ESPECIALIZACIÓN EN CIBERSEGURIDAD

ANÁLISIS DEL TRÁFICO DE RED COMO PROTECCIÓN FRENTE A LOS ATAQUES MALICIOSOS MÁS COMUNES EN UNA RED LAN PARA PYMES EN MANIZALES.

SEBASTIAN RIOS ECHEVERRI
JORGE WALTER SALAZAR AGUDELO

Universidad® Católica de Manizales
VIGILADA MINEDUCACIÓN
Obra de Iglesia de la Congregación
Hermanas de la Caridad Dominicas de La Presentación de la Santísima Virgen

ANÁLISIS DEL TRÁFICO DE RED COMO PROTECCIÓN FRENTE A LOS ATAQUES MALICIOSOS MÁS COMUNES EN UNA RED LAN PARA PYMES EN MANIZALES

Modalidad de grado: Proyecto de investigación

Asesor: Héctor Roberto Gordon Quinche

Jorge Walter Salazar Agudelo
Sebastián Ríos Echeverri

UNIVERSIDAD CATOLICA DE MANIZALES
FACULTAD DE INGENIERIA Y ARQUITECTURA
ESPECIALIZACIÓN EN CIBERSEGURIDAD
MANIZALES, CALDAS
2023

Dedicatoria

Queremos dedicar este proyecto a Dios y a nuestras familias, quienes han sido fundamentales en nuestro camino hacia la culminación de esta meta.

A Dios, agradecemos por su constante presencia en nuestras vidas, por ser nuestra guía y fortaleza en cada uno de los desafíos que enfrentamos en este camino. Sin su amor y gracia, este logro no habría sido posible.

A nuestras familias, les agradecemos por su amor incondicional, su apoyo y motivación constante. Ustedes han sido nuestro pilar fundamental y el motor que nos ha impulsado a seguir adelante en este proyecto.

A lo largo de este proceso, hemos enfrentado desafíos y sacrificios, pero con la ayuda de Dios y el apoyo de nuestras familias, hemos logrado superarlos y alcanzar nuestro objetivo.

Por eso, queremos dedicar este logro a Dios y a nuestras familias, por su amor, su apoyo y por ser nuestra fuente de inspiración y motivación. Gracias por creer en nosotros y por ser parte de este importante logro.

Agradecimientos

Primero que todo dar gracias a Dios por darnos la bendición de empezar y terminar con éxito este proceso de formación, a los docentes Héctor Roberto Gordon y Jhon Cesar Arango por El compromiso, tiempo entrega y paciencia a la hora de guiarnos y acompañarnos, clave importante para poder finalizar el proyecto de investigación con el resultado esperado.

Queremos expresar nuestros más sinceros agradecimientos A la Universidad Católica de Manizales por la formación académica que nos ha brindado durante el tiempo en sus instalaciones. Ha sido un privilegio poder formar parte de su comunidad educativa y recibir una educación de calidad. Dar la gracias a nuestras familias porque fueron un pilar fundamental para nuestro crecimiento personal y profesional.

TABLA DE CONTENIDO

RESUMEN

Las pequeñas y medianas empresas (Pymes) tienen un papel fundamental en la economía global y son una fuente importante de empleo y generación de riqueza. Sin embargo, estas empresas a menudo enfrentan desafíos significativos en términos de recursos limitados, incluida la inversión en seguridad cibernética. Las Pymes son objetivos atractivos para los ciberdelincuentes debido a su vulnerabilidad y la falta de medidas de seguridad adecuadas.

Es esencial que las Pymes implementen medidas de ciberseguridad adecuadas para proteger sus redes LAN. Esto incluye la implementación de software de seguridad, firewalls y la capacitación de los empleados para que sean conscientes de los riesgos de seguridad. La gestión de incidentes de ciberseguridad también es esencial para las Pymes, ya que deben estar preparadas para manejar cualquier incidente de seguridad que pueda ocurrir.

Es importante que las Pymes comprendan la importancia de la seguridad cibernética y tomen medidas adecuadas para proteger sus redes. La inversión en medidas de seguridad cibernética no sólo puede proteger a la empresa de posibles ataques, sino que también puede mejorar la confianza de los clientes en la empresa y proteger su reputación.

La implementación de medidas de ciberseguridad adecuadas y la gestión de incidentes de seguridad es esencial para las Pymes. Las normas ISO proporcionan un marco para que las Pymes implementen medidas de seguridad cibernética efectiva y para manejar incidentes de seguridad de manera eficaz, lo que puede mejorar la confianza del cliente, proteger la reputación de la empresa y mitigar riesgos financieros.

ABSTRACT

Small and medium-sized enterprises (SMEs) play a key role in the global economy and are an important source of employment and wealth generation. However, these businesses often face significant challenges in terms of limited resources, including investment in cybersecurity. SMEs are attractive targets for cybercriminals due to their vulnerability and lack of adequate security measures.

It is essential that SMEs implement adequate cybersecurity measures to protect their LANs. This includes implementing security software, firewalls and training employees to be aware of security risks. Cybersecurity incident management is also essential for SMBs, as they must be prepared to handle any security incident that may occur.

It is important for SMEs to understand the importance of cybersecurity and take appropriate measures to protect their networks. Investing in cyber security measures can not only protect the company from potential attacks, but can also improve customer confidence in the company and protect its reputation.

Implementing appropriate cybersecurity measures and managing security incidents is essential for SMEs. ISO standards provide a framework for SMEs to implement effective cybersecurity measures and to handle security incidents effectively, which can improve customer confidence, protect the company's reputation and mitigate financial risks.

INTRODUCCIÓN

La presente investigación se desarrolla buscando la importancia de obtener un analizador de tráfico de red LAN, que permita evaluar incidentes y gestionar los mismos, con el fin de proteger a las empresas de los principales ataques de la RED LAN.

En Manizales, Caldas, las empresas que corresponden a los tres sectores económicos como lo son la Industria, comercio y servicios, dichas empresas que disponen de una red LAN, regularmente hacen inversiones en tecnología, con el fin de estar a la vanguardia e incursionar en el mundo de los negocios y las comunicaciones, ya que actualmente están en auge de crecimiento y para estar a la altura de poder competir con otras empresas, realmente no se cuenta con un control real en el aspecto del entorno de red a nivel local.

Las pequeñas y medianas empresas (pymes), generalmente cuentan con un bajo número de trabajadores, además, de un volumen de ingresos moderados en comparación con grandes empresas mercantiles o industriales. Es decir, las pymes son organizaciones cuyas operaciones son de baja escala, por lo tanto, no suelen contar con una infraestructura que los blinde de las amenazas recurrentes a nivel de la red.

Actualmente, la información se cataloga como uno de los activos esenciales de una empresa, es por ello, que es relevante que se adopten protocolos para el manejo de la seguridad de la información. Según el estudio realizado por “BID MEJORANDO VIDAS”, éste adujo que 32 países de América Latina, no están realmente capacitados o preparados para combatir los ataques que suceden en el ciberespacio, solamente 7 países están preparados con un plan de protección de su infraestructura. ¿Qué quiere decir lo anterior?, Que es un problema denominado en masa porque son muchas las empresas o entidades de los 22 países de América Latina que no tiene la capacidad de analizar o conocer acerca de los ataques que se puedan

cometer en el ciberespacio y consiguiente no permite medir la gran vulnerabilidad a la que están expuestas todas estas entidades a los ataques maliciosos, que no permiten desarrollar o implementar mecanismos para prevenir dichos ataques, desencadenando así una afectación cultural, porque al considerar que a varias empresas no les ha pasado tal situación, no es necesario prestarle la debida atención a los procesos de ciberseguridad en cuanto a ataques que se han presentado a través de la historia.

En varios estudios independientes, se han indicado que los ataques a la red (LAN) conducen a que las pequeñas y medianas empresas (pymes) no evitan estos ataques con pautas de seguridad básicas mayormente por la falta de recursos, lo cual desencadena un problema de índole social, debido a que hacen caso omiso a las políticas de seguridad, dónde establecen las reglas para el manejo de la información de las entidades por parte de un usuario, lo cual dejará como resultado afectar dispositivos y robo de información por una mala práctica, uno de los más relevantes es el Phishing que se enfoca en lograr engañar y así extraer información por diferentes medios aprovechando la brecha de seguridad. (Schwartz , 2020)

OBJETIVOS

Objetivo general

Analizar un mecanismo de protección a la red LAN, que permita verificar y gestionar los incidentes principales en las pymes en Manizales, Caldas.

Objetivos específicos

- Implementar un analizador de tráfico Opensource para pymes.
- Analizar las principales incidencias.
- Gestionar los principales ataques de dichos incidentes.

DESCRIPCIÓN DEL PROBLEMA

La iniciativa de realizar este proyecto, surge desde la problemática que se puede evidenciar al no implementar un analizador de tráfico de red (LAN), que permita analizar los principales incidentes y gestionar los ataques de dichos incidentes de las pymes en la ciudad de Manizales, los cuales se enmarcan en una gran vulnerabilidad en cuanto a que la información de las entidades están expuestas casi todo el tiempo a ataques maliciosos camuflados en información allegada que aparentemente se denota inofensiva y termina siendo ataques que denotaremos más adelante, que podrían ser irreparables en cuanto a la seguridad de la información para las empresas, si no se tienen las respectivas medidas pertinentes implementadas para prevenir dichas vulnerabilidades en las pequeñas y medianas empresas (pymes), que permita cumplir con los tres pilares de la seguridad de la información los cuales son: la confidencialidad, integridad y disponibilidad.

Es de conocimiento que los recursos tecnológicos en la mayoría de las pequeñas y medianas empresas (pymes), lo cual es beneficioso para el desarrollo de sus actividades comerciales, industriales y demás servicios, pero al no hacer un uso adecuado, puede terminar en convertirse en una amenaza para las mismas.

Además, se debe tener en cuenta que existen peligros al navegar por las páginas web, que en muchas ocasiones contienen amenazas y virus informáticos y los recursos tecnológicos quedan expuestos al navegar sin control por el internet.

Actualmente, el buen uso de internet es muy desfavorable en las pequeñas y medianas empresas (PYMES), por lo cual encontramos diversos peligros en las redes de datos internas como la RED LAN, que se van expandiendo rápidamente sea por navegar en el internet y por vía correo electrónico.

En la 14 edición anual de la conocida encuesta de seguridad del Instituto de Seguridad de Computadoras - CSI, se muestran las pérdidas de cada encuestado. Para tener un punto de partida de la relevancia del tema que nos compete, de un total de 443 encuestados de diferentes empresas e instituciones, el promedio de pérdidas debido a los incidentes de seguridad es de 234,244 dólares anuales. (Richardson Robert, 2009).

Debido a lo anteriormente expuesto, se desencadena una mayor problemática en cuanto a la seguridad de las pequeñas y medianas empresas (pymes) por su nivel adquisitivo para desarrollar una infraestructura eficiente, por lo cual es de suma importancia que se utilicen herramientas que estén disponibles en el mercado y sean de fácil manejo, logrando así, un buen desempeño del recurso a cada una de las empresas que tienen acceso a la red.

Por estos motivos, surge la necesidad de realizar un analizador de tráfico de red LAN y así, hacer el análisis de incidentes y la gestión de los mismos, para las pequeñas y medianas empresas (pymes) en Manizales, Caldas.

PLANTEAMIENTO DEL PROBLEMA

¿Cómo mitigar los principales problemas de seguridad que tenga el tráfico de red (LAN), analizando los incidentes y gestionando los mismos en las pymes?

JUSTIFICACIÓN

El analizador de tráfico y el análisis de incidente y gestión de los mismos nacen como una necesidad de salvaguardar adecuadamente la información que se maneja en la red (LAN) de una pequeña y mediana empresa (pymes), y que tan vulnerable puede llegar a estar si no se aplican estas medidas.

Para mejorar los procesos en las empresas y aportar con el desarrollo de este proyecto, se ha optado por hacer el análisis de tráfico, para verificar los principales incidentes y conocer las amenazas más predominantes que se encuentran en la red y poder hacer la debida gestión de los incidentes.

Los más beneficiados serían las pymes, ya que podrían tener un mejor control y un gran desempeño de este recurso que hasta ahora no se ha tenido muy en cuenta, además, de conllevar una gran atribución en el desarrollo comercial de las empresas.

A nivel de ingeniería, se va a hacer la instalación de un analizador de tráfico Opensource y configuración de reglas, para mantener actualizada la base de datos del analizador y realizar una configuración para la administración a través de una interfaz web, que permita a los usuarios de las pymes identificar fácilmente las alertas.

Este proyecto busca tener un gran impacto, ya que marcará un precedente en la optimización de los recursos tecnológicos a nivel de las pequeñas y medianas empresas de la Ciudad de Manizales.

CONTEXTO GEOGRÁFICO

El área de estudio de este proyecto se enmarca dentro del País de Colombia, Departamento de Caldas, concretamente en la ciudad de Manizales.

Manizales, Caldas.

Perteneciente a la región Centro Sur del departamento de Caldas, ubicada sobre la vertiente Occidental de la Cordillera Central, articulada por los ejes viales de la troncal de Occidente, con una topografía muy pendiente. La localización dentro del territorio nacional con respecto a la distribución de la población y la actividad económica es altamente ventajosa. Se encuentra en el interior del llamado Triángulo De Oro conformando el espacio comprendido entre las ciudades de Bogotá, Medellín y Cali, los tres principales centros de consumo de Colombia.

Conforme a las cifras señaladas por la Cámara de Comercio de Manizales por Caldas (CCMPC), la cual tiene presencia en 18 municipios del departamento de Caldas, en 2021 se crearon un total de 5.309 empresas en toda la jurisdicción. Una variación del 23,5% en comparación con el año 2020 donde se crearon 4.300 empresas. (BC Noticias, 2022).

Las microempresas tuvieron una participación del 99,45% dando un total de 5.280, pequeñas empresas siendo el 0,04% un total de 2 empresas; medianas empresas tuvieron una participación del 0,49% con un total de 26 empresas y las grandes empresas del 0,02% con un total de 1 empresa. (BC Noticias, 2022)

Aunado a lo anteriormente expuesto, tomamos como referente dos (02) Pymes de la Ciudad de Manizales, que existen y operan hace más de 15 años, las cuáles evidencian que no

cuentan con un proceso que asegure la información o evite los ataques más comunes mencionados en nuestra investigación.

Profesco Consultores Y Auditores S.A.S:

La empresa Profesco Consultores Y Auditores S A S tiene como domicilio principal de su actividad la dirección, Calle 23 21 41 Edificio Bch Piso 7 Of 703 en la ciudad de Manizales, Caldas.

Esta empresa fue constituida como Sociedad Por Acciones Simplificada y se dedica a Actividades de Revisoría fiscal, contabilidad, teneduría de libros, auditoría financiera y asesoría tributaria de entidades públicas y privadas.

Dicha empresa puede aplicar y adoptar todos los procesos y recomendaciones de seguridad informática frente a la red LAN que se expuso en el presente proyecto, dónde algunos de sus enfoques y procesos en un plan general clasificado, son en las siguientes áreas:

- Revisoría fiscal.
- Auditoría legal.
- Auditoría de impuestos.
- Auditoría de costos.
- Auditoría del sistema de almacén e inventarios.
- Auditoría de sistemas.
- Auditoría de la gestión del sistema comercial y el mercado nacional e internacional.
- Entre otros.

Aseind Ltda:

La empresa Aseind Ltda, se encuentra situada en el departamento de CALDAS, en la localidad MANIZALES y su dirección postal es Calle 23 23 16 Of 803, Manizales, Caldas. Esta empresa fue constituida como Sociedad Limitada y una de sus actividades principales son de índole jurídico. Asesorando principalmente a aseguradoras del Estado, manejando bases de datos de las mismas e información legal de carácter confidencial.

Se puede evidenciar de las empresas en mención, por las prestaciones y servicios que brindan, sobre todo, por el manejo de información de entidades del Estado y privadas pueden estar muy expuestas y vulnerables frente a ataques informáticos por medio de la red LAN, es de suma importancia y puede ser de mucha utilidad que implementen los sistemas de seguridad basándose en lo expuesto en el presente proyecto frente a la red LAN que manejan dentro de ellas, además, parametrizar según las normas ISO expuestas en nuestro trabajo, cada uno de los equipos de cómputo e informáticos para la integridad de la información y mitigación de los ataques más comunes que expusimos en el presente trabajo.

MARCOS DE INVESTIGACIÓN

Antecedentes

Al realizar una revisión bibliográfica acerca del analizador de trafico de red (LAN), análisis de incidentes y gestión de los mismos se identifica que, en relación al tema de esta investigación, ha habido muy poca labor investigativa, no obstante, en el transcurso de la búsqueda, se encontraron algunos referentes bibliográficos que, a pesar de no hablar del tema puntualmente, si relacionan aspectos intrínsecamente conexos con el tema objeto de investigación, especialmente sobre el analizador de red, así como lo expone:

(Benítez Prada y Díaz Gómez, 2008) en su tema, “Recopilación Y Análisis De Técnicas Y Herramientas De Software Libre Utilizadas Para El Escaneo, Intrusión Y Defensa En Redes De Computadoras Y Su Aplicación En La Evaluación Del Nivel De Seguridad De La Red De Datos De La Universidad Autónoma De Bucaramanga (Unab)” expone las técnicas para la seguridad informática como el sistema para detección de intrusos (IDS), conocidos como IDSes basados en host, basados en red y basados en una arquitectura cliente-servidor. Sistemas de detección de intrusos pasivos y sistemas reactivos, los primeros que notifican a la autoridad competente mediante el sistema de alerta, este sensor advierte de una posible intrusión, almacena la información y manda una señal que se guarda en una base de datos, pero no actua sobre el ataque y el segundo generan un tipo de respuesta sobre la fuente de ataque y envía algún tipo de respuesta predefinida en la configuración. Además, aduce sobre las Herramientas de Software Libre empleadas para las pruebas de seguridad como Nessus, Nmap, VNC – Virtual Network Computing y Rpc.

(Chávez Zapata, 2011) en su Tema “Simulación Y Análisis De Mecanismos De Defensa Ante Los Ataques De Denegación De Servicios (Dos) En Redes De Área Local Convergentes”

aduce que, en términos de seguridad informática, un ataque de servicio (Dos – Denial Of Service) es un ataque de interrupción, que tiene como fin dejar un servicio o recurso inoperativo, para que los usuarios legítimos no puedan utilizarlos, son ataques contra la disponibilidad de un servicio, afectando el uso normal de los sistemas. Las clases de ataques DoS han ido evolucionando con el tiempo y lo más relevantes son gusano Morris, teardrop, boink, bonk, fapi, targa.c. y trinoo.

(Arias Reyes y Díaz Rodríguez, 2014) en su proyecto "Elaboración De Una Guía De Gestión De Riesgos Basados En La Norma Ntc-Iso 31000 Para El Proceso De Gestión De Incidentes Y Peticiones De Servicio Del Área De Mesa De Ayuda De Empresas De Servicios De Soporte De Tecnología En Colombia" exponen que utilizando como medio la norma NTC-ISO 31000 y con apoyo en la norma técnica Colombiana NTC 5254, se busca realizar una guía de gestión de riesgos en el proceso de gestión de incidentes, donde sea posible establecer el riesgo presente en los subprocesos que existan y poder realizar una gestión adecuada, para cumplir los objetivos de manera eficaz y eficiente en las Empresas. Existen muchas herramientas que permiten enfocarse en la realización de gestión de riesgos y para mencionar algunas son: Modelo Norteamericano COSO, Modelo Canadiense CoCo, Modelo Estándar de Control Interno MECI 1000:2005, Norma Técnica Colombiana NTC-5254 Gestión del Riesgo.

(Sánchez Lorente, 2015) en su investigación "Detección De Intrusiones Con Snort", establece que el Snort tiene una ventaja de que es muy extendido y se ha utilizado a fondo, además de contar con mucha información disponible que permite aclarar dudas. También, manifiesta que Suricata aporta otras ventajas como ejecutar varios subprocesos para disfrutar de todas las CPU o núcleos que haya disponibles y permite la extracción de ficheros. El IDS o

sistema de detección de intrusiones se encarga de prevenir e informar de actividades sospechosas, pero éste no se encarga de detener ningún ataque.

(Cuadra Sánchez, 2017), con la investigación “Contribución Al Análisis Del Tráfico De Internet”, En este tema se ha desarrollado una serie de técnicas avanzadas de análisis de tráfico que suplen nuevas necesidades en el ámbito de la monitorización de redes y servicios. Las técnicas tradicionales se basan en el mero análisis de los protocolos y su evolución en el tiempo, en lugar considerar los perfiles y las características del tráfico como se propone en esta tesis, lo que favorece su aplicación a distintas disciplinas, como la detección de anomalías en la red, la supervisión de la calidad o la gestión de la seguridad. Se implementa una metodología novedosa para analizar el tráfico denominada “análisis del perfil de día típico”, que permite caracterizar el comportamiento del tráfico para los diferentes periodos del día.

(Gonzales Valero, 2018) en su tema “Análisis De Trafico De La Red De Datos Y Su Incidencia En El Acceso Al Contenido Web De Los Estudiantes De Las Instituciones Educativas Del Distrito 12d01) aduce, que la falta de personal capacitado para controlar y administrar la red, se convierte en una debilidad importante si se busca obtener un adecuado desempeño, ya que si se presenta un problema en la red, seria complejo tomar acciones para mitigar que se expanda un ataque a toda la red. Además, manifiesta de la vital importancia de un análisis y monitoreo de la red y que se debe tener muy claro los conceptos básicos a la hora de realizar un análisis de tráfico de la red de datos. Con este conocimiento se puede controlar los paquetes de información que pueden ser dañinos que circular por la red sin algún tipo de control y así, poder tener un mejor provecho y manejo de la utilización del ancho de banda.

(Guzmán Solano, 2019) en su proyecto “Guia Para La Implementación De La Norma Iso 27032” manifiesta que, al mismo tiempo que la tecnología evoluciona, también lo hacen los

ataques en el ciberespacio volviéndose crítico para las gerencias de las organizaciones sin importar su tipo o tamaño, donde proporciona una guía con lineamientos para implementar buenas prácticas que permita actuar oportunamente ante un ataque. Es por eso que nace la necesidad de implementar una guía de las buenas prácticas que se aducen en la norma ISO 27032, la cual permite a las empresas, identificar, analizar y establecer controles que fortalezcan los niveles de seguridad y mitigue los riesgos a los cuales sean expuestos en el ciberespacio.

(Abad Parrales, Cañarte Rodríguez, Villamarin Cevallos, Mezones Santana, Delgado Pilozo, Toala Arias, Figueroa Suárez y Romero Castro (2019), en su tema “La Ciberseguridad Práctica Aplicada A Las Redes, Servidores Y Navegadores Web.” En dicha investigación, se puntualiza en diferentes ataques desde el punto de vista del pentesting o hacking ético, y que tipos de análisis de seguridad se implementan para evitar dichos ataques sean externos o internos y cómo prevenirlos, evaluarlos y darles el manejo pertinente. Así mismo, puntualizan en el análisis del tráfico y redes que tiene como objetivo de como determinar el tráfico de red y poder verificar como viaja información de un punto a otro, para determinar vulnerabilidades e implementar los correctivos necesarios en la seguridad de la red.

Marco Normativo

I. **ISO 27032:** "Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad" - facilita la colaboración segura y fiable para proteger la privacidad de las personas en todo el mundo.

II. **ISO 27001:** Permite a las organizaciones contar con los lineamientos mínimos para garantizar la integridad, confidencialidad y disponibilidad de la información.

III. **ISO 31000:** Norma internacional para la gestión del riesgo.

IV. **Ley Estatutaria 1266 de 2008**: Contiene disposiciones legales del Habeas Data y la

V. Regulación de la protección de datos personales.

VI. **Ley Estatutaria 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales, basándose en la sentencia C-748 de 2011 de la Corte Constitucional.

VII. **Ley Estatutaria 1273 de 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

VIII. **Circular Externa 007 de 2018:** Mediante la cual adicionan el Capítulo V y regula los "Requerimientos mínimos para la gestión del riesgo de Ciberseguridad"

IX. **Circular Externa 008 de 2018:** Mediante la cual se actualiza el Capítulo I y aduce los "Canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros".

Marco teórico conceptual

Las referencias seleccionadas para el desarrollo del presente acápite tienen dos finalidades. En primer lugar, instalar el programa que nos permita realizar un escaneo de las vulnerabilidades de los paquetes de red (LAN) y, en segundo lugar, analizar las principales incidencias y hacer la gestión de las mismas.

Muchas empresas (pymes), emplean un método muy básico para evitar los ciberataques, por lo cual han sido víctimas de robo de información a través del correo electrónico o por la navegación en internet, por lo cual es sumamente necesario instalar un analizador de tráfico de red (LAN).

Es así, como tiene lugar plantear los siguientes conceptos claves que serán de importancia para la comprensión de este proyecto:

Ciberseguridad: Para poder hablar de contextos seguros es apropiado hablar de la ciberseguridad, ya que son procedimientos para proteger los computadores, dispositivos móviles, sistemas electrónicos, servidores y sobre todo los datos de ataques maliciosos, de los cuales se dividen algunas categorías como la seguridad de red, seguridad de las aplicaciones, seguridad operativa. (kaspersky, 2022).

Sgsi: Conjunto de procesos que comprende la estructura organizativa, recursos, procedimientos, políticas, para hacer la mejora continúa en la seguridad de la información, tomando como base los posibles riesgos a los cuales se enfrentan las organizaciones. (Guzmán Solano, 2019)

Seguridad Informática: Está también se conoce como ciberseguridad, ya que tiene como función proteger la información y, sobre todo, el procesamiento, con el fin de evitar que se manipulen los datos a manos de ciberdelincuentes. (unir la universidad en internet, 2021).

Vulnerabilidades: las debilidades detectadas en un activo que puedan afectar el funcionamiento de los sistemas de la información de las organizaciones. (Guzmán Solano, 2019)

Ids: Sistema de detección de intrusiones: es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas. Ante cualquier actividad sospechosa, emiten una alerta a los administradores del sistema quienes han de tomar las medidas oportunas. Estos accesos pueden ser ataques esporádicos realizados por usuarios malintencionados o repetidos cada cierto tiempo, lanzados con herramientas automáticas. Estos sistemas sólo detectan los accesos sospechosos emitiendo alertas anticipatorias de posibles intrusiones, pero no tratan de mitigar la intrusión. Su actuación es reactiva. (Incibe, 2020)

Siem: o sistema de gestión de eventos e información de seguridad: es una solución híbrida centralizada que engloba la gestión de información de seguridad (Security Information Management) y la gestión de eventos (Security Event Manager). La tecnología SIEM proporciona un análisis en tiempo real de las alertas de seguridad generadas por los distintos dispositivos hardware y software de la red. Recoge los registros de actividad (logs) de los distintos sistemas, los relaciona y detecta eventos de seguridad, es decir, actividades sospechosas o inesperadas que pueden suponer el inicio de un incidente, descartando los resultados anómalos, también conocidos como falsos positivos y generando respuestas acordes en base a los informes y evaluaciones que registra, es decir, es una herramienta en la que se centraliza la información y se integra con otras herramientas de detección de amenazas. (Incibe, 2020)

Protocolo Ip: Su funcionamiento se rige en una determinada tecnología, un protocolo se define como conjunto de normas que rigen en paquetes de comunicaciones que son transmitidos

en la red. Si existe un protocolo, se pretende que hay seguridad de que todas las redes por más distintas que sean, pueden integrarse en cualquier tipo de sistema. Usualmente la mayoría de redes utilizan el protocolo IP versión 4 (IPv4) de cuatro bytes. (Equipo de Expertos de Ciencia y Tecnología de la Universidad Internacional de Valencia, 2016).

Protocolos Tcp: llamado protocolo de control de transmisión, son fundamentales en internet, es importante que los datos "segmentos" lleguen de manera correcta al destinatario, sin algún error y en orden. Además, de disponer control de congestión. (Luz, 2021).

***Protocolo Udp*:** Proporciona el envío de datagramas, sin requerir previamente una conexión, solo requiere abierto un socket en el destino para acepte los datagramas del origen. No proporciona ningún tipo de control de flujo y de congestión. (Luz, 2021).

***Analizador De Trafico De Red*:** Su definición en informática es un programa especializado de monitoreo y análisis que intercepta tramas o paquetes de una red de datos. Este es un software de computadora que intercepta y registra el tráfico de Internet. Paquetes de datos en una red de datos. A medida que los datos pasan de un lado a otro a través de la red, el sniffer intercepta cada bloque de datos de protocolo, descifra y analiza su contenido de acuerdo con la especificación del programa. (Barahona Delgado, 2011).

Ancho De Banda: El ancho de banda explicado de una manera fácil, se puede definir como el número de bits o cantidad de datos que se puede enviar de un punto a otro en una unidad de tiempo a través de un medio de conectividad. En algunos países empieza a tener características parecidas al espacio de almacenamiento siendo así que está disponible para casi todos los habitantes en gran cantidad y a un precio accesible. (Castaño Ribes & López Fernández, 2013).

***Arp (Adress Resolution Protocol) O Protocolo De Resolución De Direcciones*:** Es un protocolo utilizado para obtener la dirección física (dirección MAC) de un equipo a través de su dirección IP. Cuando un equipo quiere enviar datos a otro dentro de una red (por ejemplo, una red Ethernet) utilizando la arquitectura TCP/IP, el equipo emisor debe generar uno (o más) datagramas, y éstos deben ser pasados al nivel inferior (nivel de enlace) y encapsulados en una (o más) tramas Ethernet. En esta situación, la referencia al equipo destino suele ser su dirección IP, pero para poder generar las tramas Ethernet también es necesario conocer la dirección MAC. (Santos, 2014).

Dhcp Protocolo De Configuración Dinámica De Equipos: El protocolo DHCP es el que remite la información necesaria para que pueda conectarse a una red del tipo TCP/IP, el modelo que usa es el de Cliente/Servidor, donde el servidor DHCP asigna a los clientes que solicitan direcciones de red, estableciendo los parámetros necesarios para su configuración automática y que acceden a la red TCP/IP. (Carceller Cheza, Campos Saborido, & García Marcos, Servicios en red, 2013).

Protocolo Icmp (Internet Control Message Protocol) O Protocolo De Mensajes De Control De Internet: Este protocolo se utiliza para enviar notificaciones sobre datagramas con problemas. Los mensajes ICMP son generados normalmente en respuesta a errores producidos sobre datagramas IP o para propósitos de diagnóstico y enrutamiento. (Santos, 2014).

Wazuh Manager: Es el componente central del servidor Wazuh y se encarga de recibir, procesar y almacenar la información de seguridad recopilada por los agentes Wazuh.

Elasticsearch: Es un motor de búsqueda y análisis de datos que se utiliza para almacenar y analizar la información de seguridad recopilada por el servidor Wazuh.

Kibana: Es una interfaz web que se utiliza para visualizar y gestionar la información de seguridad almacenada en Elasticsearch.

Filebeat: Es un agente de registro que se utiliza para enviar los registros del sistema al servidor Wazuh.

Logstash: Es una plataforma de procesamiento de datos que se utiliza para procesar y clasificar la información de seguridad recibida por los agentes Wazuh y Filebeat.

Api Restful: Es una interfaz de programación de aplicaciones (API) que se utiliza para acceder a la información de seguridad almacenada en Elasticsearch a través de aplicaciones externas.

Mitre Att&Ck: es un marco de trabajo (framework) que describe tácticas y técnicas de ciberataque utilizadas por adversarios en entornos informáticos. Proporciona una base común de lenguaje y conocimiento para que los equipos de seguridad puedan entender, comunicar y mejorar su postura de seguridad. ATT&CK es mantenido por el Instituto MITRE, una organización sin fines de lucro dedicada a resolver problemas críticos de interés público.

Nist 800-53: es un conjunto de controles y medidas de seguridad para sistemas de información desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos. El documento, titulado "Security and Privacy Controls for Federal Information Systems and Organizations" (Controles de Seguridad y Privacidad para Sistemas de Información y Organizaciones Federales), establece un conjunto de controles que pueden ser utilizados por agencias gubernamentales y organizaciones privadas para proteger sus sistemas y datos contra una amplia gama de amenazas de seguridad. Los controles de NIST 800-53 abarcan una amplia variedad de áreas, como la gestión de accesos, la seguridad de la red, la protección de datos y la continuidad del negocio. NIST 800-53 es uno de los marcos de seguridad más utilizados en el

mundo y es un componente clave de la estrategia de seguridad cibernética del gobierno de los Estados Unidos.

Gdpr: significa Reglamento General de Protección de Datos (en inglés, General Data Protection Regulation). Es una ley de privacidad y protección de datos de la Unión Europea que entró en vigencia en mayo de 2018 y se aplica a cualquier organización que procese datos personales de ciudadanos de la UE. El GDPR establece una serie de requisitos y responsabilidades para las organizaciones que procesan datos personales, incluyendo el consentimiento del titular de los datos para su procesamiento, la notificación de violaciones de datos y la obligación de implementar medidas de seguridad adecuadas para proteger los datos personales. También otorga a los ciudadanos de la UE ciertos derechos, como el derecho a acceder, rectificar o eliminar sus datos personales. Las organizaciones que no cumplen con el GDPR pueden enfrentar multas significativas.

Pci Dss: significa "Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago" en inglés. Es un conjunto de requisitos de seguridad diseñados para proteger la información de tarjetas de pago y reducir el riesgo de fraude en transacciones con tarjeta de crédito o débito. Los requisitos se aplican a todas las entidades que procesan, almacenan o transmiten información de tarjetas de pago, incluyendo comerciantes, proveedores de servicios de pago, instituciones financieras y procesadores de pagos.

La implementación de PCI DSS puede beneficiar la Ciberseguridad de una organización, ya que establece medidas y controles de seguridad para proteger la información de tarjetas de pago, lo que a su vez puede reducir el riesgo de brechas de seguridad y la exposición de información confidencial. Los requisitos de PCI DSS incluyen medidas como la implementación de firewalls, el cifrado de datos, la segmentación de redes, el control de acceso y la realización

de pruebas regulares de seguridad. Al implementar estas medidas, se puede mejorar la postura de seguridad general de una organización y reducir el riesgo de ataques cibernéticos y fraude. Además, el cumplimiento de PCI DSS puede ayudar a mejorar la confianza y la reputación de una organización entre los clientes y socios comerciales.

Hipaa: Es la Ley de Portabilidad y Responsabilidad del Seguro de Salud de los Estados Unidos, que establece estándares para la protección de la privacidad y seguridad de la información médica y de salud. La ley se aplica a proveedores de atención médica, planes de salud, proveedores de servicios de atención médica y otros que manejan información médica protegida (PHI).

La implementación de los requisitos de HIPAA puede beneficiar la Ciberseguridad, ya que la ley establece controles y procedimientos para proteger la PHI contra el acceso no autorizado y la divulgación no permitida. Al implementar estas medidas, se pueden reducir los riesgos de brechas de seguridad y la exposición de información confidencial. Además, HIPAA también requiere la realización de auditorías y pruebas de seguridad regulares para evaluar la efectividad de los controles de seguridad implementados y detectar posibles vulnerabilidades. Esto puede ayudar a mejorar la postura de seguridad general de una organización y mitigar los riesgos cibernéticos.

Rbac: RBAC (Role-Based Access Control, en inglés) son un modelo de control de acceso que se utiliza para restringir el acceso a recursos dentro de un sistema informático. En este modelo, los usuarios se asignan a roles específicos en función de sus responsabilidades en la organización, y cada rol se le otorga un conjunto de permisos y restricciones predefinidos.

Sso: significa "Single Sign-On" o "Inicio de sesión único". Es un método de autenticación que permite a los usuarios acceder a varios sistemas o aplicaciones mediante una

única credencial de inicio de sesión. En lugar de tener que recordar múltiples credenciales para cada sistema o aplicación, el usuario solo necesita ingresar sus credenciales de inicio de sesión una vez, lo que les da acceso a todos los sistemas y aplicaciones que utilizan SSO.

A continuación, se harán las descripciones de los ataques más comunes que se presentan en la red Lan:

Ataque Ddos

Un ataque DDoS (Distributed Denial of Service) es un tipo de ataque cibernético que busca interrumpir el servicio de una red o sistema, haciendo que se sobrecarguen y no puedan atender las solicitudes legítimas de los usuarios.

En un ataque DDoS a una red LAN (Local Area Network), los atacantes utilizan múltiples sistemas infectados con malware (llamados "zombis") para enviar un gran volumen de solicitudes al objetivo, saturando los recursos de la red y haciéndola inaccesible. Estos ataques pueden ser muy disruptivos y pueden causar pérdidas económicas y reputacionales a las empresas afectadas.

Por lo tanto, es importante tener medidas de seguridad en su lugar para protegerse contra ataques DDoS, como la implementación de firewalls y sistemas de detección y mitigación de ataques.

Los síntomas de un ataque DDoS en una red LAN pueden variar dependiendo del tipo y la magnitud del ataque, pero algunos de los síntomas comunes que se pueden observar incluyen:

- Disminución del rendimiento de la red: Un ataque DDoS puede saturar la red con tráfico malicioso, lo que puede provocar una disminución significativa del rendimiento de la red.
- Latencia elevada: El exceso de tráfico malicioso puede causar latencias elevadas en la red, lo que puede provocar retrasos en el envío y recepción de datos.
- Tiempo de respuesta lento: Un ataque DDoS puede causar que los servidores se sobrecarguen, lo que puede provocar un tiempo de respuesta lento o incluso hacer que los servidores fallen.
- Inaccesibilidad a los servicios: Un ataque DDoS puede hacer que los servicios y aplicaciones en la red no estén disponibles para los usuarios debido a la sobrecarga de los servidores.
- Aumento de tráfico: Un ataque DDoS puede causar un aumento inesperado en el tráfico de red, lo que puede ser un signo de que la red está bajo ataque.
- Actividad sospechosa en la red: La actividad sospechosa en la red, como paquetes de datos inesperados o no identificados, puede ser una señal de que la red está siendo atacada.
- Disminución de la calidad del servicio: La calidad del servicio puede disminuir debido a la sobrecarga de los servidores, lo que puede afectar la experiencia de los usuarios.

Es importante monitorear la red de forma regular para identificar cualquier síntoma de un posible ataque DDoS y tomar medidas preventivas para evitar cualquier daño a la red. Si se sospecha que una red está siendo atacada, es importante tomar medidas inmediatas para mitigar el ataque y minimizar cualquier impacto negativo en la red.

Existen varios tipos de ataques DDoS que pueden afectar a una red LAN. Algunos de los tipos más comunes de ataques DDoS son:

- Ataques de inundación de tráfico: Este tipo de ataque DDoS implica inundar la red con tráfico malicioso para saturar los recursos y sobrecargar los servidores, lo que puede provocar una caída en el rendimiento de la red.
- Ataques de amplificación: Este tipo de ataque DDoS utiliza servidores mal configurados para enviar grandes cantidades de tráfico a un destino específico. Esto puede hacer que la red se sobrecargue y deje de responder.
- Ataques de agotamiento de recursos: Este tipo de ataque DDoS implica agotar los recursos de la red, como los recursos de CPU y memoria de los servidores, lo que puede causar una caída en el rendimiento de la red.
- Ataques de aplicación: Este tipo de ataque DDoS se dirige a aplicaciones específicas en la red, como servidores web o bases de datos, y busca sobrecargarlos con tráfico malicioso para hacerlos fallar o disminuir su rendimiento.
- Ataques de vulnerabilidades de red: Este tipo de ataque DDoS explota las vulnerabilidades de seguridad en los sistemas de la red para causar una caída en el rendimiento de la red.

Es importante implementar medidas de seguridad adecuadas para proteger la red contra estos tipos de ataques DDoS y tomar medidas preventivas para minimizar su impacto en la red.

Planificación:

La planificación para evitar ataques DDoS incluye varios aspectos importantes:

- Monitoreo: Es importante tener un sistema de monitoreo en tiempo real para detectar signos de ataque DDoS y actuar rápidamente.
- Redundancia: Es importante tener un sistema de redundancia en lugar, para que el tráfico pueda ser redirigido a otros servidores en caso de un ataque DDoS.
- Filtros: Es importante tener filtros en el lugar para bloquear el tráfico malicioso antes de que alcance los servidores.
- Protección en la nube: Las soluciones de protección en la nube, como los servicios de mitigación de ataques DDoS, pueden ayudar a filtrar y bloquear el tráfico malicioso antes de que llegue a la red.
- Capacidad de respaldo: Es importante tener una capacidad de respaldo en lugar, para poder mantener los servicios críticos en funcionamiento incluso durante un ataque DDoS.
- Formación y concienciación: Es importante capacitar a los empleados y hacerles conscientes de la importancia de la seguridad cibernética y cómo evitar ataques DDoS.
- Colaboración: Es importante establecer relaciones de colaboración con proveedores de seguridad cibernética, proveedores de servicios de Internet y otras empresas para compartir información y coordinar respuestas a los ataques DDoS.

La planificación adecuada para evitar ataques DDoS requiere un enfoque integral que incluya una combinación de medidas técnicas, de formación y concienciación, y de colaboración con otros actores relevantes.

Los objetivos de evitar ataques DDoS incluyen:

- ***Proteger la disponibilidad de los servicios y aplicaciones:*** El objetivo principal de la prevención de ataques DDoS es asegurarse de que los servicios y aplicaciones críticos estén disponibles y accesibles para los usuarios legítimos en todo momento.
- ***Minimizar la interrupción del servicio:*** Es importante minimizar la interrupción del servicio durante un ataque DDoS y recuperarse lo antes posible.
- ***Detectar ataques temprano:*** Es importante detectar ataques DDoS lo más temprano posible para poder responder rápidamente y minimizar su impacto.
- ***Mantener la confidencialidad de la información:*** Es importante mantener la confidencialidad de la información y proteger la privacidad de los usuarios durante y después de un ataque DDoS.
- ***Reducir el costo:*** Es importante minimizar el costo total asociado con la prevención y el tratamiento de ataques DDoS, incluyendo los costos de hardware, software, personal y tiempo.
- ***Mejorar la resiliencia y la capacidad de recuperación:*** Es importante mejorar la resiliencia de la red y la capacidad de recuperación en caso de un ataque DDoS.

Los objetivos principales para evitar ataques DDoS incluyen proteger la disponibilidad de los servicios, minimizar la interrupción del servicio, detectar ataques temprano, mantener la confidencialidad de la información, reducir el costo y mejorar la resiliencia y la capacidad de recuperación.

Los alcances para evitar ataques DDoS incluyen:

- ***Infraestructura de red*:** Es importante revisar y fortalecer la infraestructura de red para evitar que sea utilizada como punto de entrada para un ataque DDoS.
- ***Aplicaciones y servicios:*** Es importante revisar y fortalecer las aplicaciones y servicios para garantizar que estén protegidos contra ataques DDoS.
- ***Protección en la nube:*** Es importante considerar la utilización de soluciones de protección en la nube para mitigar los ataques DDoS.
- ***Monitoreo y detección:*** Es importante implementar sistemas de monitoreo y detección para detectar y responder a los ataques DDoS.
- ***Formación y concienciación:*** Es importante capacitar a los empleados y hacerles conscientes de la importancia de la seguridad cibernética y cómo evitar ataques DDoS.
- ***Colaboración:*** Es importante establecer relaciones de colaboración con proveedores de seguridad cibernética, proveedores de servicios de Internet y otras empresas para compartir información y coordinar respuestas a los ataques DDoS.
- ***Plan de respaldo y recuperación:*** Es importante tener un plan de respaldo y recuperación en lugar para recuperarse de un ataque DDoS.

Los alcances para ataques DDoS incluyen revisar y fortalecer la infraestructura de red, aplicaciones y servicios, considerar soluciones de protección en la nube, implementar sistemas de monitoreo y detección, capacitar a los empleados, establecer relaciones de colaboración y tener un plan de respaldo y recuperación en lugar.

Para manejar los tiempos de ejecución para ataques DDoS, es importante seguir los siguientes pasos:

Planificación y preparación: Establecer un plan de acción y un equipo de respuesta ante un ataque DDoS, identificar los recursos necesarios y preparar los sistemas y herramientas.

- ***Monitoreo continuo:*** Monitorear la red y los servicios continuamente para detectar signos tempranos de un ataque DDoS.
- ***Detección temprana:*** Detectar un ataque DDoS lo más temprano posible para minimizar su impacto y permitir una respuesta rápida.
- ***Evaluación del impacto:*** Evaluar el impacto del ataque DDoS en la red y los servicios y determinar la urgencia de la respuesta.
- ***Implementación de contramedidas*****:** Implementar contramedidas para mitigar el impacto del ataque DDoS y proteger la disponibilidad de los servicios y aplicaciones.
- ***Seguimiento y evaluación:*** Seguir de cerca el impacto del ataque DDoS y evaluar la efectividad de las contramedidas implementadas.
- ***Documentación y mejora continua:*** Documentar todas las acciones realizadas durante el ataque DDoS y utilizar esta información para mejorar la respuesta ante futuros ataques.

Para manejar los tiempos de ejecución para evitar ataques DDoS, es importante planificar y prepararse, monitorear continuamente, detectar temprano, evaluar el impacto, implementar contramedidas, seguir y evaluar, y documentar y mejorar continuamente.

Para manejar los ataques DDOS , una empresa puede implementar las siguientes Recursos como medidas de seguridad:

- Firewall: Un firewall es un sistema que protege los recursos de la red de accesos no autorizados y puede ayudar a bloquear ciertos tipos de tráfico DDoS.
- Protección en la nube: Las soluciones de protección en la nube, como Cloudflare, pueden ayudar a filtrar y mitigar el tráfico DDoS antes de que llegue a la red de la empresa. Análisis de tráfico: Es importante monitorear y analizar el tráfico de red en busca de patrones inusuales que puedan indicar un ataque DDoS en curso.
- Redundancia en la red: La implementación de redundancia en la red, como la configuración de múltiples servidores o enrutadores, puede ayudar a asegurar que la red continúe funcionando aún cuando un componente sufra un fallo.
- Mitigación de ataques DDoS: Las soluciones de mitigación de ataques DDoS, como los sistemas de detección y bloqueo de ataques, pueden ayudar a detectar y mitigar rápidamente los ataques DDoS antes de que causen un impacto significativo.

Es importante destacar que ninguna solución es infalible y es posible que un ataque DDoS sofisticado pueda superar incluso las mejores medidas de protección. Por lo tanto, es fundamental tener un plan de contingencia para responder rápidamente y minimizar el impacto de los ataques DDoS.

Análisis del riesgo - síntomas de DDOS:

- Cuando se navega por la red y la velocidad del internet es inusualmente lenta al momento de abrir archivos o acceder a sitios web.
- Problemas al momento de ingresar a cualquier plataforma web.
- Cuando al momento de navegar en un sitio web se evidencia de forma inusual y con gran elevación los spam. https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/
- Para el análisis de riesgos contamos con la norma ISO 31000 que permitirá detectar amenazas dónde puntualmente para este punto, es acerca del ataque DDOS,

Implementación de controles:

La norma ISO 27001 es un marco de trabajo para la gestión de la seguridad de la información que incluye una serie de controles específicos para garantizar la protección de los activos de información, incluyendo las redes LAN. Algunas de las normas específicas que se aplican a la protección y seguridad de las redes LAN contra ataques DDoS son:

- A.9.2 Gestión de acceso del usuario: se establece Control de acceso a activos Este control incluye medidas para garantizar que solo los usuarios autorizados tengan acceso a los activos de la red LAN, incluyendo la autenticación, autorización y restricción de acceso.
- A.9.1.2 Monitoreo de acceso: Este control incluye la implementación de medidas para supervisar y registrar el acceso a la red LAN, incluyendo la auditoría de registros y la monitoreo en tiempo real.

- A.11.2.2 Protección contra ataques a la disponibilidad: Este control se enfoca en proteger la disponibilidad de los servicios de la red contra ataques DDoS, incluyendo la identificación de las vulnerabilidades y la implementación de soluciones de mitigación de DDoS.
- A.13.2.2 Monitoreo y detección de intrusiones: Este control requiere que se monitoreen las actividades en la red para detectar posibles ataques DDoS y se adopten medidas para prevenirlos o responder rápidamente en caso de que ocurran.
- A.14.1.2 Acceso remoto seguro: Este control se enfoca en garantizar que solo se permita el acceso remoto a la red mediante mecanismos seguros, como la autenticación y la encriptación, para prevenir el acceso no autorizado y los ataques DDoS.
- A.16.1.1 Protección contra virus y software malicioso: Este control se enfoca en proteger la red contra los ataques que utilizan malware, incluyendo los ataques DDoS, mediante la implementación de soluciones de seguridad en endpoint y la actualización periódica de los sistemas y aplicaciones.
- Estos son solo algunos ejemplos de los controles incluidos en la norma ISO 27001 que se aplican a la protección y seguridad de las redes LAN contra ataques DDoS. Es importante seguir todos los controles específicos incluidos en la norma para garantizar una protección adecuada contra estos tipos de ataques.

Gestión del Incidente:

La ISO 27032 proporciona las siguientes recomendaciones para prevenir ataques DDoS:

Implementar medidas de seguridad en redes y sistemas para filtrar y bloquear paquetes maliciosos.

- Utilizar soluciones de mitigación de DDoS para detectar y filtrar ataques en tiempo real.
- Mantener software y sistemas actualizados con las últimas correcciones de seguridad.
- Realizar pruebas regulares de seguridad para identificar vulnerabilidades.
- Monitorear constantemente la actividad de red y sistemas para detectar patrones anormales.
- Tener un plan de contingencia y un proceso de respaldo en caso de un ataque DDoS.
- Colaborar con proveedores de servicios de seguridad para responder a un ataque DDoS.

Es importante tener en cuenta que la prevención de ataques DDoS es un proceso continuo que requiere monitoreo y actualización constante.

Pruebas y Evaluaciones:

Realizar pruebas y evaluaciones para verificar el funcionamiento de los controles especificados entre ellos podemos aplicar.

- ***Pruebas de estrés:*** Consiste en simular tráfico de red excesivo para determinar la capacidad de la red y los sistemas para manejar cargas pesadas. Estas pruebas ayudan a identificar posibles puntos débiles y asegurarse de que los sistemas y equipos de red están configurados para manejar la cantidad de tráfico previsto.
- ***Pruebas de penetración:*** Esta prueba implica simular un ataque real para ver cómo los controles implementados reaccionan ante la actividad malintencionada. La idea es

evaluar si los controles son efectivos en la detección y prevención de ataques DDoS y cómo se comportan en caso de una situación real.

- ***Pruebas de simulación:*** Se realizan pruebas utilizando herramientas de simulación y modelado para analizar cómo diferentes tipos de ataques DDoS afectarían a la red. Estas pruebas permiten identificar posibles vulnerabilidades y evaluar la efectividad de los controles implementados.
- ***Pruebas de monitoreo:*** Se realizan pruebas de monitoreo y análisis para evaluar la capacidad de los sistemas para detectar y responder a ataques DDoS. Estas pruebas implican el monitoreo de la red y los sistemas para detectar patrones de tráfico malicioso, actividad sospechosa o cualquier signo de un posible ataque.
- ***Pruebas de continuidad del negocio:*** Se realizan pruebas de continuidad del negocio para evaluar la capacidad de la red y los sistemas para mantener la funcionalidad en caso de un ataque DDoS. Estas pruebas ayudan a identificar posibles puntos débiles y garantizar que los sistemas y equipos de red estén configurados para minimizar el impacto de un ataque DDoS en la continuidad del negocio.

Estas pruebas y evaluaciones pueden ayudar a garantizar que los controles implementados para prevenir ataques DDoS en redes LAN sean efectivos y estén funcionando correctamente. También pueden ayudar a identificar posibles vulnerabilidades y áreas de mejora para los controles existentes. Es importante realizar estas pruebas de forma regular para mantener la seguridad y la continuidad del negocio en caso de un ataque DDoS.

Mantenimiento y mejora continua:

Para verificar y mejorar continuamente el funcionamiento de los controles aplicados para evitar ataques DDoS en redes LAN, se pueden realizar las siguientes acciones:

- Actualizar regularmente los sistemas y equipos de red: Es importante mantener los sistemas y equipos de red actualizados con los últimos parches de seguridad, actualizaciones de software y firmware para evitar posibles vulnerabilidades y debilidades en los controles de seguridad.
- Monitorear regularmente la red: El monitoreo regular de la red puede ayudar a detectar posibles ataques DDoS y actividad malintencionada en tiempo real. Las herramientas de monitoreo pueden ser configuradas para alertar al personal de seguridad si se detectan patrones de tráfico malicioso o cualquier actividad sospechosa.
- Implementar una respuesta de emergencia: Una respuesta de emergencia puede ayudar a mitigar el impacto de un ataque DDoS en la red. Es importante tener un plan de respuesta de emergencia claramente definido y probarlo regularmente para asegurarse de que esté actualizado y sea efectivo.
- Realizar pruebas regulares: Las pruebas regulares pueden ayudar a identificar posibles vulnerabilidades y debilidades en los controles de seguridad. Es importante realizar pruebas de penetración, pruebas de simulación y pruebas de monitoreo de forma regular para evaluar la efectividad de los controles implementados.
- Capacitar al personal de seguridad: El personal de seguridad debe estar capacitado para manejar situaciones de emergencia y responder adecuadamente a un ataque DDoS. La capacitación regular en seguridad de red puede ayudar a asegurarse de que el personal de seguridad esté preparado para enfrentar cualquier situación de seguridad en la red.

La mejora continua es un proceso clave para garantizar que los controles aplicados para evitar ataques DDoS en redes LAN estén funcionando correctamente. Las acciones como la actualización regular de sistemas y equipos de red, el monitoreo regular de la red, la implementación de una respuesta de emergencia, la realización de pruebas regulares y la capacitación del personal de seguridad son importantes para garantizar la efectividad de los controles de seguridad y minimizar el impacto de un ataque DDoS en la red.

Existen varios tipos de ataques DDoS que pueden afectar a una red LAN. Algunos de los tipos más comunes de ataques DDoS son:

- ***Ataques de inundación de tráfico*:** Este tipo de ataque DDoS implica inundar la red con tráfico malicioso para saturar los recursos y sobrecargar los servidores, lo que puede provocar una caída en el rendimiento de la red.
- ***Ataques de amplificación:*** Este tipo de ataque DDoS utiliza servidores mal configurados para enviar grandes cantidades de tráfico a un destino específico. Esto puede hacer que la red se sobrecargue y deje de responder.
- ***Ataques de agotamiento de recursos:*** Este tipo de ataque DDoS implica agotar los recursos de la red, como los recursos de CPU y memoria de los servidores, lo que puede causar una caída en el rendimiento de la red.
- ***Ataques de aplicación:*** Este tipo de ataque DDoS se dirige a aplicaciones específicas en la red, como servidores web o bases de datos, y busca sobrecargarlos con tráfico malicioso para hacerlos fallar o disminuir su rendimiento.

- ***Ataques de vulnerabilidades de red:*** Este tipo de ataque DDoS explota las vulnerabilidades de seguridad en los sistemas de la red para causar una caída en el rendimiento de la red.

Lista de Chequeo

Un ataque DDoS (Denegación de Servicio Distribuido) es una situación en la que un gran número de dispositivos intentan acceder a un servidor al mismo tiempo, lo que provoca una sobrecarga y hace que el servidor se vuelva inaccesible. Si tu empresa ha recibido un ataque DDoS en tu red LAN, sigue los siguientes pasos para mitigar el impacto del ataque y restaurar la funcionalidad de tu red:

- Identifica el tipo de ataque: Comprende el tipo de ataque que está afectando tu red LAN. Hay diferentes tipos de ataques DDoS, como el ataque de saturación, el ataque de agotamiento de recursos y el ataque de vulnerabilidad, cada uno con su propia estrategia de defensa.
- Desconecta el servidor: Desconecta el servidor afectado de la red inmediatamente para evitar que se propague el ataque a otros dispositivos en la red.
- Notifica al proveedor de servicios de internet (ISP): Informa al ISP para que puedan tomar medidas para proteger la red y ayudar a identificar el origen del ataque.
- Analiza los registros de tráfico de red: Revisa los registros de tráfico de red para determinar la fuente del ataque y las direcciones IP de los dispositivos involucrados. Esto puede ayudarte a identificar la mejor forma de proteger tu red en el futuro.
- Implementa soluciones de seguridad: Después de identificar la fuente del ataque, implementa soluciones de seguridad para proteger tu red de futuros ataques DDoS. Esto podría

incluir la instalación de un firewall, la actualización del software de seguridad, el aumento del ancho de banda, o la utilización de una solución de defensa DDoS.

- Restaura el servicio: Después de haber implementado medidas de seguridad, asegúrate de que el servidor afectado vuelva a estar en línea y funcionando correctamente.
- Realiza una evaluación post-ataque: Realiza una evaluación después del ataque para identificar los impactos y los daños causados, así como las áreas de mejora que se pueden implementar para aumentar la protección de la red.
- Un ataque DDoS puede ser muy perjudicial para tu red LAN y para tu empresa. Sin embargo, si sigues estos pasos, puedes minimizar los daños y proteger tu red de futuros ataques.

Arp Spoofing

El ataque ARP spoofing, también conocido como "envenenamiento de ARP" o "ARP poisoning" en inglés, es un tipo de ataque de seguridad informática en el que un atacante envía paquetes de información falsificados a una red local con el objetivo de interceptar, modificar o redirigir el tráfico de red legítimo.

El protocolo ARP (Address Resolution Protocol) es utilizado por los dispositivos en una red local para mapear las direcciones físicas (direcciones MAC) de los dispositivos en la red con sus direcciones IP correspondientes. En un ataque de ARP spoofing, el atacante envía paquetes ARP falsificados que contienen una dirección MAC diferente a la que se esperaría en respuesta a una consulta ARP, lo que hace que los dispositivos en la red local crean que la dirección MAC falsificada es la correcta para una dirección IP específica. De esta manera, el atacante puede interceptar, modificar o redirigir el tráfico de red legítimo.

Este tipo de ataque puede permitir al atacante espiar el tráfico de red para recopilar información confidencial, como contraseñas y datos de acceso, y también puede permitir la inyección de paquetes maliciosos en la red. Para protegerse contra los ataques de ARP spoofing, es importante implementar medidas de seguridad, como la configuración de listas de control de acceso (ACL) y el uso de soluciones de seguridad de red, como firewalls y sistemas de detección y prevención de intrusiones.

Los síntomas de un ataque ARP spoofing en una red LAN pueden incluir:

- Disminución en la velocidad de la red: El tráfico de red se dirige a la dirección MAC incorrecta, lo que puede hacer que la red sea más lenta.
- Conexiones no confiables: La comunicación entre dispositivos puede ser interrumpida o redirigida, lo que puede hacer que las conexiones sean no confiables.
- Mensajes de error de red: Los dispositivos pueden mostrar mensajes de error de red como "dirección IP duplicada" o "conflicto de direcciones IP".
- Dispositivos desconocidos en la red: Pueden aparecer dispositivos desconocidos en la red, lo que indica que alguien ha podido acceder a la red de manera ilegal.
- Cambios en la configuración de red: La configuración de red puede cambiar repentinamente sin ninguna razón aparente.
- Es importante implementar medidas de seguridad adecuadas, como la implementación de protocolos de seguridad como el protocolo ARP seguro (Secure ARP) o la utilización de herramientas de detección de ARP spoofing para proteger la red contra estos tipos de ataques.

Existen varios tipos de ataques ARP spoofing que pueden afectar a una red LAN, entre ellos se incluyen:

- ***ARP Cache Poisoning:*** En este tipo de ataque, el atacante envía paquetes ARP falsificados a la red para corromper la tabla ARP de los dispositivos en la red. Una vez que la tabla ARP está corrompida, el tráfico de red se dirige a la dirección MAC del atacante en lugar del dispositivo legítimo.
- ***ARP Request Spoofing:*** En este tipo de ataque, el atacante envía paquetes ARP falsificados en respuesta a las solicitudes ARP legítimas. Esto puede engañar a los dispositivos de la red para que piensen que la dirección MAC del atacante es la dirección MAC legítima.
- ***Man-in-the-Middle (MITM) Attack*:** En un ataque MITM, el atacante intercepta el tráfico de red entre dos dispositivos y reenvía los paquetes a través de su propio dispositivo. Esto permite al atacante leer o modificar el tráfico antes de que llegue al destino legítimo.
- ***Ataque ARP Spoofing por Denegación de Servicio:*** En este tipo de ataque, el atacante satura la tabla ARP de los dispositivos de la red con información ARP falsa, lo que provoca que la red se vuelva inoperable.

Es importante implementar medidas de seguridad adecuadas para evitar estos tipos de ataques, como el uso de protocolos de seguridad como Secure ARP o la utilización de herramientas de detección de ARP spoofing para proteger la red contra estos tipos de ataques.

Planificación:

Pasos para planificar y evitar un ataque de ARP spoofing en una red LAN:

- Utilice la autenticación de red: Implemente la autenticación de red, como la autenticación por contraseña o el uso de certificados digitales, para asegurarse de que los dispositivos conectados a la red sean legítimos y autorizados.
- Limite el tráfico de broadcast: Configure el hardware de red, como switches y routers, para limitar el tráfico de broadcast en la red LAN, lo que reducirá el riesgo de ataques de ARP spoofing.
- Configure las listas de control de acceso (ACL): Configure las ACL en los dispositivos de red para restringir el acceso a la red y asegurarse de que solo los dispositivos autorizados puedan acceder a ella.
- Actualice regularmente el software y el firmware: Asegúrese de mantener actualizado el software y el firmware de los dispositivos de red y servidores, ya que las actualizaciones pueden contener parches que solucionan las vulnerabilidades que los atacantes podrían aprovechar para realizar ataques de ARP spoofing.
- Utilice herramientas de monitoreo y detección de red: Implemente herramientas de monitoreo de red para identificar patrones y comportamientos sospechosos, lo que podría indicar un posible ataque de ARP spoofing. También puede utilizar herramientas de detección de ARP spoofing para detectar paquetes ARP falsificados en la red.
- Eduque a los usuarios: Capacite a los usuarios sobre la importancia de la seguridad de la red y las prácticas de seguridad recomendadas, como el uso de contraseñas seguras y la detección de señales de advertencia de un posible ataque de ARP spoofing.

- Implemente soluciones de seguridad de red: Utilice soluciones de seguridad de red, como firewalls y sistemas de detección y prevención de intrusiones, para detectar y prevenir ataques de ARP spoofing y otros tipos de ataques de seguridad informática.

Los objetivos de evitar ataques Arp Spoofing incluyen:

Los objetivos de evitar ataques ARP spoofing en una red LAN incluyen:

- Proteger la privacidad de los datos: Los ataques de ARP spoofing pueden permitir que los atacantes intercepten y roben datos confidenciales de la red, como contraseñas, información de tarjetas de crédito, etc. Al evitar estos ataques, se protege la privacidad y la confidencialidad de los datos.
- Mantener la disponibilidad de la red: Los ataques de ARP spoofing pueden causar congestión de red, lo que puede hacer que la red sea inaccesible o lenta para los usuarios legítimos. Al evitar estos ataques, se asegura la disponibilidad de la red para los usuarios autorizados.
- Asegurar la integridad de los datos: Los ataques de ARP spoofing pueden permitir que los atacantes modifiquen los datos en tránsito, lo que puede causar errores y daños en los sistemas y dispositivos de la red. Al evitar estos ataques, se asegura la integridad de los datos y se previene el daño a los sistemas y dispositivos de la red.
- Mantener la confianza en la red: Los ataques de ARP spoofing pueden dañar la reputación de la red y hacer que los usuarios pierdan la confianza en ella. Al evitar estos ataques, se mantiene la confianza en la red y se asegura su buen funcionamiento.
- Proteger los sistemas y dispositivos de la red: Los ataques de ARP spoofing pueden permitir que los atacantes tomen el control de los sistemas y dispositivos de la red, lo que

puede ser utilizado para llevar a cabo ataques más graves. Al evitar estos ataques, se protegen los sistemas y dispositivos de la red y se previenen ataques más graves.

