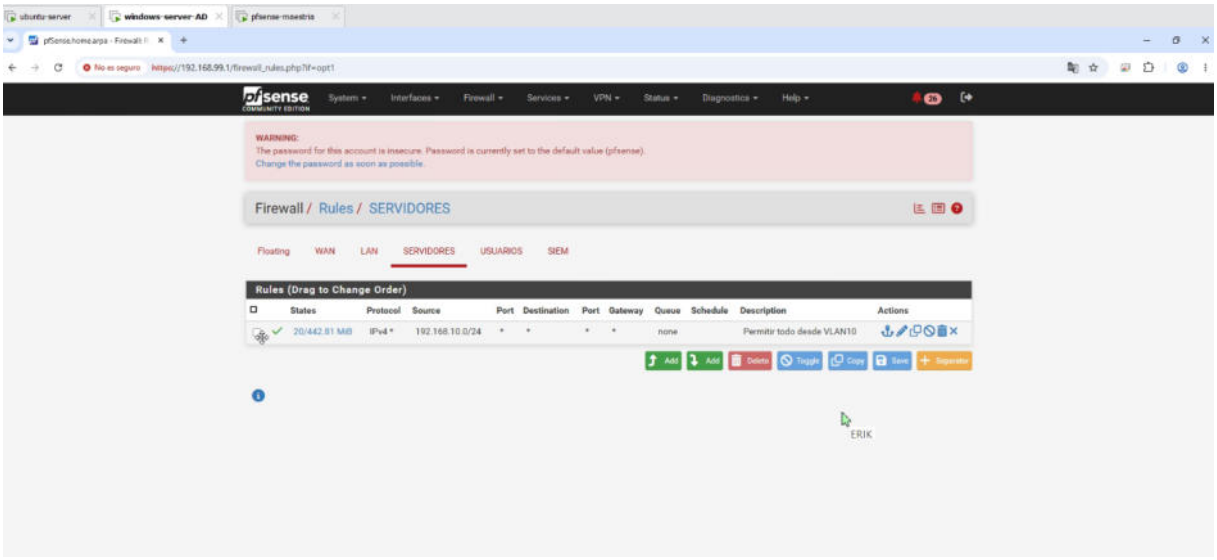


Nota: Elaboración propia.

Lógica de las reglas de firewall. El criterio general que se siguió al definir las reglas fue simple: el atacante debe poder llegar a los servidores y a los equipos de usuario, porque ahí es donde se ejecutan los escenarios de prueba, pero ni el atacante ni los equipos de usuario deben

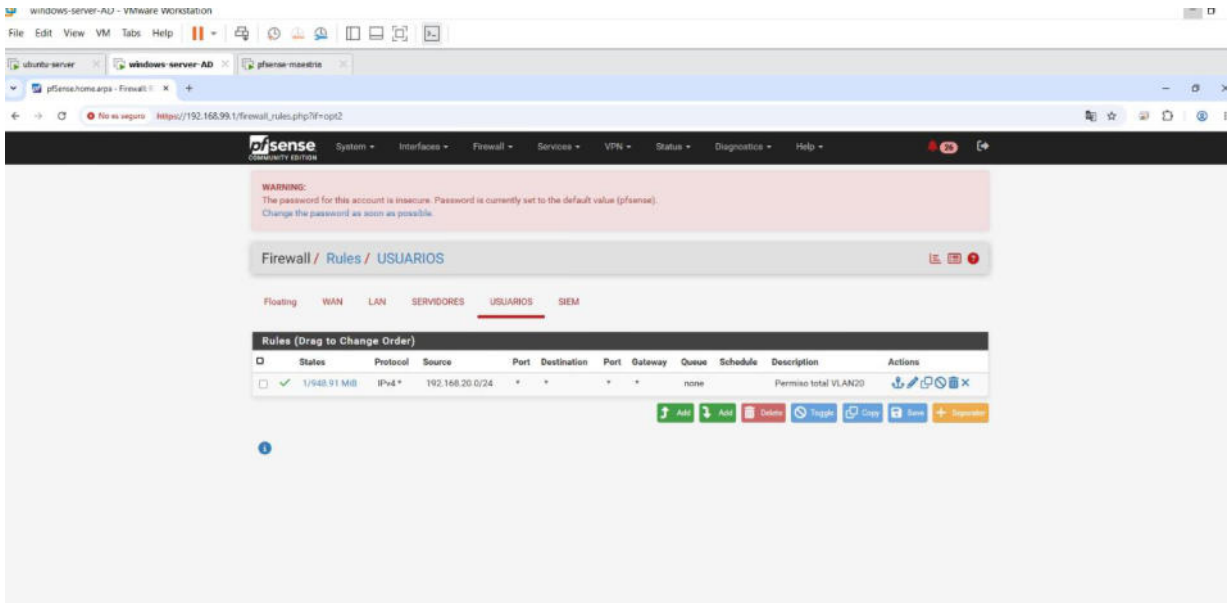
tener visibilidad directa sobre el SIEM, ya que en un escenario real un atacante tampoco vería expuesta la plataforma de monitoreo de la organización que está comprometiendo.

Figura 7
Configuración de reglas de conexión



Nota: Elaboración propia.

Figura 8
Configuración de reglas para VLAN 20

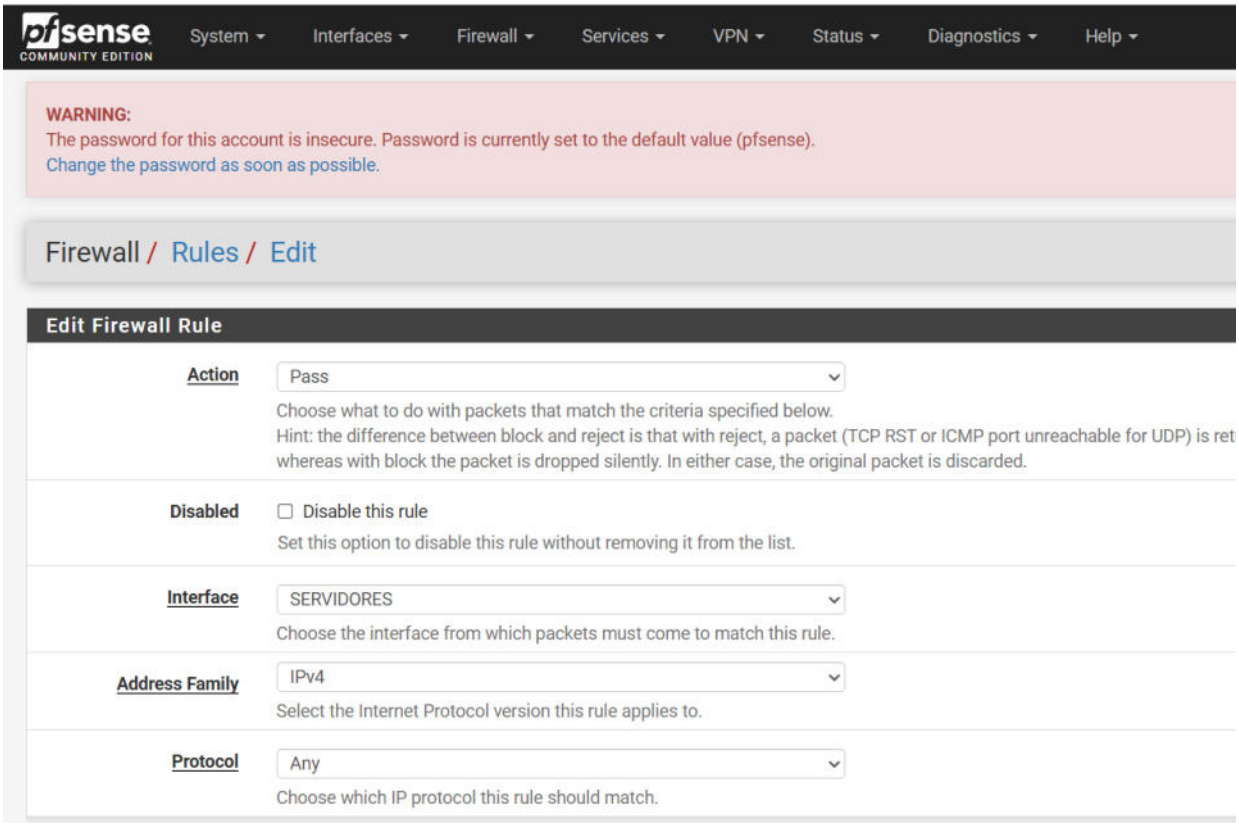


Nota: Elaboración propia.

Es importante notar que la regla que permite tráfico de VLAN10 hacia VLAN30 no es para que los servidores naveguen libremente hacia el SIEM, sino específicamente para que el tráfico

del agente Filebeat (puerto 9200) y, en el caso del servidor Ubuntu Web, el tráfico correspondiente a los logs de Apache, puedan llegar sin restricciones hasta el servidor central.

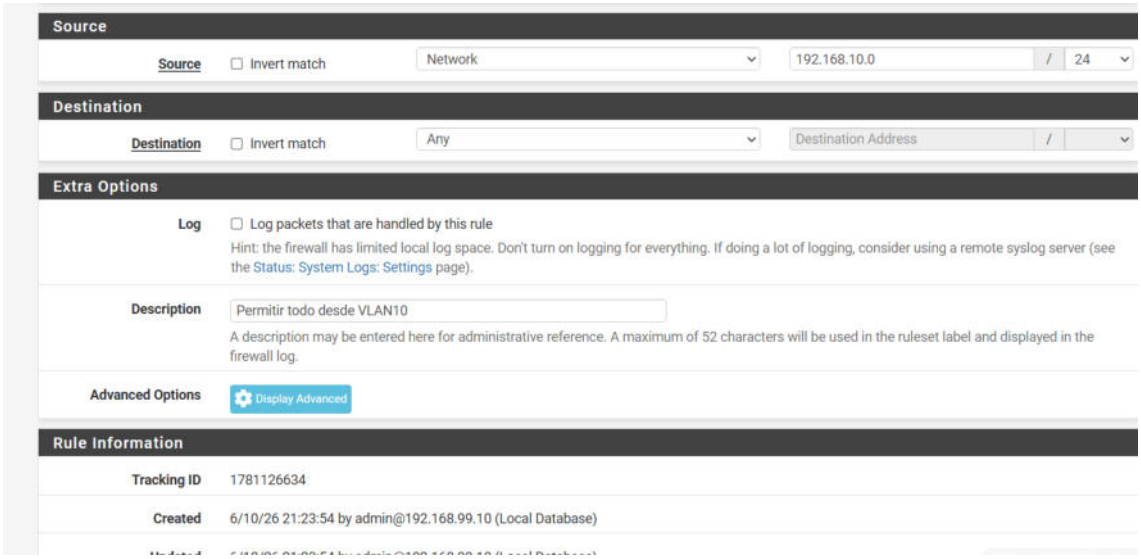
Figura 9
Configuración de reglas para la VLAN 10



Nota: Elaboración propia.

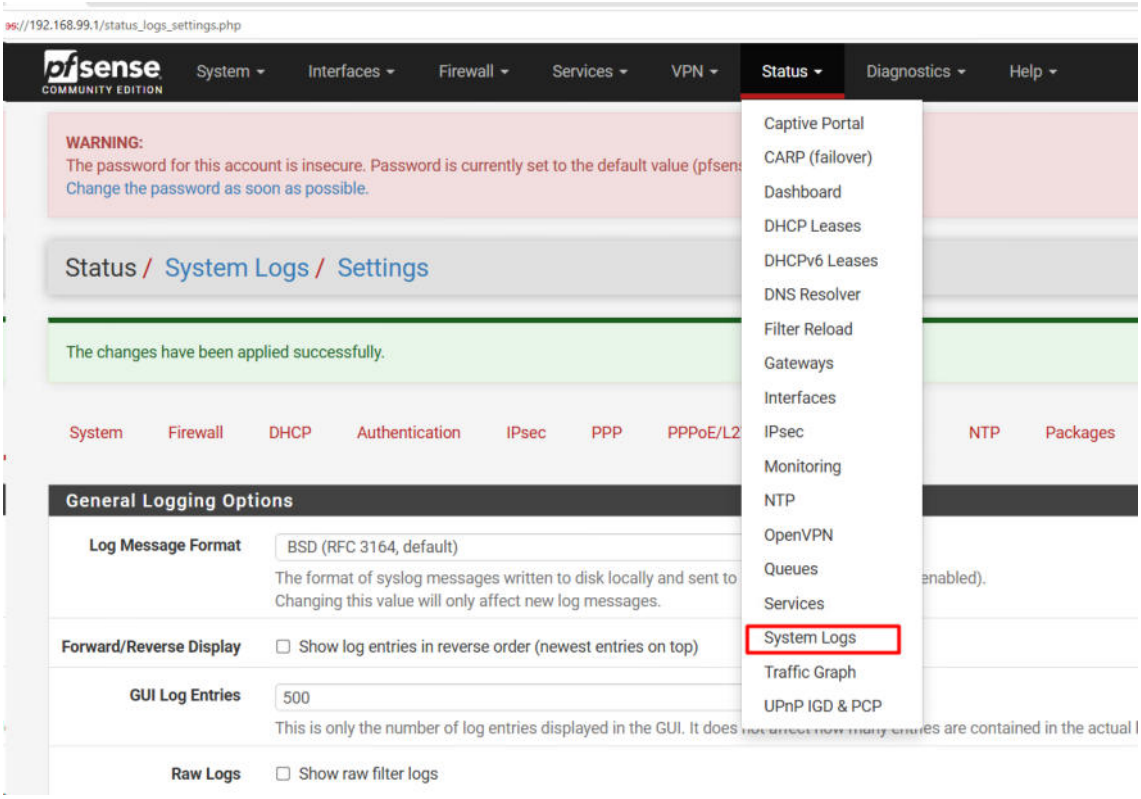
Registro de tráfico en pfsense: Además de filtrar el tráfico entre VLANs, pfSense se configuró para registrar los eventos de firewall y reenviarlos hacia el SIEM mediante Syslog, de forma que las decisiones de bloqueo o permiso tomadas por el firewall también queden disponibles como fuente de evidencia dentro de Elasticsearch. Esto resulta particularmente útil para los escenarios donde el atacante intenta alcanzar el SIEM directamente, ya que esos intentos bloqueados quedan registrados y pueden complementar el análisis de los resultados en el Capítulo 4.

Figura 10
Configuración inicial de registro de tráfico en pfsense



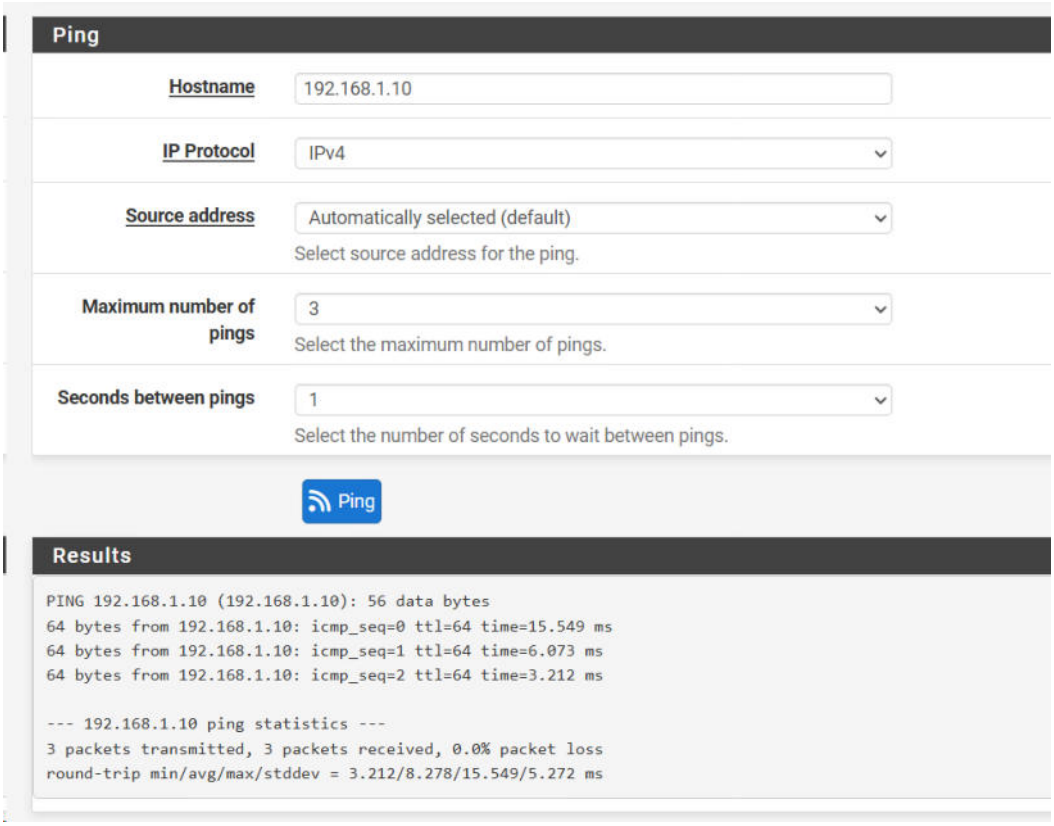
Nota: Elaboración propia.

Figura 11.
Configuración de Logs en pfsense.



Nota: Elaboración propia.

Figura 12
Verificación de conectividad al SERVIDOR SIEM



Nota: Elaboración propia.

3.3.Despliegue de servidor SIEM

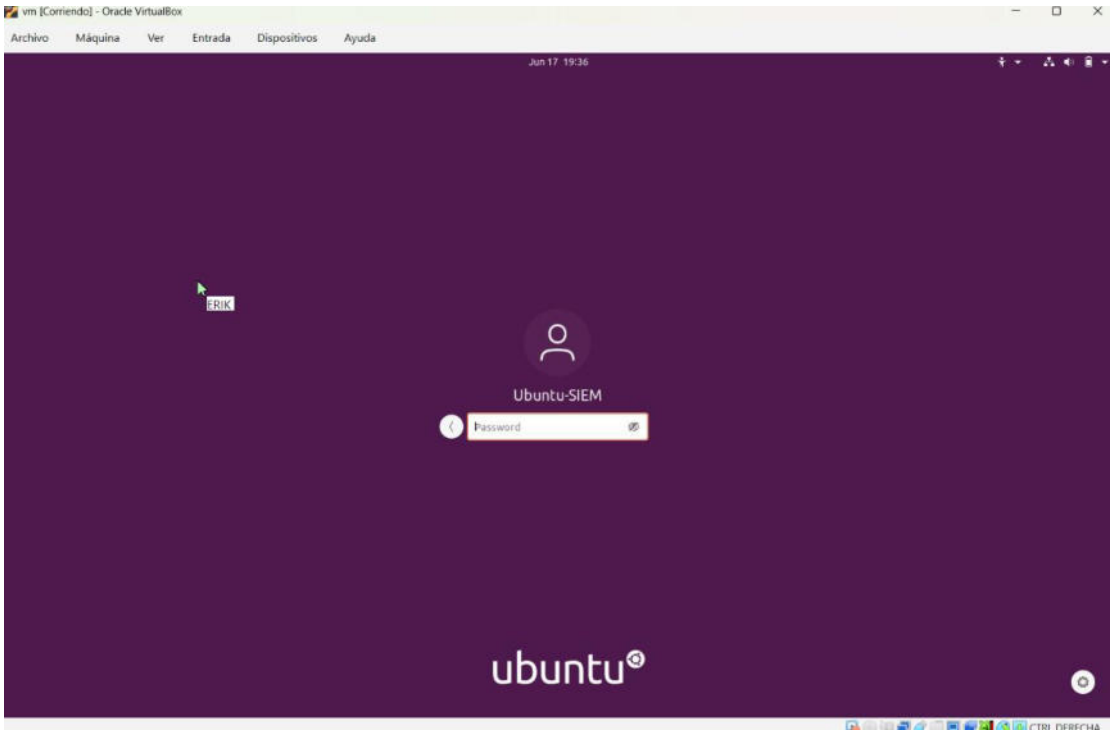
Una vez establecidas la segmentación de VLANs y la arquitectura de la red, se desplegó el servidor SIEM con dirección IP 192.168.30.100, el cual tiene sistema operativo Ubuntu Server 24.04.3 LTS, posteriormente se instaló el stack tecnológico para la detección de los eventos correspondientes, en este sentido los componentes instalados fueron:

- Elasticsearch
- Kibana
- Logstash
- Filebeat
- Suricata

Figura 13
Capacidades del SIEM

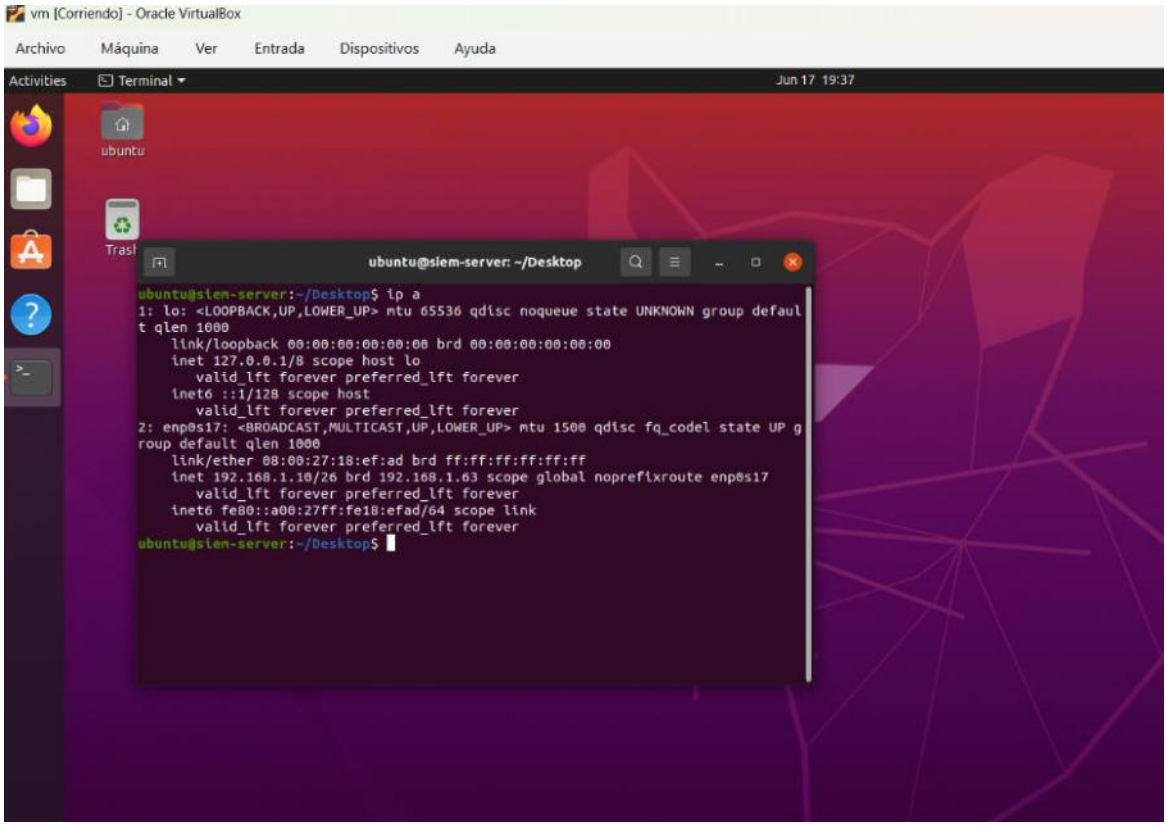
Nota: Elaboración propia.

Figura 14
Interfaz de usuario del servidor SIEM



Nota: Elaboración propia.

Figura 15
Interfaz de red de servidor SIEM: IP: 192.168.30.100



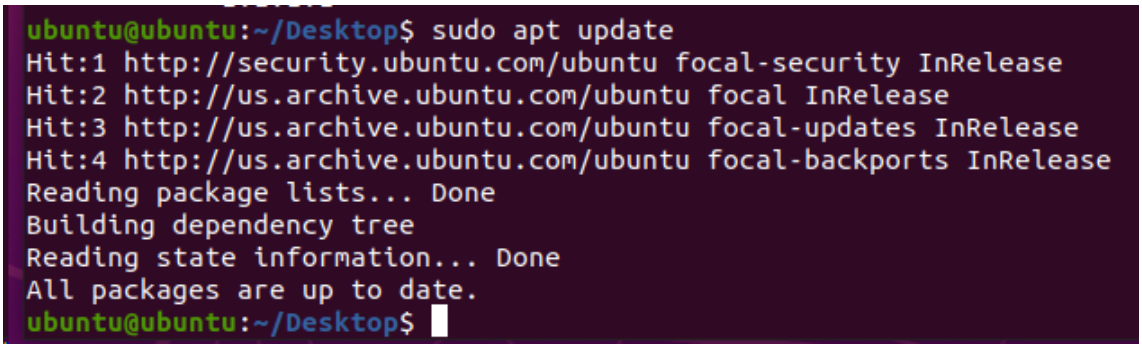
Nota: Elaboración propia.

Instalación de ElasticSearch. Elasticsearch fue el primer componente instalado, con versión 8.19.19, descargado del repositorio oficial de Elastic. Previamente, se configuró Java 17 (OpenJDK) como requerimiento necesario para una configuración exitosa en el entorno.

Posteriormente, se requiere ajustar la configuración del archivo: */etc/elasticsearch/elasticsearch.yml*, con las siguientes especficaciones, adaptados a las necesidades de un entorno de laboratorio de único:

cluster.name: siem-lab
node.name: siem-node-1
network.host: 0.0.0.0
http.port: 9200
discovery.type: single-node
xpack.security.enabled: false

Figura 16
Actualización de dependencias



Nota: Elaboración propia.

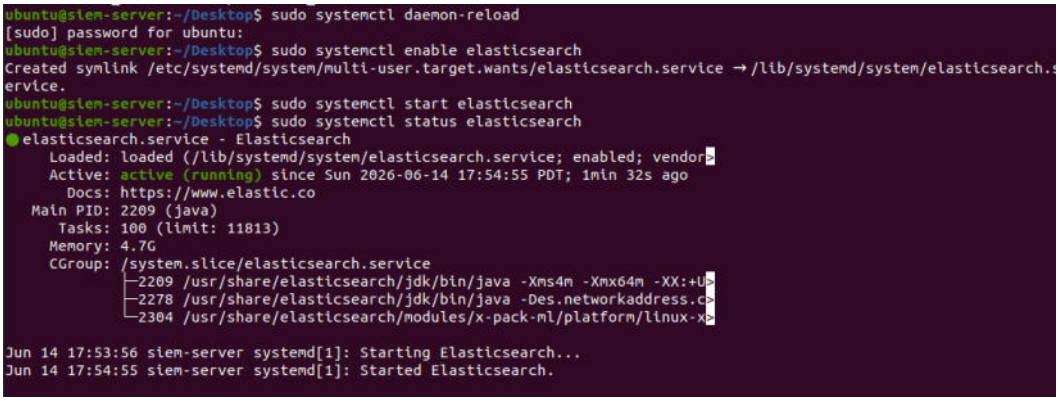
La desactivación temporal de los mecanismos de seguridad de Elasticsearch mediante el parámetro xpack.security.enabled: false se realizó exclusivamente con fines de validación funcional dentro del entorno de laboratorio. La infraestructura se encontraba separada de los sistemas de producción y segmentada mediante las redes virtuales administradas por pfSense; sin embargo, los servicios del servidor SIEM permanecieron accesibles desde determinados segmentos internos del laboratorio para permitir la comunicación entre los componentes y la ejecución de los escenarios de prueba.

Adicionalmente, Elasticsearch fue configurado con el parámetro network.host: 0.0.0.0 y el puerto HTTP 9200, lo que permitió que el servicio escuchara en las interfaces de red disponibles del servidor. Esta configuración facilitó la ingesta y consulta de eventos, pero también permitió que el puerto fuera identificado desde la máquina atacante durante las pruebas de escaneo. Por esta razón, la configuración implementada debe considerarse una condición controlada del laboratorio y no una práctica recomendada para entornos de producción.

Después de aplicar la configuración, se verificó el funcionamiento de Elasticsearch mediante una consulta al puerto 9200, confirmando que el servicio se encontraba activo y disponible para las funciones de almacenamiento, indexación y consulta de eventos. Posteriormente, durante el escenario de escaneo de red, se identificaron como accesibles los

puertos 22/TCP, 5044/TCP, 5601/TCP y 9200/TCP, correspondientes a servicios habilitados dentro del laboratorio para el despliegue y evaluación del SIEM..

Figura 17
Estado de Elasticsearch



Nota: Elaboración propia.

Instalación de kibana. Este componente requiere, luego de instalarse, configurar el archivo /etc/kibana/kibana.yml de la siguiente manera:

Figura 18
Configuración en kibana.

```
server.port: 5601
server.host: 0.0.0.0
elasticsearch.hosts: ["http://localhost:9200"]
```

Nota: Elaboración propia.

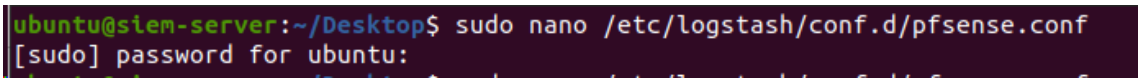
Después de iniciar el servicio, se accedió a la interfaz web mediante el navegador en la dirección http://192.168.30.100:5601, verificando que la plataforma estaba lista para la futura configuración de los Data Views, paneles y normas de detección de Elastic Security.

Figura 19
Validación de estado de kibana

Nota: Elaboración propia.

Instalación y configuración de Logstash. Logstash fue instalado para desempeñar la función de gestionar y estandarizar eventos en la estructura de SIEM. Con este fin, se establecieron pipelines específicos basados en la categoría de datos recibidos, lo que facilitó la diferenciación del manejo de logs de autenticación, registros de sitios web y eventos syslog que llegan desde el cortafuegos.

Figura 20
Ruta de configuración en pfSense para logsdtash



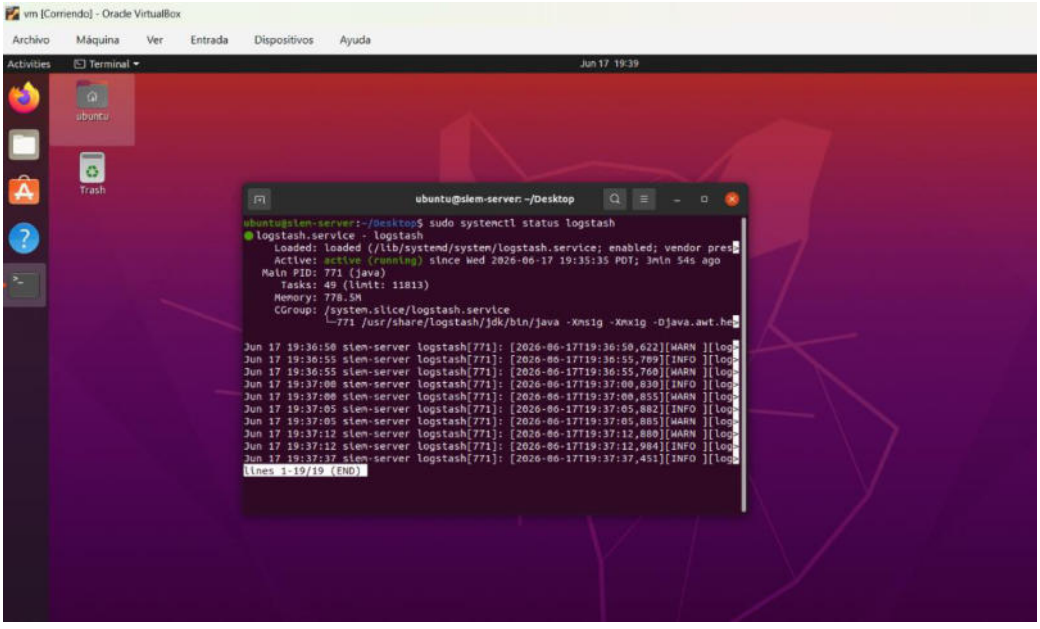
Nota: Elaboración propia.

Figura 21
Pipelines.

Pipeline	Puerto	Fuente de datos
01-beats.conf	5044/TCP	Logs de autenticación (auth.log de Linux, EventID 4624/4625 de Windows)
02-apache.conf	5045/TCP	Logs del servidor web Apache (detección de patrones SQLi)
03-syslog.conf	5140/UDP	Tráfico Syslog proveniente de pfSense

Nota: Elaboración propia.

Figura 22
Validación del servicio de Logstash.

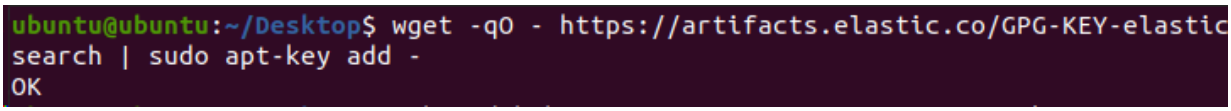


Nota: Elaboración propia.

De manera similar, el pipeline 02-apache. conf, que opera en el puerto 5045/TCP, se diseñó para manejar logros del servidor web Apache. Este incluye filtros que ayudan a identificar patrones asociados a posibles intentos de inyección SQL y vulnerabilidades en servicios web, alineándose con la técnica T1190. Por último, el pipeline 03-syslog. conf, que utiliza el puerto 5140/UDP, se dedicó a recibir los eventos syslog generados por pfSense.

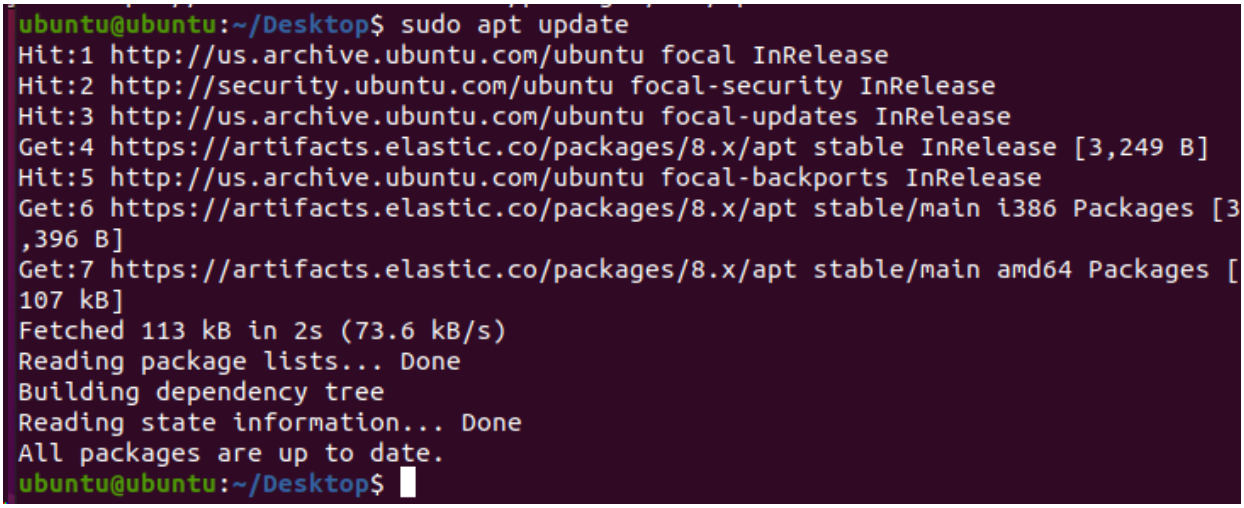
La configuración de los pipelines fue verificada utilizando el comando de comprobación de Logstash, lo que aseguró que no había errores de sintaxis en los archivos antes de poner en marcha el servicio. Luego, se confirmó que Logstash estaba funcionando y operativo, preparado para procesar eventos y enviarlos a Elasticsearch.

Figura 23
Verificación de artefacto



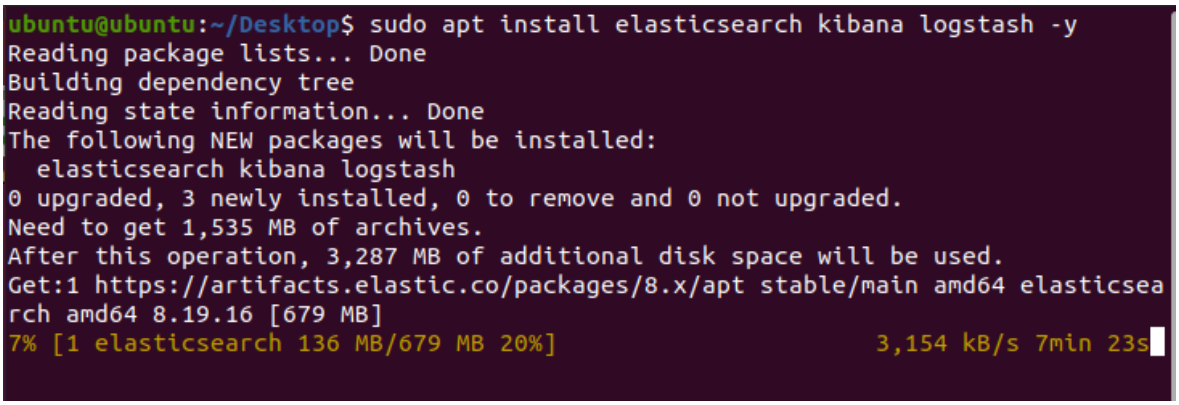
Nota: Elaboración propia.

Figura 24
Actualización del servidor.



Nota: Elaboración propia.

Figura 25
Instalación de componentes.



Nota: Elaboración propia.

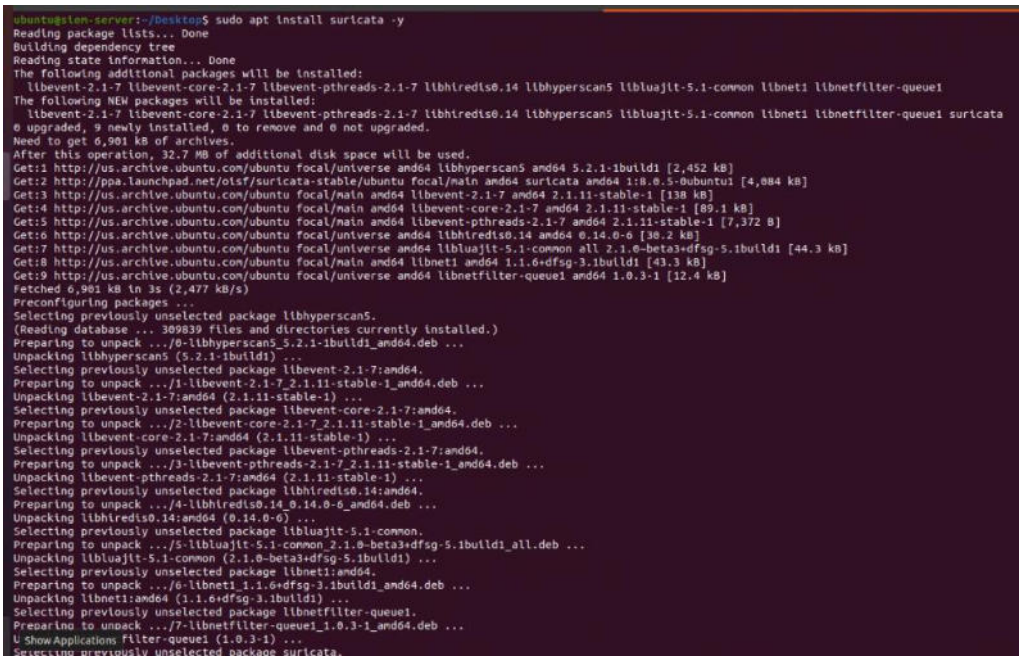
El Instalación y configuración de Suricata. Suricata se instaló en el servidor SIEM como sensor de detección de intrusiones de red, con el propósito de analizar el tráfico capturado mediante la interfaz de monitoreo y generar eventos de seguridad para su posterior procesamiento y análisis en Elastic Security. Para esta configuración se seleccionó la interfaz enp0s3 como punto de captura.

La variable HOME_NET se configuró con los segmentos internos definidos en la arquitectura del laboratorio: 192.168.10.0/24, correspondiente a la VLAN de servidores; 192.168.20.0/24, correspondiente a la VLAN de usuarios; y 192.168.30.0/24, correspondiente a la red de monitoreo donde se encuentra el servidor SIEM. La configuración aplicada fue la siguiente:

HOME_NET: "[192.168.10.0/24,192.168.20.0/24,192.168.30.0/24]"

Esta definición permite que Suricata clasifique los eventos relacionados con estos segmentos como tráfico perteneciente a las redes internas protegidas. Sin embargo, la inclusión de una red dentro de HOME_NET no garantiza por sí sola su supervisión; la detección depende de que el tráfico de las VLAN llegue efectivamente a la interfaz de captura enp0s3, de acuerdo con la topología y las reglas de enrutamiento o redirección configuradas en pfSense.

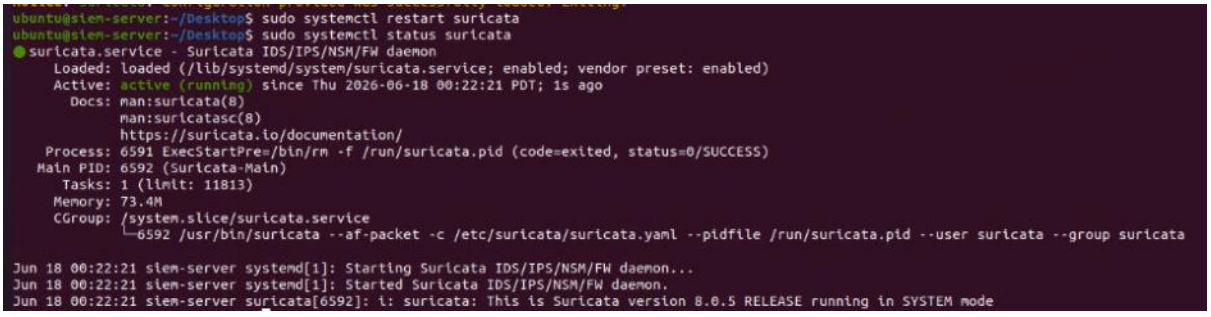
Figura 26
Instalación de Suricata en SIEM.



Nota: Elaboración propia.

Después, se llevó a cabo el proceso de actualización de reglas utilizando la herramienta suricata-update, lo que facilitó la descarga y configuración del conjunto de firmas de detección requeridas por el motor IDS. Como resultado de este procedimiento, se logró acceder a 66. 040 reglas disponibles, de las cuales 50. 119 fueron activadas tras la aplicación del filtrado automático. Con esta configuración, Suricata funcionó en modo IDS/NSM, generando eventos en formato EVE JSON en el archivo eve. json, sin llevar a cabo bloqueos o alteraciones activas sobre el tráfico. Esta configuración concuerda con los objetivos del proyecto, que se centra en la detección, análisis y correlación de eventos de seguridad dentro del SIEM.

Figura 27
Validación del servicio de suricata.



Nota: Elaboración propia.

Instalación y configuración de Filebeat

Adicionalmente, se instaló Filebeat en el servidor SIEM con la finalidad de recolectar los archivos de registro generados por Suricata, principalmente eve.json y suricata.log, y enviarlos hacia Elasticsearch para su almacenamiento e indexación. A partir de esta integración, se definieron índices específicos como suricata-alerts-* y suricata-logs-*, permitiendo separar los eventos de alerta de los registros operativos del sensor.

Filebeat será utilizado también como agente de recolección en las demás máquinas monitoreadas dentro de la infraestructura del laboratorio, tales como el servidor Windows Server, el servidor Ubuntu Web y el equipo cliente. En cada caso, el agente será configurado de acuerdo con la fuente de datos correspondiente y enviará los eventos hacia el servidor SIEM, utilizando el puerto 5044/TCP cuando la recepción se realice a través de Logstash mediante el input Beats, ubicado en la dirección 192.168.30.100.

Verificación del despliegue. Para validar que Suricata se encontraba operativo dentro del servidor SIEM, se revisó la generación de eventos en formato EVE JSON dentro del archivo eve.json. En la evidencia se observan registros estructurados generados por el motor de Suricata, incluyendo información estadística del sensor, contadores de protocolos, métricas de decodificación de paquetes, flujos de red y estado interno del motor IDS/NSM.

Esta verificación permitió confirmar que Suricata se encontraba activo y generando eventos de red en tiempo real dentro del entorno de laboratorio. Asimismo, permitió validar la primera etapa de la cadena de ingesta, correspondiente a la captura y generación de logs por parte del sensor, antes de continuar con su recolección, indexación y visualización dentro de Kibana mediante el Data View correspondiente a los logs de Suricata.

