Despliegue y funcionamiento

de Wazuh



Alejandro Montes Delgado

IES Gonzalo Nazareno

Índice

1. Objetivos que se quieren conseguir.	3
2. Escenario necesario para la realización del proyecto.	4
3. Fundamentos teóricos y conceptos.	5
3.1. Definición y funciones.	5
3.2. Componentes.	7
3.3. Arquitectura de Wazuh.	8
4. Despliegue y configuración de Wazuh.	10
4.1. Despliegue de Wazuh con Docker.	10
4.2. Instalación agente de wazuh.	13
4.3. Configuraciones extras.	15
4.3.1. Activar detección de vulnerabilidades.	15
4.3.2. Configurar servidor SMTP.	16
4.3.3. Envío del reporte diario y alertas de riesgo por correo.	17
4.3.4. Envío de alertas mediante Slack.	18
5. Explicación y prueba de funcionamiento.	22
5.1. Explicación del funcionamiento de Wazuh.	22
5.2. Prueba de funcionamiento de las alertas en Slack.	27
5.3. Prueba de funcionamiento del reporte diario vía mail.	28
6. Conclusión.	30
7. Bibliografía.	31

1. Objetivos que se quieren conseguir.

El objetivo para la finalización de este proyecto es tener desplegada la herramienta wazuh en un contenedor Docker, con métricas recogidas de un agente wazuh para su posterior explicación del funcionamiento de dicha herramienta y análisis de las métricas recogidas.

2. Escenario necesario para la realización del proyecto.

El escenario consiste en una instancia en Proxmox o OCI (Oracle Cloud

Infraestructure) con Docker donde realizaremos el despliegue de dicha herramienta.

3. Fundamentos teóricos y conceptos.

3.1. Definición y funciones.

Wazuh es una plataforma Open-Source que unifica las capacidades de XDR (detección y respuesta extendidas) y SIEM (gestión de información y eventos de seguridad), y está integrado con Elastic Stack, utilizada para la prevención, detección y respuesta a las amenazas, es capaz de proteger cargas de trabajos en entornos locales, virtualizados, en contenedores y en la nube.

La solución Wazuh consta de agentes de seguridad desplegado en los sistemas supervisados, y un servidor que recoge y analiza los datos recopilados por los agentes.

Los servicios que brinda wazuh son los siguientes:

- <u>Análisis de seguridad</u>: Wazuh es utilizado para recolectar, agregar, indexar y analizar información de seguridad, ayudando a las organizaciones a detectar intrusos, amenazas y anomalías de comportamiento.
- <u>Detección de intrusos</u>: Los agentes de Wazuh monitorizan los sistemas buscando malware, rootkits y anomalías sospechosas. Puede detectar archivos ocultos, procesos ocultos, listener de red no registrados o inconsistencias en respuestas de llamadas al sistema. Además, el servidor usa un enfoque basado en firmas para la detección usando un motor de expresiones regulares para analizar la información de los logs recolectados.

- <u>Análisis de logs:</u> Los agentes de Wazuh leen el SO y los logs de las aplicaciones, y los envían de manera segura al administrador central para ser analizados y almacenados. Las reglas de Wazuh ayudan a mantener la consistencia frente a errores de aplicación o sistemas, malas configuraciones, intentos de actividades maliciosas, violación de políticas entre otros problemas operacionales y referidos a la seguridad.
- <u>Monitorización de la integridad de los Archivos</u>: Wazuh monitorea el sistema de archivos, identificando cambios en el contenido, permisos, propiedad, y los atributos que necesitas mantener bajo control.
- <u>Detección de vulnerabilidades</u>: Los agentes de Wazuh envían información referida al servidor, donde es correlacionada con la base de datos de actualizaciones continuas de CVE (Common Vulnerabilities and Exposure), para identificar las vulnerabilidades de software conocidas
- <u>Configuración de Evaluación</u>: Wazuh monitorea los ajustes de configuración del sistema y las aplicaciones para asegurar que se alinean con las políticas de seguridad. Los agentes actúan escaneando periódicamente para detectar aplicaciones que son conocidas como vulnerables, no parcheadas o configuradas inseguramente. Adicionalmente, la configuración puede ser personalizada, adaptándose para ser alineadas con las propiedades de tu organización. Las alertas incluyen recomendaciones para mejorar la configuración, referencias y mapeo con cumplimiento normativo.
- <u>Respuesta ante incidentes</u>: Wazuh provee respuestas activas «*out-of-the-box*» para accionar varias contramedidas para la dirección de amenazas activas, como bloquear acceso al sistema para las fuentes de amenazas cuando ciertos criterios son cumplidos. Adicionalmente, Wazuh puede ser usado para correr

comandos remotamente o solicitudes del sistema, identificando indicadores de compromisos (IOCs) y ayudando a realizar otras tareas forenses o tareas automatizadas en respuestas a incidentes.

- <u>Cumplimiento Normativo</u>: Wazuh provee algunos de los controles de seguridad necesarios para cumplir con los estándares y regulaciones de la industria. Estas características combinadas con su escalabilidad y soporte multiplataforma ayuda a las organizaciones al cumplimiento técnico de los requerimientos.
- <u>Seguridad en la nube</u>: Wazuh ayuda a monitorear infraestructuras en la nube a un nivel API, usando integración de módulos que son capaces de enviar datos de manera segura desde proveedores de servicios en la nube bien conocidos, como Amazon AWS, Azure o Google Cloud.
- <u>Seguridad en contenedores</u>: Wazuh provee seguridad en los host y contenedores Docker, monitorizando su comportamiento y detectando amenazas y anomalías. El agente Wazuh tiene integración nativa con el motor de Docker permitiendo a los usuarios monitorizar las imágenes, volúmenes,modo configuraciones de red, y contenedores corriendo.

