UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES: Ing. Nelson Augusto Pillajo Casillas

Ing. Víctor Andrés Burgos Buenaño

Ing. José Andrés Arias Barros

Ing. Franklin Giovanny Gonzalez Taipe

TUTOR: Ing. Ronie Stalin Martinez Gordon, Mtr.

Simulación de ataques ofensivos basados en APT38 y control centralizado de gestión de eventos implementando Wazuh

QUITO – ECUADOR | 2024

APROBACIÓN DE TUTOR

Yo, Ronie Stalin Martinez Gordon certifico que conozco a los autores Nelson Augusto Pillajo Casillas, Víctor Andrés Burgos Buenaño, José Andrés Arias Barros, Franklin Giovanny Gonzalez Taipe, del presente trabajo siendo la responsable exclusiva tanto de su originalidad y autenticidad, como de su contenido.

Ronie Stalin Martinez Gordon
TUTOR DE TESIS

CERTIFICACIÓN DE AUTORIA

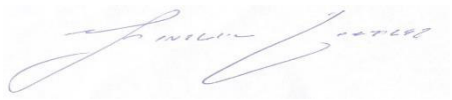
Nosotros, Nelson Augusto Pillajo Casillas, Víctor Andrés Burgos Buenaño, José Andrés Arias Barros, Franklin Giovanny Gonzalez Taipe, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos los derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Nelson Augusto Pillajo Casillas
C.I: 1723583348

Víctor Andrés Burgos Buenaño
C.I: 1723962807

José Andrés Arias Barros
C.I: 1722798996



Franklin Giovanny Gonzalez Taipe
C.I: 1720500261

RESUMEN

Los ciberataques en el Ecuador en los últimos años han aumentado en gran magnitud vulnerando sus sistemas a todo nivel, considerando objetivos como son organizaciones públicas y privadas atentando con la confidencialidad, integridad y disponibilidad. Las amenazas avanzadas persistentes son utilizadas como un tipo de ataque sigiloso que permanece vivo y oculto por periodos de tiempo extendidos. En la presente investigación se ha identificado un tipo de APT que orienta sus esfuerzos en bancos, instituciones financieras, casinos, intercambios de criptomonedas, terminales del sistema SWIFT, cajeros automáticos desde al menos el año 2014; nos referimos al APT38 y tiene como patrocinador al Estado Norcoreano. Se estudia cuáles son las técnicas utilizadas por el grupo APT38 para vulnerar los sistemas con el uso del simulador Caldera MITRE, el mismo utiliza la plantilla de habilidades del adversario y las operaciones utilizadas a menudo, una vez ejecutada la simulación al tener el agente instalado del SIEM Wazuh, alertaría de los intentos de vulneración de los servidores Windows Server sujetos del entorno de evaluación.

PALABRAS CLAVE: APT, vulnerabilidad, ciberataques

ABSTRACT

Cyberattacks in Ecuador in recent years have increased greatly, violating its systems at all levels, considering objectives such as public and private organizations, violating confidentiality, integrity and availability. Advanced persistent threats are used as a type of stealth attack that remains live and hidden for extended periods of time. In this research, a type of APT has been identified that focus its efforts in banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system terminals, ATMs and assets since at least 2014. We are referring to APT38 and its sponsor to the North Korean State. The techniques used by the APT38 group to violate the systems are studied with the use of the Caldera MITER simulator, which uses the adversary's skills template and the operations often used, once the simulation has been run by having the Wazuh SIEM agent installed. Wazuh would alert to compromise attempts on Windows Servers subject to the evaluation environment.

KEYWORDS: APT, vulnerability, cyber attacks

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO 1. INTRODUCCIÓN

1.1 Antecedentes de la situación del objeto de estudio

La naturaleza de los ataques informáticos ha sido cambiada ampliamente al entrar en la guerra cibernética por el campo de las guerras clásicas. Los ataques informáticos modernos suelen ser blanco de ataques y actúan basados en objetivos más definidos y organizados que los ataques oportunistas convencionales. Los ataques basados en Amenazas Persistentes Avanzadas (APT) son considerados como los ataques más recientes y significativos de este tipo que generalmente son diseñados y llevados a cabo por organizaciones subversivas, gobiernos, grupos profesionales, etc. para alcanzar sus objetivos estratégicos. El modelado, el análisis, la identificación y la confrontación con estos ataques son nuevos retos en el ámbito de la seguridad informática (Singh S. Sharma P. K. Moon S. Y. Moon D. & Park J. H, 2019).

En el complejo mundo de la ciberseguridad, las APT se han erigido como una forma de ataque, retando a las defensas tradicionales y poniendo a prueba la resiliencia de las organizaciones. En este contexto, la implementación de un enfoque de defensa en profundidad se presenta como una estrategia vital para contrarrestar estas amenazas en constante evolución (Felipe, 2017).

Esta investigación se enfoca en las simulaciones de ataques APT, estudiando la sofisticación de estas amenazas y cómo una perspectiva de defensa en profundidad, respaldado por la implementación de Security Information and Event Management (SIEM), puede fortalecer significativamente la seguridad de una organización.

Las simulaciones de ataques APT no solo ofrecen una visión inigualable de las tácticas y técnicas empleadas por actores maliciosos, sino que también brindan una oportunidad para evaluar la robustez de las defensas cibernéticas. En este estudio, nos

enfocaremos en la intersección analítico entre la detección proactiva, la respuesta eficiente y la planificación estratégica en la lucha contra amenazas APT (Besteiro-Calvo, L, 2016).

La implementación efectiva de SIEM emerge como un pilar esencial en esta defensa en profundidad, permitiendo la recopilación, correlación y análisis inteligente de eventos de seguridad en tiempo real. Esta herramienta no solo actúa como un "guardia digital" sino que también se convierte en un componente clave para anticipar y mitigar amenazas avanzadas de manera proactiva.

Al explorar la convergencia de simulaciones de ataques APT y defensa en profundidad con SIEM, este estudio busca aclarar sobre las estrategias más efectivas para salvaguardar la integridad de los sistemas de información en un entorno digital cada vez más desafiante y en constante cambio. Desde el análisis de amenazas hasta la implementación práctica de soluciones de seguridad, esta investigación se dirige a que no solo amplía nuestro entendimiento de las APT, sino que también ofrece perspectivas para fortalecer la resiliencia cibernética organizacional (K. O. Detken T. Rix C. Kleiner B. Hellmann and L. Renners, 2015).

1.2 Contextualización del Problema

En la actualidad pequeñas, medianas y grandes empresas están expuestas a ataques cibernéticos recurrentes, en conjunto con los crecientes ataques de las Amenazas Persistentes Avanzadas (APT), desafían las defensas tradicionales. Las simulaciones de ataques APT permiten evaluar de manera realista las nuevas defensas, identificar vulnerabilidades y mejorar la resiliencia contra amenazas avanzadas.

La estrategia de defensa en profundidad, enfocada en capas de seguridad superpuestas, se optimizará mediante la integración de simulaciones APT.

El proyecto también explorará el papel estratégico del SIEM en la detección temprana y respuesta efectiva a amenazas cibernéticas.

Además, este proyecto abordará de manera efectiva la necesidad urgente de fortalecer las defensas contra APT, mejorando la preparación ante amenazas cibernéticas en constante evolución.

Una amenaza persistente avanzada (APT) es un ciberataque sofisticado y prolongado en el que un intruso obtiene acceso a una red y permanece sin ser detectado durante un período prolongado. Los ataques APT se planifican y diseñan cuidadosamente para infiltrarse en una organización específica, evadir las medidas de seguridad existentes y pasar desapercibidos. Los atacantes suelen ser equipos de ciberdelincuentes experimentados y bien financiados que atacan a organizaciones de alto valor. Los objetivos de las APT se dividen en cuatro categorías generales: ciberespionaje, delitos electrónicos con fines de lucro, hacktivismo y destrucción.

1.3 Estudio del Arte

La seguridad se debe tener en cuenta proactivamente como defensa contra eventos que pueden desembocar en vulnerabilidades explotables, estos atentan contra el activo más importante que es la información.

Hay dos criterios generales para detectar ataques APT:

1) enfoques que buscan firmas de ataque (como intentar infectar el sistema de la víctima, intentar comunicarse con los centros C&C e intentar destruir o robar información), y

2) enfoques que buscan modelar todo el proceso de ataque. Modelar ataques APT mediante cadenas de Markov ocultas, árboles de toma de decisiones y máquinas de estado

basadas en pasos de ataque y comportamiento recíproco del atacante y el defensor son algunos ejemplos de métodos utilizados en la segunda categoría.

Al documentar reglas predictivas, personalizables de alertas basados en las simulaciones de ataques de APTs dirigidos, documentamos casos de uso para evitar intrusiones no autorizadas y generamos defensa en profundidad.

1.4 Importancia y Alcance

Elaborar un entorno informático controlado para simular ataques APT38, evaluarlos con el enfoque de seguridad ofensiva y hacking ético, realizando el análisis mediante MITRE Caldera que es una plataforma de seguridad cibernética diseñada para automatizar fácilmente la emulación de adversarios, ayudar a los equipos rojos manuales y automatizar la respuesta a incidentes para dar frente a las amenazas informáticas que día a día aplican mejores técnicas para la propagación e infección (Mitre, 2024). Conocer su definición, cómo se va a llevar a cabo y las características principales de las amenazas. Posteriormente, se realizará las instalaciones y configuraciones de la estación de trabajo a utilizar con sistema operativo Windows 10 como objetivo de los ataques APT38 con la finalidad de validar la efectividad de la solución ante las amenazas. Finalmente, se identificará el gestor de eventos Wazuh para detectar, responder y neutralizar las amenazas informáticas.

Para evitar ser descubiertos por los sistemas de seguridad, los atacantes de APT a menudo ocultan sus operaciones utilizando herramientas y procesos legítimos, ofuscación de código y medidas anti-análisis. El mayor peligro de los ataques APT es que incluso cuando son descubiertos, los atacantes pueden haber dejado múltiples puertas traseras abiertas que les permiten regresar cuando así lo deseen. Se requiere una combinación de múltiples medidas, que van desde soluciones de seguridad sofisticadas hasta puntuaciones de vulnerabilidad y

métricas de probabilidad, para detectar y mitigar el ataque APT (Bart Lenaerts-Bergmans, 2023).

1.5 Delimitación

Se realizará las pruebas de seguridad ofensiva en un ambiente controlado con la herramienta "Automatización de la emulación del adversario" con MITRE Caldera en un entorno virtualizado con la aplicación vmware, sistema operativo Ubuntu y Windows Server que es el objetivo del ataque simulado por APT38 y la consola del SIEM Wazuh OVA que registrara los eventos generados en el dashboard del SIEM.

1.6 Objetivos

1.6.1. Objetivo General

Crear el entorno informático para la simulación de ataques APT38, en un ambiente seguro controlado para monitorear las acciones ofensivas, defensivas y que permita responder con la brevedad del caso para evitar daños perjudiciales a la infraestructura.

