**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/**](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 have 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.**

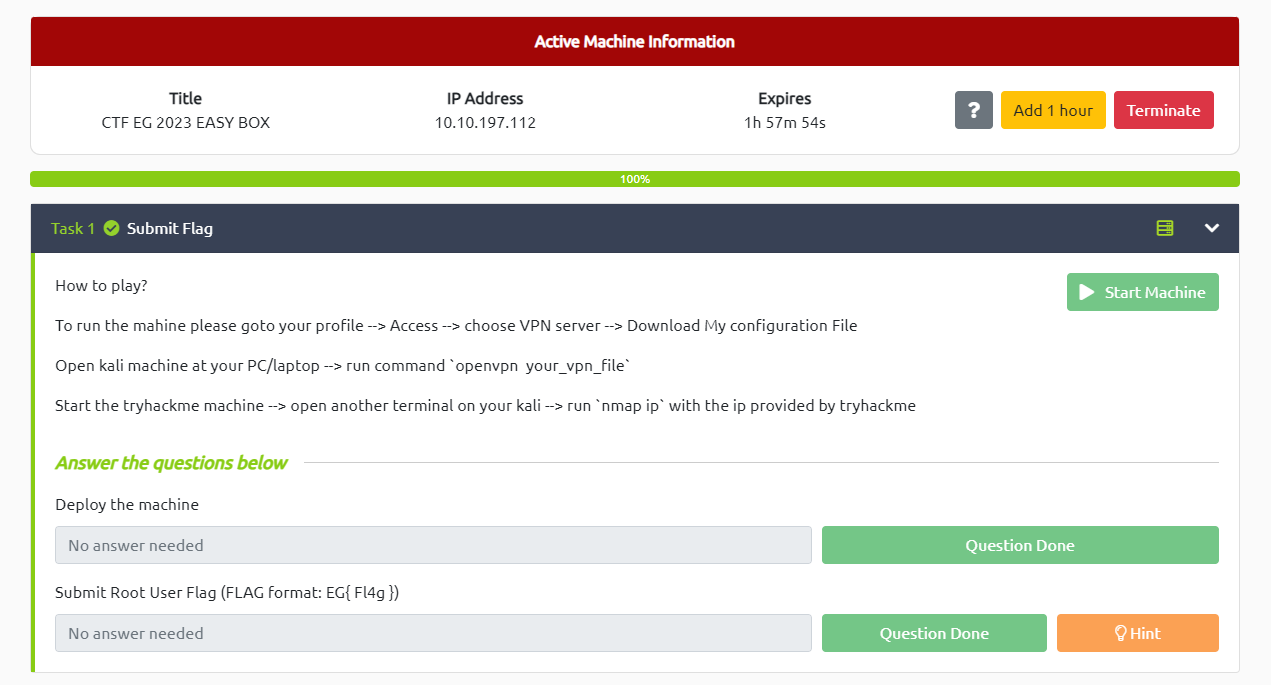


Figure Starting the target machine

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

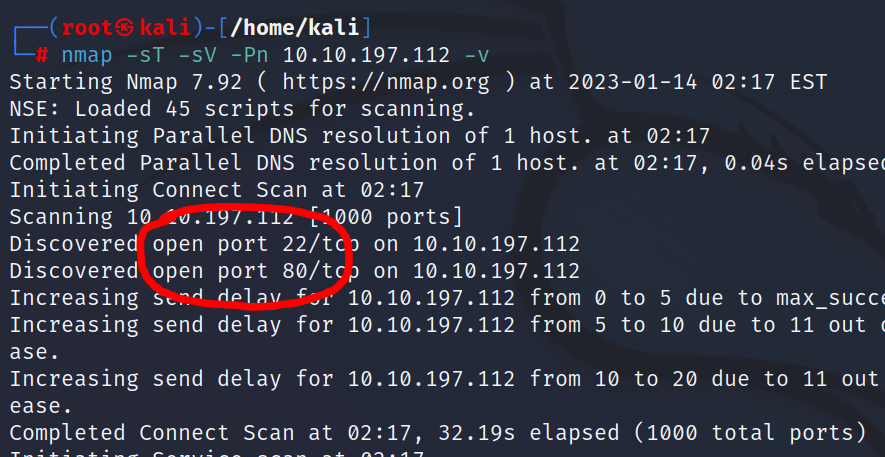


Figure Nmap scan result

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.