3.2. Componentes.

Wazuh consta de los siguientes componentes:

<u>OSSEC HIDS</u>: Es un sistema de detección de intrusos(HIDS) que es usado para la detección, visibilidad y monitorización del cumplimiento de eventos de seguridad. Está basado en un agente multiplataforma que envía datos del sistema a un gestor central, donde es analizado y procesado, dando como resultado alertas de seguridad. También es un servidor centralizado de logs.

- <u>OpenSCAP</u>: Es un intérprete que se usa para chequear las configuraciones del sistema y detectar aplicaciones vulnerables. Es una herramienta diseñada para el cumplimiento de la seguridad y el bastionado de los sistemas en un entorno empresarial.
- <u>Elastic Stack</u>: Es un conjunto de software(Elasticsearch, Kibana y Filebeat) que es usado para recolectar, comparar, almacenar, indexar, buscar y mostrar datos de logs. Proporciona una interfaz web que muestra los datos a través de un dashboard(panel de control).

3.3. Arquitectura de Wazuh.

Wazuh tiene dos componentes principales que instalar: Wazuh Manager y Elastic Stack. Hay dos tipos de arquitectura para la instalación de Wazuh:

• <u>Arquitectura centralizada:</u> Wazuh y Elastic Stack se ejecutan en el mismo servidor. La siguiente imagen muestra como es este tipo de arquitectura:



 <u>Arquitectura distribuida</u>: Wazuh y Elastic Stack se ejecutan en distintos servidores y en uno o varios formando así un clúster. En la siguiente imagen se muestra su arquitectura:

Wazuh server	Elastic Stack	Monitored server
Wazuh manager	Logstash	Wazuh agent
Filebeat	Elasticsearch	
Wazuh API	Kibana	
	Wazuh App	

4. Despliegue y configuración de Wazuh.

El escenario que se ha realizado para la demostración del proyecto es el siguiente:

- Servidor Wazuh con Docker.
- Agente de wazuh Debian.

En el servidor wazuh mostraré toda la configuración realizada y en el agente de wazuh mostraré como se instala e instalaremos algún servicio para que el servidor wazuh tenga logs que recoger.

4.1. Despliegue de Wazuh con Docker.

Lo primero que instalaremos en el servidor será docker. A continuación muestro los comandos usados para la instalación de dicha herramienta.

Lo primero que haremos será actualizara nuestro sistema e instalar los siguientes paquetes:

```
$ sudo apt-get update
$ sudo apt-get install ca-certificates curl gnupg
```

Añadimos los repositorios oficiales de Docker:

```
$ sudo install -m 0755 -d /etc/apt/keyrings
$ curl -fsSL https://download.docker.com/linux/debian/gpg |
sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg
$ sudo chmod a+r /etc/apt/keyrings/docker.gpg
```

Usamos el siguiente comando para añadir el repositorio:

```
$ echo \
"deb [arch="$(dpkg --print-architecture)"
signed-by=/etc/apt/keyrings/docker.gpg]
https://download.docker.com/linux/debian \
"$(. /etc/os-release && echo "$VERSION_CODENAME")" stable" | \
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

Ahora instalamos Docker Engine, para ello actualizaremos nuevamente los

repositorios una vez hayamos añadido el de Docker:

```
$ sudo apt-get update
$ sudo apt-get install docker-ce docker-ce-cli containerd.io
docker-buildx-plugin docker-compose-plugin
```

Una vez hayamos instalado Docker, instalaremos git y clonaremos un repositorio con

el que realizaremos el despliegue de wazuh:

```
$ sudo apt install git
$ git clone https://github.com/wazuh/wazuh-docker.git -b
v4.4.1
```

Dentro del directorio clonado, tendremos los siguientes archivos:

usual togwazun.~/wazun-uockers ts -t	
total 76	
drwxr-xr-x 5 usuario usuario 4096 may 12 17:57 <mark>build-docke</mark> r-	
-rw-rr 1 usuario usuario 14554 may 12 17:57 CHANGELOG.md	
drwxr-xr-x 3 usuario usuario 4096 may 12 17:57 <mark>indexer-certs</mark>	
-rw-rr 1 usuario usuario 24736 may 12 17:57 LICENSE	
drwxr-xr-x 3 usuario usuario 4096 may 12 17:57 multi-node	
-rw-rr 1 usuario usuario 11578 may 12 17:57 README.md	
drwxr-xr-x 3 usuario usuario 4096 may 13 19:22 <mark>single-node</mark>	
-rw-rr 1 usuario usuario 46 may 12 17:57 VERSION	

Las carpetas que nos interesan son single-node o multi-node, la cual elegiremos si lo queremos instalar en un solo nodo o como un clúster. En mi caso al estar desplegándolo en una máquina en Proxmox la cual no tiene demasiada potencia, he elegido la opción de single-node. Dentro de la carpeta single-node ejecutamos lo siguiente:

\$ docker-compose -f generate-indexer-certs.yml run --rm
generator

Esto nos generará los certificados correspondiente para los contenedores. Una vez el

comando haya finalizado levantaremos el escenario con el siguiente comando:

\$ docker up -d

Esto conllevará varios minutos ya que se tienen que bajar muchas imágenes. Una vez

finalizado como podremos ver tendremos desplegado los contenedores:

usuario@wazuh:~§	6 docker psformat '{{ .ID	}}\t{{.Image}}\t{{ .Names }}'
905bdffa99fd	wazuh/wazuh-dashboard:4.4.1	single-node-wazuh.dashboard-1
95efcc35f6c0	wazuh/wazuh-manager:4.4.1	single-node-wazuh.manager-1
ea86bccffe9d	wazuh/wazuh-indexer:4.4.1	single-node-wazuh.indexer-1

Accederemos al dashboard para comprobar que se ha desplegado correctamente:



Por defecto el usuario y contraseña son: admin y SecretPassword. Muestro el

dashboard una vez iniciada la sesión:

$\leftarrow \rightarrow \mathbf{C}$ $\bigcirc \mathbf{a}$	https://172.22.9.25/app/wazuh#/overview/?_	.g=(filters:!(),refreshInterva	l:(pause:!t,value:0),time:(from	n:now- 🔄 🏠	S S 7 1 ≤
= 🗅 wazuh. 🗸	Modules				a Ø
	Total agents Active agents	Disconnected agents	Pending agents	Never connected agents	
SECURIT	TY INFORMATION MANAGEMENT		AUDITING	AND POLICY MONITORING	
Security events Browse through your secur alerts, identifying issues ar threats in your environmen	ity ity ity id id. including permissions, conte ownership and attributes.	s, ent.	Policy monitoring Verify that your systems are configured according to your security policies baseline.	System al Audit users command e on access to	uditing behavior, monitoring execution and alerting o critical files.
		Ø	Security configuration assessment Scan your assets as part of a configuration assessment audit.		
THRE	T DETECTION AND RESPONSE		REGUL		
(MITRE ATT&CK		PCI DSS	NIST 800	-53

Como podemos ver, hay un agente wazuh conectado, el cual procederemos a mostrar paso a paso como se instala a continuación.

4.2. Instalación agente de wazuh.

Para instalar una agente de wazuh, lo primero que haremos ser ir al apartado de *Agents* y seleccionar *Deploy new Agent*:

	STATUS				DETA	LS			EVOLUTION	set 24 hour
(Active (1) Disconnected (0) Pending (0) Never connected (0)	Active 1 Last registe wazuh-a	Disconnected O ered agent agent	Pending O	Never connected O Most active agent wazuh-agent	Agents coverage	0.8- 0.6- 0.4- 0.2- 0- 00:00 timestamp	0 12:00 per 10 minu	active
er or sea	irch agent							new agent	r4) Export format	් Ref
D ↑	Name	IP address	Group(s)	Operating	j system		Cluster node	Version	Status	Act
001	wazuh-agent	172.22.9.18	default	A. Debia	n GNU/Linux 1	1	node01	v4.4.1	 active 	۲

Nos aparecerá la siguiente ventana la cual tendremos que rellenar con la información

que nos pide, el sistema operativo del agente, la dirección del servidor wazuh...

\equiv \triangle wazuh. \sim	Agents						a ©
Dep	oloy a new agen	× Close					
1	Choose the operating	ng system					
	Red Hat Enterpris	CentO	S	Ubuntu	Windows	macOS	
	\sim Show less						
	AIX	Alpine	Amazon Linux	Debian	Fedora		
	HP-UX	openSUSE	Oracle Linux	Raspbian OS	Solaris		
	SUSE						
8	Choose the version Debian 7 Deb Choose the architec 1386 x86.6	ian 8 Debia	aarch64	PowerPC			
4	Wazuh server addre	ess					
	This is the address the a name (FQDN).	agent uses to cor	nmunicate with the	Wazuh server. It can	be an IP address or a t	fully qualified domain	
	172.22.9.25						
5	Assign a name and a	a group to the	agent				
	wazuh-agent						

En los dos últimos puntos nos muestra los comandos necesarios para realizar la instalación en el cliente:



Y usamos los siguientes comando para iniciar el agente:

```
      Start the agent

      systemd

      sudo systemctl daemon-reload

      sudo systemctl enable wazuh-agent

      sudo systemctl start wazuh-agent
```

To verify the connection with the Wazuh server, please follow this document.

4.3. Configuraciones extras.

4.3.1. Activar detección de vulnerabilidades.

La primera configuración que realizaremos será activar la detección de

vulnerabilidades en nuestro wazuh manager. Para ello primero tendremos que

acceder al contenedor usando el siguiente comando:

\$ docker exec -ti 95efcc35f6c0 /bin/bash

Una vez hayamos entrado en la terminal del contenedor tendremos que editar el siguiente fichero:

root@wazuh:/# nano /var/ossec/etc/ossec.conf

Si no tenemos nano instalado procederemos a instalarlo. En el fichero tendremos que editar lo siguiente:

```
<vulnerability-detector>
<enabled>yes</enabled>
<interval>5m</interval>
<min_full_scan_interval>6h</min_full_scan_interval>
<run_on_start>yes</run_on_start>
```

```
<!-- Debian OS vulnerabilities -->
<provider name="debian">
    <enabled>yes</enabled>
    <os>buster</os>
    <os>bullseye</os>
    <update_interval>1h</update_interval>
</provider>
```

En la etiqueta enabled, tenemos que cambiar de "no" a "yes". Una vez hecho esto, reiniciaremos wazuh para que se apliquen los cambios:

root@wazuh:/# service wazuh-manager restart

4.3.2. Configurar servidor SMTP.

Una vez hecho esto, procederemos a configurar el servidor SMTP para enviar el reporte diario a nuestra cuenta de correos. Lo primero que haremos será instalar los

siguientes paquetes:

root@wazuh:/# apt-get update && apt-get install postfix
mailutils libsasl2-2 ca-certificates libsasl2-modules

Si durante la instalación nos da a elegir entre cuatro opciones, elegiremos Internet

Sites. Ahora editaremos el fichero de configuración de postfix y añadiremos lo siguiente:

```
relayhost = [smtp.gmail.com]:587
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
smtp_use_tls = yes
smtpd_relay_restrictions = permit_mynetworks,
permit_sasl_authenticated, defer_unauth_destination
```

Ahora para que una cuenta de gmail envíe correos, tendremos que crear una contraseña de aplicación, en mi caso he usado gmail. Adjunto el <u>enlace</u> con los pasos

a seguir para crear la contraseña de aplicación. Una vez tengamos la contraseña de 16

caracteres, ejecutaremos los siguientes comandos:

```
echo [smtp.gmail.com]:587 usuario@gmail.com:contraseña >
/etc/postfix/sasl_passwd
postmap /etc/postfix/sasl_passwd
chmod 400 /etc/postfix/sasl_passwd
```

También securizaremos la contraseña en el archivo de base de datos generado por el

comando postmap.

chown root:root /etc/postfix/sasl_passwd
/etc/postfix/sasl_passwd.db
chmod 0600 /etc/postfix/sasl_passwd
/etc/postfix/sasl_passwd.db

Reiniciamos postfix para que se apliquen los cambios:

```
service postfix restart
```

4.3.3. Envío del reporte diario y alertas de riesgo por correo.

Ahora procederemos a configurar que envíe un reporte diario a nuestro correo y alertas de nivel 12 o mayor que son de riesgo crítico. Para ello editaremos el siguiente fichero dentro del contenedor de wazuh manager:

root@wazuh:/# nano /var/ossec/etc/ossec.conf

Buscaremos la etiqueta email_notification y la cambiaremos a "yes", indicaremos que el contenedor docker actuará como servidor SMTP ya que previamente lo hemos configurado, indicando localhost. Indicamos la cuenta de correos de la cual enviarán los mails, en mi caso he usado mi cuenta de correos personal y la cuenta de correos que recibirá los emails:

```
<global>
<jsonout_output>yes</jsonout_output>
<alerts_log>yes</alerts_log>
<logall>no</logall>
<logall_json>no</logall_json>
<email_notification>yes</email_notification>
<smtp_server>localhost</smtp_server>
<email_from>aaleemd11@gmail.com</email_from>
<email_to>amontes.alertswazuh@gmail.com</email_to>
<email_log_source>alerts.log</email_log_source>
<agents_disconnection_time>10m</agents_disconnection_alert_time>
</global>
```

Al final del archivo añadiremos lo siguiente para que envíe el correo diario de reporte:

```
<ossec_config>
<reports>
    <category>syscheck</category>
        <title>Reporte diario de Wazuh</title>
        <email_to>amontes.alertswazuh@gmail.com</email_to>
        </reports>
</ossec_config>
```

Volvemos a reiniciar el servicio para que se apliquen los cambios:

root@wazuh:/# service wazuh-manager restart

4.3.4. Envío de alertas mediante Slack.

Ahora configuraremos para que nos lleguen alertas a un canal de slack. Para ello,

hemos creado en slack un espacio de trabajo llamado *alertas-wazuh*. A partir de este <u>enlace</u>, crearemos una app:

18

$\leftrightarrow \rightarrow G$	🔿 🗛 🎫 http	s://api. slack.com /apps				¶⊒ ☆		± 🐚 ≡
‡ slack api				Search		Documentation	Tutorials	Your Apps
🕅 Start	ilearning	Your Apps						
Auth Mess Man: Over Retri Send Modd Sche Usinj	entication > aaging messages view view verving messages uing messages uing messages uing messages view view verview view view view view view view view	Use our APIs to bui an app that's just i D	Build some ild an app that make for your workspace o Directory, where anyou Crea	thing amazing. a people's working lives b r create a public Slack Ay ine on Slack can discover te an App	etter. You can create op to list in the App it.			
Com Over Form Mess Inter Block	posing messages view latting text referen iage layouts active messages < Kit Builder	Your App Config Learn about tokens Workspace alertas-wazuh	guration Tokens Access Token (2 Copy Expires in 12 ho	Refresh Token ③	Generate Token Delete			

Elegiremos un nombre y el espacio de trabajo al que nos enviaran los mensajes y

crearemos la app:

← → C ○ A == htt	s://api. slack.com /apps	4 ∂ ☆	⊠ 🖗	শ 🔊 ≡
slack api	Q Search	Documentation	Tutorials	Your Apps
 Imaging messages Overview Retrieving messages Scheduling messages Block Kit Builder 	Your A Name app & choose workspace App Name wazuh Dart vorry -you'll be able to change this later. an ap Dart vorry -you'll be able to change this later. an ap Che or korstepace to develop your app in: I che ninind that you can't change this app's workspace. Steininto a different workspace. Steininto a different workspace. Vour F Learn a Workspace Learn a Be greating a Web API Application, you agree to the Slack API Terms of Service. Cancel Create App alertas-wazuh Cancel Expires in 12 hours			

