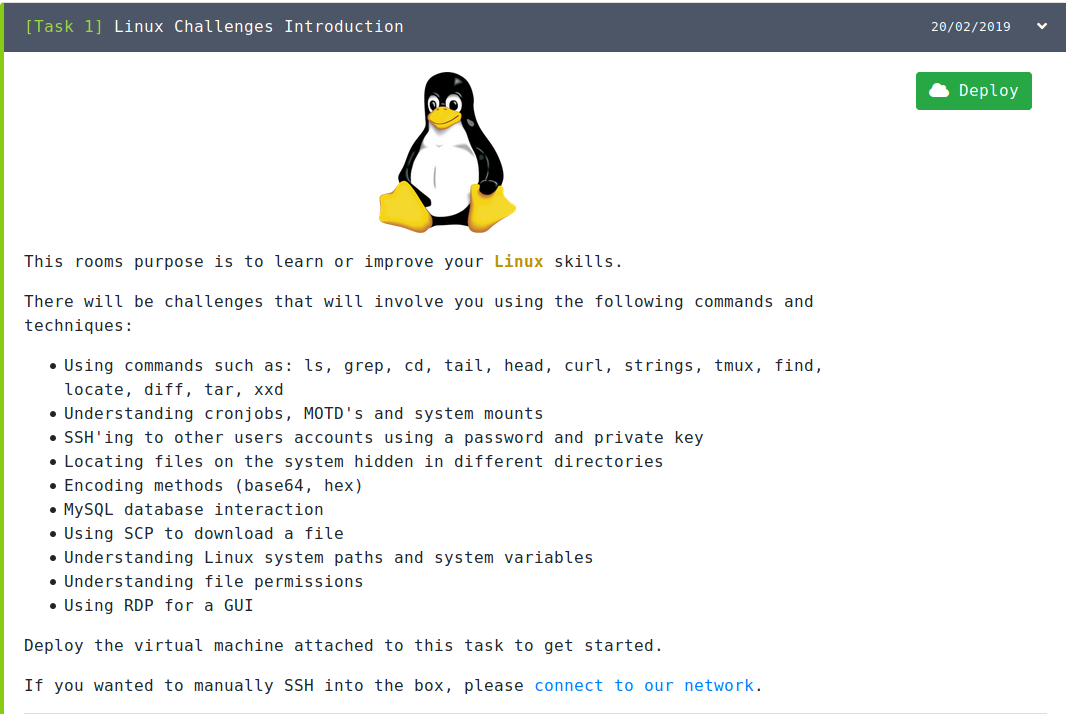
Introduction:

Hello and welcome to the tryhackme Linux CTF. This is my first CTF on tryhackme and I found it to be very enjoyable. I hope you explore other CTF on tryhackme as I will completing more and uploading them to my GitHub.

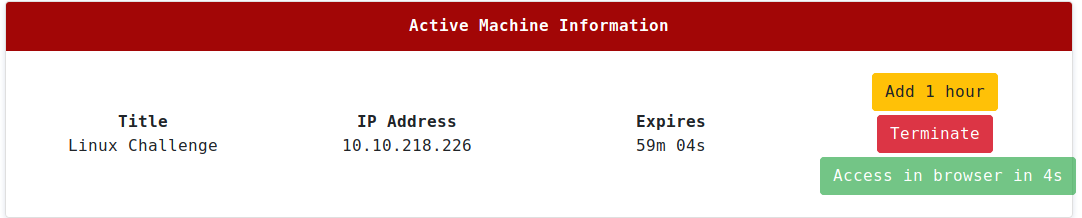
Machine Set-up:

I am running a Kali Linux machine and accessing the via OpenVPN so I do not have to use the environment I am used to. Tryhackme.com can provide further details on how to connect to their network via ssh.

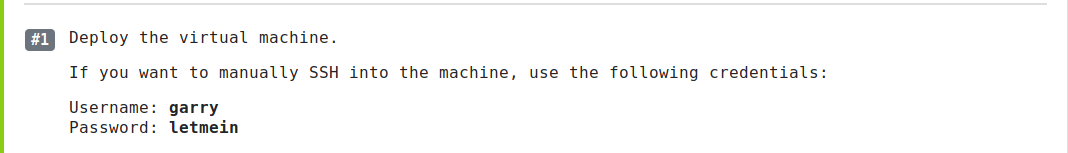
**Task 1:**



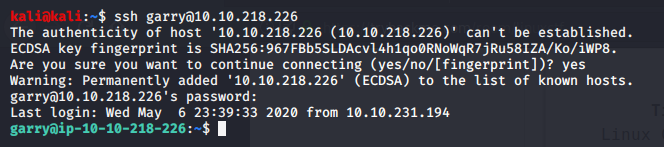
Here we find the introduction to the CTF and the challenges and techniques it will cover. In the top right corner, we see the deployed machine. Let's go ahead and deploy the machine and set up via ssh and OpenVPN.