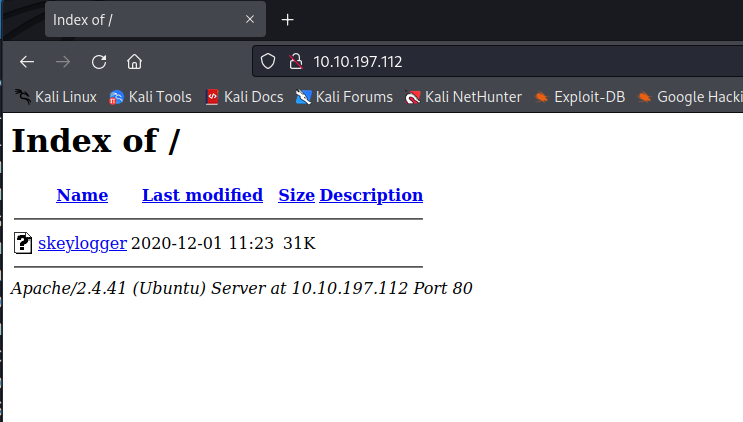


Figure http page of the target

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

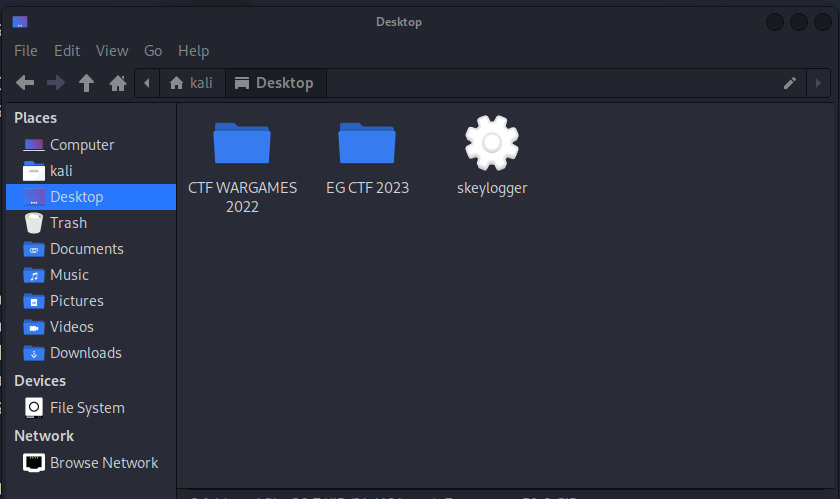


Figure Unknown file

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

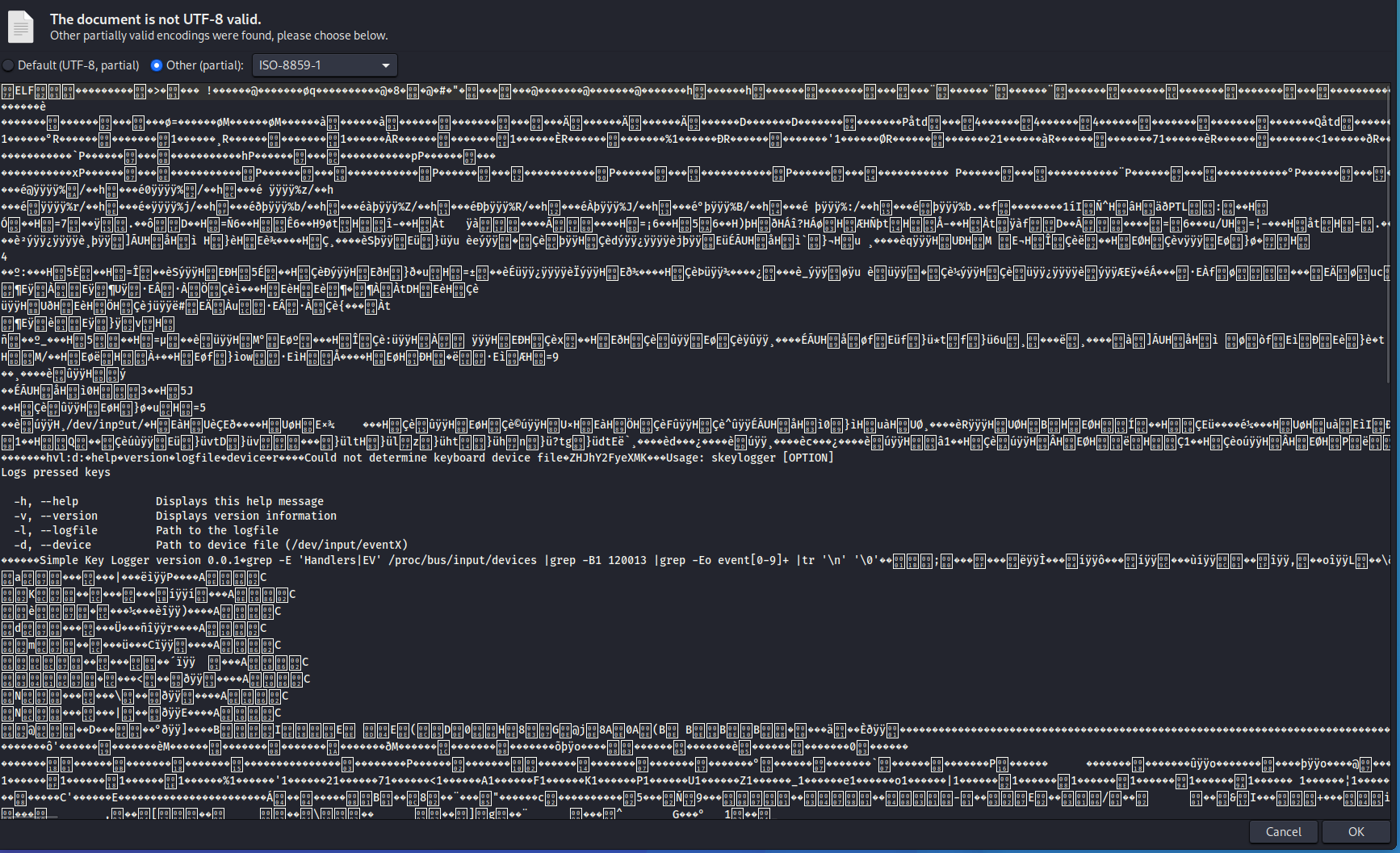


Figure Inside skeylogger

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***.