Figura 28
Eventos de Suricata en formato eve.json


{"vlan_qinq":0,"vlan_qinqinq":0,"vxlan":0,"vntag":0,"ieee8021ah":0,"teredo":0,"ipv4_in_ipv4":0,"ipv6_in_ipv4":0,"ipv4_in_ipv6":0,"ipv6_in_ipv6":0,"mpls":0,"avg_pkt_size":391,"max_pkt_size":1514,"max_mac_addrs_src":0,"max_mac_addrs_dst":0,"erspan":0,"nsh":0,"event":{"afpacket":{"trunc_pkt":0},"ipv4":{"pkt_too_small":0,"hlen_too_small":0,"iplen_smaller_than_hlen":0,"trunc_pkt":0,"opt_invalid":0,"opt_invalid_len":0,"opt_malformed":0,"opt_pad_required":5,"opt_eol_required":0,"opt_duplicate":0,"opt_unknown":0,"wrong_ip_version":0,"icmpv6":0,"frag_pkt_too_large":0,"frag_overlap":0,"frag_ignored":0},"icmpv4":{"pkt_too_small":0,"unknown_type":0,"unknown_code":0,"ipv4_trunc_pkt":0,"ipv4_unknown_ver":0},"icmpv6":{"unknown_type":0,"unknown_code":0,"pkt_too_small":0,"ipv6_unknown_version":0,"ipv6_trunc_pkt":0,"mld_message_with_invalid_hl":0,"unassigned_type":0,"experimentation_type":0},"ipv6":{"pkt_too_small":0,"trunc_pkt":0,"trunc_exthdr":0,"exthdr_dupl_fh":0,"exthdr_useless_fh":0,"exthdr_dupl_rh":0,"exthdr_dupl_hh":0,"exthdr_dupl_dh":0,"exthdr_dupl_ah":0,"exthdr_dupl_eh":0,"exthdr_invalid_optlen":0,"wrong_ip_version":0,"exthdr_ah_res_not_null":0,"hopopts_unknown_opt":0,"hopopts_only_padding":0,"dstopts_unknown_opt":0,"dstopts_only_padding":0,"rh_type_0":0,"zero_len_padn":0,"fh_non_zero_reserved_field":0,"data_after_none_header":0,"unknown_next_header":0,"icmpv4":0,"frag_pkt_too_large":0,"frag_overlap":0,"frag_invalid_length":0,"frag_ignored":0,"ipv4_in_ipv6_too_small":0,"ipv4_in_ipv6_wrong_version":0,"ipv6_in_ipv6_too_small":0,"ipv6_in_ipv6_wrong_version":0},"tcp":{"pkt_too_small":0,"hlen_too_small":0,"invalid_optlen":0,"opt_invalid_len":0,"opt_duplicate":0},"udp":{"pkt_too_small":0,"hlen_too_small":0,"hlen_invalid":0,"len_invalid":0},"sll":{"pkt_too_small":0},"sll2":{"pkt_too_small":0},"ethernet":{"pkt_too_small":0,"unknown_ethertype":0},"ppp":{"pkt_too_small":0,"vju_pkt_too_small":0,"ip4_pkt_too_small":0,"ip6_pkt_too_small":0,"wrong_type":0,"unsup_proto":0},"pppoe":{"pkt_too_small":0,"wrong_code":0,"malformed_tags":0},"gre":{"pkt_too_small":0,"wrong_version":0,"version0_recur":0,"version0_flags":0,"version0_hdr_too_big":0,"version0_malformed_sre_hdr":0,"version1_chksum":0,"version1_route":0,"version1_ssr":0,"version1_recur":0,"version1_flags":0,"version1_no_key":0,"version1_wrong_protocol":0,"version1_malformed_sre_hdr":0,"version1_hdr_too_big":0},"vlan":{"header_too_small":0,"unknown_type":0,"too_many_layers":0},"ieee8021ah":{"header_too_small":0},"vntag":{"header_too_small":0,"unknown_type":0},"ipraw":{"invalid_ip_version":0},"ltnull":{"pkt_too_small":0,"unsupported_type":0},"sctp":{"pkt_too_small":0},"esp":{"pkt_too_small":0},"mpls":{"header_too_small":0,"pkt_too_small":0,"bad_label_router_alert":0,"bad_label_implicit_null":0,"bad_label_reserved":0,"unknown_payload_type":0},"vxlan":{"unknown_payload_type":0},"geneve":{"unknown_payload_type":0},"erspan":{"header_too_small":0,"unsupported_version":0,"too_many_vlan_layers":0},"dce":{"pkt_too_small":0},"chdlc":{"pkt_too_small":0},"nsh":{"header_too_small":0,"unsupported_version":0,"bad_header_length":0,"reserved_type":0,"unsupported_type":0,"unknown_payload":0}},"too_many_layers":0},"tcp":{"syn":3,"synack":3,"rst":2,"urg":0,"active_sessions":3,"sessions":3,"ssn_memcap_drop":0,"ssn_from_cache":0,"ssn_from_pool":3,"pseudo":0,"invalid_checksum":0,"midstream_pickups":0,"pkt_on_wrong_thread":0,"ack_unseen_data":0,"segment_memcap_drop":0,"segment_from_cache":0,"segment_from_pool":35,"stream_depth_reached":0,"reassembly_gap":0,"overlap":0,"overlap_diff_data":0,"insert_data_normal_fail":0,"insert_data_overlap_fail":0,"urgent_oob_data":0,"memuse":2490368,"reassembly_memuse":4874240},"total":14,"active":11,"tcp":3,"udp":11,"icmpv4":0,"icmpv6":0,"tcp_reuse":0,"elephant":0,"get_used":0,"get_used_eval":0,"get_used_eval_reject":0,"get_used_eval_busy":0,"get_used_failed":0,"wrk":{"spare_sync_avg":100,"spare_sync":4,"spare_sync_incomplete":0,"spare_sync_empty":0,"flows_evicted_needs_work":0,"flows_evicted_pkt_inject":0,"flows_evicted":0,"flows_injected":0,"flows_injected_max":0},"end":{"state":{"new":3,"established":0,"closed":0,"local_bypassed":0,"capture_bypassed":0},"tcp_state":{"none":0,"syn_sent":0,"syn_recv":0,"established":0,"fin_wait1":0,"fin_wait2":0,"time_wait":0,"last_ack":0,"close_wait":0,"closing":0,"closed":0},"tcp_liberal":0},"mgr":{"full_hash_pass":5,"rows_per_sec":6553,"rows_maxlen":1,"flows_checked":17,"flows_notimeout":14,"flows_timeout":3,"flows_evicted":3,"flows_evicted_needs_work":0},"spare":9603,"emerg_mode_entered":0,"emerg_mode_over":0,"recycler":{"recycled":3,"queue_avg":0,"queue_max":1},"memuse":7154304},"defrag":{"ipv4":{"fragments":0,"reassembled":0},"ipv6":{"fragments":0,"reassembled":0},"max_trackers_reached":0,"max_frags_reached":0,"tracker_soft_reuse":0,"tracker_hard_reuse":0,"wrk":{"tracker_timeout":0},"memuse":33554432},"flow_bypassed":{"local_pkts":0,"local_bytes":0,"local_capture_pkts":0,"local_capture_bytes":0,"closed":0,"pkts":0,"bytes":0},"detect":{"engines":[{"id":0,"last_reload":"2026-06-18T08:22:36.044941-0700","rules_loaded":50810,"rules_failed":0,"rules_skipped":0}],"alert":0,"alert_queue_overflow":0,"alerts_suppressed":0,"lua":{"errors":0,"blocked_function_errors":0,"instruction_limit_errors":0,"memory_limit_errors":0}},"app_layer":{"flow":{"failed_tcp":0,"http":0,"ftp":0,"smtp":0,"tls":3,"ssh":0,"imap":0,"smb":0,"dcerpc_tcp":0,"dns_tcp":0,"nfs_tcp":0,"ntp":0,"ftp-data":0,"tftp":0,"ike":0,"krb5_tcp":0,"quic":0,"dhcp":0,"sip_tcp":0,"rfb":0,"mqtt":0,"telnet":0,"websocket":0,"ldap_tcp":0,"doh2":0,"rdp":0,"http2":0,"bittorrent-dht":0,"pop3":0,"mdns":2,"snmp":0,"failed_udp":2,"dcerpc_udp":0,"dns_udp":0,"nfs_udp":0,"krb5_udp":0,"sip_udp":7,"ldap_udp":0},"error":{"failed_tcp":{"gap":0},"http":{"gap":0,"alloc":0,"parser":0,"internal":0},"ftp":{"gap":0,"alloc":0,"parser":0,"internal":0},"smtp":{"gap":0,"alloc":0,"parser":0,"internal":0},"tls":{"gap":0,"alloc":0,"parser":0,"internal":0},"ssh":{"gap":0,"alloc":0,"parser":0,"internal":0},"smb":{"gap":0,"alloc":0,"parser":0,"internal":0},"dcerpc_tcp":{"gap":0,"alloc":0,"parser":0,"internal":0},"dns_tcp":{"gap":0,"alloc":0,"parser":0,"internal":0},"nfs_tcp":{"gap":0,"alloc":0,"parser":0,"internal":0},"ftp-data":{"gap":0,"alloc":0,"parser":0,"internal":0},"krb5_tcp":{"gap":0,"alloc":0,"parser":0,"internal":0},"sip_tcp":{"gap":0,"alloc":0,"parser":0,"internal":0},"rfb":{"gap":0,"alloc":0,"parser":0,"internal":0},"mqtt":{"gap":0,"alloc":0,"parser":0,"internal":0},"telnet":{"gap":0,"alloc":0,"parser":0,"internal":0},"websocket":{"gap":0,"alloc":0,"parser":0,"internal":0},"ldap_tcp":{"gap":0,"alloc":0,"parser":0,"internal":0},"doh2":{"gap":0,"alloc":0,"parser":0,"internal":0},"rdp":{"gap":0,"alloc":0,"parser":0,"internal":0},"http2":{"gap":0,"alloc":0,"parser":0,"internal":0},"pop3":{"gap":0,"alloc":0,"parser":0,"internal":0},"dcerpc_udp":{"alloc":0,"parser":0,"internal":0},"dns_udp":{"alloc":0,"parser":0,"internal":0},"nfs_udp":{"alloc":0,"parser":0,"internal":0},"ntp":{"alloc":0,"parser":0,"internal":0},"tftp":{"alloc":0,"parser":0,"internal":0},"ike":{"alloc":0,"parser":0,"internal":0},"krb5_udp":{"alloc":0,"parser":0,"internal":0},"quic":{"alloc":0,"parser":0,"internal":0},"dhcp":{"alloc":0,"parser":0,"internal":0},"sip_udp":{"alloc":0,"parser":11,"internal":0},"ldap_udp":{"alloc":0,"parser":0,"internal":0},"bittorrent-dht":{"alloc":0,"parser":0,"internal":0},"mdns":{"alloc":0,"parser":0,"internal":0},"snmp":{"alloc":0,"parser":0,"internal":0}},"tx":{"http":0,"ftp":0,"smtp":0,"tls":0,"ssh":0,"smb":0,"dcerpc_tcp":0,"dns_tcp":0,"nfs_tcp":0,"ftp-data":0,"krb5_tcp":0,"sip_tcp":0,"rfb":0,"mqtt":0,"telnet":0,"websocket":0,"ldap_tcp":0,"doh2":0,"rdp":0,"http2":0,"pop3":0,"dcerpc_udp":0,"dns_udp":0,"nfs_udp":0,"ntp":0,"tftp":0,"ike":0,"krb5_udp":0,"quic":0,"dhcp":0,"sip_udp":0,"ldap_udp":0,"bittorrent-dht":0,"mdns":3,"snmp":0},"expectations":0},"memcap":{"pressure":5,"pressure_max":5},"http":{"memuse":0,"memcap":0,"byterange":{"memuse":168384,"memcap":104857600}},"ftp":{"memuse":0,"memcap":0},"ippair":{"memuse":398144,"memcap":16777216},"host":{"memuse":382144,"memcap":33554432},"file_store":{"open_files":0}}}

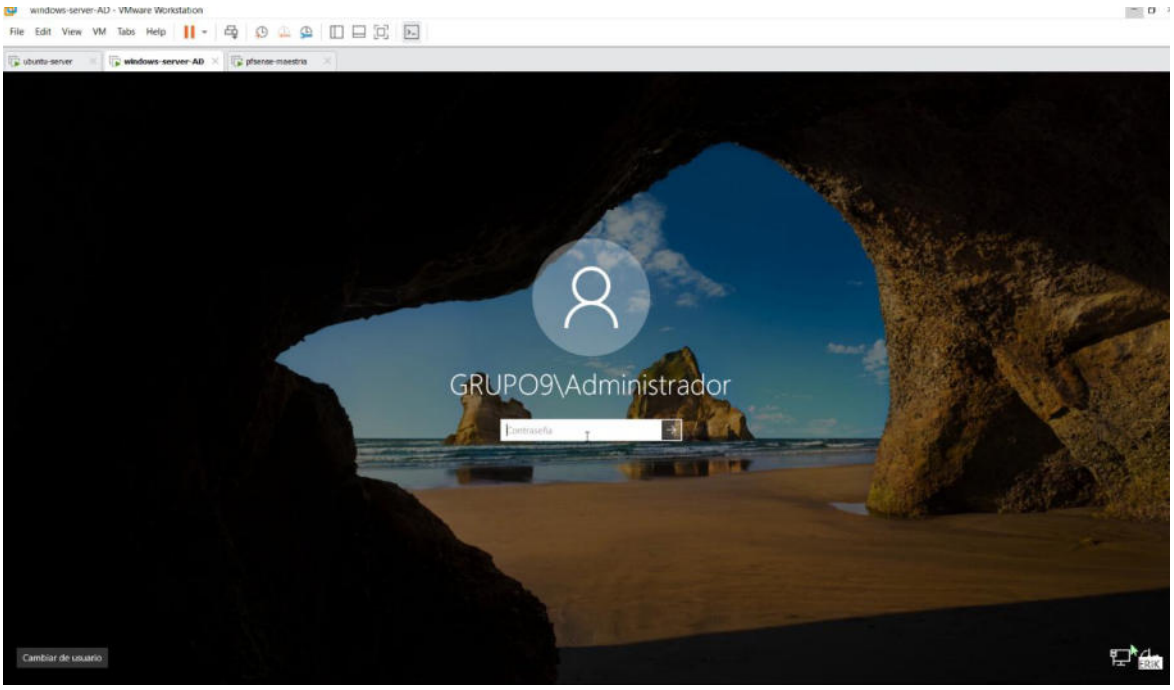
Nota: Elaboración propia.

3.4.Configuración de máquinas virtuales

Una vez desplegado el servidor SIEM y definidas las reglas de segmentación de red, se procedió a configurar las tres máquinas que componen la infraestructura monitoreada: el controlador de dominio en Windows Server, el servidor Ubuntu Web con Apache y WordPress, y el equipo cliente Windows incorporado al dominio. Cada una de estas máquinas fue configurada no solo para cumplir su función dentro de la red simulada, sino también para generar los registros de eventos necesarios que posteriormente alimentarían al SIEM a través del agente Filebeat.

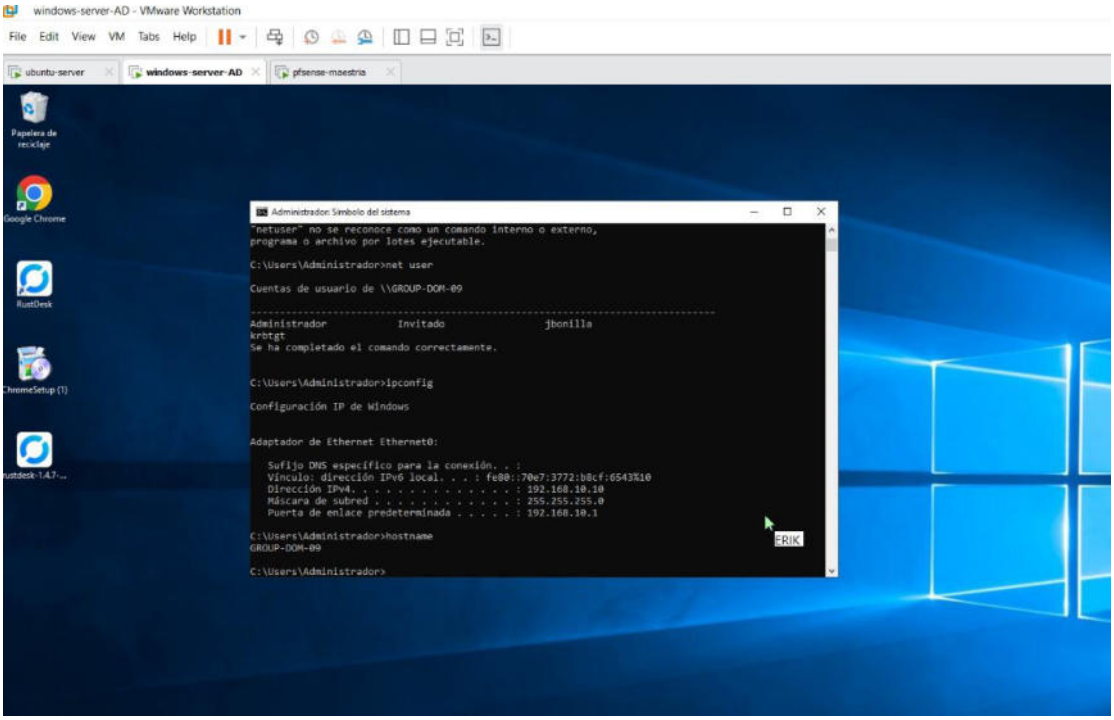
Configuración del controlador de dominio. La VM correspondiente al controlador de dominio se instaló con Windows Server 2022, ubicada en la VLAN 10 con dirección IP 192.168.10.100. Sobre esta máquina se instaló y configuró el rol de Active Directory Domain Services (AD DS), creando el dominio siem.local, el cual constituye el espacio de nombres bajo el cual se gestionan tanto las cuentas de usuario como los equipos incorporados al entorno de laboratorio.

Figura 29
Interfaz de inicio de sesión en el AD con cuenta Administrador.



Nota: Elaboración propia.

Figura 30
Validación de usuario y direcciones IP del servidor AD



Nota: Elaboración propia.

Además del rol de controlador de dominio, se habilitó el servicio de Escritorio Remoto (RDP) sobre el puerto 3389, dejando este servicio expuesto de forma intencional dentro de la

VLAN 10 con el propósito de que actúe como objetivo del escenario de fuerza bruta correspondiente a la técnica T1110. Cada intento de autenticación, exitoso o fallido, contra este servicio queda registrado en el visor de eventos de Windows bajo los identificadores EventID 4624 (inicio de sesión exitoso) y EventID 4625 (inicio de sesión fallido), los cuales constituyen la fuente principal de evidencia para las reglas de detección diseñadas en la sección anterior.

Sobre esta misma máquina se instaló el agente Filebeat 9.4.3, configurado mediante el módulo correspondiente a registros de eventos de Windows, apuntando hacia el servidor SIEM en la dirección 192.168.30.100, puerto 5044, de forma que los eventos de autenticación y de Active Directory queden disponibles en tiempo real dentro de Elasticsearch.

Configuración del servidor Ubuntu Web. La VM correspondiente al servidor web se instaló sobre Ubuntu Server, ubicada en la VLAN 10 con dirección IP dentro del rango 192.168.10.0/24. Sobre esta máquina se configuraron tres servicios simultáneos,

Servicio SSH (puerto 22), utilizado para la administración remota del servidor y, adicionalmente, como uno de los vectores de ataque evaluados en el Escenario 1 (fuerza bruta de credenciales, técnica T1110.001).

Servicio web Apache2 (puerto 80), sobre el cual se desplegó una instalación de WordPress, utilizada como aplicación web pública objetivo de los escenarios de explotación (técnica T1190).

Servicio de base de datos MySQL, utilizado por WordPress para el almacenamiento de contenido, usuarios y configuración del sitio, y que constituye el objetivo indirecto de los intentos de inyección SQL evaluados contra el parámetro de búsqueda de la aplicación.

Los registros generados por el servicio SSH quedan almacenados en /var/log/auth.log, mientras que los registros generados por Apache, incluyendo las solicitudes HTTP recibidas por WordPress, quedan almacenados en /var/log/apache2/access.log y /var/log/apache2/error.log. Sobre esta misma máquina se instaló el agente Filebeat, configurado para monitorear ambos archivos de log y enviarlos hacia el servidor SIEM, distinguiendo el tráfico de autenticación SSH

(orientado a la detección de la técnica T1110) del tráfico HTTP de WordPress (orientado a la detección de la técnica T1190).

Configuración del equipo cliente Windows

La VM correspondiente al equipo cliente se instaló con Windows 10, ubicada en la VLAN 20 con dirección IP 192.168.20.101. Esta máquina fue incorporada formalmente al dominio siem.local mediante el proceso estándar de unión a dominio de Windows, quedando autenticada contra el controlador de dominio ubicado en la VLAN 10. Esta configuración simula un equipo de usuario corporativo dentro de la infraestructura, estableciendo la base necesaria para ejecutar el escenario de movimiento lateral descrito en el alcance del proyecto.

Sobre este equipo se configuró específicamente el acceso por Escritorio Remoto hacia el controlador de dominio, de forma que, durante la ejecución del escenario correspondiente, sea posible simular que un atacante que ha comprometido previamente las credenciales de un usuario válido del dominio las utiliza desde este equipo cliente para establecer una conexión RDP hacia el controlador de dominio. Esta conexión, al originarse desde un segmento distinto (VLAN 20) hacia el segmento de servidores (VLAN 10), y al emplear credenciales legítimas en un contexto de uso que se aparta del comportamiento habitual, constituye la base de evidencia para las reglas de detección asociadas a las técnicas T1021 (Remote Services) y T1078 (Valid Accounts)hac.

De igual forma, sobre el equipo cliente se instaló el agente Filebeat, orientado principalmente a recolectar los eventos de seguridad locales generados por el propio equipo, complementando así la visibilidad que el SIEM mantiene sobre la actividad de autenticación originada desde la VLAN 20 hacia el resto de la infraestructura.

3.5. Corrección de sincronización horaria (NTP)

Previamente para comenzar a desarrollar las reglas de correlación y realizar los ataques, es necesario que todos nuestros servidores marquen el mismo reloj, para ello se levanta el servicio

NTP en el servidor SIEM, ya que se identificó un desfase de reloj de aproximadamente dieciocho horas en las máquinas virtuales Kali Linux y Ubuntu Web, AD respecto a la hora real.

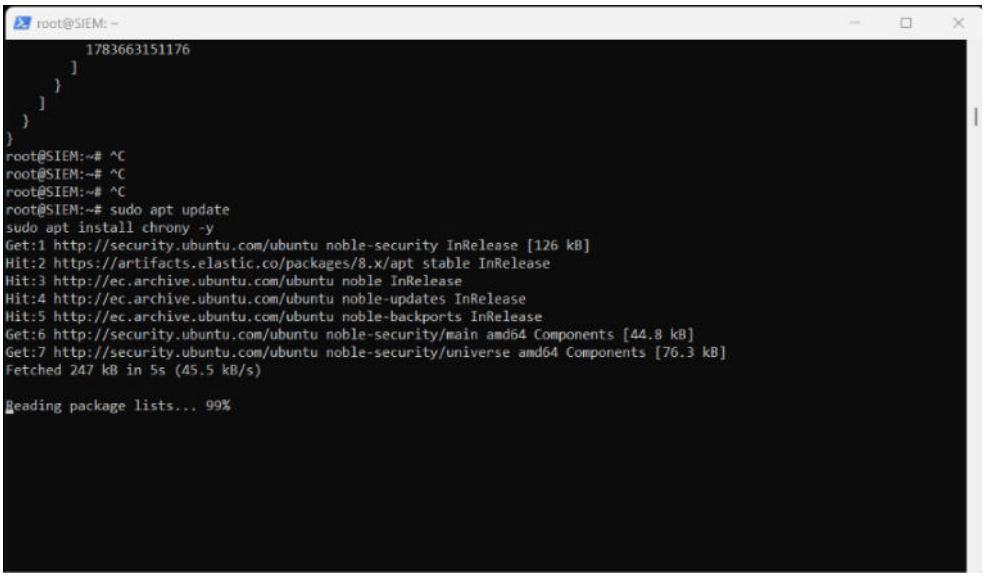
Se levanta un servidor NTP

Figura 31
Servicio NTP

Nota: Elaboración propia.

Con el propósito de unificar la referencia temporal de todos los equipos del laboratorio, se instaló el servicio Network Time Protocol (NTP) en el servidor Ubuntu que aloja la plataforma SIEM, permitiendo que éste funcione como servidor de tiempo para el resto de la infraestructura.

Figura 32
Instalación del servicio NTP en activo

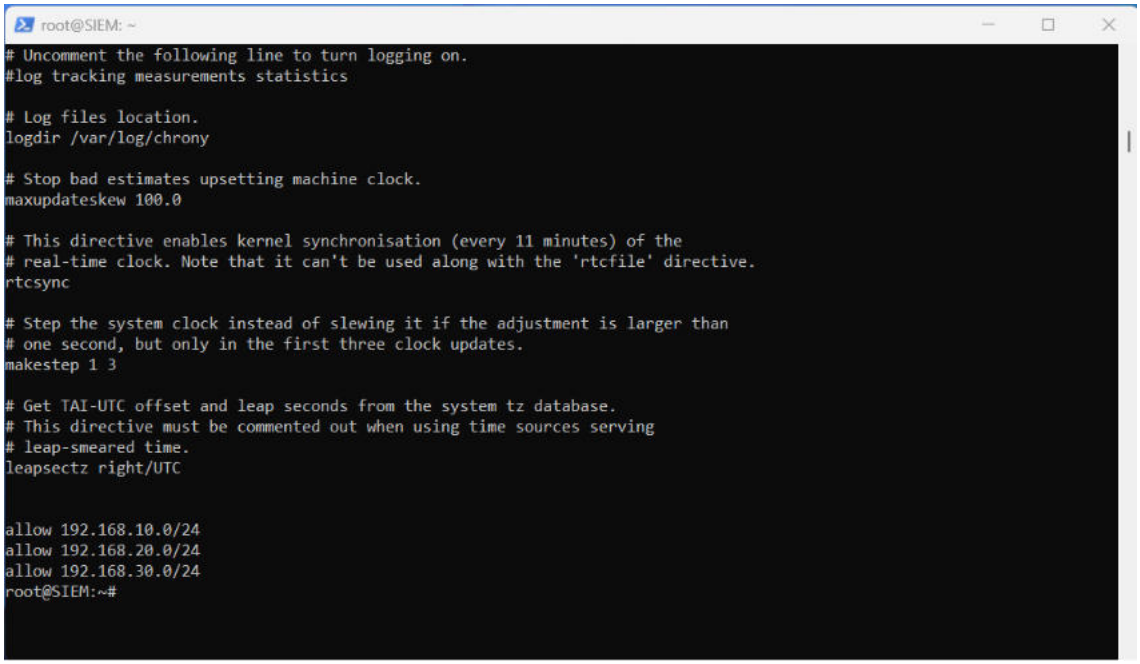


Nota: Elaboración propia.

Configuración de archivos

La figura muestra la modificación del archivo de configuración del servicio NTP, donde se definieron las fuentes de sincronización y los parámetros necesarios para permitir que los equipos clientes obtengan la hora oficial desde el servidor SIEM.

Figura 33
Modificación del archivo de configuración del servicio NTP

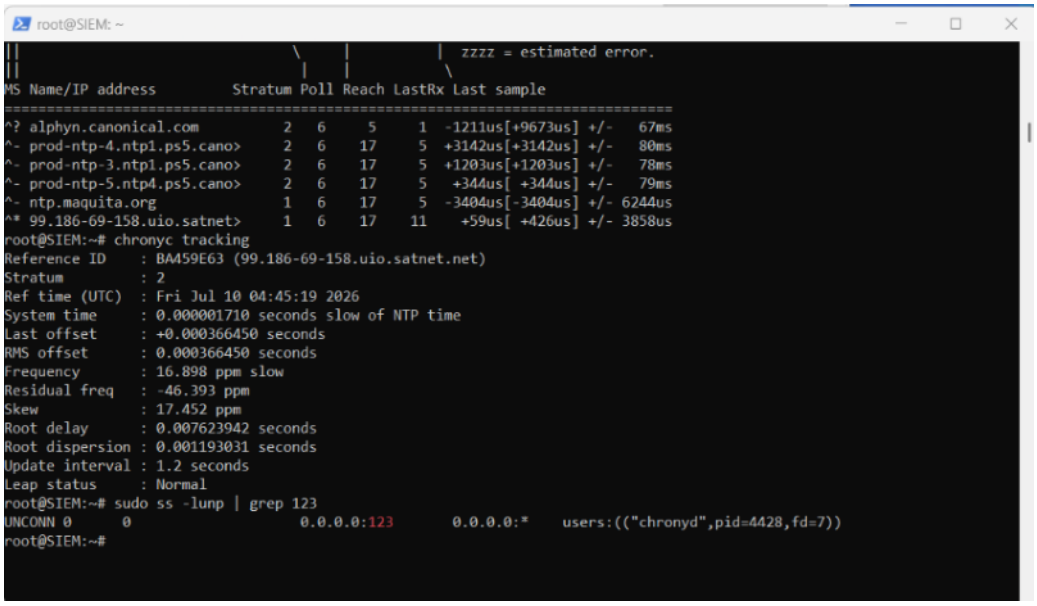


Nota: Elaboración propia.

Funcionamiento de ntp

Después de completar la configuración, se verificó el correcto funcionamiento del servicio mediante comandos de administración del sistema, confirmando que el servidor respondía correctamente a las solicitudes de sincronización.

Figura 34
Verificación el funcionamiento del servicio NTP

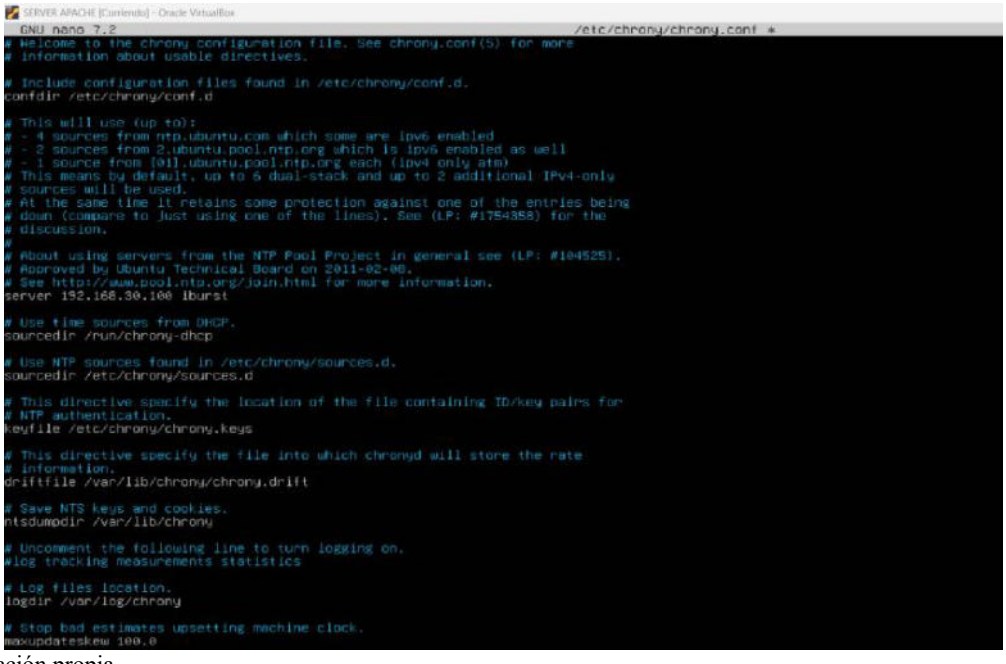


Nota: Elaboración propia.

Sincronización servidor APACHE

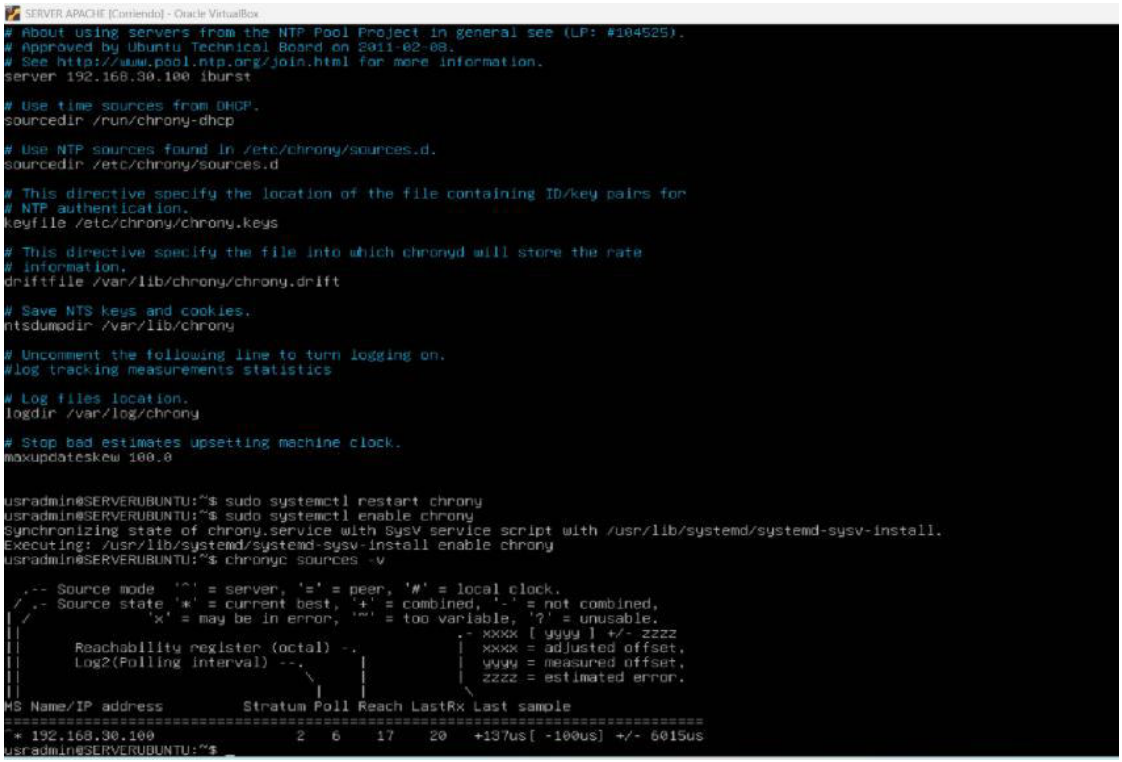
Una vez operativo el servidor NTP, se sincronizó el servidor Ubuntu que hospeda el servicio Apache. Esta acción garantiza que los registros generados por el servidor web mantengan una referencia temporal uniforme con el resto de los componentes del laboratorio.

Figura 35
Configuración de la sincronización del servidor APACHE



Nota: Elaboración propia.

Figura 36
Revisión de la sincronización del servidor APACHE

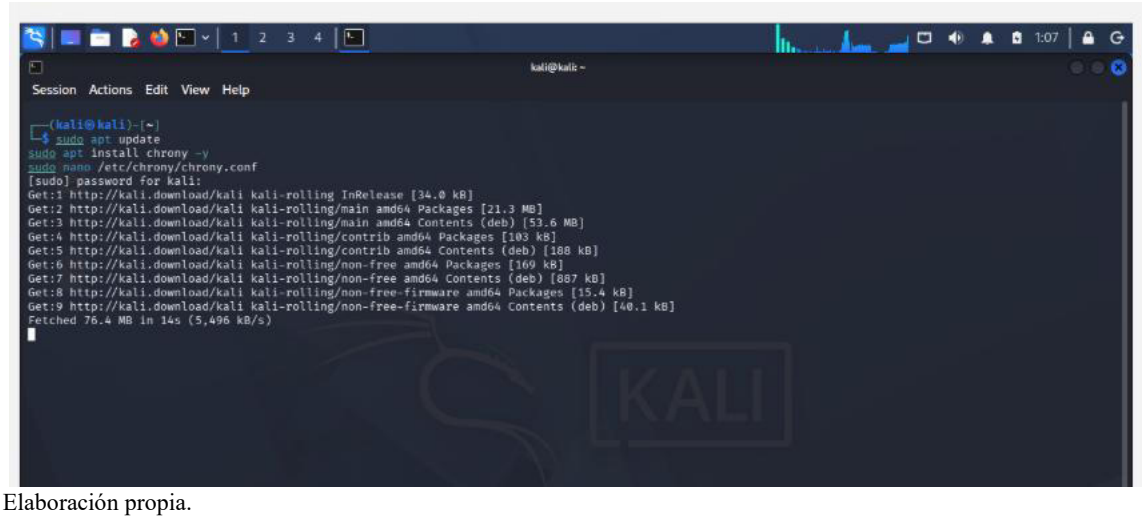


Nota: Elaboración propia.

Configuración de Kali

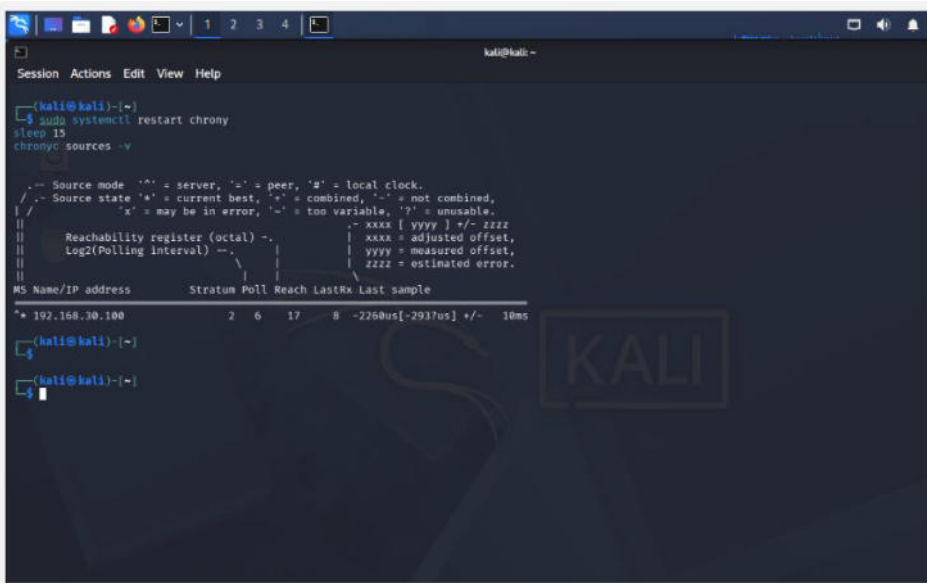
La figura presenta la configuración del cliente NTP en el equipo Kali Linux, permitiendo que las marcas de tiempo de los eventos generados durante las pruebas coincidan con las registradas por el SIEM.

Figura 37
Instalación y configuración del cliente NTP en Kali



Nota: Elaboración propia.

Figura 38
Reinicio del servicio NTP en Kali

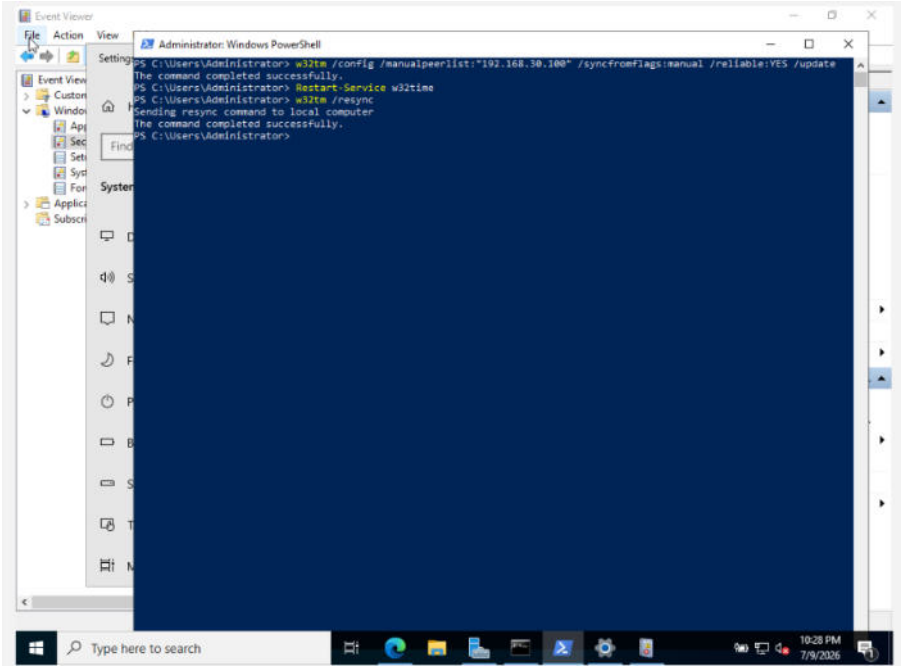


Nota: Elaboración propia

Configuración de Windows Server

En esta etapa se configuró el servidor Windows Server para utilizar el servidor NTP implementado en Ubuntu como fuente principal de sincronización, garantizando la uniformidad temporal de los registros del controlador de dominio.

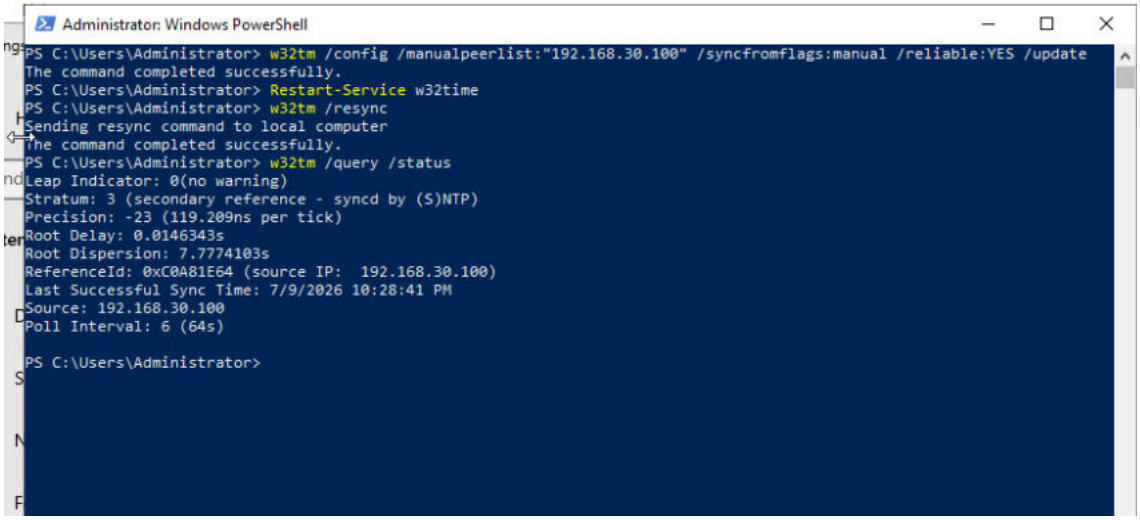
Figura 39
Configuración del servicio NTP en Windows Server



Nota: Elaboración propia

La figura evidencia que todos los equipos del laboratorio presentan una diferencia mínima de tiempo, permitiendo realizar correlaciones precisas entre eventos provenientes de diferentes dispositivos.

Figura 40
Reinicio del servicio NTP



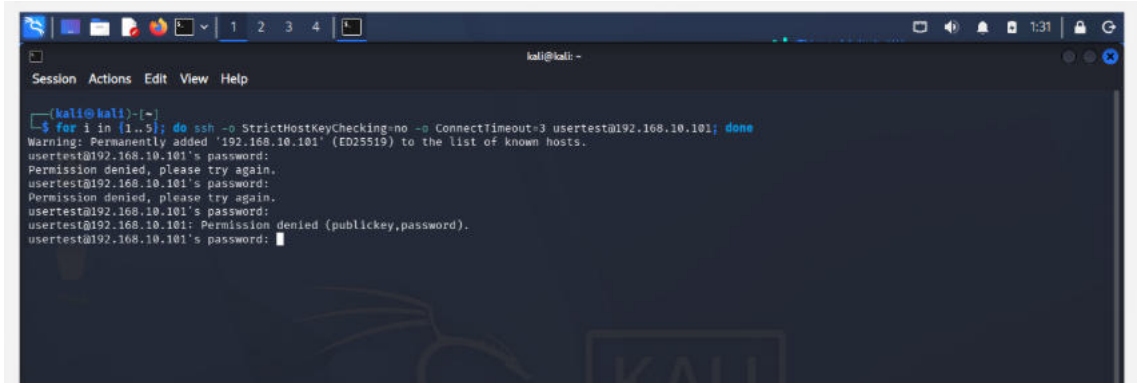
Nota: Elaboración propia

3.6. Pruebas de conectividad a los servidores.

Intentos de conexión al servidor Apache

Se instaló el servicio Apache como servidor web vulnerable que sería utilizado para ejecutar diferentes escenarios de prueba. Posteriormente se verificó su funcionamiento mediante solicitudes HTTP desde el equipo atacante.

Figura 41
Intento conexión al servidor Apache



Nota: Elaboración propia

3.7. Diseño de reglas de correlación y detección

REGLA 1 – T1110 fuerza bruta ssh (Ubuntu web)

Tomando como referencia la técnica T1110 Brute Force del frimework MITRE ATT&CK, se desarrolla la correlación orientada a detectar intentos de ataque de fuerza bruta, desde nuestra maquina atacante Kali 192.168.1.2, vía conexión ssh al servidor Ubuntu Apache/Wordpress 192.168.10.101

La regla formulada inicialmente con formato Sigma y transformándola a lenguaje de consulta para Elasticsearch

Ficha técnica de la regla

Campo	Valor
Nombre de la regla	SIEM - T1110 - Fuerza Bruta SSH (Ubuntu Web)
Técnica MITRE	T1110.001 – Brute Force: Password Guessing
Táctica	Credential Access
Host objetivo	Ubuntu Apache/WordPress (SERVERUBUNTU) — 192.168.10.101
Puerto / servicio	TCP 22 (SSH)
Fuente de datos	Data View "SIEM Auth" → índice siem-auth-*
Tipo de regla en Kibana	Threshold
Consulta (query)	event.outcome:"failure" AND program:"sshd"
Lenguaje de consulta	KQL
Campo de agrupación	source.ip.keyword
Umbral de activación	count() >= 5
Programación de ejecución	Cada 1 minuto, look-back adicional de 1 minuto
Severidad	Media (risk score 47)

Regla en formato Sigma

A continuación, se presenta la regla de detección en formato Sigma, que documenta la lógica de detección de manera independiente de la plataforma SIEM:

```
title: Fuerza Bruta SSH contra Servidor Ubuntu Web

id: 7a1f2e10-3b44-4c9a-9e21-1a2b3c4d5e01

status: stable

description: >
```

```
  Detecta múltiples intentos fallidos de autenticación SSH desde una
  misma dirección IP origen en un periodo corto, indicativo de un
  ataque de fuerza bruta (T1110.001) contra el servidor Ubuntu Web.
references:
    - https://attack.mitre.org/techniques/T1110/001/
author: Angel Aguaguiña, Jorge Bonilla, Romina Castro
date: 2026/07/12
tags:
    - attack.credential_access
    - attack.t1110.001
logsource:
    product: linux
    service: auth
detection:
    selection:
        event.outcome: 'failure'
```

REGLA 2 - T1110 Fuerza Bruta RDP (Windows Server AD)

DISEÑO DE REGLA Y CORRELACION Y DETECCION

Como segunda variante de la técnica T1110 (Brute Force) del framework MITRE ATT&CK, se diseñó una regla de correlación orientada a detectar intentos de fuerza bruta mediante el protocolo RDP contra el controlador de dominio Windows Server (192.168.10.100).

REGLA

Campo	Valor
Nombre de la regla	SIEM - T1110 - Fuerza Bruta RDP (Windows Server AD)
Técnica MITRE	T1110.001 – Brute Force: Password Guessing
Táctica	Credential Access
Host objetivo	Windows Server AD (controlador de dominio) — 192.168.10.100
Puerto / servicio	TCP 3389 (RDP)
Fuente de datos	Data View "SIEM Auth" → índice siem-auth-*
Tipo de regla en Kibana	Threshold
Consulta (query)	event.code : "4625" and winlog.event_data.LogonType : ("3" or "10")
Lenguaje de consulta	KQL
Campo de agrupación	winlog.event_data.IpAddress.keyword
Umbral de activación	count() >= 5

Programación de ejecución	Cada 1 minuto, look-back adicional de 1 minuto
Severidad	Alta (risk score 73)

REGLA 3 - T1046 Escaneo de Red (Nmap)

Diseño de la regla de correlación y detección

Con base en la técnica T1046 (Network Service Discovery) del framework MITRE ATT&CK, se diseñó una regla de correlación orientada a detectar actividad de reconocimiento de red mediante escaneo de puertos contra el servidor Ubuntu Web (192.168.10.101). A diferencia de las Reglas 1 y 2, que se basan en registros de autenticación a nivel de aplicación.

Regla

Campo	**Valor**
Nombre de la regla	SIEM - T1046 - Escaneo de Red (Nmap)
Técnica MITRE	T1046 – Network Service Discovery
Táctica	Discovery
Host objetivo	Ubuntu Apache/WordPress (SERVERUBUNTU) — 192.168.10.101
Fuente de datos	Data View "SIEM Firewall" → índice siem-firewall-*
Tipo de regla en Kibana	Threshold
Consulta (query)	action:"pass" and destination.ip:"192.168.10.101" and protocol:"tcp"
Lenguaje de consulta	KQL
Campo de agrupación	source.ip.keyword
Umbral de activación	count() >= 5
Programación de ejecución	Cada 1 minuto, look-back adicional de 1 minuto
Severidad	Media (risk score 47)

Formato sigma

```
title: Escaneo de Red contra Servidor Ubuntu Web

id: 7a1f2e10-3b44-4c9a-9e21-1a2b3c4d5e03

status: stable

description: >

 Detecta múltiples conexiones TCP permitidas hacia distintos

 puertos de un mismo host de destino, desde una única IP
```

```
 origen, en un periodo corto de tiempo, indicativo de
 actividad de reconocimiento de red (T1046) mediante
 herramientas de escaneo de puertos.
references:
  - https://attack.mitre.org/techniques/T1046/
author: Angel Aguaguiña, Jorge Bonilla, Romina Castro
date: 2026/07/12
tags:
  - attack.discovery
  - attack.t1046
logsource:
  product: pfsense
  service: filterlog
detection:
  selection:
    action: 'pass'
    destination.ip: '192.168.10.101'
    protocol: 'tcp'
  timeframe: 60s
  condition: selection | count(source.ip) by source.ip >= 5
falsepositives:
  - Administrador de red realizando pruebas de conectividad legítimas
  - Herramientas de monitoreo interno consultando múltiples servicios
```

level: medium

La conversión hacia Elastic Security agrupa los eventos mediante el subcampo source.ip.keyword sobre el índice siem-firewall-*, aprovechando los campos estructurados obtenidos mediante un filtro CSV aplicado en el pipeline de Logstash correspondiente al procesamiento del formato filterlog de pfSense (rule_num, tracker, action, protocol, source.ip, destination.ip, source.port, destination.port).

REGLA 4 - T1190 Inyección SQL (sqlmap)

Diseño de la regla de correlación y detección

Ficha técnica

Técnica MITRE ATT&CK	T1190 — Exploit Public-Facing Application
Nombre de la regla	SIEM - T1190 - Inyección SQL (WordPress)
Tipo de regla (Kibana)	Threshold
Data View / Índice	`SIEM Apache (siem-apache-*)`
Query base	`tags: "sql_injection_candidate"`
Group by	`source_ip`
Umbral	≥ 5 eventos
Ventana / Schedule	1 minuto / 1 minuto
Severidad configurada	High (corregida desde Low)
Escenario de ataque	`sqlmap contra http://192.168.10.101/wordpress/?s=`
Origen del ataque (Kali)	192.168.1.2
Objetivo (Ubuntu Web)	192.168.10.101

Formato sigma

title: SIEM - T1190 - Inyección SQL (WordPress)

id: 506cca61-dce6-4de6-add6-ee37bd2903c7

status: stable

description: >

Detecta ráfagas de peticiones HTTP hacia WordPress cuyo parámetro de búsqueda contiene patrones característicos de inyección SQL

```
 (UNION, SELECT, OR 1=1, comentarios --, comillas simples).
author: Grupo 9 - UIDE
date: 2026/07/13
references:
 - https://attack.mitre.org/techniques/T1190/
logsource:
 product: apache
 service: access
 definition: 'Data View: SIEM Apache (siem-apache-*)'
detection:
 selection:
  tags: sql_injection_candidate
 condition: selection | count(source_ip) by source_ip >= 5
timeframe: 1m
level: high
tags:
 - attack.initial_access
 - attack.t1190
```

REGLA 5 - T1190 Explotación WordPress (WP File Manager RCE)

Ficha tecnica

Técnica MITRE ATT&CK	T1190 — Exploit Public-Facing Application
Nombre de la regla	SIEM - T1190 - Explotación WordPress (WP File Manager RCE)
Tipo de regla (Kibana)	Query (custom query, sin umbral)
Data View / Índice	`SIEM Apache (siem-apache-*)`

Query base	`tags: "wp_file_manager_exploit_candidate"`
Severidad	High
Risk score	73
Schedule	1 minuto / 1 minuto (look-back 1 minuto)
Vulnerabilidad explotada	CVE-2020-25213 — WP File Manager ≤ 6.0, subida de archivo sin autenticación vía conector elFinder (RCE)
Plugin instalado deliberadamente	wp-file-manager v6.0 (obsoleto respecto a 8.0.4, instalado manualmente para el escenario)
Endpoint vulnerable	`/wp-content/plugins/wp-file-manager/lib/php/connector.minimal.php`
Herramientas de ataque	WPScan (reconocimiento) + curl (explotación manual del CVE)
Origen del ataque (Kali)	192.168.1.2
Objetivo (Ubuntu Web)	192.168.10.101

Formato sigma

```
title: SIEM - T1190 - Explotación WordPress (WP File Manager RCE)

id: 2dc828d2-bf49-40b5-be92-9965c70c2a67

status: stable

description: >

 Detecta peticiones HTTP hacia el conector elFinder del plugin

 WP File Manager (versiones vulnerables ≤6.0), utilizado para

 subir archivos sin autenticación (CVE-2020-25213) y ejecutar

 comandos remotos a través del archivo subido.

author: Grupo 9 - UIDE

date: 2026/07/14

references:

 - https://attack.mitre.org/techniques/T1190/

 - https://nvd.nist.gov/vuln/detail/CVE-2020-25213

logsource:

 product: apache
```

```
 service: access
 definition: 'Data View: SIEM Apache (siem-apache-*)'
detection:
 selection:
  tags: wp_file_manager_exploit_candidate
 condition: selection
level: high
tags:
 - attack.initial_access
 - attack.t1190
 - cve.2020-25213
```

REGLA 6 – SIEM - T1059 - Ejecución de Comandos (Post-Explotación)

Ficha técnica

Técnica MITRE ATT&CK	T1059 — Command and Scripting Interpreter
Nombre de la regla	SIEM - T1059 - Ejecución de Comandos (Post-Explotación)
Tipo de regla (Kibana)	Query (custom query, sin umbral)
Data View / Índice	`SIEM Apache (siem-apache-*)`
Query base	`tags: "remote_command_execution_candidate"`
Severidad	High
Risk score	73
Schedule	1 minuto / 1 minuto
Escenario	Post-explotación vía la webshell instalada en la Regla 5 (CVE-2020-25213)
Vector de detección	Parámetro cmd= en la URL, con patrón de comandos de sistema (whoami, uname, cat, wget, bash, /etc/, etc.)
Herramienta de ataque	curl (ejecución manual de comandos vía la webshell)
Origen del ataque (Kali)	192.168.1.2
Objetivo (Ubuntu Web)	192.168.10.101

Formato sigma

```
title: SIEM - T1059 - Ejecución de Comandos (Post-Explotación)
id: (ver UUID de la regla en Kibana)
status: stable
description: >
 Detecta peticiones HTTP con un parámetro cmd= que contiene
 comandos de sistema típicos de reconocimiento o post-
 explotación (whoami, uname, cat, wget, curl, bash, passwd,
 /etc/, chmod, nmap), independientemente del endpoint o
 vulnerabilidad utilizados para lograr la ejecución.
author: Grupo 9 - UIDE
date: 2026/07/14
references:
 - https://attack.mitre.org/techniques/T1059/
logsource:
 product: apache
 service: access
 definition: 'Data View: SIEM Apache (siem-apache-*)'
detection:
 selection:
  tags: remote_command_execution_candidate
 condition: selection
level: high
tags:
```

```
- attack.execution
- attack.t1059
```

REGLA 7 – T1021 Movimiento Lateral RDP (VLAN20 → AD)

La regla7 implementa una detección de Movimiento Lateral mediante Remote Desktop Protocol (RDP), alineada con la técnica MITRE ATT&CK T102. La regla detecta autenticaciones RDP exitosas desde la VLAN de usuarios (192.168.20.101) hacia el Controlador de Dominio (192.168.10.100).

