

# Auditoria de Seguridad en imagen DOCKER

PARTE III FINAL

**HERRAMIENTA GRATUITA**



X



HENRIQUE ALVES

## TABLA DE CONTENIDO

Introducción .....	3
Parte 3: Auditoría de Seguridad en Imágenes Docker con MySQL .....	3
Enfoque en la Seguridad de Contenedores Docker con MySQL.....	4
Resumen de lo obtenido en el informe al ejecutar Gype en la imagen anteriormente nombrada.....	9
CONCLUSIÓN .....	11

# INTRODUCCIÓN

## PARTE 3: AUDITORÍA DE SEGURIDAD EN IMÁGENES DOCKER CON MYSQL

La auditoría de seguridad es un proceso fundamental para garantizar la protección de los sistemas dentro de una infraestructura tecnológica. Este informe abordó auditorías en entornos **Windows y Linux**, aplicando herramientas especializadas para identificar y mitigar vulnerabilidades.

- **Parte 1:** Se realizó una auditoría en **Active Directory (AD)** utilizando **Nessus**, una herramienta potente para el escaneo de vulnerabilidades. Se identificaron fallos de configuración, accesos indebidos y riesgos críticos en Windows, destacando la importancia de implementar medidas de mitigación para fortalecer la administración de identidades y accesos en redes corporativas.
- **Parte 2:** Se extendió el análisis a servidores **Linux** con **Lynis**, una herramienta ampliamente utilizada para auditar configuraciones y detectar fallos de seguridad. Se revisaron permisos, autenticación y configuraciones de servicios, proporcionando recomendaciones clave para mejorar la seguridad del sistema.

Este proceso resalta la necesidad de una auditoría continua y la aplicación de buenas prácticas para proteger los entornos tecnológicos frente a amenazas potenciales.

Aunque estas auditorías estuvieron orientadas a la **detección de vulnerabilidades**, cabe destacar que, como resultado de estos análisis, se han aplicado **medidas de seguridad** para reducir los riesgos detectados y mejorar la protección de los sistemas. Entre las acciones implementadas se incluyen:

### En Active Directory (AD)

- Fortalecimiento de políticas de contraseñas y autenticación multifactor (MFA).
- Restricción de accesos privilegiados y revisión de cuentas con permisos elevados.
- Aplicación de parches de seguridad para vulnerabilidades críticas, como **ZeroLogon (CVE-2020-1472)**.
- Segmentación y endurecimiento de políticas de acceso en la red.

### En Servidores Linux

- Configuración de reglas de firewall (UFW o iptables) para restringir accesos no autorizados.
- Deshabilitación del acceso SSH para el usuario root y configuración de autenticación basada en claves.
- Aplicación de actualizaciones de software y paquetes de seguridad en el sistema.
- Monitoreo activo de logs y auditoría de eventos críticos.

En esta **Parte 3** de la auditoría, se analizará la **seguridad en contenedores Docker**, centrándose en la imagen de **MySQL**. Con la creciente adopción de contenedores en entornos de desarrollo y producción, es crucial identificar y mitigar vulnerabilidades que puedan comprometer la integridad de los datos y la estabilidad de las aplicaciones.

El informe abordará:

- **Evaluación de vulnerabilidades** en la imagen de MySQL.
- **Revisión de configuraciones inseguras** dentro del contenedor.
- **Estrategias de mitigación** para reforzar la seguridad en bases de datos contenedorizadas.

Además, se implementarán medidas correctivas como el uso de imágenes oficiales, ejecución con usuarios no privilegiados, configuración segura de volúmenes y redes, habilitación de cifrado TLS/SSL, restricción de variables sensibles y monitoreo de actividad sospechosa.

Es importante mencionar que, aunque MySQL puede ejecutarse en contenedores, en **entornos reales** hay medidas de seguridad adicionales a considerar. En producción, el uso de bases de datos en Docker puede no ser la mejor opción en ciertos casos, especialmente cuando se requiere:

- **Persistencia y alta disponibilidad:** Los contenedores son efímeros, por lo que es necesario configurar volúmenes persistentes y estrategias de respaldo.
- **Rendimiento óptimo:** Bases de datos grandes pueden verse afectadas por la capa de abstracción de Docker.
- **Seguridad avanzada:** Exponer MySQL sin restricciones de red o configuraciones adecuadas puede representar un riesgo.

## IMPORTANTE

En escenarios empresariales, se suelen utilizar soluciones administradas como **Amazon RDS**, **Google Cloud SQL** o **servidores dedicados** para bases de datos en lugar de contenedores, garantizando mayor estabilidad, seguridad y escalabilidad.

Esta práctica me permite comprender cómo analizar y mejorar la seguridad en entornos con Docker, pero en producción se deben evaluar cuidadosamente los riesgos antes de usar bases de datos en contenedores.

