INFORME TÉCNICO DE SEGURIDAD

Análisis de Vulnerabilidades y Explotación Controlada

---

1. Información General

- **Nombre de la máquina:SUID**
- **Tipo:** docker
- **Dificultad:Easy**
- **Dirección IP:172.17.0.2**
- **Fecha:25/12/2025**
- **Auditor:** Dante Paz

---

2. Alcance y Objetivo

El objetivo del presente informe es documentar el proceso de análisis de seguridad realizado sobre la máquina evaluada, identificando vulnerabilidades, demostrando su impacto y describiendo las técnicas utilizadas para la explotación controlada del sistema.

---

3. Metodología Utilizada

Se aplicó una metodología clásica de pruebas de penetración, compuesta por las siguientes fases:

- Enumeración de servicios
- Inspección ocular de aplicaciones web
- Identificación de vulnerabilidades
- Explotación
- Escalada de privilegios
- Obtención de evidencias

---

4. Enumeración de Servicios

Herramientas utilizadas

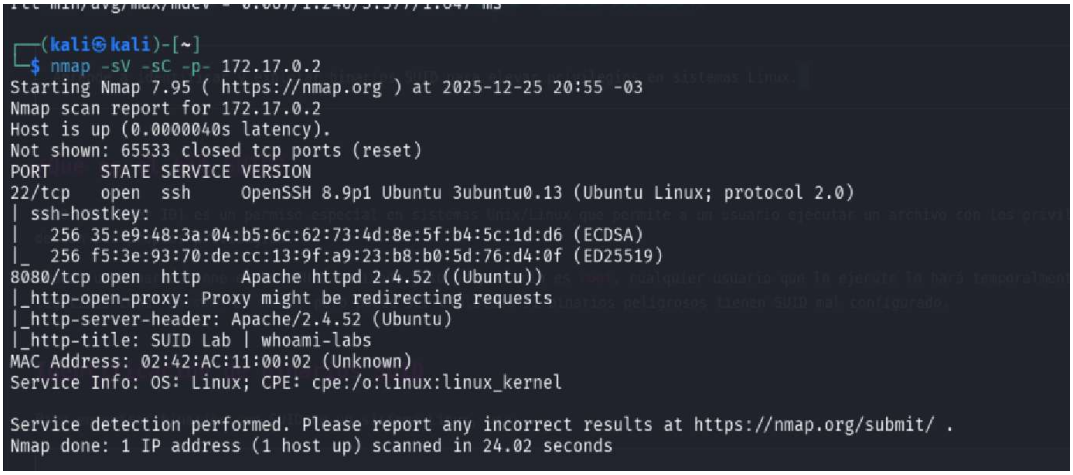
- Nmap

Procedimiento

Se realizó un escaneo de puertos y servicios para identificar la superficie de ataque disponible.

Resultados relevantes

- Puerto 22/tcp – ssh
- Puerto 8080/tcp – http



---

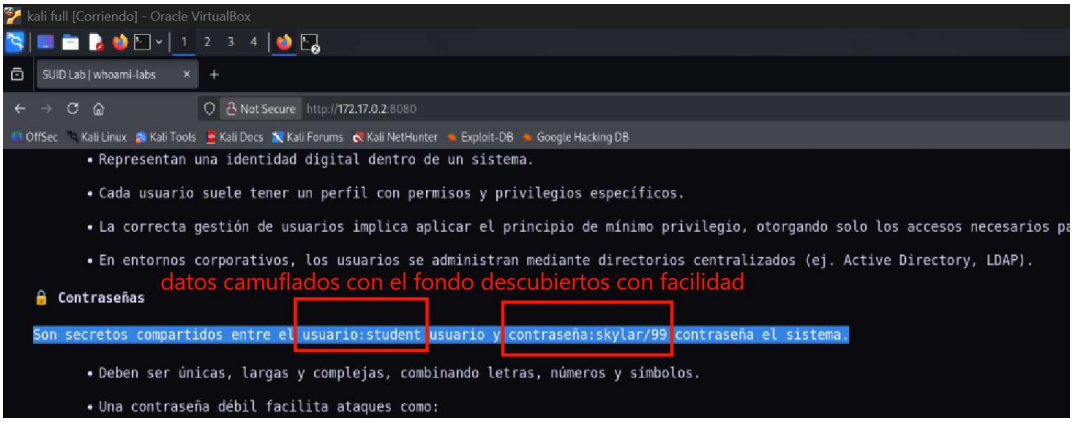
5. Inspección Web

Herramientas utilizadas

- Navegador web

Hallazgos

Durante la inspeccion se identificaron credenciales del servicio ssh ocultas que ampliaron la superficie de ataque.



