Report PSP0201 T2130 Tutorial – Week 4

Group name: **Marceline**

ID	Name	Role
1211100899	Muhammad Shahril Aiman	Leader
1211101533	Muhammad Aniq Fahmi	Member
1211101303	Aiman Faris	Member
1211102759	Muhammad Zaquan	Member

Day 11: The Rouge Gnome: Prelude

Tools used: Attackbox and Firefox

Solution/Walkthrough:

Question 1:

What type of privilege escalation 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?

= Vertical

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 filename find.sh

Question 7:

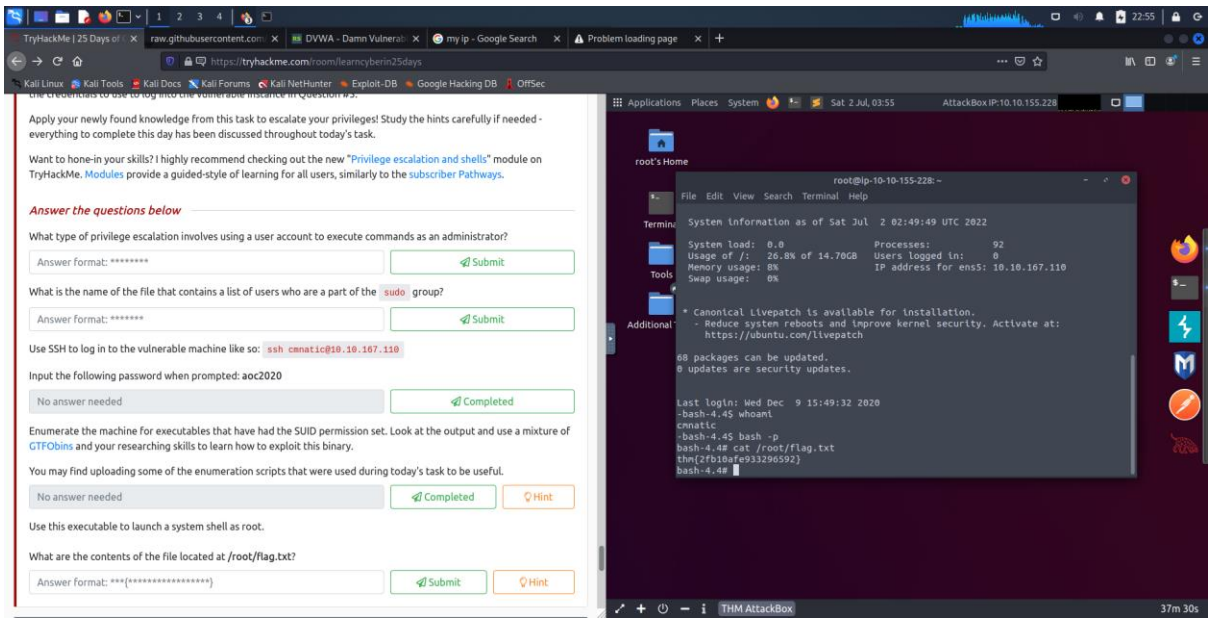
The target machine you gained a foothold into is able to run wget. What command would you use to host a http server using python3 on port 9999?

= python3 -m http.server 9999

Question 8:

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

= thm{2fb10afe933296592}



METHODOLOGY:

To complete day 11, first need to launch the machine and attackbox as usual. Using the command ssh cmnatic@IP_MACHINE, in my case it was ssh cmnatic@10.10.167.110 and I use the password given by THM which is aoc2020. it will say return bash-4.4$. key in -p and then write the command cat/root/flag.txt to find the flag and the answer will be thm{2fb10afe933296592}.

Day 12 - Networking Ready, set, elf.