## EJECUCIÓN DE GYPE EN IMAGEN MYSQL-SERVER EN UBUNTU

Para más información sobre Gype y su instalación: <https://github.com/anchore/gype>

Resultado demostrado con capturas de pantalla de los reportes que nos entrega Gype:

El archivo analizado corresponde al escaneo de vulnerabilidades generado por Gype en una imagen **mysql-server** sobre el servidor Ubuntu. Contiene información de los paquetes instalados, vulnerabilidades asociadas (CVE), versiones corregidas y su severidad.

En los reportes de **Gype**, la columna **"FIXED-IN"** indica si una vulnerabilidad tiene una versión del paquete en la que ha sido corregida. Cuando aparece el valor **"(won't fix)"**, significa que:

1. **No habrá una solución oficial:** El mantenedor del paquete o software no planea lanzar un parche para esta vulnerabilidad específica.
2. **Razones comunes para "(won't fix)":**
  - El software está en su fin de vida útil y no recibe más soporte.
  - La vulnerabilidad no se considera lo suficientemente crítica para justificar una solución.
  - Es un comportamiento esperado o inherente al diseño del sistema y no será modificado.

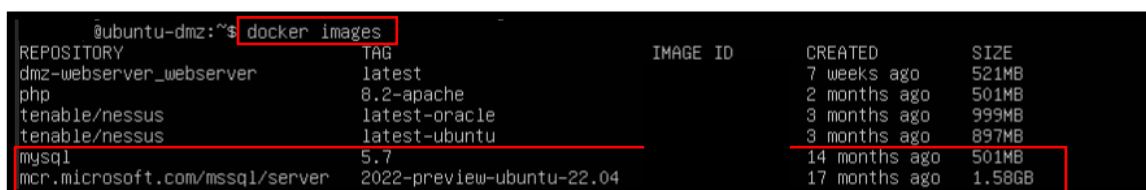
En el fichero obtenido al ejecutar Gype no hay filas en la columna **FIXED-IN** que tengan el valor **"(won't fix)"**. Todas las vulnerabilidades tienen un campo vacío o una versión específica en la columna **FIXED-IN**, indicando que existe o existirá una solución para esas vulnerabilidades.

Voy a realizar un escaneo de vulnerabilidades en **MySQL 5.7** utilizando **Gype** para identificar posibles riesgos de seguridad en la imagen del contenedor.

Comando para la instalación:

sudo snap install gype --classic o <https://github.com/anchore/gype>

Comando para ejecutarlo: gype mysql:5.7



REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
dmz-webserver_webserver	latest		7 weeks ago	521MB
php	8.2-apache		2 months ago	501MB
tenable/nessus	latest-oracle		3 months ago	999MB
tenable/nessus	latest-ubuntu		3 months ago	897MB
mysql	5.7		14 months ago	501MB
mcr.microsoft.com/mssql/server	2022-preview-ubuntu-22.04		17 months ago	1.58GB