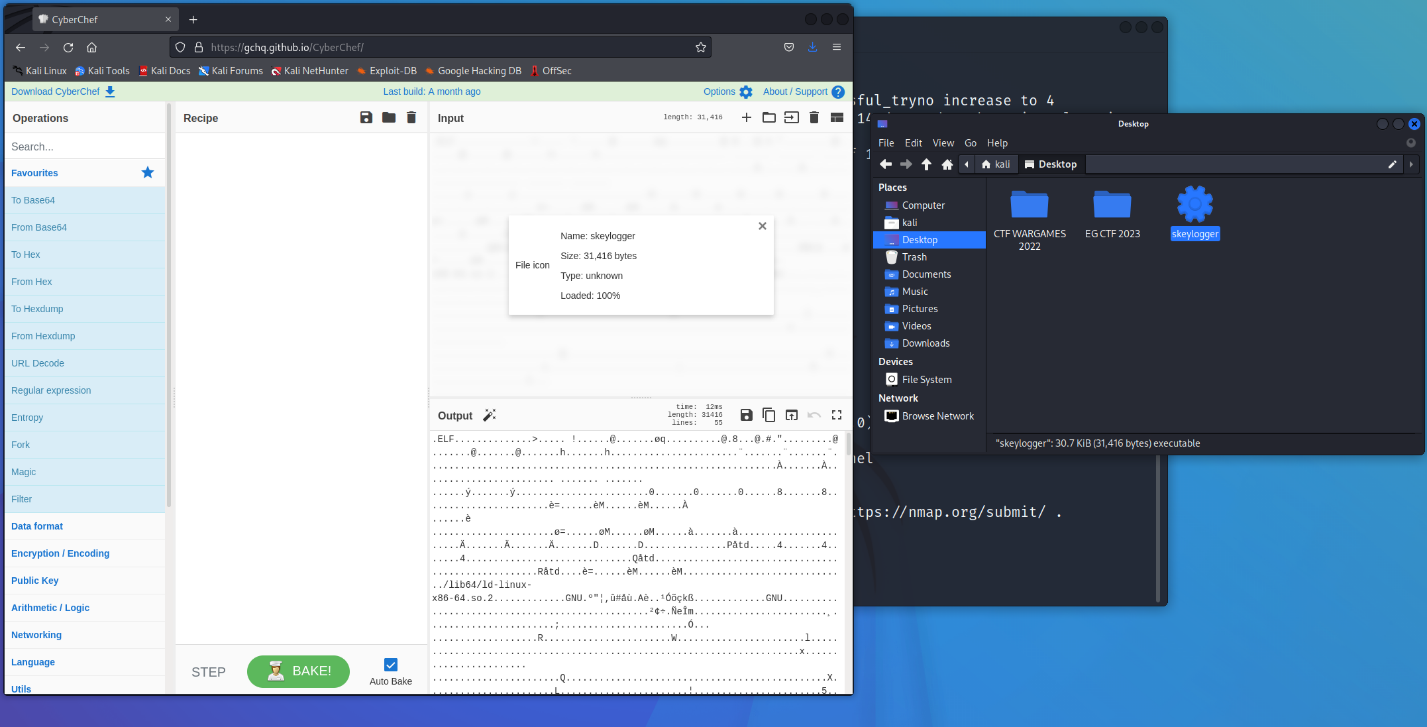


Figure Using cyberchef

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.

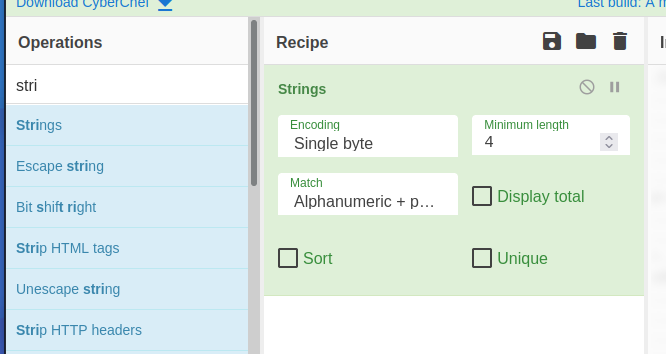


Figure Extracting strings