Los alcances para evitar ataques Arp Spoofing incluyen:

Los alcances para evitar ataques ARP spoofing en redes LAN son varios y pueden incluir:

- ***Mejora de la seguridad de la red:*** Al implementar medidas de seguridad para prevenir los ataques de ARP spoofing, se aumenta la seguridad de la red en general. Esto ayuda a proteger los sistemas y dispositivos de la red de otros tipos de ataques cibernéticos y a mantener la confidencialidad, integridad y disponibilidad de los datos.
- ***Reducción del tiempo de inactividad de la red:*** Los ataques de ARP spoofing pueden causar congestión y otros problemas en la red, lo que puede llevar a un tiempo de inactividad prolongado. Al evitar estos ataques, se reduce el tiempo de inactividad de la red, lo que puede mejorar la productividad y la eficiencia de la organización.
- ***Protección de la información confidencial:*** Al prevenir los ataques de ARP spoofing, se protege la información confidencial y personal de los usuarios, como contraseñas, información de tarjetas de crédito, etc. Esto ayuda a evitar robos de identidad y otros tipos de delitos informáticos.
- ***Cumplimiento de regulaciones y normativas:*** Muchas organizaciones están sujetas a regulaciones y normativas que requieren medidas de seguridad específicas para proteger los datos confidenciales de los usuarios. Al evitar los ataques de ARP spoofing, se puede asegurar el cumplimiento de estas regulaciones y normativas.

- ***Mantenimiento de la reputación de la organización:*** Los ataques de ARP spoofing pueden dañar la reputación de la organización y afectar su relación con sus clientes y proveedores. Al evitar estos ataques, se puede mantener la confianza en la organización y su capacidad para proteger los datos de los usuarios.

Gestión del Incidente:

La ISO 27032 proporciona las siguientes recomendaciones para prevenir ataques de suplantación (spoofing):

- Implementar autenticación de doble factor para garantizar la identidad de los usuarios.
- Utilizar técnicas de encriptación para proteger la privacidad de la información y evitar la suplantación de identidad.
- Verificar la fuente y la integridad de los datos antes de procesarlos o confiar en ellos.
- Configurar dispositivos de red para prevenir el suplantación de direcciones IP.
- Monitorear constantemente la actividad de red y sistemas para detectar patrones anormales.
- Realizar pruebas regulares de seguridad para identificar vulnerabilidades.
- Establecer políticas y procedimientos claros para la gestión de la seguridad de la información.
- Es importante tener en cuenta que la prevención de ataques de suplantación es un proceso continuo que requiere monitoreo y actualización constante para adaptarse a los nuevos métodos y técnicas utilizados por los atacantes.

Lista Chequeo

Si tu empresa ha recibido un ataque de ARP Spoofing en tu red LAN, esto significa que un atacante ha falsificado información en la tabla ARP de tu red para hacerse pasar por otro dispositivo en la red. Esto puede permitir que el atacante intercepte el tráfico de red y recopile información confidencial, entre otros riesgos de seguridad. Sigue los siguientes pasos para mitigar el impacto del ataque y restaurar la funcionalidad de tu red:

- Identifica la fuente del ataque: Utiliza herramientas de análisis de red para identificar la dirección MAC del dispositivo que está realizando el ataque de ARP Spoofing en la red.
- Bloquea la dirección MAC del atacante: Bloquea la dirección MAC del dispositivo malicioso en tu red para evitar que continúe realizando el ataque.
- Restablece las tablas ARP: Restablece las tablas ARP de los dispositivos afectados en la red para asegurarte de que la información sea correcta y no esté comprometida.
- Actualiza tus medidas de seguridad: Actualiza tus medidas de seguridad para prevenir futuros ataques de ARP Spoofing en la red. Algunas medidas que podrías tomar incluyen la utilización de autenticación de dispositivos, la implementación de un sistema de detección y prevención de intrusiones, y la configuración de políticas de seguridad de red adecuadas.
- Comunica el incidente: Comunica el incidente a los usuarios afectados y a los responsables de seguridad de la empresa. También es importante informar a los proveedores de servicios de Internet (ISP) si el ataque viene de fuera de la red de la empresa.

- Evalúa el impacto del ataque: Realiza una evaluación del impacto del ataque y documenta los daños y la información comprometida. También es importante evaluar las vulnerabilidades existentes en la red y tomar medidas para proteger la información confidencial y evitar futuros ataques.

Un ataque de ARP Spoofing puede ser muy peligroso para tu red LAN y la seguridad de la empresa. Sin embargo, si sigues estos pasos, podrás mitigar el impacto del ataque y proteger tu red de futuros ataques.

Ataque Man-In-The-Middle

Un ataque Man-in-the-Middle (MITM) es un tipo de ataque en el que un atacante intercepta el tráfico de red entre dos dispositivos y se coloca en el medio para espiar, manipular o robar información. En una red LAN, un ataque MITM puede ocurrir cuando un atacante logra interceptar el tráfico de red de un dispositivo, lo que le permite leer, modificar o incluso inyectar paquetes maliciosos en la comunicación entre los dispositivos.

El atacante puede aprovechar este tipo de ataque para obtener información confidencial, como contraseñas o datos de tarjetas de crédito, o para redirigir el tráfico a una ubicación maliciosa. Por ejemplo, en un ataque MITM en una red LAN, el atacante puede suplantar la identidad de un dispositivo de red legítimo para interceptar y leer el tráfico, o incluso modificar el tráfico antes de enviarlo al destino legítimo.

Para evitar este tipo de ataque, es importante utilizar medidas de seguridad como el cifrado de extremo a extremo para la comunicación, la autenticación de dispositivos y usuarios, y la implementación de protocolos de seguridad como HTTPS y SSL/TLS. Además, también se

pueden utilizar herramientas de detección de MITM para identificar posibles intentos de ataque en la red.

Algunos de los síntomas que pueden indicar un ataque MITM son:

- ***Redireccionamiento:*** El atacante puede redirigir el tráfico de red hacia un destino diferente al que se pretendía originalmente.
- ***Cambios en los datos:*** El atacante puede alterar los datos que se están transmitiendo, lo que puede resultar en la pérdida o corrupción de datos.
- ***Problemas de autenticación:*** El atacante puede engañar a las víctimas para que proporcionen sus credenciales de inicio de sesión, lo que permite al atacante acceder a sus cuentas y realizar acciones maliciosas.
- ***Reducción del rendimiento de la red:*** Debido a que el atacante está interceptando el tráfico de red, la velocidad de la red puede disminuir significativamente.
- ***Aparición de nuevos dispositivos en la red:*** El atacante puede agregar dispositivos maliciosos a la red para obtener información o realizar acciones maliciosas.

Si sospechas que puede haber un ataque MITM en tu red LAN, es importante que tomes medidas para proteger la seguridad de tus datos y dispositivos, como cambiar tus contraseñas, desactivar conexiones no utilizadas o realizar un análisis de seguridad de la red.

Existen varios tipos de ataques de Man-in-the-Middle (MITM) que se pueden llevar a cabo en una red LAN, algunos de los cuales incluyen:

- ***ARP Spoofing:*** Este tipo de ataque implica enviar mensajes ARP falsos a los dispositivos de la red, lo que hace que los dispositivos envíen tráfico a la dirección MAC del atacante en lugar de a la dirección MAC correcta.
- ***DNS Spoofing:*** Este tipo de ataque implica falsificar las respuestas del servidor DNS para redirigir a los usuarios a un sitio web malicioso.
- ***Session Hijacking:*** Este tipo de ataque implica robar la sesión de un usuario legítimo en la red, lo que permite al atacante realizar acciones maliciosas en nombre del usuario.
- ***SSL Stripping:*** Este tipo de ataque implica eliminar la capa de seguridad SSL/TLS entre el navegador web del usuario y el servidor web, lo que permite al atacante interceptar y leer los datos que se están transmitiendo.
- ***Wi-Fi Eavesdropping:*** Este tipo de ataque implica interceptar el tráfico de red a través de una red Wi-Fi no segura o vulnerable.
- ***ICMP Redirect:*** Este tipo de ataque implica enviar mensajes ICMP falsos a los dispositivos de la red, lo que redirige el tráfico a través del atacante.

Es importante que las empresas implementen medidas de seguridad adecuadas, como el cifrado de red y la autenticación fuerte, para prevenir y detectar ataques de MITM.

Gestión del Incidente:

La ISO 27032 proporciona las siguientes recomendaciones para prevenir ataques Man-in-the-Middle (MitM):

- Implementar autenticación de doble factor para garantizar la identidad de los usuarios y la integridad de la información.
- Utilizar técnicas de encriptación para proteger la privacidad de la información y evitar la interceptación de datos.
- Verificar la fuente y la integridad de los datos antes de procesarlos o confiar en ellos.
- Configurar dispositivos de red y sistemas para prevenir la interceptación de comunicaciones.
- Monitorear constantemente la actividad de red y sistemas para detectar patrones anormales.
- Realizar pruebas regulares de seguridad para identificar vulnerabilidades.
- Establecer políticas y procedimientos claros para la gestión de la seguridad de la información.

Es importante tener en cuenta que la prevención de ataques MitM es un proceso continuo que requiere monitoreo y actualización constante para adaptarse a los nuevos métodos y técnicas utilizados por los atacantes.

Lista de Chequeo

Un ataque Man-in-the-Middle (MITM) ocurre cuando un atacante se sitúa entre dos dispositivos que están comunicándose en una red, lo que le permite interceptar y manipular la comunicación. Si tu empresa ha recibido un ataque MITM en tu red LAN, sigue los siguientes pasos para mitigar el impacto del ataque y restaurar la funcionalidad de tu red:

- Identifica el tipo de ataque: Comprende el tipo de ataque MITM que está afectando tu red LAN. Hay diferentes tipos de ataques MITM, como el ataque de envenenamiento de ARP, el ataque de interceptación SSL, y el ataque de suplantación de identidad.
- Identifica la fuente del ataque: Utiliza herramientas de análisis de red para identificar la dirección IP o MAC del dispositivo que está realizando el ataque de MITM en la red.
- Bloquea la dirección IP o MAC del atacante: Bloquea la dirección IP o MAC del dispositivo malicioso en tu red para evitar que continúe realizando el ataque.
- Actualiza tus medidas de seguridad: Actualiza tus medidas de seguridad para prevenir futuros ataques MITM en la red. Algunas medidas que podrías tomar incluyen la utilización de autenticación de dispositivos, la implementación de un sistema de detección y prevención de intrusiones, y la configuración de políticas de seguridad de red adecuadas.
- Restablece las claves SSL y Certificados: Si el ataque fue de interceptación SSL, debes reemplazar los certificados SSL y las claves públicas y privadas para garantizar la seguridad de la información.
- Comunica el incidente: Comunica el incidente a los usuarios afectados y a los responsables de seguridad de la empresa. También es importante informar a los proveedores de servicios de Internet (ISP) si el ataque viene de fuera de la red de la empresa.
- Evalúa el impacto del ataque: Realiza una evaluación del impacto del ataque y documenta los daños y la información comprometida. También es importante evaluar las vulnerabilidades existentes en la red y tomar medidas para proteger la información confidencial y evitar futuros ataques.

Un ataque de Man-in-the-Middle puede ser muy peligroso para tu red LAN y la seguridad de la empresa. Sin embargo, si sigues estos pasos, podrás mitigar el impacto del ataque y proteger tu red de futuros ataques.

Os Finger Printing

Los ataques de OS fingerprinting son un tipo de ataque que busca identificar el sistema operativo utilizado por los dispositivos en una red LAN, generalmente para obtener información que puede ser utilizada en futuros ataques. Los atacantes utilizan técnicas de escaneo de puertos y análisis de paquetes para obtener información sobre el software y la configuración del sistema operativo utilizado por los dispositivos en la red. Esto les permite identificar vulnerabilidades específicas del sistema operativo que pueden ser explotadas para comprometer el dispositivo o la red.

Los ataques de OS fingerprinting son particularmente efectivos en redes LAN, donde los dispositivos pueden estar expuestos a amenazas internas y no tienen la protección adicional de un firewall o router de borde. Por lo tanto, es importante que los administradores de red implementen medidas de seguridad adecuadas, como la segmentación de red y la implementación de políticas de seguridad, para minimizar la exposición de los dispositivos a estos ataques. También es importante que los dispositivos estén actualizados con los parches de seguridad más recientes para evitar que los atacantes aprovechen vulnerabilidades conocidas en el sistema operativo.

Síntomas de un ataque OS fingerprinting en una red lan:

Es difícil detectar directamente un ataque de OS fingerprinting en una red LAN, ya que generalmente se realiza de manera silenciosa y pasiva, sin afectar directamente el funcionamiento de la red o de los dispositivos. Sin embargo, hay algunos síntomas que pueden indicar que se está llevando a cabo un ataque de OS fingerprinting, como:

- Escaneos de puertos no autorizados: Si se detectan escaneos de puertos no autorizados en la red, esto podría indicar que un atacante está tratando de identificar los sistemas operativos de los dispositivos.
- Tráfico de red sospechoso: Si se detecta tráfico de red inusual o sospechoso, como paquetes que no corresponden a las aplicaciones o servicios utilizados en la red, esto podría indicar que se está realizando un escaneo de OS fingerprinting.
- Cambios en la configuración de la red: Si se detectan cambios inesperados en la configuración de la red, como nuevas rutas o puertos abiertos, esto podría indicar que un atacante ha logrado identificar las vulnerabilidades en los sistemas operativos de los dispositivos y ha realizado cambios para comprometer la seguridad de la red.
- Actividad maliciosa posterior: Si se detecta actividad maliciosa posterior en la red, como intentos de explotar vulnerabilidades conocidas del sistema operativo, esto podría indicar que un atacante ha utilizado información obtenida a través de un ataque de OS fingerprinting para realizar un ataque más amplio.
- Es importante que los administradores de red estén atentos a estos síntomas y tomen medidas para proteger la seguridad de la red, como implementar medidas de seguridad de red adecuadas, actualizar los sistemas operativos y aplicaciones con los parches de seguridad más recientes y monitorear el tráfico de red para detectar posibles actividades maliciosas.

Existen varios tipos de ataques de OS fingerprinting que se pueden llevar a cabo en una red LAN, algunos de los cuales incluyen:

- ***Scanning de puertos:*** El escaneo de puertos es una técnica de OS fingerprinting que implica enviar paquetes a los diferentes puertos de un dispositivo para detectar los servicios y aplicaciones que se están ejecutando en el sistema operativo. Los atacantes pueden utilizar esta información para identificar el sistema operativo utilizado por el dispositivo.
- ***Análisis de huellas digitales de paquetes:*** El análisis de huellas digitales de paquetes es una técnica de OS fingerprinting que implica analizar los paquetes de red para identificar patrones de tráfico que sean distintivos del sistema operativo utilizado por el dispositivo. Los atacantes pueden utilizar esta información para identificar el sistema operativo utilizado por el dispositivo.
- ***Análisis de vulnerabilidades:*** Los atacantes pueden utilizar información obtenida a través de técnicas de OS fingerprinting para identificar las vulnerabilidades conocidas en el sistema operativo y las aplicaciones utilizadas por los dispositivos. Esto les permite diseñar ataques específicos que aprovechan estas vulnerabilidades.
- ***Utilización de herramientas de OS fingerprinting:*** Los atacantes pueden utilizar herramientas de OS fingerprinting, como Nmap o Xprobe, para identificar el sistema operativo utilizado por los dispositivos en la red. Estas herramientas envían paquetes específicos a los dispositivos y analizan las respuestas para identificar patrones que sean distintivos del sistema operativo utilizado por el dispositivo.

Es importante que los administradores de red implementen medidas de seguridad adecuadas, como la segmentación de red y la implementación de políticas de seguridad, para

minimizar la exposición de los dispositivos a estos ataques. También es importante que los dispositivos estén actualizados con los parches de seguridad más recientes para evitar que los atacantes aprovechen vulnerabilidades conocidas en el sistema operativo.

Gestión del Incidente:

La ISO 27032 proporciona las siguientes recomendaciones para prevenir ataques de identificación de sistema operativo (OS finger printing):

- Utilizar técnicas de encriptación para proteger la privacidad de la información y evitar la identificación de sistema operativo.
- Configurar dispositivos de red y sistemas para ocultar información sobre el sistema operativo y otros detalles de la configuración.
- Utilizar software de seguridad actualizado y configurarlo para proteger la privacidad y la seguridad de la información.
- Monitorear constantemente la actividad de red y sistemas para detectar patrones anormales.
- Realizar pruebas regulares de seguridad para identificar vulnerabilidades.
- Establecer políticas y procedimientos claros para la gestión de la seguridad de la información.
- Es importante tener en cuenta que la prevención de ataques de identificación de sistema operativo es un proceso continuo que requiere monitoreo y actualización constante para adaptarse a los nuevos métodos y técnicas utilizados por los atacantes.

Lista de Chequeo

Un ataque de OS fingerprinting es cuando un atacante intenta determinar el sistema operativo utilizado por los dispositivos en una red. El objetivo de un atacante puede ser identificar vulnerabilidades específicas en el sistema operativo para luego explotarlas. Si tu empresa ha recibido un ataque de OS fingerprinting en tu red LAN, sigue los siguientes pasos para mitigar el impacto del ataque y restaurar la funcionalidad de tu red:

- Identifica la fuente del ataque: Utiliza herramientas de análisis de red para identificar la dirección IP del dispositivo que está realizando el ataque de OS fingerprinting en la red.
- Bloquea la dirección IP del atacante: Bloquea la dirección IP del dispositivo malicioso en tu red para evitar que continúe realizando el ataque.
- Actualiza tus medidas de seguridad: Actualiza tus medidas de seguridad para prevenir futuros ataques de OS fingerprinting en la red. Algunas medidas que podrías tomar incluyen la utilización de autenticación de dispositivos, la implementación de un sistema de detección y prevención de intrusiones, y la configuración de políticas de seguridad de red adecuadas.
- Evalúa las vulnerabilidades del sistema: Realiza una evaluación de las vulnerabilidades de los sistemas operativos en tu red para determinar si existen vulnerabilidades que puedan ser explotadas por atacantes.
- Aplica actualizaciones y parches de seguridad: Implementa actualizaciones y parches de seguridad para los sistemas operativos vulnerables en la red.

- Comunica el incidente: Comunica el incidente a los usuarios afectados y a los responsables de seguridad de la empresa. También es importante informar a los proveedores de servicios de Internet (ISP) si el ataque viene de fuera de la red de la empresa.
- Refuerza la formación en seguridad: Refuerza la formación en seguridad para los empleados de la empresa para que puedan identificar y reportar futuros ataques de OS fingerprinting.

Un ataque de OS fingerprinting puede ser peligroso para tu red LAN y la seguridad de la empresa. Sin embargo, si sigues estos pasos, podrás mitigar el impacto del ataque y proteger tu red de futuros ataques.

Escaneo De Puertos:

El escaneo de puertos es una técnica utilizada para identificar los servicios y aplicaciones que se están ejecutando en un dispositivo conectado a una red. Esta técnica de ataque se utiliza comúnmente para identificar posibles vulnerabilidades en los sistemas y aplicaciones, y para detectar dispositivos que pueden ser blanco de ataques posteriores.

Los atacantes utilizan herramientas de escaneo de puertos, como Nmap, para enviar paquetes a diferentes puertos de los dispositivos conectados a la red. Estos paquetes contienen solicitudes para conectarse a los servicios o aplicaciones que se ejecutan en los puertos, y las respuestas a estas solicitudes indican si el servicio está disponible y, en algunos casos, información sobre el sistema operativo y la versión de la aplicación que se está ejecutando.

Una vez que los atacantes obtienen información sobre los servicios y aplicaciones que se ejecutan en los dispositivos de la red, pueden utilizar esta información para identificar posibles vulnerabilidades y diseñar ataques específicos que exploten estas vulnerabilidades. Por ejemplo,

si se detecta un servidor web en un dispositivo, el atacante puede intentar realizar ataques de inyección de SQL o de Cross-Site Scripting (XSS) para comprometer la seguridad del servidor.

Para protegerse contra los ataques de escaneo de puertos, es importante que los administradores de red monitoreen el tráfico de red y configuren los cortafuegos de red para bloquear el tráfico no autorizado. También es importante que los dispositivos se mantengan actualizados con los parches de seguridad más recientes para evitar que los atacantes aprovechen vulnerabilidades conocidas en los servicios y aplicaciones que se ejecutan en los dispositivos.

Síntomas de un ataque de escaneo de puertos en una red lan:

Es difícil detectar directamente un ataque de escaneo de puertos, ya que este tipo de ataque generalmente no causa daño visible a los dispositivos de la red. Sin embargo, hay algunos signos que pueden indicar un posible ataque de escaneo de puertos en una red LAN. Algunos de estos síntomas incluyen:

- ***Aumento del tráfico de red:*** Un ataque de escaneo de puertos puede generar un aumento en el tráfico de red, ya que el atacante envía paquetes a diferentes puertos de los dispositivos de la red para identificar los servicios y aplicaciones que se están ejecutando. Si se detecta un aumento inusual en el tráfico de red, puede ser una señal de que se está llevando a cabo un ataque de escaneo de puertos.
- ***Registros de cortafuegos:*** Los cortafuegos de red pueden registrar el tráfico de red entrante y saliente, lo que puede revelar intentos de escaneo de puertos por parte de atacantes externos. Si se detectan varios intentos de conexión a diferentes puertos desde una dirección IP, puede ser una señal de que se está llevando a cabo un ataque de escaneo de puertos.

- ***Actividad inusual en los registros del sistema:*** Los sistemas operativos de los dispositivos de la red pueden registrar actividad inusual, como intentos de conexión fallidos, que pueden indicar que se está llevando a cabo un ataque de escaneo de puertos. Los administradores de red deben monitorear los registros del sistema para detectar actividades sospechosas.

Es importante que los administradores de red monitoreen el tráfico de red y configuren los cortafuegos de red para bloquear el tráfico no autorizado, incluyendo el tráfico de escaneo de puertos. También es importante que los dispositivos se mantengan actualizados con los parches de seguridad más recientes para evitar que los atacantes aprovechen vulnerabilidades conocidas en los servicios y aplicaciones que se ejecutan en los dispositivos.

Hay varios tipos de ataques de escaneo de puertos que los atacantes pueden utilizar para detectar servicios y aplicaciones en una red LAN. Algunos de los tipos más comunes de ataques de escaneo de puertos incluyen:

- ***Escaneo TCP SYN:*** En este tipo de ataque, el atacante envía paquetes TCP SYN (solicitud de conexión) a diferentes puertos en un dispositivo de la red. Si el puerto está abierto, el dispositivo enviará un paquete TCP SYN/ACK (acknowledgement), lo que indica que está listo para establecer una conexión. El atacante puede utilizar esta información para identificar servicios y aplicaciones que se están ejecutando en el dispositivo.
- ***Escaneo TCP Connect:*** Este tipo de ataque implica el intento de establecer una conexión TCP completa con un dispositivo en un puerto específico. Si el puerto está abierto, el dispositivo responderá con un paquete TCP ACK (reconocimiento), lo que indica que la conexión se ha establecido con éxito. El atacante puede utilizar esta información para identificar los servicios y aplicaciones que se están ejecutando en el dispositivo.

- ***Escaneo UDP:*** A diferencia de TCP, el protocolo UDP (User Datagram Protocol) no establece una conexión antes de enviar datos, lo que hace que el escaneo de puertos UDP sea más difícil de realizar. En este tipo de ataque, el atacante envía paquetes UDP a diferentes puertos en un dispositivo de la red y espera una respuesta. Si recibe una respuesta, puede determinar que el puerto está abierto y que un servicio o aplicación está escuchando en ese puerto.
- ***Escaneo XMAS:*** Este tipo de ataque implica el envío de paquetes TCP que establecen una conexión con los tres indicadores de control establecidos: FIN (finalización), URG (urgente) y PSH (pulsar). Si el puerto está abierto, el dispositivo no responderá con ningún paquete, lo que indica que el puerto está abierto pero no hay servicio o aplicación escuchando en ese puerto.

Estos son solo algunos de los tipos de ataques de escaneo de puertos que los atacantes pueden utilizar para detectar servicios y aplicaciones en una red LAN. Es importante que los administradores de red estén al tanto de estas técnicas y utilicen medidas de seguridad adecuadas para proteger su red de estos ataques.

Gestión del Incidente:

La ISO 27032 proporciona las siguientes recomendaciones para prevenir ataques de escaneo de puertos:

- Configurar dispositivos de red y sistemas para limitar el acceso no autorizado a puertos y servicios.
- Utilizar software de seguridad actualizado y configurarlo para detectar y bloquear ataques de escaneo de puertos.

- Monitorizar constantemente la actividad de red y sistemas para detectar patrones anormales.
- Realizar pruebas regulares de seguridad para identificar vulnerabilidades.
- Mantener actualizado el software y el sistema operativo para corregir las vulnerabilidades conocidas.
- Establecer políticas y procedimientos claros para la gestión de la seguridad de la información.

Es importante tener en cuenta que la prevención de ataques de escaneo de puertos es un proceso continuo que requiere monitoreo y actualización constante para adaptarse a los nuevos métodos y técnicas utilizados por los atacantes.

Lista Chequeo

Un ataque de escaneo de puertos se produce cuando un atacante intenta identificar los puertos abiertos en los sistemas de una red para luego intentar explotarlos. Si tu empresa ha recibido un ataque de escaneo de puertos en tu red LAN, sigue los siguientes pasos para mitigar el impacto del ataque y restaurar la funcionalidad de tu red:

- ***Identifica la fuente del ataque:*** Utiliza herramientas de análisis de red para identificar la dirección IP del dispositivo que está realizando el escaneo de puertos en la red.
- ***Bloquea la dirección IP del atacante:*** Bloquea la dirección IP del dispositivo malicioso en tu red para evitar que continúe realizando el escaneo de puertos.
- ***Identifica los puertos abiertos:*** Utiliza herramientas de análisis de red para identificar los puertos abiertos en tus sistemas.

- ***Cierra los puertos no esenciales***: Cierra los puertos no esenciales en los sistemas de la red para reducir la superficie de ataque y minimizar la exposición de los sistemas a posibles ataques.
- ***Actualiza tus medidas de seguridad***: Actualiza tus medidas de seguridad para prevenir futuros ataques de escaneo de puertos en la red. Algunas medidas que podrías tomar incluyen la utilización de autenticación de dispositivos, la implementación de un sistema de detección y prevención de intrusiones, y la configuración de políticas de seguridad de red adecuadas.
- ***Comunica el incidente:*** Comunica el incidente a los usuarios afectados y a los responsables de seguridad de la empresa. También es importante informar a los proveedores de servicios de Internet (ISP) si el ataque viene de fuera de la red de la empresa.
- ***Refuerza la formación en seguridad***: Refuerza la formación en seguridad para los empleados de la empresa para que puedan identificar y reportar futuros ataques de escaneo de puertos.

Un ataque de escaneo de puertos puede ser peligroso para tu red LAN y la seguridad de la empresa. Sin embargo, si sigues estos pasos, podrás mitigar el impacto del ataque y proteger tu red de futuros ataques.

Icmp Tunneling

Un ataque de ICMP tunneling en una red LAN es un tipo de ataque en el que un atacante utiliza el protocolo ICMP (Internet Control Message Protocol) para crear un canal de comunicación oculto a través del cual puede enviar tráfico malicioso. El ataque se basa en la capacidad de ICMP para transportar datos de control entre dispositivos de red.

En un ataque de ICMP tunneling, el atacante utiliza un software malicioso para encapsular datos maliciosos dentro de paquetes ICMP y los envía a través de la red a un servidor remoto. Debido a que los paquetes ICMP no se inspeccionan generalmente de la misma manera que otros tipos de tráfico, pueden pasar desapercibidos en una red.

Una vez que los paquetes ICMP maliciosos llegan al servidor remoto, el atacante puede usarlos para tomar el control del servidor o para acceder a información confidencial. También pueden utilizar el canal creado por el protocolo ICMP para enviar tráfico adicional a través de la red y realizar otros tipos de ataques, como el robo de información de la red.

Para prevenir este tipo de ataque, se recomienda configurar los firewalls para bloquear el tráfico ICMP y configurar la red para monitorear y registrar el tráfico ICMP. También es importante tener en cuenta que algunos protocolos y servicios legítimos, como la herramienta de diagnóstico Ping, utilizan ICMP y pueden ser afectados si se bloquea todo el tráfico ICMP. En general, la prevención de los ataques de ICMP tunneling implica un equilibrio entre la seguridad y la funcionalidad de la red.

Síntomas de un ataque de ICMP tunneling en una red lan:

Los ataques de ICMP tunneling en una red LAN pueden ser difíciles de detectar debido a que los paquetes ICMP suelen ser menos monitoreados que otros tipos de tráfico de red. Sin embargo, algunos de los síntomas que podrían indicar un ataque de ICMP tunneling incluyen:

- ***Ralentización de la red:*** Los ataques de ICMP tunneling pueden causar un aumento en el tráfico de la red, lo que puede ralentizar el rendimiento de la red.

- ***Tiempo de inactividad inesperado:*** Si el ataque de ICMP tunneling se utiliza para enviar tráfico malicioso al servidor, puede causar interrupciones en el servicio y tiempo de inactividad en la red.
- ***Aumento en el tráfico de ICMP:*** Los ataques de ICMP tunneling suelen implicar un aumento en el tráfico de ICMP en la red, lo que podría ser indicativo de un ataque.
- ***Anomalías en los registros de tráfico:*** Si el ataque de ICMP tunneling se realiza a través de un canal de comunicación oculto, puede que no se refleje en los registros de tráfico normales. Sin embargo, los administradores de red pueden buscar anomalías en los registros de tráfico para detectar cualquier actividad inusual.

En general, los ataques de ICMP tunneling pueden ser difíciles de detectar, por lo que es importante que los administradores de red monitoreen cuidadosamente el tráfico de la red y estén atentos a cualquier actividad inusual que pueda indicar un ataque. Además, es importante implementar medidas de seguridad adecuadas, como la configuración del firewall y la limitación del acceso a la red para minimizar la exposición a este tipo de ataques.

Existen varios tipos de ataques de ICMP tunneling a una red LAN, algunos de los más comunes incluyen:

- ***Ataque de puerta trasera*:** En este tipo de ataque, el atacante utiliza ICMP tunneling para crear un canal de comunicación oculto a través del cual puede acceder al sistema comprometido y establecer una puerta trasera que le permita acceder al sistema en el futuro.
- ***Ataque de exfiltración de datos:*** En este tipo de ataque, el atacante utiliza ICMP tunneling para enviar información confidencial fuera de la red sin ser detectado. El atacante puede utilizar este canal para transferir información a un servidor remoto controlado por él.

- ***Ataque de control remoto*:** En este tipo de ataque, el atacante utiliza ICMP tunneling para tomar el control de un servidor remoto. Una vez que ha establecido una conexión oculta a través de la red, el atacante puede ejecutar comandos en el servidor remoto y tomar el control del sistema.
- ***Ataque de denial-of-service (DoS):*** En este tipo de ataque, el atacante utiliza ICMP tunneling para inundar la red con tráfico malicioso, lo que puede causar interrupciones en el servicio y tiempo de inactividad en la red.

En general, los ataques de ICMP tunneling pueden ser muy dañinos para una red LAN y pueden ser difíciles de detectar. Por lo tanto, es importante implementar medidas de seguridad adecuadas, como la configuración del firewall y la limitación del acceso a la red para minimizar la exposición a este tipo de ataques. Además, se recomienda monitorear cuidadosamente el tráfico de la red y estar atentos a cualquier actividad inusual que pueda indicar un ataque.

Gestión del Incidente:

La ISO 27032 proporciona las siguientes recomendaciones para prevenir ataques por túneles ICMP:

- Configurar dispositivos de red y sistemas para limitar el uso de protocolos ICMP.
- Utilizar software de seguridad actualizado y configurarlo para detectar y bloquear ataques de túneles ICMP.
- Monitorizar constantemente la actividad de red y sistemas para detectar patrones anormales.
- Realizar pruebas regulares de seguridad para identificar vulnerabilidades.

- Mantener actualizado el software y el sistema operativo para corregir las vulnerabilidades conocidas.
- Establecer políticas y procedimientos claros para la gestión de la seguridad de la información.
- ***Firewalls:*** Implementar firewalls para filtrar paquetes y prevenir ataques.
- ***Control de acceso:*** Limitación y control de acceso a los sistemas y datos críticos.
- ***Copias de seguridad:*** Realizar copias de seguridad regulares de los datos importantes y asegurarse de que estén disponibles para una recuperación rápida en caso de un ataque.
- ***Formación de los empleados:*** Capacitar a los empleados en la identificación de correos electrónicos sospechosos y otros métodos de phishing.
- ***Uso de software de seguridad:*** Utilizar software antivirus y anti-malware actualizado para proteger los sistemas y datos.
- ***Monitorización y detección de intrusiones:*** Implementar un sistema de monitorización y detección de intrusiones para detectar y responder a los ataques de manera rápida.
- ***Políticas de seguridad sólidas:*** Establecer políticas de seguridad sólidas y asegurarse de que todos los empleados las conozcan y las sigan.
- ***Configuración de red segura:*** Configurar los dispositivos de red de manera segura para prevenir ataques por ICMP tunneling y otras vulnerabilidades de red.

Lista de Chequeo

Un ataque ICMP tunneling es una técnica utilizada por los atacantes para enviar tráfico malicioso a través del protocolo ICMP (Internet Control Message Protocol). Si tu empresa ha recibido un ataque de este tipo en tu red LAN, sigue los siguientes pasos para mitigar el impacto del ataque y restaurar la funcionalidad de tu red:

- ***Identifica la fuente del ataque:*** Utiliza herramientas de análisis de red para identificar la dirección IP del dispositivo que está realizando el ataque ICMP tunneling en la red.
- ***Bloquea la dirección IP del atacante:*** Bloquea la dirección IP del dispositivo malicioso en tu red para evitar que continúe realizando el ataque ICMP tunneling.
- ***Identifica el tipo de tráfico malicioso***: Utiliza herramientas de análisis de red para identificar el tipo de tráfico malicioso que está siendo enviado a través del protocolo ICMP.
- ***Configura tu firewall:*** Configura tu firewall para bloquear el tráfico malicioso identificado. También puedes configurar el firewall para bloquear todo el tráfico ICMP, si no es esencial para tu red.
- ***Actualiza tus medidas de seguridad:*** Actualiza tus medidas de seguridad para prevenir futuros ataques de ICMP tunneling en la red. Algunas medidas que podrías tomar incluyen la utilización de autenticación de dispositivos, la implementación de un sistema de detección y prevención de intrusiones, y la configuración de políticas de seguridad de red adecuadas.
- ***Comunica el incidente:*** Comunica el incidente a los usuarios afectados y a los responsables de seguridad de la empresa. También es importante informar a los proveedores de servicios de Internet (ISP) si el ataque viene de fuera de la red de la empresa.

- ***Refuerza la formación en seguridad***: Refuerza la formación en seguridad para los empleados de la empresa para que puedan identificar y reportar futuros ataques de ICMP tunneling.

Un ataque ICMP tunneling puede ser peligroso para tu red LAN y la seguridad de la empresa. Sin embargo, si sigues estos pasos, podrás mitigar el impacto del ataque y proteger tu red de futuros ataques.

7. Ataque Loki

El ataque Loki es un tipo de ataque de malware que se utiliza para infiltrarse en los sistemas informáticos y robar información confidencial. Se sabe que el malware Loki es muy sigiloso y difícil de detectar, ya que utiliza técnicas avanzadas de encubrimiento y evasión para evitar la detección por parte de los sistemas de seguridad.

El malware Loki a menudo se envía a través de correos electrónicos, de phishing o sitios web maliciosos que engañan a los usuarios para que descarguen y ejecuten el archivo infectado. Una vez instalado en un sistema, el malware Loki utiliza una variedad de métodos para evitar la detección, incluida la inyección de código en procesos legítimos del sistema y el cifrado de sus comunicaciones.

El objetivo principal del ataque Loki: Es robar información confidencial, como contraseñas, detalles de inicio de sesión, información financiera y otra información personal. El malware Loki también se puede usar para instalar malware adicional, como registradores de pulsaciones de teclas y troyanos, en el sistema infectado.

Para protegerse de los ataques de Loki, es importante estar siempre atento a los correos electrónicos de phishing y no descargar archivos adjuntos de remitentes desconocidos. También

debe mantener su sistema actualizado con las últimas actualizaciones de seguridad y utilizar soluciones de seguridad como firewalls y sistemas de detección. Lokibot, también conocido como Loki PWS o Loki-bot, es un malware perteneciente a la familia de troyanos activo desde 2015 y utilizado en campañas globales desde entonces. Está diseñado para robar credenciales de navegadores, clientes FTP/SSH, sistemas de mensajería e incluso billeteras criptográficas.

Originalmente se desarrolló en lenguaje C y se promociona en foros y mercados clandestinos de la red oscura. Las primeras versiones fueron diseñadas para robar billeteras de criptomonedas y contraseñas para aplicaciones utilizadas por las víctimas, así como también almacenadas en Windows. Lokibot también se puede definir como “malware como servicio” (MaaS); significa software malicioso puesto a disposición como un servicio para uso de terceros. Por ello, sigue siendo una herramienta atractiva para los ciberdelincuentes ya que les permite crear sus propias versiones de Lokibot. (Gonzáles, 2021)

¿Cuáles son los síntomas?

Cuando se instala el ransomware LOCKY, puede generar perdida de archivos, bloqueos del sistema de seguridad, bloquea funciones básicas del equipo entre las cuales se podría mencionar el bloqueo de uso del teclado o el mouse, lo mismo que puede impedir el ingreso al escritorio del sistema, etc.

¿Cómo se identifica?

Lokibot es un malware similar a un troyano que roba información confidencial de las computadoras comprometidas, como nombres de usuario, contraseñas, billeteras criptográficas y otros. También se ha observado que las cargas útiles de Windows de Lokibot se distribuyen

mediante la explotación de vulnerabilidades heredadas como CVE-2017-11882 en Microsoft Office.

Entre las características clave de este malware se encuentra la capacidad de eliminar archivos, deshabilitar procesos del sistema y bloquear la instalación de soluciones de seguridad en el dispositivo de la víctima.

Lokibot es desplegado por una red de bots (cualquier grupo de computadoras infectadas y controladas de forma remota por un atacante) que consta de computadoras comprometidas que se conectan a un servidor C&C (comando y control) para enviar los datos recibidos de la víctima. Una vez que el malware obtiene acceso a la información confidencial de una víctima, recupera esa información, generalmente a través de HTTP. (Gonzáles, 2021)

¿Cómo combatir el ataque? (Planificación)

- En el caso de correo electrónico, anotar la dirección del remitente y los enlaces o archivos adjuntos que pueda contener.
- Compruebe la extensión del archivo adjunto. Por ejemplo, si el archivo termina en ".pdf.exe", la extensión final determinará el tipo de archivo, en este caso será ".exe"; es un archivo ejecutable.
- Si sospecha de un correo electrónico, no abra el archivo adjunto.
- Asegurarse de mantener el sistema operativo actualizado, ya que las actualizaciones incluyen parches de seguridad.
- Descarga la aplicación desde la tienda oficial.
- Instalar un software antivirus para detectar dicho malware a tiempo.

VII. Actualice las contraseñas para diferentes aplicaciones con regularidad. (Gonzáles, 2021)

Consecuencias

Los actores de amenazas generalmente usan Lokibot para atacar dispositivos que ejecutan Windows. Se distribuye principalmente a través de campañas de phishing que contienen archivos adjuntos maliciosos o direcciones URL incrustadas. Estos archivos adjuntos pueden ser archivos de Word, Excel o PDF, u otros tipos de extensiones de archivo, como .gz o .zip, que imitan los archivos PDF o .txt.

A lo largo de los años, estas campañas han cambiado los elementos que utilizan como trampa para enviar archivos adjuntos, que van desde facturas, ofertas o aparentes confirmaciones de pedidos.

A partir de julio de 2020, poco después de la declaración de la pandemia, la actividad de este malware aumentó significativamente y los atacantes comenzaron a enviar archivos adjuntos maliciosos sobre cualquier tema relacionado con el COVID-19 para que los usuarios incautos lo aceptaran al abrir los archivos adjuntos en el correo electrónico. (Gonzáles, 2021)

Ataque De Secuencia TCP

El ataque de secuencia del Protocolo de control de transmisión (TCP) es un tipo de ataque de red que aprovecha las vulnerabilidades en los números de secuencia de TCP que pueden interrumpir la conexión entre dos dispositivos. Un atacante puede enviar paquetes TCP maliciosos que contienen información de secuencia errónea que puede hacer que el sistema

acepte paquetes que de otro modo serían rechazados, logrando así el objetivo de terminar la conexión.

Este es un protocolo basado en conexión que requiere que se establezca una conexión formal entre el remitente y el receptor antes de que los datos puedan transferirse entre ellos. Esta conexión formal se denomina "apretón de manos de 3 vías" (la conexión se identifica por los conectores en cada extremo de la conexión). Durante este proceso, se requieren 3 mensajes (SYN, SYN/ACK y ACK) para establecer la conexión. (Jiménez, 2020)

En pocas palabras, se utiliza un ataque de predicción de secuencia TCP basado en la predicción del número de secuencia para identificar paquetes en una conexión TCP. De esta manera pueden manipular paquetes y comprometer la seguridad. (Jiménez, 2020)

El objetivo del atacante en este caso es determinar qué número de secuencia utilizará el servidor que está a punto de enviar el paquete. Si el atacante conoce este número, puede enviar paquetes falsificados al servidor de destino que parecen ser reales y son enviados por el servidor de destino. (Jiménez, 2020)

¿Cómo se identifica?

Aquí hay algunos pasos generales a seguir para detectar un ataque de flujo TCP en su red local:

- ***Supervisar y analizar el tráfico de red.*** Utilice herramientas de monitoreo de red como analizadores de red o sistemas de detección de intrusos (IDS) para capturar y analizar el tráfico de red en busca de anomalías en la secuencia de paquetes TCP. Preste especial atención a los números de secuencia y los números de reconocimiento en los

encabezados TCP, ya que los atacantes pueden intentar manipularlos para obtener conexiones falsas o cadenas no válidas.

- ***Analice los patrones de tráfico:*** Supervise los patrones de tráfico de la red local en busca de comportamientos inusuales. Por ejemplo, si ve una gran cantidad de paquetes TCP con números de secuencia secuenciales o repetidos, esto podría ser una señal de un ataque de secuencia TCP. Los atacantes pueden intentar adivinar o falsificar números de secuencia para entrar en la red o realizar ataques de denegación de servicio.

- ***Supervisión del registro de eventos:*** vea los registros de eventos de los dispositivos de red, como cortafuegos, enrutadores y conmutadores, en busca de actividad de transmisión TCP sospechosa. Por ejemplo, los registros de eventos de reinicio de la conexión TCP inesperados, las fallas de conexión frecuentes o las desconexiones inexplicables podrían ser indicativos de un ataque a la transmisión TCP.

- ***Análisis del comportamiento del servidor:*** Verifique el comportamiento de los servidores en su red local en busca de actividad sospechosa. Por ejemplo, si un servidor muestra paquetes TCP de alto rendimiento con números de secuencia no válidos o inusuales, podría estar relacionado con un ataque de secuencia TCP.

- ***Utilice herramientas de detección especializadas.*** Existen herramientas especializadas para detectar ataques en flujos TCP que pueden ayudar a identificar estos ataques. Por ejemplo, Snort, Suricata, wazuh y Bro son sistemas populares de detección de intrusos que pueden detectar patrones de tráfico inusuales relacionados con ataques de flujo TCP.

- Cuando no se recibe la información del paquete o llegan paquetes que nunca se envían.

a. Cabe señalar que identificar un ataque en un flujo TCP puede ser complejo y requiere un enfoque integral que incluya monitoreo del tráfico de red, análisis de patrones de tráfico, visualización de registros de eventos y análisis del comportamiento de los nodos de red en la red. Si sospecha un ataque de flujo TCP en su red local, le recomendamos que contrate a un equipo de expertos en seguridad cibernética y tome las medidas adecuadas para mitigar y remediar la situación.

¿Cómo combatir el ataque?

Es importante que el servidor de destino pueda identificar los paquetes genuinos y falsos que recibe. Y para que esto suceda, la información puede transmitirse con diferencias horarias. Esto puede ayudar a comparar los números de secuencia recibidos y evitar que se reciban paquetes falsificados. (Delva, 2021)

Puede protegerse contra TCP o ataques de predicción de secuencias mediante el uso de un firewall. Lo que evita que pasen paquetes externos, lo mismo se puede lograr configurando el enrutador para ello. (Delva, 2021)

En respuesta a sus propias observaciones, el Grupo de trabajo de ingeniería de Internet (IETF) emitió un estándar actualizado en 2012 (RFC 6528) que establece un algoritmo mejorado para generar números de secuencia iniciales para transmisiones a través de TCP. Está diseñado para mejorar la confiabilidad de la generación de números de secuencia en comparación con el análisis predictivo y el monitoreo, lo que brinda a los ciberdelincuentes un fácil acceso a los números de secuencia en el sistema heredado.

A nivel corporativo, los proveedores de sistemas operativos respondieron a la amenaza mediante la introducción de métodos nuevos y más impredecibles para generar números de secuencia, con un éxito parcial.

Una estrategia más eficaz para las organizaciones y los administradores de red es interceptar los paquetes enrutables de origen y los paquetes direccionables en sus propias redes. Los servicios que dependen de la autenticación basada en IP se desconectarán por completo cuando detecten la presencia de opciones de enrutamiento de origen. (Ramiro, 2018)

Consecuencias

También es importante saber qué puede pasar si un atacante tiene éxito y envía paquetes falsificados. (Jiménez, 2020)

Uno de los resultados que se pueden obtener de este tipo de amenazas es la denominada inyección de conexión TCP. El atacante ingresa los datos de su elección. Esto puede hacer que la conexión TCP actual se cierre cuando se reciben paquetes falsificados. (Jiménez, 2020).

Tenga en cuenta que este tipo de ataque generalmente se dirige a dispositivos más antiguos que no tienen las actualizaciones necesarias o que están desactualizados. Por ello, es importante que todos los equipos que conectemos a la red tengan instalados todos los parches y actualizaciones disponibles para eliminar estas vulnerabilidades. (Jiménez, 2020)

Ataques de redireccionamiento ICMP:

ICMP (Protocolo de Mensajes de Control de Internet). Si el enrutador detecta que la ruta desde el host hasta el destino no es óptima, envía un paquete de redirección ICMP al servidor solicitando la redirección. Al mismo tiempo, el enrutador envía el datagrama original a su

destino. ICMP no es un protocolo de enrutamiento, pero puede redirigir direcciones o flujos de datos (al puerto correcto).

En los ataques de redirección de ICMP, el atacante envía ICMP para reenviar preferentemente paquetes al servidor de la víctima para que los paquetes no puedan reenviarse a la puerta de enlace. Estos tipos de ataques pueden lanzarse desde redes locales y globales.

Al recibir un paquete ICMP inalcanzable que indica que la red o el host es inalcanzable, algunos sistemas consideran directamente que los paquetes de seguimiento a la red o al host no pueden llegar a su destino y, por lo tanto, cierran la conexión con el servidor o la red. Sabiendo esto, los atacantes falsifican paquetes ICMP inaccesibles para romper la conexión entre la víctima y el receptor para llevar a cabo ataques. (Jimenez, 2019)

¿Cuáles son los síntomas?

Los ataques de redirección ICMP en una red de área local (LAN) son una forma de ataque a la red que puede comprometer la seguridad y la integridad de una red. Estos son algunos síntomas posibles de un ataque de redirección ICMP en su red local:

- ***Cambios de ruta de red no deseados.*** Uno de los síntomas más obvios de un ataque de redirección ICMP es que los paquetes de red comienzan a seguir una ruta diferente a la habitual. Esto puede generar tráfico inusual que pasa por servidores o enrutadores que no forman parte del tráfico normal.
- ***Reducción del rendimiento de la red:*** los ataques de redirección ICMP pueden causar congestión en la red, lo que puede conducir a una reducción en el rendimiento general de la LAN. Es posible que notes que la red se ralentiza o que hay un retraso en la comunicación entre dispositivos.

- ***Actividad anormal en el registro del cortafuegos.*** Si supervisa los registros de su cortafuegos, es posible que observe una actividad inusual de redirección de ICMP. Esto puede incluir una gran cantidad de paquetes ICMP entrantes o salientes o patrones de tráfico que no son típicos de la red.
- ***Acceso no autorizado a los recursos de la red:*** los atacantes pueden usar ataques de redirección ICMP para redirigir el tráfico de la red a servidores o dispositivos bajo su control. Esto puede permitirles acceder a recursos de red a los que normalmente no tendrían acceso, como sistemas o datos confidenciales.
- ***Comportamiento anormal de los dispositivos de red.*** Los dispositivos de red afectados por el ataque de redirección ICMP pueden mostrar un comportamiento inusual, como reinicios inesperados, desconexiones o errores de configuración. Esto podría significar que los atacantes están manipulando la configuración de red del dispositivo para redirigir el tráfico.

a. Tenga en cuenta que estos síntomas también pueden deberse a otros problemas de red o errores de configuración de red. Por lo tanto, es esencial contar con las herramientas y soluciones de seguridad adecuadas, como firewalls, sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS), y realizar análisis de red a fondo para confirmar la presencia de un ataque. redirigido Si sospecha un ataque, le recomendamos que se comunique con un profesional de ciberseguridad para que lo ayude a investigar y mitigar adecuadamente el problema.

¿Cómo se identifica?

Identificar un ataque de redirección ICMP en una red local puede ser un proceso complejo pero importante para proteger su red. Estos son algunos pasos generales que puede seguir para detectar este tipo de ataque:

- ***Supervise el tráfico de la red***. Use herramientas de monitoreo de red como el analizador de red para capturar y analizar el tráfico de red en su red local. Preste especial atención a los paquetes ICMP (Protocolo de mensajes de control de Internet) enviados a través de la red.
- ***Detección de patrones sospechosos***: busque patrones inusuales o sospechosos en el tráfico ICMP. Por ejemplo, si observa una gran cantidad de paquetes ICMP que provienen de o hacia la misma dirección IP, podría tratarse de un ataque de redirección ICMP.
- ***Verifique las direcciones IP de origen y destino***: verifique las direcciones IP de origen y destino de los paquetes ICMP. Un atacante puede intentar redirigir el tráfico ICMP a través de su propia dirección IP o a una dirección IP falsificada. Si observa que los paquetes ICMP que provienen de una dirección IP no deberían enviar este tipo de tráfico, o si los paquetes ICMP se envían a una dirección IP que no debería recibirlos, es posible que ICMP los esté redirigiendo. ataque.
- ***Ver los registros del cortafuegos***: Verifique los registros del cortafuegos de la LAN en busca de posibles reglas de redirección ICMP no autorizadas o inusuales. Un atacante podría explotar una vulnerabilidad de configuración del firewall para configurar reglas de redirección ICMP y redirigir el tráfico de forma malintencionada.

- ***Realizar análisis de tráfico:*** Realice un análisis detallado del tráfico ICMP capturado para detectar patrones o características inusuales. Por ejemplo, si ve una gran cantidad de paquetes ICMP de tamaño inusual o en un orden extraño, podría tratarse de un ataque de redirección ICMP.
- ***Esté atento a otros signos de infracciones de seguridad:*** además del tráfico ICMP, también debe estar alerta a otros signos de infracciones de seguridad en su red local, como cambios inusuales en la configuración de la red, actividad de inicio de sesión sospechosa o comportamiento anormal de los dispositivos de red.
- ***Consulta fuentes confiables***. Si sospecha ataques de redirección ICMP en su red local, es importante ponerse en contacto con fuentes confiables, como otros expertos en seguridad cibernética, para obtener más orientación y resolución de situaciones adecuadas.
- En resumen, la detección de un ataque de redireccionamiento ICMP en su red local requiere un control cuidadoso del tráfico de la red, el análisis de los patrones de tráfico, la revisión de los registros del cortafuegos y la consulta de fuentes confiables. Es importante adoptar un enfoque proactivo para la detección de amenazas y mantenerse actualizado con las mejores prácticas de ciberseguridad para proteger su red local de posibles ataques.

¿Cómo combatir el ataque? (Planificación)

Aquí hay algunas estrategias y mejores prácticas que puede seguir para combatir un ataque de redirección ICMP en su red local:

- ***Filtrar ICMP.*** Configure dispositivos de red como enrutadores y firewalls para filtrar el tráfico ICMP. Puede bloquear o restringir ciertos tipos de mensajes ICMP, como los mensajes de redireccionamiento ICMP, para reducir la probabilidad de ataques de redireccionamiento ICMP exitosos.
- ***Actualizaciones de firmware y parches:*** mantenga sus dispositivos de red actualizados con las últimas actualizaciones de firmware y parches de seguridad. Esto ayuda a cerrar vulnerabilidades potenciales y vulnerabilidades conocidas que un atacante podría explotar.
- ***Seguridad multinivel.*** Implemente una estrategia de seguridad de varias capas, lo que significa que debe usar varias medidas de seguridad, como firewalls, segmentación de red, autenticación de dispositivos y cifrado de datos para proteger su red de ataques cibernéticos, incluidos los ataques de redirección ICMP.
- ***Supervisión de la red.*** Configure un sistema de monitoreo de red para detectar actividades sospechosas, como redireccionamientos ICMP no autorizados. Esto puede incluir la configuración de alertas y notificaciones para que pueda responder rápidamente a cualquier actividad sospechosa.
- ***Autenticación y autorización***. Configure la autenticación y autorización de la red correctamente para que solo los dispositivos y usuarios autorizados puedan acceder a los servicios y recursos de la red. Esto ayuda a prevenir el acceso malicioso y los ataques de redirección ICMP.
- ***Educación del usuario:*** eduque a los usuarios sobre las mejores prácticas de seguridad cibernética, como no hacer clic en enlaces o descargar archivos adjuntos de correo electrónico sospechosos, no compartir contraseñas y no conectar dispositivos no autorizados a la

red local. La concienciación y la educación de los usuarios son elementos clave de la protección de la red contra los ciberataques.

- ***Plan de respuesta a incidentes:*** Desarrolle un plan de respuesta a incidentes de red que incluya procedimientos claros y funciones definidas para hacer frente a los ataques de redireccionamiento ICMP u otros tipos de ciberataques. Esto ayuda a minimizar los tiempos de respuesta y reducir los posibles daños.
- Es importante recordar que la ciberseguridad es un proceso continuo y en evolución. Para proteger su red local de ataques de redireccionamiento ICMP y otros tipos de ataques de red, manténgase actualizado con las últimas amenazas y mejores prácticas de seguridad. Consulta con expertos en ciberseguridad o expertos en la materia.

Consecuencias

La redirección ICMP es una técnica de ataque utilizada para manipular las tablas de enrutamiento de los dispositivos en una red, lo que puede conducir a la redirección no autorizada del tráfico de la red a una ruta no deseada. Esto puede tener una serie de consecuencias negativas para su red local, que incluyen:

- ***Recolectar datos.*** Un ataque de redirección ICMP podría permitir que un atacante intercepte e intercepte el tráfico de red que se está redirigiendo a través de su propio dispositivo. Esto podría revelar datos importantes o confidenciales transmitidos a través de la red, como contraseñas, información financiera o información personal.
- ***Espionaje y vigilancia.*** Al redirigir el tráfico de la red a través de su propio dispositivo, un atacante puede obtener acceso no autorizado a la información y la actividad del usuario en su red local. Esto puede incluir el seguimiento de mensajes, el seguimiento de

actividades en línea y la obtención de información sobre las actividades de navegación de los usuarios sin su consentimiento.

- ***Denegación de servicio:*** los redireccionamientos ICMP también se pueden utilizar para provocar una denegación de servicio (DoS) en su red local. Al redirigir el tráfico de la red a través de rutas no válidas o incorrectas, puede provocar la congestión de la red, lo que resulta en un rendimiento deficiente de la red o incluso la pérdida total de comunicación entre los dispositivos de la red.

- ***Manipulación de datos.*** Un ataque de redirección ICMP podría permitir que un atacante modifique o manipule los datos que se transmiten. Esto puede implicar alterar o insertar datos en la red de comunicación, lo que puede generar resultados incorrectos, errores o fallas en los sistemas y aplicaciones que dependen de la integridad de los datos.

- ***Brecha de seguridad***: al destruir las tablas de enrutamiento de un dispositivo en la red local, un ataque de redirección ICMP puede abrir brechas de seguridad en la red. Esto podría permitir que un atacante obtenga acceso a áreas o recursos de red a menudo restringidos, lo que podría dar lugar a un acceso no autorizado a sistemas, aplicaciones o datos confidenciales.

- Por lo general, un ataque de redirección ICMP puede tener graves consecuencias para la red local, incluida la divulgación de datos confidenciales, espionaje, degradación del rendimiento de la red y manipulación de datos. Es importante implementar medidas de seguridad adecuadas, como configuraciones de firewall, actualizaciones de software, autenticación de dispositivos y monitoreo de red para protegerse de este tipo de amenazas y mantener la red segura.

Ataque de transferencia de zona DNS

Una solicitud de transferencia de zona a un servidor DNS devuelve una lista completa de nombres de host y direcciones IP en el dominio. El roaming generalmente solo ocurre entre servidores DNS que tienen autoridad para el dominio. Los atacantes pueden consultar los servidores DNS para obtener una lista de servidores que pueden ser pirateados. Esta firma detecta intentos de roaming de fuentes distintas a los servidores DNS.

Cuando se trata de la presencia de servicios, nombres de dominio, sitios web y otros detalles como la configuración del servidor DNS, a menudo se pasan por alto, por lo que veremos qué es el roaming de DNS y qué puede hacer para divulgar información e infraestructura.

Un servidor DNS es básicamente la computadora responsable de traducir los nombres de dominio en direcciones IP. Esto facilita que los usuarios accedan al servicio porque es más difícil recordar la dirección IP.

Sin embargo, los atacantes suelen utilizarlos para recopilar información sobre la infraestructura y los subdominios de las víctimas potenciales, aunque existen herramientas automatizadas como Dnsnum para este fin.

Los atacantes realizan roaming y recopilan registros de servidores DNS porque pueden recopilar información de redes corporativas, a veces revelando direcciones IP internas, servidores y hardware. Cuando haga eso, si el ataque tiene éxito, verá mucha información expuesta. (Pérez, 2015)

¿Cuáles son los síntomas?

Un ataque de roaming de DNS es un tipo de ataque cibernético que se dirige a la infraestructura de nombres de dominio (DNS) de un sitio web o red. Este tipo de ataque se usa para obtener información sobre los registros DNS de un sitio web y se puede usar con fines maliciosos, como crear sitios web falsos o redirigir el tráfico web. Algunos síntomas de un ataque de migración de zona DNS incluyen:

- ***Aumente la cantidad de solicitudes de DNS.*** Los ataques de roaming de DNS pueden generar una gran cantidad de solicitudes de DNS a un sitio web o servidor DNS en particular. Si nota un aumento inusual en la cantidad de solicitudes de DNS, podría tratarse de un ataque continuo.
- ***Tiempos de respuesta más lentos:*** un ataque de roaming de DNS puede ralentizar significativamente los tiempos de respuesta del servidor DNS. Si notas que los tiempos de respuesta son más lentos de lo habitual, es posible que te hayan pirateado.
- ***Aparición de un nuevo registro DNS:*** en un ataque de roaming de DNS, un atacante puede agregar un nuevo registro DNS a un sitio web o servidor DNS. Si observa nuevas entradas que no le son familiares o que no están relacionadas con su sitio o red, es posible que se esté produciendo un ataque.
- ***Problemas de autenticación.*** Los ataques de roaming de DNS también se pueden usar para eludir la autenticación de sitios web o redes. Si tiene problemas de autenticación, como no poder iniciar sesión o acceder a ciertas partes de un sitio web o una red, es posible que se esté produciendo un ataque.
- Tenga en cuenta que estos síntomas también pueden estar relacionados con otros servidores DNS o problemas de red, por lo que es importante investigar más a fondo para

determinar si un ataque de migración de zona DNS está causando el problema, intente o no. Si sospecha que su sitio web o su red se han visto comprometidos, es importante que tome medidas de seguridad inmediatas, como ponerse en contacto con su proveedor de alojamiento o profesional de ciberseguridad.

¿Cómo se identifica?

Estos son algunos posibles signos de un ataque de migración de zona DNS:

- ***Solicitud para mover un área anormal***. Si observa un aumento repentino e inusual en la cantidad de solicitudes de migración de zona DNS en los registros de su servidor DNS, podría ser una señal de un ataque. Los atacantes pueden intentar enviar varias solicitudes de itinerancia en un breve período de tiempo para obtener la información de la zona DNS de su dominio.
- ***Solicitudes de roaming de servidores desconocidos***. Si recibe solicitudes de migración de zona de servidores DNS desconocidos o no autorizados, podría haber un intento de ataque. Los atacantes pueden intentar usar servidores DNS no autorizados o comprometidos para obtener acceso a su zona DNS.
- ***El registro de roaming falló o se bloqueó***. Si el registro de roaming muestra intentos fallidos o bloqueados, es posible que alguien esté intentando realizar un roaming no autorizado. Esto podría indicar un ataque en curso.
- ***Cambios de configuración de zona DNS no deseados***. Si observa cambios inesperados en la configuración de la zona DNS, como agregar nuevos registros DNS, modificar registros existentes o eliminar registros importantes, sin una explicación razonable, es un problema, podría ser indicativo de un ataque de migración de zona DNS. Un atacante puede

intentar cambiar la configuración de la zona DNS para redirigir el tráfico a servidores malintencionados u obtener información confidencial.

- ***Actividad sospechosa en otros registros DNS.*** Además de los registros de roaming, también debe revisar otros registros de DNS, como las actualizaciones de DNS y los registros de consultas. Si ve actividad sospechosa, como una gran cantidad de consultas de DNS o actualizaciones provenientes de la misma dirección IP o de una región geográfica específica, podría tratarse de un ataque de migración de zona DNS.
- Por lo tanto, para detectar un ataque de roaming de DNS, es importante monitorear regularmente los registros del servidor DNS en busca de actividad inusual, como solicitudes de roaming no autorizadas, cambios de configuración de zona, DNS no deseado y actividad sospechosa en otros registros de DNS. Además, asegúrese de tener implementadas las políticas de seguridad adecuadas, como restringir el roaming solo a servidores DNS autorizados e implementar medidas de seguridad como firewalls y sistemas de detección de intrusos (IDS) para proteger su infraestructura DNS de posibles ataques.

Planificación

¿Cómo combatir el ataque?