GNU nano 4.8		dockeriescaneo.txt			
NAME	INSTALLED	FIXED-IN	TYPE	VULNERABILITY	SEVERITY
bash	5.1-6ubuntu1	5.1-6ubuntu1.1	deb	CVE-2022-3715	Medium
bsdutils	1:2.37.2-4ubuntu3	2.37.2-4ubuntu3.3	deb	CVE-2024-28085	Medium
coreutils	8.32-4.1ubuntu1		deb	CVE-2016-2781	Low
gcc-12-base	12.3.0-1ubuntu1~22.04		deb	CVE-2023-4039	Medium
gcc-12-base	12.3.0-1ubuntu1~22.04		deb	CVE-2022-27943	Low
gdb	12.1-0ubuntu1~22.04		deb	CVE-2024-36699	Medium
gdb	12.1-0ubuntu1~22.04	12.1-0ubuntu1~22.04.2	deb	CVE-2023-39130	Low
gdb	12.1-0ubuntu1~22.04	12.1-0ubuntu1~22.04.2	deb	CVE-2023-39129	Low
gdb	12.1-0ubuntu1~22.04	12.1-0ubuntu1~22.04.2	deb	CVE-2023-39128	Low
gdb	12.1-0ubuntu1~22.04	12.1-0ubuntu1~22.04.2	deb	CVE-2023-1972	Low
gdb	12.1-0ubuntu1~22.04	12.1-0ubuntu1~22.04.2	deb	CVE-2022-4285	Low
gdb	12.1-0ubuntu1~22.04	12.1-0ubuntu1~22.04.2	deb	CVE-2022-27943	Low
gpgv	2.2.27-3ubuntu2.1		deb	CVE-2022-3219	Low
libarchive13	3.6.0-1ubuntu1	3.6.0-1ubuntu1.2	deb	CVE-2024-48958	Medium
libarchive13	3.6.0-1ubuntu1	3.6.0-1ubuntu1.2	deb	CVE-2024-48957	Medium
libarchive13	3.6.0-1ubuntu1	3.6.0-1ubuntu1.1	deb	CVE-2024-26256	Medium
libarchive13	3.6.0-1ubuntu1	3.6.0-1ubuntu1.3	deb	CVE-2024-20636	Medium
libarchive13	3.6.0-1ubuntu1	3.6.0-1ubuntu1.2	deb	CVE-2022-36227	Low
libatomic1	12.3.0-1ubuntu1~22.04		deb	CVE-2023-4039	Medium
libatomic1	12.3.0-1ubuntu1~22.04		deb	CVE-2022-27943	Low
libblkid1	2.37.2-4ubuntu3	2.37.2-4ubuntu3.3	deb	CVE-2024-28085	Medium
libc++1-14	1:14.0.0-1ubuntu1.1		deb	CVE-2023-29942	Low
libc++1-14	1:14.0.0-1ubuntu1.1		deb	CVE-2023-29935	Low
libc++abi1-14	1:14.0.0-1ubuntu1.1		deb	CVE-2023-29942	Low
libc++abi1-14	1:14.0.0-1ubuntu1.1		deb	CVE-2023-29935	Low
libc-bin	2.35-0ubuntu3.3	2.35-0ubuntu3.4	deb	CVE-2023-4911	High
libc-bin	2.35-0ubuntu3.3	2.35-0ubuntu3.8	deb	CVE-2024-33602	Medium
libc-bin	2.35-0ubuntu3.3	2.35-0ubuntu3.8	deb	CVE-2024-33601	Medium
libc-bin	2.35-0ubuntu3.3	2.35-0ubuntu3.8	deb	CVE-2024-33600	Medium
libc-bin	2.35-0ubuntu3.3	2.35-0ubuntu3.8	deb	CVE-2024-33599	Medium
libc-bin	2.35-0ubuntu3.3	2.35-0ubuntu3.7	deb	CVE-2024-2961	Medium
libc-bin	2.35-0ubuntu3.3	2.35-0ubuntu3.5	deb	CVE-2024-2961	Medium
libc-bin	2.35-0ubuntu3.3	2.35-0ubuntu3.5	deb	CVE-2023-5156	Medium
libc-bin	2.35-0ubuntu3.3	2.35-0ubuntu3.5	deb	CVE-2023-4813	Low
libc-bin	2.35-0ubuntu3.3	2.35-0ubuntu3.5	deb	CVE-2023-4806	Low
libc-bin	2.35-0ubuntu3.3		deb	CVE-2016-20013	Negligible
libc6	2.35-0ubuntu3.3	2.35-0ubuntu3.4	deb	CVE-2023-4911	High
libc6	2.35-0ubuntu3.3	2.35-0ubuntu3.8	deb	CVE-2024-33602	Medium
libc6	2.35-0ubuntu3.3	2.35-0ubuntu3.8	deb	CVE-2024-33601	Medium
libc6	2.35-0ubuntu3.3	2.35-0ubuntu3.8	deb	CVE-2024-33600	Medium
libc6	2.35-0ubuntu3.3	2.35-0ubuntu3.8	deb	CVE-2024-33599	Medium
libc6	2.35-0ubuntu3.3	2.35-0ubuntu3.7	deb	CVE-2024-2961	Medium
libc6	2.35-0ubuntu3.3	2.35-0ubuntu3.5	deb	CVE-2023-5156	Medium
libc6	2.35-0ubuntu3.3	2.35-0ubuntu3.5	deb	CVE-2023-4813	Low
libc6	2.35-0ubuntu3.3	2.35-0ubuntu3.5	deb	CVE-2023-4806	Low
libc6	2.35-0ubuntu3.3		deb	CVE-2016-20013	Negligible

GNU nano 4.8		dockeriescaneo.txt			
libc6-dbg	2.35-0ubuntu3.3	2.35-0ubuntu3.4	deb	CVE-2023-4911	High
libc6-dbg	2.35-0ubuntu3.3	2.35-0ubuntu3.8	deb	CVE-2024-33602	Medium
libc6-dbg	2.35-0ubuntu3.3	2.35-0ubuntu3.8	deb	CVE-2024-33601	Medium
libc6-dbg	2.35-0ubuntu3.3	2.35-0ubuntu3.8	deb	CVE-2024-33600	Medium
libc6-dbg	2.35-0ubuntu3.3	2.35-0ubuntu3.8	deb	CVE-2024-33599	Medium
libc6-dbg	2.35-0ubuntu3.3	2.35-0ubuntu3.7	deb	CVE-2024-2961	Medium
libc6-dbg	2.35-0ubuntu3.3	2.35-0ubuntu3.5	deb	CVE-2023-5156	Medium
libc6-dbg	2.35-0ubuntu3.3	2.35-0ubuntu3.5	deb	CVE-2023-4813	Low
libc6-dbg	2.35-0ubuntu3.3	2.35-0ubuntu3.5	deb	CVE-2023-4806	Low
libc6-dbg	2.35-0ubuntu3.3		deb	CVE-2016-20013	Negligible
libc6-dbg	2.35-0ubuntu3.3		deb	CVE-2023-38545	High
libc6-dbg	2.35-0ubuntu3.3		deb	CVE-2024-8096	Medium
libc6-dbg	2.35-0ubuntu3.3		deb	CVE-2024-7964	Medium

