PSP0201

Week 4

Writeup

Group Name: F4urDeveloper

Members:

ID	NAME	ROLE
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	LEADER
1211104237	ALIA MAISARA BINTI SHAHRIN	MEMBER
1211102287	TERRENCE CHENG	MEMBER
1211101153	MISCHELLE THANUSHA JULIUS	MEMBER

Day 11: Networking - The Rogue Gnome

Tools used: THM Machine/THM Attackbox/Kali Linux/Mozilla Firefox

Solution/Walkthrough:

Question 1:

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

The answer for this particular question can be found by reading through the passage on Day 11 as shown in the image below (highlighted for viewing purposes).

> 11.4.2. Vertical Privilege Escalation:
>
> A bit more traditional, a vertical privilege escalation attack involves exploiting a vulnerability that allows you to perform actions like commands or accessing data acting as a higher privileged account such as an administrator.
>
> Remember the attack you performed on "*Day 1 - A Christmas Crisis*"? You modified your cookie to access Santa's control panel. This is a fantastic example of a vertical privilege escalation because you were able to use your user account to access and manage the control panel. This control panel is only accessible by Santa (an administrator), so you are moving your permissions upwards in this sense.

Question 2:

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?

The clue/hint for this question can be found in the statement ‘can run sudo commands’ as proven in the image below (highlighted for viewing purposes).

> 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 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?

The clue/hint for this question can be found in the sentence ‘The privileges are almost similar’ as proven in the image below (highlighted for viewing purposes).

> 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.

Question 4:

What is the name of the file that contains a list of users who are a part of the sudo group?

The answer for this question can be found by reading through 11.8 on Day 11 as shown in the image below (highlighted for viewing purposes). The answer should be sudoers.

> 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:

What is the Linux Command to enumerate the key for SSH?

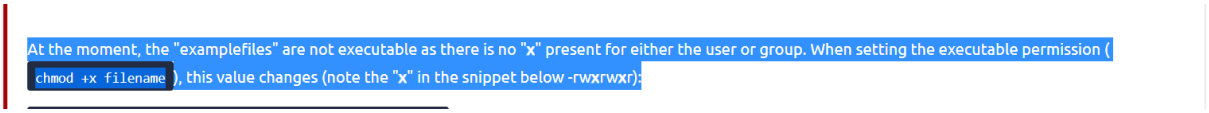
The answer for this question can be found by reading through 11.6 on Day 11 as shown in the image below (highlighted for viewing purposes).

> ### 11.6. You Thought Enumeration Stopped at Nmap?
>
> Wrong! We were just getting started. After gaining initial access, it's essential to begin to build a picture of the internals of the machine. We can look for a plethora of information such as other services that are running, sensitive data including passwords, executable scripts of binaries to abuse and more!
>
> For example, we can use the find command to search for common folders or files that we may suspect to be on the machine:
>
> - backups
> - password
> - admin
> - config
>
> 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:

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?

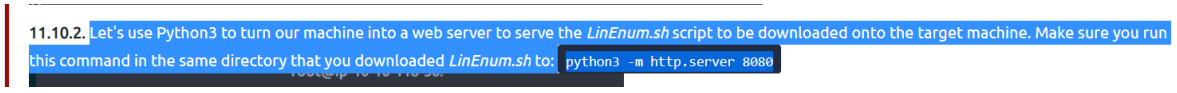
The hint for the answer for this question can be found by reading through 11.8 on Day 11 as shown in the image below. Instead of typing in “chmod +x filename”, we replace the filename with “find.sh” therefore typing in “chmod +x find.sh”.

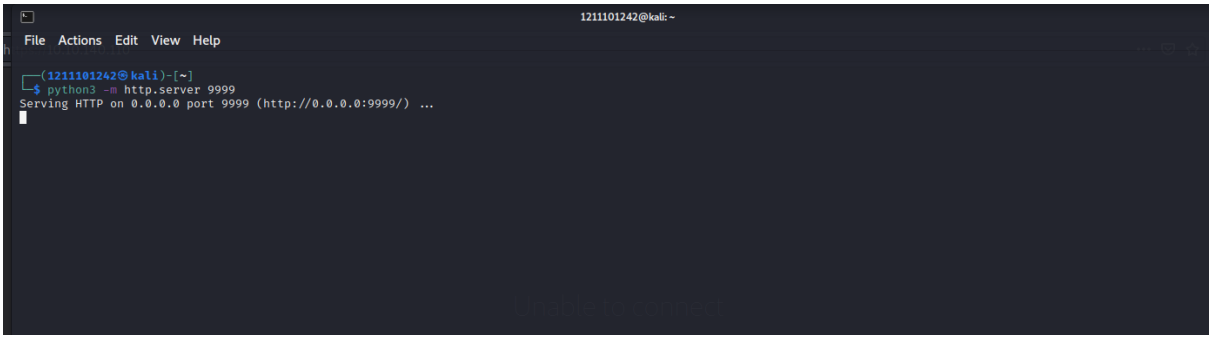


Question 7:

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?

The hint for the answer for this question can be found by reading through 11.10.2 on Day 11 as shown in the image below. Instead of typing in python “-w http.server 8080”, replace the port with 9999 therefore typing in “-w http.server 9999” to host the server.

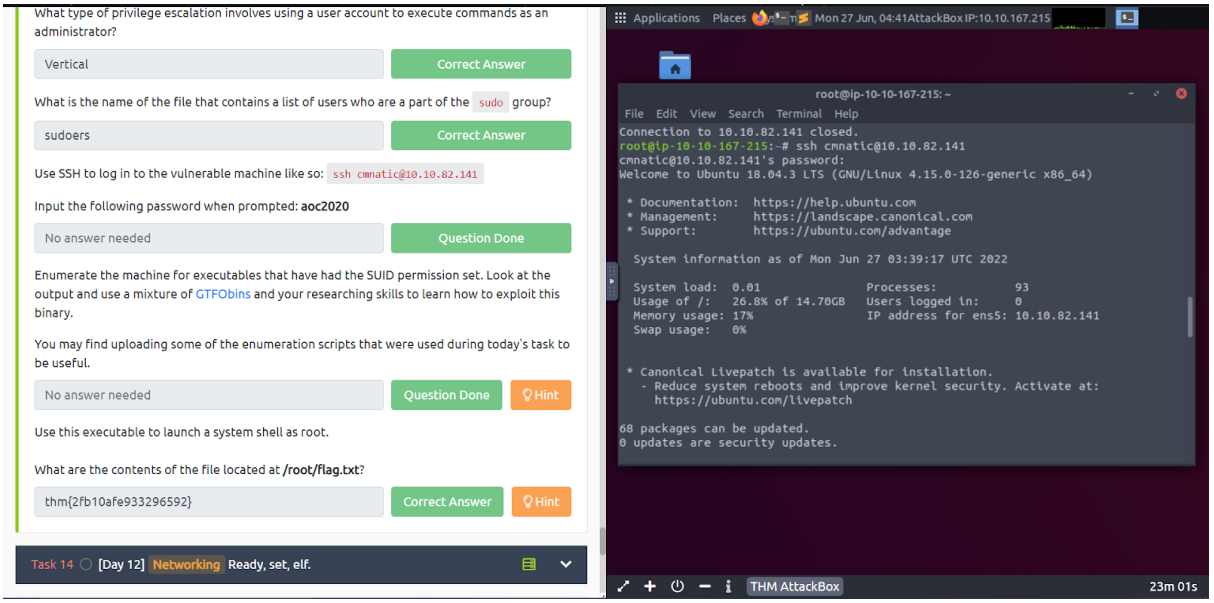




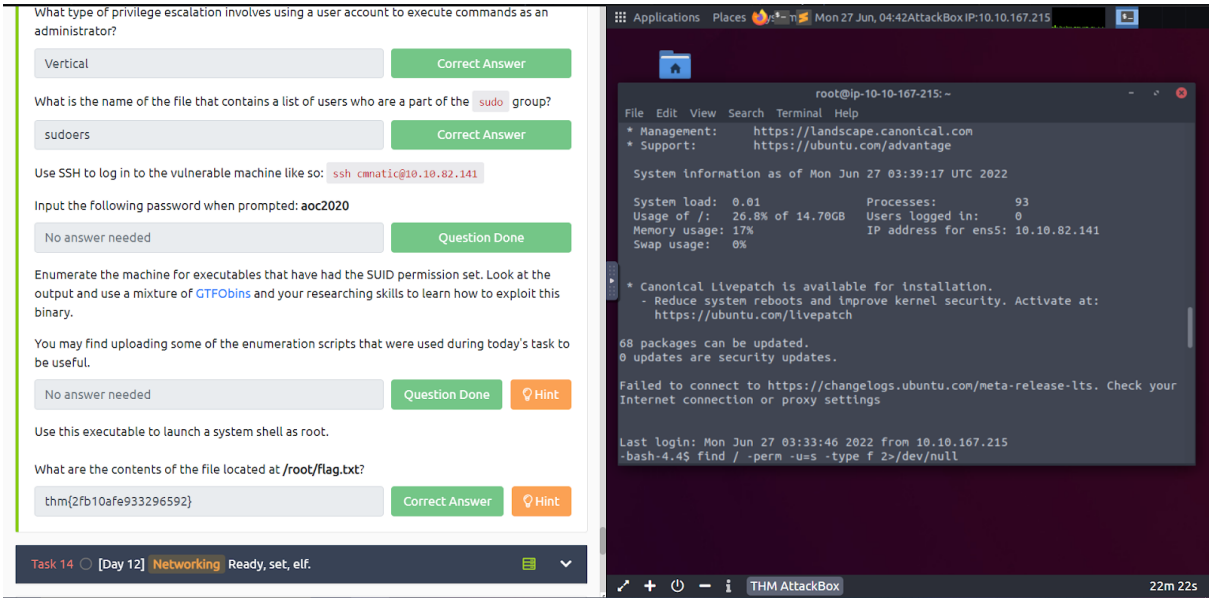
Question 8:

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

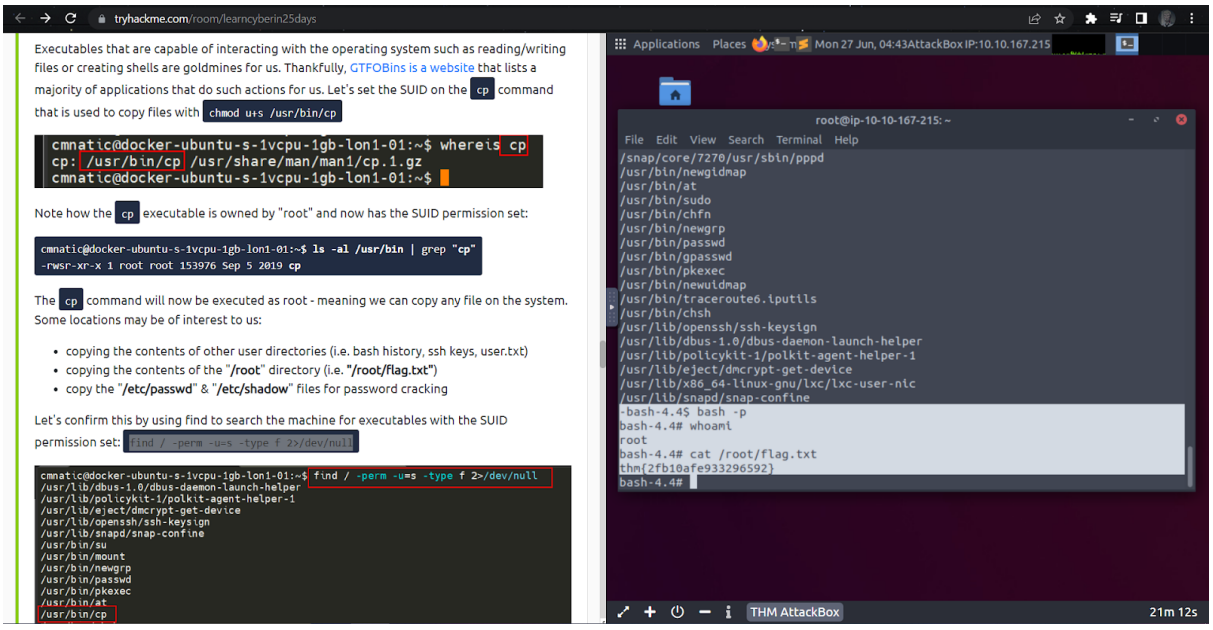
Run the following command in the THM Attackbox terminal, “ssh cmnatic@10.10.82.141” (Note: IP Address is different for each users)



Type in the following command at the bottom of the terminal "`find / -perm -u=s -type f 2>/dev/null`"



Use the "bash -p" command to return back to root from cmnatic and type in "cat /root/flag.txt" to obtain the flag.



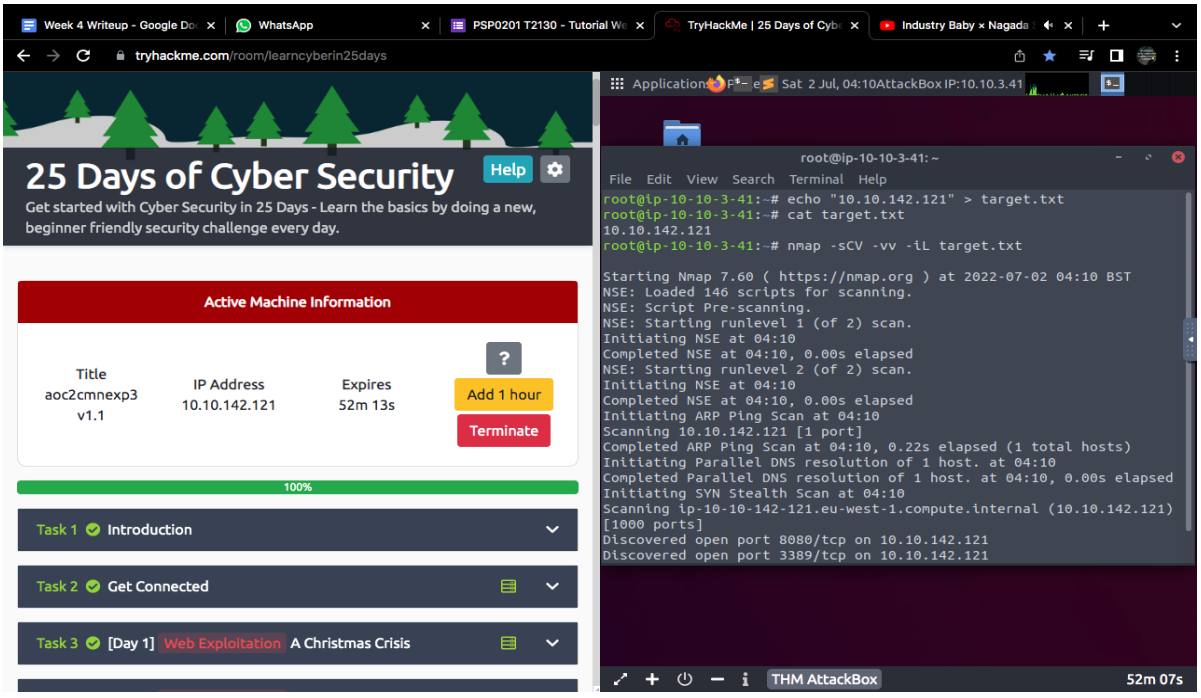
Thought Process/Methodology:

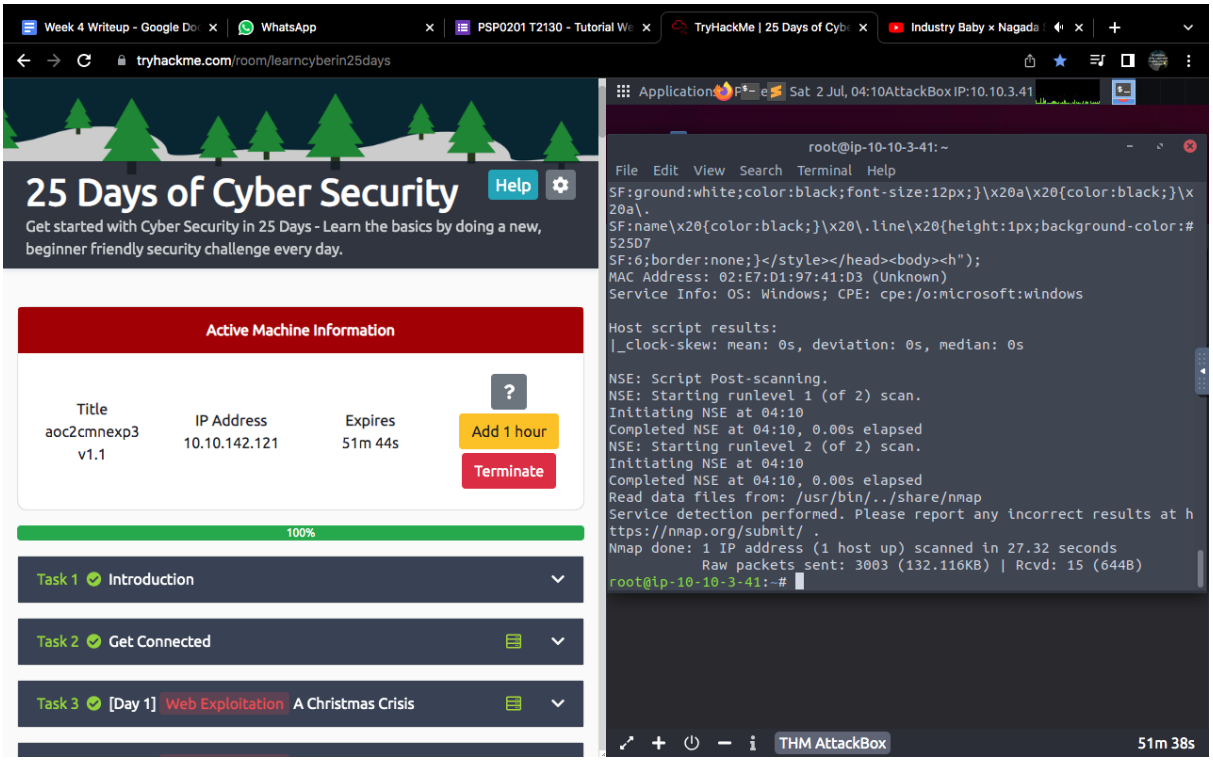
As for question 1, question 2, question 3, question 4, question 5, question 6 and question 7, the answers can be found by reading the entire passage on Day 11. Question 1's and question 2's answer can be found on 11.4.2, question 3's answer can be found on 11.4.1, question 4's answer can be found by reading through 11.8, question 5's answer can be found on 11.6, question 6's answer can also be found on 11.8 but change the filename to file.sh as given in the questions, question 7's answer can be found on 11.10.2 but change the port to 9999 as given in the questions. As for question 8, we have to run the following command first before proceeding "ssh cmnatic@IP ADDRESS". After doing so, scroll down to the bottom of the terminal and type in the following command "find / -perm -u=s -type f 2>/dev/null". Scroll down to the bottom of the terminal again to type in the following bash command which is bash -p to return to the root and type in "cat /root/flag.txt" to obtain the flag.