Una vez creada la app, nos dirigiremos a *Start learning* \rightarrow *Overview*.

‡ slack api			Qs	earch		Documentation	Tutorials	Your Apps
C Start le	earning v	Your Apps						
Intro tr Planni Overvi Planni Choos Comm Interac Design	or the Sinck plat fo Overview ng your app iew ng interaction ing APIs unicating ction guidelines ning a great	Use our APIs to b an app that's jus	Build someth uild an app that makes pr t for your workspace or c Directory, where anyone Create	ing amazing. cople's working lives be reate a public Slack Ap on Slack can discover i an App	tter. You can create to list in the App t.			
experi Overvi Desigr Desigr Shortc Choos Localiz	ience iew ing home tabs ing modals ut guidelines ing voice & tone ing apps rding experiences	Your App Conf Learn about token Workspace alertas-wazuh	Access Token ⑦ Copy Expires in 12 hours	Refresh Token ⑦	Generate Token Delete			

Buscamos Webhooks entrantes:

	$\leftarrow \ \ \rightarrow \ \ \mathbf{C}$	◯ 👌 🗝 https://alert	rtas-wazuhespacio. slack.com /apps 🛛 🛱 🔂 🦁	\$≓ ± \$j ≡
	‡ slack ap	op directory	Explorar Gestionar Crear apps	wazuh 🗸
Y lo añad	Mps/Aleta-wardies	Nuestra selección Destacadas Aplicaciones empresariales Trabajo remoto Herramientas diarias Aplicaciones esencialas Nuevas y diparas de atención Robots brillantes Colecciones de aplicaciones Office 365 Google Workspace Attasian Aplicaciones de colaboracia. Trabajo remoto Acreso Gimertos Pacioadade decembro JAFF710UA22	Q. incoming Send data into Stack in real-time. Send data into Stack in real-time.	
	‡ slack app	o directory	Q Buscar en el Directorio de Aplicaciones Explorar Gestionar Crear apps	ılertas-wazuh
		< Explorar aplicaciones	WebHooks entrantes	

Elegimos el canal donde nos enviaran los mensajes y pulsamos el botón para

añadirlo.

$\epsilon \rightarrow c$	🔿 👌 ≅ https://alertas	-wazuhespacio. s	l lack.com /apps/new/A0F7XDUAZ-web	phooks-entrantes	4 ☆	``````````````````````````````````````
‡ slack app a	directory	Q Buscar er	n el Directorio de Aplicaciones	Explorar	Gestionar Crear apps	👕 alertas-wa 🔻
	ciaves para desarrolla para recibas actualiza	r ia tuya. Adema ciones futuras de	s, puedes registrarte como desarrollad e nuestras API.	ior para que nos cuentes en	i que estas trabajando y	
	Publicar en el canal	al dondo				
	Empieza por elegir el canal donde publicará mensajes tu Webhook		# wazuh-alertas		~	
	entrante.				o crear un nuevo canal	
			Añadir integración con	WebHooks entrantes		
			Al crear una webhook entrante, ace Slack.	eptas las Condiciones de ser	rvicio de la API de	
						I
	UTILIZAR SLACK	SLACK 🛡	LEGAL	ENLAC	ES HABITUALES	

Al añadir la integración nos proporciona una URL webhook:

$\leftarrow \rightarrow \mathbf{C}$	🔿 👌 ≅ https://alertas-wa	zuhespacio. slack.com /services/B059ACF0FL1?added=1	8 ⊑ ☆	© \$7 ± \$1
‡ slack ap	p directory	2 Buscar en el Directorio de Aplicaciones Explore	ar Gestionar Crear apps	alertas-wa 🔻
	Te iremos indicando los pasos	necesarios para que configures un webhook entrante y empieces a enviar o	datos a Slack.	
	URL de Webhook	https://hooks.slack.com/services/T058XE11R42/8059ACF0FL1/I	TUux9ylokDc8VD12sysuV3J	
	Envío de mensajes	Tienes dos opciones para enviar datos a la URL del webhook ant • Enviar una secuencia JSON como parámetro de la carga ot solicitud POST	erior: 11 en una	
		 Enviar una secuencia JSON como cuerpo de una solicitud Pi En un mensaje sencillo, tu carga útil JSON puede contener una p de <u>texto</u> como mínimo. Este es el texto que se publicará en el c Un ejemplo sencillo: 	DST ropiedad anal.	
		<pre>payload={"text": "Esta es una línea de texto en un canal." es otra línea de texto."}</pre>	nY esta	
		Esto se mostrará en el canal como:		
		testing-bot 11:41AM This is a line of text in a channel.		

Con esta URL, editaremos el fichero de configuración que hemos editado

anteriormente y añadiremos lo siguiente:

root@wazuh:/# nano /var/ossec/etc/ossec.conf

