PSP0201 Week 4 Writeup

Group Name: Gold
Members:

ID	Name	Role
1211101707	Nur’aina Binti Ikhwan Moeid	Leader
1211103984	Nur Afreen Junaidah Binti Noorul Mohamed Eliyas	Member
1211101519	Aisyah Binti Ahmad Komarolaili	Member
1211102590	Nur Hanisah Binti Mohd Pauzi	Member

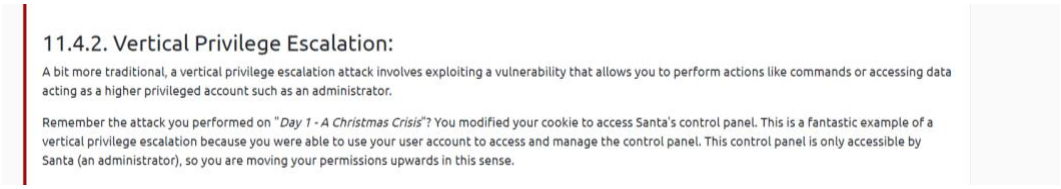
Day 11: Networking – The Rogue Gnome

Tools used: Kali, Firefox

Solution/walkthrough:

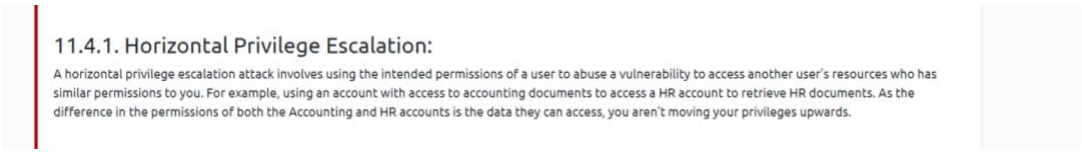
Question 1

What type of privilege escalation involves using a user account to execute commands as an administrator? -vertical



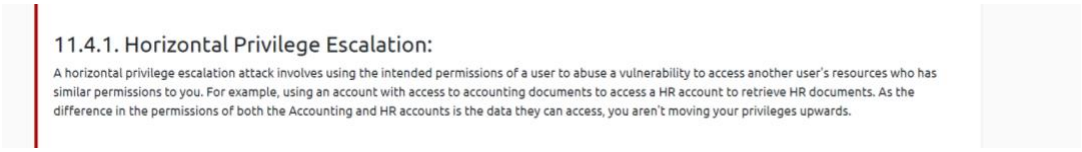
Question 2

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? -horizontal



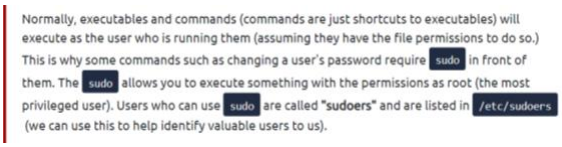
Question 3

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? -horizontal



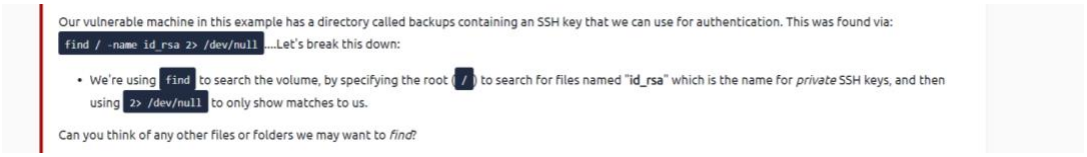
Question 4

What is the name of the file that contains a list of users who are a part of the sudo group? -sudoers



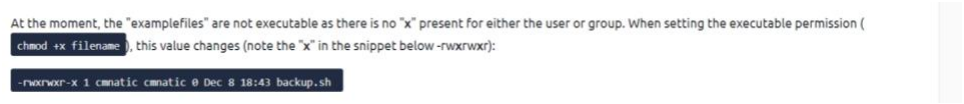
Question 5

What is the Linux Command to enumerate the key for SSH? - find / -name id_rsa 2> /dev/null



