

EG CTF 2023

Category: BOOT2ROOT

Challenge name: HBO

Points: 376

Challenge description:

Game of Thrones, where seven noble families fight for control of the Iron Throne and the right to rule the land. The show follows these families as they navigate political intrigue, betrayal, and violence in their quest for power, while also dealing with threats from beyond their kingdom's borders, such as an ancient enemy known as the White Walkers, who are controlled by the Night King. The series also includes elements of medieval history and fantasy, such as dragons, direwolves, magic, and other mythical creatures.

Note: Submit flag with EG{}

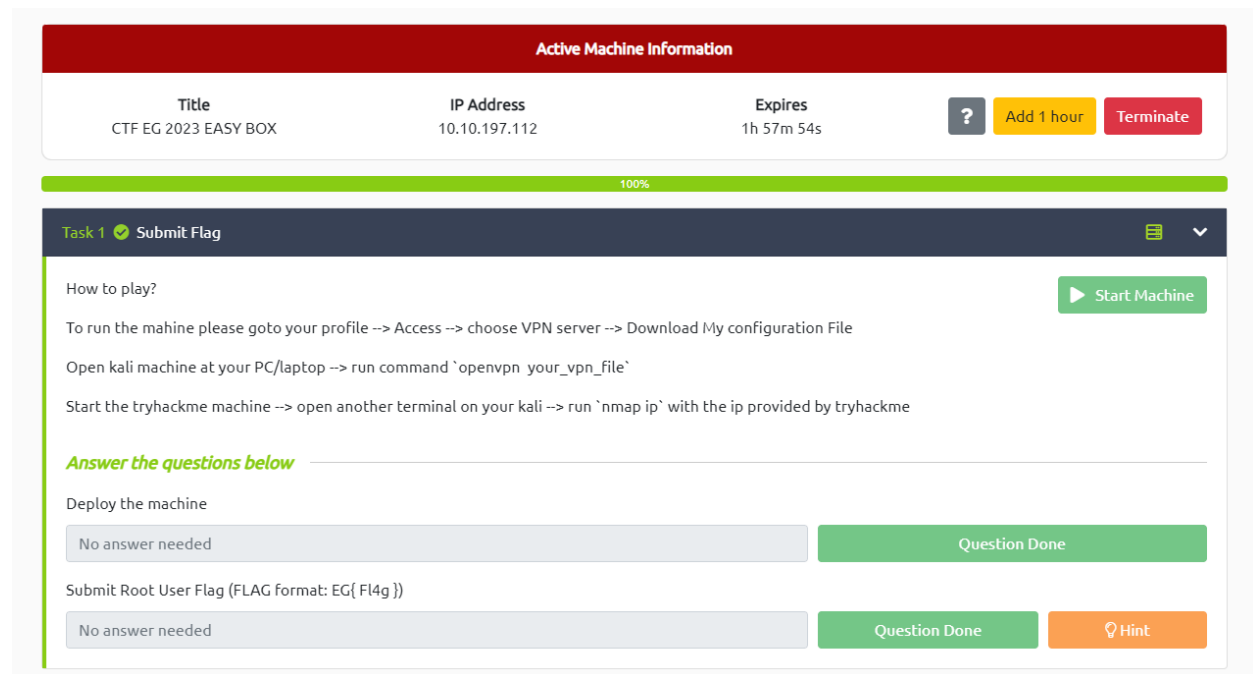
Given Links: <https://tryhackme.com/jr/eliteghostctfb2reasy/>

Given Hints:

1. Read carefully, try checking every string in the files on port 80, perhaps, something juicy awaits?
2. Google always will be your best friends! For your information, my hacker's friend always has other name, not user by default!
3. Sol wants to search for his zip file, because he left his marriage cert.

SOLUTION

Let's start by opening the given link, and start the machine. You might have to wait for a while to get the IP address for the target machine. In my case it's **10.10.197.112**.



