PSP0201
Week 4
Writeup

GROUP NAME: Cyborgs

MEMBERS

ID NUMBER	NAME	ROLE
1211102066	Hemma Ravindran	Leader
1211100614	Tivaasheny Ananthan	Member
1211102168	Nicholas Cheok Jia Jie	Member
1211100986	Sarvesh Munusamy	Member

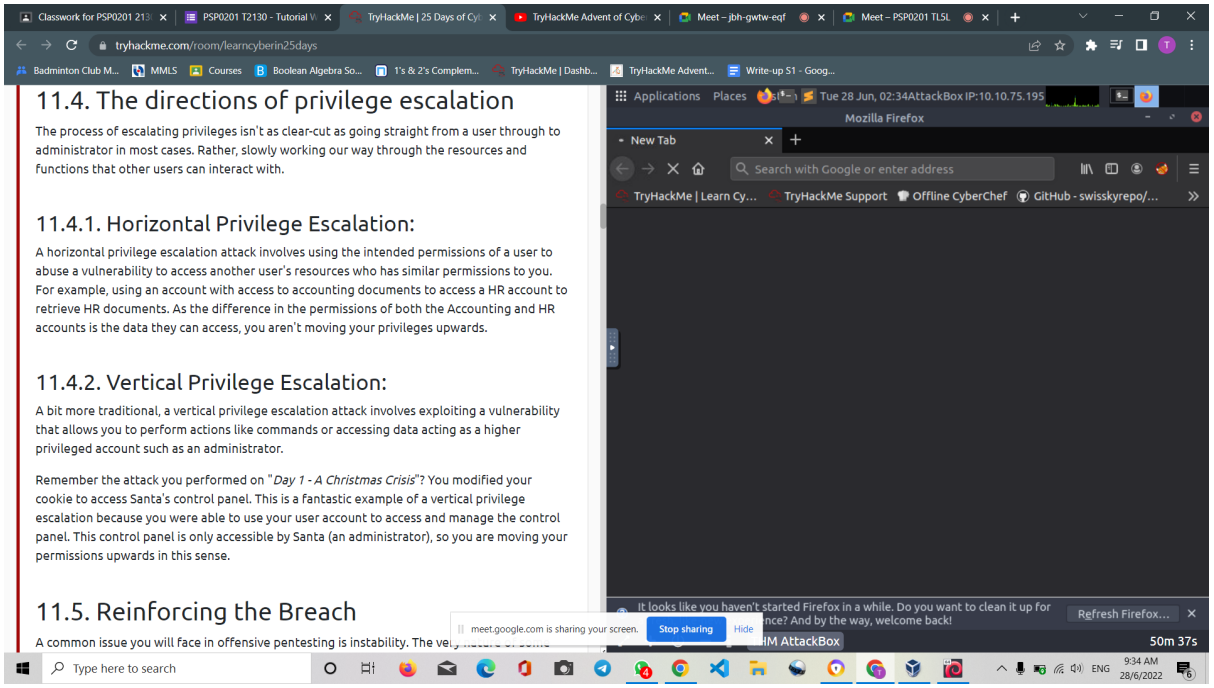
Day 11 - Networking The Rogue Gnome

Tool used: google and kali

Solution/walkthrough:

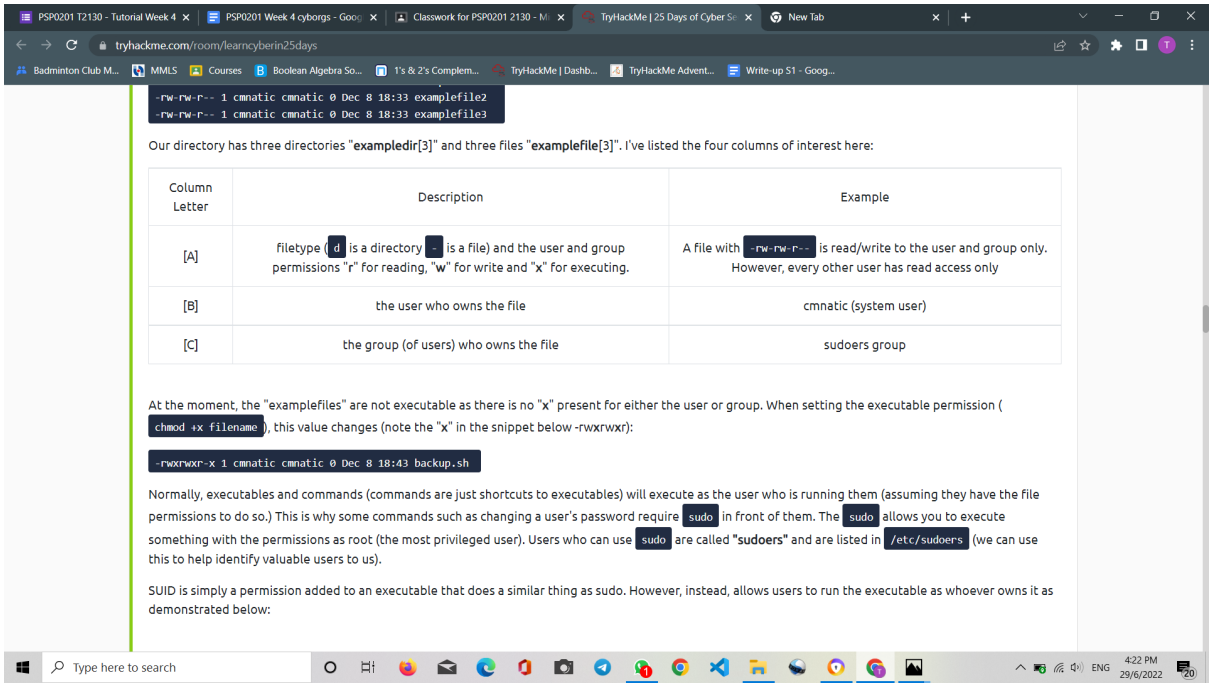
Question 1 , 2 and 3 :

We can get answers from the try hack me page on day 11.



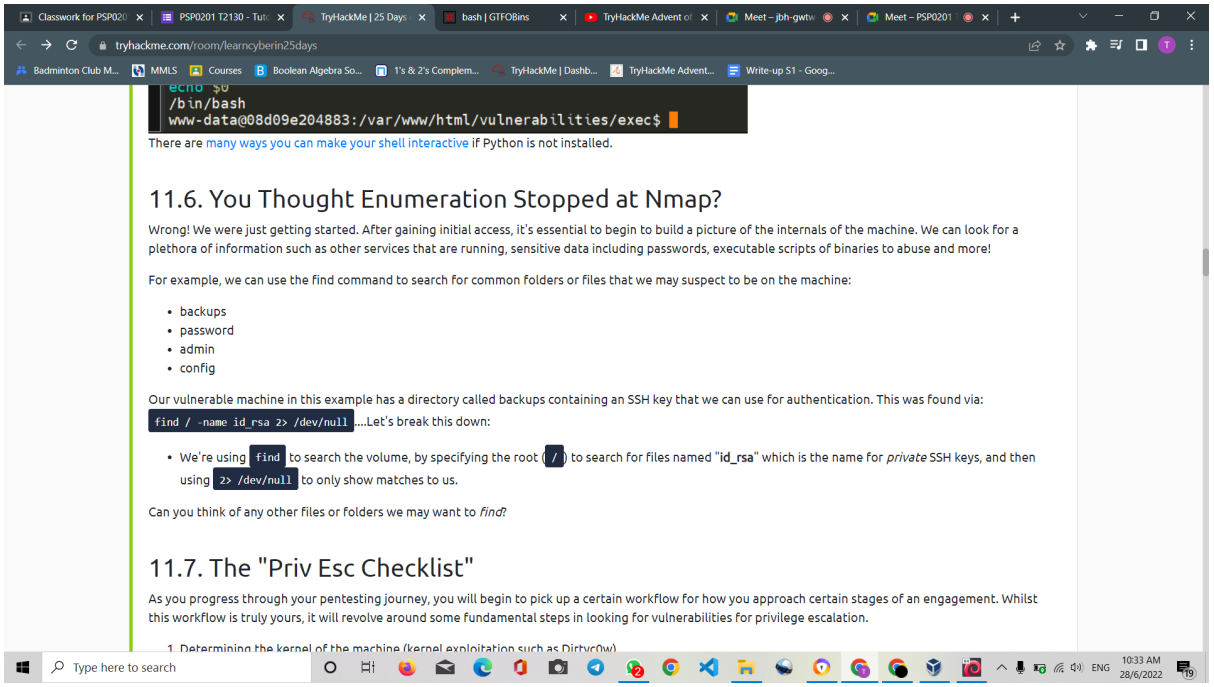
Question 4 :

The name of the file that contains a list of users who are a part of the sudo group is shown at the picture below.