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? -chmod +x find.sh

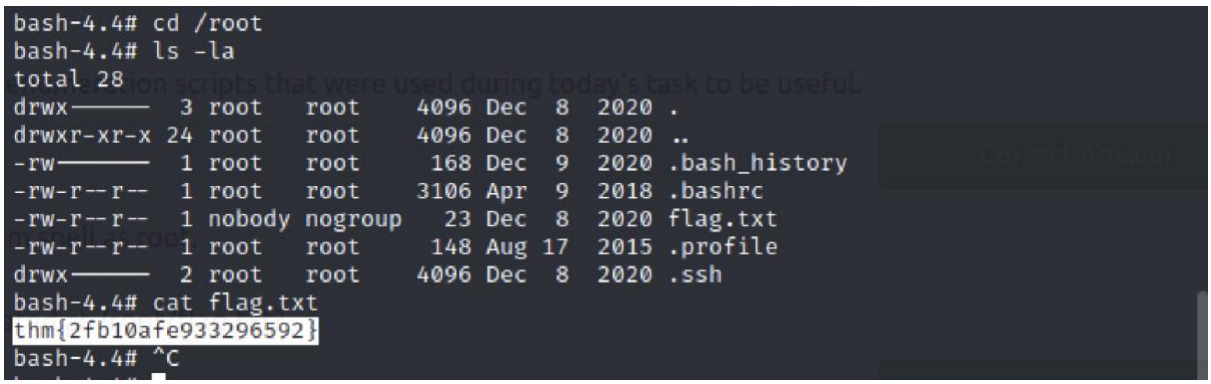


Question 7

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? - python3 -m http.server 9999

Question 8

What are the contents of the file located at /root/flag.txt? - thm{2fb10afe933296592}



Thought Process/ Methodology:

Once we have logged in to the vulnerable instance using the password that was given, we use **find -perm -u=s -type f 2>/dev/null** to find for executables. Once we have located the contents of **/root** and copied it into our directory, we can navigate to **/root** to find the content of **flag.txt**.

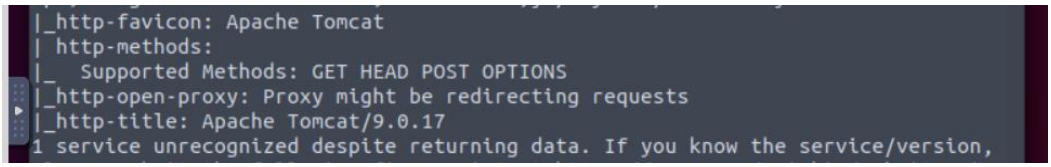
Day 12: Networking – Ready, set, elf.

Tools used: THM AttackBox

Solution/walkthrough:

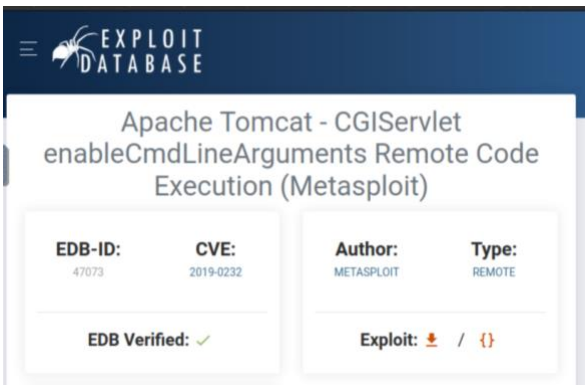
Question 1

What is the version number of the web server? -9.0.17



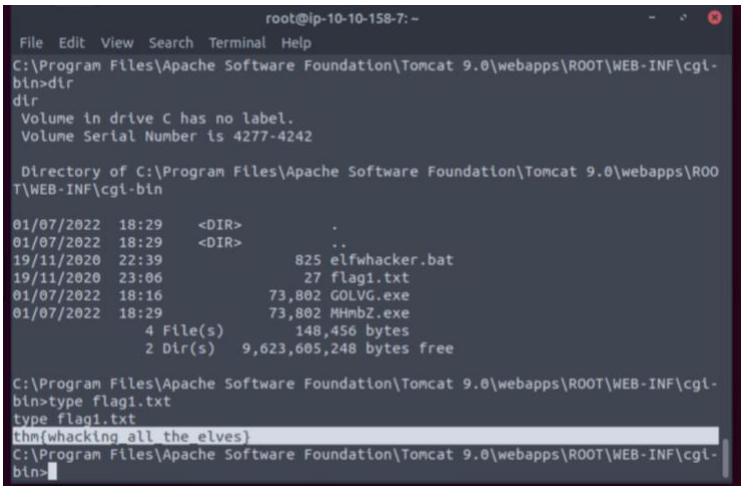
Question 2

What CVE can be used to create a Meterpreter entry onto the machine? - CVE-2019-0232



Question 3

What are the contents of flag1.txt - thm{whacking_all_the_elves}



Question 4

What were the Metasploit settings you had to set? -LHOST, LPORT

Thought Process/ Methodology:

We're using nmap tool on Metasploit to enumerate the web server to get the version number of the web server.Next, using the information given, Apache Tomcat 9.0.17 and CGI we browse it on google we found the CVE that can be used to create a Meterpreter entry onto the machine.On Metasploit Framework we use search command to look up for the exploit module we're going to use and run the exploit to create the session. We then execute command shell followed by command dir to get the contents of flag1.txt.

Day 13: Networking – Coal for Christmas

Tools used: Attackbox, DirtyCow

Solution/walkthrough:

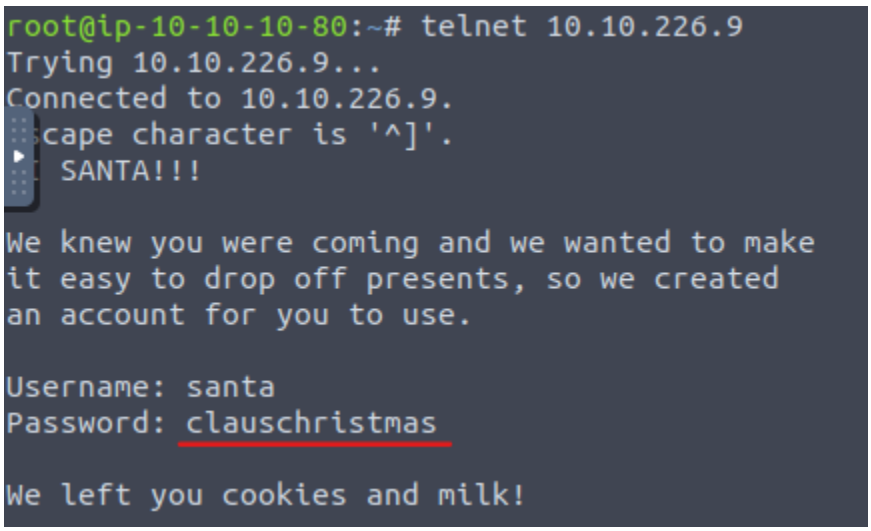
Question 1

What old, deprecated protocol and service is running? - telnet

```
telnet 10.10.194.194 <PORT_FROM_NMAP_SCAN>
```