1.6.2. Objetivos Específicos

- Conocer las tácticas utilizadas por grupos maliciosos y en específico APT38, mediante simulaciones de ataques ofensivos.
- Establecer un entorno virtual simulado de ataques APT38, que permita identificar proactivamente eventos de seguridad con reglas de correlación especificas en el SIEM Wazuh.
- Ejecutar ataques simulados APT en base a las plantillas de pruebas de MITRE ATT&CK, en específico APT38.

CAPÍTULO 2. MÉTODO

2.1 Marco Teórico

2.1.1. Ataques APT

La definición para ataques APT se puede tomar en base al siguiente concepto (Giura, P., & Wang, W. (2012):

- Avanzados (A): Los atacantes APT son sofisticados y bien organizados, sus recursos financieros se suministran, y utilizan amplias tecnologías de intrusión, acceso a datos y herramientas de manipulación de datos.

- Persistente (P): Los ataques basados en APT se mantienen estables a largo plazo. Los atacantes buscan un objetivo altamente prioritario y específico en lugar de metas instantáneas y temporales y mantienen su presencia en la red de víctimas durante mucho tiempo (acción lenta y permanente).

- Amenaza (T): Los atacantes quieren dañar, perturbar y/o robar datos o servicios específicos.

La tecnología es dinámica y en constante avance, se expande a pasos agigantados, también genera millones de nuevas amenazas, vulnerabilidades que deben tener un tratamiento preventivo de alerta, análisis para su contención y respuesta.

2.1.2. Etapas de ataques APT

Los pasos de un ataque basado en APT se pueden considerar de la siguiente manera:

- Reconocimiento: los atacantes en este paso recopilan datos sobre los recursos, los empleados y las relaciones de la organización objetivo con otras instituciones para obtener los objetivos mencionados.
- Entrega: este paso incluye realizar un correo electrónico o un enlace de código destructivo basado en los datos recopilados en el paso anterior y enviarlo a través de un servidor de Internet válido o evaluar a los usuarios de la organización para acceder a ese enlace.
- Explotación: después de que una víctima ejecuta el código destructivo, el atacante crea la ruta de ataque y brinda la posibilidad de explotación. El siguiente paso es configurar un centro C&C para gestionar todas las comunicaciones con el sistema víctima.
- Operaciones: este paso incluye la presencia del atacante (por ejemplo, mediante malware o código malicioso) en la red de la organización víctima y su explotación durante un largo período.
- Recopilación de datos: el atacante recopila los datos del objetivo en este paso a través de los permisos de acceso obtenidos en los pasos anteriores. Además, en este paso se ejecutan otras acciones como cambiar la configuración o dañar sistemas.
- Exfiltración: en este paso, la información obtenida se empaqueta y codifica con precisión y se envía a los servidores predeterminados. Además, el atacante intenta limpiar su rastro de presencia en el sistema víctima.

Los pasos mencionados anteriormente de un ataque basado en APT se conocen como Intrusion Kill Chain (IKC). Los pasos IKC normalmente son comunes en los ataques APT, y lo que distingue a los ataques APT es el objetivo del ataque y las técnicas utilizadas en cada etapa. Los atacantes utilizan diversas técnicas nuevas y sofisticadas para obtener los objetivos de ataque en cada paso del IKC que generalmente dejarán un rastro muy ligero en forma de alertas de bajo riesgo. El atacante utiliza todo tipo de técnicas de engaño, ocultamiento, cifrado e imitación de comportamiento normal, además de utilizar ataques nuevos y variados para reducir su probabilidad de detección. Este asunto suele mover las alertas generadas por los sensores de seguridad por debajo del nivel del umbral de detección (por ejemplo, alertas de bajo riesgo) (M. Khosravi and B. T. Ladani, 2020).

2.1.3. Modelo de Intrusión APT

Aunque diferentes pasos y técnicas utilizados en cada fase de ataque pueden ser transversales, podría ser descrito por el modelo Intrusion Kill Chains que se muestra como Tabla 1. Cuando las acciones sospechosas como la vulnerabilidad escaneada, el escaneo de puertos, la grieta de la contraseña se detectó en las redes, podría inferirlo al ataque está en la etapa de reconocimiento. Después de detectar algunas acciones controladas, se pudo inferir al atacante que estaba a punto de controlar o ya había controlado el objetivo. Por lo tanto, detallar los procedimientos y técnicas de ataque ayuda a los defensores a estimar con precisión la situación actual y hacer inferencias razonables después de que se descubrió la amenaza.

Tabla 1.

Escalas y técnicas comunes de ataques de red

Intrusión	Serial	Técnicas de ataque
	1	Adquisición de información externa
Reconocimiento	2	Escaneo de vulnerabilidad
	3	Descifrado de contraseña
	4	Escaneo de puertos
	5	Flujo de paquetes
	6	Vulnerabilidades y formas de explotar
Armamento	7	Herramientas de penetración
	8	Armas de control
	9	Técnicas antivirus
	10	Spear Phishing attack
	11	Watering Hole attack
Entrega	12	Supply chain attack
	13	Proximity attack
	14	Ferry attack
Explotación	15	Desbordamiento de memoria
	16	Vulnerabilidad en la web

	17	Vulnerabilidades lógicas
	18	Escalamiento de privilegios
Instalación	19	Botnets, Trojans, worms
	20	Backdoors
	21	Rootkits
	22	WebShell
	23	Advanced Trojans
Comando y Control	24	Comando y control
	25	Covert channels
	26	Abnormal communication modes
Acciones en objetivos	27	Destruir los datos o dispositivos
	28	Fuga de datos
	29	Desconfiguración de datos
	30	Supervisión a largo plazo

Nota: Creación propia.

El desarrollo de la tecnología de ciberataque se basa esencialmente en la tecnología de defensa actual. Al mismo tiempo, el desarrollo de la tecnología de defensa es esencialmente base en las técnicas de ataque actualmente descubiertas. Por lo tanto, adherir al pensamiento de la confrontación rojo-azul, clasificar las técnicas de ataque y descubrir más nuevos métodos y nuevos modos de ataque son las formas eficaces de mejorar las capacidades técnicas de los defensores.

La mayoría de los productos de protección tradicionales adoptan tecnología de detección basada en características. Por ejemplo, los motores antivirus detectan principalmente las características de los archivos de muestras maliciosas, y los dispositivos de red como IDS y IPS se detectan principalmente las características del flujo de red. Las ventajas de la detección de funciones son identificar los archivos maliciosos conocidos o las técnicas de ataque rápidamente, y decir las amenazas con precisión. Pero las limitaciones también son obvias, si las características de las amenazas no están contenidas en la base de datos, la protección perderá su eficacia.

Por lo tanto, si nos encontramos con amenazas desconocidas, construiremos nuestra protección basada en una alta visión de la confrontación con el rojo-azul en lugar de utilizar una sola detección basada en características (Li, Y., Zhang, T., Li, X., & Li, T. ,2019).

2.1.4. Operaciones APT38

Se tiene conocimiento que al menos desde el año 2014, APT38 ha generado operaciones en más de 16 organizaciones distintas de alrededor de al menos 11 países, en ocasiones, de manera simultánea por lo que se consolida como un grupo con recursos extensos. (Ramírez,2018).

2.1.5. Características APT38

Una de las características es la larga planificación en periodos de acceso a entornos comprometidos de las distintas víctimas, además el grupo es cuidadoso al permanecer durante al menos 155 días en la red, utilizan herramientas desarrolladas a la medida con el enfoque:

- **Recopilación de información**: Comprometer las transacciones SWIFT en las redes de las víctimas.
- **Compromiso inicial**: Utiliza el ataque "watering hole" dirigido a grupos de usuarios infectando sitios web que visitan habitualmente y explota versiones desactualizadas de Apache Structs2 para ejecuciones remotas de código fuente.
- **Reconocimiento interno**: Utilizan el despliegue de malware para recopilar credenciales de las víctimas.
- **Destruir evidencias**: Elimina registros de manera segura.

2.2 Desarrollo

2.2.1. Diseño e Implementación

El capítulo considera el proceso de diseño del entorno virtualizado seguro para la automatización de pruebas ofensivas y recomendaciones generadas por el siem Wazuh para la atención de las alertas y eventos sobre el ataque APT38.

2.2.2. Consideraciones Importantes

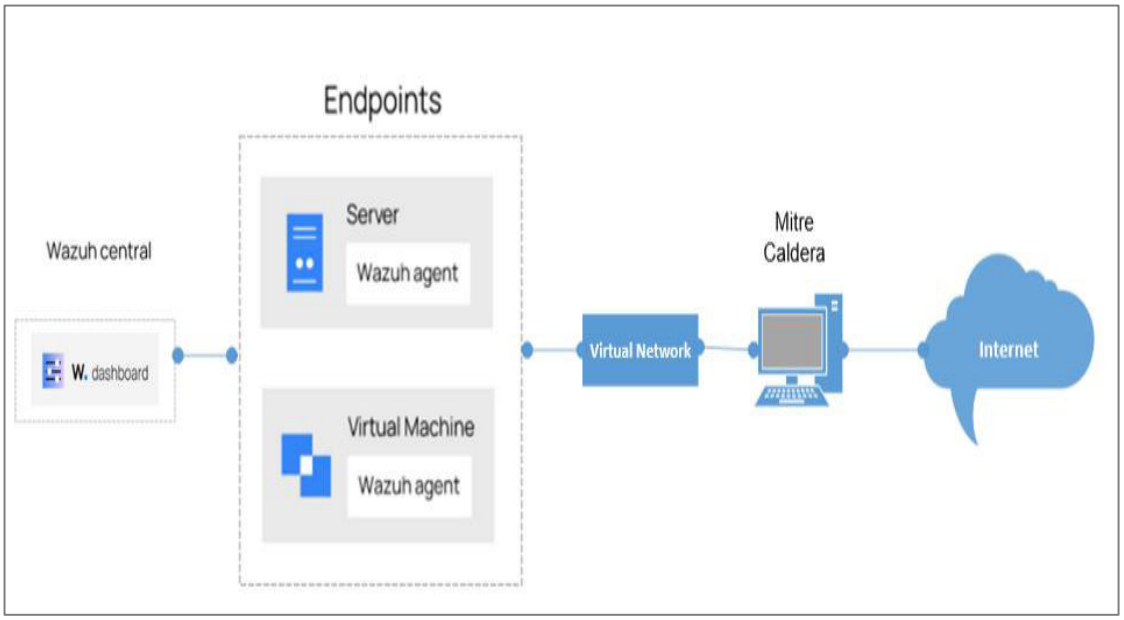
Crear el entorno informático para la simulación de ataques APT38, en el que consta una máquina con sistema operativo Linux para la implementación de MITRE Caldera, la siguiente máquina virtual sería Windows 10 como host objetivo a ser atacado, por último, se disponibilizaria la máquina virtual con la consola de administración de Wazuh, para monitorear las acciones ofensivas, defensivas y que permita responder con la brevedad del caso para evitar daños perjudiciales a la infraestructura.

2.2.3. Arquitectura

La arquitectura referencial del entorno virtualizado seguro con el que se realizará la simulación del ataque APT38 con la herramienta MITRE CALDERA a los servidores Ubuntu y Windows Server integrados con el SIEM Wazuh por medio de agentes, monitoreados los eventos además de las alertas de seguridad como se muestra en la figura 1.

