
# PSP0201

# Week 4 Writeup

Group Name : Ilomilo

Members:

| ID NUMBER | STUDENT NAME | Role |
|---|---|---|
| 1211103196 | Adriana Iman binti Noor Azrai | Leader |
| 1211103282 | Aida Maisarah binti Hisam | Member |
| 1211103216 | Sofea Hazreena binti Hasdi | Member |
| 1211103227 | Wan Alia Adlina binti Wan Azman | Member |

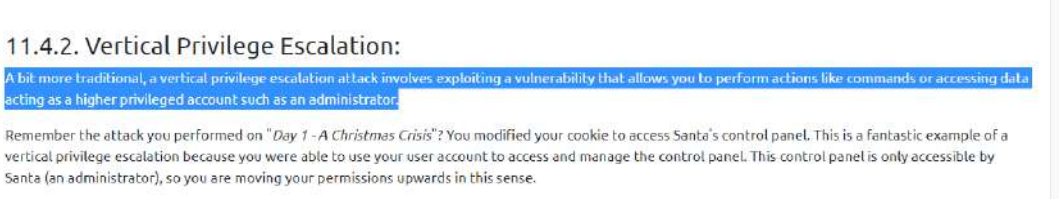
# Day 11 - Networking The Rogue Gnome

**Tools Used :** terminal

**Solution/Walkthrough:**

Question 1 : What type of privilege escalation involves using a user account to execute commands as an administrator?

On tryhackme, part 11.4.2 about the vertical privilege escalation, in the first paragraph stated that we can execute commands as an administrator.

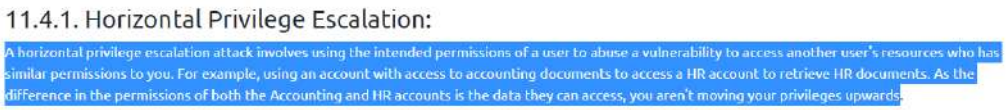



Question 2 : You gained a foothold into the server via www-data account. You managed to pivot it to another account that can run sudo commands. What kind of privilege escalation is this?

If we can run the sudo command, it means we can execute the command as an administrator, hence it is vertical privilege.

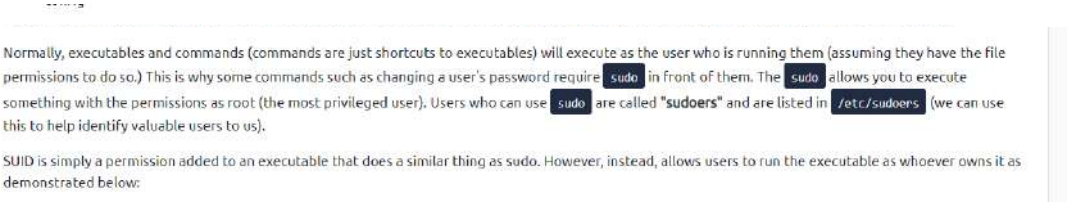
Question 3 : You gained a foothold into the server via www-data account. You managed to pivot it to Sam the analyst's account. The privileges are almost similar. What kind of privilege escalation is this?

On tryhackme, part 11.4.1, about the horizontal privilege escalation, it is stated that we can access another user's resources who has similar permissions like us.



Question 4 : What is the name of the file that contains a list of users who are a part of the sudo group?

At tryhackme, part 11.8, about the vulnerability: SUID 101, it is stated that the file name that contains a list of users who are a part of the sudo group is called sudoers.


Normally, executables and commands (commands are just shortcuts to executables) will execute as the user who is running them (assuming they have the file permissions to do so.) This is why some commands such as changing a user's password require `sudo` in front of them. The `sudo` allows you to execute something with the permissions as root (the most privileged user). Users who can use `sudo` are called "**sudoers**" and are listed in `/etc/sudoers` (we can use this to help identify valuable users to us).

SUID is simply a permission added to an executable that does a similar thing as sudo. However, instead, allows users to run the executable as whoever owns it as demonstrated below:

Question 5 : What is the Linux Command to enumerate the key for SSH?

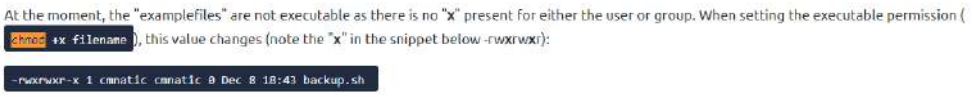
At part 11.6, the Linux Command to enumerate the key for SSH is
'find / -name id_rsa 2> /dev/null'


Our vulnerable machine in this example has a directory called backups containing an SSH key that we can use for authentication. This was found via: `find / -name id_rsa 2> /dev/null` ....Let's break this down:

- We're using `find` to search the volume, by specifying the root (`/`) to search for files named "**id_rsa**" which is the name for *private* SSH keys, and then using `2> /dev/null` to only show matches to us.

Question 6 : If we have an executable file named find.sh that we just copied from another machine, what command do we need to use to make it be able to execute?

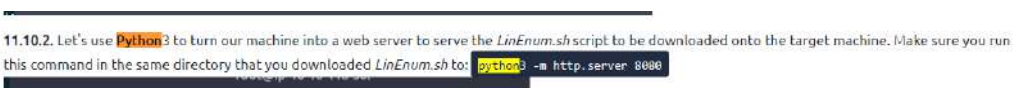
In part 11.8, they taught us how to execute a file.


At the moment, the "examplefiles" are not executable as there is no "**x**" present for either the user or group. When setting the executable permission ( `chmod +x filename` ), this value changes (note the "**x**" in the snippet below -rwxrwxr):

```
-rwxrwxr-x 1 cmnatic cmnatic 0 Dec 8 18:43 backup.sh
```

Question 7 : The target machine you gained a foothold into is able to run wget. What command would you use to host a http server using python3 on port 9999?

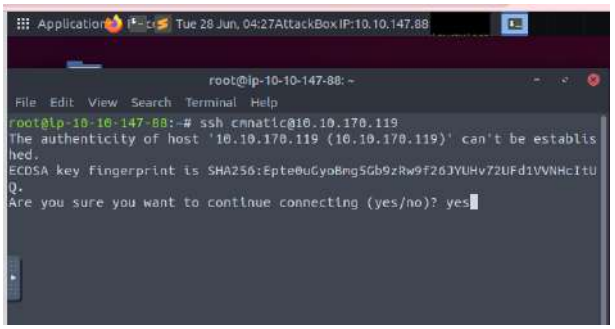
In part 11.10.2, they taught us the command to host a http server.

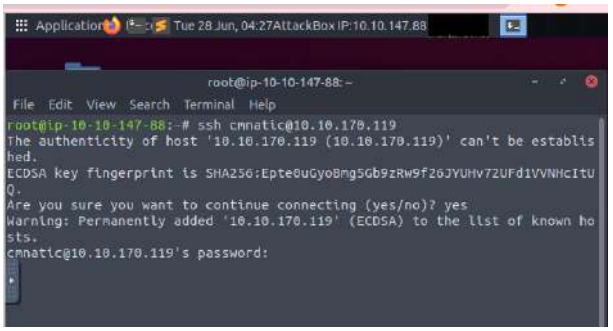

**11.10.2.** Let's use Python3 to turn our machine into a web server to serve the *LinEnum.sh* script to be downloaded onto the target machine. Make sure you run this command in the same directory that you downloaded *LinEnum.sh* to: `python3 -m http.server 8000`

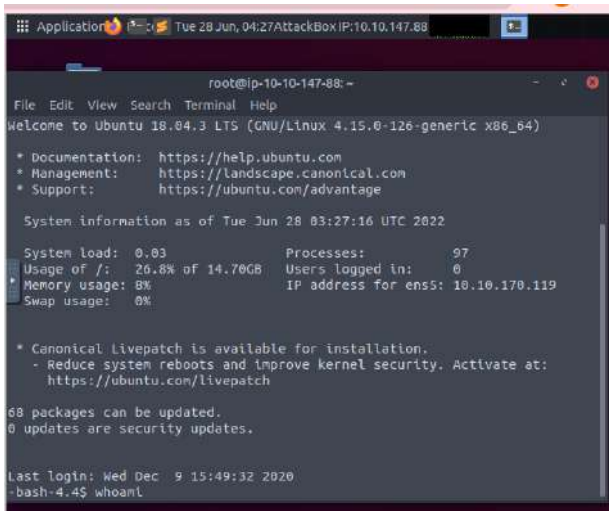
Question 8 : What are the contents of the file located at /root/flag.txt?

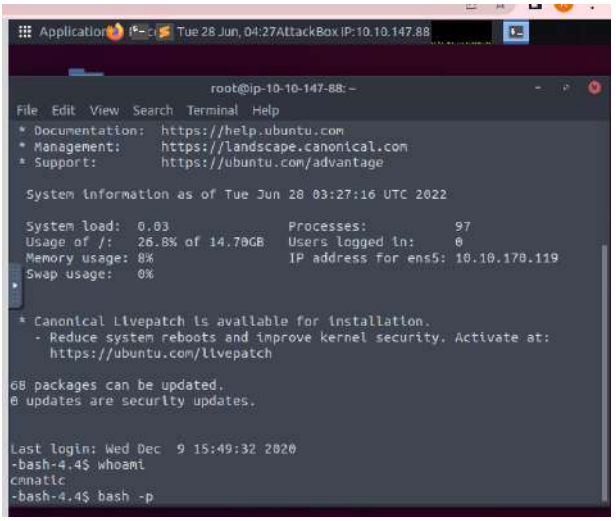
We first deployed the machine and then started the attackbox. After that we open the terminal and log in the vulnerable machine by entering 'ssh cmnatic@IP_MACHINE'. Then

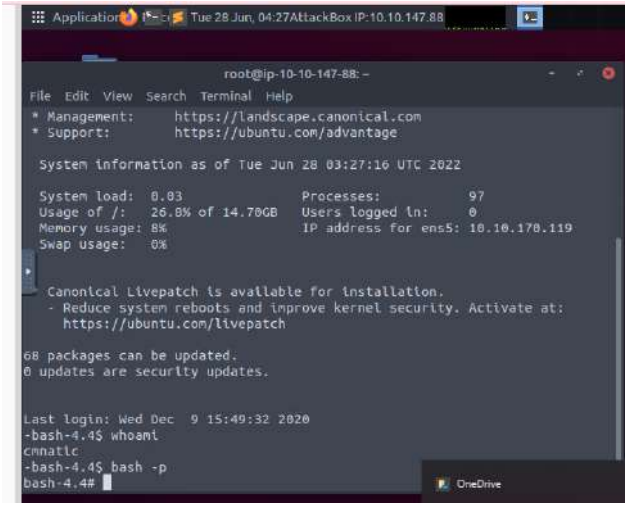
after we press enter, they will return the confirmation if we are sure to connect. We then type in ‘yes’ and press enter. After that we were asked to enter the password which is aoc2020, which was given at tryhackme. After that we successfully log in, at the lowest part, it will return us “bash-4.4$”. There we then enter “whoami” and it will return us back to “cmnatic”. We then enter “bash -p” to escalate our privilege to “root”. After that we then type in “cat /root/flag.txt” to see the contents in that file.

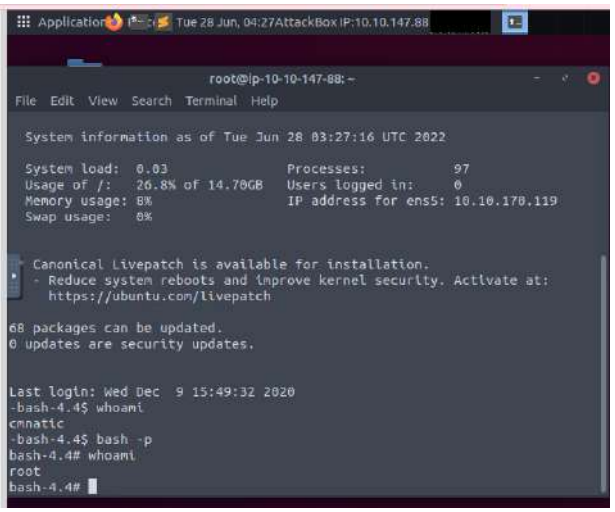


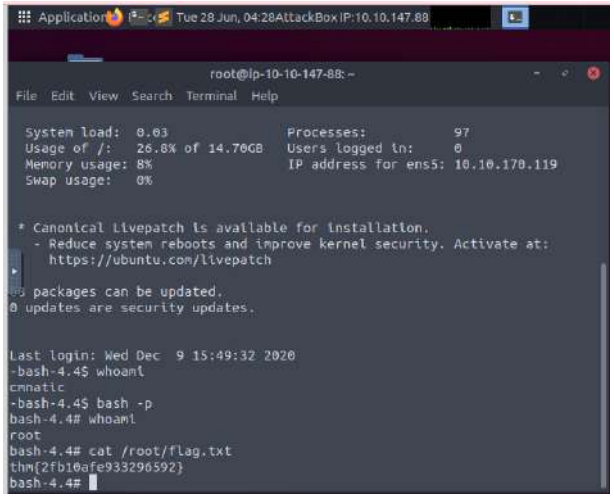






**Throughout process :**

At tryhackme page, in 11.4.1 and 11.4.2, we acknowledge that vertical privilege allows us to execute commands as an administrator and if we were using sudo, that means we run the command as administrator, also we know that horizontal privilege allows us to access another user's resources which has the similar permissions as us. In 11.8, the text clearly stated that the file name contains the list of users who are part of the sudo group called as sudoers. In 11.6, we know the Linux command to enumerate the key for SSH is 'find / -name id_rsa 2> /dev/null'. In 11.8, it is said that to execute a file the command will be like 'chmod +x filename'. On 11.10.2, we learned how to host a http server. We first deployed the machine and then started the attackbox. After that we open the terminal and log in the vulnerable machine by entering 'ssh cmnatic@IP_MACHINE'. Then after we press enter, they will return the confirmation if we are sure to connect. We then type in 'yes' and press enter. After that we were asked to enter the password which is aoc2020, which was given at tryhackme. After we successfully log in, at the lowest part, it will return us "bash-4.4$". There we then enter "whoami" and it will return us back to "cmnatic". We then enter "bash -p" to escalate our privilege to "root". After that we then type in "cat /root/flag.txt" to see the contents in that file.