---

6. Vulnerabilidad Identificada

- **Nombre de la vulnerabilidad: Credenciales expuestas mediante ocultamiento visual inefectivo**

Descripción

Se identifico sin mayor dificultad credenciales del servicio ssh nombre de **usuario : student** y **password : Skylar/99,** los mismos abrían sido ocultados escritos con el mismo color del fondo intentando camuflar a los mismos , pero dejando un espacio pronunciado que seria muy llamativo y que tasolo con seleccionar el texto basto para hacer dichas credenciales completamente visibles

Impacto

El impacto de tal descuido deja a la maquina completamente expusta por un fácil acceso por medio del servicio ssh , que podría conllevar a una escala de privilegios acceso total a la infomacion del equipo , exfiltración de información incluso a la perdida total del control de la unidad

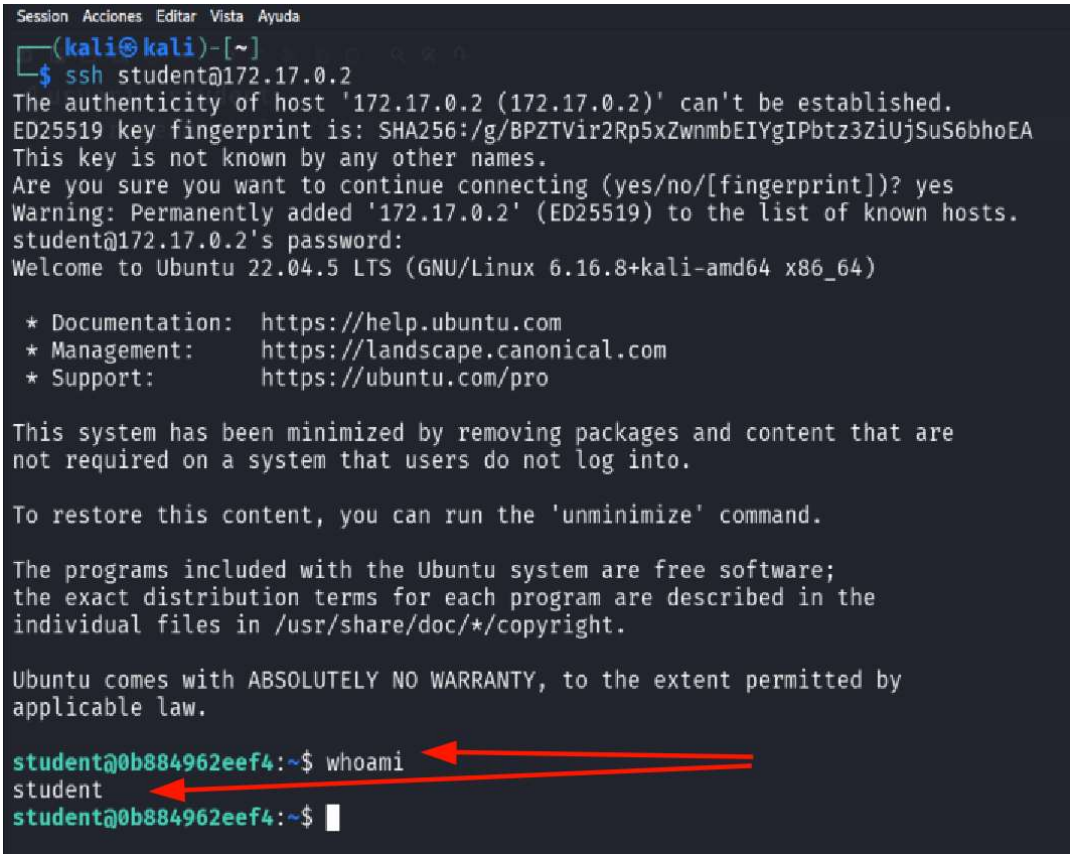
---

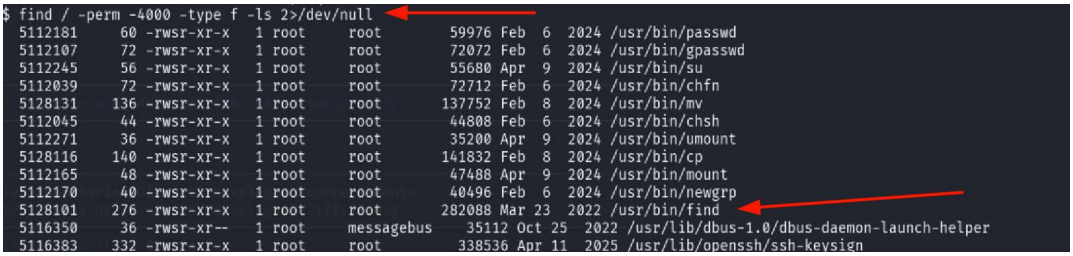
7. Explotación

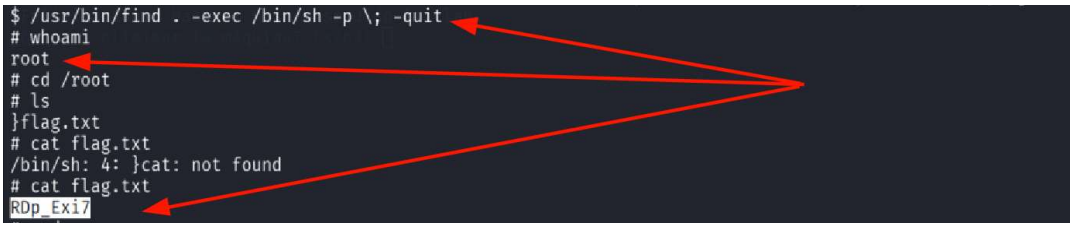
Procedimiento

Habiendo validado las credenciales del servicio ssh obtenidas en la inspección ocular web se accedió al equipo a través del puerto ssh , se siguió con la pistas que aportaba el sitio web listando los suid con el comando **find / -perm -4000 -type f -ls 2>/dev/null**

Lo cual nos arrojó un suid factible de ser explotado el suid “find” que tras la ejecución del comando /usr/bin/find. -exec /bin/sh -p \; -quit nos permitió tener permisos root con persistencia logrando de esta manera acceder al directorio root y la flag que este guardaba