After we deploy the machine we are given the IP we need to launch our ssh shown in the box.

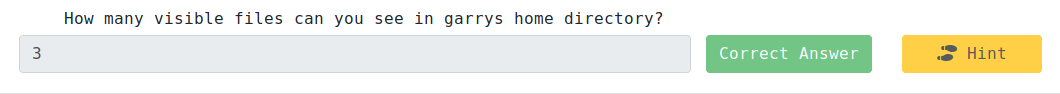


Before we connect to the network via ssh let look at the first task. It is asking us to ssh into the machine with the following credentials.

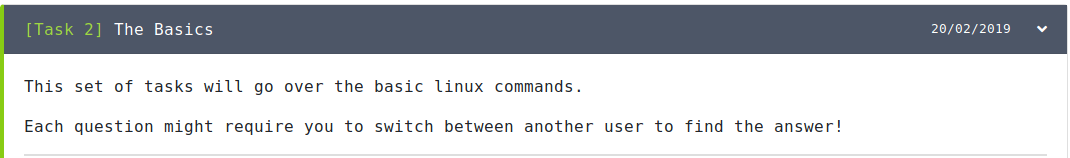


We have now logged into the machine with the login credentials that were given and can see that we are now the user garry.

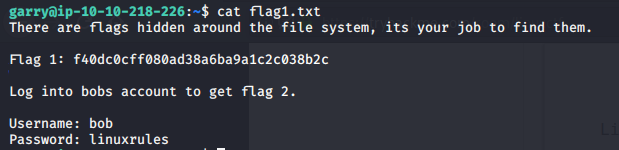
In this task, we need to list all the files in garrys home directory. This can be done using the ls command.



**Task 2:**



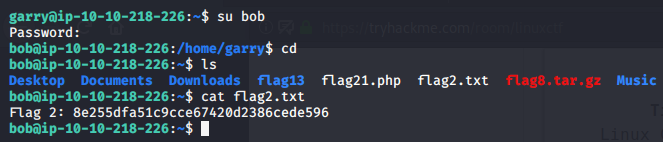
In this task, we cover basic Linux commands. I have some experience working in Linux from my past semester so this was not too hard to complete but cool to see how we get to each flag. I also completed this section before starting the write-up.

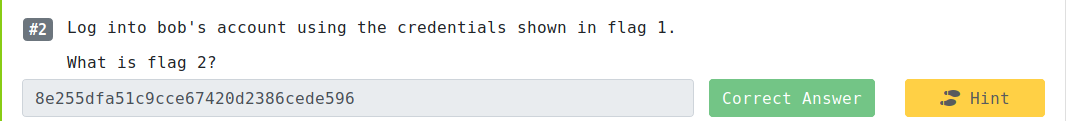




This once was easy but that’s what we excepted considering it is the first flag we need to find. I cat the flag1.txt file and we can see that the flag came up and instructions for the next flag appeared.

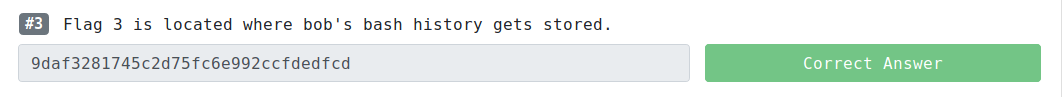
For #2 we log into bobs account and go to his home directory. Then using ls we see that there is a flag2.txt file. We cat the flag2.txt file and are given the second flag.



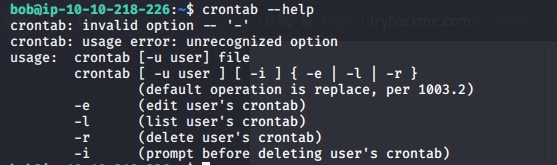


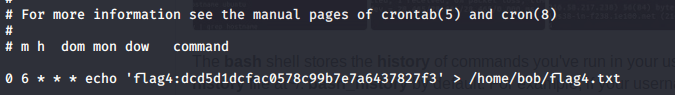
To find this flag we needed to extract info about the bash history. This can be found in the *.bash\_history*  file. So again I just used the cat command to extract the data. The flag was the first line in the bash history.