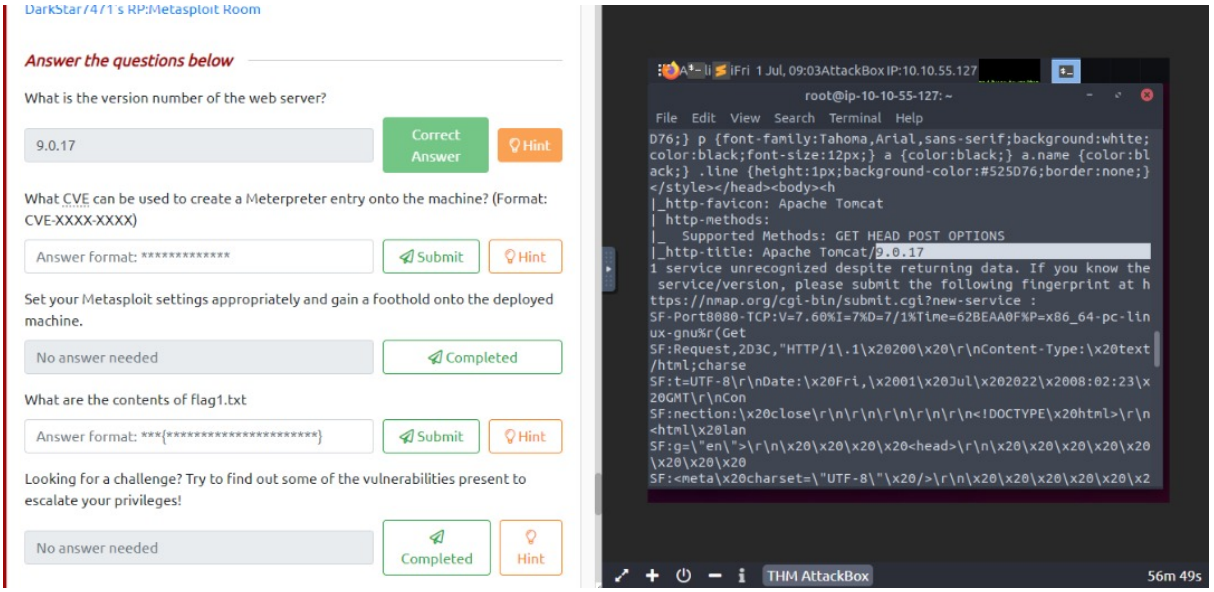
Day 12 - Networking Ready, set, elf.
Tools used: THM Machine/THM Attackbox

Solution/walkthrough

Question1
What is the version number of the web server?



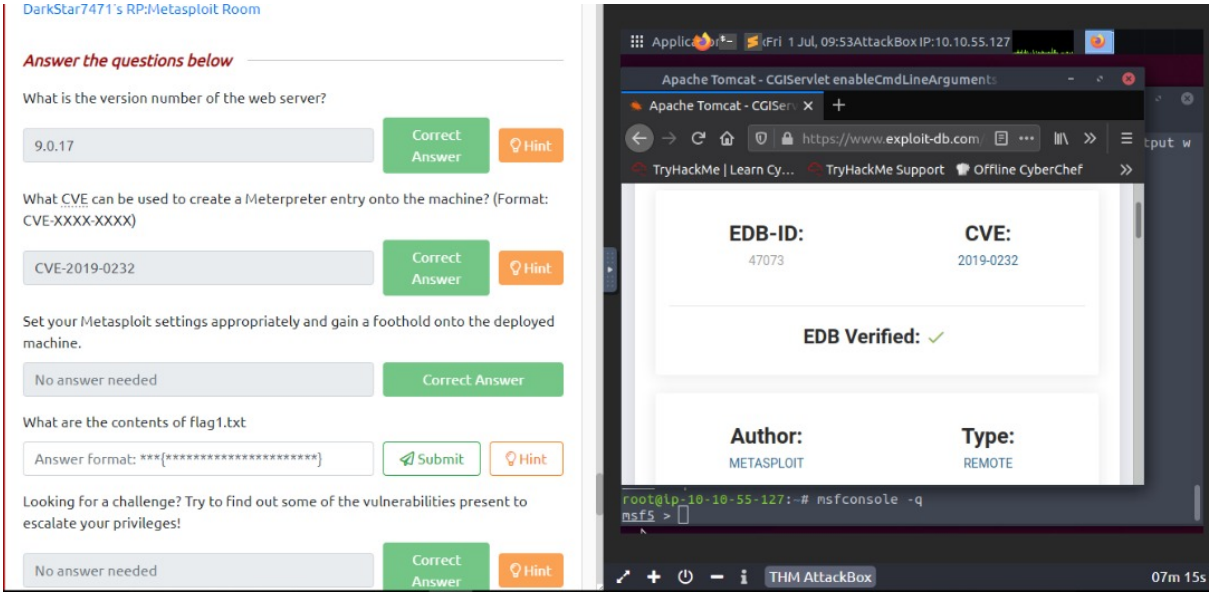




The version of the web series is 9.0.17.

Question 2

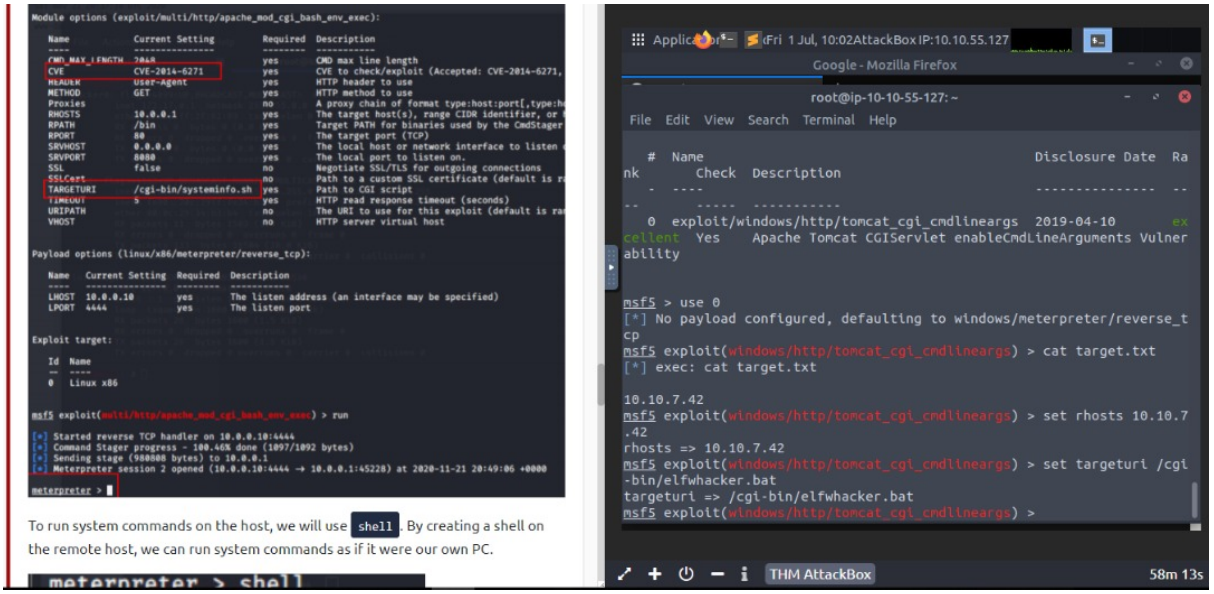
What CVE can be used to create a Meterpreter entry onto the machine?

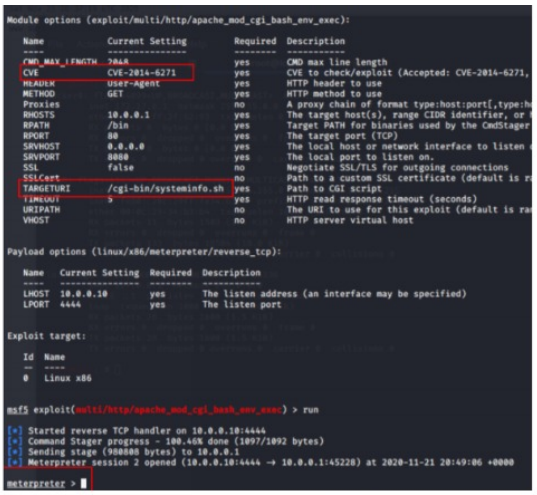


The CVE that can be used to create a Meterpreter entry onto the machine is CVE 2019-0232.

Question 3

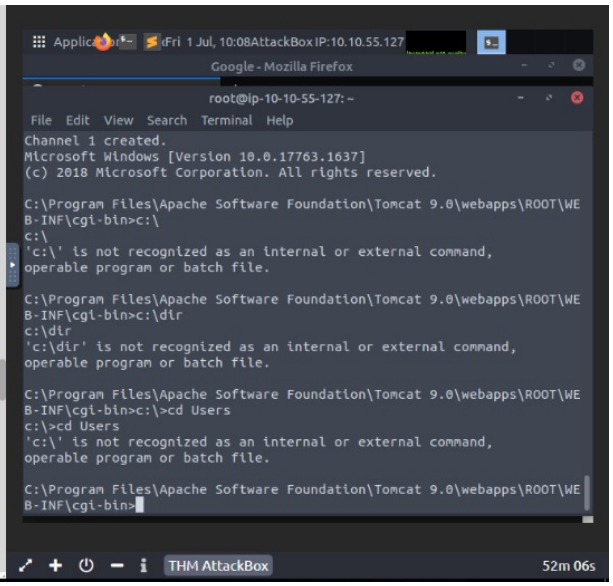
What are the contents of flag1.txt?

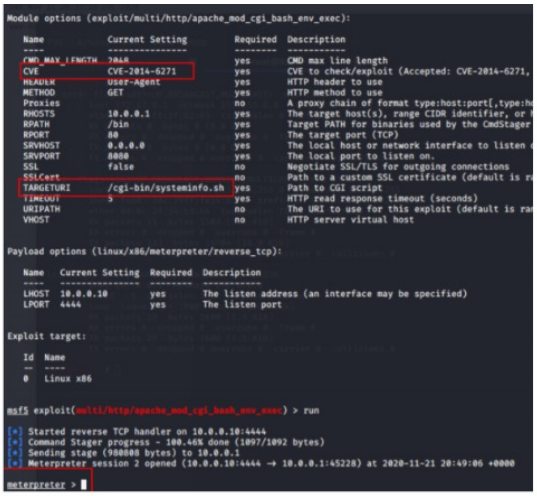




To run system commands on the host, we will use `shell`. By creating a shell on the remote host, we can run system commands as if it were our own PC.

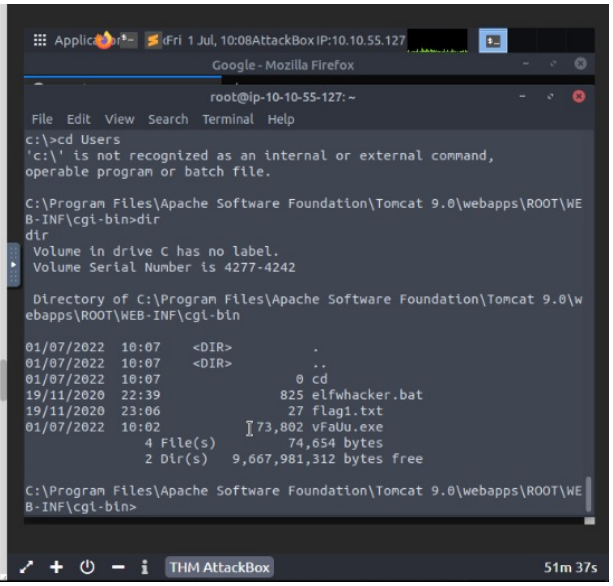
```
meterpreter > shell
```

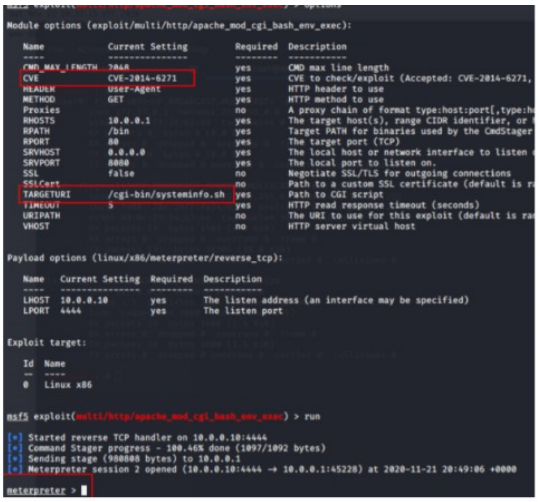




To run system commands on the host, we will use `shell`. By creating a shell on the remote host, we can run system commands as if it were our own PC.

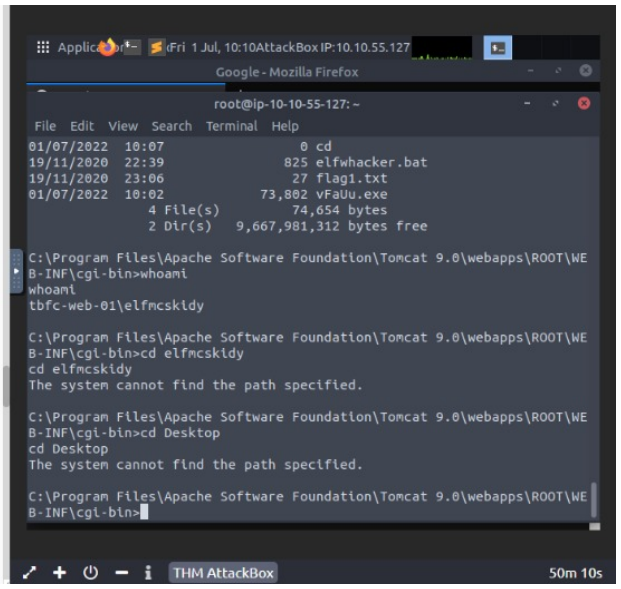
```
meterpreter > shell
```

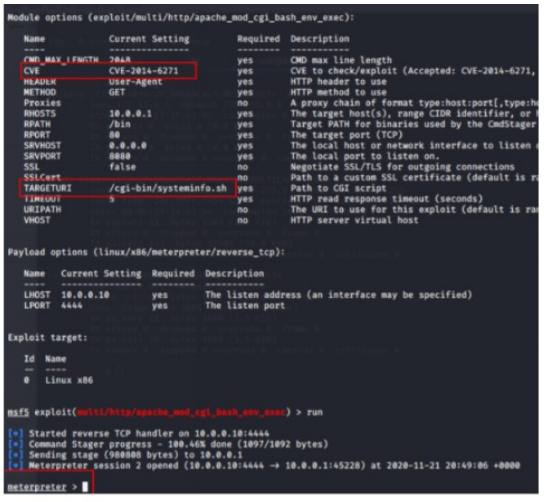




To run system commands on the host, we will use `shell`. By creating a shell on the remote host, we can run system commands as if it were our own PC.

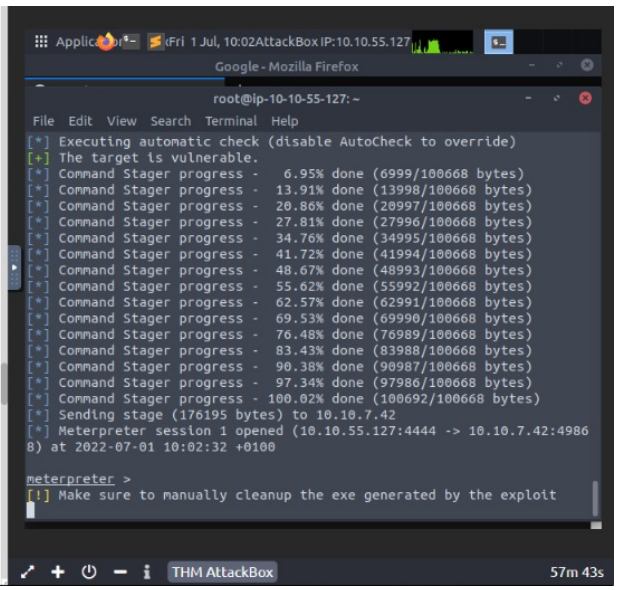
```
meterpreter > shell
```

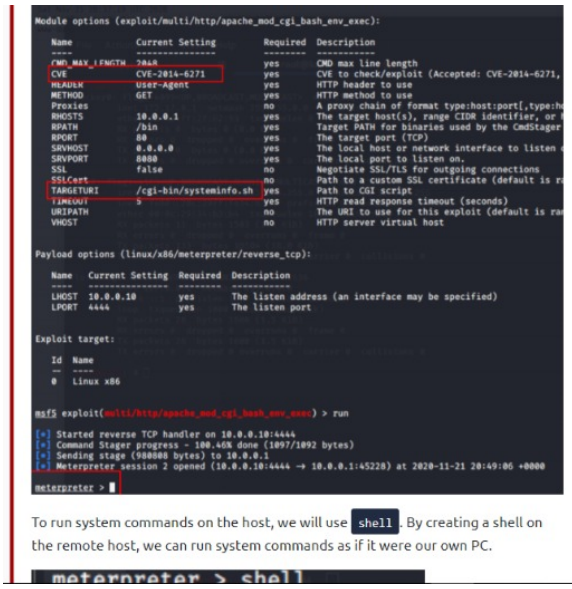




To run system commands on the host, we will use `shell`. By creating a shell on the remote host, we can run system commands as if it were our own PC.

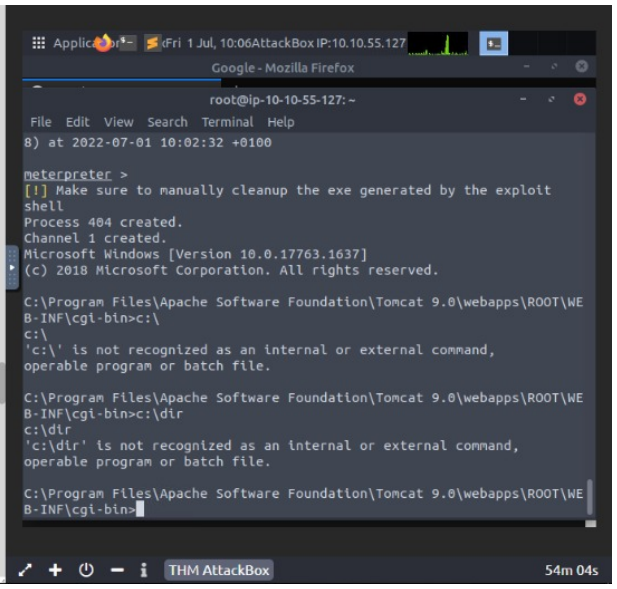
```
meterpreter > shell
```

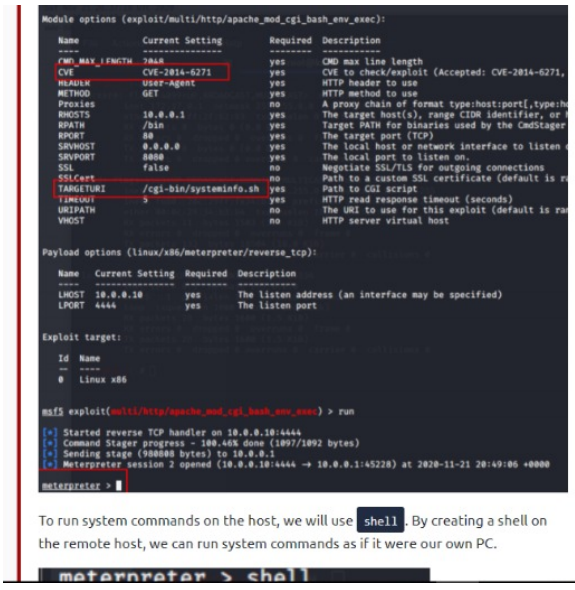




To run system commands on the host, we will use `shell`. By creating a shell on the remote host, we can run system commands as if it were our own PC.