Figura 1

Entorno virtualizado seguro de simulación de ataques APT38



Nota: Creación propia.

2.2.4. Especificaciones de las maquinas utilizadas

Las tablas 2, 3 y 4 especifican las características de los recursos de hardware utilizados en el entorno virtualizado seguro de simulación de ataques ATP38.

Tabla 2

Descripción de máquina Wazuh

HARDWARE	ESPECIFICACIONES
PROCESADOR	4 vCPU
MEMORIA RAM	8 GB
ALMACENAMIENTO	50 GB
SISTEMA OPERATIVO	Amazon Linux 2
ARQUITECTURA	64 bits

Nota: Creación propia.

Tabla 3

Descripción de máquina Windows

HARDWARE	ESPECIFICACIONES
PROCESADOR	4 vCPU
MEMORIA RAM	2 GB
ALMACENAMIENTO	40 GB
SISTEMA OPERATIVO	Windows 11
ARQUITECTURA	64 bits

Nota: Creación propia.

Tabla 4

Descripción de máquina Kali Linux – Caldera Mitre

HARDWARE	ESPECIFICACIONES
PROCESADOR	4 vCPU
MEMORIA RAM	2 GB
ALMACENAMIENTO	80 GB
SISTEMA OPERATIVO	Debian GNU/Linux
ARQUITECTURA	64 bits

Nota: Creación propia.

2.2.5. Instalación Wazuh OVA

El entorno virtualizado seguro de SIEM Wazuh, fue descargado del OVA Wazuh desde la página oficial de Wazuh, al cargarlo se habilita como muestra la figura 2.

Figura 2

Welcome to Wazuh

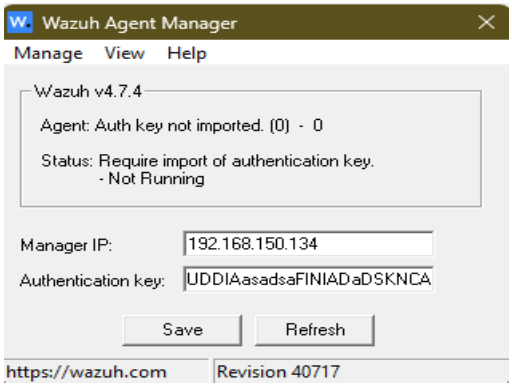
Nota: Inicio de máquina virtual Wazuh

2.2.6. Instalación agente wazuh en endpoint Windows

Para que el SIEM Wazuh registre eventos o alertas de los endpoint debe configurarse los agentes como se muestra en la figura 3.

Figura 3

Configuración agente Wazuh en windows



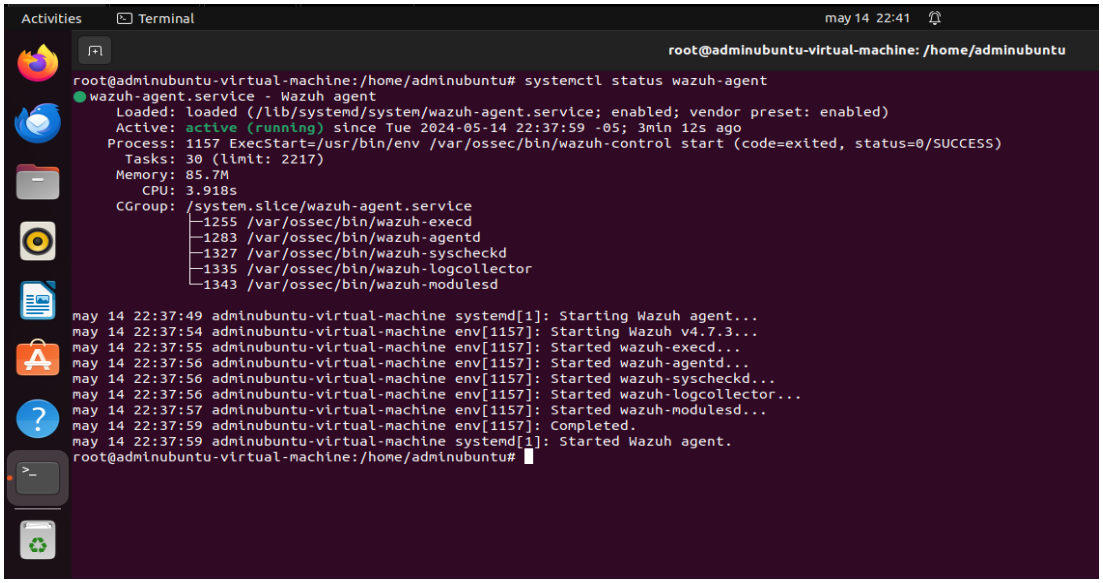
Nota: Configuración agente

2.2.7. Instalación agente wazuh en endpoint Ubuntu

Para que el SIEM Wazuh registre eventos o alertas de los endpoint debe configurarse los agentes como se muestra en la figura 4.

Figura 4

Configuración agente Wazuh en ubuntu



Nota: Configuración agente

CAPÍTULO 3. RESULTADOS

3.1 Análisis de resultados

3.1.1. Configuración Máquina Kali Linux - Caldera Mitre

Para la simulación del APT38 se ha configurado los recursos necesarios en la máquina virtual, cumpliendo con los pre requisitos para emular el entorno real de ataque. La figura 5 muestra el sistema operativo funcional.

Figura 5

Instalación de Kali Linux

Nota: Kali Linux habilitado

3.1.2. Resultados

Habilitado el entorno, se valida y comprueba su funcionamiento mediante el análisis y plantilla de ataques respecto del grupo APT38. Se menciona una síntesis de los hallazgos que muestran la integración desde el ataque APT38 al host objetivo y alerta de eventos con el SIEM Wazuh.

3.1.3. MITRE Caldera

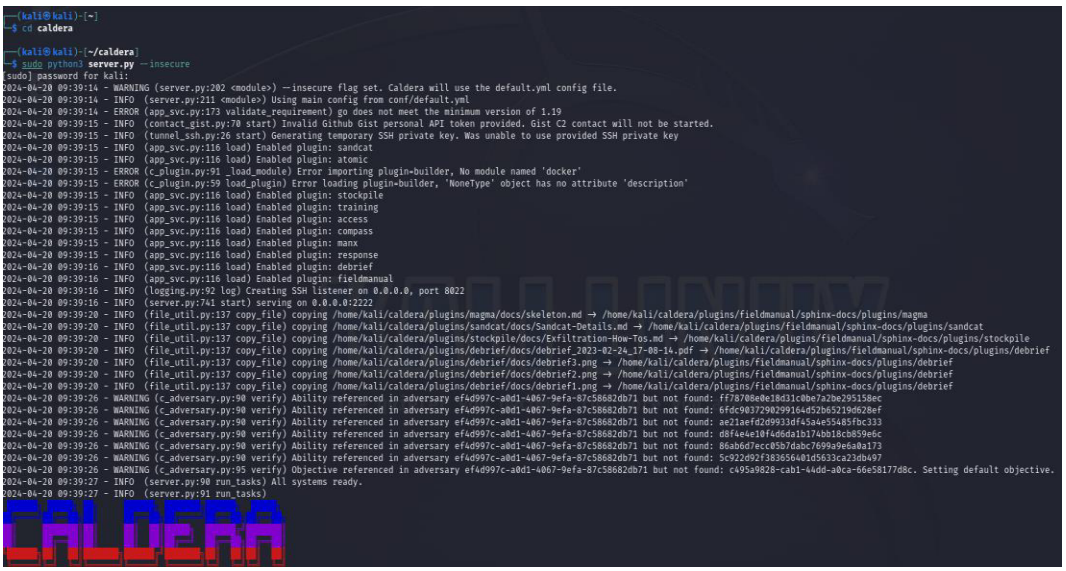
La herramienta a utilizar es Caldera que en su definición es un marco de ciberseguridad desarrollado por MITRE que permite ejecutar evaluaciones de seguridad automatizadas.

3.1.4. Interfaz MITRE Caldera

Para acceder a la interfaz gráfica de Caldera es necesario la ejecución del comando: **sudo python3 server.py --insecure** en consola como se muestra en la figura 6.

Figura 6

Ejecución servicio Caldera

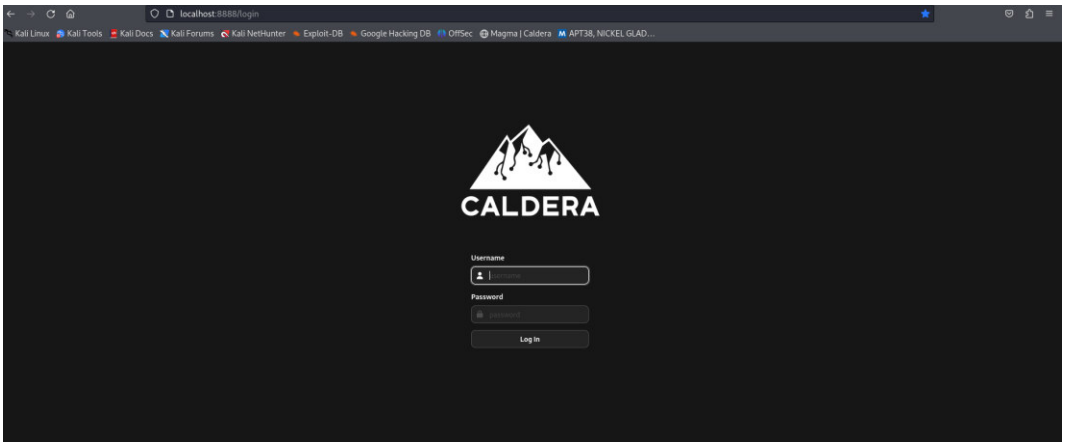


Nota: Se ha iniciado Caldera correctamente (hook.py:58 build_docs)

Al acceder desde el navegador, en nuestro caso el preconfigurado por defecto, se visualiza la aplicación similar al de la figura 7. Se muestra el login para la autenticación del usuario que desplegará los componentes necesarios para el inicio de la simulación de ataques APT38.

Figura 7

Login plataforma MITRE Caldera



Nota: Inicio de sesión para autenticación.

Para la creación del payload se necesita el ingreso de comandos que se muestran en la tabla 5 en el host objetivo.