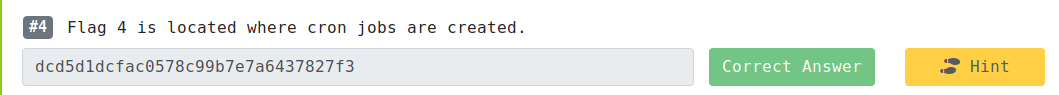


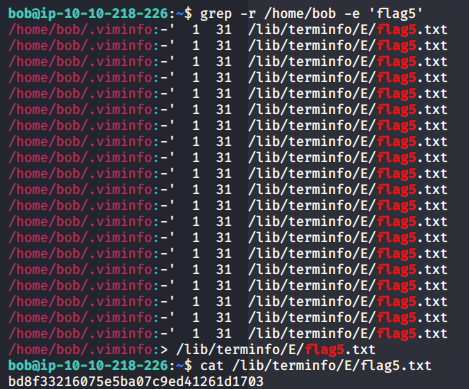


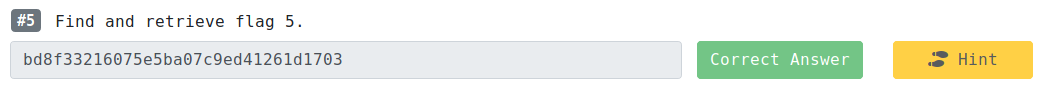
In this task, we need to find where cron jobs are created. I used the hint to give me some direction as to where to start. It prompted crontabs. Again I did not know what crontabs were so I looked at the manual on how to use them. I then used the command crontab -e to look at the user’s crontab file. Sure enough flag four was at the bottom.



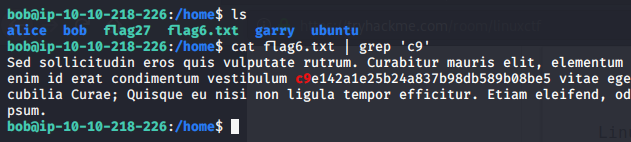


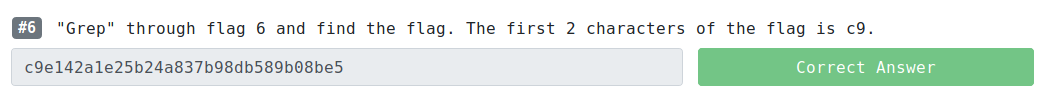


For this flag, we needed to search all the directories in /home/bob to find the directory that holds falg5.txt. I used grep -r /home/bob -e ‘flag5’ as my command specifying this needs to be recursive(-r) and we need to search for all patterns ‘flag5’ (-e). This outputted all the files that contain ‘flag5’. We can then see the file using the cat command.

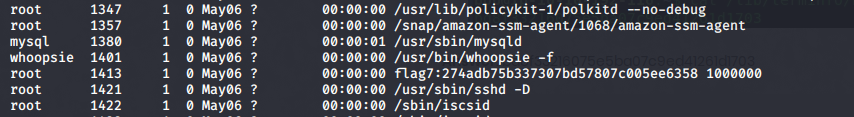


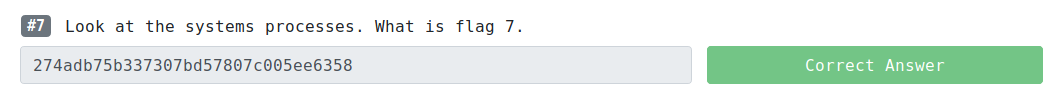
To find flag 6 it was much easier than the last flag we needed to find. I first went to Bob's home directory and listed all the files. Flag6.txt was already in there so I used the cat command combined with grep to get the exact location of the flag.



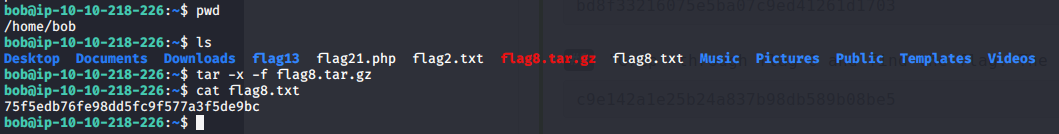


For flag 7 we needed to look at the processes that were running on this machine. Using the ps command is the best way to do this. I first looked at the ps manual and saw that to list every running process you use the command *ps -ef.* I used this command and was able to find flag7 in the mix of all the processes.