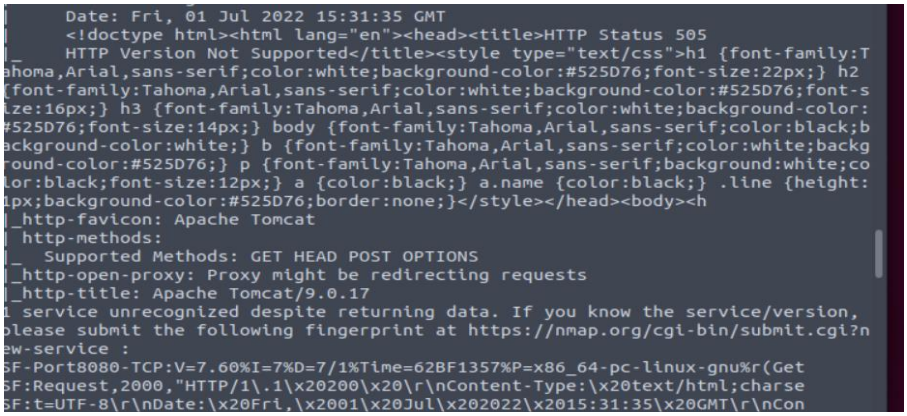
Tools used: AttackBox and FireFox

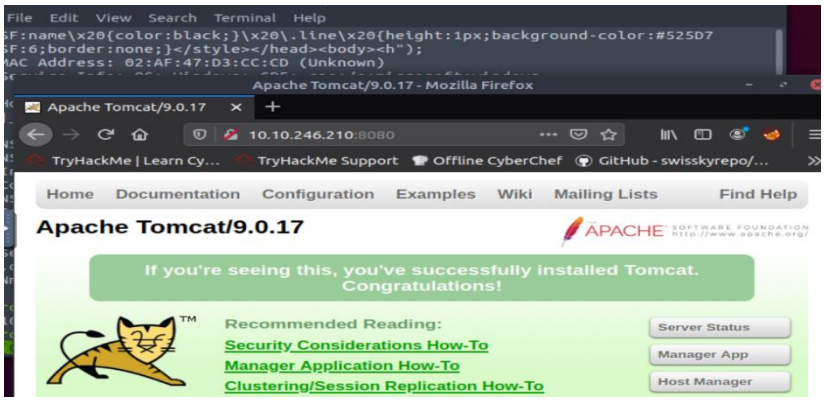
Solution/Walkthrough:

Question 1:

What is the version number of the web server?

= 9.0.17

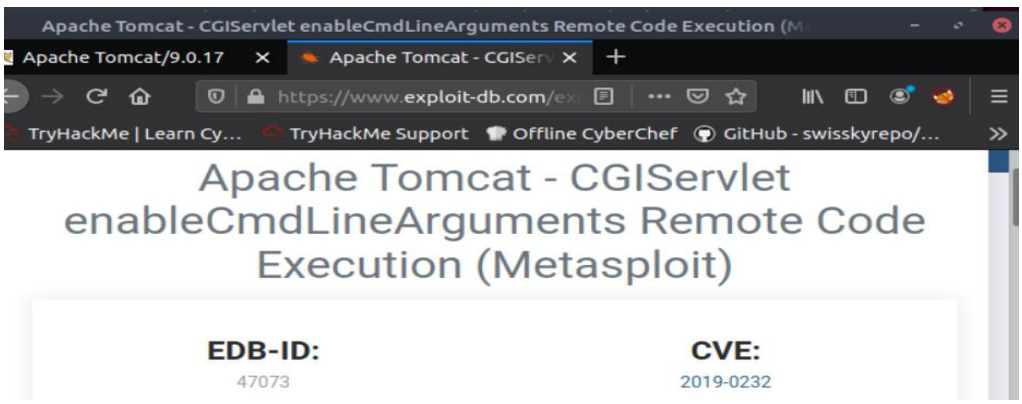




Question 2:

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

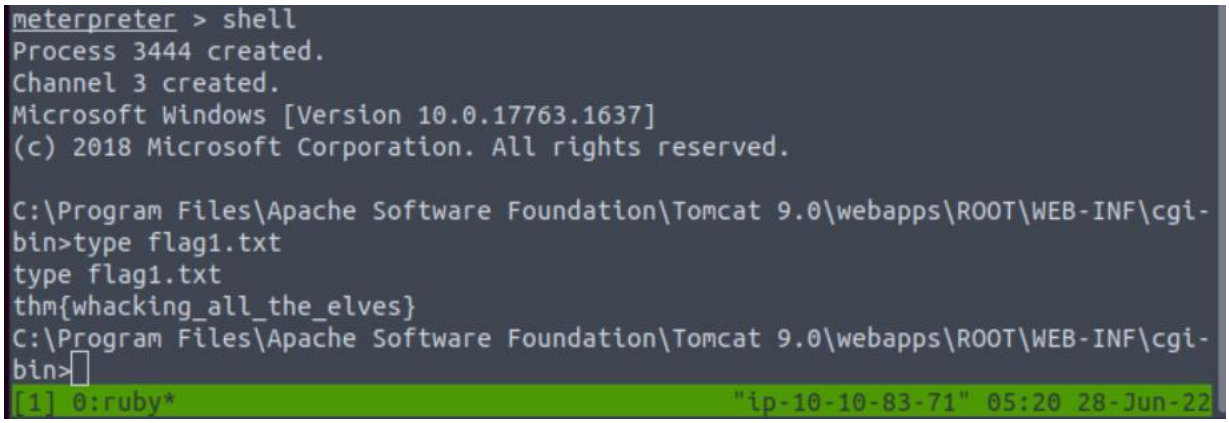
= CVE-2019-0232



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 and RHOST

METHODOLOGY:

We start the machine and the AttackBox to receive Ip address. We scan the Ip address using nmap with few settings such (-sVC -vv and -iL) to see the command script and to get the version number of the web server. We use Firefox to find out the CVE of Apache Tomcat CGI. Next, we set the Metasploit settings appropriately and gain a foothold onto the deployed machine. After that, we set the RHOSTS and TARGETURI values accordingly, the LHOST are already set with the local Ip. We ensure first our options are set right then, we run the exploit to get a Meterpreter connection and we apply shell to run system commands on the host and proceed to finish the challenge.

Day 13 - Networking Coal for Christmas

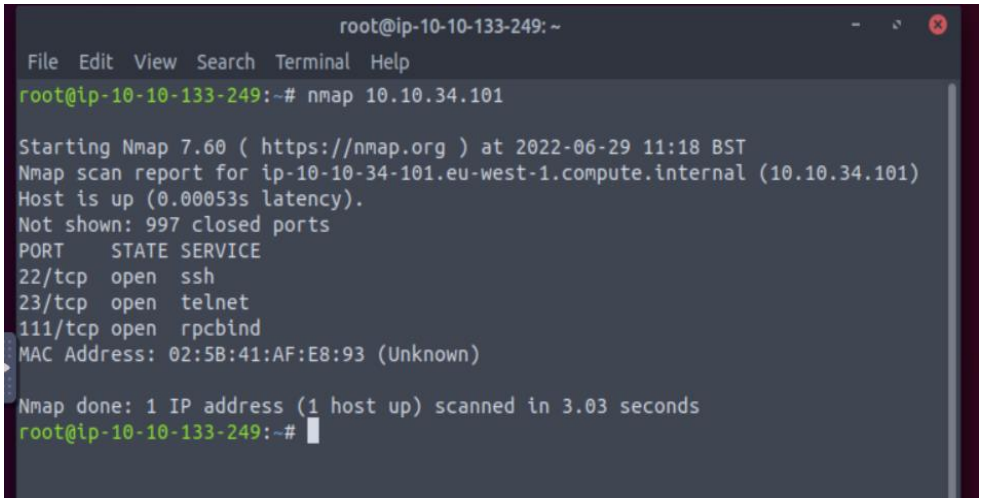
Tools used: **AttackBox**

Solution/Walkthrough:

Question 1:

What old, deprecated protocol and service is running?