```
<integration>
  <name>slack</name>
<hook_url>https://hooks.slack.com/services/T058XE11R42/.../P45Y0
006h08cHCg3sRhmGGYo</hook_url>
  <alert_format>json</alert_format>
  <level>3</level>
```

```
</integration>
```

Solo nos queda reiniciar el servicio para que se apliquen los cambios:

root@wazuh:/# service wazuh-manager restart

5. Explicación y prueba de funcionamiento.

5.1. Explicación del funcionamiento de Wazuh.

Lo primero que veremos será la pantalla de inicio de Wazuh.

←		C O	A https://172.	22.9.25/app/wazuh#/overview/?_g=(i			al:(pause:!t,value:0),time:(fro 90%)	ጫ ☆	⊘ 💥 ⊻	A 3	
≡	\bigcirc	wazuh. 🗸	Modules							a	٥
			Total agents	Active agents	Disconnected a	gents	Pending agents Ne	ever connected agents			
			1	1	0		0	0			
		SECI	URITY INFORMATIO	NMANAGEMENT			AUDITING AND P				
	80	Security events Browse through your security identifying issues and threats environment.	alerts, in your	Lintegrity monitoring Alerts related to file changes, including permissions, content, ownership and attributes.	3	٩	Policy monitoring Verify that your systems are configured according to your security policies baseline. Security configuration assessment Scan your assets as part of a	System Audit use commanc access to	auditing rs behavior, monitoring i execution and alerting on critical files.		
		TH Vulnerabilities Discover what applications in environment are affected by t	Your well-known	MITRE ATT&CK Security events from the knowledge by of adversary tactics and techniques	ase		Configuration assessment audit. REGULATOR PCI DSS Global security standard for entities that process, store or transmit payment	Y COMPLIANCE NIST 80 National I Technolog	0-53 nstitute of Standards and y Special Publication 800-53	8	
		vulnerabilities.		based on real-world observations			cardholder data.	(NIST 800 information	-53) sets guidelines for fede on systems.	ral	

Como podemos ver, la pantalla de inicio está dividida en 4 apartados, gestión de la información de seguridad, auditoría y control de políticas, detección de amenazas y respuesta, cumplimiento normativo y arriba de estos apartados nos indica los agentes conectados y el estado de los mismos.

En el apartado de gestión de la información de seguridad, nos encontramos 2 herramientas, eventos de seguridad que examina las alertas de seguridad, identificando los problemas y las amenazas de nuestro entorno y monitorización de integridad que nos alerta de cambios en los archivos incluidos permisos, contenido, propiedad y atributos. Si entramos en el apartado de eventos de seguridad, nos muestra mediante gráficos las alertas, el nivel de alertas y los agentes que tienen dicha alerta, como en mi caso solo he indicado un agente, solo nos aparecerá alertas de un agente.



Si scrolleamos, al final nos aparecen todas las alertas de seguridad, indicándonos la hora en que se ha producido, el nombre del agente, una descripción de la alerta y el nivel de la alerta.

Secu	ity Alerts								Ì
	Time \downarrow	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID	
>	May 27, 2023 @ 13:44:10.563	001	wazuh-agent			The CVE-2023-32681 that affected python3-requests was solved due to a package removal/update or a system upgrade	3	23502	
>	May 27, 2023 @ 13:44:10.553	001	wazuh-agent			The CVE-2023-2004 that affected libfreetype6 was solved due to a package removal/update or a system upgrade	3	23502	
>	May 27, 2023 @ 13:44:10.542	001	wazuh-agent			The CVE-2023-28322 that affected libcurl4 was solved due to a package removal/update or a system upgrade	3	23502	
>	May 27, 2023 @ 13:44:10.532	001	wazuh-agent			The CVE-2023-28322 that affected libcurt3-gnutts was solved due to a package removal/update or a system upgrade	3	23502	
>	May 27, 2023 @ 13:44:10.522	001	wazuh-agent			The CVE-2023-28322 that affected curl was solved due to a package removal/update or a system upgrade	3	23502	
>	May 27, 2023 @ 13:44:10.511	001	wazuh-agent			The CVE-2023-28321 that affected libcurl4 was solved due to a package removal/update or a system upgrade	3	23502	
>	May 27, 2023 @ 13:44:10.501	001	wazuh-agent			The CVE-2023-28321 that affected libcurl3-gnutls was solved due to a package removal/update or a system upgrade	3	23502	
>	May 27, 2023 @ 13:44:10.491	001	wazuh-agent			The CVE-2023-28321 that affected curi was solved due to a package removal/update or a system upgrade	3	23502	
>	May 27, 2023 @ 05:10:00.856	001	wazuh-agent	T1565.001	Impact	Integrity checksum changed.	7	550	
>	May 27, 2023 @ 01:37:16.482	001	wazuh-agent			The CVE-2023-28320 that affected libcurl4 was solved due to a package removal/update or a system upgrade	3	23502	
Row	s per page: 10 \smallsetminus								< <u>1</u> 2 >

IES Gonzalo Nazareno

En el apartado de monitorización de la integridad, nos muestra gráficos con alertas de modificación, borrado o añadido, los agentes que lo realizan y los usuarios.



Ahora, veremos en detalle el apartado de auditoría y políticas de monitorización. La herramienta de monitorización de politicas, verifica que nuestro sistema esté configurado acorde a las politícas de seguridad que hemos indicado.

≡ 🛆 wazuh. ∨ Modules / wazuh-agent Policy monitoring ()	
Dashboard Events	fei wazuh-agent (001) 🖡 📑 Generate report
₿ ✓ Search	DQL 🛗 🗠 Last 24 hours Show dates 🔿 Refresh
agent.id: 001 × + Add filter	
Aferts over time -	Rule distribution Image: Control of the second seco
Events per control type evolution	Lond .

críticos.

En el apartado auditoría del sistema, audita el comportamiento de los usuarios, supervisando la ejecución de comandos y alertando sobre el acceso a archivos