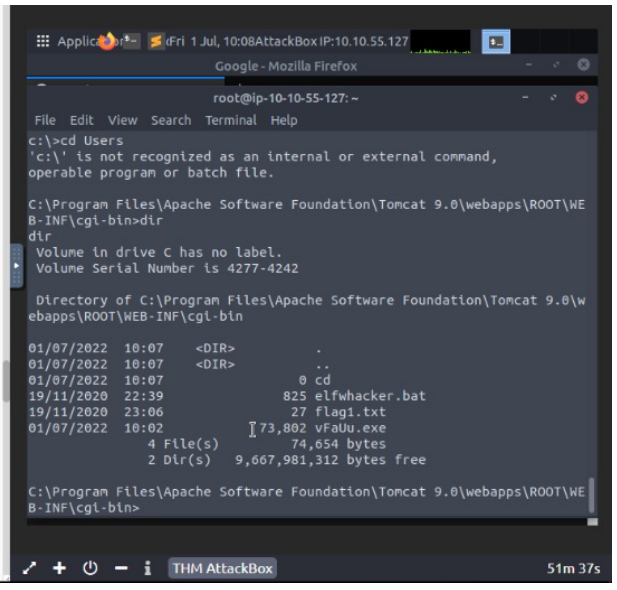
```
meterpreter > shell
```

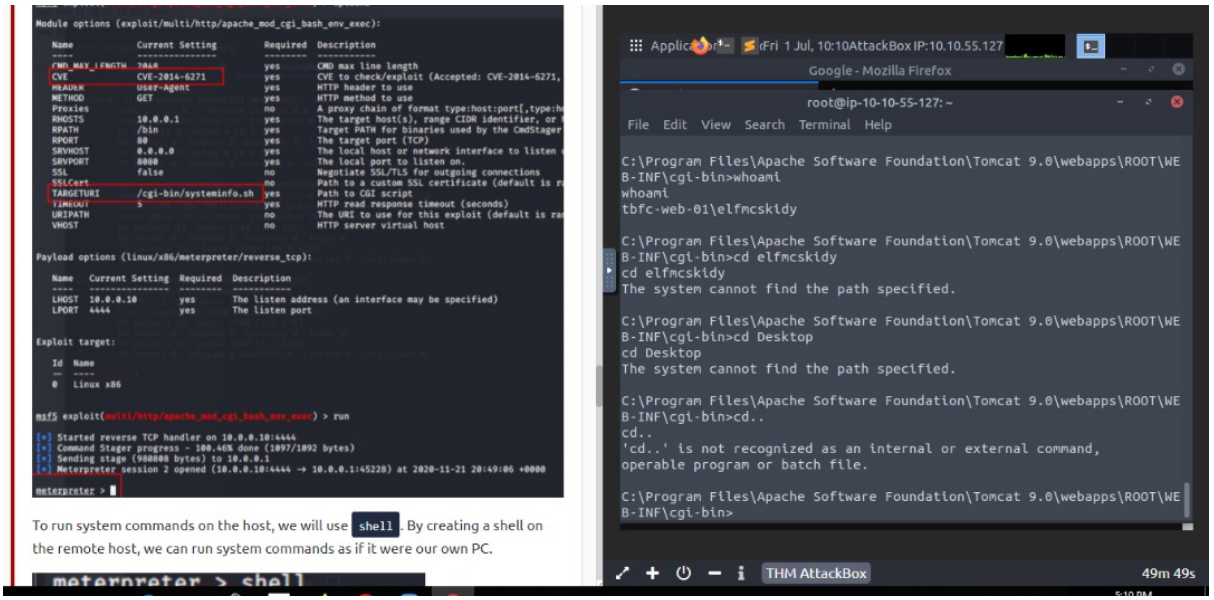




To run system commands on the host, we will use `shell`. By creating a shell on the remote host, we can run system commands as if it were our own PC.

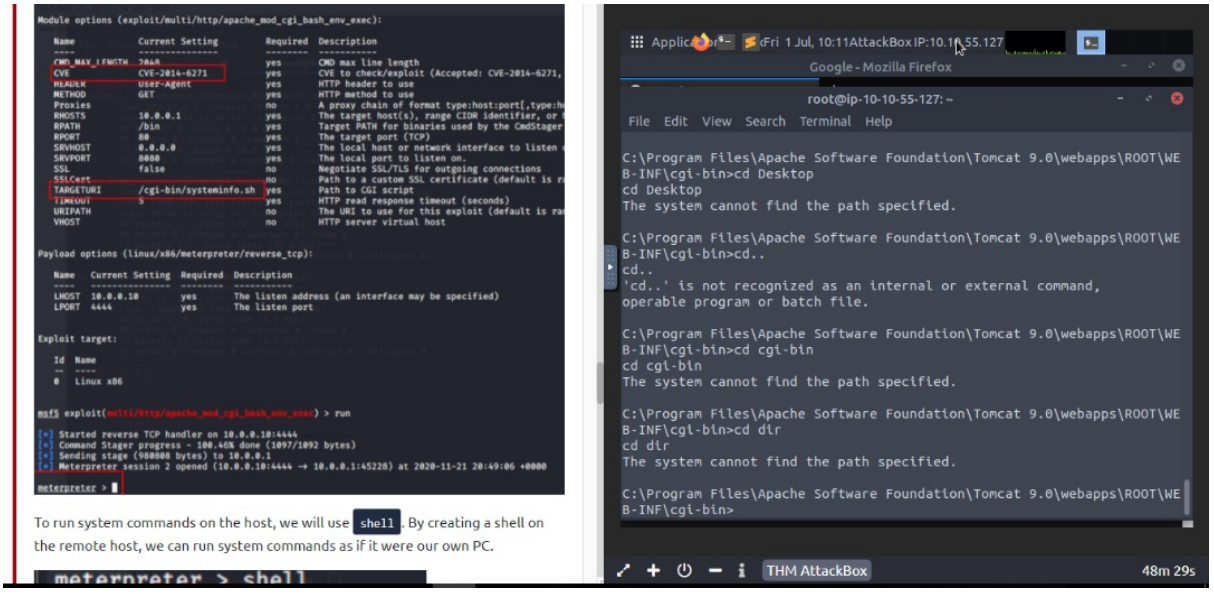
```
meterpreter > shell
```





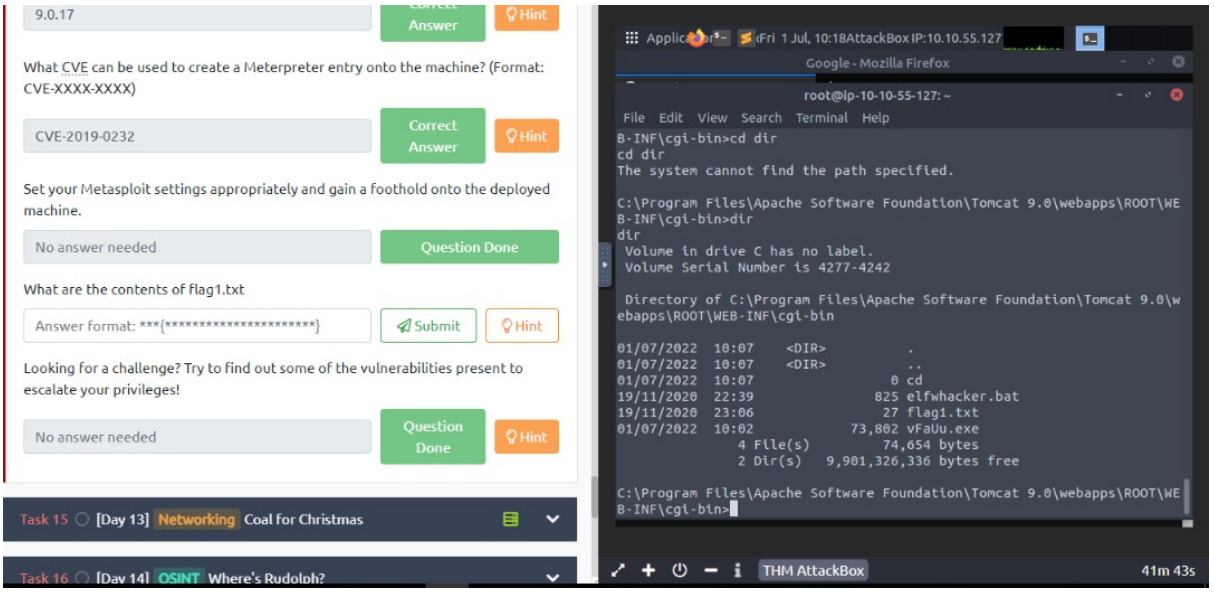
To run system commands on the host, we will use `shell`. By creating a shell on the remote host, we can run system commands as if it were our own PC.

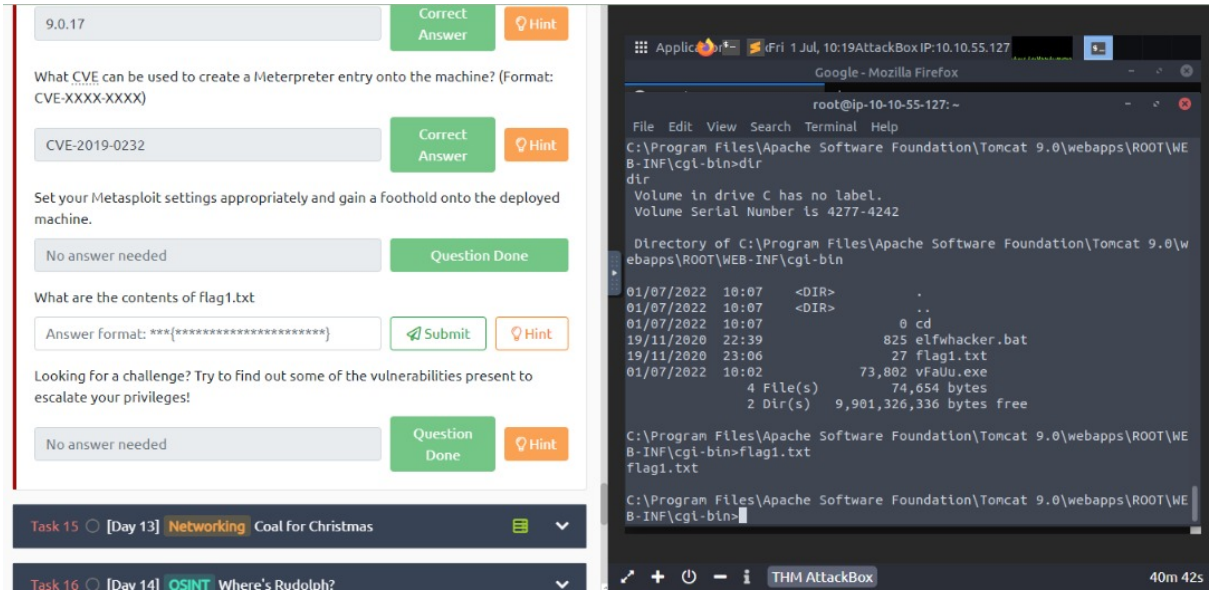
```
meterpreter > shell
```

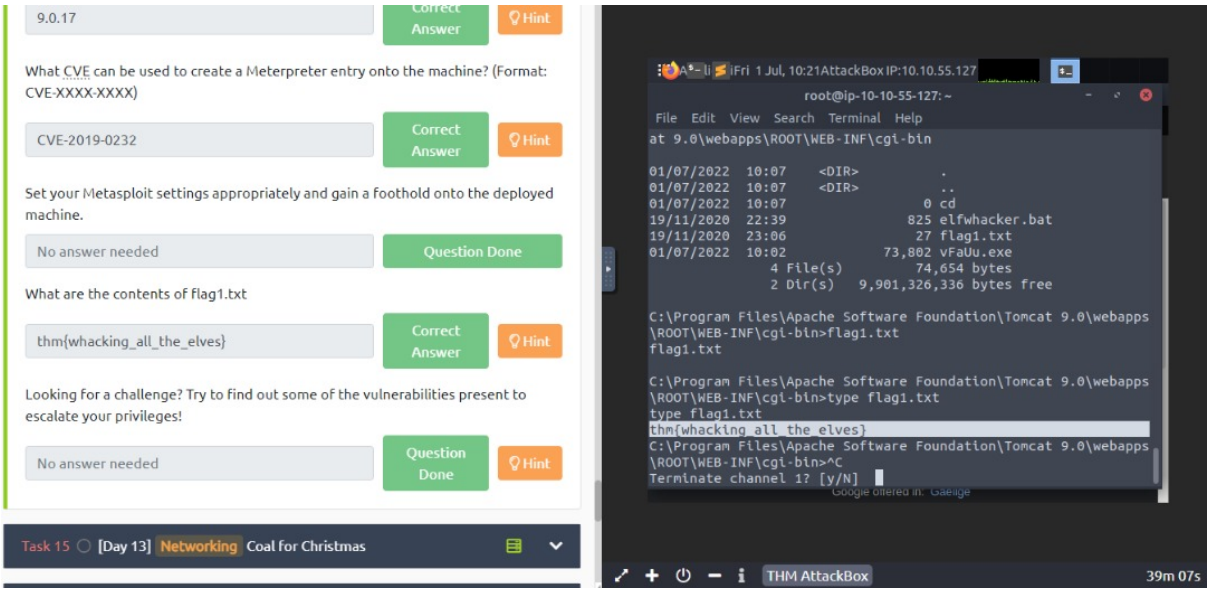


To run system commands on the host, we will use `shell`. By creating a shell on the remote host, we can run system commands as if it were our own PC.

```
meterpreter > shell
```


9.0.17
Correct Answer
Hint
What CVE can be used to create a Meterpreter entry onto the machine? (Format: CVE-XXXX-XXXX)
CVE-2019-0232
Correct Answer
Hint
Set your Metasploit settings appropriately and gain a foothold onto the deployed machine.
No answer needed
Question Done
What are the contents of flag1.txt
Answer format: ***{**********}
Submit
Hint
Looking for a challenge? Try to find out some of the vulnerabilities present to escalate your privileges!
No answer needed
Question Done
Hint
Task 15 [Day 13] Networking Coal for Christmas
Task 16 [Day 14] OSINT Where's Rudolph?
Fri 1 Jul, 10:18
AttackBox IP:10.10.55.127
Google - Mozilla Firefox
root@ip-10-10-55-127: ~
File Edit View Search Terminal Help
B-INF\cgi-bin>cd dir
cd dir
The system cannot find the path specified.
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WE
B-INF\cgi-bin>dir
dir
Volume in drive C has no label.
Volume Serial Number is 4277-4242
Directory of C:\Program Files\Apache Software Foundation\Tomcat 9.0\w
ebapps\ROOT\WEB-INF\cgi-bin
01/07/2022 10:07 <DIR> .
01/07/2022 10:07 <DIR> ..
01/07/2022 10:07 0 cd
19/11/2020 22:39 825 elfwhacker.bat
19/11/2020 23:06 27 flag1.txt
01/07/2022 10:02 73,802 vFaUu.exe
4 File(s) 74,654 bytes
2 Dir(s) 9,901,326,336 bytes free
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WE
B-INF\cgi-bin>
THM AttackBox
41m 43s

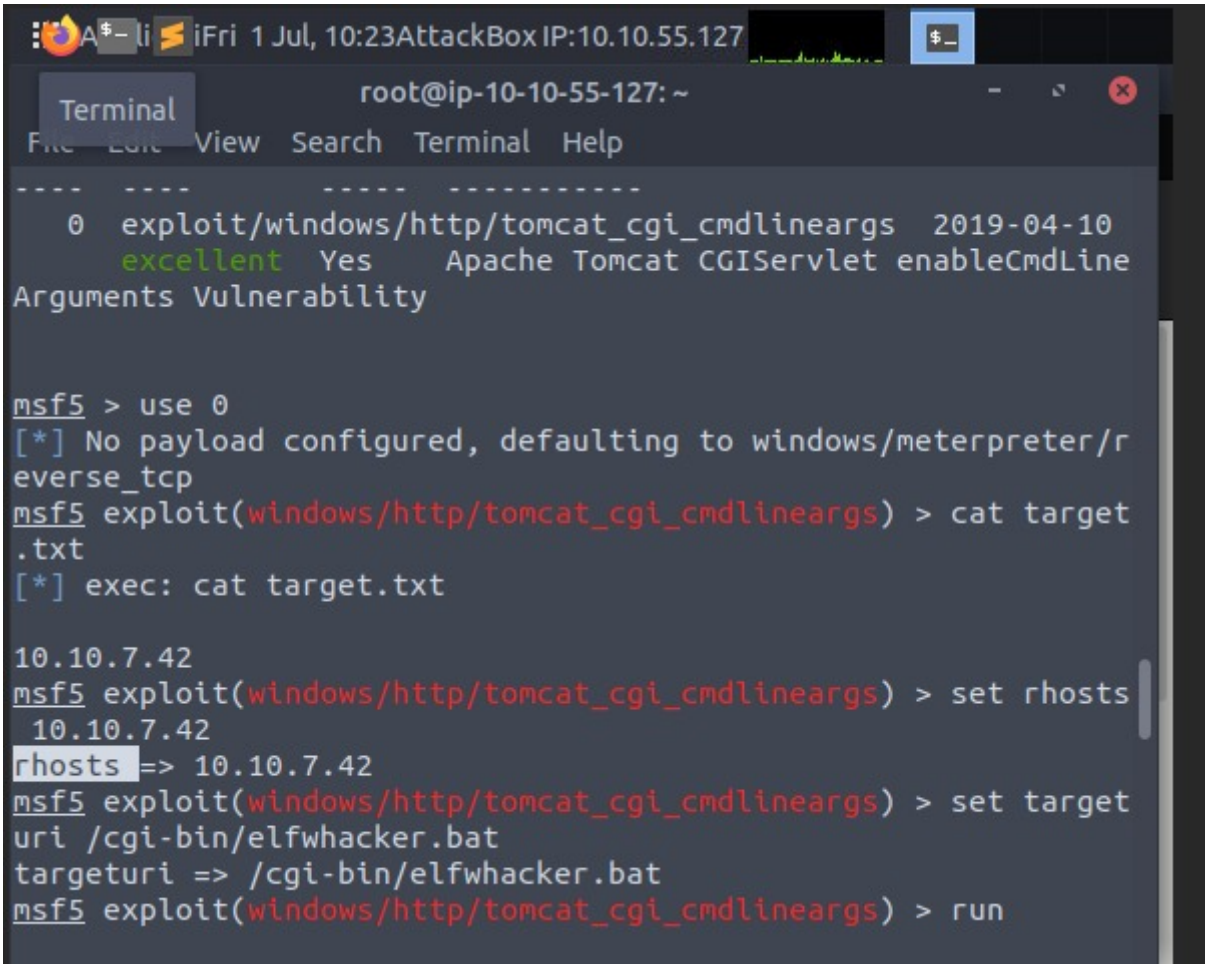

9.0.17
Correct Answer
Hint
What CVE can be used to create a Meterpreter entry onto the machine? (Format: CVE-XXXX-XXXX)
CVE-2019-0232
Correct Answer
Hint
Set your Metasploit settings appropriately and gain a foothold onto the deployed machine.
No answer needed
Question Done
What are the contents of flag1.txt
Answer format: ***{**********}
Submit
Hint
Looking for a challenge? Try to find out some of the vulnerabilities present to escalate your privileges!
No answer needed
Question Done
Hint
Task 15 [Day 13] Networking Coal for Christmas
Task 16 [Day 14] OSINT Where's Rudolph?
Fri 1 Jul, 10:19
AttackBox IP:10.10.55.127
Google - Mozilla Firefox
root@ip-10-10-55-127: ~
File Edit View Search Terminal Help
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WE
B-INF\cgi-bin>dir
dir
Volume in drive C has no label.
Volume Serial Number is 4277-4242
Directory of C:\Program Files\Apache Software Foundation\Tomcat 9.0\w
ebapps\ROOT\WEB-INF\cgi-bin
01/07/2022 10:07 <DIR> .
01/07/2022 10:07 <DIR> ..
01/07/2022 10:07 0 cd
19/11/2020 22:39 825 elfwhacker.bat
19/11/2020 23:06 27 flag1.txt
01/07/2022 10:02 73,802 vFaUu.exe
4 File(s) 74,654 bytes
2 Dir(s) 9,901,326,336 bytes free
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WE
B-INF\cgi-bin>flag1.txt
flag1.txt
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WE
B-INF\cgi-bin>
THM AttackBox
40m 42s



The flag will be thm{whacking_all_the_elves} that is highlighted in the terminal.

