PSP0201

WEEK 4

WRITE UP

ID	*NAME*	*ROLE*
1211102582	AMEER IRFAN BIN NORAZIMAN	leader
1211101873	MUHAMMAD NABEEL SHAMIME BIN KHAEROZI	member
1211102269	MUHAMMAD ANIQ SYAHMI BIN SHAHARIL	member
1211101915	NURDINA AISHAH BINTI KASUMA SATRIA	member

Day 11 - Networking The Rogue Gnome

Tools Used: Kali Linux, Firefox

Solutions:

Question 1,2,3 : The directions of privilege escalation based on statements given

All answers were referred to in the notes in tryhackme.

> 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.

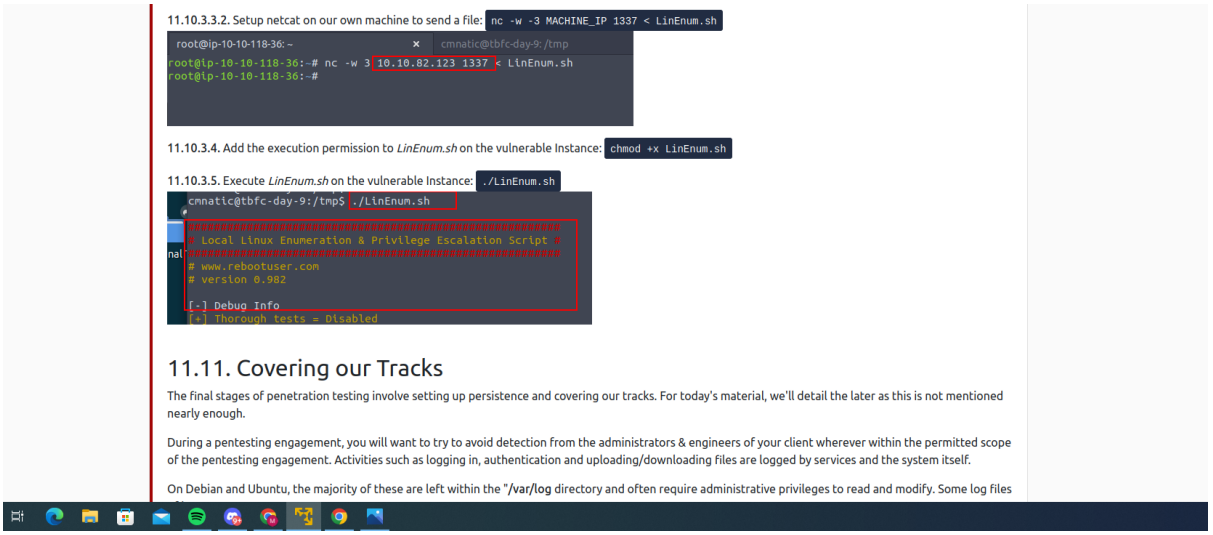
Question 4: What is the name of the file that contains a list of users who are a part of the sudo group?

Answer: Sudoers

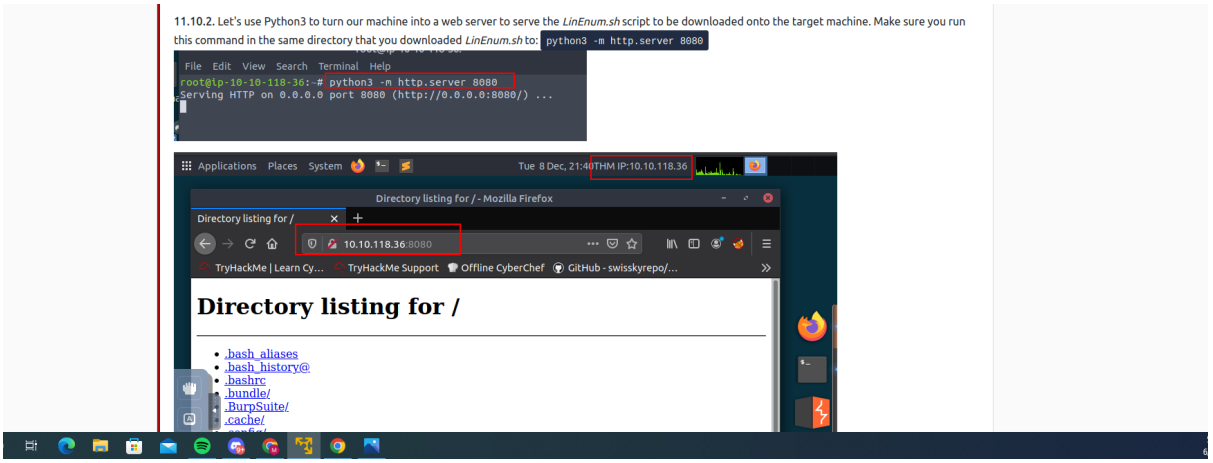
Question 5: What is the Linux Command to enumerate the key for SSH?