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.

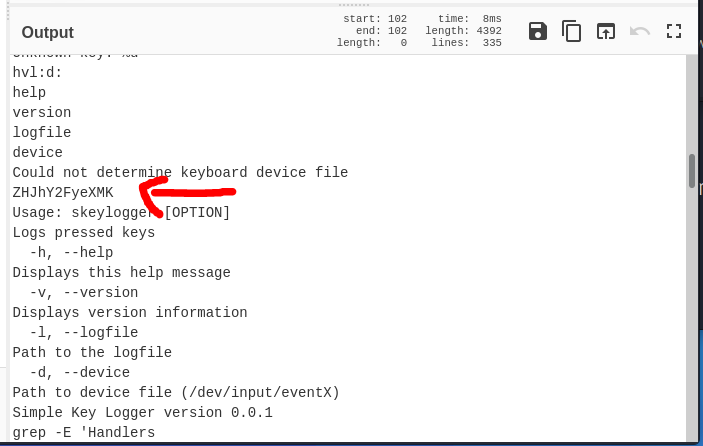


Figure Potential clue?

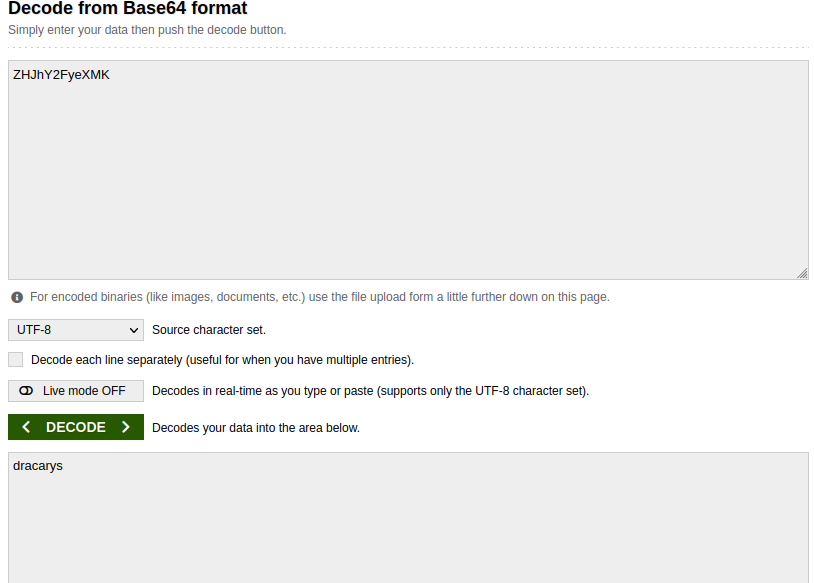


Figure Decoded clue

Nice! 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.