Ficha técnica regla

Técnica MITRE ATT&CK	T1021.001 — Remote Services: Remote Desktop Protocol
Nombre de la regla	SIEM - T1021 - Movimiento Lateral RDP (VLAN20 → AD)
Tipo de regla (Kibana)	Query (custom query, sin umbral)
Data View / Índice	`SIEM Auth (siem-auth-*)`
Query base	`winlog.event_id: 4624 and winlog.event_data.IpAddress: "192.168.20.101" and not winlog.event_data.TargetUserName: "WIN-TK9UVU2B5F9$"`
Severidad	High
Risk score	75
Schedule	1 minuto / 1 minuto
Escenario	Autenticación RDP de un usuario de dominio (aaguaguina) desde un PC cliente en VLAN20 hacia el Controlador de Dominio en VLAN10
Herramienta de ataque	mstsc (cliente RDP nativo de Windows)
Origen (PC cliente)	192.168.20.101 — VLAN20 (USUARIOS_VLAN20)
Objetivo (AD)	192.168.10.100 — WIN-TK9UVU2B5F9.siem.local
Cuenta utilizada	aaguaguina (cuenta de dominio de prueba)

Formato sigma

```
title: SIEM - T1021 - Movimiento Lateral RDP (VLAN20 -> AD)
id: 3a4aa85a-b175-4652-a038-8722efbe4a4d
status: stable
description: >
 Detecta autenticaciones RDP exitosas contra el Controlador de
 Dominio (Windows Server AD) originadas desde la red interna de
 usuarios (VLAN20), excluyendo el trafico interno propio de la
```

```
 cuenta de maquina del servidor.
author: Grupo 9 - UIDE
date: 2026/07/15
references:
 - https://attack.mitre.org/techniques/T1021/001/
logsource:
 product: windows
 service: security
 definition: 'Data View: SIEM Auth (siem-auth-*)'
detection:
 selection:
  winlog.event_id: 4624
  winlog.event_data.IpAddress: '192.168.20.101'
 filter:
  winlog.event_data.TargetUserName: 'WIN-TK9UVU2B5F9$'
 condition: selection and not filter
level: high
tags:
 - attack.lateral_movement
 - attack.t1021.001
```

REGLA 8 SIEM - T1078 - Cuentas Válidas (Autenticación de Dominio)

La regla8 implementa una detección asociada a la técnica MITRE ATT&CK T1078 – Valid Accounts, enfocada en identificar el uso exitoso de una cuenta de dominio válida dentro del entorno. La regla monitoriza la cuenta aaguaguina y genera alertas cuando se producen autenticaciones exitosas distintas de los inicios de sesión de red habituales.

Ficha técnica

Técnica MITRE ATT&CK	T1078 — Valid Accounts
Nombre de la regla	SIEM - T1078 - Cuentas Válidas (Autenticación de Dominio)
Tipo de regla (Kibana)	Query (custom query, sin umbral)
Data View / Índice	`SIEM Auth (siem-auth-*)`
Query base	`winlog.event_id: 4624 and winlog.event_data.TargetUserName: "aaguaguina" and not winlog.event_data.LogonType: "3"`
Severidad	Medium
Risk score	47
Schedule	1 minuto / 1 minuto
Escenario	Autenticación exitosa de una cuenta de dominio real (aaguaguina) mediante RDP, correlacionada con el mismo evento que dispara la Regla 7 (T1021)
Herramienta	mstsc (cliente RDP nativo de Windows)
Cuenta monitoreada	aaguaguina (cuenta de dominio de prueba)
Host afectado	WIN-TK9UVU2B5F9.siem.local (192.168.10.100)
Regla relacionada	SIEM - T1021 - Movimiento Lateral RDP (VLAN20 → AD) — correlación confirmada por 'Alerts related by source event'

Formato sigma

```
title: SIEM - T1078 - Cuentas Validas (Autenticacion de Dominio)
id: 6e8b501a-5316-487e-9a08-92215da2733b
status: stable
description: >
  Detecta autenticaciones exitosas de la cuenta de dominio de
  prueba (aaguaguina) con tipos de logon interactivo/remoto,
  excluyendo logons de red de bajo nivel (LogonType 3) generados
  constantemente por procesos internos de Windows. Disenada para
  correlacionar con la Regla 7 (T1021) sobre el mismo origen de
  evento, evidenciando el uso de credenciales validas en un
  contexto de movimiento lateral.
author: Grupo 9 - UIDE
date: 2026/07/15
references:
  - https://attack.mitre.org/techniques/T1078/
logsource:
  product: windows
  service: security
```

```
 definition: 'Data View: SIEM Auth (siem-auth-*)'
detection:
 selection:
  winlog.event_id: 4624
  winlog.event_data.TargetUserName: 'aaguaguina'
 filter:
  winlog.event_data.LogonType: '3'
 condition: selection and not filter
level: medium
tags:
 - attack.defense_evasion
 - attack.persistence
 - attack.t1078
```

3.8 Diseño de escenarios de ataque

3.8.1 Matriz de referencia de los escenarios de ataque ground truth

Matriz de referencia de los escenarios de ataque ground truth

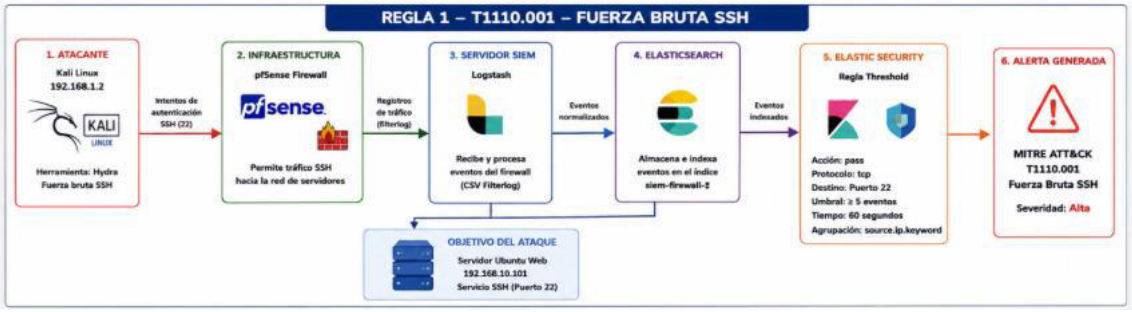
Escenario	Origen	Objetivo	Técnica MITRE	Herramienta o comando	Resultado esperado	Evidencia
Fuerza bruta SSH	Kali Linux	Ubuntu Server	T1110	Comandos SSH ejecutados	Generar intentos fallidos y una alerta	Sección 4.1.1
Fuerza bruta RDP	Kali Linux	Windows Server AD	T1110	Herramienta o comando utilizado	Generar fallos de autenticación RDP	Sección 4.1.2
Escaneo de red	Kali Linux	Servidor SIEM/objetivo	T1046	nmap -sS -p- -T4 ...	Identificar múltiples puertos y generar alerta	Sección 4.1
Inyección SQL	Kali Linux	Aplicación web	T1190	sqlmap o solicitudes curl	Generar tráfico compatible con intento de inyección	Sección 4.1.3

Escenario	Origen	Objetivo	Técnica MITRE	Herramienta o comando	Resultado esperado	Evidencia
Explotación de WordPress	Kali Linux	Servidor WordPress	T1190	WPScan, Nikto o herramienta utilizada	Generar actividad de reconocimiento o explotación	Sección 4.1
Movimiento lateral	Cliente Windows	Controlador de dominio	T1021/T1078	RDP o servicio remoto con cuenta válida	Registrar acceso mediante servicio remoto	Sección 4.1

Con base en las reglas de correlación documentadas en la sección anterior, se diseñaron escenarios de ataque controlados, ejecutados desde la máquina Kali Linux ubicada en la red externa del laboratorio (192.168.1.x), con el objetivo de generar evidencia real que permita validar la capacidad de detección del SIEM frente a cada una de las técnicas MITRE ATT&CK seleccionadas. Cada escenario fue diseñado especificando la herramienta utilizada, los parámetros de ejecución, el objetivo dentro de la infraestructura y la técnica MITRE asociada.

Escenario 1 — T1110 fuerza bruta ssh (Ubuntu web)

Escenario de ataque.



Para validar la Regla 1 se ejecutó un escenario de fuerza bruta SSH desde la máquina atacante Kali Linux (192.168.1.2) contra el servidor Ubuntu Web (192.168.10.101), generando múltiples intentos de autenticación fallida en un intervalo controlado de tiempo.

Comando de ejecución

```
date -u

for i in {1..10}; do

 sshpass -p "wrongpass$i" ssh -o StrictHostKeyChecking=no \

  -o PubkeyAuthentication=no -o ConnectTimeout=3 \

  -o PreferredAuthentications=password \

  fakeuser@192.168.10.101 exit 2>/dev/null

done

date -u
```

El siguiente script se ejecutó desde un equipo Kali Linux con el propósito de simular múltiples intentos de autenticación fallidos contra un servidor SSH. Esta actividad permite generar eventos de seguridad que son detectados por Suricata y posteriormente correlacionados por el SIEM.

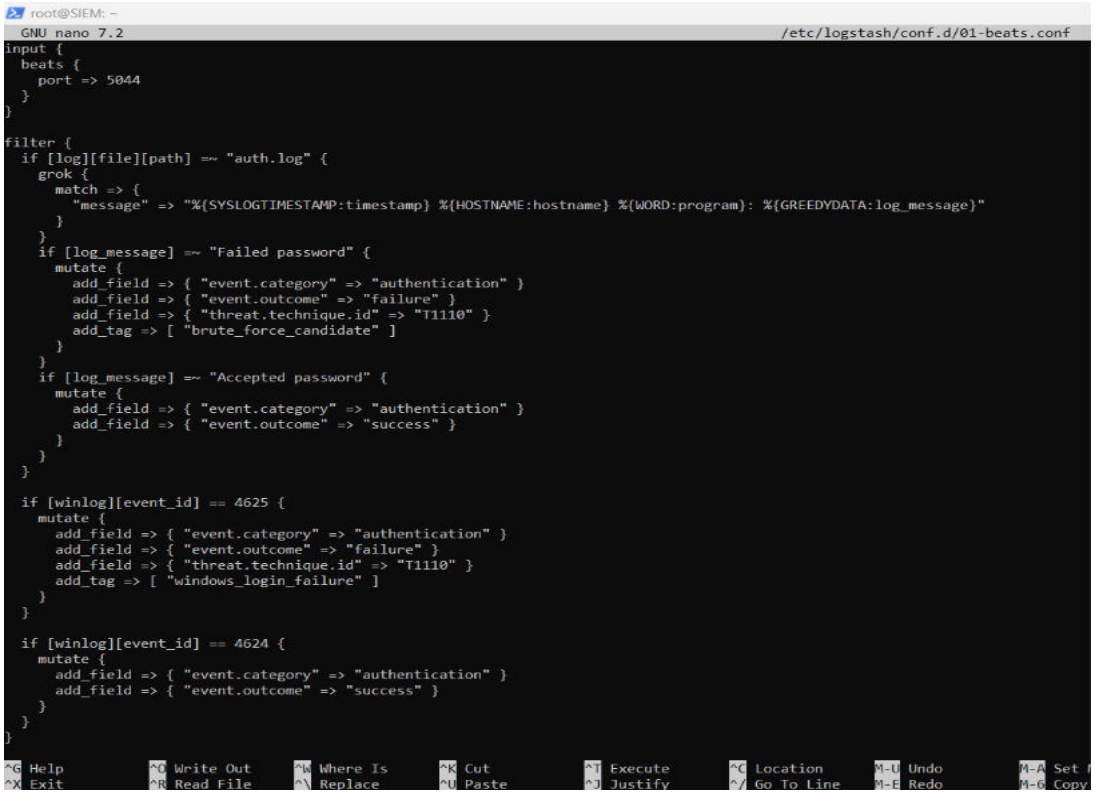
Descripción del funcionamiento

Comando	**Descripción**
date -u	Muestra la fecha y la hora actual en formato UTC (Tiempo Universal Coordinado). Se ejecuta antes y después del proceso para registrar el intervalo de tiempo durante el cual se realizaron los intentos de autenticación.
for i in {1..10}; do	Inicia un ciclo que se ejecuta diez veces. Cada iteración representa un intento independiente de autenticación mediante SSH.
sshpass -p "wrongpass$i"	Utiliza la herramienta **sshpass** para proporcionar automáticamente una contraseña al cliente SSH. La contraseña cambia en cada iteración (wrongpass1, wrongpass2, ..., wrongpass10), simulando diferentes intentos de acceso con credenciales incorrectas.
ssh	Inicia una conexión al servicio SSH del servidor objetivo.
-o StrictHostKeyChecking=no	Deshabilita la verificación de la clave del servidor, evitando que SSH solicite confirmación cuando el host es desconocido. Esto permite automatizar completamente la prueba.

Comando	Descripción
-o PubkeyAuthentication=no	Desactiva la autenticación mediante claves públicas, obligando al cliente a utilizar únicamente autenticación por contraseña.
-o ConnectTimeout=3	Establece un tiempo máximo de tres segundos para intentar establecer la conexión. Si el servidor no responde dentro de ese tiempo, el intento finaliza automáticamente.
-o PreferredAuthentications=password	Indica que el método de autenticación preferido será mediante contraseña.
fakeuser@192.168.10.101	Especifica el usuario y la dirección IP del servidor objetivo. En este caso se utiliza un usuario inexistente (fakeuser) para garantizar que todos los intentos de autenticación sean rechazados.
exit	Comando que se ejecutaría únicamente si la autenticación fuera exitosa. Debido a que las credenciales son incorrectas, este comando nunca llega a ejecutarse.
2>/dev/null	Redirige los mensajes de error al dispositivo /dev/null, evitando que los errores de autenticación aparezcan en pantalla y manteniendo la salida del script limpia.
done	Finaliza el ciclo de diez intentos de autenticación.
date -u	Registra nuevamente la hora UTC al finalizar la prueba, permitiendo conocer la duración total del proceso.

Figura 42

Parseo de la informaciónParseo de la información



Nota: Elaboración propia

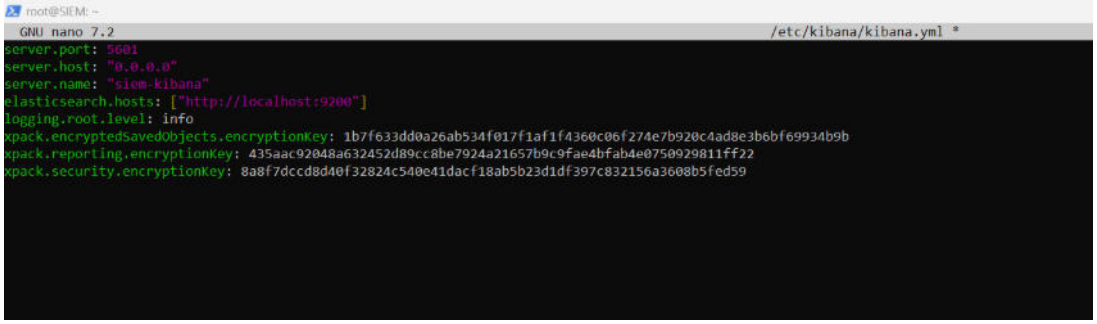
Configuración de Filebeat

La figura muestra la configuración realizada en Filebeat, agente encargado de recopilar los registros del servidor Ubuntu Web. Se observa la definición del archivo auth.log como fuente de datos, permitiendo capturar automáticamente los eventos relacionados con procesos de autenticación SSH. Posteriormente, estos registros son enviados al servidor Logstash para su procesamiento y almacenamiento, constituyendo la primera etapa del flujo de recolección de eventos implementado en el SIEM.

Figura 43
Configuración en Filebeat

Nota: Elaboración propia

Figura 44
Configuración en Filebeat

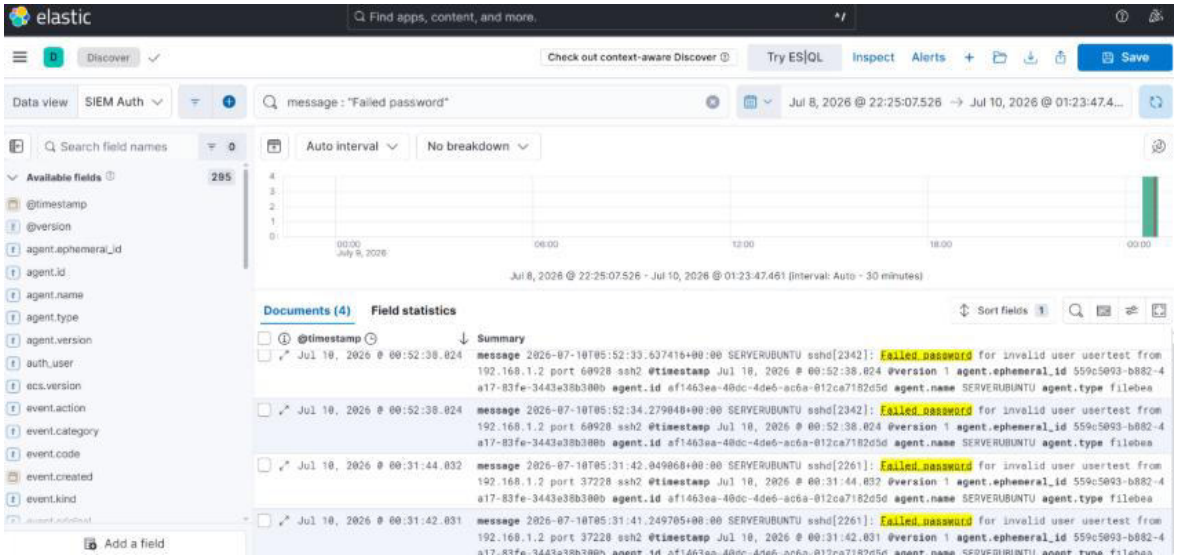


Nota: Elaboración propia

Visualización de eventos

En esta figura se evidencia la recepción de los eventos generados por el servidor Ubuntu dentro de Elasticsearch. Cada intento de autenticación fallida es almacenado como un documento independiente, conservando información como la dirección IP de origen, el usuario utilizado, la fecha del evento, el servicio afectado y el resultado de la autenticación. Esta información constituye la base para la posterior correlación de eventos mediante Elastic Security.

Figura 45
Visualización de eventos en elastic

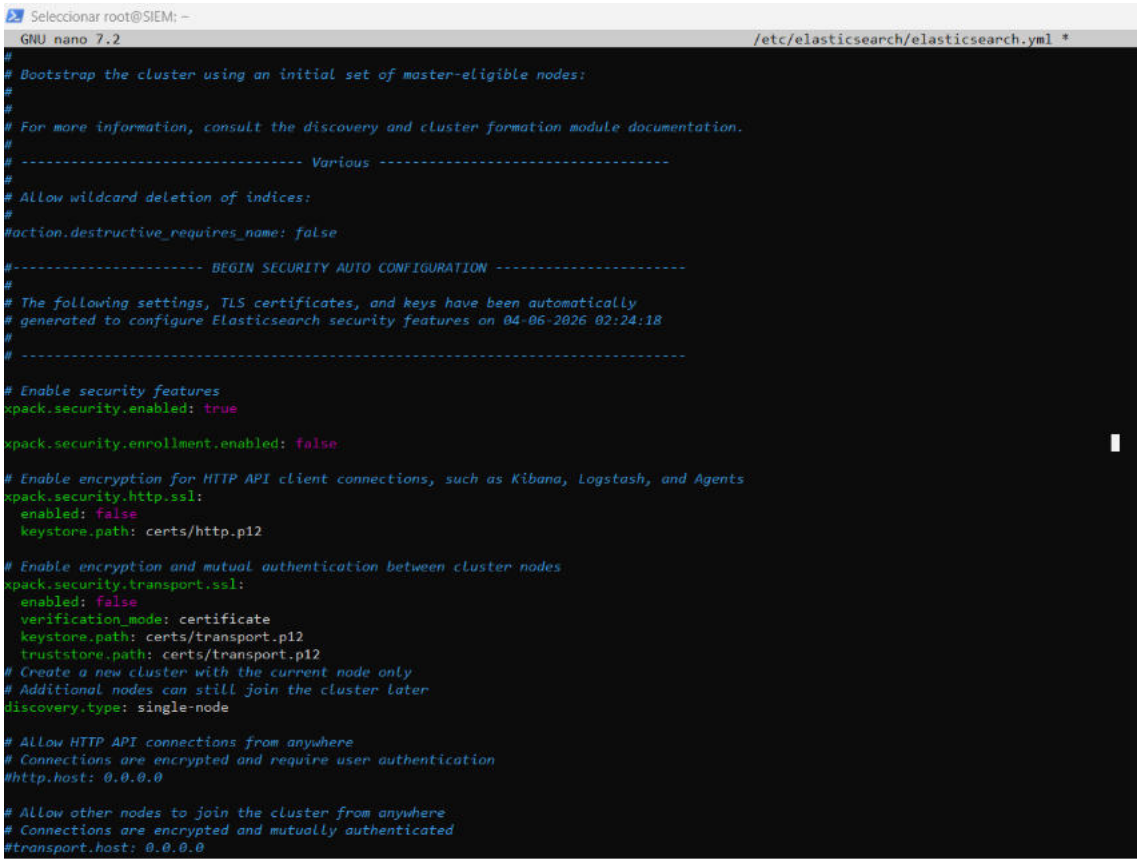


Nota: Elaboración propia

Configuración de usuarios internos.

La figura presenta la configuración de los usuarios internos de Elastic Security utilizados para la administración del SIEM. La asignación de roles y privilegios permite controlar el acceso a las funciones de monitoreo, administración y gestión de alertas, garantizando el cumplimiento del principio de mínimo privilegio dentro de la plataforma.

Figura 46
Configuración de usuarios internos

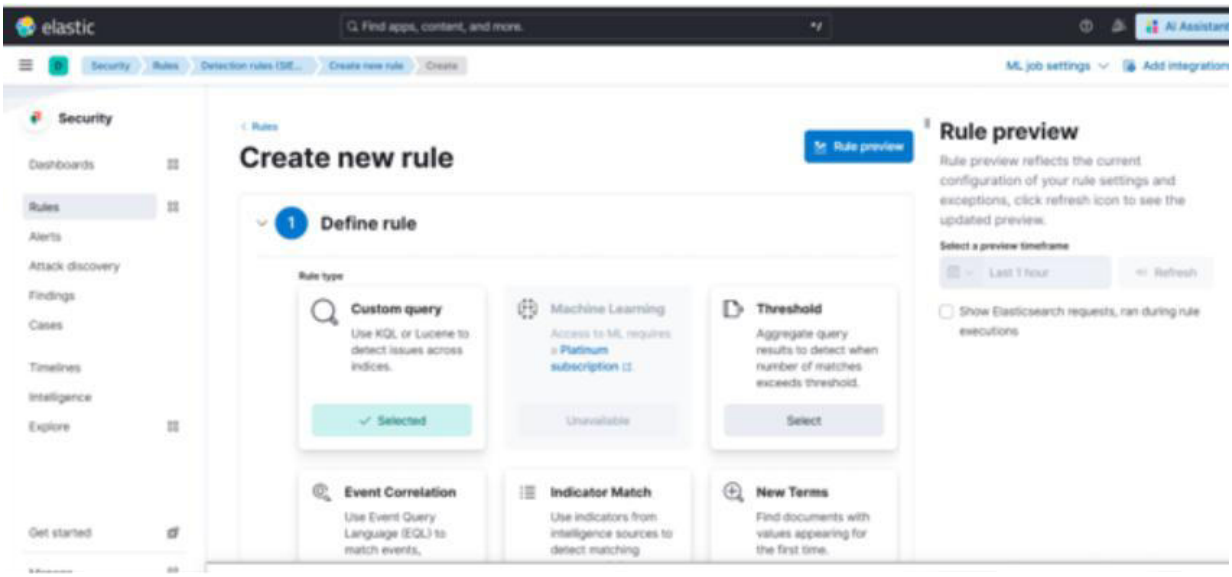


Nota: Elaboración propia

Creación de la regla, correlación y alertas

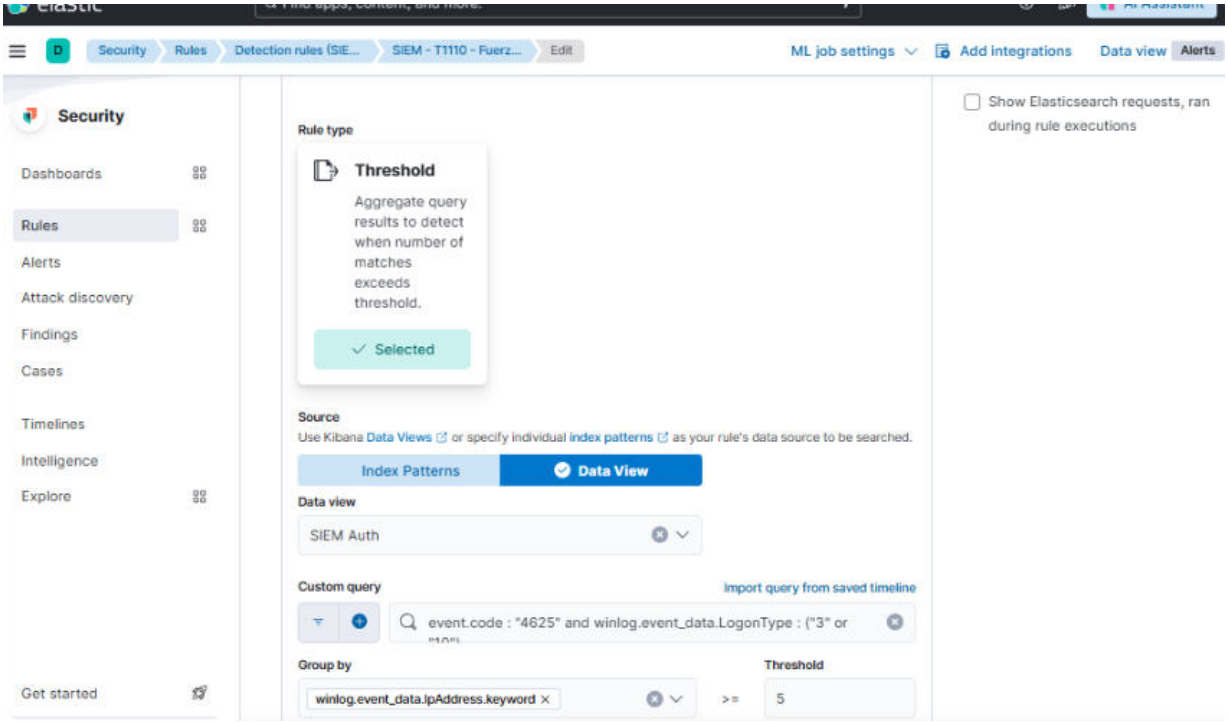
En esta etapa se configura la regla de correlación SIEM – T1110 – Fuerza Bruta SSH, utilizando una regla de tipo Threshold. Se define la consulta KQL para identificar eventos de autenticación fallida provenientes del servicio SSH y se establece un umbral mínimo de cinco eventos originados desde una misma dirección IP dentro del intervalo de análisis. Cuando dicha condición se cumple, Elastic Security genera automáticamente una alerta de seguridad asociada a la técnica T1110 – Password Guessing del framework MITRE ATT&CK.

Figura 47
Interfaz de creación de nueva regla



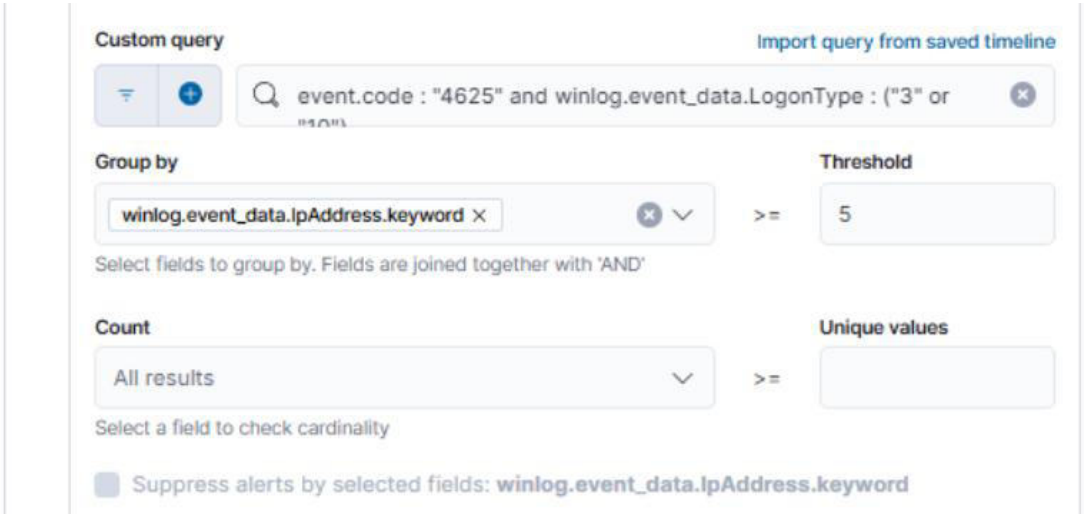
Nota: Elaboración propia

Figura 48
Configuración de caso de uso o regla



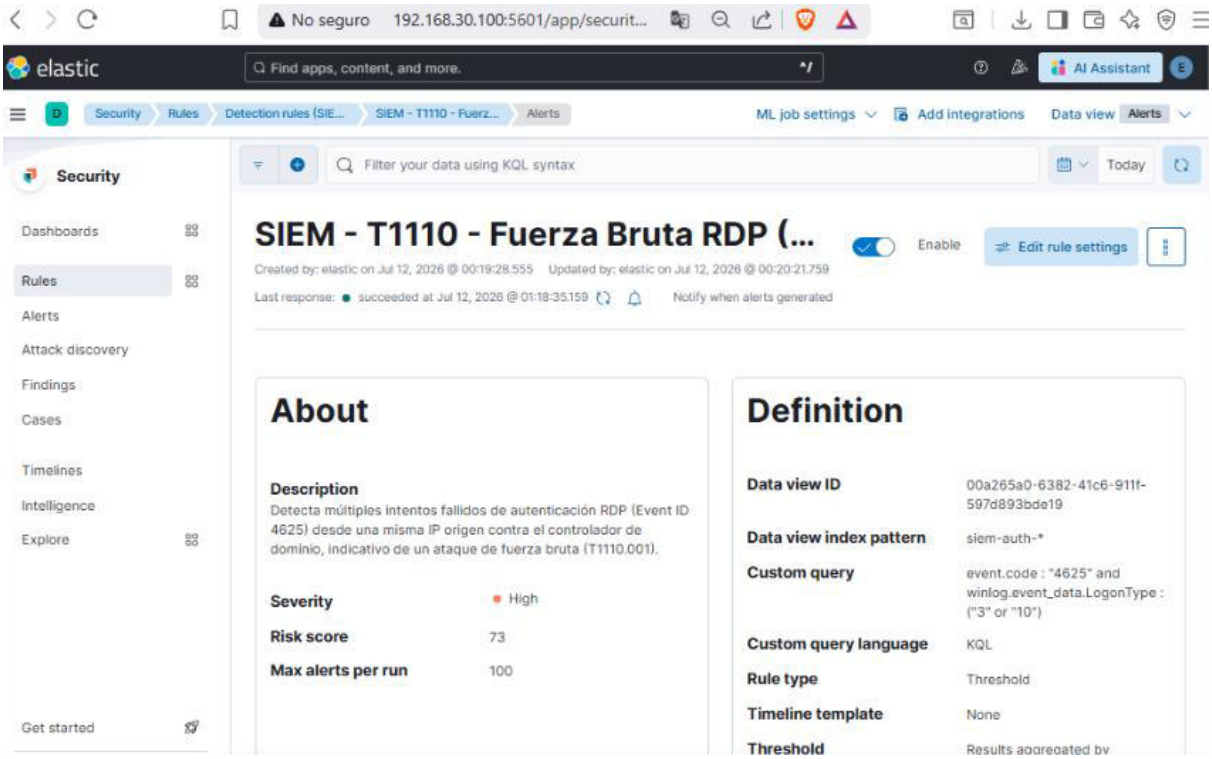
Nota: Elaboración propia

Figura 49
Caso de uso implementado



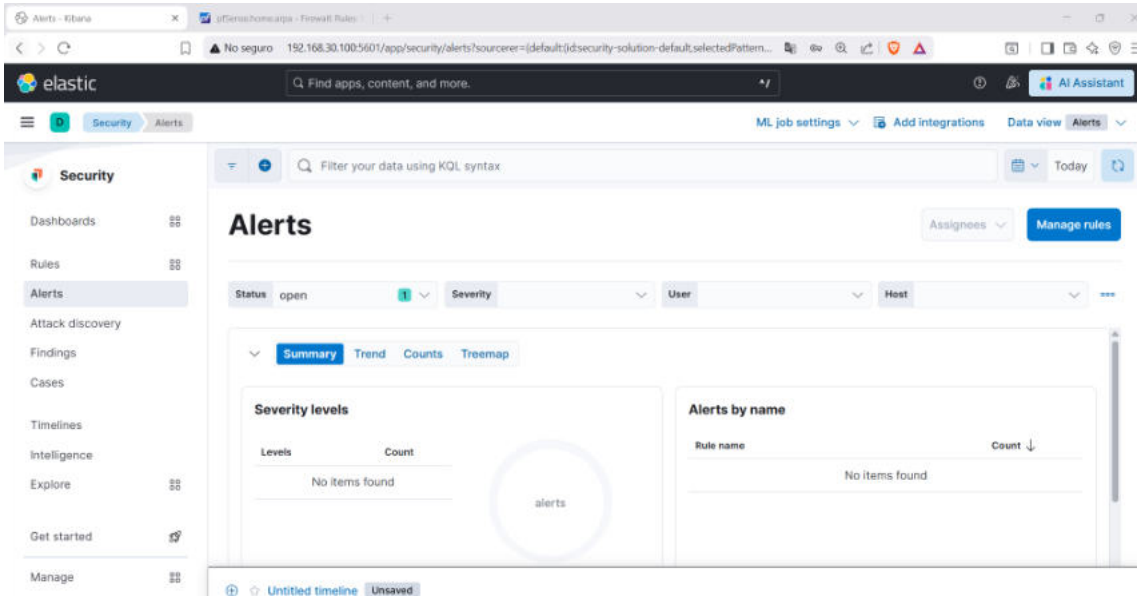
Nota: Elaboración propia

Figura 50
Caso de uso: T1110 Fuerza bruta



Nota: Elaboración propia

Figura 51
Alerta generada

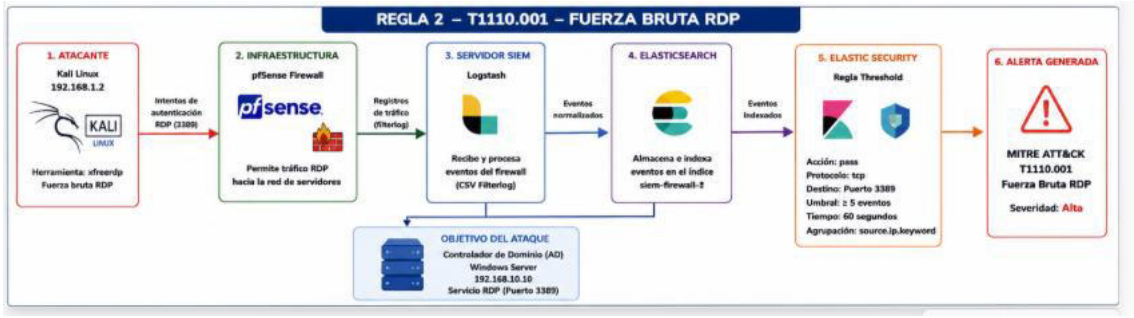


Nota: Elaboración propia

Escenario 2 – T1110 Fuerza Bruta RDP (Windows Server AD)

Escenario de ataque

Figura 52
Escenario de ataque propuesto



Nota: Elaboración propia

Esta regla está diseñada para detectar intentos de fuerza bruta mediante el protocolo RDP (Remote Desktop Protocol) contra un Controlador de Dominio de Windows, utilizando los eventos registrados en el log de seguridad de Windows.

La regla monitorea el Evento de Seguridad 4625, que corresponde a:

Event ID 4625: An account failed to log on (Error de inicio de sesión).

Posteriormente verifica que:

El tipo de inicio de sesión (LogonType) sea:

10: Inicio de sesión remoto mediante RDP (Remote Desktop Services).

3: Inicio de sesión por red (incluido en algunos escenarios donde intervienen servicios de autenticación o recursos compartidos).

Finalmente cuenta los eventos provenientes de una misma dirección IP.

Es decir:

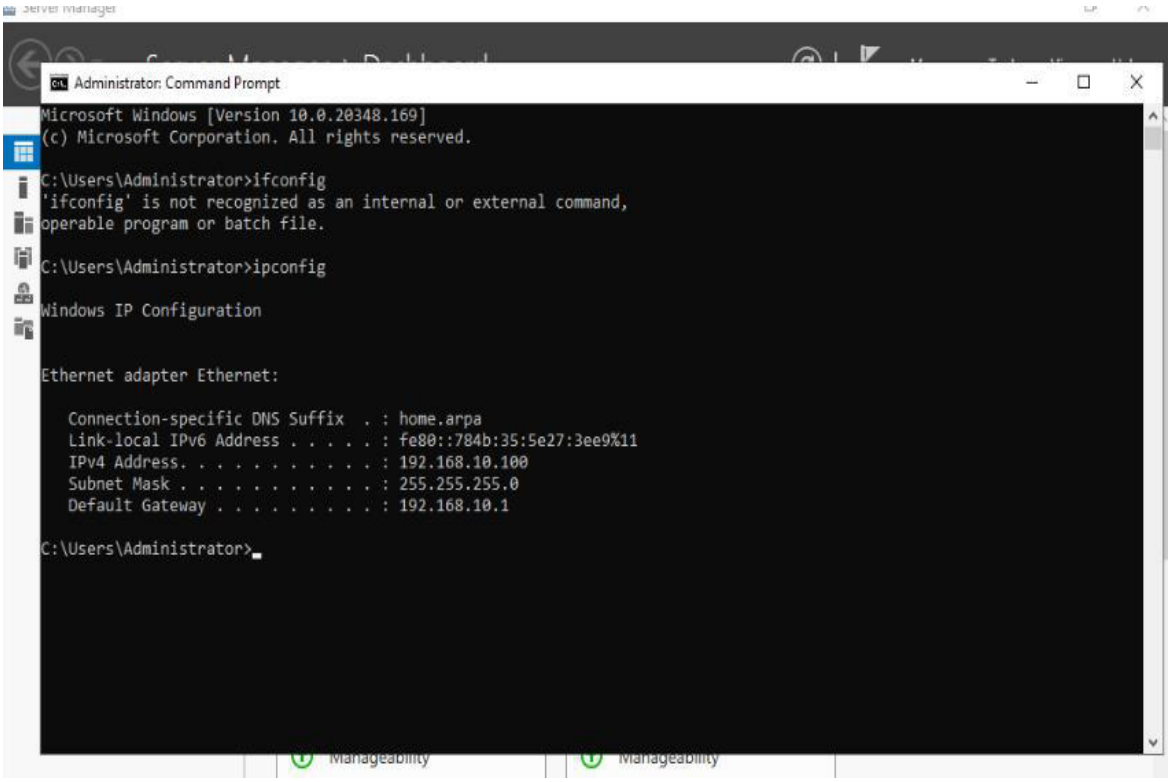
Si una misma dirección IP genera 5 o más eventos 4625 en un período de 60 segundos, la regla genera una alerta.

Verificación de sincronización de reloj.

Se verifica la IP del servidor AD.

La figura muestra la verificación de la configuración de red del servidor Windows Server que cumple la función de Controlador de Dominio. En esta etapa se confirma la dirección IP asignada al servidor, la cual será utilizada posteriormente como destino del ataque de fuerza bruta mediante el protocolo RDP.

Figura 53
Verificación de IP del servidor AD

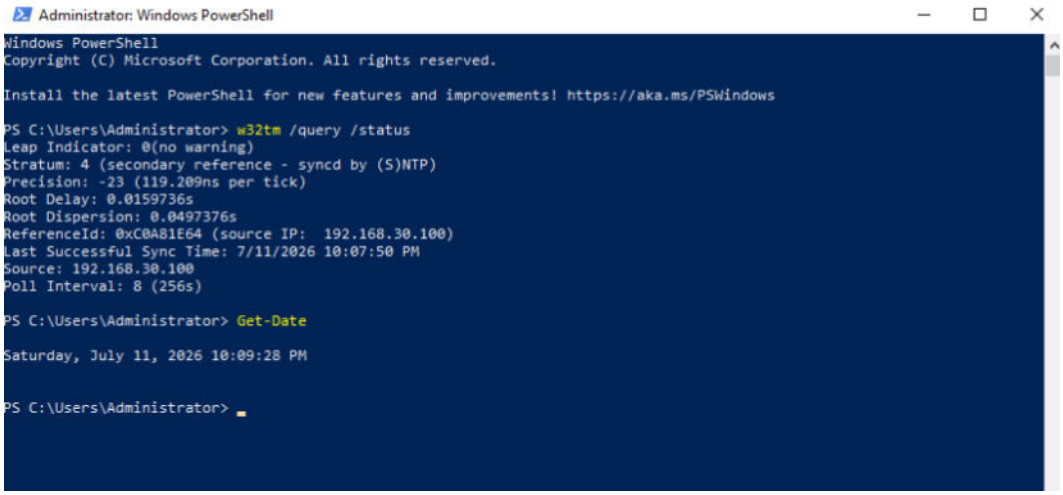


Nota: Elaboración propia

Verificación de la sincronización horaria.

La figura presenta la comprobación de la sincronización del reloj entre el servidor Active Directory y la infraestructura SIEM mediante el servicio NTP. Mantener una hora sincronizada es indispensable para asegurar la correcta correlación temporal de los eventos registrados por Windows, Filebeat, Logstash y Elasticsearch, permitiendo que las alertas reflejen con precisión la secuencia real del ataque.

Figura 54
Verificación del servicio NTP del servidor AD

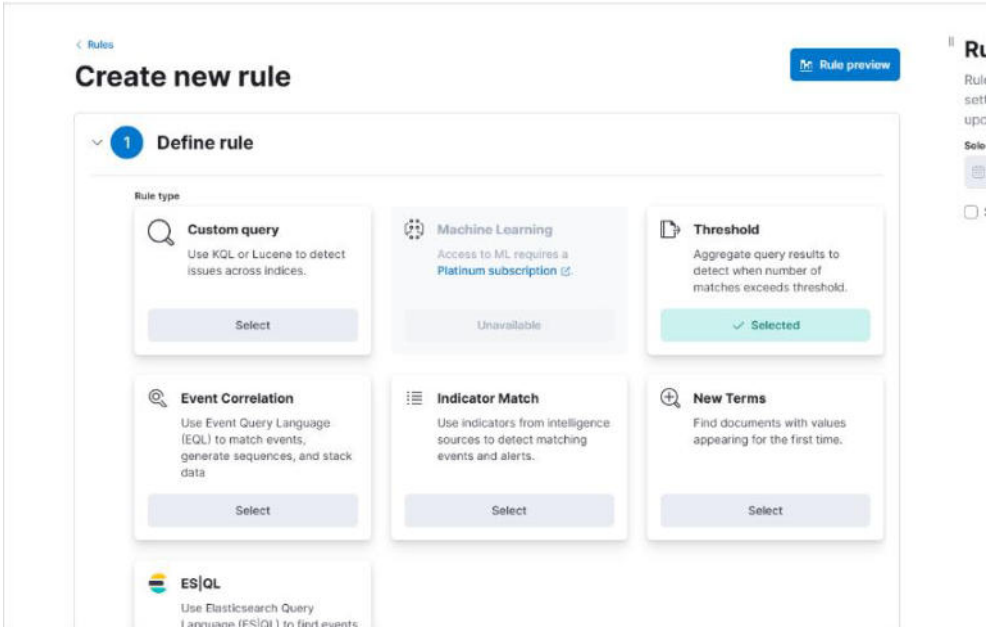


Nota: Elaboración propia

Creación de la regla

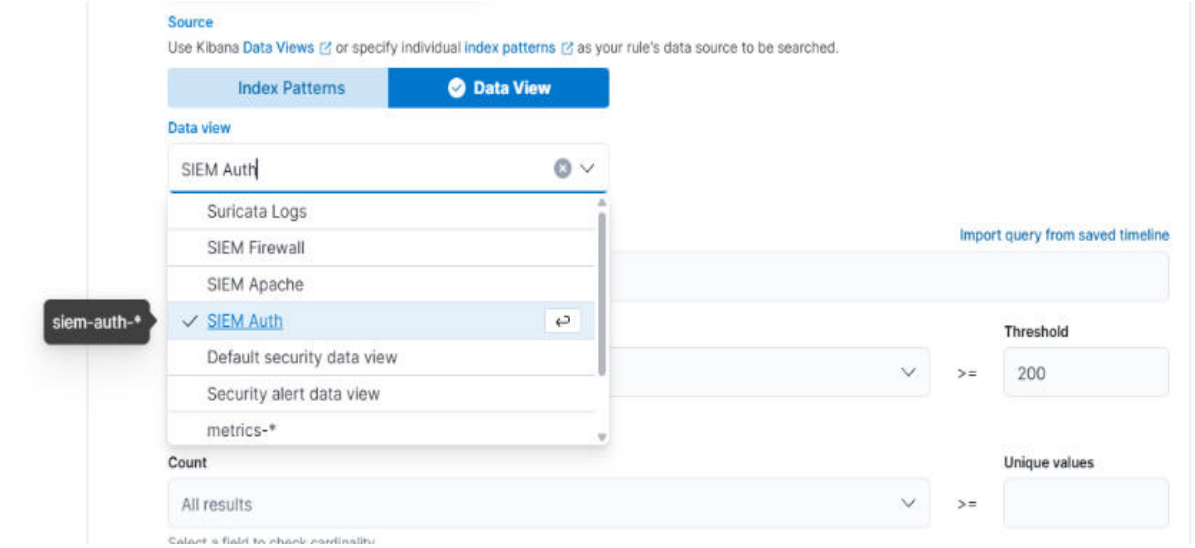
La figura muestra la configuración del parámetro Threshold, utilizado para establecer el número mínimo de intentos fallidos de autenticación necesarios para generar una alerta. En este caso se definió un umbral de cinco eventos dentro de un intervalo de sesenta segundos, permitiendo identificar comportamientos compatibles con ataques de fuerza bruta sin generar alertas por errores aislados de autenticación.