> 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*?

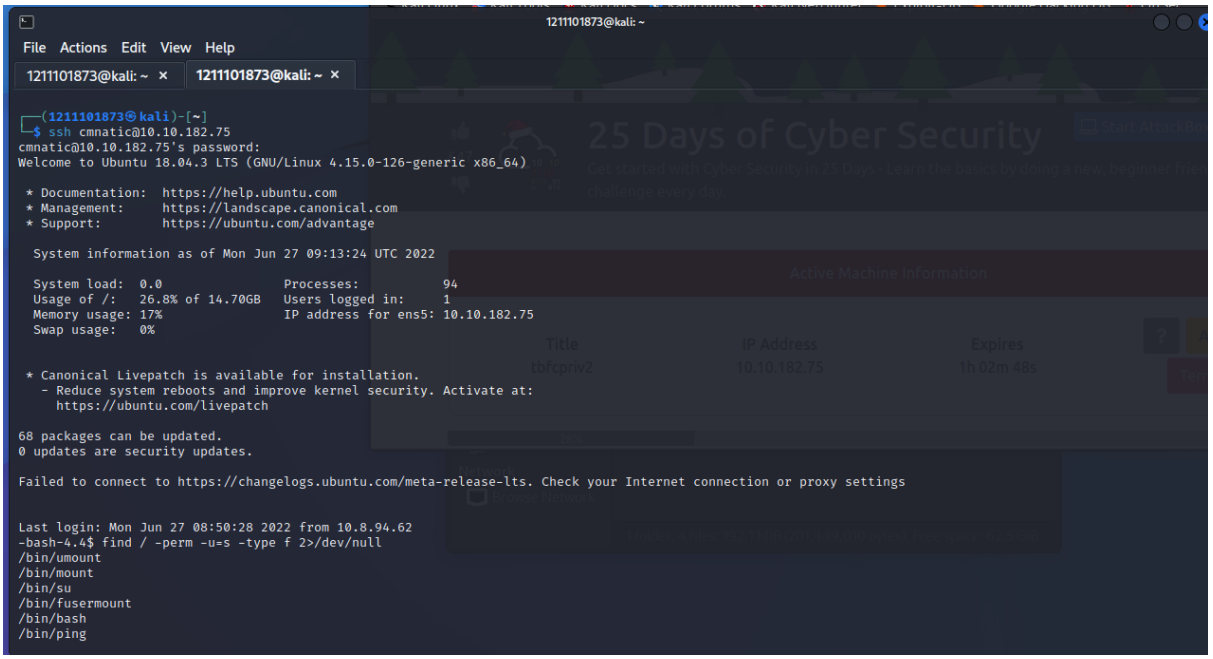
Question 6: If we have an executable file named find.sh that we just copied from another machine, what command do we need to use to make it be able to execute?