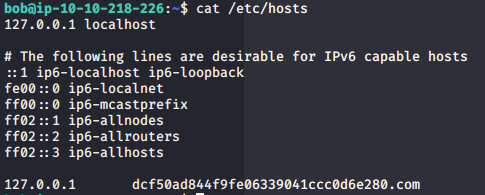


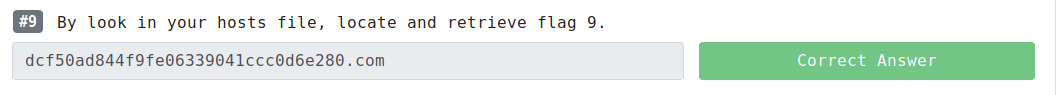
To get flag 8 all we needed to do was extract it from the flag8.tar.gz file. To do this I remembered this was in bobs directory so I used the command tar -x (for extraction) -f (use archive file) flag8.tar.gz. This extracted all the data and we can then use the cat command on flag8.txt.qw





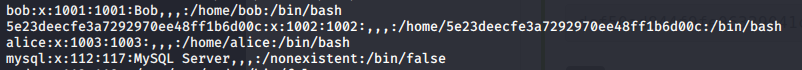
Flag 9 was quite simple as well I just used the cat command to extract all the contents of the /etc/hosts file. Instantly I saw the flag.

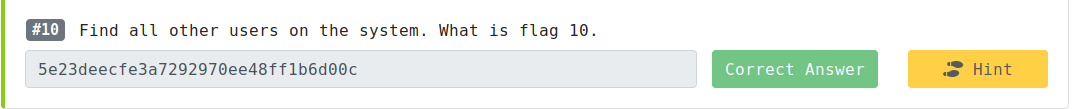




This was fairly simple as well. I know that users are stored in the passwd file so I used the command

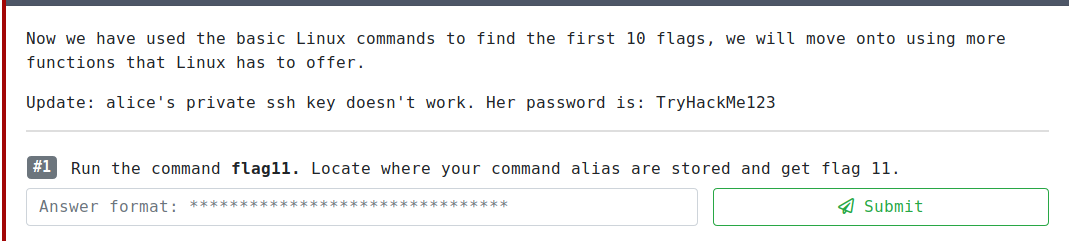
cat /etc/passwd. I then was given all the users and in the middle was the flag!!





**Task 3: Linux Functionality**

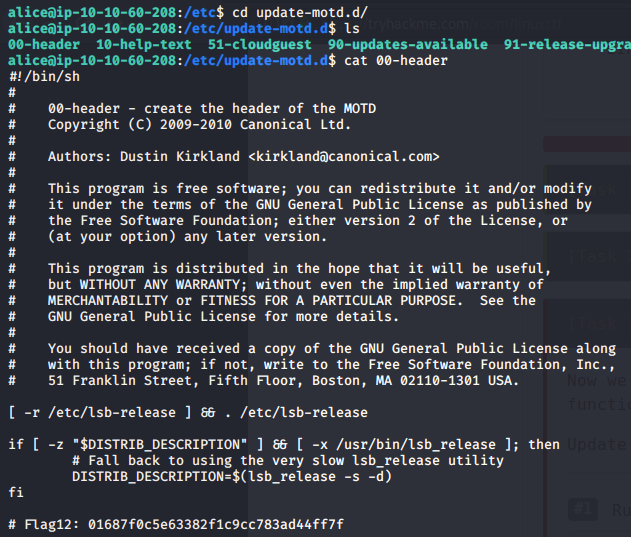
YAY!! We completed our first real section of looking and finding flags using Linux commands! Now we are going to move into different functionalities Linux has to offer.

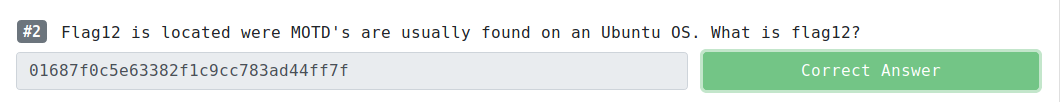
****

To get this flag I had to find where the command alias is stored. After some research, I found that typically they are stored in the .bashrc file for ubuntu. I then logged into Alice's account and went to the ubuntu directory. I then used the command *cat .bashrc*  and we were able to find flag11.