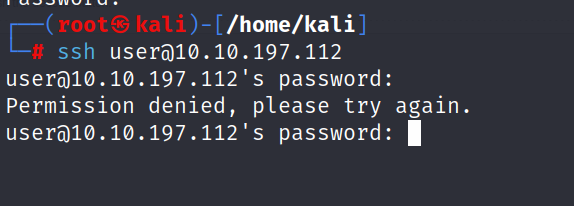


Figure trying login

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 confirmed 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.

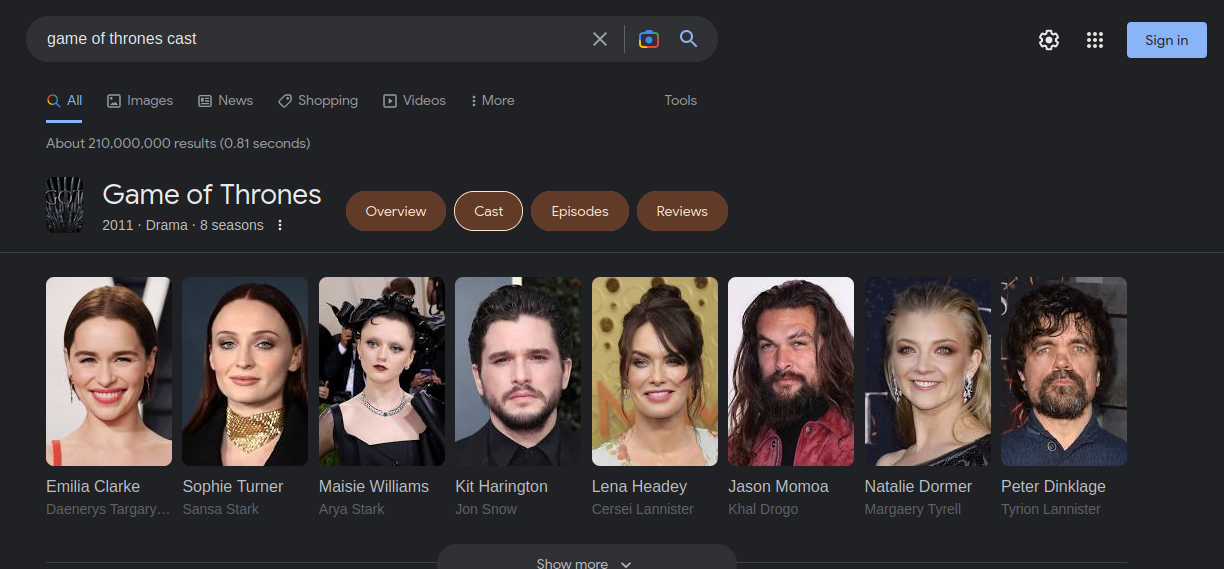


Figure Google search result

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.

