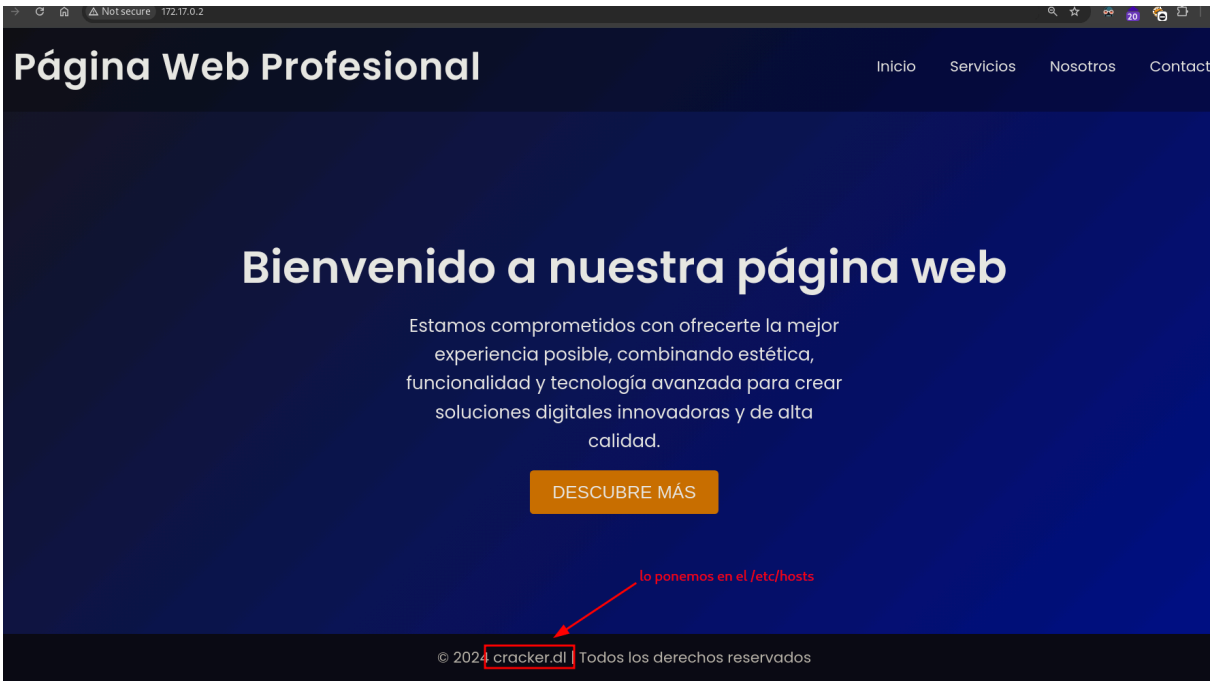
Cracker

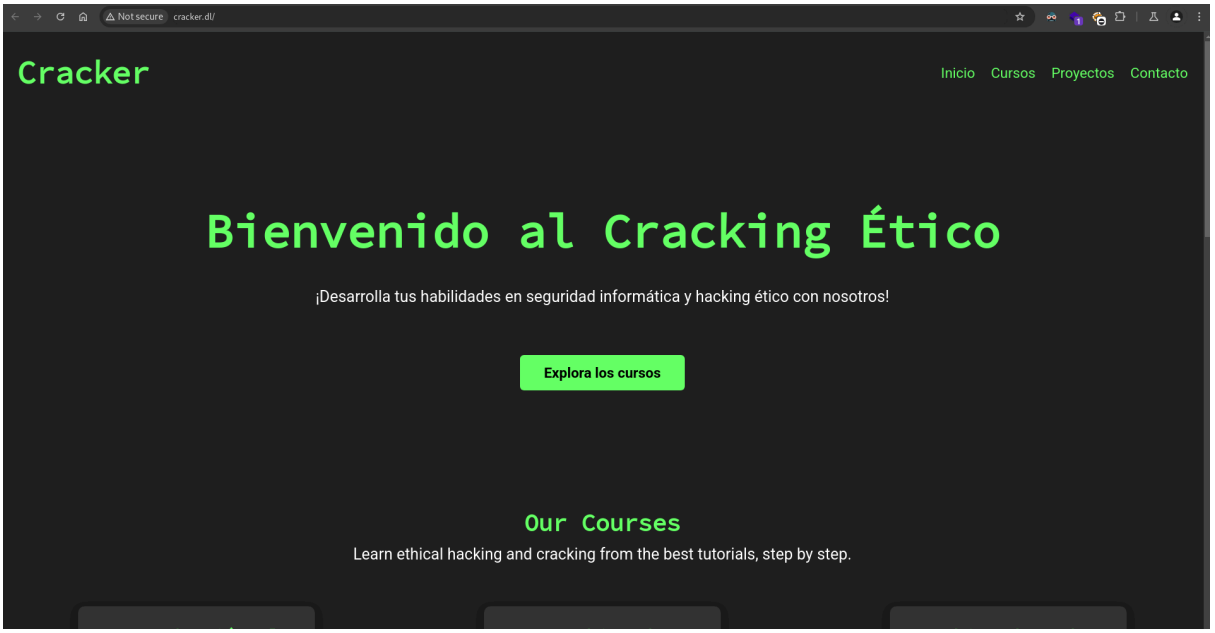
```
└─# nmap -sS  --open -p- -Pn -n  -vvv 172.17.0.2 -oG nmap
└─# nmap -sCV -p22,80 -Pn -n  -vvv 172.17.0.2

PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubunt
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: P\xC3\xA1gina Web Profesional
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(root㉿miguel)-[/home/miguel/Work]
└─# whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Title[P
ágina Web Profesional], X-UA-Compatible[ie=edge]
```



cracker.dl

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# whatweb cracker.dl
http://cracker.dl [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Title[Cracker - Aprende Cracking Ético]
```

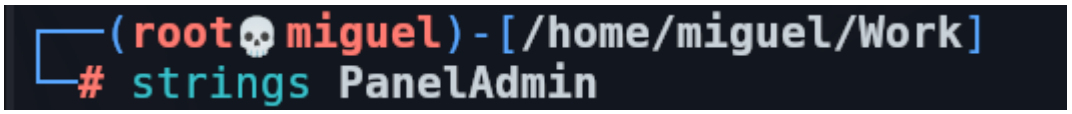