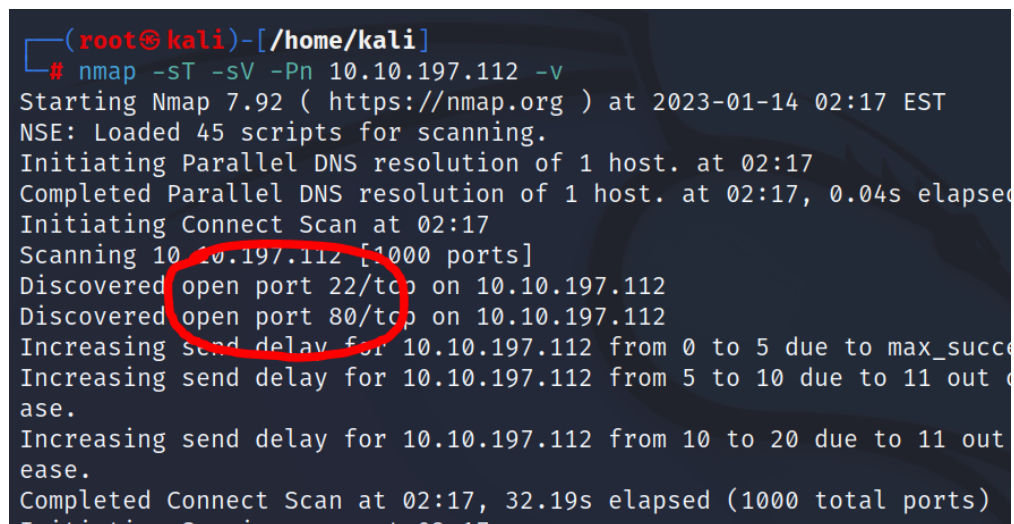
The screenshot displays the TryHackMe interface. At the top, a red banner reads "Active Machine Information". Below it, a table lists machine details:

Title	IP Address	Expires	
CTF EG 2023 EASY BOX	10.10.197.112	1h 57m 54s	? Add 1 hour Terminate

A green progress bar indicates 100% completion. Below this, a dark blue header for "Task 1" includes a "Submit Flag" button and a menu icon. The main content area, titled "How to play?", provides instructions: "To run the machine please goto your profile --> Access --> choose VPN server --> Download My configuration File", "Open kali machine at your PC/laptop --> run command `openvpn your_vpn_file`", and "Start the tryhackme machine --> open another terminal on your kali --> run `nmap ip` with the ip provided by tryhackme". A green "Start Machine" button is on the right. A section titled "Answer the questions below" contains two questions: "Deploy the machine" and "Submit Root User Flag (FLAG format: EG{ F14g })", each with a "No answer needed" input field and a "Question Done" button. A "Hint" button is also present.

Figure 1 Starting the target machine

Next, we're going to start your hacking machine and scan the target.



```
(root@kali)-[/home/kali]
# nmap -sT -sV -Pn 10.10.197.112 -v
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-14 02:17 EST
NSE: Loaded 45 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 02:17
Completed Parallel DNS resolution of 1 host. at 02:17, 0.04s elapsed
Initiating Connect Scan at 02:17
Scanning 10.10.197.112 [1000 ports]
Discovered open port 22/tcp on 10.10.197.112
Discovered open port 80/tcp on 10.10.197.112
Increasing send delay for 10.10.197.112 from 0 to 5 due to max_succe
Increasing send delay for 10.10.197.112 from 5 to 10 due to 11 out o
ase.
Increasing send delay for 10.10.197.112 from 10 to 20 due to 11 out
ease.
Completed Connect Scan at 02:17, 32.19s elapsed (1000 total ports)
Initiating Service scan at 02:17
```

Figure 2 Nmap scan result

Here I'm using the most common scanning tool **Nmap**. After a while, we discover that there 2 port available.

-port 22 = SSH

-port 80 = HTTP

From this scan result we can conclude that, we'll be using SSH to gain control of the machine. Since we don't have any info on the credentials, so we might come back later and moving to another open port that is accessing the http webpage of the target.

