PSP0201 Week 4 Writeup

Group Name : Mali Pape

Members:

ID	Name	Role
1211102895	Muhammad Irfan Bin Mohd Nazri	Leader
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazariee	Member
1211103634	Ho Tian Ming	Member
1211101035	Mohamad Zuhir Bin Mohamad Zailani	Member

Day 11: Networking - The Rogue Gnome
Tools used: Kali Linux
Solution/walkthrough:

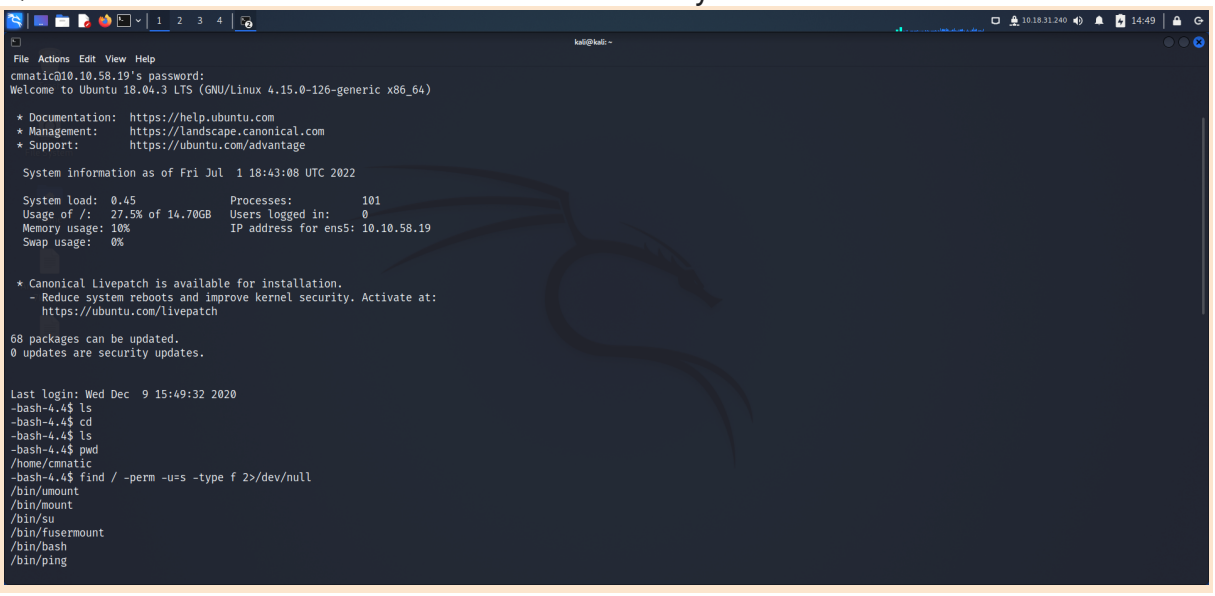
Question 1(commands as an administrator)
Question 2(managed to pivot it to another account that can run sudo commands)
Question 3(The privileges are almost similar):

> ## 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:

> 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).
>
> SUID is simply a permission added to an executable that does a similar thing as sudo. However, instead, allows users to run the executable as whoever owns it as demonstrated below:

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



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?)

11.9. Abusing SUID (GTFOBins)

Now that we understand why executables with this SUID permission are so enticing, let's begin to learn how to find these and understand the capabilities we can do with some of these executables. At the surface, SUID isn't inherently insecure. It's only when you factor in the misconfiguration of permissions (and given the complexity on Linux - is very easy to do); Administrators don't adhere to the rule of least privileges when troubleshooting.

Executables that are capable of interacting with the operating system such as reading/writing files or creating shells are goldmines for us. Thankfully, GTFOBins is a website that lists a majority of applications that do such actions for us. Let's set the SUID on the `cp` command that is used to copy files with

```
chmod u+s /usr/bin/cp
```

Question 7:(command used to host a http server using python3 on port 9999)

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: (flag)

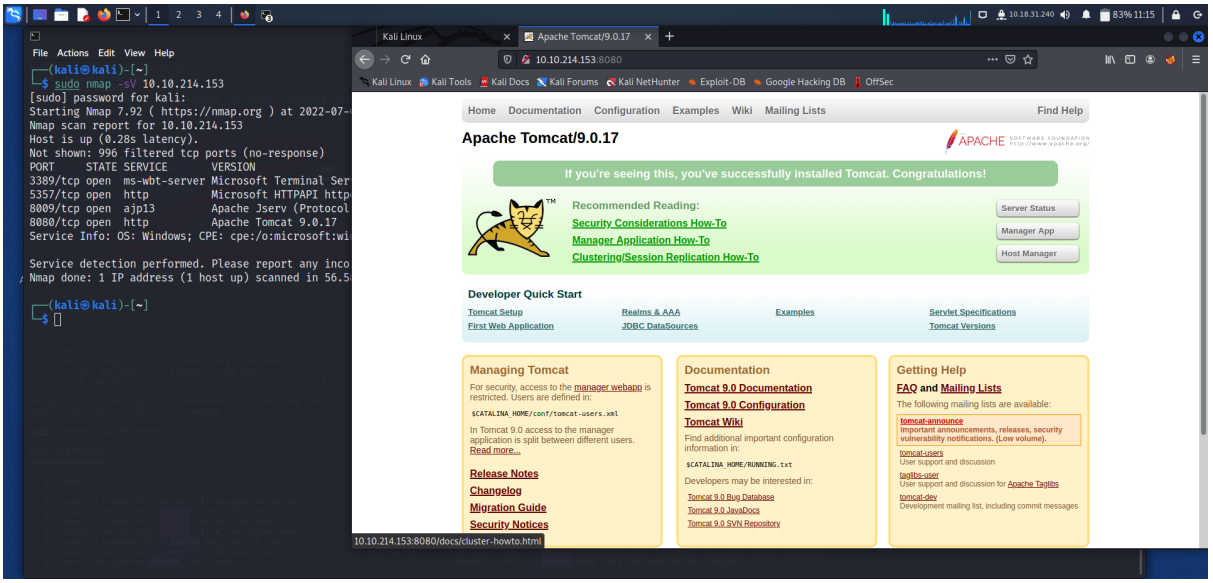
```
File  Actions  Edit  View  Help
/snap/core/7270/usr/bin/chfn
/snap/core/7270/usr/bin/chsh
/snap/core/7270/usr/bin/gpasswd
/snap/core/7270/usr/bin/newgrp
/snap/core/7270/usr/bin/passwd
/snap/core/7270/usr/bin/sudo
/snap/core/7270/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/7270/usr/lib/openssh/ssh-keysign
/snap/core/7270/usr/lib/snapd/snap-confine
/snap/core/7270/usr/sbin/pppd
/usr/bin/newgidmap
/usr/bin/at
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/newuidmap
/usr/bin/traceroute6.iputils
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
-bash-4.4$ bash -p
bash-4.4# whoami
root
bash-4.4# cd /root
bash-4.4# ls
flag.txt
bash-4.4# cat flag.txt
thm{2fb10afe933296592}
bash-4.4#
```

Thought Process/Methodology:

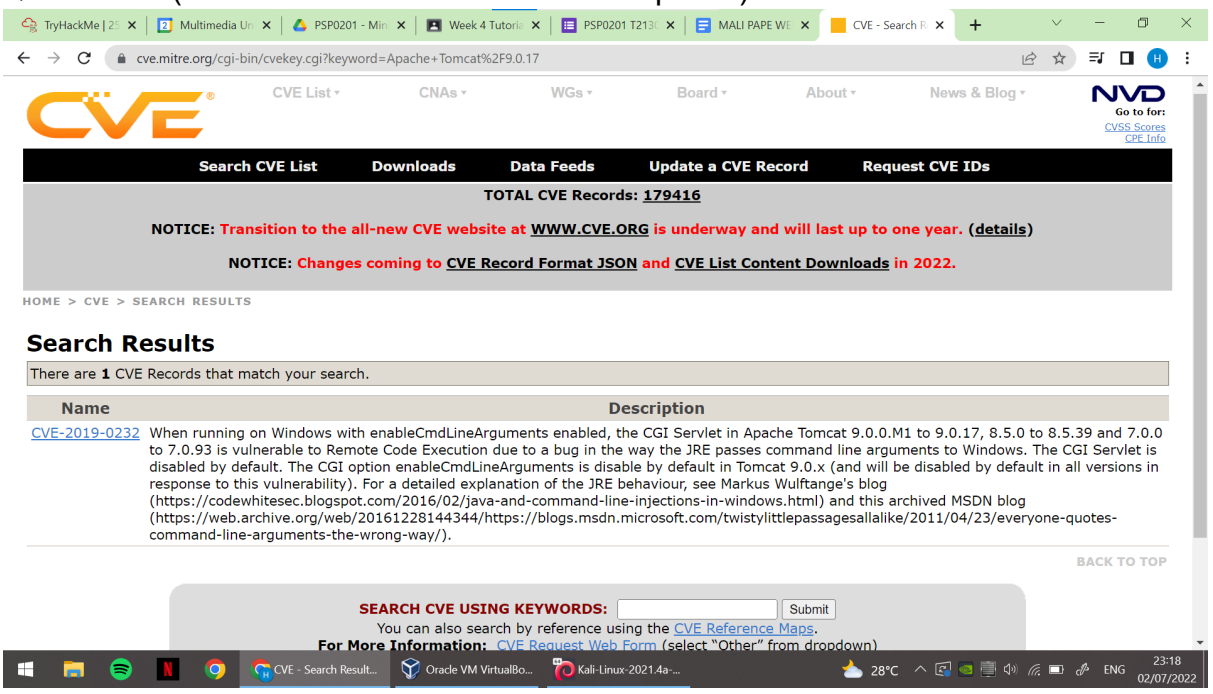
First of all, open your terminal and type ssh cmnatic@(ip address). It will ask (continue connecting)[fingerprint] type yes for it. Then, type the password that is provided in tryhackme which was aoc2020. Next you will enter into Ubuntu 18.04.3 Then, you have to type find / -perm -u=s -type f 2>/dev/null in the (-bash-4.4$) line. There will appear a lot of SUID permission sets. Find the bash one and use it by typing bash -p in (-bash-4.4$) line. After you press enter, the (-bash-4.4$) will become bash4.4#. Now you are a root. So, now you type cd/root. Then, type ls. It will show flag.txt. Next, netcat it by typing cat flag.txt. There you go, the flag will appear.