Tabla 5

Comandos para desplegar en el host objetivo

Descripción	***Comando***
Agent	Sandcat Caldera's default agent, written in GoLang. Communicates through the HTTP(S) contact by default.
App.contact.http	http://localhost:8888
Agents.implant.name	splunkd
Linux sh	server="http://0.0.0.0:8888";curl -s -X POST -H "file:sandcat.go" -H "platform:linux" $server/file/download>

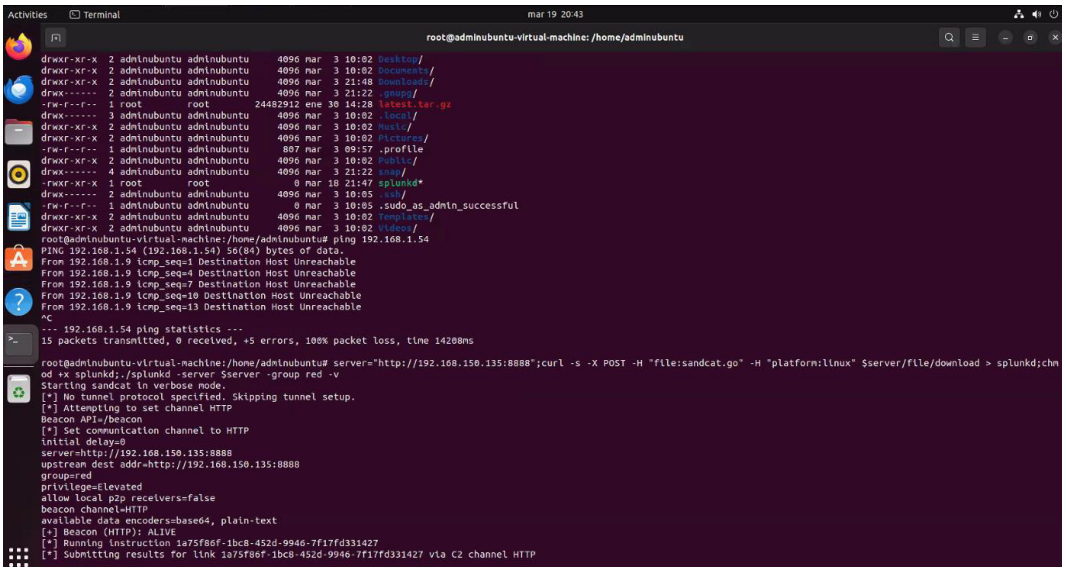
	splunkd;chmod +x splunkd;./splunkd - server $server -group red -v

Nota: Creación propia.

Una vez ejecutada la autenticación visualizamos la pantalla principal de Caldera, en la misma seleccionamos **agents**, para la configuración del payload a ejecutar en el host objetivo. La secuencia de comandos de la tabla 5, se ejecutan en el host objetivo para tomar control inicial y ejecutar la simulación de ataques APT38.

Figura 8

Ejecución secuencia de comandos en host objetivo

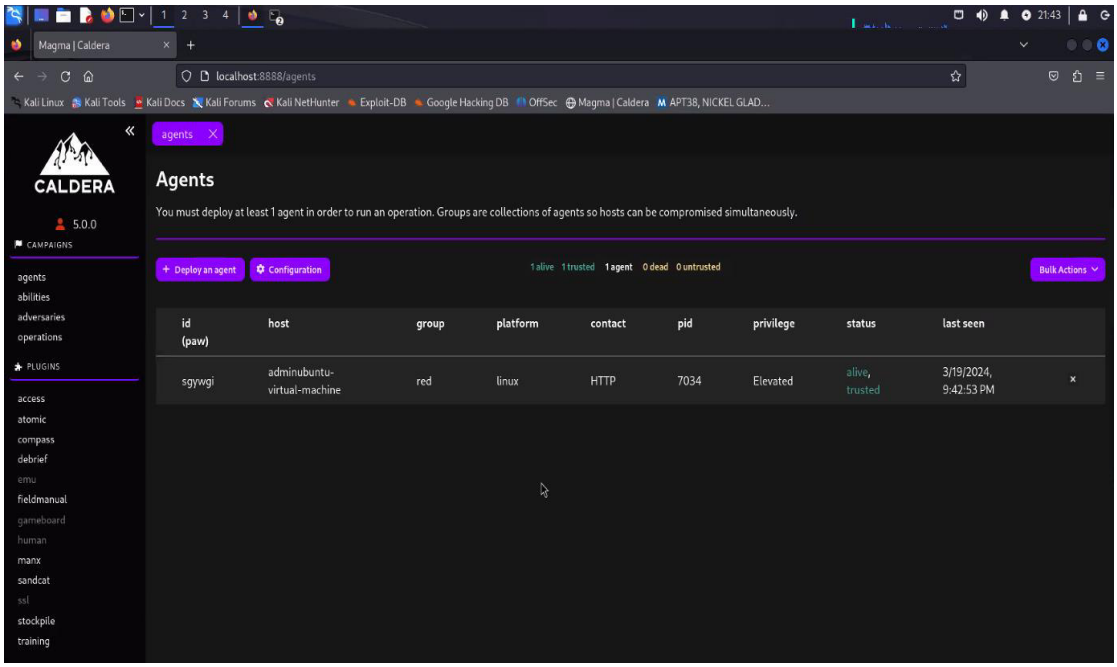


Nota: Ejecución exitosa de secuencia de comandos.

Si la ejecución fue completada con éxito, en la plataforma de Caldera mostrará el hostname (**adminubuntu-virtual-machine**) del host objetivo, como se muestra en la figura 9.

Figura 9

Agente activo y visualizado en consola Caldera



Nota: Agente activo consola MITRE Caldera

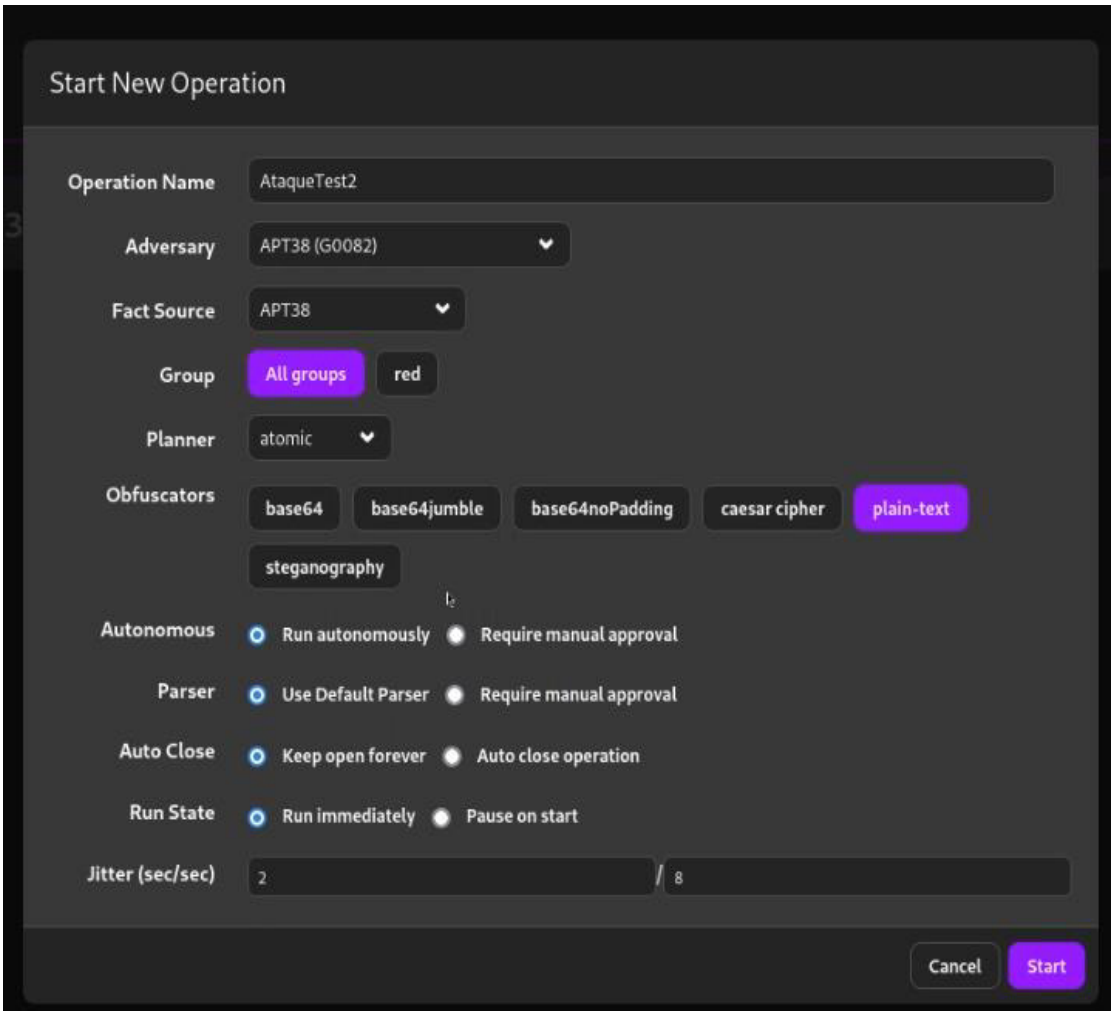
3.2 Ataque APT38

3.2.1. Capaz de navegador

MITRE ha realizado la consolidación de los ataques comunes respecto de los grupos APT, las mismas se encuentran publicadas en las plantillas de simulación de ataques (APT38) y sobre el que se carga en MITRE Caldera para el inicio de las operaciones al host objetivo, como se muestra en la figura 10.

Figura 10

Plantilla ataques APT38



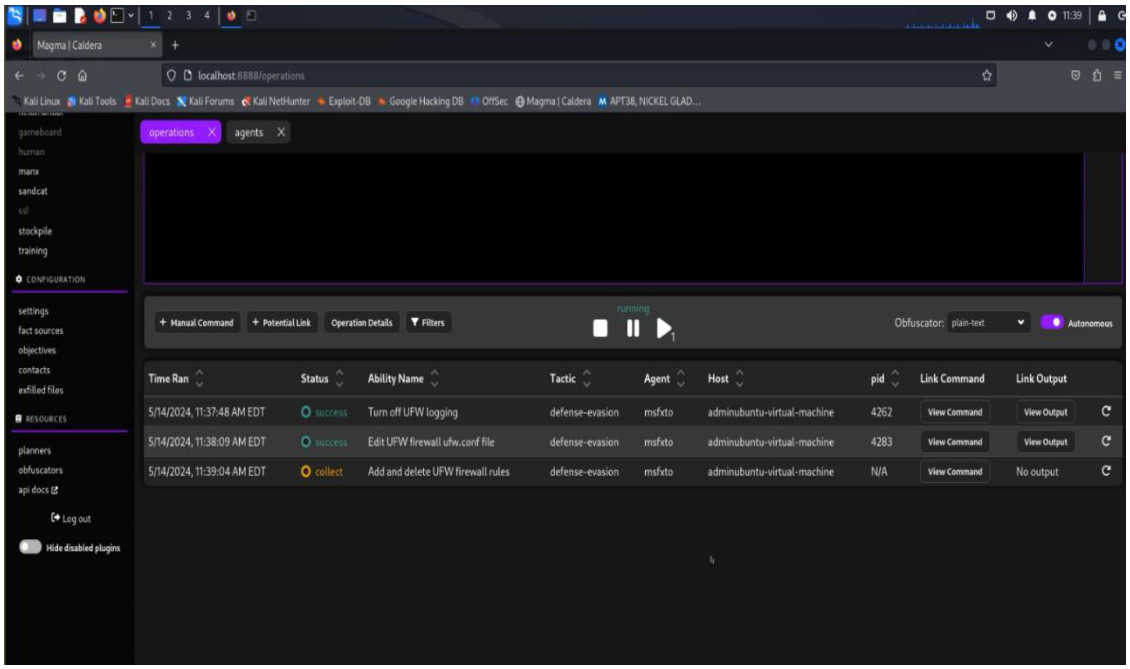
Nota: Plantilla APT38

3.2.2. Operación APT38

El inicio de la simulación de ataques APT38 hacia el host objetivo, queda sujeto al running que se lo ejecuta desde la consola de Magna/Caldera como se muestra en la figura 11.