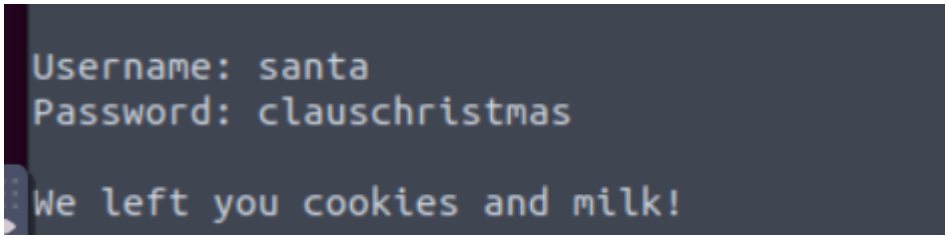
= telnet



Question 2:

What credential was left for you?

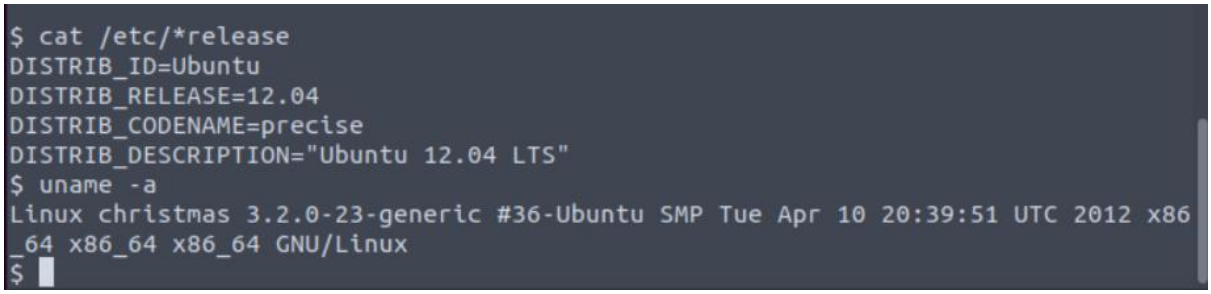
= clauschristmas



Question 3:

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

= Ubuntu 12.04



Question 4:

Who got here first?

= Grinch

```
/*************************************************
// 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

```
//
// Compile with:
//   gcc -pthread dirty.c -o dirty -lcrypt
//
```

Question 6:

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

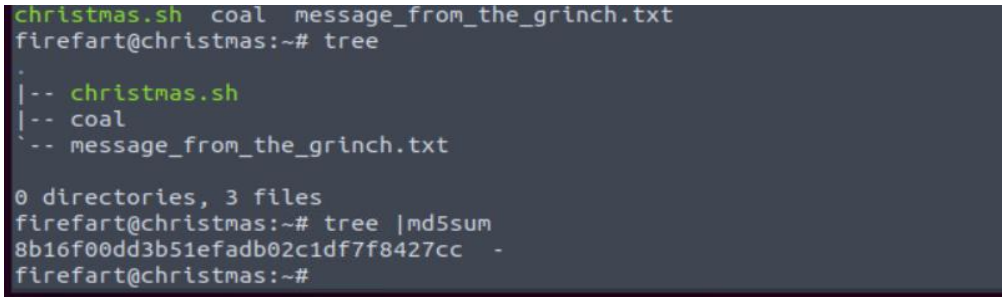
= firefart