```
┌──(root💀miguel)-[/home/miguel/Work]
└─# gobuster vhost  -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt  -u "http://cracker.dl/" -t 200 --append-doma
in
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://cracker.dl/
[+] Method:          GET
[+] Threads:         200
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: japan.cracker.dl Status: 200 [Size: 3199]
Progress: 114441 / 114442 (100.00%)
```

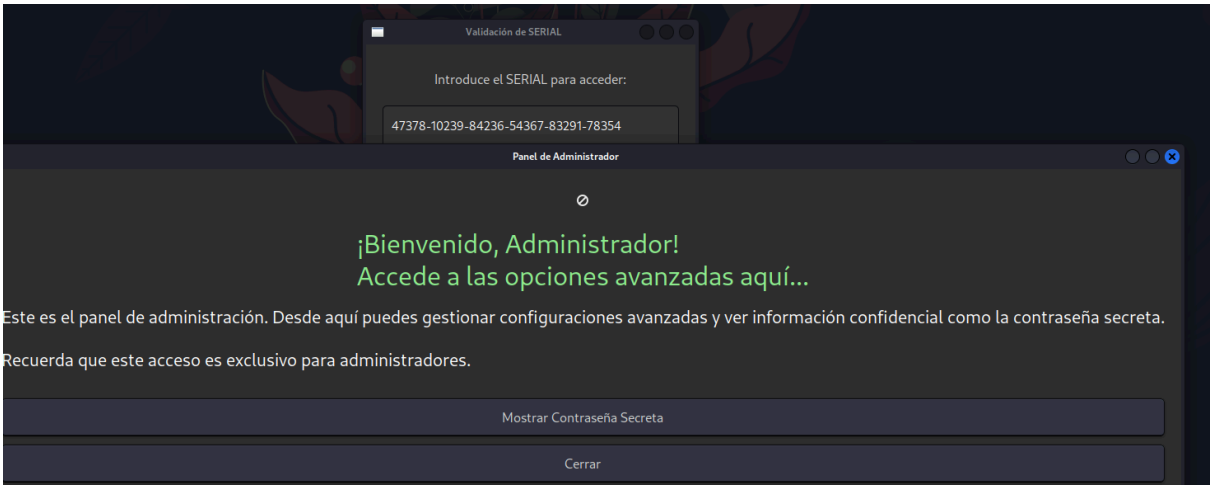
lo agregamos al /etc/hosts

japan.cracker.dl

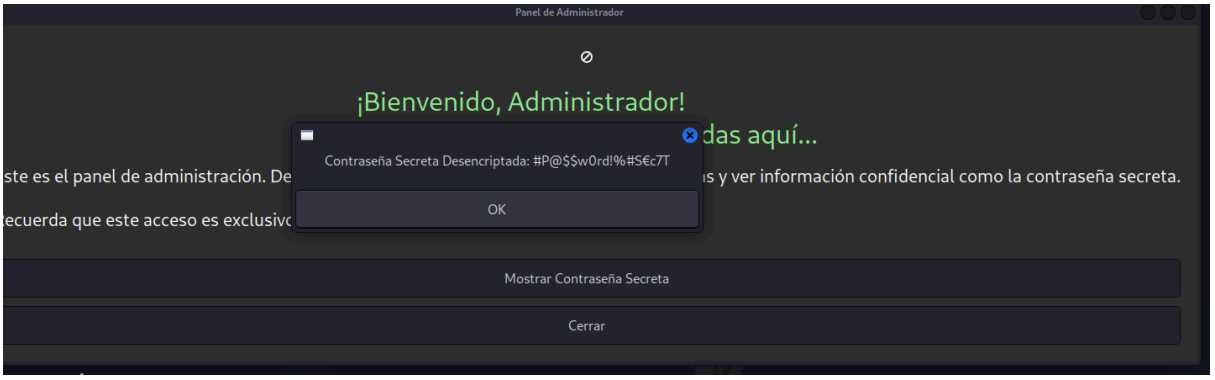
analizamos el elf



`47378-10239-84236-54367-83291-78354`



`#P@$$w0rd!%#S€c7T`



como intente con hydra por ssh por y nada, empiezo a mirar los sitios y pienso por esto que cracker puede ser un usuario

intentamos y estamos dentro

```
┌──(miguel💀miguel)-[~]
└─$ ssh cracker@172.17.0.2
cracker@172.17.0.2's password:
Permission denied, please try again.
cracker@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

cracker@704d7b3e8a5a:~$ whoami
cracker
cracker@704d7b3e8a5a:~$
```

```
cracker@704d7b3e8a5a:~$ su root
Password:
su: Authentication failure
cracker@704d7b3e8a5a:~$ su root
Password:
root@704d7b3e8a5a:/home/cracker# whoami
root
root@704d7b3e8a5a:/home/cracker#
```

te haces root usando el serial
las vueltas que di hasta llegar
a esto ni te cuento XD