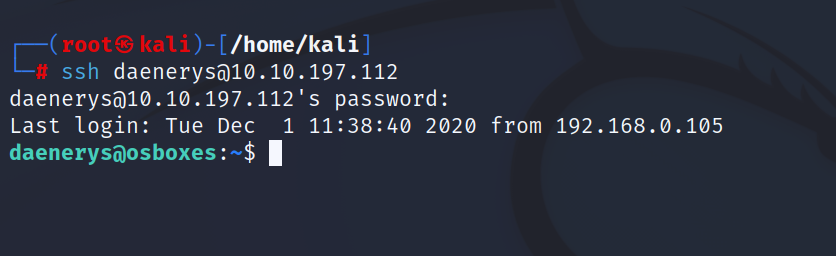


Figure SSH success

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*

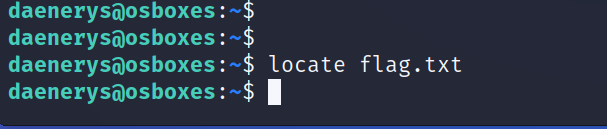
**

Figure Finding the flag

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

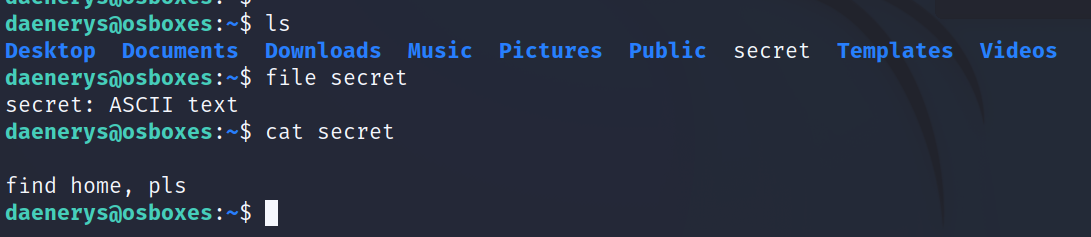


Figure secret.txt

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*

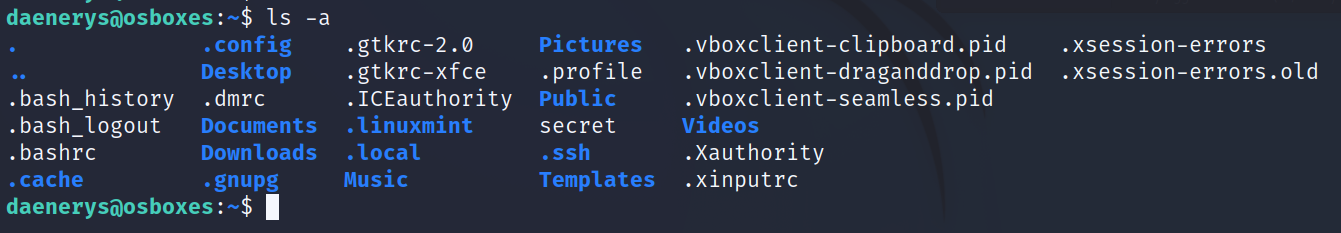
**

Figure 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.

