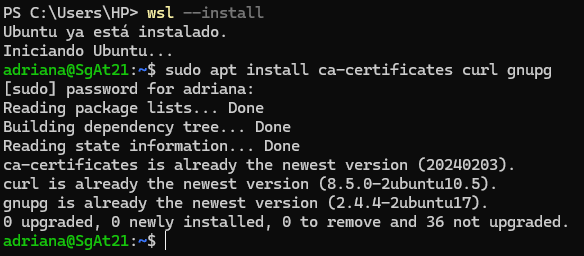
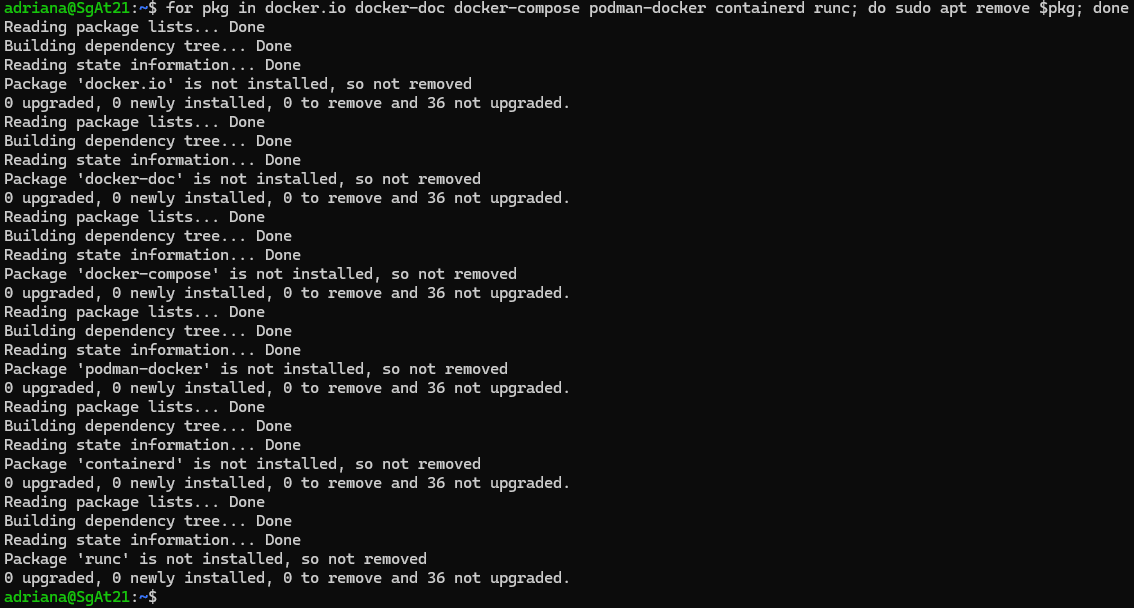
INSTALAR DEPENDENCIAS