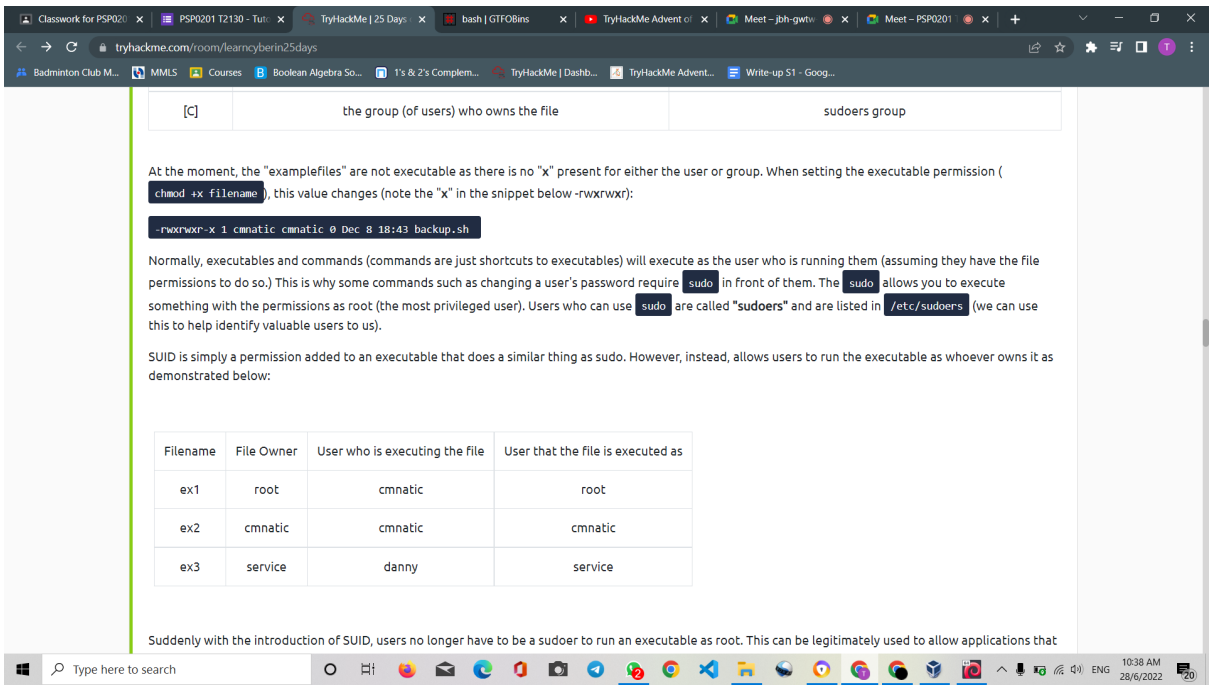
Question 5:

The Linux Command to enumerate the key for SSH is also shown in try hack me page on day 11 at (11.6).



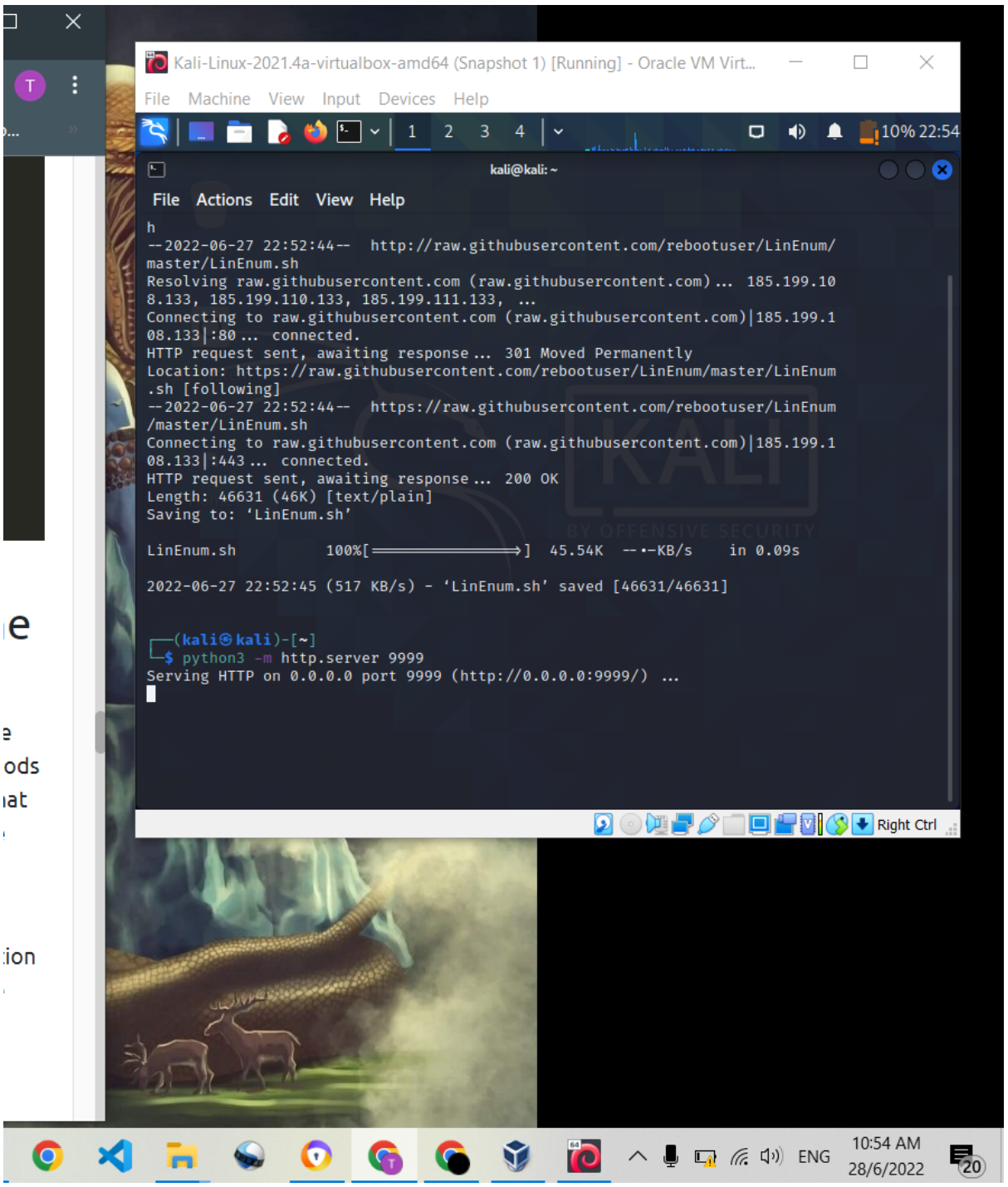
Question 6:

If we have an executable file named find.sh that we just copied from another machine, we have to write it with given format to get the answer by refering the try hack me (Vulnerability: SUID 101)



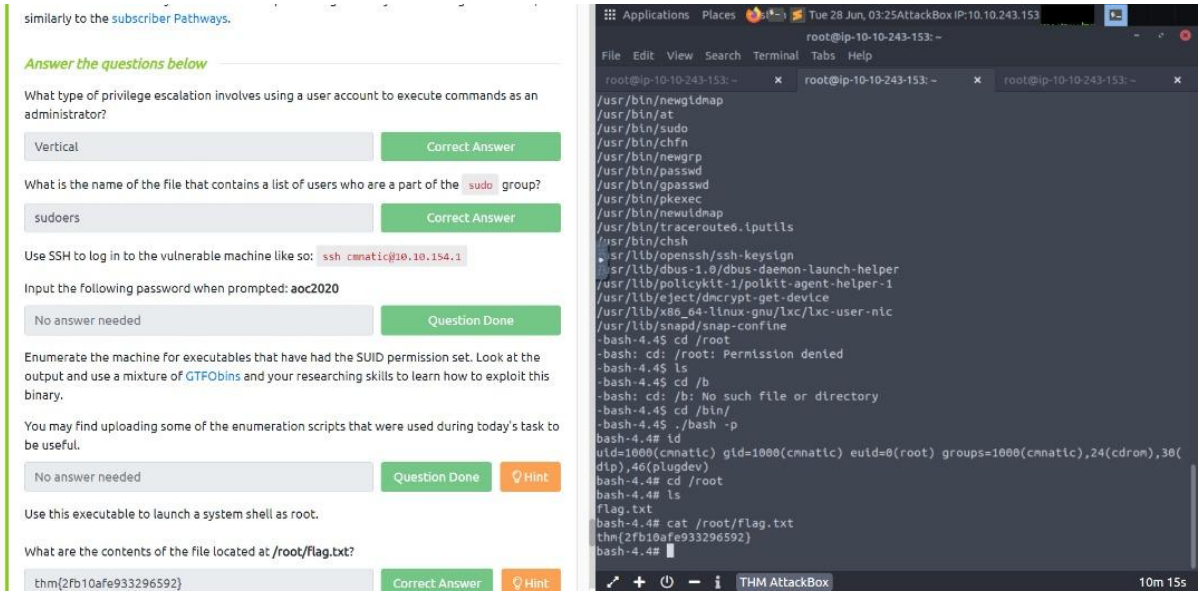
Question 7:

We used kali to get the command to host a http server using python3 on port 9999. We also refer to the (11.10.2.) in try hack me.



Question 8:

This is the content of the file located at /root/flag.txt.



Thought Process/Methodology:

Firstly, we need to start machine and also our attackbox. Next we need to type tmux. Then, we have to type ssh cmnatic@10.10.52.17 and type yes also it's password aoc2020. After that, we need to type sudo -il enter sudo -l and followed by password. Then type ls, enter and all we need based on the youtube channel. We did in kali to get the command to host a http server using python3 on port 9999. Then in order to to get flag we need to type find / -perm -4000 2>/dev/null. Then type some command. After that at last we need to type cat /root/flag.txt then we will get answer for flag.