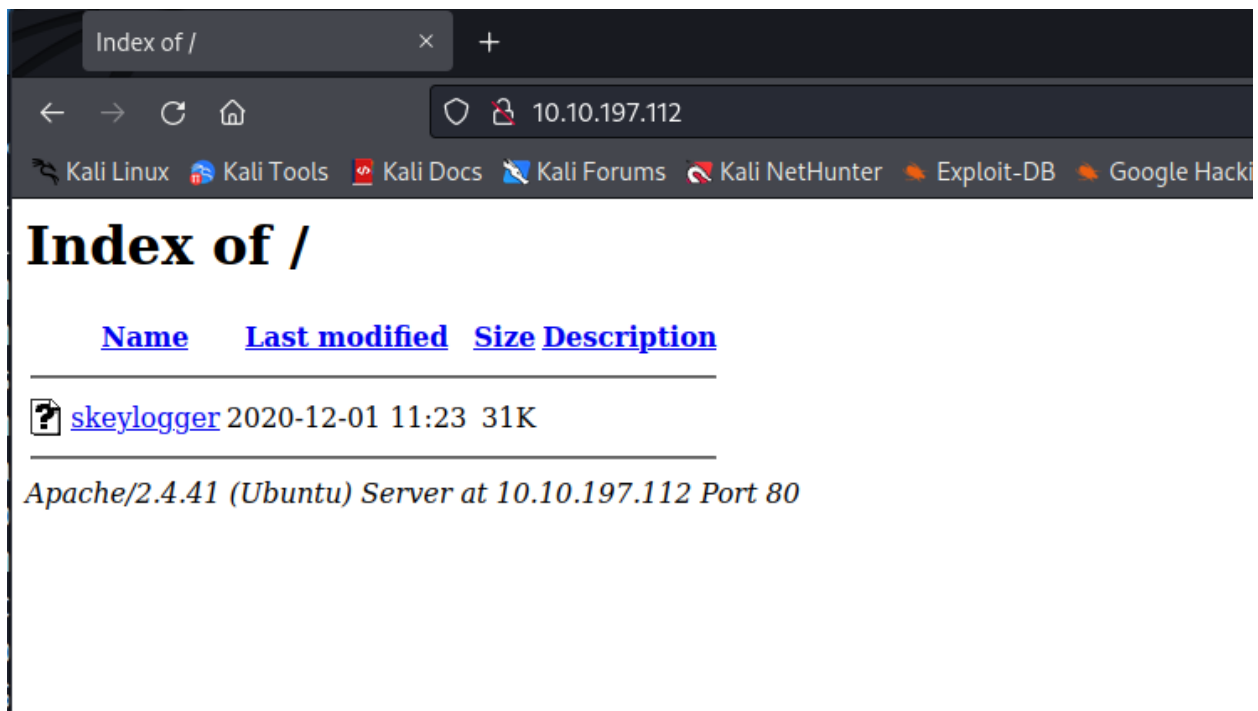


Figure 3 http page of the target

Looks like we a single file named **skeylogger**. We're going to download that and see what it's about.

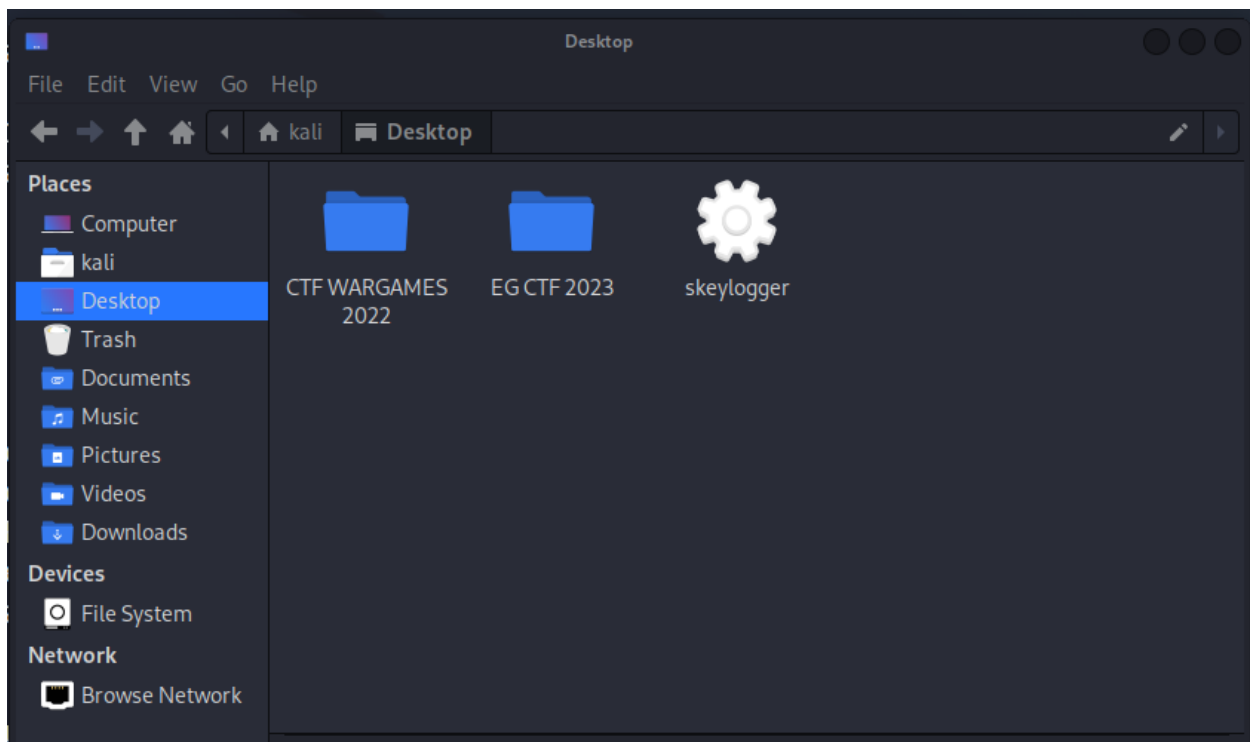


Figure 4 Unknown file

At a first glance it doesn't look like anything helpful, so I'm going to open it with a text editor.