Figura 55
Interfaz de creación de regla



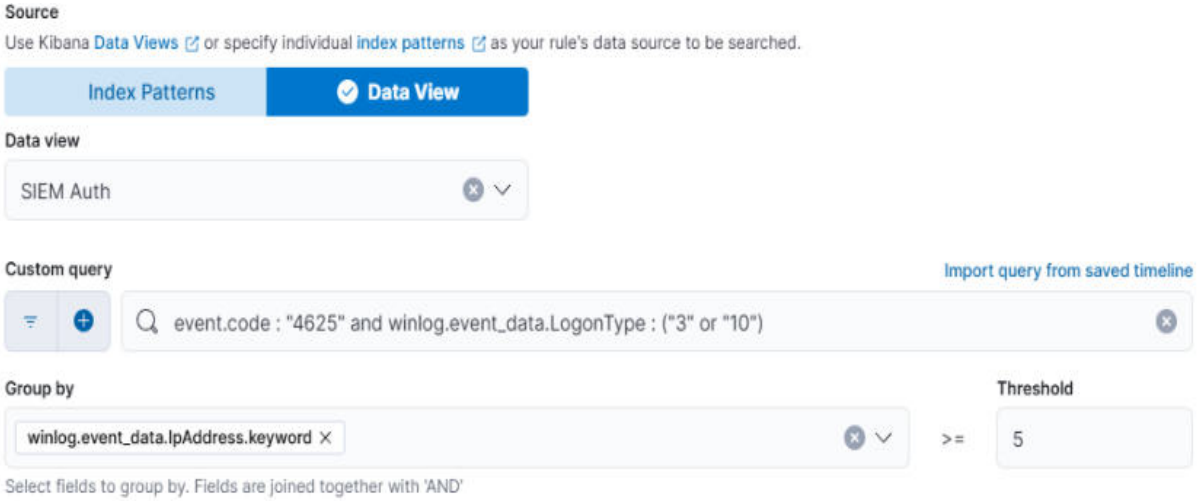
Nota: Elaboración propia

Figura 56
Configurando los datos de regla



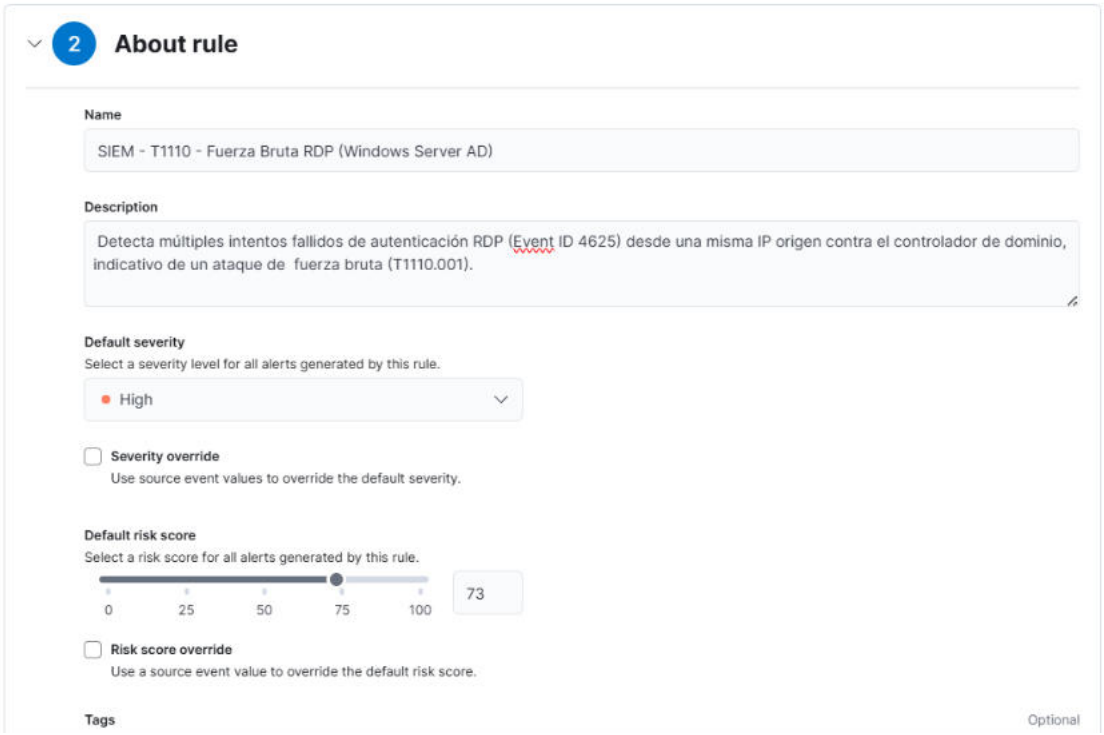
Nota: Elaboración propia

Figura 57
Ingreso del caso de uso o regla de detección



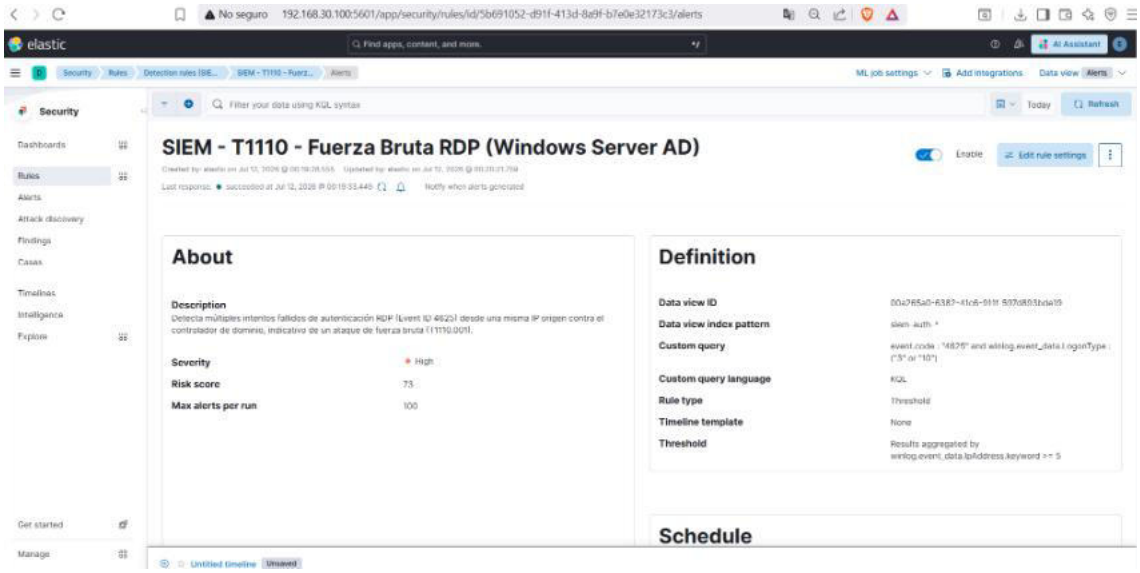
Nota: Elaboración propia

Figura 58
Configuración de alertamiento de la regla de detección



Nota: Elaboración propia

Figura 59
Regla de detección creada



Nota: Elaboración propia

Escenario de ataque: Fuerza bruta RDP

Verificación de conexión ping, y puerto RDP desde el host ataque al servidor victima AD

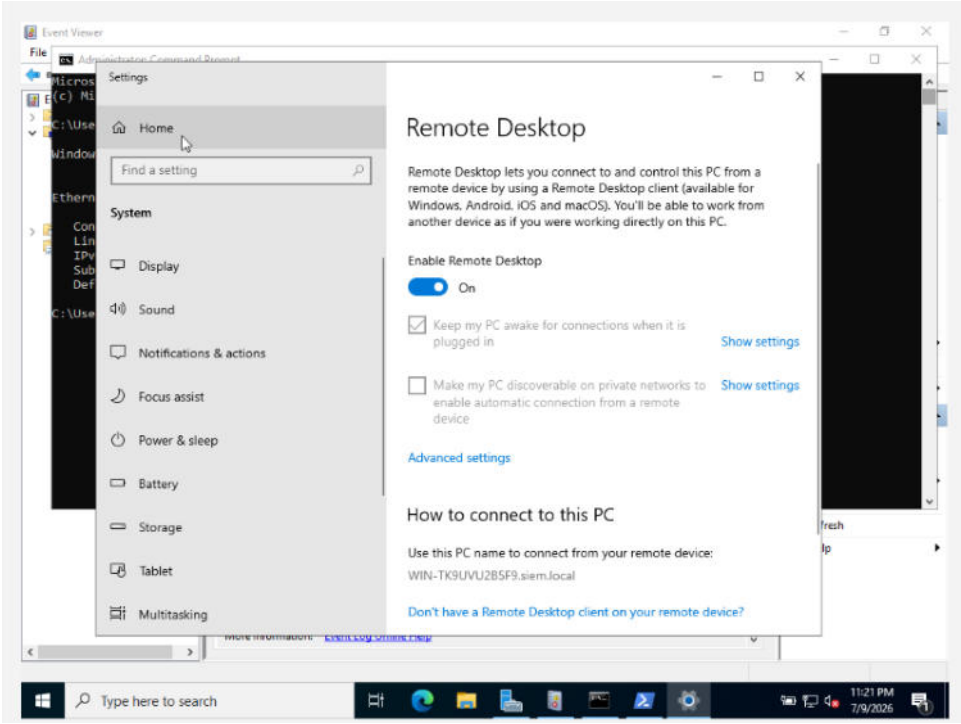
La Figura presenta la primera prueba de conectividad realizada desde el equipo atacante Kali Linux hacia el servidor Windows Server Active Directory. Durante esta etapa no fue posible establecer comunicación mediante el protocolo ICMP ni acceder al servicio RDP, evidenciando problemas de configuración en la infraestructura de red que debían ser corregidos antes de iniciar las pruebas de detección.

Figura 60
Ataque de fuerza bruta ejecutada desde kali

Nota: Elaboración propia

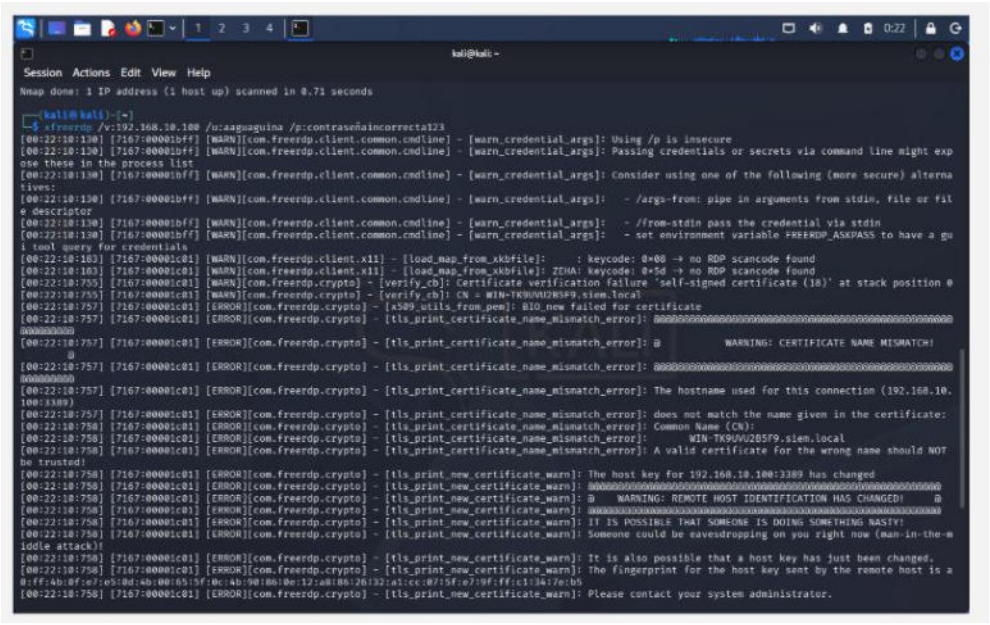
En esta figura se observa el primer intento de acceso remoto al servidor Active Directory utilizando el protocolo Remote Desktop Protocol (RDP). La conexión fue rechazada debido a que el servicio aún no se encontraba habilitado, permitiendo identificar la necesidad de ajustar la configuración del servidor para continuar con las pruebas experimentales.

Figura 61
Habilitación del protocolo RDP en el servidor



Nota: Elaboración propia

Figura 62
Primer intento de conexión fallido



Nota: Elaboración propia

Lanzamos el ataque

Esto va a intentar 8 conexiones RDP con contraseñas incorrectas.

```
date -u
for i in {1..8}; do
 timeout 5 xfreerdp /v:192.168.10.100 /u:aaguaguina /p:wrongpass$i /cert:ignore 2>/dev/null
done
date -u
```

El script ejecuta ocho intentos consecutivos de autenticación utilizando el cliente xfreerdp con contraseñas incorrectas, limitando cada conexión a cinco segundos y registrando la hora de inicio y finalización del procedimiento. Como resultado, el servidor genera múltiples eventos 4625 (Failed Logon), los cuales son recopilados por la infraestructura SIEM para validar el funcionamiento de la regla Sigma encargada de detectar ataques de fuerza bruta sobre el servicio de Escritorio Remoto.

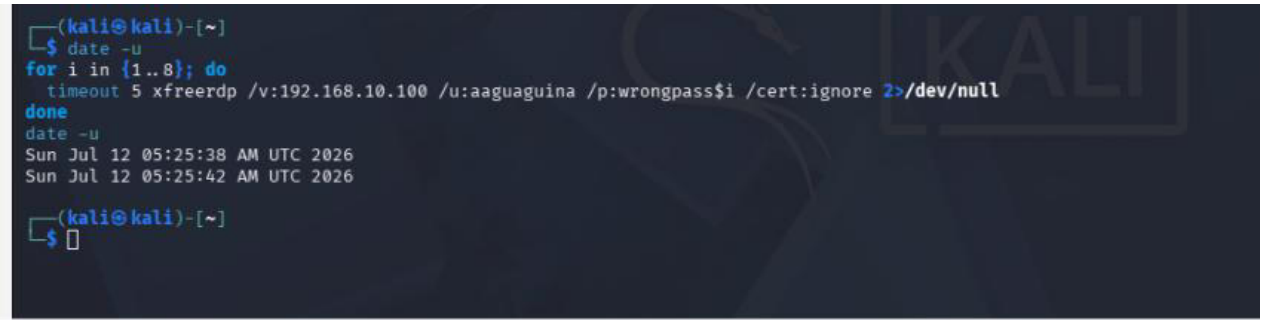
Tabla 13
Detalle de los parámetos usados en el comando correspondiente

Comando	**Descripción**
date -u	Este comando muestra la fecha y hora actual en formato **UTC.**
for i in {1..8}; do	Esta instrucción crea un ciclo que se ejecutará **ocho veces**.
timeout 5	Limita la duración de cada intento de conexión a **cinco segundos**.
xfreerdp	Es el cliente de **Remote Desktop Protocol (RDP)** utilizado en Linux para conectarse a equipos Windows.
/v:192.168.10.100	Indica la dirección IP del servidor Windows que recibirá los intentos de autenticación.
/u:aaguaguina	Especifica la cuenta de usuario contra la cual se intentará iniciar sesión.
/p:wrongpass$i	Define la contraseña utilizada en cada intento.
/cert:ignore	Indica a FreeRDP que ignore advertencias relacionadas con certificados TLS.
2>/dev/null	Redirige los mensajes de error hacia **/dev/null**, evitando que aparezcan en la consola.
done	Finaliza el bucle después de completar los ocho intentos de autenticación.

Comando	Descripción
date -u	Registra la hora exacta en la que termina la ejecución del script.

Nota: Elaboración propia

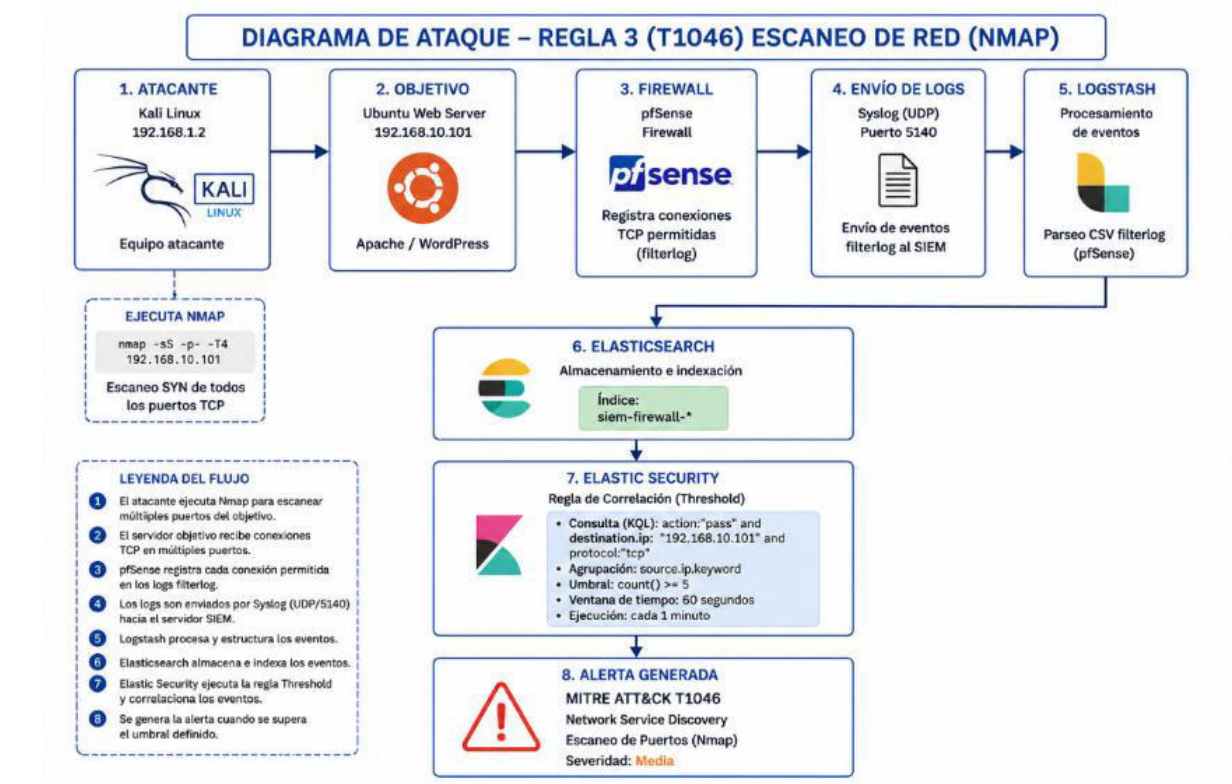
Figura 63
Script usado para la prueba



Nota: Elaboración propia

Escenario 3 - T1046 Escaneo de Red (Nmap)

Figura 64
Escenario T1046 Escaneo de red

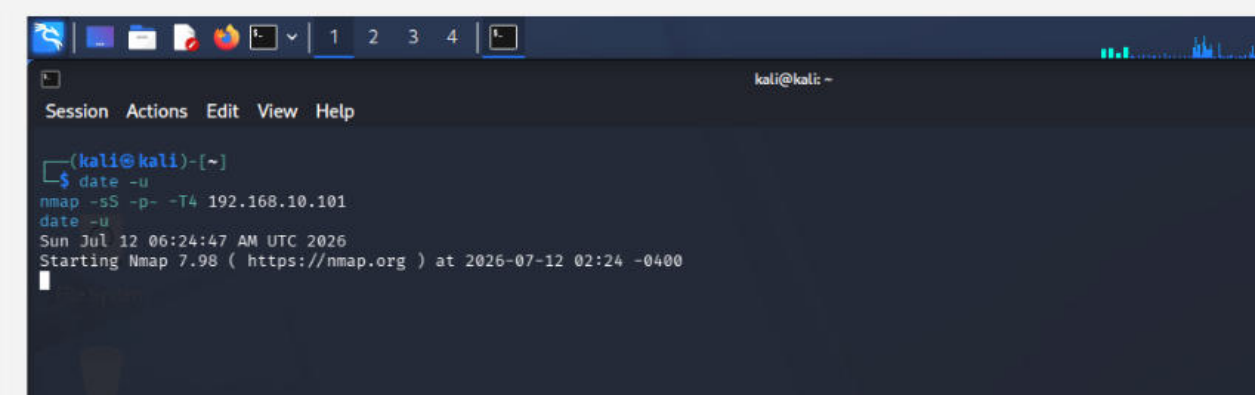


Nota: Elaboración propia

Se realiza un análisis de logs para luego lanzar el escaneo propuesto.

```
date -u
nmap -sS -p- -T4 192.168.10.101
date -u
```

Figura 65
Prueba de escaneo de red con Nmap



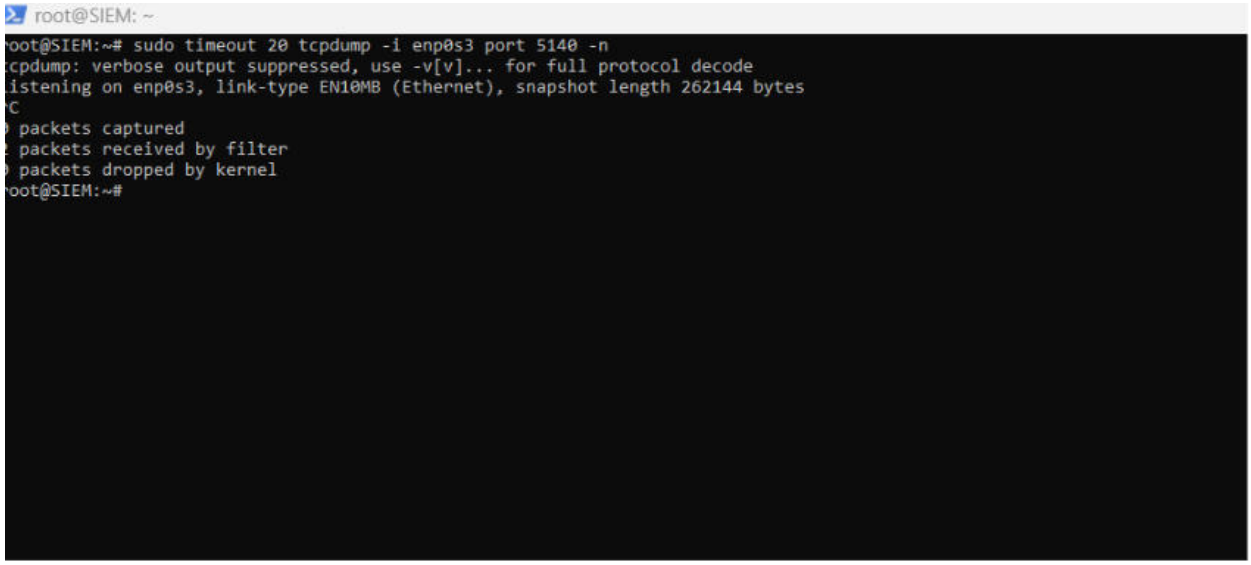
Nota: Elaboración propia

Prueba1 fallida sin registros en SIEM.

Captura de paquetes en el SIEM en el puerto 5140 perdidos.

La figura presenta el resultado de la primera ejecución del escaneo de puertos. Aunque el ataque fue ejecutado correctamente desde la máquina atacante, no se registraron eventos dentro del SIEM debido a que los mensajes Syslog provenientes del firewall pfSense no estaban siendo recibidos por el servidor de monitoreo. Esta situación permitió identificar un problema en la comunicación entre el firewall y la plataforma SIEM que debía corregirse antes de continuar con las pruebas.

Figura 66
Paquetes perdidos en la prueba inicial

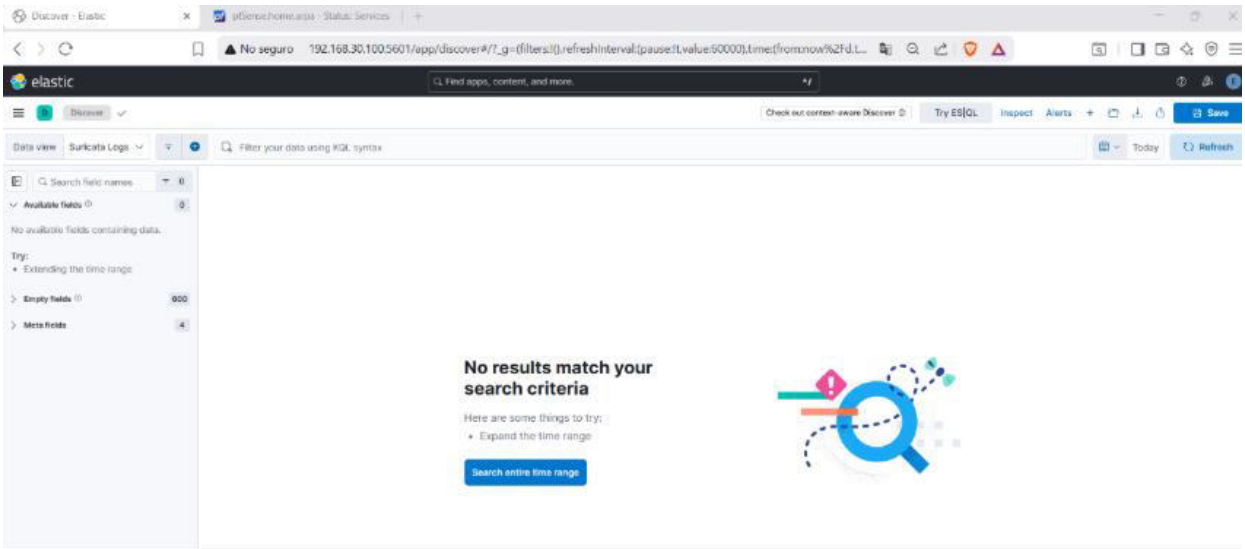


Nota: Elaboración propia

Detalle de registro de paquetes en el siem.

La figura muestra la captura de tráfico realizada sobre el puerto 5140, utilizado para recibir los mensajes Syslog enviados por pfSense. Durante esta verificación se comprobó que los paquetes no llegaban correctamente al servidor SIEM, confirmando que la ausencia de eventos no era causada por la regla de correlación sino por un problema en el proceso de envío de registros desde el firewall.

Figura 67
Fallo en la captura de logs en pfsense

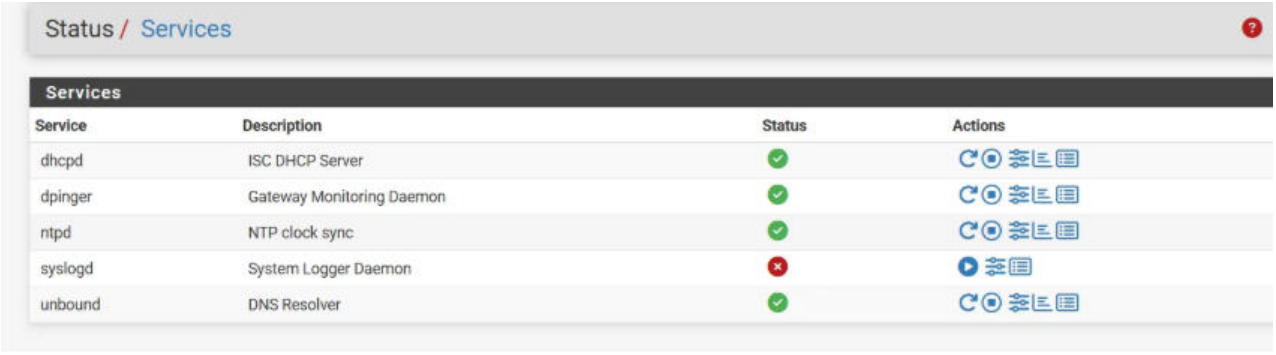


Nota: Elaboración propia

Revisión de la configuración del firewall

La figura presenta la revisión de la configuración del firewall pfSense después de detectar la ausencia de eventos en el SIEM. Durante esta actividad se verificaron los parámetros relacionados con el servicio de registro remoto (Remote Logging), identificando que el servicio Syslog no estaba enviando correctamente los registros hacia el servidor SIEM.

Figura 68
Revisión de la configuración en pfSense

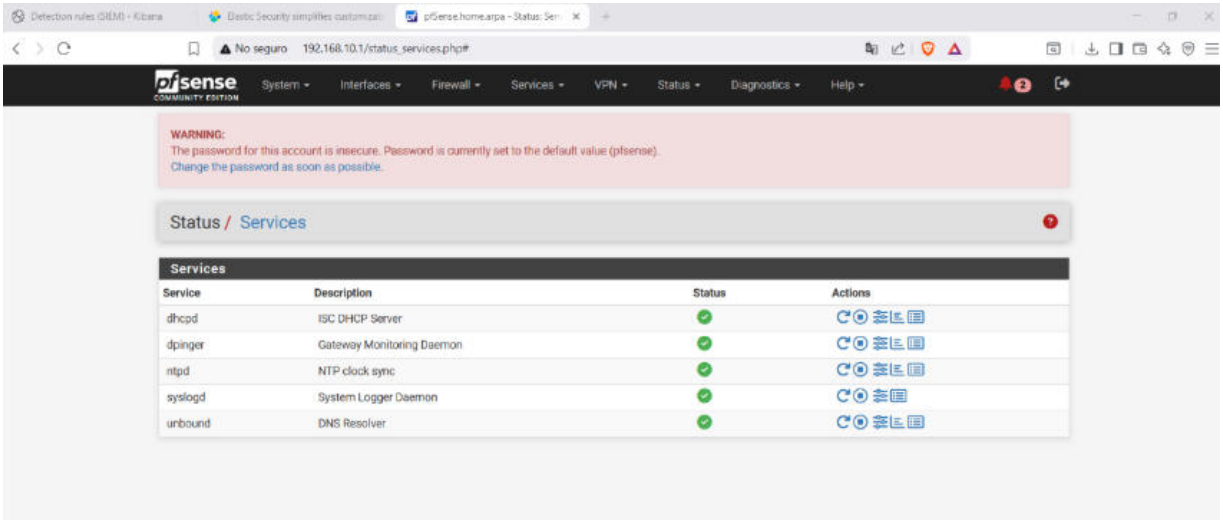


Nota: Elaboración propia

Corrección y activación de syslogd

La figura muestra la habilitación del servicio syslogd en pfSense para permitir el envío de los registros del firewall hacia Logstash. Una vez activado el servicio, los eventos comenzaron a transmitirse correctamente, restableciendo el flujo de información necesario para el funcionamiento de la plataforma SIEM.

Figura 69
Habilitación del servicio syslogd en pfSense

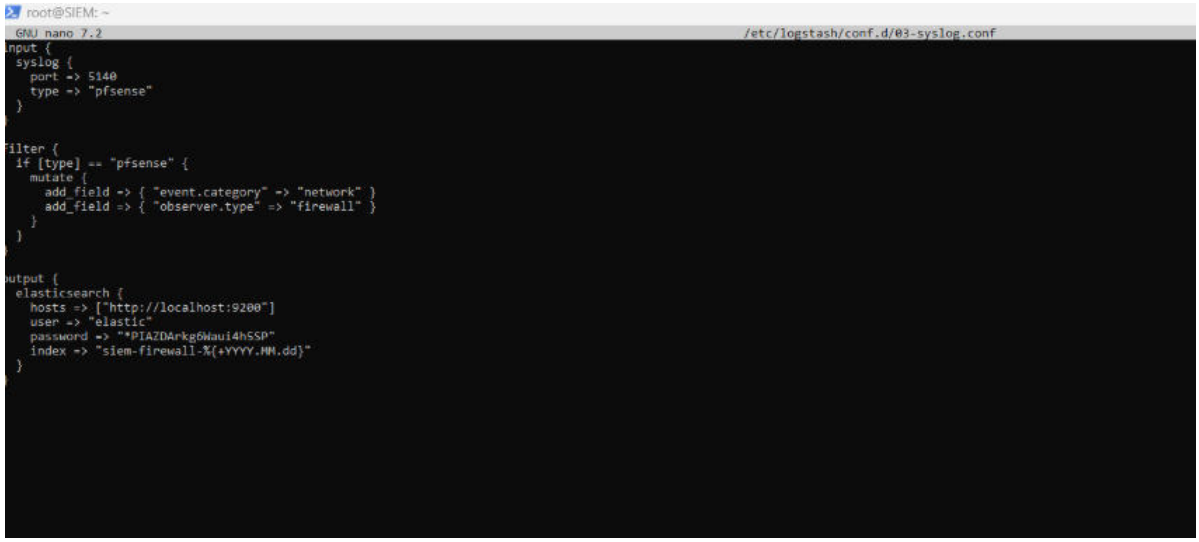


Nota: Elaboración propia

Corrección de formato de eventos.

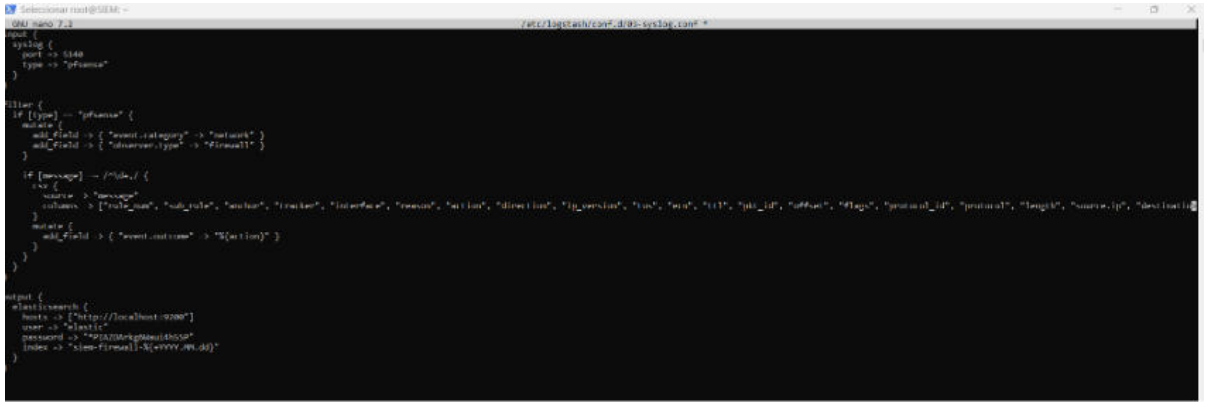
La figura presenta la modificación realizada en el pipeline de procesamiento de Logstash para corregir el formato de los eventos recibidos desde pfSense. Esta corrección permitió extraer adecuadamente campos como la dirección IP de origen, dirección IP de destino, protocolo, puertos y acción del firewall, información indispensable para que la regla de correlación pudiera evaluar correctamente los registros recibidos.

Figura 70
Modificación en el formato de eventos



Nota: Elaboración propia

Figura 71
Caso Corregido

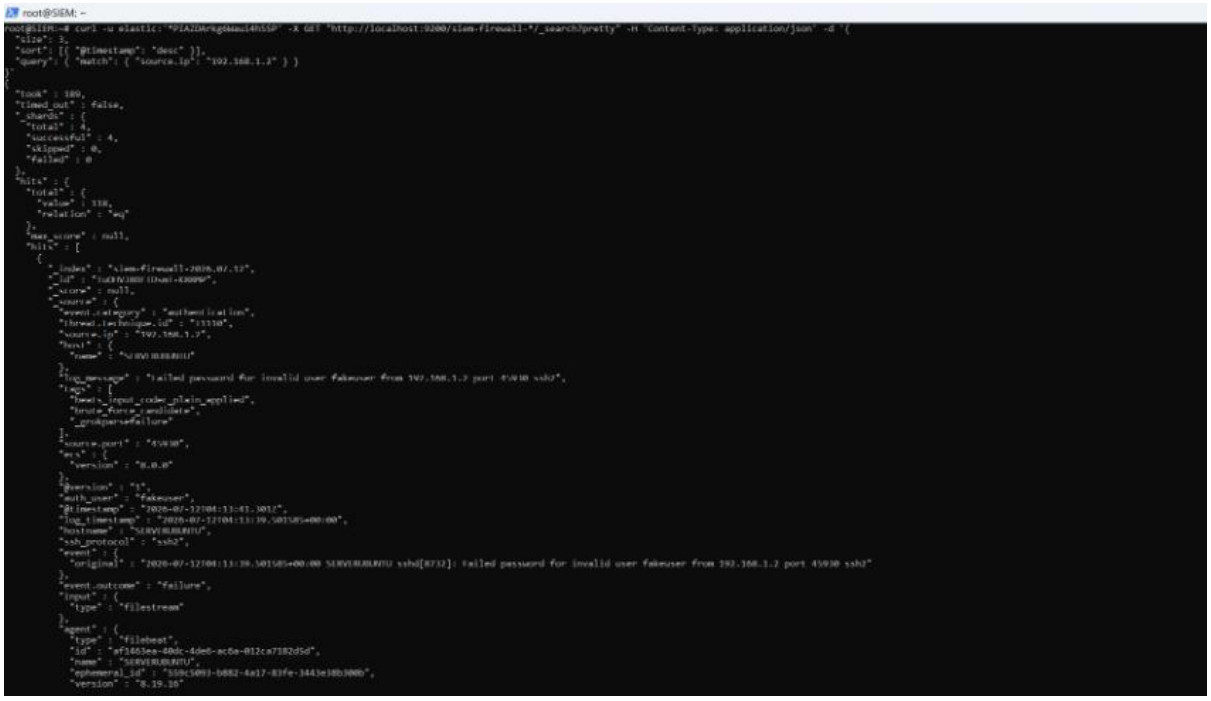


Nota: Elaboración propia

Reiniciamos los servicios y generamos el nuevo ataque.

La figura muestra el reinicio de los servicios de la infraestructura SIEM después de aplicar las correcciones realizadas tanto en el firewall como en el procesamiento de eventos. Esta acción garantiza que la nueva configuración sea aplicada correctamente antes de repetir el escenario de ataque y validar nuevamente la detección.

Figura 72
Reinicio de servicios del SIEM

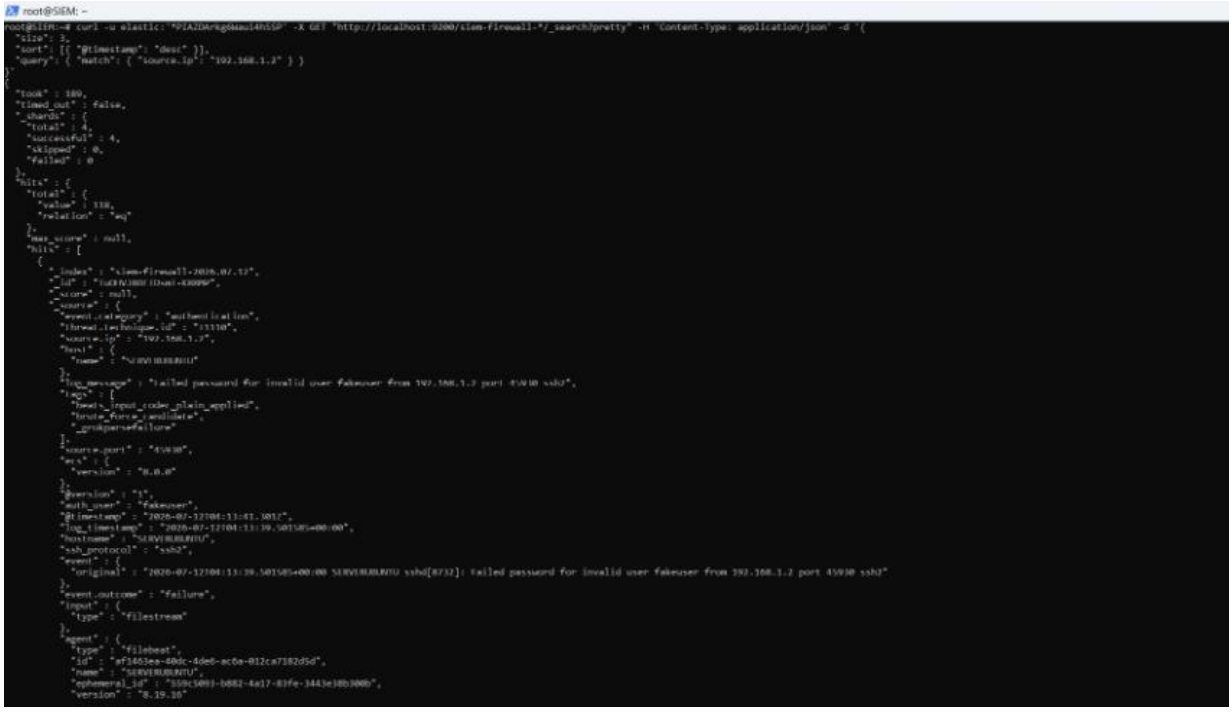


Nota: Elaboración propia

Verificamos elasticc search

La figura presenta la comprobación del funcionamiento de Elasticsearch mediante la consulta de los índices donde se almacenan los eventos provenientes del firewall.

Figura 73
Comprobación de elastic search

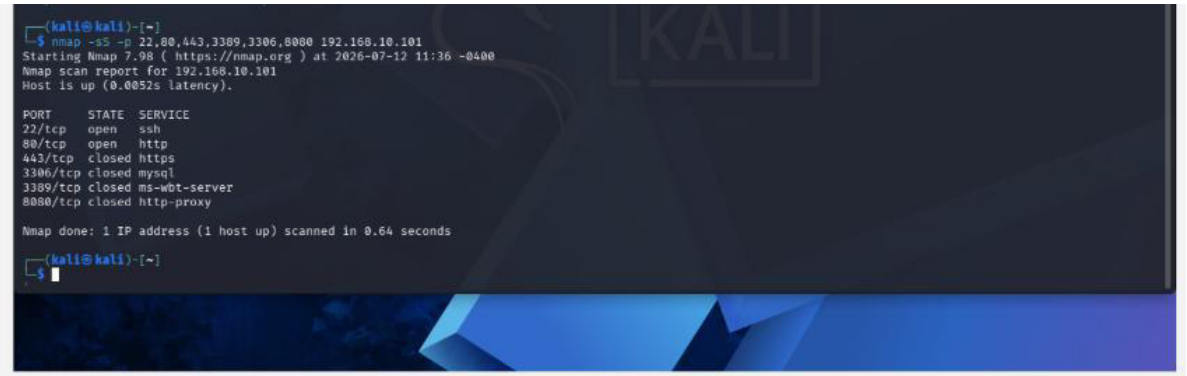


Nota: Elaboración propia

Generamos el ataque

La figura muestra la repetición del ataque de reconocimiento mediante Nmap una vez corregidos los problemas detectados en la infraestructura. Durante esta segunda ejecución los registros fueron enviados correctamente desde pfSense hacia Logstash, indexados en Elasticsearch y puestos a disposición de Elastic Security para su análisis.

Figura 74
Generación de ataque desde kali



Nota: Elaboración propia

Escenario 4 - T1190 Inyección SQL (sqlmap)

Implementación del filtro en Logstash

La figura muestra el archivo 02-apache.conf utilizado en Logstash para procesar los registros provenientes del servidor Apache. Mediante expresiones regulares se identifican patrones característicos de inyección SQL, tales como UNION, SELECT, INSERT, DROP, OR 1=1, comentarios SQL y comillas simples. Cuando alguno de estos patrones es detectado dentro de la URL solicitada, Logstash agrega automáticamente la etiqueta sql_injection_candidate, permitiendo posteriormente que la regla de correlación identifique el ataque.

El filtro de 02-apache.conf agrega el tag sql_injection_candidate de forma automática cuando la URL contiene los patrones union, select, insert, drop, or 1=1, -- o comillas simples, y mapea el hallazgo a la técnica T1190 de MITRE ATT&CK:

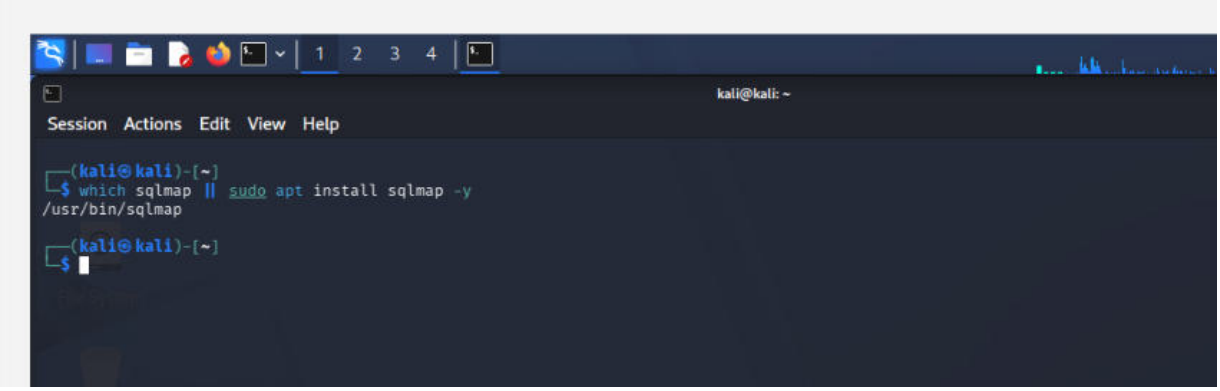
```
# Verificación de pipeline (Logstash 02-apache.conf)
$ cat /etc/logstash/conf.d/02-apache.conf
filter {
 if [module] == "apache" {
  grok { match => { "message" =>
   '%{IPORHOST:source_ip} - - \[%{HTTPDATE:timestamp}\]
    \"%{WORD:http_method} %{URIPATHPARAM:url_path}
    HTTP/%{NUMBER:http_version}\" %{NUMBER:response_code}
    %{NUMBER:response_bytes}' } }
  if [url_path] =~ "(?i)(union|select|insert|drop|or 1=1|--|')" {
   mutate { add_tag => ["sql_injection_candidate"] }
  }
```

```
 }
}
```

Preparación del escenario de ataque.

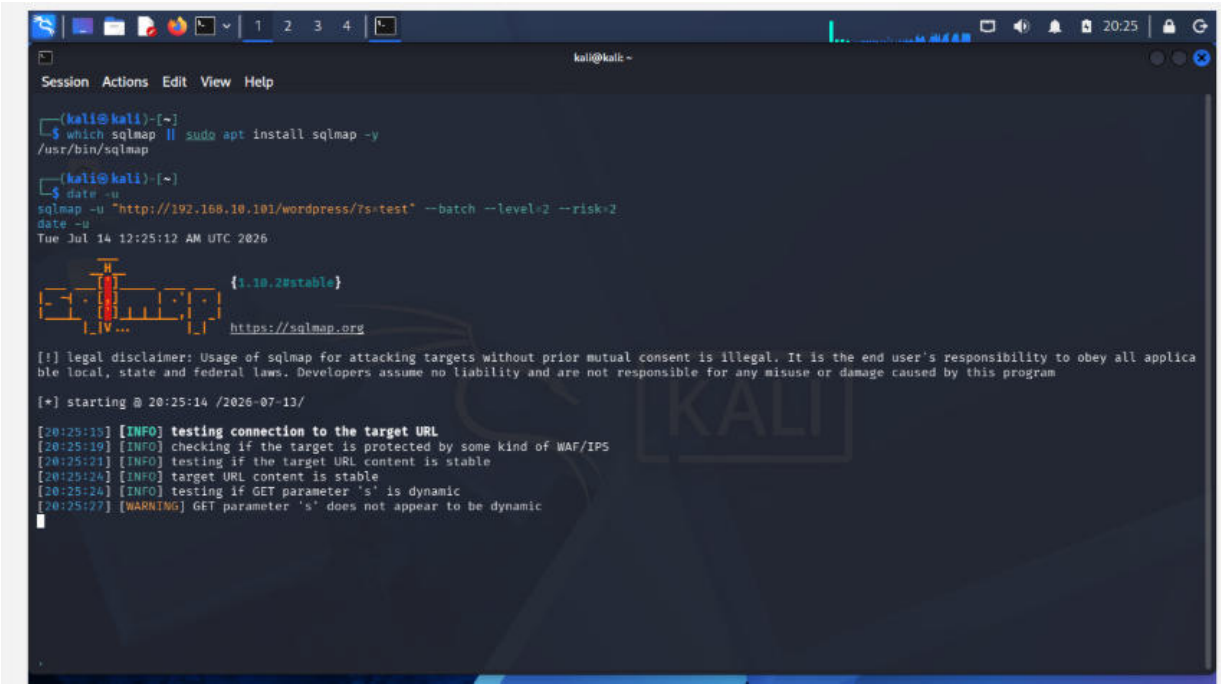
La figura presenta la preparación del entorno de pruebas previo a la ejecución del ataque. En esta etapa se verifica la disponibilidad del servidor Ubuntu Web, el funcionamiento del servicio Apache y del sitio WordPress que actuará como objetivo del ataque. Asimismo, se comprueba la conectividad entre la máquina atacante Kali Linux y el servidor web para garantizar que el escenario experimental se encuentre operativo antes de iniciar la validación de la regla.

Figura 75
Preparación del entorno de pruebas



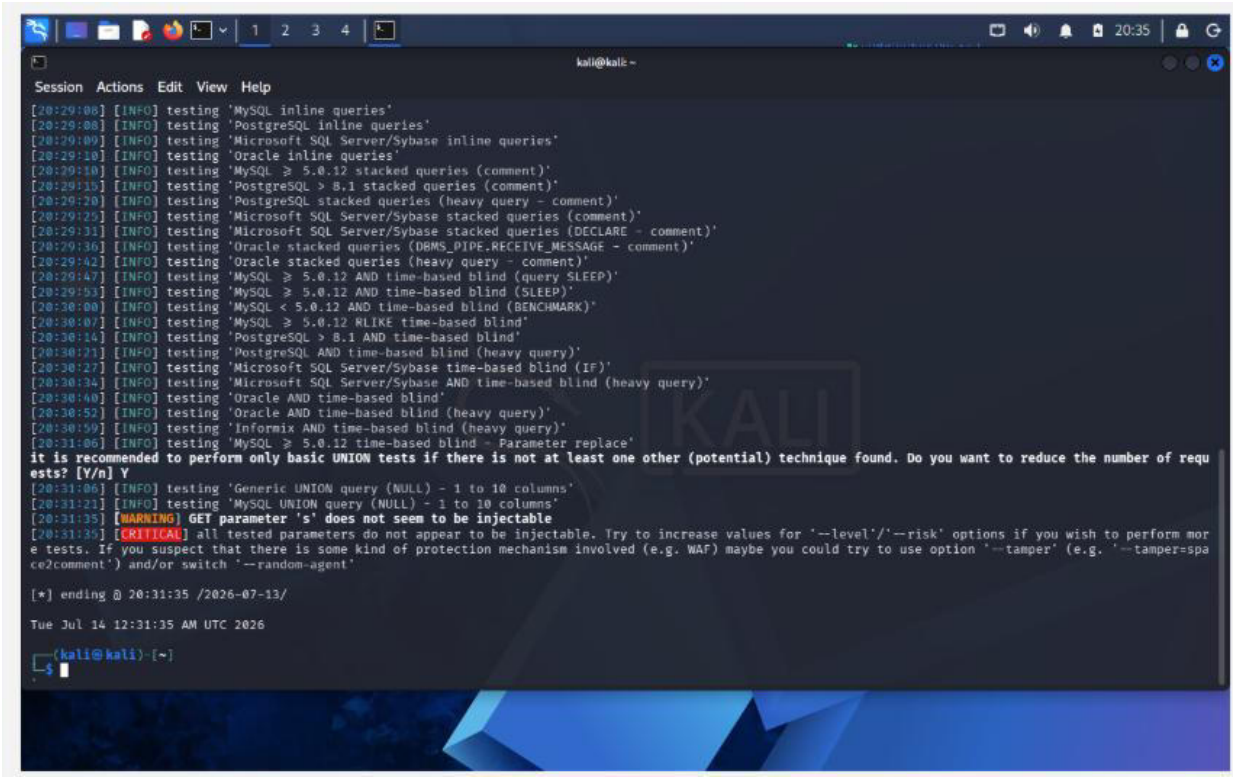
Nota: Elaboración propia

Figura 76
Preparación de SQLMap



Nota: Elaboración propia

Figura 77
Culminación del ataque con SQLMap

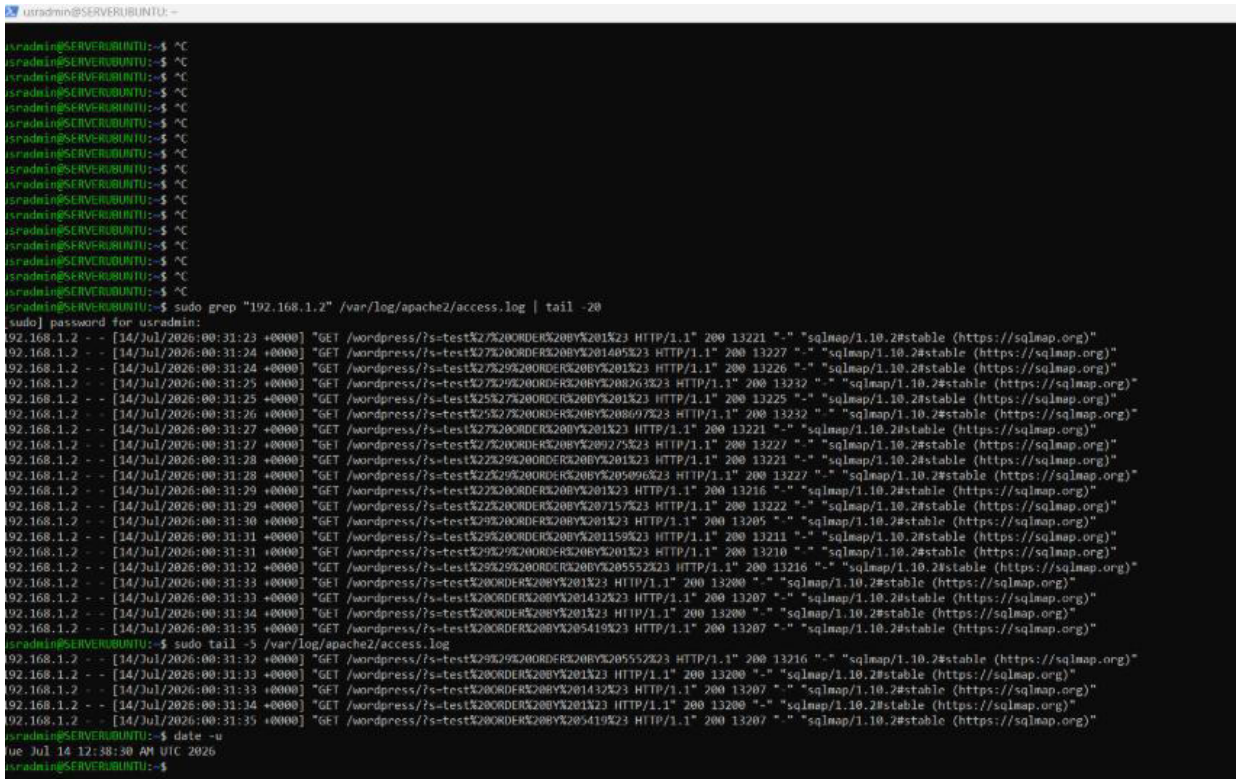


Nota: Elaboración propia

Registro de ataque en apache server

La figura muestra los registros generados por el servidor Apache durante la ejecución del ataque de inyección SQL. Cada solicitud HTTP enviada por la herramienta sqlmap queda registrada en el archivo de acceso del servidor, permitiendo observar la dirección IP de origen, la URL solicitada, el método HTTP utilizado y el código de respuesta generado por el servidor.