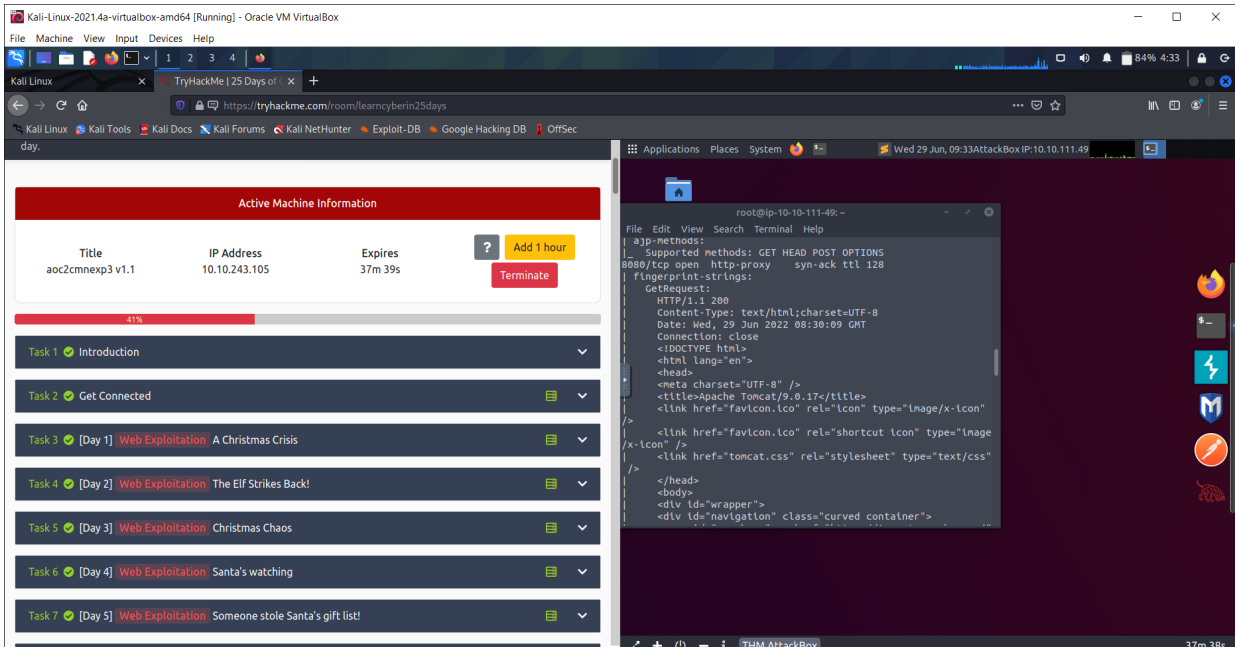
Day 12 - Networking Ready, set, elf

Tools used: google, attack box, Firefox,

Solution/walkthrough:

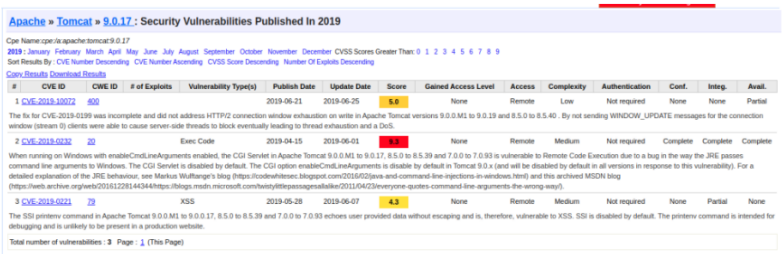
Question 1:

We found the version number of the web server .



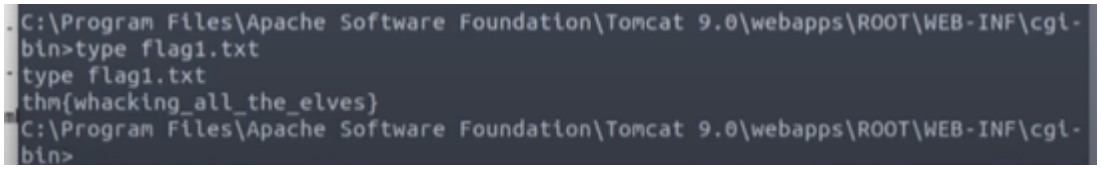
Question 2:

If we google Apache Tomcat 9.0.17 we can find a page called CVE Details which talks about remote code execution.



Question 3 :

We must run the shell to drop into a shell and find the flag, which is in the same directory you landed in C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin\. We must run type flag.txt to get the flag.



Question 4 :

We must set the Metasploit settings.

Thought Process/Methodology:

Firstly, we need to open up the terminal and put in the IP Address that we will be attacking.We have to do nmap to get the common scripts.After getting the scripts we can get the answer for the first question by scrolling through .We are supposed to find the port number and then type out exploit.db.com in the firefox to find the CVE number.After getting the CVE number we are supposed to put it in the terminal as msfconsole -q following the CVE number.we can go ahead and start configuring our settings.After that we have to type http://10.0.0.1/cgi-bin/systeminfo.sh with our ip address and get the information needed.We must run the shell to drop into a shell and find the flag, which is in the same directory you landed in C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin\. We must run type flag.txt to get the flag.

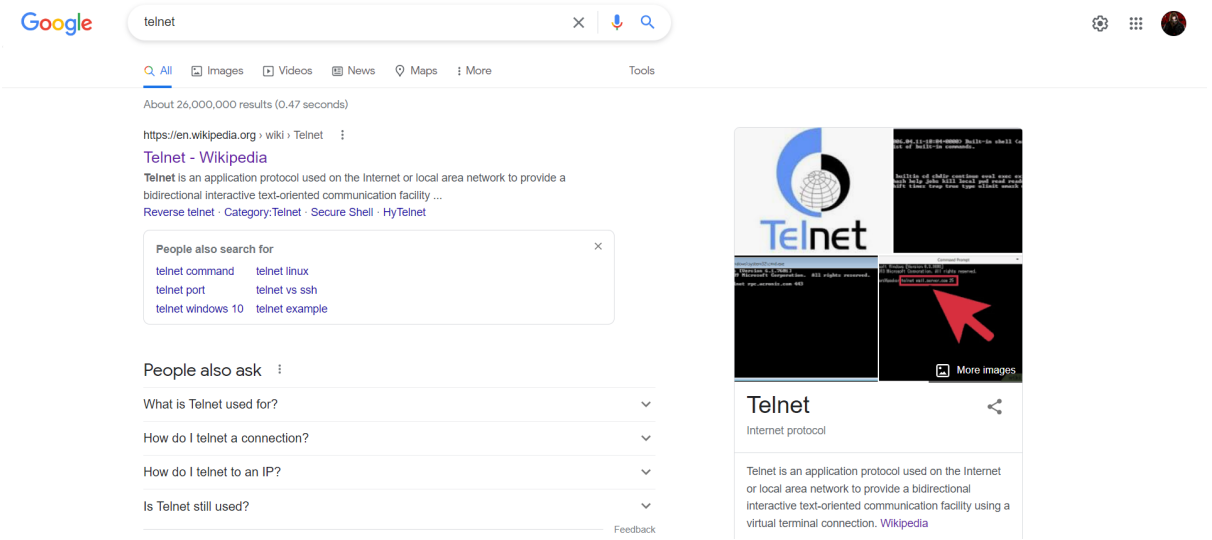
Day 13 - Coal for Christmas

Tools used: google, attack box, Firefox,

Solution/walkthrough:

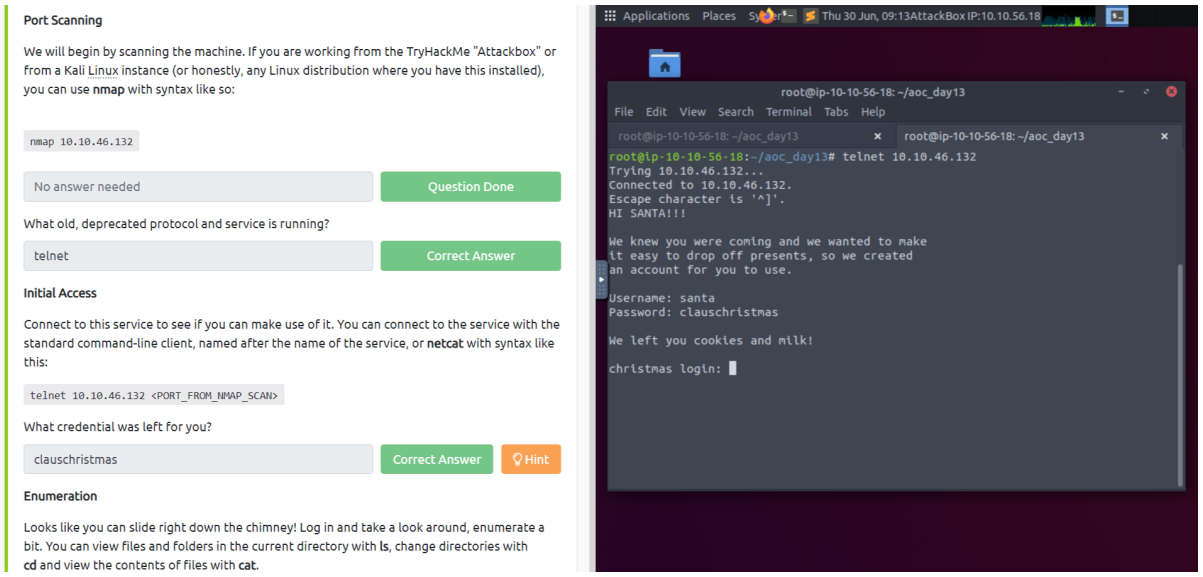
Question 1:

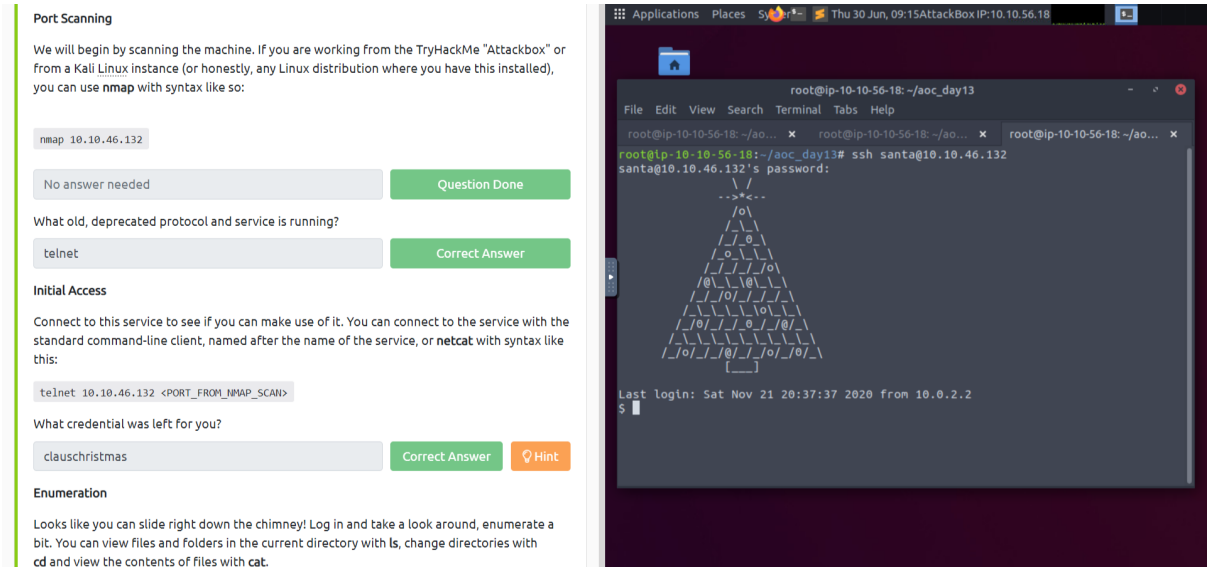
We google searched about the old, deprecated protocol and service is running which is Telnet.



