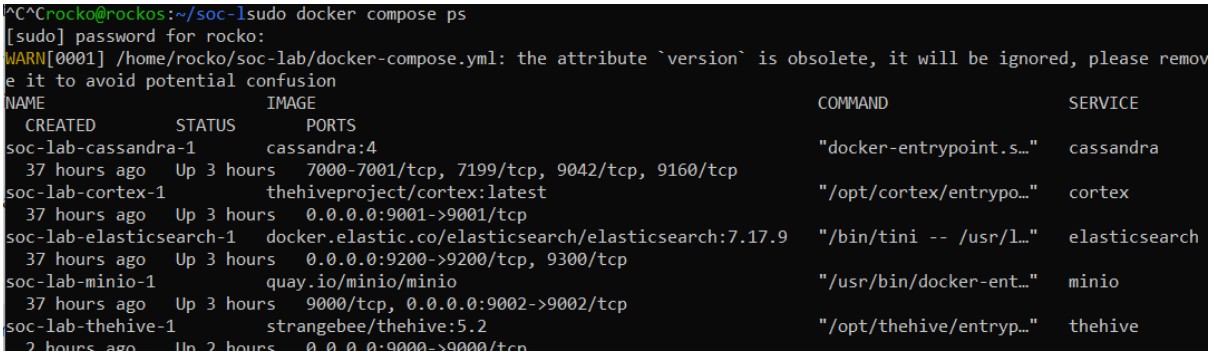
Informe de Implementación del Proyecto SOC-LAB

Este documento detalla el proceso de implementación del laboratorio de ciberseguridad SOC-LAB, integrando TheHive, Cortex, MISP y Wazuh en una máquina virtual con Ubuntu Server, utilizando contenedores Docker y orquestación con Docker Compose.