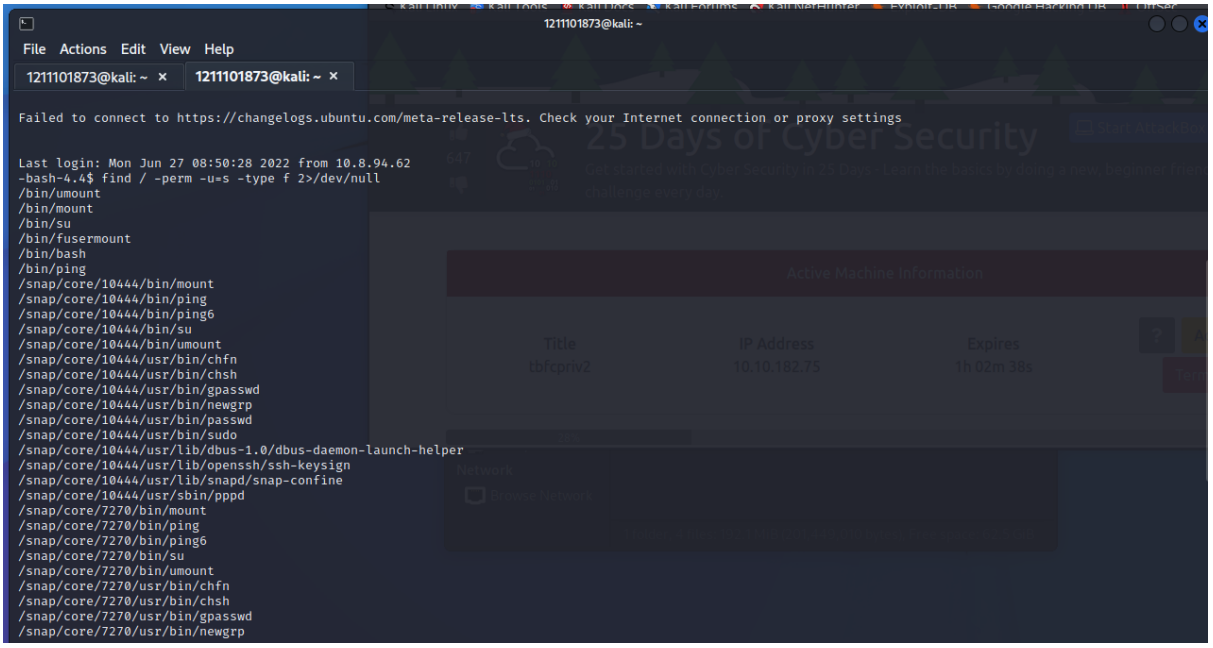


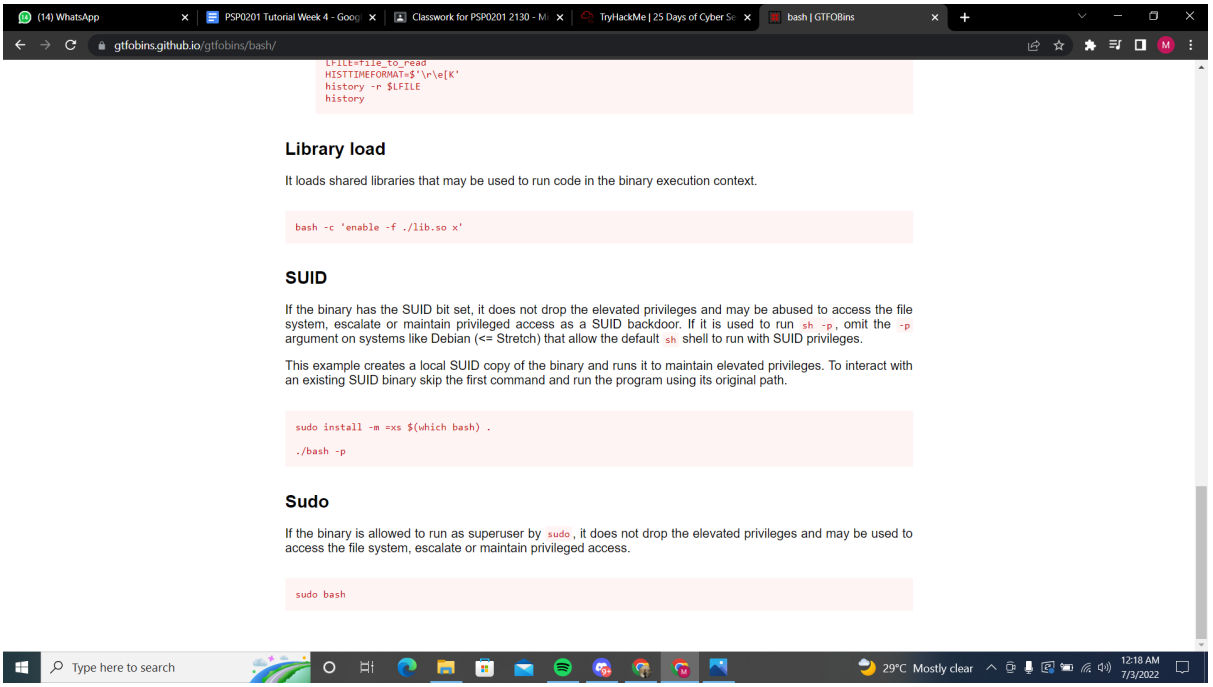
Question 7: The target machine you gained a foothold into is able to run wget. What command would you use to host a http server using python3 on port 9999?