Figure 5 Inside skeylogger

After opening it, the file is barely readable for the most part, except for the center. Apparently, it is some kind of a script or a program. To further analyze this, I'm going to use another tool called **cyberchef**.

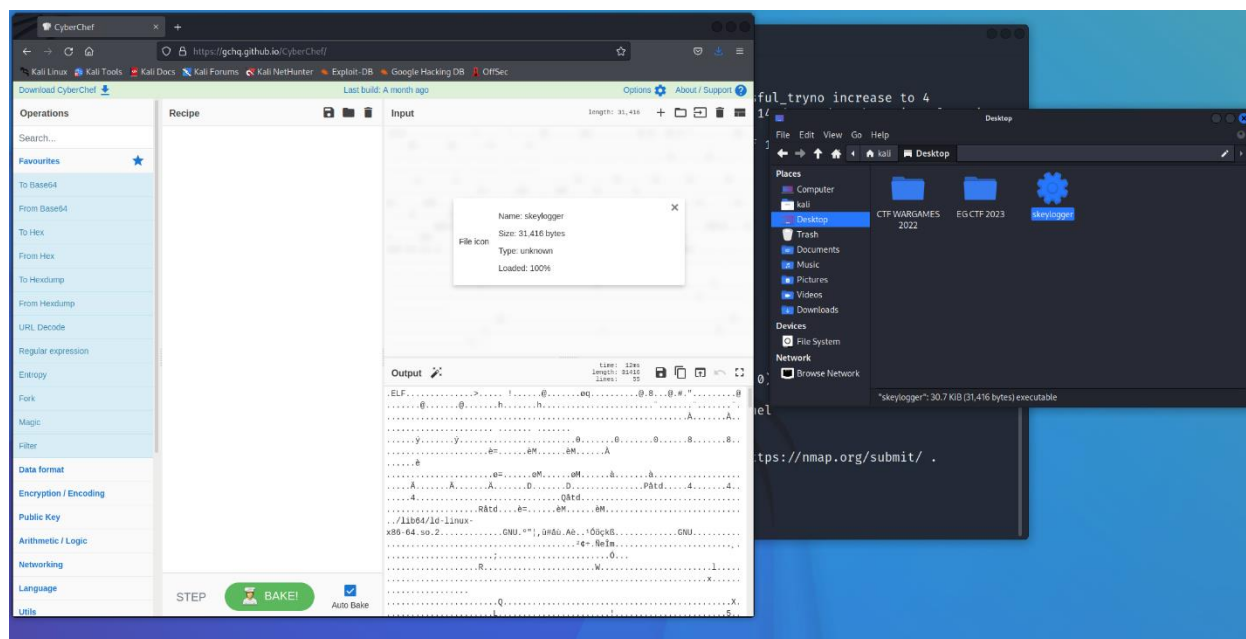


Figure 6 Using cyberchef

Then I would just drag the file into the input. The next step is to make the file readable and to do that we need to extract strings.