Question 2:

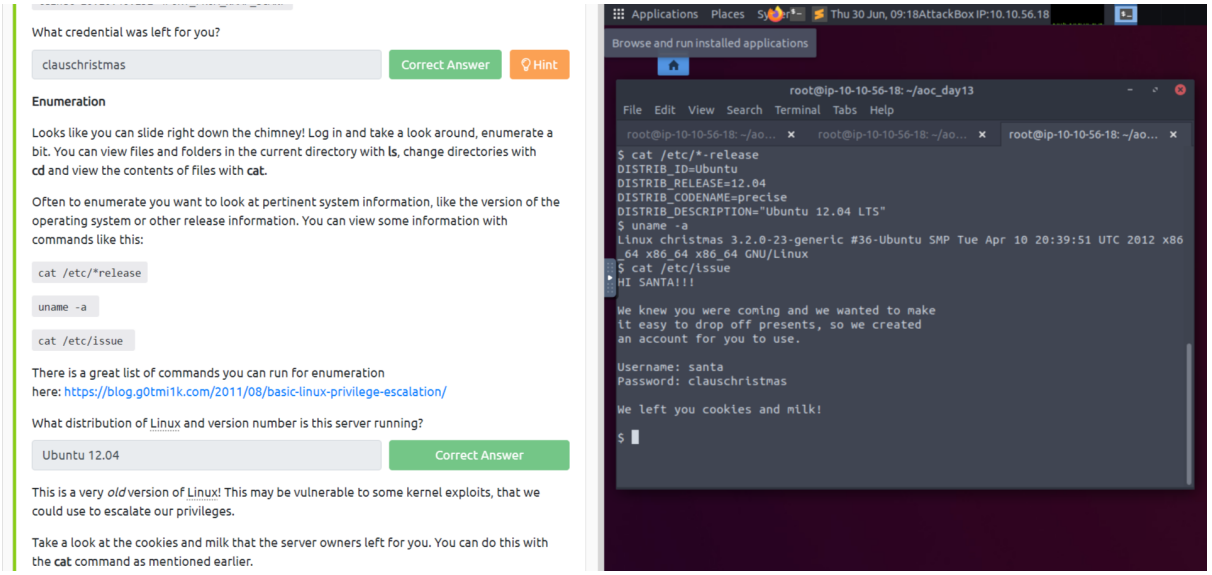
We typed in the command Telnet_MACHINE IP and we got the user name and also the password which is “clauschristmas”.





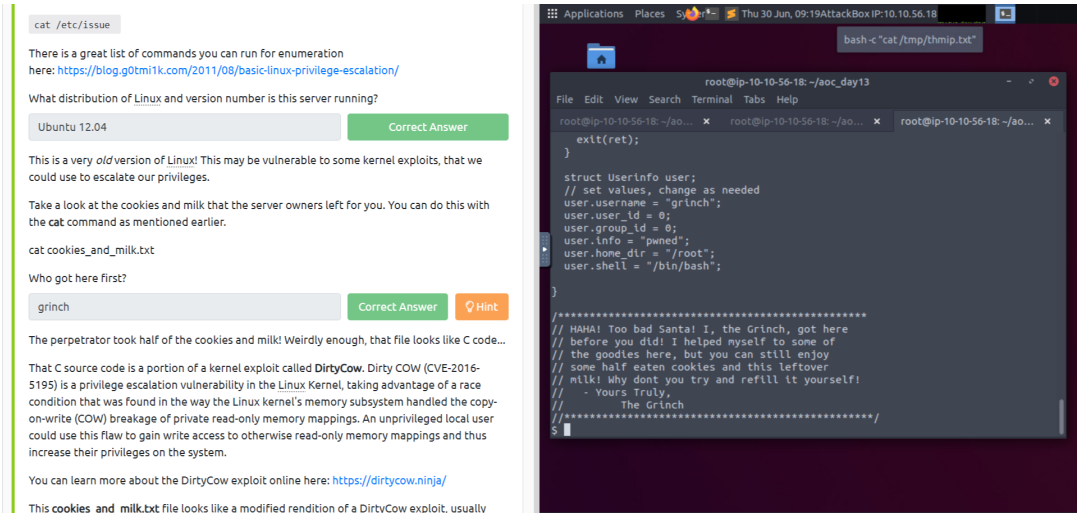
Question 3:

We typed in the command "cat /etc/*release" to get the distribution of Linux and version number is this server running which is "Ubuntu 12.04".



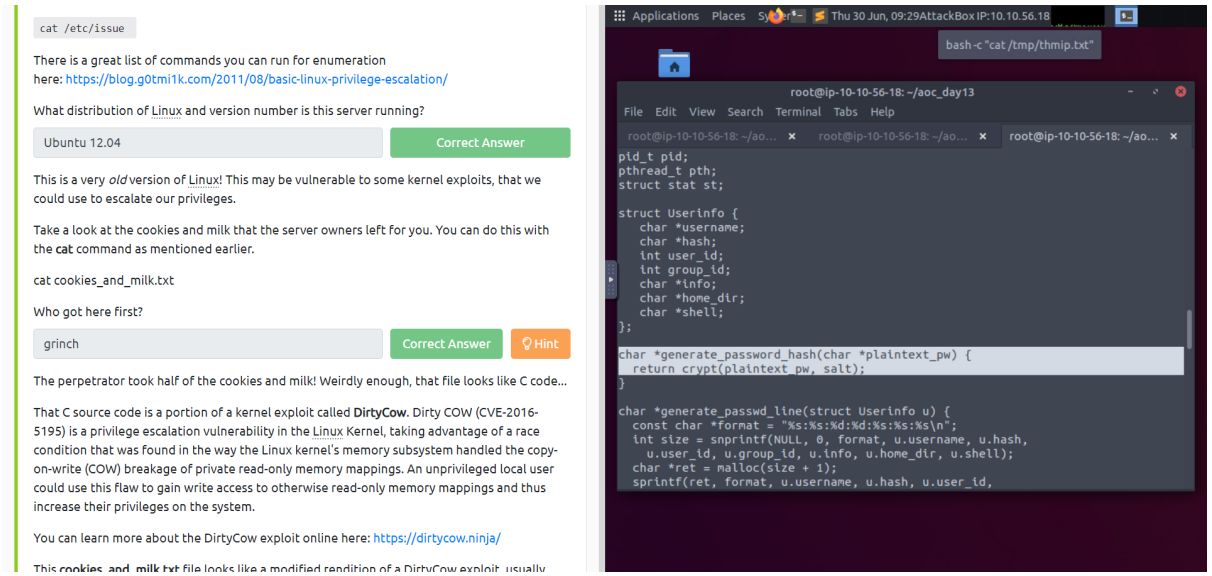
Question 4:

We typed in the command "cat cookies_and_milk.txt" and ran the command and we received a message saying that The Grinch got there before Santa did.



Question 5:

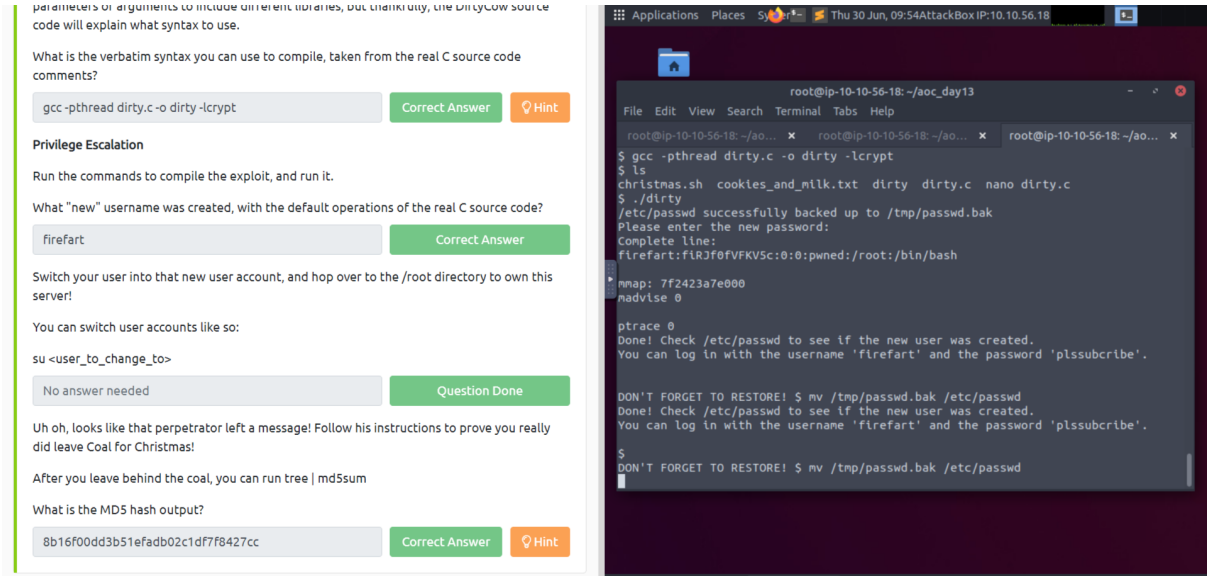
We pasted (char generate_password_hash(charplaintext_pw) {) in google and we searched up for the real C source and got the verbatim syntax we can use to compile.



```
//
// This exploit uses the pokemon exploit of the dirtycow vulnerability
// as a base and automatically generates a new passwd line.
// The user will be prompted for the new password when the binary is run.
// The original /etc/passwd file is then backed up to /tmp/passwd.bak
// and overwrites the root account with the generated line.
// After running the exploit you should be able to login with the newly
// created user.
//
// To use this exploit modify the user values according to your needs.
//   The default is "firefart".
//
// Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
//   https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c
//
// Compile with:
//   gcc -pthread dirty.c -o dirty -lcrypt
//
// Then run the newly create binary by either doing:
//   "./dirty" or "./dirty my-new-password"
//
// Afterwards, you can either "su firefart" or "ssh firefart@..."
//
// DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!
//   mv /tmp/passwd.bak /etc/passwd
//
// Exploit adopted by Christian "FireFart" Mehlmauer
// https://firefart.at
//
```