Question 4

What were the Metasploit settings you had to set?



The Metasploit settings that we have to set is the rhosts setting as had been already highlighted in the terminal.

Thought Process/Methodology:

As for question number 1, the answer can be found after typing in echo “ip address” > target.txt , cat target.txt and nmap -sCV -vv -iL target.txt and we can found the answer by scrolling the terminal .Next for question 2, type in apache 9.0.17(web series number) to get the CVE that can be used to create a Meterpreter entry onto the machine. For question 3, find the Metasploit and then type in shell, c:\ , c:\dir, c:\>cd Users, dir,: whoami, cd elfmcskidy , cd Desktopcd, cd.., cgi-bin, cd dir and dir to get the flag. Lastly, for question 4, the Metasploit settings that have to set is rhost that can be found in the terminal.

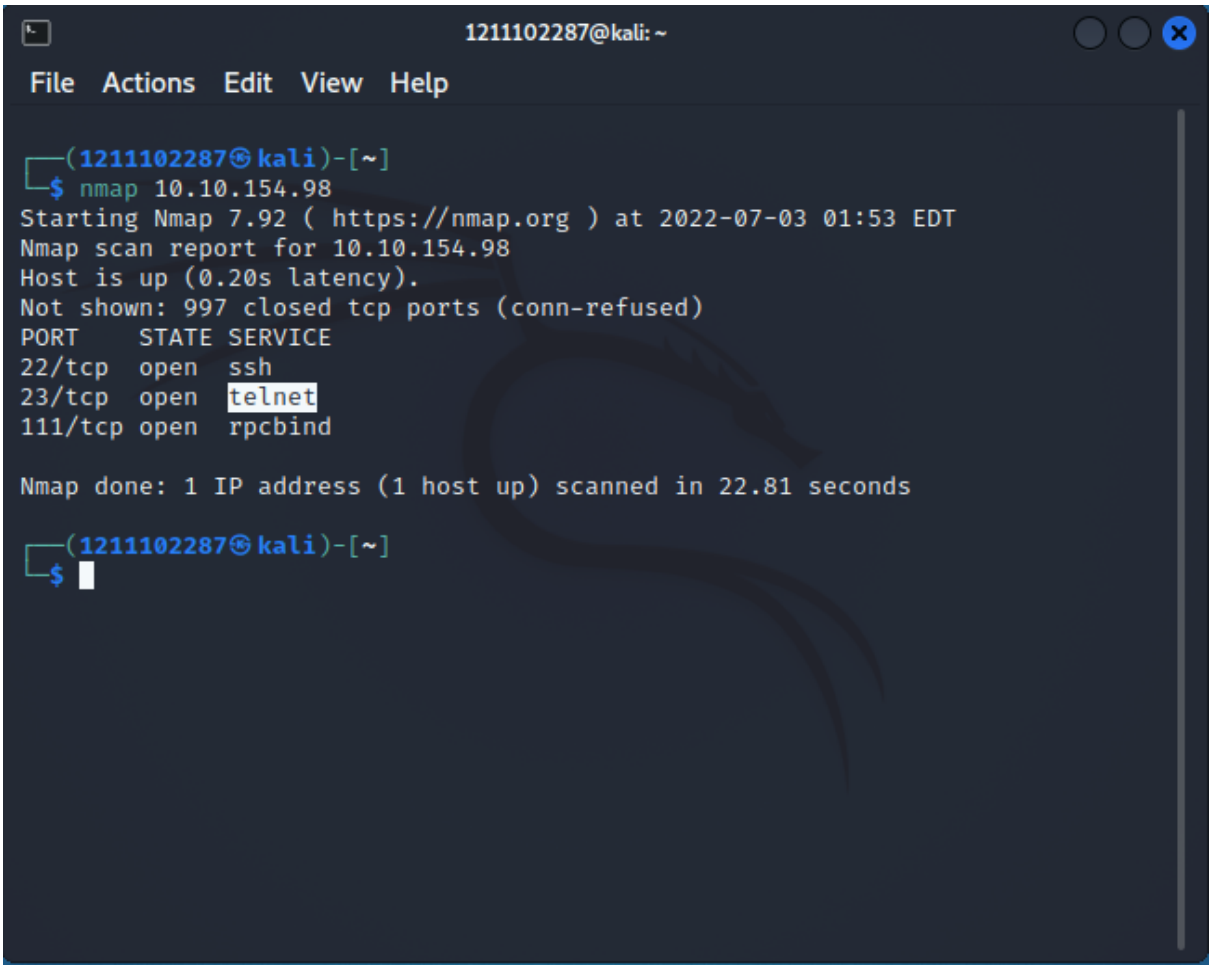
Day 13 : Networking - Coal for Christmas

Tools used: THM Machine/Kali Linux/Mozilla Firefox/Nmap

Solution/Walkthrough:

Question 1

What old, deprecated protocol and service is running?



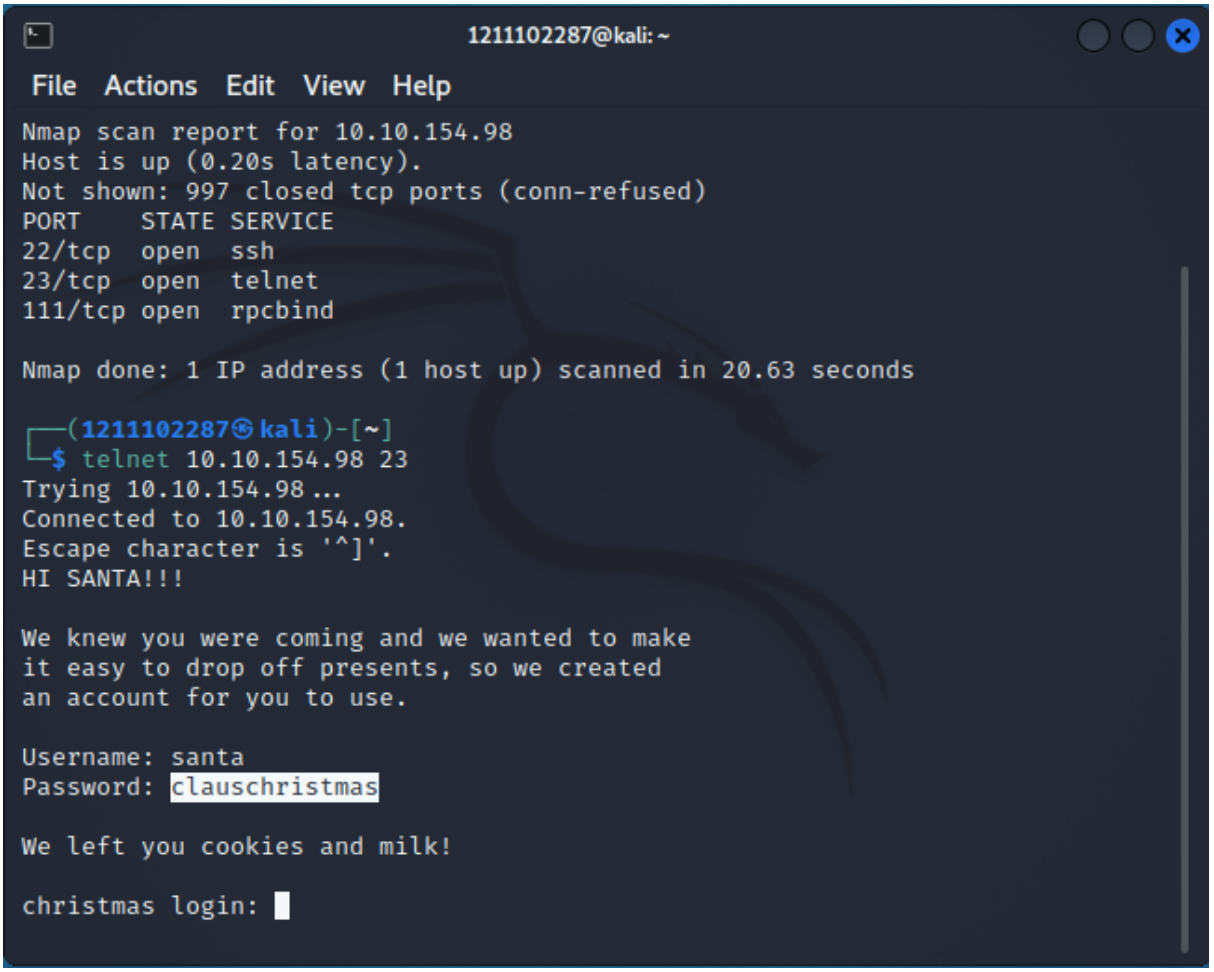
To scan the machine, use nmap with syntax by entering the command nmap IP address (10.10.154.98) on the terminal window. The deprecated protocol and service is shown on the second line of the Service section.

Question 2

What credential was left for you?

Connect to this service to see if you can make use of it. You can connect to the service with the standard command-line client, named after the name of the service, or **netcat** with syntax like this:

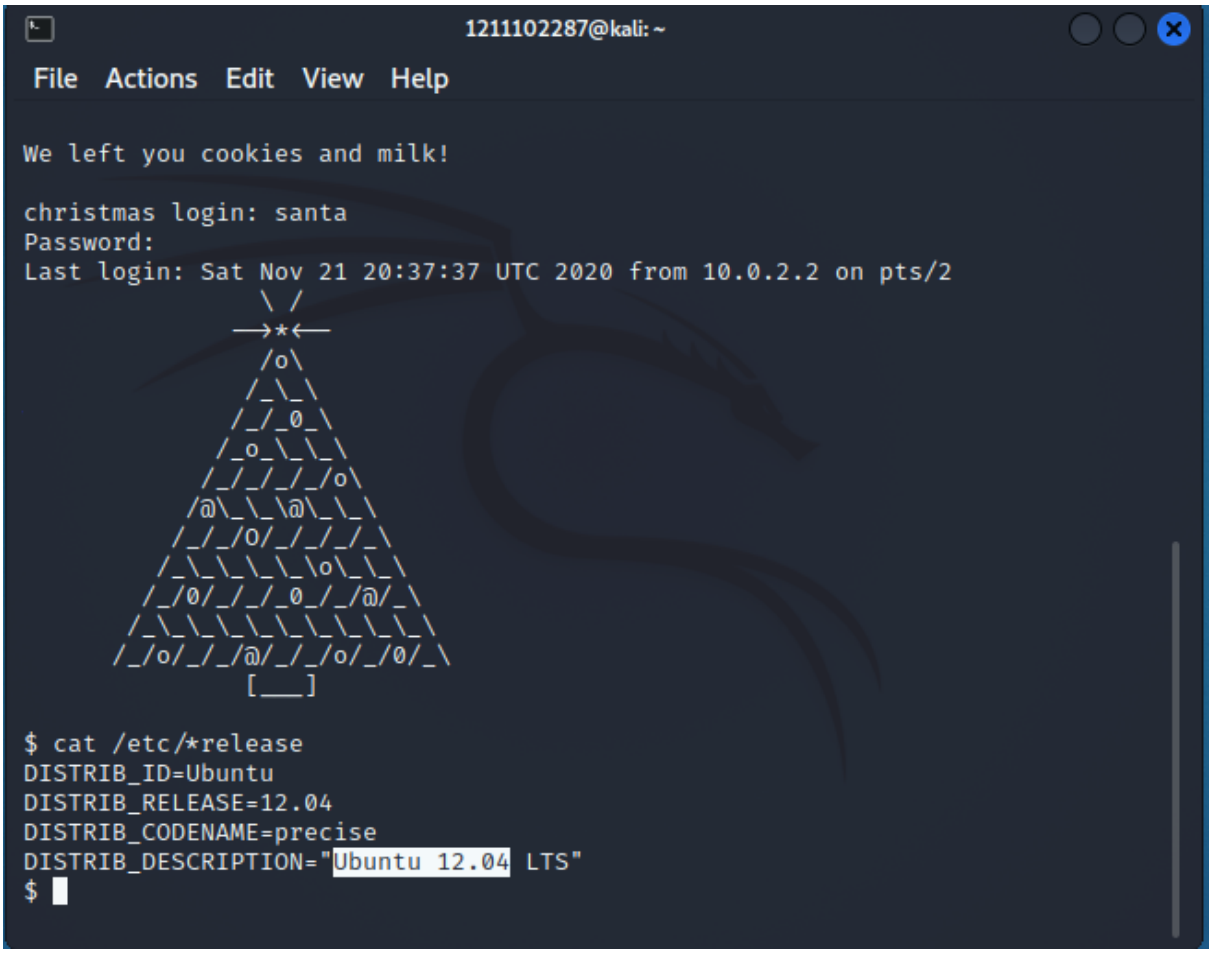
```
telnet 10.10.254.24 <PORT_FROM_NMAP_SCAN>
```



Following the hint, use the netcat with syntax with the command **telnet 10.10.254.24 23 (23 means the port we are referring to)** to connect to the service. Scrolling down we can see the credential (password) being left in the terminal (highlighted for reference).

Question 3

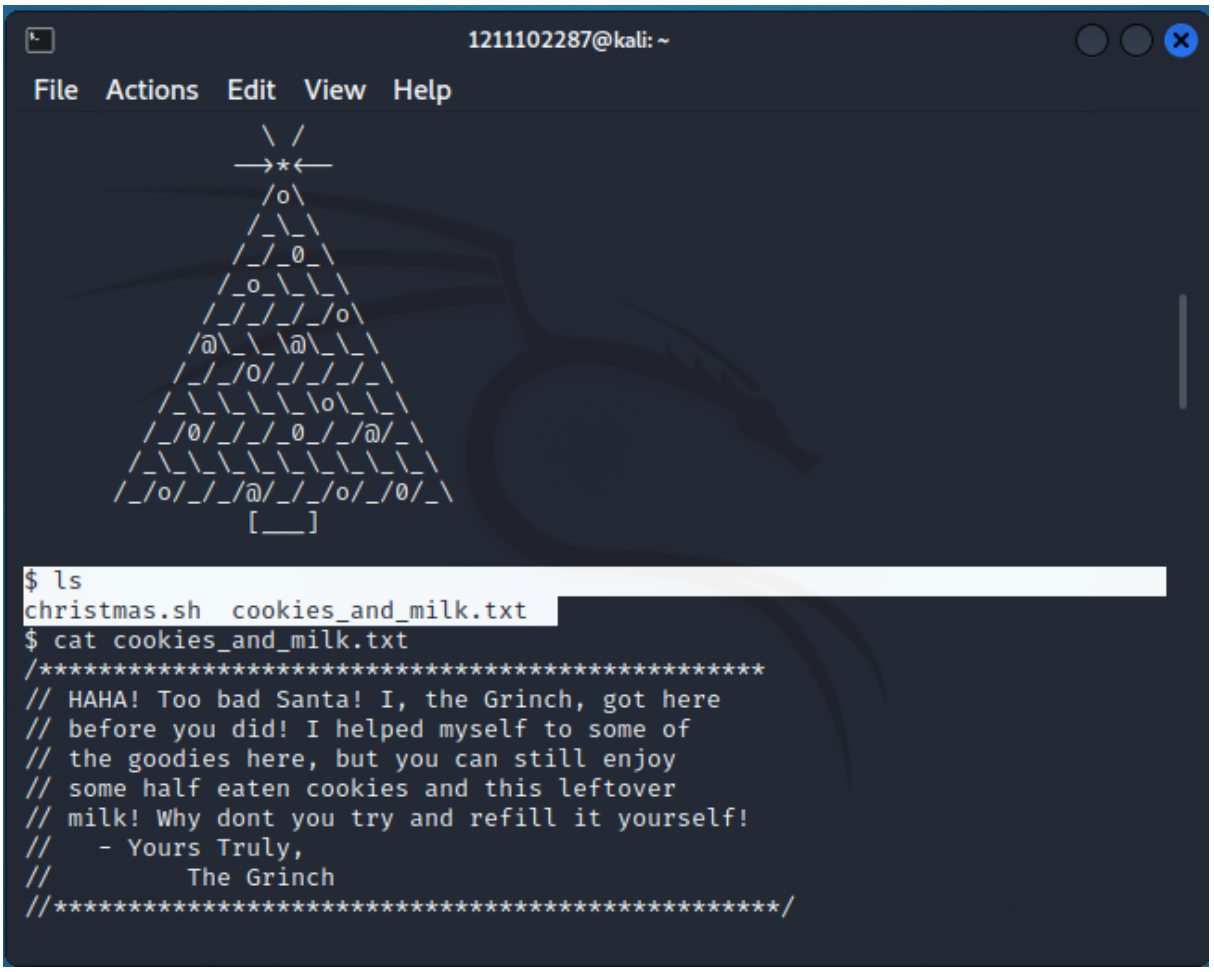
What distribution of Linux and version number is this server running?



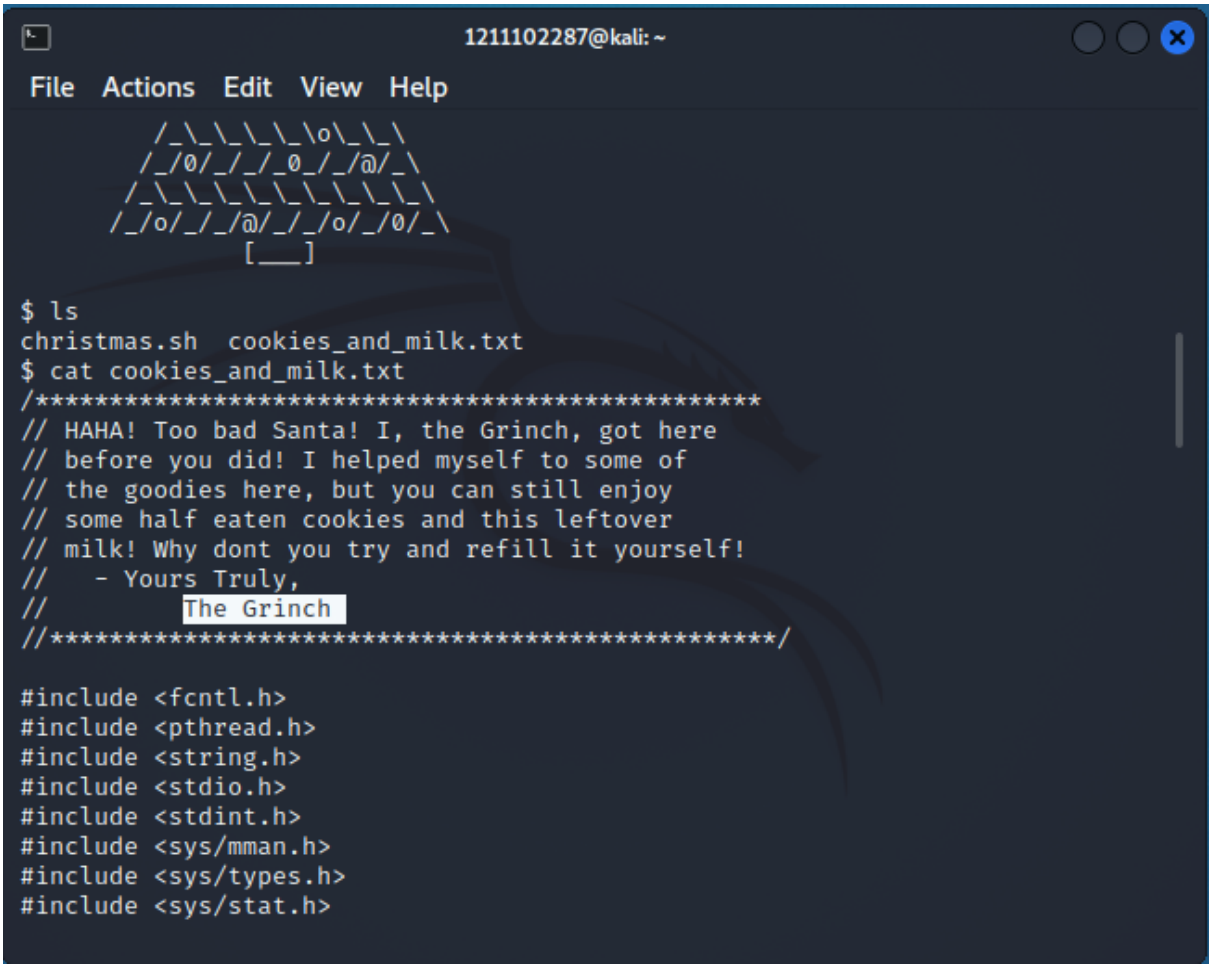
Log into the account by typing the credentials given there. We can look for the distribution of Linux and version number running in the server by typing the `cat /etc/*release` command. We can see the version in the description part (highlighted in the picture)

Question 4

Who got here first?