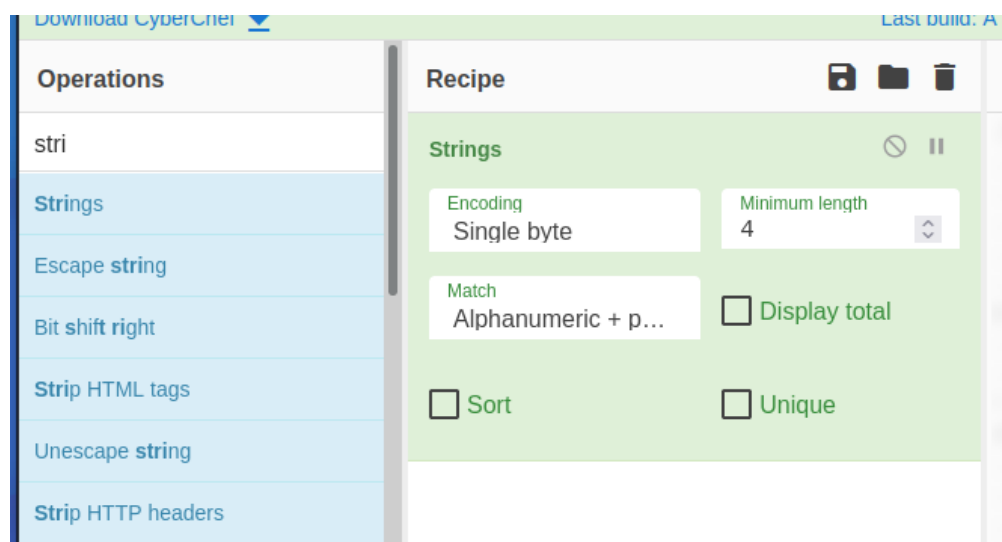
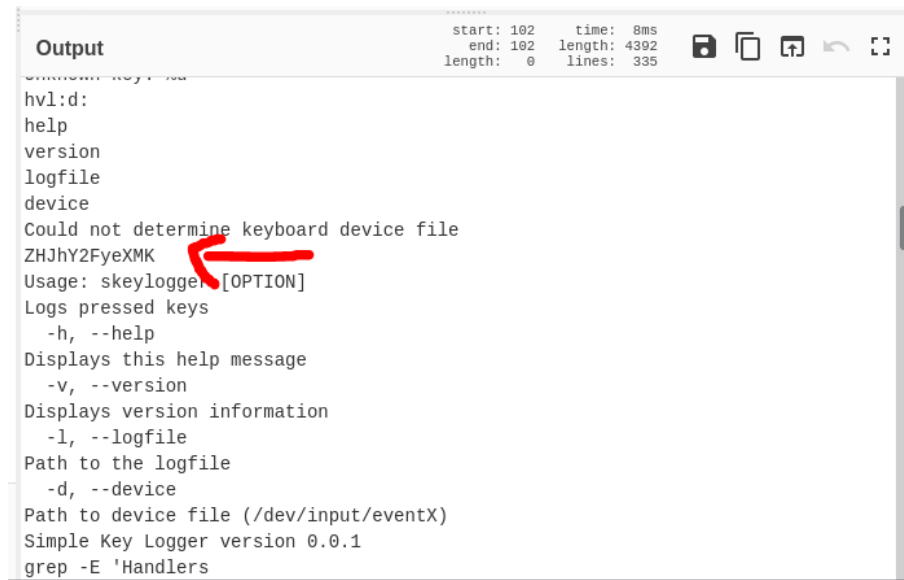


Figure 7 Extracting strings

After scrolling up and down through the output section we might have found something of a clue but it is encoded. So, we have to decode it first using base64.



```
Output
start: 102    time: 8ms
end: 102     length: 4392
length: 0    lines: 335

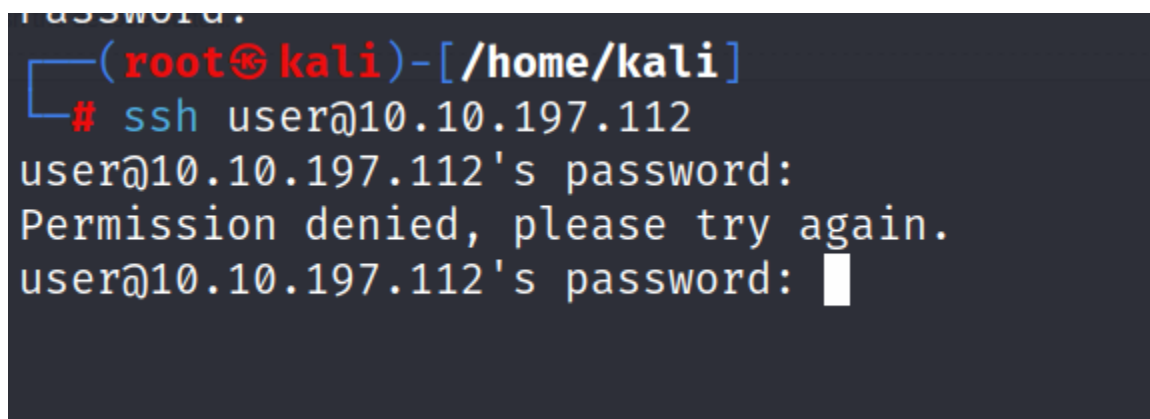
hvl:d:
help
version
logfile
device
Could not determine keyboard device file
ZHJhY2FyeXMK
Usage: skeylogger [OPTION]
Logs pressed keys
-h, --help
Displays this help message
-v, --version
Displays version information
-l, --logfile
Path to the logfile
-d, --device
Path to device file (/dev/input/eventX)
Simple Key Logger version 0.0.1
grep -E 'Handlers'
```

Figure 8 Potential clue?