Day 12: Networking - Ready, set ,elf
Tools used: Kali Linux
Solution/walkthrough:

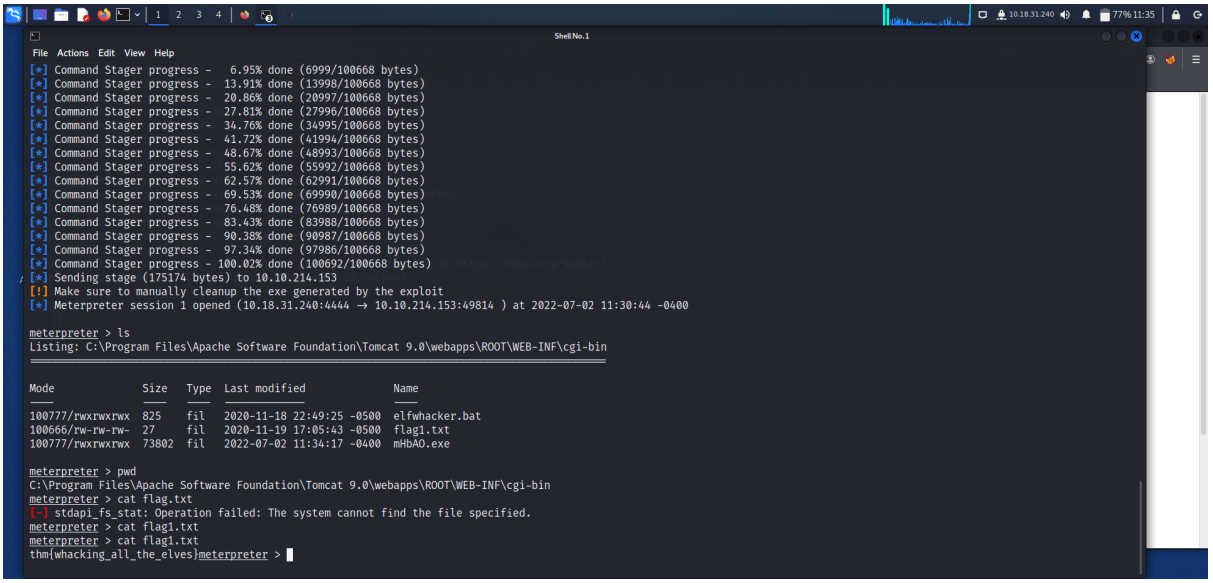
Question 1:(version number of web server)



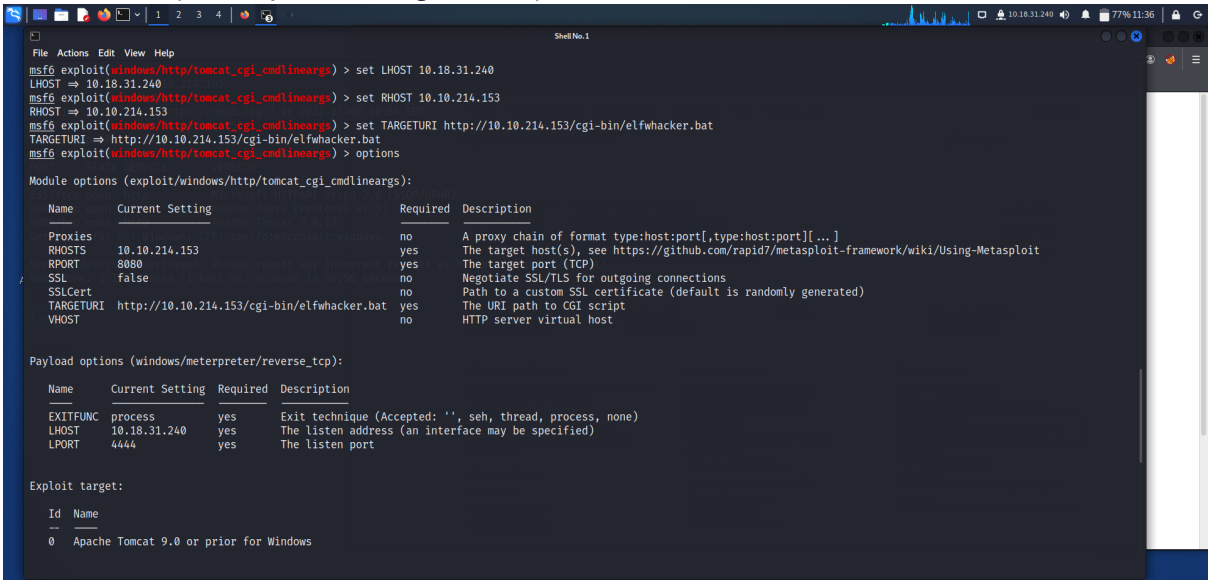
Question 2: (CVE can be used to create meterpreter)



Question 3: (flag)



Question 4: (metasploit settings to set)



Thought Process/Methodology:
First of all, type nmap -sV (ip address) in the terminal to run a scan. Next, find the port which are open. Open your browser and type the target ip address and add :(port number). One of the port number will work and direct you to a website. Well, the website is Apache Tomcat /9.0.17 and the go to cve website to find the cve number to exploit it. After you found the cve number, you need to open Metasploit and enter your password in it. Next, you type search cve-2019-0232 which are the cve number that found in website. Then, type use 0. Next, type options to check the settings whether they are correct or not. Set your LPORT to machine ip address, RPORT to your target ip address and TARGETURI into http:///(target ip)/cgi-bin/elfwhacker.bat. After setting them, type options to make a double c heck. If correct, then type run. It will appear meterpreter. Next type ls.You will find the flag file. Then type pwd. Lastly, type cat flag1.txt. Congratulations, you found the flag!

Day 13: Networking - Coal for Christmas
Tools used: Kali Linux
Solution/walkthrough:

Question 1:

Using nmap to see protocol and services running.

Answer : telnet

```
┌──(1211104288㉿kali)-[~]
└─$ sudo nmap -sV 10.10.250.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-03 02:35 EDT
Nmap scan report for 10.10.250.196
Host is up (0.21s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2
.0)
23/tcp  open  telnet  Linux telnetd
111/tcp open  rpcbind 2-4 (RPC #100000)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.60 seconds
```

Question 2:

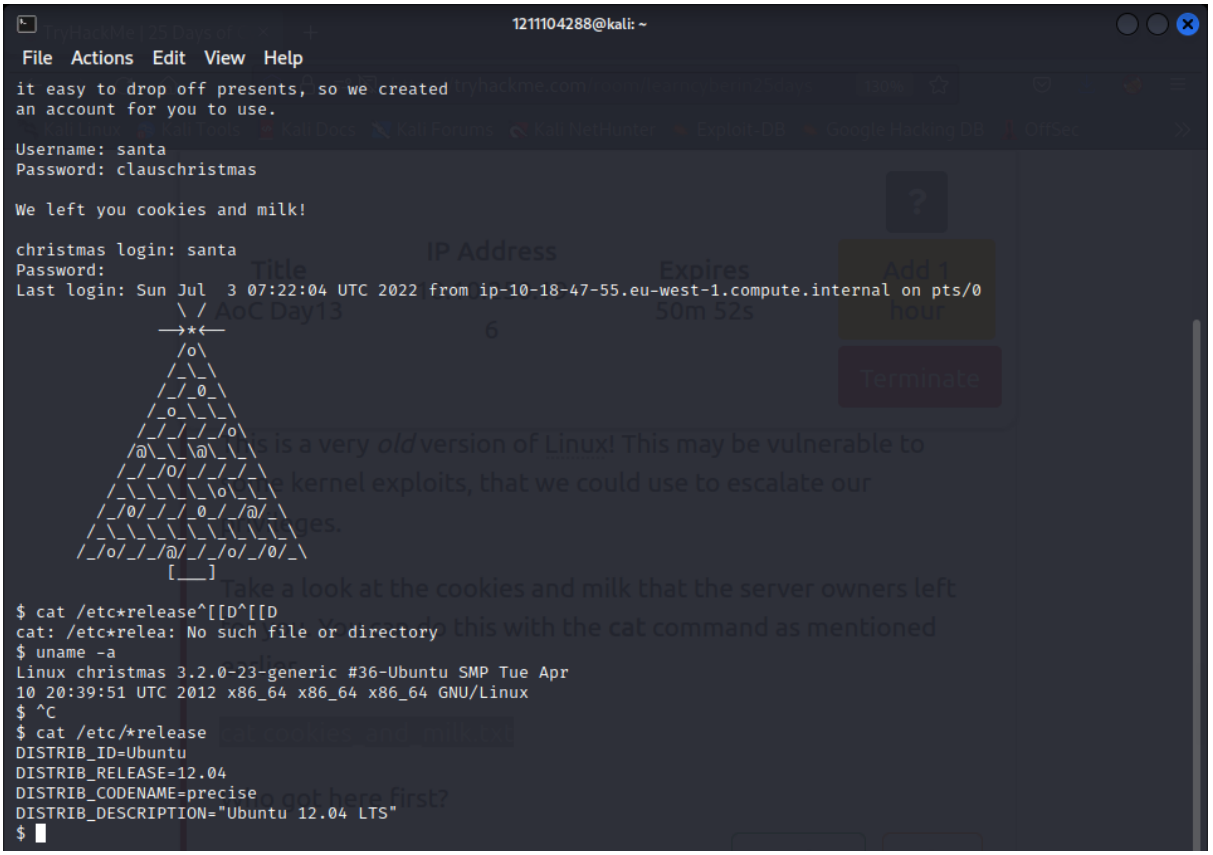
Use nmap syntax telnet <ip address of the machine> to connect to the service and search for the password.