Figura 78
Registros generados por el servidor Apache durante la ejecución

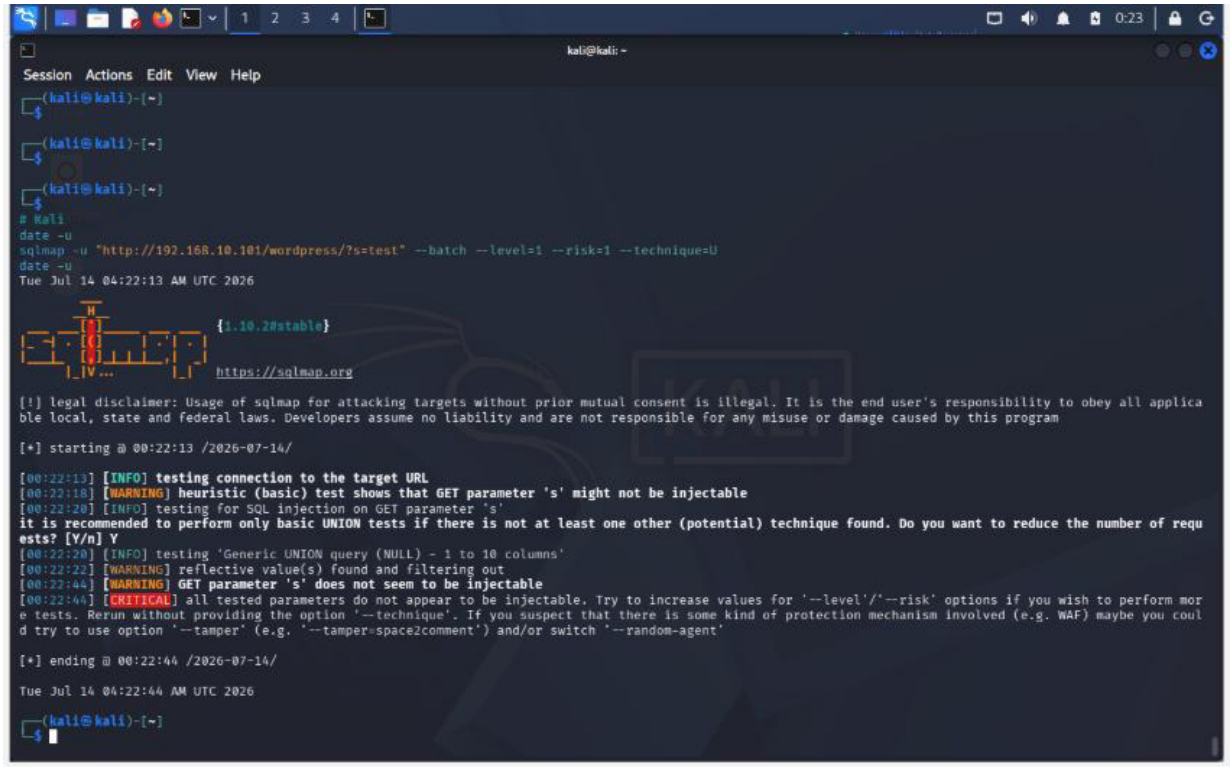


Nota: Elaboración propia

Ejecución del ataque mediante sqlmap

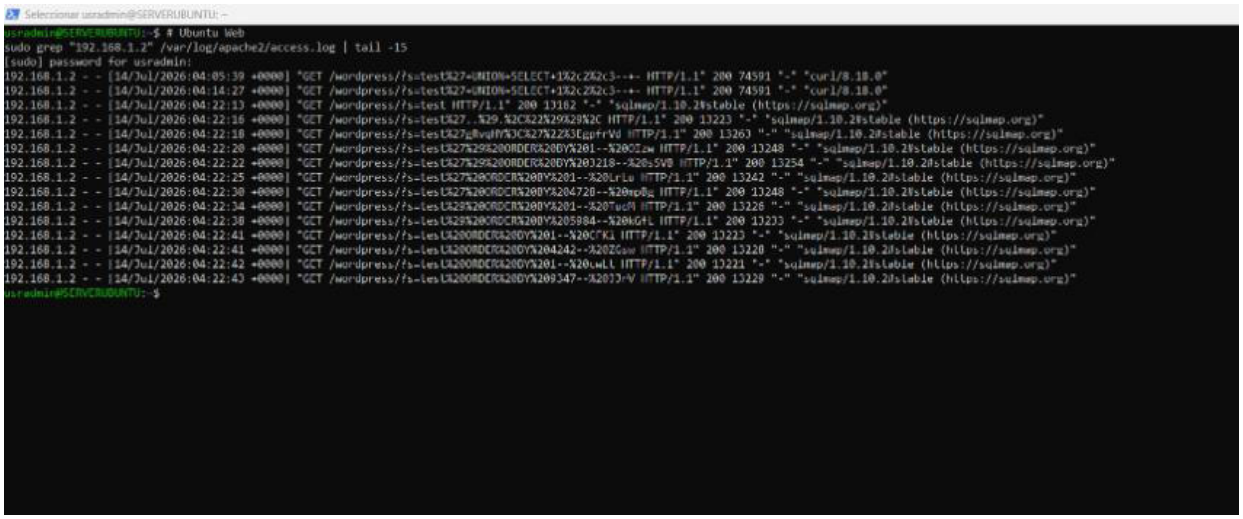
La figura presenta la ejecución del ataque desde la máquina Kali Linux utilizando la herramienta sqlmap contra el sitio WordPress alojado en el servidor Ubuntu Web. Durante esta fase, sqlmap envía múltiples solicitudes HTTP modificando automáticamente los parámetros de la URL con diferentes cargas útiles (payloads) orientadas a detectar vulnerabilidades de inyección SQL. Como consecuencia, el servidor genera múltiples registros de acceso que serán procesados por el SIEM.

Figura 79
Ejecución del ataque



Nota: Elaboración propia

Figura 80
Registro de eventos en el aplicativo



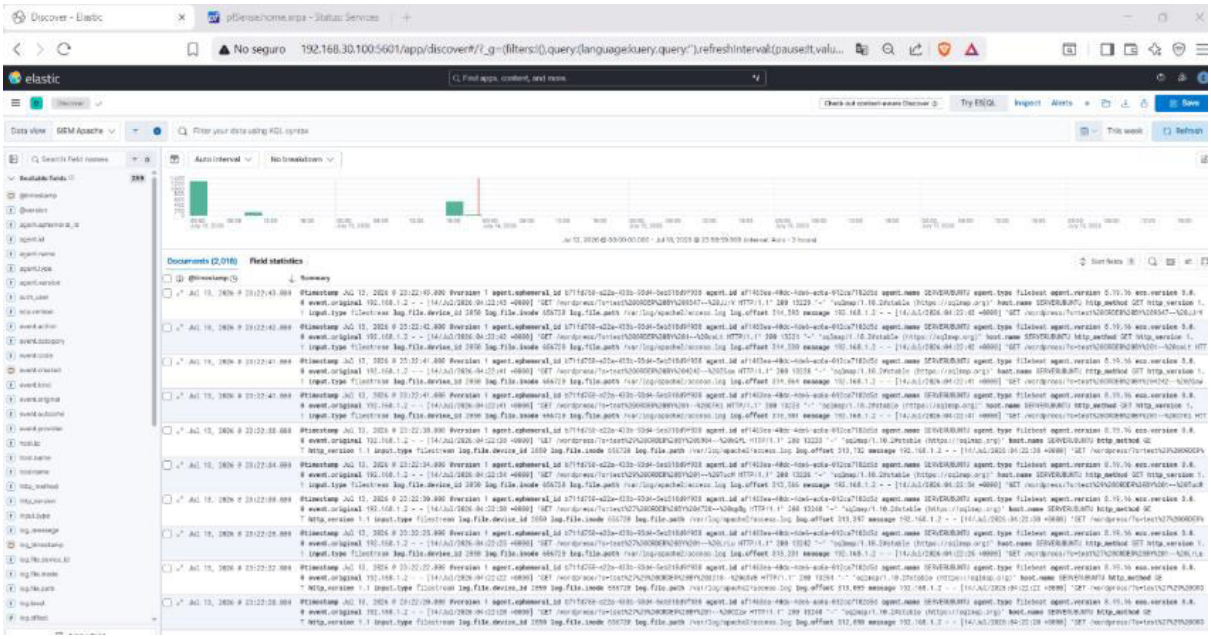
Nota: Elaboración propia

Visualización del ataque en Elastic Security

La figura muestra los eventos procesados por Elastic Security después de la ejecución del ataque. Se observa que las solicitudes HTTP fueron etiquetadas como sql_injection_candidate por

Logstash y almacenadas en Elasticsearch, permitiendo que la regla de correlación contabilice los eventos provenientes de la misma dirección IP para determinar la existencia de un posible intento de explotación de la aplicación web.

Figura 81
Registro de eventos en Elastic Security



Nota: Elaboración propia

Escenario 5 - T1190 Explotación WordPress (WP File Manager RCE)

Se reutilizó el pipeline existente de Apache (mismo grok de la Regla 4) agregando una condición adicional que identifica el patrón de explotación por ruta, en vez de por contenido de parámetro:

```
# 02-apache.conf - bloque agregado dentro de
#   filter { if [module] == "apache" { ... } }
if [url_path] =~ "(?i)wp-file-manager/lib/
                (php/connector|files/)" {
 mutate {
  add_tag => [ "wp_file_manager_exploit_candidate" ]
  add_field => { "threat.technique.id" => "T1190" }
 }
```

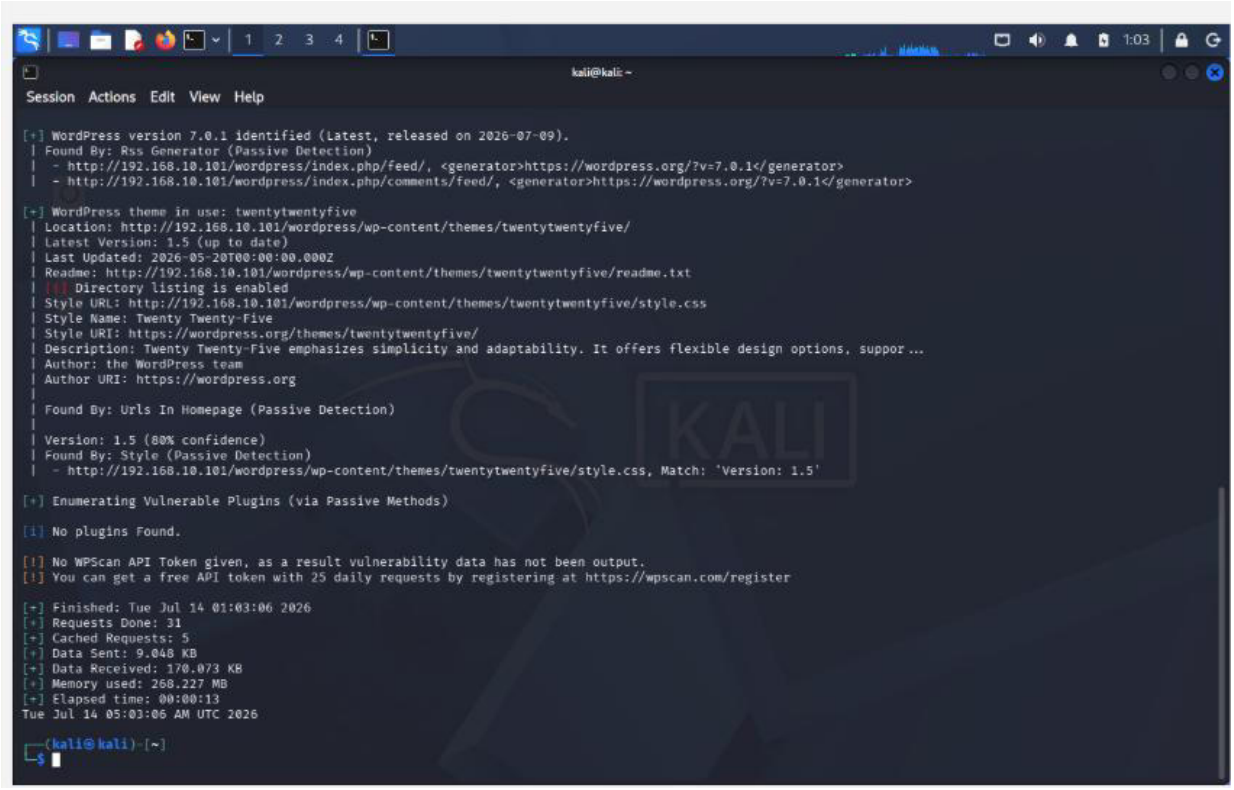
Reconocimiento mediante WPScan

La figura presenta la ejecución de la herramienta WPScan desde la máquina atacante Kali Linux para realizar el reconocimiento inicial del sitio WordPress. Durante esta fase se recopila información sobre la versión del CMS, los plugins instalados y posibles vulnerabilidades conocidas, con el objetivo de identificar componentes susceptibles de explotación antes de ejecutar el ataque.

Figura 82
Ejecución de la herramienta WPScan

Nota: Elaboración propia

Figura 83
Resultados de ejecución de WPScan

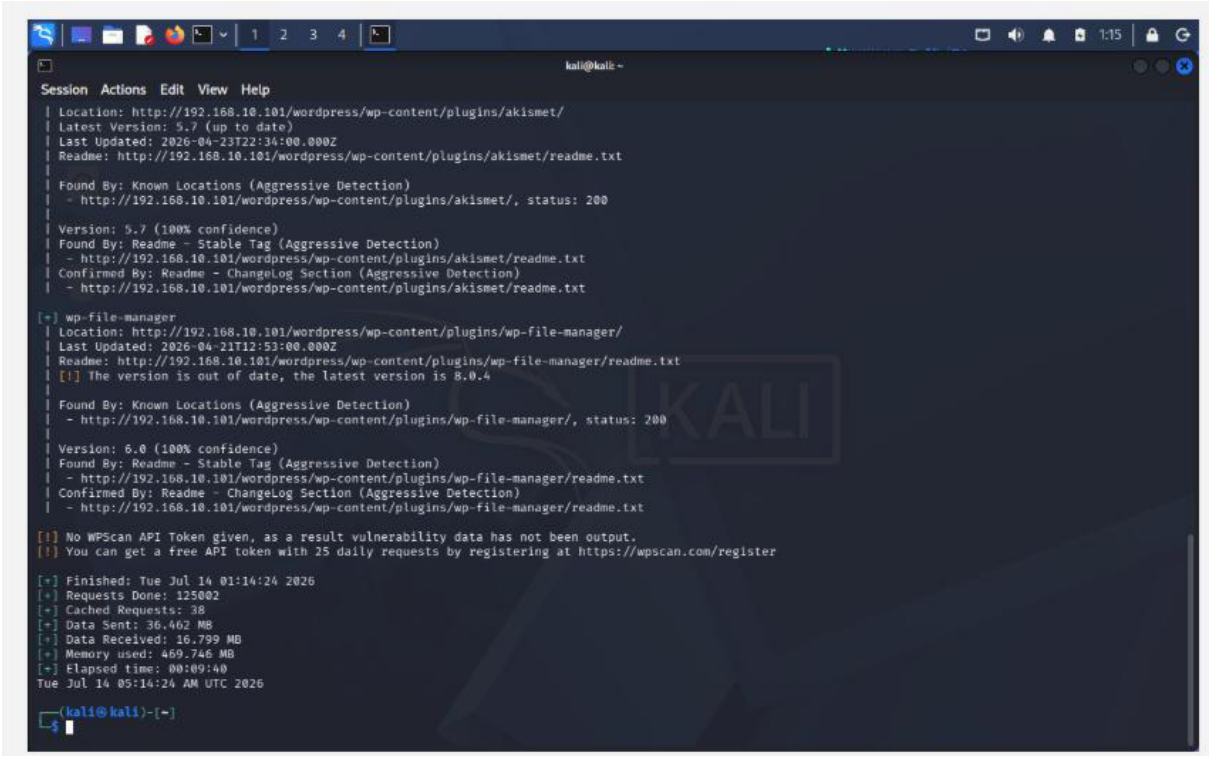


Nota: Elaboración propia

Ejecución de segunda prueba agresiva debido a falta de resultados

La figura muestra una segunda ejecución de WPScan utilizando opciones de análisis más agresivas, debido a que el primer reconocimiento no identificó vulnerabilidades explotables. Esta etapa incrementa el nivel de enumeración del sitio, buscando detectar plugins ocultos o versiones vulnerables que no fueron identificadas durante el análisis inicial.

Figura 84
Ejecución agresiva de WPScan



Nota: Elaboración propia

Figura 85
Resultados de segunda ejecución

Nota: Elaboración propia

Ejecución remota

La figura presenta la ejecución del ataque contra el plugin WP File Manager mediante el envío de solicitudes HTTP dirigidas al conector vulnerable connector.minimal.php. Aprovechando la vulnerabilidad CVE-2020-25213, el atacante intenta cargar un archivo sin autenticación para

obtener ejecución remota de código sobre el servidor web. Esta fase representa la explotación directa de la aplicación pública y constituye el evento principal que la regla SIEM busca identificar.

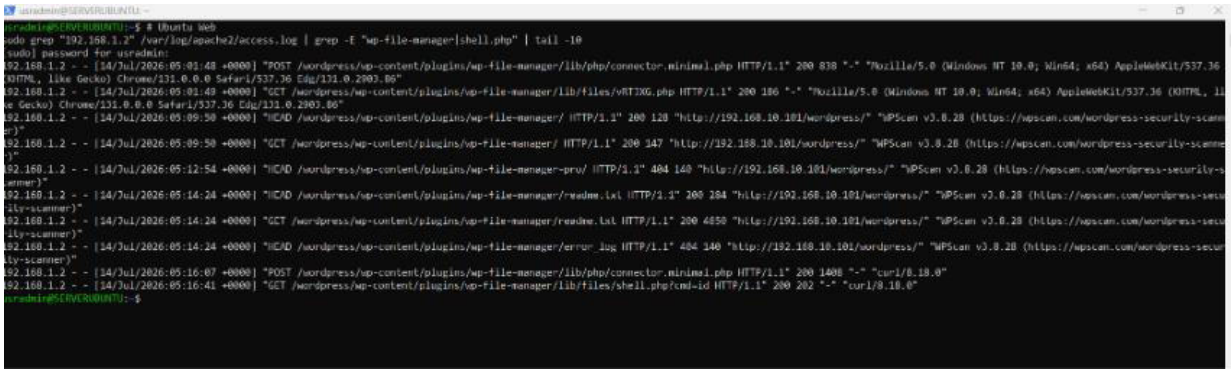
Figura 86
Ejecución del ataque contra el plugin WP File Manager

Nota: Elaboración propia

Registro del servidor web

La figura muestra los registros generados por el servidor Apache durante la ejecución del ataque. En los archivos de acceso se observan las solicitudes HTTP dirigidas al plugin vulnerable, incluyendo la dirección IP del atacante, la ruta solicitada, el método HTTP empleado y el código de respuesta del servidor. Estos registros constituyen la evidencia utilizada por Logstash para etiquetar automáticamente el evento como un posible intento de explotación.

Figura 87
Registros generados por el servidor Apache durante la ejecución del ataque

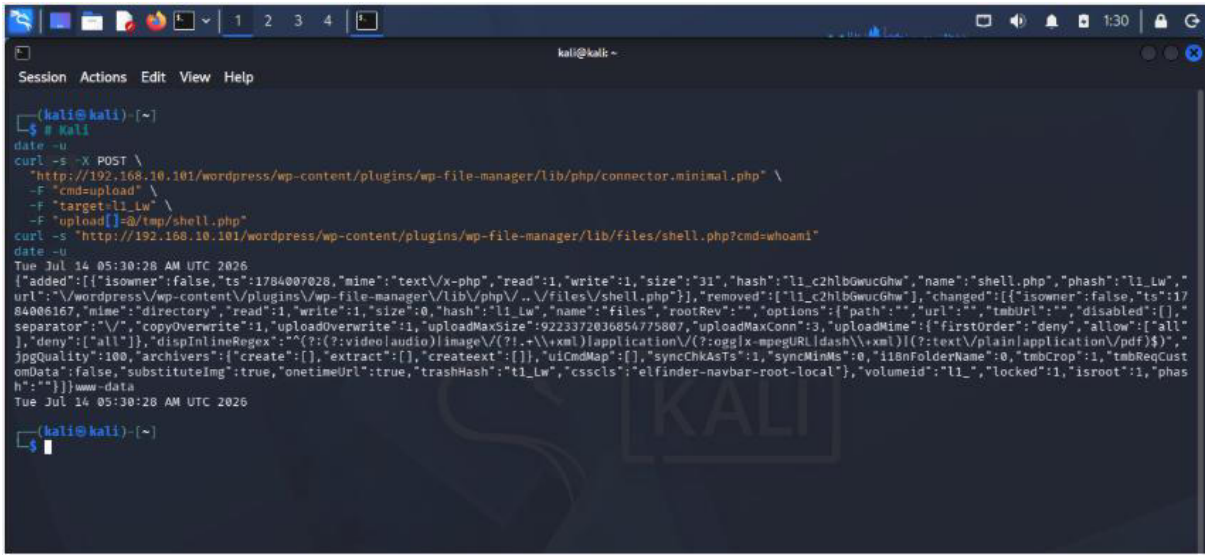


Nota: Elaboración propia

Ataque de evaluación

La figura presenta la validación del resultado obtenido tras la ejecución del ataque. En esta etapa se verifica si la carga útil enviada logró ejecutarse correctamente sobre el servidor y si el comportamiento generado corresponde al patrón definido para la vulnerabilidad evaluada. Esta comprobación permite confirmar que el escenario reproduce adecuadamente una explotación de una aplicación web pública.

Figura 88
Validación del resultado del ataque

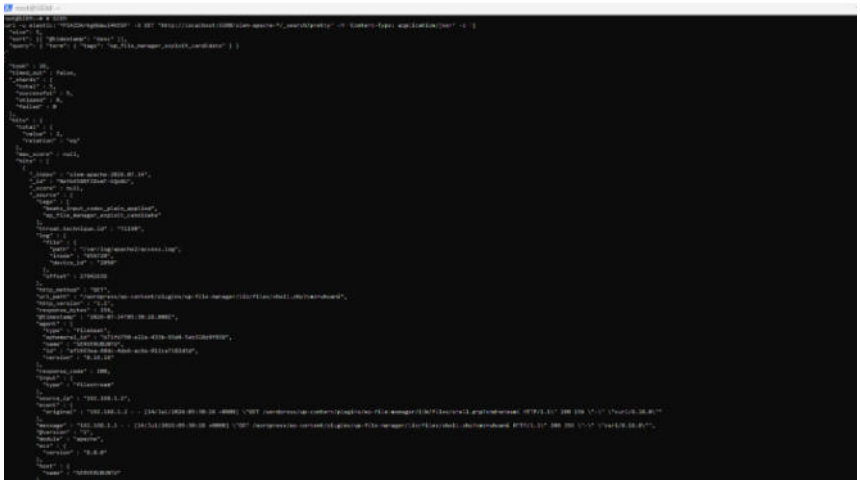


Nota: Elaboración propia

Registro en el siem

La figura muestra los eventos procesados por la infraestructura SIEM después de la ejecución del ataque. Los registros provenientes de Apache son procesados por Logstash, enriquecidos con la etiqueta wp_file_manager_exploit_candidate e indexados en Elasticsearch, permitiendo que Elastic Security identifique automáticamente la actividad sospechosa relacionada con la explotación del plugin vulnerable.

Figura 89
Eventos procesados por el SIEM

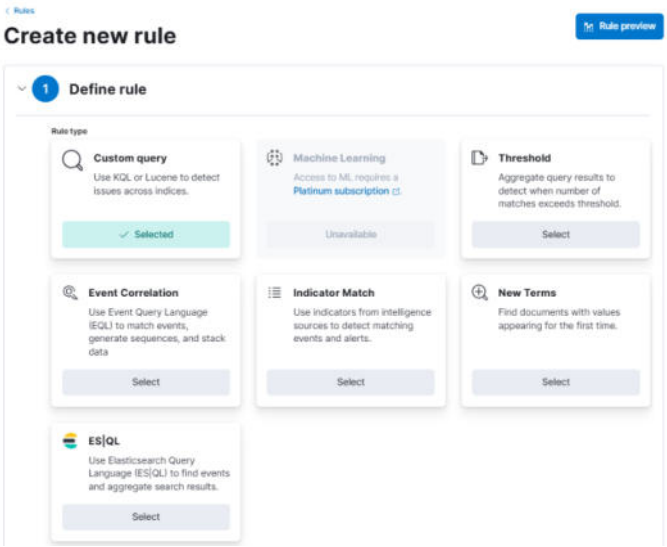


Nota: Elaboración propia

Creación de la regla.

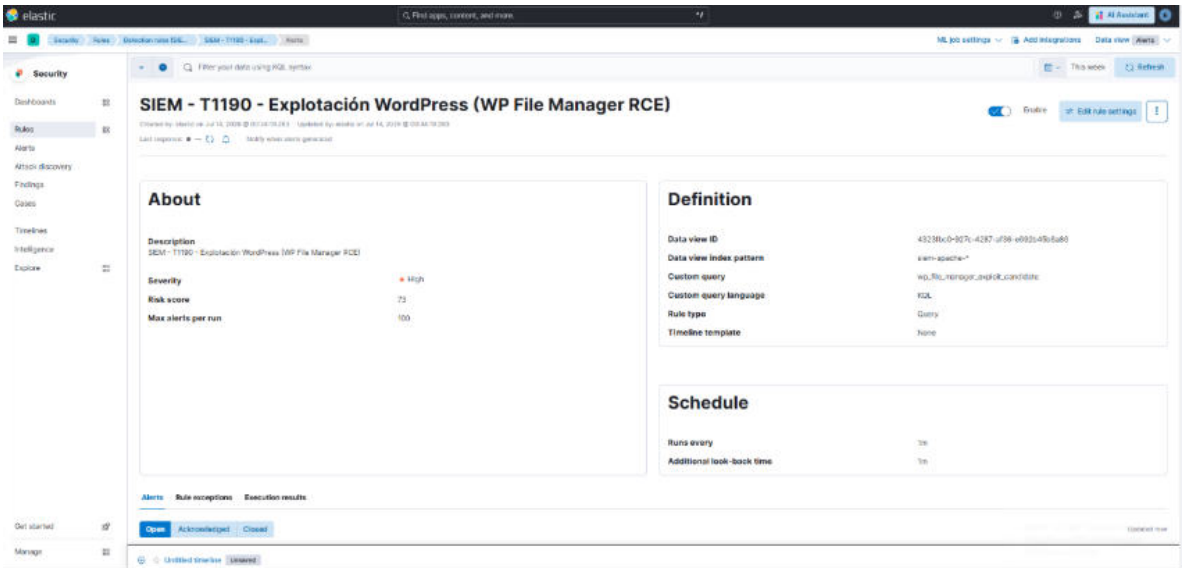
La figura presenta la configuración de la regla de detección dentro de Elastic Security. La regla utiliza una consulta personalizada sobre el índice siem-apache-* para identificar eventos previamente etiquetados por Logstash, sin necesidad de utilizar un umbral de correlación, debido a que una única solicitud dirigida al endpoint vulnerable constituye un comportamiento altamente sospechoso.

Figura 90
Configuración de la regla de detección



Nota: Elaboración propia

Figura 91
Detalle del caso de uso implementado

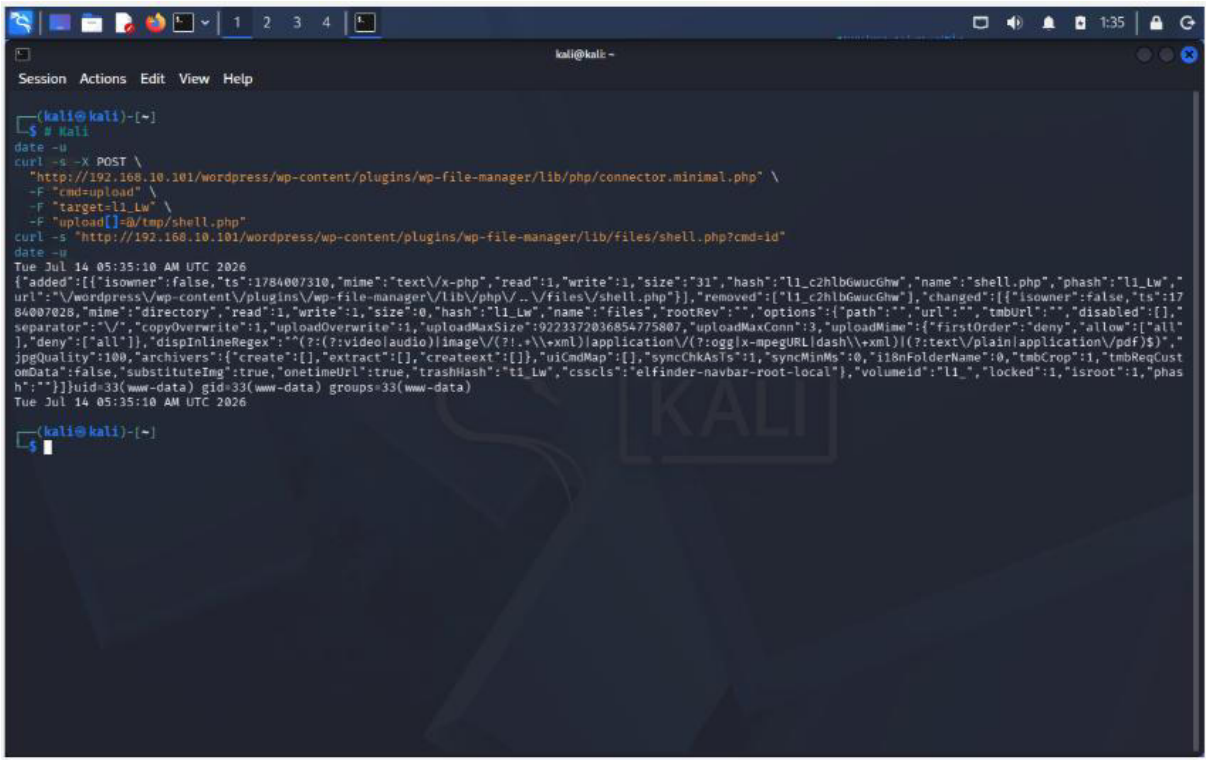


Nota: Elaboración propia

Ejecución final del ataque.

La figura muestra la repetición del escenario de explotación una vez implementada la regla de detección. Durante esta prueba se verifica que las solicitudes enviadas hacia el endpoint vulnerable sean registradas correctamente y procesadas por la plataforma SIEM, permitiendo validar el funcionamiento de la lógica de detección implementada.

Figura 92
Nueva ejecución de ataque

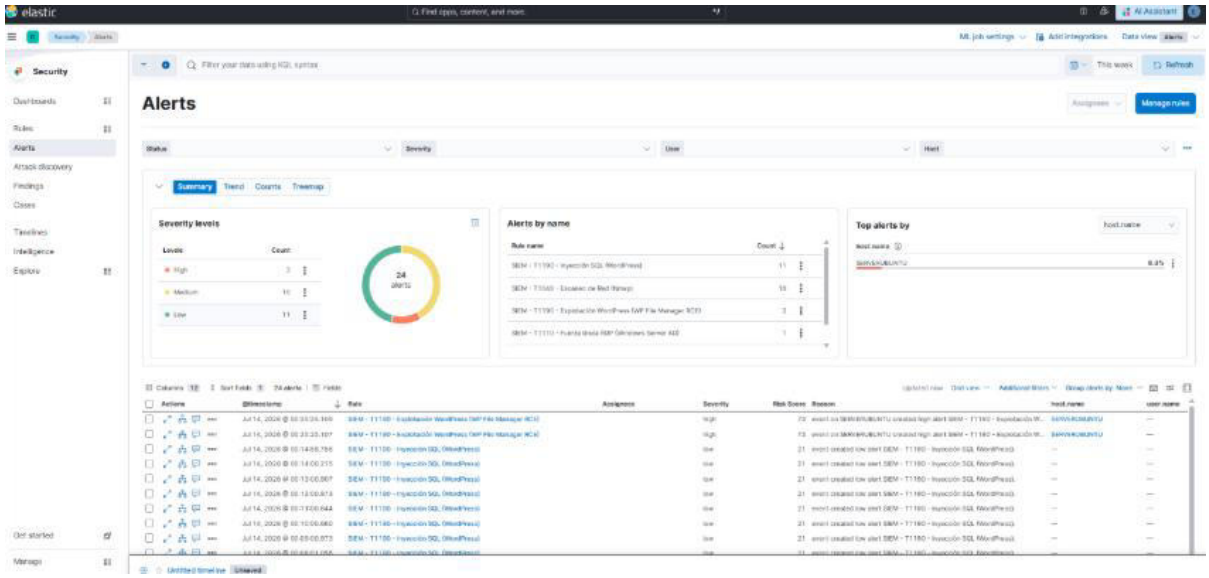


Nota: Elaboración propia

Generación de la alerta.

La figura presenta la alerta generada por Elastic Security después de detectar el patrón correspondiente a la explotación del plugin WP File Manager. La alerta clasifica el evento con severidad High, lo asocia a la técnica MITRE ATT&CK T1190 e identifica la posible explotación de la vulnerabilidad CVE-2020-25213, proporcionando al analista información suficiente para iniciar el proceso de respuesta ante incidentes.

Figura 93
Registro de alertas en SIEM



Nota: Elaboración propia

Escenario 6 – SIEM - T1059 - Ejecución de Comandos (Post-Explotación)

Se agregó un tercer bloque de detección al mismo pipeline de Apache (reutilizando 01-beats.conf → 02-apache.conf sin crear pipelines nuevos), diseñado deliberadamente para generalizar la detección por contenido del parámetro cmd=, en vez de por la ruta específica del plugin vulnerable — de forma que la regla cubra cualquier webshell o mecanismo de ejecución remota, no solo WP File Manager:

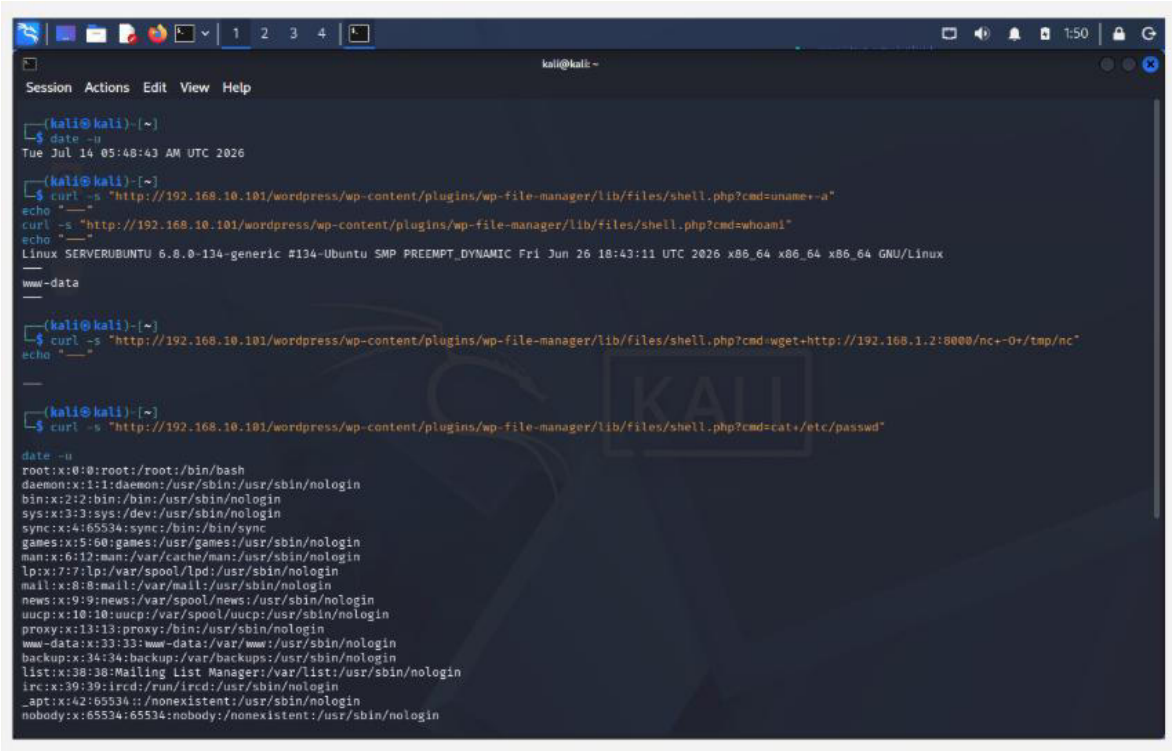
```
# 02-apache.conf - bloque agregado dentro de
#   filter { if [module] == "apache" { ... } }
if [url_path] =~ "(?i)[?&]cmd=.*(whoami|uname|cat\+|
            wget|curl|nc\+|bash|sh\+|passwd|
            id$|/etc/|chmod|nmap)" {
 mutate {
  add_tag => [ "remote_command_execution_candidate" ]
  add_field => { "threat.technique.id" => "T1059" }
 }
```

```
}
```

Reconocimiento

En esta imagen se observa la fase de reconocimiento posterior a la explotación. Desde el equipo atacante Kali Linux (192.168.1.2) se realizan peticiones HTTP hacia la webshell alojada en el servidor Ubuntu Web (192.168.10.101).

Figura 94
Fase de reconocimiento posterior a la explotación



Nota: Elaboración propia

Eventos del servidor.

La captura presenta los registros de acceso Apache generados por las peticiones maliciosas. Cada entrada contiene solicitudes HTTP dirigidas al archivo shell.php con distintos valores en el parámetro cmd=.

Los registros evidencian:

La dirección IP de origen del atacante.

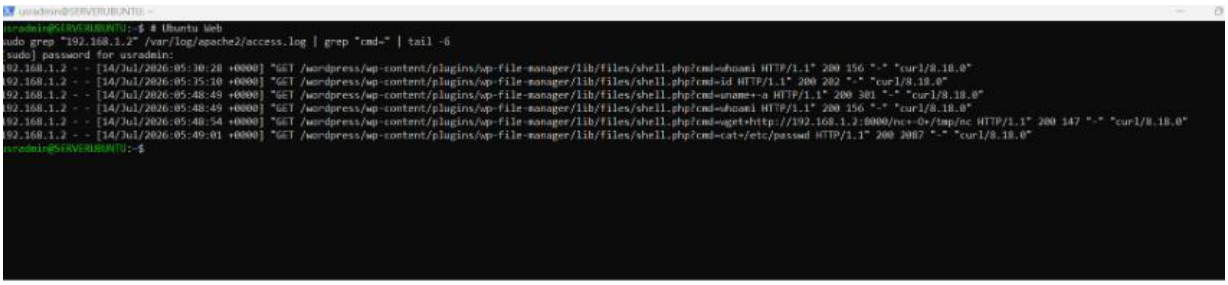
El recurso accedido.

Los comandos enviados.

El código de respuesta HTTP del servidor.

Esta información constituye la fuente principal utilizada por Logstash y Elastic para identificar intentos de ejecución remota de comandos.

Figura 95
Registros de acceso Apache



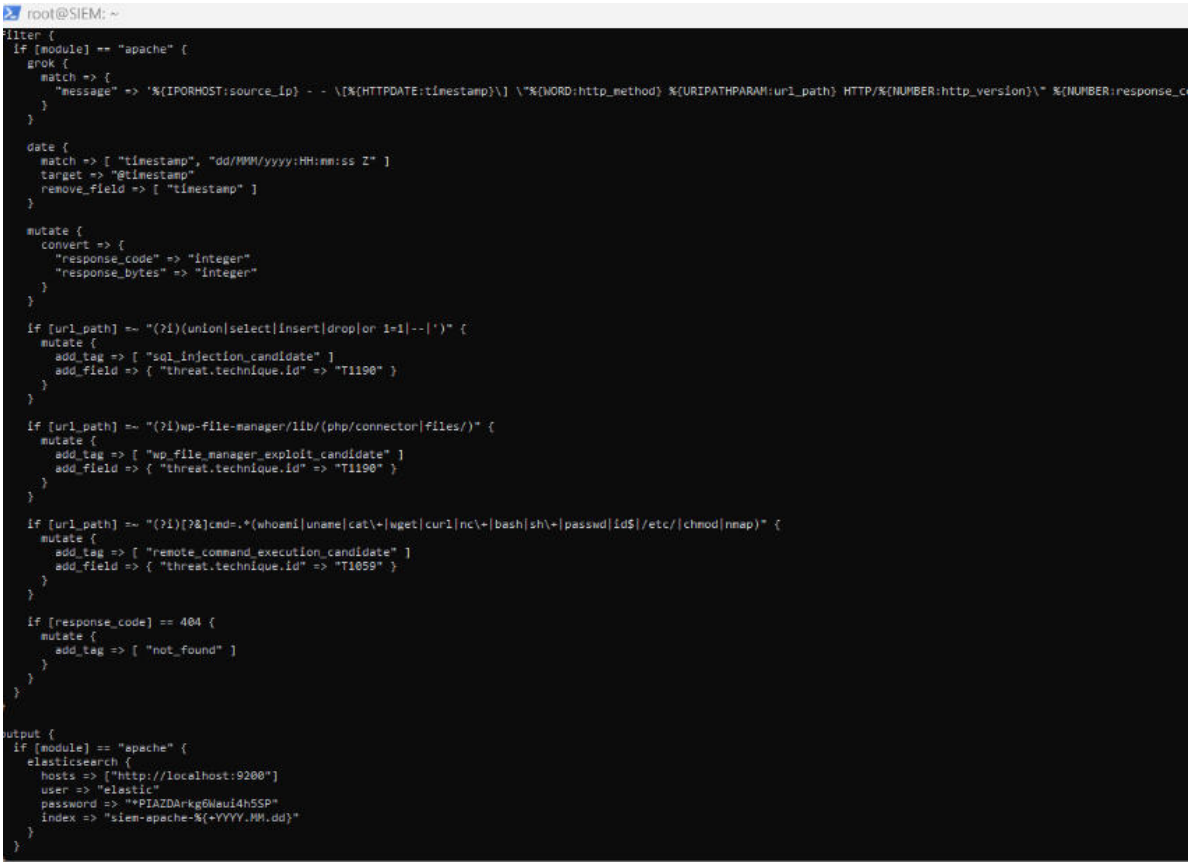
Nota: Elaboración propia

Configuración de la regla

La imagen muestra el bloque agregado dentro del pipeline de Logstash. La lógica utiliza expresiones regulares para detectar el parámetro cmd= acompañado de comandos comúnmente usados en explotación.

```
if [url_path] =~ "(?i)wp-file-manager/lib/(php/connector|files/)" {
 mutate {
  add_tag => [ "wp_file_manager_exploit_candidate" ]
```

Figura 96
Bloque agregado dentro del pipeline de Logstash



Nota: Elaboración propia

Evaluación de la regla

Esta evidencia muestra el resultado del procesamiento del evento después de pasar por el pipeline.

Se observa que:

El log fue analizado correctamente.

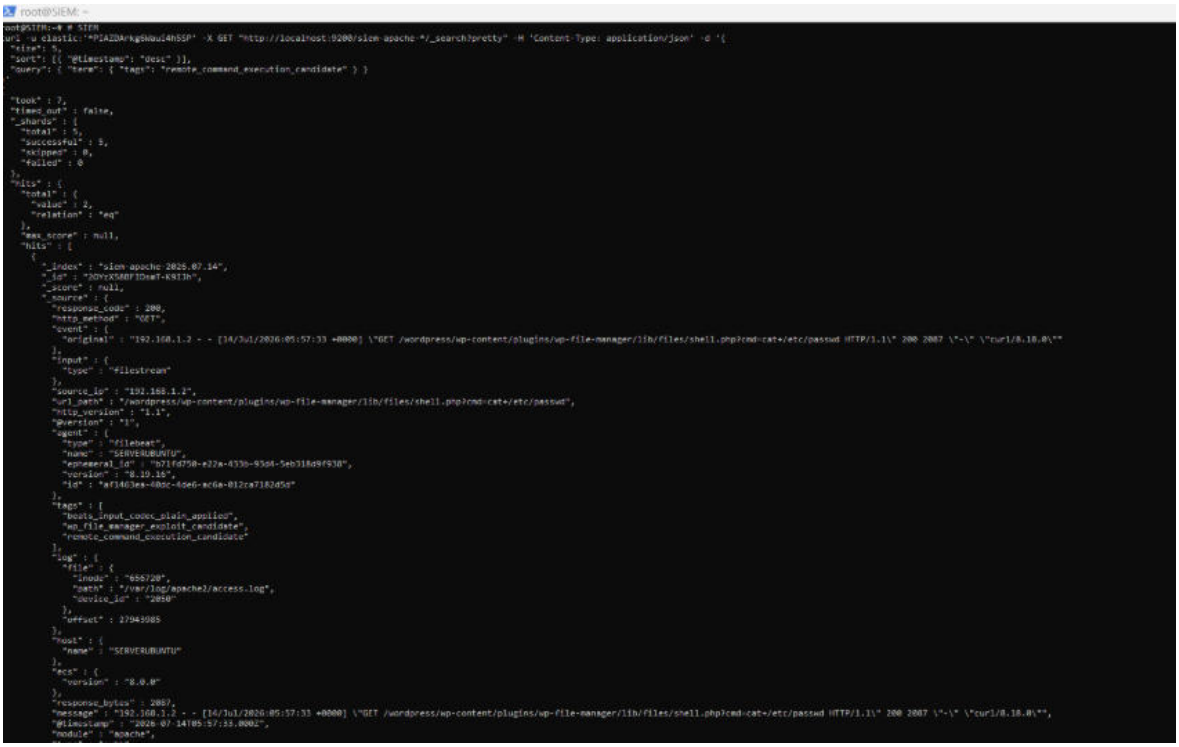
Se agregó el tag remote_command_execution_candidate.

Se incorporó la referencia a la técnica T1059.

El evento se encuentra preparado para ser indexado en Elasticsearch y posteriormente consumido por la regla de detección de Kibana.

La captura valida que el mecanismo de enriquecimiento funciona correctamente antes de generar alertas.

Figura 97
Resultado del procesamiento del evento

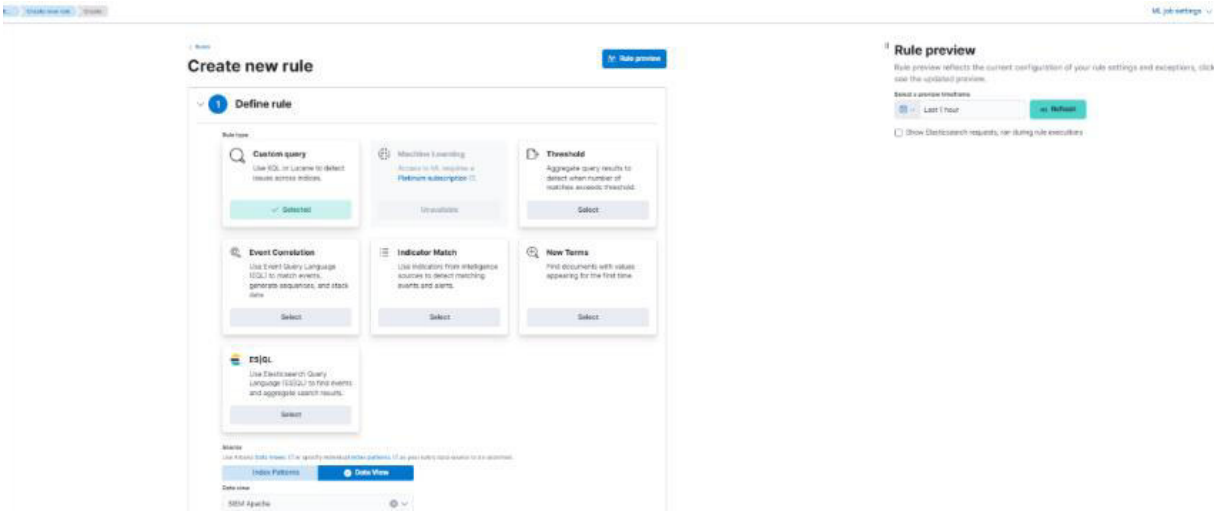


Nota: Elaboración propia

Creación de la regla

La primera captura muestra la selección del tipo de regla dentro de Elastic Security. Se utiliza una regla basada en consulta (Query Rule), adecuada para detectar eventos etiquetados previamente por Logstash.

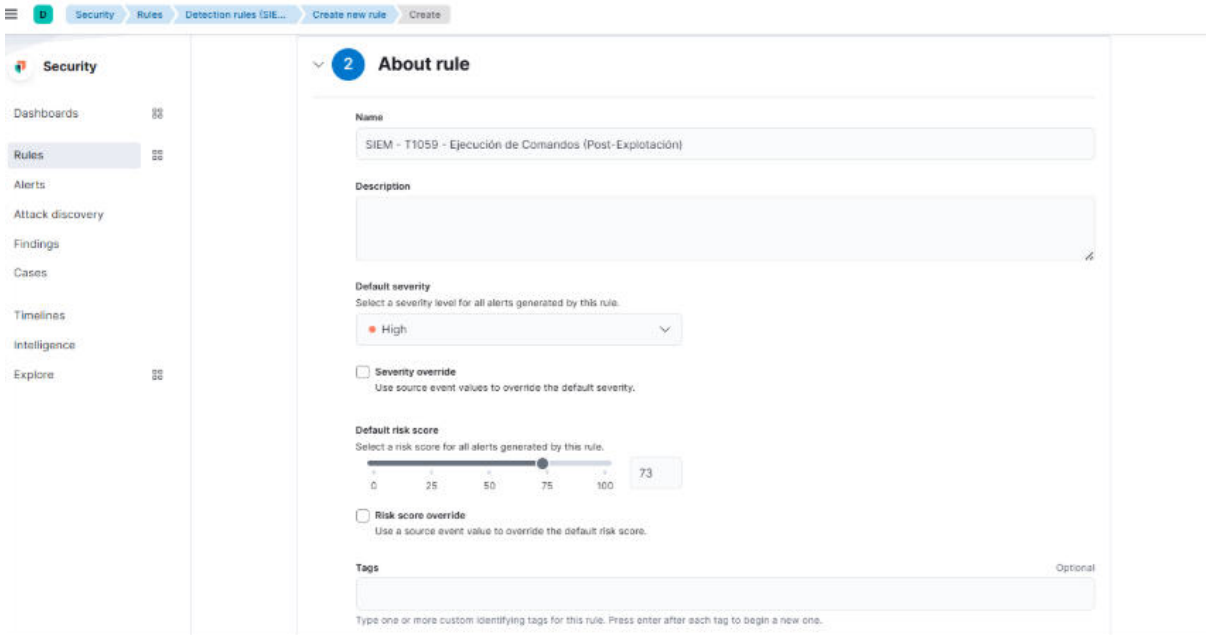
Figura 98
Tipo de regla dentro de Elastic Security



Nota: Elaboración propia

Estos parámetros indican que la actividad detectada representa una amenaza significativa dentro del entorno monitorizado.