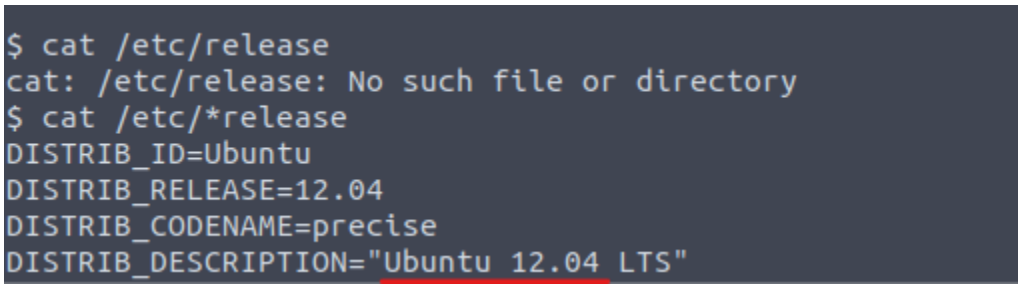
Question 2

What credential was left for you? - clauschristmas



Question 3

What distribution of Linux and version number is this server running? - Ubuntu 12.04



Question 4

Who got here first? - grinch

```
$ cat cookies_and_milk.txt
/**********************************************
// HAHA! Too bad Santa! I, the Grinch, got here
// before you did! I helped myself to some of
// the goodies here, but you can still enjoy
// some half eaten cookies and this leftover
// milk! Why dont you try and refill it yourself!
//    - Yours Truly,
//          The Grinch
//**********************************************/
```

Question 5

What is the verbatim syntax you can use to compile, taken from the real C source code comments? - gcc -pthread dirty.c -o dirty -lcrypt

```
//
// 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"
//
```

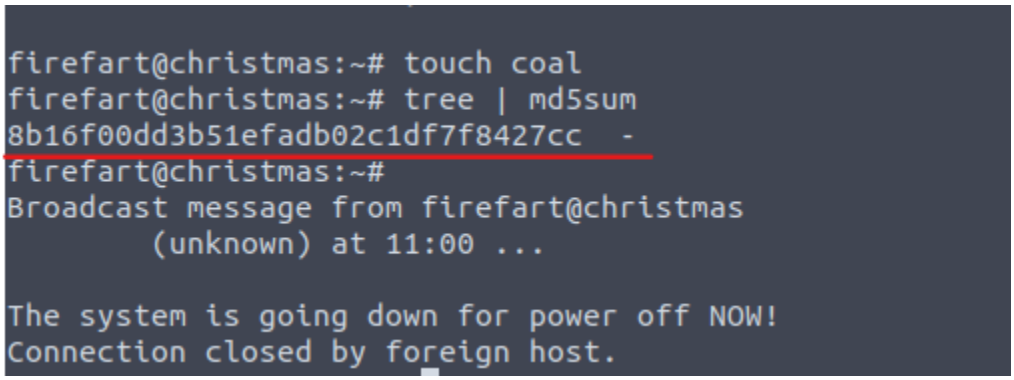
Question 6

What "new" username was created, with the default operations of the real C source code? - firefart

```
^C
$ su firefart
Password:
firefart@christmas:/home/santa# cd /root
firefart@christmas:~# ls
christmas.sh  message_from_the_grinch.txt
firefart@christmas:~# cat message_from_the_grinch.txt
Nice work, Santa!
```

Question 7

What is the MD5 hash output? - 8b16f00dd3b51efadb02c1df7f8427cc -



Question 8

What is the CVE for DirtyCow? - CVE-2016-5195

DirtyCow. Dirty COW (CVE-2016-5195)

Thought Process/ Methodology:

First as usual, start the machine on the attackbox and start deploying. On the terminal and just put all the commands given with the reference given which is dirty cow and just browse the codes there and just continue the steps until all the answers come out based on THM questions.

Day 14: OSINT – Where's Rudolph?