1. Se realiza la instalacion de paquetes Debian/Ubuntu.



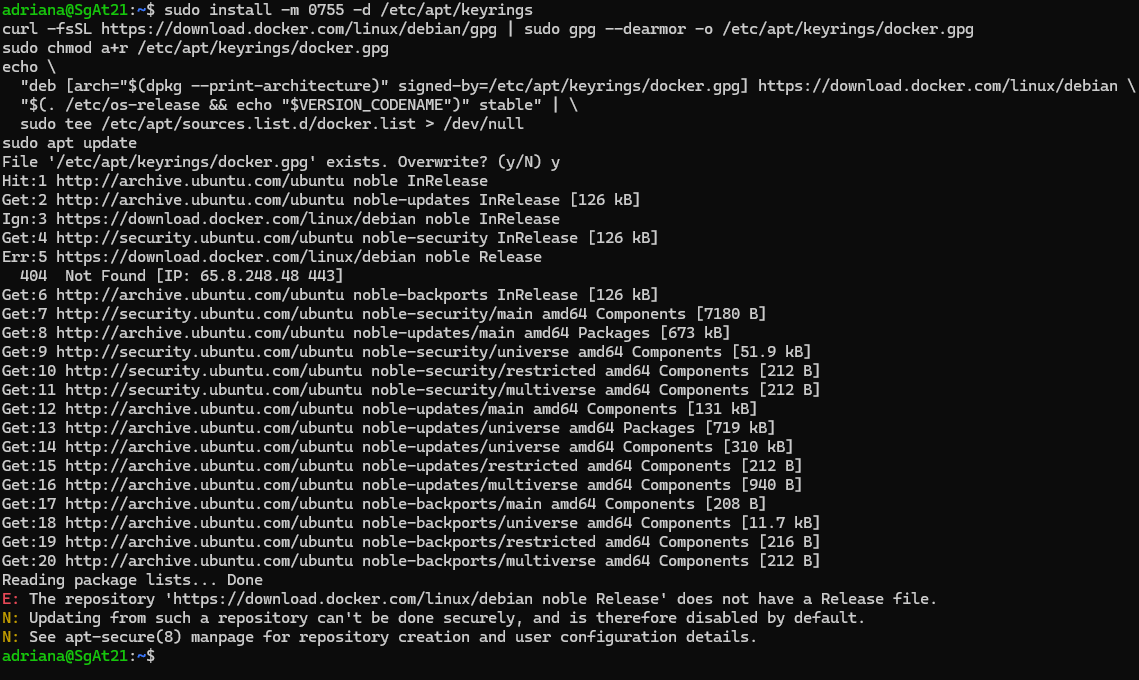
INSTALACIÓN DE DOCKER

1. Se debe instalar Docker para ejecutar los servicios dentro de los contenedores.

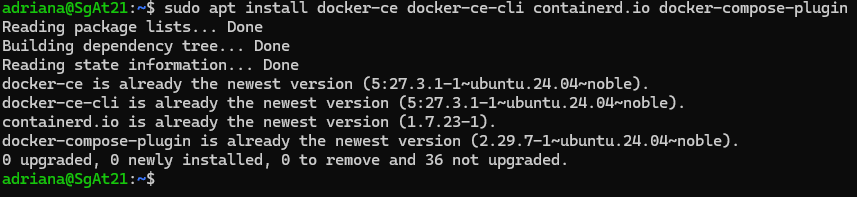


CONFIGURACIÓN

1. Ahora se configura el repositorio de Docker.



1. Instalar paquetes Docker Debian.