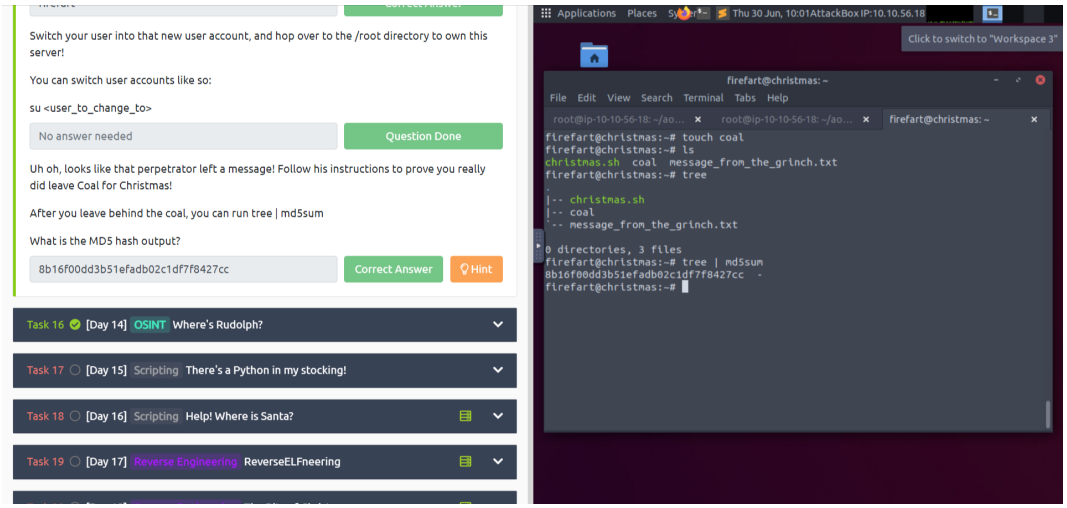
Question 6:

We typed in “gcc -pthread dirty.c -o dirty -lcrypt” under the file name “nano dirty.c” and ran the command and we got the new username which is “firefart”.



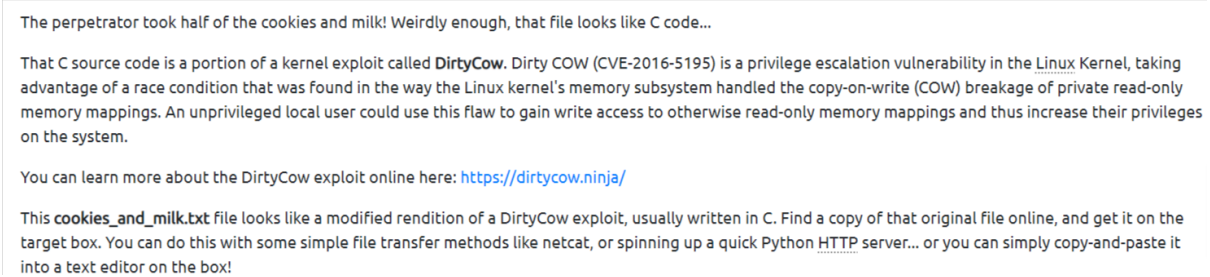
Question 7:

We typed in “tree | md5sum” and we got the MD5 hash output.



Question 8:

We searched in the THM text and we found that (CVE-2016-5195) is the CVE for Dirty COW.



The perpetrator took half of the cookies and milk! Weirdly enough, that file looks like C code...

That C source code is a portion of a kernel exploit called **DirtyCow**. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel, taking advantage of a race condition that was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

You can learn more about the DirtyCow exploit online here: https://dirtycow.ninja/

This **cookies_and_milk.txt** file looks like a modified rendition of a DirtyCow exploit, usually written in C. Find a copy of that original file online, and get it on the target box. You can do this with some simple file transfer methods like netcat, or spinning up a quick Python HTTP server... or you can simply copy-and-paste it into a text editor on the box!

Thought Process/Methodology:

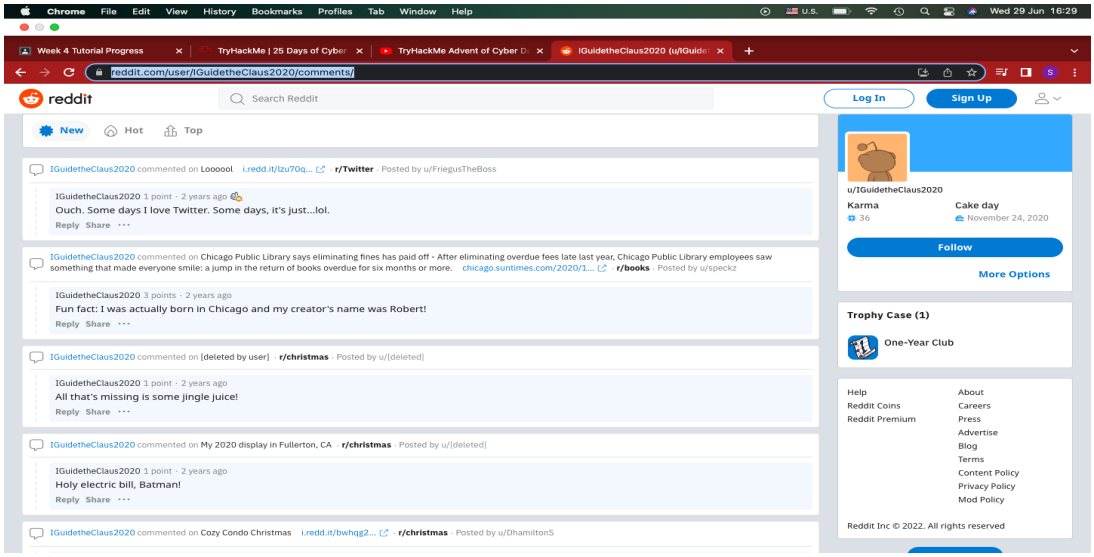
Firstly, we started our machine and attacked box and got our IP addresses. We google searched about SSH and Telnet about their details. We used the terminal to scan our machine by using nmap MACHINE_IP and ran it. After that we created a new tab, we entered the command Telnet MACHINE_IP so that we get the username and the password. After getting the username and password, we then opened a new tab and we typed in the command “ssh@santa MACHINE_IP” and we entered santa’s password. Then, we typed in the command “cat /etc/*release” to get the distribution of Linux and version number is this server running which was Ubuntu 12.04 . We also used the command “cat cookies_and_milk.txt” and received a message from The Grinch to Santa saying that he got there before Santa did. We explored the DirtyCow website. We scrolled up and we copied (char generate_password_hash(charplaintext_pw) {) and pasted it in google to get the real C source and we copied the sources in the website and pasted it under “nano dirty.c” file and we saved the file in the terminal. Then, we typed in “gcc -pthread dirty.c -o dirty -lcrypt” under “nano dirty.c” file and got our new username and also the new password that we created. We also typed in “touch coal” and “tree” and got 3 files and piped them into “md5sum” and we got the MD5 hash output. Last but not least, We searched in the THM text and we found that (CVE-2016-5195) is the CVE for Dirty COW and terminated our machines.

Day 14 - Where's Rudolph?

Tools used: Google
Solution/walkthrough:

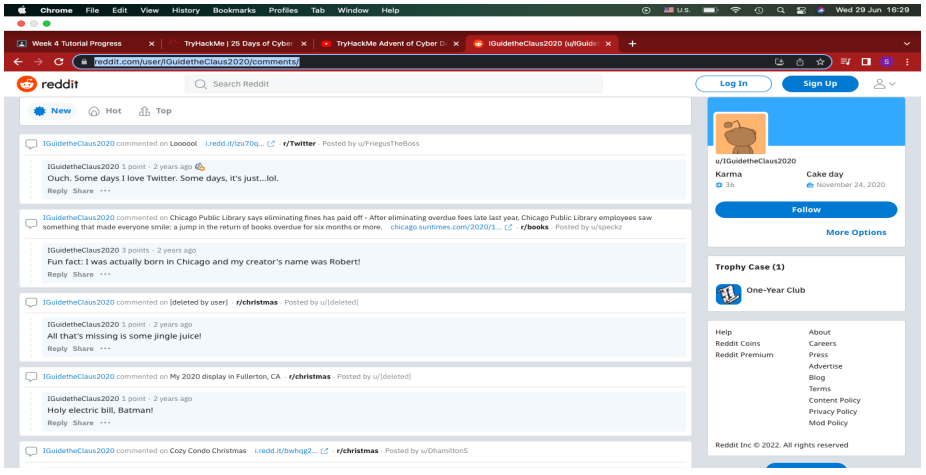
Question 1:

First, we should search reddit and find Rudolph's reddit page and then open the comment section while copying the url link above.