We can view files and folders in the current directory with the command “ls”. Two files are stored inside (highlighted).



To view the content inside of the text file which is shown in the terminal, “cat” is being used in front of the file we want to access. Read the context and we can see the name in the terminal (Highlighted).

Question 5

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

PoCs

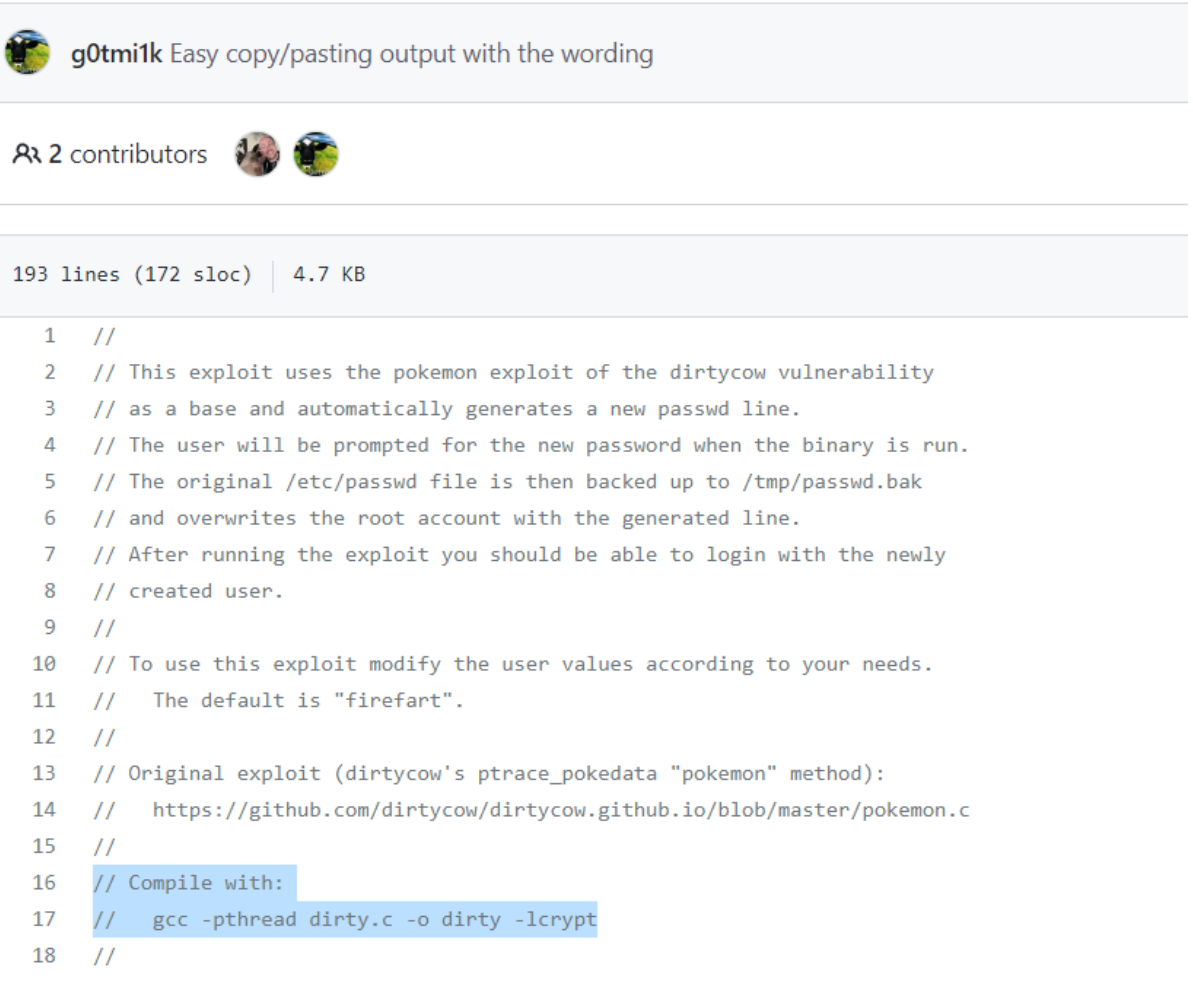
Nick Bulischeck edited this page on Apr 9, 2019 · 51 revisions

Table of PoCs

Note: if you experience crashes or locks take a look at this fix.

Link	Usage	Description	Family
dirtyc0w.c	`./dirtyc0w file content`	Read-only write	/proc/self/mem
cowroot.c	`./cowroot`	SUID-based root	/proc/self/mem
dirtycow-mem.c	`./dirtycow-mem`	libc-based root	/proc/self/mem
pokemon.c	`./d file content`	Read-only write	PTRACE_POKEDATA
dirtycow.cr	`dirtycow --target --string --offset`	Read-only write	/proc/self/mem
dirtyc0w.c	`./dirtycow file content`	Read-only write (Android)	/proc/self/mem
dirtycow.rb	`use exploit/linux/local/dirtycow` and `run`	SUID-based root	/proc/self/mem
0xdeadbeef.c	`./0xdeadbeef`	vDSO-based root	PTRACE_POKEDATA
naughtyc0w.c	`./c0w suid`	SUID-based root	/proc/self/mem
c0w.c	`./c0w`	SUID-based root	PTRACE_POKEDATA
dirty_pass[...].c	`./dirty_passwd_adjust_cow`	/etc/passwd based root	/proc/self/mem
mucow.c	`./mucow destination < payload.exe`	Read-only write (multi page)	PTRACE_POKEDATA
cowpy.c	`r2pm -i dirtycow`	Read-only write (radare2)	/proc/self/mem
dirtycow.fasm	`./main`	SUID-based root	/proc/self/mem
dcow.cpp	`./dcow`	/etc/passwd based root	/proc/self/mem
dirtyc0w.go	`go run dirtyc0w.go -f=file -c=content`	Read-only write	/proc/self/mem
dirty.c	`./dirty`	/etc/passwd based root	PTRACE_POKEDATA

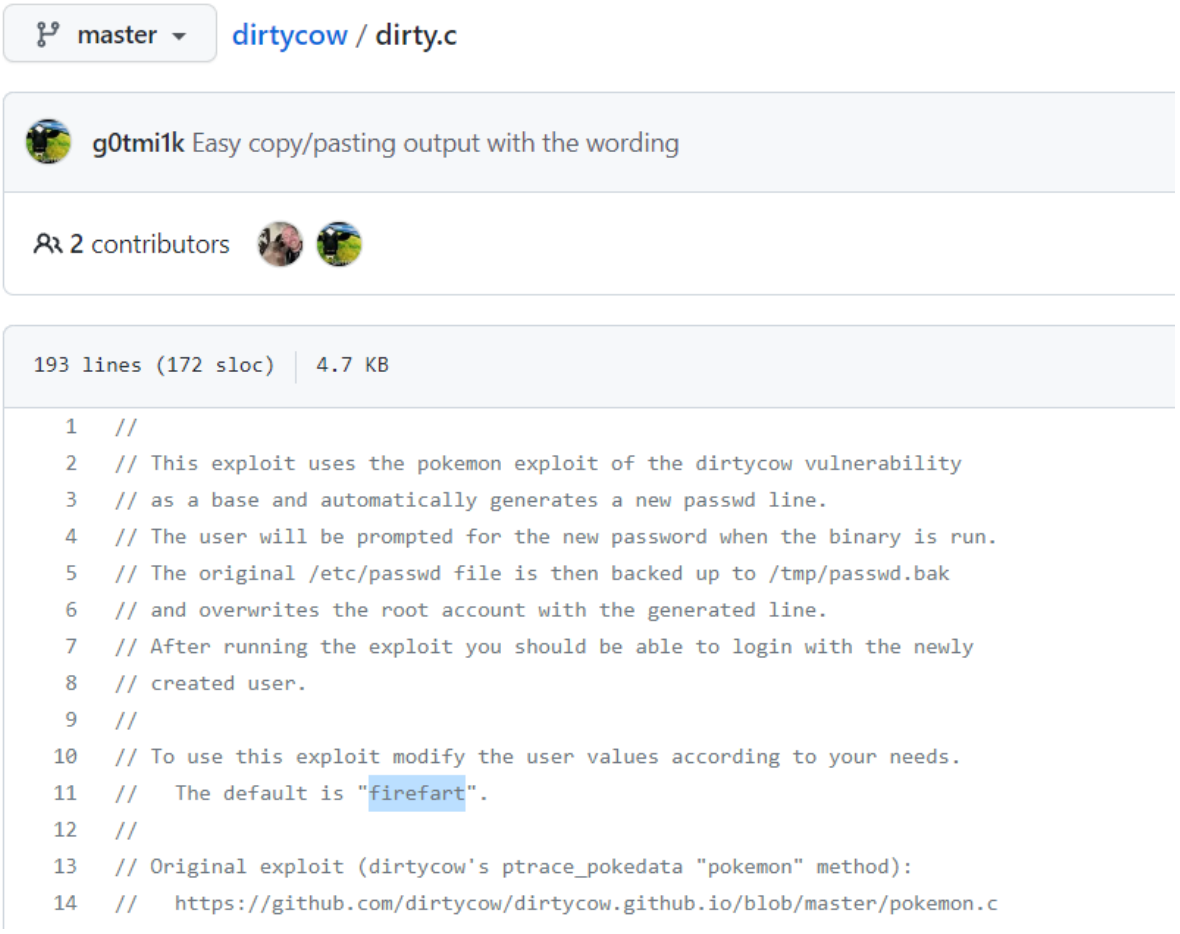
Looking into the DirtyCow exploit online, we need to find the **Original** C source code in the certain folder. We can find one link which is **dirty.c** that saves the C source code.



The verbatim syntax we can use to compile, taken from the real C source code comments, is written on the **17th line** in the folder.

Question 6

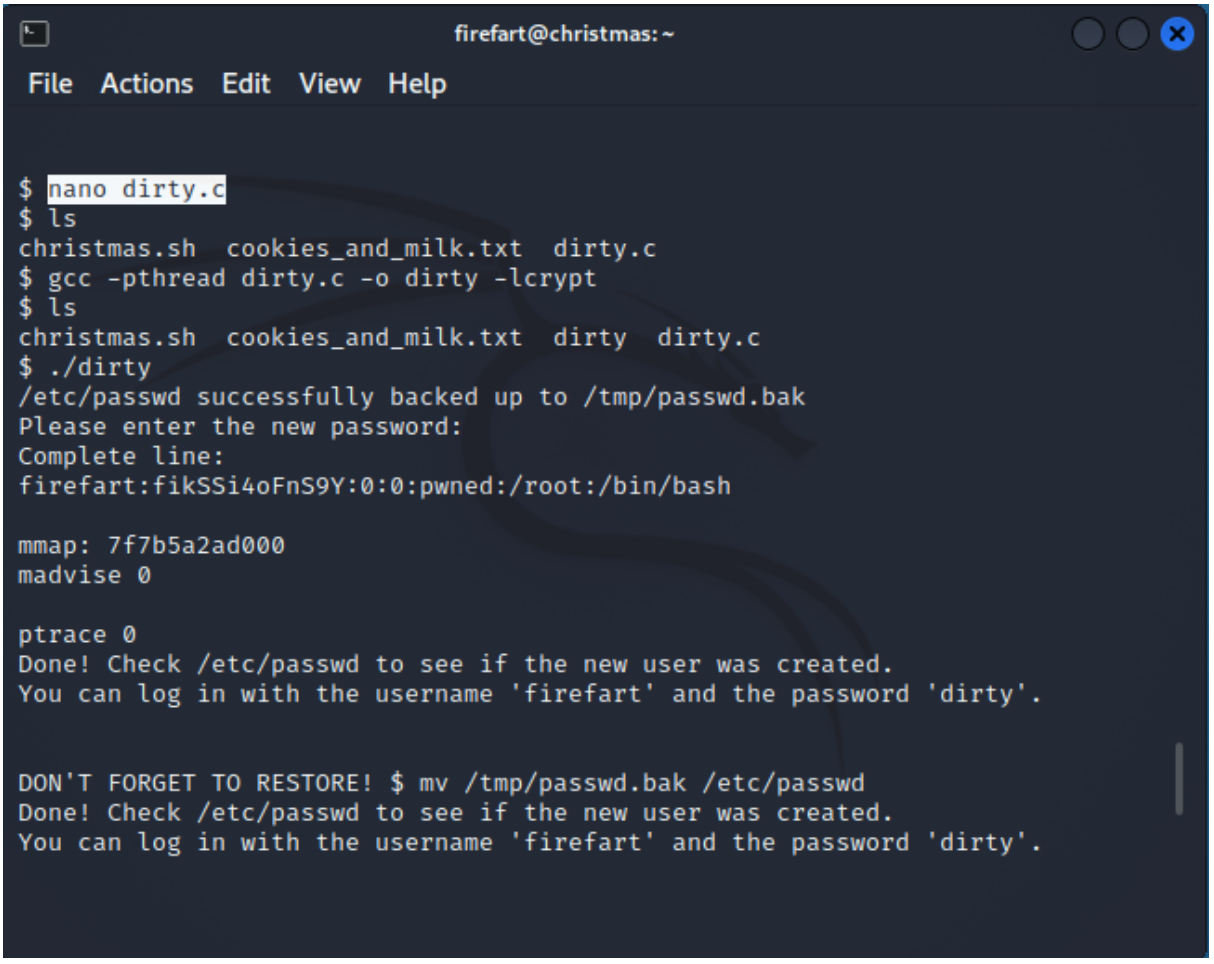
What "new" username was created, with the default operations of the real C source code?



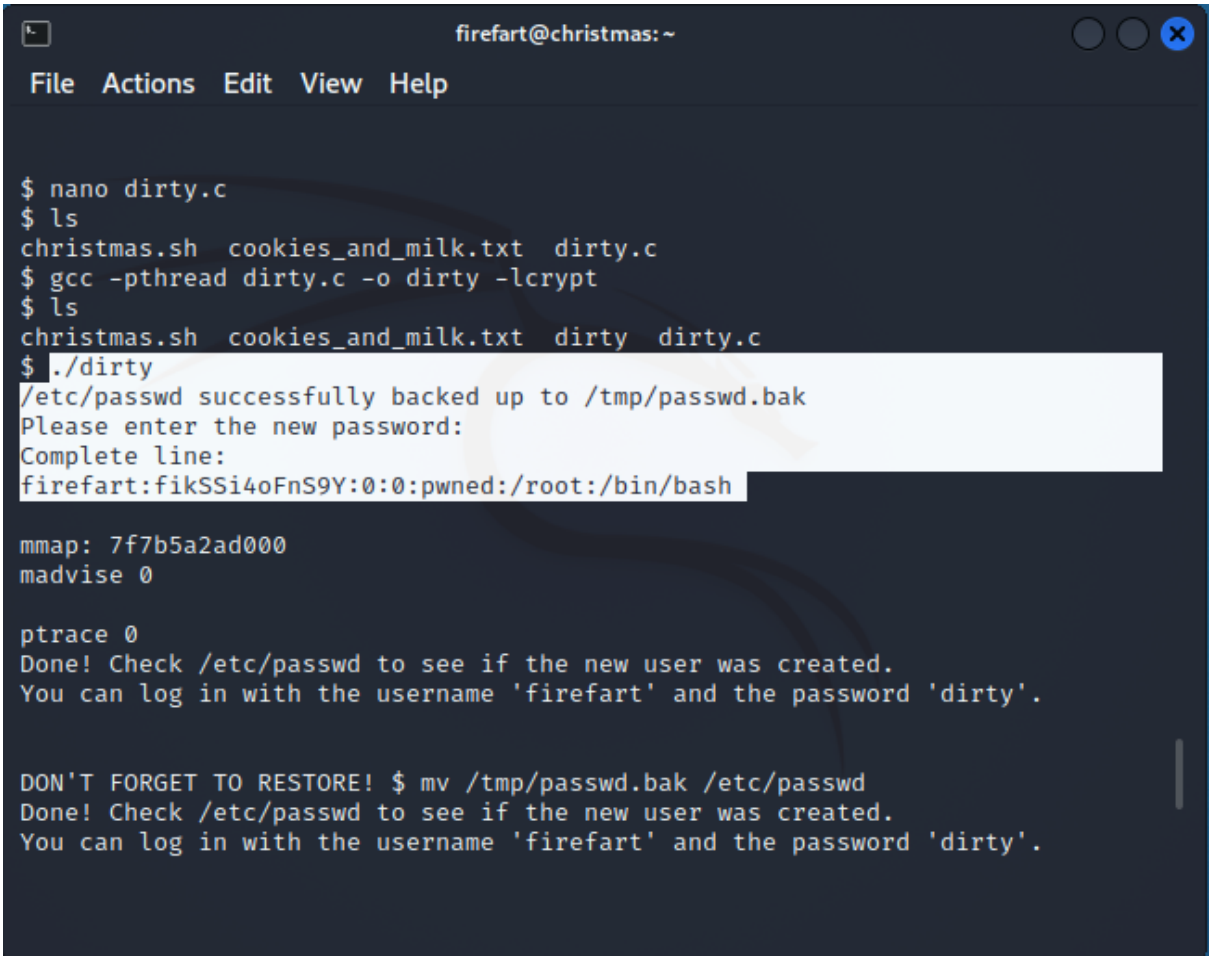
The default operations of the real source code could be seen in **line 11**

Question 7

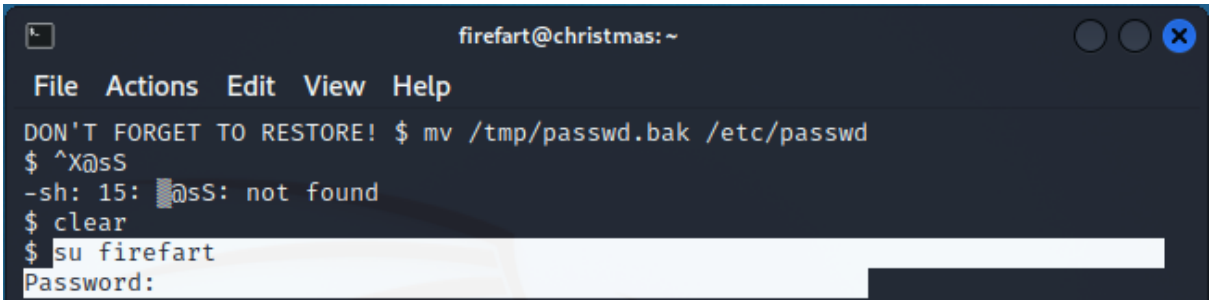
What is the MD5 hash output?