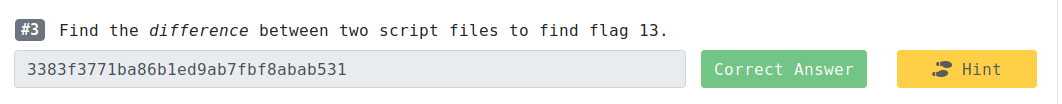
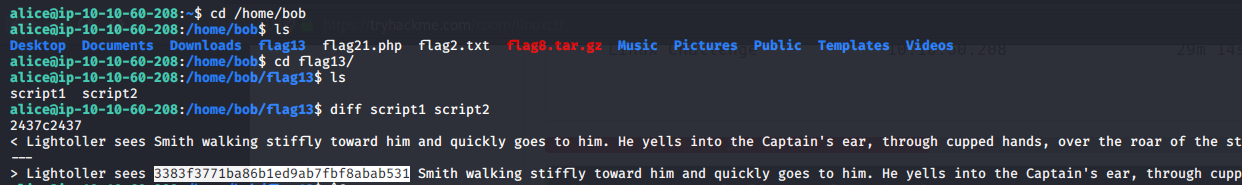


To locate flag 12 also need some research. I found that motd is dynamic now in ubuntu OS systems so I had to find the update.motd.d folder which was inside of /etc. I then navigated to the 00-header file and used cat to see the contents. Sure enough, there was flag12.

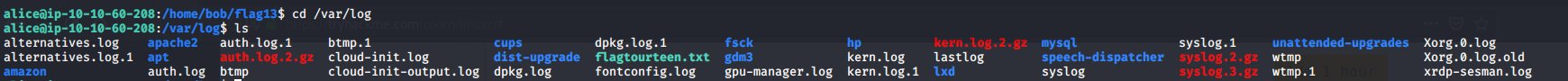


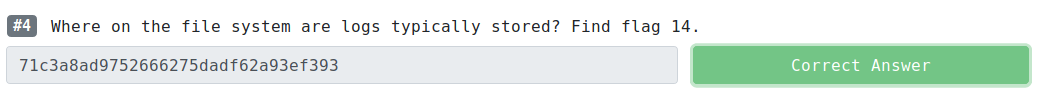


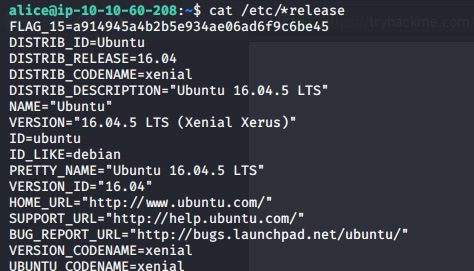
This flag was easy as we already know where the flag13 directory is. I then used the diff command and was able to see the difference between both scripts and get the flag.

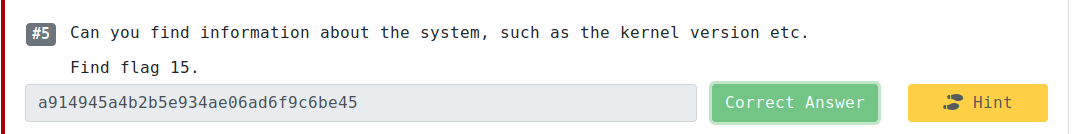


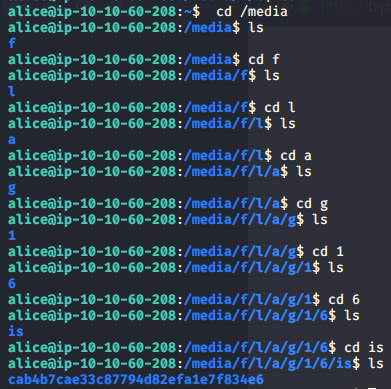
For flag14 all I did was go to the directory that logs are found in */var/log.* Inside there was the flag14 text file. I then used cat to look at the contents and the flag was at the very bottom.





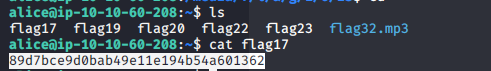
For flag 15 we just needed to find out the information the system. I wasn’t sure where I was going wrong using the uname command but then found it.

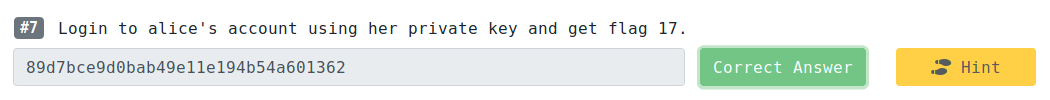




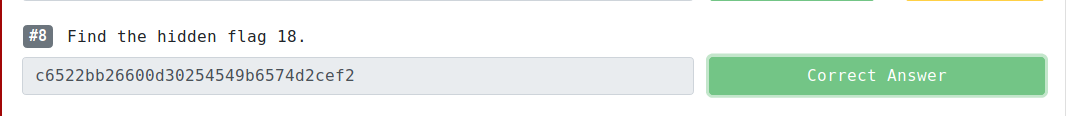
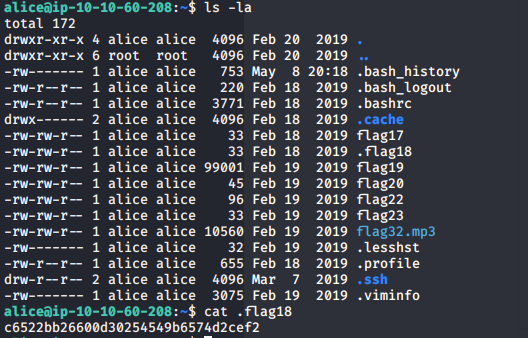