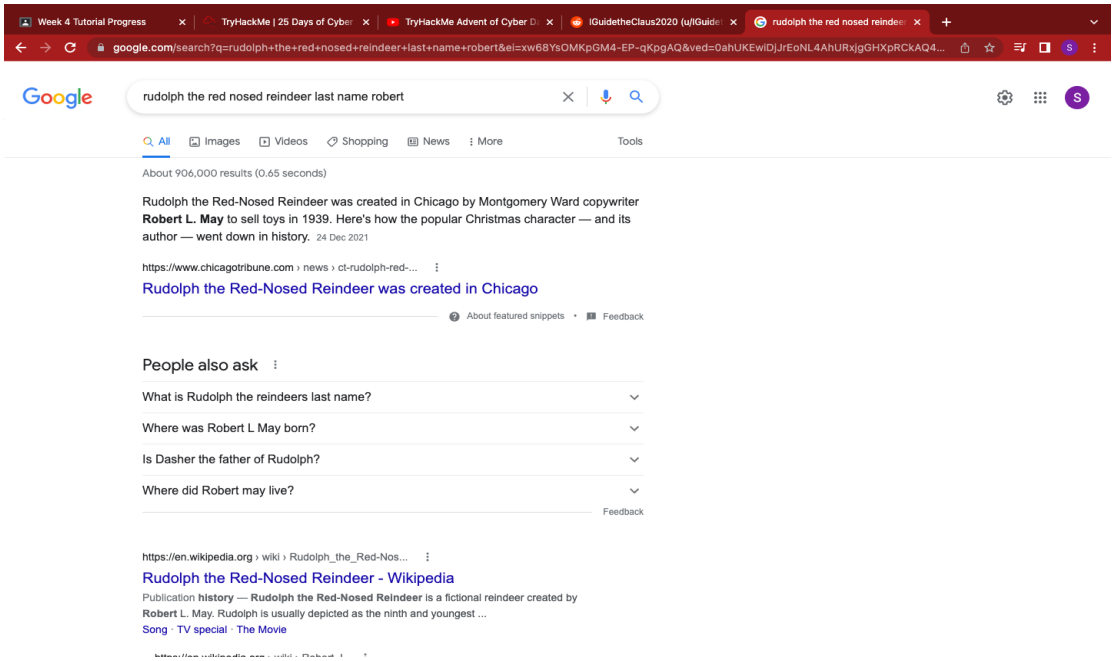
Question 2:

We should scroll through rudolph's comment section and find out where he born.



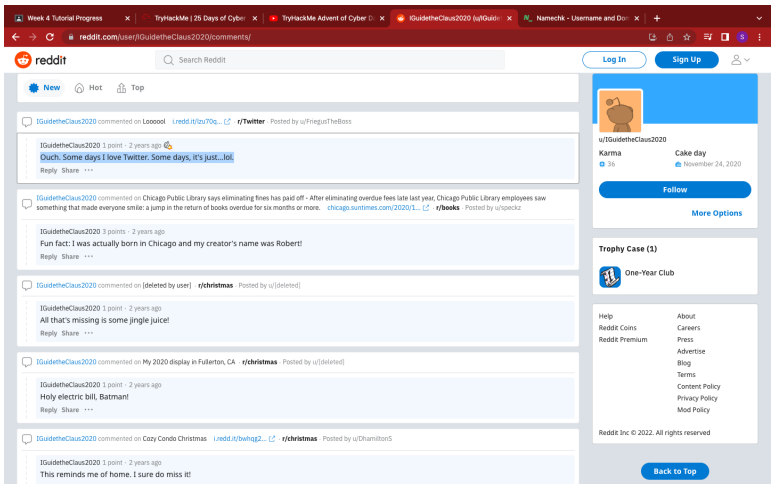
Question 3:

We should search for Rudolph the red reindeer last name robert in google in order to get Roberts's last name.



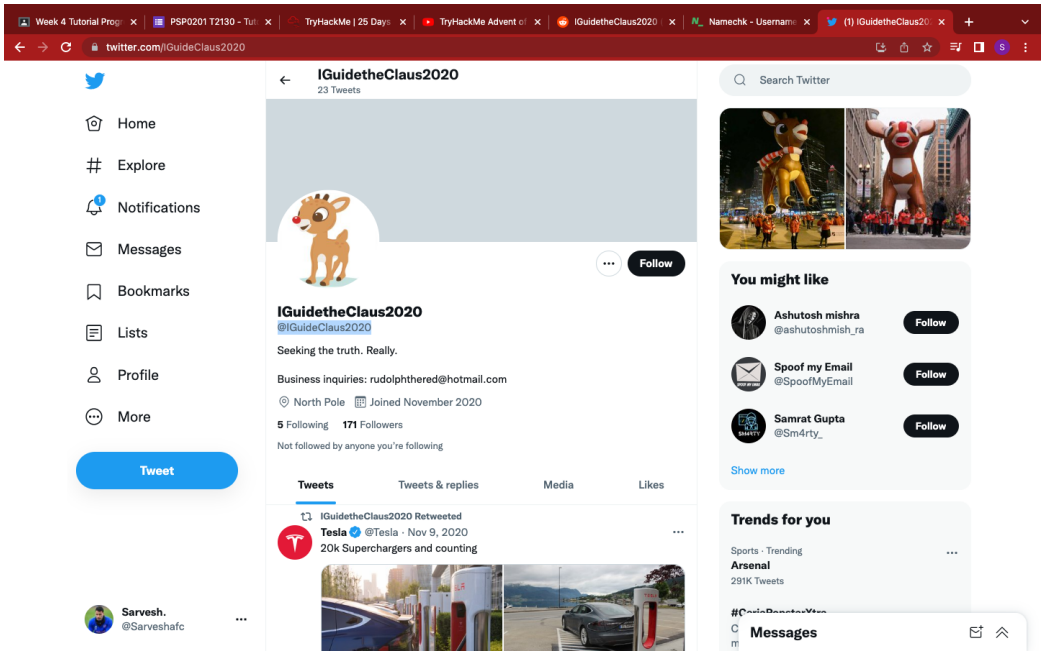
Question 4:

We should scroll through Rudolph's comment section and find out what other social platforms Rudolph uses.



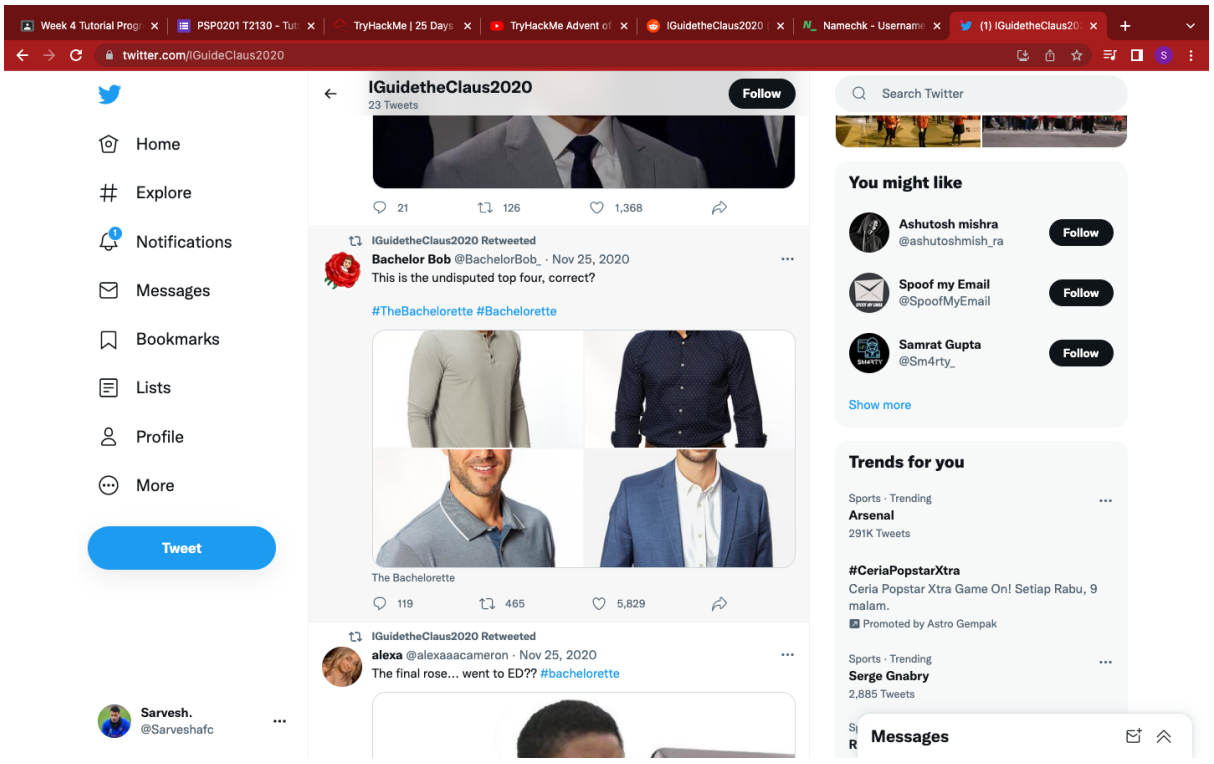
Question 5:

We should search rudolph’s twitter id using his reddit id and find his username.