Figura 11

Ejecución de ataques APT38



Nota: Inicio de Ataques APT38.

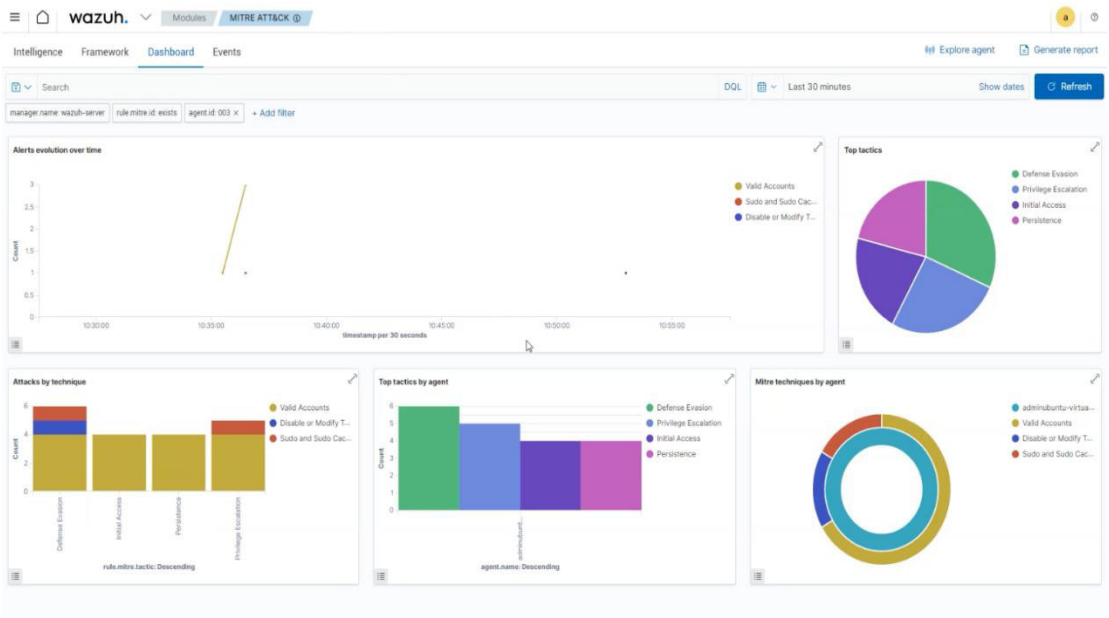
3.3 Eventos SIEM Wazuh

3.3.1. Eventos de Seguridad

El SIEM Wazuh registra los eventos del host objetivo ya que cuenta con el agente instalado para el monitoreo, en el mismo se alertan una vez iniciados los ataques APT38, como se muestra en la figura 12.

Figura 12

Eventos de seguridad ataques APT38



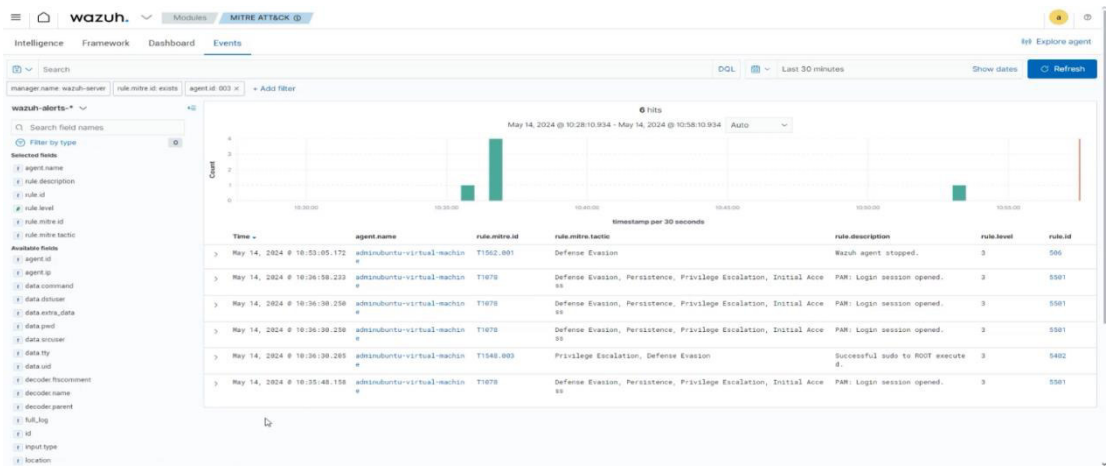
Nota: Alertas seguridad ataques APT38

3.3.2. Reglas de Seguridad

Identificado los ataques, se han mapeado las reglas en el SIEM Wazuh respecto de la simulación de las técnicas de los ataques APT38, como se muestra en la figura 13.

Figura 13

Reglas de seguridad ataques APT38



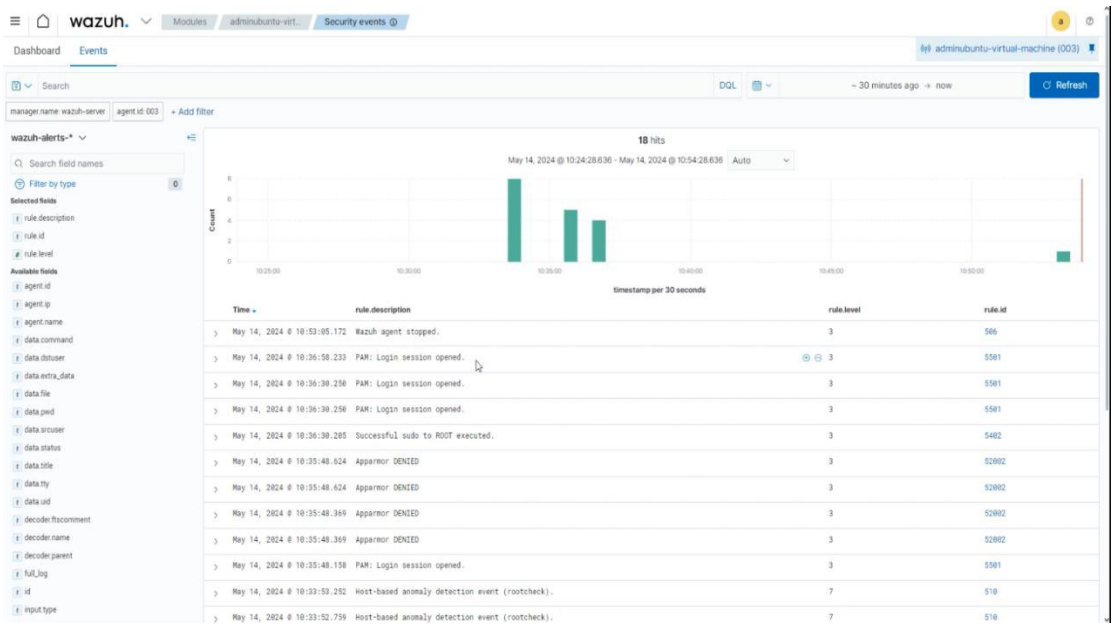
Nota: Alertas de seguridad con mapeo de reglas ataques APT38

3.3.3. Mitre ATT&CK

Las técnicas de los ataques APT38 son mapeadas en SIEM Wazuh con Mitre ATT&CK, como se muestra en la figura 14.

Figura 14

Mitre ATT&CK ataques APT38



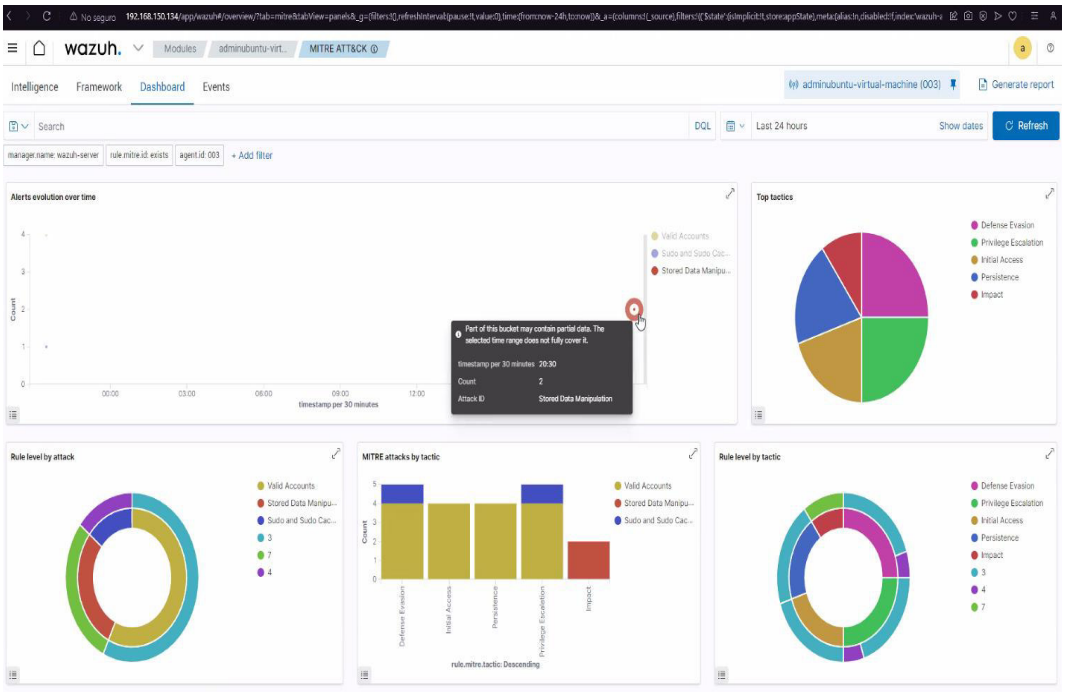
Nota: Mitre ATT&CK ataques APT38

3.3.4. Dashboard SIEM Wazuh

En el dashboard del SIEM Wazuh, se tiene las tácticas identificadas como ataques de APT38 desarrolladas por Mitre ATT&CK las mismas que son alertadas por las reglas de SIEM Wazuh, en el dasboard principal se visualiza la evolución de alertas en tiempo real incluyendo la hora y tácticas de ataque explotados visualizándolas con gráficos de barras y circulares con el detalle de las vulnerabilidades explotadas como se muestra en la figura 15.

Figura 15

Dashboard SIEM Wazuh



Nota: Dashboard SIEM Wazuh ataques APT38

Tabla 6

MITRE Técnicas utilizadas por APT38

Técnicas	***Tácticas***	***Descripción***	***Reglas ID Wazuh***
T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM Loggin session opened	5501

Nota: Creación propia.

Tabla 7

SCA – Security Configuration Assessment

Política	***Aprobadas***	***Fallidas***	***No Aplicables***	***Score***
CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0	62	99	21	38%

Nota: Creación propia.