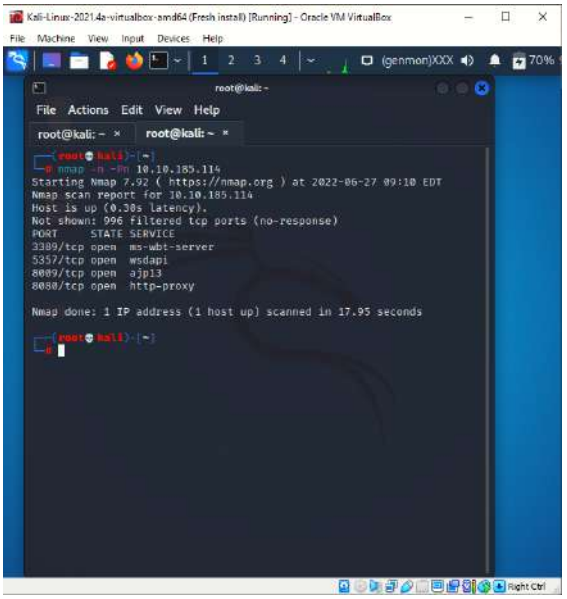
# Day 12 - Networking Ready, Set, Elf.

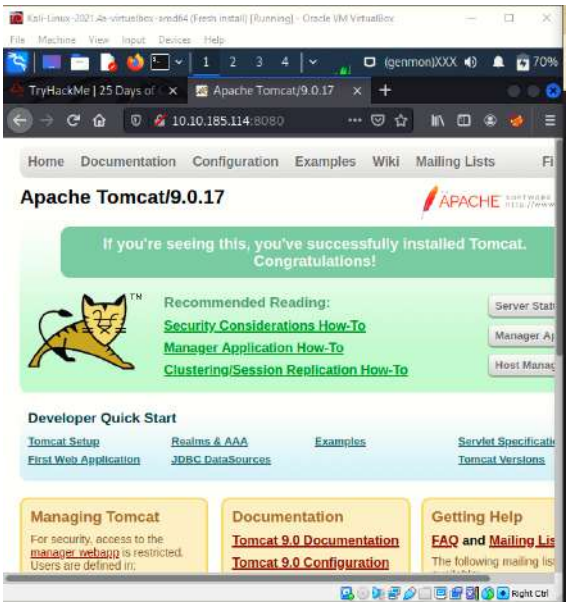
**Tools used:** Terminal, FireFox

**Solution/Walkthrough:**

Question 1: What is the version number of the web server?

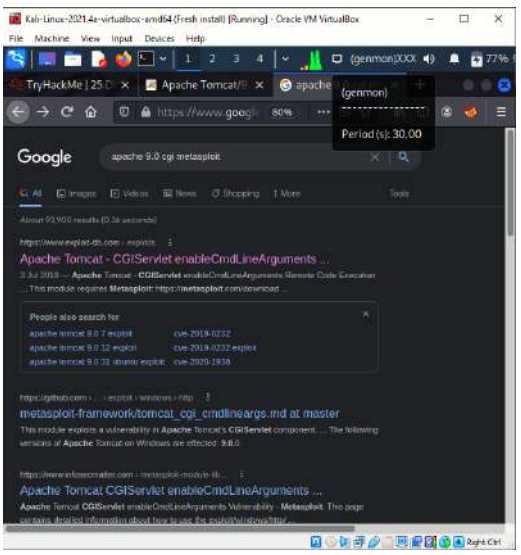
Use nmap to identify the port number. In Firefox, use id number and port number for http-proxy which is 8080 and press enter. Then, the version number of the web server appeared.

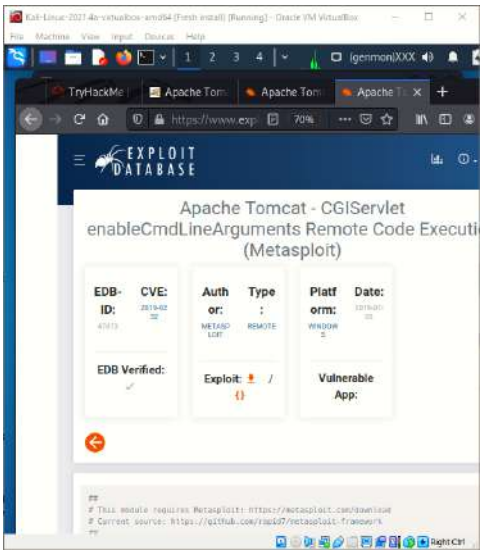



Question 2: What CVE can be used to create a Meterpreter entry onto the machine?

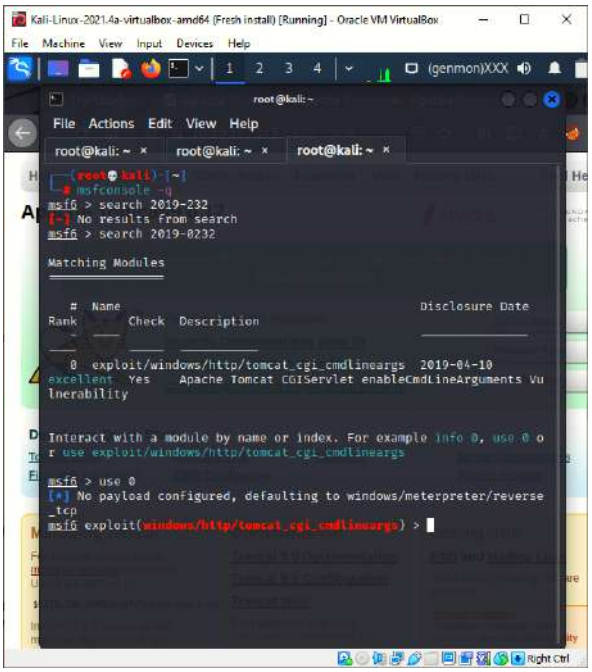
Open a new tab in Firefox and search for Apache 9.0 cgi metasploit. Open the first link and the CVE that can be used is CVE-2019-0232.

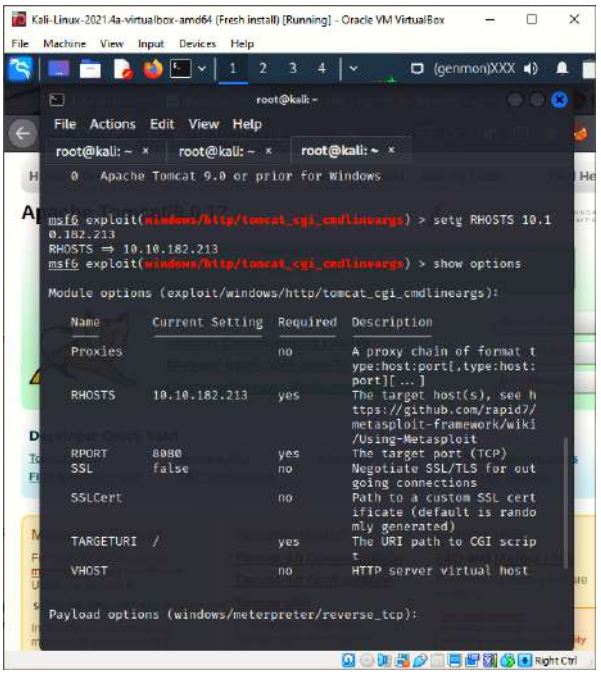


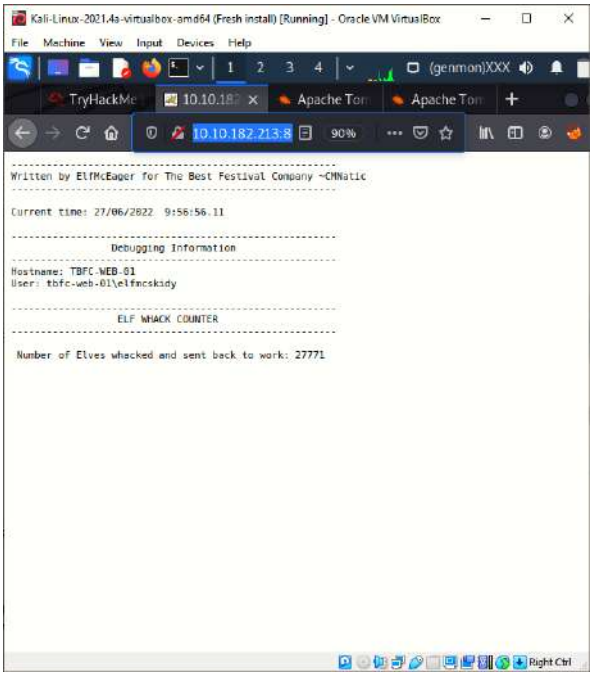
Question 3: What are the contents of flag1.txt ?

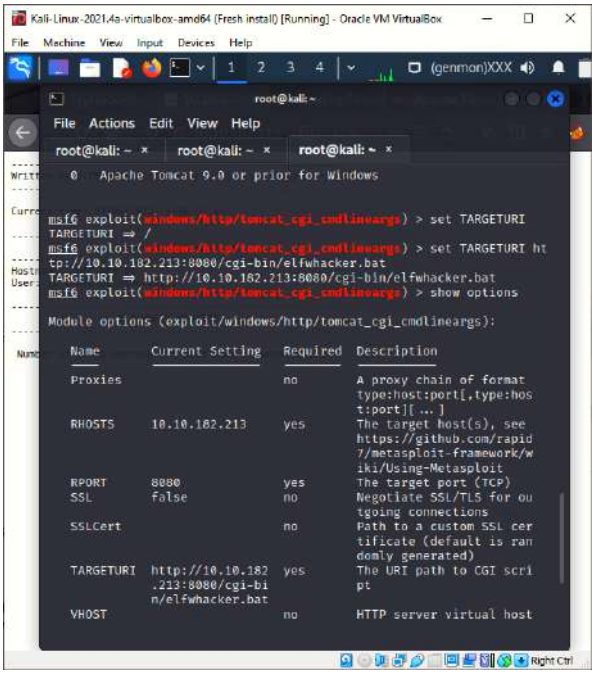
Open a new tab terminal, we use metasploit and search command with the CVE number. After its running, it shows that exploit/windows/http/tomcat/cgilineargs. Then we entered use 0 and it stated that no payload was configured. We enter show options to see the current setting. Then, we set the RHOST.