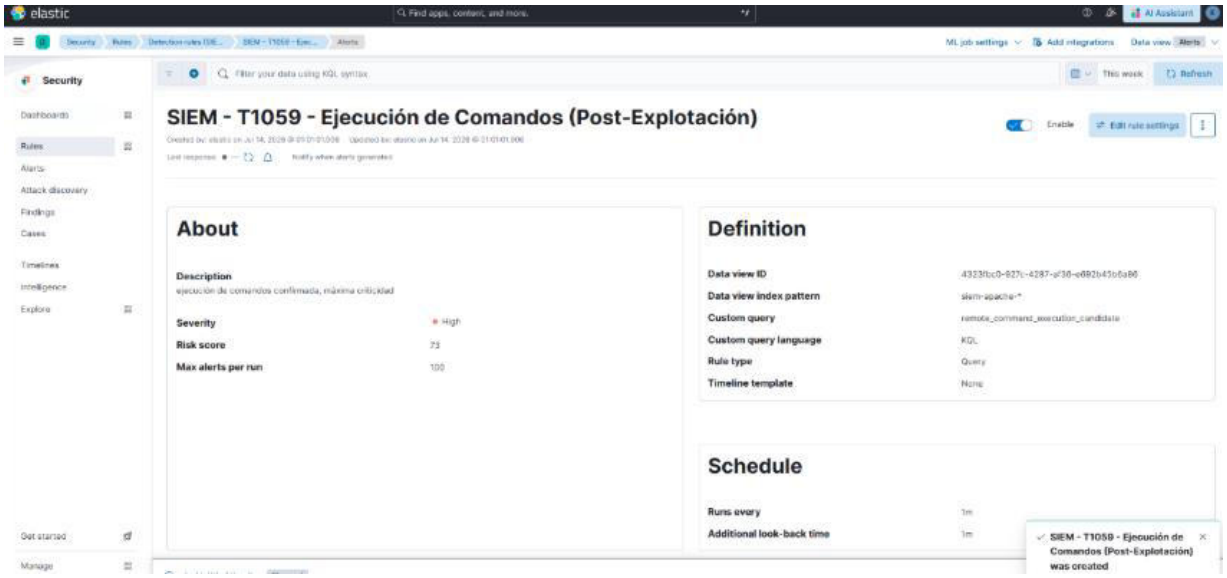
Figura 99
Configuración de regla



Nota: Elaboración propia

La captura corresponde al resumen final de la regla ya creada y habilitada dentro de Elastic Security, mostrando su definición, programación y parámetros operativos.

Figura 100
Regla de detección implementada



Nota: Elaboración propia

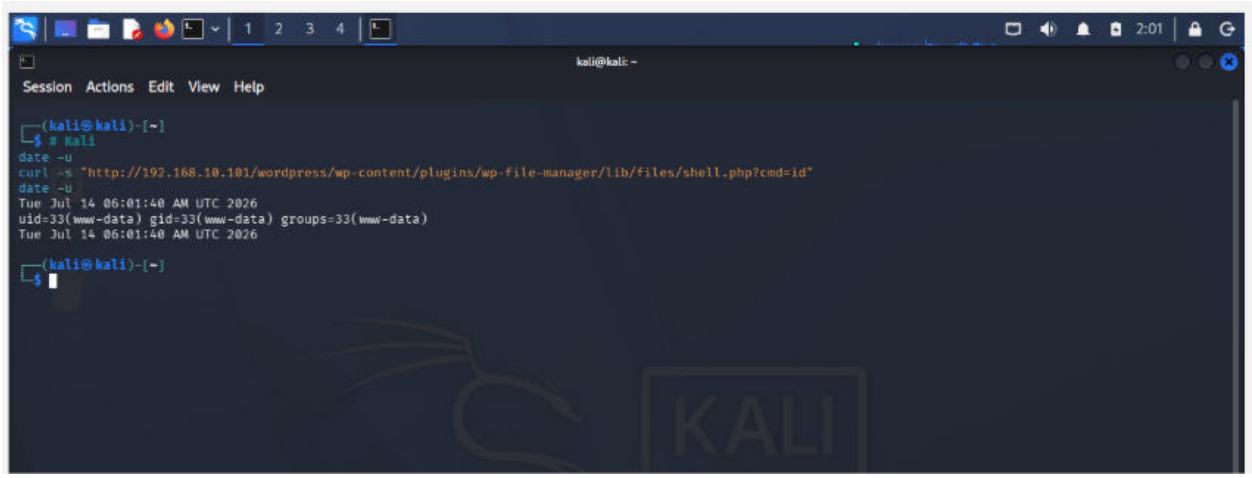
Evaluación de la regla

Inicio de ataque.

La imagen muestra la ejecución de la prueba final de detección. Desde Kali Linux se envía una solicitud HTTP que contiene: cmd=id

El servidor responde con información del usuario que ejecuta el proceso web, confirmando nuevamente la ejecución remota de comandos y generando la evidencia necesaria para activar la regla de detección.

Figura 101
Ejecución remota de comandos



Nota: Elaboración propia

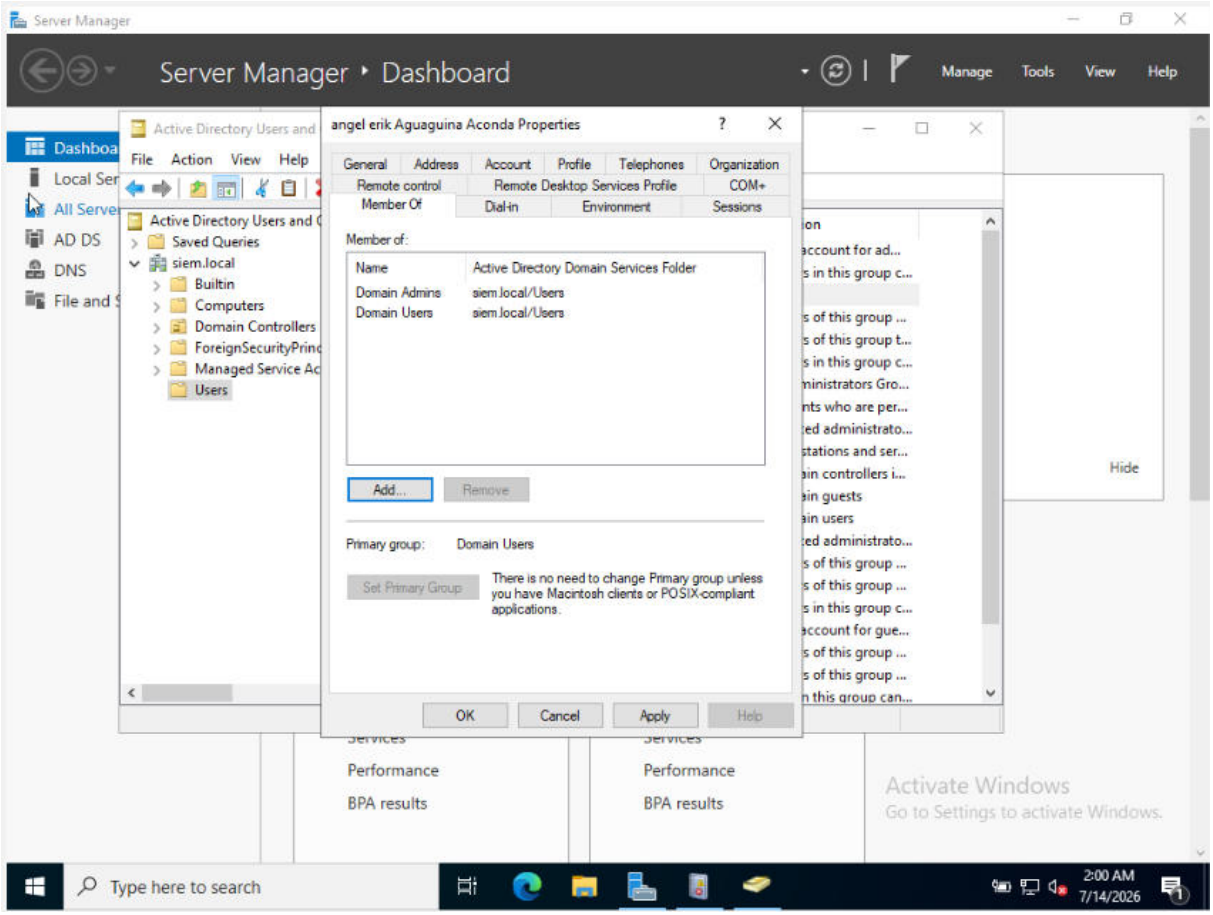
Escenario 7 – T1021 Movimiento Lateral RDP (VLAN20 → AD)

Agregar usuario administrador

La imagen muestra la consola de Active Directory donde se configura la cuenta de dominio aaguaguina, utilizada para simular el movimiento lateral. Esta cuenta es añadida al dominio para realizar las pruebas de autenticación remota hacia el servidor Active Directory.

El objetivo es disponer de una credencial válida que permita comprobar si el SIEM detecta el acceso RDP hacia el controlador de dominio.

Figura 102
Configuración de la cuenta de dominio aaguaguina

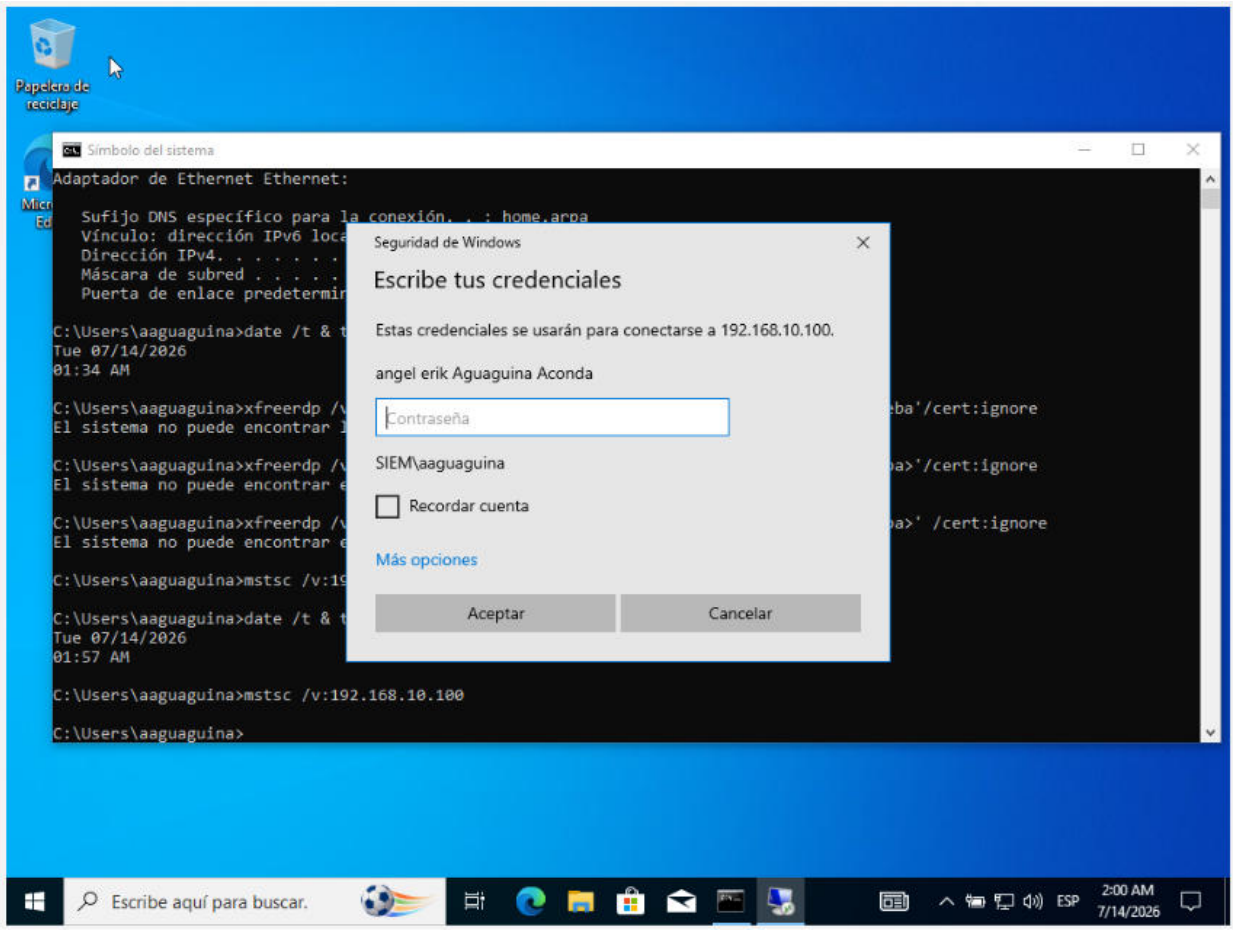


Nota: Elaboración propia

Inicio de sesión remoto desde el cliente

En esta captura se observa el equipo cliente ubicado en la VLAN20 ejecutando: mstsc /v:192.168.10.100, posteriormente se introducen las credenciales del usuario de dominio para establecer la conexión remota hacia el servidor Windows AD.

Figura 103
Ingreso de credenciales del usuario



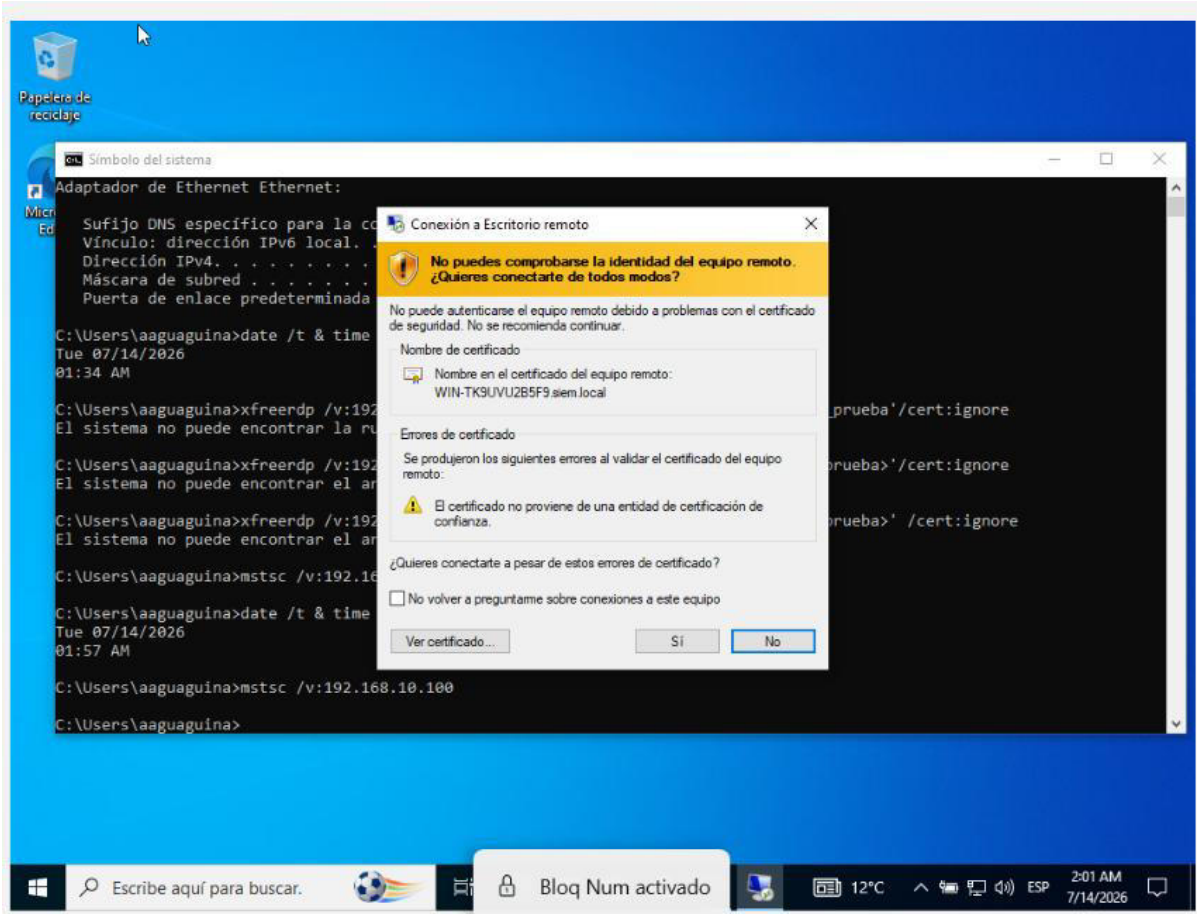
Nota: Elaboración propia

Advertencia del certificado RDP

La captura muestra la advertencia habitual de Escritorio Remoto cuando el certificado presentado por el servidor no ha sido validado por una entidad de confianza.

La conexión continúa porque la prueba busca generar una autenticación válida que pueda registrarse en los logs de seguridad de Windows.

Figura 104
Advertencia habitual de Escritorio Remoto

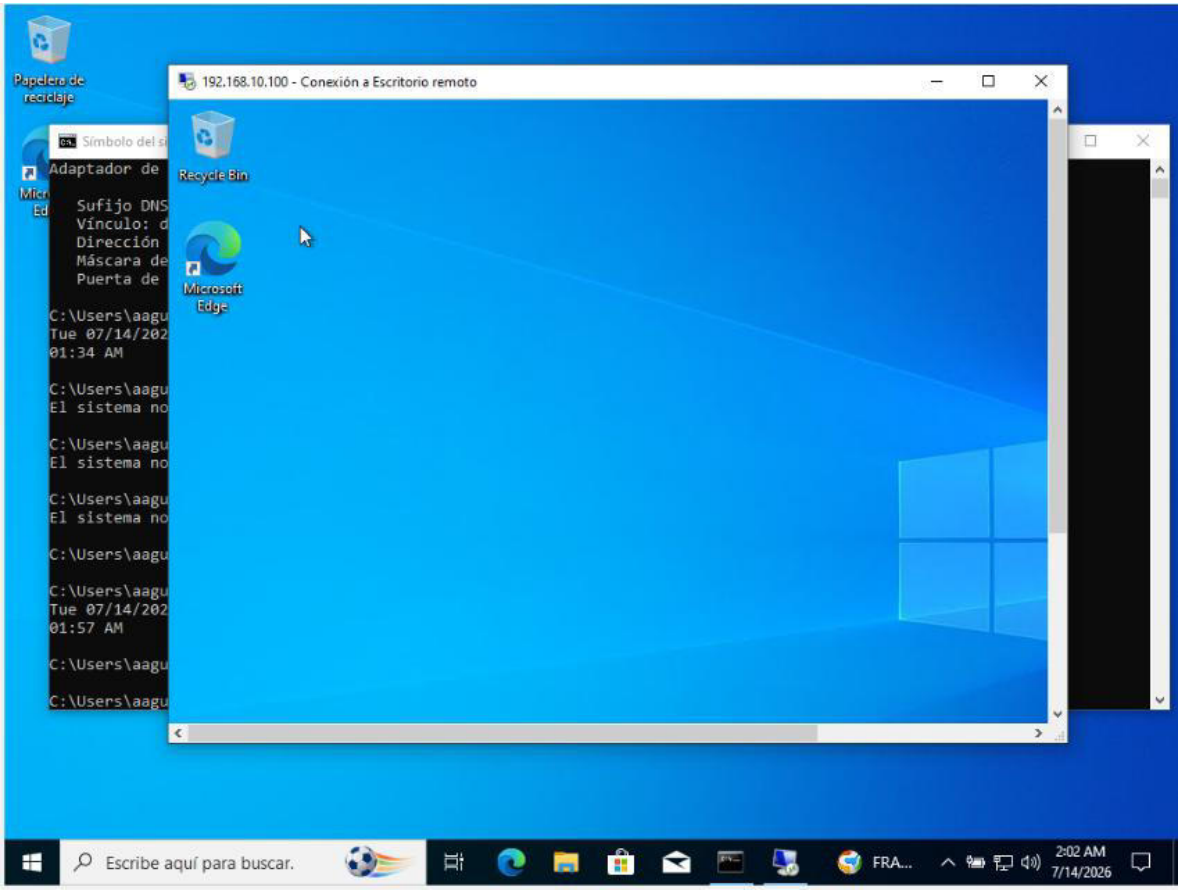


Nota: Elaboración propia

Conexión establecida

La imagen confirma que la sesión RDP fue establecida correctamente hacia el controlador de dominio. El usuario obtiene acceso interactivo al escritorio remoto del servidor Windows.

Figura 105
Conexión RDP establecida

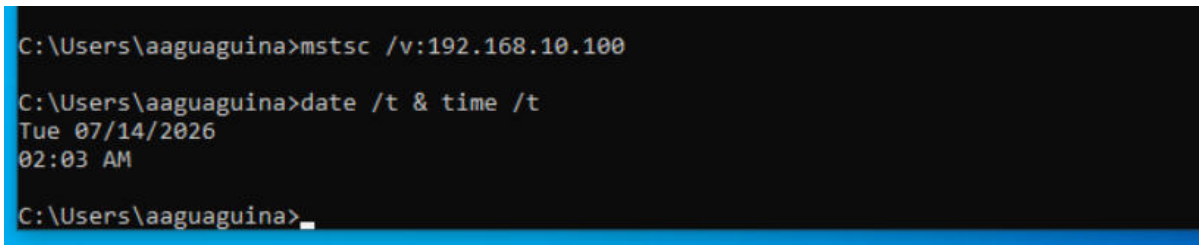


Nota: Elaboración propia

Evidencia de ejecución

La captura muestra la ejecución del comando y la fecha/hora de la prueba, sirviendo como evidencia del origen de la conexión desde el equipo cliente.

Figura 106
La ejecución del comando y la fecha/hora de la prueba



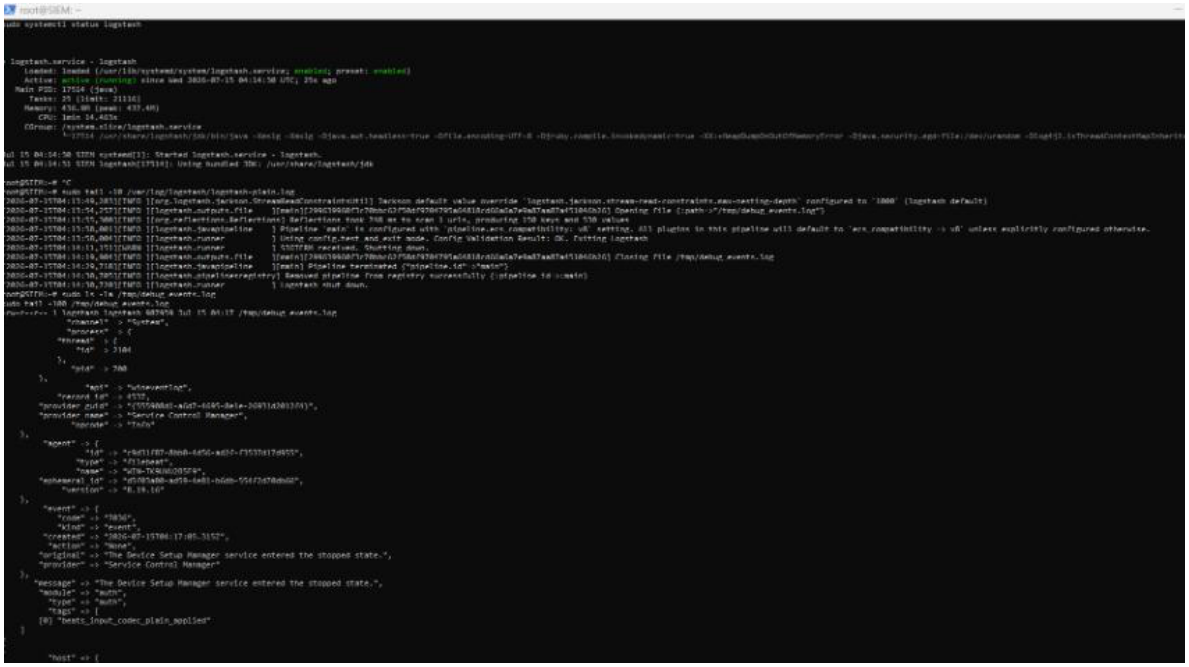
Nota: Elaboración propia

Registro generado en los logs

La imagen presenta el evento capturado por el sistema de monitorización. El punto clave es el Event ID 4624, que corresponde a un inicio de sesión exitoso en Windows.

La regla utiliza precisamente este identificador para detectar autenticaciones remotas válidas provenientes del host: 192.168.20.101 y descartar la cuenta de máquina del servidor.

Figura 107
Registro del evento



Nota: Elaboración propia

Configuración del parser Logstash

Esta captura muestra la lógica de procesamiento implementada en Logstash para los eventos de autenticación.

El bloque identifica:

Eventos de autenticación.

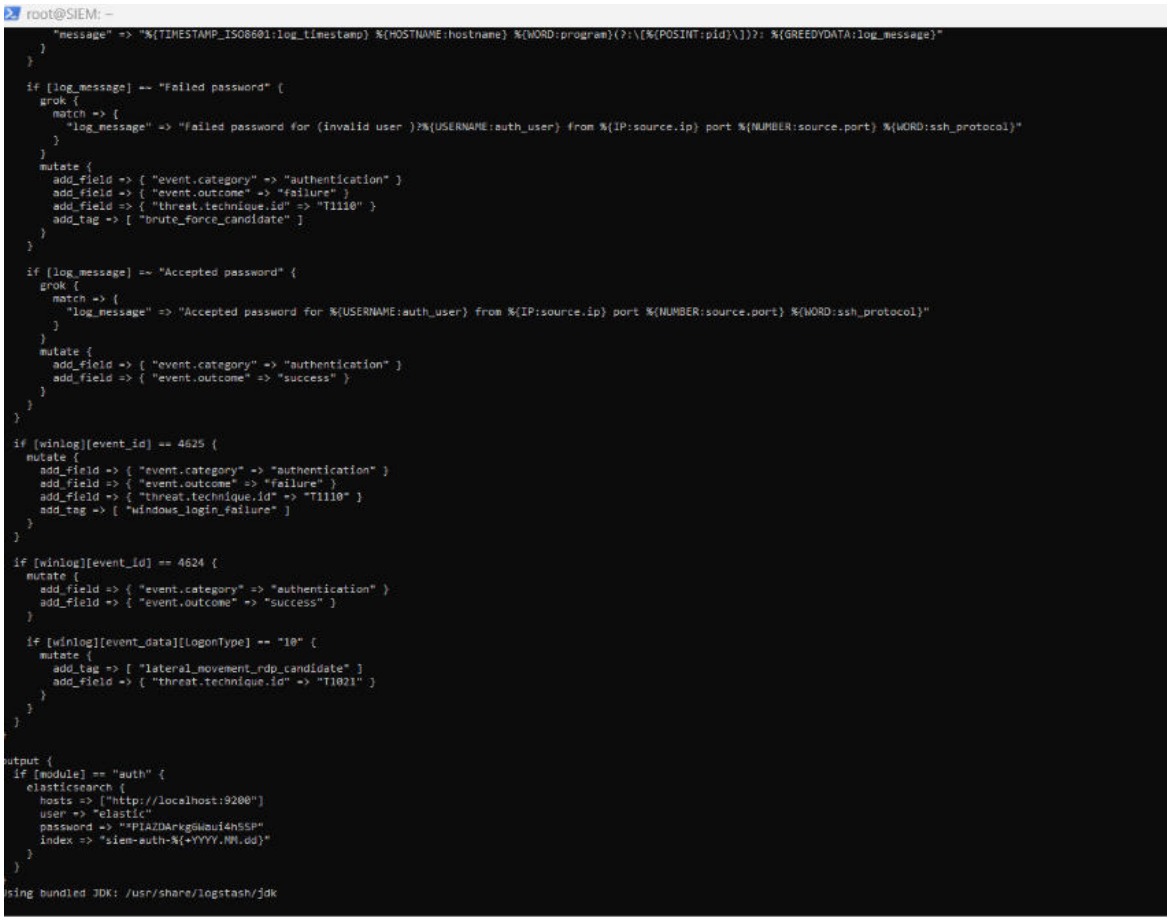
Inicios de sesión correctos.

Event ID 4624.

Clasificación de la técnica T1021.

Cuando se cumplen las condiciones establecidas, el evento es enriquecido para que Elasticsearch y Kibana puedan utilizarlo posteriormente en la generación de alertas.

Figura 108
Lógica de procesamiento implementada en Logstash

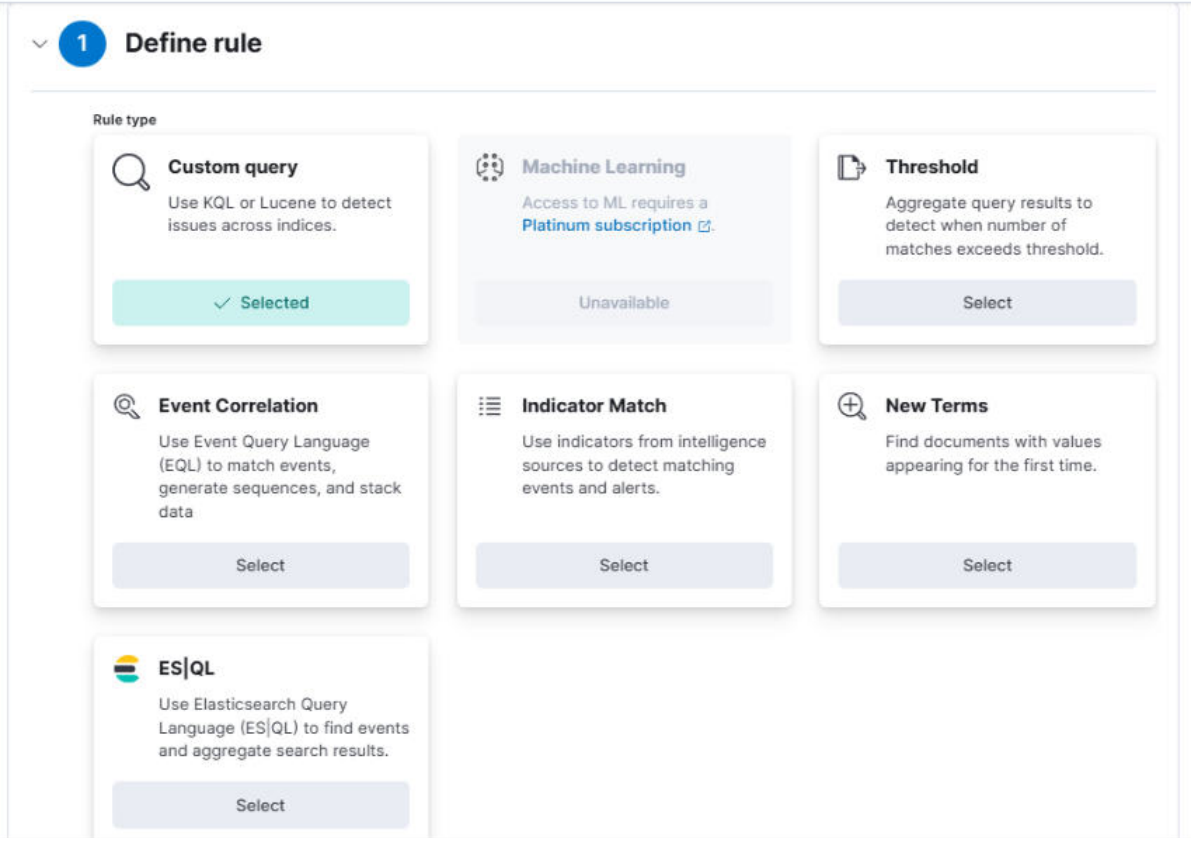


Nota: Elaboración propia

Creación de la regla en Kibana

La imagen muestra la creación de una regla de tipo Custom Query, apropiada para detectar eventos específicos previamente procesados por Elastic.

Figura 109
Creación de una regla de tipo Custom Query

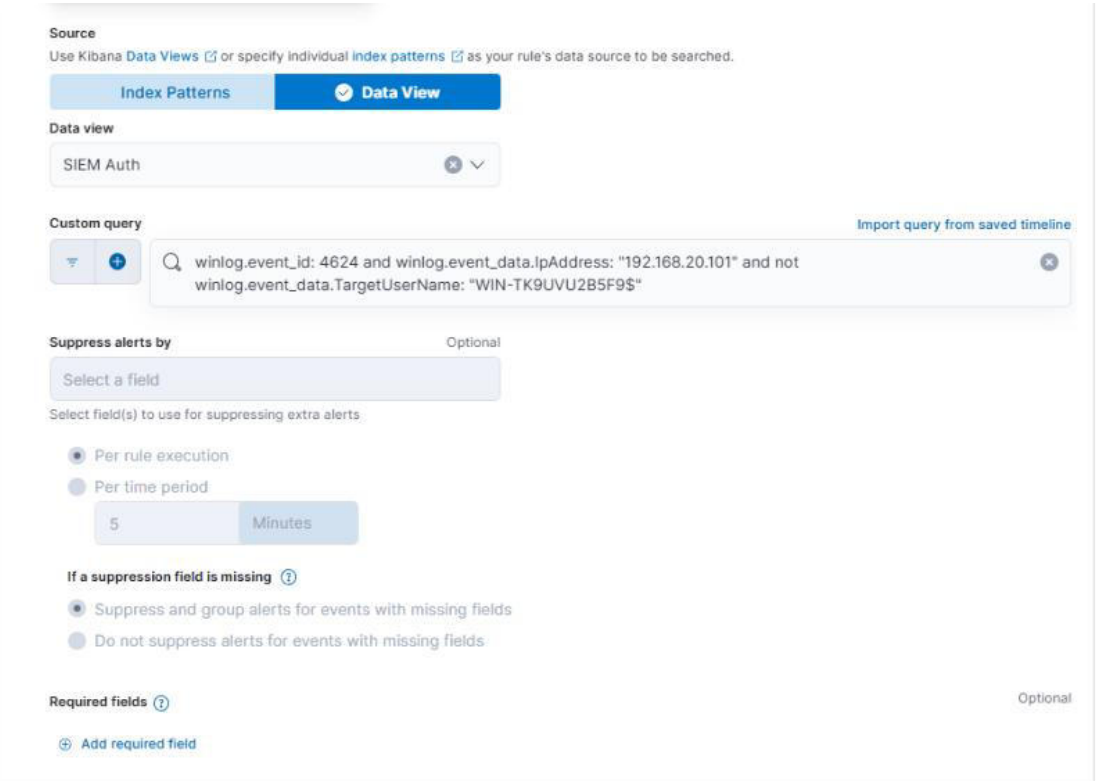


Nota: Elaboración propia

Configuración de la consulta

La captura contiene la lógica que permite identificar únicamente conexiones RDP realizadas por usuarios reales desde la VLAN20 hacia el controlador de dominio.

Figura 110
Lógica de identificación del evento



Nota: Elaboración propia

Resumen de la regla

La captura muestra la regla ya implementada con:

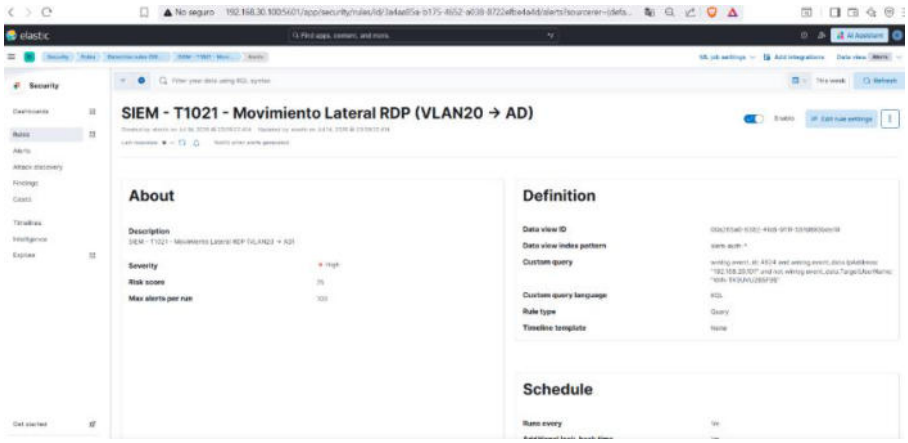
Severidad: High.

Risk Score: 75.

Data View: SIEM Auth.

Estos parámetros reflejan la criticidad de un posible movimiento lateral dentro de la red corporativa.

Figura 111
Regla de detección implementada

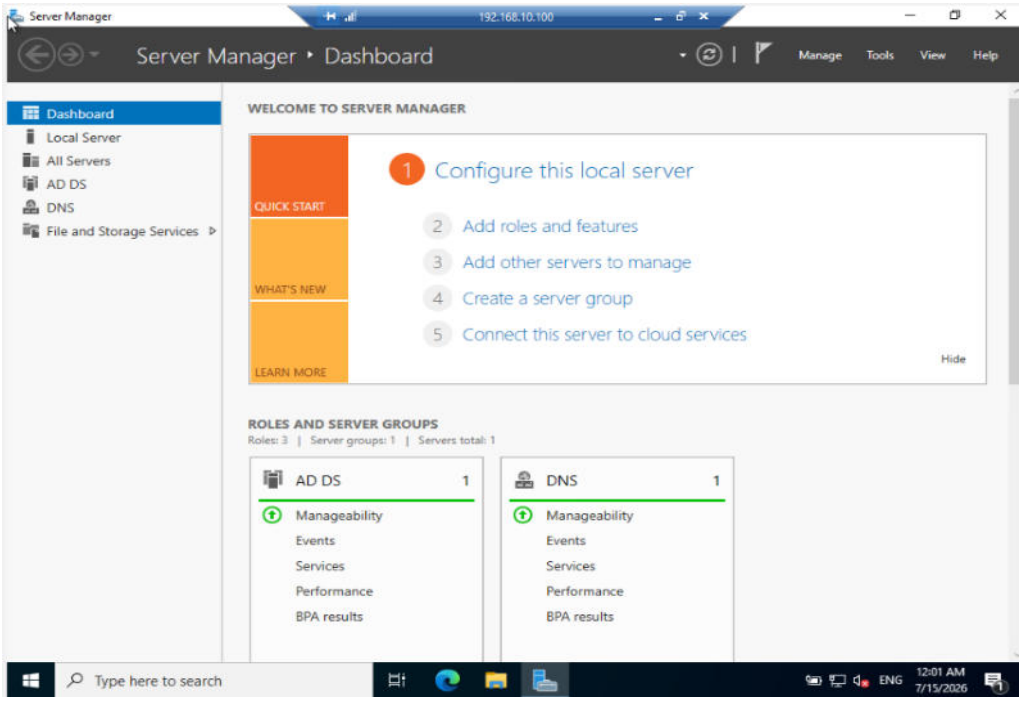


Nota: Elaboración propia

Conexión remota rdp

La imagen confirma que el usuario logró acceder al servidor Windows Active Directory mediante RDP. Desde la perspectiva de seguridad, esto representa exactamente el comportamiento que la regla intenta detectar: un equipo de usuario accediendo remotamente a infraestructura crítica.

Figura 112
Acceso exitoso del usuario al servidor por RDP



Nota: Elaboración propia

Escenario 8 – SIEM T1078 - Cuentas Válidas (Autenticación de Dominio)

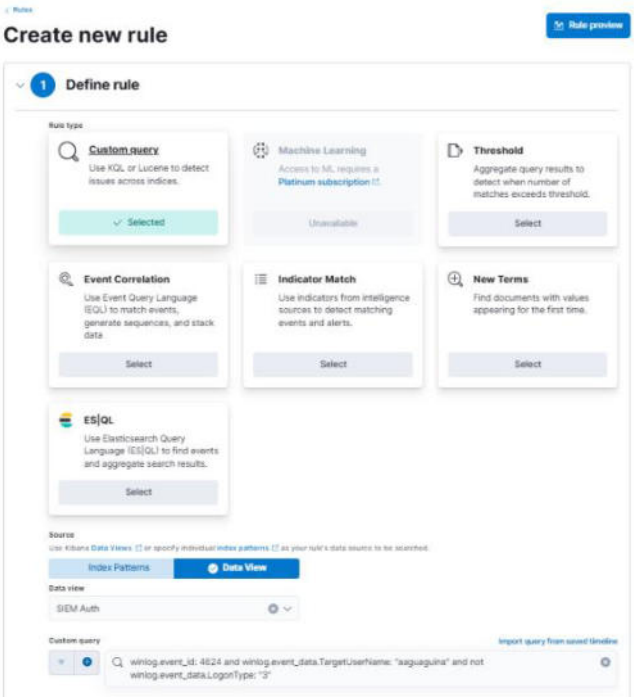
Diseño y alcance de la regla

A diferencia de las Reglas 1-7, orientadas a detectar patrones de ataque o explotación, la Regla 8 (T1078) detecta el uso legítimo de credenciales de dominio válidas es un indicador que, por sí solo, no es malicioso, pero que adquiere valor cuando se correlaciona con otras señales (origen de red inusual, horario atípico, o antecedentes de intentos fallidos). Por esta razón se asignó severidad Medium en lugar de High: la alerta representa un evento a revisar en contexto, no una amenaza confirmada de forma aislada.

Creación de la regla en Kibana

La captura muestra el asistente de Elastic Security durante la definición de una nueva regla. Se selecciona el tipo Custom Query, que permite utilizar consultas específicas sobre los registros almacenados en Elasticsearch para detectar eventos de autenticación relacionados con la cuenta monitorizada.

Figura 113
Definición de una nueva regla



Nota: Elaboración propia

Configuración final

La segunda imagen presenta la configuración definitiva de la regla:

Nombre: SIEM - T1078 - Cuentas Válidas (Autenticación de Dominio).

Data View: SIEM Auth.

Severidad: Medium.

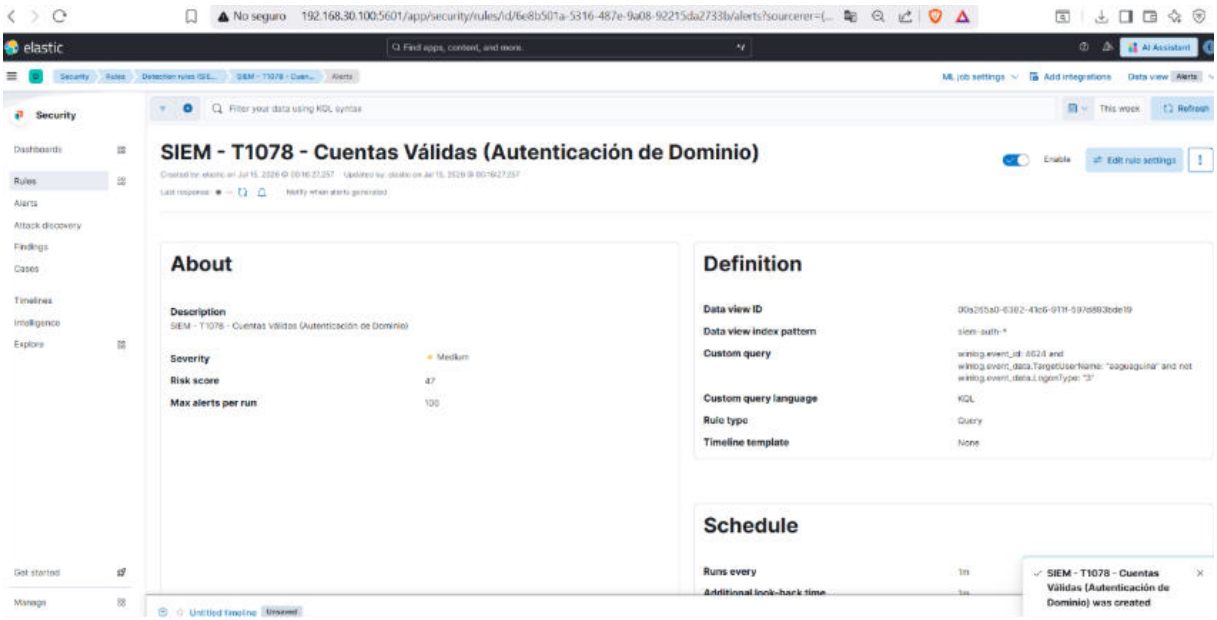
Risk Score: 47.

Programación de ejecución periódica.

Esta configuración refleja que el evento requiere revisión por parte del analista, aunque no representa necesariamente una amenaza confirmada.

Figura 114

Configuración de la regla



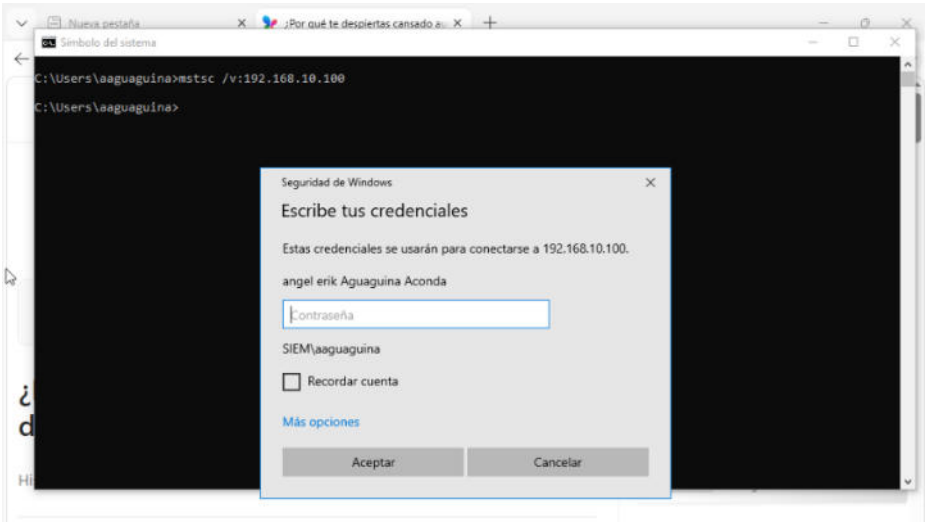
Nota: Elaboración propia

Ingreso de una cuenta valida

Inicio de conexión RDP

La imagen muestra el inicio de una conexión mediante Escritorio Remoto utilizando el comando: mstsc /v:192.168.10.100

Figura 115
Inicio de una conexión mediante Escritorio Remoto



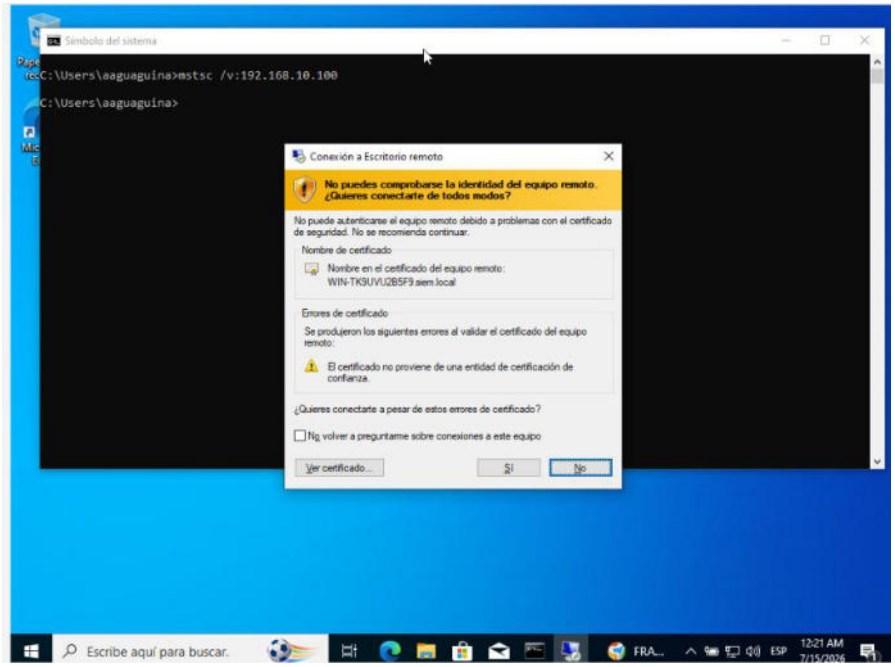
Nota: Elaboración propia

Validación del acceso remoto

La captura muestra la advertencia de seguridad habitual durante la conexión RDP cuando el certificado presentado por el servidor no procede de una entidad certificadora de confianza.

A pesar de la advertencia, el establecimiento de la conexión permite generar el evento de autenticación que posteriormente activará la regla T1078 dentro del SIEM.

Figura 116
Advertencia de seguridad por conexión RDP



Nota: Elaboración propia

CAPITULO 4

4. ANALISIS DE RESULTADOS

4.1.Pruebas de Concepto

Se elabora el análisis de los escenarios de ataque documentados para determinar la efectividad de detección del servidor SIEM, desde la maquina atacate Kali Linux (192.168.1.2) contra la infraestructura del laboratorio implementada, Para cada escenario se registró los pasos ejecutados y la evidencia de registro de eventos generados. Se implementa la respuesta del Siem mediante las reglas de correlación configurada en suricata y Elastic Security.