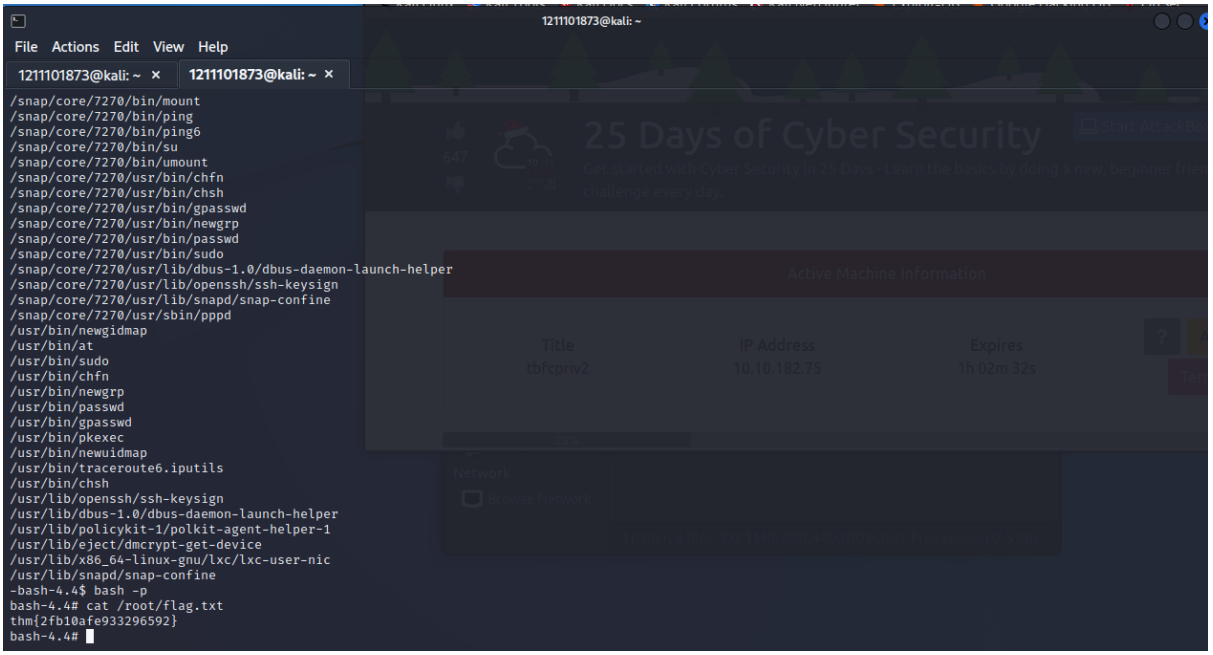


Question 8: What are the contents of the file located at /root/flag.txt?






(14) WhatsApp
PSP0201 Tutorial Week 4 - Goog
Classwork for PSP0201 2130 - M
TryHackMe | 25 Days of Cyber Se
bash | GTFOBins
gtfobins.github.io/gtfobins/bash/
LFILE=file_to_read
HISTTIMEFORMAT=$'\r\e[K'
history -r $LFILE
history
Library load
It loads shared libraries that may be used to run code in the binary execution context.
bash -c 'enable -f ./lib.so x'
SUID
If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run sh -p, omit the -p argument on systems like Debian (<= Stretch) that allow the default sh shell to run with SUID privileges.
This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.
sudo install -m =xs $(which bash) .
./bash -p
Sudo
If the binary is allowed to run as superuser by sudo, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.
sudo bash
Type here to search
29°C Mostly clear
12:18 AM
7/3/2022