Es muy importante entender que los atacantes pueden usar toda esta información para atacar su computadora o toda su red. Sabiendo esto de antemano, contamos con herramientas de análisis proactivas para evitar que esto suceda. Para evitar fugas de información, el Laboratorio de Investigación de América Latina de ESET recomienda verificar los archivos de configuración en el servidor DNS. Tenga en cuenta que, según el software utilizado para este servicio, habrá un

archivo de configuración aquí para permitir o evitar que el hardware autorizado realice una transferencia en particular. (Pérez, 2015)

- ***Establecer límites de roaming:*** el roaming de DNS debe restringirse solo a servidores DNS autorizados. Asegúrese de configurar su servidor DNS para que solo permita el roaming de fuentes confiables y autorizadas. Esto se puede hacer configurando la ACL (Lista de control de acceso) en la configuración del servidor DNS.
- ***Actualice su servidor DNS.*** Mantenga sus servidores DNS actualizados con los últimos parches y actualizaciones de seguridad. Esto ayuda a cerrar posibles vulnerabilidades que un atacante podría explotar.
- ***Usar DNSSEC:*** DNSSEC (Sistema de Extensión de Seguridad DNS) es una tecnología que permite asegurar las respuestas del Sistema de Nombres de Dominio (DNS) con una firma digital. Esto ayuda a prevenir ataques de envenenamiento de caché de DNS, una técnica común utilizada en ataques de roaming.
- ***Configuración de cortafuegos y cortafuegos.*** Configure cortafuegos y cortafuegos para bloquear el tráfico no autorizado al servidor DNS. Restrinja el acceso a los puertos y protocolos necesarios para que DNS funcione y bloquee todo lo demás.
- ***Monitoree y pruebe los servidores DNS***: configure un sistema de monitoreo y prueba para sus servidores DNS. Esto le permitirá detectar y responder rápidamente a cualquier actividad sospechosa, como intentos no autorizados de mover un área.
- ***Aplica el principio de privilegio mínimo***: Asegúrate de que tus servidores DNS estén configurados con los privilegios mínimos necesarios para su funcionamiento. Esto reduce la superficie de ataque y reduce las posibilidades de que un atacante acceda a información confidencial o realice actividades maliciosas.

- ***Copia de seguridad y almacenamiento seguros***: haga una copia de seguridad de sus zonas DNS con regularidad y guárdelas de forma segura fuera de línea. Esto le permitirá recuperar rápidamente sus zonas DNS en caso de un ataque exitoso.

- ***Educa a tus usuarios***. La conciencia de seguridad juega un papel importante en la prevención de ataques cibernéticos. Informe a los usuarios de las mejores prácticas de seguridad en línea, como no hacer clic en enlaces sospechosos o descargar archivos adjuntos de fuentes desconocidas, ya que esto puede convertirse en un intermediario para el ataque de migración de la zona DNS.

- ***Mantener un plan de respuesta a incidentes.*** Tener un plan de respuesta a incidentes bien definido lo ayudará a reaccionar rápidamente en caso de un ataque exitoso de migración de zona DNS.

Asegúrese de tener procedimientos de emergencia y contactos actualizados. Por lo tanto, la protección contra los ataques de roaming de DNS implica una combinación de configuración adecuada, actualizaciones de software, monitoreo continuo, educación del usuario y planificación de respuesta a incidentes.

Por lo tanto, la protección contra los ataques de roaming de DNS implica una combinación de configuración adecuada, actualizaciones de software, monitoreo continuo, educación del usuario y planificación de respuesta a incidentes. Al aplicar estas medidas de seguridad, puede fortalecer la seguridad de su infraestructura DNS y reducir el riesgo de ataques de roaming exitosos.

Consecuencias

- ***Divulgación de información confidencial:*** durante una transferencia de zona DNS, toda la información contenida en la zona DNS está disponible, incluido el registro de nombre de dominio, el registro de subdominio, el registro de correo electrónico, la dirección IP y

otra información de configuración. Si un atacante obtiene acceso no autorizado al roaming de DNS, puede obtener acceso a información confidencial y usar esa información para actividades maliciosas como robo de identidad, phishing o espionaje.

- ***Cambio no autorizado de la configuración de DNS.*** Un ataque de roaming de DNS también puede permitir que un atacante cambie la configuración de DNS de un dominio. Esto puede incluir cambiar los registros DNS, como los registros de direcciones IP, para redirigir el tráfico de un sitio web legítimo a un sitio web malicioso. Esto puede tener consecuencias graves, como el tiempo de inactividad del sitio web, la pérdida de clientes y la pérdida de reputación.

- ***Denegación de servicio (DoS):*** un ataque de roaming de DNS también se puede utilizar como parte de un ataque de denegación de servicio (DoS). Por ejemplo, un atacante podría enviar varias solicitudes de roaming de DNS para agotar los recursos del servidor DNS de destino y hacer que falle. Esto puede resultar en la falta de disponibilidad de los servicios y sitios web alojados en este servidor DNS.

- ***Exposición a vulnerabilidades conocidas:*** DNS Roaming revela información detallada sobre la configuración del servidor DNS que podría revelar posibles vulnerabilidades conocidas. Un atacante puede usar esta información para identificar posibles vulnerabilidades en los servidores DNS y usarla para obtener acceso no autorizado o realizar otras actividades maliciosas.

- ***Daño a la reputación y pérdida de confianza.*** El impacto de un ataque de roaming de DNS va más allá de las implicaciones técnicas. También puede tener un impacto significativo en la reputación de una organización y la confianza de sus clientes y socios comerciales. Una violación de la seguridad del DNS puede hacer que una organización pierda la

confianza en su capacidad para proteger información confidencial y mantener la disponibilidad de los servicios en línea.

Por lo tanto, un ataque de migración de zona DNS puede tener graves consecuencias, incluida la divulgación de información confidencial, la modificación no autorizada de la configuración de DNS, la interrupción del servicio, la exposición a vulnerabilidades conocidas, así como daños y perjuicios a la reputación. Es muy importante que las organizaciones implementen medidas de seguridad adecuadas, como configurar correctamente los servidores DNS, aplicar parches de seguridad, autenticación y autorización.

¿Cómo prevenir los ataques CAM Overflow?

Para prevenir este tipo de ataque, cambiaremos el puerto a un puerto de acceso emitiendo acceso en modo de puerto de conmutación. Luego asignaremos la cantidad máxima de direcciones MAC en las que se almacenará la tabla CAM para esta interfaz.

Finalmente elegiremos nuestra acción de violación que se aplicará cuando el usuario (atacante) intente generar más de X direcciones MAC asociadas al mismo puerto. Elegimos cerrar este puerto, ahora si el atacante intenta realizar este ataque nuevamente en dicho switch su puerto se apagará automáticamente, también se generará un registro en este que informa al administrador que el (atacante) MAC la dirección en este puerto estaba tratando de atacarnos y el estado del puerto ahora está abajo/cerrado. (Ramiro, 2018)

Ataques DHCP:

Los servidores pueden ser víctimas de ataques como el secuestro de DHCP; donde el hacker usa una dirección MAC falsa para enviar solicitudes al servidor, lo que resulta en la

cancelación de la dirección IP, no hay más direcciones disponibles para asignar a clientes legítimos en la red. Otro ataque es la suplantación de identidad del servidor DHCP, en el que se implementa un servidor no autorizado para engañar a los clientes para que establezcan configuraciones distintas a las del servidor legítimo con el fin de interceptar el tráfico de la red y obtener información.

La indagación DHCP es una tecnología de seguridad de capa 2 integrada en los sistemas operativos de los conmutadores de red avanzados que rechaza las conexiones DHCP consideradas inapropiadas. La indagación de DHCP evita que los servidores DHCP no autorizados (maliciosos) compartan direcciones IP con clientes DHCP. La indagación de DHCP hace lo siguiente:

Comprueba si hay mensajes DHCP de fuentes no confiables y filtra los mensajes no válidos. Cree y mantenga una base de datos de federación de indagación de DHCP que contenga información sobre servidores que no son de confianza con direcciones IP alquiladas.

Utilice la base de datos de la federación de agentes de escucha DHCP para verificar las solicitudes posteriores de servidores que no son de confianza.

La indagación de DHCP generalmente divide las interfaces de los conmutadores en dos categorías: puertos confiables y puertos no confiables. Un puerto de confianza es un puerto o una fuente en la que confía el servidor DHCP. Un puerto que no es de confianza es un mensaje de puerto de un servidor DHCP que no es de confianza. Si DHCP Snooping está habilitado, los mensajes de oferta de DHCP solo se pueden enviar a través de puertos confiables. De lo contrario, se restablecerá. El protocolo de enlace crea una tabla de asociación DHCP basada en un mensaje DHCP ACK. Registre la dirección MAC del servidor, la dirección IP arrendada, el período de arrendamiento, el tipo de conexión, el número de VLAN y la información de la

interfaz asociada con el servidor. Si se reciben paquetes DHCP posteriores de servidores que no son de confianza, es decir, si el servidor no coincide con la información, se descartan. La suplantación de DHCP ocurre cuando un atacante intenta lanzar un ataque indirecto respondiendo a una solicitud de DHCP e intentando especificarse (suplantar) a sí mismo como la puerta de enlace predeterminada o el servidor DNS. De esta forma, pueden interceptar el tráfico de usuarios antes de redirigirlo al puerto real o evitar un ataque DoSed a los recursos de la dirección IP mediante el envío de solicitudes al servidor DHCP real. Si bien DHCP simplifica el direccionamiento IP, también plantea problemas de seguridad. DHCP Snooping es un mecanismo de protección que evita que direcciones DHCP no válidas ingresen a servidores DHCP maliciosos para resolver estos problemas y puede proteger contra intentos de agotamiento de recursos. Agotar todas las direcciones DHCP existentes. Los conmutadores gestionados apilables Gigabit de la serie FS S3900 pueden aprovechar al máximo esta característica para proteger su red. (Howard, 2021)

¿Cuáles son los síntomas?

- ***Fuera de la dirección IP.*** Si nota que las direcciones IP disponibles en su red se agotan rápidamente sin razón aparente, podría ser una señal de un ataque DHCP. Los atacantes pueden inundar su servidor DHCP con solicitudes falsificadas para agotar el rango de direcciones IP disponibles, lo que puede causar problemas de conexión para dispositivos legítimos en la red.
- ***Duplicar la dirección IP.*** Si tiene dispositivos en su red con direcciones IP en conflicto, es decir, varios dispositivos que solicitan la misma dirección IP, esto podría ser una

señal de un ataque DHCP. Un atacante puede asignar intencionalmente la misma dirección IP a varios dispositivos, lo que puede provocar interrupciones en la red y conflictos de direcciones IP.

- ***Asignación no autorizada de direcciones IP.*** Si observa que se están asignando direcciones IP no autorizadas en su red o estas no coinciden con el rango de direcciones IP configurado en el servidor DHCP, podría tratarse de un ataque DHCP. Los atacantes pueden intentar asignar direcciones IP falsas o no autorizadas para obtener acceso a la red o realizar actividades maliciosas.

- ***Error de conexión de red***. Si tiene problemas de conectividad de red, como dispositivos que no pueden obtener una dirección IP válida o no pueden comunicarse con otros dispositivos en la red, podría tratarse de un ataque DHCP. Los atacantes pueden interferir con la asignación de direcciones IP válidas, lo que puede provocar fallas en la conexión.

- ***Actividad sospechosa en los registros del servidor DHCP***. Si revisa los registros de su servidor DHCP y nota actividad inusual o sospechosa, como una gran cantidad de solicitudes de IP o solicitudes provenientes de direcciones MAC desconocidas, esto puede indicar que ve un ataque de DHCP. Los atacantes pueden intentar inundar el servidor DHCP con solicitudes falsificadas o utilizar direcciones MAC falsificadas para obtener direcciones IP de forma ilegal.

Es importante tener en cuenta que estos síntomas también pueden ser causados por otras causas legítimas, por lo que es importante realizar una investigación exhaustiva e involucrar a expertos en ciberseguridad para confirmar si se trata realmente de un ataque DHCP o no. Además, la aplicación de las medidas de seguridad adecuadas, como una configuración sólida del servidor DHCP, la autenticación del dispositivo y el monitoreo continuo de la red, puede ayudar a prevenir y detectar posibles ataques DHCP.

¿Cómo se identifica?

Varias formas de detectar un ataque DHCP:

- ***Analice el tráfico de la red.*** Use herramientas de monitoreo de red como Wireshark o tcpdump para capturar y analizar el tráfico DHCP en su red. Tenga en cuenta los paquetes DHCP Discover, DHCP Offer, DHCP Request y DHCP Acknowledgement. Si observa actividad inusual o excesiva en estos paquetes, podría tratarse de un ataque DHCP.
- ***Registro de eventos DHCP:*** los servidores DHCP registran eventos en su registro o registro de eventos. Verifique el registro de eventos de DHCP en busca de actividad sospechosa, como solicitar direcciones IP de direcciones MAC desconocidas, múltiples intentos de asignar direcciones IP o asignar direcciones IP a varios clientes desde la misma dirección MAC.
- ***Supervise los cambios de configuración de DHCP***: un atacante puede intentar reconfigurar el servidor DHCP para lanzar ataques. Supervise cualquier cambio en la configuración del servidor DHCP, como cambios en los parámetros de configuración o exclusiones de direcciones IP. Esto podría indicar un intento de ataque.
- movimiento anormal Supervise el tráfico de la red para detectar anomalías, como un gran tráfico de paquetes DHCP para una única dirección IP o MAC, la asignación de direcciones IP con tiempos de concesión inusuales o varias solicitudes de las mismas direcciones IP de diferentes clientes.
- ***Autenticación del servidor DHCP:*** un atacante puede usar un servidor DHCP falso para lanzar ataques. Valide el servidor DHCP utilizado en la red y asegúrese de que solo se utilicen servidores DHCP autorizados y de confianza.

- ***Análisis de registros de seguridad***. Compruebe los registros de seguridad de los sistemas y dispositivos de su red en busca de actividades sospechosas, como intentos de acceso no autorizado a un servidor DHCP, denegación de servicio (DoS) en un servidor DHCP o cambios no autorizados en la configuración del servidor DHCP.

Es importante comprender completamente cómo funciona DHCP y monitorear de manera proactiva su red en busca de signos de actividad sospechosa para identificar posibles ataques de DHCP y tomar medidas correctivas oportunas para proteger su red de posibles amenazas de ciberseguridad.

Planificación

¿Cómo combatir el ataque?

Algunos pasos que puede seguir para proteger su red de un ataque DHCP:

- ***Configuración segura del servidor DHCP.*** Asegúrese de haber configurado y mantenido de forma segura el servidor DHCP. Esto incluye cambiar la contraseña predeterminada, aplicar actualizaciones de seguridad y configurar el servidor para que solo acepte solicitudes de direcciones IP de subredes autorizadas.
- ***Filtrado de direcciones MAC:*** habilita el filtrado de direcciones MAC en el servidor DHCP para permitir solo direcciones MAC autorizadas. Esto ayuda a evitar que se asignen direcciones IP a dispositivos no autorizados.
- ***Supervisión de la red.*** Implementar un sistema de monitoreo de red para detectar y advertir de actividad sospechosa al momento de asignar direcciones IP. Esto puede incluir la identificación de direcciones IP duplicadas o la detección de patrones de asignación de direcciones IP inusuales.

- ***Segmentación de red:*** divida su red en segmentos o subredes para limitar la propagación de un ataque DHCP. Esto ayudará a limitar el impacto del ataque y proteger otras partes de la red.
- ***Actualice el sistema de seguridad.*** Asegúrese de que los parches de seguridad y las actualizaciones para el servidor DHCP y los dispositivos de red relacionados estén actualizados. Esto ayudará a proteger contra vulnerabilidades conocidas que pueden explotarse en un ataque de DHCP.
- ***Autenticación y cifrado***: implemente medidas de autenticación y cifrado para proteger las comunicaciones entre el servidor DHCP y el cliente. Esto puede incluir el uso de autenticación basada en certificados y el cifrado de mensajes a través de VPN u otros métodos de seguridad.
- ***Capacitación del personal.*** Capacite a su personal sobre las mejores prácticas de seguridad de la red, incluida la forma de detectar y responder a posibles ataques de DHCP. La concienciación y la formación de los empleados son factores clave para defenderse de los ciberataques.
- ***Cortafuegos:*** Instale y mantenga un cortafuegos adecuado para proteger su red de posibles amenazas externas, incluidos los ataques DHCP. Los firewalls pueden ayudar a bloquear el tráfico no autorizado y limitar la superficie de ataque.
- ***Copia de seguridad:*** haga una copia de seguridad periódica de la configuración y los datos de su servidor DHCP para que pueda restaurar rápidamente su configuración en caso de un ataque o falla del sistema.

- ***Respuesta a incidentes.*** Desarrolle un plan de respuesta a incidentes que incluya acciones a tomar en caso de un ataque DHCP. Esto ayudará a minimizar el tiempo de inactividad y hará que su red vuelva a la normalidad lo más rápido posible.

Recuerde que la ciberseguridad es un proceso continuo y en evolución. Es importante mantenerse actualizado con las últimas amenazas de ciberseguridad y las mejores prácticas, y ajustar sus medidas de seguridad en consecuencia.

Consecuencias:

Un ataque DHCP (Protocolo de configuración dinámica de host) puede tener una serie de consecuencias negativas. Éstos son algunos de ellos:

- ***Falta de direcciones IP:*** en el caso de un ataque DHCP, un atacante puede inundar el servidor DHCP con solicitudes de asignación de direcciones IP incorrectas o no válidas, lo que puede provocar el agotamiento de la disponibilidad del grupo de direcciones IP. Como resultado, es posible que los dispositivos legítimos no tengan una dirección IP válida para conectarse a la red, lo que resulta en la pérdida de conexión y la interrupción del servicio.
- ***Denegación de servicio (DoS):*** los ataques de DHCP también pueden causar ataques de denegación de servicio (DoS) al sobrecargar el servidor DHCP con una gran cantidad de solicitudes de asignación de direcciones IP, lo que puede hacer que el servidor no esté disponible o bloqueado, evitando actividades legítimas. Dispositivo antes de obtener una dirección IP y conectarse a la red.
- ***Asigne direcciones IP maliciosas***. Un atacante puede configurar un servidor DHCP malicioso para asignar direcciones IP falsificadas o maliciosas a los dispositivos de la red.

Esto podría permitirles interceptar o redirigir el tráfico de red legítimo, realizar ataques de intermediarios, espiar o robar datos.

- ***Reconfiguración de la red:*** un atacante puede usar un ataque DHCP para reconfigurar la red de los dispositivos afectados. Esto puede incluir cambios en las rutas de la red, servidores DNS o ajustes de configuración de la red, que pueden interferir con la conectividad de la red y afectar el funcionamiento normal del dispositivo.
- ***Divulgación de Información Confidencial.*** En algunos casos, los ataques de DHCP pueden revelar información confidencial, como direcciones IP internas, nombres de host o información de configuración de la red que los atacantes pueden usar para planificar ataques, ataques posteriores o violaciones de la seguridad de la red.
- ***La reputación está dañada.*** Si una organización se ve afectada por un ataque DHCP exitoso, puede tener un impacto negativo en la reputación de esa organización. La pérdida de servicio, la interrupción de la red o la divulgación de datos confidenciales pueden afectar la confianza de los clientes, socios comerciales y otras partes interesadas en la seguridad de una organización.

Como resultado, los ataques de DHCP pueden tener consecuencias graves, que van desde interrupciones del servicio y pérdida de conexiones hasta la divulgación de información confidencial y daños a la reputación de una organización. Por lo tanto, es extremadamente importante implementar las medidas de seguridad adecuadas, como la configuración segura de DHCP, la segmentación de la red, el monitoreo continuo y las actualizaciones de seguridad para protegerse y mitigar los ataques DHCP latentes.

¿Cómo mitigar un ataque DHCP?

Para mitigar un ataque de inanición de DHCP en los conmutadores de Cisco, se puede establecer una función de seguridad denominada seguridad de puertos, cuya función es vincular las direcciones MAC de los clientes conocidas a cada puerto del conmutador para que la red no pueda filtrar a los atacantes. El conmutador mantendrá una lista de direcciones MAC permitidas para cada puerto y aplicará las comprobaciones necesarias en caso de incumplimiento de las restricciones de seguridad al conectar un host desconocido, deshabilitar el puerto o simplemente evitar que ingrese a la red. (Auz Cadena, 2019)

¿Cómo mitigar un ataque DHCP?

Para mitigar el ataque DHCP starvation en los Switch cisco se puede configurar una característica de seguridad llamada port-security, su función es asociar las direcciones MAC de los clientes conocidos a cada puerto del switch con el fin de que no se puedan filtrar clientes maliciosos a la red.

El switch guardara la lista de direcciones MAC permitidas en cada puerto y se aplicará el control necesario en caso de que se viole la restricción de seguridad al conectarse un host no conocido, ya sea desactivando el puerto o simplemente no permitiendo que ingrese en la red. (Auz Cadena, 2019)

TCP Session Hijacking:

Este es el caso cuando un "Hacker" secuestra una sesión TCP existente que se ha establecido entre dos partes. En la mayoría de las sesiones TCP, la autenticación ocurre al comienzo de la sesión, que es cuando el hacker realiza este ataque. (Ramiro, 2018)

El robo o secuestro es un intento de apoderarse de un componente específico del entorno de Internet de manera no autorizada. Además del secuestro de URL, existen nombres de dominio, DNS, navegadores, TCP, secuestro de sesiones y más.

Hackear el navegador: El secuestro del navegador generalmente lo realiza un programa muy pequeño en su computadora, invisible debido a su tamaño. Este programa anula las funciones estándar de los navegadores de Internet sin el consentimiento o conocimiento del usuario. Eliminar este tipo de software suele requerir mucho esfuerzo.

Cómo podría funcionar:

La página de inicio del navegador afectado se sobrescribe. Cuando se inicia el navegador, el usuario es redirigido automáticamente al sitio web del intruso.

- El motor de búsqueda no muestra la clasificación normal, sino que redirige a la página del motor de búsqueda del intruso. Hijacker gana dinero con este sitio a través de la publicidad.
- Cuando intente visitar el sitio web de un vendedor en particular, se le presentará una página que pertenece a un anunciante asociado con el intruso en lugar de usted sin su conocimiento.

Prevención: La instalación de dicho software en una computadora requiere el consentimiento previo del propietario. Esto sucede accidentalmente cuando hace clic en Aceptar en la ventana emergente. Estas ventanas también pueden contener falsas advertencias de seguridad que el usuario intuitivamente quiere desactivar haciendo clic en el botón "Aceptar". Para evitar que este tipo de software se instale en su computadora, siempre debe revisar las ventanas emergentes rápidamente. En caso de duda, nunca haga clic en Aceptar.

Hijacking de Dominios: Cuando se incauta un nombre de dominio, se le quita ilegalmente a su propietario legítimo. Su forma más agresiva es el robo de nombres de dominio. Estos estafadores a menudo obtienen acceso al registro de nombres de dominio a través del robo de identidad. El secuestrador asume la identidad del propietario legítimo y modifica la información de registro para reasignarse el dominio a sí mismo con el fin de robarlo. Algunos servicios de suscripción actúan rápidamente cuando se detecta este tipo de fraude. Sin embargo, también hay casos en los que las medidas se toman solo cuando se usan legalmente. En algunos casos, el secuestrador puede retener el control del dominio. En la mayoría de los casos, las víctimas no tienen la voluntad o los recursos financieros para emprender procesos judiciales largos y arduos para recuperar sus bienes. El hecho de que los secuestradores estuvieran operando en otro país también fue un elemento disuasorio. Mientras tanto, el atacante tiene control total sobre el dominio y puede manipular libremente el contenido o redirigir el código de estado HTTP.

Prevención: Muchos registros de dominio tienen la capacidad de trabajar con códigos de autenticación especiales que solo conoce el propietario del dominio. Esto proporciona protección contra el acceso no autorizado. (Ryte Wiki, s.f.)

Suplantación De Identidad (Phishing)

El phishing es la práctica de enviar mensajes fraudulentos que parecen provenir de fuentes confiables, generalmente por correo electrónico. El objetivo es robar datos confidenciales como credenciales de inicio de sesión y detalles de tarjetas de crédito, o instalar malware en la computadora de la víctima. El phishing es una amenaza cibernética cada vez más común. (cisco, s.f.)

Robo de identidad, también conocido como phishing, en el contexto de la ciberseguridad.

El phishing es una técnica utilizada por los ciberdelincuentes para obtener información confidencial, como contraseñas, números de tarjetas de crédito, información bancaria u otra información personal confidencial. Esto generalmente se hace a través de correos electrónicos, mensajes de texto, llamadas telefónicas o publicaciones en las redes sociales que parecen legítimas, pero en realidad son falsas y provienen de una empresa, organización o entidad legal de confianza.

El objetivo del phishing es obtener acceso no autorizado a una cuenta o robar información valiosa. Los atacantes a menudo usan tácticas de ingeniería social para engañar a las personas para que revelen información confidencial sin saberlo. Por ejemplo, pueden enviar un correo electrónico falso que pretenda ser de un banco legítimo, solicitando al destinatario información bancaria para solucionar el problema de la cuenta falsa. También pueden crear sitios web falsos que imitan a una empresa u organización legítima para engañar a los usuarios para que ingresen su información personal.

Es importante tener cuidado al abrir correos electrónicos, mensajes de texto o publicaciones en redes sociales, especialmente si solicitan información confidencial o parecen sospechosos. Estos son algunos consejos para protegerse de las estafas:

- No haga clic en enlaces ni descargue archivos adjuntos en correos electrónicos, mensajes de texto o mensajes de redes sociales de remitentes desconocidos o sospechosos.
- Verifique el correo electrónico o los mensajes de texto antes de proporcionar información confidencial. Puede hacerlo poniéndose en contacto con la empresa u organización directamente a través de su sitio web oficial o número de teléfono.

- No proporcione información personal o financiera a través de sitios web inseguros o dudosos. Asegúrese de que el sitio esté bloqueado o comience con "https://" para asegurarse de que el sitio sea seguro.
- Mantenga sus dispositivos y software actualizados con los últimos parches de seguridad y use un software antivirus confiable.
- Tenga cuidado con los mensajes urgentes o amenazantes, ya que los atacantes pueden intentar que actúe impulsivamente sin verificar la autenticidad de la solicitud.

Recuerde que las empresas legítimas nunca le pedirán información confidencial a través de correos electrónicos, mensajes de texto o llamadas telefónicas no solicitadas. Debe mantenerse alerta y proteger su información personal en línea para evitar el phishing y otros tipos de ataques cibernéticos.

¿Cuáles son los síntomas?:

Algunos signos comunes de una estafa son:

- ***Correo electrónico o mensaje no solicitado.*** Los atacantes a menudo envían correos electrónicos o mensajes de texto que parecen provenir de compañías legítimas como bancos, redes sociales o servicios en línea que no esperarías. Estos mensajes pueden contener información urgente o amenazante que lo obligue a actuar rápidamente, como hacer clic en un enlace o proporcionar información personal.
- ***URL sospechosas.*** Los enlaces en los correos electrónicos de phishing a menudo conducen a sitios web falsos que parecen legítimos. Sin embargo, si observa detenidamente la URL del enlace, es posible que observe errores tipográficos, otros dominios o caracteres sospechosos que indiquen que el sitio no es genuino.

- ***Solicitar Información Confidencial.*** Los correos electrónicos de phishing a menudo solicitan información confidencial, como contraseñas, números de tarjetas de crédito, números de seguro social u otra información personal confidencial. Cabe señalar que las empresas legítimas nunca solicitan información confidencial a través de correos electrónicos o mensajes de texto no solicitados.
- ***Mensajes de miedo o urgentes.*** Los atacantes a menudo usan el miedo o tácticas impulsivas para que usted actúe apresuradamente. Por ejemplo, pueden amenazar con cerrar su cuenta, suspender el acceso o tomar otras medidas drásticas si no proporciona la información solicitada de inmediato.
- ***Gramática y ortografías incorrectas.*** Los correos electrónicos de phishing a menudo contienen errores gramaticales o de ortografía. Esto podría significar que el mensaje no fue enviado por una empresa legítima, ya que las empresas profesionales suelen revisar y corregir el contenido.
- ***Remitente desconocido o sospechoso.*** Si el remitente del correo electrónico o SMS es desconocido o sospechoso, lo más probable es que sea una señal de phishing. Los atacantes a menudo usan direcciones de correo electrónico falsas o nombres de remitentes que parecen reales, pero no lo son.
- ***Sin personalización.*** Los correos electrónicos de phishing generalmente no incluyen información personalizada como su nombre o información de cuenta. En cambio, te hablan en un idioma común.

Cabe señalar que los ciberdelincuentes son cada vez más sofisticados en sus métodos de phishing, por lo que es importante mantenerse alerta y no confiar ciegamente en los mensajes o correos electrónicos que recibe. Siempre valide los mensajes y enlaces antes de proporcionar

cualquier información confidencial, y mantenga sus dispositivos y software de seguridad actualizados para protegerlo de posibles ataques de phishing.

¿Cómo se identifica?:

Algunas formas de detectar estafas:

- ***Verifique la URL.*** Una URL sospechosa puede indicar phishing. Los ciberdelincuentes suelen utilizar direcciones URL similares a las de los sitios web legítimos, pero con algunas ligeras diferencias, como caracteres adicionales o alternativos, para engañar a la gente. Por eso es importante verificar dos veces las URL de su sitio web antes de proporcionar información confidencial.
- ***Solicitar Información Confidencial.*** Los correos electrónicos de phishing a menudo solicitan información confidencial, como contraseñas, números de tarjetas de crédito o números de seguro social. Tenga cuidado si se le solicita que proporcione este tipo de información por correo electrónico, mensaje de texto u otras formas de comunicación en línea, especialmente si no espera recibir dicha solicitud.
- ***Errores gramaticales y ortográficos.*** Los correos electrónicos de phishing a menudo contienen errores gramaticales y ortográficos. Los ciberdelincuentes suelen cometer errores de redacción porque estas notificaciones se generan rápidamente y no prestan atención al contenido. Si nota errores ortográficos o gramaticales en un mensaje o en un sitio web, podría tratarse de una estafa.
- ***Amenaza o urgencia:*** los correos electrónicos de phishing a menudo incluyen amenazas o solicitudes urgentes para alentar a las personas a actuar rápidamente sin pensar. Pueden usar frases como "su cuenta ha sido comprometida" o "su cuenta se cerrará si no toma

medidas inmediatas". Es importante estar atento a este tipo de mensajes y comprobar la información antes de realizar cualquier acción.

- ***Enlaces o archivos adjuntos sospechosos.*** Los correos electrónicos de phishing a menudo contienen enlaces o archivos adjuntos sospechosos que pueden contener malware o conducir a sitios web de phishing. Es importante no hacer clic en enlaces ni descargar archivos adjuntos sospechosos en correos electrónicos o mensajes de texto no solicitados. 6. Sin personalización. Los correos electrónicos de phishing a menudo se envían de forma masiva y no están personalizados. Si recibe un correo electrónico o mensaje de texto que no contiene su nombre u otra información personal, podría generar sospechas.
- ***Sin datos de contacto***. Los sitios de confianza suelen contener información de contacto, como direcciones físicas y números de teléfono de contacto. La falta de información de contacto en un sitio web o en un correo electrónico o simplemente en una dirección de correo electrónico puede indicar phishing.

Cabe señalar que los ciberdelincuentes utilizan constantemente nuevos métodos y tácticas para llevar a cabo ataques de phishing, por lo que debe estar atento y tener cuidado al compartir información confidencial en línea. Siempre debe verificar la autenticidad de los sitios web y los mensajes antes de proporcionar información confidencial. Si tiene alguna duda sobre la confiabilidad de un mensaje o sitio web, lo mejor es comunicarse directamente con la empresa u organización a través de los canales de comunicación oficiales para confirmar.

Planificación

¿Cómo combatir el ataque?

Estos son algunos pasos que puede seguir para combatir el phishing:

- ***Tenga cuidado:*** tenga cuidado con los correos electrónicos o mensajes de texto sospechosos que solicitan información confidencial. Compruebe siempre la autenticidad de un mensaje antes de responder o hacer clic en un enlace.
- ***Comprueba la autenticidad de los mensajes:*** comprueba la dirección de correo electrónico o el número de teléfono del remitente para asegurarte de que son reales. Algunos estafadores usan direcciones de correo electrónico que son muy similares a las de empresas legítimas, pero con una ligera diferencia en la ortografía o el dominio.
- ***Utilice software de seguridad.*** Actualice y habilite el software antivirus y de malware en su dispositivo. Estos programas pueden detectar y bloquear sitios web y archivos maliciosos.
- ***No haga clic en enlaces sospechosos***. Si recibe un correo electrónico sospechoso, no haga clic en ningún enlace del mensaje. En su lugar, visite el sitio web de la empresa directamente en su navegador para buscar información importante.
- ***Utilice contraseñas seguras***. Utilice contraseñas largas y complejas que contengan letras, números y caracteres especiales. Nunca use la misma contraseña para diferentes cuentas.
- ***Activa la autenticación de dos factores.*** La autenticación de dos factores brinda una capa adicional de seguridad al requerir un segundo factor de autenticación, como un código de verificación, además de su contraseña.
- ***Manténgase informado:*** mantenga su software y sistema operativo actualizados con las últimas versiones y parches de seguridad. Esto puede ayudar a cerrar posibles vulnerabilidades en su sistema.

Estos son algunos pasos que puede seguir para combatir el phishing. Tenga en cuenta que siempre debe estar al tanto de las posibles amenazas en Internet.

Consecuencias:

Las consecuencias del robo de identidad pueden ser graves y variadas, entre ellas:

- ***Robo de identidad***. La información personal obtenida a través del phishing puede usarse para robar la identidad de una persona. Esto puede dar lugar a pagos fraudulentos con tarjetas de crédito, préstamos y otros tipos de fraude financiero.
- ***Pérdida de información personal y financiera.*** Si los ciberdelincuentes obtienen acceso a la información personal y financiera de una persona, pueden usar esa información con fines maliciosos, como el robo de identidad o la extorsión.
- ***Pérdida de dinero***: si una persona cae en una estafa y proporciona información financiera confidencial, como detalles de cuentas bancarias o números de tarjetas de crédito, esa información puede ser robada y utilizada para otros pagos fraudulentos.
- ***Daño a la reputación***: si un ataque de phishing tiene éxito y la información personal de alguien se ve comprometida, su reputación, tanto personal como profesional, puede verse afectada negativamente.
- ***Daño a la empresa***: si un empleado de la empresa es víctima de fraude y proporciona información confidencial, puede tener consecuencias negativas para la empresa, incluida la pérdida de información valiosa o daños a la reputación de la empresa.
- ***Pérdida de tiempo y recursos***: si alguien es víctima de una estafa, puede llevar mucho tiempo recuperar su identidad y proteger su información personal y financiera, lo que puede ser un proceso muy costoso y estresante.

Tales estafas pueden tener consecuencias graves tanto para las personas como para las empresas, por lo que es importante tomar medidas para protegerse de las estafas, como la educación y la concientización, el uso de herramientas de seguridad en línea y el uso de contraseñas seguras y actualizadas periódicamente.

Ataques De Día Cero

El ataque no pudo afectar después de anunciar la sensibilidad a la red, pero antes de realizar un parche o solución. Los atacantes dijeron que la sensibilidad se reveló en esta ventana de tiempo. La detección de amenazas de día cero requiere una atención constante. (cisco, s.f.)

Los ataques de día cero, son un tipo de ataque cibernético que explota una vulnerabilidad en un sistema o software antes de que el desarrollador o proveedor de seguridad lo reconozca. Estas vulnerabilidades no son conocidas por el público y, por lo tanto, no han sido reparadas o parcheadas, lo que las hace particularmente peligrosas. Los ataques de día cero pueden ser realizados por ciberdelincuentes, piratas informáticos éticos, agencias gubernamentales u otros actores malintencionados. Los atacantes aprovechan estas vulnerabilidades para obtener acceso no autorizado a los sistemas informáticos, robar información confidencial, realizar actos de sabotaje, chantajear a las víctimas y otras actividades ilegales. Una de las características de los ataques de día cero es que son difíciles de detectar porque no hay un parche de seguridad para protegerse contra ellos. Además, los atacantes suelen mantener en secreto la existencia de estas vulnerabilidades para explotarlas durante el mayor tiempo posible y causar el mayor daño posible. Para protegerse de los ataques el día 0, es importante seguir las buenas prácticas de ciberseguridad, por ejemplo, para mantener una actividad sospechosa o extraordinaria en sistemas y redes.

Además, lo importante es que los programadores y proveedores de software realizan pruebas de seguridad estrictas en sus productos antes de lanzarlos para la sociedad y responder de manera rápida y efectiva al espacio que se detecta, proporciona innovación de reparación y seguridad para sus usuarios. En resumen, los ataques de día cero son vulnerabilidades desconocidas que los atacantes explotan antes de que se apliquen parches o parches. Son peligrosos y difíciles de detectar, por lo que es importante seguir las mejores prácticas de ciberseguridad y adoptar un enfoque proactivo para protegerse contra ellos.

¿Cuáles son los síntomas?

Síntomas que pueden indicar la presencia de un ataque de día cero:

- ***Comportamiento anormal del sistema***. Si nota que su sistema o red se comporta de manera anormal, como lentitud, fallas frecuentes, reinicios inesperados o errores inusuales, podría ser una señal de un ataque cero.
- ***Actividad de red sospechosa***. Si detecta actividad de red sospechosa, como tráfico de red inusual o patrones de tráfico inesperados, podría tratarse de un ataque de día cero. Por ejemplo, la transferencia de grandes cantidades de datos a ubicaciones desconocidas o no autorizadas podría ser una señal de un ataque en curso.
- ***Cambios no autorizados en archivos o configuraciones***. Si observa cambios no autorizados en los archivos, la configuración del sistema o el registro, podría significar que alguien ha obtenido acceso no autorizado a su sistema a través de un ataque de día cero.
- ***Mensajes sospechosos:*** si ve mensajes sospechosos, como correos electrónicos o mensajes inusuales que parecen provenir de fuentes desconocidas o solicitan información

confidencial, esto podría ser un día de cero ataques, especialmente si se solicita información confidencial o se intenta obtener acceso a la cuenta. o sistemas.

- ***Advertencia de seguridad***. Si recibe advertencias de seguridad de herramientas de seguridad como antivirus o firewalls de que se ha detectado actividad sospechosa o malware desconocido, puede ser víctima de un ataque de día cero.

Es importante tener en cuenta que estos síntomas también pueden ser causados por otras causas, y tener uno o más de estos síntomas no significa necesariamente que esté siendo afectado por el Día Cero. Sin embargo, si sospecha que puede ser víctima de un ataque de día cero, es muy importante que tome medidas inmediatas de reducción de riesgos, como notificar al equipo de seguridad su seguridad, aplicar parches o actualizaciones de software y revisar y fortalecer sus políticas de privacidad. En realidad.

¿Cómo se identifica?

- ***Analice el tráfico de la red***. Los profesionales de la ciberseguridad pueden monitorear el tráfico de la red en busca de patrones inusuales o sospechosos que podrían indicar un ataque de día cero. Esto puede incluir identificar el tráfico de direcciones IP sospechosas o escanear paquetes de red en busca de comportamientos inusuales.
- ***Análisis de registro del sistema***. Los registros del sistema, como los registros de eventos del sistema operativo, pueden contener información sobre actividades sospechosas que podrían indicar un ataque de día cero. Los profesionales de la ciberseguridad pueden analizar estos registros en busca de eventos inusuales, intentos de acceso no autorizado o cambios en la configuración del sistema.

- ***Supervisar el comportamiento de los usuarios.*** Supervisar el comportamiento de los usuarios puede ser una forma eficaz de detectar ataques de día cero. Los profesionales de la ciberseguridad pueden usar soluciones de análisis de comportamiento para detectar cambios en el comportamiento común de los usuarios, como intentos de acceder a recursos a los que normalmente no tendrían acceso o cambios en el estilo de navegación.
- ***Investigación de amenazas***: los profesionales de la ciberseguridad pueden realizar una investigación activa de amenazas en la dark web o en foros de piratas informáticos para encontrar información sobre posibles ataques de día cero. Esto podría incluir la identificación de proveedores para la venta de exploits de día cero o la búsqueda de discusiones sobre vulnerabilidades no reveladas en la comunidad de piratas informáticos.
- Pruebas de penetración. Los profesionales de la ciberseguridad también pueden realizar pruebas de penetración o pruebas de vulnerabilidad de sistemas y aplicaciones para identificar posibles vulnerabilidades desconocidas que pueden explotarse en ataques de día cero. Estas pruebas pueden ayudar a identificar y corregir vulnerabilidades antes de que los atacantes las exploten.

Cabe señalar que la detección de ataques de día cero puede ser difícil porque estos ataques son muy sofisticados y están diseñados para evadir la detección. Por lo tanto, para protegerse contra los ataques de día cero, se requiere un equipo de expertos en ciberseguridad altamente calificado y soluciones de seguridad avanzadas.

Planificación

¿Cómo combatir el ataque?

- ***Mantenga su sistema actualizado***. Es esencial mantener su sistema operativo, software y aplicaciones actualizados con las últimas actualizaciones y parches de seguridad. Los fabricantes y desarrolladores a menudo lanzan parches para abordar vulnerabilidades conocidas, incluido el día cero. Actualice su sistema regularmente para asegurarse de tener la seguridad más reciente.

- ***Implemente seguridad en capas***: no confíe en una solución de seguridad. En su lugar, implemente un enfoque en capas que incluya firewalls, antivirus, antimalware, control de acceso, detección de intrusos y otras soluciones de seguridad. Esto ayudará a garantizar que si falla una capa de seguridad, las otras capas pueden brindar protección adicional.

- ***Realice análisis de vulnerabilidades y pruebas de penetración***. Realice análisis de vulnerabilidades y pruebas de penetración en sus sistemas y aplicaciones para identificar posibles vulnerabilidades, incluidas las vulnerabilidades de día cero. Esto le permitirá tomar precauciones para proteger su sistema y eliminar posibles brechas de seguridad.

- ***Capacite a su personal***. La conciencia de seguridad es crucial para combatir los ataques de día cero. Capacite a sus empleados sobre las mejores prácticas de seguridad, como no abrir correos electrónicos o enlaces sospechosos, no descargar archivos adjuntos no deseados y no hacer clic en enlaces desconocidos. Además, asegúrese de que sus empleados usen contraseñas seguras y cámbielas con frecuencia.

- ***Supervisar y registrar actividades sospechosas***. Implemente sistemas de monitoreo de seguridad que registren y analicen su sistema y las actividades de la red en busca

de actividades sospechosas. Esto detectará posibles ataques de día cero o anomalías en el comportamiento del sistema y reaccionará rápidamente ante posibles amenazas.

- ***Mantenga sus copias de seguridad actualizadas***: Realice copias de seguridad de sus datos y sistemas con regularidad y asegúrese de que estén guardados en un lugar seguro. Las copias de seguridad pueden ser útiles en caso de un ataque de día cero exitoso porque permiten restaurar los sistemas a un estado seguro antes del ataque.
- ***Colabore con la comunidad de seguridad***: manténgase actualizado con las últimas amenazas de seguridad e interactúe con la comunidad de seguridad, incluidos proveedores, desarrolladores, organizaciones de seguridad y otros profesionales de ciberseguridad. Compartir información y trabajar juntos puede ayudar a detectar y mitigar los ataques de día cero.

Consecuencias:

Algunas de las principales consecuencias de los ataques de día cero son:

- ***Explotar vulnerabilidades desconocidas.*** Los ataques de día cero explotan vulnerabilidades de software desconocidas para el fabricante y, por lo tanto, sin parches. Esto permite que un atacante ingrese al sistema o aplicación sin ser detectado y cause daños ilimitados.
- ***Violación de la privacidad:*** los atacantes pueden obtener acceso a datos confidenciales, como información personal, detalles de la empresa o secretos comerciales, lo que puede comprometer significativamente la seguridad y la confidencialidad de la información. Esto puede provocar fugas de datos y pérdida de reputación de las empresas afectadas.

- ***Violación de la integridad.*** Los delincuentes pueden cambiar o modificar los datos en el sistema comprometido, lo que puede comprometer la integridad de la información. Esto puede conducir a errores o manipulación de datos, lo que puede afectar significativamente la precisión y confiabilidad de la información.
- ***Acceso al daño.*** Los ataques de día cero pueden provocar interrupciones del servicio y la indisponibilidad del sistema o de la aplicación, lo que puede afectar la disponibilidad de los servicios en línea. Esto puede conducir a pérdidas financieras y de productividad para las organizaciones afectadas.
- ***Costes económicos.*** La mitigación de los ataques de día cero puede ser costosa y requiere que las vulnerabilidades se identifiquen y resuelvan rápidamente antes de que los atacantes puedan causar más daños. Esto significa esfuerzos humanos y técnicos adicionales, así como posibles pérdidas económicas por interrupciones del servicio o pérdida de clientes.
- ***Afecta la confianza y la reputación.*** Las organizaciones afectadas por ataques de día cero pueden perder la confianza de sus clientes, socios comerciales y el público en general. Esto puede tener un efecto duradero en la reputación de la empresa y afectar su capacidad para hacer negocios en el futuro.
- ***Implicaciones legales y regulatorias.*** Según la naturaleza de los datos en riesgo y las leyes y regulaciones aplicables, las organizaciones afectadas por ataques de día cero podrían enfrentar consecuencias legales y regulatorias. Esto puede incluir multas, sanciones y responsabilidades, que pueden sumarse a los costos asociados con el ataque.

Como tal, los ataques de día cero pueden tener implicaciones significativas para la seguridad, la integridad, la disponibilidad, los costos económicos, la confianza y la reputación, así como impactos legales y normativos. Es importante que las organizaciones implementen

medidas rigurosas de ciberseguridad, como parches de seguridad regulares, para protegerse contra este tipo de ataques y minimizar su impacto en caso de que ocurran.

Accesibilidad al contenido web para todos

Últimamente en nuestro país, ha evolucionado la tecnología en cuanto a los diversos planteamientos, comerciales, educativos y sociales, por lo que es indispensable seguir trabajando para que exista una igualdad de oportunidades en cualquier tipo de empresa, lo cual es indispensable contar con dos aspectos:

- Una pequeña y mediana empresa, que cuente con la diversidad de medios los cuales suplan las necesidades de los que en ella trabajan.
- Una pequeña y mediana empresa donde los medios se encuentren disponibles para las necesidades de los receptores de la información.
- Dado a la gran capacidad de acceder a los altos niveles de información que se encuentran en la red de manera masiva e indiscriminada, es posible que existan problemas mayores, sobre todo, en las pymes que no han implementado medidas para el buen uso del recurso tecnológico.

Se conoce que cerca de un 97% del tejido empresarial está conformado por pequeñas y medianas empresas (pymes), las mismas no pueden realizar inversiones en cuanto a ciberseguridad, lo cual tienen como consecuencia un sinnúmero de amenazas solo por estar conectadas a internet.

Muchas de estas empresas se les dificulta su trabajo productivo, dado a las pérdidas millonarias que generan los delitos informáticos para ellas.

Durante el año 2021, el número de personas que fueron víctimas de delitos cibernéticos aumentó en un 17% en comparación con el año 2020. Conforme a las cifras expuestas por el Centro Cibernético Policial, se registraron 33.465 delitos cibernéticos. Además de los casos de delito, el Centro Cibernético Policial informó que 18.578 URL fueron bloqueadas en 2021 por contenidos maliciosos.

Dentro de los problemas de seguridad más recurrentes y graves, desde el Pishing, ingeniería social y secuestro de datos encontramos:

- ***Pishing:*** Es un mecanismo de suplantación de identidad, haciendo que el usuario comparta contraseñas, número de tarjetas de crédito, haciéndose pasar por una institución confiable en un correo electrónico o llamada. (Malwarebytes)
- ***Ingenieria Social:*** Es una técnica que emplean los ciberdelincuentes para generar confianza en el usuario y lograr conseguir bajo manipulación y engaño algo, como claves privadas o comprar en sitios web fraudulentos. (Incibe)
- ***Secuestro De Datos:*** Muchas empresas ya han tenido que vivir lo rápido que se agrava una situación de emergencia con ordenadores cifrados y ransomware, y saben que lo primero es responder adecuadamente. (Avetest, 2020).

Tendencias que repercuten en la seguridad en redes.

Existen muchas tendencias que incrementan la necesidad de redes seguras, que son las siguientes:

- Incremento de requisitos de ancho de banda
- Acceso inalámbrico
- Salvaguardar la privacidad

- Situaciones legales

Métodos de protección.

En las empresas, las políticas de protección son el primer paso para estar en el ambiente de seguridad, pues propicia el poder detener un posible ataque antes de que suceda.

- ***Sistemas de detección de intrusos:*** Analiza y busca en los sistemas, eventos o acciones que puedan ser sospechosos, con respecto a la información.
- ***Sistemas direccionados a conexión de red:*** Herramientas como lo Wrappers y Firewall, permiten revisar si en las redes hay acciones no permitidas, orientando e informando a los administradores de la red, todo lo que está sucediendo, para que se hagan las gestiones y correctivos necesarios.
- ***Sistemas de protección a la privacidad de la información:*** Existen varias herramientas que utilizan criptografía para salvaguardar la información de tal manera, que solo pueda ser vista por quien tenga autorización para verla.

Beneficios de la ciberseguridad

Permite trabajar a las empresas, bajo un esquema confiable, como lo son:

- Mayor productividad
- Mejores relaciones laborales
- Compromiso con la empresa
- Tranquilidad empresarial

Objetivos de la seguridad en redes

Existen tres pilares fundamentales en cuanto a la seguridad en las redes:

- La confidencialidad: Corresponde a la protección de los datos ante una divulgación no permitida a terceras partes o personas.
- La transferencia de información confidencial, debe realizarse mediante un método seguro, para así, evitar cualquier acceso no permitido.
- La integridad: Se refiere a la certeza de que los datos no son modificados o destruidos sin autorización.
- La disponibilidad: Es definida como el funcionamiento continúo de los sistemas, teniendo presente los niveles de tiempo de inactividad y disponibilidad.
- El acceso transparente y eficaz a la red, se logra teniendo en cuenta puntos clave como son: Facilidad de uso, conectividad, manejabilidad, rendimiento y disponibilidad.
- Incidencia de las ISO 27001, 31000 y 27032 en informática, frente a los ataques más comunes en la red LAN.

La importancia de la ISO 27001 sobre seguridad y privacidad de la información:

La ISO 27001, como norma internacional, que garantiza y permite certificar la confiabilidad y seguridad a nivel de procesos y disponibilidad de la información, busca que las organizaciones a través de un estándar como indica la ISO, puedan evaluar los riesgos y aplicar los controles necesarios para su eliminación o mitigación.

- La ISO 27001 para poder implementar su norma debe escoger un SGSI de acuerdo con las políticas y procesos que rigen la empresa u organización que permitan identificar los riesgos y vulnerabilidades, los problemas pueden ser tanto internos como externos. Para

poder llevar cabo la aplicación de la norma, es necesario seguir los siguientes pasos: planificar, hacer, verificar y actuar.

Lo primero a tener en cuenta al momento de aplicar la ISO 27001 para la mitigación de los incidentes de acuerdo a los ataques más comunes de la red LAN, se debe tener en cuenta el contexto de la organización, según el apartado 4 de dicha ISO, en el cual se indica lo siguiente:

- Apartado "4.3 Determinación del alcance del sistema de gestión de seguridad de la información" (ISO 27001): Se enfoca en encontrar en las entidades los límites y la aplicabilidad para llegar a tener un alcance, se desarrollará en 3 puntos, los cuales se componen en los siguientes apartados:

- **En el apartado 4.1** (Comprensión de la organización y de su contexto) : De acuerdo a lo antes mencionado, el manejo interno y externo de las organizaciones, como se mencionó anteriormente, depende de su estructura frente a las políticas y proceso; después de tener un amplio conocimiento del funcionamiento, se tendrá en cuanta cual es el propósito, dónde se enfocará en los ataques más comunes a la red LAN que mencionamos dentro de este proyecto, es la mitigación de cada uno de los incidentes que se puedan presentar por cada uno de los ataques, donde su fuente de origen principal se verá reflejado a través de la Red LAN.

Una vez comprendido lo anterior, los aspectos que afectan dichos incidentes, se vería ocasionado y particionado por falta de capacitación del personal, por no destinar a una persona en específico para el uso y tratamiento de la información, por no brindar capacitación constante de las buenas prácticas acerca de la manipulación de los datos y por no usar todos los medios de protección para la integridad de los datos.

- **En el apartado 4.2** (Comprensión de las necesidades y expectativas de las partes interesada): De acuerdo a la actividad económica de la empresa u organización, las partes

interesadas por lo general pueden ser: proveedores, clientes, usuarios, etc. Los requisitos de las partes interesadas, es que siempre que vayan a compartir información confidencial de la empresa o todo lo relacionado con la misma, sea bajo la misma red LAN, que es la que va estar parametrizada bajo los estándares de seguridad de acuerdo a la ISO 27001, esto quiere decir, que siempre se debe evitar que las parte interesadas se conecten a una red wifi pública, ya que esta no cuenta con ningún protocolo de seguridad, evitar tener programas instalados que no hacen parte de las labores y funciones de la empresa o institución y más cuando son programas que no están licenciados o evitar realizar cualquier acción que esté fuera de los estándares de seguridad impuestos por dicha norma.

- Las incidencias de estos ataques a la red LAN dentro de una organización si pueden interferir y afectar cada una de las actividades que tengan entre las empresas o dependencias que estén relacionadas a los equipos de cómputo que están conectadas a la red LAN afectada o atacada. Un caso hipotético puede ser cuando los equipos de cómputo conectados a una red LAN de una empresa, se conectan a un servidor dónde varias organizaciones lo usan para el mismo fin, si un ataque de los mencionados en este proyecto afecta o ataca cualquiera de las redes LAN de estas organizaciones, podría afectar las demás redes LAN que están conectadas a dicho servidor, entonces por eso usamos y tomamos como referencia el software de wazuh que sirve para que todo lo que quiera interferir o introducir dentro de la red LAN sea detectado y nos muestre una alarma, para posteriormente realizar una acción para proteger la RED afectada, por eso hay que instalar los agentes de wazuh en todos los equipos de cómputo que estén conectado a dicha red o estén compartiendo el mismo servidor, para mitigar dichas vulnerabilidades.

Después de hablar de las ISO 27001 en el cual da un aterrizaje frente a la organización cómo está conformado cado uno de los procesos y sus políticas para dar cavidad a las ISO 31000 que refiere acerca de cómo se podrá realizar una buena gestión en el riesgo, especificando el objeto, la normatividad y los términos.

Para una aplicación de gestión de riesgo eficaz, se debería cumplir con los siguientes principios:

- La gestión del riesgo crea y protege el valor
- La gestión del riesgo es una parte integral de todos los procesos de Atento Colombia
- La gestión del riesgo es parte de la toma de decisiones
- La gestión del riesgo aborda explícitamente la incertidumbre
- La gestión del riesgo es sistemática, estructurada y oportuna
- La gestión del riesgo se basa en la mejor información disponible
- La gestión del riesgo está adaptada
- La gestión del riesgo toma en consideración los factores humanos y culturales
- La gestión del riesgo es transparente e inclusiva
- La gestión del riesgo es dinámica, reiterativa y receptiva al cambio
- La gestión del riesgo facilita la mejora continua de Atento Colombia (Arias León & Ibáñez Márquez, 2020)

Con referencia a la normatividad ISO 31000 en el apartado 3.1 riesgo para el desarrollo de los efectos de los objetivos se divide en tres entradas en donde se van a especificar con detalle cómo serían sus efectos:

- ***Entrada 1:*** los riesgos frente a la red LAN, son tanto positivos como negativos; dónde lo negativo se puede ver reflejado en la productividad de los procesos de la organización, en cuanto al robo de información confidencial y extorsión por parte de la misma, entre otras; lo positivo, a medida que se detecta vulnerabilidades y se puedan mitigar, existe una ventaja competitiva frente al crecimiento, fortalecimiento y/o oportunidad relacionada con este riesgo.
- ***Entrada 2:*** Los objetivos para proteger la red LAN de los riesgos se ajustarán en la categoría a corto plazo, dando cavidad a mitigar los riesgos en la compañía y combatirlos de inmediato, para evitar daños en el área local de la red y así no comprometer dicha infraestructura ni los equipos de cómputo que hacer parte de dicha red.
- ***Entrada 3:*** El riesgo se expresa en diferentes terminologías donde se encuentra: fuente de riesgo, eventos potenciales, consecuencias y sus probabilidades que a continuación se dará una clara definición y proceso que se trata en cada uno de ellos:

Apartado 3.4 Fuente de riesgo: Esta puede deberse a una mala estructuración y parametrización de los sistemas de información en especial con los protocolos de seguridad que debe tener la RED LAN de una empresa, ya que por lo general, puede estar vulnerables a los ataques presentes en este artículo; por una configuración, instalación y/o parametrización estándar o básica, cuando en ella se compromete información confidencial de dicha entidad, ya que por la misma red es dónde se transfiere toda la información compartida entre los diferentes dispositivos conectados a la misma red LAN y también los que comparten un mismo servidor. También toca evaluar cada uno de los ámbitos internos y externos que puedan afectar y generar amenazas de pérdidas o impedimentos para alcanzar los objetivos.

Apartado 3.5 Eventos: Nota 1 a la entrada: Las principales ocurrencias se pueden ver sujetas por la inadecuada aplicabilidad y manipulación de los medios informáticos y, por no

tener como se ha mencionado en diferentes puntos de este artículo, una buena parametrización de la misma, que en especialidad sería la protección y de la red LAN y lo mencionado puede ser una causa primordial el cual puede tener como consecuencia la pérdida de información, y retraso en los procesos de la empresa.

Nota 2 a la entrada: La intención principal de este proyecto es poder prever todos los eventos posibles con el software wazuh para mitigar todos los riesgos posibles dentro de la red LAN.

Nota 3 a la entrada: Al ver que cualquier evento puede ser una fuente de riesgo para la integridad de la empresa, es por eso que se estudia y prevé los ataques más comunes a la red LAN, mencionado en este artículo, teniendo en cuenta que pueden haber muchos más.

Apartado 3.6 Consecuencias: Una vez se hace el análisis del evento 3.5 y se obtienen los resultados entramos a analizar las notas de la presente entrada (apartado 3.6).

Nota 1 a la entrada: Las consecuencias se deben analizar y estudiar según su grado de complejidad; dentro de los ataques más comunes a la red LAN, se puede evidenciar que todos son directos ya que hacen un ataque a una red de área local, lo que indica que el atacante necesita algo específico de dicha empresa a la que hace su ataque.

Nota 2 a la entrada: Dentro de las consecuencias cualitativas se puede expresar que pueden ocasionar retrasos en los procesos de la empresa, incumplimiento con los objetivos de la misma, pérdida de credibilidad de dicha empresa, entre otros factores que pueden hacer que la empresa baje su rendimiento y productividad. Por otro lado las consecuencias se pueden medir de forma cuantitativa y esto lo podemos relacionar y llevar con la pérdida de información, económica, de clientes que confiaban en la seguridad e integridad de su información que la empresa les brinda y garantiza.

Nota 3 de la entrada: Si las consecuencias no se tratan de manera oportuna, puede incrementarse de forma incontrolable dicho riesgo, lo cual puede repercutir en un futuro cercano o lejano de acuerdo a la problemática que esta misma presenta, por no intervenir de forma oportunidad ante los incidentes que tiene como consecuencia los ataques que se mencionan en dicho artículo.

Apartado 3.7 Probabilidades:

Nota 1 a la entrada: Acá es muy importante establecer un tiempo de estudio en el cual se pueda recopilar información acerca del tráfico dentro de la red LAN para así analizar cuáles han sido todas las vulnerabilidades presentadas durante este tiempo de análisis, para posteriormente estudiar qué mecanismos y medios se pueden usar y aplicar para la mitigación de las mismas y esto lo ofrece wazuh, el software a implementar.

Después de hablar de las ISO 31000 en el cual da un aterrizaje frente a la gestión de los riesgos para dar cavidad a las ISO 27032 que refiere acerca del plan director de ciberseguridad los cuales marcan las prioridades, los responsables y los recursos que se van a emplear el nivel de la empresa en materia de ciberseguridad.

Esta norma busca planear a través de una dirección de ciberseguridad, las actividades que ayudarán a la mitigación del riesgo, y a llevar a cabo todo lo que conlleva la protección de la infraestructura de la red LAN y los parámetros adecuados para cada uno de los elementos, dispositivos y componentes que se conectan la red LAN y se interconectan entre los dispositivos por medio de la misma.

El plan directivo de la ciberseguridad de acuerdo a la ISO 27032, con respecto al proyecto que se va a abordar, se debe enfocar desde el punto de vista técnico, legal y organizativo, lo que le da un enfoque de carácter macro frente a las incidencias que puedan tener

los ataques más comunes a la red LAN que se mencionan en este proyecto, de acuerdo al tipo de organización y sus políticas de desarrollo informático, que se maneja a través de las diferentes aplicaciones y medios de hardware que se manejan en el desarrollo de la actividad económica.

Es por ello que el software a implementar como herramienta para la medición de ciberseguridad en la infraestructura de la red LAN, es wazuh, que es una herramienta que servirá como detector para las vulnerabilidades e incidentes que se mencionan en el presente trabajo.

Es de anotar que cada una de las ISO que mencionamos con anterioridad, forman parte de un proceso de regularización y de norma, que permite mitigar y ordenar adecuadamente cada uno de los medios que se utilizan dentro de la informática y la red LAN, para mejorar los procesos que se desarrollan dentro de cada organización o empresa, basados en las políticas y proyecciones de las mismas. (Hwang, 2015)

Políticas de Seguridad

Las políticas de seguridad son procedimientos y reglas diseñados para garantizar la confidencialidad, y disponibilidad de los datos de red y los recursos. Es esencial la implementación de unas políticas de seguridad que garanticen la debida protección de una red.

El contar con una adecuada implementación de políticas de seguridad ayuda a proporcionar información valiosa sobre el uso de la red. Esto se desarrolla y logra por medio de la implementación de tecnologías y herramientas de monitoreo y análisis de la red que detecta y registra el tráfico de red, los protocolos utilizados, los dispositivos de red , las aplicaciones y los usuarios que acceden a la red.

Lo anterior, permite que los administradores de red obtengan una comprensión profunda de cómo se está manejando la red y que posibles amenazas pueden enfrentar. Un ejemplo,

cuando se identifica que hay un alto volumen de tráfico de una aplicación en específico, los administradores pueden establecer reglas de firewall, para restringir el acceso a la aplicación y así, evitar o prevenir posibles ataques.

Es importante mencionar que las políticas que se implementan para la protección de una red, depende exclusivamente de las necesidades específicas de la organización y la estructura de red que tengan.

En el caso de pequeñas y medianas empresas (Pymes), es relevante crear políticas de seguridad de la red por las siguientes razones:

- Proteger los datos confidenciales
- Cumplimiento normativo
- Proteger la red y los sistemas
- Prevenir la interrupción del negocio

Dado a lo anterior, desarrollamos unas políticas de seguridad de la red en las pymes, que estará establecida en el "Anexo Instalación de Wazuh" dependiendo de los resultados de los ataques lo cual genera que sea dinámico y están cambiando las políticas, ya que las mismas no suelen contar con ellas, para la protección de ataques a las que pueden estar expuestas.

Sin embargo, mencionamos unas generales que son relevantes en las Pymes, que son las siguientes:

- ***Política de contraseñas seguras:*** Todas las contraseñas que son utilizadas en la red deben cumplir con unos requisitos, como tener una cantidad mínima de dígitos, combinación de letras mayúsculas y minúsculas, caracteres especiales y números. También, la exigencia de que los usuarios cambien periódicamente sus contraseñas.