← → C O A https://172.22.9.25/app/wazuh#,	:/overview/?_g=(filters:!(),refreshInterval:(pause	e:!t,value:0),time:(from:now-24h,to:now))&_a=(r	columns:!(_source),filters:!(('\$state':(isImplic	it:It,s: 90% 🖣 🏠	© %7 ± № ≡
≡ 🛆 wazuh. ∨ Modules / wazuh-agent / System a	auditing ()				• •
Dashboard Events				(v) wazuh-agen	t (001) 📮 📑 Generate report
🖫 🗸 Search			DQL 📋 🗸 Last	24 hours	Show dates C Refresh
agent.id: 001 × + Add filter					
Croups	Commands dinerability-detector sase sase sobrekk.entry.mo- notherk./fie	k2: No results found	✓ Files	kîi No results found	~
Aterts over time	0109	tinestamp po 20 minutes	tuise	1500	Enlegity checkum The CVE-2023-000- The CVE-2023-000- The CVE-2023-080- The CVE-2023-083- The CVE-2023-083- The CVE-2023-083- The CVE-2023-083-

En el apartado de evaluación de la configuración de seguridad(SCA), escanea el agente como parte de una auditoría de evaluación de la configuración.

\rightarrow G	○ 🔒 https://172.22.9.25/ap	p/wazuh#/overview/?_g=(filters:!(),refreshInterval:	pause:!t,value:0),time:(from:now-24h,to:now))&_a=(column	s:!(_source),filters:!(('\$state':(isImplicit:!t	◎ 90% 🖣 🔂 🔍 🛱 💐
	wazuh. 🗸 Modules wazuh-agent	Security configuration assessment ()			a
ventory	Events				0१0 wazuh-agent (001)
< cis	Benchmark for Debian/Linux 11 0				
	Passed 55	Failed	Not applicable	score 31%	End scan May 27, 2023 @ 07:19:42.000
Checks (1	198) Rarch				් Refresh 👜 Export formatted
ID 🛧	Title		Target		Result
29500	Ensure /tmp is a separate partition.		Command: findmntkernel /tmp		• Failed V
29501	Ensure nodev option set on /tmp partition.		Command: findmntkernel /tmp		• Failed V
29502	Ensure noexec option set on /tmp partition.		Command: findmntkernel /tmp		• Failed 🗸
29503	Ensure nosuid option set on /tmp partition.		Command: findmntkernel /tmp		• Failed 🗸 🗸
29504	Ensure separate partition exists for /var.		Command: findmntkernel /var		• Falled 🗸 🗸
29505	Ensure nodev option set on /var partition.		Command: findmntkernel /var		• Failed 🗸
29506	Ensure nosuid option set on /var partition.		Command: findmntkernel /var		• Falled V
29507	Ensure separate partition exists for /var/tmp.		Command: findmntkernel /var/tmp		• Failed V
29508	Ensure noexec option set on /var/tmp partition.		Command: findmntkernel /var/tmp		• Falled V
29509	Ensure nosuid option set on /var/tmp partition.		Command: findmntkernel /var/tmp		• Failed 🗸 🗸
Rows per p	page: 10 🗸				< 1 2 3 4 5 20 >

Nos muestra los chequeo que realiza, el comando y el resultado. Arriba nos muestra las evaluaciones exitosas, las que han fallado y las que no son aplicables y nos da un porcentaje que es la puntuación, cuanto mas alto es el porcentaje, significa que más chequeos han pasado la prueba. Ahora veremos el apartado de detección y respuesta ante amenazas, la herramienta de vulnerabilidades nos muestra las aplicaciones de nuestro escenario que están afectadas por vulnerabilidades bien conocidas.

$\leftarrow \rightarrow \mathbf{C}$	O A https://172.22.9.25/app	/wazuh#/overview/?_g=(filter:	s:!(),refreshInterval:(pause:It,value:0),time:(i	from:now-24h,to:now))&tab=	=vuls&tabView=panels&a	gentId=001&_a=(column 90%	₲₷ ♥ ₺ ■
≡ 🗅 wazuh. ~	Modules wazuh-agent	Vulnerabilities ()					• 0
Inventory Events							💖 wazuh-agent (001) 🌹
	SEVERITY Critical (0) High (99) Medium (31) Low (5)		Critical High 0 99 Last full scan May 28, 2023 @ 074618.000	Medium 31 Last partial scan May 28, 2023 @ 12:48	Low 5	C	SUMMARY Vin-common (24) vim-timy (24) exercitable exercitable exercitable
Vulnerabilities (139) Filter or search							(a) Export formatted
Name 1	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time
busuber	5.1-2+0eD11U1	amd64	High	CVE-2022-3715	0	7.8	May 22, 2023 @ 19:10:51.000
busybox	1:1:30.1-0	amd84	- High	CVE-2021-42380	0.5	7.2	May 22, 2023 @ 10:10:40.000
busybox	1:1:30:1-6	amd64	High	CVE-2021-42381	6.5	7.2	May 22, 2023 @ 19-10-40.000
busybox	1:130.1-6	amd64	High	CVE-2021-42384	6.5	7.2	May 22, 2023 @ 19:10:41.000
busybox	1:1.30.1-6	amd64	High	CVE-2021-42385	6.5	7.2	May 22, 2023 @ 19:10:41.000
busybox	1:1.30.1-6	amd64	High	CVE-2021-42386	6.5	7.2	May 22, 2023 @ 19:10:41.000
busybox	1:1.30.1-6	amd64	High	CVE-2022-28391	6.8	8.8	May 22, 2023 @ 19:10:47.000
busybox	1:1.30.1-6	amd64	High	CVE-2021-42378	6.5	7.2	May 22, 2023 @ 19:10:52.000
busybox	1:1.30.1-6	amd64	High	CVE-2021-42379	6.5	7.2	May 22, 2023 @ 19:10:52.000
Rows per page: 10 $ \smallsetminus$							< <u>1</u> 2 3 4 5 14 >

Como vemos, nos muestra un gráfico con la gravedad de la vulnerabilidad, también nos detalla el numero de vulnerabilidades según su gravedad y un gráfico con las aplicaciones afectadas. En la parte de abajo, nos indica todas las vulnerabilidades con el nombre, la versión, la arquitectura de la máquina, el nivel de gravedad, el CVE-ID que es una lista donde se encuentra registradas todas las vulnerabilidades y nos muestra puntuaciones del nivel de gravedad y la fecha en la que ha sido detectada la vulnerabilidad.

Por último, veremos el apartado de MITRE ATT&CK que indica eventos de seguridad de la base de conocimientos y técnicas de los adversarios basados en observaciones del mundo real.

Despliegue y funcionamiento de Wazuh

← → C O & https://172.22.9.25/app/wazuh#/overview/?_g=(filters:!),refreshInterval:(p	pause:lt,value:0),time:(from:now-24h,to:now))&_a=(columns:l(_source),filters:l((!\$state':(isImplicit:lt,s 🛛 💁 🏠	© & ⊀ № ≡
Intelligence Framework Dashboard Events	00 wazuh	-agent (001) 📮 📄 Generate report
😰 🗸 Search	DQL 👩 🗸 Last 24 hours	Show dates C Refresh
manager.name: wazuh.manager rule.mitre.id: exists agent.id: 001 + Add filter		
Alerts evolution over time	رگ Top tactics	P
1 6.6 6.2 9 10.00 10.00 21.00 00.00 0.000 00 0.000 00 0.0000 00 0.0000 00 0.0000 00 0.0000 00 0.0000 00 0.0000 00 0.0000 00 0.0000 00 0.00000000		• Inpact