Tabla 8

Compliance – NIST 800-53

Técnica	***NIST 800-53***
T1078	AU14
	AC7
	AU5
	AU6
	AC6

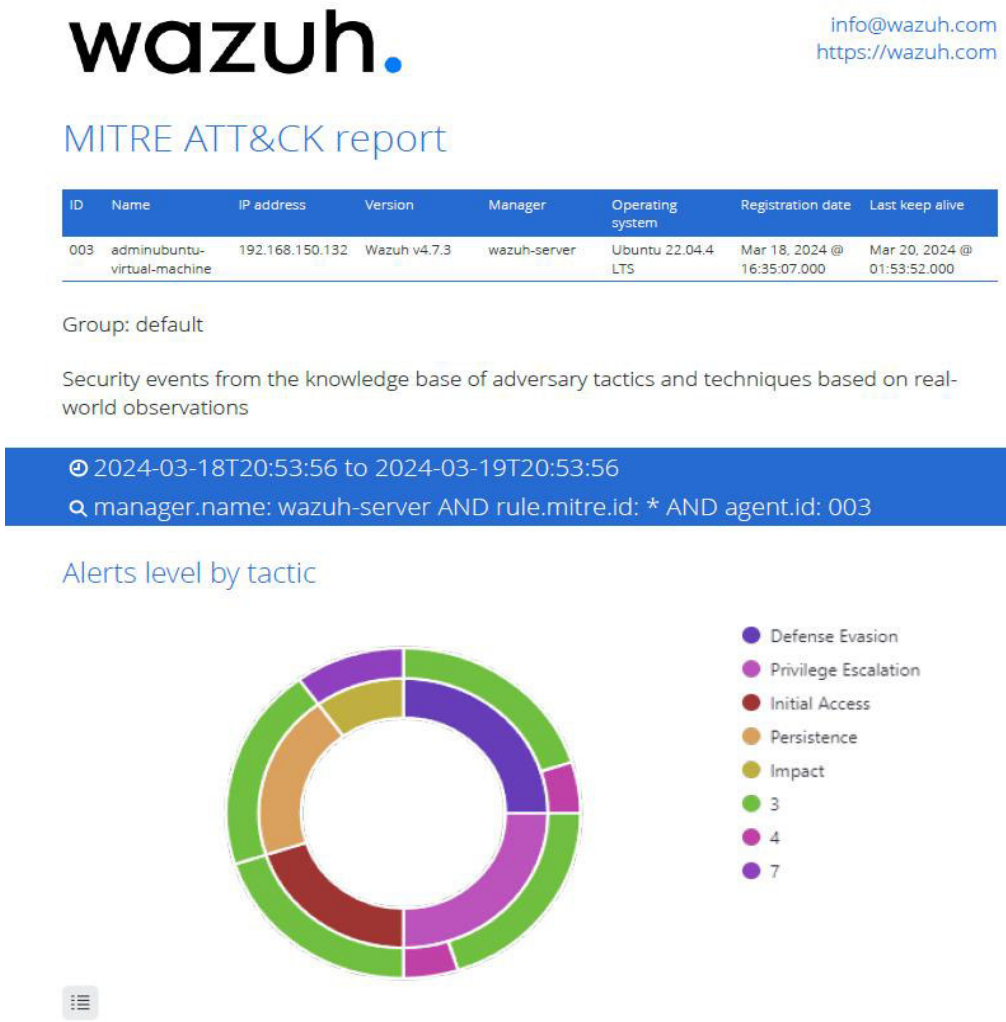
Nota: Creación propia.

3.3.5. Reporte SIEM Wazuh

El reporte generado por SIEM Wazuh contiene las tácticas, reglas con Mitre ATT&CK, evolución de alertas en tiempo real como se muestra en la figura 15.

Figura 16

Informe SIEM Wazuh



Nota: Reporte SIEM Wazuh ataques APT38

CAPITULO 4. CONCLUSIONES

El presente trabajo muestra en sus conclusiones el valor generado en la ejecución de la simulación de ataques APT38 automatizados y las alertas integradas con el SIEM Wazuh para alertar eventos de seguridad.

En virtud de lo evidenciado en las pruebas automatizadas, se ha identificado que existen plantillas a utilizar disponibilizados por MITRE ATT&CK para de una manera holística abordar las técnicas que son comúnmente aplicados por grupos APT y tomar control de los sistemas o plataformas tecnológicas objetivos.

Al ejecutar las pruebas en un entorno virtualizado y controlado, fue posible explotar vulnerabilidades en las maquinas host objetivos modificando sus configuraciones iniciales, por lo que al no tener un blindaje adecuado de seguridad tanto en el sistema operativo y software base, es posible acceder a los objetivos con facilidad.

A partir del análisis precedente se ha identificado que es posible afinar tanto las pruebas automatizadas ofensivas, así como las reglas de detección del siem Wazuh y en constante evolución evitar proactivamente intrusiones en la plataforma tecnológica.

Como consecuencia de lo expuesto, el laboratorio virtualizado es posible utilizarlo para validar controles implementados en la infraestructura, así como su entorno para evitar que usuarios maliciosos exploten vulnerabilidades y evitar que se generen accesos no autorizados o se comprometa la plataforma tecnológica.

CAPITULO 5. RECOMENDACIONES

Concluido el presente trabajo, se sugeriría tomar en cuenta alcances mayores que permitan abordar evaluaciones en plataformas cloud, que permitan validar los controles y políticas de seguridad implementados en las plataformas tecnológicas.

Generar valor en las pruebas del red team para que se realicen pruebas planificadas y en ejecución continua para evitar que usuarios maliciosos accedan a los sistemas, vulnerando principios mínimos de cumplimiento de seguridad.

Crear casos de uso y umbrales de cumplimiento de controles de seguridad, implementado blindajes de seguridad en sistemas operativos, software base como componentes web, software utilitario, librerías actualizadas, vigentes y no vulnerables o con CVE asociados.

Incluir escenarios de prueba que engloben el ciclo de evaluación continuo con la metodología Unified Kill Chain (IN, THROUGH, OUT) que es la evolución del Ciber Kill Chain.

6. REFERENCIAS BIBLIOGRÁFICAS

Singh S. Sharma P. K. Moon S. Y. Moon D. & Park J. H. (2019). A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. The University of Aberdeen Research Portal.

https://abdn.elsevierpure.com/en/publications/a-comprehensive-study-on-apt-attacks-and-countermeasures-for-futu

Felipe, C. N. A. (2017, 30 enero). Amenazas Persistentes Avanzadas (APT): modelo de funcionamiento y análisis al caso de estudio ProjectSauron.

http://repository.unipiloto.edu.co/handle/20.500.12277/2677

Besteiro-Calvo, L. (2016, 18 septiembre). Detección de APT con herramientas de seguridad de carácter libre.

https://reunir.unir.net/handle/123456789/4457

K. O. Detken T. Rix C. Kleiner B. Hellmann and L. Renners. (2015). SIEM approach for a higher level of IT security in enterprise networks. IEEE Xplore.

https://ieeexplore.ieee.org/abstract/document/7340752

Bart Lenaerts-Bergmans. (2023). What is an Advanced Persistent Threat (APT)? - CrowdStrike. crowdstrike.com.

https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/

Giura, P., & Wang, W. (2012). Using Large Scale Distributed Computing to Unveil Advanced Persistent Threats. *Science, 1, 93-105.*

M. Khosravi and B. T. Ladani. (2020). Alerts Correlation and Causal Analysis for APT Based Cyber Attack Detection. IEEE Xplore.

https://ieeexplore.ieee.org/abstract/document/9186060

Li, Y., Zhang, T., Li, X., & Li, T. (2019). A model of APT attack defense based on cyber threat detection. En *Communications in computer and information science* (pp. 122-135).

https://doi.org/10.1007/978-981-13-6621-5_10

Ramírez, V. (2018, 9 de octubre). APT38: nuevo grupo de amenazas apoyado por el régimen norcoreano. https://cybersecuritynews.es/apt38-nuevo-grupo-de-amenazas-apoyado-por-el-regimen-norcoreano/.

Mitre. (2024). GitHub - mitre/caldera: Automated Adversary Emulation Platform. GitHub. https://github.com/mitre/caldera

BBVAOPEN4U. (2024, 20 de enero). Qué es el método Kanban y por qué funciona en la programación de software. Obtenido de

https://bbvaopen4u.com/es/actualidad/que-es-el-metodo-kanban-y-por-quefunciona-en-la-programacion-de-software

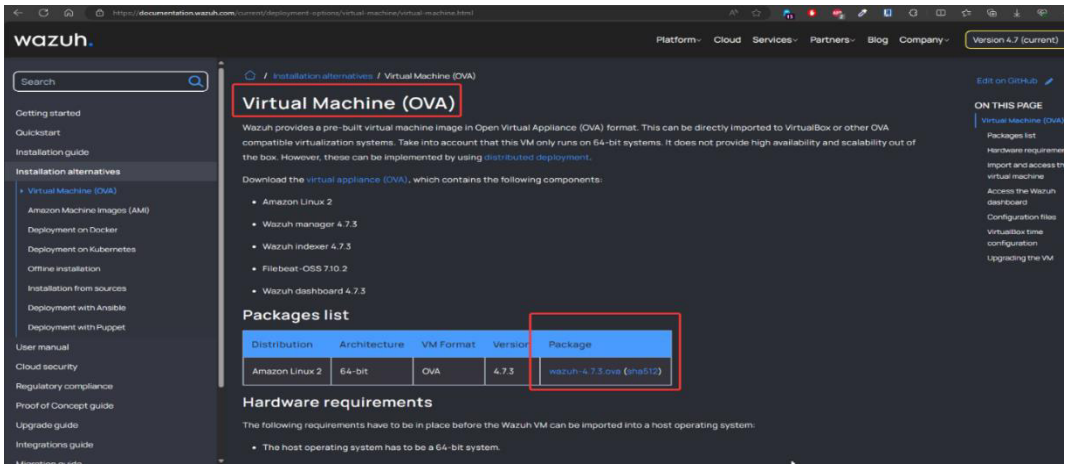
A. APÉNDICE

A.1 Instalación completa Siem Wazuh

El entorno virtualizado seguro de SIEM requiere la descarga del OVA Wazuh que se descargaría desde la página oficial de Wazuh como se muestra en la figura A1.

Figura A1

Wazuh OVA

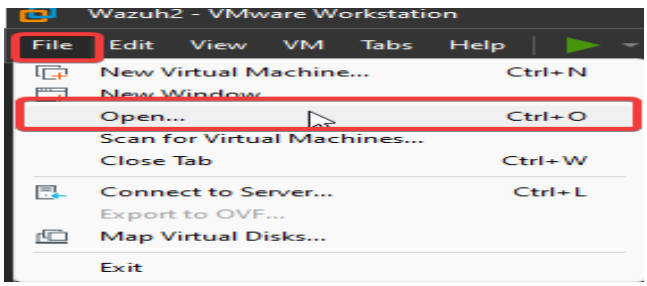


Nota: Página oficial de descarga de Wazuh

Lo siguiente es abrir la descarga del OVA Wazuh como se muestra en la figura A2.