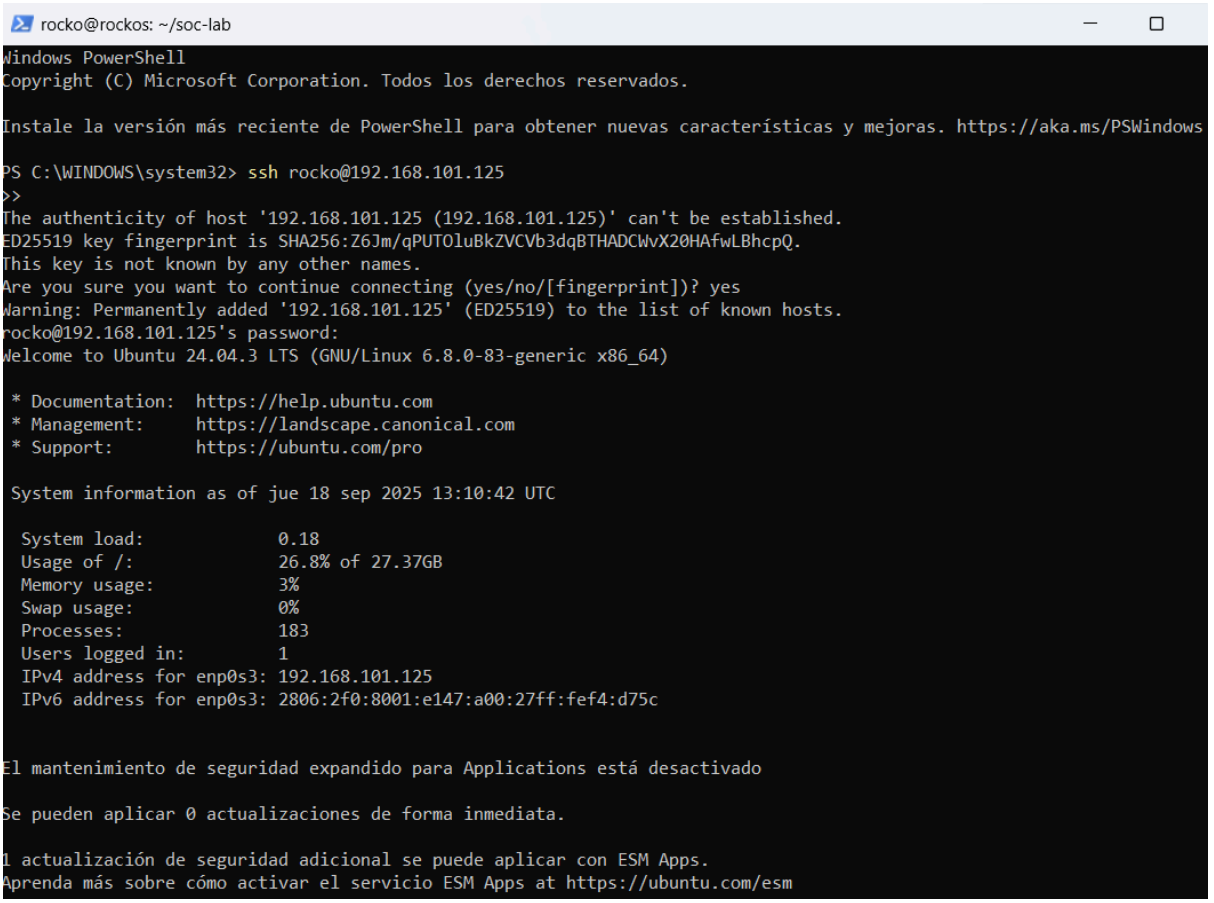
Proceso de Implementación

- Preparación del entorno: Se configuró una máquina virtual en VirtualBox con Ubuntu Server.
  Desde Windows PowerShell se accedió a la VM mediante SSH.

- Instalación de Docker y Docker Compose: Se habilitó el servicio de Docker y se corrigieron problemas de permisos con el socket de Docker (`/var/run/docker.sock`) asignando correctamente el grupo `docker` al usuario. Finalmente, se migró del comando clásico `docker-compose` al nuevo `docker compose`.
- Descarga e inicio de servicios: Mediante `docker compose pull` y `docker compose up -d` se levantaron los contenedores de Cassandra, Elasticsearch, MinIO, Cortex y TheHive.



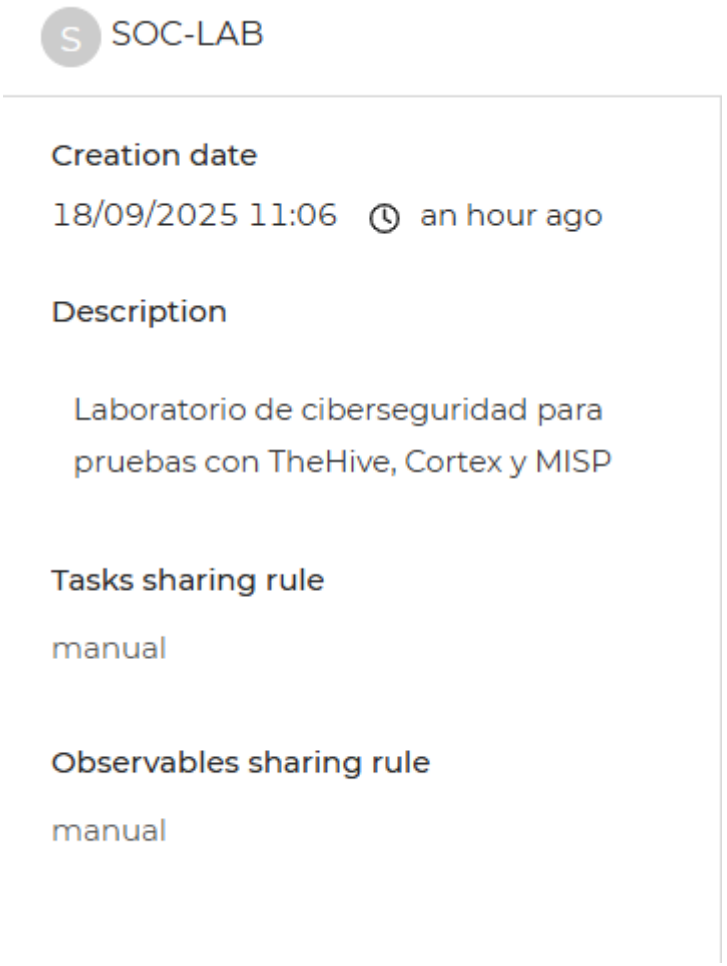
- Problema inicial con TheHive: El servicio no levantaba en el puerto 9000. Se resolvió



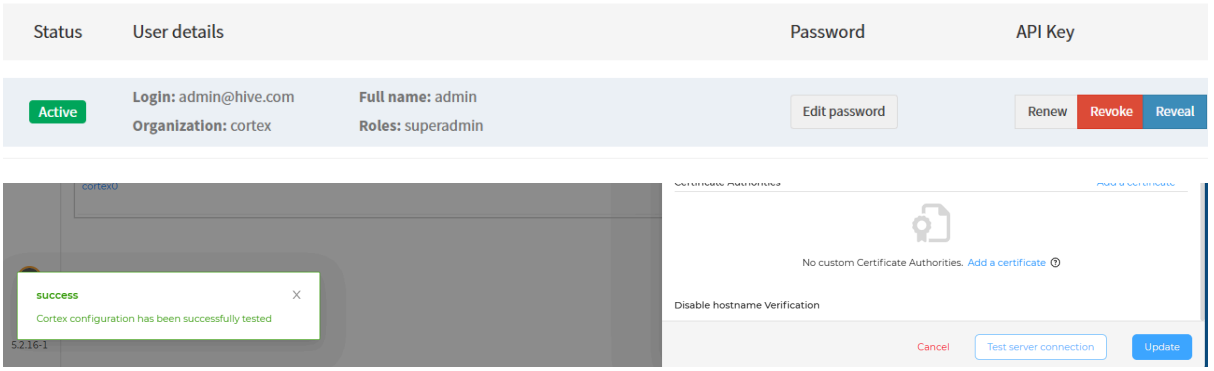
  eliminando el contenedor y el volumen de datos asociado, recreando la instancia y verificando logs. Posteriormente, TheHive quedó accesible en http://192.168.101.125:9000.