This one was quite hard for me to find as I wasn’t sure where to look for system mounts. I eventually found that mounted items are stored in the */media* folder and decided to look there. This led me through a bunch of directories that spelled out flag 16 and we were able to find the flag.

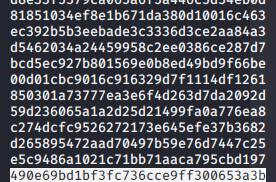


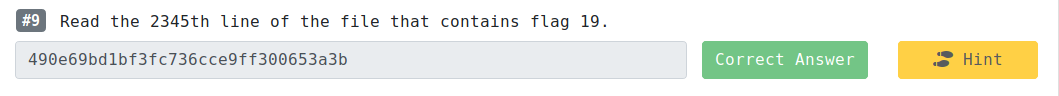


Flag 17 was easy. Since we were already logged into Alice's account and knew where flag 17 was I simply looked at the file and was able to find it.



This task was also simple. We used *ls -la*  to show all files in the current directory. This gave us the hidden file for flag 18.

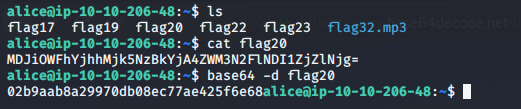




This was also simple as I used the command *head -n 2345 file19.* The -n is used to read lines instead of bytes which is -c. The last line outputted to screen was your flag!!

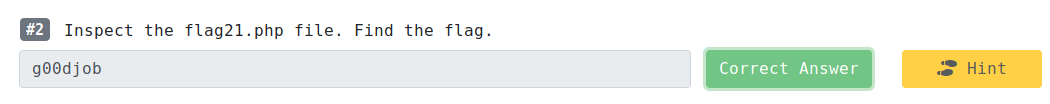
**Task 4: Data Representation, Strings, and Permissions**

Now we are moving onto the fourth task of the CTF learning about data representation, strings, and permissions. Now since we are still logged into Alice's account we can find flag20 fairly easily. Finding the contents of the flag was kinda weird. When we used the cat command you can see that this is not the flag. I then used the hint and it said “*base64”*. I then figured I could use the base64 command to decrypt the message.

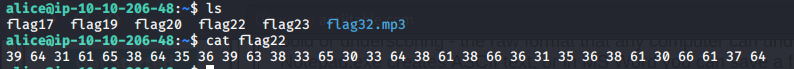


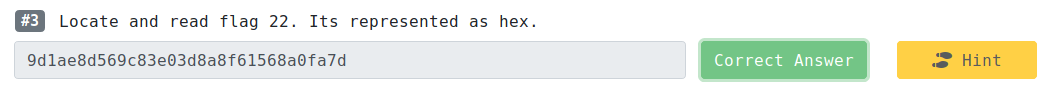


Flag 21 was simple as well as we just opened flag 21 in vim to see all the code of the PHP file. I was also surprised to see that this flag was very short.

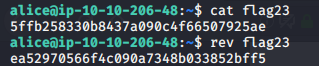


For this flag, I brute-forced the answer, which was just a long and tedious process. We were given the hex values for the flag. I then looked at an ASCII table so I could translate it to the flag.





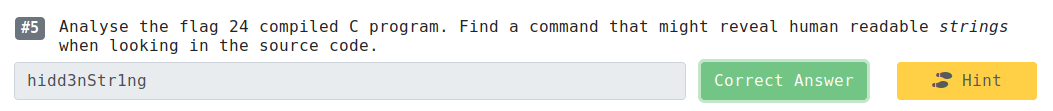
Flag 23 was also simple as I just reversed the string that was used for flag23.





For this flag, I used the strings command to print out all the readable strings in the flag24 executable. This printed out a bunch of information so I then used the grep command to search for ‘flag’ to get a better search.