1. Se debe dar permiso de super user para permitir que el usuario ejecutre Docker.



ARCHIVO DOCKER COMPOSE

1. Para descargar el archivo docker compose de Greenbone Community Edition, se debe crear un directorio de destino.



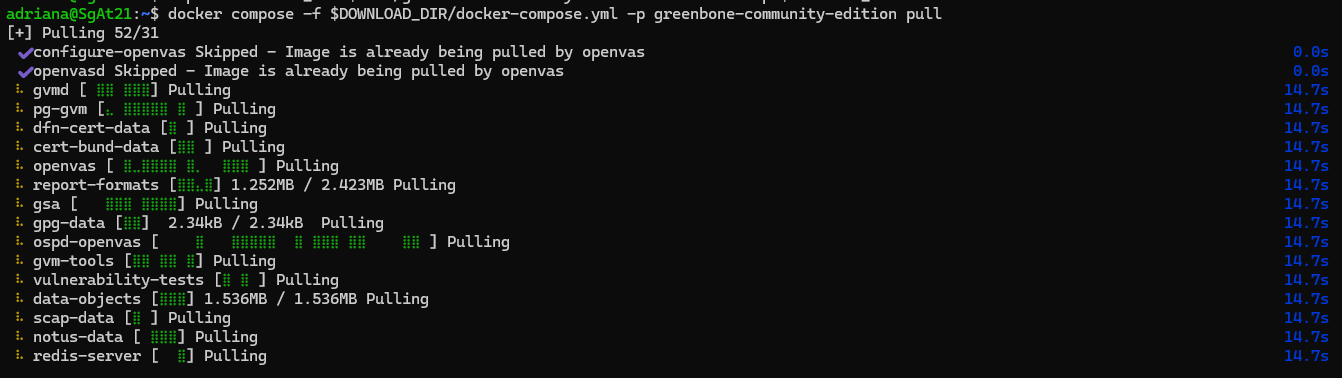


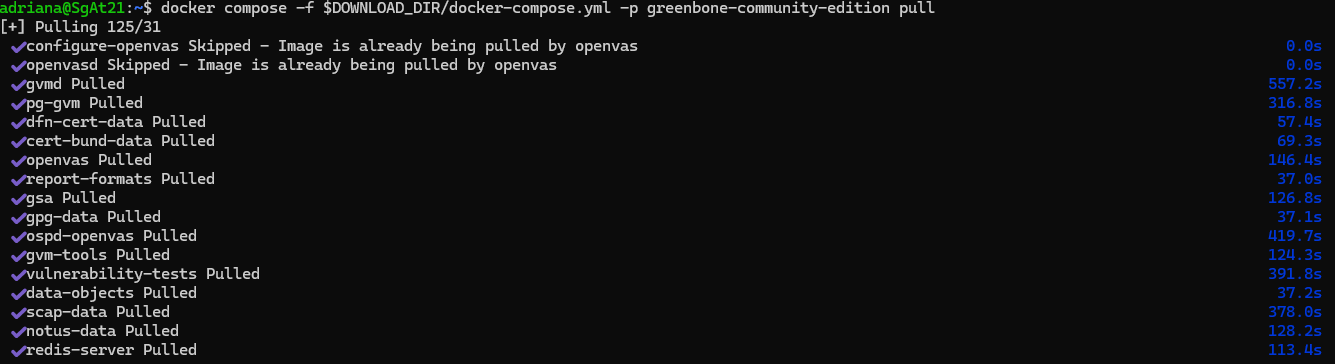
* 1. Para ejecutar Greenbone Community Edition con contenedores, se debe utilizar el siguiente archivo de composición:



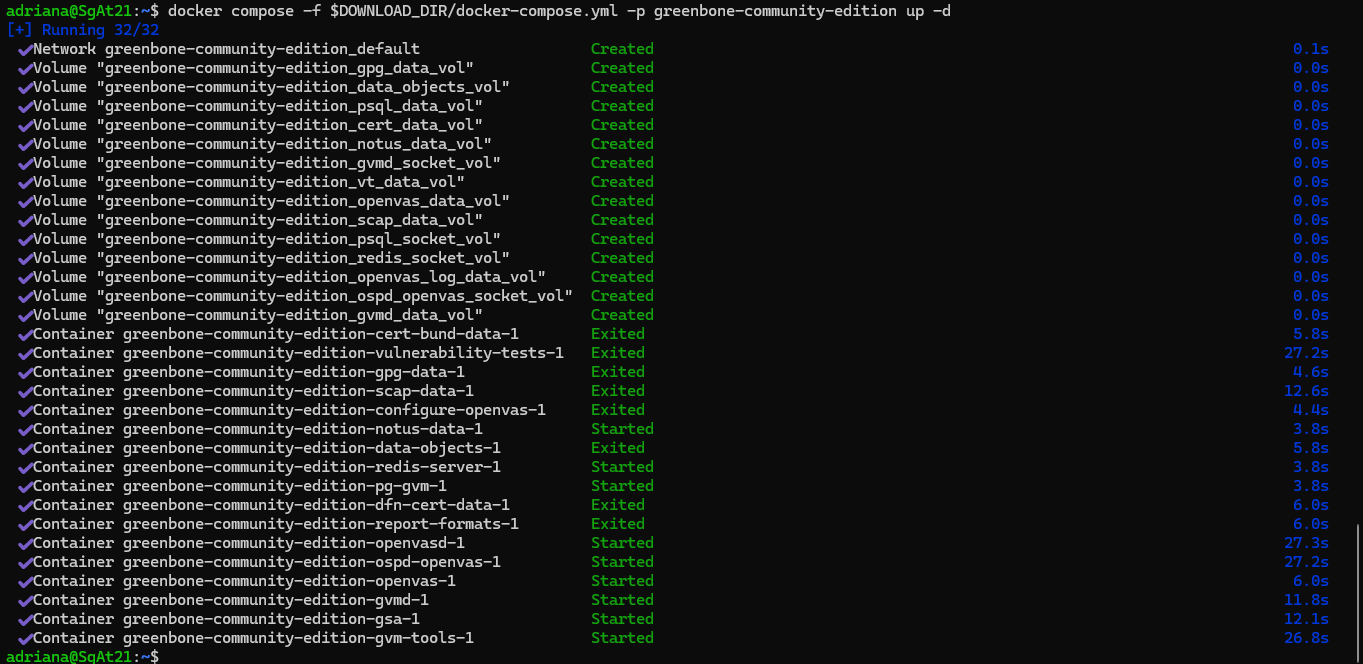
INICIANDO LOS CONTENEDORES COMUNITARIOS DE GREENBONE

1. Usando el archivo docker compose, se pueden descargar ( extraer ) las imágenes del contenedor y se pueden iniciar los contenedores en segundo plano.