Answer : clauschristmas

```
┌──(1211104288㉿kali)-[~]
└─$ telnet 10.10.250.196 23
Trying 10.10.250.196...
Connected to 10.10.250.196.
Escape character is '^]'.
HI SANTA!!!

We knew you were coming and we wanted to make
it easy to drop off presents, so we created
an account for you to use.

Username: santa
Password: clauschristmas

We left you cookies and milk!

christmas login:
```

Question 3 :

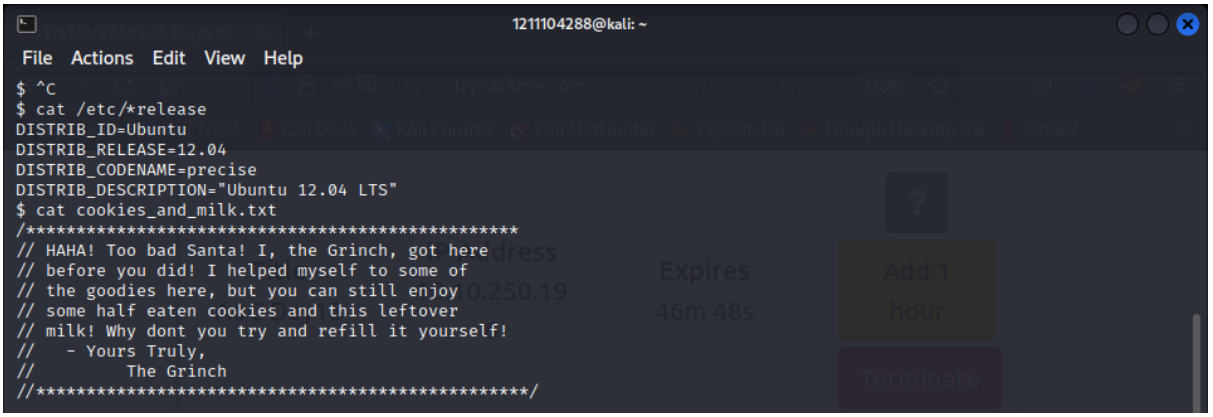
Use cat /etc/*release after log in to search the linux distribution.
Answer : Ubuntu 12.04



Question 4 :

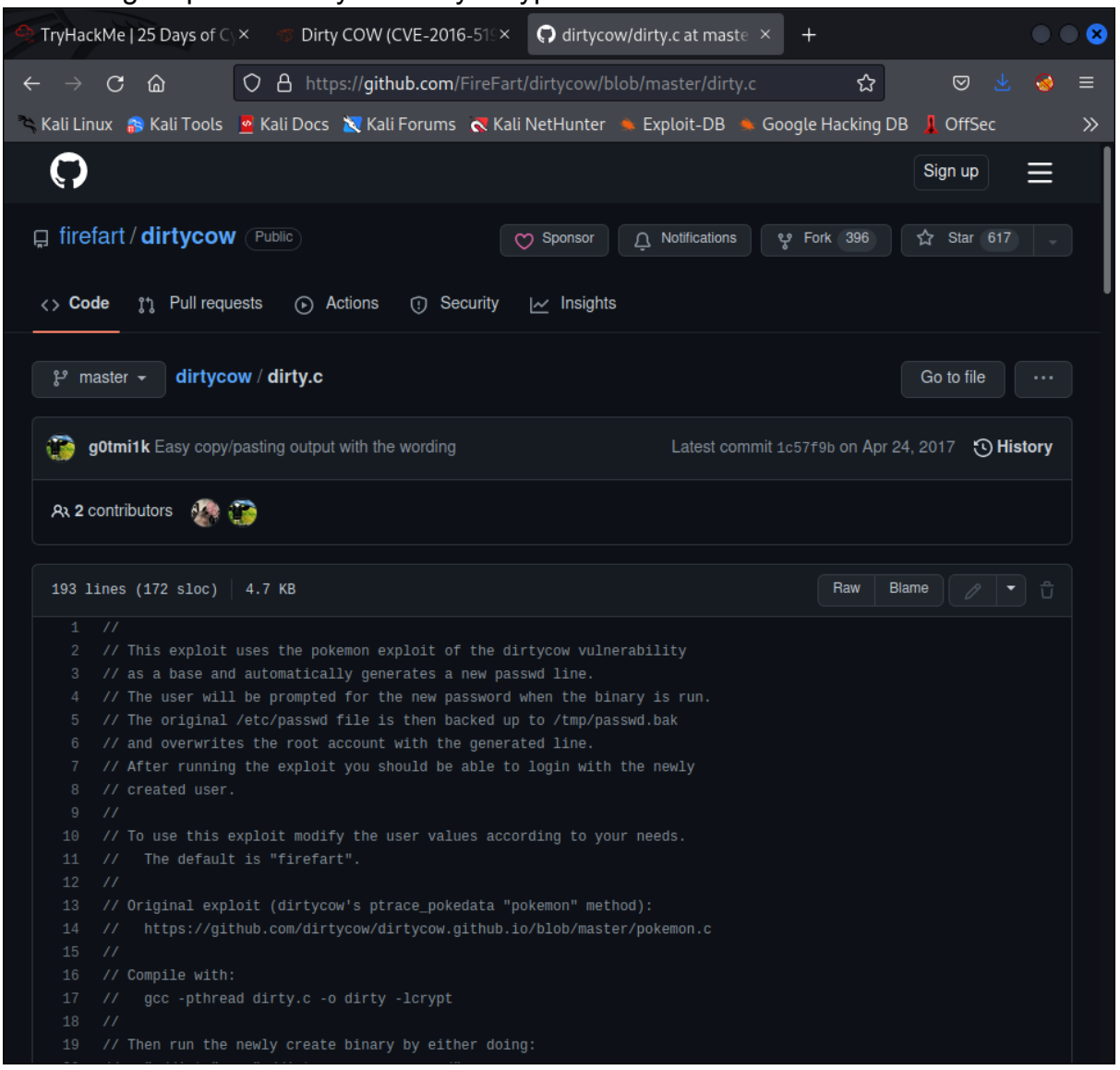
Open the file left by the owner using cat command

Answer : grinch

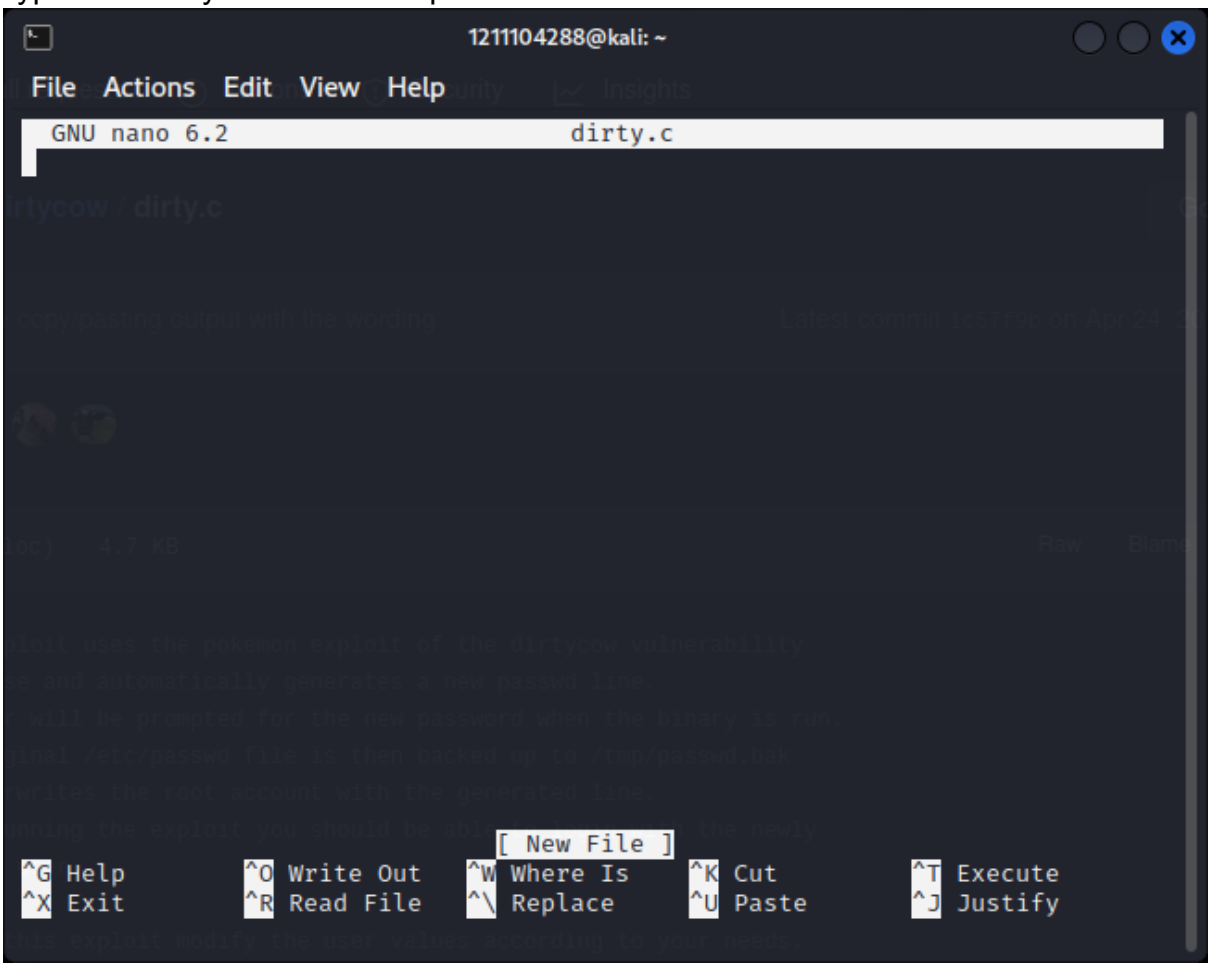


Question 5 :
Use the syntax provided in the test from dirty.c file.