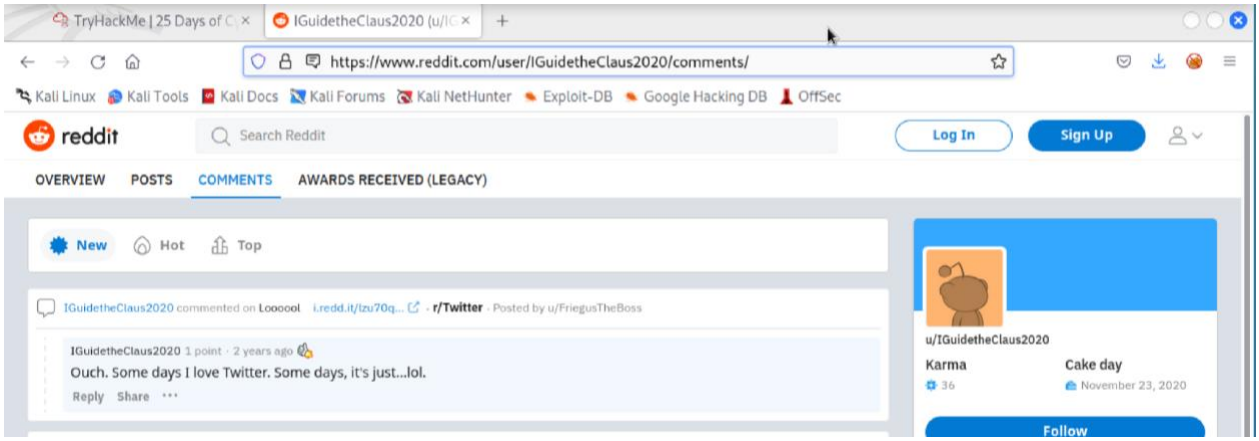
Tools used: Firefox

Solution/walkthrough:

Question 1

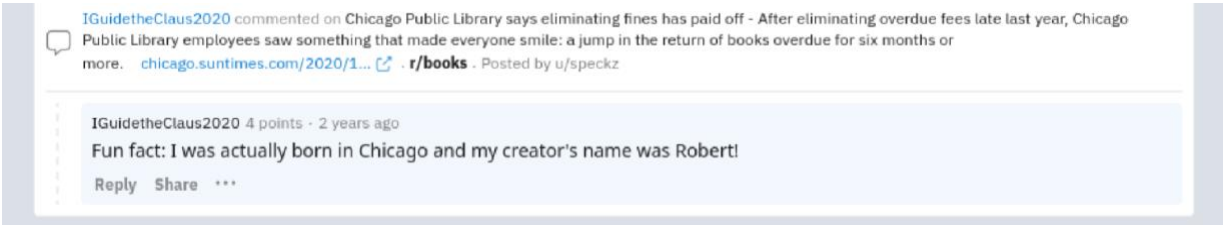
What URL will take me directly to Rudolph's Reddit comment history? -

https://www.reddit.com/user/IGuidetheClaus2020/comments



Question 2

According to Rudolph, where was he born? - Chicago

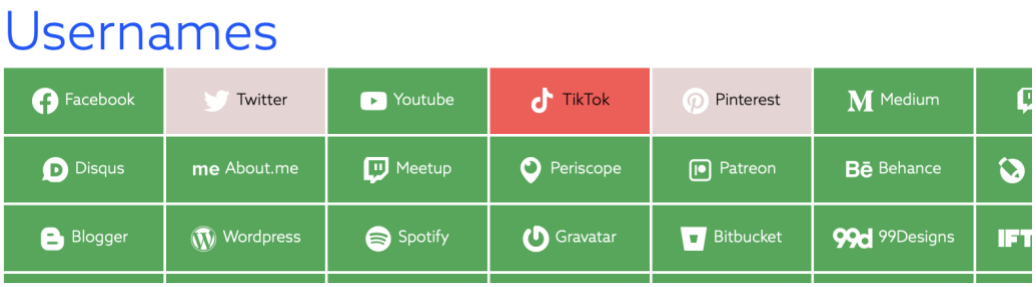


Question 3

Rudolph mentions Robert. Can you use Google to tell me Robert's last name? - May

Question 4

On what other social media platform might Rudolph have an account? - Twitter



Question 5

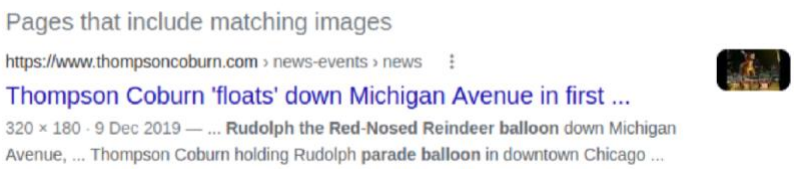
What is Rudolph's username on that platform? - IGuideClaus2020