GNU nano 4.8		dockeriescaneo.txt			
libk5crypto3	1.19.2-2ubuntu0.2	1.19.2-2ubuntu0.4	deb	CVE-2024-37371	Medium
libk5crypto3	1.19.2-2ubuntu0.2	1.19.2-2ubuntu0.4	deb	CVE-2024-37370	Medium
libk5crypto3	1.19.2-2ubuntu0.2		deb	CVE-2024-3596	Medium
libk5crypto3	1.19.2-2ubuntu0.2		deb	CVE-2024-26462	Medium
libk5crypto3	1.19.2-2ubuntu0.2	1.19.2-2ubuntu0.3	deb	CVE-2023-36054	Medium
libk5crypto3	1.19.2-2ubuntu0.2		deb	CVE-2024-26461	Low
libk5crypto3	1.19.2-2ubuntu0.2		deb	CVE-2024-26458	Negligible
libkrb5-3	1.19.2-2ubuntu0.2	1.19.2-2ubuntu0.4	deb	CVE-2024-37371	Medium
libkrb5-3	1.19.2-2ubuntu0.2	1.19.2-2ubuntu0.4	deb	CVE-2024-37370	Medium
libkrb5-3	1.19.2-2ubuntu0.2		deb	CVE-2024-3596	Medium
libkrb5-3	1.19.2-2ubuntu0.2		deb	CVE-2024-26462	Medium
libkrb5-3	1.19.2-2ubuntu0.2	1.19.2-2ubuntu0.3	deb	CVE-2023-36054	Medium
libkrb5-3	1.19.2-2ubuntu0.2		deb	CVE-2024-26461	Low
libkrb5-3	1.19.2-2ubuntu0.2		deb	CVE-2024-26458	Negligible
libkrb5support0	1.19.2-2ubuntu0.2	1.19.2-2ubuntu0.4	deb	CVE-2024-37371	Medium
libkrb5support0	1.19.2-2ubuntu0.2	1.19.2-2ubuntu0.4	deb	CVE-2024-37370	Medium
libkrb5support0	1.19.2-2ubuntu0.2		deb	CVE-2024-3596	Medium
libkrb5support0	1.19.2-2ubuntu0.2		deb	CVE-2024-26462	Medium
libkrb5support0	1.19.2-2ubuntu0.2	1.19.2-2ubuntu0.3	deb	CVE-2023-36054	Medium
libkrb5support0	1.19.2-2ubuntu0.2		deb	CVE-2024-26461	Low
libkrb5support0	1.19.2-2ubuntu0.2		deb	CVE-2024-26458	Negligible
libldap-2.5-0	2.5.16+dfsg-0ubuntu0.22.04.1	2.5.16+dfsg-0ubuntu0.22.04.2	deb	CVE-2023-2953	Low
libldap-common	2.5.16+dfsg-0ubuntu0.22.04.1	2.5.16+dfsg-0ubuntu0.22.04.2	deb	CVE-2023-2953	Low
libmount1	2.37.2-4ubuntu3	2.37.2-4ubuntu3.3	deb	CVE-2024-28085	Medium
libncurses5	6.3-2ubuntu0.1		deb	CVE-2023-50495	Low
libncurses5	6.3-2ubuntu0.1		deb	CVE-2023-45918	Low
libncurses6	6.3-2ubuntu0.1		deb	CVE-2023-50495	Low
libncurses6	6.3-2ubuntu0.1		deb	CVE-2023-45918	Low
libncursesw6	6.3-2ubuntu0.1		deb	CVE-2023-50495	Low
libncursesw6	6.3-2ubuntu0.1		deb	CVE-2023-45918	Low
libnghttp2-14	1.43.0-1build3	1.43.0-1ubuntu0.1	deb	CVE-2023-44487	High
libnghttp2-14	1.43.0-1build3	1.43.0-1ubuntu0.2	deb	CVE-2024-28182	Medium
libodbc2	2.3.9-5	2.3.9-5ubuntu0.1	deb	CVE-2024-1013	Medium
libodbcinst2	2.3.9-5	2.3.9-5ubuntu0.1	deb	CVE-2024-1013	Medium
libpam-modules	1.4.0-11ubuntu2.3	1.4.0-11ubuntu2.4	deb	CVE-2024-22365	Medium
libpam-modules	1.4.0-11ubuntu2.3		deb	CVE-2024-10963	Medium
libpam-modules	1.4.0-11ubuntu2.3		deb	CVE-2024-10041	Medium
libpam-modules-bin	1.4.0-11ubuntu2.3	1.4.0-11ubuntu2.4	deb	CVE-2024-22365	Medium
libpam-modules-bin	1.4.0-11ubuntu2.3		deb	CVE-2024-10963	Medium
libpam-modules-bin	1.4.0-11ubuntu2.3		deb	CVE-2024-10041	Medium
libpam-runtime	1.4.0-11ubuntu2.3	1.4.0-11ubuntu2.4	deb	CVE-2024-22365	Medium
libpam-runtime	1.4.0-11ubuntu2.3		deb	CVE-2024-10963	Medium
libpam-runtime	1.4.0-11ubuntu2.3		deb	CVE-2024-10041	Medium
libpam0g	1.4.0-11ubuntu2.3	1.4.0-11ubuntu2.4	deb	CVE-2024-22365	Medium
libpam0g	1.4.0-11ubuntu2.3		deb	CVE-2024-10963	Medium
libpam0g	1.4.0-11ubuntu2.3		deb	CVE-2024-10041	Medium