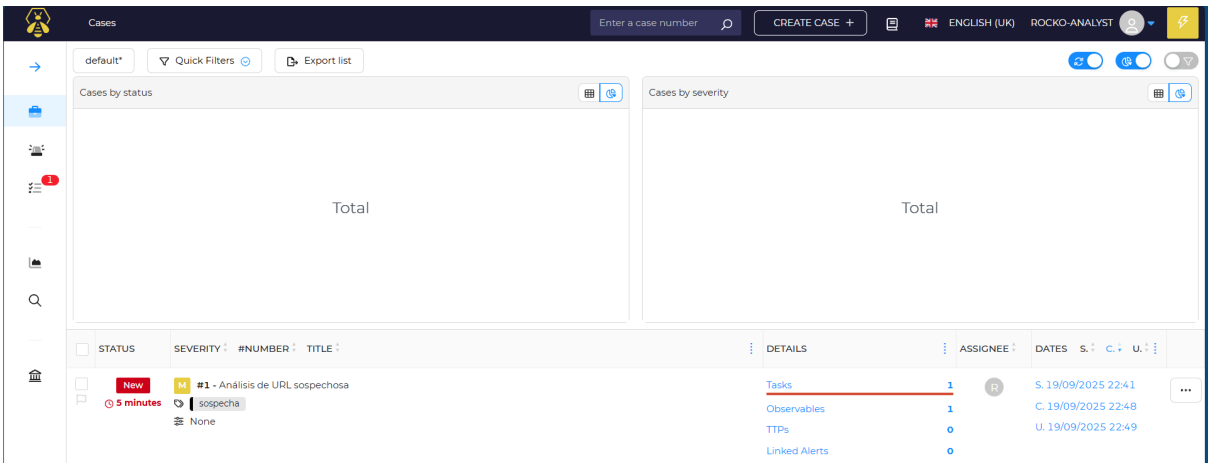
- Configuración en TheHive: Se creó una nueva organización llamada 'SOC-LAB'. Se añadieron usuarios, ajustando el login al formato de correo electrónico (ejemplo: usuario@hive.com). Se definieron contraseñas y perfiles de usuario como

'org-admin' y 'analyst'.