Question 6

What appears to be Rudolph's favourite TV show right now? - Bachelorette

Question 7

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



Question 8

Okay, you found the city, but where specifically was one of the photos taken? - 41.891815, -87.624277

Question 9

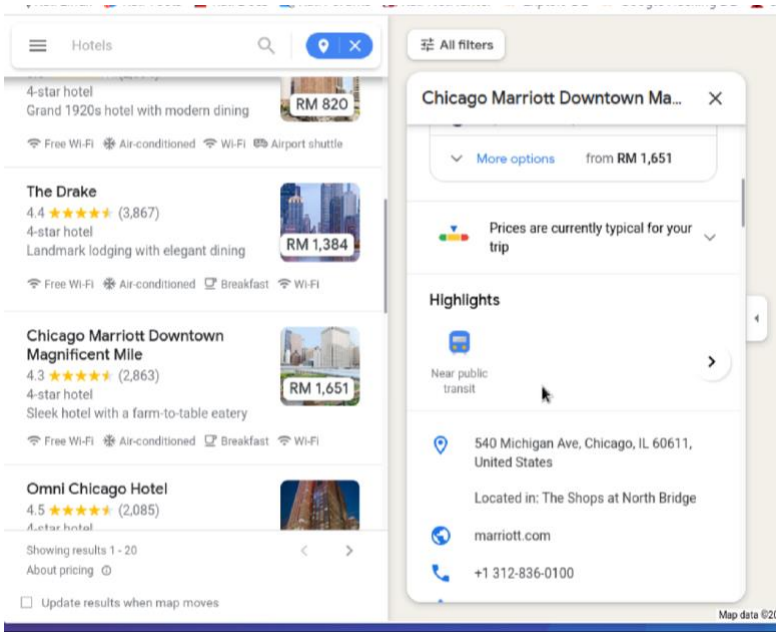
Did you find a flag too? - {FLAG}ALWAYSCHECKTHEEXIFD4T4

Question 10

Q10: Has Rudolph been pwned? What password of his appeared in a breach? - spygame

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? - 540



Thought Process/ Methodology:

OSINT investigation can be done with just browsing the internet. By using certain websites such as https://exifdata.com we can find more detailed information. For example, https://exifdata.com allows us to utilize image EXIF data to uncover critical details, such as exact photo location.

Day 15: Scripting- There's a Python in my stoking!

Tools used: Firefox

Solution/walkthrough:

Question 1

What's the output of True + True? - 2

Question 2

What's the database for installing other peoples libraries called? - PyPi

You've seen how to write code yourself, but what if we wanted to use other peoples code? This is called *using a library* where a *library* means a bunch of someone else's code. We can install libraries on the command line using the command:
`pip install X` Where *X* is the library we wish to install. This installs the library from PyPi which is a database of libraries. Let's install 2 popular libraries that we'll need:

Question 3

What is the output of bool("False")? -True

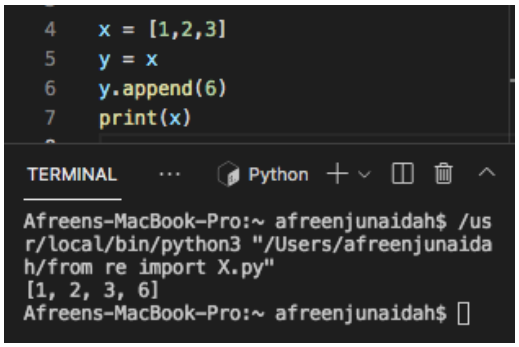
Question 4

What library lets us download the HTML of a webpage? - requests

```
# replace testurl.com with the url you want to use.
# requests.get downloads the webpage and stores it as
a variable
html = requests.get('testurl.com')
```