Decode it and we have:

“dracarys”

So, we have some kind of a name. But now the question arise, is it the username? Is it the password? Well, we have to find out. Let's try it as a password.



```

(root@kali)-[/home/kali]
# ssh user@10.10.197.112
user@10.10.197.112's password:
Permission denied, please try again.
user@10.10.197.112's password: 
```

Figure 9 trying login

Well, this is expected. Since we don't have any real solid info about the machine credentials, but from the hint "username is not user" we can confirm that we already have the password and the username is something related to game of thrones character. Unfortunately, I have never saw any of the shows so I will conduct a google search to find the username.

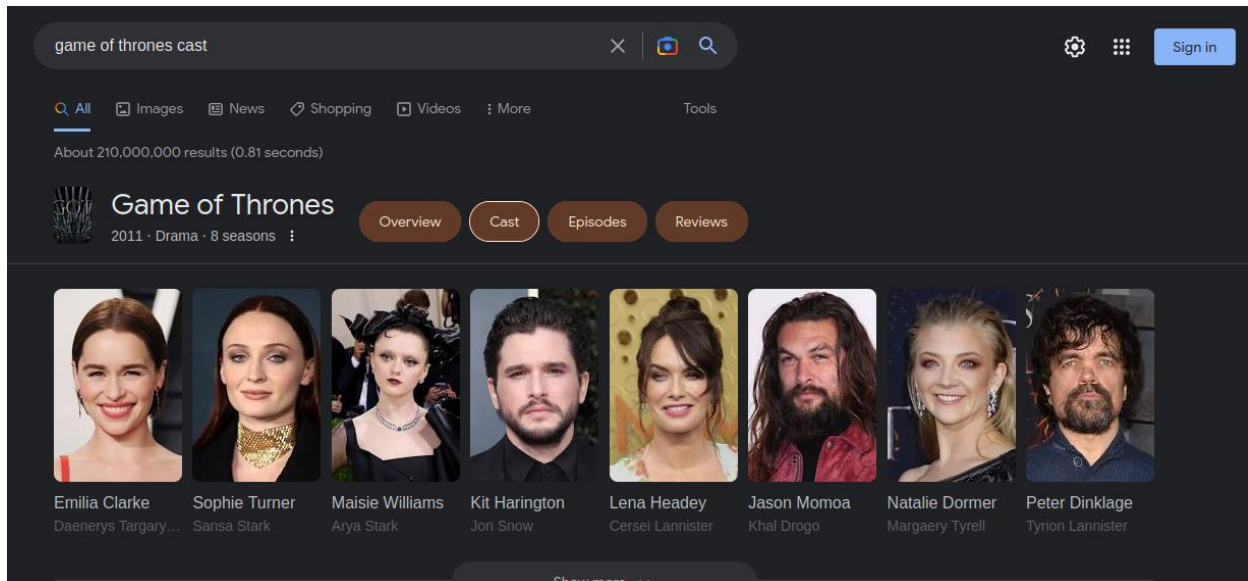


Figure 10 Google search result

After doing some google search, we have a list of the main actors. The only things that grab my attention is the main character named Daenerys played by Emilia Clarke so let's do that.

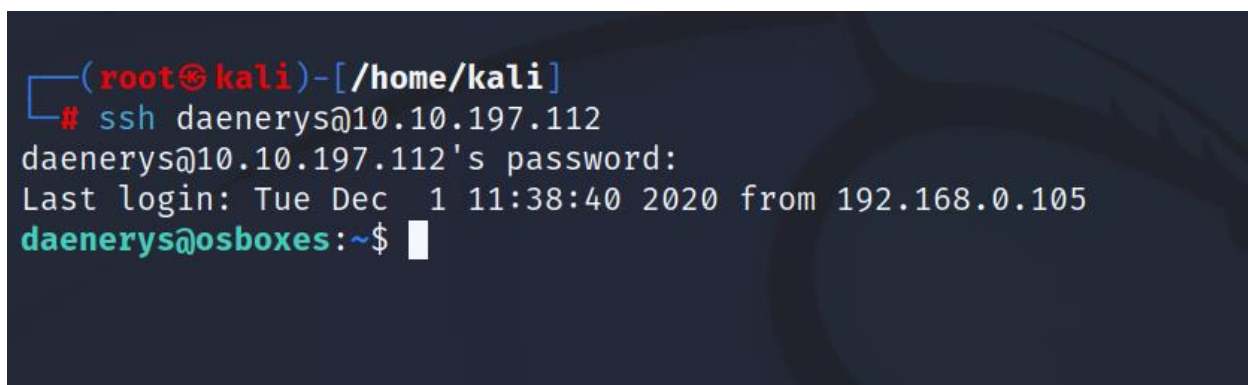


Figure 11 SSH success

We have successfully entered the machine by using **daenerys** as username and **dracarys** as password. Now we have to explore a bit to know more about the machine, but knowing the goal is to find the flag, so I entered the command

locate flag.txt

```
daenerys@osboxes:~$  
daenerys@osboxes:~$  
daenerys@osboxes:~$ locate flag.txt  
daenerys@osboxes:~$
```