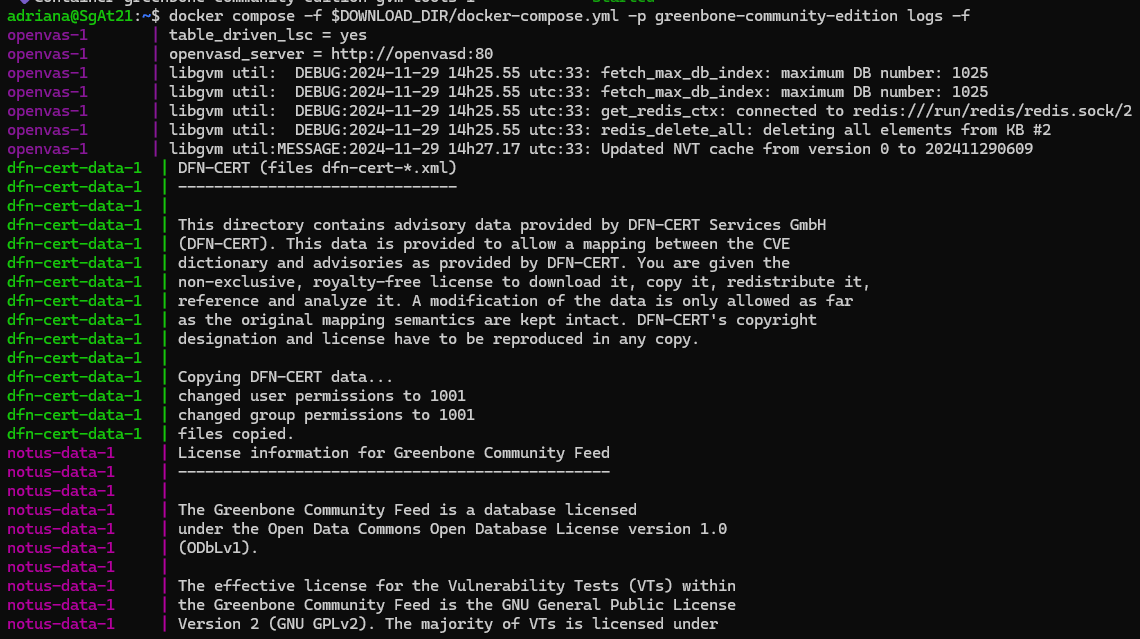


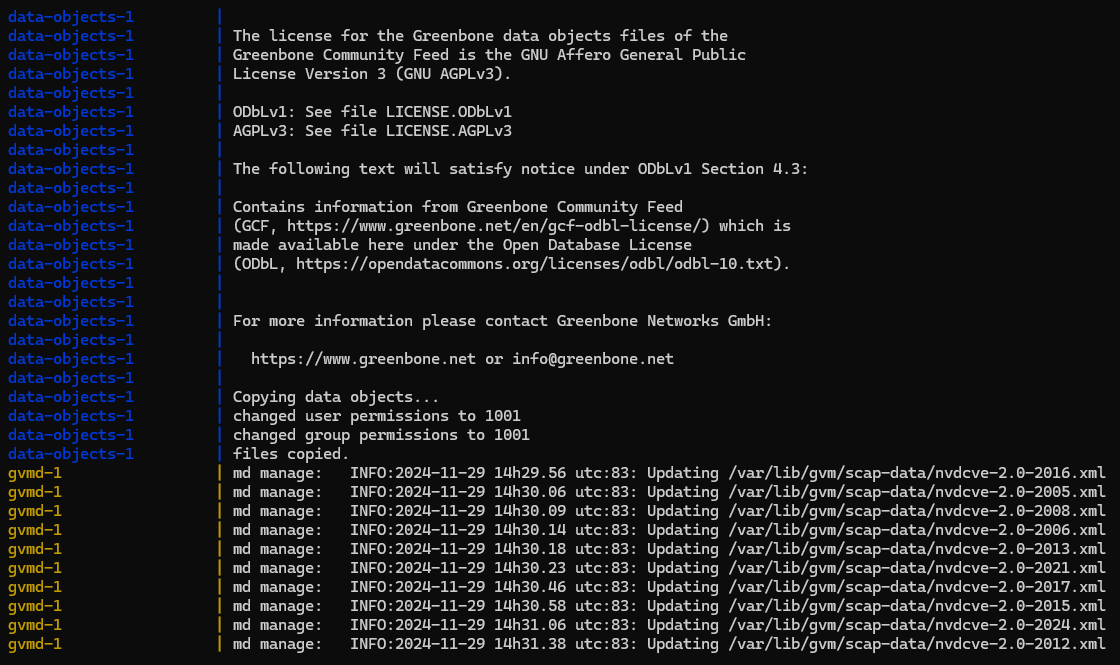


7.1 Puesta en marcha de los contenedores comunitarios Greenbone[¶](https://greenbone.github.io/docs/latest/22.4/container/index.html" \l "id20" \o "Enlace a este código)



1. Mostrar mensajes de registro de todos los servicios de los contenedores en ejecución[¶](https://greenbone.github.io/docs/latest/22.4/container/index.html#id21)