Rule level by attack 🖉 MITRE attacks by tactic	∠ [™] Rule level by tactio	2
Striet Dis Marga- 7	the Store Data Maripu-	● Inpact ● 7

5.2. Prueba de funcionamiento de las alertas en Slack.

A continuación, voy a demostrar que el servidor Wazuh envía correctamente las

alertas mediante Slack entrando en el canal de alertas-wazuh.



Como se puede apreciar en la imagen, vemos una alerta de nivel 7 y nos indica que el fichero /etc/resolv.conf ha sido modificado y que los atributos afectados son el mtime y el inodo.

IES Gonzalo Nazareno

5.3. Prueba de funcionamiento del reporte diario vía mail.

Para ello iniciaré sesión en la cuenta de gmail la cual indiqué que iba a recibir los

correc	OS.						
	$\leftarrow \ \ \rightarrow \ \ C$	0	a a https://mail.google.com/mai	//u/J?/zx=ks79ttcqbrmn9#inbox 🛛 🖗 🏠 💿	R	*	∎ ≣
	= 附 Gmail		Q Buscar correo	74 (0)	۲		A
	🖉 Redactar		□ • C i	1-7 de 7	<	>	
	Recibidos	1	Empieza a utilizar Gmail			×	
	 ☆ Destacados ③ Pospuestos ➢ Enviados 		Personaliza tu bandeja de entrada	Cambia la imagen de perfit Cambia la imagen de perfit Importa contactos ymenages Descarga Gmail ymenages			•
	 Borradores Más 		🗆 🚖 Wazuh	Reporte diario de Wazuh - Report Reporte diario de Wazuh completed		2:00	-
	Etiquetas	+	 ☆ Wazuh ☆ Wazuh 	Reporte danio de Wazuh - Report Baprice diario de Wazuh : completed		27 may 26 may	+
			🗆 🚖 root	Test Postfix - Test mail from postfix		25 may	
			🗆 🚖 Wazuh	Reporte diarlo - Report: Reporte diarlo' completed,		25 may	
			the Google Account.	Alejandro, revisa la configuración de tu cuenta de Google - Hola, Alejandro: Te damos la bienvenida a Google en tu dispositivo OnePlus 10 Pro 5G. A continuación, sigue estos dos pasos para c		25 may	
			El equipo de Cuenta.	Información sobre tu nueva cuenta de Google - Hola, Alejandro: Te damos la bienvenida a Google. Con tu nueva cuenta, puedes acceder a productos, aplicaciones y servicios de Google. C.,	-	24 may	

Como podemos ver, hay 4 correos enviados a través del nombre Wazuh con el asunto Reporte diario de Wazuh, el primer correo en el asunto indica reporte diario porque más adelante decidí cambiar el asunto para indicara el nombre de la herramienta. Ahora muestro el contenido del correo y lo explicaré brevemente.

Card of the Card o			
🗙 inglés 🔹 > español 🕶	Traducir mensaje		Desactivar para: in
Report 'Reporte diario de Wazuh' con	pleted.		
->Processed alerts: 14			
>Post-filtering alerts: 2			
>First alert: 2023 May 27 03:10:00			
>Last alert: 2023 May 27 15:10:03			
Top entries for 'Level':			
Severity 7	2		
Top entries for 'Group':			
ador II 5.1 f	12		
apa13 4 11	12 1		
hinaa 164 312 c 1	12 1		
hinaa 164 312 c 2	12 1		
nist 800 53 SL7	12 1		
DSSEC	12 1		
oci dss 11.5	12 1		
syscheck	12 1		
syscheck entry modified	12 1		
syscheck file	12 1		
ISC CC6.1	2		
sc CC6.8	12		
sc CC7.2	12		
ISC CC7.3	12 1		
sc PI1.4	12 1		
tsc_PI1.5	2		

Primero nos muestra el numero de alertas procesadas y el número de alertas post filtrado, no indica cuando fue la primera alerta del día y la última, nos indica cual fue el nivel mas alto de alerta y por cada grupo cuantas alertas hubo.

6. Conclusiones.

Este proyecto a nivel me personal me ha resultado muy positivo ya que he aprendido mucho sobre una herramienta la cual desconocía, en cuanto al despliegue he tenido algunos problemas ya que en primera instancia mi idea era usar OpenStack y Kubernetes pero no ha sido posible debido a que en la red del instituto el puerto 80 está capado por Andared y he tenido muchos problemas para el despliegue así que decidí usar una instancia en OpenStack y Docker para el despliegue del contenedor. Claramente para un entorno de pruebas y un escenario pequeño sí es viable desplegar un contenedor para ver el funcionamiento de dicha herramienta pero en un escenario real es necesario el despliegue de un clúster.

La mayor ventaja de Wazuh es que es una herramienta muy completa que ofrece muchas funcionalidades y es modular, es decir, se pueden añadir módulos externos para complementar dicha herramienta.

Una de las principales desventajas que veo en esta herramienta es que sólo soporta sistemas operativos conocidos y no se puede instalar en un router o en un switch o un firewall etc.

Para seguir profundizando creo que sería interesante añadir otros módulos, ver como se instala y su funcionamiento, por otro lado también sería interesante indagar en el apartado de *Regulatory Compliance* aunque yo he decidido no verlo en este proyecto ya que no lo veo tan interesante, está mas enfocado al cumplimiento normativo de una empresa y haría demasiado largo el proyecto.

7. Bibliografía.

- Instalación de Docker: https://docs.docker.com/engine/install/debian/

- Despliegue de wazuh: <u>https://documentation.wazuh.com/current/deployment-options/docker/wazuh-</u> <u>container.html</u>

- Instalación de wazuh agent: https://documentation.wazuh.com/4.4/installation-guide/wazuh-agent/wazuhagent-package-linux.html

- Activar detección de vulnerabilidades:<u>https://tutorialesit.com/habilitar-la-deteccion-de-vulnerabilidades-en-</u>wazuh/

- Configurar SMTP: <u>https://documentation.wazuh.com/current/user-manual/manager/manual-email-report/smtp-authentication.html</u>

- Configurar alertas por e-mail: <u>https://documentation.wazuh.com/current/user-manual/manager/manual-email-</u> report/index.html

- Configurar reporte diario e-mail: <u>https://documentation.wazuh.com/current/user-manual/manager/automatic-</u> reports.html

- Integrar wazuh con API: <u>https://documentation.wazuh.com/current/user-manual/manager/manual-</u> integration.html

- Envío de alertas por Slack: <u>https://www.youtube.com/watch?v=9SaPUxSxTy0</u>