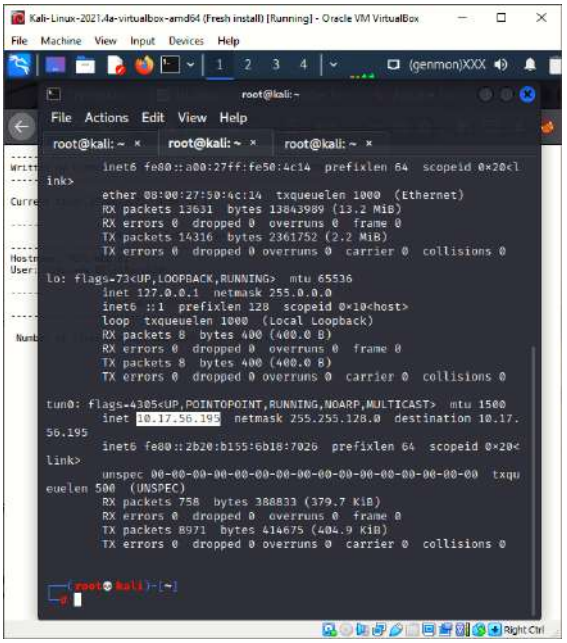



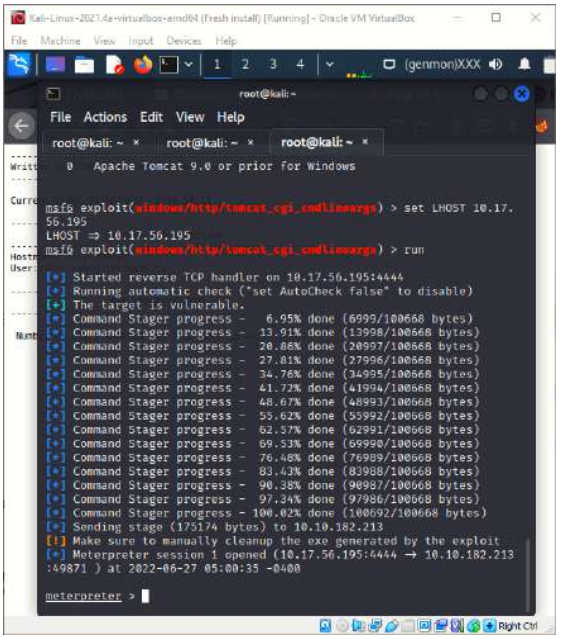

In Firefox, we add /cgi-bin/elfwhacker.bat behind the port number and press enter. The script is shown. Then copy the url and paste in the terminal with the set TARGETURI command and press enter.



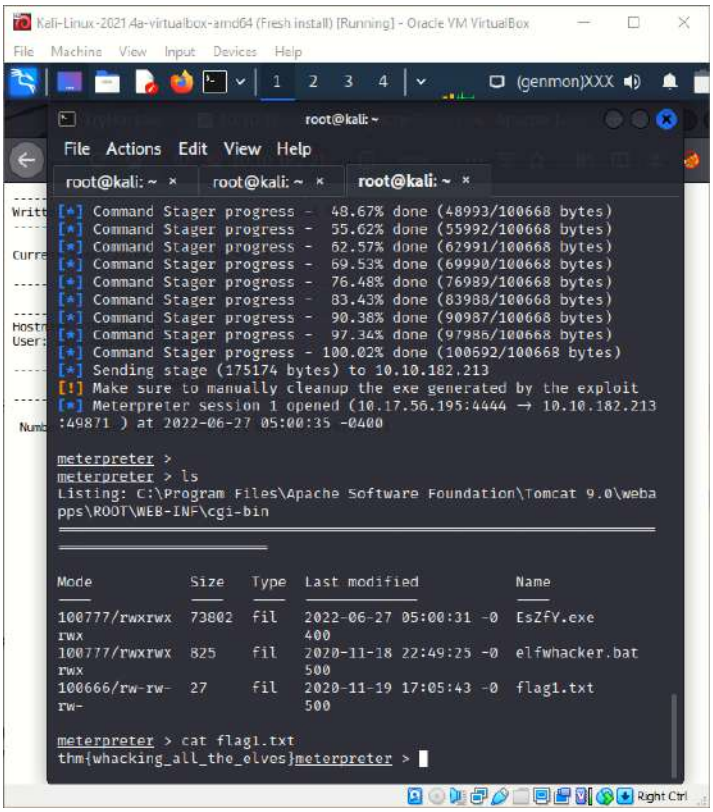



In the new tab of the terminal, we use the ifconfig command to find the ip number. then , use the set LHOST command followed by the ip number and run. It's seeking the target and we have set the Metasploit settings.



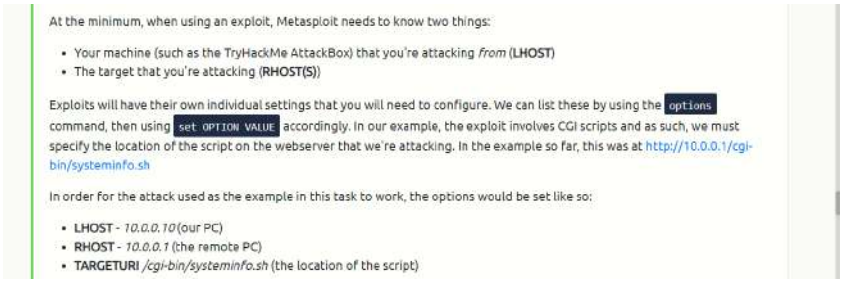



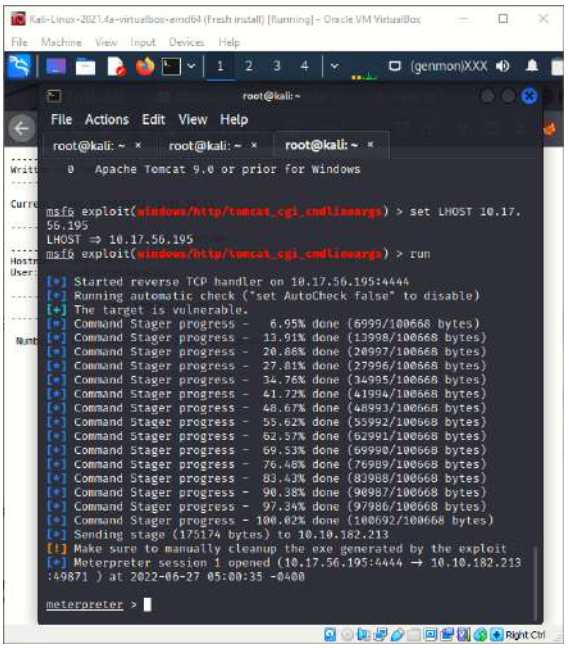

We enter ls command and it shows flag1.txt. Next, we enter cat flag1.txt and the flag is displayed.

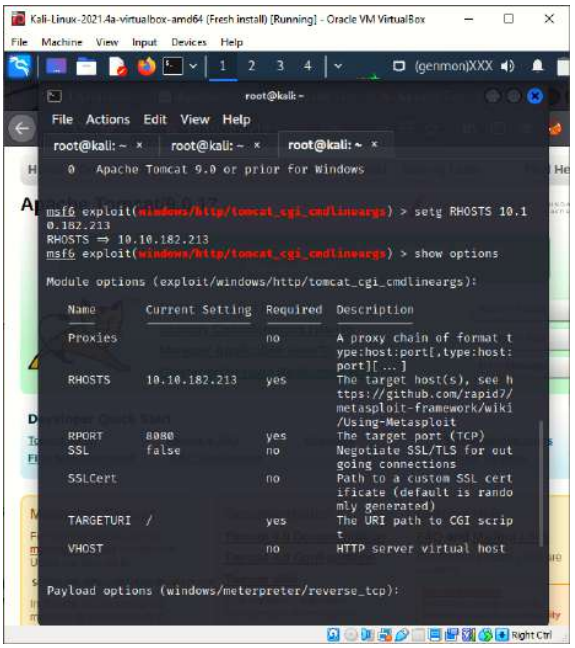


Question 4: What were the Metasploit settings you had to set?

The Metasploit we had to set was LHOST in order for us to know the machine that we are attacking and RHOST in order for us to know the target that we are attacking.




Throughout process:
In the targeted machine, to find the port number, use nmap. In Firefox, enter the id number and port number for http-proxy, which is 8080. The web server's version number then showed. Open a new Firefox tab and look for Apache 9.0 cgi metasploit. After we press enter, open the first link to find the CVE that we are looking for and CVE can be used is CVE-2019-0232. Open a new terminal tab and enter metasploit and the search command with the CVE number. It displays exploit/windows/http/tomcat/cgilineargs after running. Then we typed in use 0, and it said that no payload was specified. To see the current setting, we enter display options. Then, we set the RHOST. We add /cgi-bin/elfwhacker.bat behind the port number and hit enter in Firefox. The script is shown. Then copy the url and paste it into the terminal using the set TARGETURI command, then hit enter. We use the ifconfig command in the new tab of the terminal to find the IP address. Then, run the set LHOST command, followed by the IP address. It's looking for the target, and we've configured Metasploit. We type ls and it displays flag1.txt. The flag is shown once we enter cat flag1.txt. We had to set up Metasploit using LHOST to identify the machine we were attacking and RHOST to identify the target we were targeting.

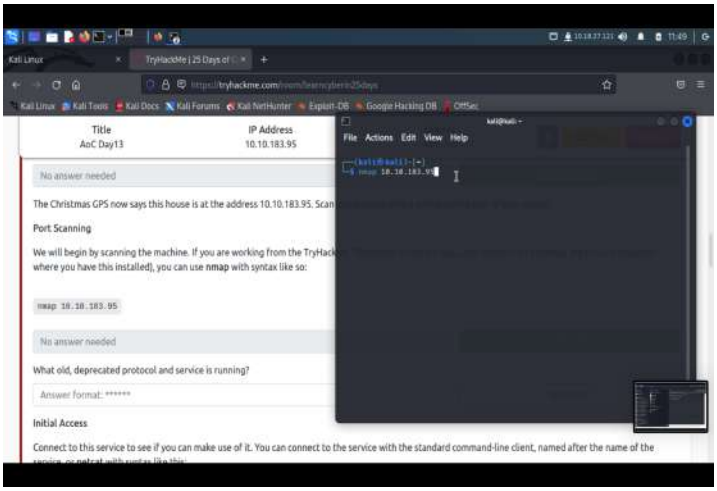
# Day 13 - Networking Coal for Christmas.

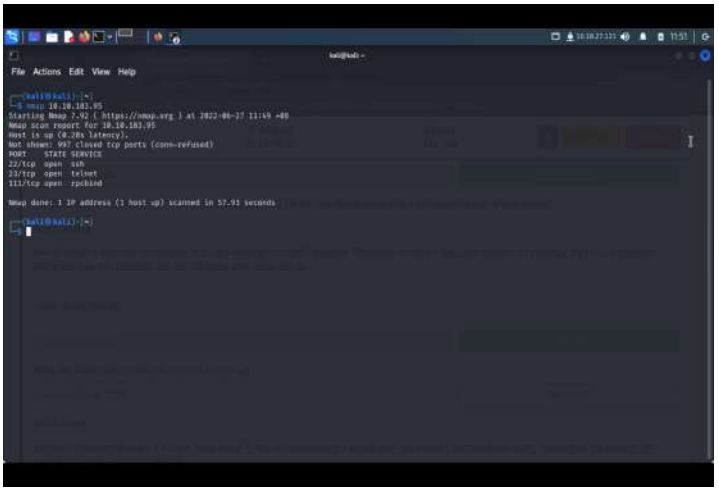
**Tools used: Kali Linux, Firefox, Terminal**

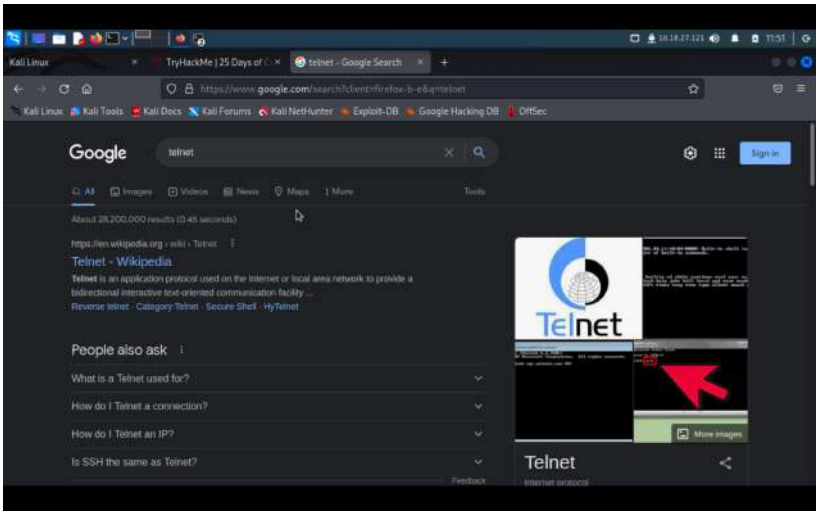
**Solution/Walkthrough:**

Question 1: What old, deprecated protocol and service is running?

By typing nmap with the machine IP address, we manage to receive port,state and service. According to research in  firefox, telnet was the one which was shown as protocol.