- ***Política de acceso a la red:*** Los usuarios deben tener acceso a los recursos necesarios para su trabajo y deben estar limitados los permisos para evitar accesos no autorizados.
- ***Política de firewall:*** Establece que deben ser implementadas las reglas de firewall para limitar el tráfico de la red, por medio de ciertos puertos y protocolos. También, bloquear ciertos sitios web.
- ***Política de respaldo de datos:*** Deben realizarse copias de seguridad de los datos importantes y deben ser almacenadas en un lugar fuera de la red principal de manera segura.

Evaluación de Riesgos

Por medio de la evaluación de riesgos se identifican las vulnerabilidades de la red LAN que tiene la entidad, donde se identificaran los potenciales riesgos con el fin de minimizar las causas en los diversos puntos de evaluación.

La valoración de los riesgos generales se realiza en dos pasos:

- Identificación de riesgos
- Análisis de riesgo

Es importante tener en cuenta que para evaluar riesgos hay que considerar la información almacenada y procesada, la tecnología que se implementó, el marco legal y la entidad misma.

El objetivo principal para análisis de riesgos, es establecer una valoración y priorización de los mismos, basándose en la información ofrecida por la etapa de identificación, para clasificar los riesgos y proveer información, para establecer el riesgo en que nivel se encuentra y las acciones a seguir para mitigar.

Matriz de Riesgos General Para Ataques de La Red LAN de Las Pymes

RIESGO	DESCRIPCIÓN	PROBABILIDAD	IMPACTO POTENCIAL	PRIORIDAD
Ataques DDoS	Ataques masivos que pretenden sobrecargar los recursos de la red.	Alta	Alto	Alta
Ataque Man-in-the-Middle	Ataque que permite a un atacante interceptar la comunicación entre dos dispositivos.	Media	Alto	Media
ARP Spoofing	Ataque que implica la manipulación de direcciones MAC y/o IP para interceptar tráfico de red.	Media	Alto	Media
TCP Session Hijacking	Ataque que busca tomar el control de una conexión TCP ya establecida.	Baja	Muy Alto	Alta

Suplantación de Identidad (Phishing)	Ataque que busca engañar a los usuarios para obtener información confidencial.	Media	Alto	Media
Tunelización de DNS	Ataque que busca utilizar túneles DNS para evadir la seguridad de la red.	Baja	Alto	Baja
Tráfico de red o datos	Pérdida, alteración o robo de información que circula en la red.	Alta	Muy Alto	Alta
Ataque de intermediario	Ataque que permite a un atacante interceptar y manipular el tráfico de la red.	Media	Alto	Media
Ataque de denegación de servicio	Ataque que busca sobrecargar los recursos de la red para impedir su uso normal.	Alta	Muy Alto	Alta

TCP Session Hijacking	Ataque que busca tomar el control de una conexión TCP ya establecida.	Baja	Muy Alto	Alta
OS Fingerprinting	Ataque que busca obtener información sobre el sistema operativo utilizado en los dispositivos de la red.	Media	Medio	Media
Ataque de Ransomware	Ataque que cifra los datos de la empresa para pedir un rescate.	Baja	Muy Alto	Alta
Malware	Software malicioso que puede infectar la red y comprometer la seguridad de los datos.	Alta	Medio	Alta
ICMP Tunneling	Ataque que utiliza paquetes ICMP para evadir los firewalls de la red.	Baja	Medio	Media

Ataque de Phishing	Ataque que busca obtener información confidencial de los usuarios de la red, como contraseñas o datos de tarjetas de crédito.	Media	Alto	Media
Escaneo de Puertos	Ataque que busca encontrar los puertos abiertos en los dispositivos de la red.	Alta	Medio	Alta
Ataques DHCP	Ataque que busca obtener información de los dispositivos de la red a través de la asignación DHCP.	Media	Alto	Media
ICMP Tunneling	Ataque que utiliza paquetes ICMP para evadir los firewalls de la red.	Baja	Medio	Media

Inyección de SQL	Ataque que busca aprovechar vulnerabilidades en la implementación de bases de datos.	Baja	Muy Alto	Alta
Ataques de día cero	Ataque que busca aprovechar vulnerabilidades desconocidas o recién descubiertas.	Baja	Muy Alto	Alta

Un ataque DDoS es una red LAN, puede ser catalogado como:

- ***Bajo riesgo:*** Cuando el ataque es de corta duración, de baja intensidad y la red tiene recursos suficientes para absorberlo sin sufrir impactos significativos en la operación de los servicios.
- ***Riesgo medio:*** Cuando el ataque es de mayor duración, intensidad y puede impactar la operación normal de los servicios de la red LAN. La red puede necesitar la intervención de los administradores para mitigar el ataque y restablecer la operación normal de los servicios.
- ***Alto riesgo:*** Cuando el ataque es muy intensivo, de larga duración y la red no tiene suficientes recursos para absorberlo, lo que puede provocar una interrupción significativa de los servicios de la red LAN. La intervención de personas especializadas en seguridad puede ser necesaria para mitigar el ataque y restablecer la operación normal de los servicios.

FACTOR	CONTROL A CONSIDERAR	NIVEL DE RIESGO
Tamaño de la empresa	Tamaño de la empresa – infraestructura de red	Pequeña: 1 Mediana: 2
Tipo de servicio	Servicios ofrecidos a través de la red LAN	Bajo: 1 Medio: 2 Alto: 3
Nivel protección	Nivel de protección de la red LAN contra ataques DDoS	Bajo: 1 Medio: 2 Alto: 3
Impacto económico / financiero	Tipo de impacto financiero de un ataque DDoS	Se define la parte financiera de la entidad
Frecuencia de los ataques	recurrencia en la que se da en la empresa	Poco recurrente:1 Recurrente: 2 Muy recurrente: 3

El nivel de riesgo se mide en una escala de 1 a 3

1: bajo

2: medio

3: Alto

Factores

Tamaño de la empresa

Se clasificara de la siguiente manera:

Pequeña empresa: Menos de 50 trabajadores, **Se clasifica en riesgo bajo (1)**

Mediana empresa: 50 y 250 trabajadores, **Se clasifica en riesgo medio (2)**

Tipo de servicio

Comunicación en tiempo real: Los servicios de comunicación en tiempo real, como la mensajería instantánea y la videoconferencia, también pueden verse afectados por un ataque DDoS. Esto puede dificultar la colaboración y la comunicación entre los miembros del equipo. **Se clasifica en riesgo bajo (1)**

Correo electrónico: El correo electrónico puede verse afectado si los servidores de correo electrónico están en la red LAN afectada por el ataque. Esto puede impedir el envío o la recepción de correos electrónicos, lo que puede ser crítico para algunas organizaciones. **Se clasifica en riesgo medio (2)**

Servicios en línea: Los servicios en línea, como la banca en línea, el comercio electrónico y otros servicios similares que se ejecutan en la red LAN, también pueden verse afectados por un ataque DDoS. Esto puede impedir que los usuarios accedan a estos servicios y afectar gravemente la reputación de la empresa. **Se clasifica en riesgo alto (3)**

Acceso a Internet: El ataque DDoS puede inundar la red LAN con tráfico malicioso, lo que puede hacer que el acceso a Internet sea extremadamente lento o incluso inaccesible. **Se clasifica en riesgo alto (3)**

Nivel de Protección

Existen los siguientes mecanismos de protección:

- Actualizar y mantener los sistemas de seguridad
- Limitar el ancho de banda
- Utilizar servicios de protección DDoS
- Implementar políticas de seguridad
- Monitorear la red
- Tener un plan de contingencia

Si cuenta con 1 solo mecanismo de protección: **Se clasifica en riesgo alto (3)**

Si cuenta con dos o 3 mecanismos de protección: **Se clasifica en nivel (2)**

Si cuenta con los 6 mecanismos de protección: **Se clasifica en nivel (1)**

Frecuencia de los ataques

(Kaspersky Lab, 2020) mediante un informe adujo que las empresas de tamaño pequeño y mediano recibieron en promedio 66 ataques DDoS al día en todo el mundo. Esto significa que, en un término de tres meses (90 días), una PYME podría recibir en promedio más de 5.900 ataques DDoS.

Más de 5.900 ataques DDoS: Se clasifica en riesgo alto (3)

De 3.000 a 5.800 ataques DDos: Se clasifica en riesgo medio (2)

Menos de 3.000 ataques DDos: Se clasifica en riesgo bajo (1)

Matriz de riesgo para ataque de red lan Man-in-the-Middle

RIESGO	DESCRIPCIÓN	PROBABILIDAD	IMPACTO POTENCIAL	PRIORIDAD
Alta de autenticación	Protocolos de red sin autenticación, permitiendo la intercepción de tráfico	Alta	Alto	Alta
Falta de cifrado	Protocolos de red sin cifrado, permitiendo la interceptación y lectura de tráfico	Media	Alto	Media
Falta de actualizaciones	Software y firmware de dispositivos sin actualizaciones, dejando vulnerabilidades conocidas	Media	Medio	Media
Conexiones no autorizadas	Acceso a la red LAN por parte de dispositivos no autorizados	Baja	Bajo	Baja

Uso de redes Wi-Fi públicas	Conexión a redes Wi-Fi públicas inseguras, permitiendo el acceso a la red LAN	Media	Alto	Media
Contraseñas débiles	Contraseñas fáciles de adivinar o sin cambios periódicos	Baja	Medio	Baja
Falta de segmentación de red	Falta de segmentación de la red LAN, permitiendo el acceso no autorizado a dispositivos sensibles	Alta	Alto	Alta

- ***Riesgo:*** Se identifican los diferentes riesgos asociados a un ataque de red LAN Man-in-the-Middle.
- ***Descripción:*** Se relaciona cada uno de los riesgos identificados, para tener una comprensión más clara de los mismos.
- ***Probabilidad:*** Se evalúa la probabilidad de ocurrencia de cada riesgo, es decir, la posibilidad de que suceda.

- ***Impacto potencial:*** Se valora el impacto que tendría cada riesgo si llegara a ocurrir. Se evalúa el impacto tanto en términos económicos, como de pérdida de información o daño reputacional.
- ***Prioridad:*** Se establece la prioridad de cada riesgo, teniendo en cuenta tanto la probabilidad de ocurrencia como el impacto potencial. La prioridad se establece en términos de alta, media o baja.

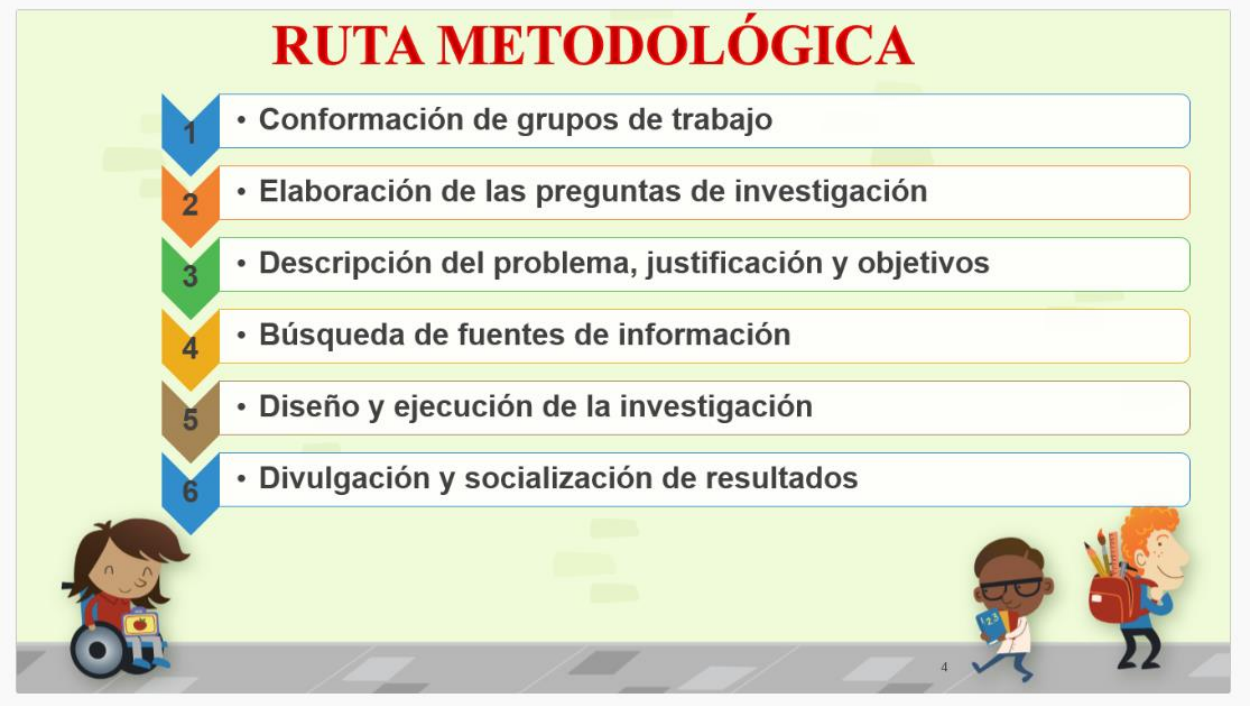
METODOLOGÍA DE INVESTIGACIÓN

Tipo de investigación: Cualitativo en cuanto que produce datos descriptivos, de las palabras propias de las personas o escritas, y además, la conducta observable de los mismos. Investigación de corte transversal que mediante el análisis de datos descriptivos recolectados en la ciudad de Manizales pretende identificar si las empresas medianas y pequeñas utilizaban los recursos para implementación de infraestructura, protección en su red local y si es viable la implementación de una herramienta Open source, que ayude a detectar, analizar y responder a amenazas de seguridad en tiempo real que proporcione una solución integral para la seguridad de los sistemas y aplicaciones, incluyendo el monitoreo de tráfico, detección de intrusiones y análisis de vulnerabilidades y gestión de logs, que tenga como fin el análisis y la gestión de los incidentes mencionados en esta investigación.

Método: Inductivo porque se desarrollan conceptos intelecciones y comprensiones partiendo de datos y de pautas desde los sujetos mismos, es decir, un acercamiento teórico, conceptual y metodológico; determinación de técnicas para la recolección de información; aplicación de técnicas para la recolección de información; selección de información y sistematización y elaboración de informe final y socialización de resultados.

Enfoque: Descriptivo interpretativo (Mayumi Okuda Benavides y Carlos Gómez Restrepo, s.f) establecen en su investigación sobre métodos en investigación cualitativa: Triangulación, que la investigación cualitativa es mucho más compleja debido a que el análisis debe ser mucho más exhaustivo que en una investigación cuantitativa, por ellos la triangulación ha sido el método más fácil para lograr un buen enfoque cualitativo de una investigación ya que esta se enfoca principalmente, en la teoría de la investigación, participantes y fuentes de datos.

Ruta Metodológica



Fuente: http://www.investigonypreguntina.appcotecnova.es/index.php/ruta-metodologica/

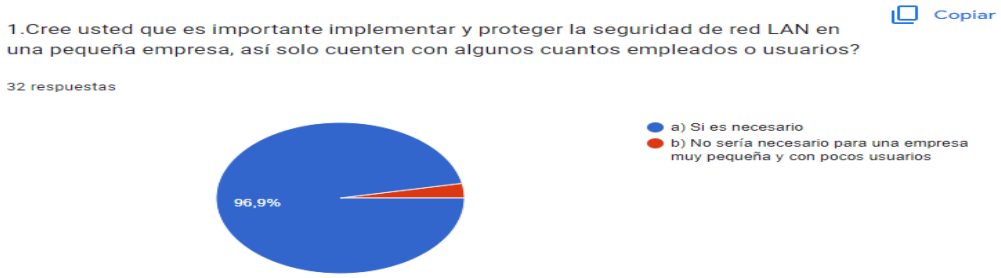
RESULTADOS Y DISCUSIÓN

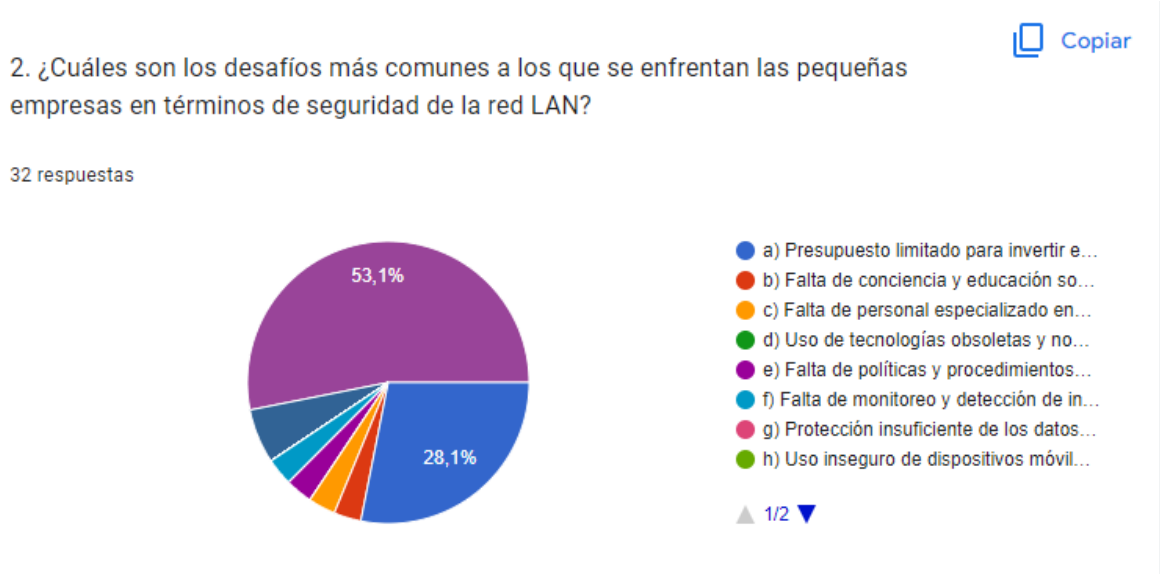
Dentro de este paso se debe analizar profundamente la información obtenida durante el proceso a través de la encuesta aplicada a todo tipo de persona, donde 32 personas que laboran en medianas y pequeñas empresas participaron y de allí se sacará las muestras para el análisis de cada uno de los planteamientos, donde se explicarán a continuación por medio de graficar expresadas porcentualmente.

En este acápite nos enfocamos en lo que expusieron los entrevistados, en razón a que según lo afirmado por la totalidad, manifiestan la importancia de proteger la red Lan de las (pymes), ya que por falta de políticas y procedimientos se logran evidenciar la mayor vulnerabilidad, generando un gran impacto económico la no implementación de los parámetros que protejan la red LAN de estas empresas, generando la necesidad de la implementación y el uso de una herramienta de código abierto que genera protección a la red LAN.

ANÁLISIS DE RESULTADOS:

- Se puede observar que en la actualidad la sociedad ha ido adoptando la importancia de la tecnología en el ahora, en donde se puede ver una participación, donde el 96,9% están de acuerdo que también las entidades pequeñas deberían adoptar y dar más importancia a la protección de la red LAN.

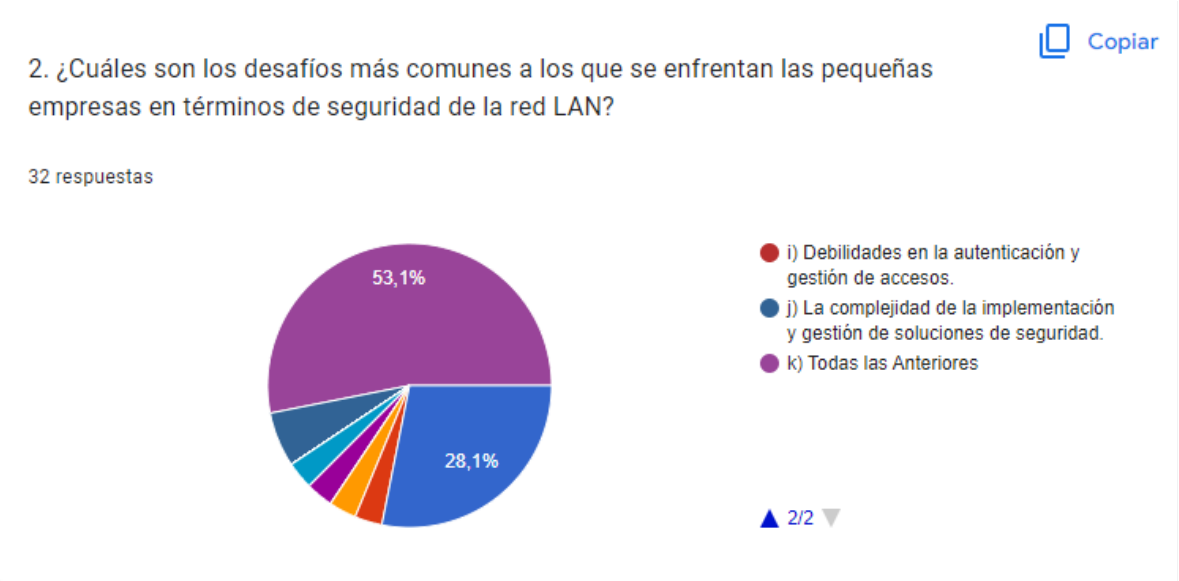




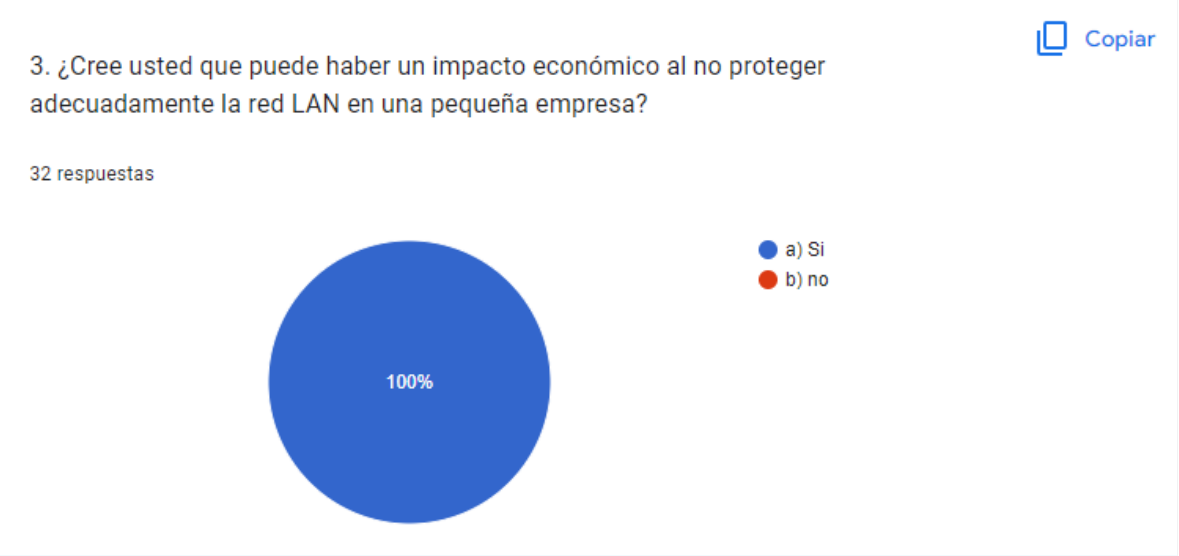
- La respuesta con mayor puntuación fue: Falta de políticas y procedimientos de seguridad adecuados.

Las respuestas más comunes frente a los desafíos más comunes que enfrentan las empresas pymes en términos de seguridad de la red LAN, por parte de los participantes en la presente encuesta fue todas las anteriores que corresponden a: “Debilidades en la autenticación y

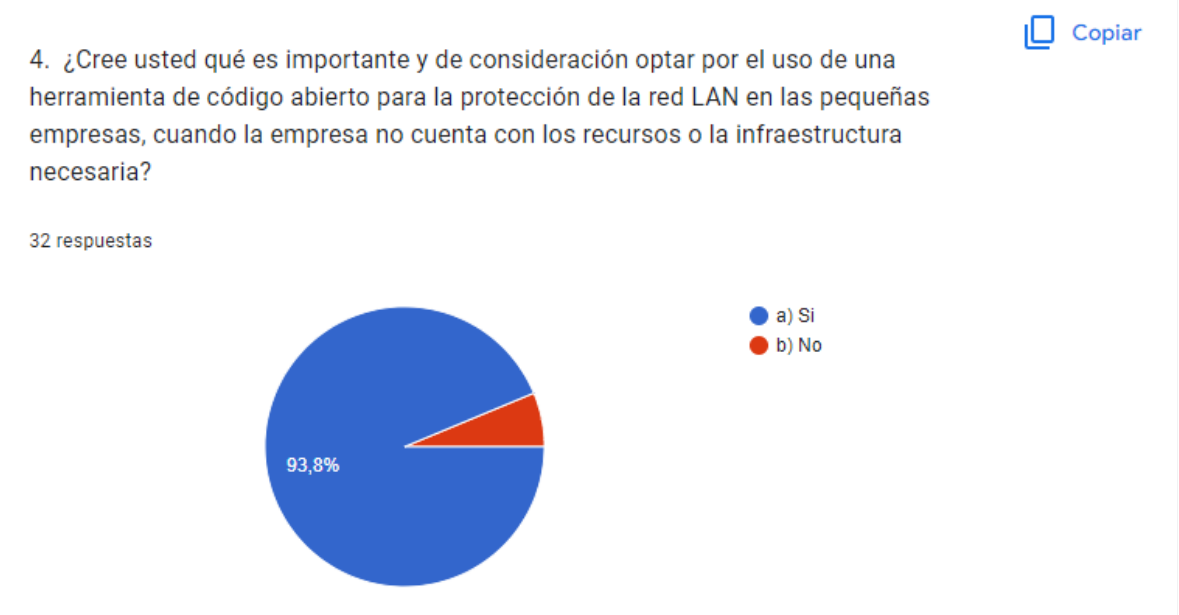
gestión de accesos” y “La complejidad de la implementación y gestión de soluciones de seguridad” con un porcentaje superior de 53,1% por encima de un porcentaje del 28,1% el cual corresponde a “La complejidad de la implementación y gestión de soluciones de seguridad”.



- Los desafíos más comunes de acuerdo a los participantes la gran mayoría concordaron en dos, los cuales uno tiene una participación del 53,1% están de acuerdo que sea por falta de políticas y procedimientos y el 28,1% por presupuesto limitado para invertir.



- En este ítem el resultado fue en su totalidad un 100% donde todos dijeron que, si era necesario la protección adecuada de la red LAN en las empresas pequeñas, ya que la tecnología ha tomado gran importancia en las labores cotidianas, desde la actividad más básica como la más compleja.

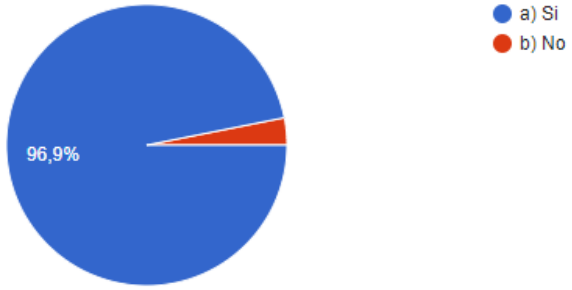


- Toda empresa y toda persona busca en su totalidad la protección de su información, ya que las redes sociales, correos electrónicos, almacenamiento en los equipos, etc… a generado en la actualidad como una herramienta fácil y a la mano que se puede adquirir en cuales lugar, donde el 93,8% de las personas están de acuerdo que se trabaje en el uso de una herramienta de código abierto que genera protección a la red LAN.

Copiar

5. ¿Cree usted que pueden traer ventajas importantes la implementación de una herramienta de código abierto que ofrezca una visibilidad de la actividad de seguridad, que pueda detectar y responder a las amenazas de seguridad para la protección de la red LAN en las pequeñas empresas?

32 respuestas

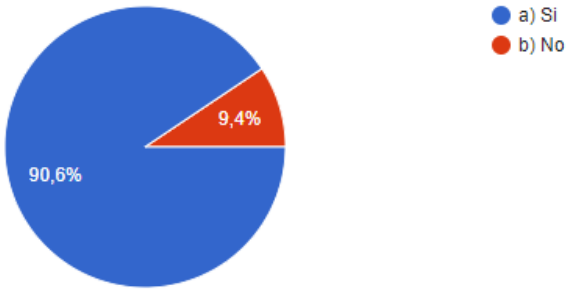


- La opinión de los encuestados frente a las ventajas que pueden traer la importancia de implementar una herramienta de código abierto que ofrezca una visibilidad de la actividad de seguridad para la detección de amenazas dentro de una red LAN fue asertiva con un 96,9%, lo cual indica que si consideran de gran importancia la aplicabilidad de una herramienta que pueda ayudar a la gestión y monitorización de las amenazas dentro del tráfico de la red LAN.

Copiar

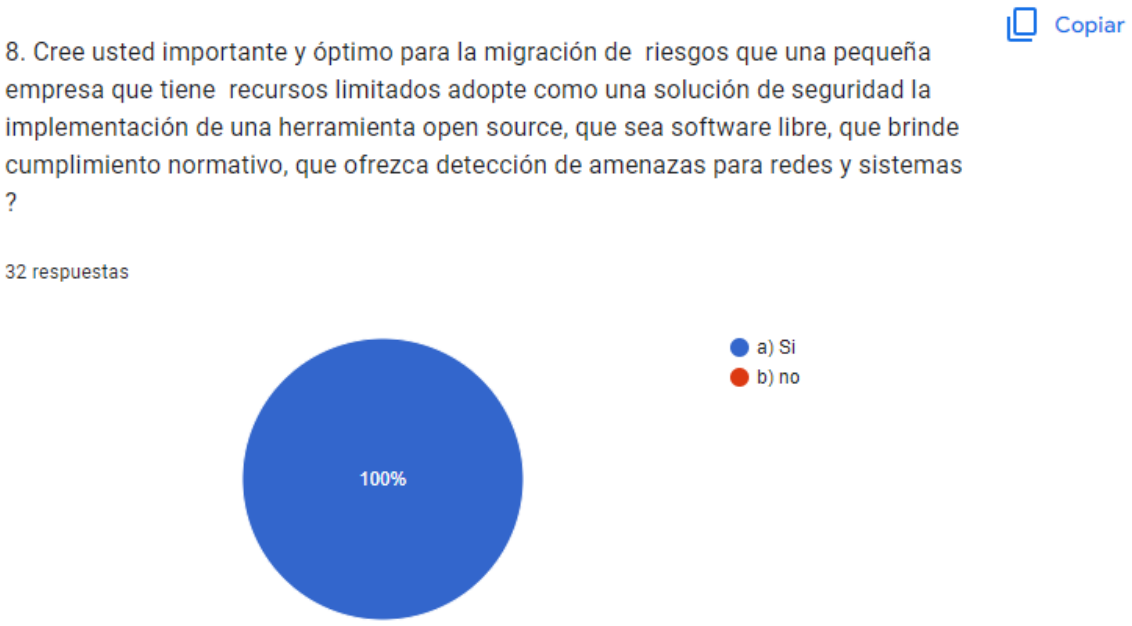
6. ¿Cree usted que afectará de forma positiva a la infraestructura y al presupuesto de la empresa si se implementan herramientas de seguridad open source?

32 respuestas



- La mayoría de personas considera que sí es de gran utilidad y beneficio, tanto económicamente como en materia de seguridad, la implementación de un software open source, que brinde seguridad en cuanto a lo que nos compete cómo materia principal de la investigación, que es la red LAN con un 90,6% con las personas de acuerdo contra un 9,4% de personas que no están de acuerdo con dicha implementación.

- Para el 96,9% de los encuestados, sí es de impacto positivo en materia de productividad y eficiencia que una empresa pyme implemente herramientas de seguridad open source.



- El 100% de los encuestados está de acuerdo con que se implemente herramientas de seguridad open source para la mitigación de riesgos frente a la red LAN y todo lo que abarca dicha brecha, lo cual brinda cumplimiento normativo de acuerdo las normas ISO mencionadas en el presente trabajo además de que ofrece detección de amenazas.

CONCLUSIONES:

Una vez realizado el estudio de factibilidad del presente proyecto, se cuenta con la información necesaria y suficiente que permite llegar a las siguientes conclusiones:

- El presente trabajo busca exponer y dar a conocer los ataques más comunes que se han presentado en los últimos años en la red LAN dentro de las pymes, para la mitigación de las mimas.
- La seguridad en la red LAN, garantiza la integridad de la información y sostenibilidad de las pymes que hacen uso de dicha red.
- El uso oportuno y adecuado de herramientas open source que ayudan a detectar amenazas, monitorización de integridad, respuesta a incidentes es de suma importancia para mantener la seguridad de los datos y mantener los criterios planteados y ofrecidos al cliente por parte de las pymes.

RECOMENDACIONES

- Para una adecuada administración y aplicabilidad de los reglamentos en cuanto a el marco legal e integridad y seguridad informática en lo que compete todo lo relacionado con la red LAN, es necesario tener un área específica de seguridad informática o contar con funcionarios dentro de las pymes que estén capacitados y que cuenten con la destreza y conocimientos suficientes para abordar dichos problemas y poder hacer uso, aplicabilidad y mantenimiento a la herramienta open source (wazuh) que exponemos en el anexo del presente proyecto.
- Mantener a todo el personal de la pyme que su trabajo tenga relación directo con la red LAN, capacitado para mantener las buenas prácticas de la integridad de los datos que se transfiere o se comunica por medio de la red LAN.
- Mantener actualizado el hardware, incluido servidores y enrutadores.
- Realizar, periódicamente, un respaldo de datos e información.

REFERENCIAS

Barahona Delgado , E. M., & Gellibert López, P. F. (2011). *dspace espol.* https://www.dspace.espol.edu.ec/bitstream/123456789/20042/3/Tesis%20Barahona-Gellibert.pdf

Barahona Delgado, E. M. (2011). *dspace espol.* https://www.dspace.espol.edu.ec/bitstream/123456789/20042/3/Tesis%20Barahona-Gellibert.pdf

Bautista García, I. J. (08 de febrero de 2021). *servnet.* https://www.servnet.mx/blog/hacking-etico-en-que-consiste-y-por-que-es-importante

Council of the European Union. (2019). Cybersecurity for SMEs: Challenges and Recommendations. Brussels: Council of the European Union.

dk diseño kreativo. (s.f.). *dk diseño kreativo.*

Equipo de Expertos de Ciencia y Tecnología de la Universidad Internacional de Valencia. (25 de agosto de 2016). *Universidad Internacional de Valencia.* Obtenido de https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-y-como-funciona-el-protocolo-ip

Hernandez Cueto, C. C. (febrero de 2018). *repository unipiloto.* http://repository.unipiloto.edu.co/handle/20.500.12277/2464

Howard. (22 de julio de 2021). Obtenido de https://community.fs.com/es/blog/what-is-dhcp-snooping-and-how-it-works.html

https://dkreativo.es/index.php/noticias-y-eventos-6/que-es-un-proveedor-de-servicios-de-internet-o-un-isp-237

https://forum.huawei.com/enterprise/es/ataques-de-redirecci%C3%B3n-e-inaccesibilidad-de-paquetes-icmp/thread/525357-100233

Instituto Nacional de Ciberseguridad. (s.f). https://www.incibe.es/aprendeciberseguridad/ingenieria-social

Jimenez, L. (6 de mayo de 2019). huawei.

Kaspersky Lab. (2021). DDoS Attacks in Q4 2020. https://securelist.com/ddos-attacks-in-q4-2020/101547/

kaspersky. (26 de 04 de 2022). *kaspersky*. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

López, J. M. (2019). *Thinkbig.* https://blogthinkbig.com/analizar-paquetes-de-red-wireshark

Luz, S. d. (13 de agosto de 2021). *msp360.* https://www.redeszone.net/tutoriales/internet/tcp-udp-caracteristicas-uso-diferencias/

Mahmood, Z. (2019). The Importance of Cyber Security for SMEs: A Literature Review. International Journal of Advanced Computer Science and Applications, 10(2), 338-345.

mcafee. (s.f.). *McAfee.* https://www.mcafee.com/esco/antivirus/firewall.html#:~:text=Los%20firewall%20son%20programas%20de,de%20su%20conexi%C3%B3n%20a%20Internet.

Pérez, I. (2015). welivesecurity. https://www.welivesecurity.com/la-es/2015/06/17/trata-ataque-transferencia-zona-dns/

Ponemon Institute. (2019). The 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses. Traverse City, MI: Ponemon Institute LLC.

Schwartz , M. J. (2020). Ciberseguridad Riesgos, Avances Y El Camino A Seguir En América Latina Y El Caribe. *Banco Interamericano de Desarrollo (BID)*, 1-204.

Sharma, M. (2015). Importance of Network Security in Small and Medium Sized Business. International Journal of Advanced Research in Computer Science and Software Engineering, 5(8), 158-163.

Unir la universidad en internet. (2021). *unir la universidad en internet.* Obtenido de https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/

Valencia, A. (2019). *openaccess uoc.* http://openaccess.uoc.edu/webapps/o2/bitstream/10609/97586/8/avalenciapTFM0619memoria.pdf

LISTADO DE ANEXOS

Anexo Instalación de WAZUH.

Wazuh La Plataforma De Seguridad De Código Abierto Protección Unificada Xdr Y Siem

Instalación y primeros pasos con Wazuh - Host IDS

https://documentation.wazuh.com/current/getting-started/index.html

https://www.youtube.com/watch?v=X2n5mzbPx0g

Documentación:

https://documentation.wazuh.com/current/index.html

Wazuh server:

https://documentation.wazuh.com/current/installation-guide/wazuh-server/index.html

Wazuh es un sistema de detección de intrusiones de seguridad de código abierto (IDS) y plataforma de gestión de seguridad de eventos (SIEM) diseñada para ayudar a las empresas a monitorear y proteger sus redes y sistemas contra amenazas cibernéticas. Es ampliamente utilizado por miles de organizaciones en todo el mundo, desde pequeñas empresas hasta grandes empresas.

En general, Wazuh es una herramienta de seguridad muy útil para cualquier organización que necesite monitorear y proteger sus sistemas y redes contra amenazas cibernéticas.

Wazuh en pequeñas empresas PYMES nos ofrece:

- ***Protección contra amenazas cibernéticas:*** Las pequeñas empresas son cada vez más susceptibles a ataques cibernéticos, ya que a menudo no tienen el mismo nivel de recursos y protecciones de seguridad que las grandes empresas. Wazuh puede ayudar a proteger a estas empresas al detectar y alertar sobre amenazas cibernéticas en tiempo real, lo que les permite tomar medidas inmediatas para mitigar los riesgos.

- ***Cumplimiento normativo:*** Algunas regulaciones gubernamentales y de la industria exigen que las empresas implementen medidas de seguridad para proteger los datos personales y confidenciales de los clientes y empleados. Wazuh puede ayudar a las PYMES a cumplir con estos requisitos y evitar multas y sanciones legales.

- ***Visibilidad y control de la red:*** Las PYMES pueden tener redes de TI complejas y heterogéneas con múltiples sistemas operativos y dispositivos. Wazuh puede proporcionar una vista unificada de la red y permitir a los administradores de seguridad monitorear y controlar la actividad de la red en tiempo real, lo que les permite detectar y mitigar las amenazas antes de que causen daño.

- ***Escalabilidad y flexibilidad:*** Wazuh es una herramienta de seguridad escalable y flexible que puede adaptarse a las necesidades y recursos de las PYMES. Es fácil de instalar y usar, y puede ejecutarse en una variedad de plataformas, lo que lo convierte en una opción atractiva para empresas con presupuestos limitados y recursos de TI limitados.

Wazuh en pequeñas empresas PYMES puede ayudar a protegerlas contra amenazas cibernéticas, cumplir con las regulaciones normativas, proporcionar visibilidad y control de la red, y ofrecer escalabilidad y flexibilidad.

Componentes centrales de Wazuh:

- ***indexador Wazuh:*** El indexador de Wazuh es un motor de análisis y búsqueda de texto completo altamente escalable. Este componente central indexa y almacenas alertas generadas por el servidor Wazuh.
- ***servidor Wazuh:*** El servidor procesa y almacena la información recibida de los agentes, realiza análisis de seguridad y activas alertas cuando se detectan posibles amenazas. Un solo servidor puede analizar datos de miles de agentes y escalar cuando se configura como un clúster. También se utiliza para gestionar los agentes, configurándolos de forma remota cuando sea necesario.
- ***Panel de Wazuh:*** El panel de control de Wazuh es la interfaz de usuario web para la visualización, el análisis y la gestión de datos. Incluye tableros para cumplimiento normativo, vulnerabilidades, integridad de archivos, evaluación de configuración, eventos de infraestructura en la nube, entre otros. La interfaz de usuario proporciona una vista centralizada de la información de seguridad y las alertas, permitiendo a los administradores de seguridad monitorear y responder a los eventos de seguridad en tiempo real.
- ***Agente Wazuh:*** Los agentes de Wazuh se instalan en puntos finales, como computadoras portátiles, computadoras de escritorio, servidores, instancias en la nube o máquinas virtuales. Proporcionan capacidades de prevención, detección y respuesta ante

amenazas.

Hardware:

Los requisitos dependen en gran medida de la cantidad de puntos finales protegidos y cargas de trabajo en la nube. Este número puede ayudar a calcular cuántos datos se analizarán y cuántas alertas de seguridad se almacenarán e indexarán.

Podemos implementar el servidor, el indexador y el panel Wazuh en un mismo host, y esto nos puede dar para monitorea hasta 100 puntos finales durante 90 dias de datos de alerta consultables indexados, para este caso podemos utilizar la siguiente tabla.

Agentes	UPC	RAM	Almacenamiento (90 días)
1–25	4 vCPU	8 GB	50GB
25–50	8 vCPU	8 GB	100GB
50–100	8 vCPU	8 GB	200GB

Para entornos grandes se recomienda la implementación Distribuida, configurando en clúster de varios nodos está disponible para el servidor y el indexador wazuh, esto proporciona alta disponibilidad y equilibrio de carga.

Sistema Operativo:

Wazuh lo podemos en un sistema operativo Linux 64x bit pero se recomienda en las siguientes versiones.

Amazon Linux 2

Centos 7,8

Red Hat Enterprise Linux 7,8,9

Ubuntu 16.04,18.04,20.04,22.04.

Compatibilidad con el navegador:

El panel de control de Wazuh es compatible con los siguientes navegadores web:

Chrome 95 o posterior

Firefox 93 o posterior

Safari 13.7 o posterior

Otros navegadores basados en Chromium también podrían funcionar. Internet Explorer 11 no es compatible.

Instalación de Wazuh

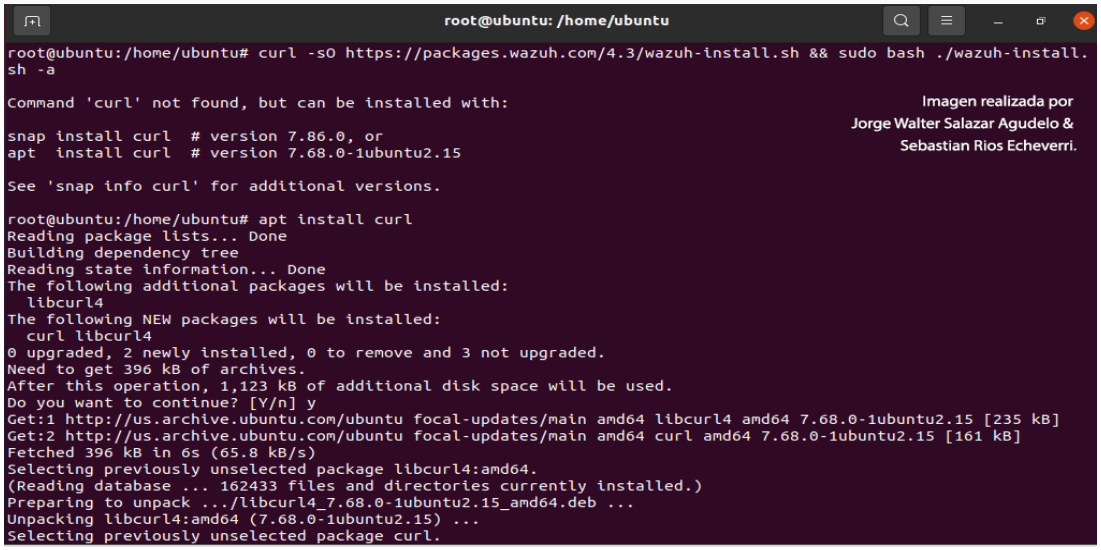
1. ***El inicio rápido*** es una forma automatizada de instalar Wazuh en solo unos minutos.
2. ***La guía de instalación (instalación paso a paso)*** proporciona instrucciones sobre cómo instalar cada componente central y cómo implementar los agentes de Wazuh.

Inicio Rápido: Instalación Del Servidor Wazuh

Descarga y ejecuta el asistente de instalación de Wazuh.

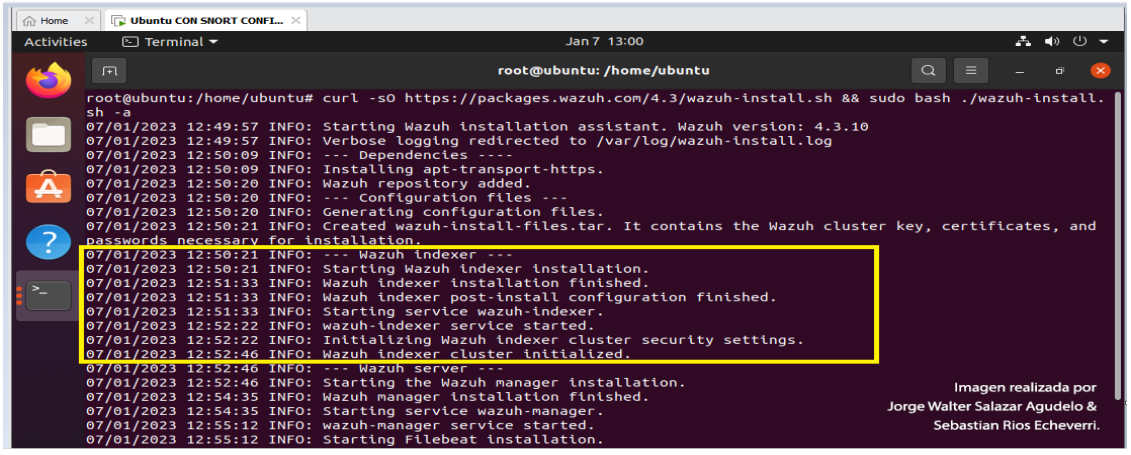
```
apt install curl
```

```
curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh && sudo bash

./wazuh-install.sh -a
```

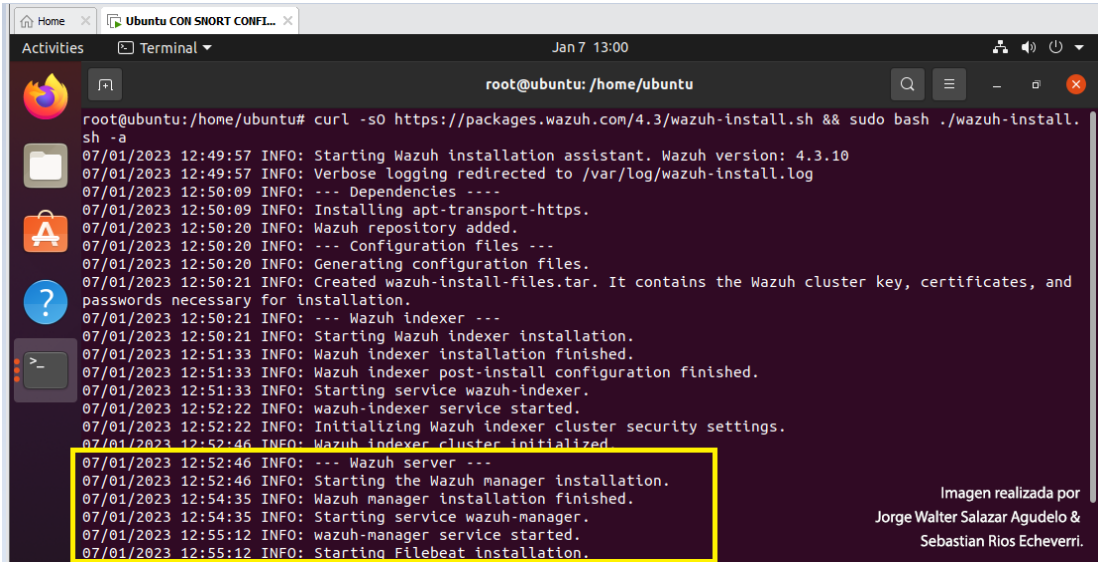


Arrancamos la instalación

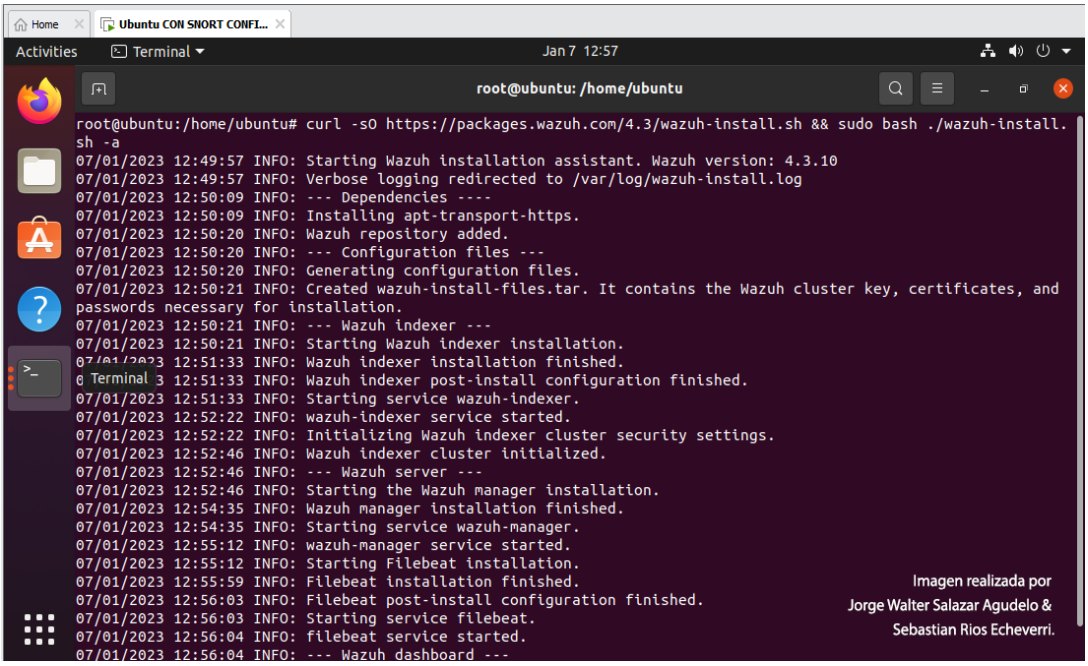
Instalación del Indexer

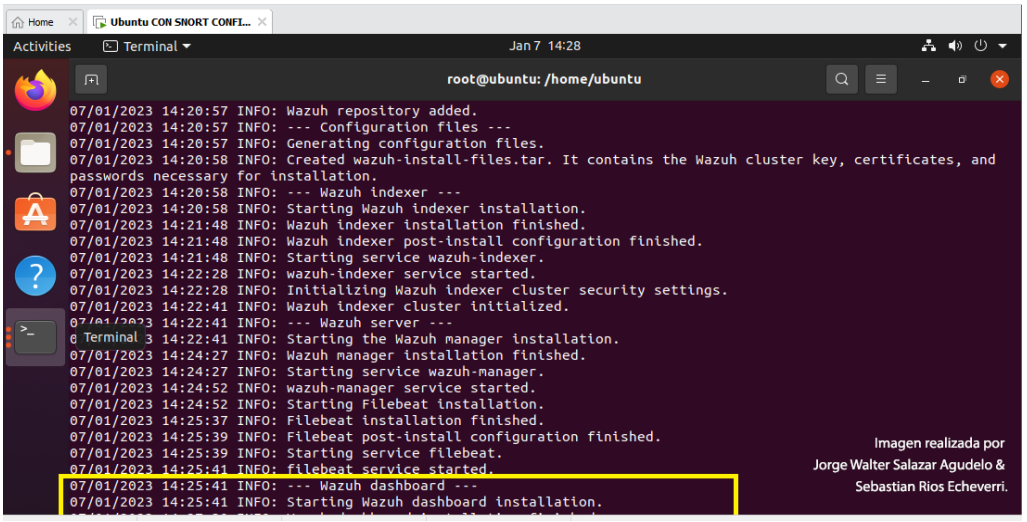


Instalación de Wazuh server

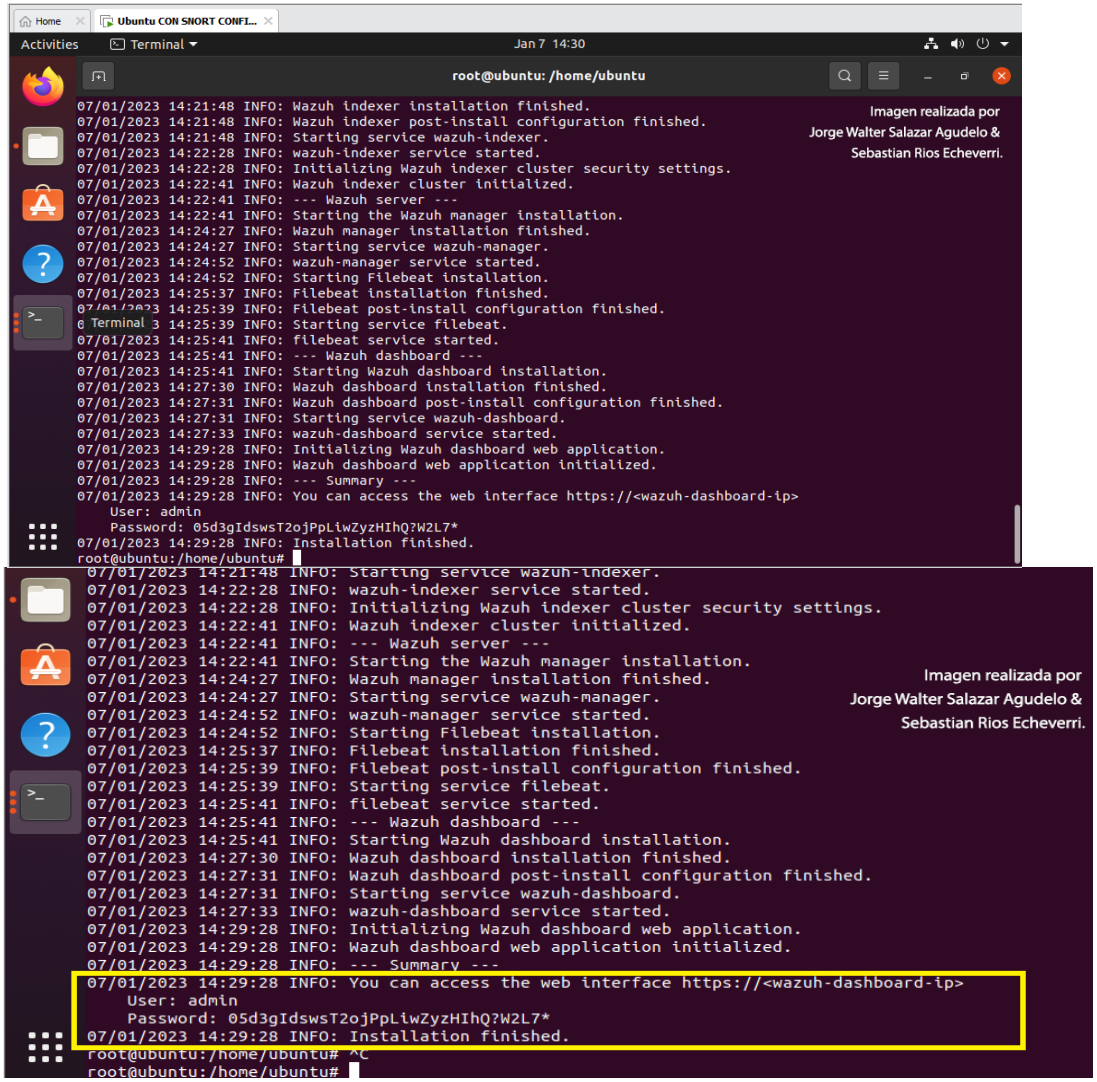


Instalación de Wazuh Dashboard





Final de instalación:



NOTA: Solo si te da el siguiente error

```
ERROR: The Wazuh API user wazuh does not exist ERROR: The Wazuh
API user wazuh-wui does not exist
ERROR: User  is not registered in Wazuh API
```

Instalas los siguientes paquetes:

```
apt-get install curl apt-transport-https lsb-release gnupg2

curl -sL https://deb.nodesource.com/setup_10.x | bash - sudo apt-get
update && sudo apt-get install yarn
apt-get install wazuh-api=3.11.4-1
```

Sino tenemos ningún error, continuamos con la instalación normalmente:

al finalizar no dará las credenciales, guardarlas ya que las necesitaremos para poder ingresar:

```
You can access the web interface https://<wazuh-dashboard-ip> User: admin
Password: O5d3gIdswsT2ojPpLiwZyzHIhQ?W2L7*
```

Una vez que el asistente finaliza la instalación, la salida muestra las credenciales de acceso y un mensaje que confirma que la instalación fue exitosa.

```
INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
    User: admin
    Password: <ADMIN_PASSWORD>
INFO: Installation finished.
```

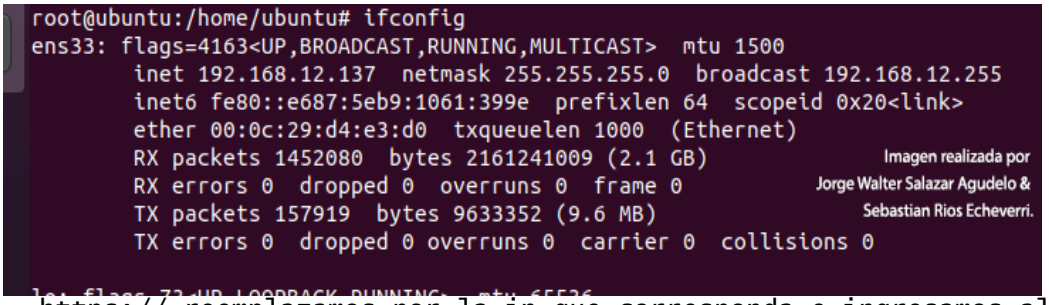
Ahora ha instalado y configurado Wazuh.