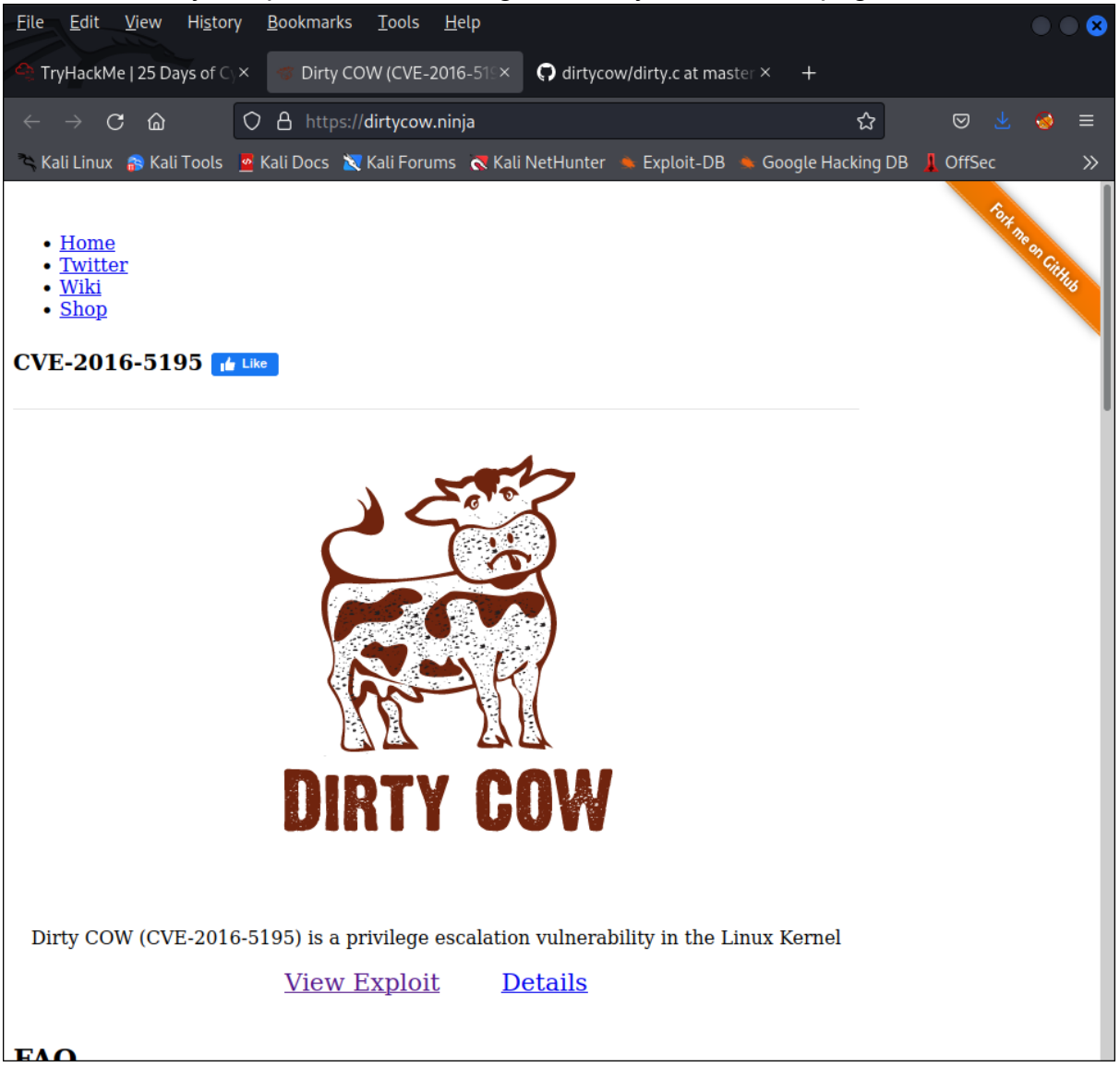
Answer : gcc -pthread dirty.c -o dirty -lcrypt



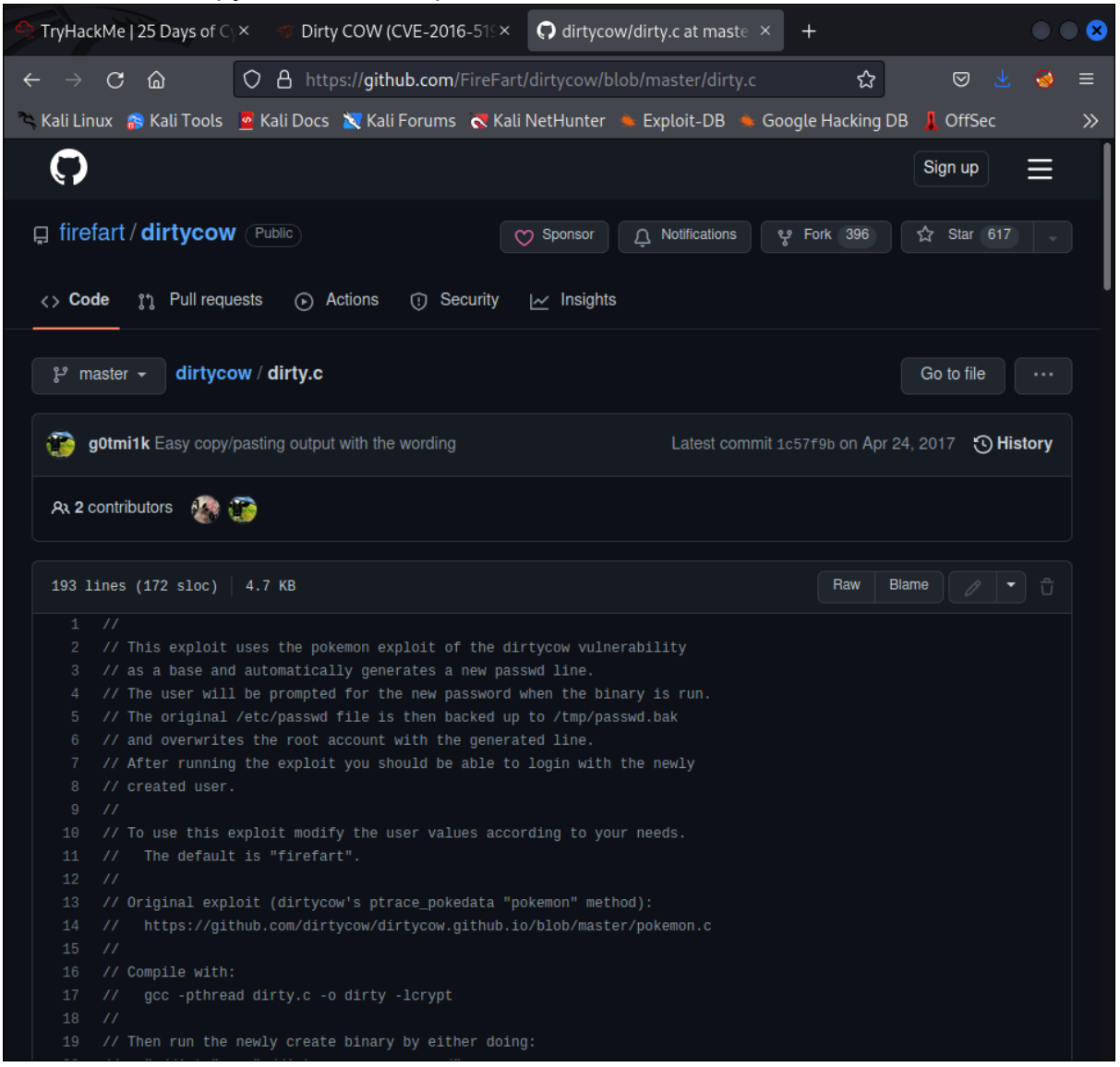
Question 6 :
Type nano dirty command to open the text editor.



Search the dirty.c exploit from the link given in TryHackMe webpage



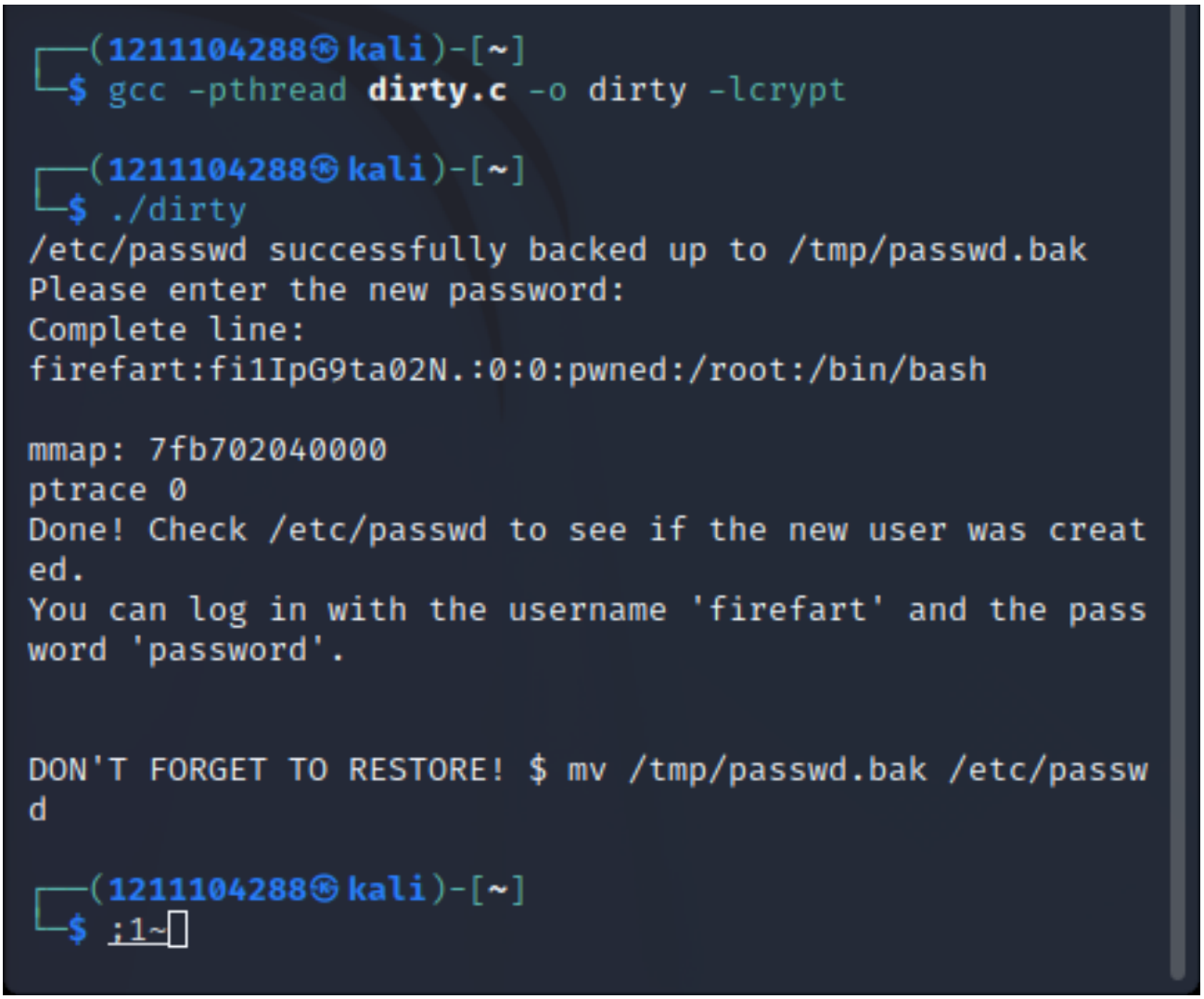
Click raw and copy the code and paste in the nano text editor.