GNU nano 4.8		dockeriescaneo.txt			
libpam-runtime	1.4.0-11ubuntu2.3		deb	CVE-2024-10041	Medium
libpam0g	1.4.0-11ubuntu2.3	1.4.0-11ubuntu2.4	deb	CVE-2024-22365	Medium
libpam0g	1.4.0-11ubuntu2.3		deb	CVE-2024-10963	Medium
libpam0g	1.4.0-11ubuntu2.3		deb	CVE-2024-10041	Medium
libpcre2-8-0	10.39-3ubuntu0.1		deb	CVE-2022-41409	Low
libpcre3	2:8.39-13ubuntu0.22.04.1		deb	CVE-2017-11164	Negligible
libprocps8	2:3.3.17-6ubuntu2	2:3.3.17-6ubuntu2.1	deb	CVE-2023-4016	Low
libpython3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.7	deb	CVE-2024-9287	Medium
libpython3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-8088	Medium
libpython3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-6923	Medium
libpython3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-6232	Medium
libpython3.10	3.10.12-1~22.04.2		deb	CVE-2024-11168	Medium
libpython3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.4	deb	CVE-2024-0450	Medium
libpython3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.5	deb	CVE-2024-0397	Medium
libpython3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.4	deb	CVE-2023-6597	Medium
libpython3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.3	deb	CVE-2023-40217	Medium
libpython3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2023-27043	Medium
libpython3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-7592	Low
libpython3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.5	deb	CVE-2024-4032	Low
libpython3.10-minimal	3.10.12-1~22.04.2	3.10.12-1~22.04.7	deb	CVE-2024-9287	Medium
libpython3.10-minimal	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-8088	Medium
libpython3.10-minimal	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-6923	Medium
libpython3.10-minimal	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-6232	Medium
libpython3.10-minimal	3.10.12-1~22.04.2		deb	CVE-2024-11168	Medium
libpython3.10-minimal	3.10.12-1~22.04.2	3.10.12-1~22.04.4	deb	CVE-2024-0450	Medium
libpython3.10-minimal	3.10.12-1~22.04.2	3.10.12-1~22.04.5	deb	CVE-2024-0397	Medium
libpython3.10-minimal	3.10.12-1~22.04.2	3.10.12-1~22.04.4	deb	CVE-2023-6597	Medium
libpython3.10-minimal	3.10.12-1~22.04.2	3.10.12-1~22.04.3	deb	CVE-2023-40217	Medium
libpython3.10-minimal	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2023-27043	Medium
libpython3.10-minimal	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-7592	Low
libpython3.10-minimal	3.10.12-1~22.04.2	3.10.12-1~22.04.5	deb	CVE-2024-4032	Low
libpython3.10-stdlib	3.10.12-1~22.04.2	3.10.12-1~22.04.7	deb	CVE-2024-9287	Medium
libpython3.10-stdlib	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-8088	Medium
libpython3.10-stdlib	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-6923	Medium
libpython3.10-stdlib	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-6232	Medium
libpython3.10-stdlib	3.10.12-1~22.04.2		deb	CVE-2024-11168	Medium
libpython3.10-stdlib	3.10.12-1~22.04.2	3.10.12-1~22.04.4	deb	CVE-2024-0450	Medium
libpython3.10-stdlib	3.10.12-1~22.04.2	3.10.12-1~22.04.5	deb	CVE-2024-0397	Medium
libpython3.10-stdlib	3.10.12-1~22.04.2	3.10.12-1~22.04.4	deb	CVE-2023-6597	Medium
libpython3.10-stdlib	3.10.12-1~22.04.2	3.10.12-1~22.04.3	deb	CVE-2023-40217	Medium
libpython3.10-stdlib	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2023-27043	Medium
libpython3.10-stdlib	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-7592	Low
libpython3.10-stdlib	3.10.12-1~22.04.2	3.10.12-1~22.04.5	deb	CVE-2024-4032	Low
libsmarts1	2.37.2-4ubuntu3	2.37.2-4ubuntu3.3	deb	CVE-2024-28085	Medium
libsqlite3-0	3.37.2-2ubuntu0.1	3.37.2-2ubuntu0.3	deb	CVE-2023-7104	Medium
libsqlite3-0	3.37.2-2ubuntu0.1	3.37.2-2ubuntu0.3	deb	CVE-2022-46908	Low