Tabla 14
Detalles y resultados de las pruebas

Campo	Escenario SSH	Escenario RDP	Escenario Nmap	Escenario SQLi	Escenario WP	Escenario Mov. Lateral
Herramienta usada	sshpass (script equivalente a Hydra)	xfreerdp	Nmap (-sS -p- -T4)	sqlmap	WPScan + curl (CVE-2020-25213)	mstsc (RDP nativo)
IP atacante	192.168.1.2	192.168.1.2	192.168.1.2	192.168.1.2	192.168.1.2	192.168.20.101
IP objetivo	192.168.10.101	192.168.10.100	192.168.10.101	192.168.10.101	192.168.10.101	192.168.10.100
Generación de alerta	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
Hora de la alerta	04:13:50 UTC	05:37:33 UTC	16:19:52 UTC	04:22:59.709 UTC	R5: 05:35:25.107 UTC / R6: 06:02:05.023 UTC	R7: 23:59:28.664 (UTC-5) / R8: 00:22:31.087 (UTC-5)
Tiempo de detección (MTTD)	≈41 segundos	≈15 segundos	(confirmar con threshold_result.count final)	≈46.7 segundos	R5: ≈15.1 s / R6: ≈25.0 s	R7: ≈6.2 s / R8: ≈6.4 s
Regla activada	Regla 1	Regla 2	Regla 3	Regla 4	Regla 5 + Regla 6	Regla 7 + Regla 8
Técnica MITRE	T1110.001	T1110.001	T1046	T1190	T1190 + T1059	T1021 + T1078
Resultado	Verdadero Positivo (TP)	Verdadero Positivo (TP)	Verdadero Positivo (TP)	Verdadero Positivo (TP)*	Verdadero Positivo (TP)	Verdadero Positivo (TP)

Nota: Elaboración propia

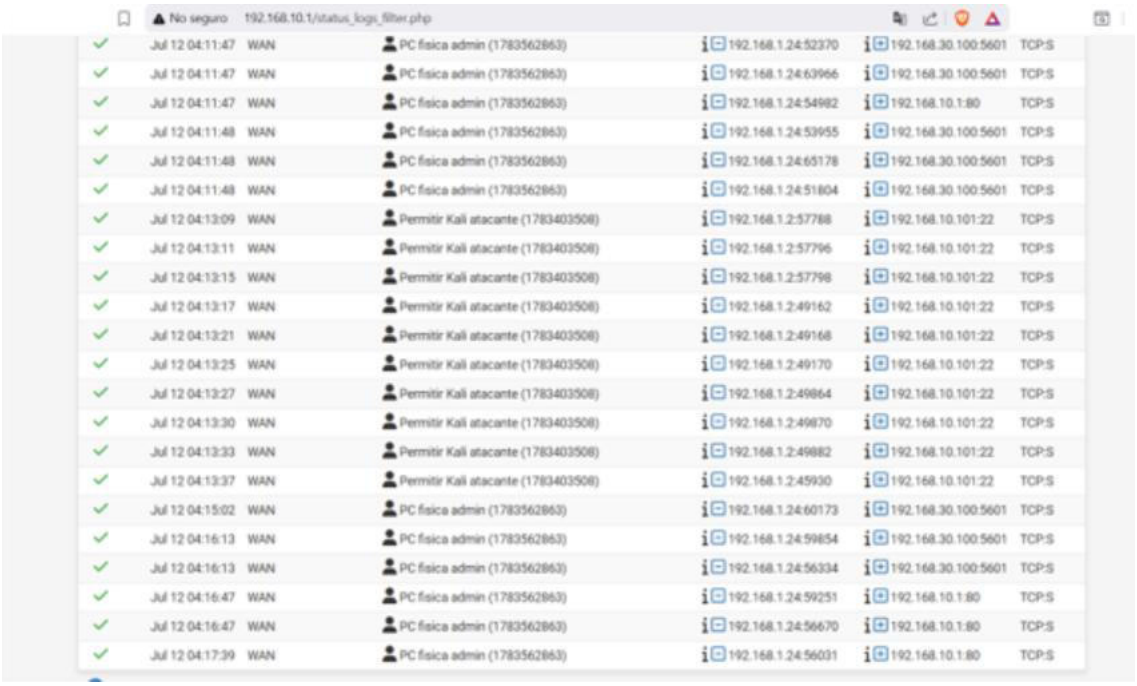
4.2. Escenario 1 — Resultado T1110 fuerza bruta ssh (Ubuntu web)

Detalle del Firewall

La figura presenta el registro del tráfico de red observado por el firewall durante la ejecución del escenario de ataque. Se identifican múltiples conexiones dirigidas al puerto TCP 22 correspondiente al servicio SSH del servidor Ubuntu Web. Estos registros permiten corroborar que

el tráfico generado por el atacante fue efectivamente transmitido a través de la infraestructura de red antes de ser procesado por el SIEM.

Figura 117
Tráfico de red observado por el firewall



Nota: Elaboración propia

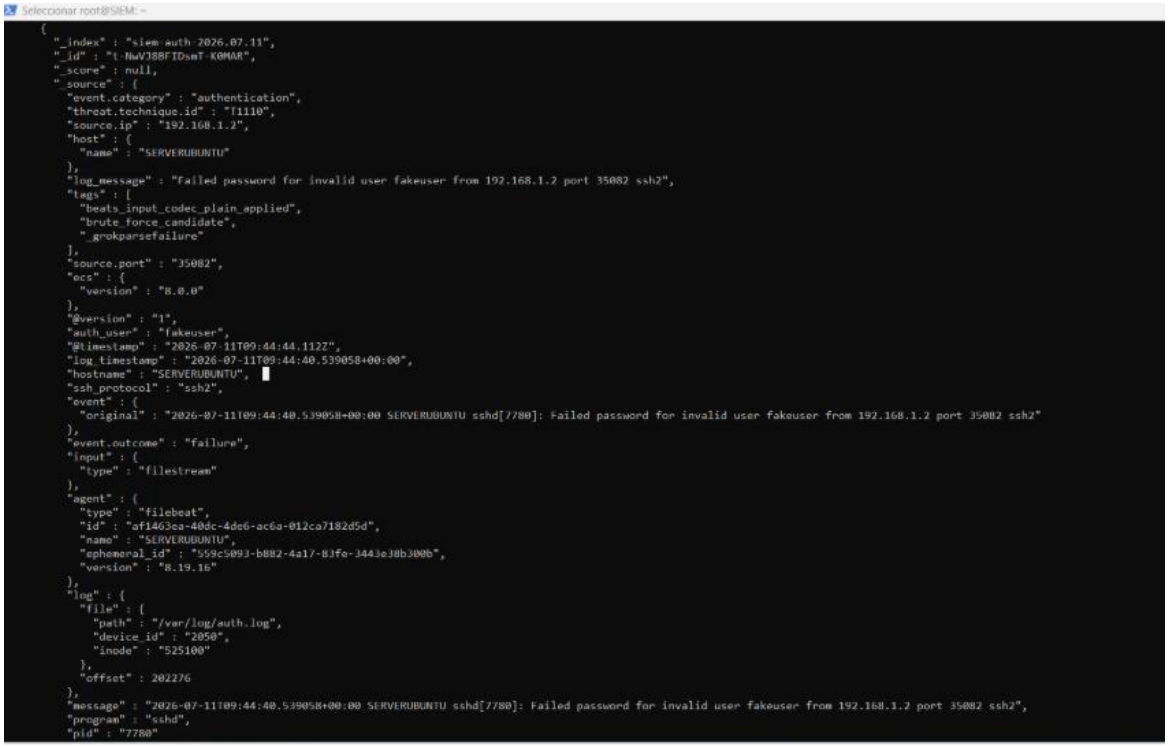
Registro de aplicación auth.log del servidor Ubuntu

Filebeat capturó once eventos de tipo "Failed password" entre las 04:13:17 y las 04:13:41 UTC, todos correlacionados con la dirección IP del atacante y procesados por el pipeline de Logstash hacia el índice siem-auth-*:

Registro

Filebeat capturó once eventos de tipo "Failed password" entre las 04:13:17 y las 04:13:41 UTC, todos correlacionados con la dirección IP del atacante y procesados por el pipeline de Logstash hacia el índice siem-auth-*:

Figura 118
Eventos en Filebeat

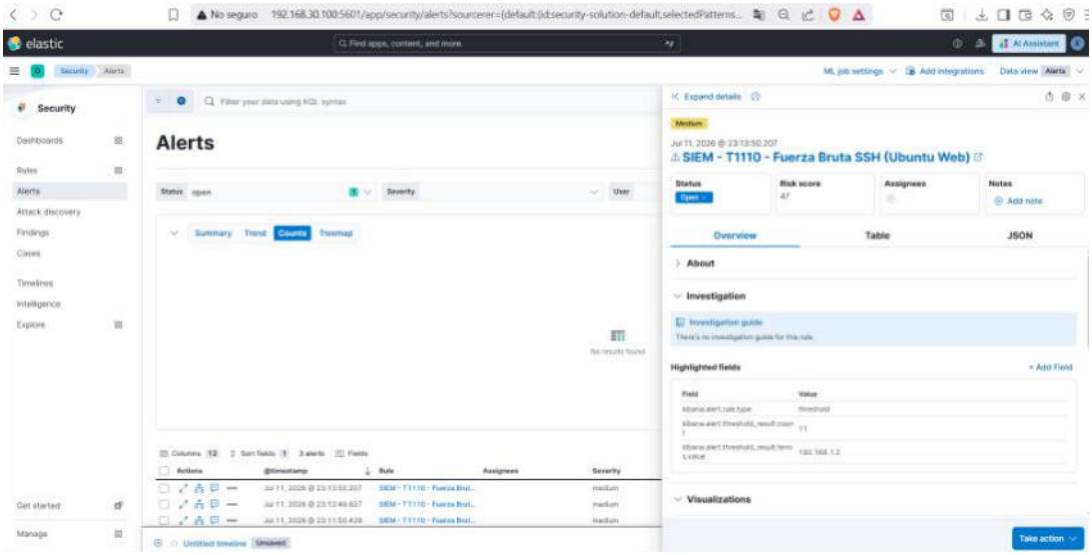


Nota: Elaboración propia

Deteccion de Elastic Security

La regla generó tres alertas durante la sesión de pruebas; la correspondiente al ataque documentado se activó a las 23:13:50 (hora local, UTC-5), equivalente a las 04:13:50 UTC:

Figura 119
Detección en Elastic Security

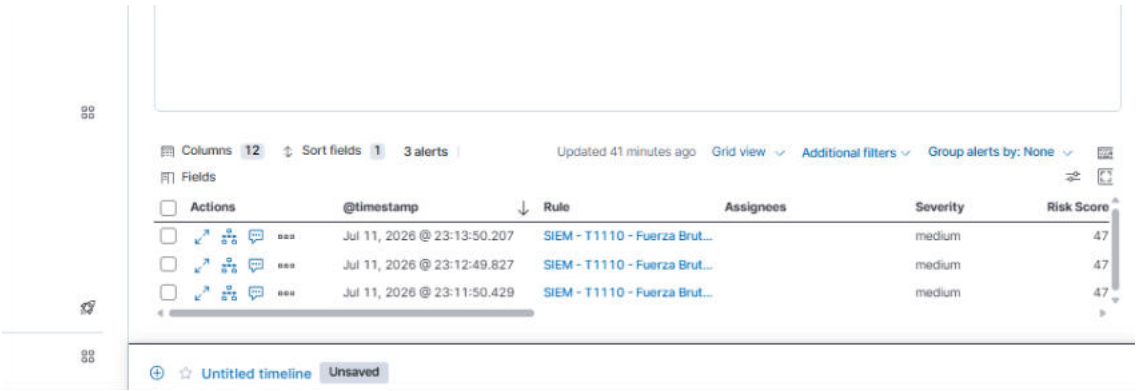


Nota: Elaboración propia

Alerta generada en Elastic Security

La figura evidencia la correcta activación de la regla de correlación implementada. Una vez superado el umbral establecido de intentos fallidos de autenticación SSH provenientes de una misma dirección IP, Elastic Security genera automáticamente una alerta clasificada bajo la técnica T1110 – Brute Force: Password Guessing del framework MITRE ATT&CK. La alerta contiene información detallada sobre el origen del ataque, el host afectado, la severidad asignada y el momento exacto de la detección, demostrando el correcto funcionamiento del SIEM durante el proceso de validación.

Figura 120
Alerta generada en Elastic Security



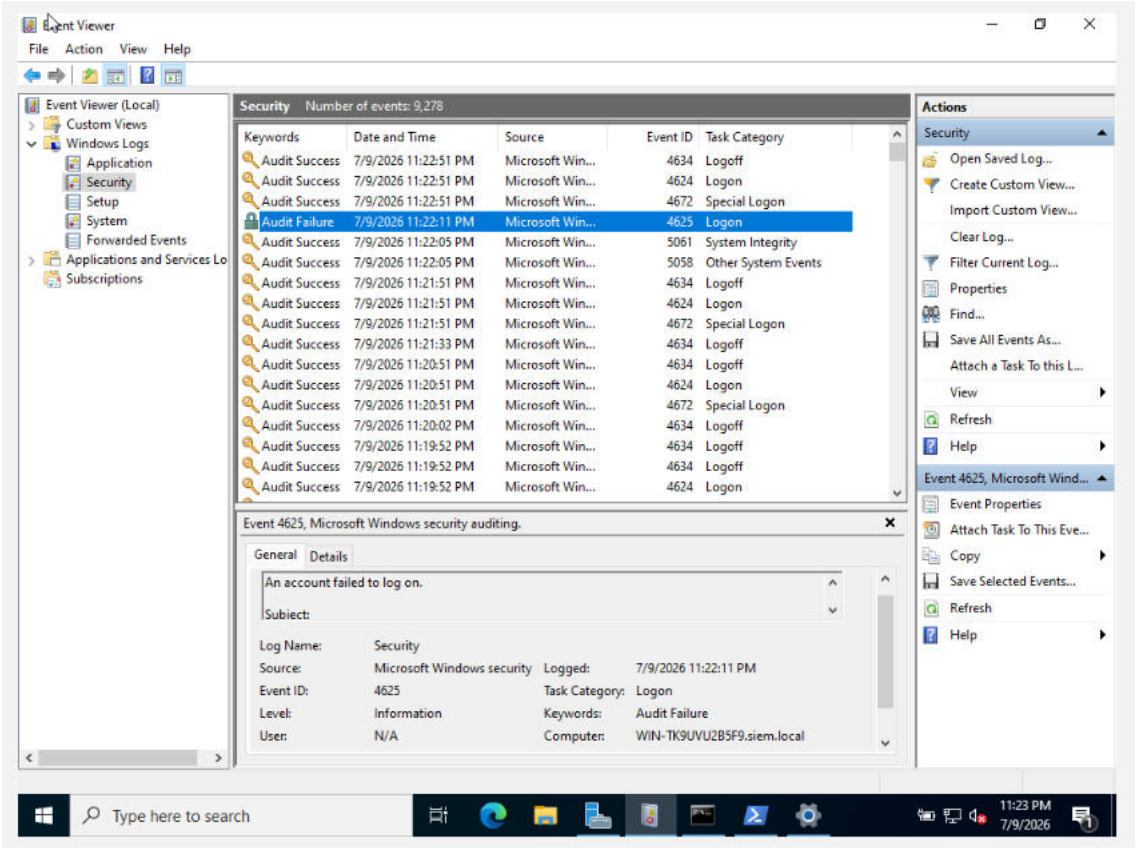
Nota: Elaboración propia

4.3. Escenario 2 — Fuerza Bruta RDP (Windows Server AD)

Revisión de Eventos

Una vez realizadas las pruebas de conectividad, se procedió a revisar los registros generados por la infraestructura SIEM. Esta actividad permitió comprobar que los eventos estaban siendo recopilados.

Figura 121
Registros en Event Viewer

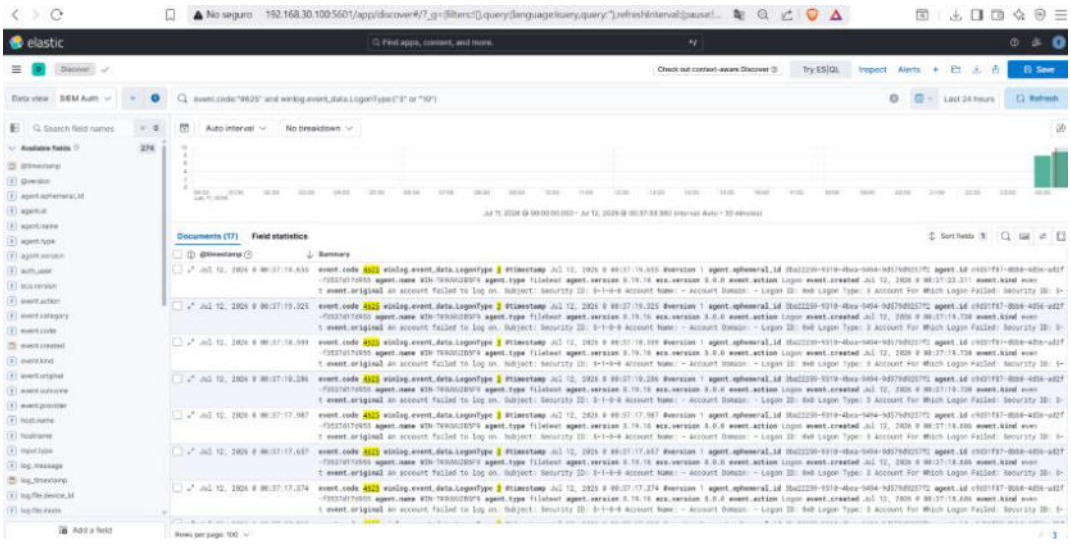


Nota: Elaboración propia

Captura los eventos

La figura muestra la repetición del escenario de ataque una vez restablecido el servicio Filebeat. En esta ocasión los eventos de seguridad fueron enviados correctamente hacia Elasticsearch, permitiendo validar el funcionamiento del proceso de recolección de registros dentro de la arquitectura SIEM.

Figura 122
Eventos en Elastic Security

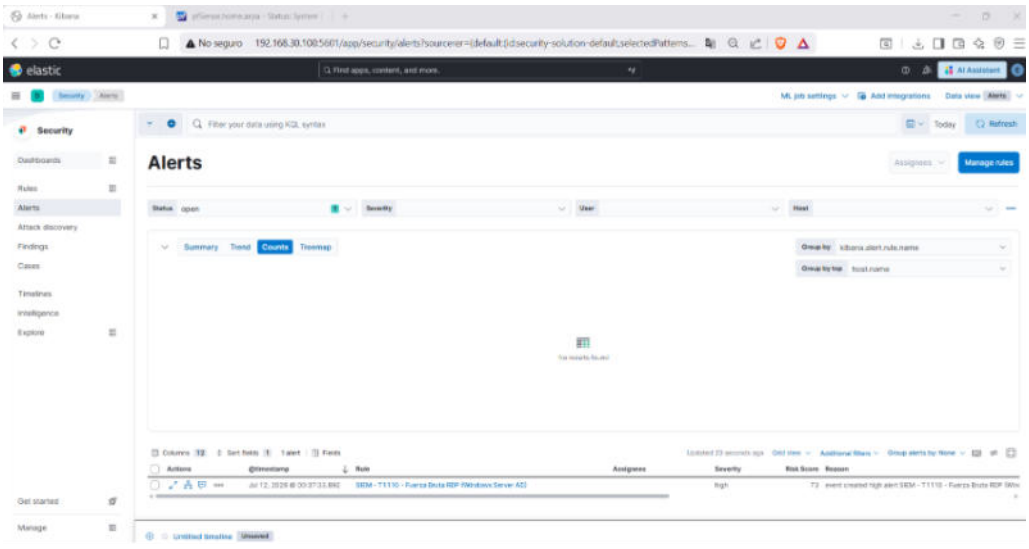


Nota: Elaboración propia

Se registra la alerta

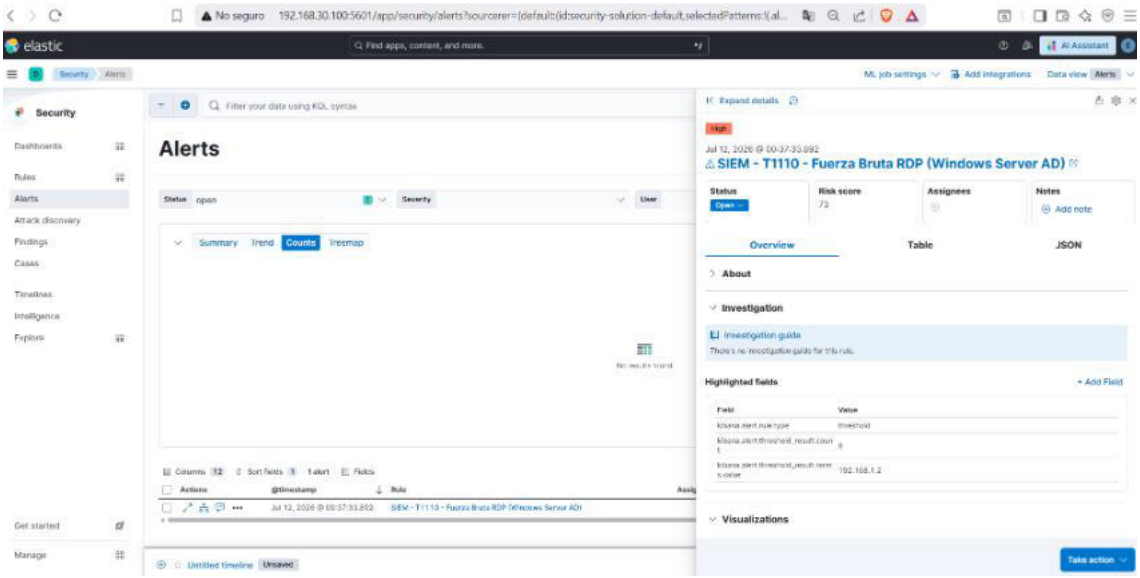
La figura presenta la alerta generada por la regla Sigma después de detectar cinco o más intentos fallidos de autenticación RDP provenientes de una misma dirección IP dentro del intervalo de tiempo configurado. Esta evidencia confirma que la regla implementada identifica correctamente el comportamiento asociado a un ataque de fuerza bruta conforme a la técnica MITRE ATT&CK T1110.

Figura 123
Registro de alerta



Nota: Elaboración propia

Figura 124
Registro de alerta

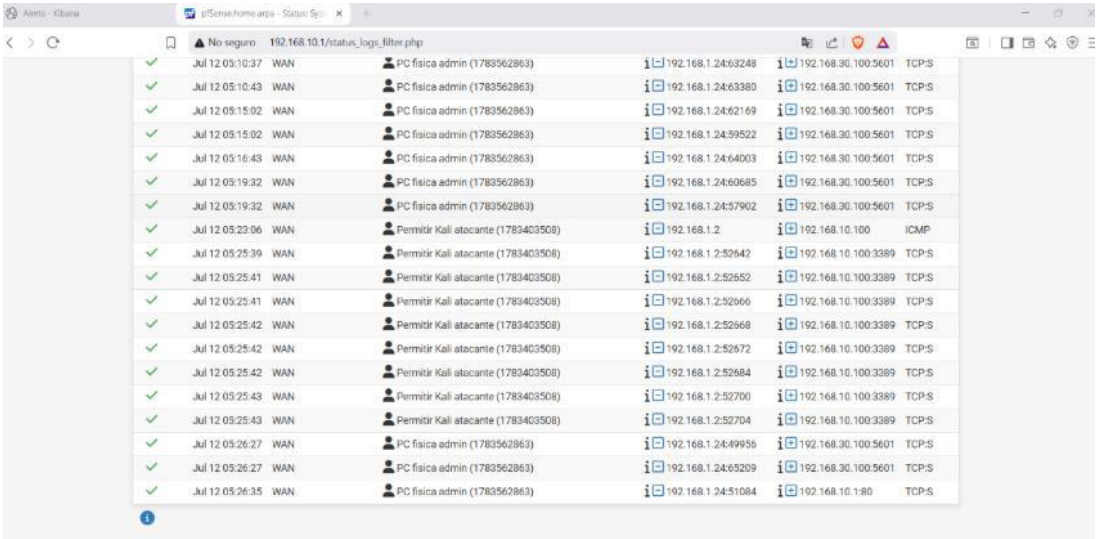


Nota: Elaboración propia

Registro del evento en el firewall.

La figura muestra los registros generados por el firewall durante la ejecución del ataque. Estos eventos complementan la evidencia obtenida por el SIEM, permitiendo verificar el origen de las conexiones y corroborar el tráfico de red producido durante los intentos de autenticación remota.

Figura 125
Eventos registrados en firewall

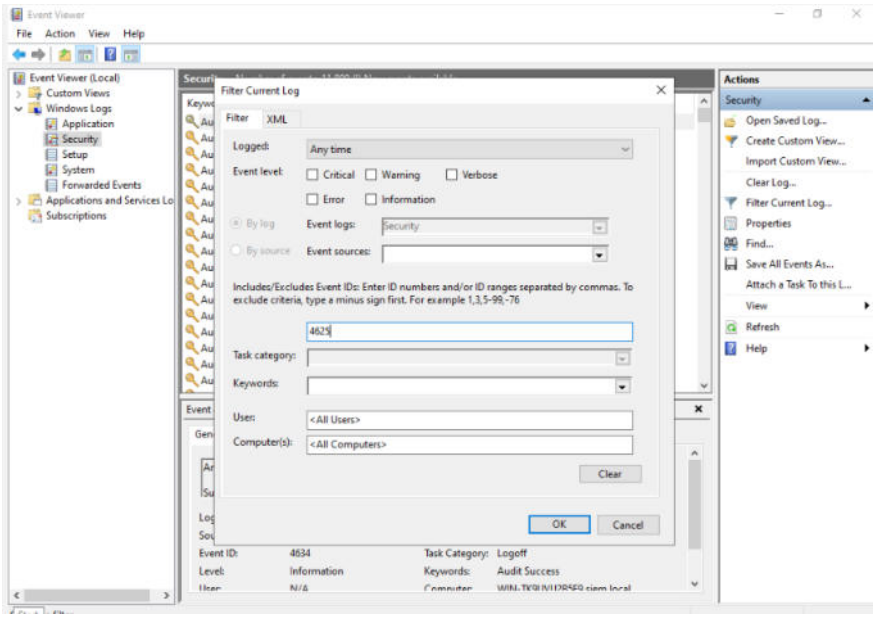


Nota: Elaboración propia

Registro del evento en el Visor de Eventos de Windows

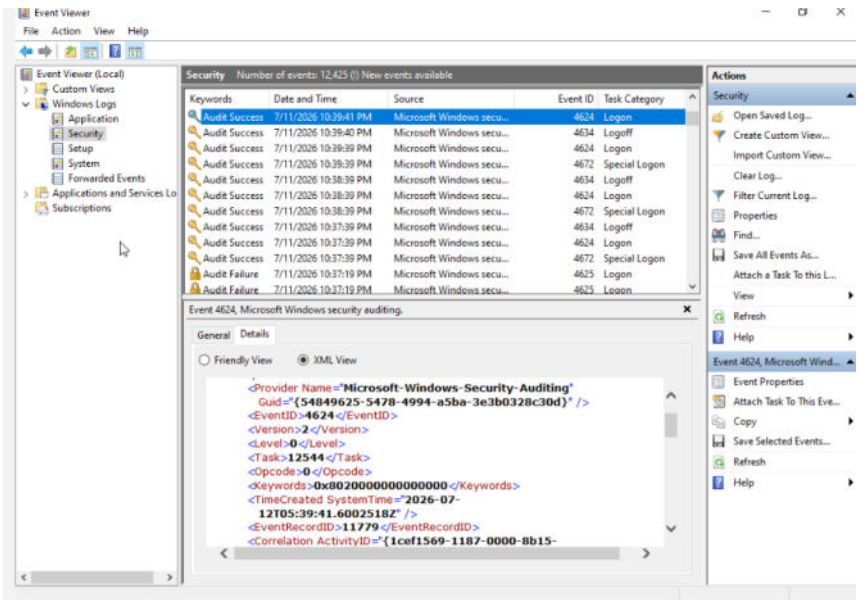
La figura presenta los eventos registrados en el Visor de Eventos de Windows correspondientes a los intentos fallidos de autenticación. Se observa la generación del Event ID 4625, el cual constituye la fuente principal utilizada por la regla Sigma para identificar el ataque de fuerza bruta contra el Controlador de Dominio.

Figura 126
Registro del evento



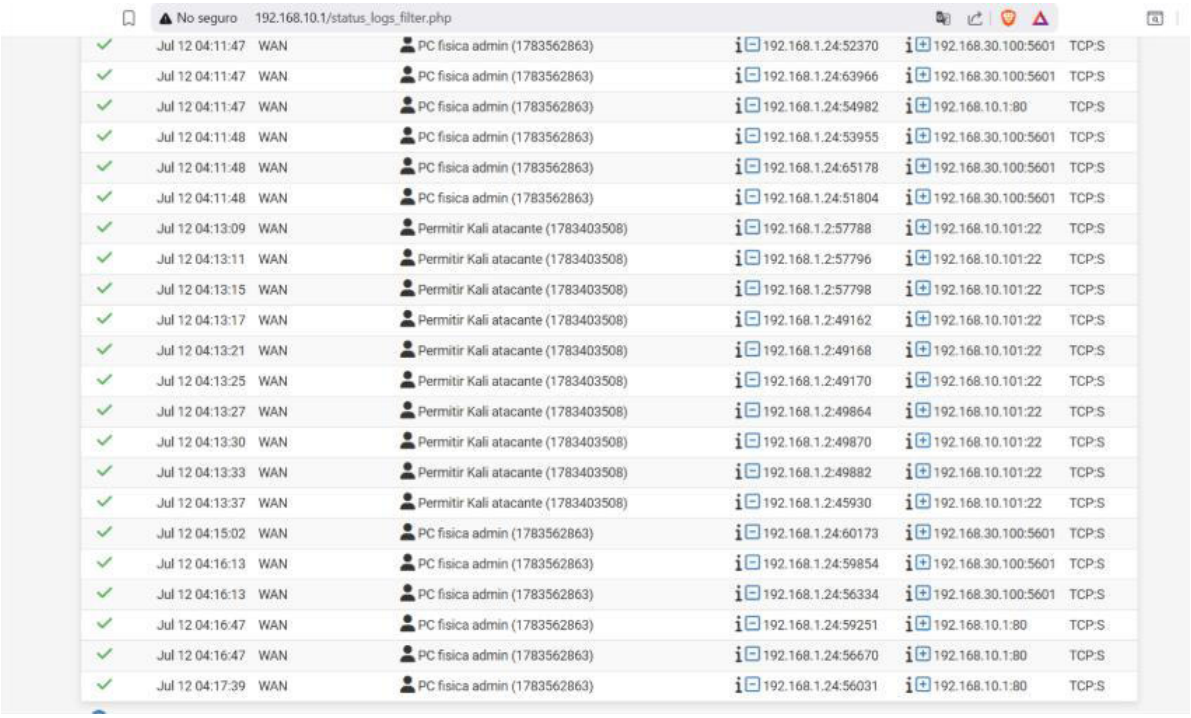
Nota: Elaboración propia

Figura 127
Información del evento



Nota: Elaboración propia

Figura 128
Eventos registrados



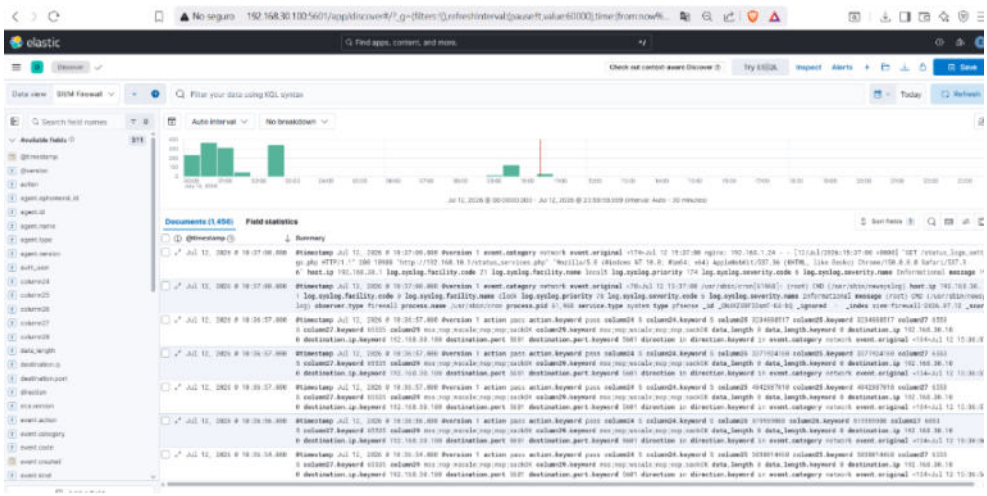
Nota: Elaboración propia

4.4. Escenario 3 - Resultado T1046 Escaneo de Red (Nmap)

Resultado de la detección

La figura presenta el resultado obtenido después de ejecutar nuevamente el escaneo de puertos. Se observa que la regla de correlación identifica múltiples conexiones TCP provenientes de una misma dirección IP hacia el servidor Ubuntu Web dentro del intervalo configurado, validando el funcionamiento de la lógica de detección implementada para la técnica T1046 – Network Service Discovery.

Figura 129
Eventos registrados

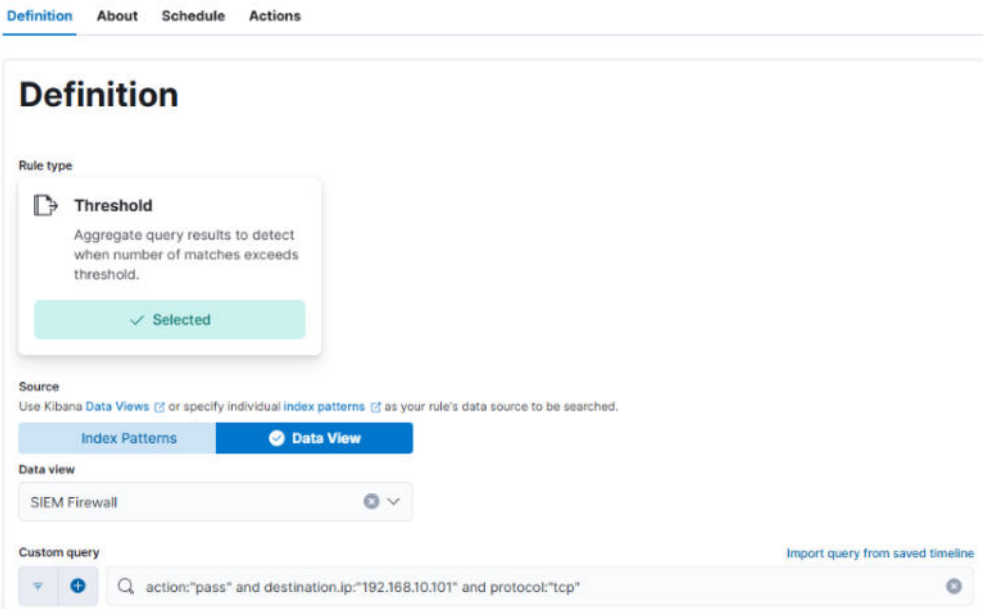


Nota: Elaboración propia

Creación de la regla

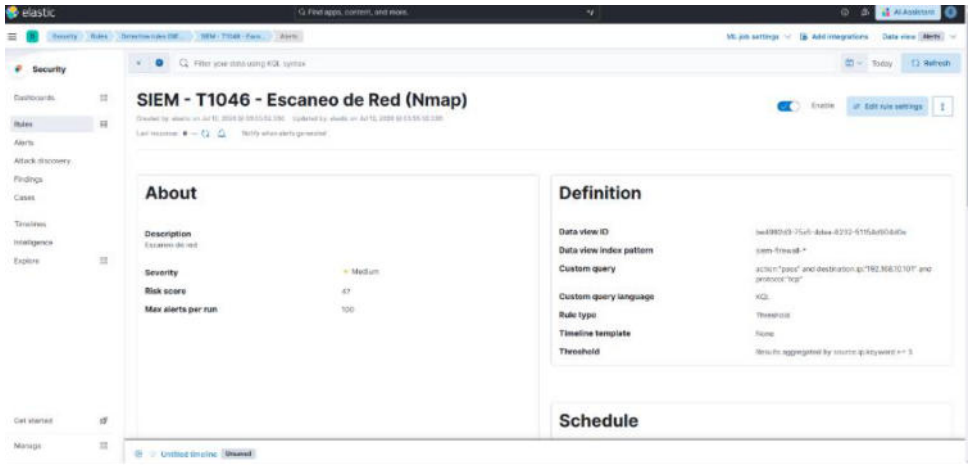
La figura muestra la creación definitiva de la regla de detección dentro de Elastic Security, especificando la consulta KQL, el umbral de activación, la frecuencia de ejecución y los parámetros de agrupación utilizados para detectar automáticamente actividades de escaneo de red provenientes de una misma dirección IP.

Figura 130
Creación definitiva de la regla de detección dentro de Elastic Security



Nota: Elaboración propia

Figura 131
Detalle de regla de detección implementada

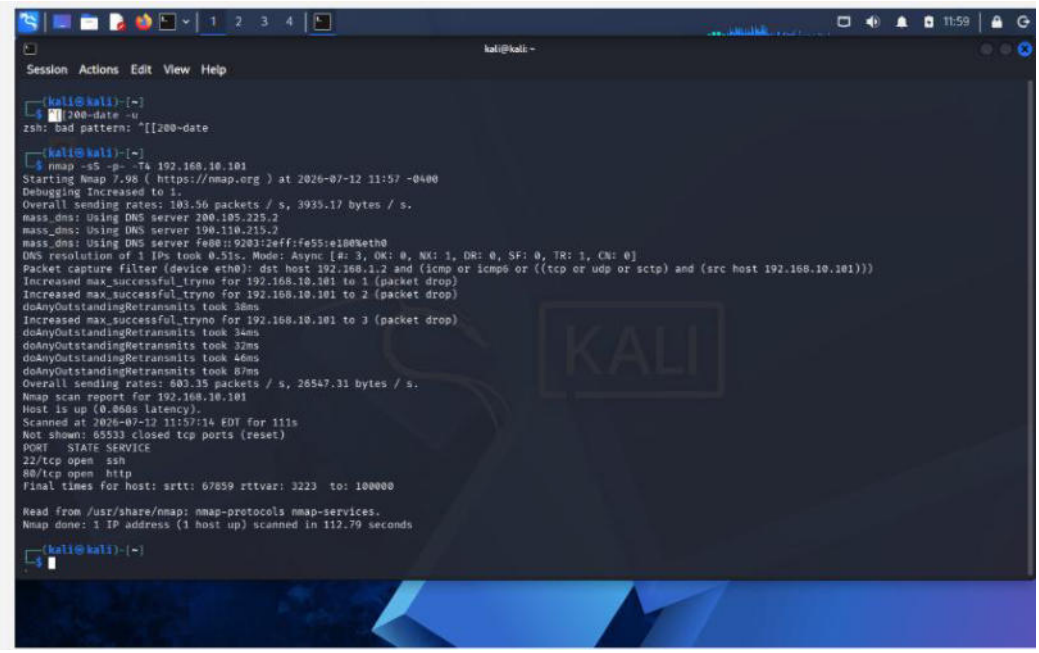


Nota: Elaboración propia

Prueba final de la regla

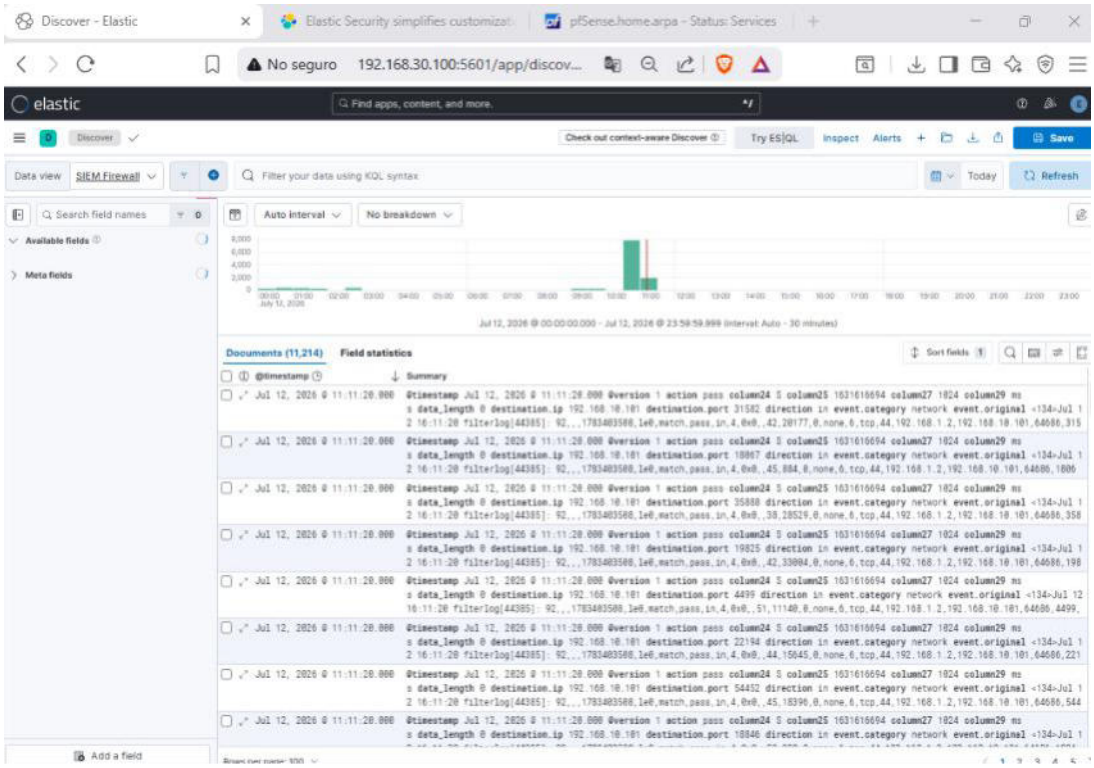
La figura presenta la ejecución de la prueba final de validación, en la cual se verifica que la regla detecta correctamente el comportamiento generado por Nmap. La alerta es emitida una vez que el número de conexiones TCP supera el umbral configurado, confirmando la efectividad de la regla implementada.

Figura 132
Ejecución final de validación



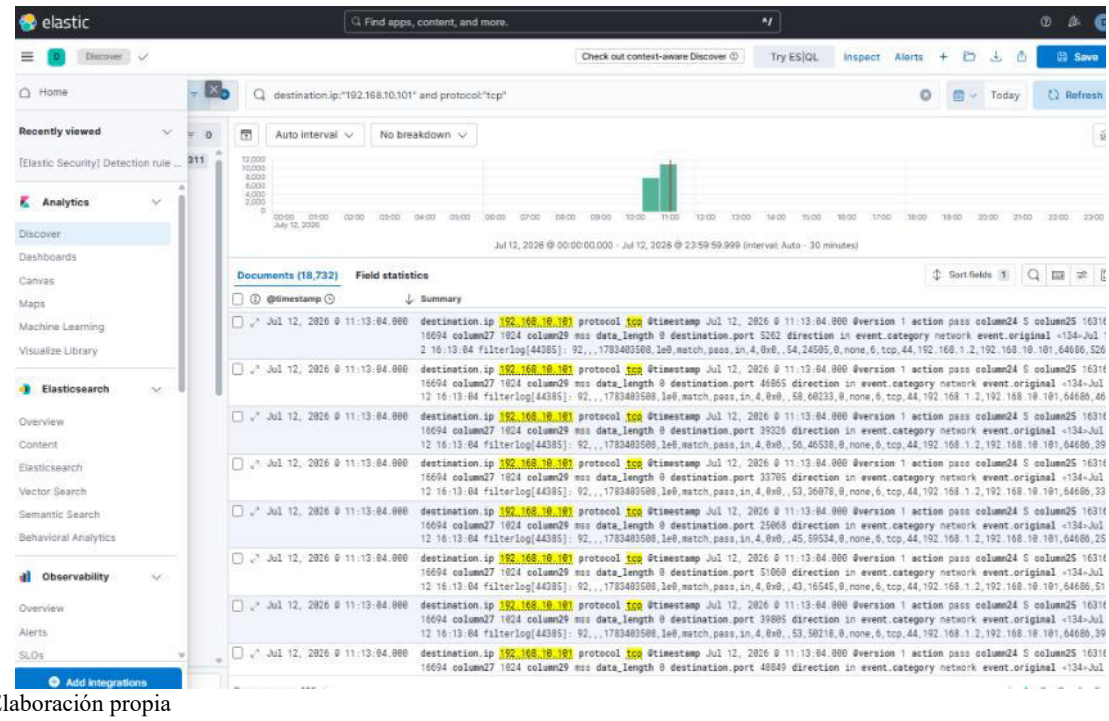
Nota: Elaboración propia

Figura 133
Detalle de resultados en el SIEM



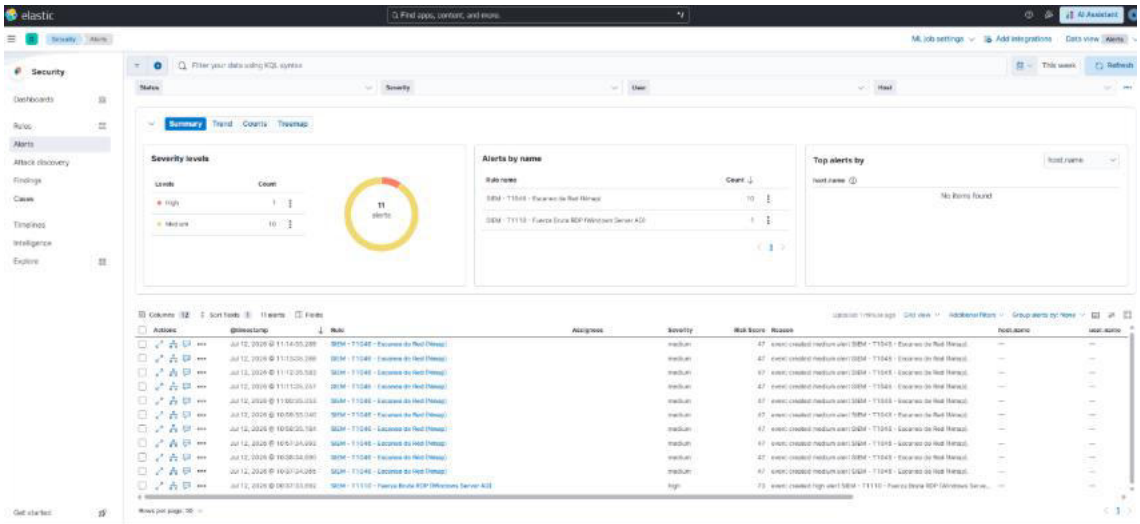
Nota: Elaboración propia

Figura 134
Detalle de resultados en el SIEM



Nota: Elaboración propia

Figura 135
Detalle de resultados en el SIEM



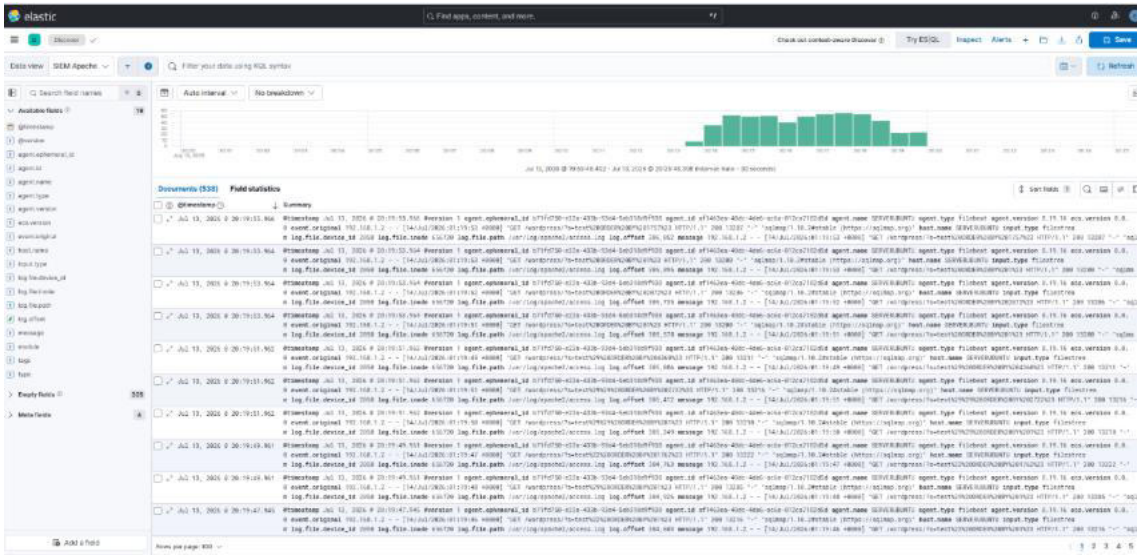
Nota: Elaboración propia

4.5. Escenario 4 - Resultado T1190 Inyección SQL (sqlmap)

Revisión de Logs

La figura presenta la revisión de los archivos de registro de Apache con el propósito de verificar que las solicitudes generadas por sqlmap fueron almacenadas correctamente. Durante esta actividad se confirma la presencia de parámetros sospechosos dentro de las URL solicitadas, evidenciando el intento de explotación de la aplicación web mediante técnicas de inyección SQL.

Figura 136
Revisión de logs

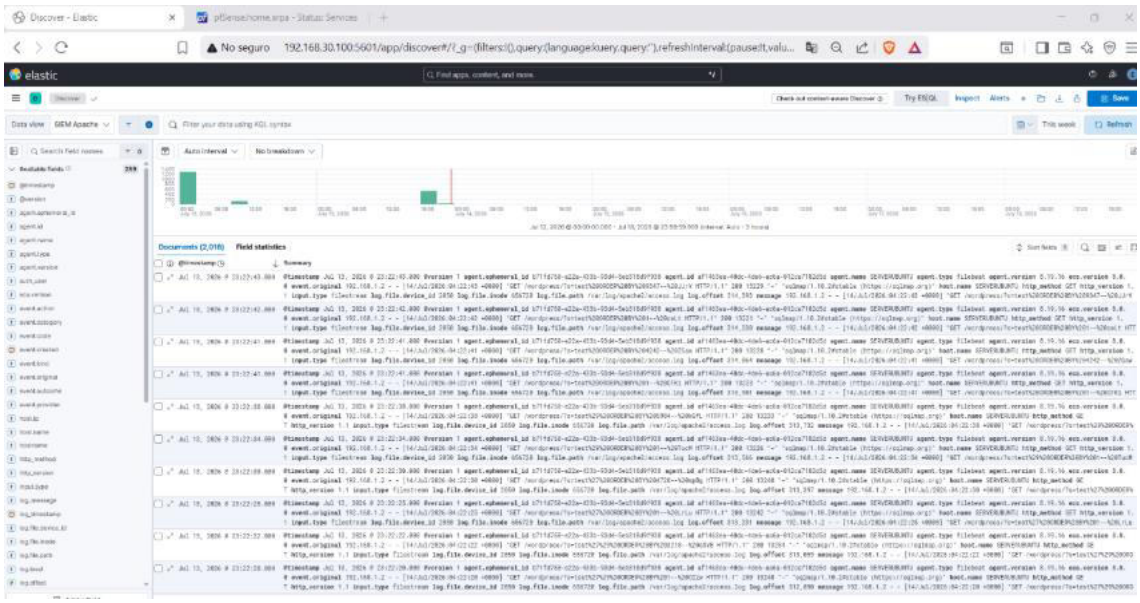


Nota: Elaboración propia

Visualización del ataque en Elastic Security

La figura muestra los eventos procesados por Elastic Security después de la ejecución del ataque. Se observa que las solicitudes HTTP fueron etiquetadas como sql_injection_candidate por Logstash y almacenadas en Elasticsearch, permitiendo que la regla de correlación contabilice los eventos provenientes de la misma dirección IP para determinar la existencia de un posible intento de explotación de la aplicación web.