Use gcc -pthread dirty.c -o dirty -lcrypt to compile the file and set up password.

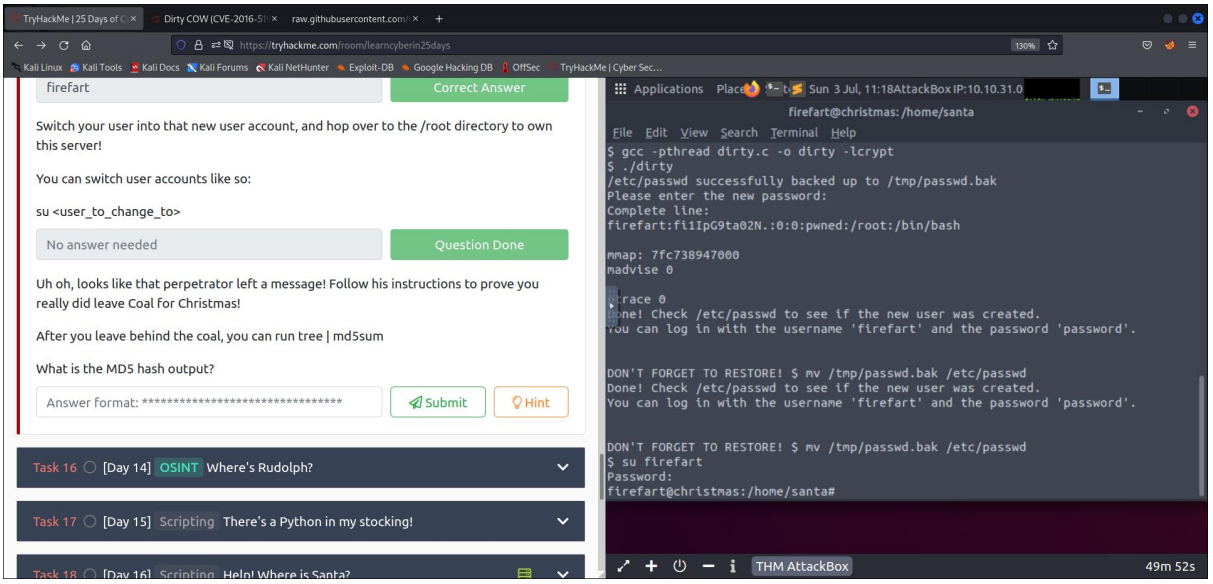
Search for the new username from the compiled dirty.c file.

Answer : firefart

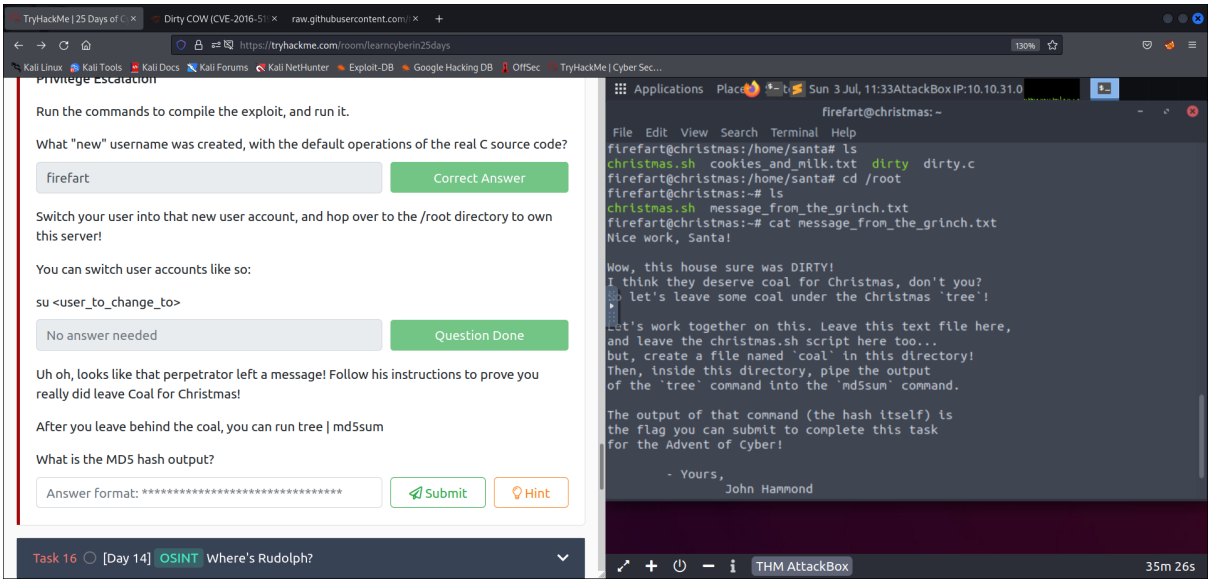


Question 7 :

Log in into firefart profile.

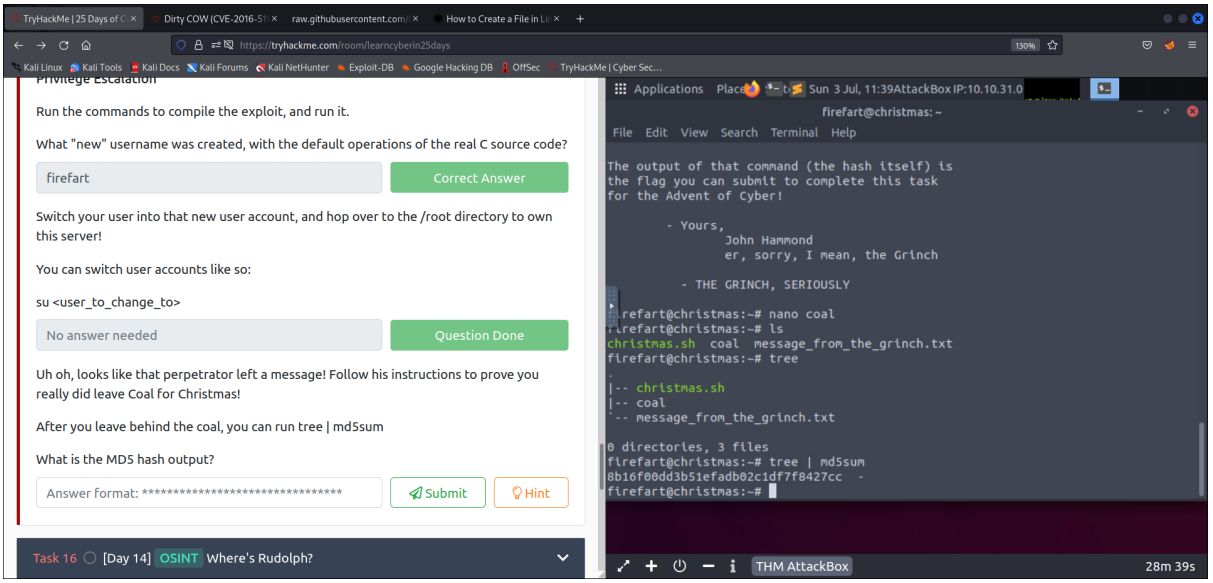


Change directory to /root and use ls command to see the list of available items. Use cat command to open the message_from_the_grinch.txt



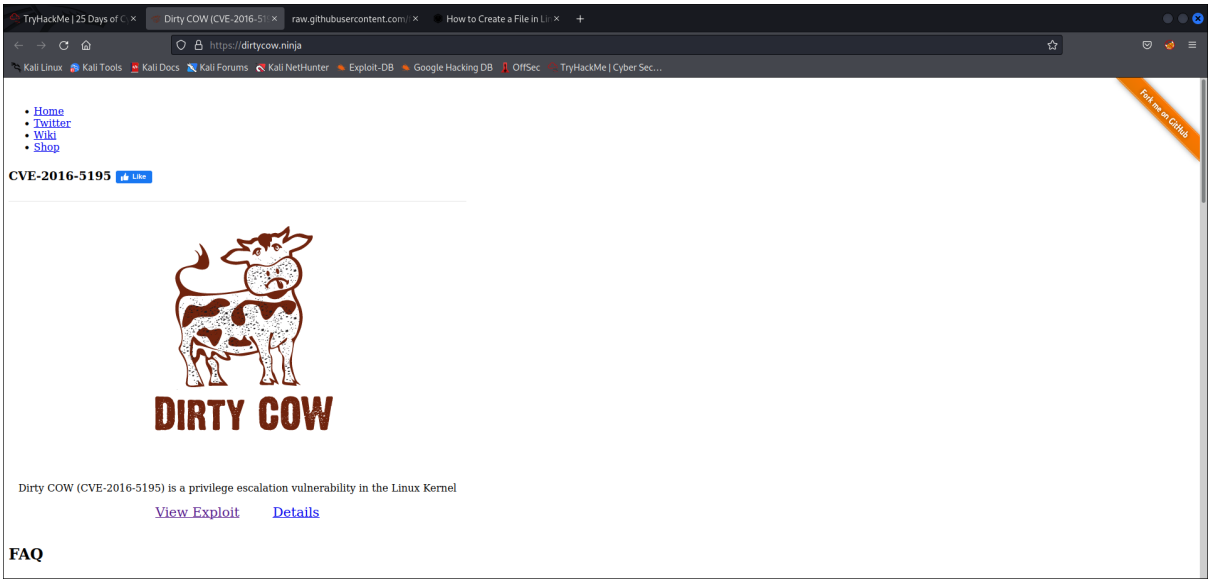
Create a file name coal to leave coal for Santa. Then open tree | md5sum to get the MD5 hash output.