Figure 12 Finding the flag

Looks like it didn't work out. So, we have to continue our investigation.

```
daenerys@osboxes:~$  
daenerys@osboxes:~$ ls  
Desktop Documents Downloads Music Pictures Public secret Templates Videos  
daenerys@osboxes:~$ file secret  
secret: ASCII text  
daenerys@osboxes:~$ cat secret  
  
find home, pls  
daenerys@osboxes:~$
```

Figure 13 secret.txt

Above figure shows that we have a text file called secret. However, I didn't find it helpful at all so I entered the following command to view hidden files.

ls -a


```

daenerys@osboxes:~$ ls -a
.          .config    .gtkrc-2.0  Pictures   .vboxclient-clipboard.pid  .xsession-errors
..         Desktop  .gtkrc-xfce .profile   .vboxclient-draganddrop.pid .xsession-errors.old
.bash_history .dmrc     .ICEauthority Public      .vboxclient-seamless.pid
.bash_logout Documents .linuxmint secret      Videos
.bashrc      Downloads .local      .ssh       .Xauthority
.cache       .gnupg    Music       .ssh       .xinputrc
Templates
daenerys@osboxes:~$

```

Figure 14 Hidden file revealed

Now we know all the hidden files. From here things going to get interesting, especially 1 particular file named **.bash_history**. Let's further our investigation by viewing the said file.

```

daenerys@osboxes: ~
File Actions Edit View Help
cd .local
ls
cd share
ls
cd /home
cd daenerys/
find / -username daenerys 2>&1 ~ grep zip
find / -user daenerys 2>&1 ~ grep zip
find / -user /home/daenerys 2>&1 ~ grep zip
find / -user /home/daenerys 2>&1 | grep zip
find / -user daenerys 2>&1 | grep zip
ls
cd /home/daenerys/.local/share/
ls
unzip daenerys.zip
file djkdskjdsn
cat djkdskjdsn
sudo su
ls
rm djkdskjdsn
clear
cd /home/daenerys/
clear
ls
sudo su
su root
ipconfig
ifconfig
exit
ifconfig

```

Figure 15 bash_history

From the figure 16, there is so much information that we can make out. Mainly the zip file named **daenerys.zip** that is located in directory **/home/daenerys/.local/share/**. I would say that's our temporary goal for now. Besides that, it seems like in the zip file there's a file named **djkdsnkjdsn**. Pretty sure that is going to be our next clue.

Now, what we need to do now is to go the directory where **daenerys.zip** file exist and unzipped it.

```
daenerys@osboxes:~$ cd .local
daenerys@osboxes:~/.local$ ls
share
daenerys@osboxes:~/.local$ cd share
daenerys@osboxes:~/.local/share$ ls
daenerys.zip  evolution  flatpak  gnote  nano  recently-used.xbel
daenerys@osboxes:~/.local/share$ ls -a
.  ..  daenerys.zip  evolution  flatpak  gnote  nano  recently-used.xbel
daenerys@osboxes:~/.local/share$ unzip daenerys
Archive:  daenerys.zip
  extracting: djkdskjdsn
daenerys@osboxes:~/.local/share$
```

Figure 16 daenerys.zip

```
daenerys@osboxes:~/.local/share$ ls
daenerys.zip  djkdskjdsn  evolution  flatpak  gnote  nano  recently-used.xbel
daenerys@osboxes:~/.local/share$ file djkdskjdsn
djkdskjdsn: ASCII text
daenerys@osboxes:~/.local/share$ cat djkdskjdsn
/usr/share/sounds/note.txt
daenerys@osboxes:~/.local/share$
```

Figure 17 Another potential clue

Looks like we have another clue. Another directory, with a text file. Hoping we are getting close to the flag.

```
daenerys@osboxes:~/.local/share$ cd /usr/share/sounds
daenerys@osboxes:/usr/share/sounds$ ls
alsa          LinuxMint      linuxmint-login.wav  note.txt
freedesktop   linuxmint-gdm.wav  linuxmint-logout.wav  speech-dispatcher
daenerys@osboxes:/usr/share/sounds$ cat note.txt
I'm khal.....
daenerys@osboxes:/usr/share/sounds$
```

Figure 18 note.txt

In the **note.txt** file, we have some kind of a name. Knowing the challenge thus far, this clue must be related to Game of Thrones series. So, now we are going to do another google search.