Figura A2

Entorno virtualizado

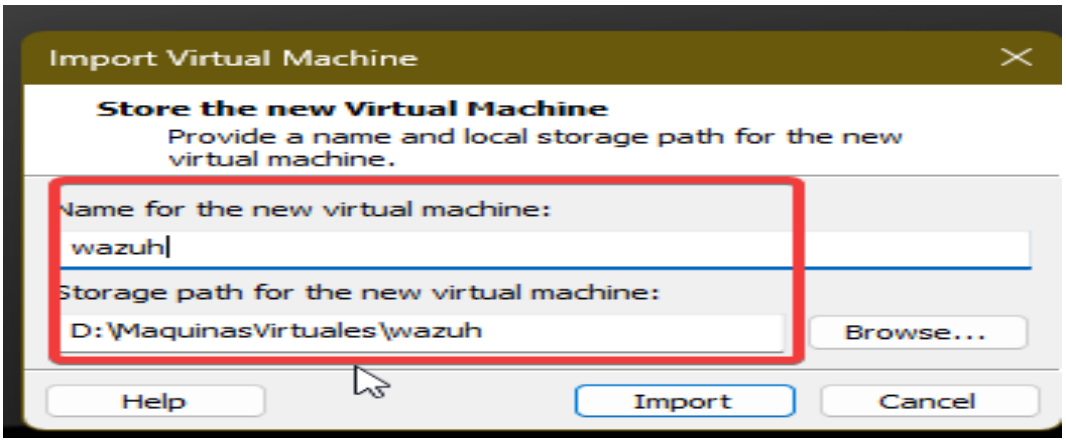


Nota: Abrir el OVA Wazuh descargado

Se importa la OVA Wazuh en la dirección local como se muestra en la figura A3.

Figura A3

Ruta de importe OVA Wazuh



Nota: Almacenamiento máquina virtual

Se inicia la máquina virtual Wazuh como se muestra en la figura A4.

Figura A4

Inicio Wazuh

Nota: Inicio de máquina virtual Wazuh

En proceso de inicio de la máquina virtual Wazuh como se muestra en la figura A5.

Figura A5

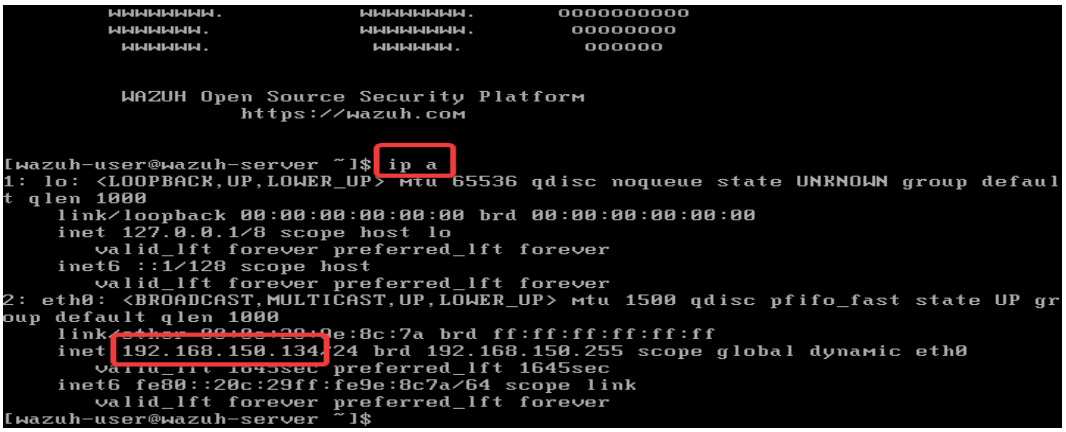
Habilitado Wazuh

Nota: Inicio de máquina virtual Wazuh

Una vez inicio a máquina virtual Wazuh como se muestra en la figura A6.

Figura A6

Inicio ip Wazuh

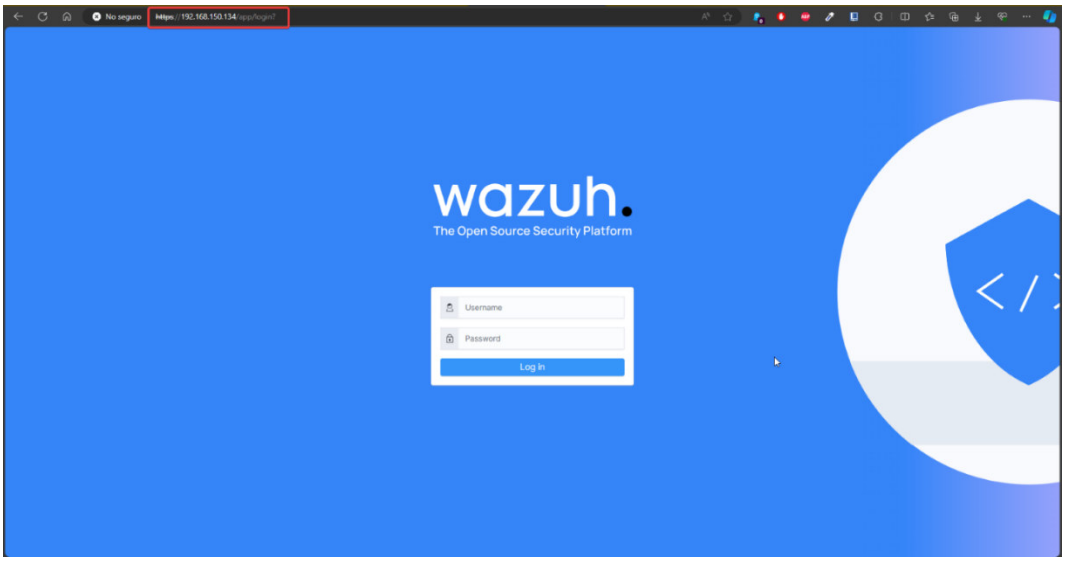


Nota: Se genera la IP

Login consola de administración Wazuh como se muestra en la figura A7.

Figura A7

Inicio consola de administración Wazuh

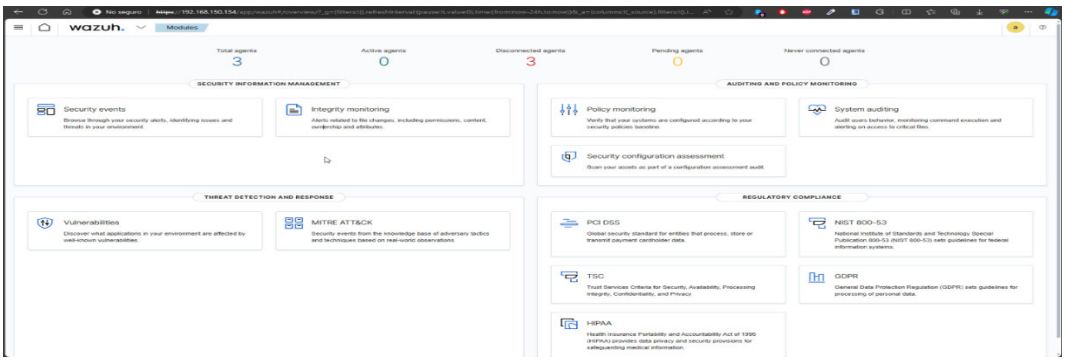


Nota: Consola administración

Se muestra el dashboard de la consola de administración Wazuh como se muestra en la figura A8.

Figura A8

Dashboard consola de administración Wazuh



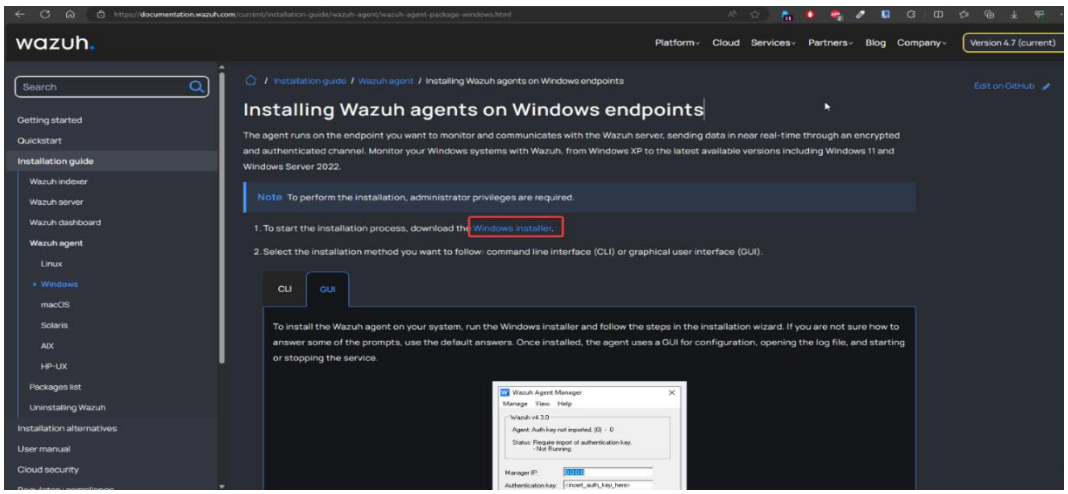
Nota: Dashboard consola administración

A.2Instalación completa agente Wazuh en endpoint Windows

Para que el SIEM Wazuh registre eventos o alertas de los endpoint debe configurarse los agentes como se muestra en la figura A9.

Figura A9

Agente Wazuh en windows

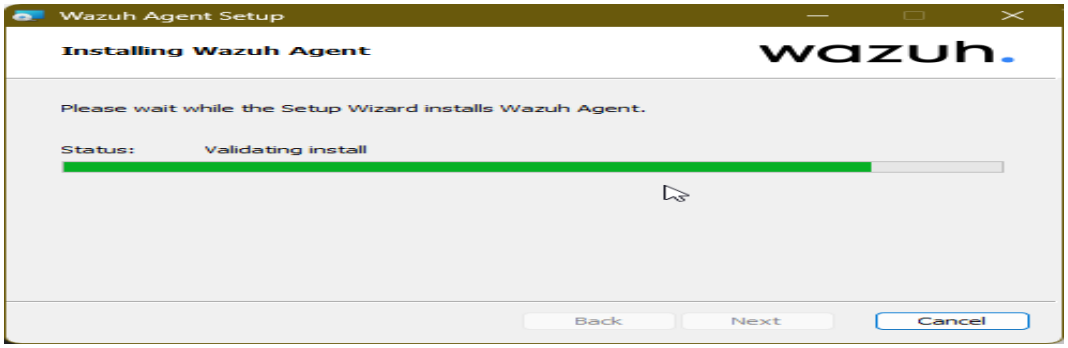


Nota: Página oficial de descarga de agente Wazuh

Instalación de agente wazuh en Windows como se muestra en la figura A10.