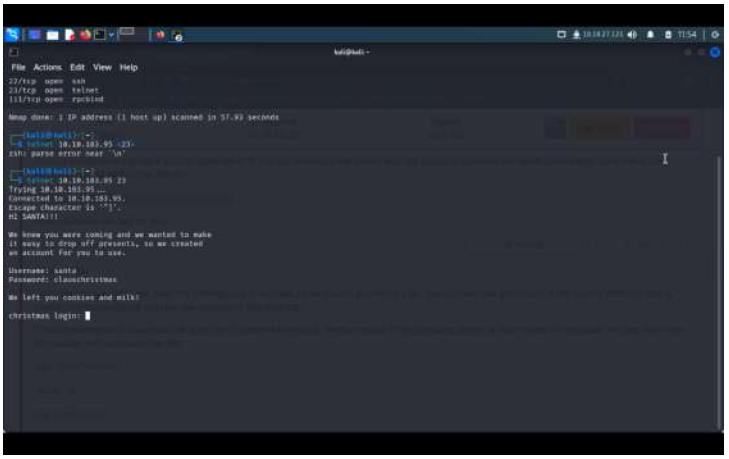


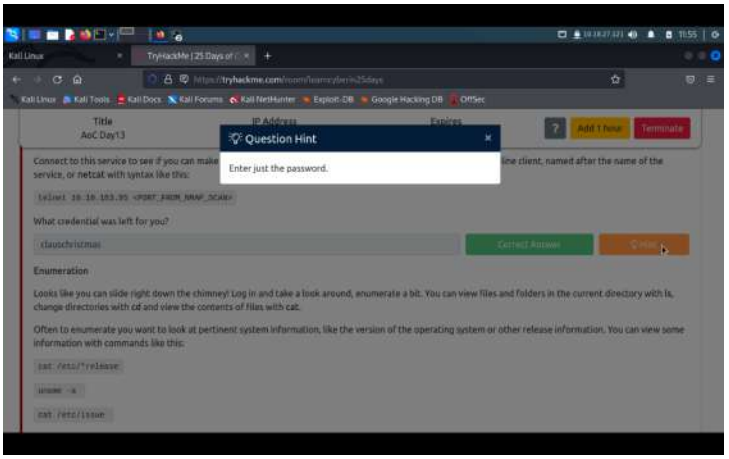





Question 2: What credential was left for you?

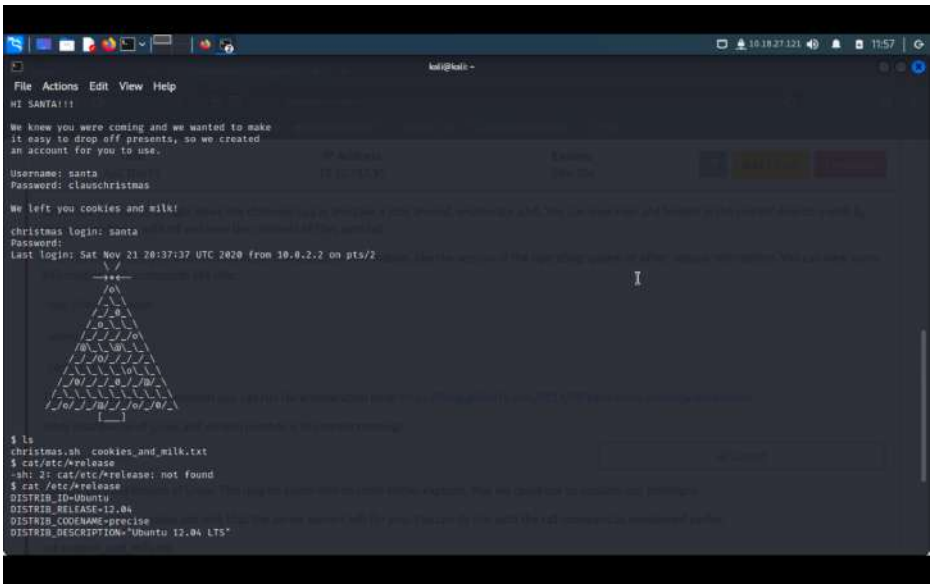
By typing telnet, the machine ip address and the port number of telnet, we received the log in details of santa and the password.



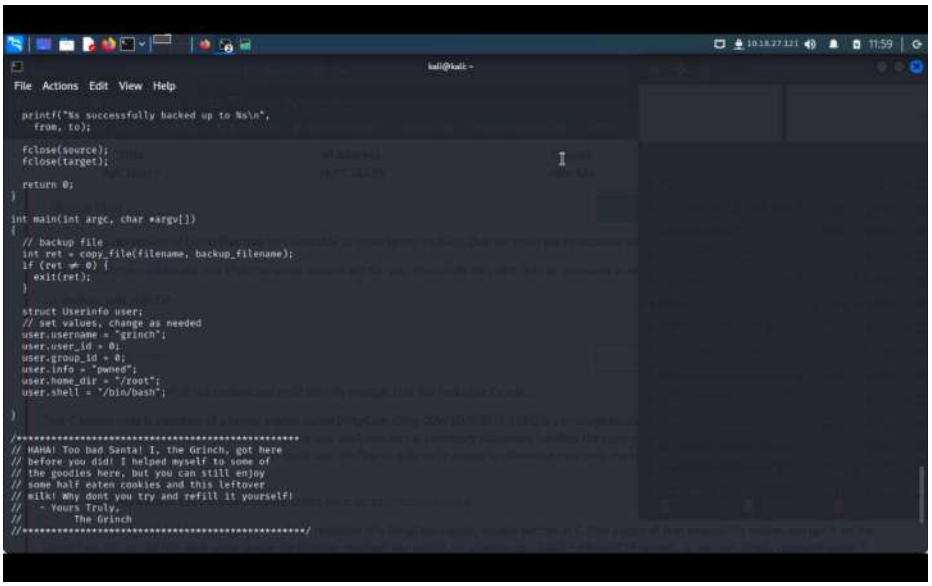

Question 3: What distribution of Linux and version number is this server running?

Next we log in to the ‘christmas login’ and we receive the distribution ID and the version number by copying and pasting the following command from TryhackMe.



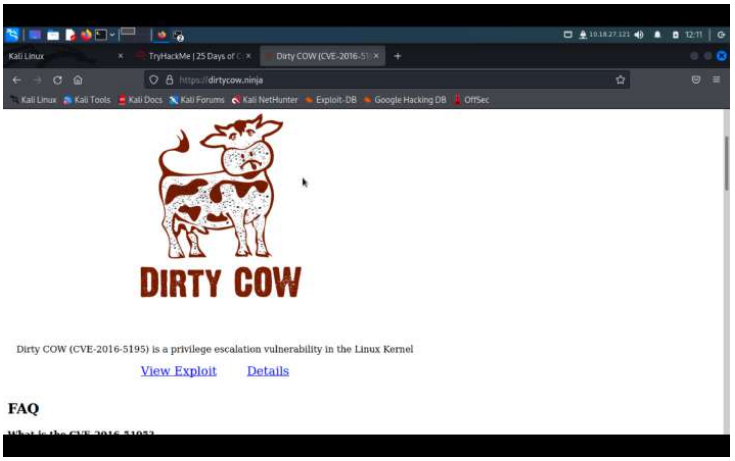
Question 4: Who got here first?

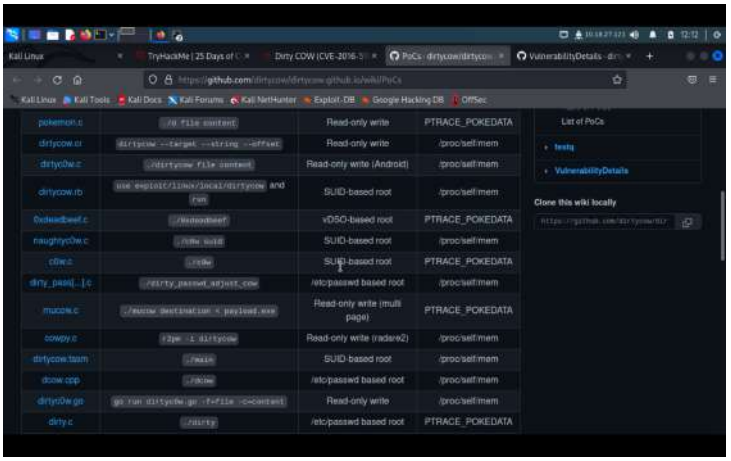
By typing the command, cat cookies_and_milk.txt, we received the following result and a ‘message’ from Grinch stating that he got here first.

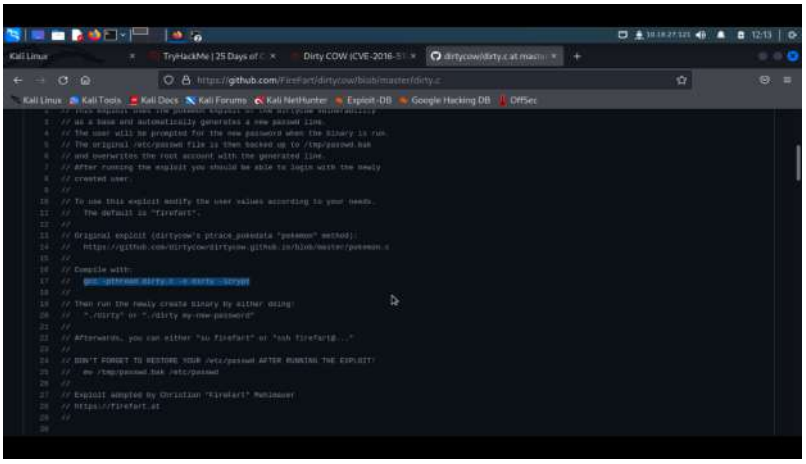



Question 5: What is the verbatim syntax you can use to compile, taken from the real C source code comments?

We navigate to the link given in the TryhackMe, navigating me to The Dirty Cow website. By clicking on the dirty.c, we received a whole coding for a new file and also a command to compile.

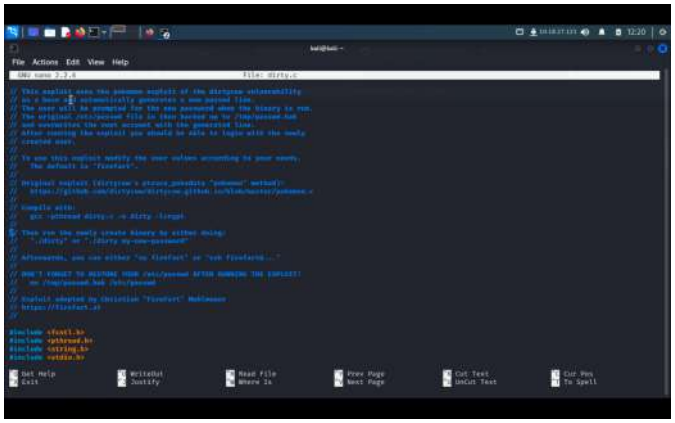


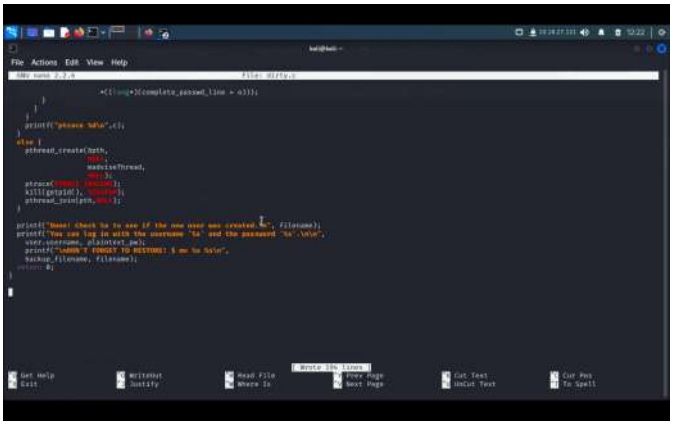



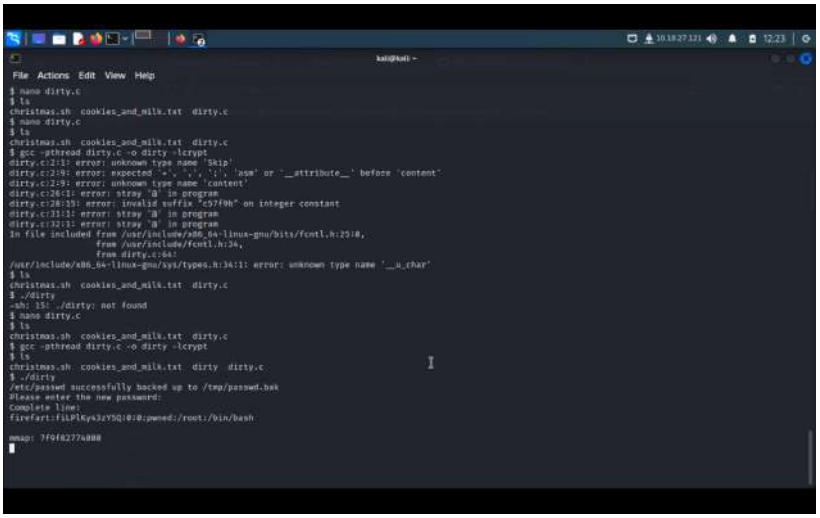


Question 6: What "new" username was created, with the default operations of the real C source code?