Acceda a la interfaz web de Wazuh con

https:// sus credenciales: Nombre de usuario: administrador

Contraseña: <CONTRASEÑA_ADMIN>

Ingresamos para este caso: con la ip del servidor= 192.168.12.137



https:// reemplazamos por la ip que corresponda e ingresamos al aplicativo:

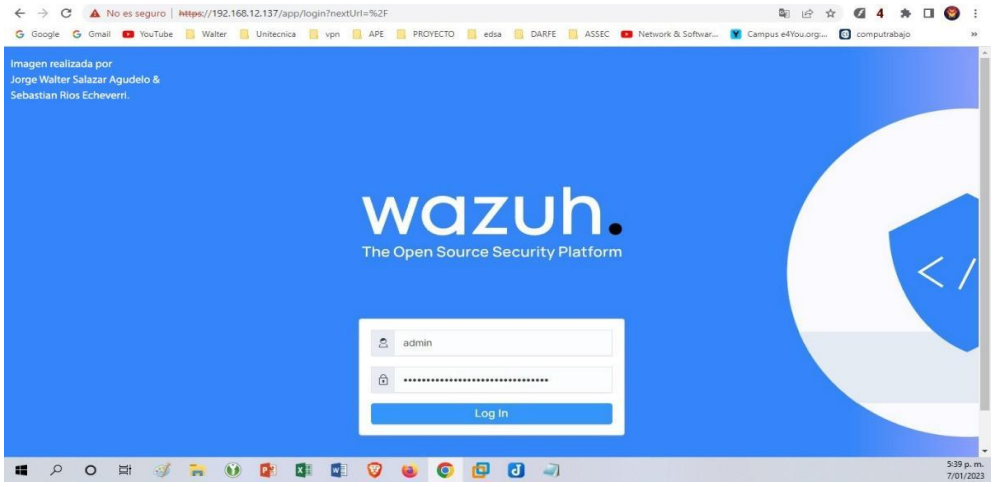
para este caso es: 192.168.12.137

User: admin

Password: O5d3gIdswsT2ojPpLiwZyzHIhQ?W2L7*

Cuando accede al panel de control de Wazuh por primera vez, el navegador muestra un mensaje de advertencia que indica que el certificado no fue emitido por una autoridad de confianza. Esto es de esperar y el usuario tiene la opción de aceptar el certificado como una

excepción o, alternativamente, configurar el sistema para usar un certificado de una autoridad de confianza.



si nos da este error : [API connection] No API available to connect

lo tenemos que solucionar

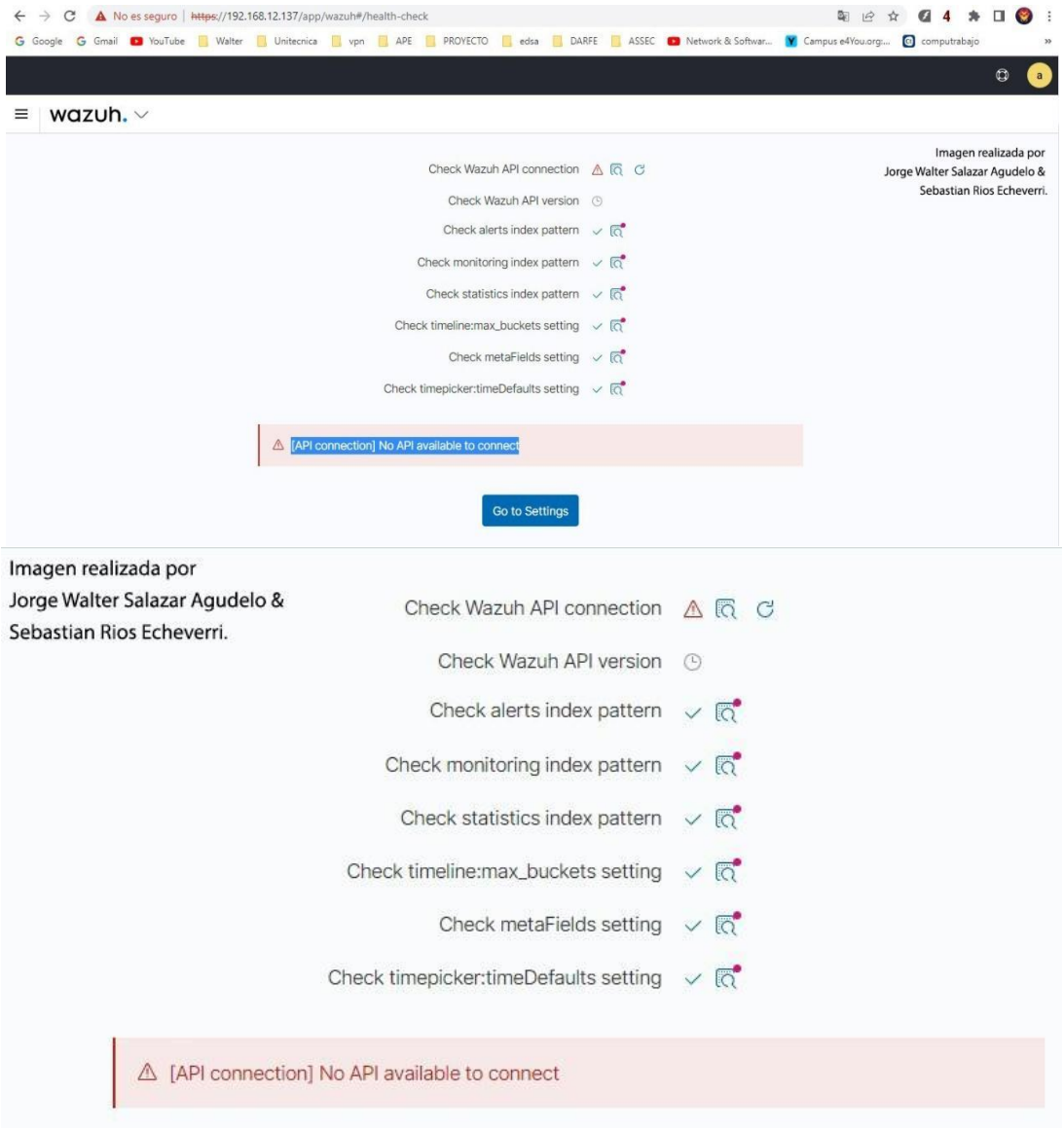


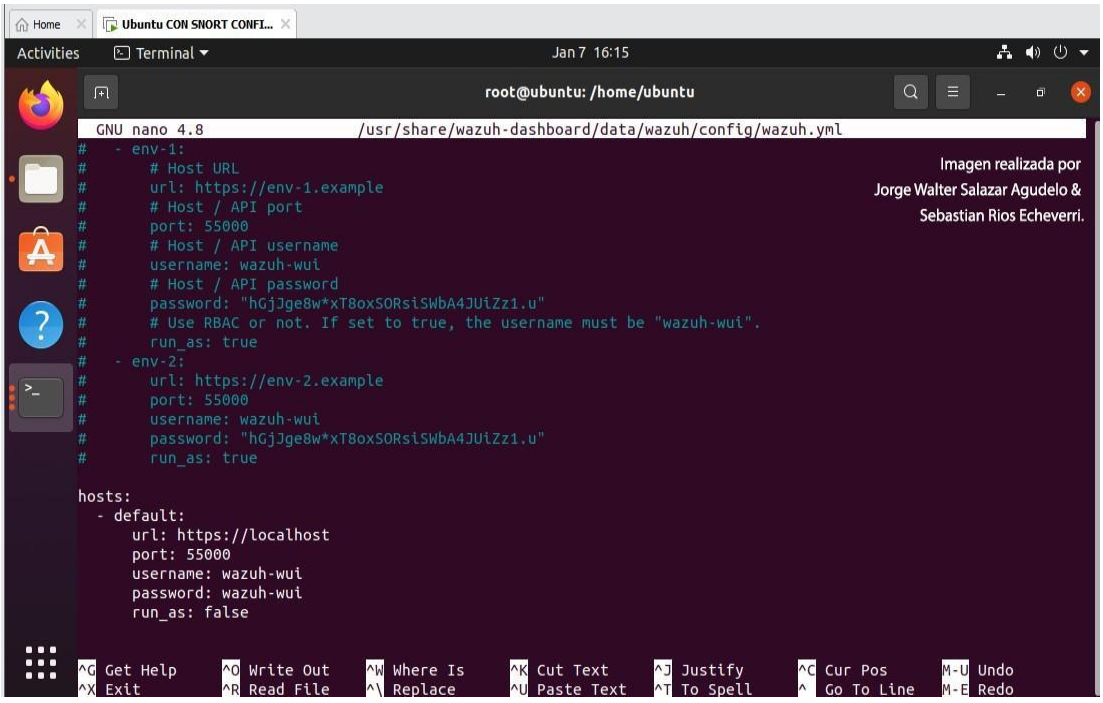
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri.
Check Wazuh API connection
Check Wazuh API version
Check alerts index pattern
Check monitoring index pattern
Check statistics index pattern
Check timeline:max_buckets setting
Check metaFields setting
Check timepicker:timeDefaults setting
[API connection] No API available to connect

Solución al error `ERROR3099 [API connection] No API available to connect`**

`el archivo de configuracion /usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml`

Lo debemos editar y dejarlo así:

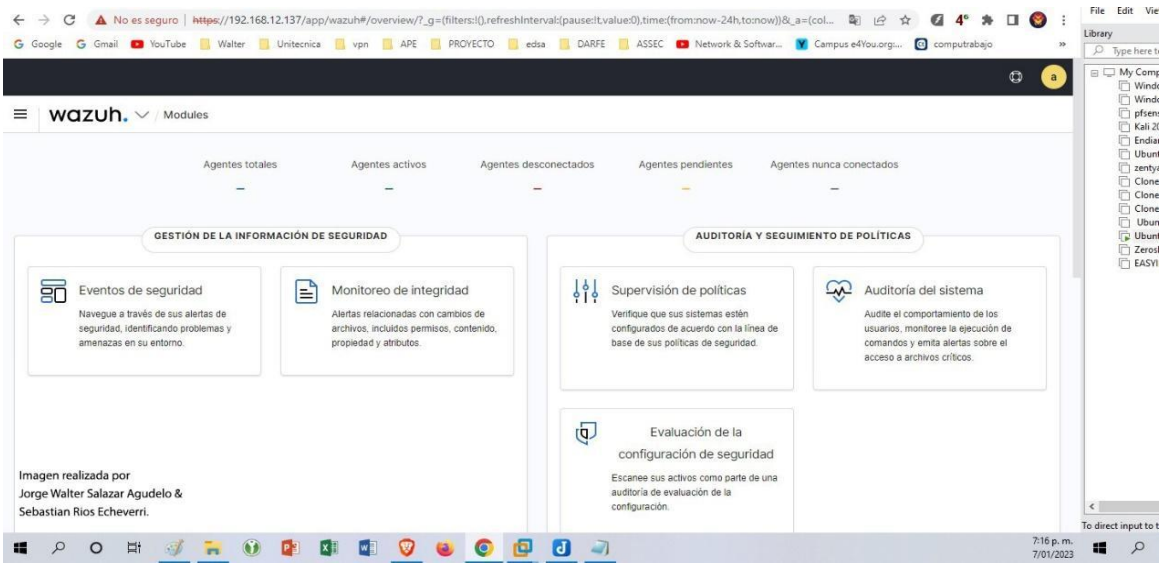
```
nano/usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml
```




```
hosts:
- default:
url: https://localhost port: 55000
username: wazuh-wui password: wazuh-wui
run_as: false
```

y problema solucionado!!!

Puede encontrar las contraseñas de todos los usuarios del indexador de Wazuh y de la API de Wazuh en el **wazuh-passwords.txt** archivo que se encuentra dentro de **wazuh-install-files.tar**. Para imprimirlos, ejecute el siguiente comando:




```
sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-
```

Otras contraseñas que el aplicativo arroja al instalar Wazuh que debemos guardar y tener en cuenta:

```
Admin user for the web user interface and Wazuh indexer. Use this user to log
in to Wazuh dashboard indexer_username: 'admin'
indexer_password: 'O5d3gIdswsT2ojPpLiwZyzHIhQ?W2L7*'
```

Wazuh dashboard user for establishing the connection with Wazuh indexar

```
indexer_username: 'kibanaserver'
```

```
indexer_password: '4rgVgOAvqEcHYt3E6G1PPCyBDnu6H?Wx'
```

Regular Dashboard user, only has read permissions to all indices and all permissions on the .kibana index

```
indexer_username: 'kibanaro'
indexer_password: '?glZGz93O2yFVAVFs2G8YHUmQz4bWOQZ'
```

Filebeat user for CRUD operations on Wazuh indices

```
indexer_username: 'logstash'
indexer_password: 'UMp?GzgWttxY.OWNbLoPht3pXm5IWDxe'
```

User with READ access to all indices

```
indexer_username: 'readall'
indexer_password: '*T9eR3xo.5CjK45ca5LQB5Tk5XkWmoZk'
```

User with permissions to perform snapshot and restore operations

```
indexer_username: 'snapshotrestore'
indexer_password: 'xuHs5HSPzci4qt5+.Rbd+Fu81ZrEdwNX'
```

Reiniciamos los servicios

```
sudo systemctl restart wazuh-manager sudo service wazuh-manager status sudo
systemctl start wazuh-manager
```

Si desea desinstalar los componentes centrales de Wazuh, ejecute el asistente de instalación de

```
-uo --uninstall
```

Wazuh usando la opción

Próximos pasos

Ahora que su instalación de Wazuh está lista, puede comenzar a implementar el agente de Wazuh. Esto se puede usar para proteger computadoras portátiles, computadoras de escritorio, servidores, instancias en la nube, contenedores o máquinas virtuales. El agente es liviano y multipropósito, y proporciona una variedad de capacidades de seguridad.

2.La guía de instalación: esta es la segunda forma de instalar wazuh, al anterior lo hace de una forma más automática, pero en esta opción se realizara paso a paso, ambas opciones son válidas para la instalación.

2.1 Instalación Del Servidor Wazuh Paso A Paso

https://documentation.wazuh.com/current/installation-guide/wazuh-server/step-by-step.html

Instale y configure el servidor de Wazuh como un clúster de un solo nodo o de varios nodos siguiendo las instrucciones paso a paso.

El servidor de Wazuh es un componente central que incluye el administrador de Wazuh y Filebeat.

El administrador de Wazuh recopila y analiza datos de los agentes de Wazuh desplegados. Activa alertas cuando se detectan amenazas o anomalías.

Filebeat reenvía de forma segura alertas y eventos archivados al indexador de Wazuh.

El proceso de instalación se divide en dos etapas.

1. Instalación del nodo del servidor Wazuh
2. Configuración de clúster para implementación de múltiples nodos

Nota Se requieren privilegios de usuario raíz para ejecutar los comandos que se describen a continuación.

Paso 1. Instalación del nodo del servidor Wazuh

Agregar el repositorio de Wazuh

Si está instalando el servidor de Wazuh en el mismo host que el indexador de Wazuh, puede omitir estos pasos, ya que es posible que ya haya agregado el repositorio de Wazuh.

```
sudo su
apt-get update apt-get upgrade
```

```
apt install curl
```

Instale los siguientes paquetes si faltan.

```
apt-get install gnupg apt-transport-https
```

Instale la clave GPG.

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default- keyring --
keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod
644 /usr/share/keyrings/wazuh.gpg
```

Agregar el repositorio.

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg]
https://packages.wazuh.com/4.x/apt/ stable main" | tee -a
/etc/apt/sources.list.d/wazuh.list
```

Actualice la información de los paquetes.

```
apt-get update
```

Paso 2. Instalación del administrador de Wazuh

Instale el paquete del administrador de Wazuh.

```
apt-get -y install wazuh-manager
```

Habilite e inicie el servicio de administrador de Wazuh.

```
systemctl daemon-reload systemctl enable wazuh-manager
systemctl start wazuh-manager
```

1. **Ejecute el siguiente comando para verificar el estado del administrador de Wazuh.**

```
systemctl status wazuh-manage
```

Instalación de Filebeat

```
apt-get -y install filebeat
```

Configuración de Filebeat

1. Descargue el archivo de configuración de Filebeat preconfigurado.

```
curl -so /etc/filebeat/filebeat.yml
https://packages.wazuh.com/4.3/tpl/wazuh/filebeat/filebeat.yml
```

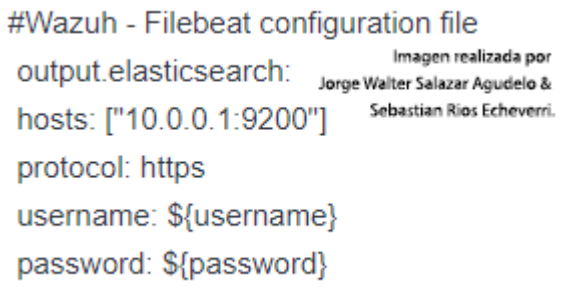
2. Edite el **/etc/filebeat/filebeat.yml** archivo de configuración y reemplace el siguiente valor:

a. hosts: La lista de nodos indexadores de Wazuh a los que conectarse. Puede utilizar direcciones IP o nombres de host. De forma predeterminada, el host se establece en `localhost` .

Reemplácelo con la dirección del indexador de Wazuh según `corresponda.hosts: ["127.0.0.1:9200"]`

Si tiene más de un nodo indexador de Wazuh, puede separar las direcciones con comas. Por ejemplo,`hosts: ["10.0.0.1:9200", "10.0.0.2:9200", "10.0.0.3:9200"]`

Ejemplo:



3. Cree un almacén de claves de Filebeat para almacenar de forma segura las credenciales de autenticación.

```
filebeat keystore create
```

4. Agregue el nombre de usuario y la contraseña predeterminados **admin: admin** al almacén de claves de secretos.

```
echo admin | filebeat keystore add username --stdin --force
echo admin | filebeat keystore add password --stdin --force
```

5. Descarga la plantilla de alertas para el indexador de Wazuh.

```
curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/4.3/extensions/elasticsearch/7
.x/wazuh-template.json
chmod go+r /etc/filebeat/wazuh-template.json
```

6. Instale el módulo Wazuh para Filebeat.

```
curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.2.tar.gz
```

Implementación de certificados

Nota: Asegúrese de **wazuh-certificates.tar**

Colocar una copia del archivo, creado durante el paso de configuración inicial, en su directorio de trabajo.

1. Reemplácelo con el nombre del certificado del nodo del servidor de Wazuh, el mismo que se usó **config.yml** al crear los certificados. Luego, mueva los certificados a su ubicación correspondiente. NODE_NAME=<server-node-name> continuamos con:

```
mkdir /etc/filebeat/certs
tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./$NODE_NAME.pem
./$NODE_NAME-key.pem ./root-ca.pem
mv -n /etc/filebeat/certs/$NODE_NAME.pem /etc/filebeat/certs/filebeat.pem mv -n
/etc/filebeat/certs/$NODE_NAME-key.pem /etc/filebeat/certs/filebeat- key.pem
chmod 500 /etc/filebeat/certs
chmod 400 /etc/filebeat/certs/*
chown -R root:root /etc/filebeat/certs
```

Inicio del servicio Filebeat

1. Habilite e inicie el servicio Filebeat.

```
systemctl daemon-reload systemctl enable filebeat
systemctl start filebeat
```

```
systemctl daemon-reload systemctl enable filebeat
systemctl start filebeat
```

2. Ejecute el siguiente comando para verificar que Filebeat se instaló correctamente.

```
filebeat test output
```

Nos debe dar de respuesta algo así, ejemplo:

Su nodo de servidor Wazuh ahora está instalado correctamente.

Repita esta etapa del proceso de instalación para cada nodo del servidor de Wazuh en su clúster de Wazuh, luego continúe con la configuración del clúster de Wazuh.

Si desea un clúster de nodo único del servidor de Wazuh, todo está configurado y puede continuar directamente con **Instalación del panel de control de Wazuh paso a paso.**

Instalación del panel de control de Wazuh paso a paso.

Instale y configure el panel de control de Wazuh siguiendo las instrucciones paso a paso.

El panel de control de Wazuh es una interfaz web para extraer y visualizar las alertas del servidor de Wazuh y los eventos archivados.

Nota Se requieren privilegios de usuario raíz para ejecutar los comandos que se describen a continuación.

Instalación del tablero Wazuh

Instalación de dependencias de paquetes

```
apt-get install debhelper tar curl libcap2-bin #debhelper version 9 or later
```

Agregar el repositorio de Wazuh

Nota Si está instalando el panel de control de Wazuh en el mismo host que el indexador de Wazuh o el servidor de Wazuh, puede omitir estos pasos, ya que es posible que ya haya agregado el repositorio de Wazuh.

Instale los siguientes paquetes si faltan.

```
apt-get install gnupg apt-transport-https
```

Instale la clave GPG.

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default- keyring
--keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod
644 /usr/share/keyrings/wazuh.gpg
```

Agregar el repositorio.

1. **Actualice la información de los paquetes.**

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg]
https://packages.wazuh.com/4.x/apt/ stable main" | tee -a
/etc/apt/sources.list.d/wazuh.list
```

```
apt-get update
```

Instalación del administrador de wazuh

1. **Instale el paquete del panel de Wazuh.**

```
apt-get -y install wazuh-dashboard
```

Configuración del panel de control de Wazuh

1. Edite el **/etc/wazuh-dashboard/opensearch_dashboards.yml** archivo y reemplace los siguientes valores:

a. ***server.host:*** esta configuración especifica el host del servidor del panel de control de Wazuh. Para permitir que los usuarios remotos se conecten, establezca el valor en la dirección IP o el nombre DNS del servidor del panel de control de Wazuh. El valor **0.0.0.0** aceptará todas las direcciones IP disponibles del host.

b. ***opensearch.hosts:*** las URL de las instancias del indexador de Wazuh que se usarán para todas sus consultas.

El tablero de Wazuh se puede configurar para conectarse a varios nodos indexadores de Wazuh en el mismo clúster.

Las direcciones de los nodos se pueden separar por comas. Por ejemplo, ["https://10.0.0.2:9200", "https://10.0.0.3:9200","https://10.0.0.4:9200"]

```
server.host: 0.0.0.0
server.port: 443
opensearch.hosts: https://localhost:9200
opensearch.ssl.verificationMode: certificate
```

Imagen realizada por Jorge Walter Salazar Agudelo & Sebastian Rios Echeverri.

Implementación de certificados

Nota: Asegúrese de **wazuh-certificates.tar** colocar una copia del archivo, creado durante el paso de configuración inicial, en su directorio de trabajo.

1. Reemplácelo con el nombre de nodo del tablero de Wazuh, el mismo que se usó config.yml para crear los certificados, y mueva los certificados a su ubicación correspondiente.

```
NODE_NAME=<dashboard-node-name>
```

continuamos con:

```
mkdir /etc/wazuh-dashboard/certs
tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/
./$NODE_NAME.pem ./$NODE_NAME-key.pem ./root-ca.pem
mv -n /etc/wazuh-dashboard/certs/$NODE_NAME.pem /etc/wazuh-
dashboard/certs/dashboard.pem
mv -n /etc/wazuh-dashboard/certs/$NODE_NAME-key.pem /etc/wazuh-
dashboard/certs/dashboard-key.pem
chmod 500 /etc/wazuh-dashboard/certs
chmod 400 /etc/wazuh-dashboard/certs/*
chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
```

Inicio del servicio del panel de control de Wazuh

Habilite e inicie el servicio del panel de control de Wazuh.

```
systemctl daemon-reload systemctl enable wazuh-dashboard
systemctl start wazuh-dashboard
```

Nota: Solo para implementaciones distribuidas

Edite el **/usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml** archivo y reemplace el urlvalor con la dirección IP o el nombre de host del nodo maestro del servidor de Wazuh.

```
hosts:
  - default:
    url: https://localhost
    port: 55000
    username: wazuh-wui
    password: wazuh-wui
    run_as: false
```

Acceda a la interfaz web de Wazuh con sus credenciales.

URL: https://<wazuh-dashboard-ip>

Nombre de usuario: administrador

Contraseña : administrador

Cuando accede al panel de control de Wazuh por primera vez, el navegador muestra un mensaje de advertencia que indica que el certificado no fue emitido por una autoridad de confianza.

Se puede agregar una excepción en las opciones avanzadas del navegador web. Para mayor seguridad, el root-ca.pem archivo generado anteriormente se puede importar al administrador de certificados del navegador.

Como alternativa, se puede configurar un certificado de una autoridad de confianza.

Asegurar su instalación de Wazuh

Ya ha instalado y configurado todos los componentes centrales de Wazuh.

Recomendamos **cambiar las credenciales predeterminadas para proteger su infraestructura de posibles ataques.**

Implementación todo en uno e implementación Distribuida

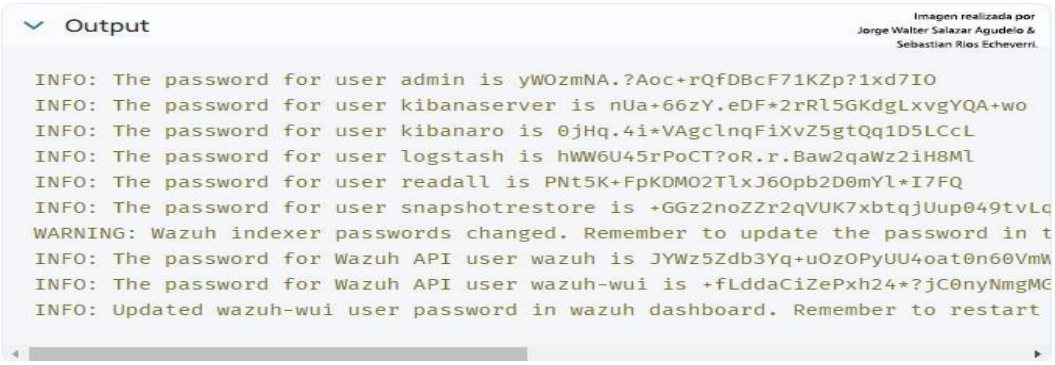
1. Implementación todo en uno

1. Utilice la herramienta de contraseñas de Wazuh para cambiar las contraseñas de todos los usuarios internos.

```
/usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh --change-all --admin-user wazuh --admin-password wazuh
```

Nos mostrara como salida:

2. si se instaló la implementación Distribuida haga lo siguiente.

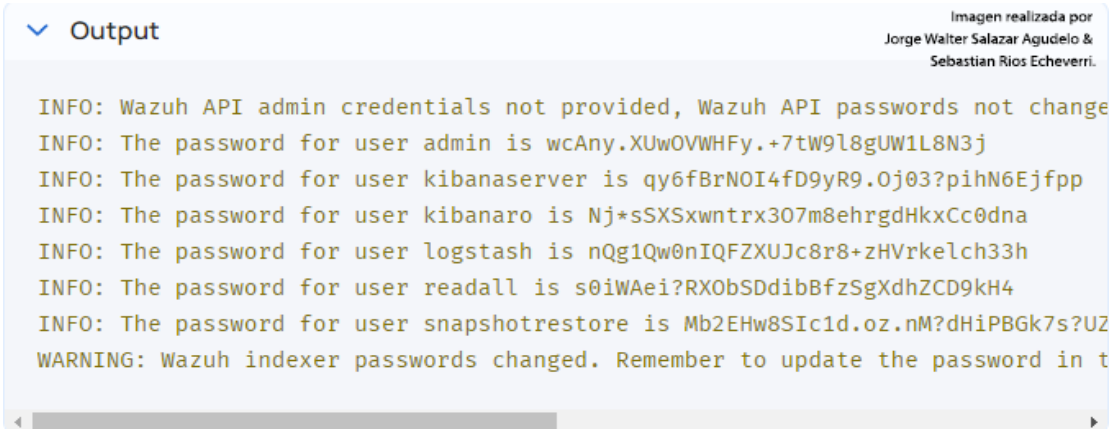



```
/usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh --change-all
```

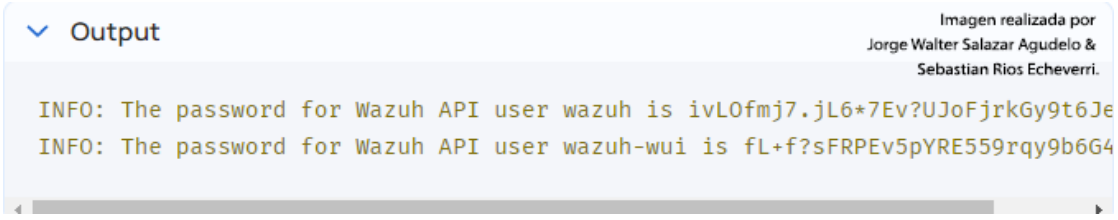
1. En cualquier nodo del indexador de Wazuh , use la herramienta de contraseñas de Wazuh para cambiar las contraseñas de los usuarios del indexador de Wazuh.

Nos mostrara como salida:

2. En el nodo maestro de su servidor de Wazuh , descargue la herramienta de contraseñas de Wazuh y utilícela para cambiar las contraseñas de los usuarios de la API de Wazuh.




```
curl -sO https://packages.wazuh.com/4.3/wazuh-passwords-tool.sh
bash wazuh-passwords-tool.sh --change-all --admin-user wazuh --
admin- password wazuh
```



3. En todos los nodos de su servidor Wazuh , ejecute el siguiente comando para actualizar la contraseña de administrador en el almacén de claves de Filebeat. Reemplace con la contraseña aleatoria generada en el primer paso.

```
echo <admin-password> | filebeat keystore add password --stdin --force
```

4. Reinicie Filebeat para aplicar el cambio.

```
systemctl restart filebeat
```

Nota: Repita los pasos 3 y 4 en cada nodo del servidor Wazuh .

5. En su nodo del tablero de Wazuh , ejecute el siguiente comando para actualizar la contraseña del servidor kibana en el almacén de claves del tablero de Wazuh.

Reemplace con la contraseña aleatoria generada en el primer paso.

```
echo <kibanaserver-password> | /usr/share/wazuh-dashboard/bin/opensearch-dashboards-keystore --allow-root add -f --stdin opensearch.password
```

6. Actualice el **/usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml** archivo de configuración con la nueva contraseña wazuh-wui generada en el segundo paso.

Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri.

```
hosts:
  - default:
      url: https://localhost
      port: 55000
      username: wazuh-wui
      password: <wazuh-wui-password>
      run_as: false
```

7. Reinicie el panel de control de Wazuh para aplicar los cambios.

```
systemctl restart wazuh-dashboard
```

Próximos pasos

Todos los componentes centrales de Wazuh están correctamente instalados y asegurados.

El entorno de Wazuh ahora está listo y puede continuar con la instalación del agente de Wazuh en los puntos finales que se van a monitorear.

Instalación Agente Wazuh en puntos finales agente wazuh

El agente de Wazuh es multiplataforma y se ejecuta en los puntos finales que el usuario desea monitorear. Se comunica con el servidor de Wazuh y envía datos casi en tiempo real a través de un canal encriptado y autenticado.

El agente se desarrolló teniendo en cuenta la necesidad de monitorear una amplia variedad de puntos finales diferentes sin afectar su rendimiento. Es compatible con los sistemas operativos más populares y requiere 35 MB de RAM en promedio.

El agente de Wazuh proporciona funciones clave para mejorar la seguridad de su sistema.

recolector de troncos	Ejecución de comandos
Monitoreo de integridad de archivos (FIM)	Evaluación de configuración de seguridad (SCA)
Inventario del sistema	Detección de malware
Respuesta activa	Seguridad del contenedor
seguridad en la nube	

Imagen realizada por Jorge Walter Salazar Agudelo & Sebastian Rios Echeverri.

Para instalar un agente de Wazuh, seleccione su sistema operativo y siga las instrucciones.

Teminales Linux:

https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package- linux.html

Terminales Windows:

https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package- windows.html

Para iniciar el proceso de instalación, descargue el instalador de Windows.

Seleccione el método de instalación que desea seguir: interfaz de línea de comandos (CLI) o interfaz gráfica de usuario (GUI).

link de descarga para windows :

https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.10-1.msi

wazuh-agent-4.3.10-1.msi

Terminales

MacOS

https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package- macos.html

Terminales Solaris

https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package- solaris.html

Terminales AIX

https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package- aix.html

Terminales HP-UX

https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package- hpux.html

Nota La compatibilidad entre el agente de Wazuh y el administrador de Wazuh está garantizada cuando la versión del administrador de Wazuh es posterior o igual a la del agente de Wazuh.

Terminales Windows: Instalacion Desde La Consola De Windows

https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html

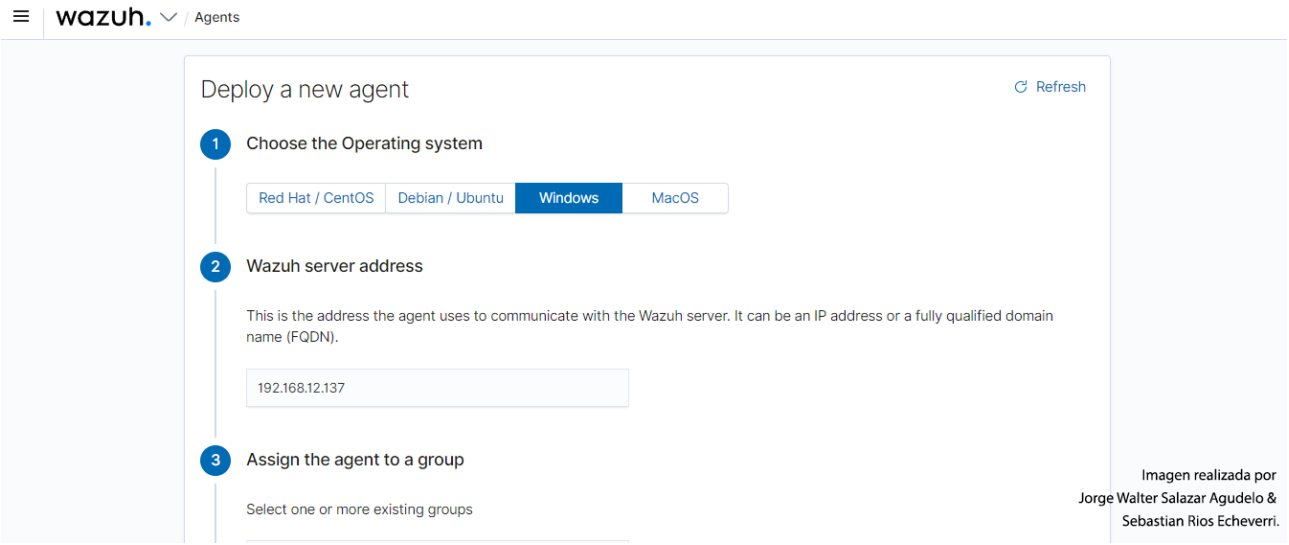
Nota Para realizar la instalación, se requieren privilegios de administrador.

desde Windows XP hasta las últimas versiones disponibles, incluidos Windows 11 y Windows Server 2022.

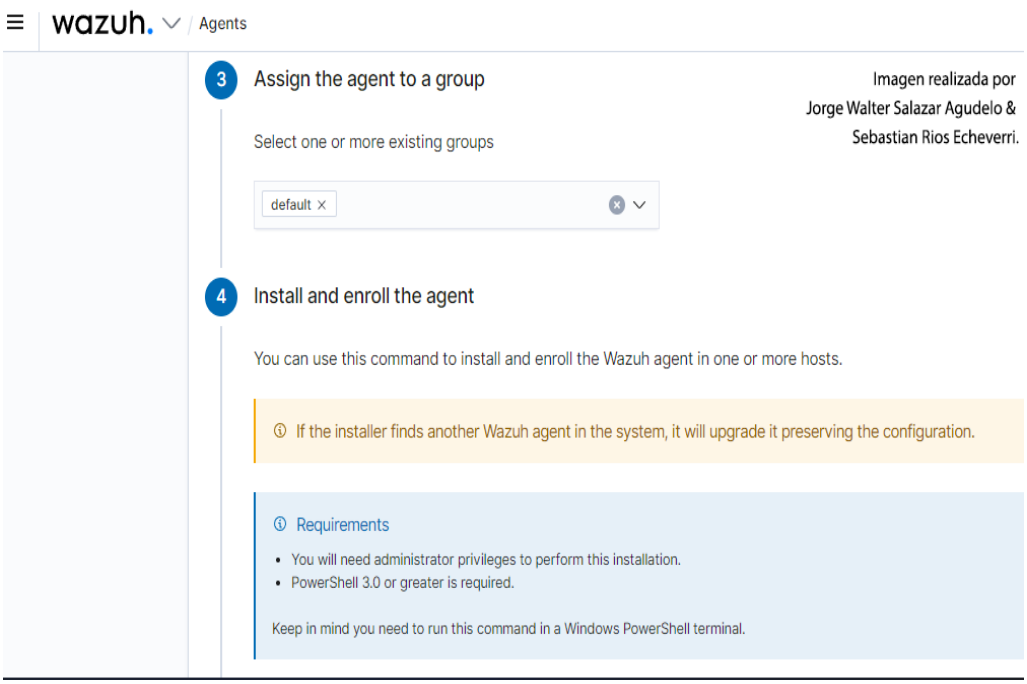
1. la instalación la podemos generar desde el servidor Wazuh, él nos dará los parámetros para la configuración de cada sistema operativo, windows, linux, mac etc.

En Windows vamos a crear agente Windows como en la imagen.

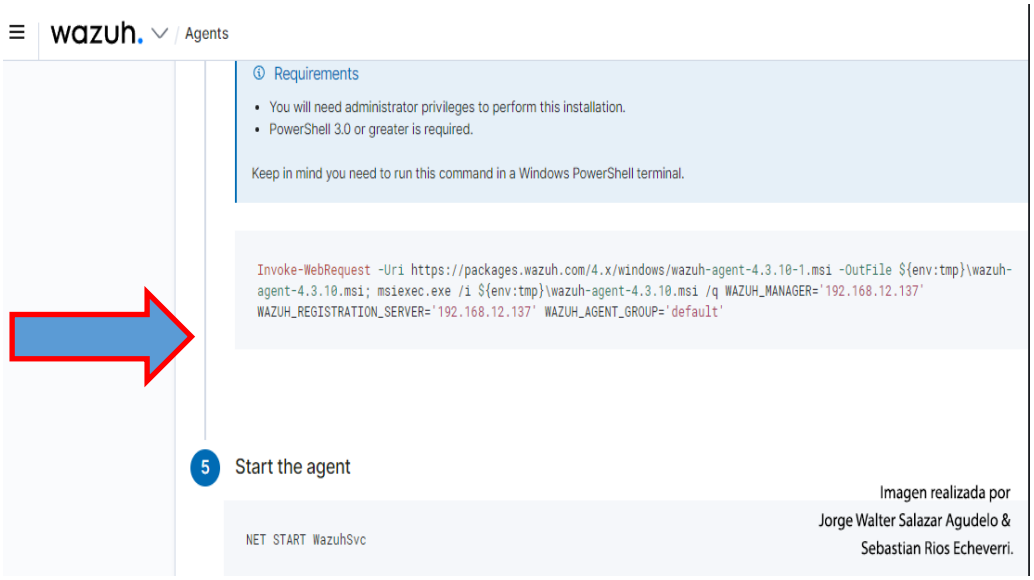
a. seleccionamos la ip del servidor.



b. seleccionamos el grupo



c. Él nos indica que la instalación la debemos hacer por el powershell como administrador, y nos indica los comando a realizar

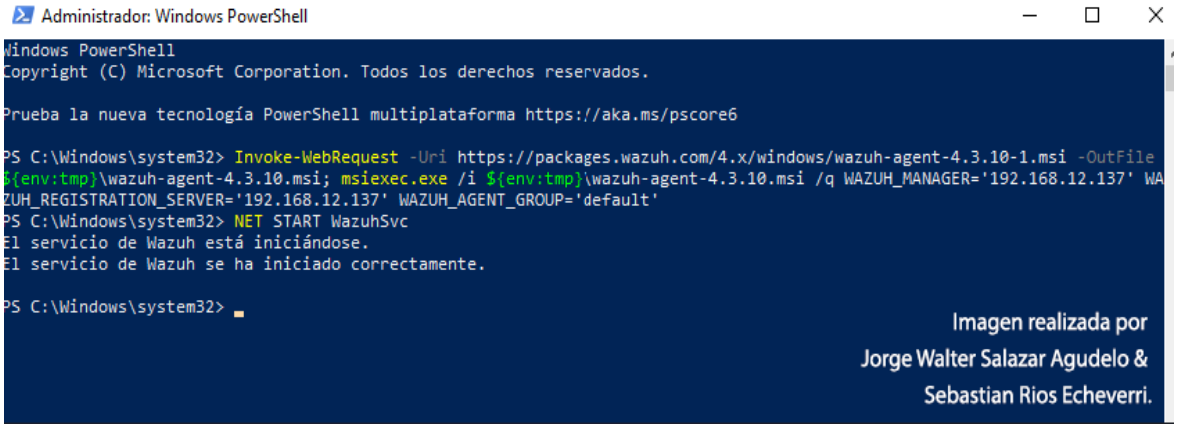


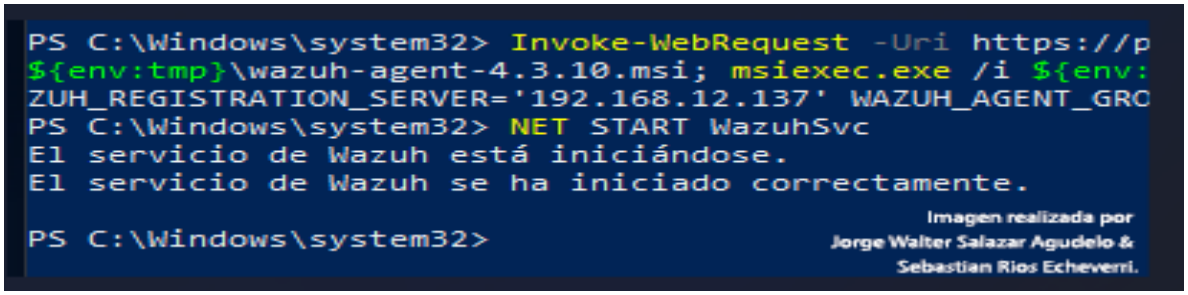
d. comando a ejecutar en powershell: lo ejecutamos en windows

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.10-1.msi -OutFile ${env:tmp}\wazuh-agent-4.3.10.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.10.msi /q WAZUH_MANAGER='192.168.12.137' WAZUH_REGISTRATION_SERVER='192.168.12.137' WAZUH_AGENT_GROUP='default'
```

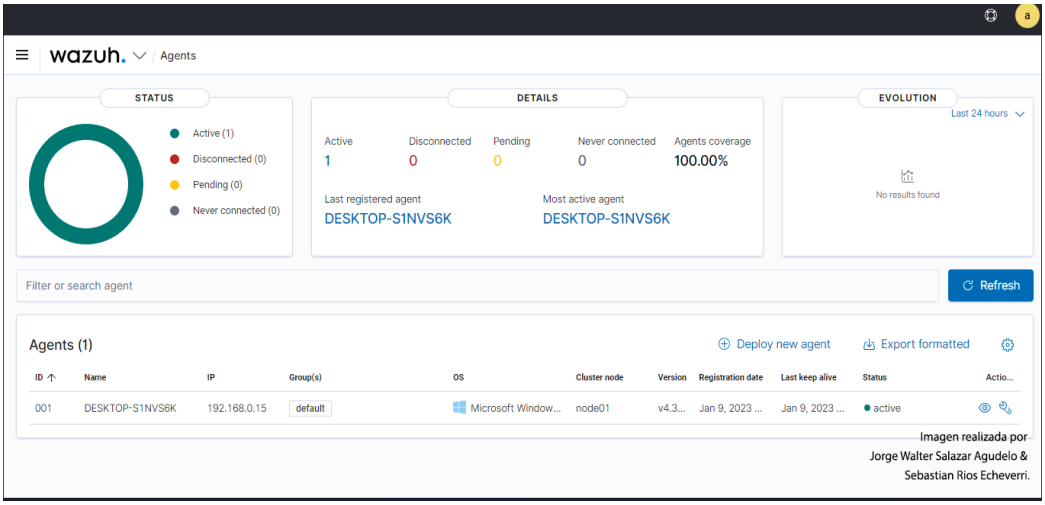
e. iniciamos el agente

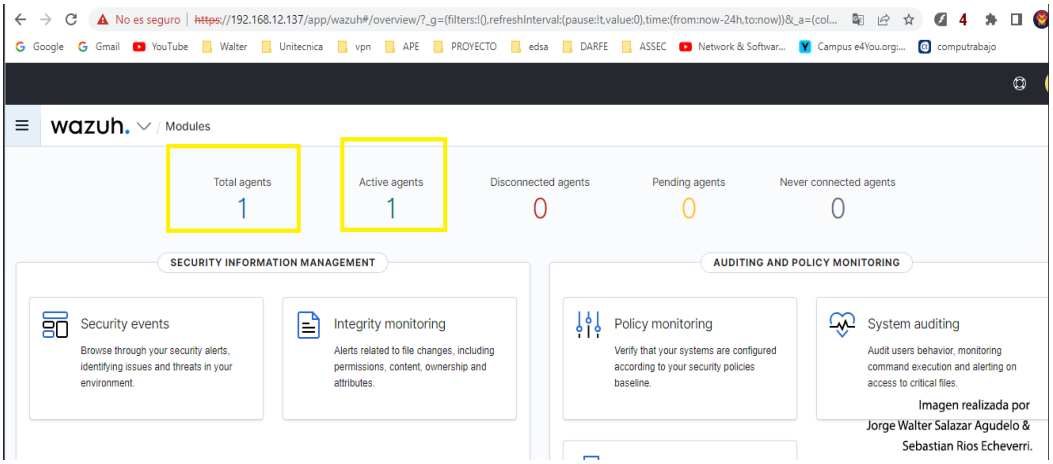
```
NET START WazuhSvc
```



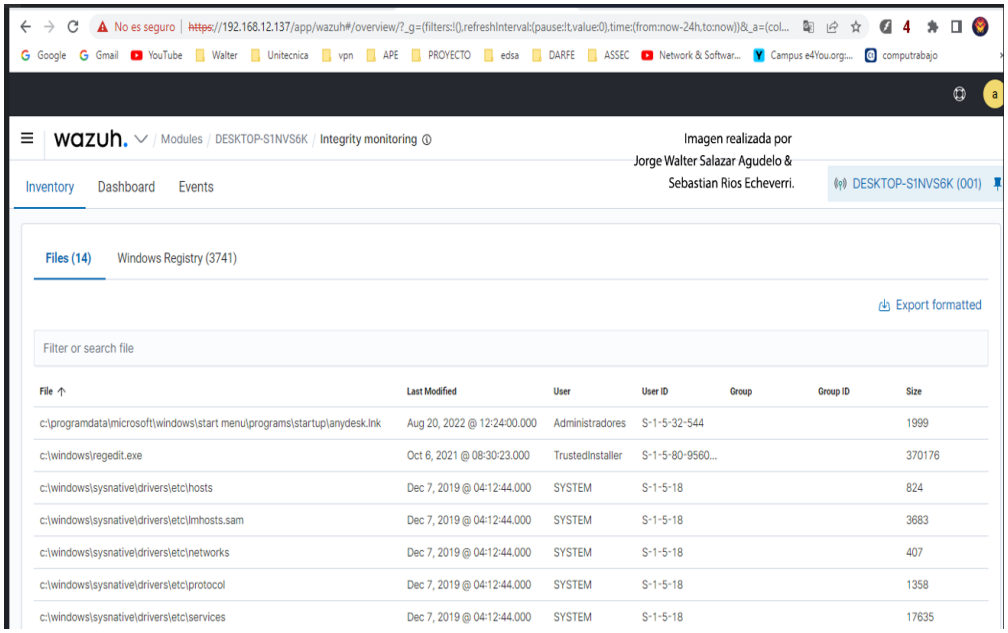


f. vamos a la consola de wazuh y miramos si el agente se instalo y si ya lo podemos detectar


wazuh. / Agents
STATUS
Active (1)
Disconnected (0)
Pending (0)
Never connected (0)
DETAILS
Active 1
Disconnected 0
Pending 0
Never connected 0
Agents coverage 100.00%
Last registered agent DESKTOP-S1NVS6K
Most active agent DESKTOP-S1NVS6K
EVOLUTION
Last 24 hours
No results found
Filter or search agent
Refresh
Agents (1)
Deploy new agent
Export formatted
ID Name IP Group(s) OS Cluster node Version Registration date Last keep alive Status Actio...
001 DESKTOP-S1NVS6K 192.168.0.15 default Microsoft Window... node01 v4.3... Jan 9, 2023 ... Jan 9, 2023 ... active
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri.


No es seguro | https://192.168.12.137/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(col...
Google Gmail YouTube Walter Unitecnica vpn APE PROYECTO edsa DARFE ASSEC Network & Softwar... Campus e4You.org:... computrabajo
wazuh. / Modules
Total agents 1
Active agents 1
Disconnected agents 0
Pending agents 0
Never connected agents 0
SECURITY INFORMATION MANAGEMENT
Security events
Browse through your security alerts, identifying issues and threats in your environment.
Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.
AUDITING AND POLICY MONITORING
Policy monitoring
Verify that your systems are configured according to your security policies baseline.
System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri.

Inventory



El proceso de instalación ahora está completo y el agente de Wazuh se instaló correctamente en su terminal de Windows.

Conectividad saliente desde el agente de Wazuh a los servicios del administrador de Wazuh.

Los siguientes puertos son configurables:

1514/TCP para comunicación con agentes.

1515/TCP para inscripción mediante solicitud automática de agente.

55000/TCP para la inscripción a través de la API del administrador.

Nota Puede encontrar instrucciones para instalar e inscribir agentes en el panel de control de Wazuh utilizando las variables de implementación. Vaya a Wazuh > Agentes y haga clic en Implementar nuevo agente.

Solución de problemas

Consulte la sección Solución de problemas para obtener detalles sobre cómo probar la conectividad entre el agente y el administrador.

https://documentation.wazuh.com/current/user-manual/agent-enrollment/troubleshooting.html

Probando conectividad con el gerente de Wazuh desde windows:

https://documentation.wazuh.com/current/user-manual/agent-enrollment/troubleshooting.html#troubleshooting-testing-communication

En Windows, abra una terminal de PowerShell y ejecute el siguiente comando:

```
(new-object Net.Sockets.TcpClient).Connect("<MANAGER_IP>", 1514)
(new-object Net.Sockets.TcpClient).Connect("<MANAGER_IP>", 1515)
(new-object Net.Sockets.TcpClient).Connect("<MANAGER_IP>", 55000)
```

Si hay conectividad, no hay salida, de lo contrario, se muestra un error:

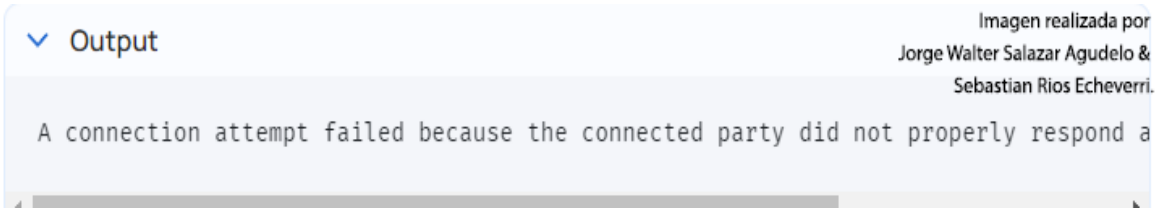


Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri.

De forma predeterminada, todos los archivos del agente se almacenan después de la instalación.

C:\Program Files (x86)\ossec-agent

Desinstalar un agente de Wazuh

Para desinstalar el agente, se requiere el archivo de instalación original de Windows para realizar el proceso desatendido:

```
msiexec.exe /x wazuh-agent-4.3.10-1.msi /qn
```

El agente de Wazuh ahora está completamente eliminado de su terminal de Windows.

El agente de Wazuh ahora está completamente eliminado de su terminal de Windows.

Monitoreo Ataque Man-In-The-Middle

Un ataque de "Man-in-the-middle" (MITM) es un tipo de ataque informático en el que un atacante intercepta la comunicación entre dos partes y se posiciona en el medio para escuchar, alterar o manipular la información que se está transmitiendo.

pueden ser particularmente peligrosos en situaciones en las que se transmiten información confidencial, como nombres de usuario y contraseñas, información financiera o de tarjetas de crédito, o cualquier otra información privada.

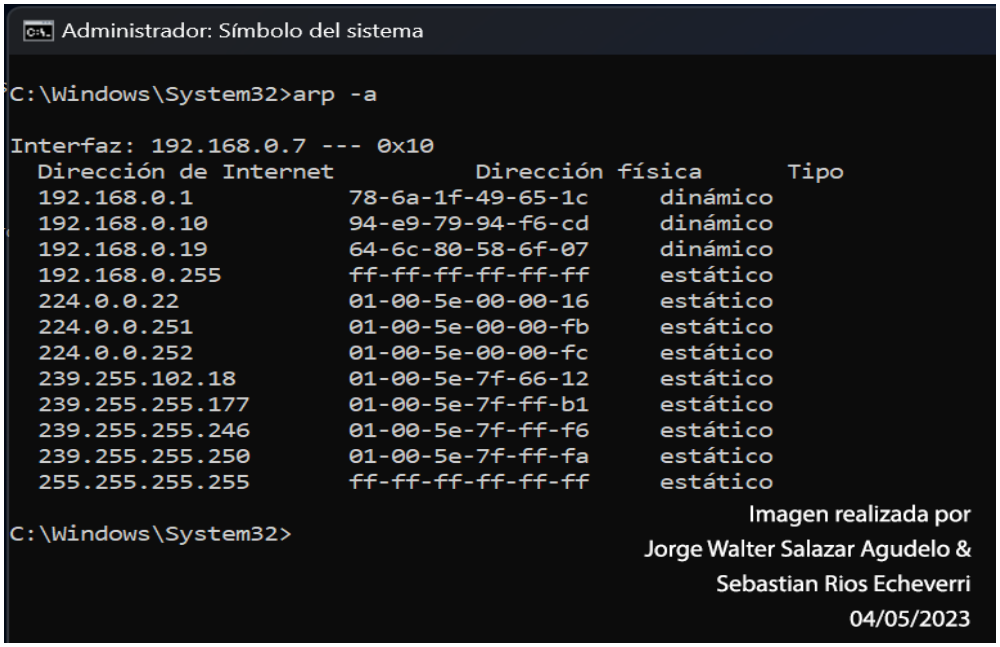
Escenario infraestructura:

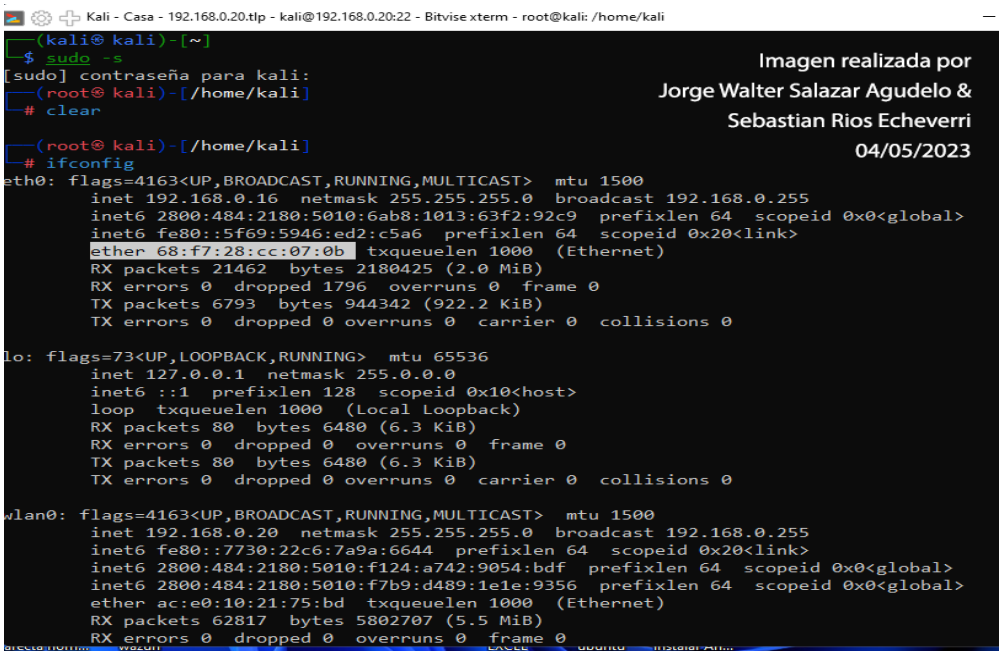
UBUNTU 22.04	Wazuh – 192.168.0.10
WINDOWS 11	Victima – 192.168.0.7
KALI 2023.1	Atacante – 192.168.0.16 eth0 y 192.168.0.20 wlan0
ROUTER (IPS)	192.168.0.1

Emulación del ataque:

En Windows revisamos las Mac de los equipos en la red; específicamente la Mac del router 192.168.0.1 que para este caso es : 78-6a-1f-49-65-1c

```
arp -a
```





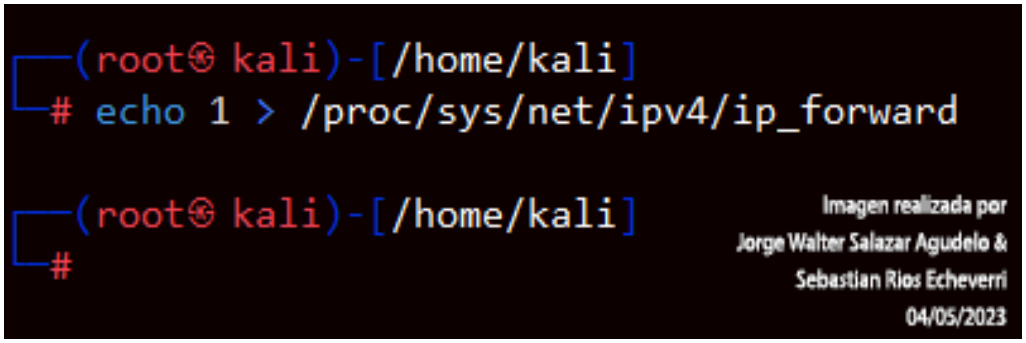
1. Verificamos que en Kali que el forward esté habilitado.

```
sudo -s
cat /proc/sys/net/ipv4/ip_forward
```

sí da 1 está habilitado:

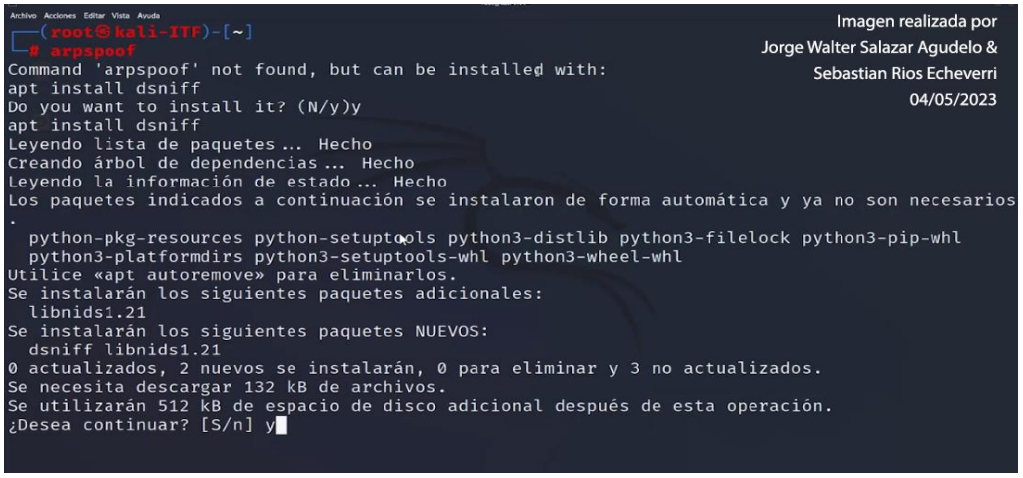
En caso de que no esté habilitado nos da 0, lo habilito:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```



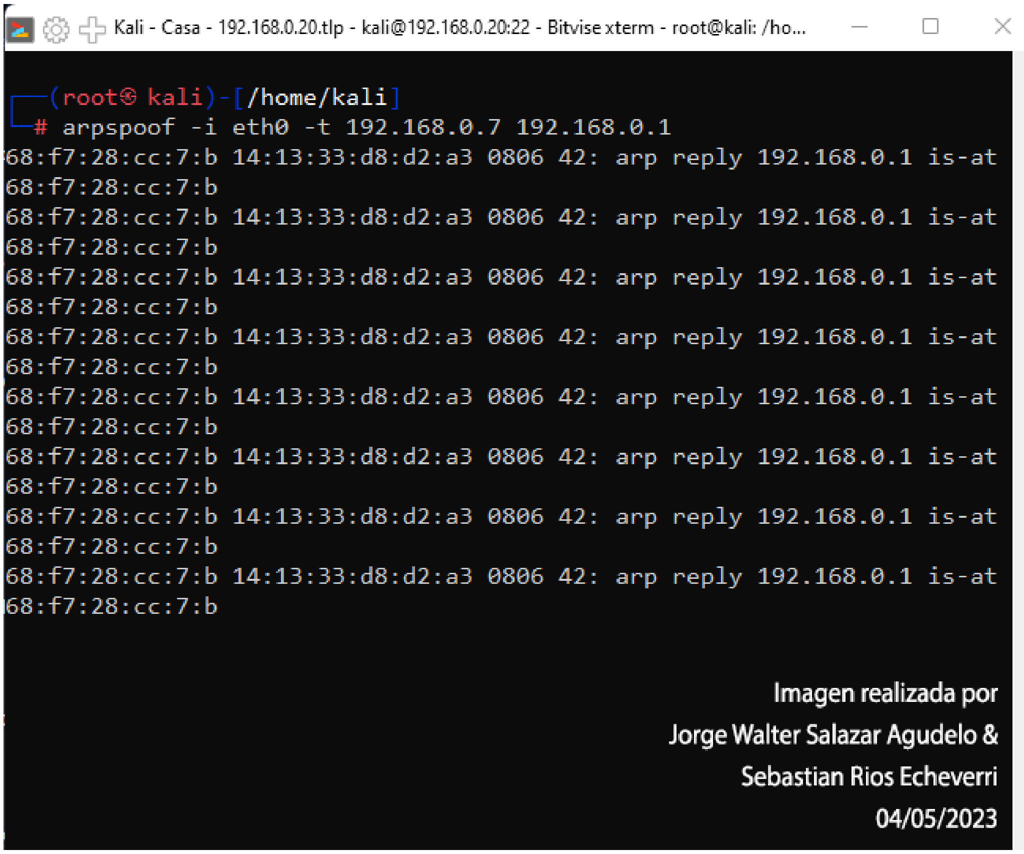
Instalamos arpspoof, sino tenemos instalado el paquete dsniff lo instalamos.

```
apt install dsniff
```



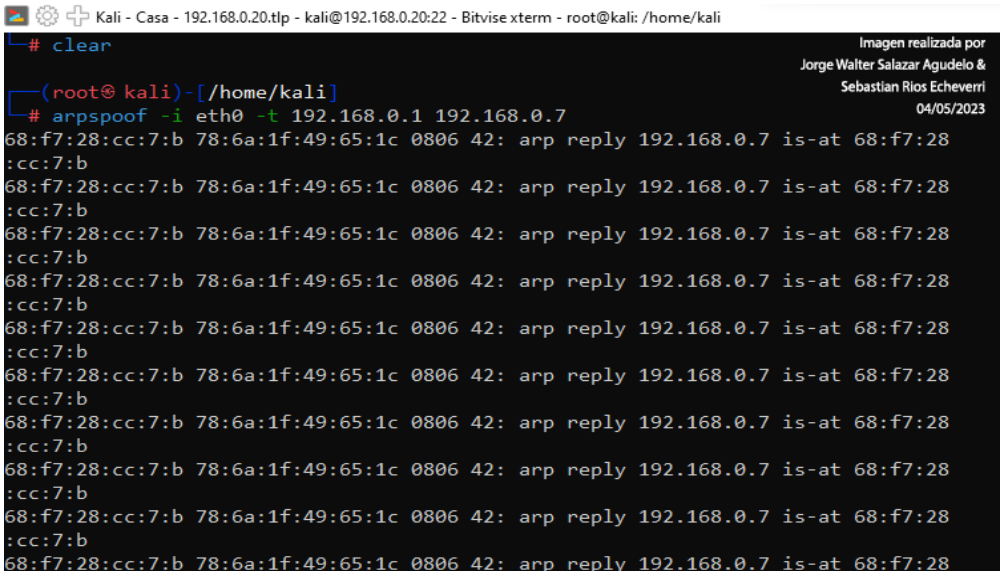
Victima -->> lanzamos el ataque a la víctima para hacerle creer que el Kali es el Router.

```
arpspoof -i eth0 -t 192.168.0.7 192.168.0.1
```

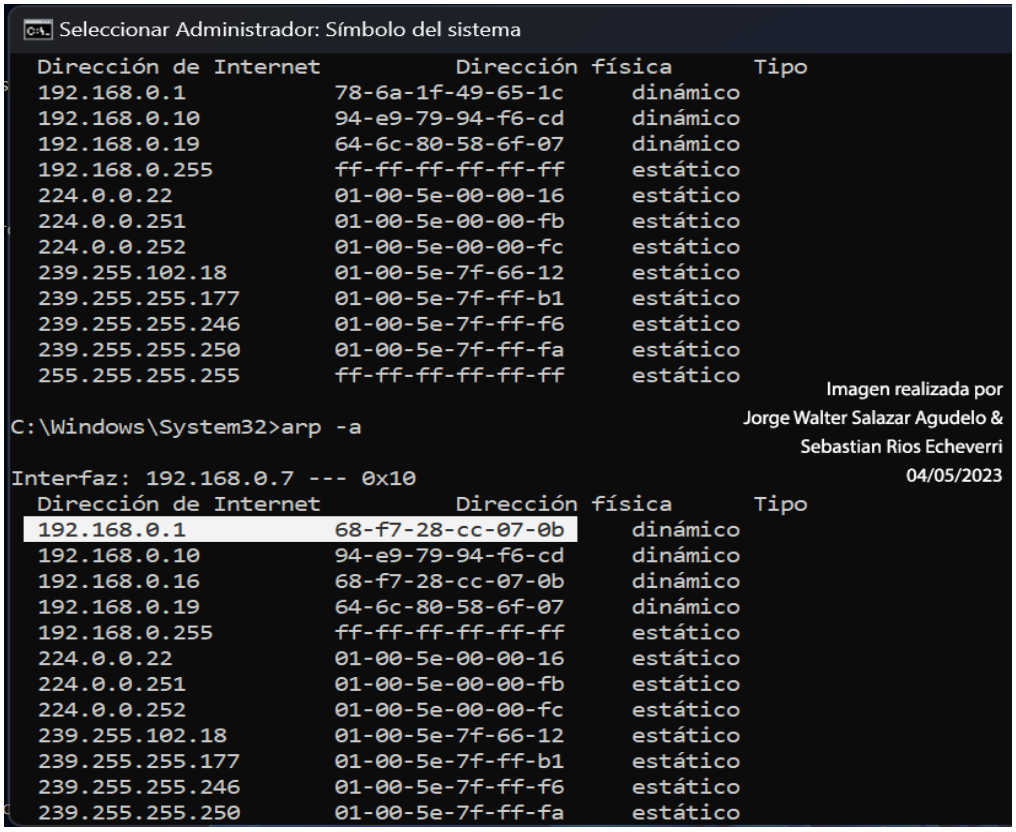


Router--> en otra terminal diferente, Lanzo el ataque al router para hacerle creer que al Kali es el equipo víctima, de esta manera Kali quedara entre los equipos router y victima interceptando la comunicación entre las dos partes.