Question 5

What is the output of the program provided in "Code to analyse for Question 5" in today's material? -[1, 2, 3, 6]

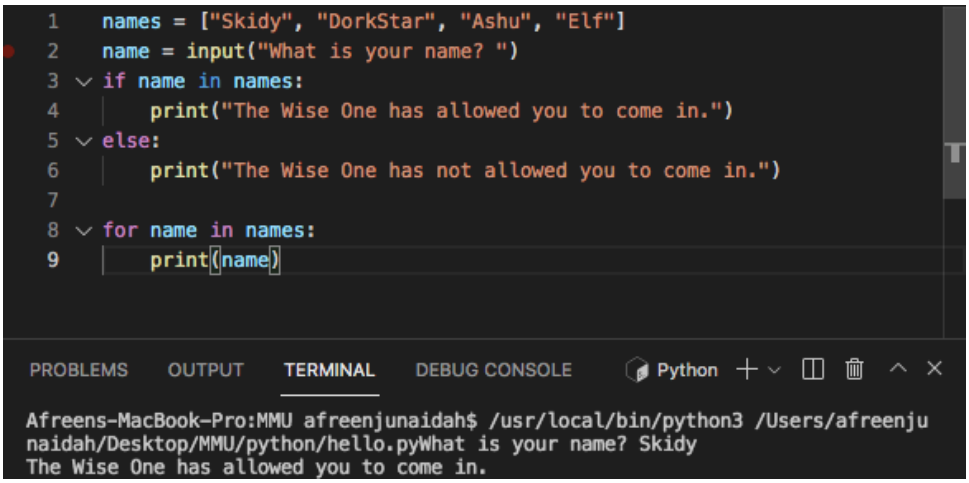


Question 6

What causes the previous task to output that? - Pass by reference

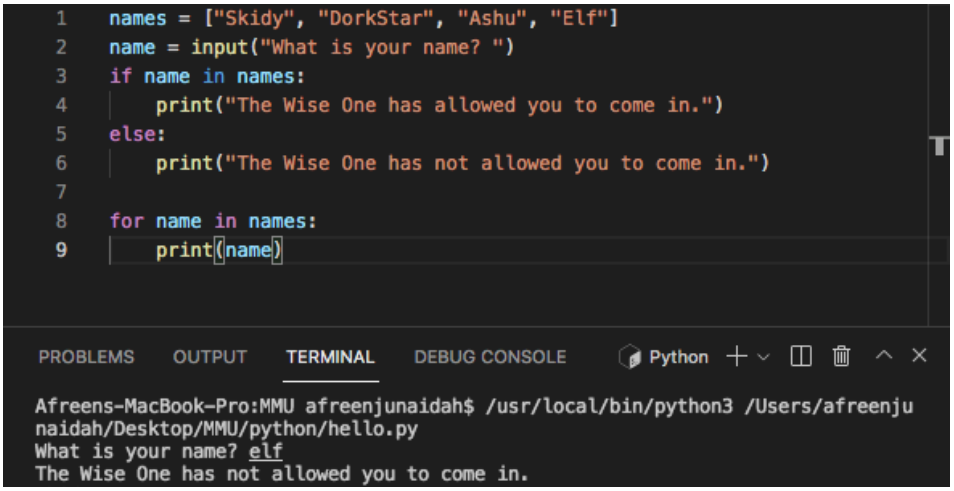
Question 7

If the input was "Skidy", what will be printed? - The Wise One has allowed you to come in.



Question 8

If the input was "elf", what will be printed? - The Wise One has not allowed you to come in.



Thought Process/ Methodology:

We come to understand how python is used. Starting from printing “Hello World” to different functions, variables, operators, booleans, if statements and loops. Libraries can be used to use othe people’s codes and improvise.