By creating a new file called dirty.c with a command nano, we managed to link the file with the compile command and get the new username called ‘firefart’.

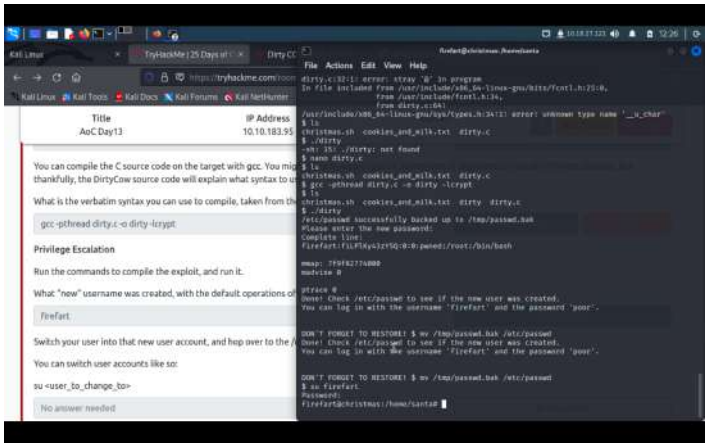


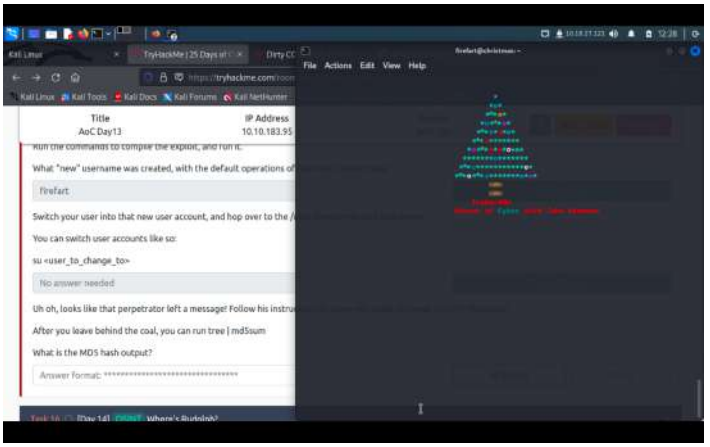




Question 7: What is the MD5 hash output?

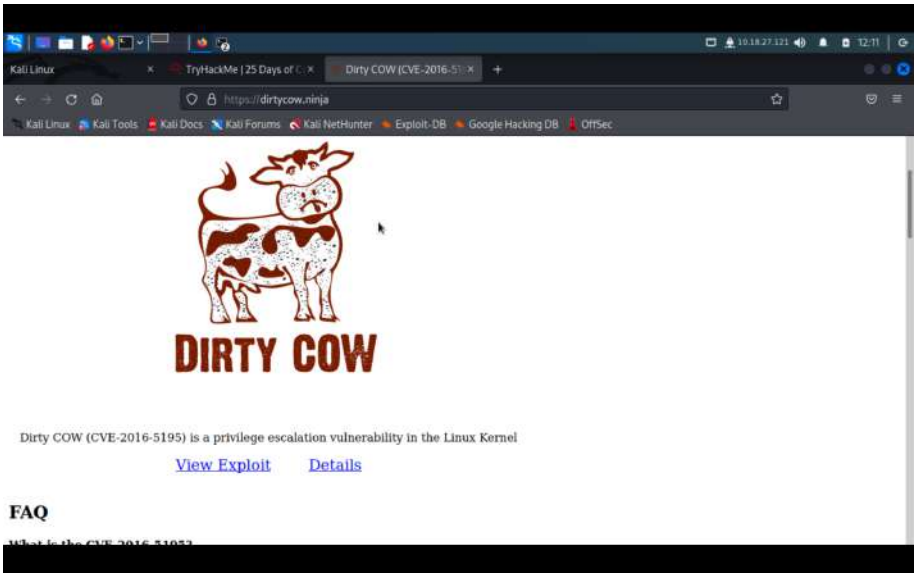
By using command ‘su’, we set the username to firefart and set it to our own password and we managed to get into the christmas directory. We were shown a christmas tree however we exit and by navigating the message from Grinch and cat it, we received a message from Grinch. By following the instructions by Grinch, we managed to get the MD5 hash output by creating a coal file by using a command touch and get the hash output by using command ‘tree | midsum’ .





Question 8: What is the CVE for DirtyCow?

We get the CVE from the website, The Dirty Cow.



Throughout process:

By using Kali Linux, we opened Terminal to start day 13. By ‘nmap’ to the machine IP address we managed to connect to the TryhackMe. When we connected, we were shown some ports from the machine IP address where we use telnet since it was a protocol as we searched it in Firefox. We connected to the service (telnet) by using telnet MACHINE_IP <PORT_FROM_NMAP_SCAN>, and we were provided with some credentials such as username or password. However, according to the hint given by TryhackMe, we have to provide a password for the answer. Then, we login using santa username and password, then we type the command given, ‘ cat /etc/*release’ we were provided with distribution id and the version number. After that, by commanding ‘cat cookies_and_milk.txt’ , we received the following result and a ‘message’ from Grinch stating that he got here first. Next, we navigate to the link given in the TryhackMe, navigating me to The Dirty Cow website. By clicking on the dirty.c, we received a whole coding for a new file and also a command to compile. For this part, we are required to create a new file called dirty.c using a demand nano and link the file with the compile command. After pasting the coding, we are required to save the file and exit the directory. When we successfully link the file with ‘cookies_and_milk.txt’, we are required to set up a new password and get the new username called ‘firefart’. Next, by using command ‘su’, we set the username to firefart and set it to our own password and we managed to get into the christmas directory. We were shown a christmas tree however we exit and by navigating the message from Grinch and cat it, we received a message from Grinch. By following the instructions by Grinch, we manage to get the MD5 hash output by creating a ‘coal’ file by using a command touch and get the hash output by using command ‘tree | midsum’ . Lastly, we get the CVE from the website, The Dirty Cow.

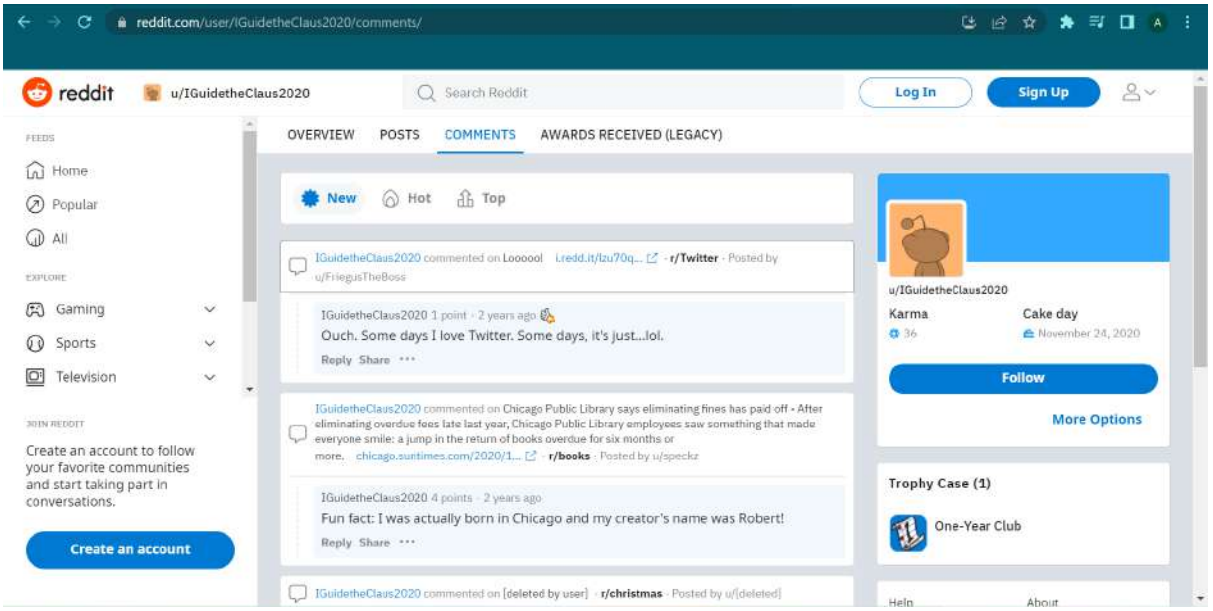
# Day 14 - OSINT Where's Rudolph?

## Tools used: Google Chrome

## Solution/Walkthrough:

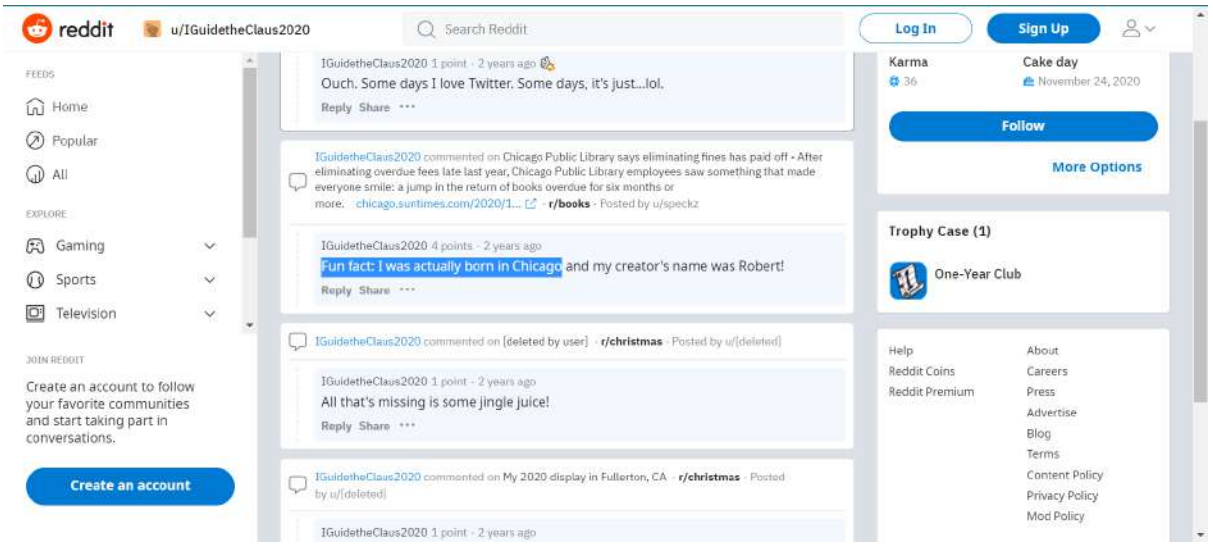
Question 1: What URL will take me directly to Rudolph's Reddit comment history?

Go to reddit.com and search up the username given which is "IGuidetheClaus2020" and click on their profile. Then go to the comments section and copy the url.



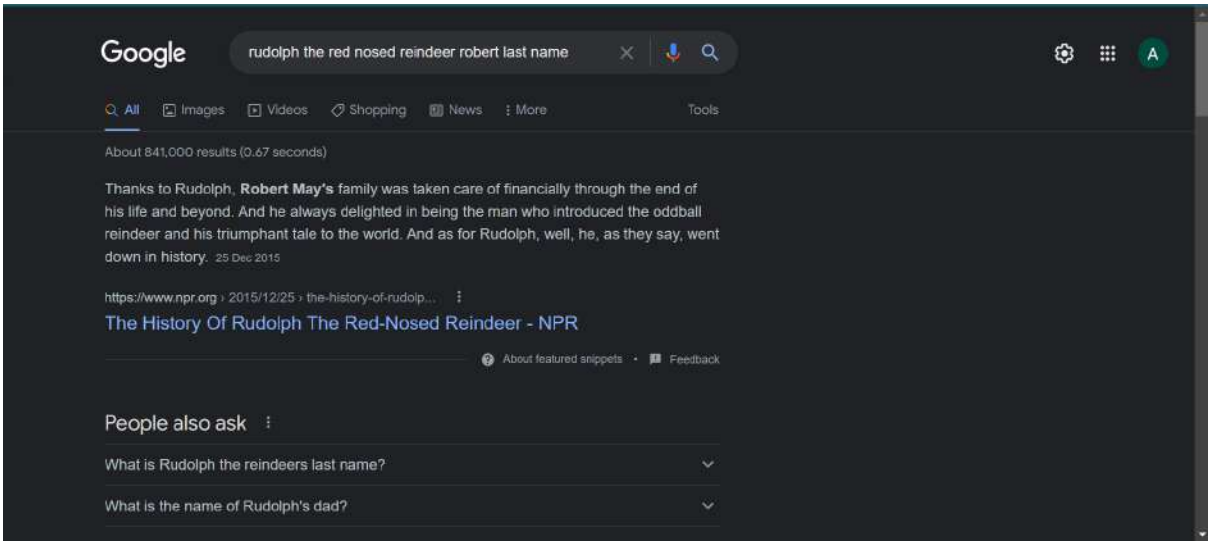

Question 2 : According to Rudolph, where was he born?