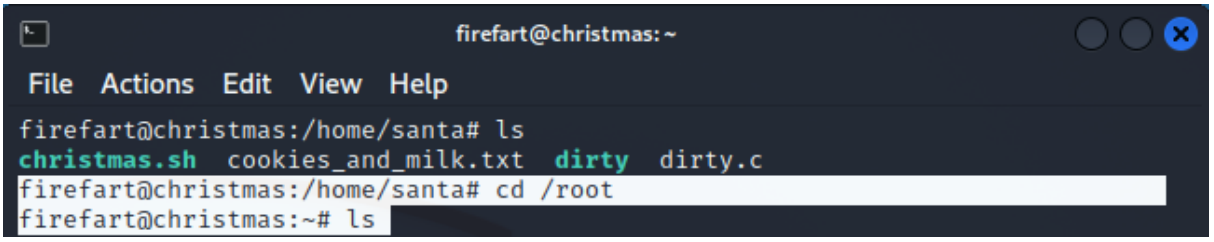
We need to use the Original Source Code so that we could track the Grinch file. Create a new text file (dirty.c) by using the command “nano”. Copy and paste the Source Code inside the file. To compile it, use the verbatim syntax **gcc -pthread dirty.c -o dirty -lcrypt**.



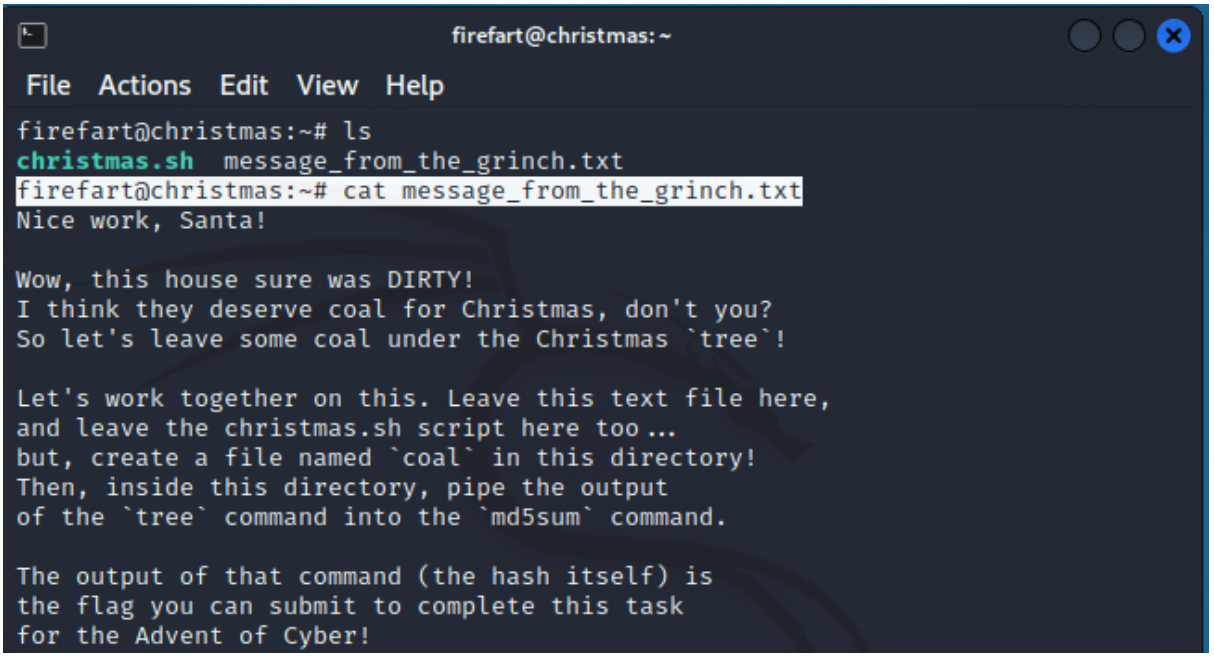
A “dirty” binary could be seen. After that, we should reset a new password for the new user we want to use afterwards.



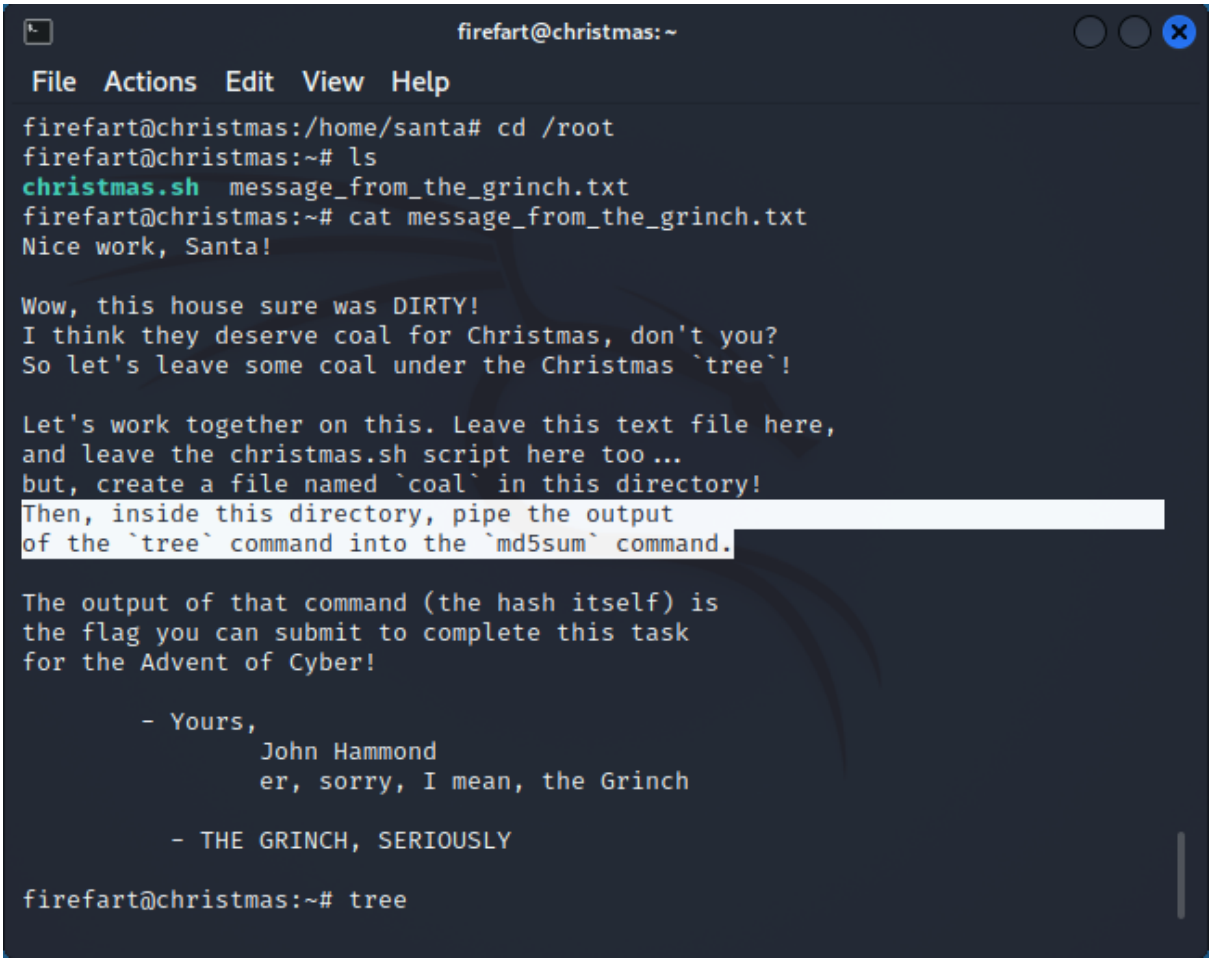
Enter the new password which has been set and change into our original user which is firefart. The command “su” is being used to switch users to another.

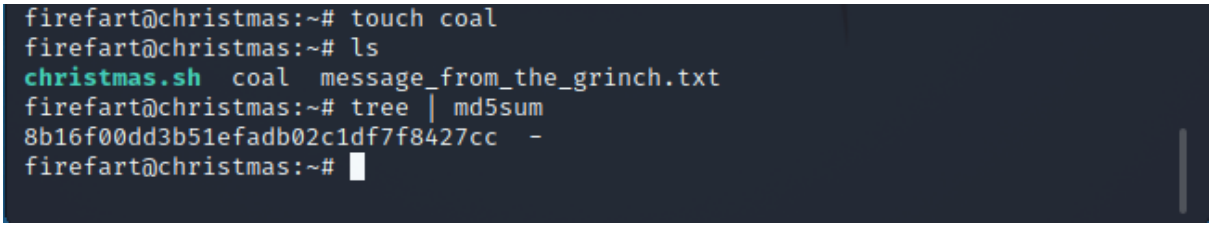


Use the /root directory so that we could own and run the server.



We could view the files and context in the directory in Grinch's server by using the "ls" command. In the folder we could see that there is a text file named **"message_from_the_grinch.txt".** Use the "cat" command to view the context inside text file.





Now, we should use “touch” coal to rewrite the coal in the directory. After that, run tree | md5sum to check the MD5 hash output in the directory.

Question 8

What is the CVE for DirtyCow?

By searching on the Web browser, the CVE for dirty cow could be seen as **CVE-2016-5195** which is highlighted in the picture.

Thought Process/Methodology:

Enter the command nmap IP address (10.10.154.98) on the terminal window. We could see deprecated protocol and service on the second line of the Service section. Following the hint, use the netcat with syntax with the command **telnet IP address following port number** to connect to the service. Scrolling down we can see the credential (password) being left in the terminal (highlighted for reference). We can log into the account with the credentials given there and look for the distribution of Linux and version number running in the server by typing the `cat /etc/*release` command. We can view files and folders in

the current directory with the command “ls”. Two files are stored inside. “cat” is being used in front of the file we want to access. We can see the name in the terminal. By Referring DirtyCow exploit online, we need to find the **Original** C source code in the certain folder. We can find one link which is **dirty.c** that saves the C source code. The verbatim syntax we can use to compile, taken from the real C source code comments, is written on the **17th line** in the folder while the default operations of the real source code could be seen in **line 11 in the dirty.C file.** We need to use the Original Source Code so that we could track the Grinch file. Creating a new text file (dirty.c) by using the command “nano”. Copy and paste all of the Source Code inside the file and compile it, using the verbatim syntax **gcc -pthread dirty.c -o dirty -lcrypt**. A “dirty” binary could be seen in the directory. After that, we should reset a new password for the new user we want to use afterwards. Enter the new password which has been set and change into our original user which is **firefart**. The command “su” is being used to switch users to another. After switching to Firefart, use the /root directory so that we could own and run the server. We could view the files and context in the directory in Grinch’s server by using the “ls” command. In the folder we could see that there is a text file named **“message_from_the_grinch.txt”.** Use the “cat” command to view the context inside the text file. Now, we should use “touch” coal to rewrite the coal in the directory. After that, run tree | md5sum to check the MD5 hash output in the directory. To find the CVE for dirty cow, use the web browser and search for it.

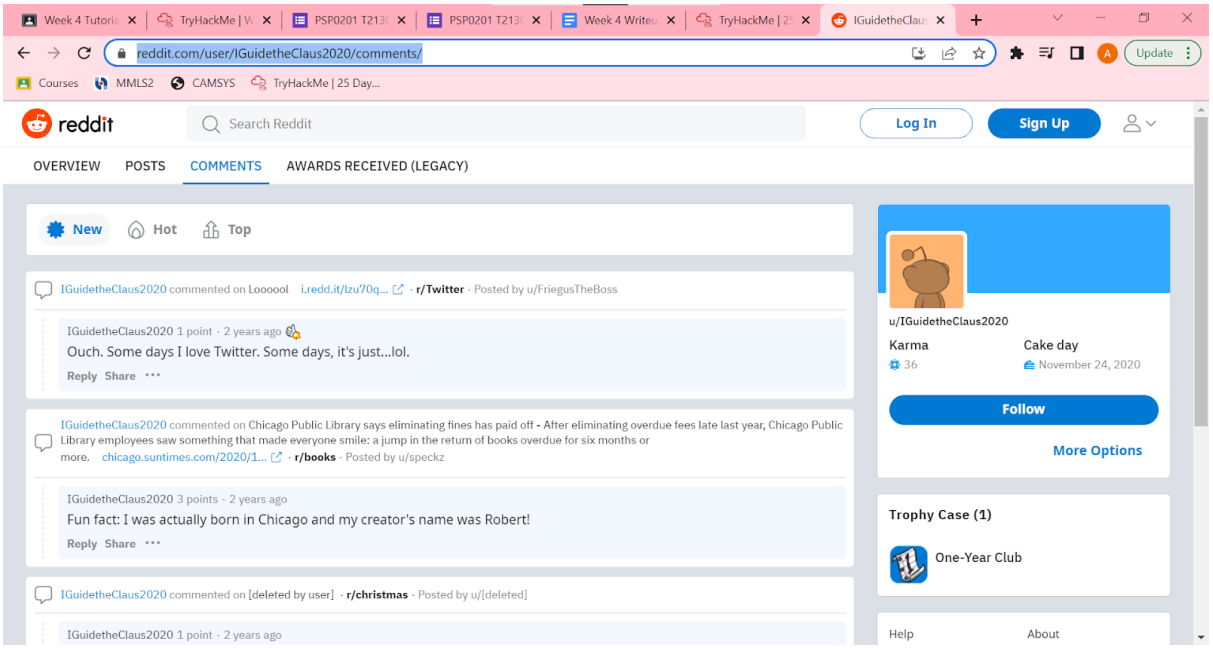
Day 14 : OSINT - Where's Rudolph ?

Tools : TryHackMe Attackbox, Chrome

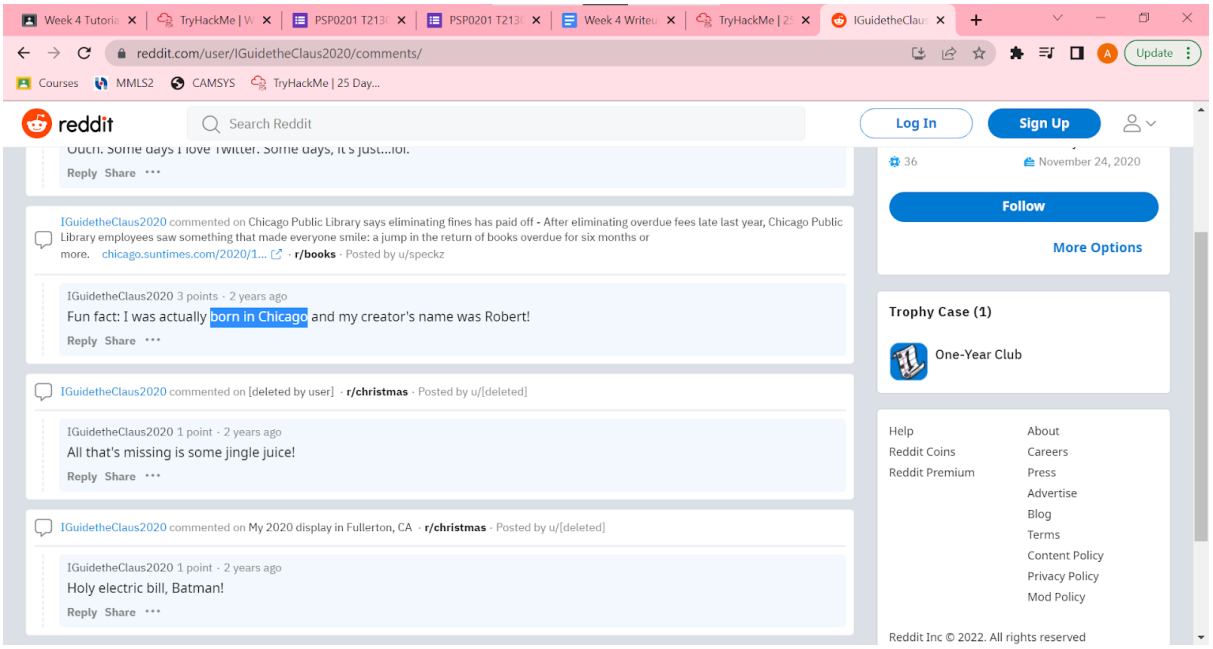
Solution / Walkthrough :

Q1: What URL will take me directly to Rudolph's Reddit comment history?

Open reddit and search for IGuidetheClaus 2020 and click on the comments section
The URL is https://www.reddit.com/user/IGuidetheClaus2020/comments/

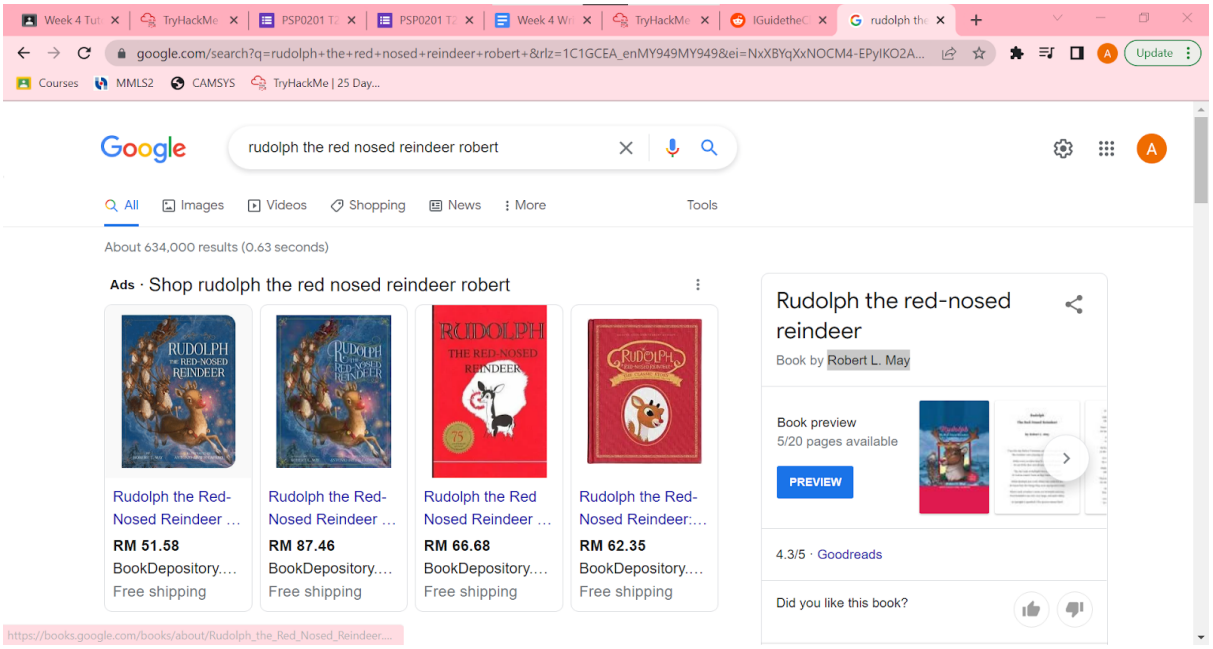


Q2: According to Rudolph, where was he born?