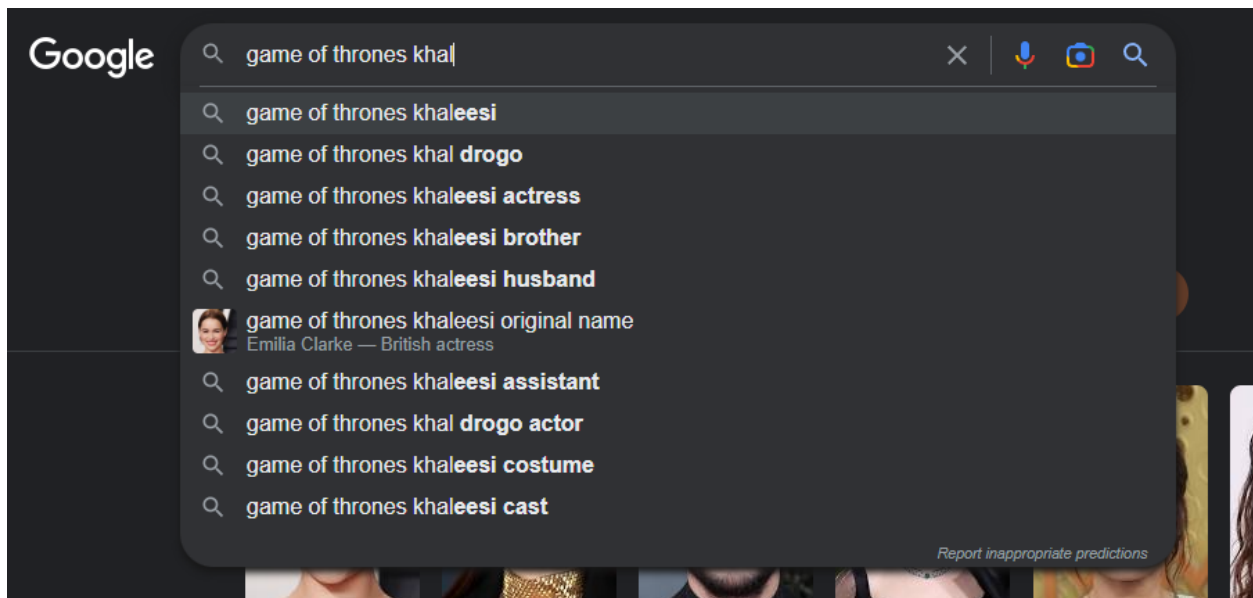


Figure 19 Naming research

Google search result shows we have 2 name that potentially could be the password for our root access.

-khaleesi

-khal drogo

However when taking a closer look at the **note.txt** earlier, "**I'm khal. . . .**", the 5 dots probably an indicator for 5 alphabets. Therefore, our best option would be using **khaldrogo** as our root password.

If this succeed then we just have to access our root folder.

```
daenerys@osboxes: /usr/share/sounds$  
daenerys@osboxes: /usr/share/sounds$ su  
Password:  
su: Authentication failure  
daenerys@osboxes: /usr/share/sounds$ su  
Password:  
root@osboxes: /usr/share/sounds# cd /home  
root@osboxes: /home# ls  
daenerys  
root@osboxes: /home# cd ..  
root@osboxes: /# ls  
bin    cdrom  etc    lib    lost+found  mnt  proc  run  srv  tmp  var  
boot  dev   home  lib64  media      opt  root  sbin sys  usr  
root@osboxes: /# cd root  
root@osboxes: ~# ls  
root.txt  
root@osboxes: ~# cat root.txt  
RUd7VEgxU18xNV9CNFMxQ19CMnJfTUBDSDFOM180U1VSMYF9  
root@osboxes: ~#
```

Figure 20 gained root access

We made it! We have gained root access of our machine and we also have the content to our **root.txt**. Just need a little bit of decoding.

Decode from Base64 format


Simply enter your data then push the decode button.

```
RUd7VEgxU18xNV9CNFMxQ19CMnJtTUBDSDFOM180U1VSMYf9
```

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8  Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

 Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

 **DECODE**  Decodes your data into the area below.

```
EG{TH1S_15_B4S1C_B2r_M@CH1N3_4SUR3!}
```

Figure 21 decoded flag

FLAG OBTAINED! CHALLENGE COMPLETED.