In the comment section, Rudolph stated the place where he was born.



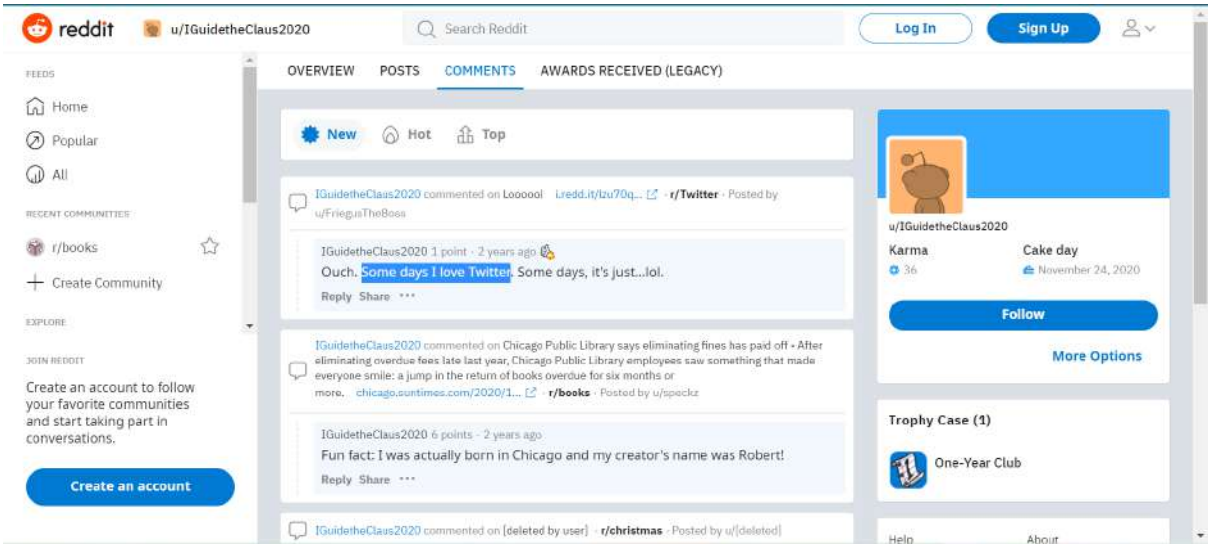
Question 3 : Rudolph mentions Robert. Can you use Google to tell me Robert's last name?

Search up on google.com to find Robert's last name. Make sure to insert Rudolph the red nosed reindeer to obtain results related to him.



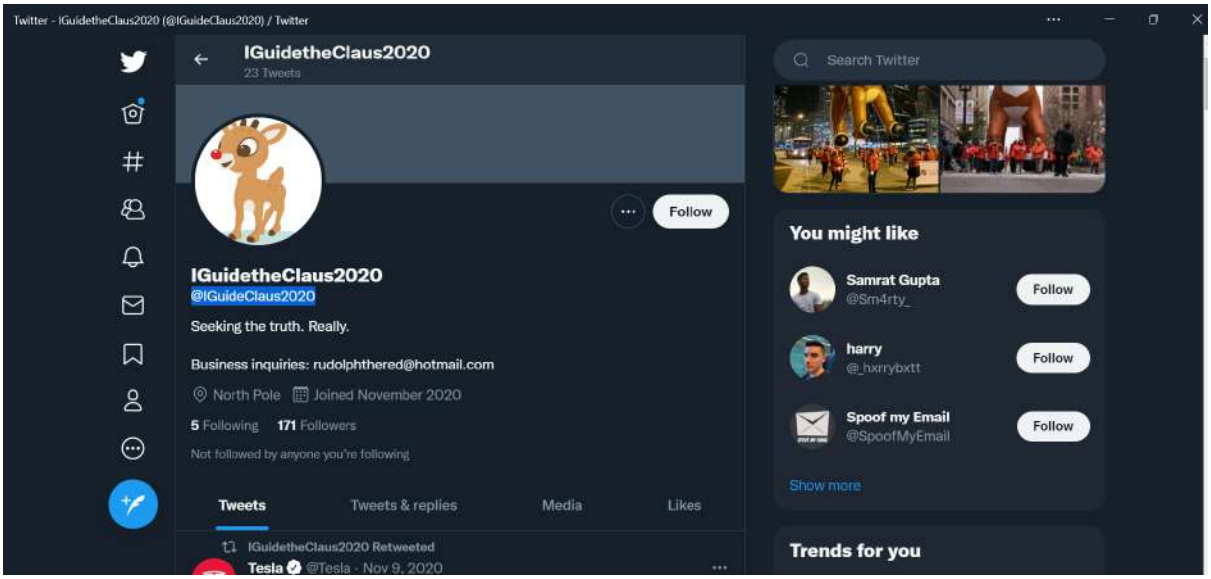

Question 4 : On what other social media platform might Rudolph have an account?

In his reddit comment section, he mentioned the other social media platform that he has.



Question 5 : What is Rudolph's username on that platform?

Go on twitter.com and search using the same username as it will lead to his account. Copy his username as it is different from his display name.

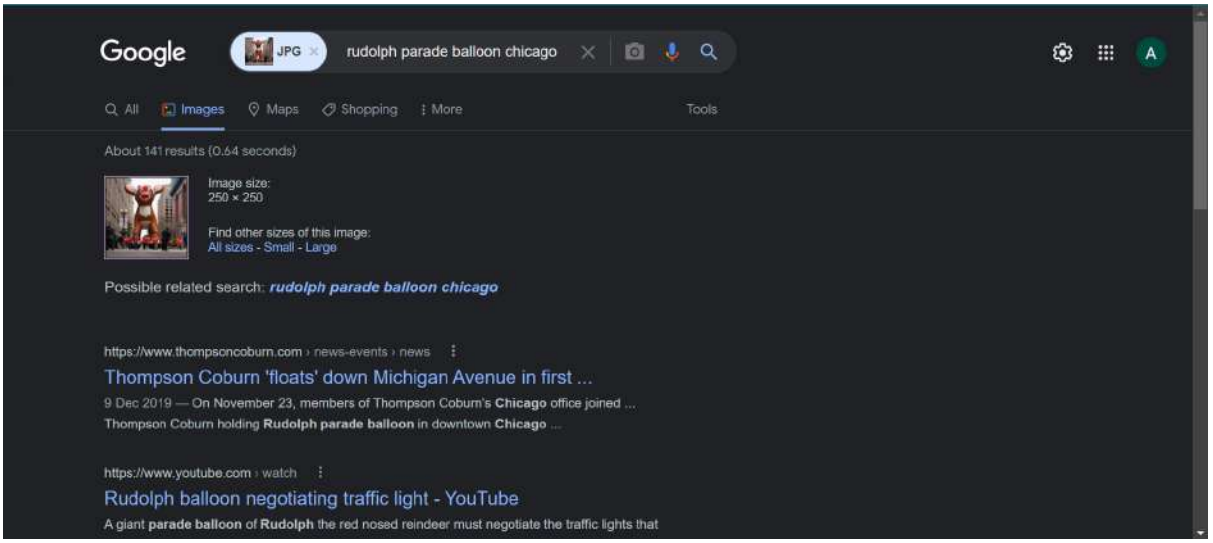



Question 6 : What appears to be Rudolph's favourite TV show right now?

Scroll through Rudolph’s twitter account and we see that he mentioned the show’s name a few times as well as he retweeted tweets about the show.

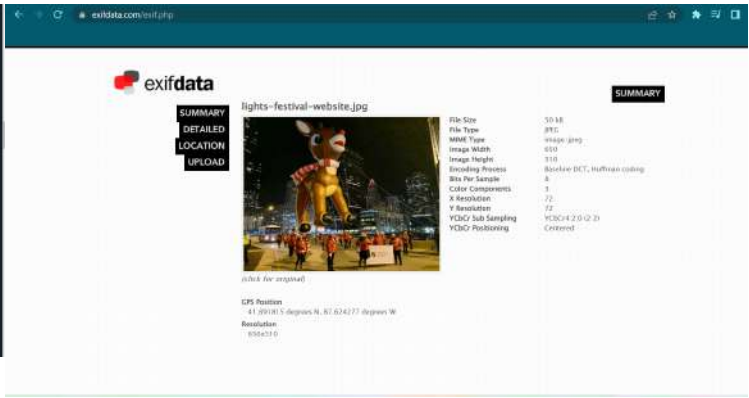
Question 7 : Based on Rudolph's post history, he took part in a parade.  Where did the parade take place?

In one of Rudolph's tweets, he posted a picture of a parade. So by saving that picture and putting it into google image search, we can easily identify where the parade took place.



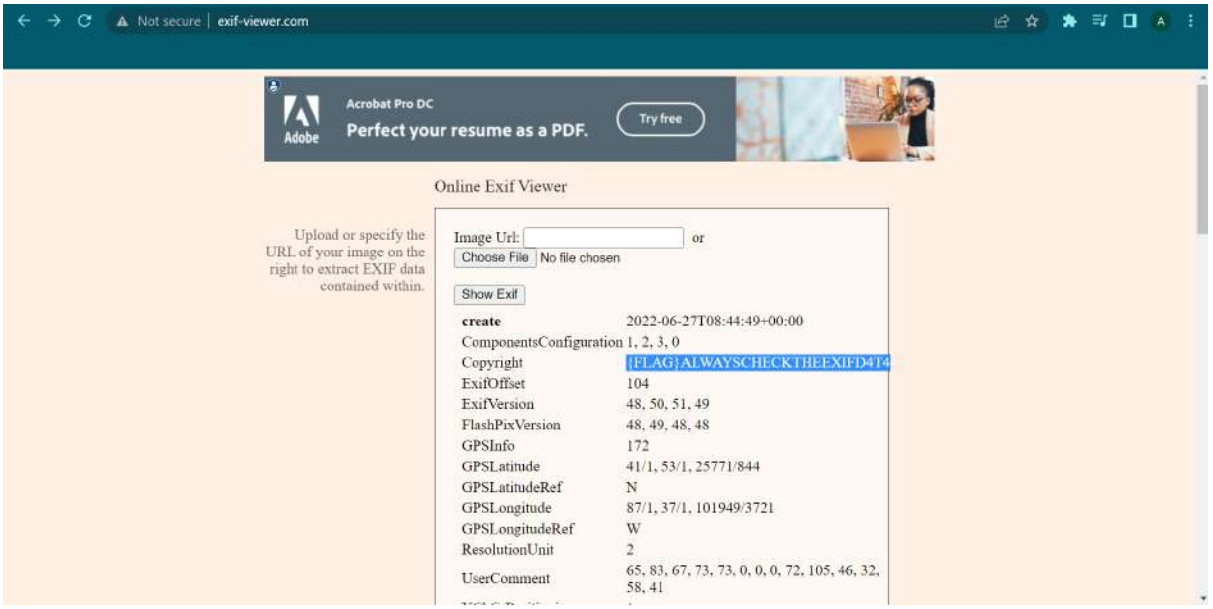

Question 8 : Okay, you found the city, but where specifically was one of the photos taken?

Rudolph had tweeted a higher resolution to one of the photos from the parade, so we downloaded the picture first. Then, we go to exifdata.com, upload the photo and let the information load. There. We can find out the specific location including the longitude and latitude of the picture.

Question 9 : Did you find a flag too?

The flag is located after exif to the picture has fully loaded.