```
mmap: 7f46ed1a5000

madvise 0

mv /tmp/passwd.bak /etc/passwdptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'firefart'.
```

Question 7:

What is the MD5 hash output?

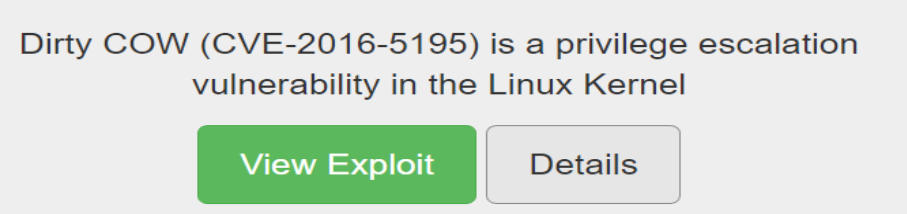
= 8b16f00dd3b51efadb02c1df7f8427cc



Question 8:

What is the CVE for DirtyCow?

= CVE-2016-5195



METHODOLOGY:

We deploy the machine and the AttackBox along the Ip address provided. Initially, we scan the nmap of Ip address (nmap 10.10.188.141) to gain the port and state service in the machine. We pursue connect to the service with the standard command-line client (telnet 10.10.188.141 23) and then obtain the username and the password account. We log in the account, apply the command such (cat /etc/*release) to look at pertinent system information for distribution of Linux and version number in the server running. We carry on by finding “who got here first?” task with command (cat cookies_and_milk.txt). Then we exploit the Dirty Cow to find the source code from its original website, we copy and paste it in a new command line