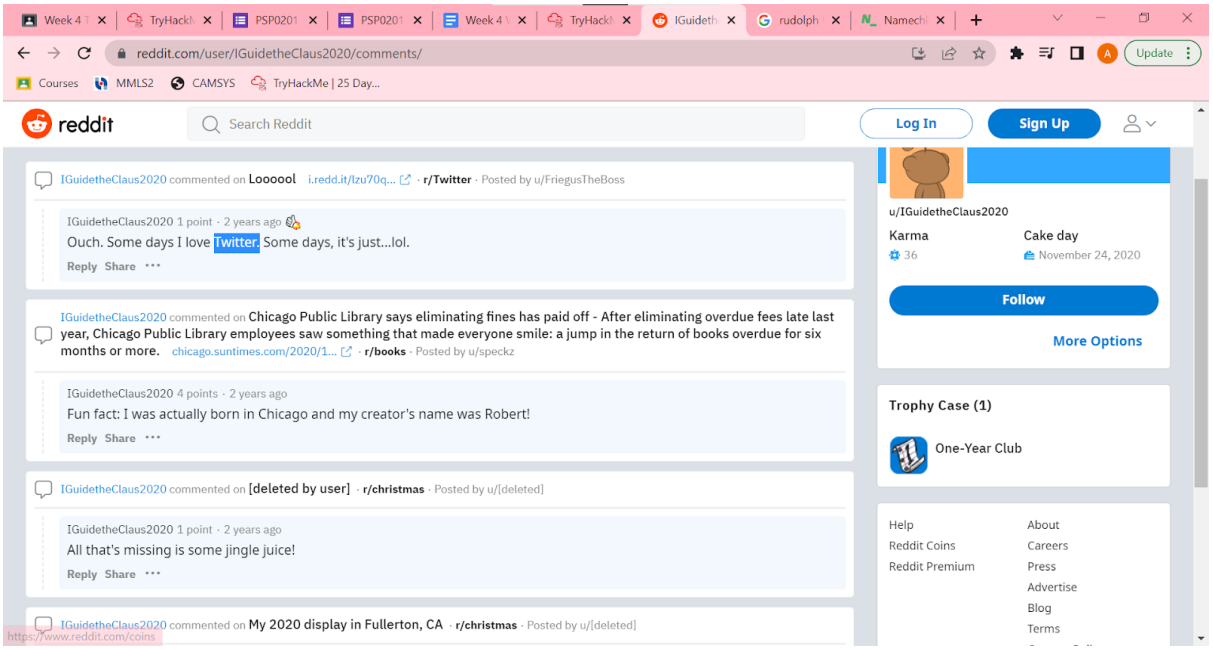
Q3: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?

Search for rudolph the red nosed reindeer robert in Google. Robert last name is May



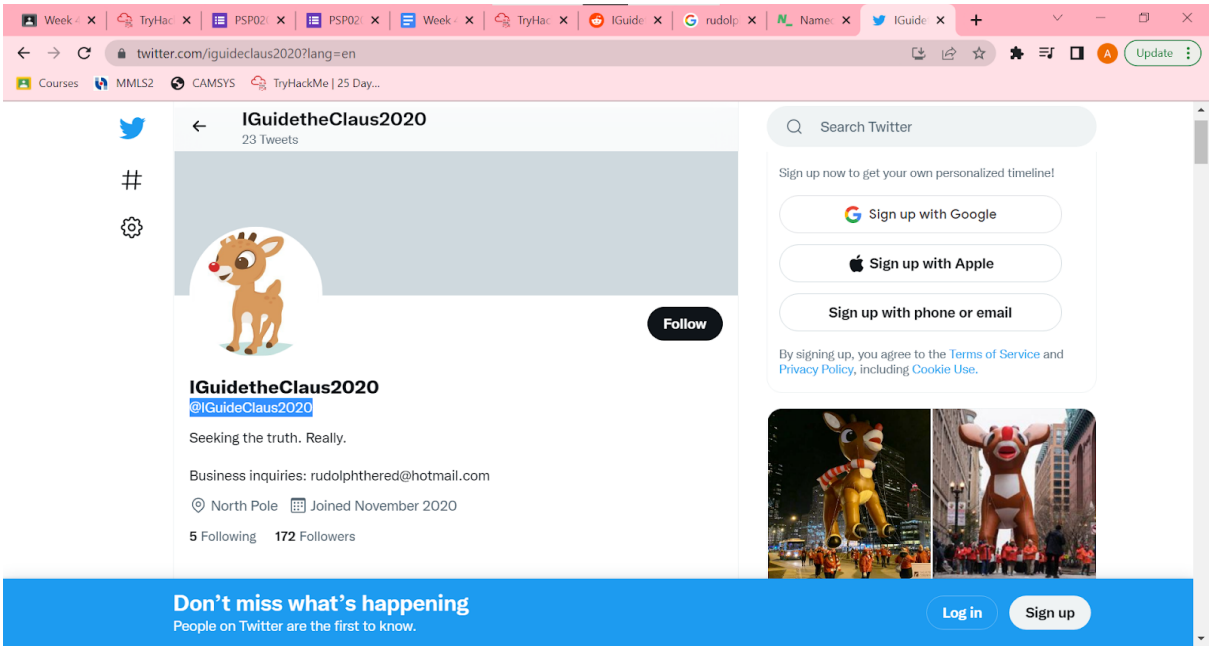
Q4: On what other social media platform might Rudolph have an account?

Based on his comments on reddit, Rudolph said he loves Twitter. So, Rudolph has a twitter account.



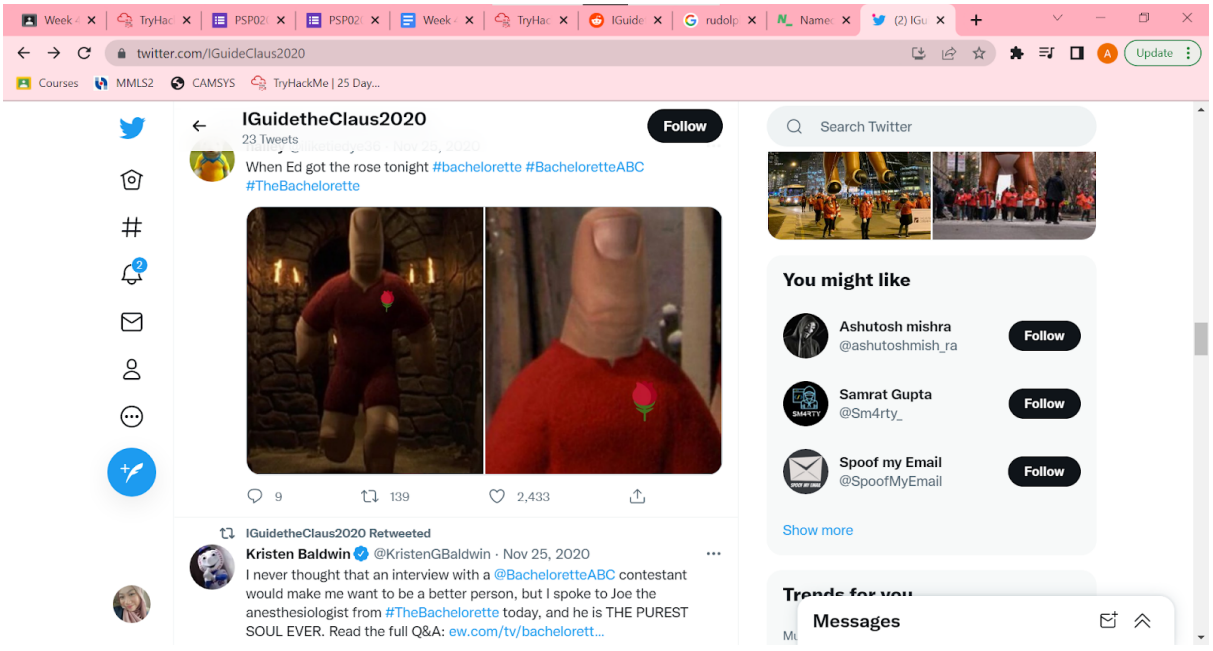
Q5: What is Rudolph's username on that platform?

Search for IGuidetheClaus2020 in Twitter. Click on the user found and the username is IGuideClaus2020



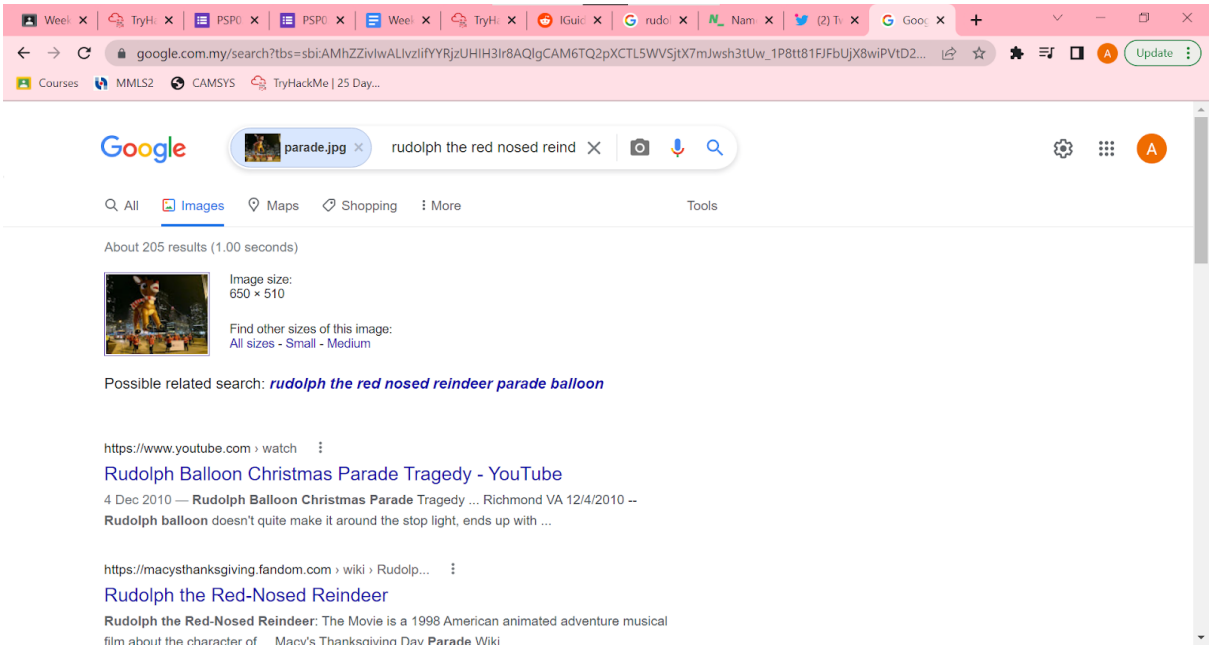
Q6: What appears to be Rudolph's favorite TV show right now?

Bachelorette

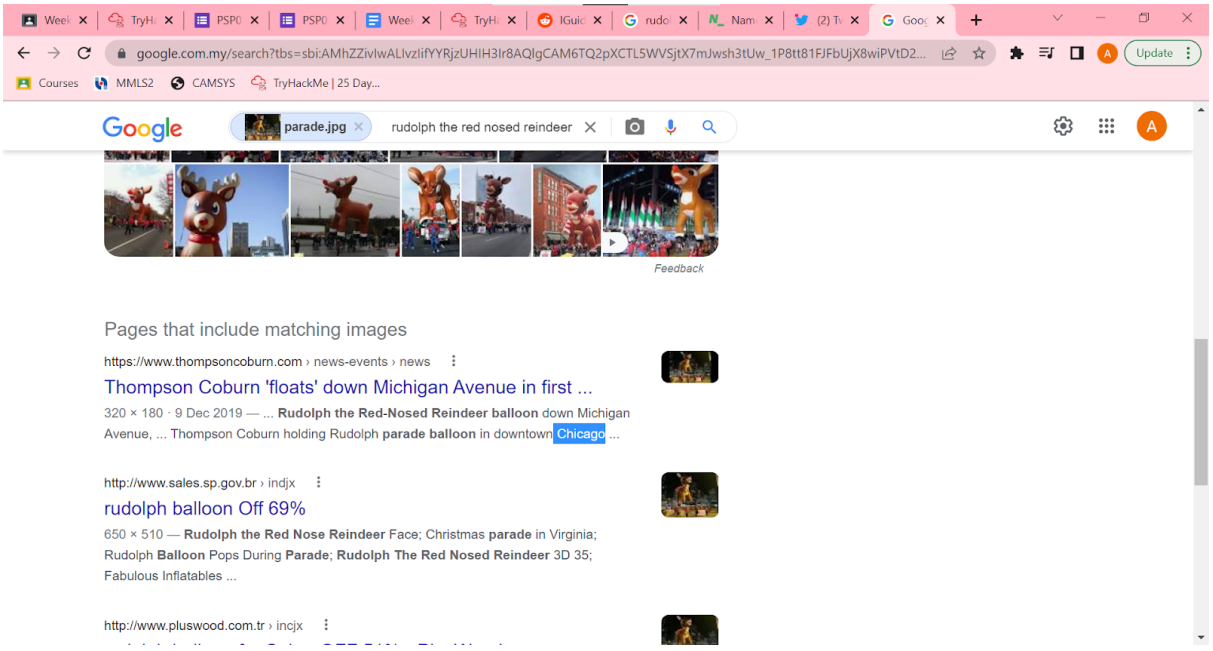


Q7: Based on Rudolph's post history, he took part in a parade. Where did the parade take place?

Google the image.

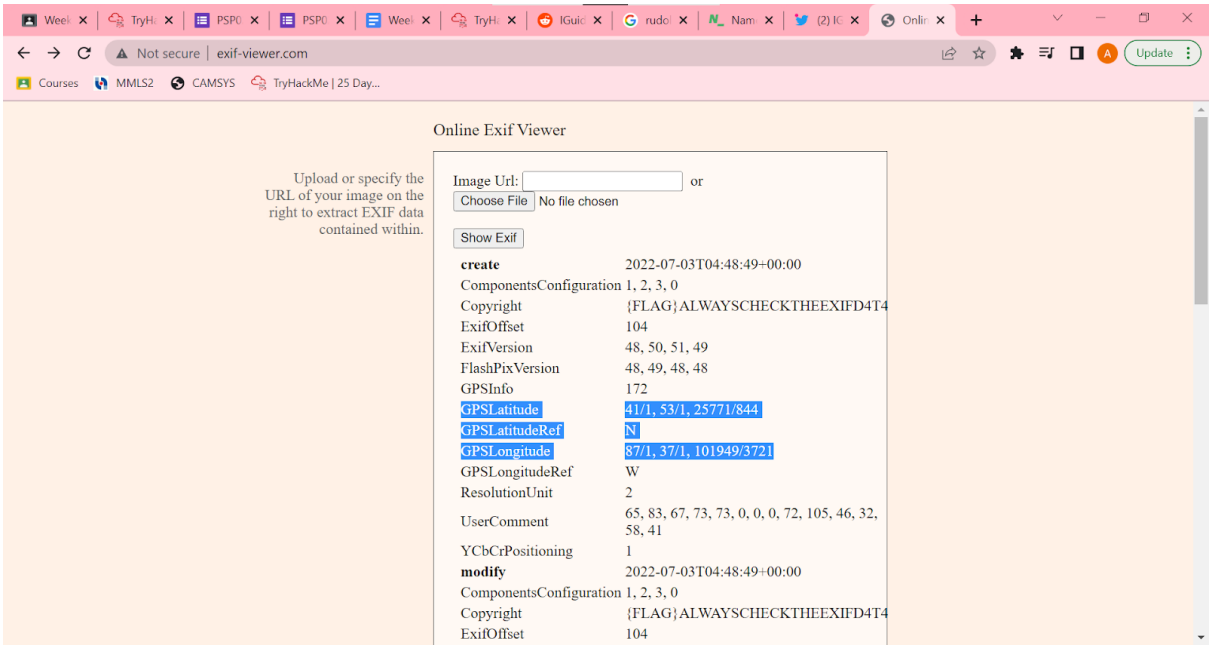


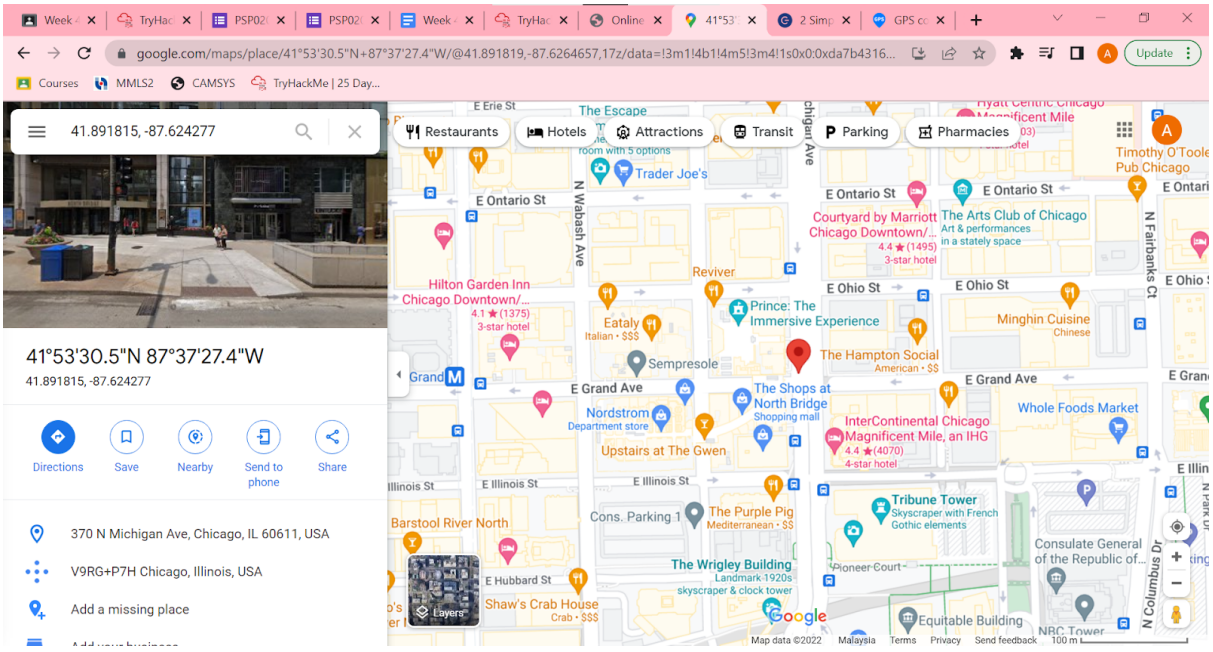
Scroll down until you can find where the parade takes place. Google said it was in Chicago.



Q8: Okay, you found the city, but where specifically was one of the photos taken?