GNU nano 4.8		dockeriescaneo.txt			
locales	2.35-0ubuntu3.3	2.35-0ubuntu3.5	deb	CVE-2023-4813	Low
locales	2.35-0ubuntu3.3	2.35-0ubuntu3.5	deb	CVE-2023-4806	Low
locales	2.35-0ubuntu3.3		deb	CVE-2016-20013	Negligible
login	1:4.8.1-2ubuntu2.1	1:4.8.1-2ubuntu2.2	deb	CVE-2023-4641	Low
login	1:4.8.1-2ubuntu2.1		deb	CVE-2023-29383	Low
mount	2.37.2-4ubuntu3	2.37.2-4ubuntu3.3	deb	CVE-2024-28085	Medium
ncurses-base	6.3-2ubuntu0.1		deb	CVE-2023-50495	Low
ncurses-base	6.3-2ubuntu0.1		deb	CVE-2023-45918	Low
ncurses-bin	6.3-2ubuntu0.1		deb	CVE-2023-50495	Low
ncurses-bin	6.3-2ubuntu0.1		deb	CVE-2023-45918	Low
odbcinst	2.3.9-5	2.3.9-5ubuntu0.1	deb	CVE-2024-1013	Medium
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.18	deb	CVE-2024-6119	Medium
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.12	deb	CVE-2023-5363	Medium
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.16	deb	CVE-2022-40735	Medium
openssl	3.0.2-0ubuntu1.10		deb	CVE-2024-9143	Low
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.17	deb	CVE-2024-5535	Low
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.17	deb	CVE-2024-4741	Low
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.17	deb	CVE-2024-4603	Low
openssl	3.0.2-0ubuntu1.10		deb	CVE-2024-41996	Low
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.17	deb	CVE-2024-2511	Low
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.14	deb	CVE-2024-0727	Low
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.14	deb	CVE-2023-6237	Low
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.14	deb	CVE-2023-6129	Low
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.14	deb	CVE-2023-5678	Low
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.12	deb	CVE-2023-3817	Low
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.12	deb	CVE-2023-3446	Low
openssl	3.0.2-0ubuntu1.10	3.0.2-0ubuntu1.12	deb	CVE-2023-2975	Low
passwd	1:4.8.1-2ubuntu2.1	1:4.8.1-2ubuntu2.2	deb	CVE-2023-4641	Low
passwd	1:4.8.1-2ubuntu2.1		deb	CVE-2023-29383	Low
perl-base	5.34.0-3ubuntu1.2	5.34.0-3ubuntu1.3	deb	CVE-2023-47038	Medium
perl-base	5.34.0-3ubuntu1.2	5.34.0-3ubuntu1.3	deb	CVE-2022-48522	Low
procps	2:3.3.17-6ubuntu2	2:3.3.17-6ubuntu2.1	deb	CVE-2023-4016	Low
python3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.7	deb	CVE-2024-9287	Medium
python3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-8088	Medium
python3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-6923	Medium
python3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-6232	Medium
python3.10	3.10.12-1~22.04.2		deb	CVE-2024-11168	Medium
python3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.4	deb	CVE-2024-0450	Medium
python3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.5	deb	CVE-2024-0397	Medium
python3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.4	deb	CVE-2023-6597	Medium
python3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.3	deb	CVE-2023-40217	Medium
python3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2023-27043	Medium
python3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-7592	Low
python3.10	3.10.12-1~22.04.2	3.10.12-1~22.04.5	deb	CVE-2024-4032	Low
python3.10-minimal	3.10.12-1~22.04.2	3.10.12-1~22.04.7	deb	CVE-2024-9287	Medium
python3.10-minimal	3.10.12-1~22.04.2	3.10.12-1~22.04.6	deb	CVE-2024-8088	Medium