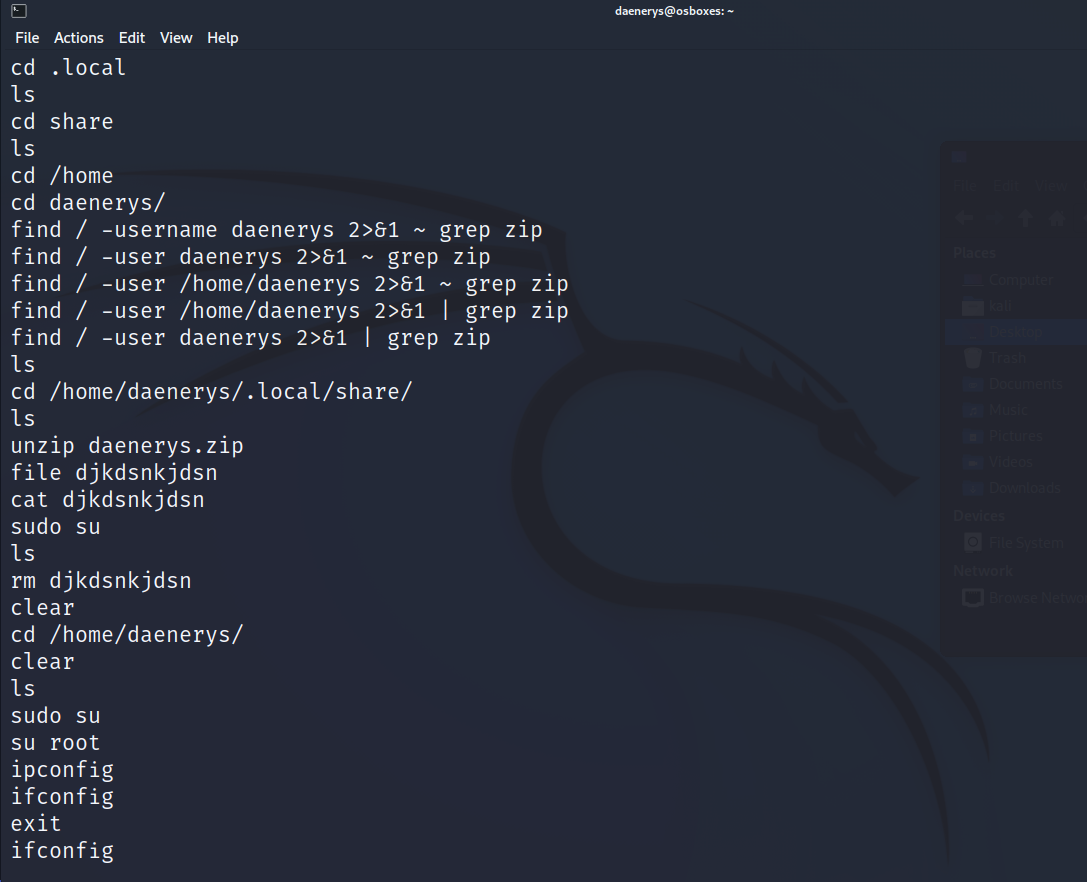


Figure bash\_history

From the above figure, 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.

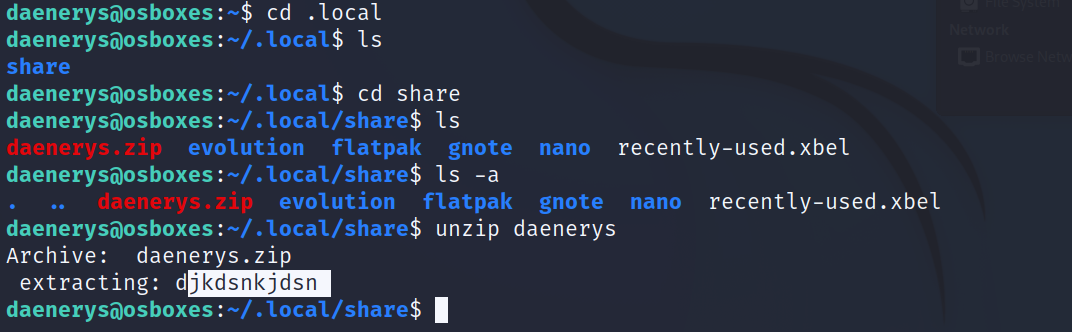


Figure daenerys.zip

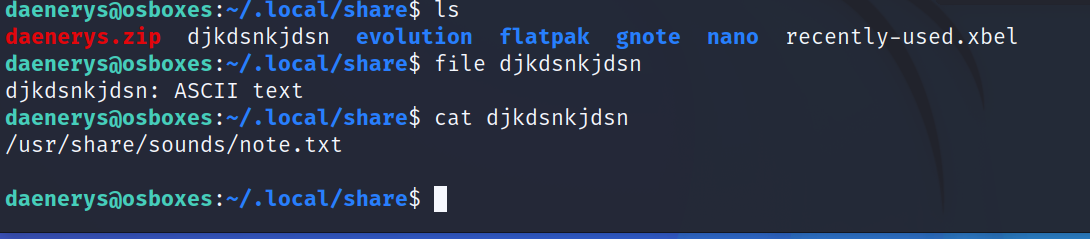


Figure Another potential clue

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

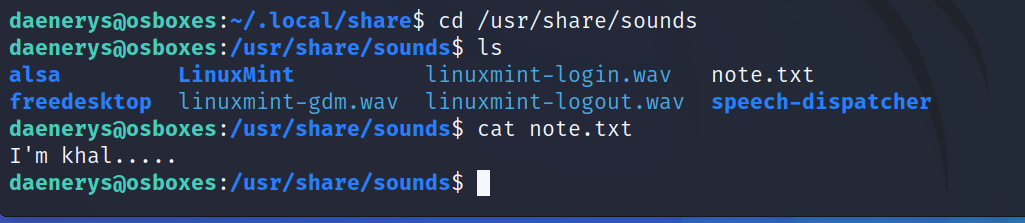


Figure note.txt

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.