Answer : 8b16f00dd3b51efadb02c1df7f8427cc



Question 8:

Answer : CVE-2016-5195



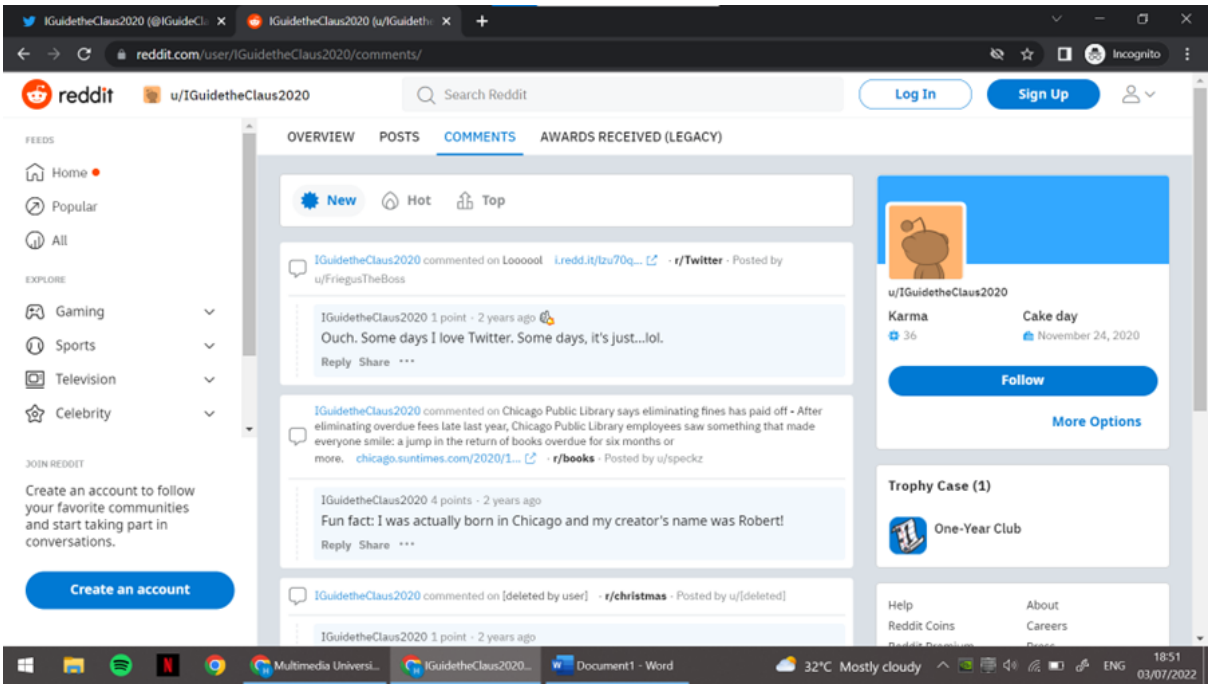
Thought Process / Methodologies :

At first, I used the nmap command in order to show me the available protocols and services in the IP Address which gives out the old, deprecated protocol and service running that is telnet. After that , I run the command of nmap syntax telnet <ip address of the machine> to connect to the service and search for the password we needed and the answer is clauschristmas. Moreover to proceed with the 4th question, I use cat /etc/*release after log in to search the linux distribution. This will gives out the Linux Distribution used which is Ubuntu 12.04. I then used cat command on the cookies_and_milk.txt file to open up the person who arrived first

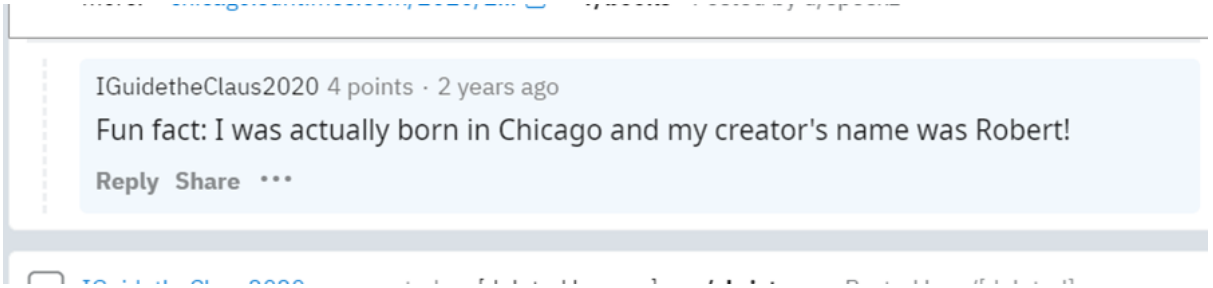
that is the grinch. To continue, I search and go to github included link given it the TryHackMe website and read the comment in the top the code. Here, it is included that we need to use command gcc -pthread dirty.c -o dirty -lcrypt to compile the file. For Question 5, I type nano dirty.c to create a file and then I copy pasted the code from the raw code of dirty.c exploit from the github link. I clicked ctrl+x to close and save the file. Then I used gcc -pthread dirty.c -o dirty -lcrypt command to compile the file and set up password. It then shows the password I chosen and the username of 'firefart' - the new user asked in Question 6. I then switch user using su firefort Command and change directory to /root to see the message file left by the grinch. To continue, I then followed his instruction by making a file named 'coal to left in the directory and open the command of tree | md5sum to get the MD5 hash output - 8b16f00dd3b51efadb02c1df7f8427cc. Last but not least, before I end this day, I search for website that guide me to the dirty exploitation github link which relieved the CVE number needed in the question that is CVE-2016-5195.

Day 14: OSINT - Where's Rudolph?
Tools used: Kali Linux, Firefox, Twitter, Reddit
Solution/walkthrough:

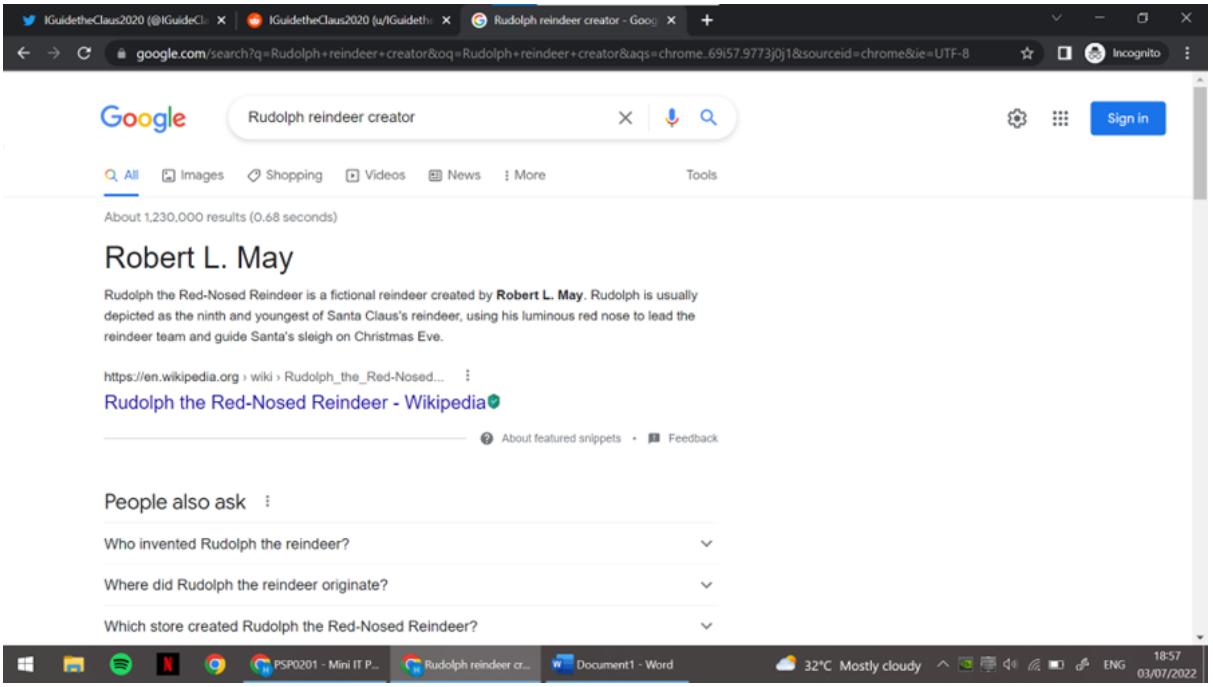
Question 1: (reddit comments)



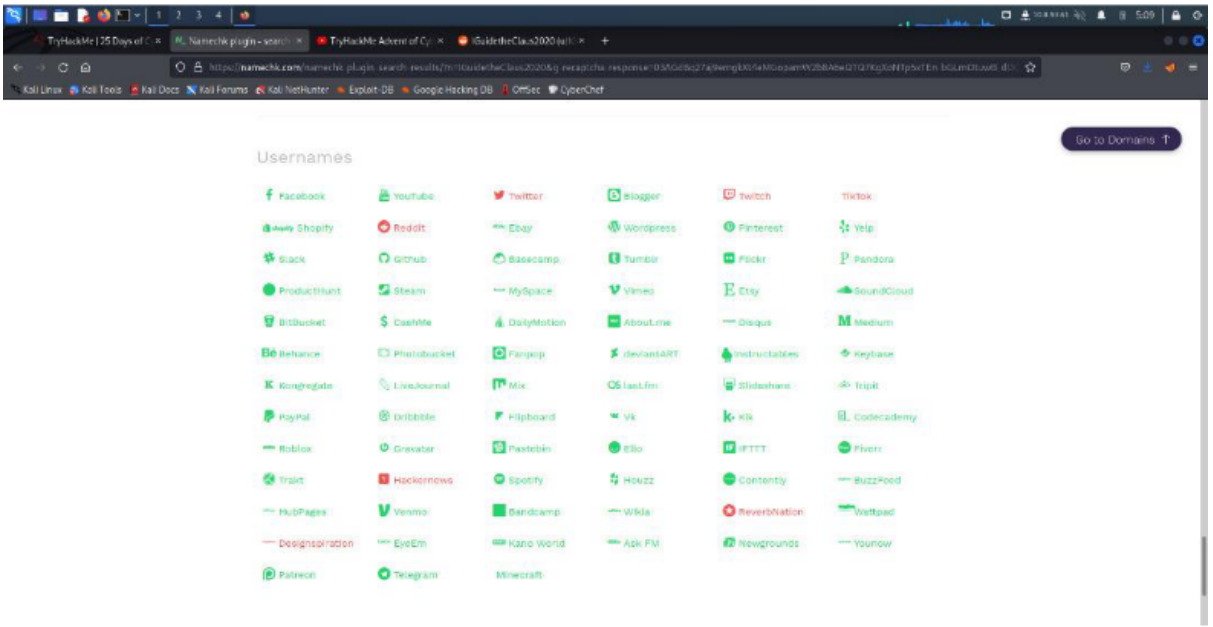
Question 2: (Where did Rudolph born?)