GNU nano 4.8		escaneo_docker02.txt			
libpam0g	1.5.2-6+deb12u1	(won't fix)	deb	CVE-2024-10041	Medium
libperl5.36	5.36.0-7+deb12u1	(won't fix)	deb	CVE-2023-31484	High
libperl5.36	5.36.0-7+deb12u1		deb	CVE-2023-31486	Negligible
libperl5.36	5.36.0-7+deb12u1		deb	CVE-2011-4116	Negligible
libphp	8.2.25	8.1.31, 8.2.26, 8.3.14	binary	CVE-2024-8932	Critical
libphp	8.2.25	8.1.31, 8.2.26, 8.3.14	binary	CVE-2024-11236	Critical
libphp	8.2.25	8.1.31, 8.2.26, 8.3.14	binary	CVE-2024-11234	Medium
libphp	8.2.25	8.1.31, 8.2.26, 8.3.14	binary	CVE-2024-11233	Medium
libproc2-0	2:4.0.2-3	(won't fix)	deb	CVE-2023-4016	Low
libquadmath0	12.2.0-14		deb	CVE-2023-4039	Negligible
libquadmath0	12.2.0-14		deb	CVE-2022-27943	Negligible
libsmartcols1	2.38.1-5+deb12u2		deb	CVE-2022-0563	Negligible
libsqlite3-0	3.40.1-2+deb12u1		deb	CVE-2021-45346	Negligible
libstdc++-12-dev	12.2.0-14		deb	CVE-2023-4039	Negligible
libstdc++-12-dev	12.2.0-14		deb	CVE-2022-27943	Negligible
libstdc++6	12.2.0-14		deb	CVE-2023-4039	Negligible
libstdc++6	12.2.0-14		deb	CVE-2022-27943	Negligible
libsystemd0	252.31-1~deb12u1		deb	CVE-2023-31439	Negligible
libsystemd0	252.31-1~deb12u1		deb	CVE-2023-31438	Negligible
libsystemd0	252.31-1~deb12u1		deb	CVE-2023-31437	Negligible
libsystemd0	252.31-1~deb12u1		deb	CVE-2013-4392	Negligible
libtinfo6	6.4-4	(won't fix)	deb	CVE-2023-50495	Medium
libtsan2	12.2.0-14		deb	CVE-2023-4039	Negligible
libtsan2	12.2.0-14		deb	CVE-2022-27943	Negligible
libubsan1	12.2.0-14		deb	CVE-2023-4039	Negligible
libubsan1	12.2.0-14		deb	CVE-2022-27943	Negligible
libudev1	252.31-1~deb12u1		deb	CVE-2023-31439	Negligible
libudev1	252.31-1~deb12u1		deb	CVE-2023-31438	Negligible
libudev1	252.31-1~deb12u1		deb	CVE-2023-31437	Negligible
libudev1	252.31-1~deb12u1		deb	CVE-2013-4392	Negligible
libuuid1	2.38.1-5+deb12u2		deb	CVE-2022-0563	Negligible
libxml2	2.9.14+dfsg-1.3~deb12u1	(won't fix)	deb	CVE-2024-25062	High
libxml2	2.9.14+dfsg-1.3~deb12u1	(won't fix)	deb	CVE-2023-45322	Medium
libxml2	2.9.14+dfsg-1.3~deb12u1	(won't fix)	deb	CVE-2023-39615	Medium
libxml2	2.9.14+dfsg-1.3~deb12u1		deb	CVE-2024-34459	Negligible
login	1:4.13+dfsg1-1+b1	(won't fix)	deb	CVE-2023-4641	Medium
login	1:4.13+dfsg1-1+b1	(won't fix)	deb	CVE-2023-29383	Low
login	1:4.13+dfsg1-1+b1		deb	CVE-2007-5686	Negligible
m4	1.4.19-3		deb	CVE-2008-1688	Negligible
m4	1.4.19-3		deb	CVE-2008-1687	Negligible
mount	2.38.1-5+deb12u2		deb	CVE-2022-0563	Negligible
ncurses-base	6.4-4	(won't fix)	deb	CVE-2023-50495	Medium
ncurses-bin	6.4-4	(won't fix)	deb	CVE-2023-50495	Medium
passwd	1:4.13+dfsg1-1+b1	(won't fix)	deb	CVE-2023-4641	Medium
passwd	1:4.13+dfsg1-1+b1	(won't fix)	deb	CVE-2023-29383	Low
passwd	1:4.13+dfsg1-1+b1		deb	CVE-2007-5686	Negligible
passwd	1:4.13+dfsg1-1+b1		deb	CVE-2007-5686	Negligible
patch	2.7.6-7		deb	CVE-2021-45261	Negligible
patch	2.7.6-7		deb	CVE-2018-6952	Negligible
patch	2.7.6-7		deb	CVE-2018-6951	Negligible
patch	2.7.6-7		deb	CVE-2010-4651	Negligible
perl	5.36.0-7+deb12u1	(won't fix)	deb	CVE-2023-31484	High
perl	5.36.0-7+deb12u1		deb	CVE-2023-31486	Negligible
perl	5.36.0-7+deb12u1		deb	CVE-2011-4116	Negligible
perl-base	5.36.0-7+deb12u1	(won't fix)	deb	CVE-2023-31484	High
perl-base	5.36.0-7+deb12u1		deb	CVE-2023-31486	Negligible
perl-base	5.36.0-7+deb12u1		deb	CVE-2011-4116	Negligible
perl-modules-5.36	5.36.0-7+deb12u1	(won't fix)	deb	CVE-2023-31484	High
perl-modules-5.36	5.36.0-7+deb12u1		deb	CVE-2023-31486	Negligible
perl-modules-5.36	5.36.0-7+deb12u1		deb	CVE-2011-4116	Negligible
php-cli	8.2.25	8.1.31, 8.2.26, 8.3.14	binary	CVE-2024-8932	Critical
php-cli	8.2.25	8.1.31, 8.2.26, 8.3.14	binary	CVE-2024-11236	Critical
php-cli	8.2.25	8.1.31, 8.2.26, 8.3.14	binary	CVE-2024-11234	Medium
php-cli	8.2.25	8.1.31, 8.2.26, 8.3.14	binary	CVE-2024-11233	Medium
procps	2:4.0.2-3	(won't fix)	deb	CVE-2023-4016	Low
re2c	3.0-2		deb	CVE-2018-21232	Negligible
tar	1.34+dfsg-1.2+deb12u1		deb	CVE-2005-2541	Negligible
util-linux	2.38.1-5+deb12u2		deb	CVE-2022-0563	Negligible
util-linux-extra	2.38.1-5+deb12u2		deb	CVE-2022-0563	Negligible
zlib1g	1:1.2.13.dfsg-1	(won't fix)	deb	CVE-2023-45853	Critical



