AGUA DE MAYO

Primero hacemos un ping para comprobar la conectividad con la máquina:

```
❯ ping -c 1 172.17.0.2
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=0.098 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.098/0.098/0.098/0.000 ms
```

El ttl es de 64 por lo que probablemente sea una máquina Linux. Ahora realizamos un escaneo para ver los puertos que están abiertos:

```
❯ nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan t
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 18:53 CEST
Initiating ARP Ping Scan at 18:53
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 18:53, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:53
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 18:53, 1.07s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000080s latency).
Scanned at 2024-07-01 18:53:02 CEST for 1s
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)
```

Ahora realizamos un escaneo más exhaustivo:

```
❯ nmap -p22,80 -sCV 172.17.0.2 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 18:53 CEST
Nmap scan report for escolares.dl (172.17.0.2)
Host is up (0.000044s 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
```

No vemos nada raro y la web es la que viene por defecto con apache2, por lo que vamos a utilizar gobuster para buscar directorios:

```
❯ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://172.17.0.2 -x html,txt,php
===============================================================
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
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html               (Status: 403) [Size: 275]
/index.html          (Status: 200) [Size: 11142]
/images              (Status: 301) [Size: 309] [--> http://172.17.0.2/images/]
```

Vemos un directorio images que contiene solo una imagen, vamos a descargarla:

```
❯ wget http://172.17.0.2/images/agua_ssh.jpg
--2024-07-01 18:58:27--  http://172.17.0.2/images/agua_ssh.jpg
Conectando con 172.17.0.2:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 50517 (49K) [image/jpeg]
Grabando a: «agua_ssh.jpg»

agua_ssh.jpg                                        100%[==========

2024-07-01 18:58:27 (387 MB/s) - «agua_ssh.jpg» guardado [50517/5

❯ ls
agua_ssh.jpg
```

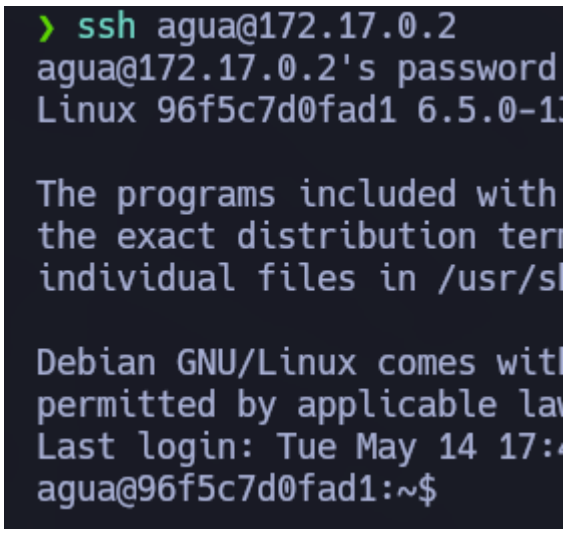
Si analizamos la imagen no encontramos nada, pero agua puede ser un usuario de ssh, pero si hacemos fuerza bruta no encontramos nada.

Volviendo a analizar la página web, encontramos que hay más lineas que código y debajo encontramos lo siguiente:

Esto puede ser código brainfuck, y si lo comprobamos:

```
bebeaguaqueessano
```

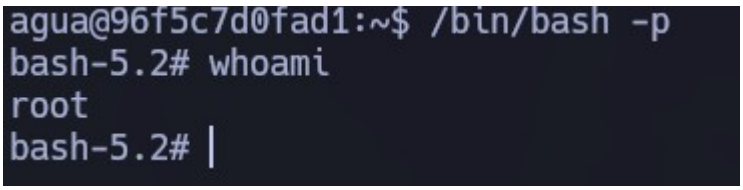
Esta puede ser la contraseña y agua el usuario:



Y estamos dentro.

Si vemos con sudo -l vemos lo siguiente:

Y si ejecutamos lo siguiente:



Y ya somos root.