```
sudo -s
arpspoof -i eth0 -t 192.168.0.1 192.168.0.7
```

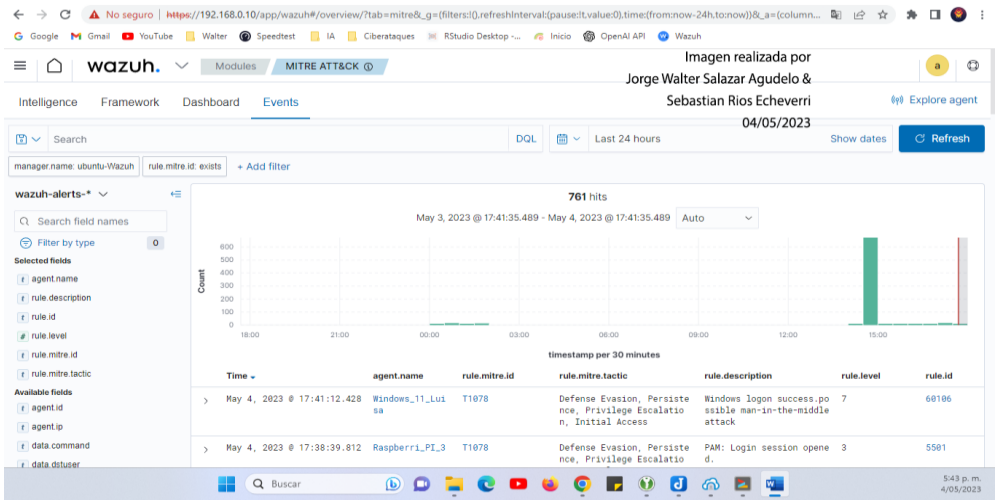


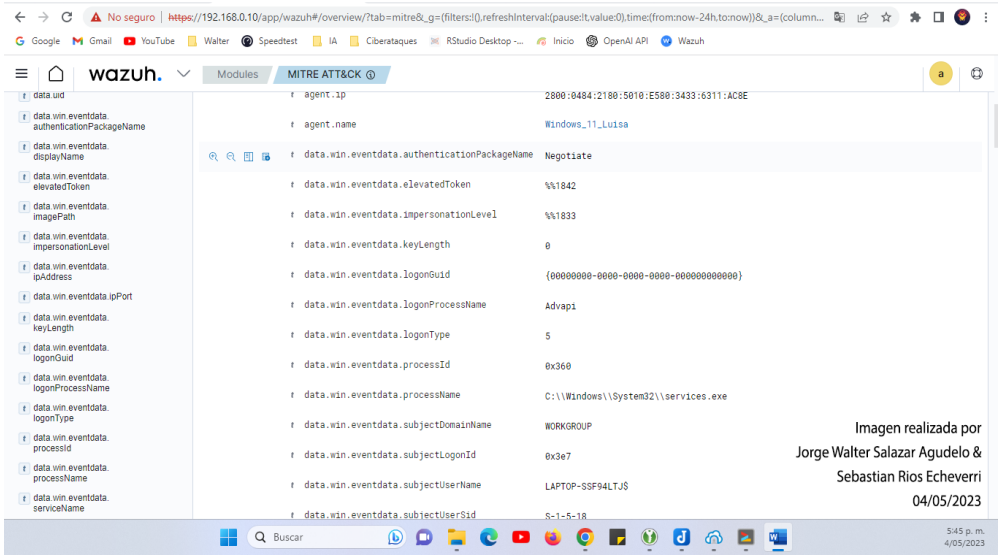
Windows : verificamos la MAC de router nuevamente y después del ataque , verificamos que el router ya no tiene la Mac anteriormente mencionada sino que ya el router tiene la Mac de la tarjeta eth0 de Kali - 192.168.0.1 - 68-f7-28-cc-07-0b

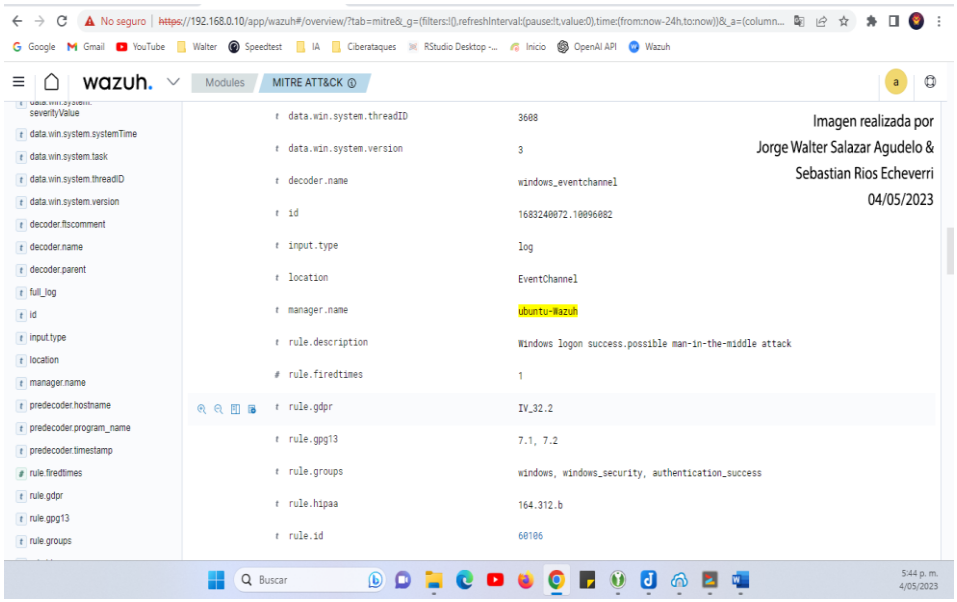


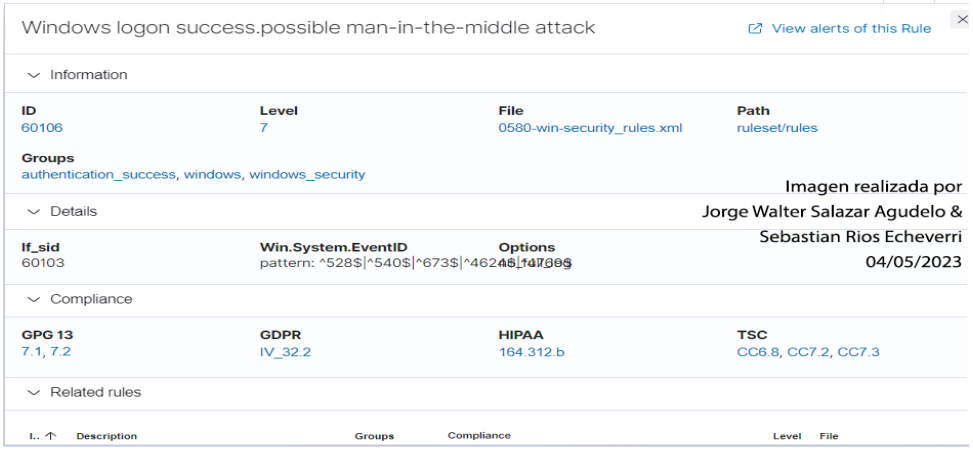
Lo que nos indica que la maquina Kali esta de intermediario entre Windows (victima) y el router (IPS) , en este momento se está ejecutando el ataque MAN-IN-THE-MIDDLE, ya el atacante entrará a capturar la información con herramientas como wireshark.

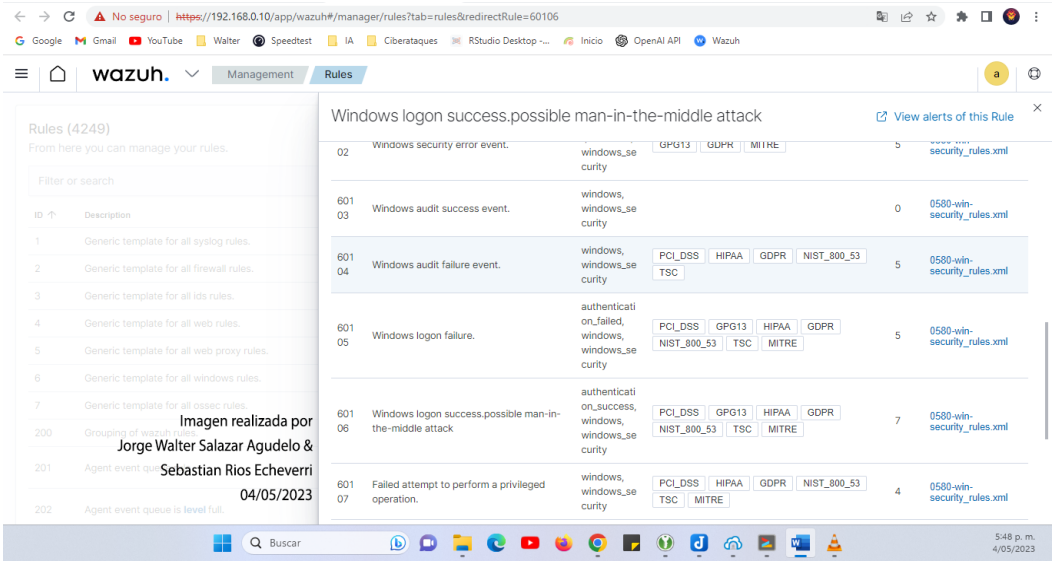
Monitorización en Wazuh

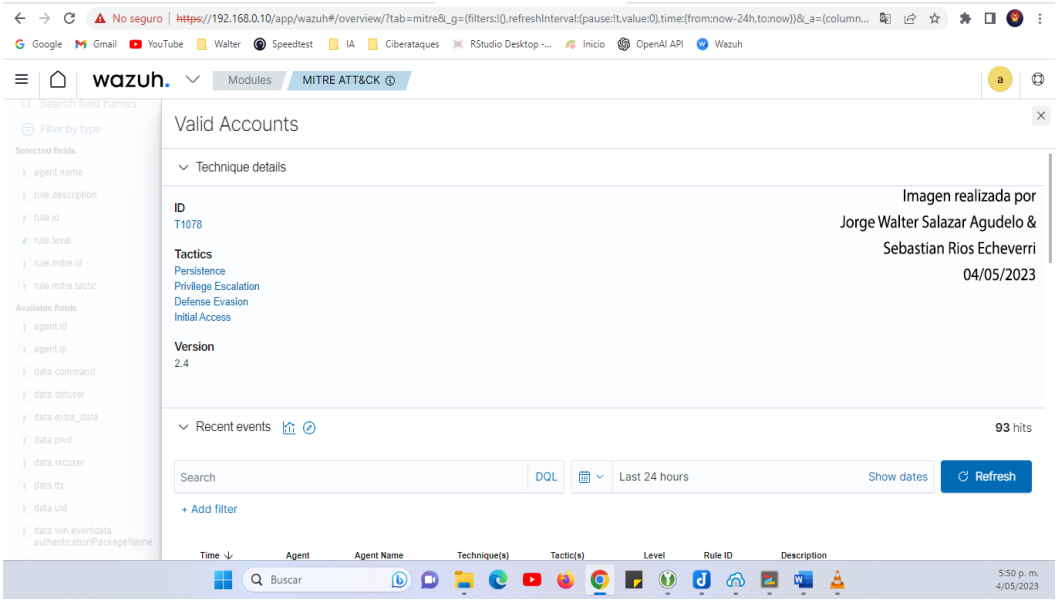





wazuh.
Modules
MITRE ATT&CK
data.win.system.threadID 3608
data.win.system.version 3
decoder.name windows_eventchannel
id 1683240072.10096082
input.type log
location EventChannel
manager.name ubuntu-illazuh
rule.description Windows logon success.possible man-in-the-middle attack
rule.firedtimes 1
rule.gdpr IV_32.2
rule.gpg13 7.1, 7.2
rule.groups windows, windows_security, authentication_success
rule.hipaa 164.312.b
rule.id 60106
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023


Windows logon success.possible man-in-the-middle attack
View alerts of this Rule
Information
ID 60106
Level 7
File 0580-win-security_rules.xml
Path ruleset/rules
Groups authentication_success, windows, windows_security
Details
If_sid 60103
Win.System.EventID pattern: ^528$|^540$|^673$|^462
Options
Compliance
GPG 13 7.1, 7.2
GDPR IV_32.2
HIPAA 164.312.b
TSC CC6.8, CC7.2, CC7.3
Related rules
Description
Groups
Compliance
Level
File
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023


wazuh.
Management
Rules
Windows logon success.possible man-in-the-middle attack
View alerts of this Rule
Rules (4249)
Windows audit success event.
Windows audit failure event.
Windows logon failure.
Windows logon success.possible man-in-the-middle attack
Failed attempt to perform a privileged operation.
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023


wazuh.
Modules
MITRE ATT&CK
Valid Accounts
Technique details
ID
T1078
Tactics
Persistence
Privilege Escalation
Defense Evasion
Initial Access
Version
2.4
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023
Recent events
93 hits
Search
DQL
Last 24 hours
Show dates
Refresh
+ Add filter

Monitoreo Ataque Dos

Un ataque de Denegación de Servicio (DoS) es un intento malintencionado de inundar un servidor, servicio o red con tráfico inútil o sobrecargarlo con solicitudes para que no pueda responder a solicitudes legítimas de los usuarios. Este tipo de ataques pueden afectar el rendimiento y la disponibilidad de la red.

Un ataque DoS se puede dirigir a un servidor o dispositivo dentro de la red, como un enrutador o un switch, con el objetivo de interrumpir la comunicación de los usuarios o provocar fallos en los sistemas.

Escenario infraestructura:

UBUNTU 22.04	Wazuh – 192.168.0.10
WINDOWS 11	Victima – 192.168.0.7
KALI 2023.1	Atacante – 192.168.0.16 eth0 y 192.168.0.20 wlan0

Emulación del ataque:

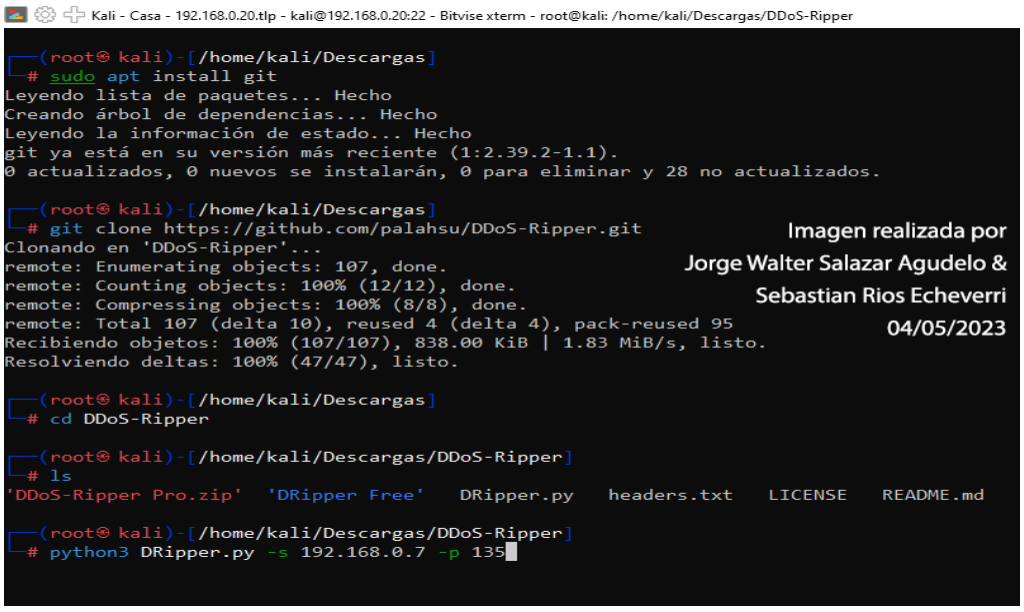
En Windows haremos seguimiento al rendimiento en el equipo 192.168.0.7 para ver el comportamiento al iniciar el ataque

Utilizaremos DDos Ripper

https://github.com/palahsu/DDoS-Ripper

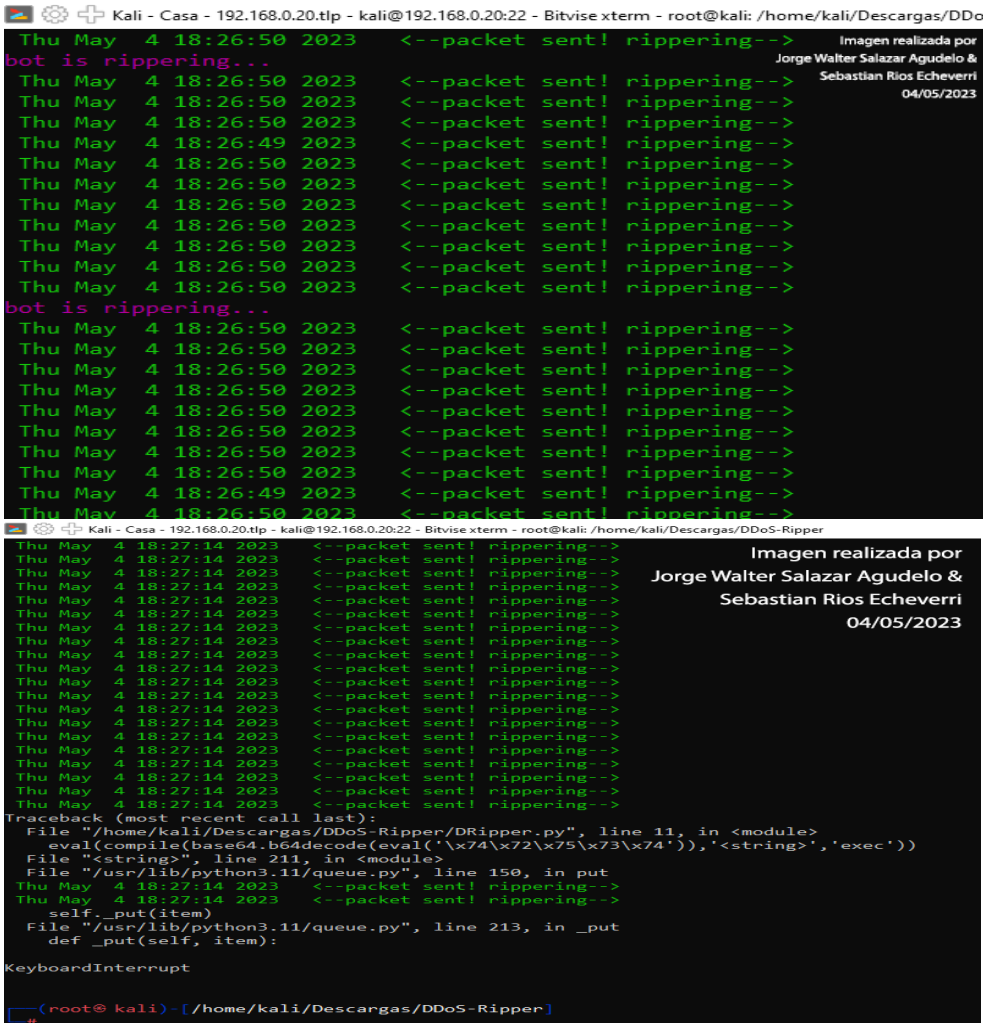
Instalamos en Kali DDos Ripper el Linux basadas en Debian

```
sudo apt install git
git clone https://github.com/palahsu/DDoS-Ripper.git
cd DDoS-Ripper
ls
python3 DRipper.py   o  python2 DRipper.py
```



Lanzamos el ataque DDos a el equipo victima 192.168.0.7

python3 DRipper.py -s 192.168.0.7 -p 135

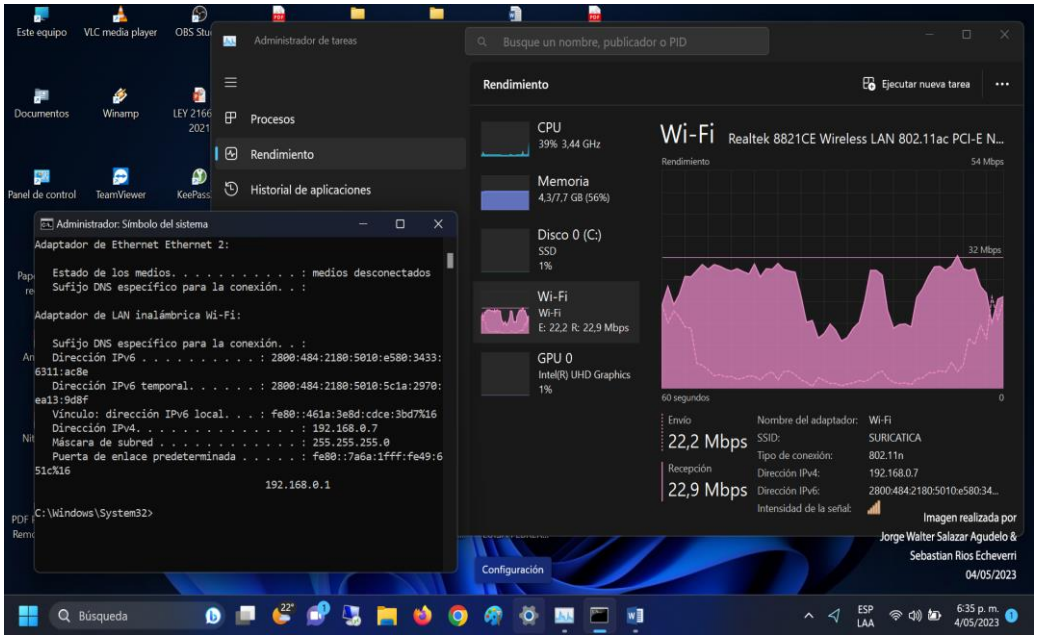


También podemos hacer un ping para provocar el ataque DOS desde Kali

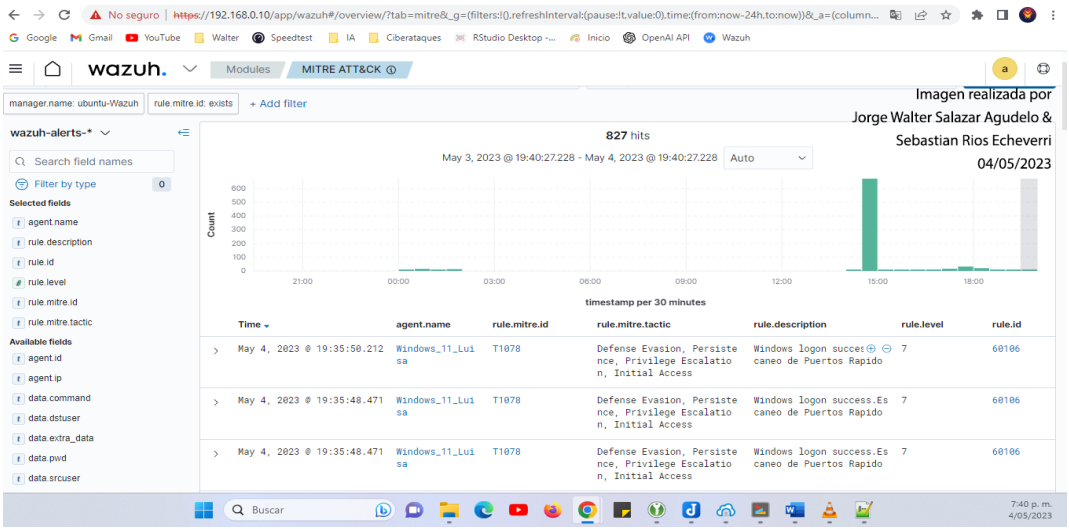
```
sudo ping -s 8192 -i 0.0001 192.168.0.7
```

```
Kali - Casa - 192.168.0.20.tlp - kali@192.168.0.20:22 - Bitvise xterm - root@kali: /home/kali/Descargas/DDoS-Ripper
└─# clear

┌──(root㉿kali)-[/home/kali/Descargas/DDoS-Ripper]
└─# sudo ping -s 8192 -i 0.0001 192.168.0.7
PING 192.168.0.7 (192.168.0.7) 8192(8220) bytes of data.
8200 bytes from 192.168.0.7: icmp_seq=1 ttl=128 time=4.15 ms
8200 bytes from 192.168.0.7: icmp_seq=2 ttl=128 time=5.12 ms
8200 bytes from 192.168.0.7: icmp_seq=3 ttl=128 time=4.95 ms
8200 bytes from 192.168.0.7: icmp_seq=4 ttl=128 time=5.49 ms
8200 bytes from 192.168.0.7: icmp_seq=5 ttl=128 time=7.73 ms
8200 bytes from 192.168.0.7: icmp_seq=6 ttl=128 time=8.50 ms
8200 bytes from 192.168.0.7: icmp_seq=7 ttl=128 time=6.80 ms
8200 bytes from 192.168.0.7: icmp_seq=8 ttl=128 time=10.9 ms
8200 bytes from 192.168.0.7: icmp_seq=9 ttl=128 time=5.81 ms
8200 bytes from 192.168.0.7: icmp_seq=10 ttl=128 time=14.3 ms
8200 bytes from 192.168.0.7: icmp_seq=11 ttl=128 time=5.64 ms
8200 bytes from 192.168.0.7: icmp_seq=12 ttl=128 time=4.81 ms
8200 bytes from 192.168.0.7: icmp_seq=13 ttl=128 time=20.2 ms
8200 bytes from 192.168.0.7: icmp_seq=14 ttl=128 time=7.98 ms
8200 bytes from 192.168.0.7: icmp_seq=15 ttl=128 time=4.96 ms
8200 bytes from 192.168.0.7: icmp_seq=16 ttl=128 time=9.69 ms
8200 bytes from 192.168.0.7: icmp_seq=17 ttl=128 time=6.61 ms
8200 bytes from 192.168.0.7: icmp_seq=18 ttl=128 time=4.94 ms
8200 bytes from 192.168.0.7: icmp_seq=19 ttl=128 time=7.97 ms
8200 bytes from 192.168.0.7: icmp_seq=20 ttl=128 time=4.52 ms
8200 bytes from 192.168.0.7: icmp_seq=21 ttl=128 time=10.3 ms
8200 bytes from 192.168.0.7: icmp_seq=22 ttl=128 time=8.20 ms
8200 bytes from 192.168.0.7: icmp_seq=23 ttl=128 time=17.7 ms
8200 bytes from 192.168.0.7: icmp_seq=24 ttl=128 time=5.60 ms
8200 bytes from 192.168.0.7: icmp_seq=25 ttl=128 time=9.71 ms
```

Observamos los recursos de Windows consumidos por el ataque



Monitorización en Wazuh



La regla 60106 de Wazuh se refiere a la detección de "scan de puertos rápido". Esta regla se activa cuando se detectan múltiples intentos de conexión a diferentes puertos en un corto período de tiempo desde la misma dirección IP.

Aunque esta regla no se enfoca específicamente en los ataques de denegación de servicio (DoS), podría indicar que alguien está intentando escanear los puertos de un sistema para encontrar vulnerabilidades o puertos abiertos. En algunos casos, los escaneos de puertos pueden ser un precursor de un ataque DoS o de otro tipo de ataque más avanzado.

Clasificación de Reglas:

Las reglas se clasifican en varios niveles, desde el más bajo (0) hasta el más alto (16). Algunos niveles están actualmente sin usar. La siguiente tabla describe cada alerta, lo que puede ayudar a comprender la gravedad de cada advertencia activada o crear una regla personalizada.

Nivel	Título	Descripción
0	Ignorado	No se ha tomado ninguna medida. Se utiliza para evitar falsos positivos. Estas reglas se escanean antes que todas las demás. Incluya eventos sin relevancia de seguridad.
2	Notificación de baja prioridad del sistema	Notificación del sistema o mensajes de estado. Estos no tienen relevancia de seguridad.
3	Eventos exitosos/autorizados	Estos incluyen intentos de inicio de sesión exitosos, eventos de permiso de firewall, etc.

Documentación Wazuh. (2023, 02 de mayo). Página oficial de wazuh [captura de pantalla]. Tomado de https://documentation.wazuh.com/current/user-manual/ruleset/rules-classification.html#rules-classification

4	Error de prioridad baja del sistema	Errores relacionados con configuraciones incorrectas o dispositivos/aplicaciones no utilizados. Estos no tienen relevancia de seguridad y generalmente son causados por instalaciones predeterminadas o pruebas de software.
5	Error generado por el usuario	Estos incluyen contraseñas perdidas, acciones denegadas, etc. Por sí mismos, estos no tienen relevancia de seguridad.
6	Ataque de baja relevancia	Estos indican un gusano o un virus que no afecta al sistema (como el código rojo para servidores apache, etc.). Estos también incluyen eventos IDS frecuentes y errores frecuentes.
7	Coincidencia de "mala palabra"	Estos incluyen palabras como "malo", "error", etc. Estos eventos son la mayoría de las veces no clasificados y pueden tener cierta relevancia de seguridad.

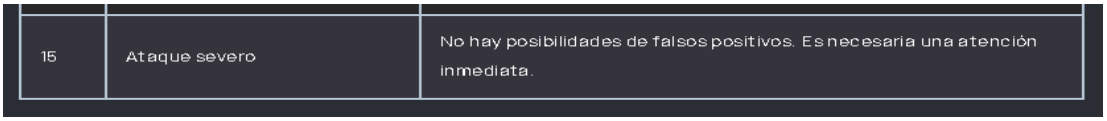
Documentación Wazuh. (2023, 02 de mayo). Página oficial de wazuh [captura de pantalla]. Tomado de https://documentation.wazuh.com/current/user-manual/ruleset/rules-classification.html#rules-classification

8	Primera vez visto	Incluye eventos vistos por primera vez. La primera vez que se activa un evento IDS o la primera vez que un usuario inicia sesión. También incluye acciones relevantes para la seguridad (como el inicio de un sniffer o algo así).
9	Error de origen no válido	Incluya los intentos de iniciar sesión como usuario desconocido o desde una fuente no válida. Puede tener relevancia para la seguridad (especialmente si se repite). Estos también incluyen errores relacionados con la cuenta "admin" (root).
10	Múltiples errores generados por el usuario	Estos incluyen múltiples contraseñas incorrectas, múltiples inicios de sesión fallidos, etc. Estos pueden indicar un ataque o simplemente pueden ser que un usuario acaba de olvidar sus credenciales.

Documentación Wazuh. (2023, 02 de mayo). Página oficial de wazuh [captura de pantalla]. Tomado de https://documentation.wazuh.com/current/user-manual/ruleset/rules-classification.html#rules-classification

11	Advertencia de comprobación de integridad	Estos incluyen mensajes relacionados con la modificación de binarios o la presencia de rootkits (por Rootcheck). Estos pueden indicar un ataque exitoso. También se incluyeron eventos IDS que serán ignorados (alto número de repeticiones).
12	Evento de gran importancia	Estos incluyen mensajes de error o advertencia del sistema, kernel, etc. Estos pueden indicar un ataque contra una aplicación específica.
13	Error inusual (alta importancia)	La mayoría de las veces coincide con un patrón de ataque común.
14	Evento de seguridad de gran importancia	La mayoría de las veces se hace con correlación e indica un ataque.

Documentación Wazuh. (2023, 02 de mayo). Página oficial de wazuh [captura de pantalla]. Tomado de https://documentation.wazuh.com/current/user-manual/ruleset/rules-classification.html#rules-classification



15	Ataque severo	No hay posibilidades de falsos positivos. Es necesaria una atención inmediata.

Documentación Wazuh. (2023, 02 de mayo). Página oficial de wazuh [captura de pantalla]. Tomado de https://documentation.wazuh.com/current/user-manual/ruleset/rules-classification.html#rules-classification

Políticas de seguridad que se generan ante los resultados obtenidos en wazuh:

Para prevenir y mitigar los ataques MITM, es fundamental implementar las políticas de seguridad adecuadas para proteger los sistemas y la información de una organización. Se pueden tomar varias medidas:

- ***Encriptación de datos:*** La empresa debería asegurarse de que toda la información sensible se encuentra encriptada para protegerla de posibles interceptaciones en el futuro.
- ***Autenticación de usuarios:*** La empresa debería implementar medidas para garantizar la autenticación de los usuarios, como contraseñas seguras o autenticación de dos factores.
- ***Actualizaciones de software:*** La empresa debería asegurarse de que todos los dispositivos y programas utilizados estén actualizados con las últimas versiones de seguridad, ya que estas actualizaciones suelen incluir parches para vulnerabilidades conocidas. Mantener su software actualizado es esencial para evitar que los atacantes exploten las vulnerabilidades conocidas. Los parches de seguridad y las actualizaciones de software deben aplicarse lo antes posible.
- ***Uso de redes seguras:*** La empresa debería utilizar redes seguras, como VPN, para proteger las comunicaciones entre sus dispositivos.

- ***Capacitación de empleados:*** La empresa debería capacitar a sus empleados en la prevención de ataques de "Hombre en el medio" y en las mejores prácticas de seguridad informática en general.
- ***Monitoreo de la red:*** La empresa debería implementar medidas de monitoreo de red para detectar posibles intentos de ataque y responder a ellos de manera oportuna.
- ***Plan de contingencia:*** La empresa debería tener un plan de contingencia en caso de que se produzca otro ataque de "Hombre en el medio". Esto podría incluir medidas como la desconexión de dispositivos afectados, la notificación a las autoridades competentes y la evaluación del daño potencial.
- ***Implementar encriptación de extremo a extremo:*** esta medida protege la información transmitida con encriptación. Cuando se implementa el cifrado de extremo a extremo, la información solo puede ser descifrada por el destinatario previsto y no puede ser interceptada por un atacante.
- ***Autenticación fuerte.*** Es importante implementar una autenticación sólida para que los intrusos no puedan acceder a su información con credenciales robadas o falsificadas. Debe implementar políticas de contraseñas seguras, autenticación multifactor (MFA) y otros métodos de autenticación seguros.
- ***Red Privada Virtual (VPN).*** Una VPN es una red privada que se utiliza para conectar dispositivos de forma segura a través de Internet. La información enviada a través de la VPN está encriptada y no puede ser interceptada por un atacante.
- ***Inspección de tráfico***: es importante implementar medidas de control de tráfico para detectar y prevenir ataques MITM. Las soluciones de seguridad como los sistemas de

prevención de intrusiones (IPS) y los sistemas de detección de intrusiones (IDS) pueden detectar y bloquear ataques MITM.

- ***Política de seguridad de la red.*** Las políticas de ciberseguridad deben ser lo suficientemente fuertes para prevenir ataques MITM. Algunas de las políticas que se pueden implementar incluyen la segmentación de la red, el monitoreo de actividades sospechosas y la aplicación de políticas de acceso a la red.

Estas son solo algunas de las políticas de seguridad que podrían implementarse después de un ataque de "Hombre en el medio" - “Man in the middle”. Es importante recordar que la seguridad informática es un proceso continuo y que la empresa debería estar constantemente evaluando y mejorando sus medidas de seguridad para mantenerse protegida contra posibles amenazas.

Cabe señalar que la prevención y mitigación de ataques MITM es un esfuerzo continuo y que las políticas de seguridad deben actualizarse y ajustarse a medida que surgen nuevas amenazas y vulnerabilidades.

- ***Reforzamiento de la infraestructura:*** La empresa debería fortalecer su infraestructura de red para resistir futuros ataques DDoS. Esto podría incluir la implementación de firewalls, sistemas de detección y prevención de intrusiones (IDP), sistemas de mitigación DDoS y la implementación de un plan de continuidad de negocio para garantizar que la empresa pueda seguir funcionando durante un ataque.

- ***Servicio de protección DDoS:*** La empresa debería considerar contratar un servicio de protección DDoS que pueda detectar y mitigar los ataques DDoS antes de que lleguen a su red.

- ***Monitoreo constante:*** La empresa debería monitorear continuamente su red para detectar y responder rápidamente a cualquier actividad sospechosa o anormal. Esto podría incluir la monitorización del tráfico de red, el monitoreo de la actividad de los usuarios y el análisis de registros de eventos.
- ***Plan de contingencia:*** La empresa debería tener un plan de contingencia en caso de que se produzca otro ataque DDoS. Esto podría incluir medidas como la desconexión de dispositivos afectados, la notificación a las autoridades competentes y la evaluación del daño potencial.
- ***Capacitación de empleados:*** La empresa debería capacitar a sus empleados en la prevención de ataques DDoS y en las mejores prácticas de seguridad informática en general.
- ***Actualizaciones de software:*** La empresa debería asegurarse de que todos los dispositivos y programas utilizados estén actualizados con las últimas versiones de seguridad, ya que estas actualizaciones suelen incluir parches para vulnerabilidades conocidas.
- ***Evaluación de terceros:*** La empresa debería evaluar la seguridad de cualquier proveedor o contratista que tenga acceso a su red para garantizar que no representen una amenaza para su seguridad.
- ***Configure el firewall y el sistema de filtrado de tráfico.*** Configure políticas de seguridad en estos sistemas para restringir el tráfico dentro y fuera de su organización.
- ***Desarrolle un plan de respuesta a ataques DDoS.*** Es muy importante que una organización tenga un plan de respuesta DDoS. Este plan debe incluir las acciones a realizar, la identificación de los responsables y la coordinación con los proveedores externos de servicios de seguridad (en caso de que la entidad cuente con ellos).

- ***Notifique a su proveedor de servicios de Internet (ISP).*** Los ISP pueden ayudar a mitigar los ataques DDoS al bloquear el tráfico malicioso.
- ***Bloquea el tráfico malicioso.*** Mediante el uso de sistemas de filtrado y firewalls, puede bloquear la transmisión de paquetes de tráfico dañinos a los sistemas de su organización.
- ***Capacitación del personal***. Capacite a los empleados para que reconozcan las amenazas de seguridad y respondan a los ataques DDoS.

Por ello, una política de seguridad frente a ataques DDoS es fundamental para proteger los sistemas informáticos de una organización. Tomar medidas preventivas antes, durante y después de una vulnerabilidad, son esenciales para proteger a una organización de los ataques DDoS.

RPO y RTO:

RPO: 1 hora

Es importante para la gestión de la continuidad del negocio la recuperación de desastres establecer el RPO basado y teniendo en cuenta la identificación de los datos y los sistemas críticos de la pyme, los cuales son necesarios para mantener la operación del negocio. Es importante también evaluar la frecuencia de los backups con que se realizan las copias de estos datos críticos, esto puede variar dependiendo de la criticidad de los datos y la frecuencia con las que se actualizan. Después de tener establecido esto, se puede generar un RPO adecuado.

RTO: 4 horas

Es el tiempo máximo que una organización está dispuesta a estar fuera de operación, sin afectar la continuidad del negocio.

Para establecer el RPO adecuado que permita a una pyme recuperar los datos y la funcionalidad esencial del negocio sin perder información crítica en caso de un ataque man in the

middle, puede ser establecido una vez se haya evaluado en diferentes aspectos, que varían dependiendo de la empresa.

Activos que afectan el DDOS y MITM en la red LAN de las pymes:

RIESGO	ACTIVO	RAZÓN
Un ataque hombre en el medio puede afectar a varios activos de una pyme, dependiendo de la naturaleza y el alcance del ataque. Algunos de los activos que pueden verse afectados por este tipo de ataque, que son:		
	Información confidencial	Si la empresa maneja información confidencial como contraseñas, información financiera o datos personales, un ataque MITM puede permitir que los atacantes tengan acceso a esa información.
	Datos sensibles	Un ataque hombre en el medio puede comprometer los datos sensibles de una pyme, como información financiera, contraseñas, información de clientes, Si estos datos caen en manos de un atacante, pueden ser utilizados para realizar actividades maliciosas.
	Sistemas de información	Un ataque hombre en el medio puede afectar los sistemas de información de una pyme, como servidores, bases de datos, aplicaciones web, etc. Si estos sistemas son comprometidos, pueden resultar en la interrupción de los servicios esenciales para la pyme.

MITM	**Reputación**	Un ataque hombre en el medio puede afectar la reputación de una pyme si se descubre que se ha comprometido la seguridad de sus sistemas o datos. La pérdida de confianza de los clientes y la mala publicidad pueden tener un impacto negativo en la imagen de la pyme.
	Cumplimiento normativo	Un ataque hombre en el medio puede afectar el cumplimiento normativo de una pyme si se comprometen datos sensibles que están protegidos por leyes y regulaciones específicas. La pyme puede enfrentar multas y sanciones si se descubre que no ha cumplido con estas normas.
Un ataque de denegación de servicios puede afectar a varios activos de una pyme, dependiendo de la naturaleza y el alcance del ataque. Algunos de los activos que pueden verse afectados por este tipo de ataque, que son:		
	Servicios en línea	Un ataque DOS puede afectar la disponibilidad de los servicios en línea de la pyme, como el sitio web, la tienda en línea, los sistemas de pago, entre otros. Si estos servicios no están disponibles, la pyme puede perder ingresos y clientes.
	Sistemas de información	Un ataque DOS puede afectar los sistemas de información de la pyme, como servidores, bases de datos, aplicaciones web, etc. Si estos sistemas son inundados con solicitudes maliciosas, pueden resultar en la interrupción de los servicios esenciales para la pyme.

DDOS	Reputación	Un ataque DOS puede afectar la reputación de una pyme si se descubre que no ha sido capaz de mantener la disponibilidad de sus servicios en línea. La pérdida de confianza de los clientes y la mala publicidad pueden tener un impacto negativo en la imagen de la pyme.
	Cumplimiento normativo	Un ataque DOS puede afectar el cumplimiento normativo de una pyme si se compromete la disponibilidad de servicios esenciales que están protegidos por leyes y regulaciones específicas. La pyme puede enfrentar multas y sanciones si se descubre que no ha cumplido con estas normas.

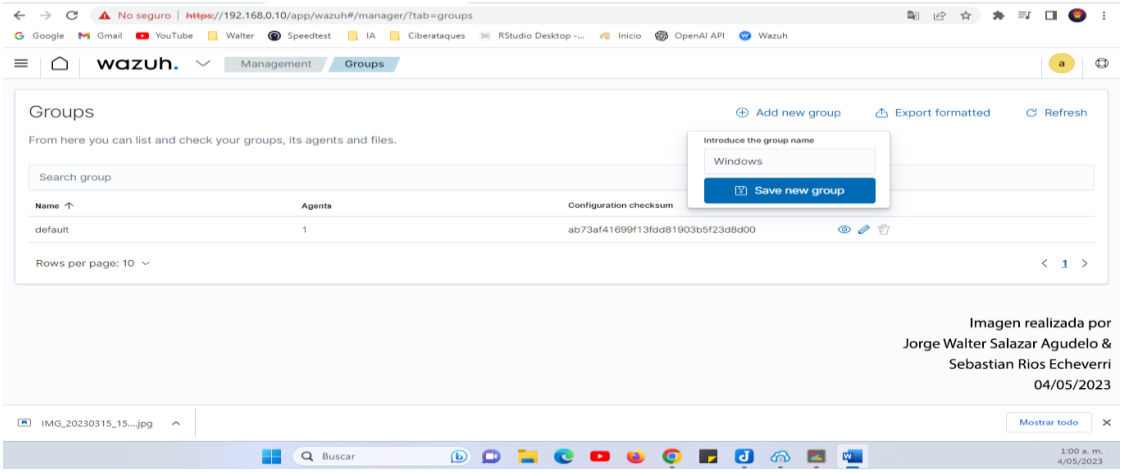
Para evaluar la experiencia de un administrador de redes ante los ataques DDOS y MITM, se pueden considerar los siguientes puntos:

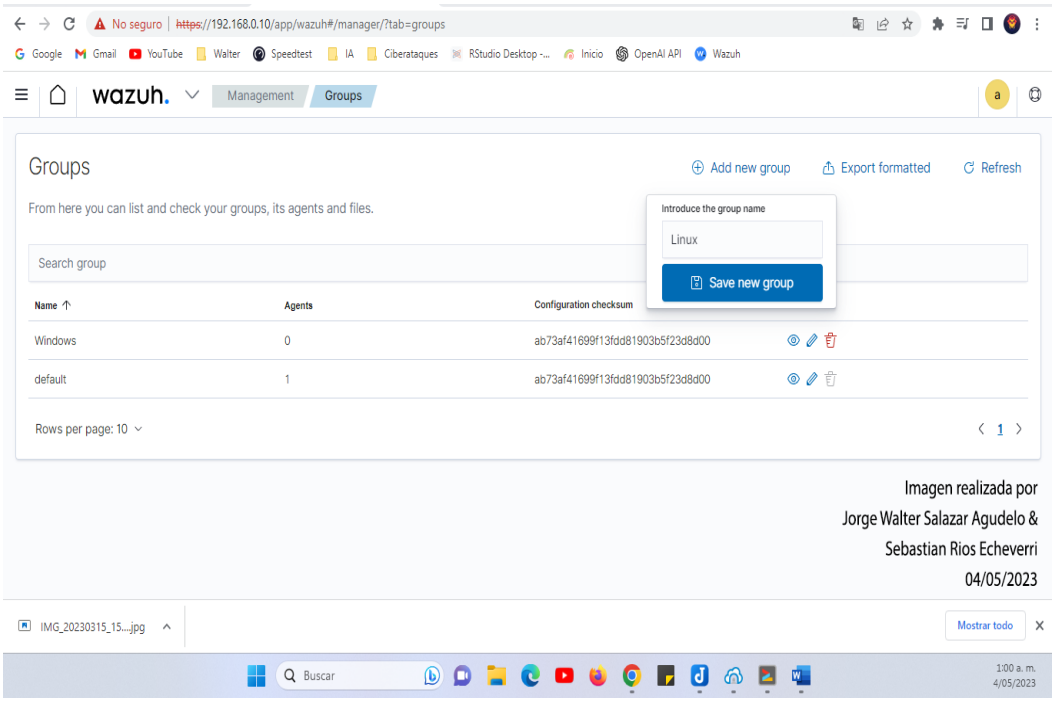
Administrador de Redes	
Experiencia	**Descripción**
Conocimiento técnico	Es importante que la persona encargada de evaluar la experiencia ante un ataque hombre en el medio tenga un conocimiento técnico sólido en el área de seguridad informática, incluyendo los conceptos básicos de redes, criptografía, sistemas operativos, etc.

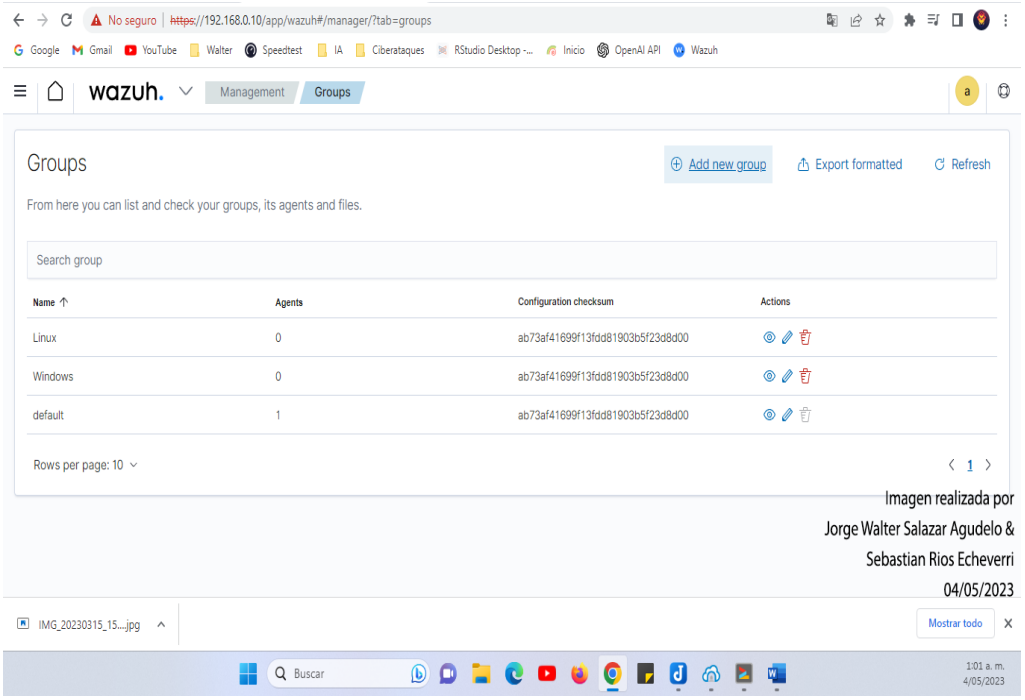
Experiencia previa	La experiencia previa en la prevención, detección y mitigación de ataques hombre en el medio es un factor importante a considerar. Una persona con experiencia previa en la resolución de incidentes de seguridad informática puede ser capaz de manejar mejor situaciones complejas y de alta presión.
Capacidades analíticas	La capacidad de analizar los datos y extraer información valiosa es crucial en la evaluación de la experiencia ante un ataque hombre en el medio. La capacidad de identificar patrones y tendencias, y de tomar decisiones informadas basadas en la información disponible, puede ser clave para mitigar los efectos del ataque.
Conocimiento de las herramientas	Es importante que la persona encargada de la evaluación tenga un conocimiento profundo de las herramientas de seguridad utilizadas para prevenir, detectar y mitigar ataques al hombre en el medio. Esto incluye herramientas de monitoreo de redes,

	herramientas de análisis de tráfico, firewalls, etc.
Capacidad de adaptación	Un ataque hombre en el medio puede ser impredecible y evolucionar rápidamente. Es importante que la persona encargada de la evaluación tenga la capacidad de adaptarse a situaciones cambiantes y de tomar decisiones rápidas y efectivas.

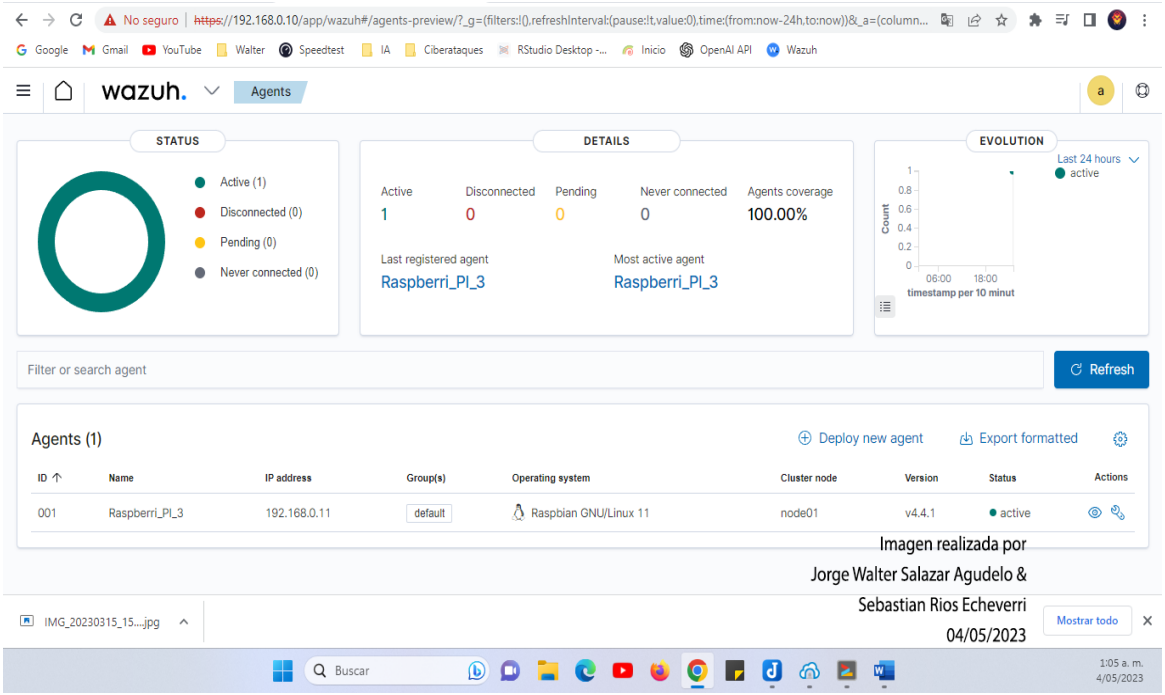
Creación De Grupos:

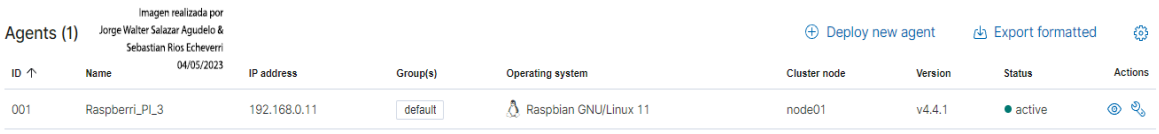






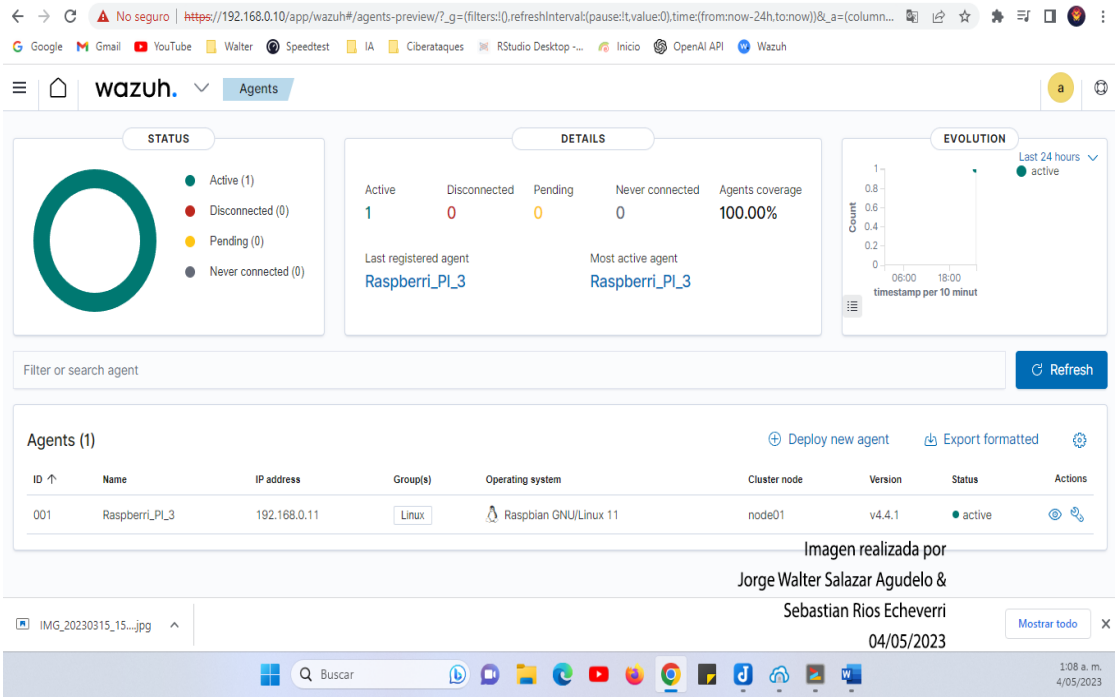
Cambiar un agente de un grupo a otro: cambiar el agente con id 001 del grupo default al grupo Linux.

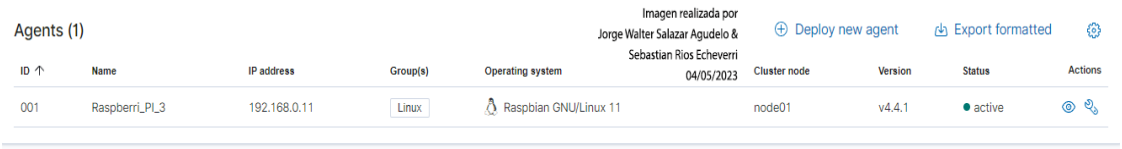




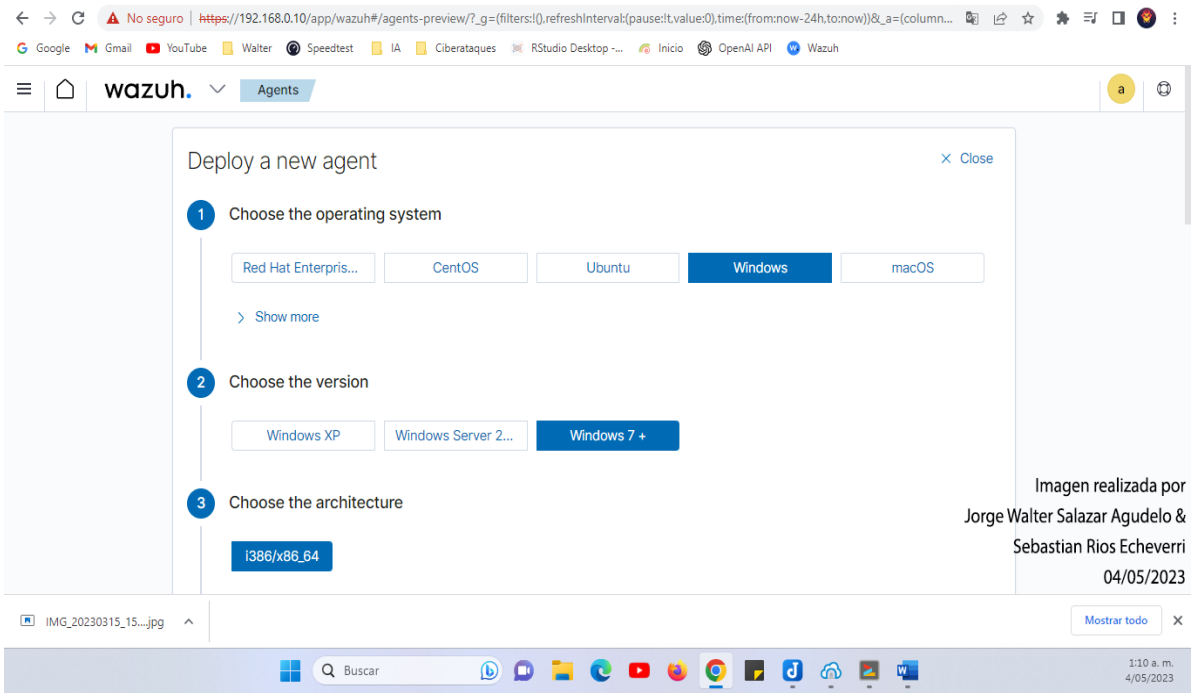
Ejecutamos el siguiente comando (para este caso)

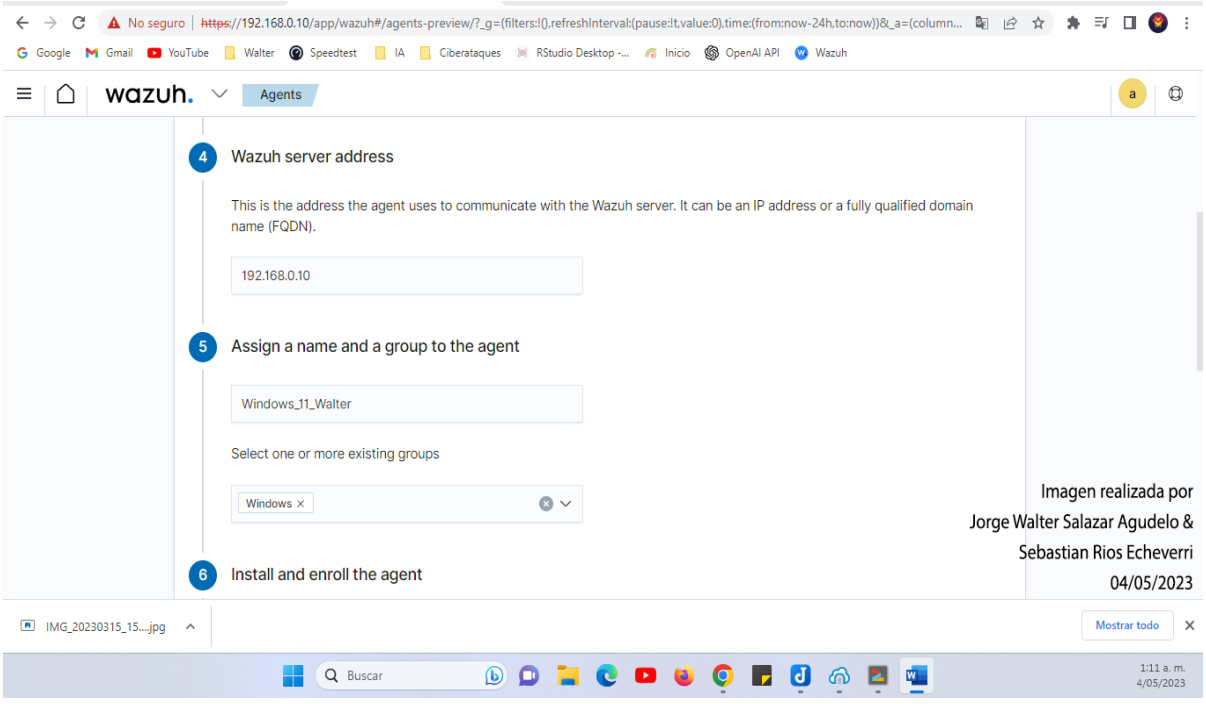
```
/var/ossec/bin/agent_groups -a -f -i 001 -g Linux
```

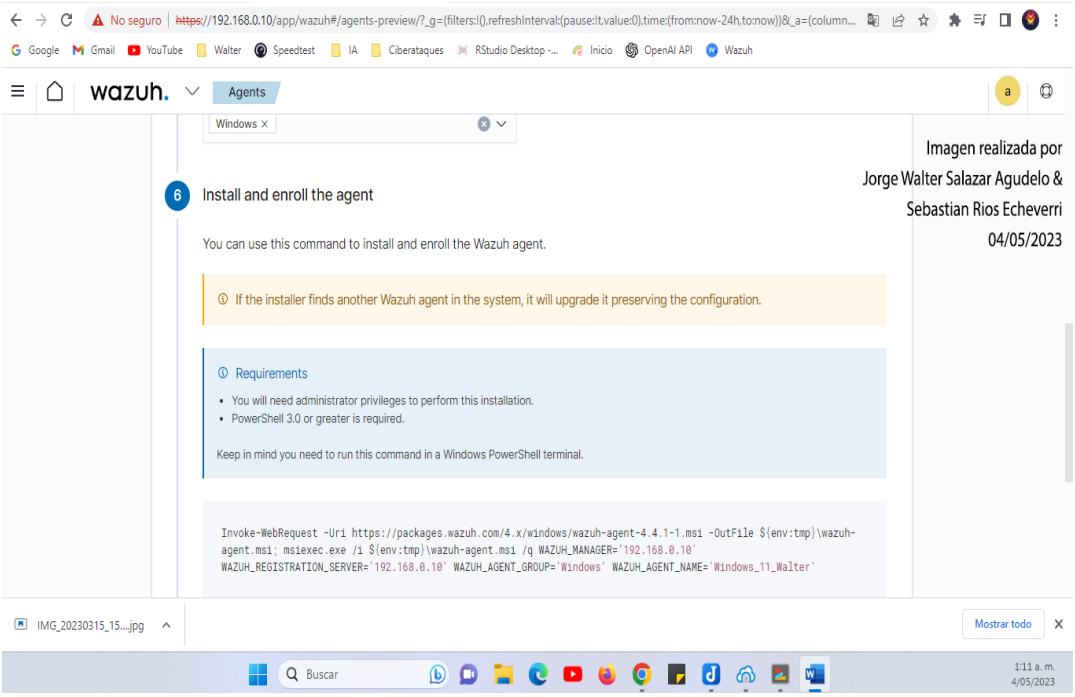


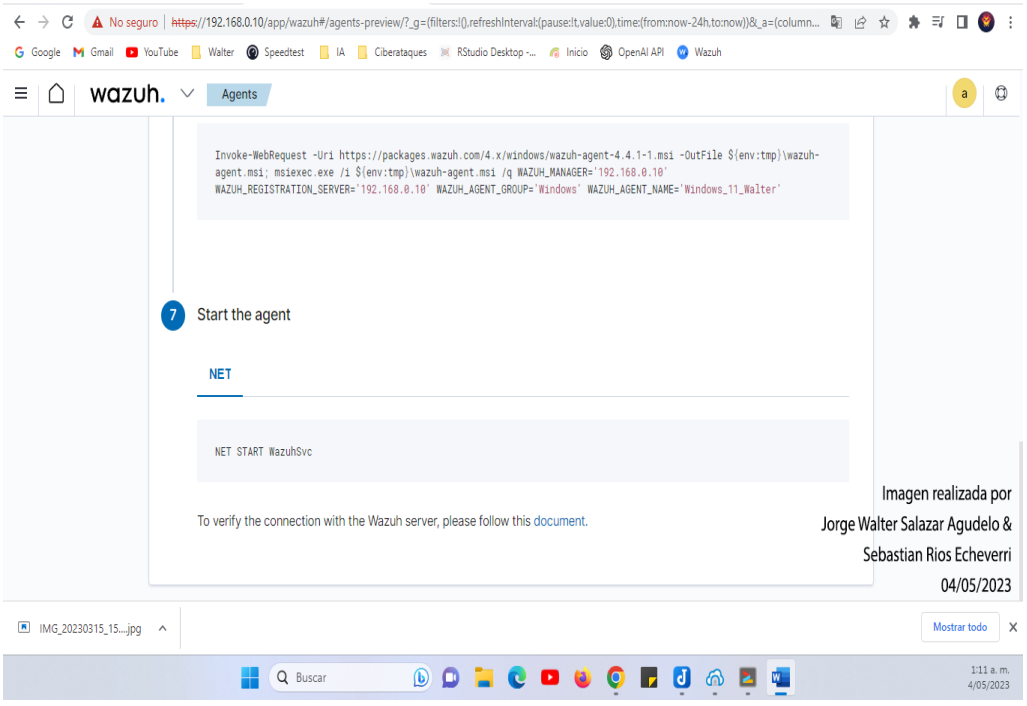


Agregamos los nuevos agentes a Wazuh como ya está estipulado en el anexo dependiendo del sistema operativo en el agente.


wazuh.
Agents
Deploy a new agent
Close
1 Choose the operating system
Red Hat Enterpris...
CentOS
Ubuntu
Windows
macOS
Show more
2 Choose the version
Windows XP
Windows Server 2...
Windows 7 +
3 Choose the architecture
i386/x86_64
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023


wazuh.
Agents
4 Wazuh server address
This is the address the agent uses to communicate with the Wazuh server. It can be an IP address or a fully qualified domain name (FQDN).
192.168.0.10
5 Assign a name and a group to the agent
Windows_11_Walter
Select one or more existing groups
Windows
6 Install and enroll the agent
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023

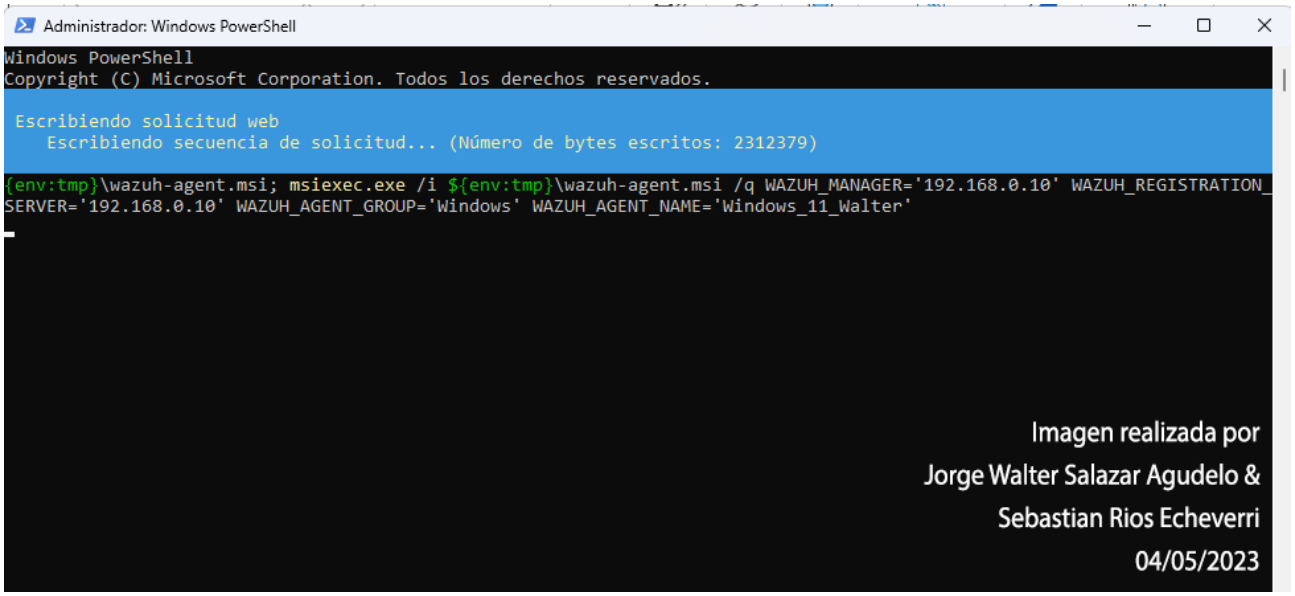


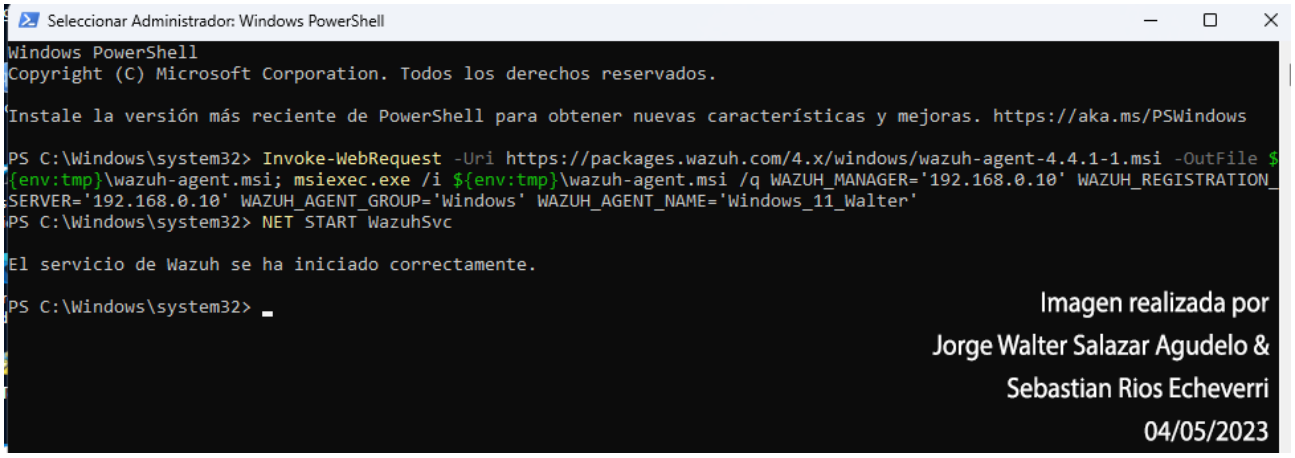


Comandos para Windows para este caso:

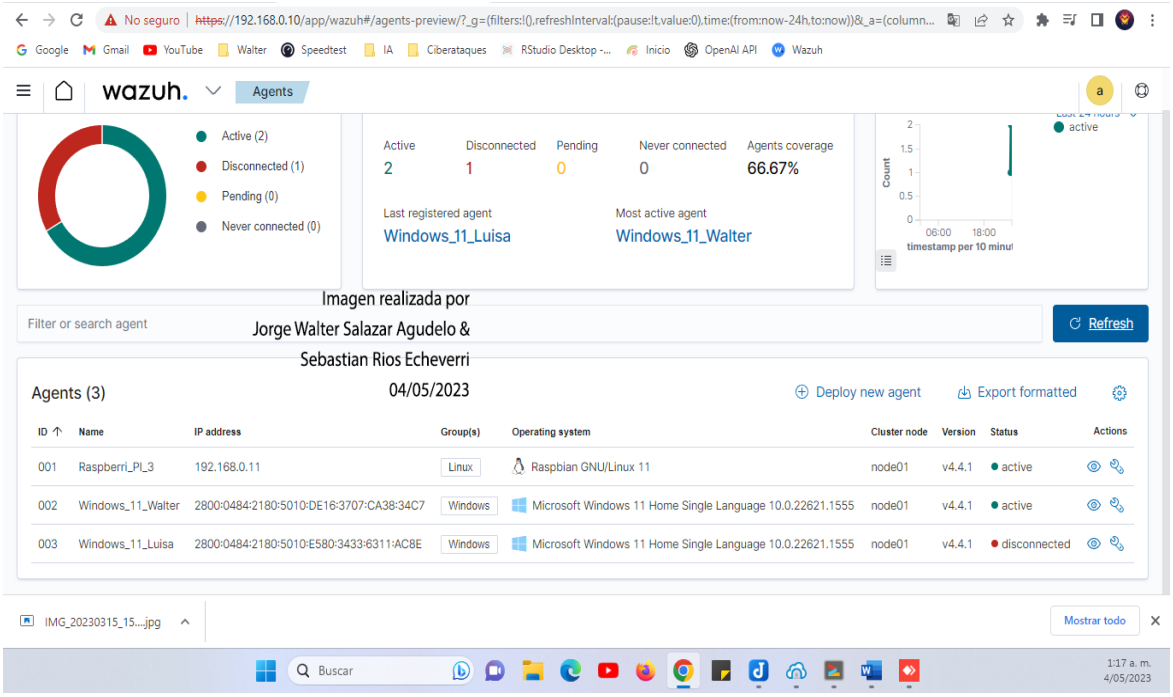
```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.4.1-1.msi -OutFile ${env:tmp}\wazuh-agent.msi; msiexec.exe /i
```

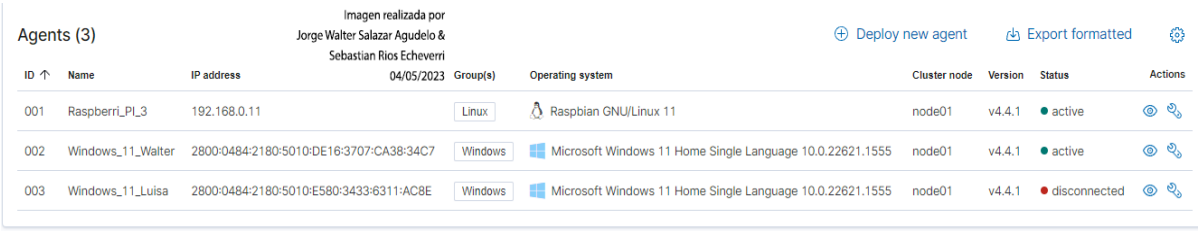
```
${env:tmp}\wazuh-agent.msi /q WAZUH_MANAGER='192.168.0.10'
WAZUH_REGISTRATION_SERVER='192.168.0.10' WAZUH_AGENT_GROUP='Windows'
WAZUH_AGENT_NAME='Windows_11_Walter'
NET START WazuhSvc
```





Ya instalamos 3 agentes 2 Windows y 1 Linux en una raspberry pi 3



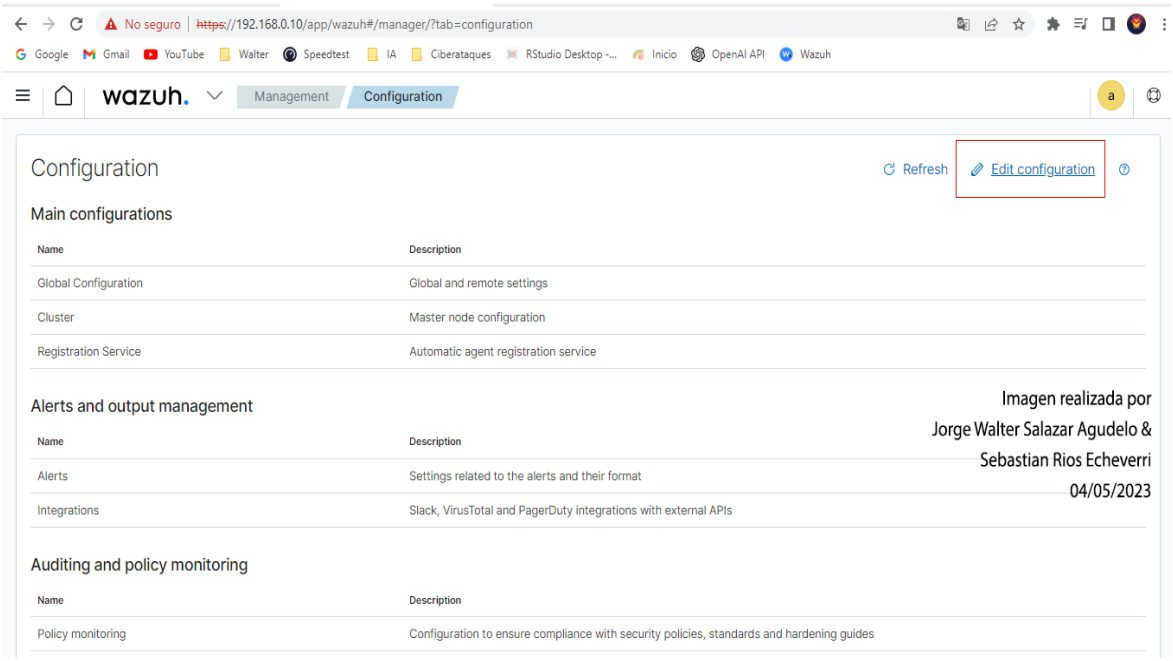


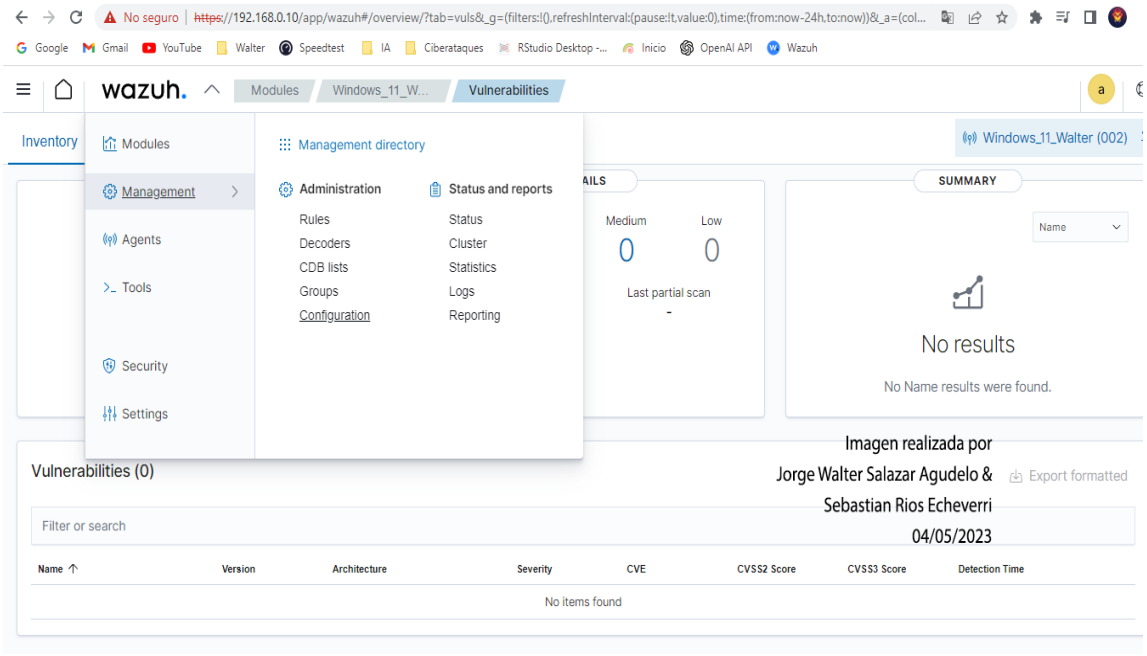
Activar detección de vulnerabilidades de los agentes:

Allí podremos activar para que wazuh revise los agentes y encuentre en ellos las vulnerabilidades a corregir con actualizaciones o parches en algunos casos.

Modules à vulnerabilities (observamos que no tiene activo el servicio de vulnerabilidades. El cual podemos activar de la siguiente manera:

Management → configuración → edit configuration





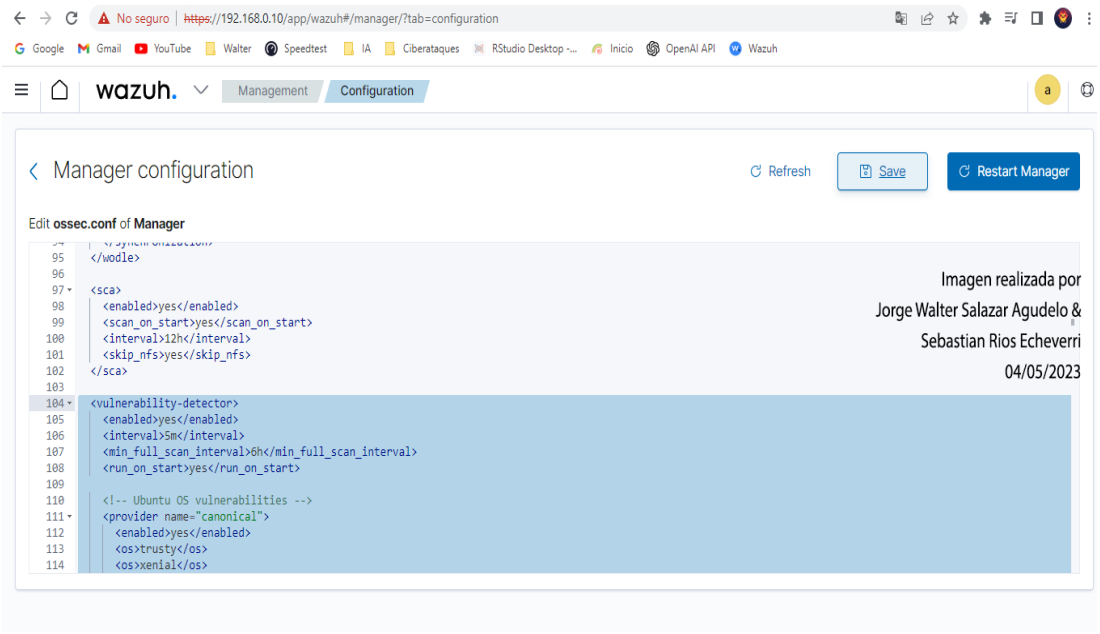
Cambiamos por yes en los siguientes campos:

```
<vulnerability-detector>
    <enabled>yes</enabled>
 <interval>5m</interval>
 <min_full_scan_interval>6h</min_full_scan_interval>
```

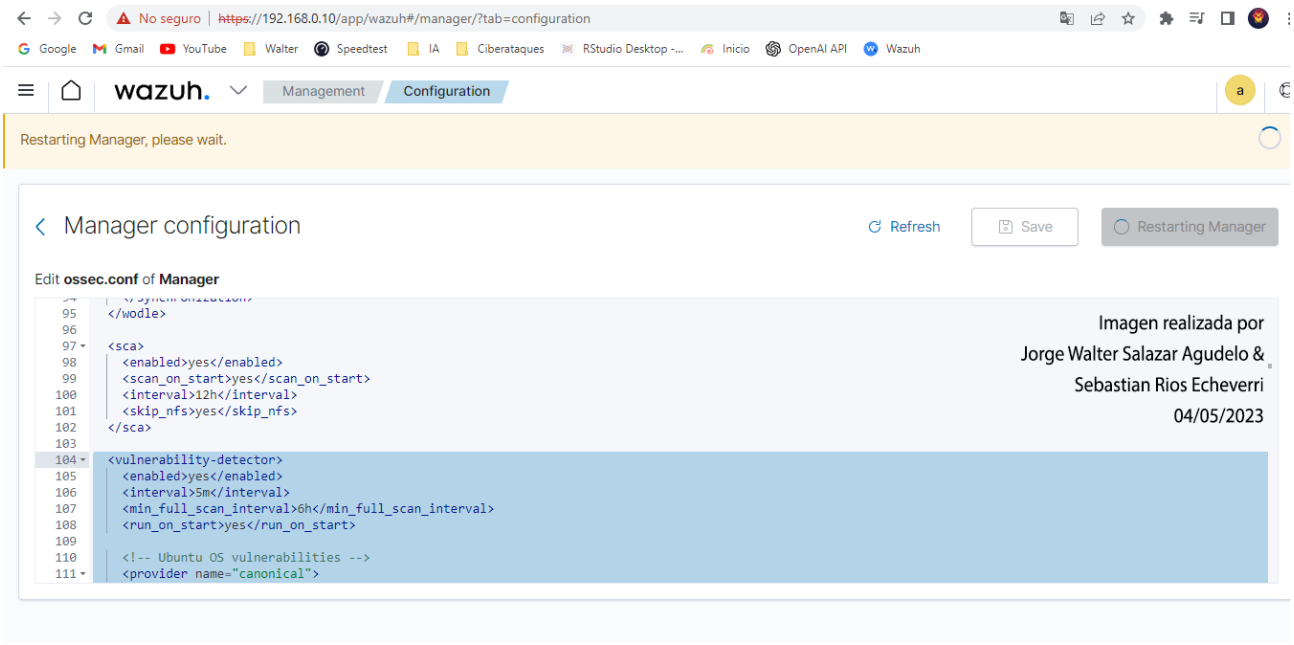
```
<run_on_start>yes</run_on_start>

  <!-- Ubuntu OS vulnerabilities -->
  <provider name="canonical">
  <enabled>yes</enabled>
  <os>trusty</os>
  <os>xenial</os>
  <os>bionic</os>
  <os>focal</os>
  <os>jammy</os>
  <update_interval>1h</update_interval>
  </provider>

  <!-- Debian OS vulnerabilities -->
  <provider name="debian">
  <enabled>yes</enabled>
  <os>buster</os>
  <os>bullseye</os>
  <update_interval>1h</update_interval>
  </provider>

  <!-- RedHat OS vulnerabilities -->
  <provider name="redhat">
  <enabled>yes</enabled>
  <os>5</os>
  <os>6</os>
  <os>7</os>
  <os>8</os>
  <os>9</os>
  <update_interval>1h</update_interval>
  </provider>
```

```
<!-- Amazon Linux OS vulnerabilities -->
<provider name="alas">
<enabled>yes</enabled>
<os>amazon-linux</os>
<os>amazon-linux-2</os>
<update_interval>1h</update_interval>
</provider>

<!-- SUSE OS vulnerabilities -->
<provider name="suse">
<enabled>yes</enabled>
<os>11-server</os>
<os>11-desktop</os>
<os>12-server</os>
<os>12-desktop</os>
<os>15-server</os>
<os>15-desktop</os>
<update_interval>1h</update_interval>
</provider>

<!-- Arch OS vulnerabilities -->
<provider name="arch">
<enabled>yes</enabled>
<update_interval>1h</update_interval>
</provider>

<!-- Windows OS vulnerabilities -->
<provider name="msu">
<enabled>yes</enabled>
<update_interval>1h</update_interval>
</provider>
```

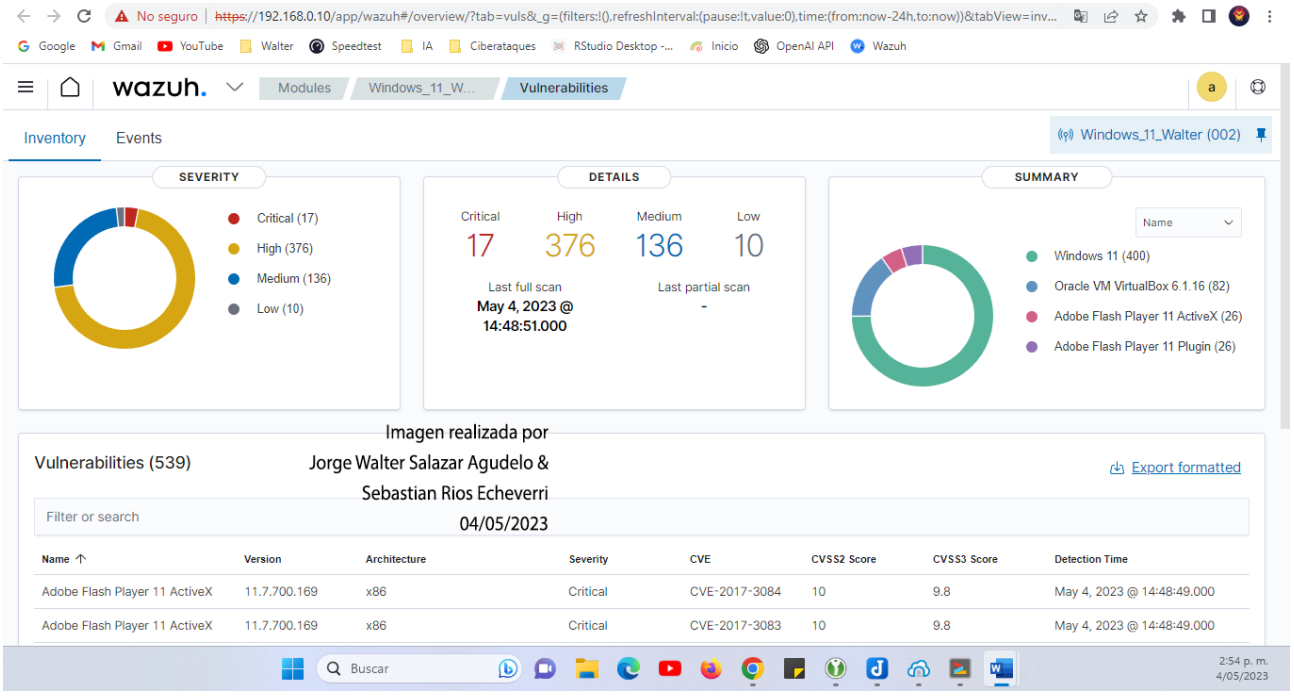
```
<!-- Aggregate vulnerabilities -->
<provider name="nvd">
<enabled>yes</enabled>
<update_from_year>2010</update_from_year>
<update_interval>1h</update_interval>
</provider>
```

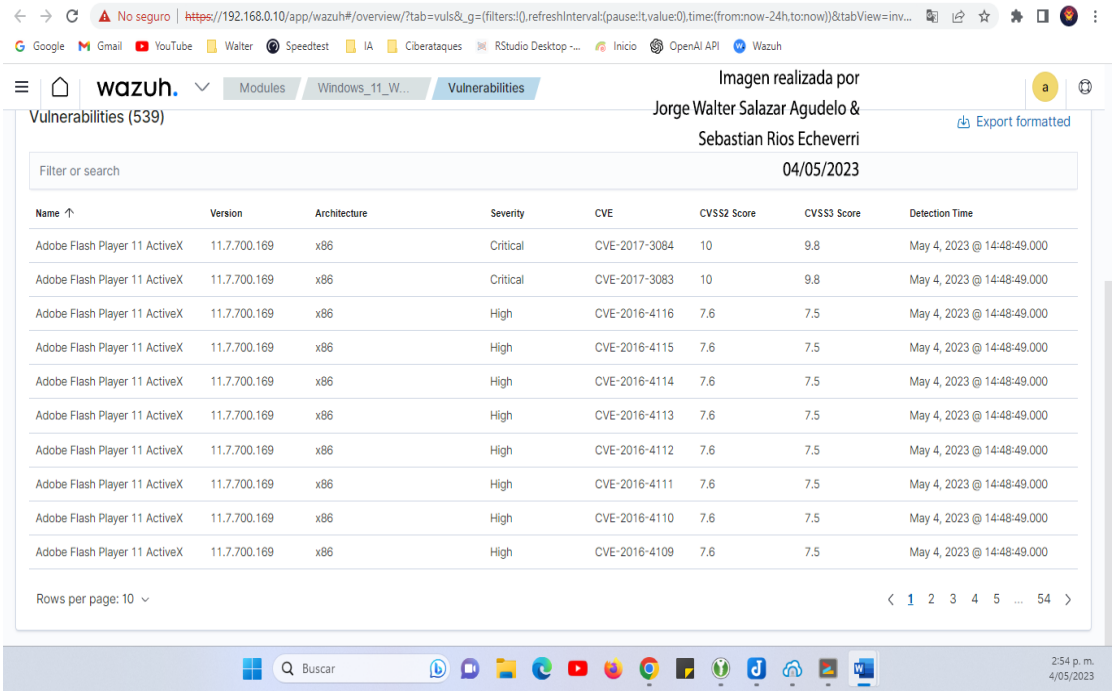


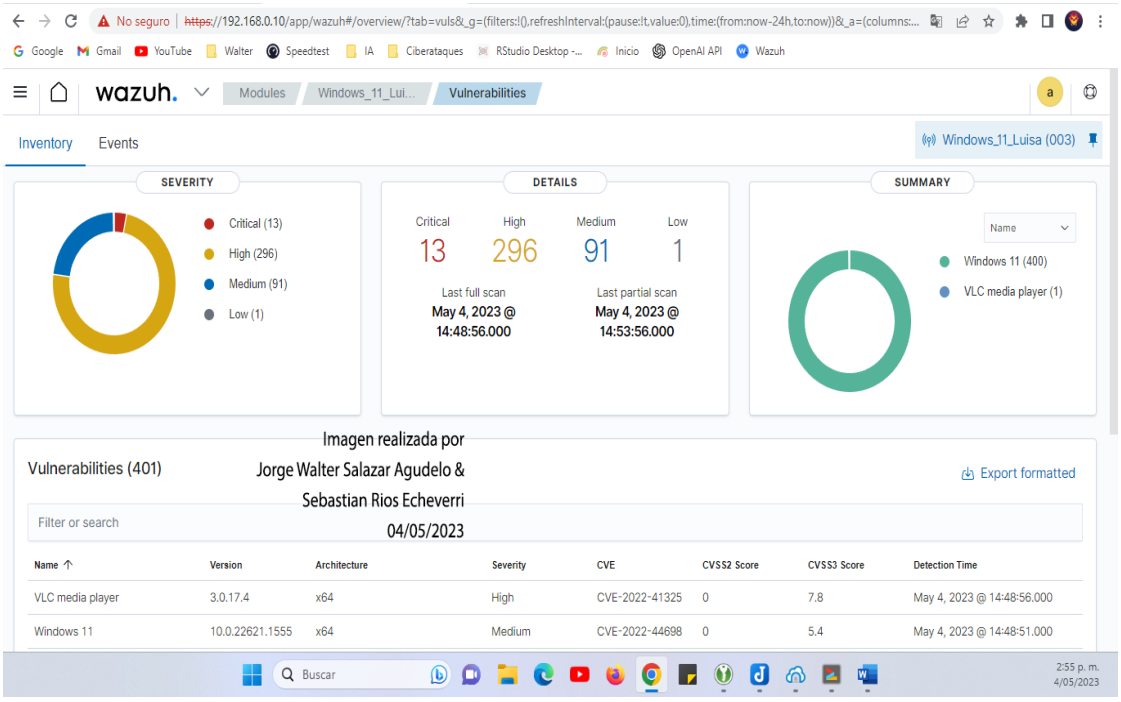
Grabamos con: `save à restart Manager`

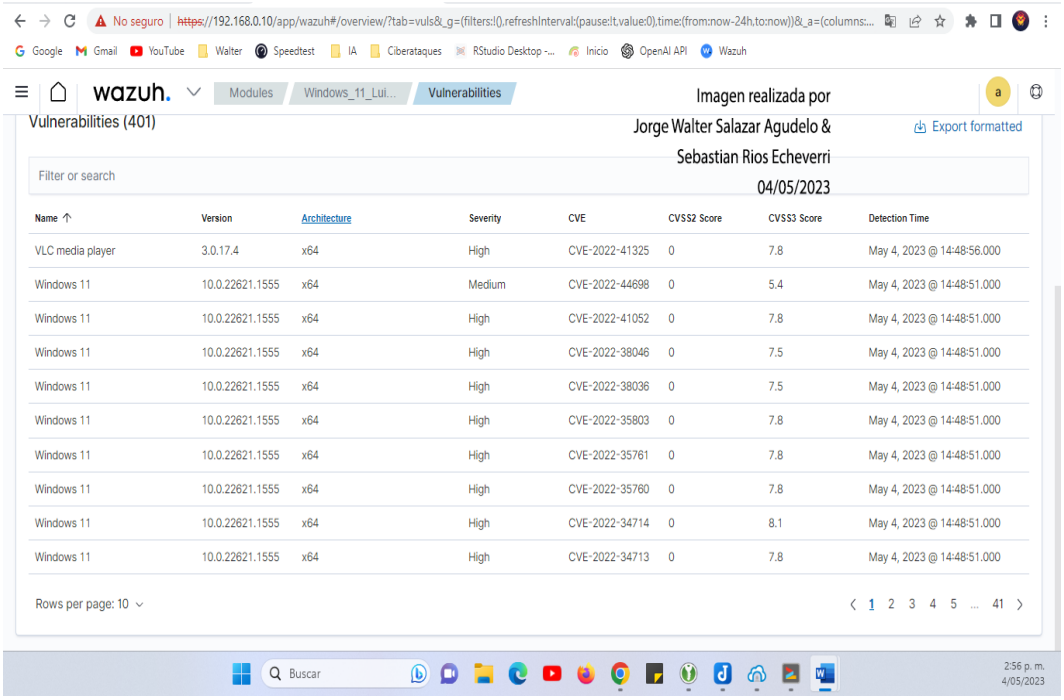


Nos toca esperar unos minutos para escanee los agentes y establezca sus vulnerabilidades




wazuh.
Modules
Windows_11_W...
Vulnerabilities
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023
Vulnerabilities (539)
Export formatted
Filter or search
Name
Version
Architecture
Severity
CVE
CVSS2 Score
CVSS3 Score
Detection Time
Adobe Flash Player 11 ActiveX 11.7.700.169 x86 Critical CVE-2017-3084 10 9.8 May 4, 2023 @ 14:48:49.000
Adobe Flash Player 11 ActiveX 11.7.700.169 x86 Critical CVE-2017-3083 10 9.8 May 4, 2023 @ 14:48:49.000
Adobe Flash Player 11 ActiveX 11.7.700.169 x86 High CVE-2016-4116 7.6 7.5 May 4, 2023 @ 14:48:49.000
Adobe Flash Player 11 ActiveX 11.7.700.169 x86 High CVE-2016-4115 7.6 7.5 May 4, 2023 @ 14:48:49.000
Adobe Flash Player 11 ActiveX 11.7.700.169 x86 High CVE-2016-4114 7.6 7.5 May 4, 2023 @ 14:48:49.000
Adobe Flash Player 11 ActiveX 11.7.700.169 x86 High CVE-2016-4113 7.6 7.5 May 4, 2023 @ 14:48:49.000
Adobe Flash Player 11 ActiveX 11.7.700.169 x86 High CVE-2016-4112 7.6 7.5 May 4, 2023 @ 14:48:49.000
Adobe Flash Player 11 ActiveX 11.7.700.169 x86 High CVE-2016-4111 7.6 7.5 May 4, 2023 @ 14:48:49.000
Adobe Flash Player 11 ActiveX 11.7.700.169 x86 High CVE-2016-4110 7.6 7.5 May 4, 2023 @ 14:48:49.000
Adobe Flash Player 11 ActiveX 11.7.700.169 x86 High CVE-2016-4109 7.6 7.5 May 4, 2023 @ 14:48:49.000
Rows per page: 10
1 2 3 4 5 ... 54
Buscar
2:54 p. m.
4/05/2023

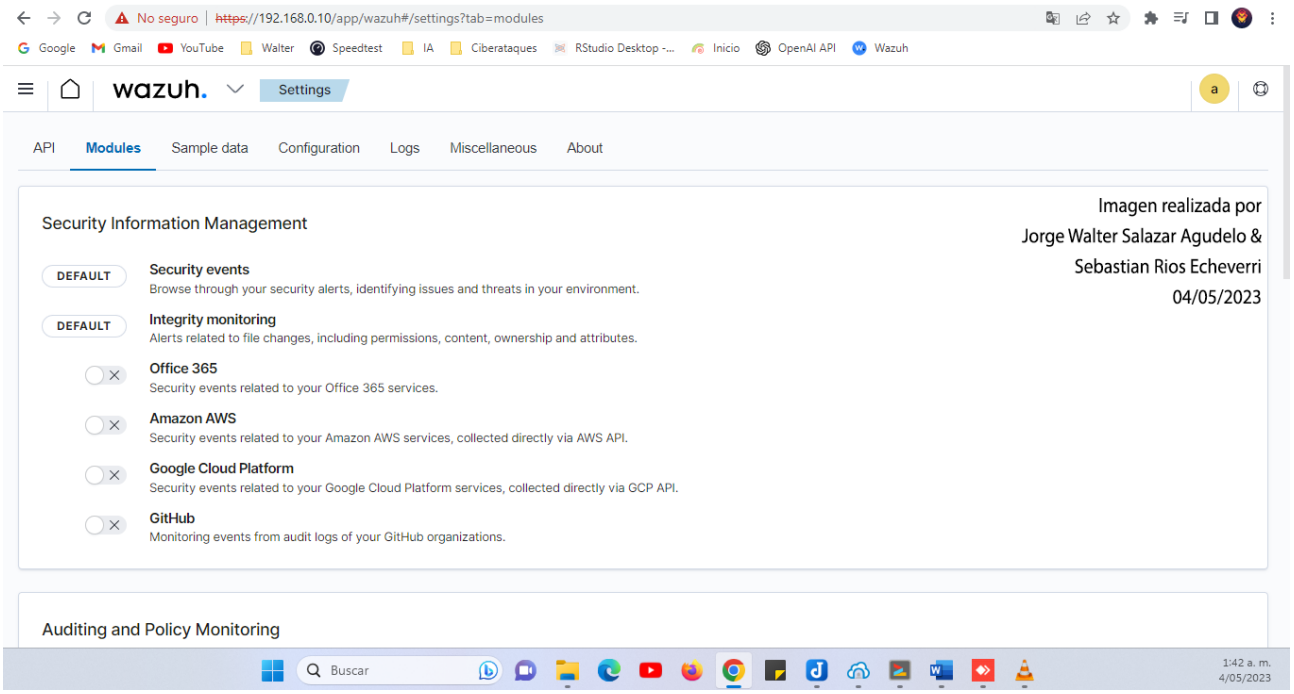

wazuh.
Modules
Windows_11_Lui...
Vulnerabilities
Inventory
Events
Windows_11_Luisa (003)
SEVERITY
Critical (13)
High (296)
Medium (91)
Low (1)
DETAILS
Critical
High
Medium
Low
13
296
91
1
Last full scan
May 4, 2023 @
14:48:56.000
Last partial scan
May 4, 2023 @
14:53:56.000
SUMMARY
Name
Windows 11 (400)
VLC media player (1)
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023
Vulnerabilities (401)
Export formatted
Filter or search
Name
Version
Architecture
Severity
CVE
CVSS2 Score
CVSS3 Score
Detection Time
VLC media player 3.0.17.4 x64 High CVE-2022-41325 0 7.8 May 4, 2023 @ 14:48:56.000
Windows 11 10.0.22621.1555 x64 Medium CVE-2022-44698 0 5.4 May 4, 2023 @ 14:48:51.000
Buscar
2:55 p. m.
4/05/2023


wazuh.
Modules
Windows_11_Lui...
Vulnerabilities
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023
Vulnerabilities (401)
Export formatted
Filter or search
Name
Version
Architecture
Severity
CVE
CVSS2 Score
CVSS3 Score
Detection Time
VLC media player 3.0.17.4 x64 High CVE-2022-41325 0 7.8 May 4, 2023 @ 14:48:56.000
Windows 11 10.0.22621.1555 x64 Medium CVE-2022-44698 0 5.4 May 4, 2023 @ 14:48:51.000
Windows 11 10.0.22621.1555 x64 High CVE-2022-41052 0 7.8 May 4, 2023 @ 14:48:51.000
Windows 11 10.0.22621.1555 x64 High CVE-2022-38046 0 7.5 May 4, 2023 @ 14:48:51.000
Windows 11 10.0.22621.1555 x64 High CVE-2022-38036 0 7.5 May 4, 2023 @ 14:48:51.000
Windows 11 10.0.22621.1555 x64 High CVE-2022-35803 0 7.8 May 4, 2023 @ 14:48:51.000
Windows 11 10.0.22621.1555 x64 High CVE-2022-35761 0 7.8 May 4, 2023 @ 14:48:51.000
Windows 11 10.0.22621.1555 x64 High CVE-2022-35760 0 7.8 May 4, 2023 @ 14:48:51.000
Windows 11 10.0.22621.1555 x64 High CVE-2022-34714 0 8.1 May 4, 2023 @ 14:48:51.000
Windows 11 10.0.22621.1555 x64 High CVE-2022-34713 0 7.8 May 4, 2023 @ 14:48:51.000
Rows per page: 10
1 2 3 4 5 ... 41
Buscar
2:56 p. m.
4/05/2023

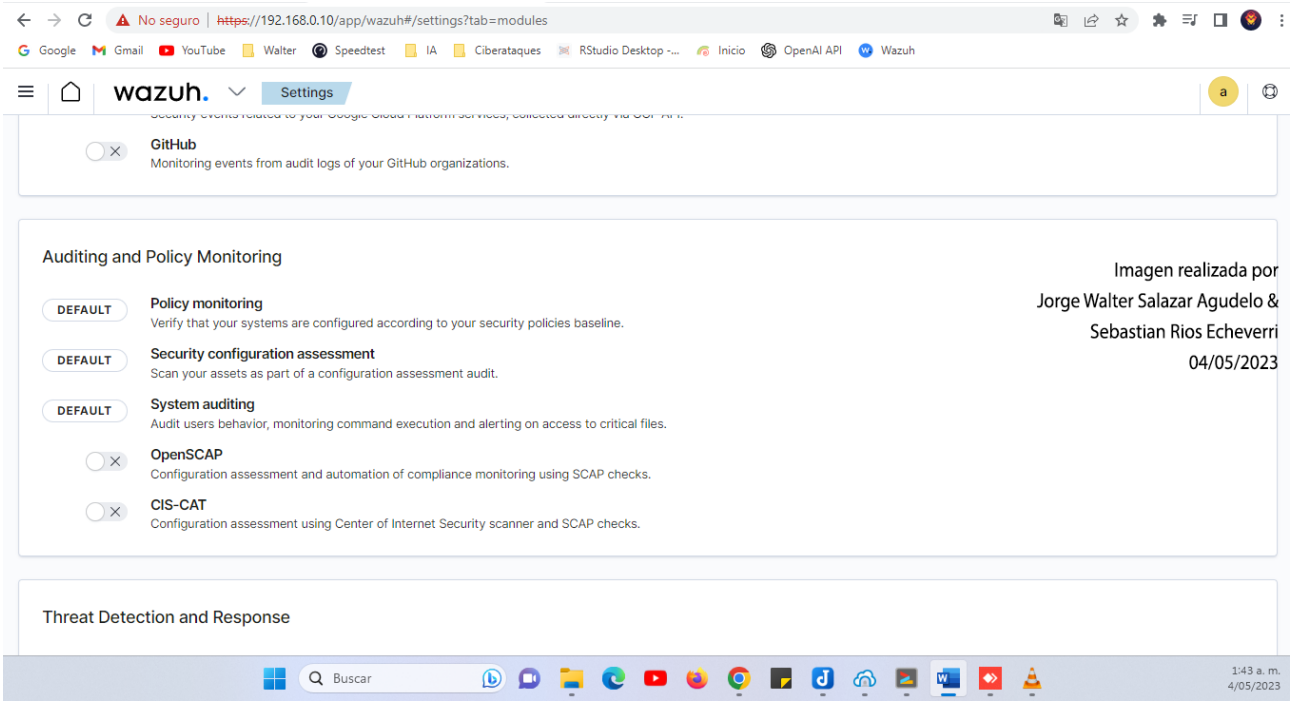
Activar Otros Módulos De Wazuh:

Ingresando a Setting à modules

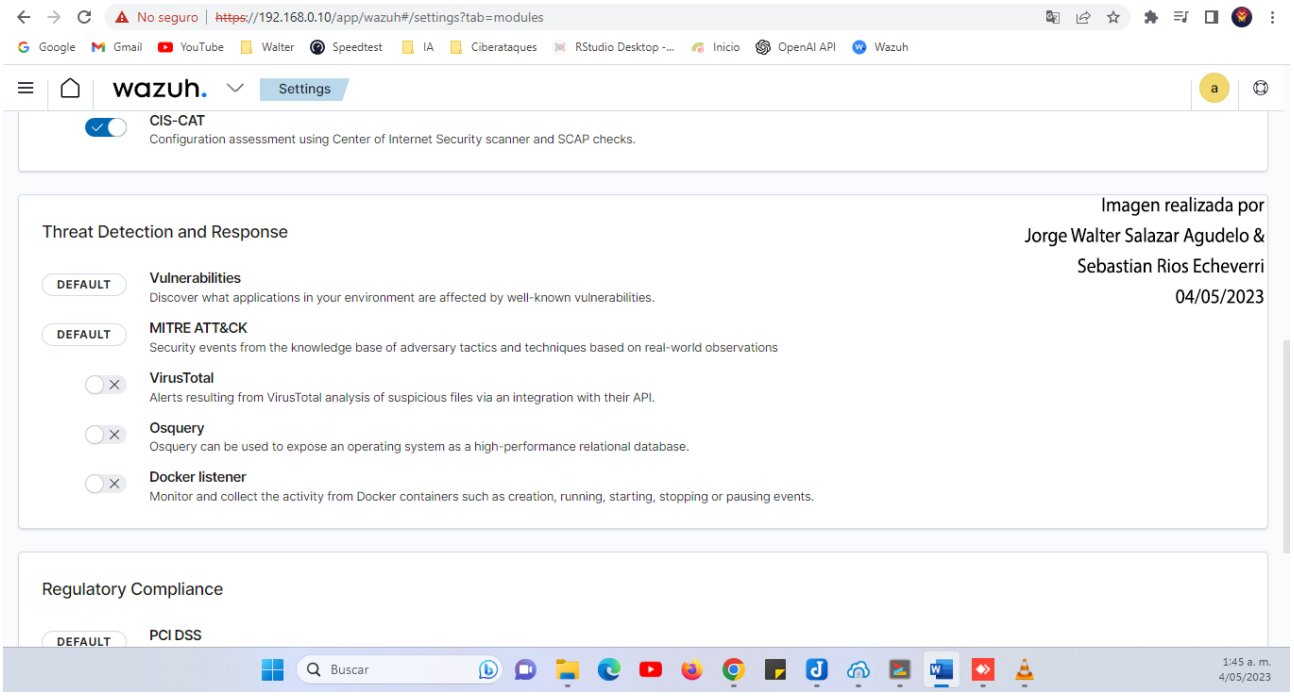
Vamos a encontrar los módulos de wazuh en donde tendremos algunos activos y otros desactivados. En este caso los activaremos todos



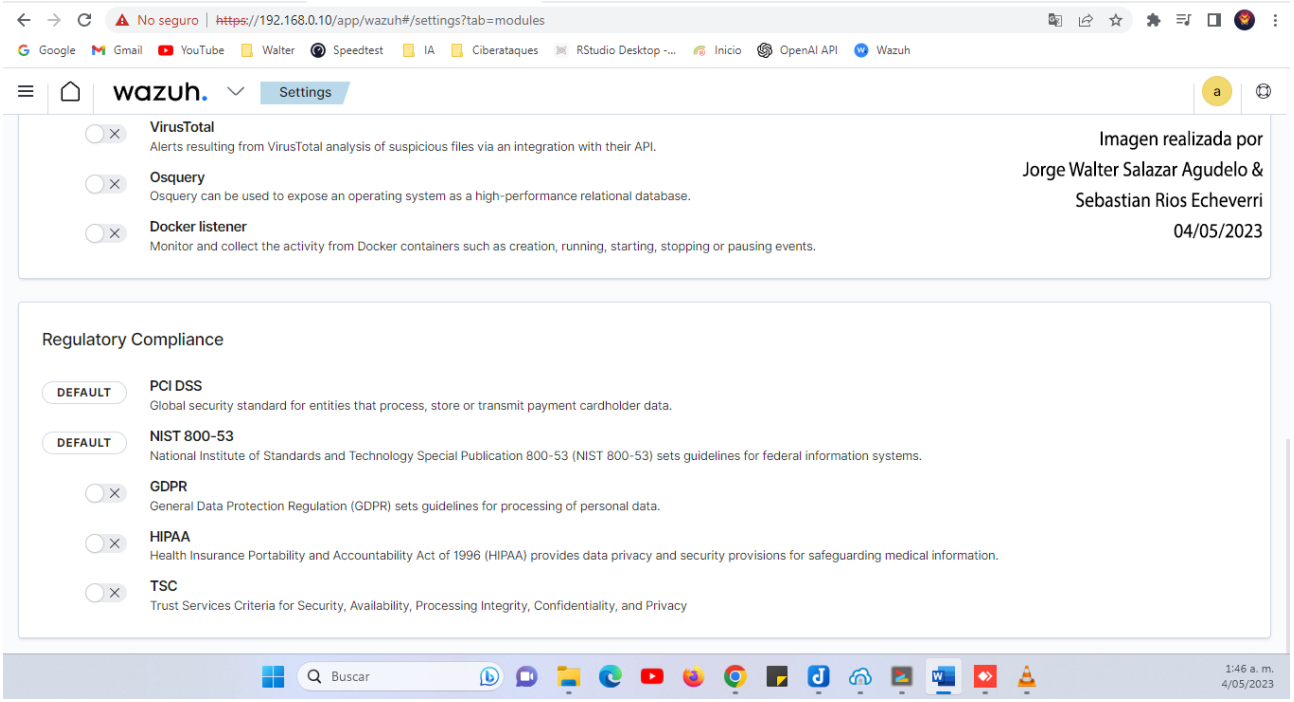
Encontraremos allí también las políticas de monitoreo y auditoria, las cuales debemos activar también.



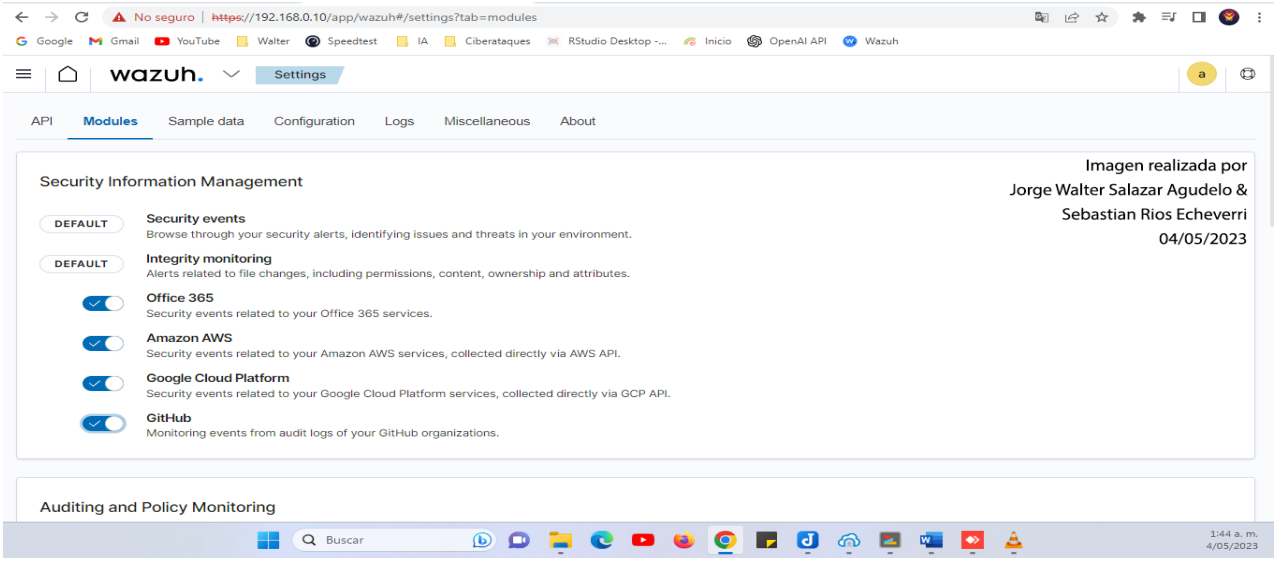
Encontramos la activación y detección y respuesta a ataques los cuales debemos activar entre ellas virustotal y osquery y escaneo de docker



Encontramos para activar las otras políticas adicionales:



Quedando entonces así:



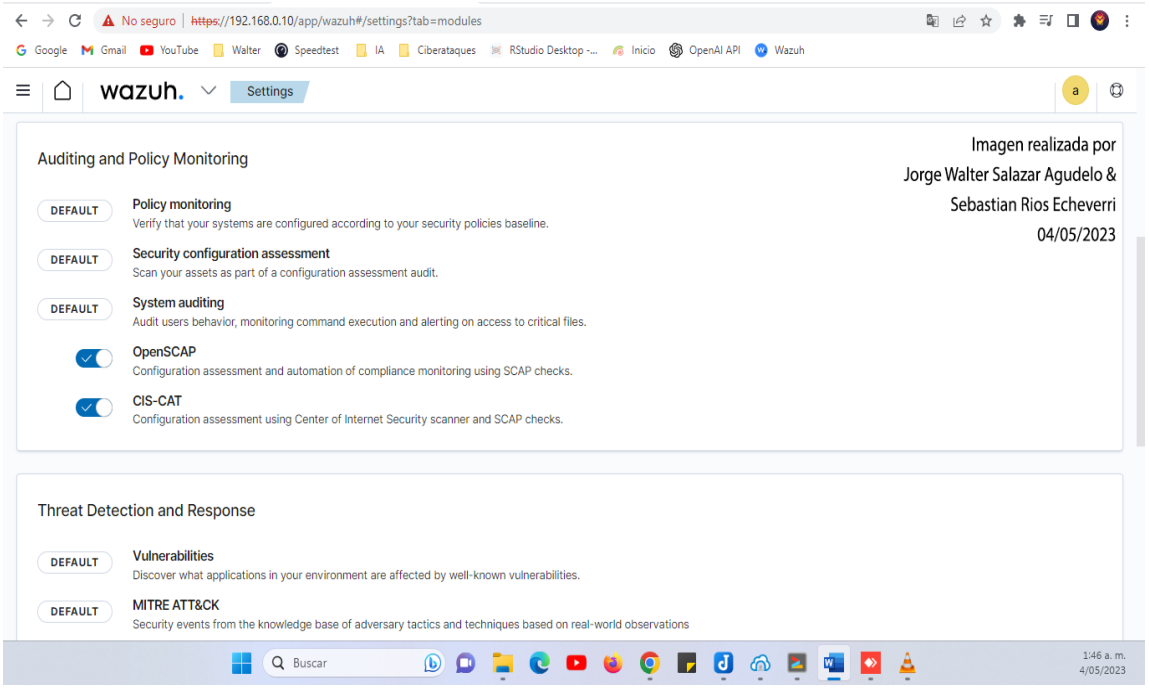


Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023

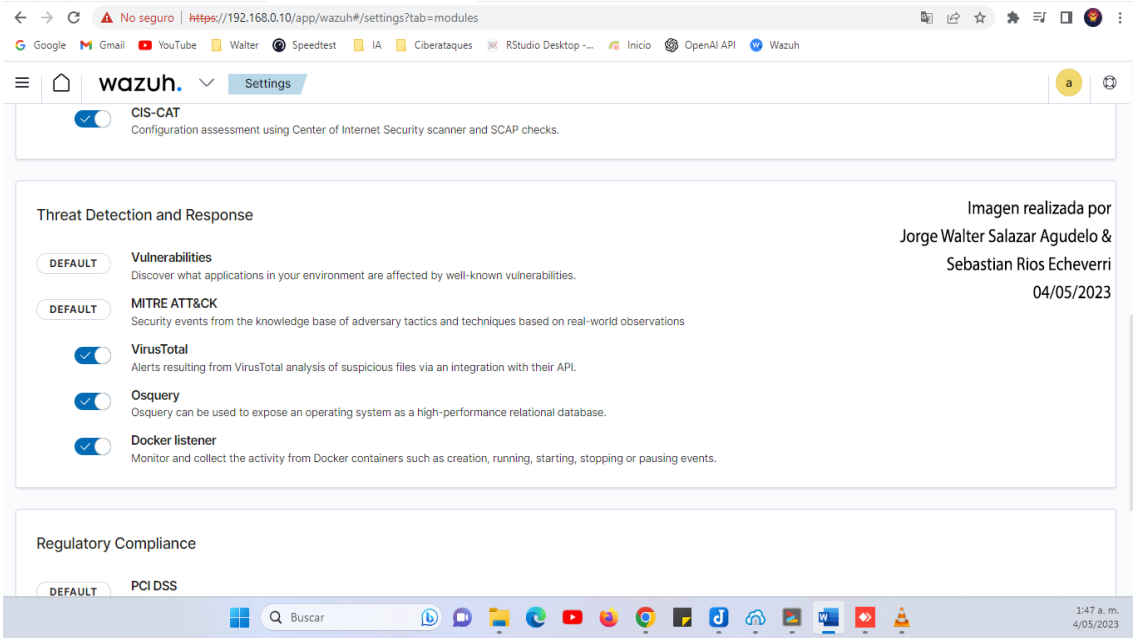
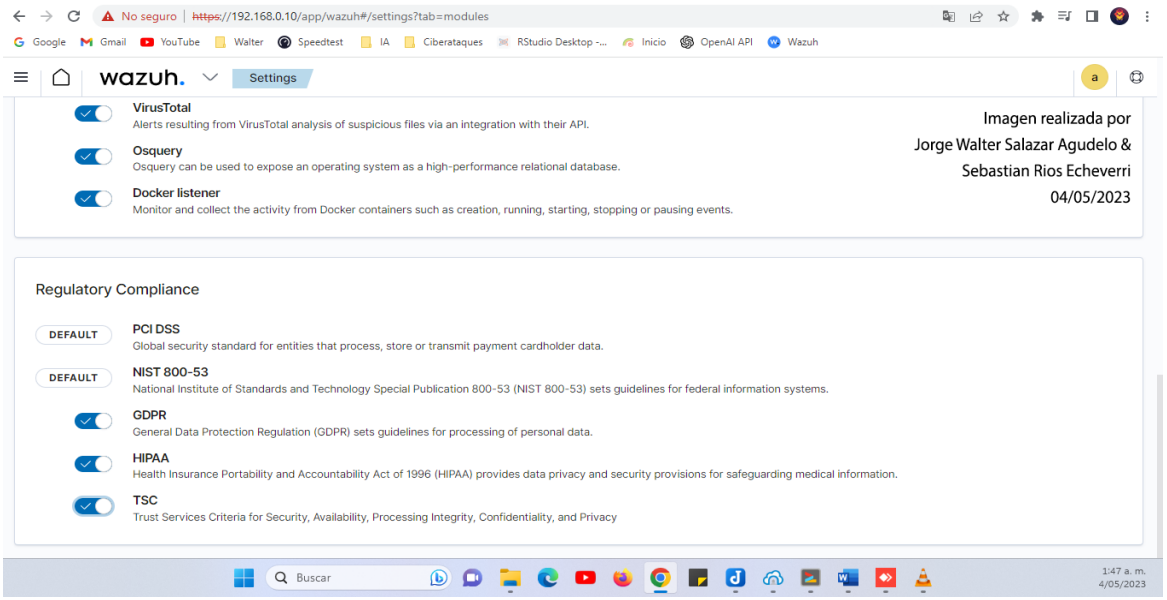
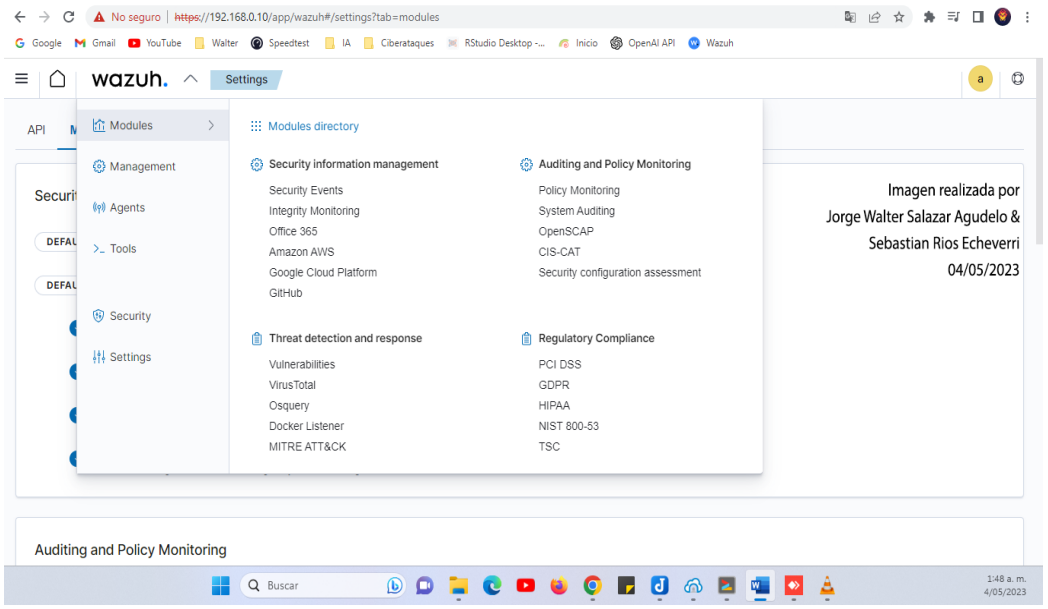
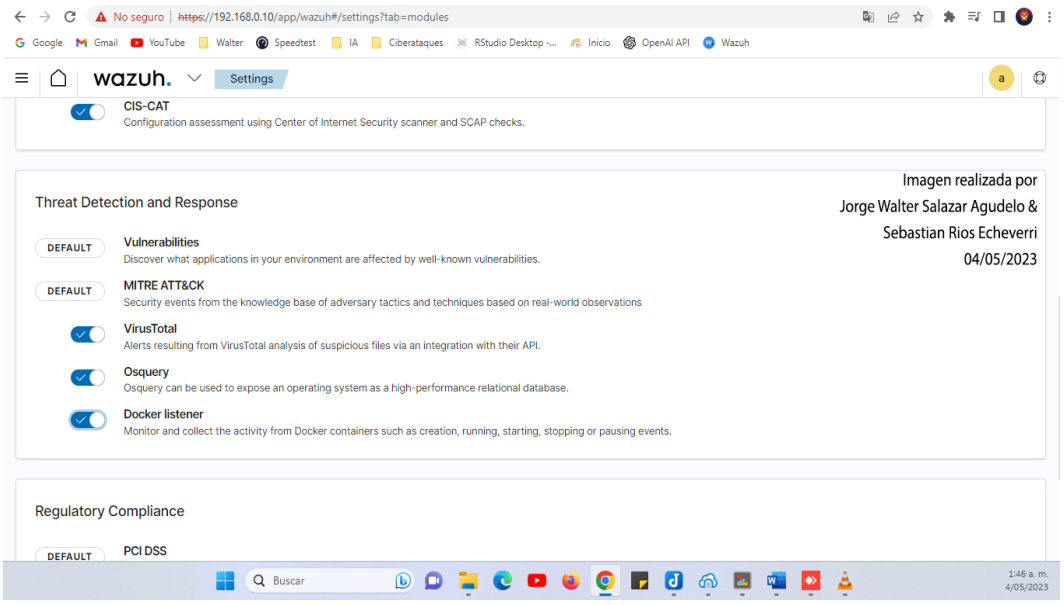


Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023



Quedando todo activo lo cual yo lo podremos visualizar en el panel de **modules**


No seguro | https://192.168.0.10/app/wazuh#/settings?tab=modules
wazuh.
Settings
Modules
Management
Agents
Tools
Security
Settings
Modules directory
Security information management
Security Events
Integrity Monitoring
Office 365
Amazon AWS
Google Cloud Platform
GitHub
Auditing and Policy Monitoring
Policy Monitoring
System Auditing
OpenSCAP
CIS-CAT
Security configuration assessment
Threat detection and response
Vulnerabilities
VirusTotal
Osquery
Docker Listener
MITRE ATT&CK
Regulatory Compliance
PCI DSS
GDPR
HIPAA
NIST 800-53
TSC
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023
Auditing and Policy Monitoring


No seguro | https://192.168.0.10/app/wazuh#/settings?tab=modules
wazuh.
Settings
CIS-CAT
Configuration assessment using Center of Internet Security scanner and SCAP checks.
Threat Detection and Response
DEFAULT
Vulnerabilities
Discover what applications in your environment are affected by well-known vulnerabilities.
DEFAULT
MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations
VirusTotal
Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.
Osquery
Osquery can be used to expose an operating system as a high-performance relational database.
Docker listener
Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.
Regulatory Compliance
DEFAULT
PCI DSS
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023

Configuración Centralizada:

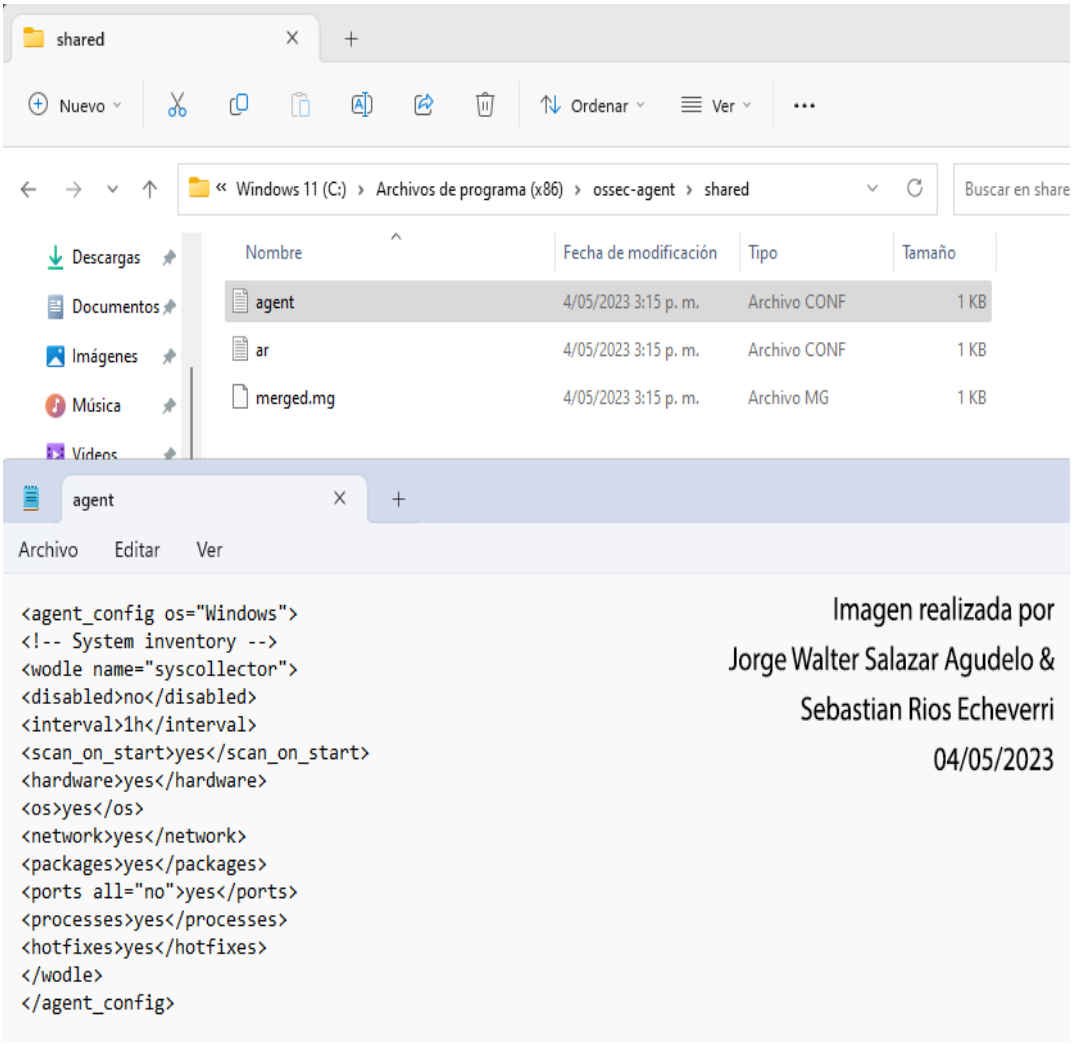
Al tener creados los grupos los agentes pueden configurarse remotamente por medio del fichero agent.conf si queremos modificar Windows se edita el fichero agent.conf en la siguiente ruta:

```
Cd /var/ossec/etc/shared/Windows
nano agent.conf
```

Dicho fichero lo dejamos así:

```
<agent_config os="Windows">
<!-- System inventory -->
<wodle name="syscollector">
<disabled>no</disabled>
<interval>1h</interval>
<scan_on_start>yes</scan_on_start>
<hardware>yes</hardware>
<os>yes</os>
<network>yes</network>
<packages>yes</packages>
<ports all="no">yes</ports>
<processes>yes</processes>
<hotfixes>yes</hotfixes>
</wodle>
</agent_config>
```

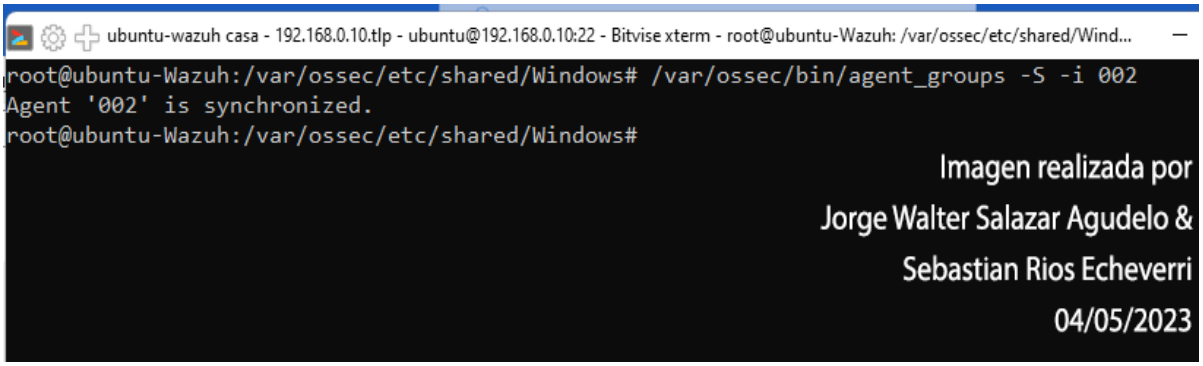
Y en pocos minutos tendríamos en cada uno de los servidores Windows, dicho fichero en la ruta C:\Program Files (x86)\ossec-agent\shared.



`<hotfixes>yes</hotfixes>**` que nos permite detectar los hotfixes aplicados

Para comprobar que el agente con ID 002 - Servidor Windows, está sincronizado ejecutamos:

```
/var/ossec/bin/agent_groups -S -i 002
```

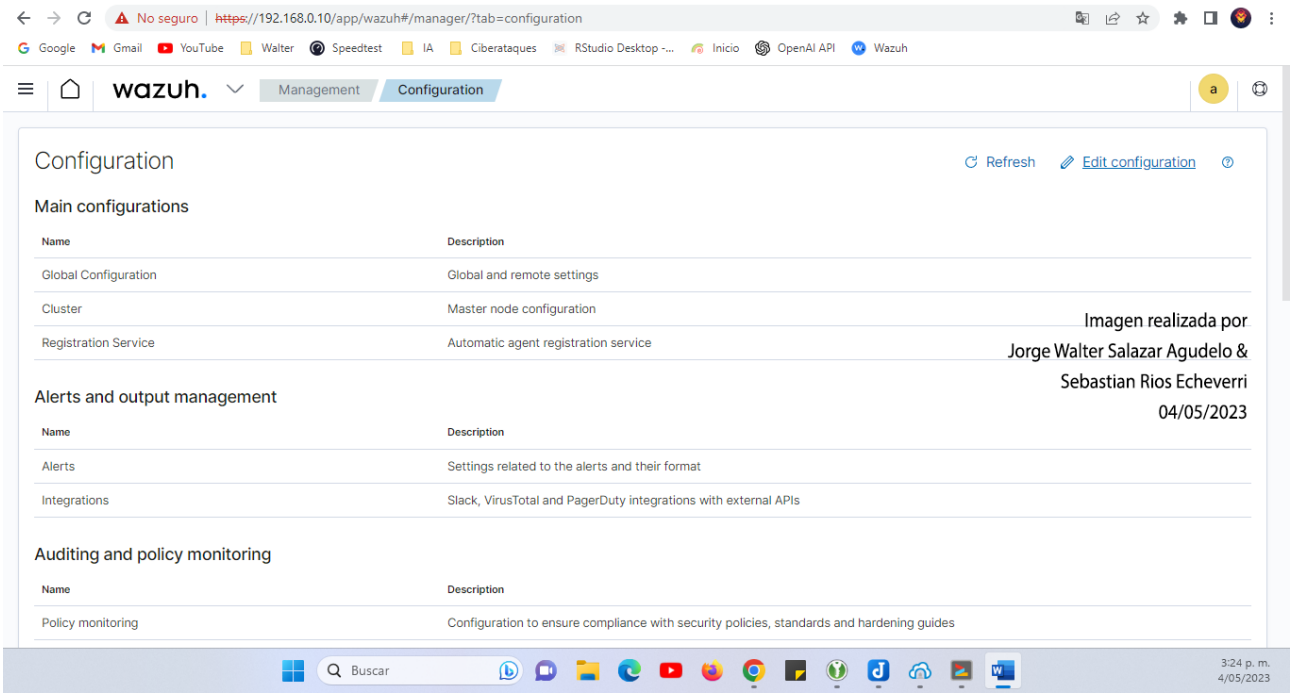


Una vez desplegado, ya empezaría a detectar las vulnerabilidades en los sistemas Windows.

Configuración Del Servidorwazuh

Configuramos el servidor para que obtenga las actualizaciones desde el año 2010 y que se actualice cada hora:

Wazuh → Management → Configuration à edit configuration



Y en la configuración buscamos:

```
<!-- Aggregate vulnerabilities -->
      <provider name="nvd">
      <enabled>yes</enabled>
      <update_from_year>2010</update_from_year>
      <update_interval>1h</update_interval>
      </provider>
```

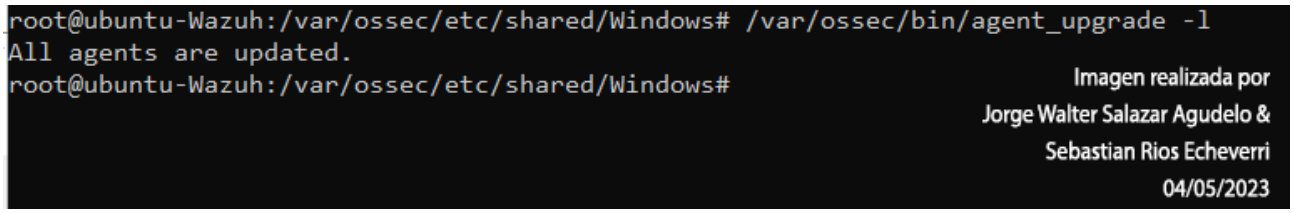
Actualización Remota De Agentes:

https://documentation.wazuh.com/current/user-manual/agents/remote-upgrading/upgrading-agent.html

Lo podemos hacer por línea de comando desde el servidor wazuh con los siguients comandos.

1. Para enumerar los agentes obsoletos.

```
/var/ossec/bin/agent_upgrade -l
```



En este caso nos indica que todos están actualizados.

1. Actualice el agente con el ID 002 mediante el parámetro '-a' seguido del ID del agente:

```
/var/ossec/bin/agent_upgrade -a 002
```

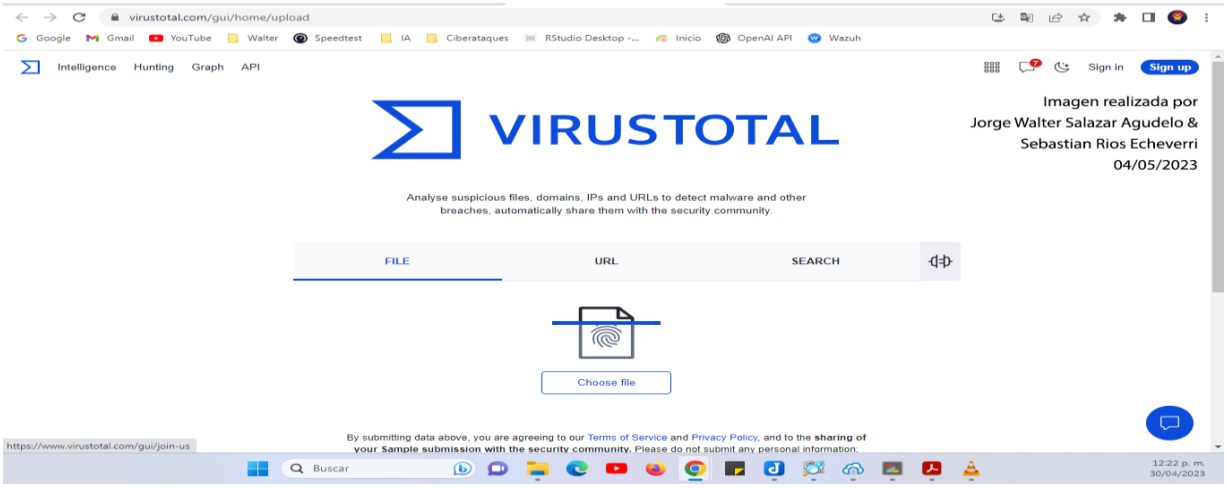
2. Después de actualizarse el agente se reinicia y podemos verificar si se actualizo adecuadamente:

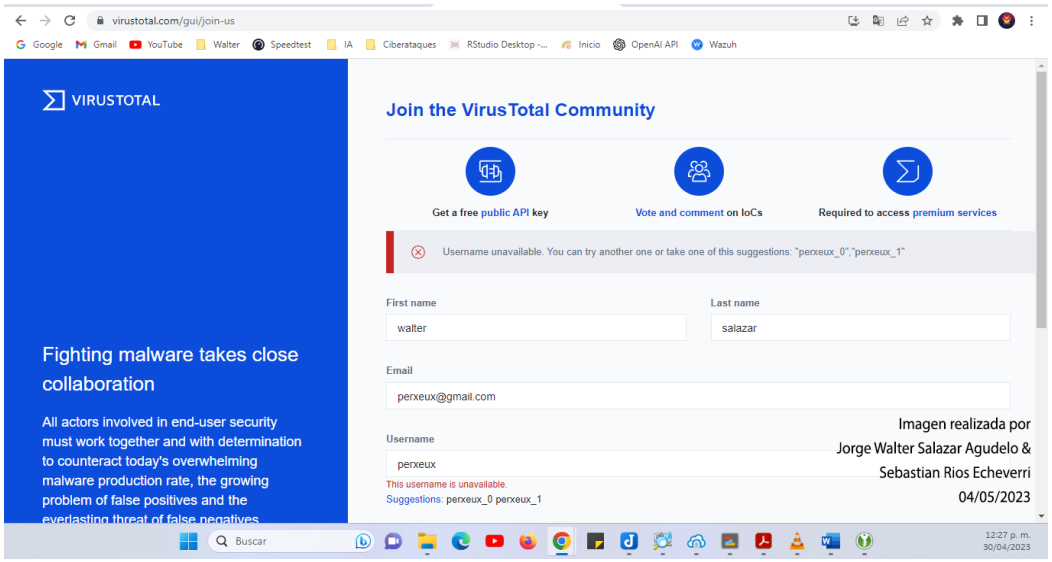
```
/var/ossec/bin/agent_control -i 002
```

Integración Con Virustotal:

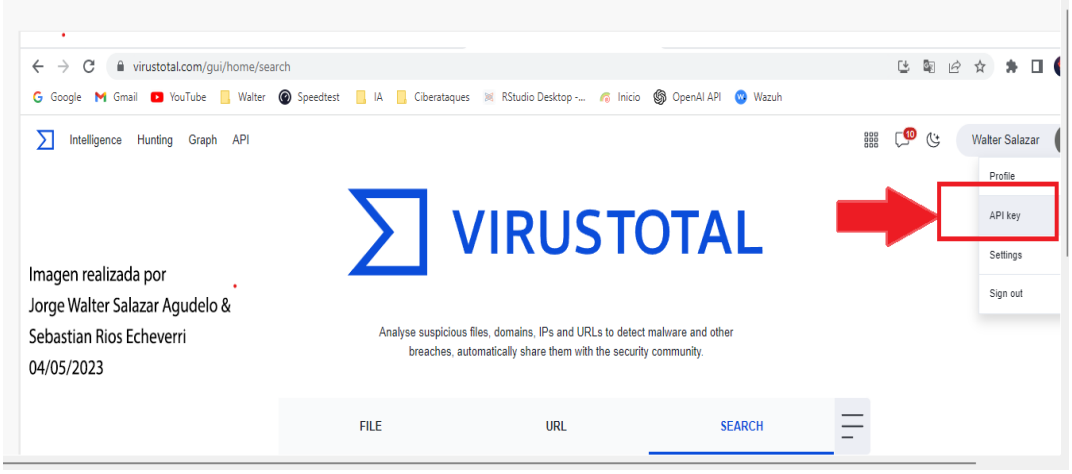
https://documentation.wazuh.com/current/proof-of-concept-guide/detect-remove-malware-virustotal.html

Entro a virustotal y me registro:

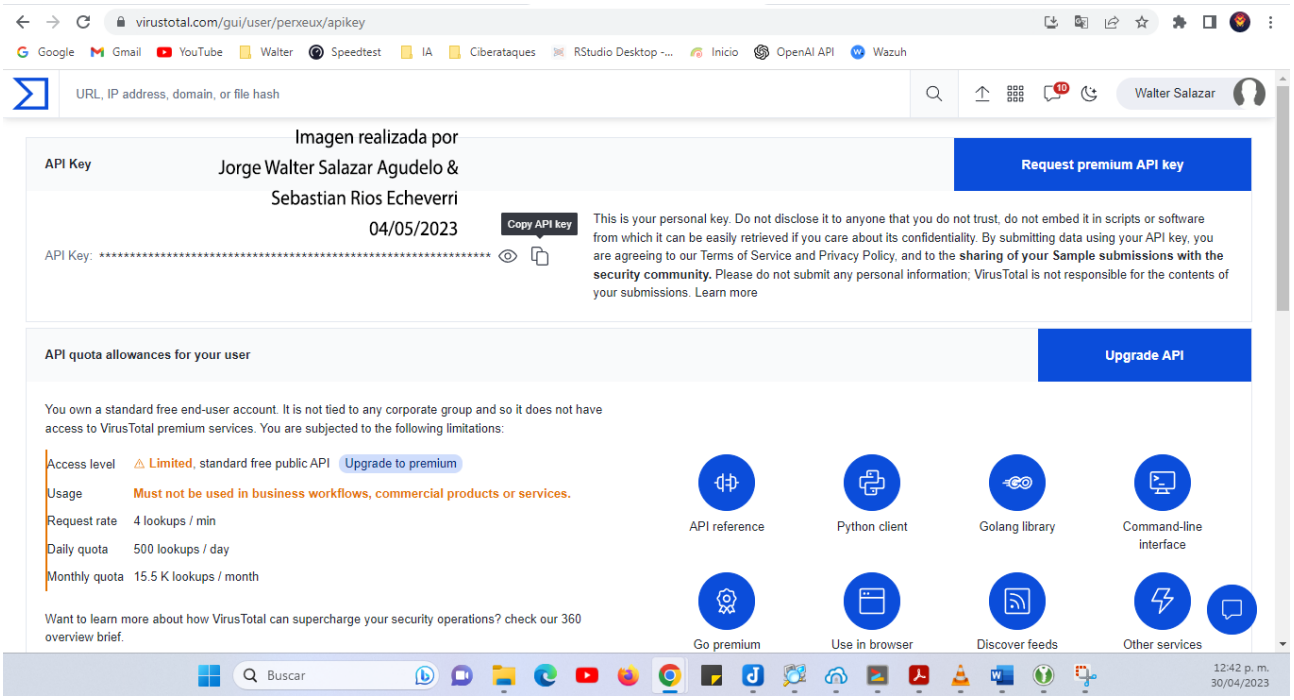




Después de registrarme ingreso a la API KEY



Copio y guardo mi api Key



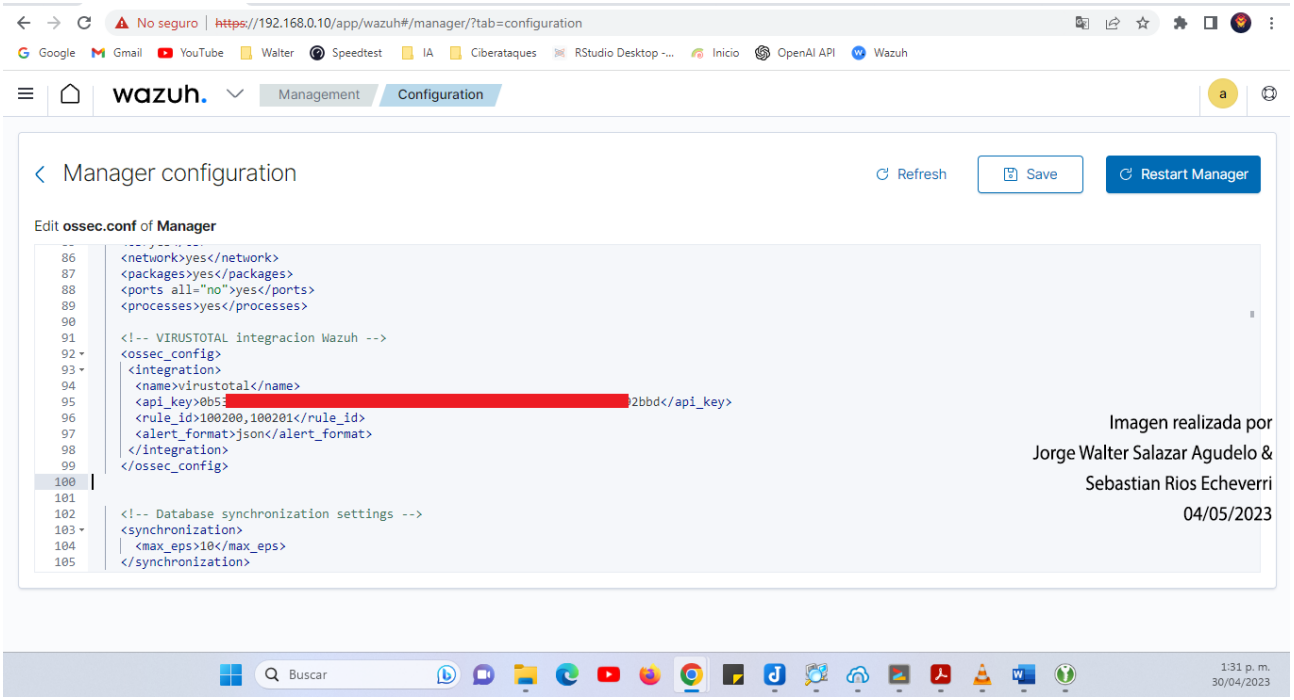
Esta api key la voy a necesitar para configurar en wazuh à management à configuration à edit configuration y allí agregamos las líneas que nos indica la documentación wazuh

https://documentation.wazuh.com/current/proof-of-concept-guide/detect-remove-malware-virustotal.html

```
<!-- VIRUSTOTAL integracion Wazuh -->
<ossec_config>
  <integration>
    <name>virustotal</name>
    <api_key><remplazamos aquí por la api key de virustotal></api_key>
    <rule_id>100200,100201</rule_id>
    <alert_format>json</alert_format>
  </integration>
```

```
</ossec_config>
```

Quedando así:



Utilizar Fim Para Monitoreo De Descargas En Directorios Linux

Vamos a utilizar para este caso un servidor Linux en una raspberry pi 3.

Lo que pretendemos es a las rutas:

```
 /home
/home/raspberry/descargas
/var/www/
```

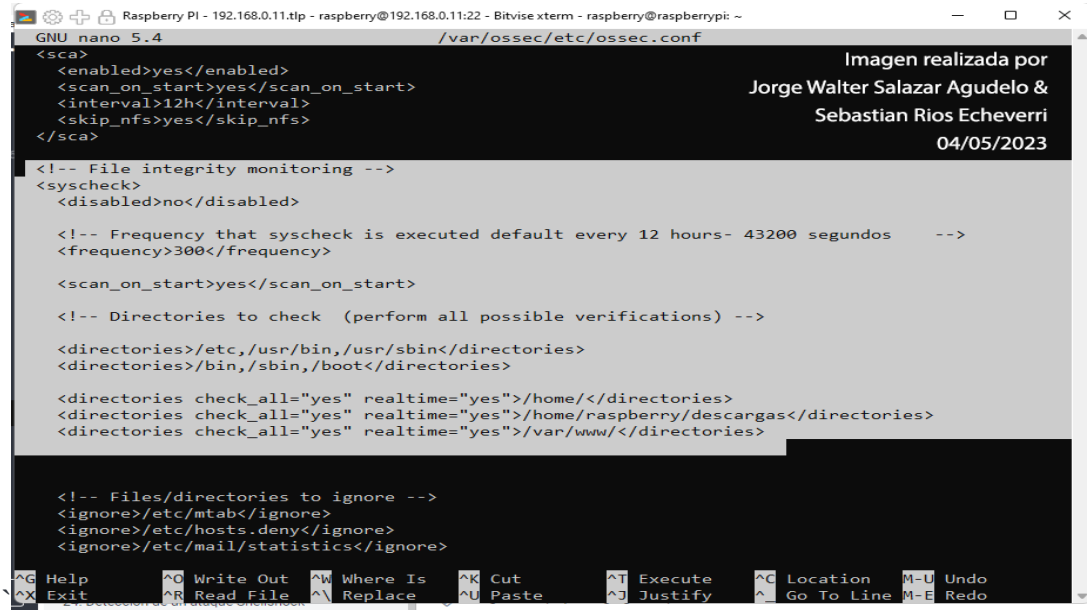
Estos Directorios sean escaneados de malware cada que descargamos algo en ellos o cada determinado tiempo.

Editaríamos el fichero de agente:

```
sudo nano /var/ossec/etc/ossec.conf
```

Añadiendo lo siguiente para monitorizar el directorio de subidas en tiempo real:

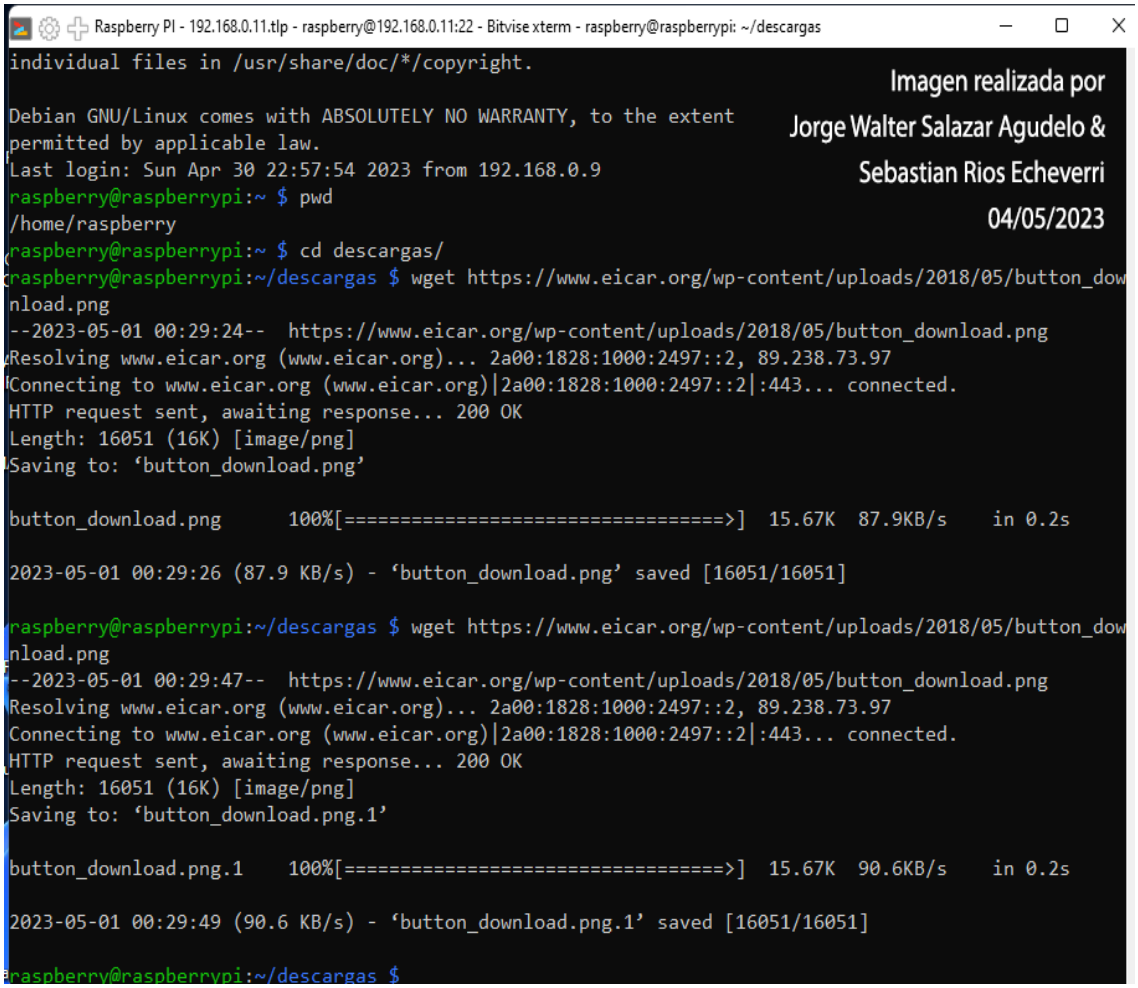
```
<syscheck>
...
<directories check_all="yes" realtime="yes">/home>
 <directories check_all="yes"
realtime="yes">/home/raspberry/descargas</directories>
 <directories check_all="yes" realtime="yes">/var/www/</directories>
...
</syscheck>
```



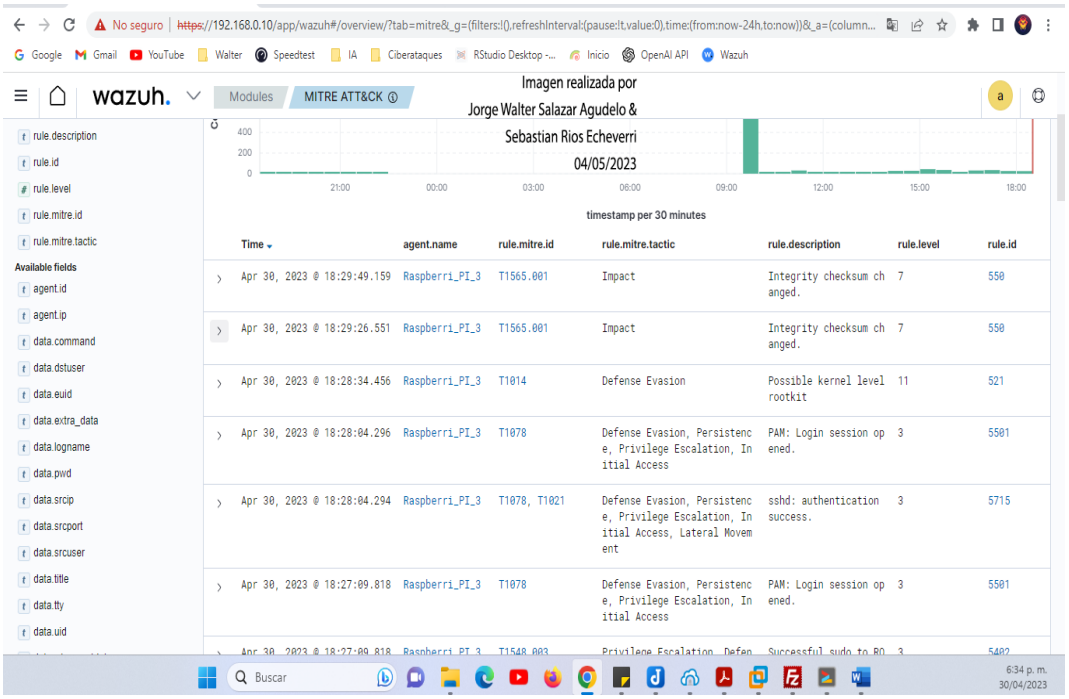
Salimos y guardamos.

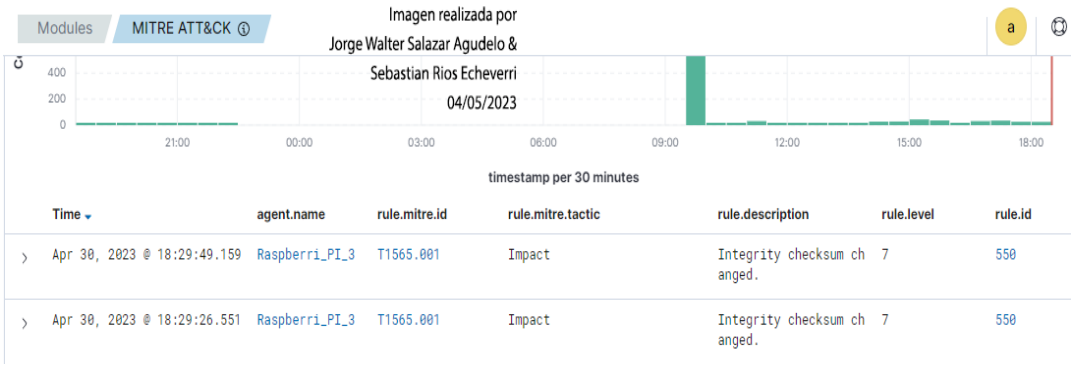
Ingresamos por ssh a la Raspberry y vamos hacer la prueba con un virus que descargaremos del siguiente Link.

wget https://www.eicar.org/wp-content/uploads/2018/05/button_download.png



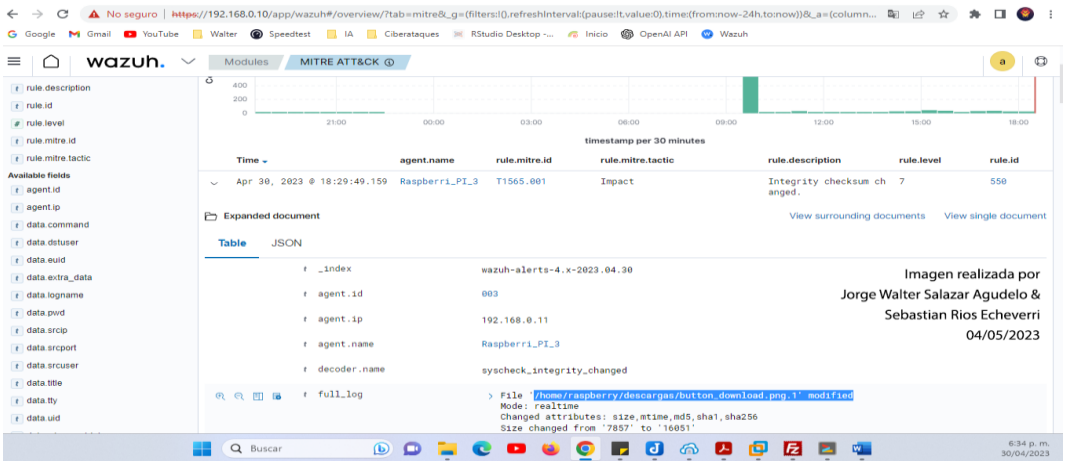
Inmediatamente Wazuh detecta una alerta nivel 7 de impacto que afecta la integridad.

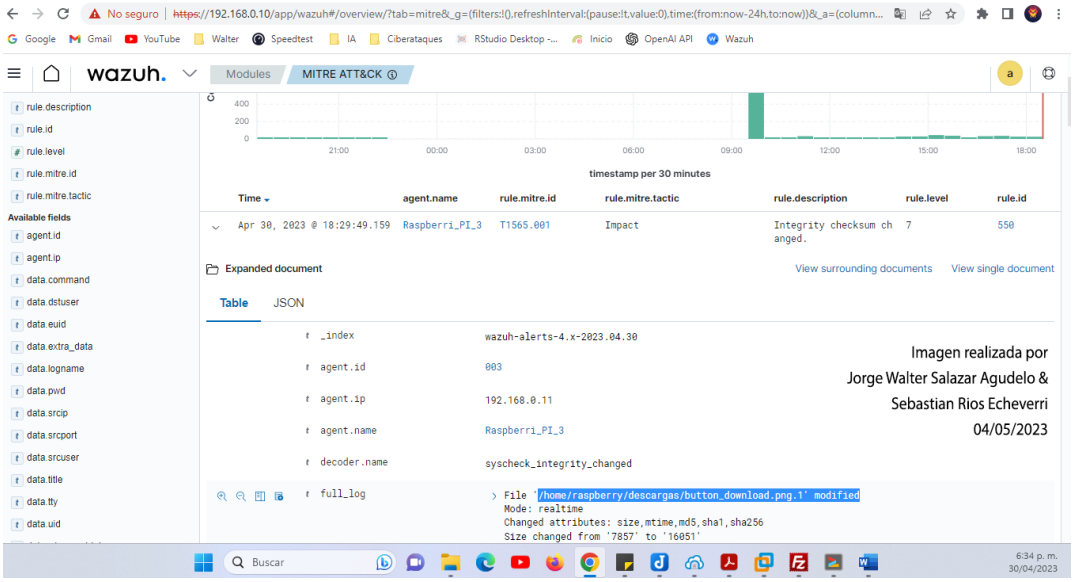


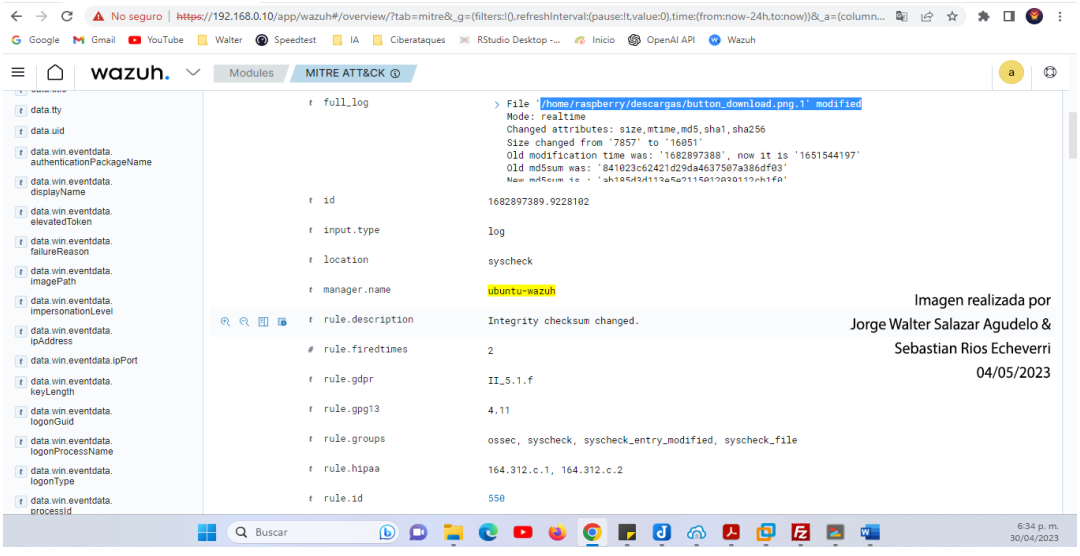


Y nos indica que la fila afectada está en la ruta

`/home/raspberry/descargas`


wazuh.
Modules
MITRE ATT&CK
timestamp per 30 minutes
Time
agent.name
rule.mitre.id
rule.mitre.tactic
rule.description
rule.level
rule.id
Apr 30, 2023 @ 18:29:49.159
Raspberri_PI_3
T1565.001
Impact
Integrity checksum changed.
7
550
Expanded document
View surrounding documents
View single document
Table
JSON
_index
wazuh-alerts-4.x-2023.04.30
agent.id
003
agent.ip
192.168.0.11
agent.name
Raspberri_PI_3
decoder.name
syscheck_integrity_changed
full_log
File '/home/raspberry/descargas/button_download.png.1' modified
Mode: realtime
Changed attributes: size,mtime,md5,sha1,sha256
Size changed from '7857' to '16051'
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023


wazuh.
Modules
MITRE ATT&CK
timestamp per 30 minutes
Time
agent.name
rule.mitre.id
rule.mitre.tactic
rule.description
rule.level
rule.id
Apr 30, 2023 @ 18:29:49.159
Raspberri_PI_3
T1565.001
Impact
Integrity checksum changed.
7
550
Expanded document
View surrounding documents
View single document
Table
JSON
_index
wazuh-alerts-4.x-2023.04.30
agent.id
003
agent.ip
192.168.0.11
agent.name
Raspberri_PI_3
decoder.name
syscheck_integrity_changed
full_log
File '/home/raspberry/descargas/button_download.png.1' modified
Mode: realtime
Changed attributes: size,mtime,md5,sha1,sha256
Size changed from '7857' to '16051'
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023


wazuh.
Modules
MITRE ATT&CK
full_log
File '/home/raspberry/descargas/button_download.png.1' modified
Mode: realtime
Changed attributes: size,mtime,md5,sha1,sha256
Size changed from '7857' to '16051'
Old modification time was: '1682897388', now it is '1651544197'
Old md5sum was: '841023c62421d29da4637507a386df03'
id
1682897389.9228102
input.type
log
location
syscheck
manager.name
ubuntu-wazuh
rule.description
Integrity checksum changed.
rule.firedtimes
2
rule.gdpr
II_5.1.f
rule.gpg13
4.11
rule.groups
ossec, syscheck, syscheck_entry_modified, syscheck_file
rule.hipaa
164.312.c.1, 164.312.c.2
rule.id
550
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023

Utilizar Fim Para Monitoreo De Descargas En Directorios Windows

Para monitorear carpetas en un agente Windows en una ruta específica para este caso la ruta:

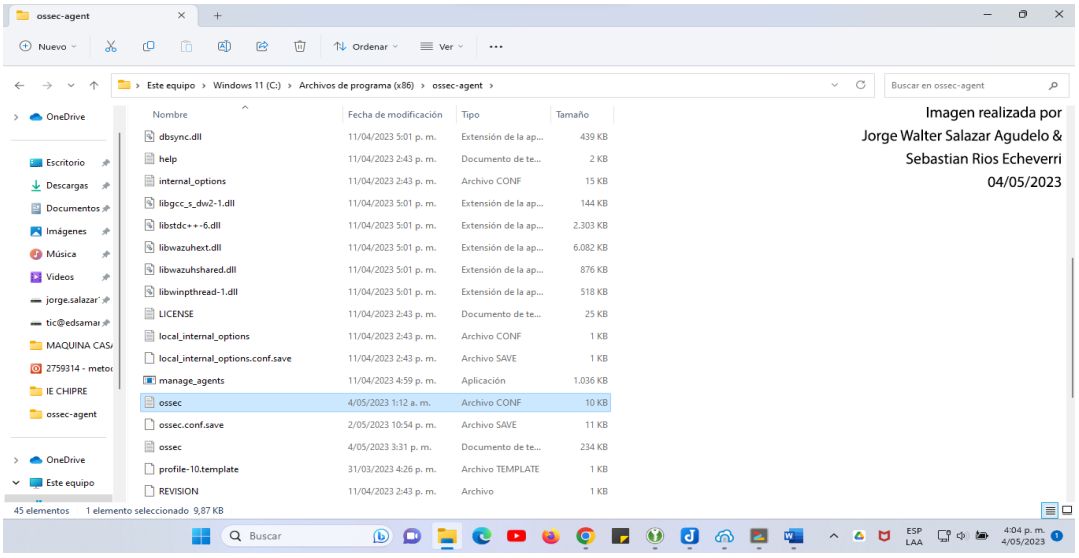
```
 D:\WALTER\Downloads
 Buscamos el archivo ossec.conf , que lo podrá encontrar en la ruta :
C:\Program Files (x86)\ossec-agent\ossec.conf
Allo mofificaremos el archivo ossec.conf agregando en el <syscheck> las
siguientes líneas con la ruta del directorio de windows
```

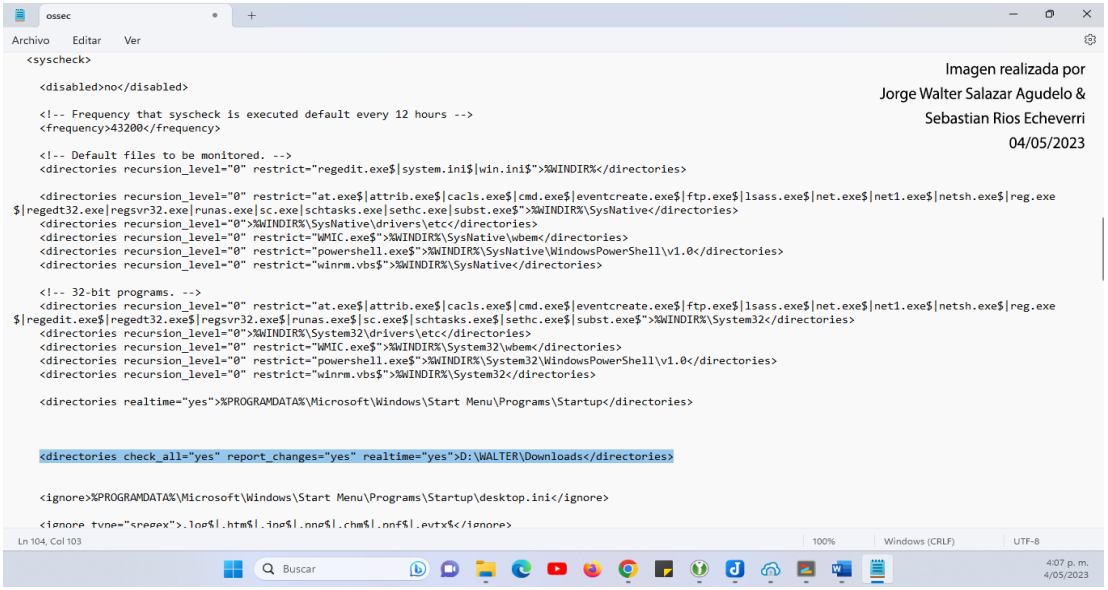
Ejemplo:

```
<syscheck>
.................................

<directories check_all="yes" report_changes="yes"
realtime="yes">C:\Users\<USER_NAME>\Desktop</directories>
```

Para este caso sería así con la ruta que en mi caso necesito:

```
<directories check_all="yes" report_changes="yes"
realtime="yes">D:\WALTER\Downloads</directories>
```





Guardamos los cambios y reiniciamos el servicio en powershell en windows

```
Restart-Service -Name wazuh
```

Probar la configuración:

Nos notificara cuando un archivo sea editado y eliminado y nos revisara los archivos descargados en la carpeta descargas.

Ejemplo:

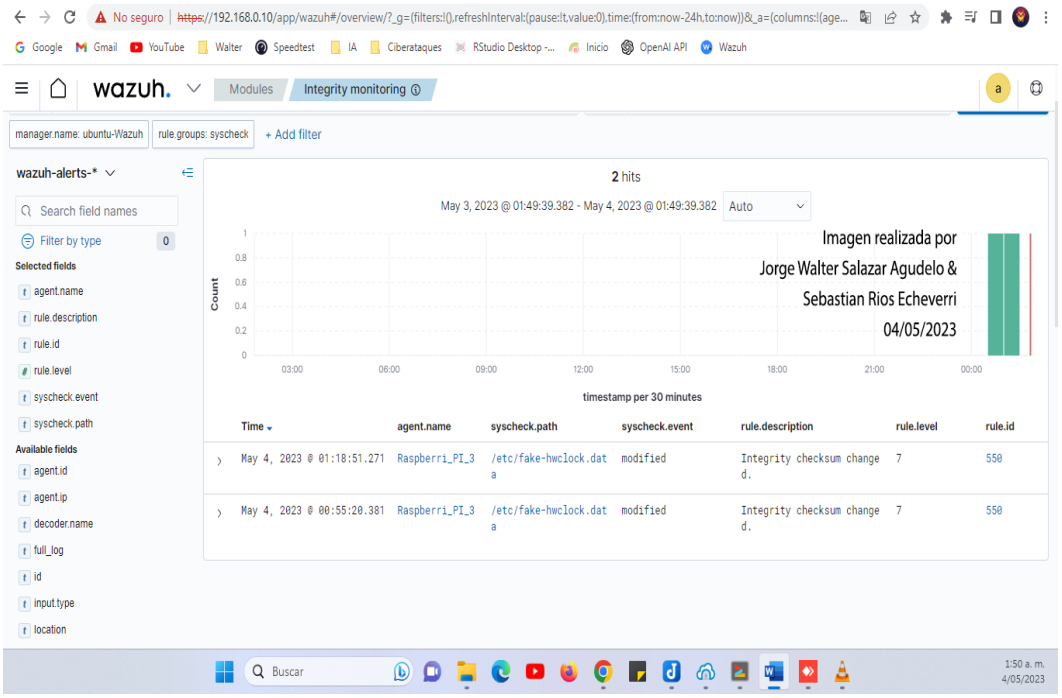
1. Cree un archivo de texto en el directorio monitoreado y luego espere 5 segundos.
2. Agregue contenido al archivo de texto y guárdelo. Espere 5 segundos.
3. Elimine el archivo de texto del directorio supervisado.

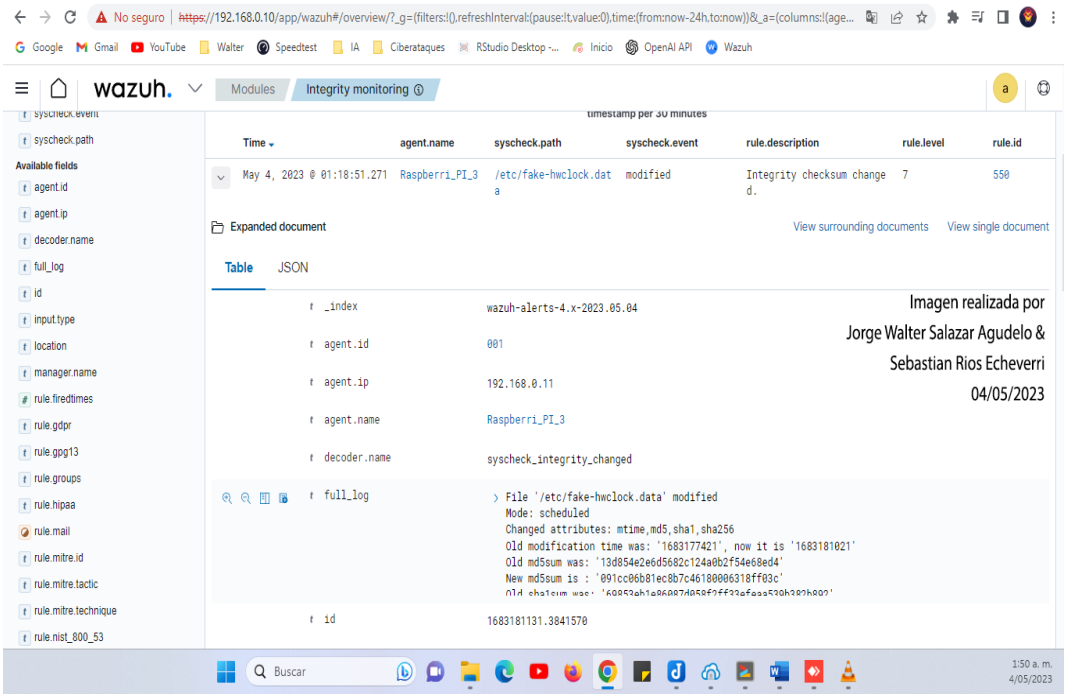
Vamos a copiar atube cátcher .exe que es un aplicativo que se descarga y virustotal reconoce virus en el, y lo vamos a descargar en la carpeta descargas

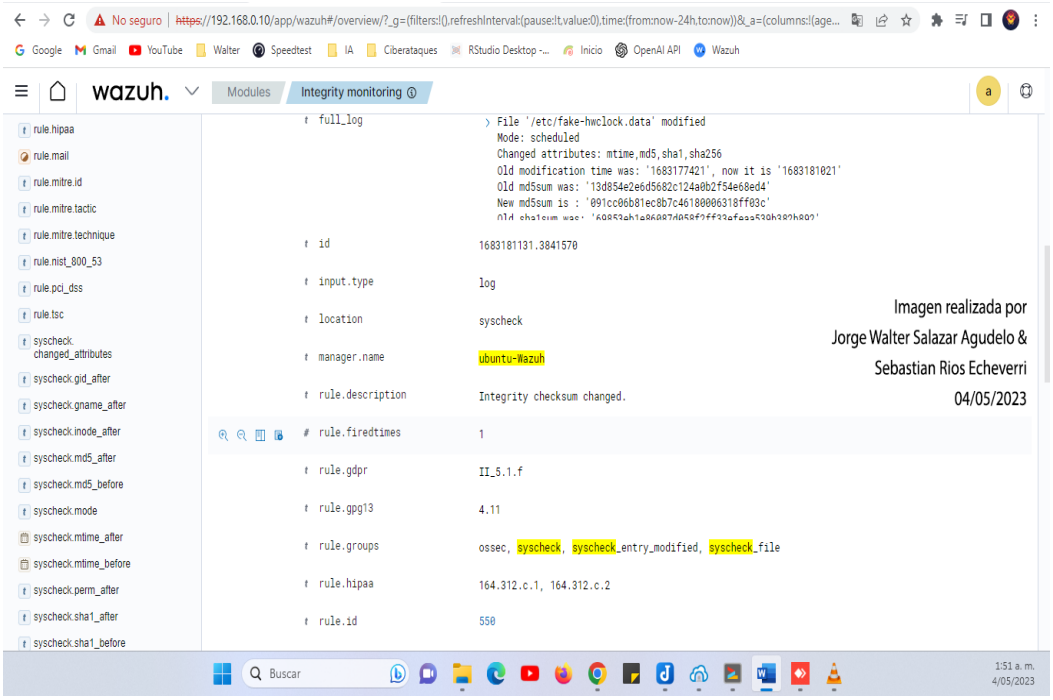
Visualización en wazuh:

Vera en el Dashboard alertas de seguridad en alertas como: `ubuntu-rule.id: is one of 550,553,554`

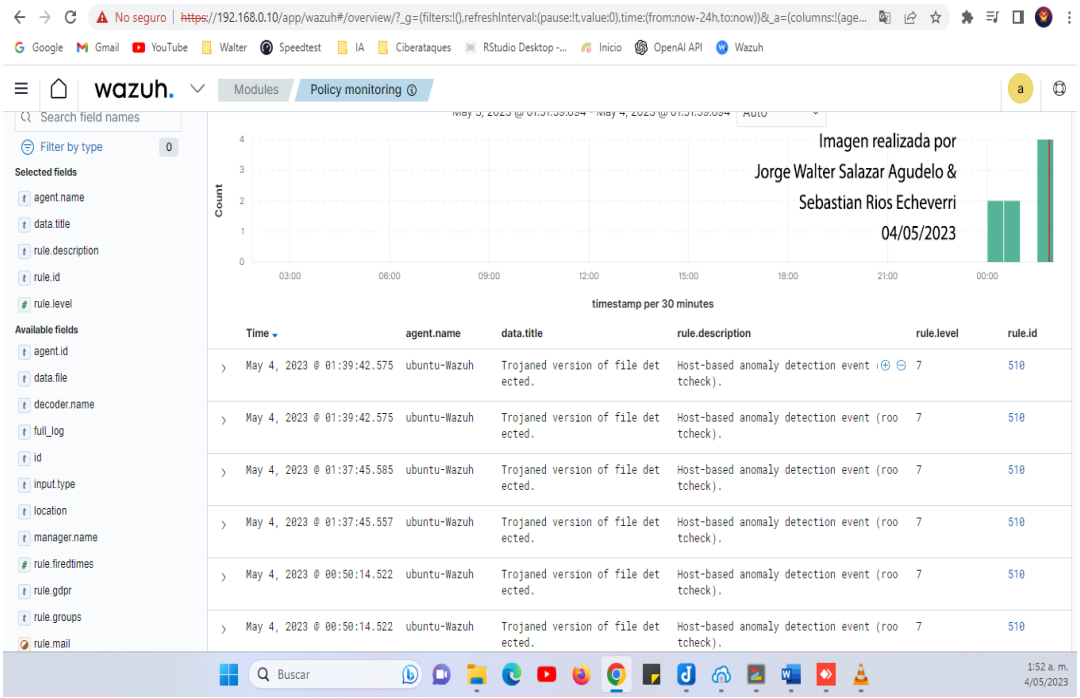
Rasberry pi

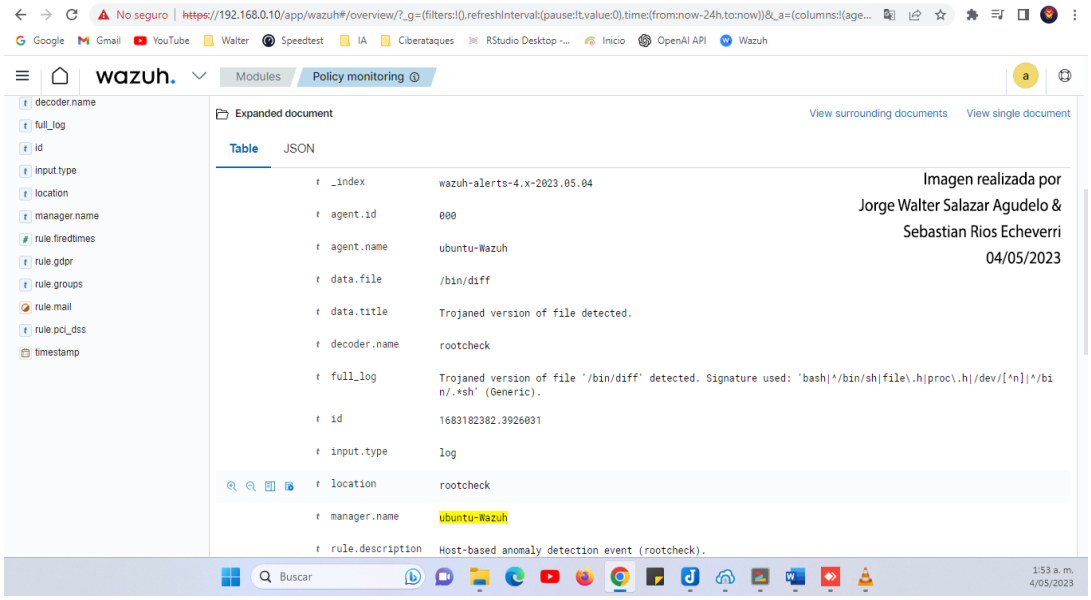

wazuh.
Modules
Integrity monitoring
manager.name: ubuntu-Wazuh
rule.groups: syscheck
+ Add filter
wazuh-alerts-*
2 hits
May 3, 2023 @ 01:49:39.382 - May 4, 2023 @ 01:49:39.382
Auto
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023
timestamp per 30 minutes
Time
agent.name
syscheck.path
syscheck.event
rule.description
rule.level
rule.id
May 4, 2023 @ 01:18:51.271
Raspberri_PI_3
/etc/fake-hwclock.data
modified
Integrity checksum changed.
7
550
May 4, 2023 @ 00:55:20.381
Raspberri_PI_3
/etc/fake-hwclock.data
modified
Integrity checksum changed.
7
550


wazuh.
Modules
Integrity monitoring
Expanded document
View surrounding documents
View single document
Table
JSON
_index
wazuh-alerts-4.x-2023.05.04
agent.id
001
agent.ip
192.168.0.11
agent.name
Raspberri_PI_3
decoder.name
syscheck_integrity_changed
full_log
File '/etc/fake-hwclock.data' modified
Mode: scheduled
Changed attributes: mtime,md5,sha1,sha256
Old modification time was: '1683177421', now it is '1683181021'
Old md5sum was: '13d854e2e6d5682c124a0b2f54e68ed4'
New md5sum is : '091cc06b81ec8b7c46180006318ff03c'
id
1683181131.3841570
Imagen realizada por
Jorge Walter Salazar Agudelo &
Sebastian Rios Echeverri
04/05/2023

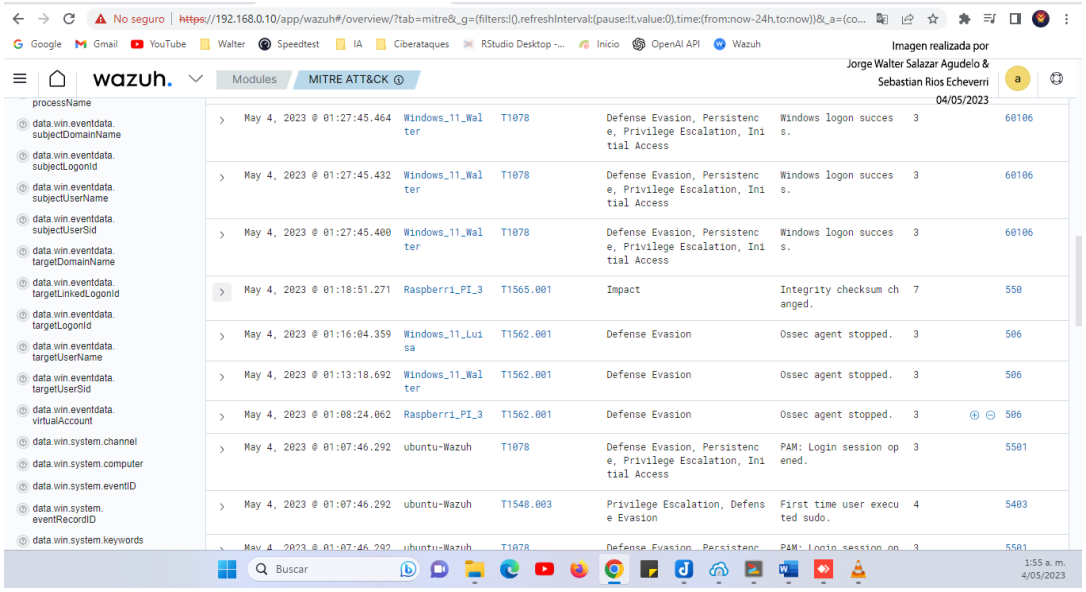


Servidor wazuh





Ejemplo Mitre Att&Ck



Universidad® Católica de Manizales

VIGILADA MINEDUCACIÓN

Obra de Iglesia de la Congregación

Hermanas de la Caridad
Dominicas de La Presentación
de la Santísima Virgen

Universidad Católica de Manizales
Carrera 23 # 60-63 Av. Santander / Manizales - Colombia
PBX (6)8 93 30 50 - www.ucm.edu.co