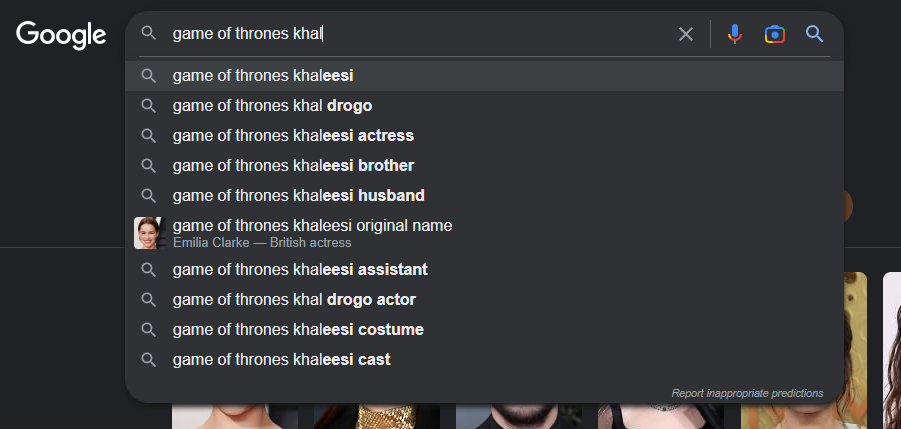


Figure Naming research

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.

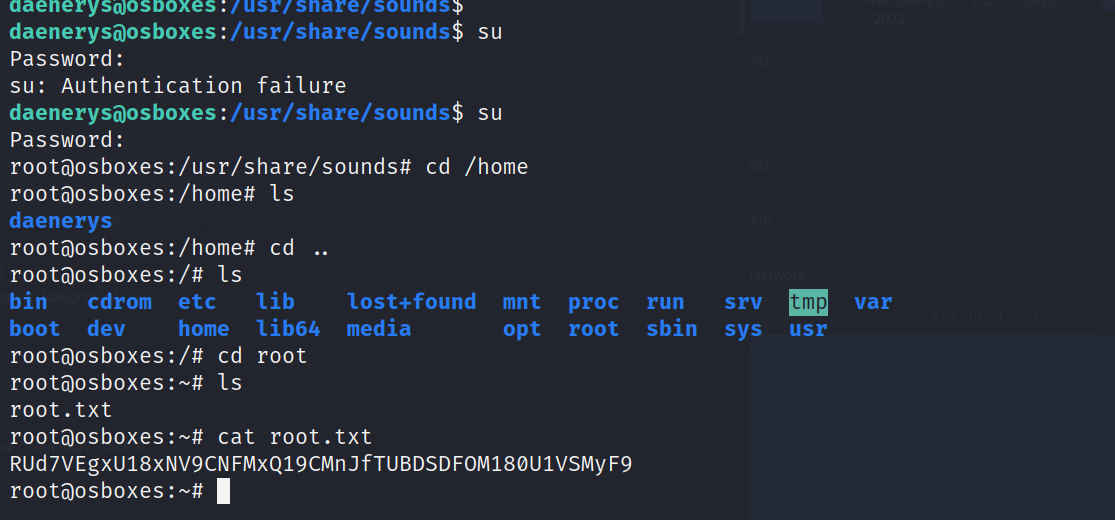


Figure gained root access

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.

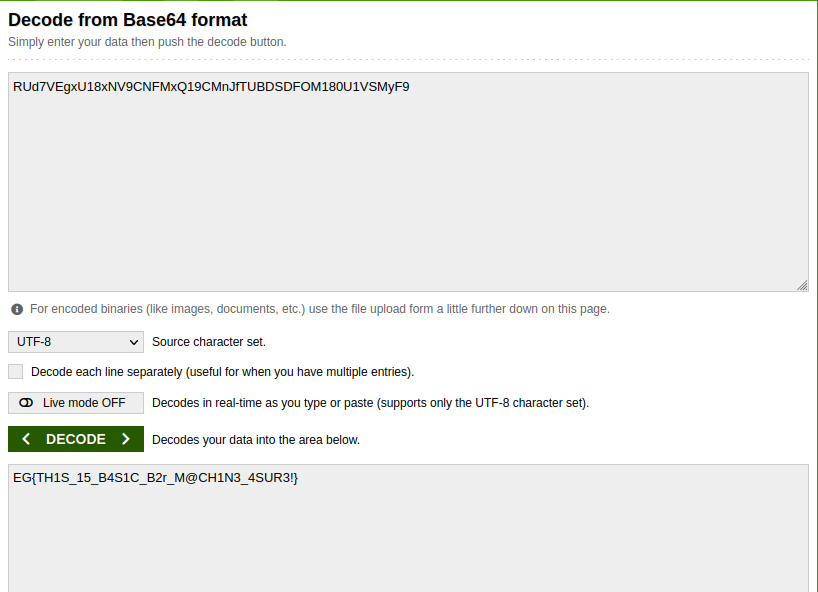


Figure decoded flag

FLAG OBTAINED! CHALLENGE COMPLETED.