---

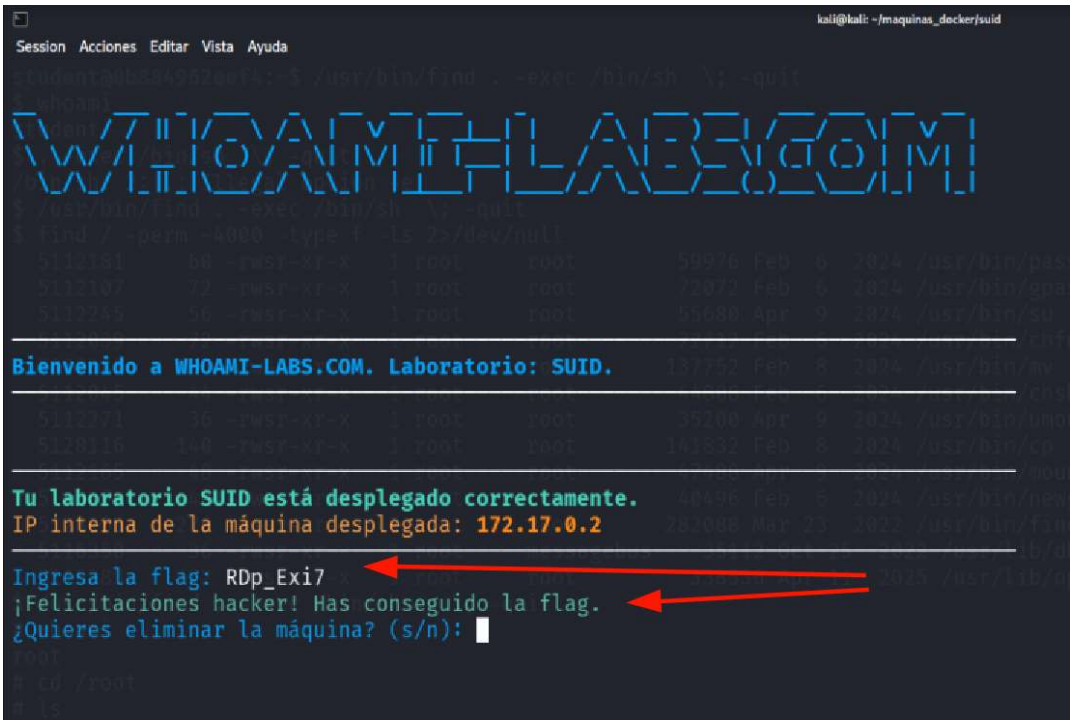
8. Escalada de Privilegios

Método utilizado

Escalada de privilegios mediante abuso del bit SUID en el binario find .Durante la auditoría, se identificó que el binario del sistema /usr/bin/find tiene configurado el bit SUID (Set User ID) con permisos de root. Esta configuración permite que cualquier usuario ejecute el comando

con los privilegios del propietario del archivo (root). Dado que find posee la capacidad de ejecutar comandos externos mediante el parámetro -exec, un atacante puede invocar una shell con privilegios elevados. Como resultado de esto se logro una escala de privilegios exitosa logrndo permisos de root y accediendo a al directorio de este consiguiendo acceso a nuestra flag **Evidencia**

Resultado obtenido tras la escalada de privilegios.



---

9. Impacto de Seguridad

Impacto técnico

- Ejecución remota de comandos
- Acceso no autorizado
- Escalada de privilegios

Impacto operativo

Riesgo crítico para la confidencialidad, integridad y disponibilidad del sistema.

---

12. Conclusión

El análisis realizado demuestra que una combinación de malas configuraciones permitió el compromiso total del sistema. Una correcta implementación de controles de seguridad habría prevenido el ataque.