text editor (GNU nano). After that we employ command (gcc -pthread dirty.c -o dirty -lcrypt) to compile the exploit and create new password to receive new username. In addition, we switch our user into the new account and hop over to the /root directory to own the server. Lastly, we run (tree | md5sum) to acquire MD5 hash output.

Day 14 - Where's Rudolph?

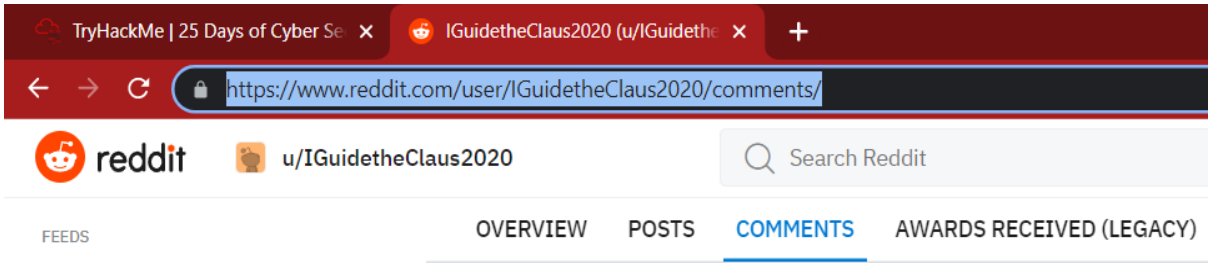
Tools used: Twitter, Google, Reddit

Solution/Walkthrough:

Question 1:

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

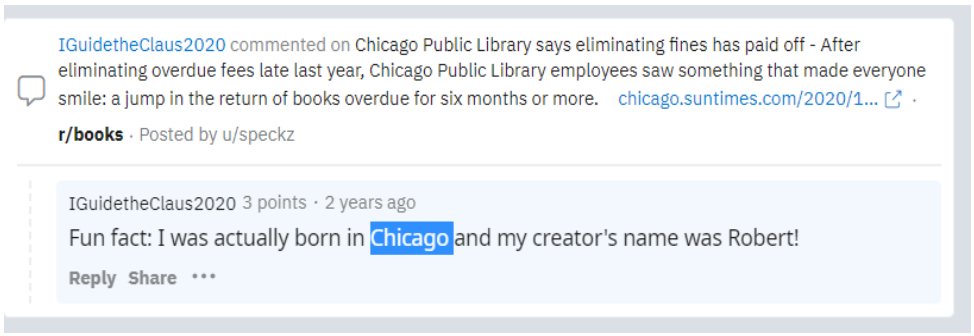
= https://www.reddit.com/user/IGuidetheClaus2020/comments



Question 2:

According to Rudolph, where was he born?

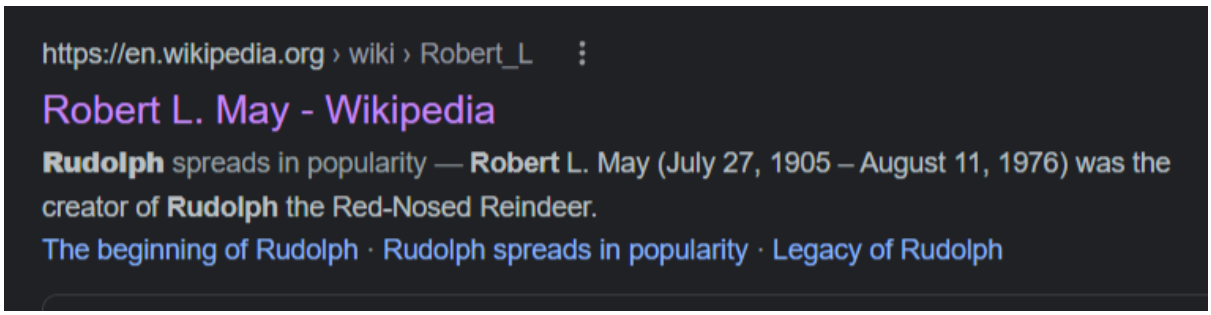
= Chicago



Question 3:

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

= May



Queston 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:

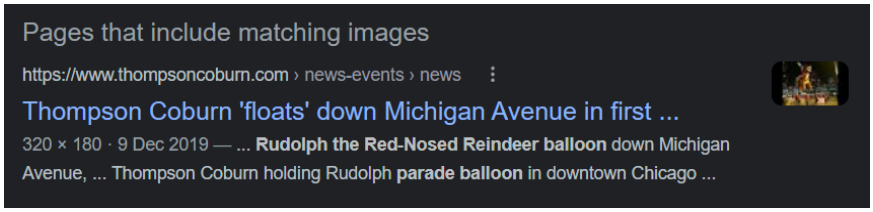
What appears to be Rudolph's favourite TV show right now?

= 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:

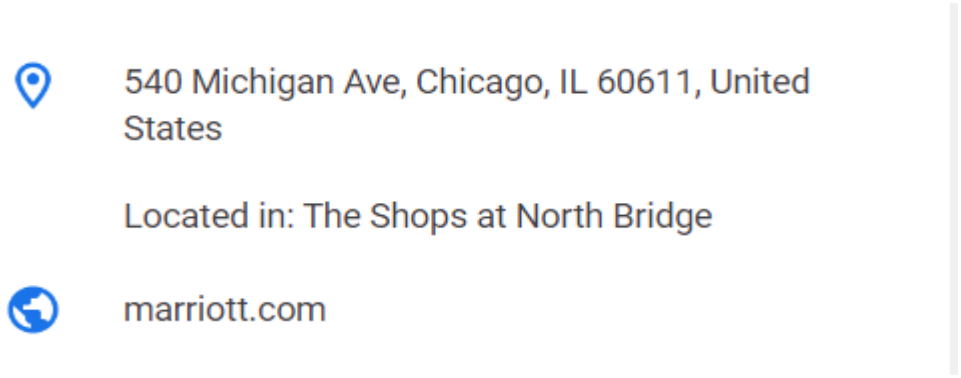