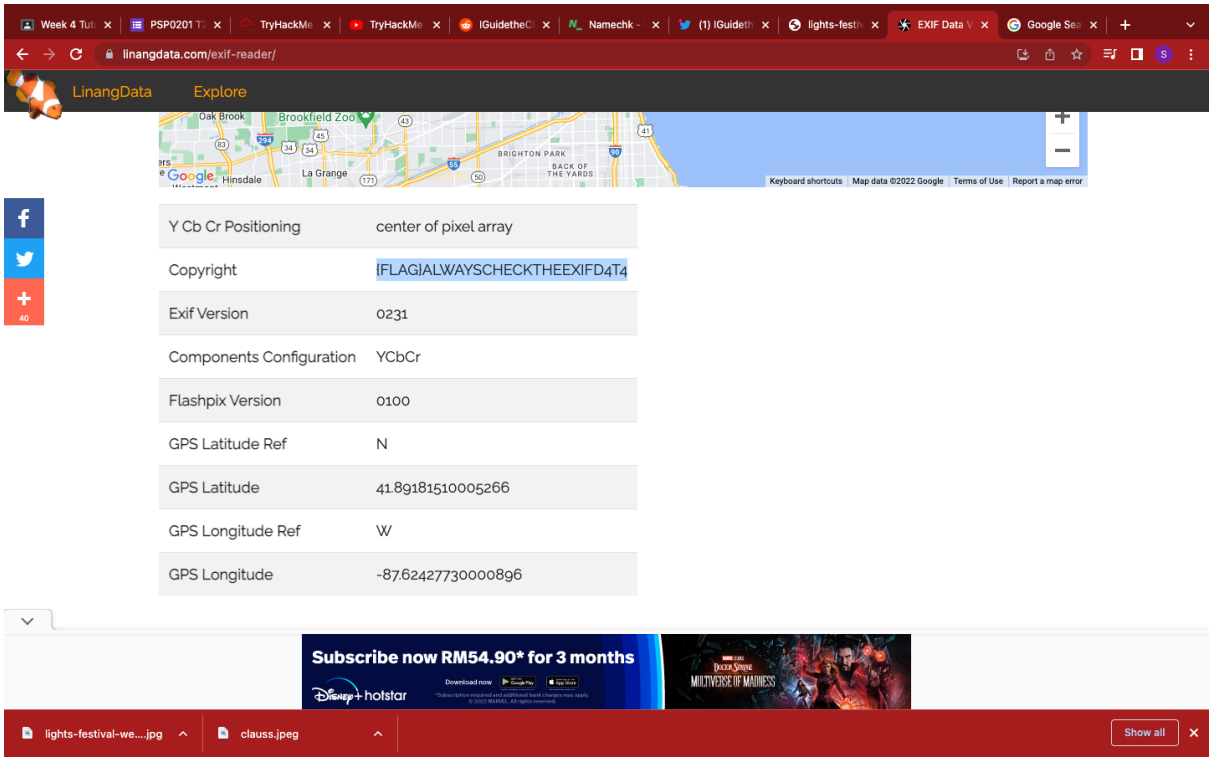
Question 6:

We should scroll through rudolph's twitter feed and find out what is his favourite tv show.



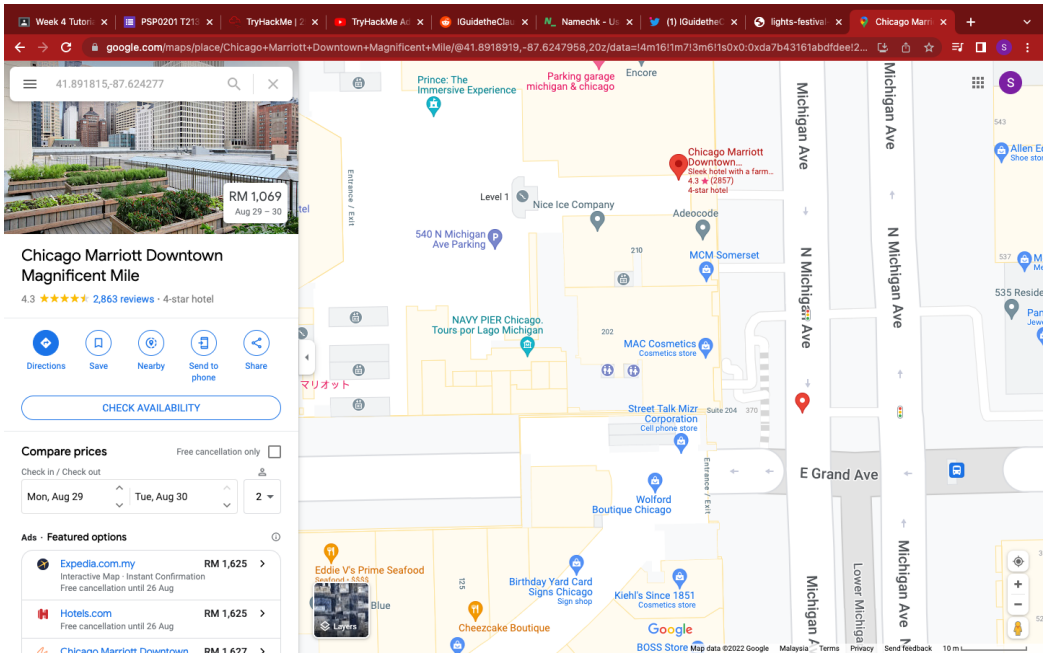
Question 7,8, and 9:

We should use exiff data retriever and find out the location and exact coordinate. Then we can receive the flag that was given.



Question 11:

Paste the coordinate in maps and find out which hotel he stayed. Then, we can find out the street number of the hotel.



Though Process/Methodology:

Firstly, we should read the instructions given and we should search reddit and find Rudolph's reddit page and then open the comment section while copying the url link above. Later on, after opening Rudolph's reddit, we should scroll through Rudolph's comment section and find out where he was born. Next, we should search for Rudolph the red reindeer last name robert in google in

order to get Roberts’s last name which is May. Next, we should scroll through Rudolph's comment section and find out what other social platforms Rudolph uses, such as twitter. Later, we should search rudolph’s twitter id using his reddit id and find his username which is @iguideclauss2020. After scrolling through his twitter feed, we will be able to find his favourite show, which is bachorollate and also gain information about where he was paraded in. Next, we should use exiff data retriever and find out the location and exact coordinate. Then we can receive the flag that was given. Lastly, we should paste the coordinates in maps and find out which hotel he stayed. Then, we can find out the street number of the hotel.

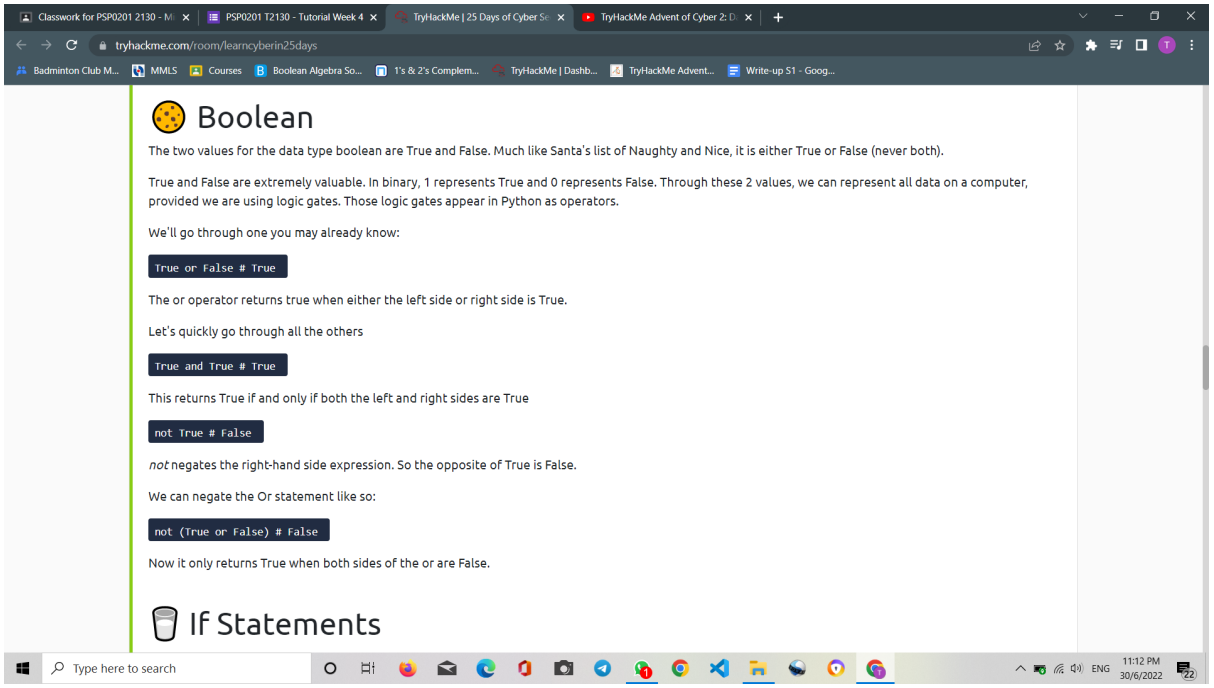
Day 15 - There's a Python in my stocking!