Question 3: (Robert's last name)

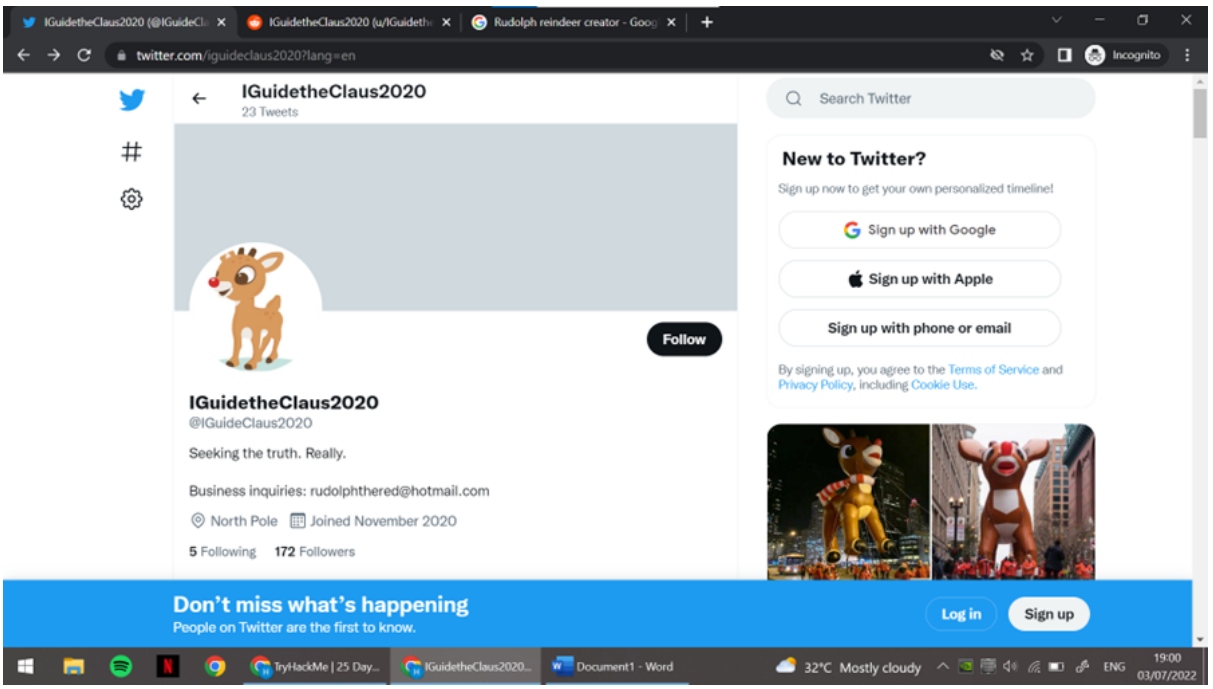


Question 4: (social media platform)

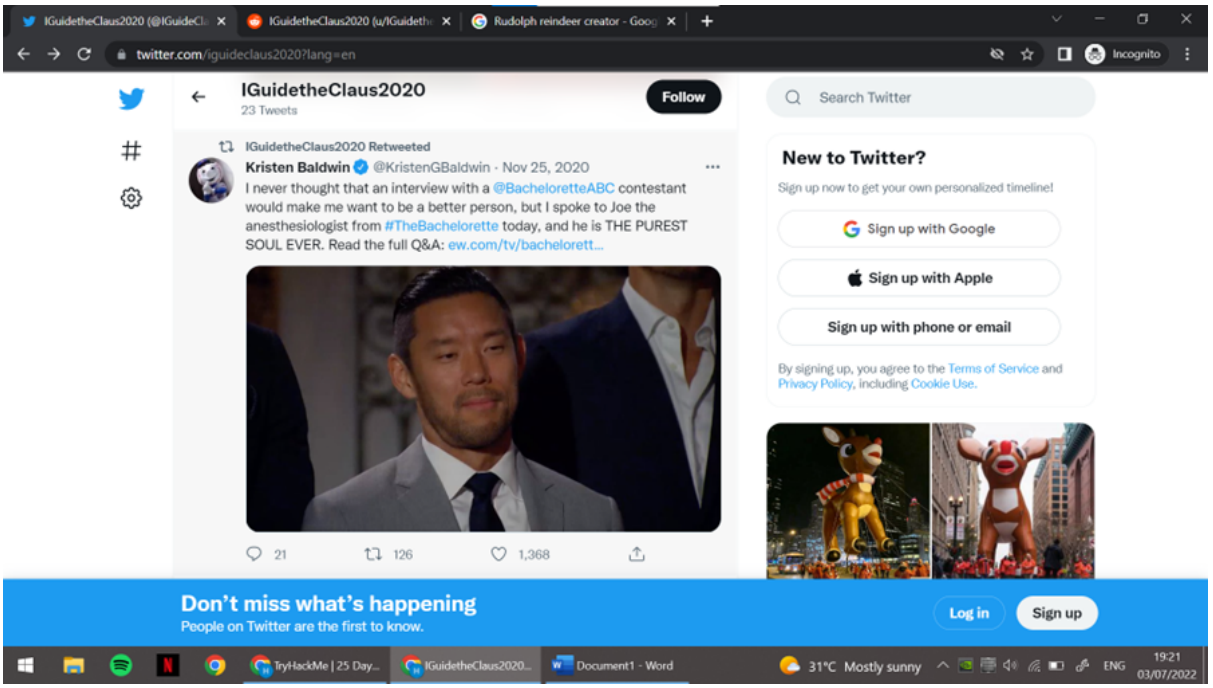


Social media platform that he has.

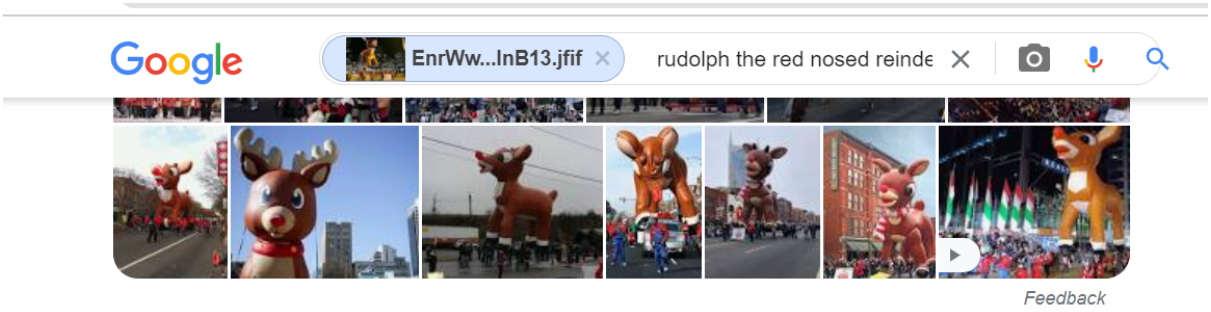
Question 5: (Rudolph's username)



Question 6: (Rudolph's favourite TV show)

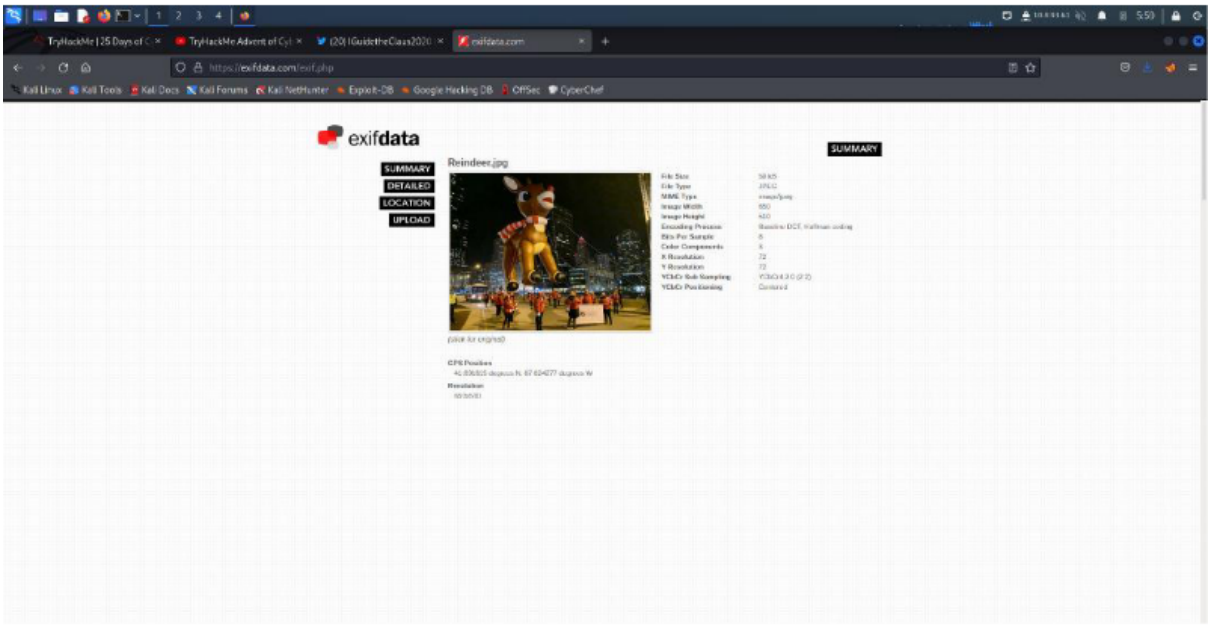


Question 7: (parade location)