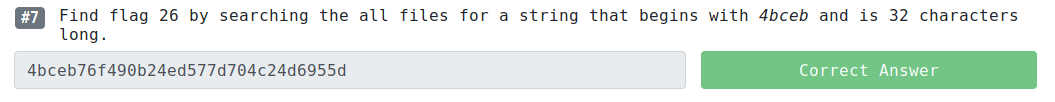




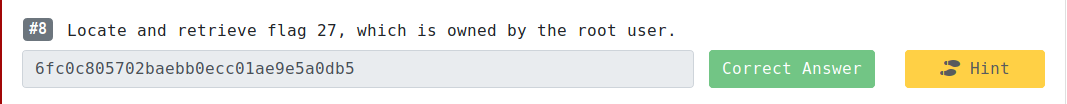
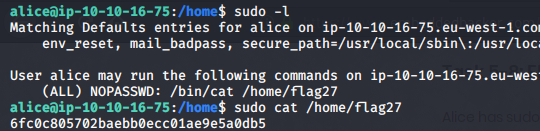
There was no flag 25 ☹

I was able to find this flag after one-two hours of research on the different command-line syntax to use but we ended up finding it in the /var directory.





For this flag, it was super simple. We can use the command *sudo -l*  to see all the files that sudo can access without a password. We can see that we don’t need a password for flag27 so we run *sudo cat /home/flag27*  and are given the flag.



Using the uname command with the -r parameter allows us to get the kernel release version. I also used the -v parameter but this did not match the answer format so I switch it the -r.

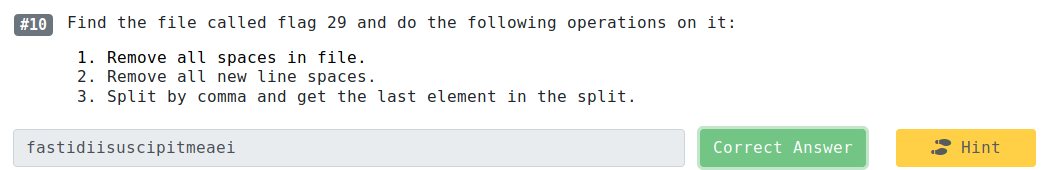




I used the tr command to remove all the white space and then the new lines as well. I then looked at the final to see the last comma and saw that it was at the end of the file so assumed that was the flag and I was correct.







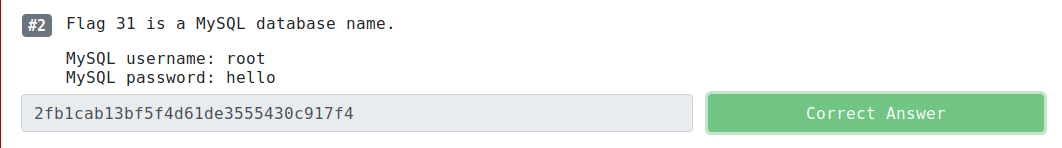
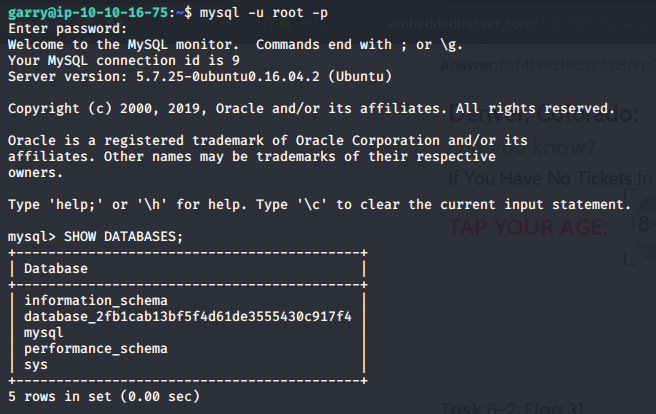
**Task 6: MySQL, FTP, groups, and RDP**

Now we are onto the last tasks in this CTF. I wasn’t sure how to go about this first task since we need to use the curl command and were not given an address. I used the hint and it suggested seeing if anything was running on localhost. I then was able to get flag30.

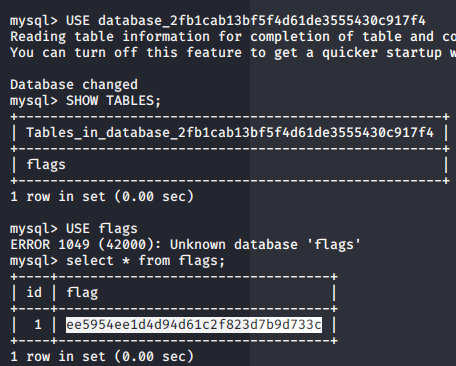


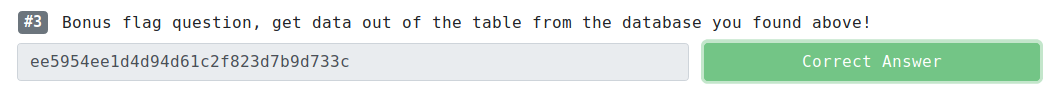


Flag 31 had us log into a MySQL database. I have not worked too much in this environment so I had to do some additional research but I ended up using the SHOW DATABASES; command and was able to find flag31.