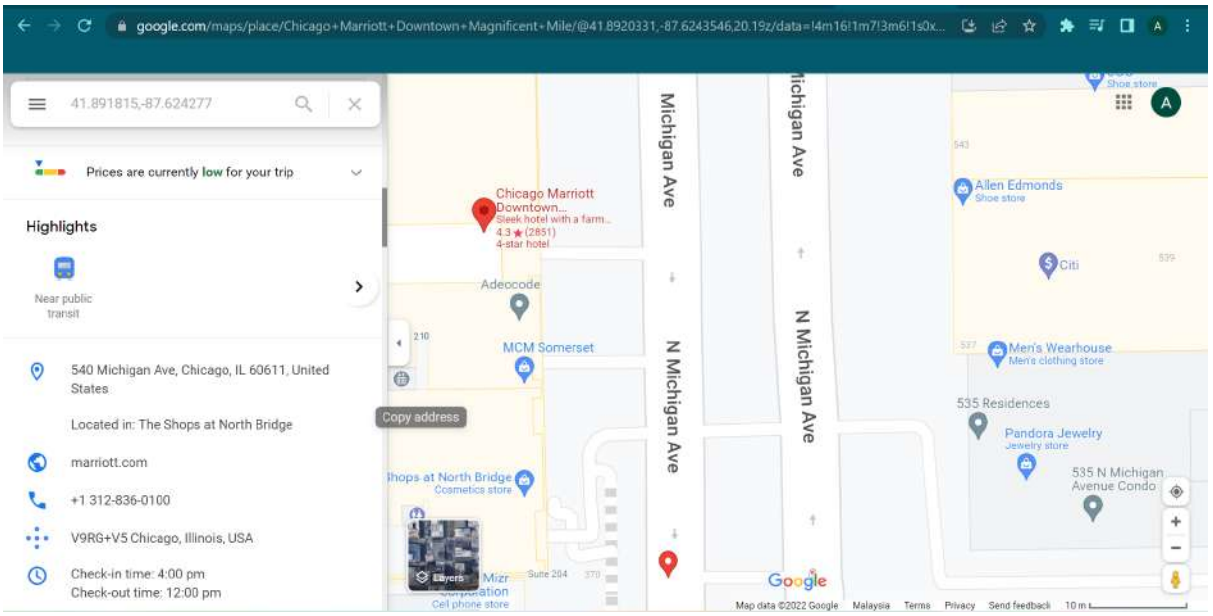



Question 10 : Has Rudolph been pwned? What password of his appeared in a breach?

Go to sylla.sh and type in email:rudolphthered@hotmail.com to find information about Rudolph's email address and there, we found the password.

Question 11 : Based on all the information gathered. It's likely that Rudolph is in the Windy City and is staying in a hotel on Magnificent Mile. What are the street numbers of the hotel address?

Paste the longitude and latitude coordinates that we have obtained into google and click onto maps. Zoom into the location until we see a hotel since that is most likely the place where Rudolph stayed at as he mentioned. Then click onto the hotel location and find the street number.




Throughout process:

First, go to reddit.com and search up the username given which is “IGuidetheClaus2020” and click on their profile. Then go to the comments section and copy the url. In the comment section, Rudolph stated the place where he was born. Then, search up on google.com to find Robert’s last name. Make sure to insert Rudolph the red nosed reindeer to obtain results related to him. To find Rudolph’s other social media platform, go to his reddit comment section again, and find where he mentioned the other social media platform that he has. Next, go on twitter.com and search using the same username as it will lead to his account. Copy his username as it is different from his display name. In one of Rudolph’s tweets, he posted a picture of a parade. So by saving that picture and putting it into google image search, we can easily identify where the parade took place. Rudolph had tweeted a higher resolution to one of the photos from the parade, so we downloaded the picture first. Then, we go to exifdata.com, upload the data and let the information load. There, we can find out the specific location including the longitude and latitude of the picture. The flag is located after exif to the picture has fully loaded. Next, go to sylla.sh and type in “email:rudolphthered@hotmail.com” to find information about Rudolph’s email address and there, we found the password. Paste the longitude and latitude coordinates that we have obtained into google and click onto maps. Zoom into the location until we see a hotel since that is most likely the place where Rudolph stayed at as he mentioned. Then click onto the hotel location and find the street number.

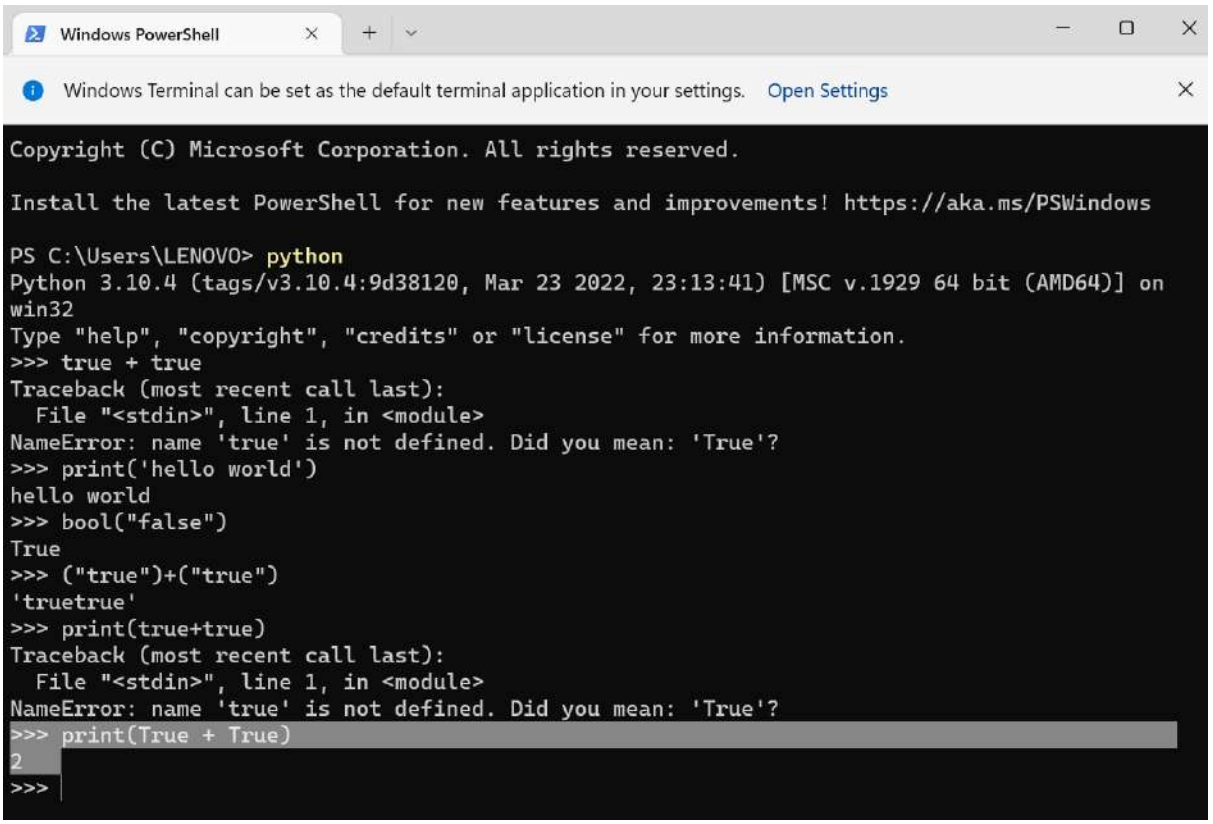
# Day 15 - Scripting There's a Python in my stocking!

**Tools used: Terminal, Visual Studio Code**

**Solution/Walkthrough:**

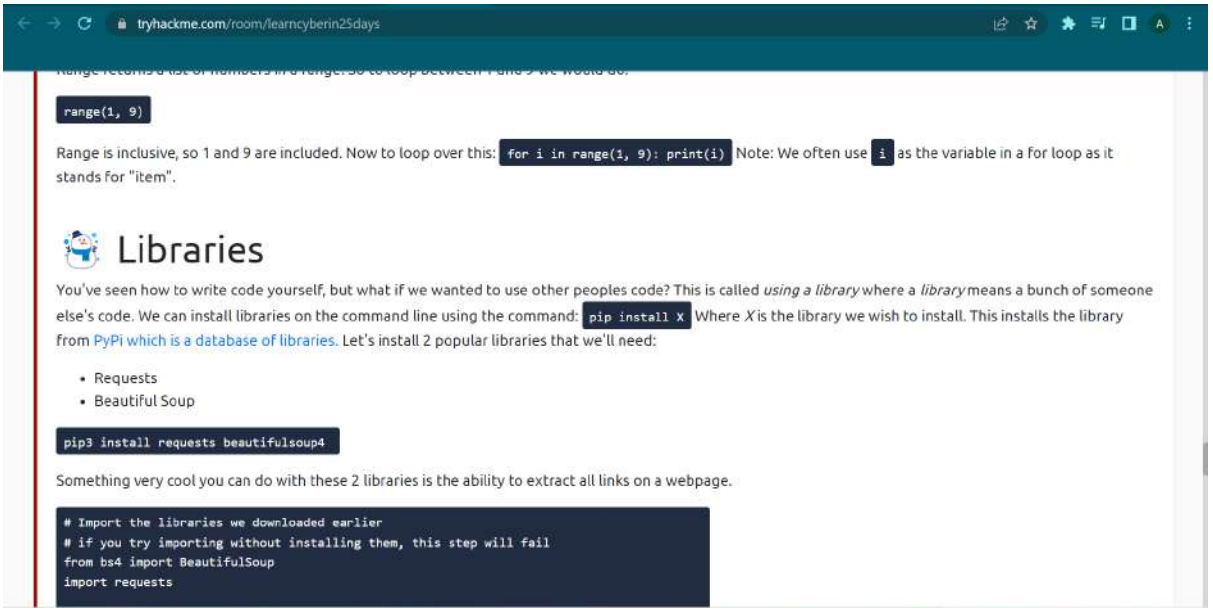
Question 1 : What's the output of True + True?

Open terminal and activate python. Then type in print(True + True)



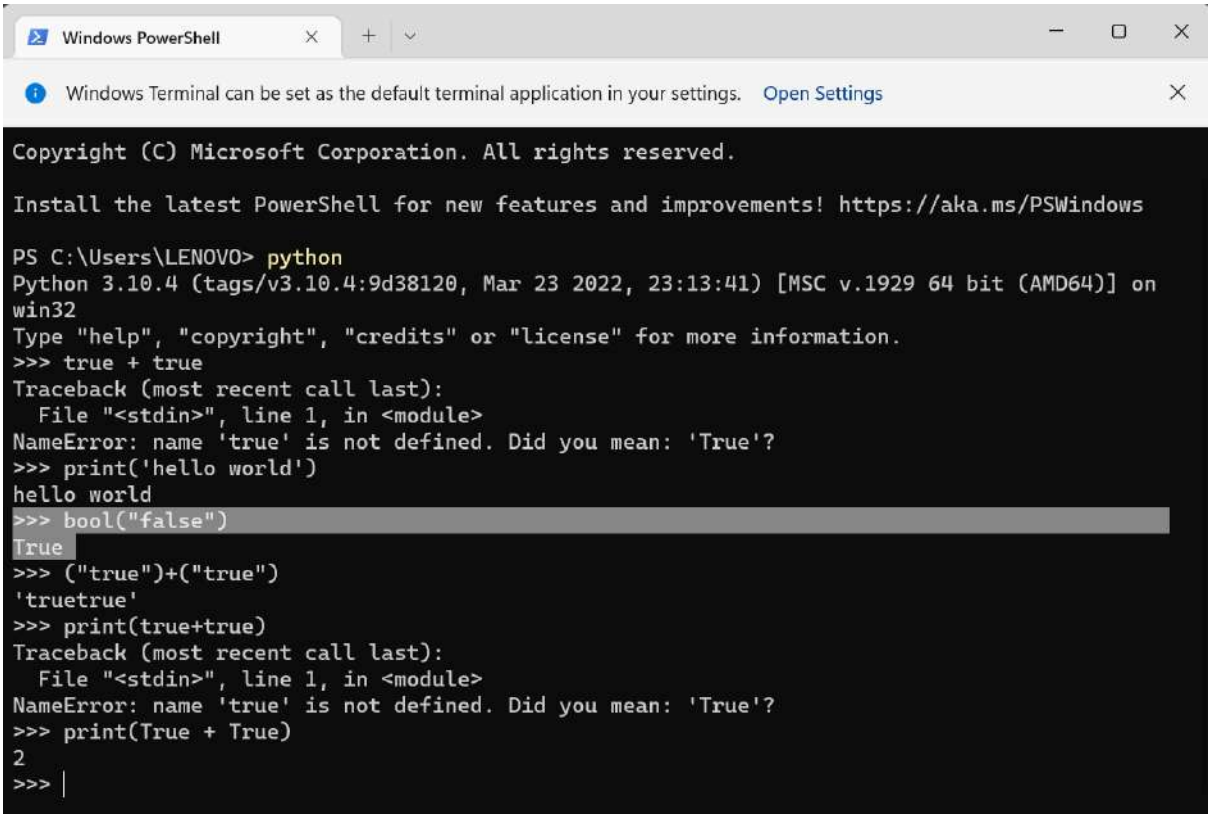
Question 2 : What's the database for installing other people's libraries called?