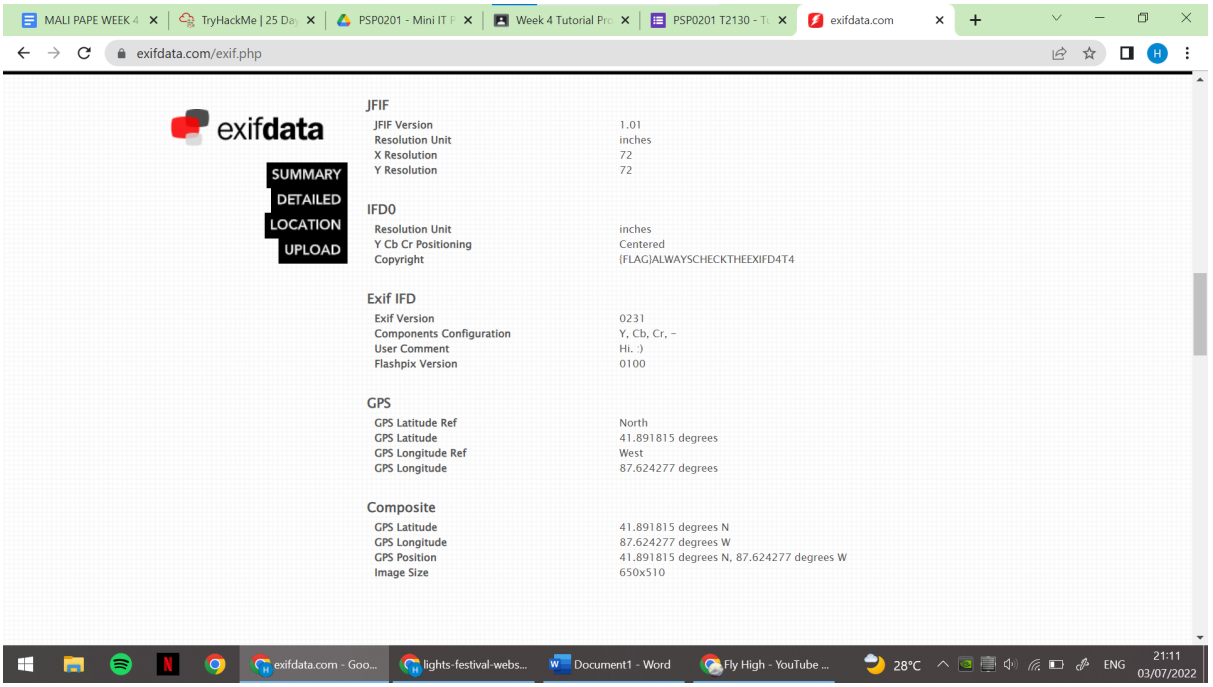
We have to save Rudolph's parade pic.

Question 8: (specific location)



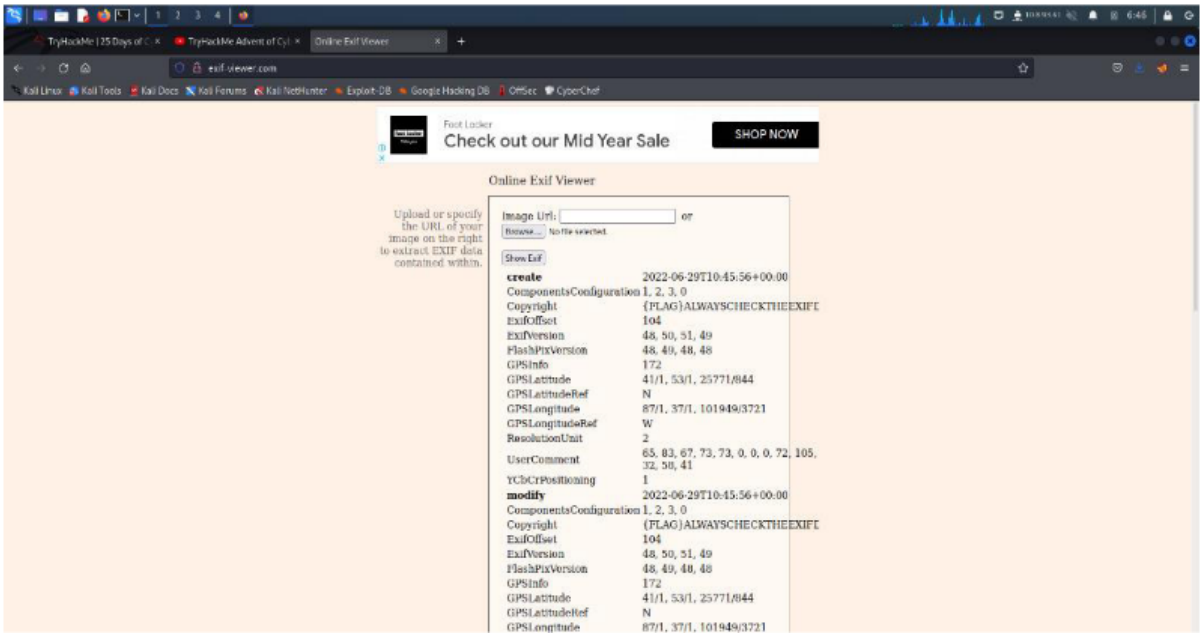
Use **EXIF** to locate the picture location.

Question 9: (flag)



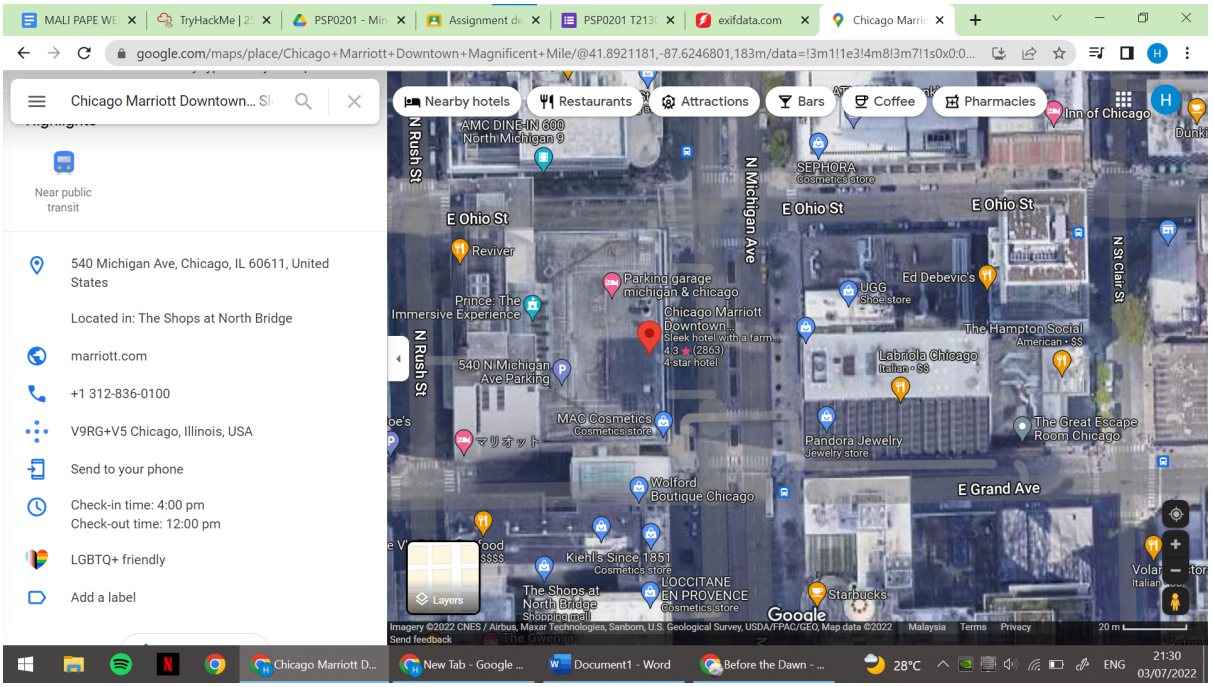
After using the method, we can find the flag we were given.

Question 10: (Has Rudolph been pwned?)



The scylla server is down. Answer: Spygame

Question 11: (street number of hotel address)



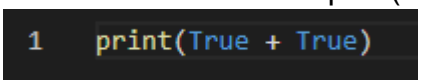
We can locate the street address of Rudolph staying at by using information that he put on twitter.

Thought process / Methodologies : First, find the reddit page and find the comments. After finding the comments we can get information about Rudolph. Search the word **"IGuidetheClaus2020",** then we can get his information like locate where he lives. Next, We can get the flag online exif viewer (copyright) . And finally we locate the address of where Rudolph staying.

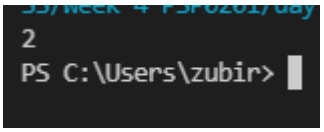
Day 15: Scripting - There's a Python in my stocking
Tools used: Visual Studio Code, Python
Solution/walkthrough:

Question 1:

First we write the code print(True + True) in VS Code



Then we run the code to get the output 2.



Question 2:

We can get the answer from the note in TryHackMe.

Question 3:

We write the code print(bool(“False”) in VS code

```
1   print(bool("False"))
```

Then we run the code to get the following output.

```
RESS/Week 4 PSP0201/day
True
PS C:\Users\zubir>
```

Question 5:

We copy paste the code in question 5 from thm into VS code

```
1   x = [1, 2, 3]
2
3   y = x
4
5   y.append(6)
6
7   print(x)
8
```

s

The output of the code is as follows.

```
RESS/Week 4 PSP0201/day
[1, 2, 3, 6]
PS C:\Users\zubir>
```

Question 7:

We copy and paste the code given into VS code

```
Examine the following code:
names = ["Skidy", "DorkStar", "Ashu", "Elf"]
name = input("What is your name? ")
if name in names:
   print("The Wise One has allowed you to come in.")
else:
   print("The Wise One has not allowed you to come in.")
```

By inputting Skidy while running the code, we can get the answers for question 7.

```
What is your name? Skidy
The Wise One has allowed you to come in.
PS C:\Users\zubir>
```

Question 8

We run the same code from the previous question but instead of inputting Skidy, we input “elf” and we’ll get a different answer.

```
What is your name? elf
The Wise One has not allowed you to come in.
PS C:\Users\zubir>
```

Thought Process/Methodology:

First of all I use Visual Studio Code to complete all the questions on Day 15. For question 1, I wrote “ print(True + True) “ in VSCode then, I ran it and received the output as 2. The next question, the answer is PyPi in which i get from the notes given in the TryHackMe website. For question 3, I ran the code print(bool(“False”)) in VSCode and got the output as “True”. For question 5, we copy and paste the code given in the question into VSCode. After running the code we get the answer [1, 2, 3, 6]. For the last question, we will be using the same code for both of them. To get the answer for question 7, after we ran the code we input the word Skidy in the terminal, the output that we got is “The Wise One has allowed you to come in.”. Next, we will run the code again but this time, we will input the word “elf” and the answer that we got will be different which is “The Wise One not has allowed you to come in.”