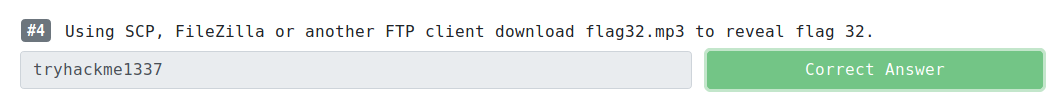


Going off the last flag I needed to look up syntax but was still able to extract the data from the flag table inside the database with flag31.

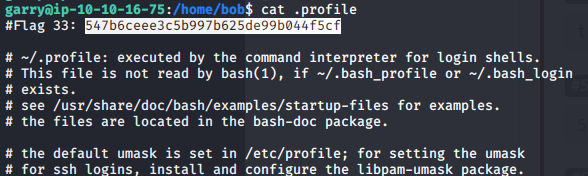


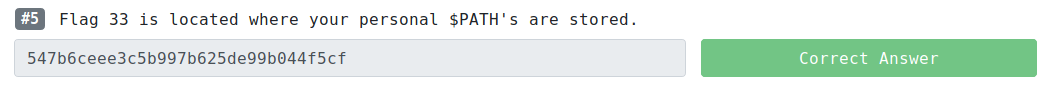


This flag was cool because I had ever worked with Filezilla and it was cool to learn another tool on Kali Linux. I had to install Filezilla but after that was able to connect to Alice and transfer her file onto my machine and was able to listen to it. It gave the password “tryhackme1337”.



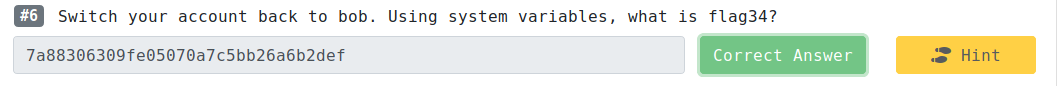
This was a trial and error flag. I knew the $PATH’s could be found in the .profile file in each user but I did not know what user the flag was in. I finally found it in Bob's profile.



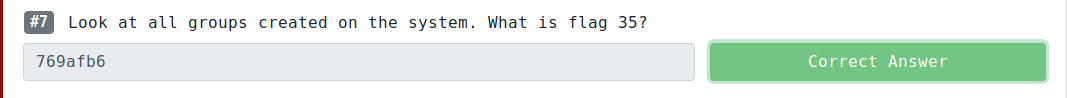


This flag was easy I just printed out the system variable that was associated with flag34.

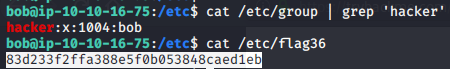


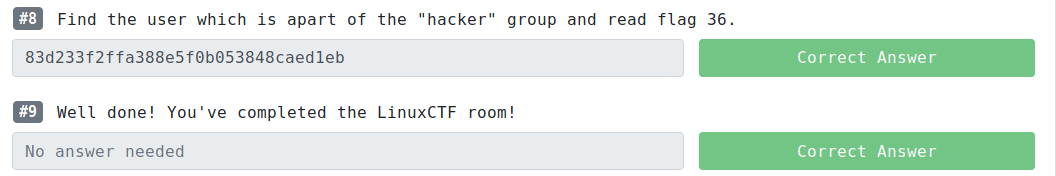


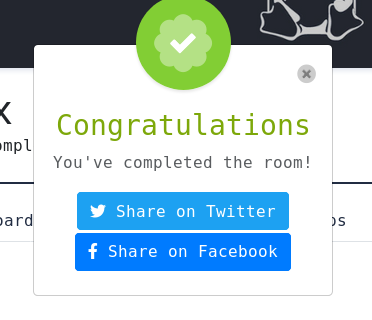
For this flag, I used the cat command to view the contents in the /etc/group folder. Flag 35 was given at the bottom.



This was the last flag in the CTF and was fun to find. I was able to see that bob was part of the ‘hacker’ group. We also knew that the flag was stored in the /etc directory from exploring all the directories throughout the CTF. I was able to get the last flag and finish the Linux CTF.







\*\*\*\*\*END NOTE\*\*\*\*\*

This was my first CTF on tryhackme as I am trying to grow my skills over the summer. I enjoyed exploring this machine and all the things that we can do with Linux. I hope you enjoyed reading this and can find this informative.

\*If you have any questions please feel free to contact me at [matthew.barich@western.edu](mailto:matthew.barich@western.edu). GOOD LUCK AND HAPPY HUNTING!!!