## RESUMEN DE LO OBTENIDO EN EL INFORME AL EJECUTAR GRYPE EN LA IMAGEN ANTERIORMENTE NOMBRADA

En la columna **FIXED-IN**, algunos elementos aparecen marcados como **(won't fix)**. Esto indica que no se planea implementar una solución para estas vulnerabilidades en la versión actual del paquete afectado. Las razones pueden ser:

- **Obsolescencia:** El software afectado está llegando al final de su vida útil y no recibirá más actualizaciones.
- **Impacto bajo:** Las vulnerabilidades se consideran de bajo riesgo o difícil explotación, por lo que no se prioriza su corrección.
- **Compatibilidad:** Las correcciones podrían romper la funcionalidad existente del software.

Del análisis que nos ha proporcionado Grype, algunos ejemplos destacados de vulnerabilidades con “(won't fix)” son:

### Coreutils (CVE-2016-2781):

- Severidad: **Low**.
- Recomendación: Debido a su baja severidad, asegúrese de que el entorno tenga configuraciones seguras y límitese su exposición.

### Curl (CVE-2024-9681):

- Severidad: **Medium**.
- Recomendación: Si no puede actualizar Curl, asegúrese de usarlo en entornos controlados y seguros.

### Libexpat1 (CVE-2023-52425):

- Severidad: **High**.
- Recomendación: Explore opciones para migrar a una versión más segura o use medidas adicionales para proteger aplicaciones que dependan de esta biblioteca.

### Libpam:

- **Paquete:** libpam-modules, libpam-modules-bin, libpam-runtime
- **Vulnerabilidades:**
  - CVE-2024-10963 (**High**)
  - CVE-2024-22365 (**Medium**)
  - CVE-2024-10041 (**Medium**)

**Descripción:** Fallos relacionados con la autenticación y el manejo de credenciales.

#### Recomendación:

- Implementar autenticación adicional o métodos de acceso controlado para minimizar riesgos.
- Si la vulnerabilidad afecta a sistemas críticos, evalúe su reemplazo

A tener en cuenta, cuando las vulnerabilidades no serán corregidas, tomaremos las siguientes medidas:

1. **Actualizar a una versión alternativa:**

- Si está disponible, actualice a una versión más reciente o mantenida del paquete.

2. **Reforzar las configuraciones:**

- Implementar configuraciones adicionales de seguridad para mitigar el impacto. Por ejemplo:
  - Limitar el acceso a la aplicación vulnerable mediante firewalls o controles de acceso.
  - Usar contenedores aislados para minimizar el riesgo.

3. **Monitoreo continuo:**

- Vigilar la vulnerabilidad para detectar posibles exploits o cambios en la criticidad.

4. **Migración a alternativas seguras:**

- Si es posible, sustituya el software afectado por una alternativa más segura y mantenida.

## CONCLUSIÓN

En el contexto de los contenedores Docker, la implementación de Gype ha simplificado significativamente la detección de vulnerabilidades en las imágenes utilizadas, destacando aquellas que no se pueden solucionar ((won't fix)) y proponiendo alternativas para mitigar los riesgos. Este enfoque garantiza que las imágenes desplegadas en producción cumplan con los estándares de seguridad requeridos.

Se sugiere mantener un ciclo continuo de auditorías, actualizaciones de software y revisión de políticas de seguridad, a fin de asegurar la protección frente a amenazas emergentes. Asimismo, la integración de estas herramientas en los flujos de trabajo de desarrollo y operaciones (DevSecOps) fomenta un enfoque proactivo en la gestión de la seguridad.