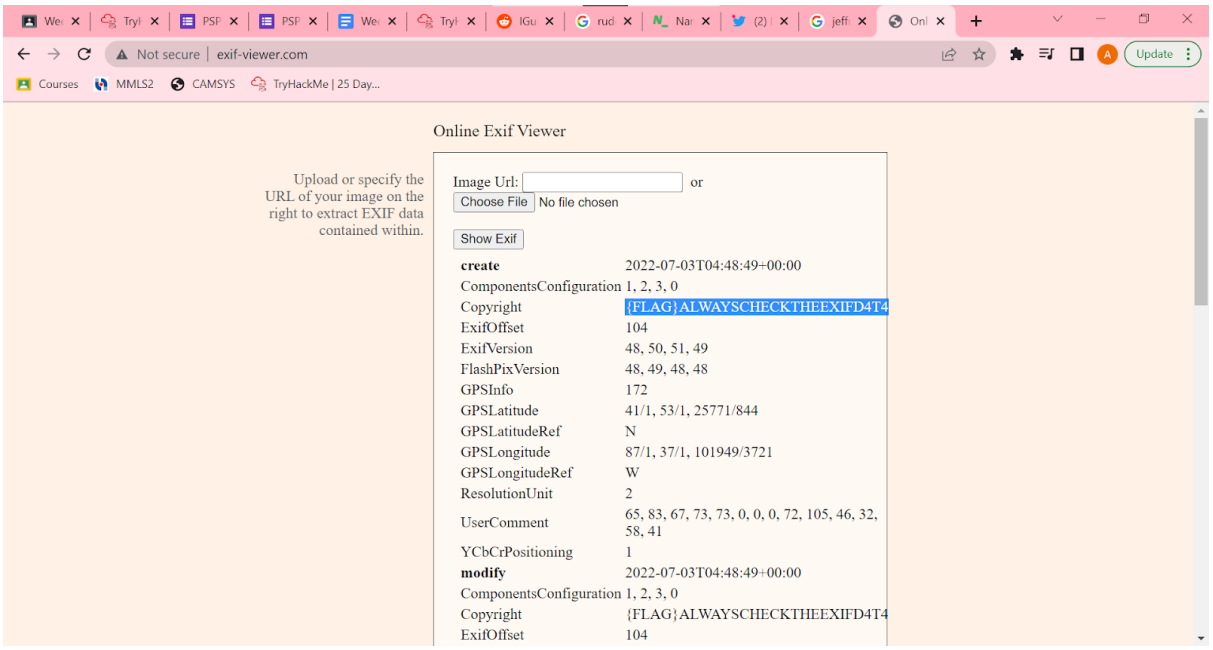
Upload the higher resolution image to http://exif-viewer.com/ and find the latitude longitude . The answer is 41.891815, -87.624277





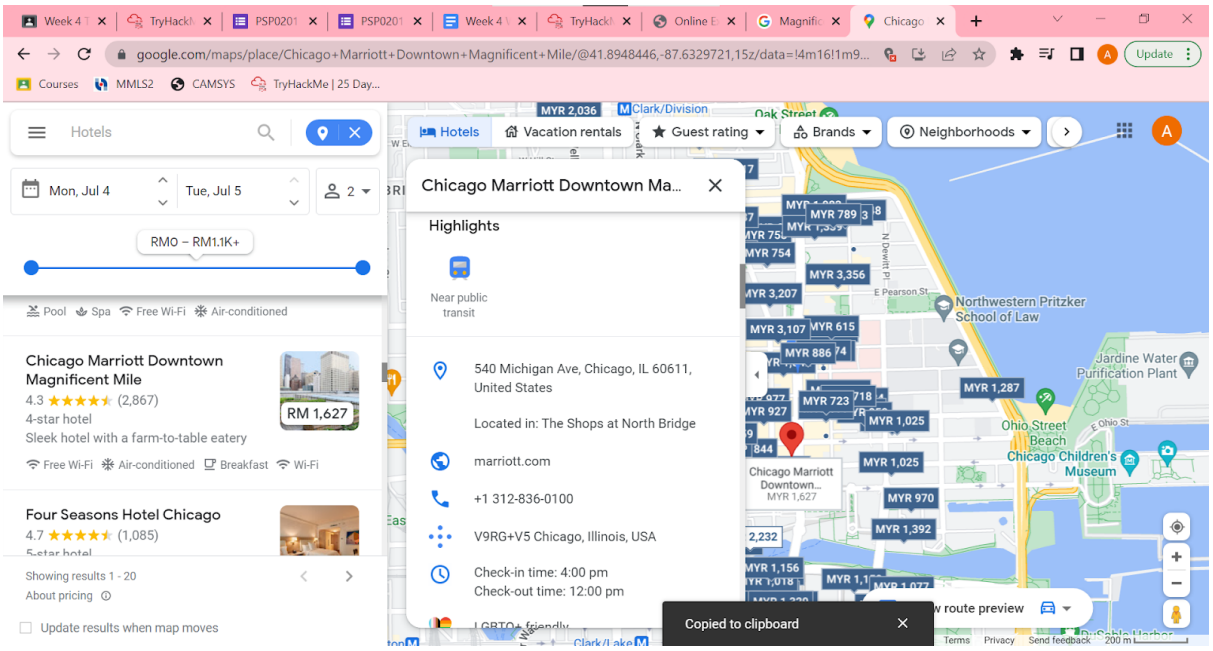
Q9: Did you find a flag too?

{FLAG}ALWAYSCHECKTHEEXIFD4T4



Q11: 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?

540



Thought Process/Methodology:
From someone's social media account, we can know a lot about them. When there's an image involved, we can see where that person took the picture by using exif-viewer.com. After the image was uploaded, we can know the latitude and

longitude of where the picture is taken. Just put the coordinates into google maps to find the exact location.

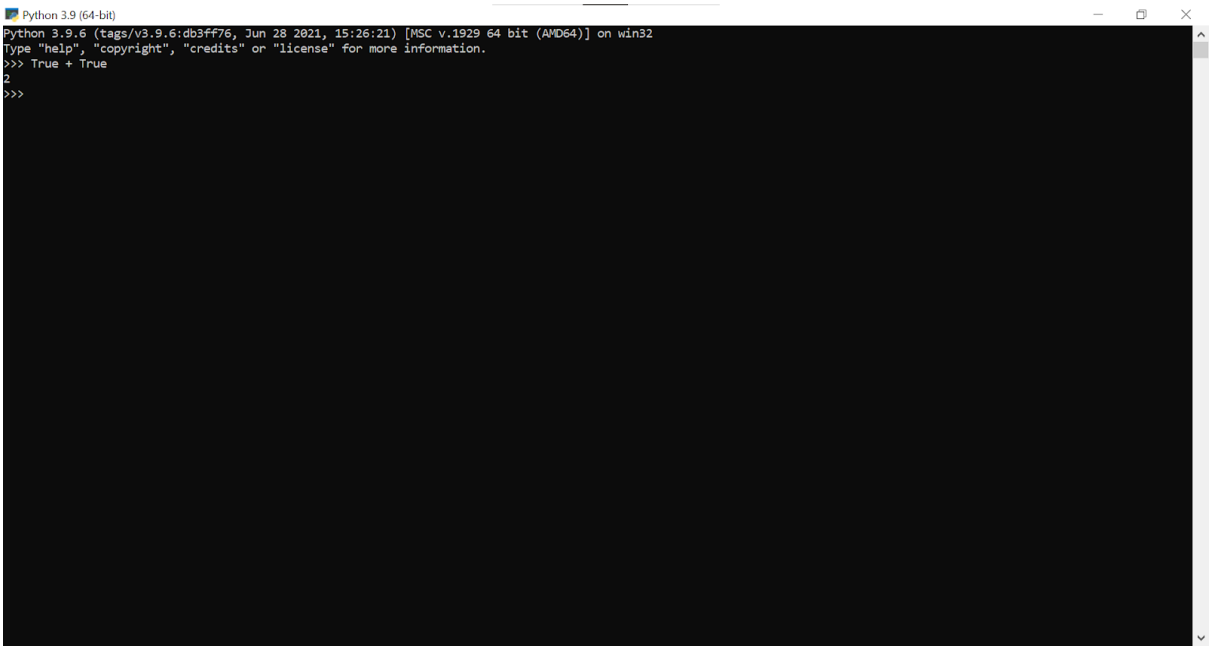
Day 15 : Scripting - There’s a Python in my stockings!

Tools : THM Attackbox, Chrome, VS Code, Python

Solutions / Walkthrough :

Q1: What's the output of True + True?

2



Q2: What's the database for installing other people's libraries called?

PyPi

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

```
pip3 install requests beautifulsoup4
```

Q3: What is the output of bool("False")?

True

```
oot@ip-10-10-251-89:~# python3
Python 3.6.9 (default, Jul 17 2020, 12:50:27)
[GCC 8.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information
.
>>> ("False")
'False'
>>> bool("False")
True
```

Q4: What library lets us download the HTML of a webpage?

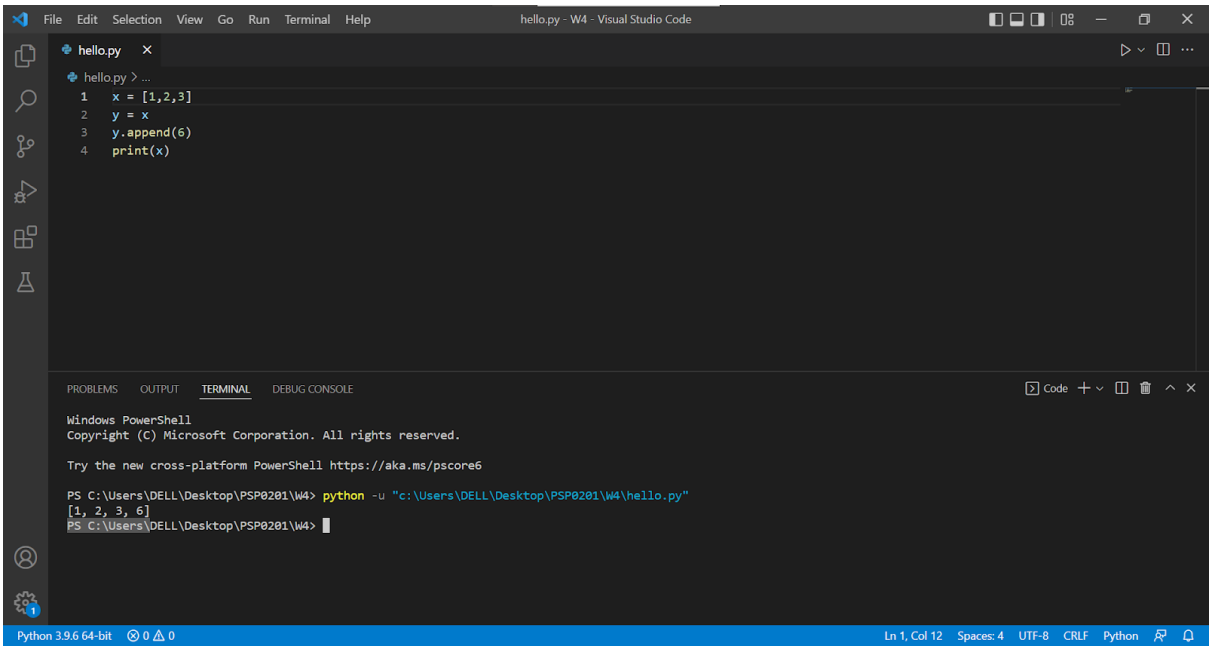
Requests

```
# 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')
```

Q5: What is the output of the program provided in "Code to analyse for Question 5" in today's material?

[1, 2, 3, 6]



Q6: What causes the previous task to output that?

Pass by reference

And more....

```
hello = "Hello, World!"
```

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

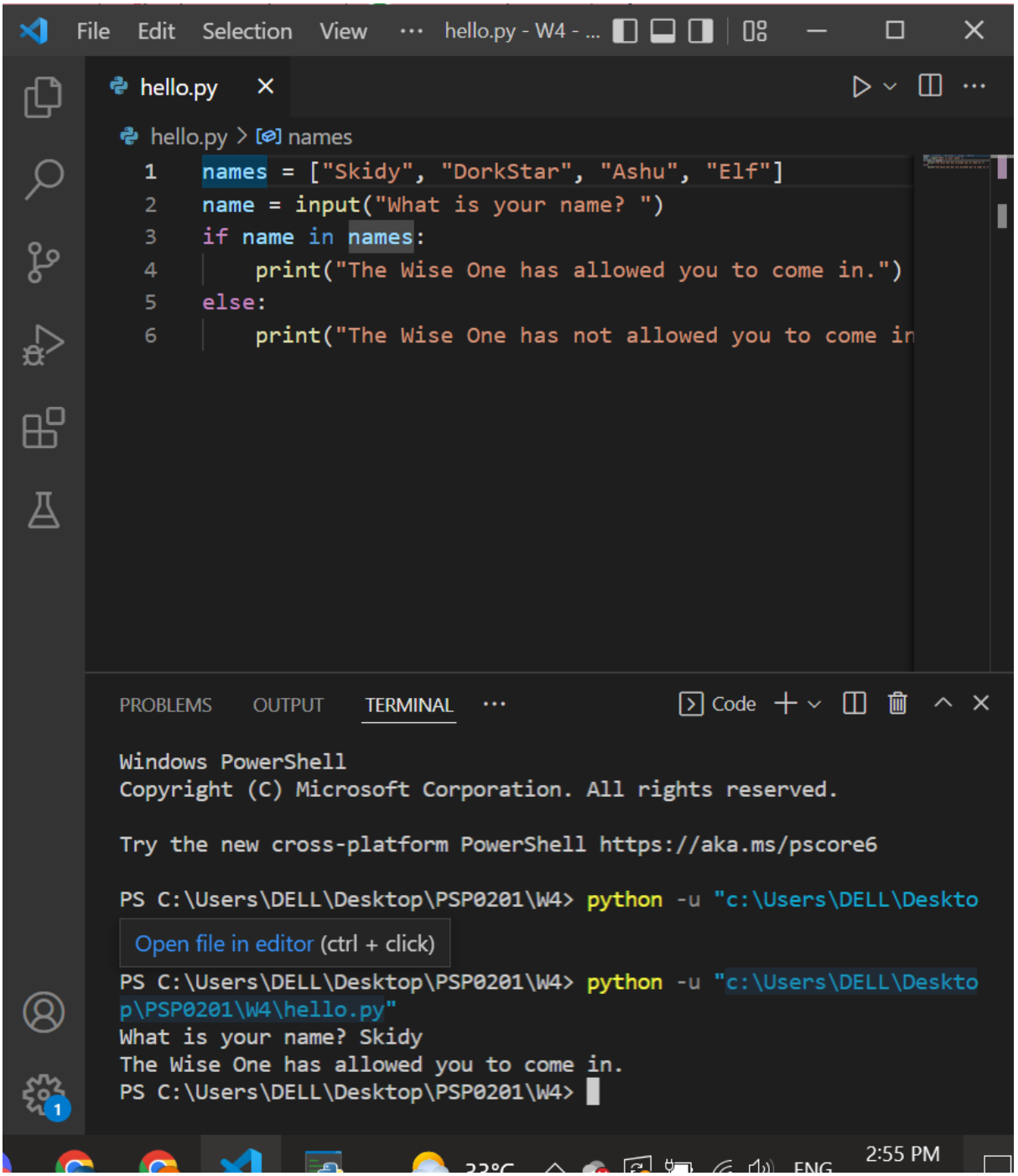
Now let's say we wanted to add this variable to another variable. A common misconception is that we take the bucket itself and use that. But in Python, we don't. We **pass by reference**. As in, we merely pass a location of the variable — we do not pass the variable itself. The alternative is to pass by value. This is very important to understand, as it can cause a significant amount of headaches later on.

Examine the following code:

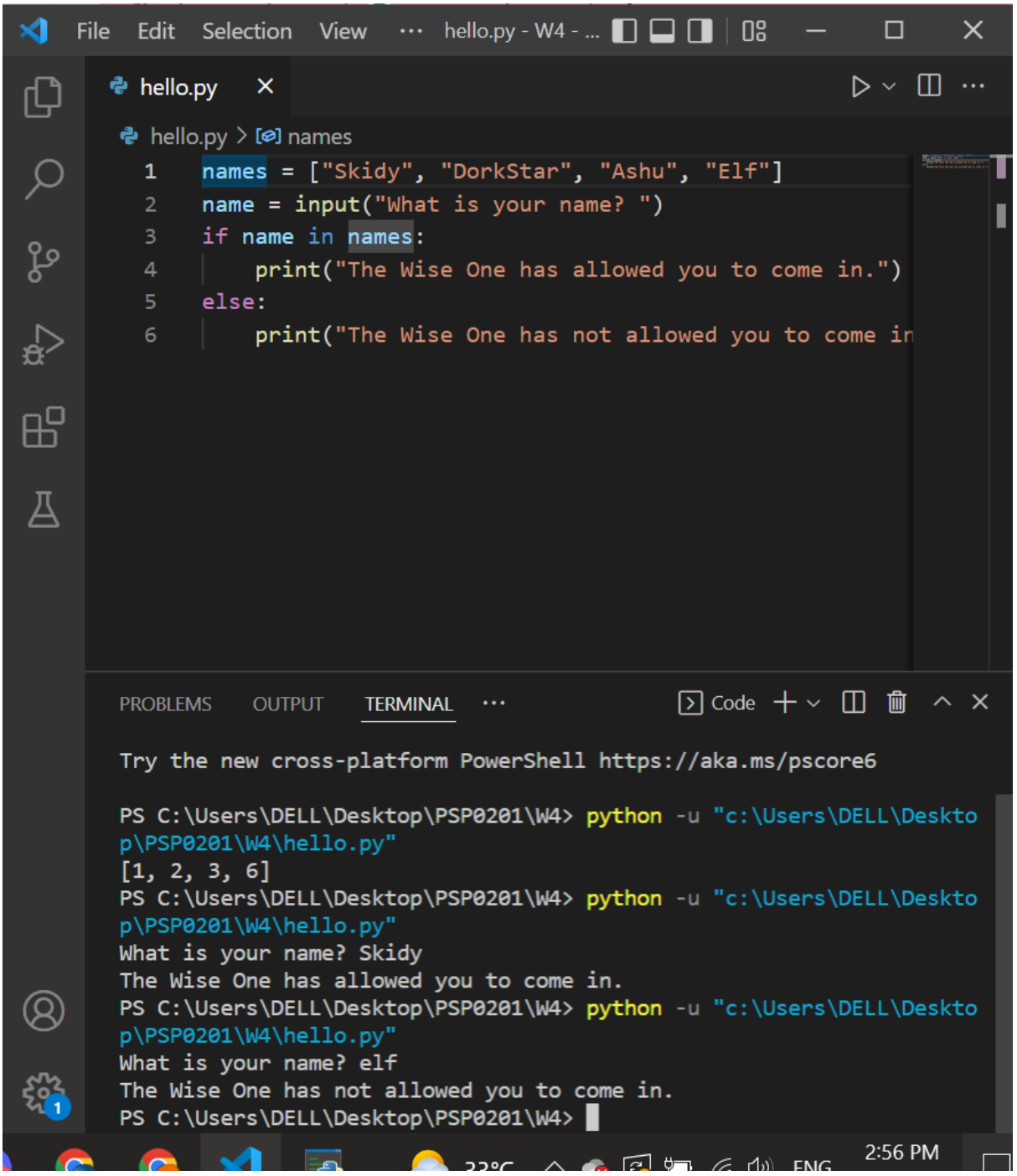
```
names = ["Skidy", "DorkStar", "Ashu", "Elf"]
name = input("What is your name? ")
```

```
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.")
```

Q7: if the input was "Skidy", what will be printed?



Q8: If the input was "elf", what will be printed?



Thought Process/Methodology:

For Day 15, we've been taught on how to use Python. There's a print command to print what we want and def command to define our functions. There are also 4 types of data which are string, integer, float and bool. There's also operators in python. There are also if statements and for loops in python. We can also install libraries in python by using the " pip install " command.