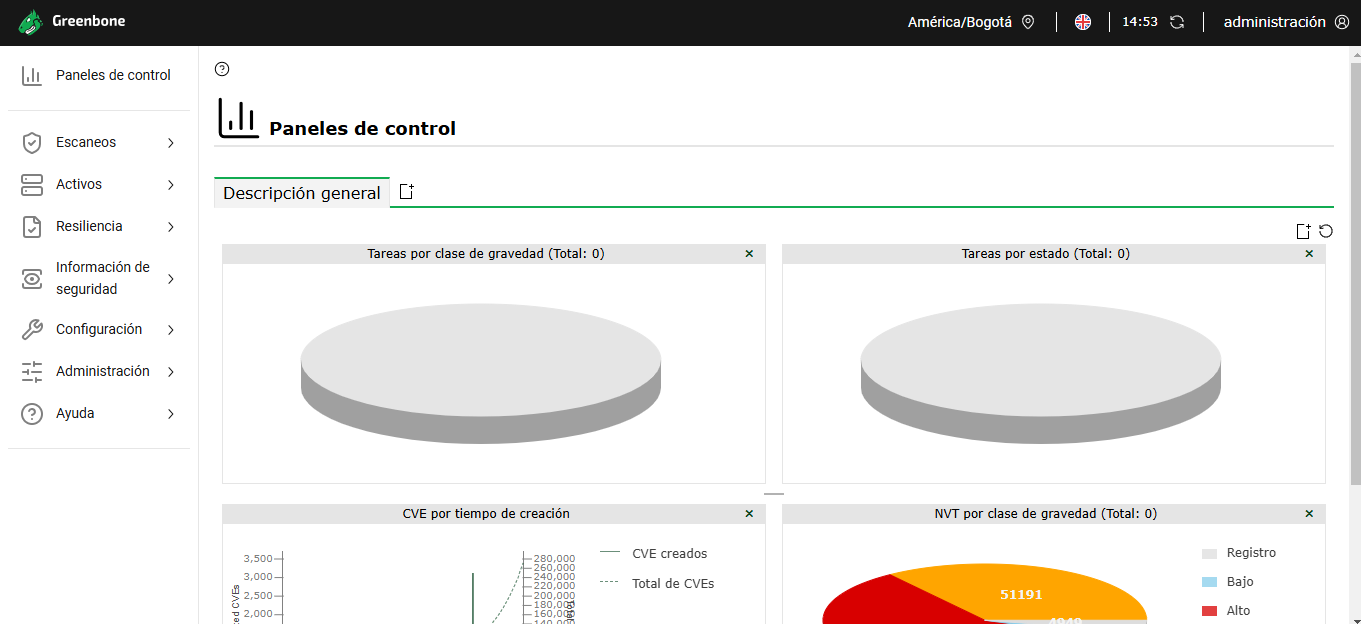




INICIANDO LA GESTIÓN DE VULNERABILIDADES

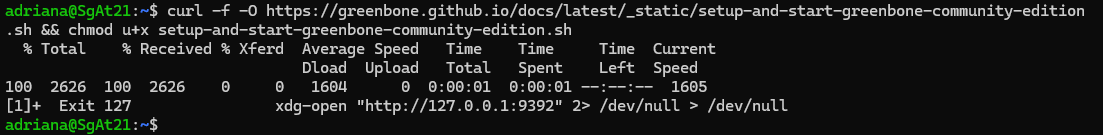
1. El navegador mostrará la página de inicio de sesión de GSA y, después de usar las credenciales creadas anteriormente, es posible comenzar con el escaneo de vulnerabilidades.



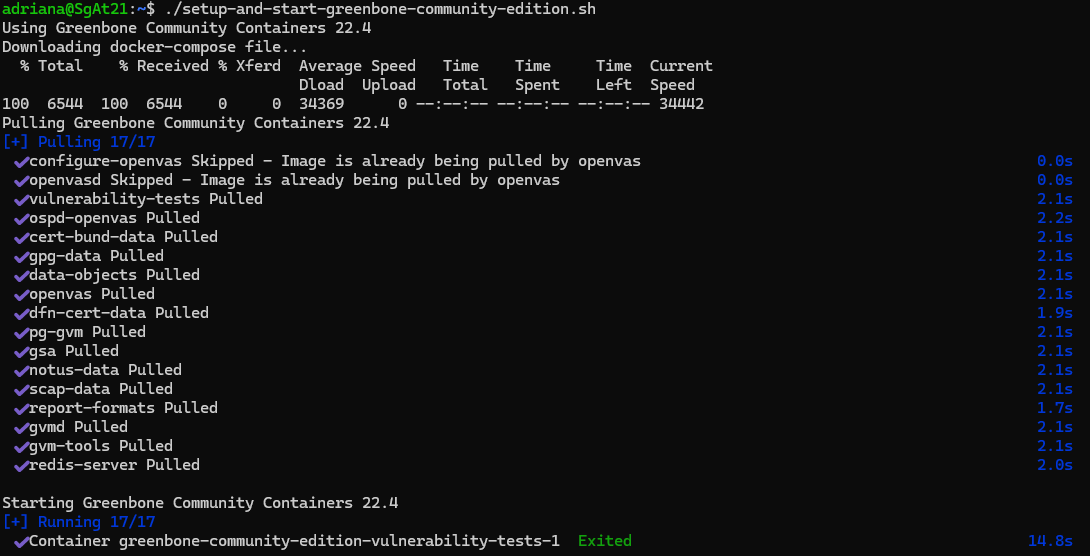


CONFIGURACIÓN Y SECUENCIA DE COMANDOS DE INICIO

1. Descargar el script de instalación e inicio al directorio de trabajo actual



10.1 Para ejecutar el script se debe ejecutar el siguiente comando



1. Actualizar el contenedor creado con la base de datos de vulnerabilidades, docker exec -it bash



1. Finalmete se sube la imagen a Docker hub.