Has Rudolph been pwned? What password of his appeared in a breach?

= 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



METHODOLOGY:

For Task 16 we only use twitter, google and reddit to solve it. First of all, we search Rudolph reddit and went to comment section to provide the link also gain the place where Rudolph born. Then we explore the google to find out Roberts last name. Next, we use twitter to know Rudolph username on that platform, his favourite show and the place he took part in a parade. Beside that, we use EXIF data website to receive the GPS for the place and the flag. Furthermore, we navigate Scylla.sh but currently the website service is down so we just take the answer from the guidance video. Finally we use google maps and use the GPS of the image to discover the street numbers of the hotel address.

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

Tools used: Vs Code, Phyton

Solution/Walkthrough

Question 1:

What's the output of True + True?

= 2

Question 2:

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

= PyPi

Question 3:

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

= True

Question 4:

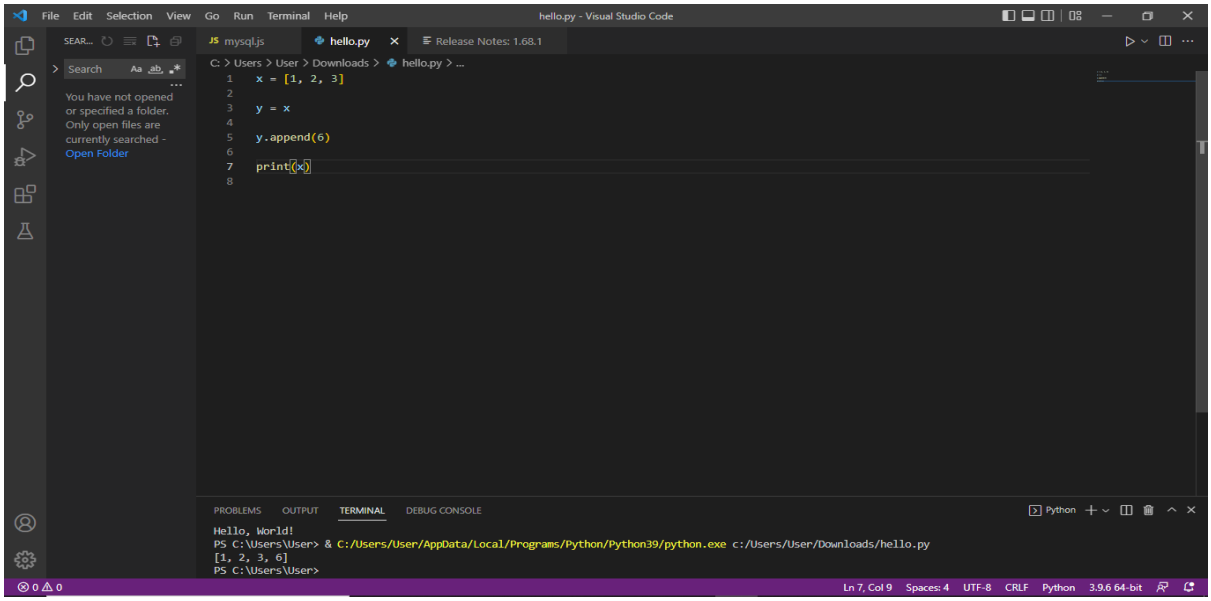
What library lets us download the HTML of a webpage?

= Requests

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:

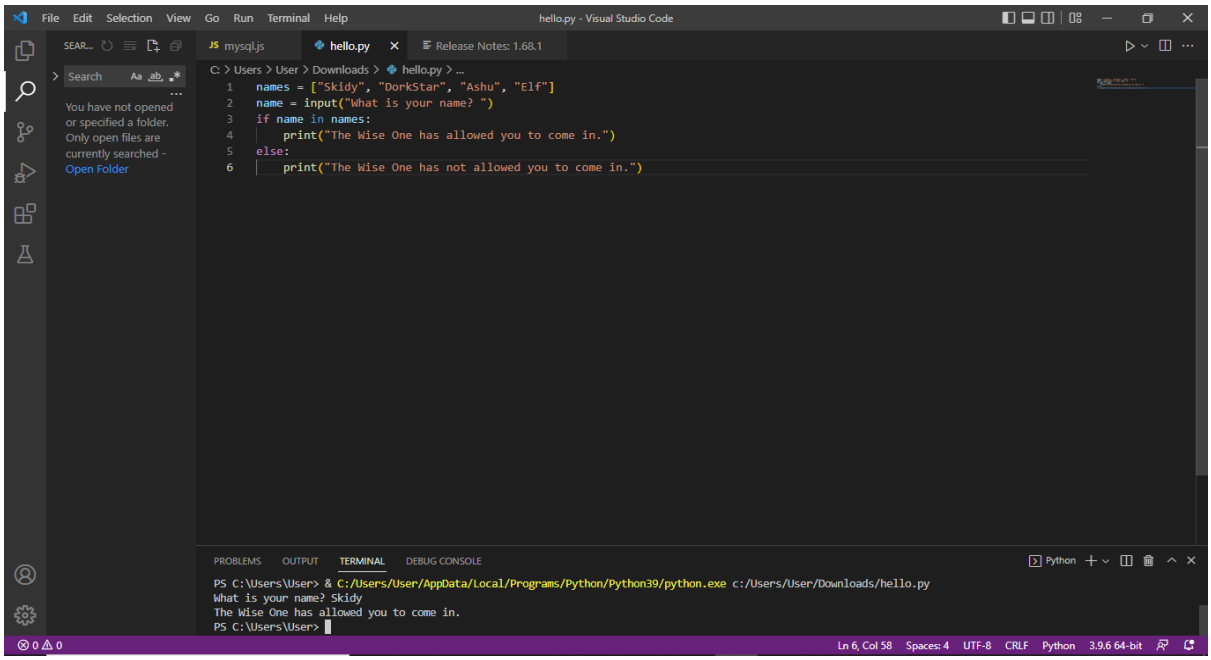
What causes the previous task to output that?

= Pass by reference

Question 7:

if the input was "Skidy", what will be printed?

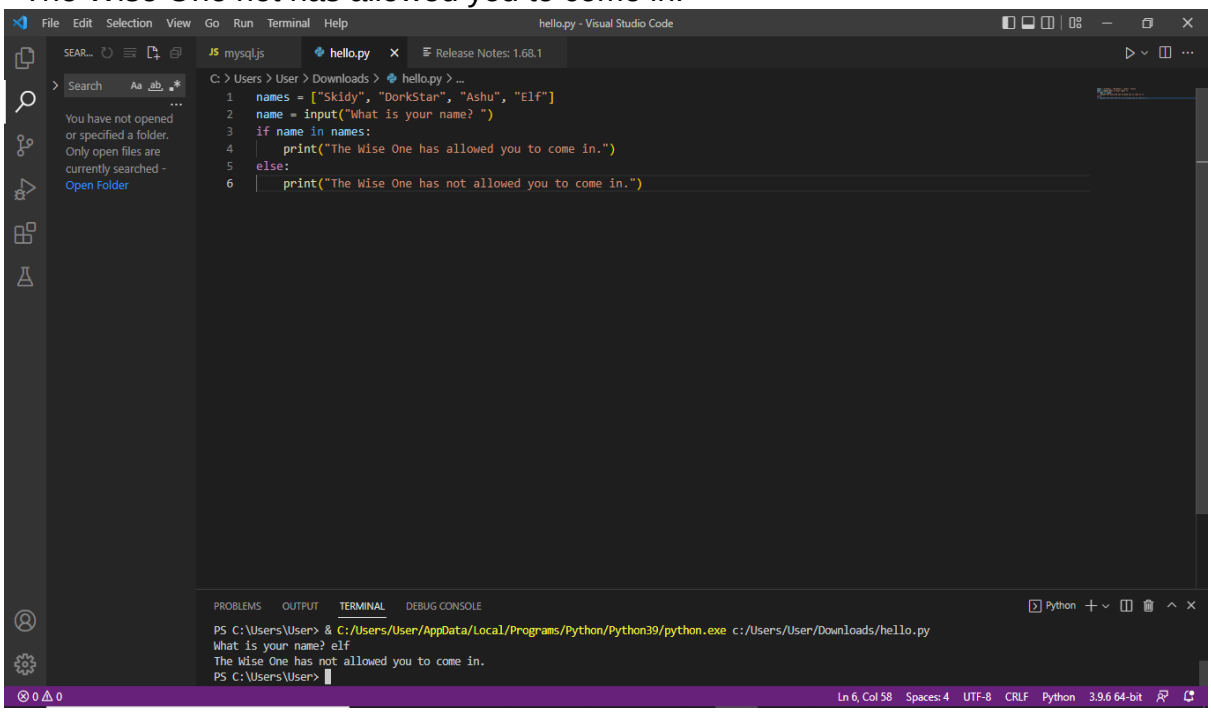
= The Wise One has allowed you to come in.



Question 8:

If the input was "elf", what will be printed?

=The Wise One not has allowed you to come in.



METHODOLOGY:

In day 15, We learn the basics of using phyton. First, we downloaded vs code as our scripting platform and we downloaded phyton as our coding language. Then we created a file named “hello.py”and tried out all the commands that have been prepared for us in try hack me. Finally, we answer the questions given to us by entering the codes given in try hack me in to vs code which has phyton running in it.