In tryhackme, there is a paragraph that stated the name of the database



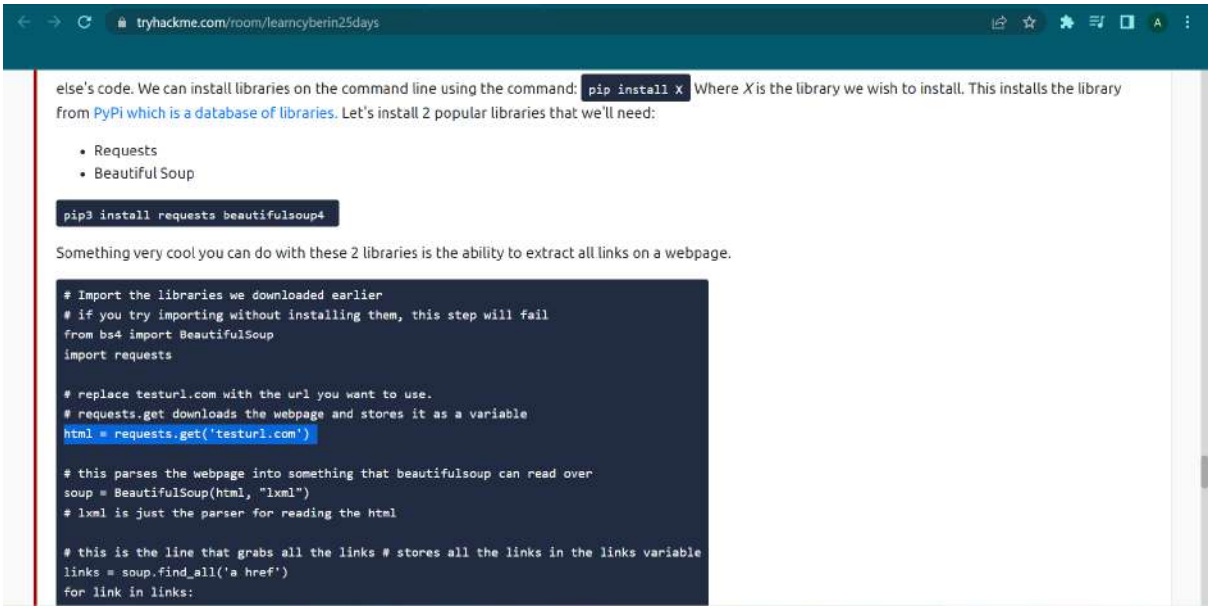

Question 3 : What is the output of bool("False")?

Type bool(“False”) into terminal that has python activated



Question 4 : What library lets us download the HTML of a webpage?

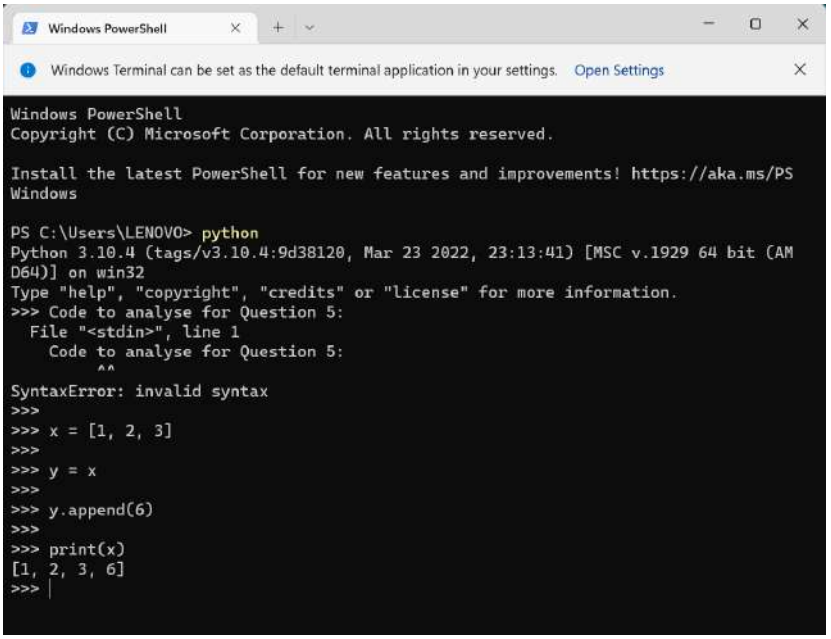
This is also available in one of the paragraphs in tryhackme




Question 5 : What is the output of the program provided in "Code to analyse for Question 5" in today's material?

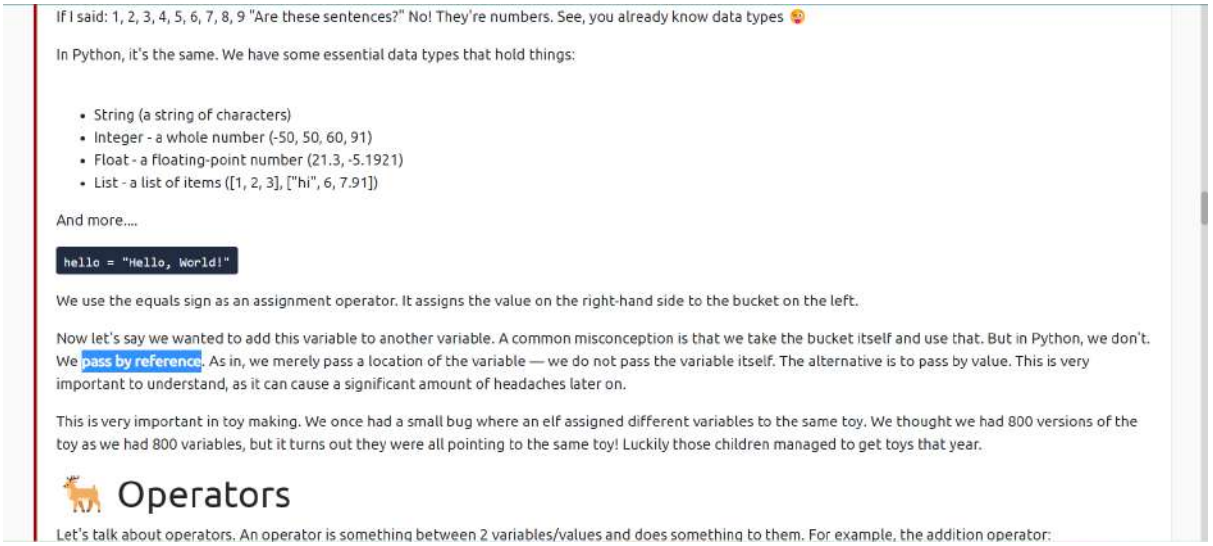
```
x = [1, 2, 3]

y = x

y.append(6)

print(x)
```

Type in this code into terminal and obtain the output



Question 6 : What causes the previous task to output that?

The answer can be obtained in one of the paragraphs in tryhackme as well



If I said: 1, 2, 3, 4, 5, 6, 7, 8, 9 "Are these sentences?" No! They're numbers. See, you already know data types

In Python, it's the same. We have some essential data types that hold things:

- String (a string of characters)
- Integer - a whole number (-50, 50, 60, 91)
- Float - a floating-point number (21.3, -5.1921)
- List - a list of items ([1, 2, 3], ["hi", 6, 7.91])

And more....

```
hello = "Hello, World!"
```

We use the equals sign as an assignment operator. It assigns the value on the right-hand side to the bucket on the left.

Now let's say we wanted to add this variable to another variable. A common misconception is that we take the bucket itself and use that. But in Python, we don't. We pass by reference. As in, we merely pass a location of the variable — we do not pass the variable itself. The alternative is to pass by value. This is very important to understand, as it can cause a significant amount of headaches later on.

This is very important in toy making. We once had a small bug where an elf assigned different variables to the same toy. We thought we had 800 versions of the toy as we had 800 variables, but it turns out they were all pointing to the same toy! Luckily those children managed to get toys that year.

Operators

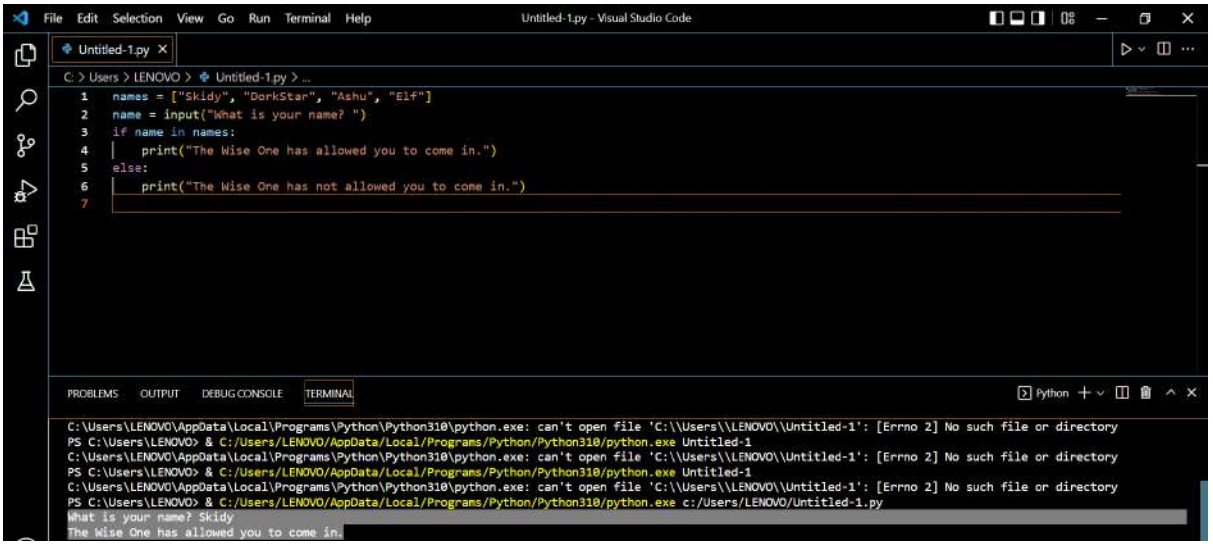
Let's talk about operators. An operator is something between 2 variables/values and does something to them. For example, the addition operator:

Examine the following code:

```
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.")
```

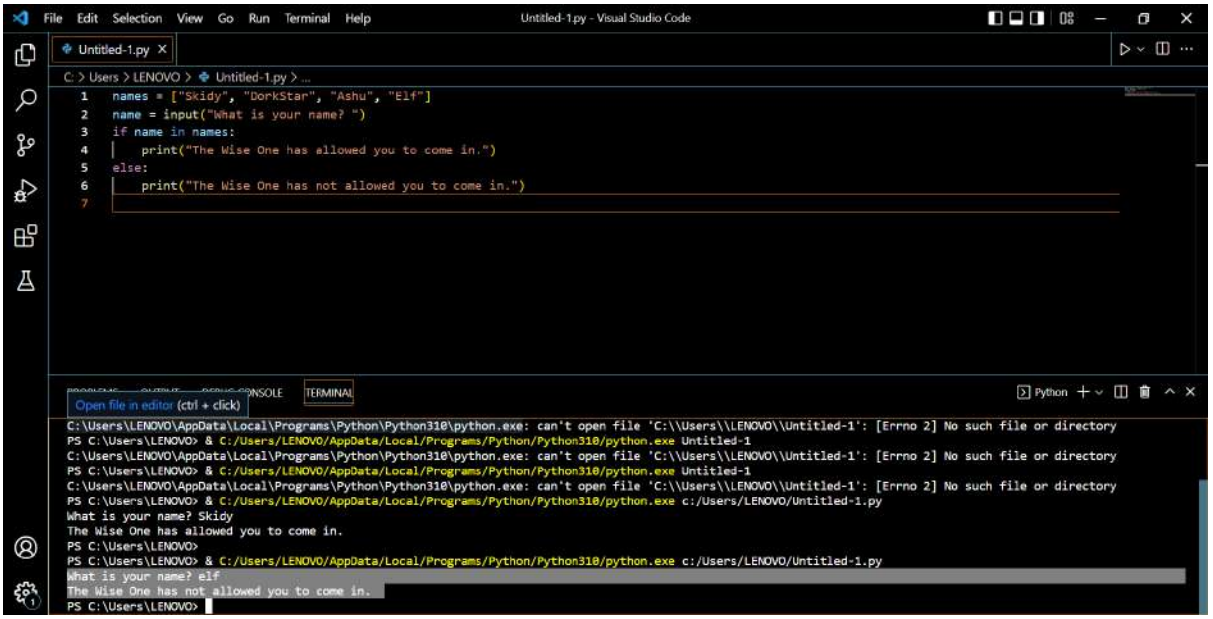
Question 7 : If the input was "Skidy", what would be printed?

Open Visual Studio Code and paste the code into it. Then run the code and put in “Skidy”. The output will be given.



Question 8 : If the input was "elf", what would be printed?

Just like question 7, but type in “elf” into the input. The the output will be shown




Throughout process:
First, we open up the terminal and activate python. Then type in print(True + True). Next, type bool(“False”) and obtain its output. Then, type in the code given and check the output. After that, open Visual Studio Code and put in the code given and run the code. Type in “Skiddy” and “elf” into input and obtain their outputs.