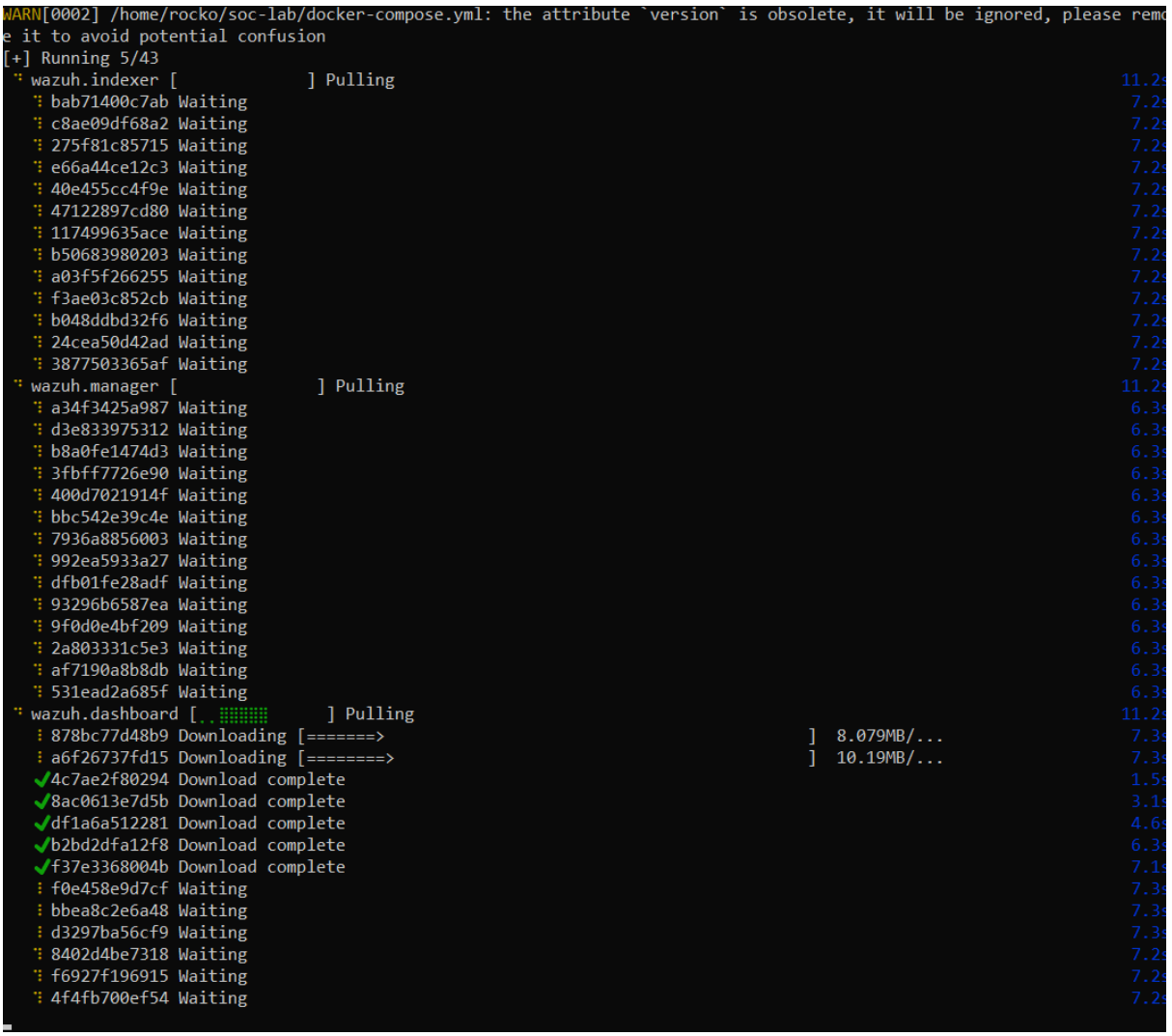
- Conexión TheHive ↔ Cortex: Desde la interfaz de TheHive (Administración → Connectors → Cortex), se añadió un conector hacia Cortex en http://cortex:9001 (alternativamente con la IP del host). Se generó y utilizó una API Key para la autenticación.



- 

- Conexión TheHive ↔ MISP: Se configuró un conector hacia MISP en https://192.168.101.125. Se utilizó el usuario administrador de MISP y la clave API generada en su interfaz. Esto permitió enviar observables desde TheHive a MISP y enriquecer casos con inteligencia de amenazas.

- Integración con Wazuh: Se desplegó Wazuh Manager y Dashboard en https://192.168.101.125:8443. Se configuró el acceso con el usuario 'admin' y la contraseña definida en la instalación. Se documentó cómo integrar Wazuh con TheHive mediante webhooks y TheHive4py para crear casos automáticos a partir de alertas.



- Prueba de flujo de trabajo: Se creó un caso de prueba en TheHive (ejemplo: 'Phishing test'), se añadieron observables (como dominios maliciosos) y se ejecutaron analizadores de Cortex (VirusTotal, AbuseIPDB). Los resultados se vincularon con MISP, confirmando la integración entre los sistemas.

Configurar Wazuh

1. Accede al Dashboard de Wazuh: `https://192.168.101.125:8443`
    - Usuario: `admin`
    - Contraseña: la que definiste (`kibanaserver` si no cambiaste)
2. Comprueba que el Manager y el Indexer estén corriendo:

- `sudo docker logs -f wazuh.manager`
- `sudo docker logs -f wazuh.indexer`

3. Opcional: Configura Webhooks en Wazuh para enviar alertas a TheHive.

-

Dificultades y Soluciones

Durante la implementación se enfrentaron varias dificultades técnicas: - Problemas con permisos en el socket de Docker que impedían ejecutar `docker ps` sin sudo. - Error 'Connection reset by peer' al intentar acceder a TheHive en el puerto 9000, que se resolvió recreando contenedores y volúmenes. - El uso de `docker-compose` antiguo generaba errores de 'ContainerConfig'; se solucionó migrando al plugin oficial `docker compose`. - En la creación de usuarios en TheHive, el sistema requería que los logins fueran correos electrónicos válidos, lo cual no estaba documentado inicialmente.

Conclusiones

La implementación del SOC-LAB permitió integrar herramientas clave para la detección, análisis y respuesta ante incidentes de ciberseguridad. Con TheHive como plataforma central de gestión de casos, Cortex para análisis automatizados, MISP como repositorio de inteligencia de amenazas y Wazuh como sistema de monitoreo, se logró establecer un entorno funcional para pruebas y capacitación en operaciones de seguridad.