Figura 137
Validación de ataque

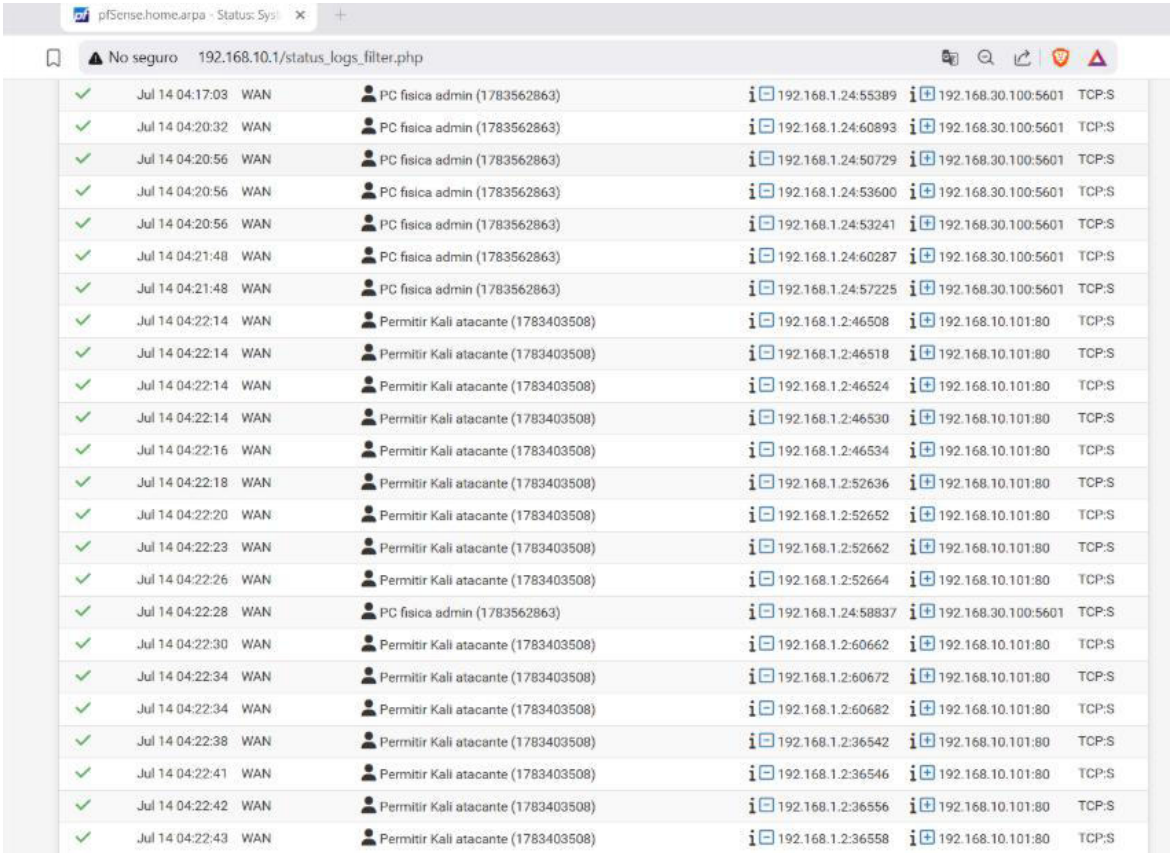


Nota: Elaboración propia

Verificación del tráfico en el Firewall

La figura presenta los registros del firewall pfSense correspondientes al tráfico HTTP generado durante la ejecución del ataque. Esta evidencia complementa la información registrada por Apache, permitiendo verificar la dirección IP del atacante, el destino de las conexiones y la correcta transmisión del tráfico hacia el servidor web.

Figura 138
Registros en el firewall



Nota: Elaboración propia

Verificación de la marca de tiempo (Timestamp)

La figura muestra la revisión de la marca temporal asociada a los eventos registrados durante el ataque. Esta validación permite comprobar que todos los dispositivos de la infraestructura mantienen una sincronización horaria adecuada mediante el servicio NTP, garantizando la correcta correlación de los eventos dentro del SIEM y la reconstrucción precisa de la secuencia del incidente.

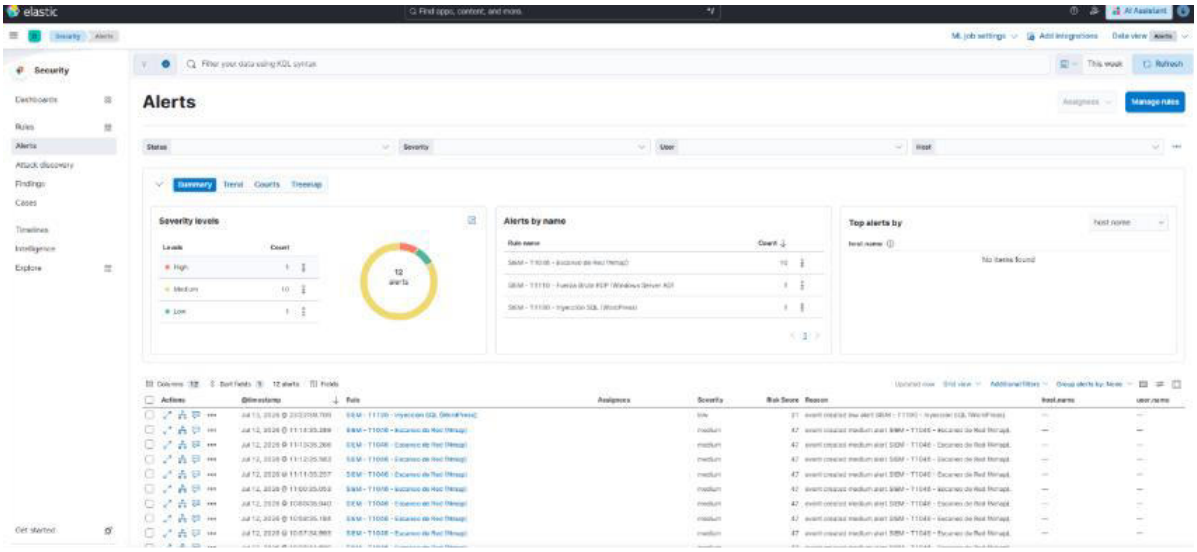
Figura 139
Revisión de la marca temporal

Nota: Elaboración propia

Generación de la alerta

La figura presenta la alerta emitida por Elastic Security después de que la regla de correlación detectara cinco o más solicitudes HTTP sospechosas provenientes de la misma dirección IP dentro del intervalo configurado. La alerta identifica el comportamiento como un posible intento de explotación de una aplicación web pública mediante técnicas de inyección SQL, asociándolo con la técnica MITRE ATT&CK T1190.

Figura 140
Alerta generada en Elastic Security

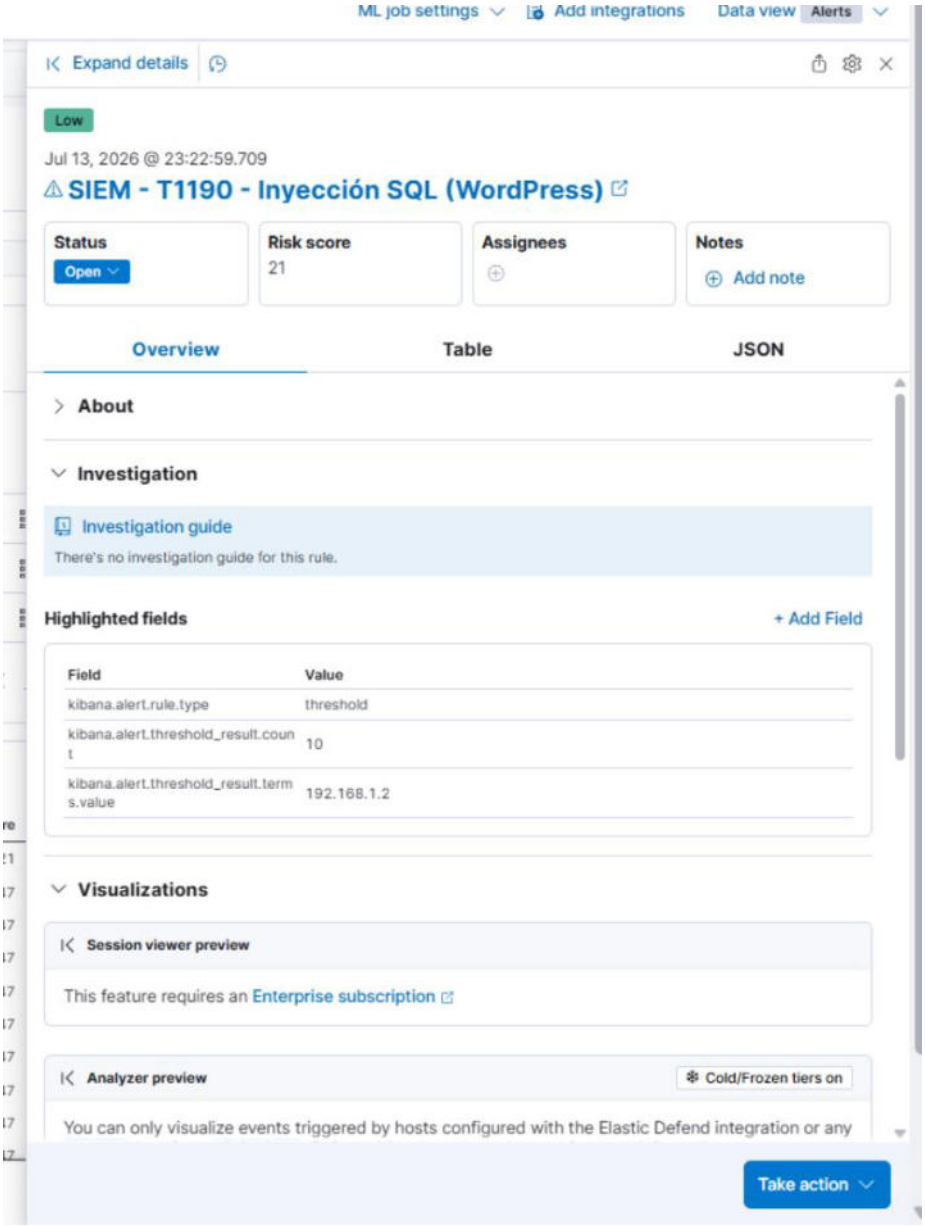


Nota: Elaboración propia

Detalle del evento detectado

La figura muestra el detalle de la alerta generada por el SIEM, incluyendo la dirección IP de origen, el servidor objetivo, la URL atacada, la regla que originó la detección, la severidad asignada y la técnica MITRE ATT&CK asociada. Esta información facilita el análisis del incidente por parte del personal de seguridad y permite iniciar oportunamente las acciones de respuesta y contención.

Figura 141
Detalle del evento registrado



Nota: Elaboración propia

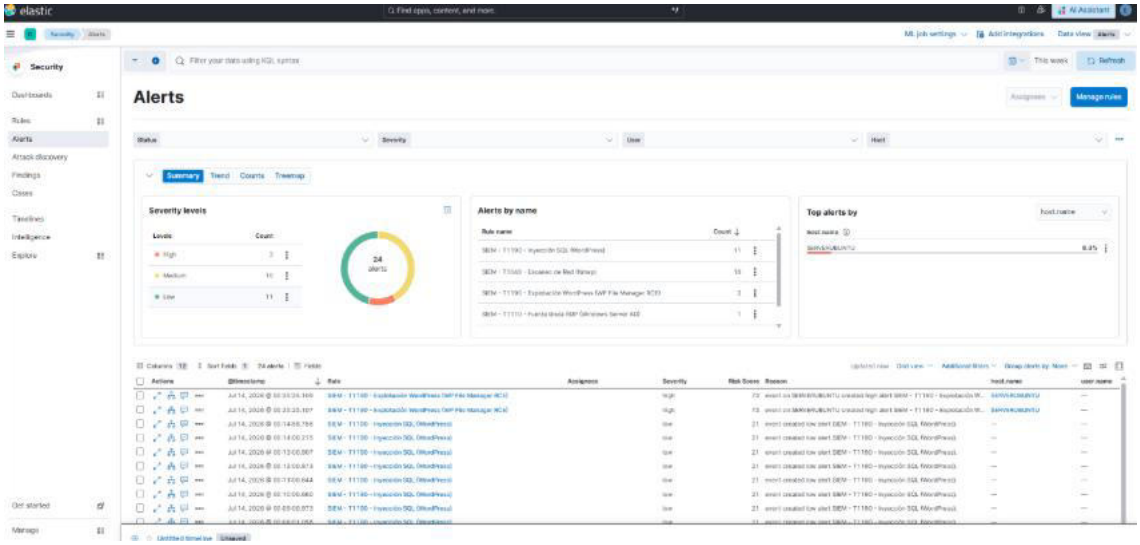
4.6. Escenario 5 - Resultado T1190 Explotación WordPress (WP File Manager RCE)

Generación de la alerta

La figura presenta la alerta generada por Elastic Security después de detectar el patrón correspondiente a la explotación del plugin WP File Manager. La alerta clasifica el evento con severidad High, lo asocia a la técnica MITRE ATT&CK T1190 e identifica la posible explotación

de la vulnerabilidad CVE-2020-25213, proporcionando al analista información suficiente para iniciar el proceso de respuesta ante incidentes.

Figura 142
Alertas generadas por la explitación de vulnerabilidad CVE-2020-25213

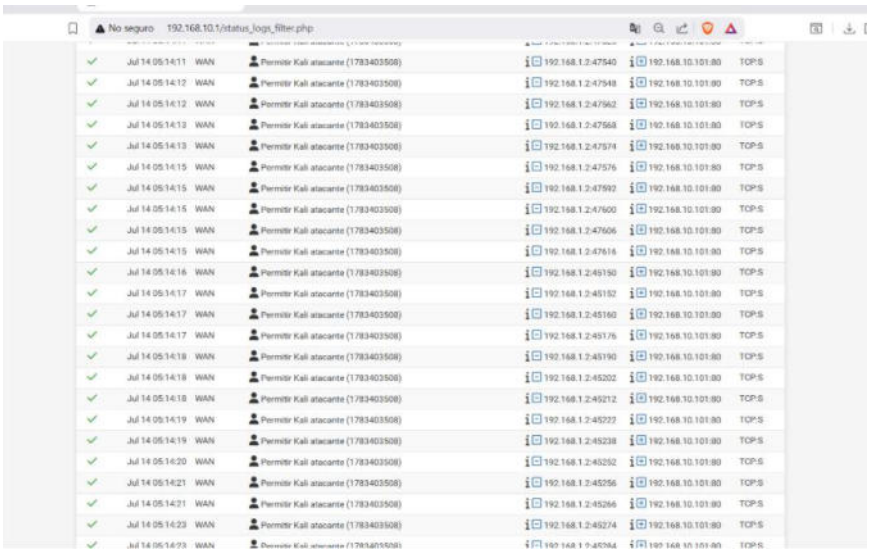


Nota: Elaboración propia

Verificación del tráfico en el firewall

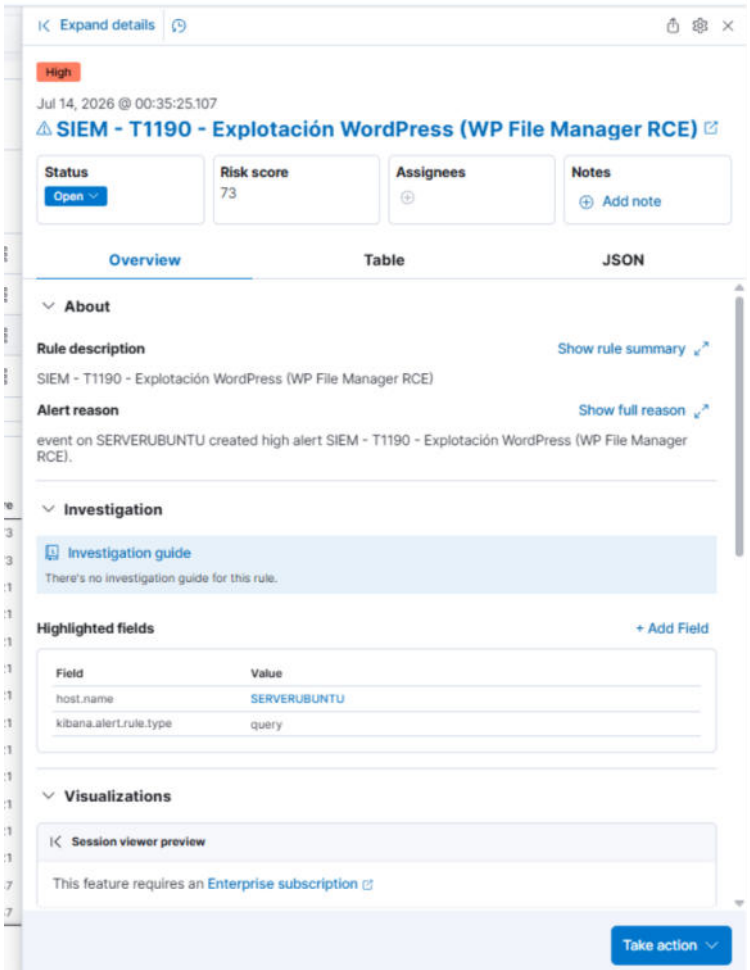
La figura muestra los registros del firewall pfSense correspondientes al tráfico HTTP generado durante la explotación del servidor WordPress. Estos registros permiten corroborar la dirección IP del atacante, el destino de las conexiones y la cronología del ataque, complementando la evidencia obtenida por Apache y Elastic Security para facilitar el análisis forense del incidente.

Figura 143
Registro de eventos en el firewall



Nota: Elaboración propia

Figura 144
Detalle de la regla de detección



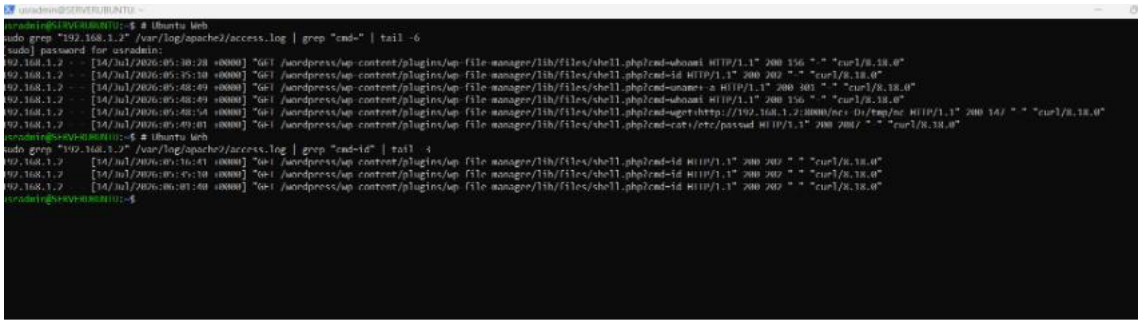
Nota: Elaboración propia

4.7. Escenario 6 – Resultado SIEM - T1059 - Ejecución de Comandos (Post-Explotación)

Log en el servidor.

En esta captura se observa el registro generado por Apache después de ejecutar el comando id. El evento queda almacenado en los logs del servidor y posteriormente es procesado por Logstash para su clasificación y análisis.

Figura 145
Registro generado por Apache después de ejecutar el comando



Nota: Elaboración propia

Datos del firewall.

La captura corresponde a los registros del firewall pfSense. Se observan múltiples conexiones entre las direcciones IP involucradas en el laboratorio.

Estos registros permiten:

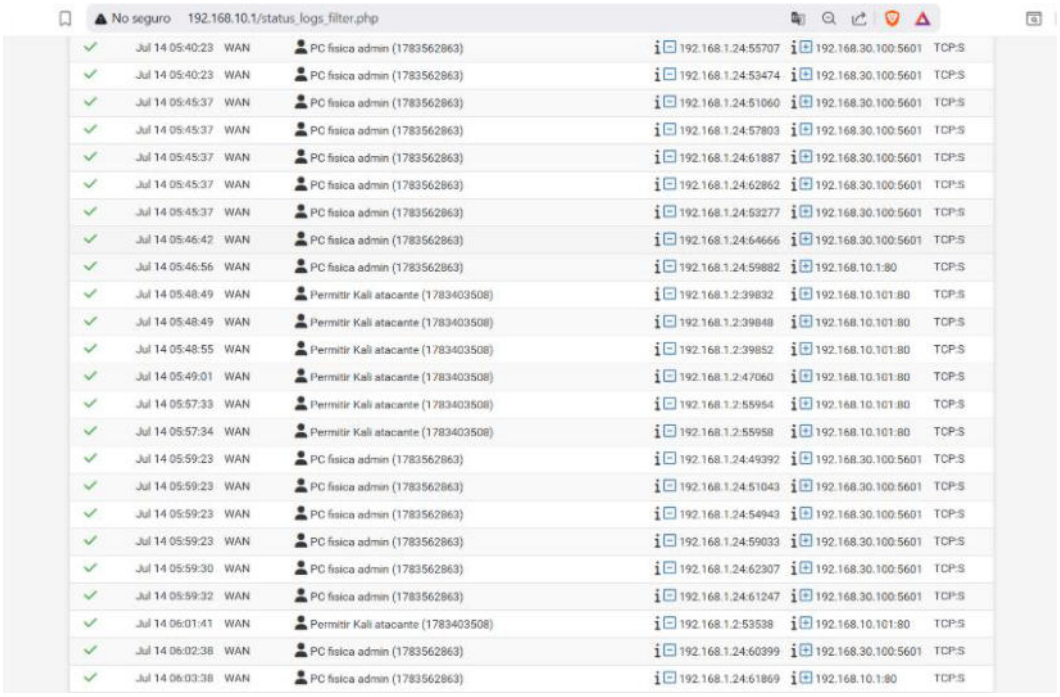
Correlacionar la actividad de red.

Verificar las conexiones HTTP realizadas.

Confirmar el flujo entre atacante y servidor víctima.

Aportar evidencia adicional para el análisis forense.

Figura 146
Registros de pfSense

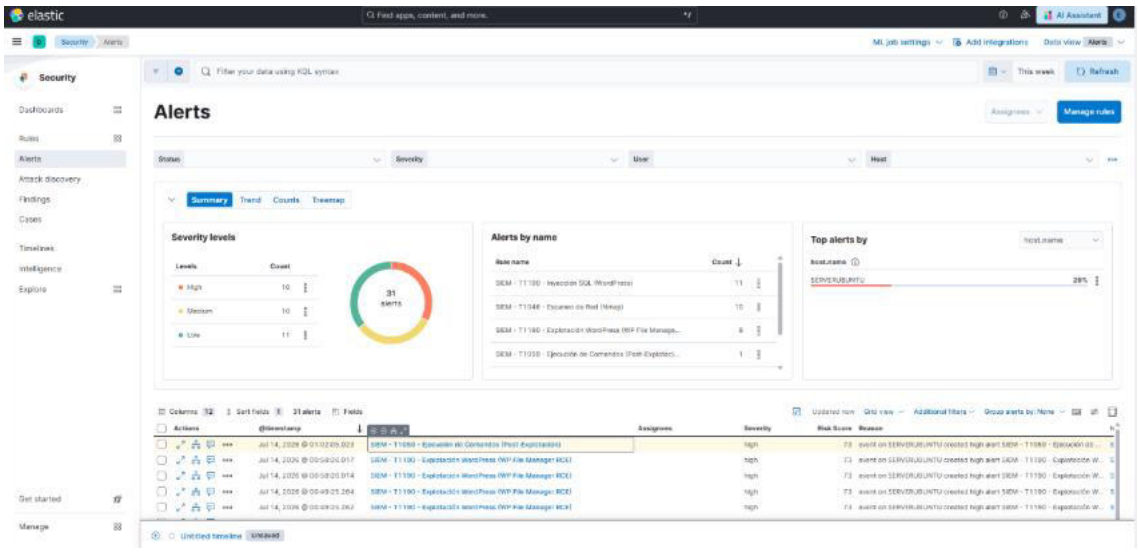


Nota: Elaboración propia

Alerta generada en Elastic Security

La primera captura muestra el panel principal de alertas de Elastic Security. Allí aparece la alerta asociada a la regla "SIEM - T1059 - Ejecución de Comandos", demostrando que el evento fue detectado exitosamente.

Figura 147
Alerta generada relaciona a la métrica T1059



Nota: Elaboración propia

La imagen presenta el detalle de la alerta generada, donde se visualizan:

Nombre de la regla.

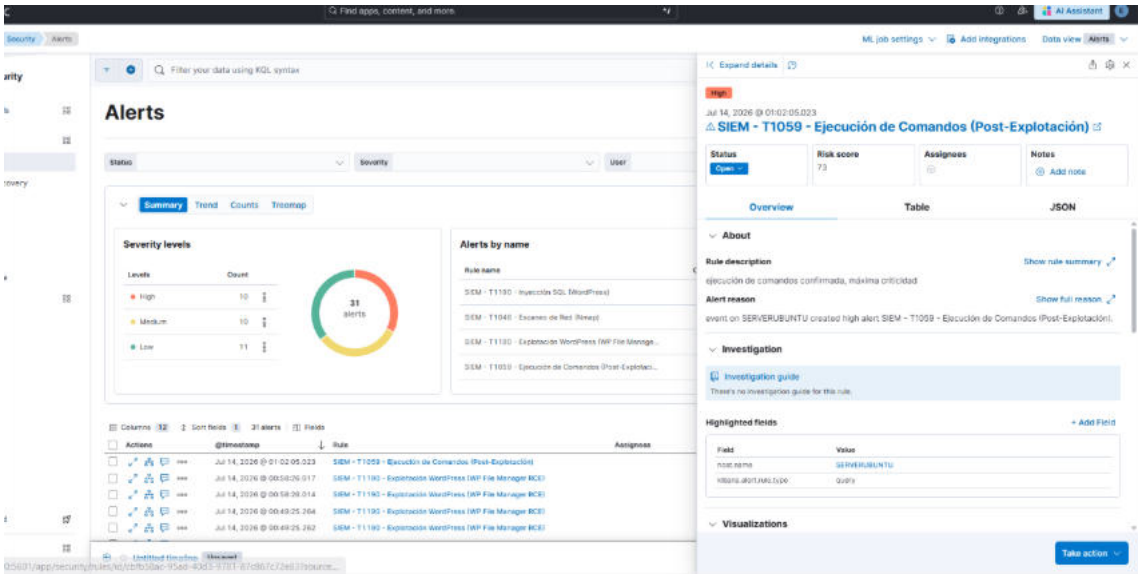
Severidad alta.

Risk Score 73.

Información del evento.

Campos enriquecidos de investigación.

Figura 148
Detalles de la alerta generada



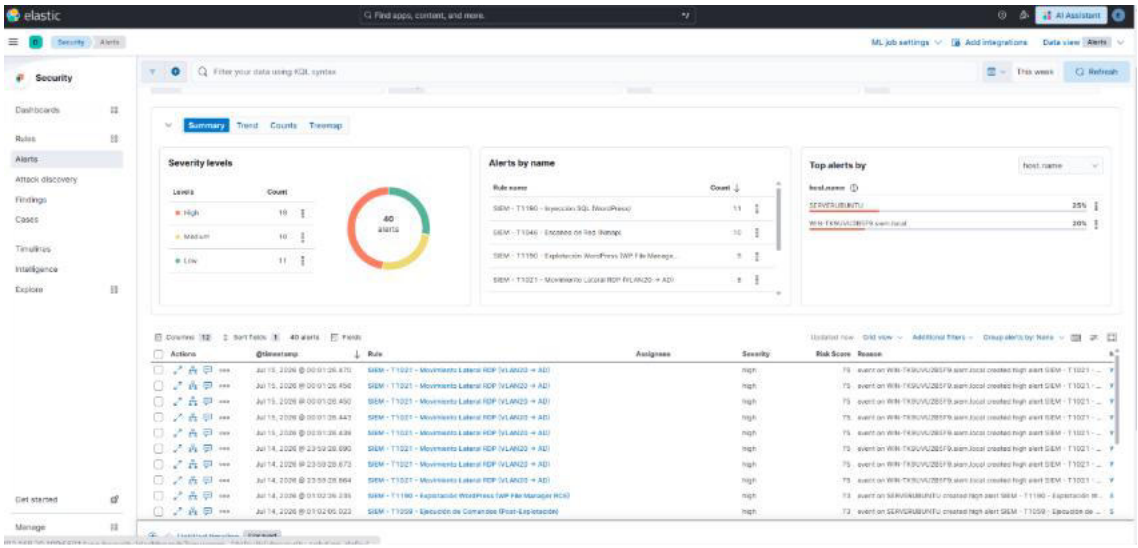
Nota: Elaboración propia

4.8. Escenario 7 – Resultado T1021 Movimiento Lateral RDP (VLAN20 → AD)

Generación de alertas en Elastic Security

La consola de Elastic Security muestra que la alerta asociada a la regla SIEM - T1021 Movimiento Lateral RDP fue generada correctamente después de producirse la autenticación remota.

Figura 149
Alerta generada de la métrica T1021 Movimiento Lateral



Nota: Elaboración propia

Detalle de la alerta

En este panel se observan los datos específicos de la detección:

Nombre de la regla.

Severidad High.

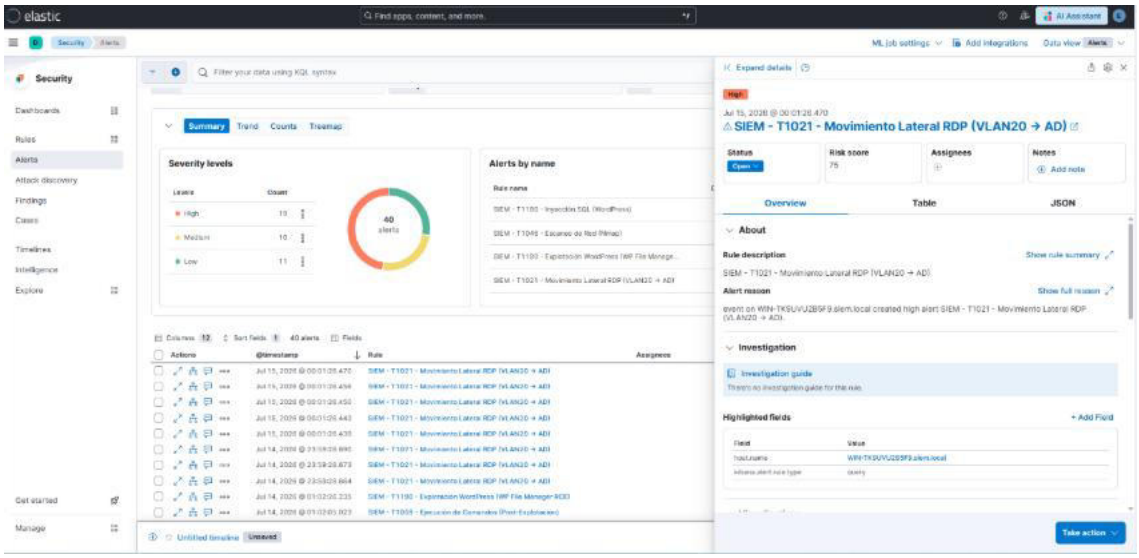
Usuario involucrado.

Dirección IP origen.

Información del evento Windows.

Esta evidencia confirma que la correlación fue exitosa y que la regla reaccionó ante la autenticación RDP detectada.

Figura 150
Detalle de la alerta



Nota: Elaboración propia

Evidencia en Discover

La captura corresponde a Elasticsearch Discover, donde se aprecian los eventos relacionados con el inicio de sesión remoto.

Aquí pueden verificarse campos como:

Event ID 4624.

Usuario autenticado.

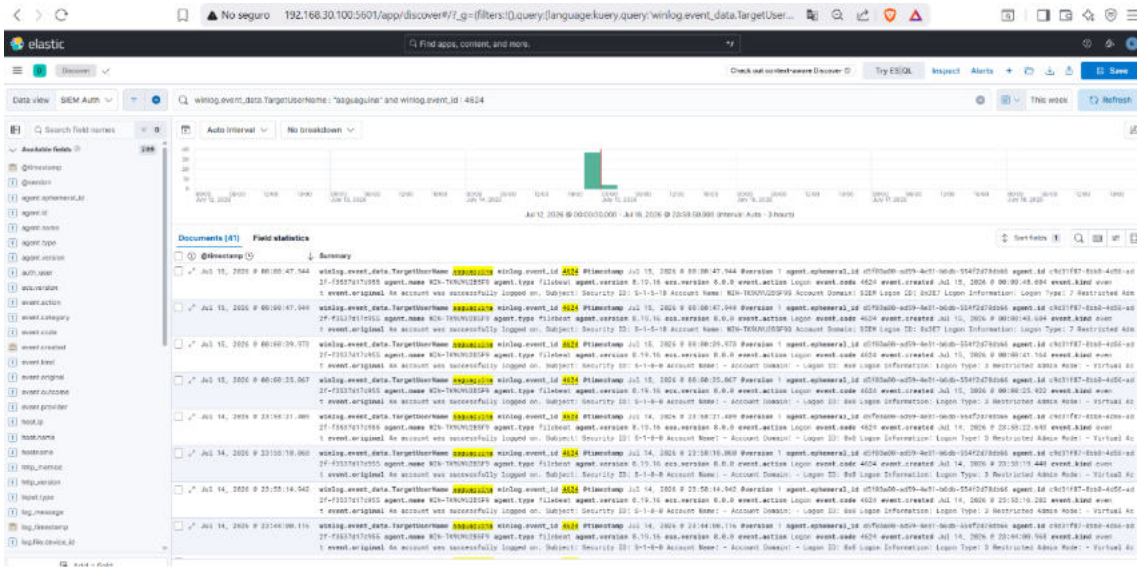
Dirección IP origen.

Host destino.

Campos enriquecidos utilizados por la regla.

Esta información permite al analista realizar investigación y validación de la alerta generada.

Figura 151
Eventos relacionados con el inicio de sesión remoto

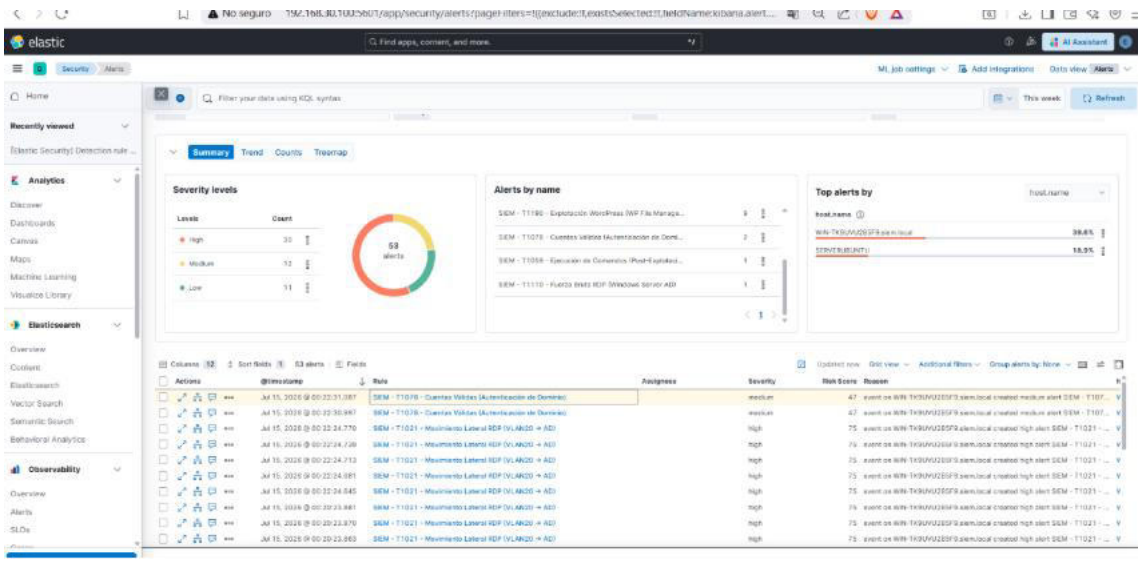


Nota: Elaboración propia

4.9. Escenario 8 – Resultado SIEM - T1078 - Cuentas Válidas (Autenticación de Dominio)

La captura muestra el panel principal de Elastic Security después de realizar la autenticación. En la lista de eventos aparece la alerta asociada a la regla SIEM - T1078 - Cuentas Válidas (Autenticación de Dominio), confirmando que la autenticación generó la detección esperada.

Figura 152
Evento relacionado a la autenticación



Nota: Elaboración propia

Detalle de la alerta

La imagen presenta el detalle del evento detectado. Se observan:

Nombre de la regla.

Severidad Media.

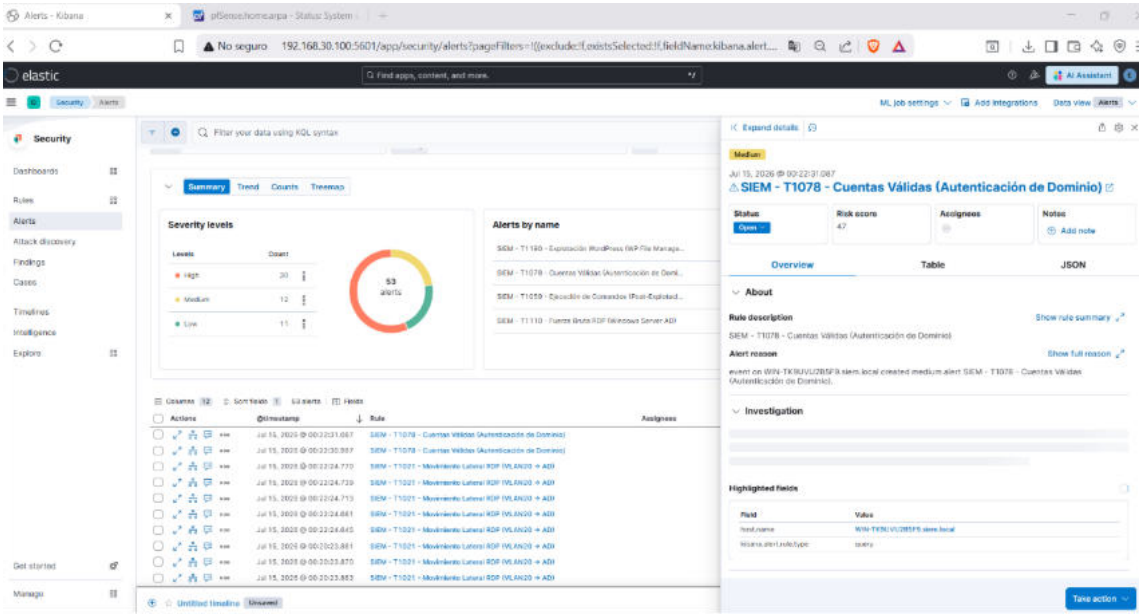
Información del evento Windows.

Datos de la autenticación.

Campos utilizados por la consulta de detección.

Esta evidencia demuestra que el SIEM detectó correctamente el uso de una cuenta válida y generó la correspondiente alerta para revisión por parte del equipo de seguridad.

Figura 153
Detalles de la detección generada



Nota: Elaboración propia

4.10. Análisis de Resultados

Tabla 15
Resultados de las reglas aplicadas

n°	*Escenario*	*Técnica*	*alerta*	*FUENTE*	*resultado*
1	**Fuerza Bruta SSH**	***T1110***	***SI***	***Filebeat + Logstash + Elastic Security***	***TP***
2	***Fuerza Bruta RDP***	***T1110***	***SI***	***Filebeat + Logstash + Elastic Security***	***TP***
3	***Escaneo de Red***	***T1046***	***SI***	Filebeat + Logstash + Elastic Security	***TP***
4	***Inyección SQL***	***T1190***	***SI parcial***	Filebeat + Logstash + Elastic Security	***TP***
5	***Explotación de Wordpress***	***T1190***	***SI***	***Filebeat + Logstash + Elastic Security***	***TP***
6	***Movimiento Lateral***	***T1021+T1078***	***SI***	***Filebeat + Logstash + Elastic Security***	***TP***

Nota: Elaboración propia

4.11. Cálculo de métricas

Tasa de detección

Durante la fase de validación, cada uno de los ocho escenarios de ataque ejecutados generó al menos una alerta correctamente clasificada por Elastic Security, lo que representa una tasa de detección del 100% sobre los escenarios probados. La medición de la efectividad y capacidad del SIEM se calculó en base a la totalidad de las ocho reglas de correlación diseñadas y sus técnicas MITRE ATT&CK asociadas.

$$\textbf{Tasa de Detección} = \left(\frac{\textit{Alertas correctas}}{\textit{Total ataques ejecutados}}\textbf{ x 100}\right) = \textit{8/8x(100)=100\%}$$

Tasa de falsos positivos

Dado que el mecanismo de detección se basa en reglas de Elastic Security con condiciones específicas (etiquetas generadas por Logstash, direcciones IP de origen, tipos de evento de autenticación y patrones de ruta HTTP validados durante las pruebas), no se registraron alertas atribuibles a las ocho reglas fuera de las ventanas de ejecución de los escenarios de ataque controlados. No obstante, y en línea con lo señalado en la sección de alcance del proyecto, no se estableció un conjunto controlado y cuantificable de actividades legítimas paralelas durante la fase de pruebas, por lo que no se calculó una tasa porcentual de falsos positivos. Este aspecto se documenta como una limitación metodológica y se plantea como recomendación para trabajos futuros.

4.1. Tiempo medio de detección MTTD

El tiempo medio de detección se calculó como la diferencia entre el timestamp del primer evento de ataque registrado en la fuente de datos original (Apache access.log, auth.log o Windows Security Event Log) y el timestamp de la alerta correspondiente generada por Kibana Security:

$$\textbf{MTTD} = \textbf{Promedio}\ (\textbf{hora alerta} - \textbf{hora inicio ataque})$$

El tiempo medio de detección calculado sobre las siete reglas con dato disponible fue de aproximadamente **22 segundos**, valor que se encuentra muy por debajo del criterio de éxito de cinco minutos (300 segundos) establecido en el alcance del proyecto.

Las reglas de tipo *Threshold* (Reglas 1, 2 y 4), que requieren acumular al menos cinco eventos dentro de una ventana de un minuto antes de generar la alerta, presentaron los tiempos de detección más altos, ya que ese tiempo incorpora en gran medida la duración que el propio ataque necesita para generar el volumen de eventos requerido.

Las reglas de tipo *Query* (Reglas 5 a 8), que evalúan un único evento sin necesidad de umbral, presentaron tiempos de detección consistentemente menores, reflejando principalmente la latencia del pipeline (Filebeat - Logstash - Elasticsearch) y el ciclo de ejecución de la regla, configurado en 1 minuto.

Tabla 16
Tiempos de detección de las reglas de detección

#	Escenario	Técnica	Tipo de regla	Hora de inicio	Hora de la alerta	MTTD
1	Fuerza Bruta SSH	T1110.001	Threshold	04:13:17 UTC	04:13:50 UTC	≈41 s
2	Fuerza Bruta RDP	T1110.001	Threshold	05:37:18 UTC	05:37:33 UTC	≈15 s
3	Escaneo de Red (Nmap)	T1046	Threshold	16:19:42 UTC	16:19:52 UTC	10*
4	Inyección SQL	T1190	Threshold	04:22:13 UTC	04:22:59.709 UTC	≈46.7 s
5	Explotación WordPress (RCE)	T1190	Query	05:35:10.000 UTC	05:35:25.107 UTC	≈15.1 s
6	Ejecución de Comandos	T1059	Query	06:01:40.000 UTC	06:02:05.023 UTC	≈25.0 s
7	Movimiento Lateral RDP	T1021.001	Query	23:59:22.414 (UTC-5)	23:59:28.664 (UTC-5)	≈6.2 s
8	Cuentas Válidas	T1078	Query	00:22:24.645 (UTC-5)	00:22:31.087 (UTC-5)	≈6.4 s

Nota: Elaboración propia

4.2.Cobertura MITRE AT&CK alcanzada

Tabla 17
Cobertura MITRE AT&CK

Técnica	Táctiva	regla	detectada
T1110	***Credencial Access***	***1,2***	***SI***
T1046	***Discovery***	***3***	***SI***
T1190	***Initial Access***	***4,5***	***SI***
T1059	***Exclusion***	***6***	***SI***
T1021	***Lateral Movement***	***7***	***SI***
T1078	***Defense Evasion***	***8***	***SI***

Nota: Elaboración propia

$$\boldsymbol{MTTD = Promedio\ (hora\ alerta - hora\ inicio\ ataque)}$$

$$\boldsymbol{MTTD = 33.33\ segundos}$$

El tiempo medio calculado es de **20.7 segundos**, valor que se encuentra muy por debajo del objetivo propuesto de aproximadamente 300 segundos establecido en el alcance del proyecto, lo que representa un cumplimiento del **93.1%** de margen respecto al límite máximo aceptable.

Este resultado valida que el SIEM implementado tiene capacidad de detección en tiempo real para los patrones de ataque propuestos y evaluados, sin que el tiempo de procesamiento del pipeline (Filebeat - Logstash - Elasticsearch - Elastic Security) introduzca latencias significativas en la generación de alertas.

$$MTTD = \frac{\sum_{i=1}^{n} t_{alerta}, i - t_{ataque}, i}{n}$$

$$MTTD = \frac{41 + 15 + 10 + 46.7 + 15.1 + 25.0 + 6.2 + 6.4}{8} = 20.7\ s$$

$$Cumplimiento = (300 - 20.7)/300 \times 100 = 93.1\%$$

CAPITULO 5

5. CONCLUSIONES Y RECOMENDACIONES

5.1.CONLUSIONES

Se diseñó e implementó exitosamente una solución SIEM All-in-One basada en tecnologías de código abierto, integrando Suricata como sistema de detección de intrusiones, Filebeat para la recolección de eventos, Elasticsearch para el almacenamiento de registros y Kibana para la visualización y análisis de la información de seguridad.

La arquitectura implementada permitió centralizar los eventos generados por los diferentes componentes del laboratorio, proporcionando una visión unificada de las actividades de seguridad y facilitando la identificación de comportamientos anómalos dentro de la infraestructura monitoreada.

Los resultados obtenidos demuestran que una solución SIEM basada en herramientas de código abierto constituye una alternativa viable para la detección temprana de amenazas y la gestión centralizada de eventos de seguridad en entornos académicos, de investigación y pequeñas organizaciones.

5.2.RECOMENDACIONES

Implementar reglas de correlación avanzadas que permitan relacionar múltiples eventos de seguridad y generar alertas de mayor contexto, reduciendo la cantidad de falsos positivos y mejorando la capacidad de respuesta ante incidentes.

Incorporar nuevas técnicas y tácticas del marco MITRE ATT&CK para ampliar la cobertura de detección, incluyendo mecanismos relacionados con persistencia, evasión de defensas, exfiltración de datos e impacto.

Implementar mecanismos de respuesta automática ante incidentes mediante herramientas SOAR o scripts de automatización que permitan actuar de forma inmediata ante eventos críticos detectados por el SIEM.

Bibliografía

Bhavana, D., Salman, M., Sujith, P., & Raj, S. (2025). Integration of SIEM And SOAR For Advanced Threat Defense. *International Journal for Science and Advance Research in Technology, 11*(4), 763-770. https://ijsart.com/public/storage/paper/pdf/IJSARTV11I4103239.pdf

Elastic. (2026). *Elastic Security solution & project type overview*. https://www.elastic.co/docs/solutions/security

Elastic. (2026). *Suricata Integration for Elastic*. https://www.elastic.co/docs/reference/integrations/suricata

European Union Agency for Cybersecurity [ENISA]. (2025). https://www.enisa.europa.eu/

Gartner. (2026). *Security Information and Event Management (SIEM) Reviews and Ratings*. https://www.gartner.com/reviews/market/security-information-event-management

González-Granadillo, G., González-Zarzosa , S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors, 21*, 14. https://doi.org/https://doi.org/10.3390/s21144759

IBM. (2023). *IBM QRadar SIEM*. https://www.ibm.com/es-es/products/qradar-siem

IBM Security. (2023). *Cost of a Data Breach Report 2023.* Armonk, New York: IBM Corporation.

Kent, K., & Souppaya, M. (2006). Guide to Computer Security Log Management. *Computer Security Resource Center*. https://doi.org/https://doi.org/10.6028/NIST.SP.800-92

Kidd, C. (2025). *SIEM: Security Information & Event Management Explained*. Splunk. https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html

Lisnevskyi, R., Amanzholova, S., Akhmetzhanova, J., Ikembayeva, A., & Naumova, D. (2026). *Development of an integrated network threat detection system based on Wazuh, Suricata and Telegram Bot*. https://ceur-ws.org/Vol-4180/Paper3.pdf

Microsoft. (2026). *Microsoft Sentinel*. https://www.microsoft.com/es-es/security/business/siem-and-xdr/microsoft-sentinel

MITRE Corporation. (2018). *ATT&CK: Design and Philosophy.* McLean, Virginia: MITRE Corporation. https://attack.mitre.org/

National Insitute of Standars and Technology. (2006). *Guide to Computer Security Log Management*. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf

National Insitute of Standars and Technology. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf

pen Information Security Foundation. (2026). https://oisf.net/

Raml, M., & Soewito, B. (2023). Monitoring dan Evaluasi Keamanan Jaringan dengan Pendekatan Security Information and Security Management (SIEM). *Faktor, 16*(1), 50-56. https://doi.org/10.30998/faktorexacta.v16i1.16534

Red Canary. (2025). *2025 Threat Detection Report*. Red Canary. https://resource.redcanary.com/rs/003-YRU-314/images/2025ThreatDetectionReport_RedCanary.pdf?version=0

Security Onion. (2026). *Introduction*. https://docs.securityonion.net/en/2.4/introduction.html

Setiawan, H., & Sulistyo, W. (2023). SIEM (Security Information Event Management) Model for Malware Attack Detection. *International Journal of Engineering, Technology and Natural Sciences, 5*(2). https://doi.org/10.46923/ijets.v5i2.241

Suricata. (2026). *15.1.1. Eve JSON Output*. https://docs.suricata.io/en/latest/output/eve/eve-json-output.html

Suricata. (2026). *15.1.2. Eve JSON Format*. https://docs.suricata.io/en/latest/output/eve/eve-json-format.html

Suricata. (2026). *Eve JSON Format*ℑ. https://docs.suricata.io/en/latest/output/eve/eve-json-format.html

Suricata. (2026). *Eve JSON Output*. https://docs.suricata.io/en/latest/output/eve/eve-json-output.html

Suricata. (2026). *Suricata module*. https://www.elastic.co/docs/reference/beats/filebeat/filebeat-module-suricata

Suritcata. (2026). *Suricata*. https://suricata.io/

Wazuh. (2026). *Wazuh*. https://wazuh.com/

Apéndices

Documentación

- Manuales de Instalación Sistemas Operativos Windows y Ubuntu

Enlace de Máquinas virtuales implementadas.

- https://mailinternacionaledu-my.sharepoint.com/:f:/g/personal/anaguaguinaac_uide_edu_ec/IgCdFhml2mO1R5hEVhDcrQAFAQhe958uZCHJyARS8ipeTzI?e=eGBVJg