Figura A10

Instalación agente Wazuh en windows

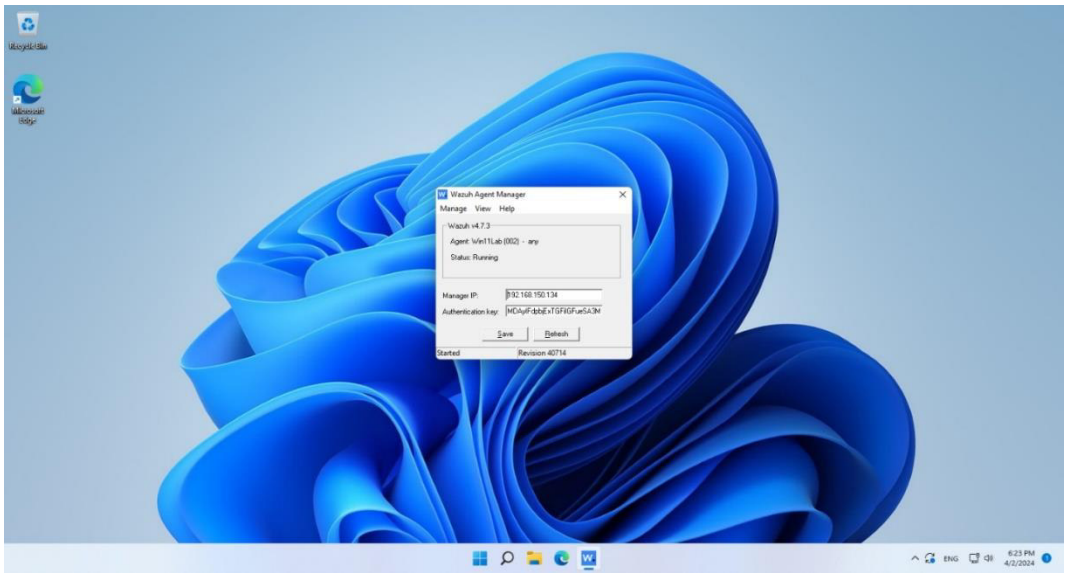


Nota: Instalación agente

Configuración agente wazuh en Windows como se muestra en la figura A11.

Figura A11

Configuración agente Wazuh en windows

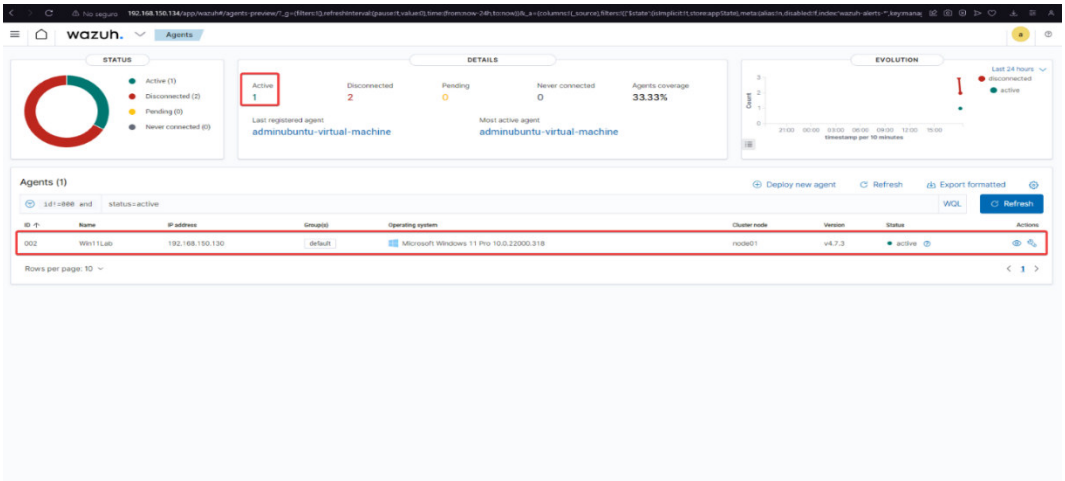


Nota: Configuración agente

Integración agente wazuh en Windows como se muestra en la figura A12.

Figura A12

Integración agente Wazuh en windows



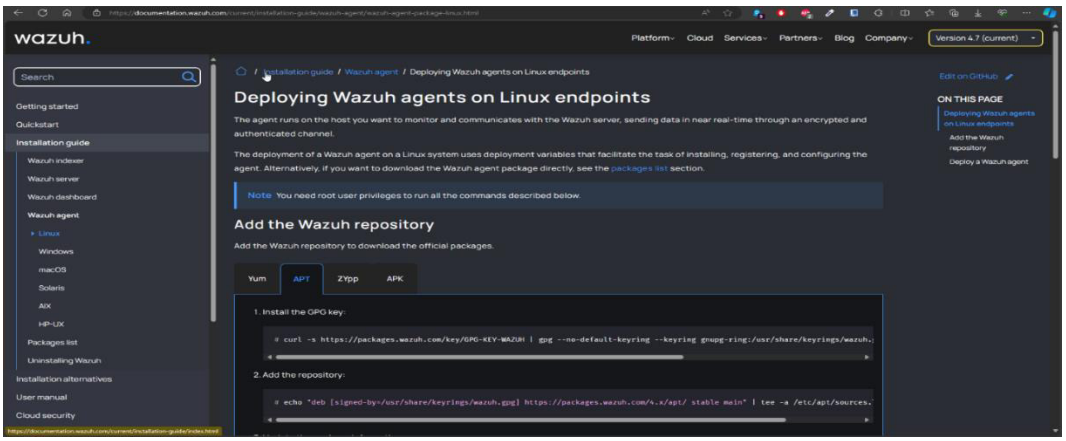
Nota: Integración agente

A.3Instalación completa agente wazuh en endpoint Ubuntu

Para que el SIEM Wazuh registre eventos o alertas de los endpoint debe configurarse los agentes como se muestra en la figura A13.

Figura A13

Agente Wazuh en ubuntu

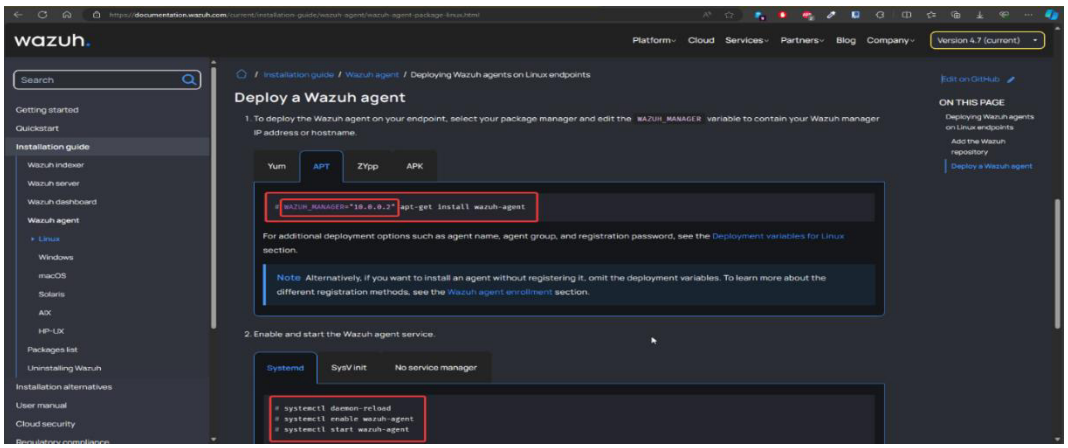


Nota: Página oficial de descarga de agente Wazuh

Instalación de agente wazuh en Ubuntu como se muestra en la figura A14.

Figura A14

Instalación agente Wazuh en ubuntu

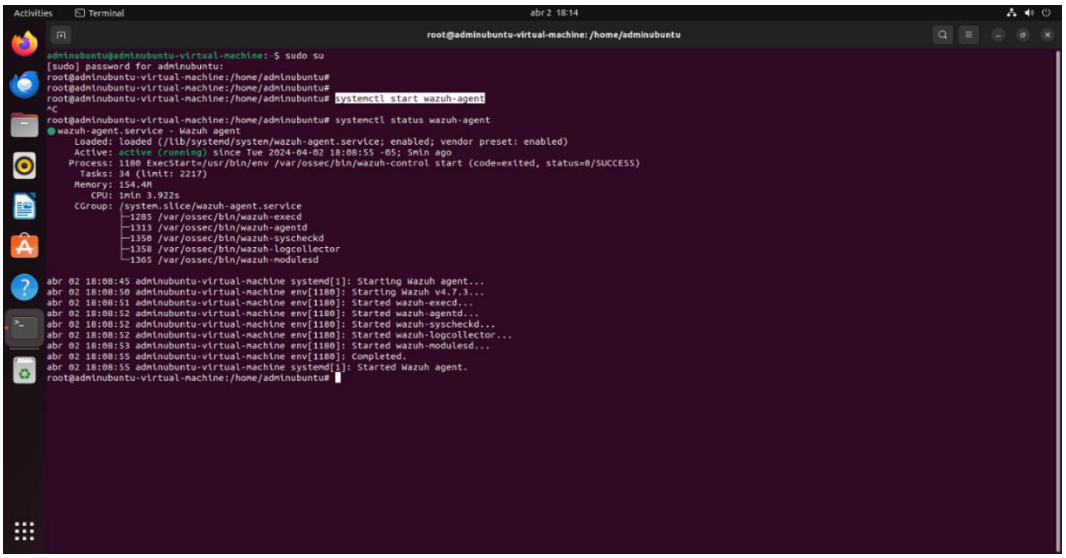


Nota: Instalación agente

Configuración agente wazuh en Ubuntu como se muestra en la figura A15.

Figura A15

Configuración agente Wazuh en Ubuntu

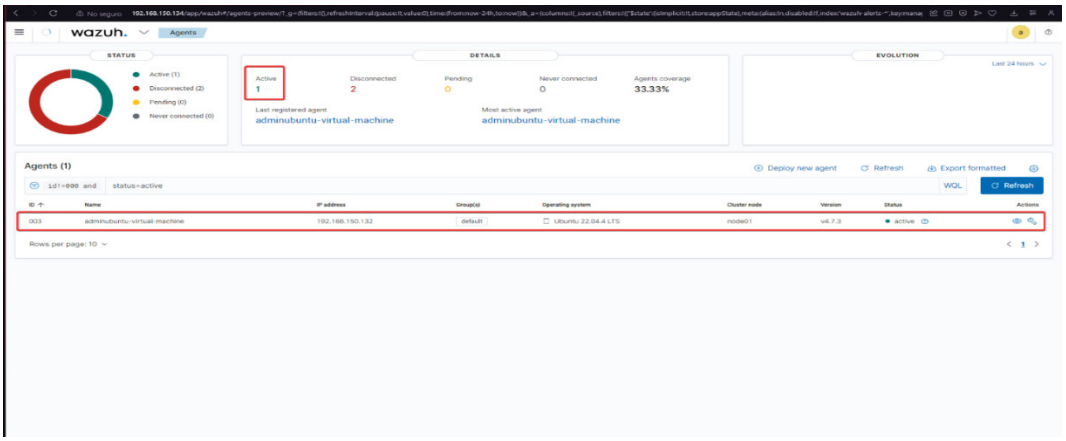


Nota: Configuración agente

Integración agente wazuh en Ubuntu como se muestra en la figura A16.

Figura A16

Integración agente Wazuh en Ubuntu



Nota: Integración agente