Tools used: tryhackme , Vscode

Solution/walkthrough:

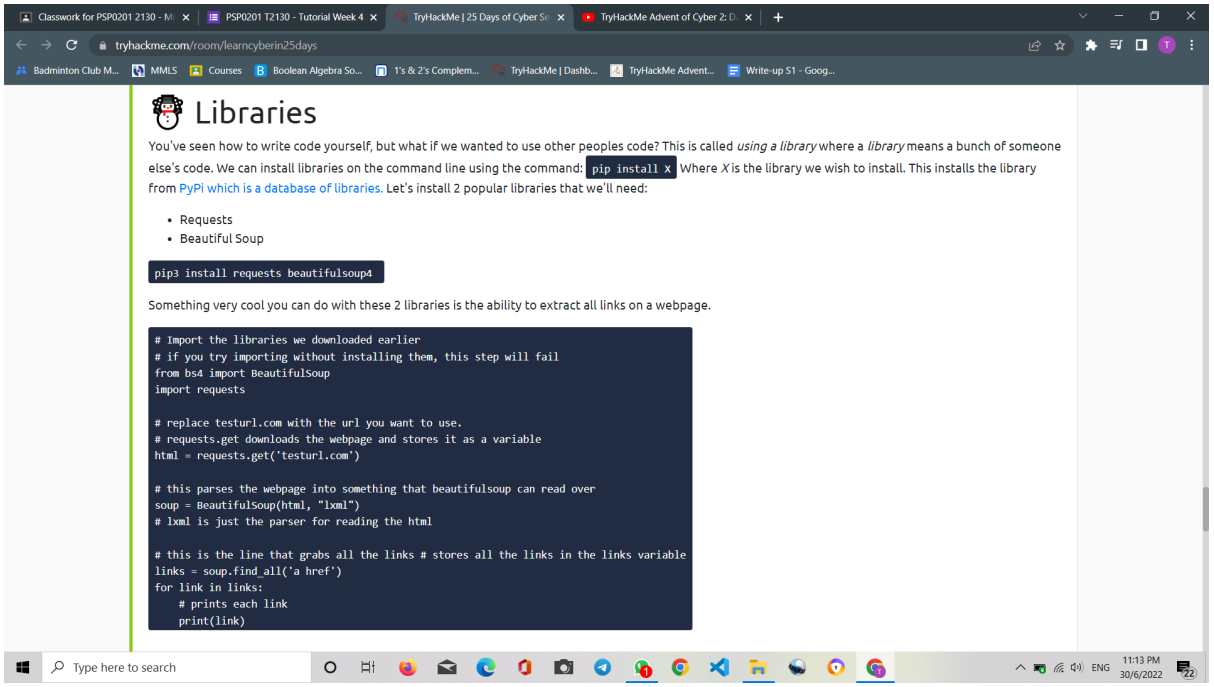
Question 1:

The first question asks us to find the output of True + True. We got this answer by reading the information given.



Question 2:

The next question asks us the name of the database for installing other people's libraries. We found this by simply reading the challenge description. The name of this database is PyPi.

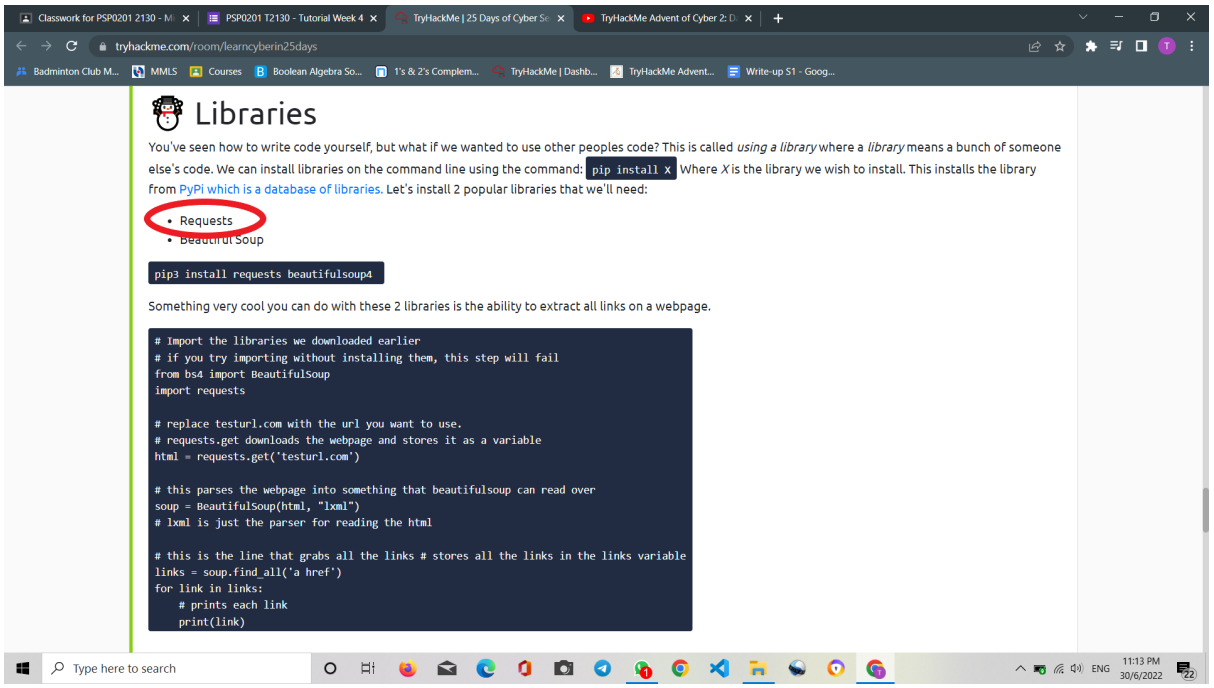


Question 3:

The next question asks us the output of bool("False"). The output is True.We are actually passing in a String containing the word False.

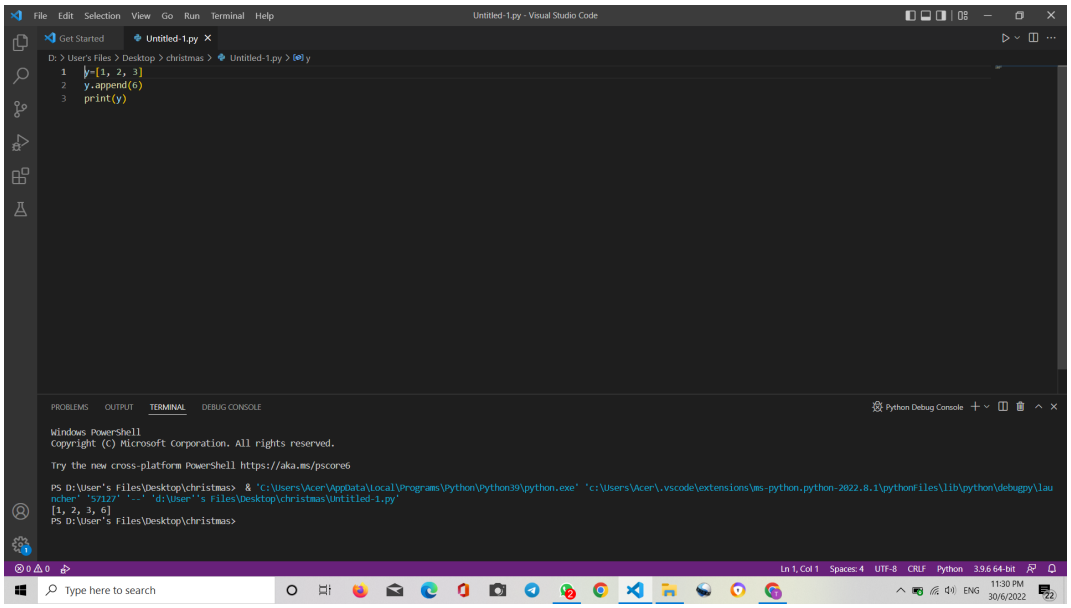
Question 4:

The next question asks us what library can be used to download the HTML of a webpage.We can find it by reading the description.



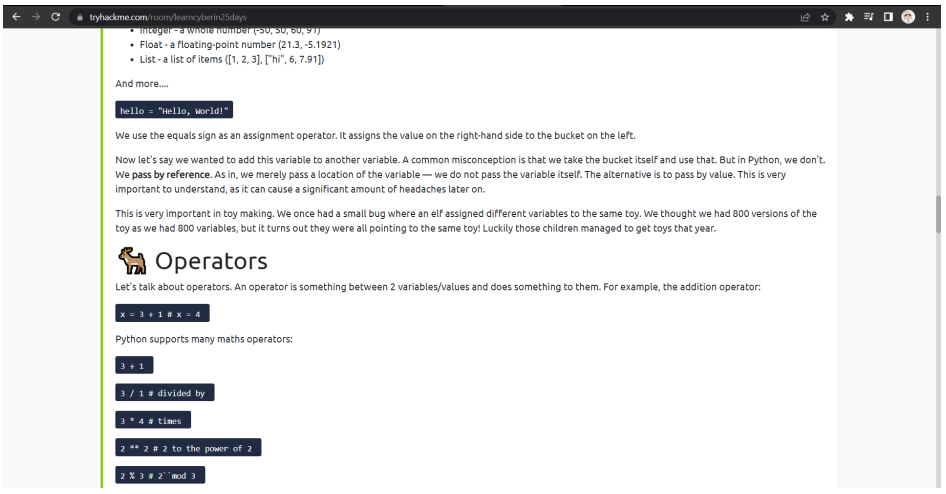
Question 5:

The next question asks us to analyse some code which uses the append function and some interesting variables. When we run through the code, we see that the output is [1, 2, 3, 6]. This is because the append functions as adding that input inside the y.



Question 6:

The next question asks us the reason why the output is such.This can happen because of pass by reference. With pass by reference, when we pass a variable into a function, we are passing a reference to the location in memory where the variable is stored.



Question 7:

This question asks us the output if the input is “Skiddy”. The output will be ``The Wise One has allowed you to come in." because it's in the names list.

```
names = ["Skidy", "DorkStar", "Ashu", "Elf"]
name = input("What is your name? ")
if name in names:
   print("The Wise One has allowed you to come in.")
else:
   print("The Wise One has not allowed you to come in.")
```

Question 8:

This question asks us the output if the input is “elf”. The output will be ``The Wise One has not allowed you to come in." because it's in the names list but with a capital ‘E’.

```
names = ["Skidy", "DorkStar", "Ashu", "Elf"]
name = input("What is your name? ")
if name in names:
   print("The Wise One has allowed you to come in.")
else:
   print("The Wise One has not allowed you to come in.")
```

Though Process/Methodology:

Firstly, we read through the instructions and the information given.It was easy to find the answers because all the answers were in the description. We just have to look through .