1211101873@kali: ~
File Actions Edit View Help
1211101873@kali: ~ ×
1211101873@kali: ~ ×
/snap/core/7270/bin/mount
/snap/core/7270/bin/ping
/snap/core/7270/bin/ping6
/snap/core/7270/bin/su
/snap/core/7270/bin/umount
/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# cat /root/flag.txt
thm{2fb10afe933296592}
bash-4.4#
25 Days of Cyber Security
Active Machine Information
Title
IP Address
Expires
tbfcpriv2
10.10.182.75
1h 02m 32s
Network

The Throughout Process:

Most of the questions were answered by referring to the notes that tryhackme have provided except for question 8. For question 8, we were required to use SSH to log in to the vulnerable machine by running the command **"ssh cmnatic@MACHINE_IP"**. Once we had done that, the machine asked for the machine_ip's password. The password was provided in tryhackme and we inserted the password **"aoc2020"**. Once we've logged in, we run the command "`find / -perm -u=s -type f 2>/dev/null`" to search for the executables. We noticed that there was an executable named **"/bin/bash"**. Therefore, we used the bash method, by running the command "**bash -p**" which we got from the GTFObins link that was provided in tryhackme.This method is for us to get into the root account. Once we have done that, we run "**cat /root/flag.txt**" to see the contents of the file. And from there, we received the flag.

Day 12 Ready,set,elf

Tools used: Kali, Firefox, Terminal

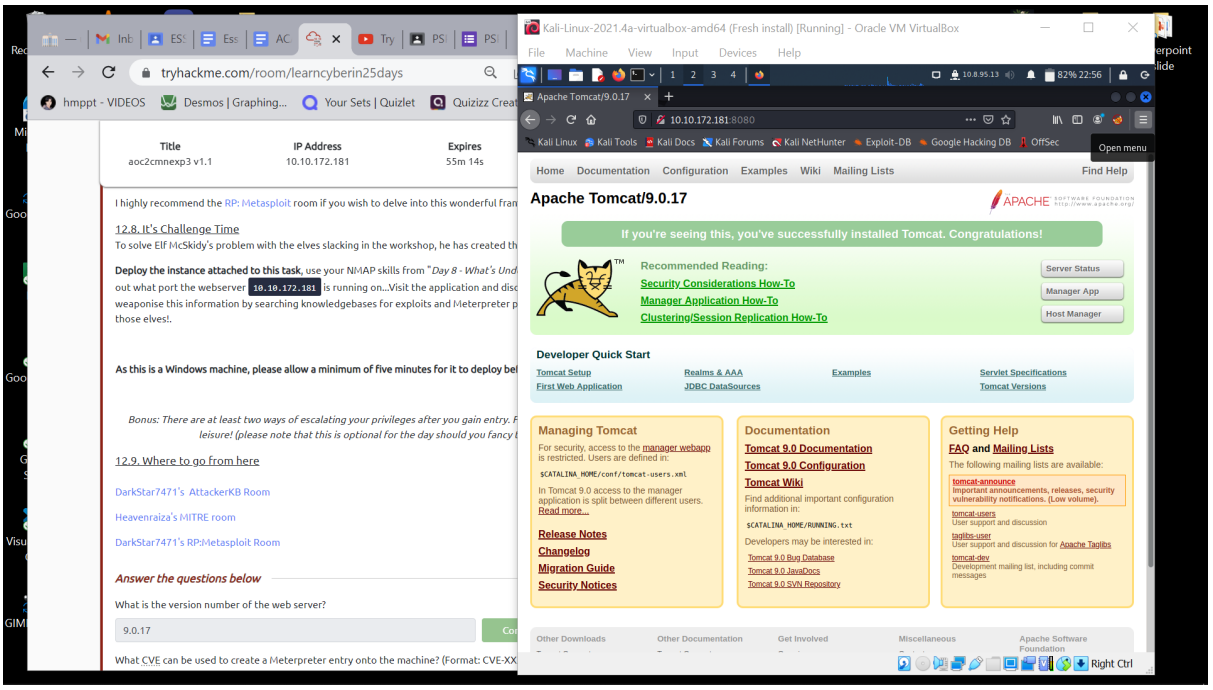
Solution:

Question 1

What is the version number of the web server?

ans : 9.0.17

To search up the version number typed in (ip address :8080) in Firefox, and you'll get a website title **Apache Tomcat/9.0.17**

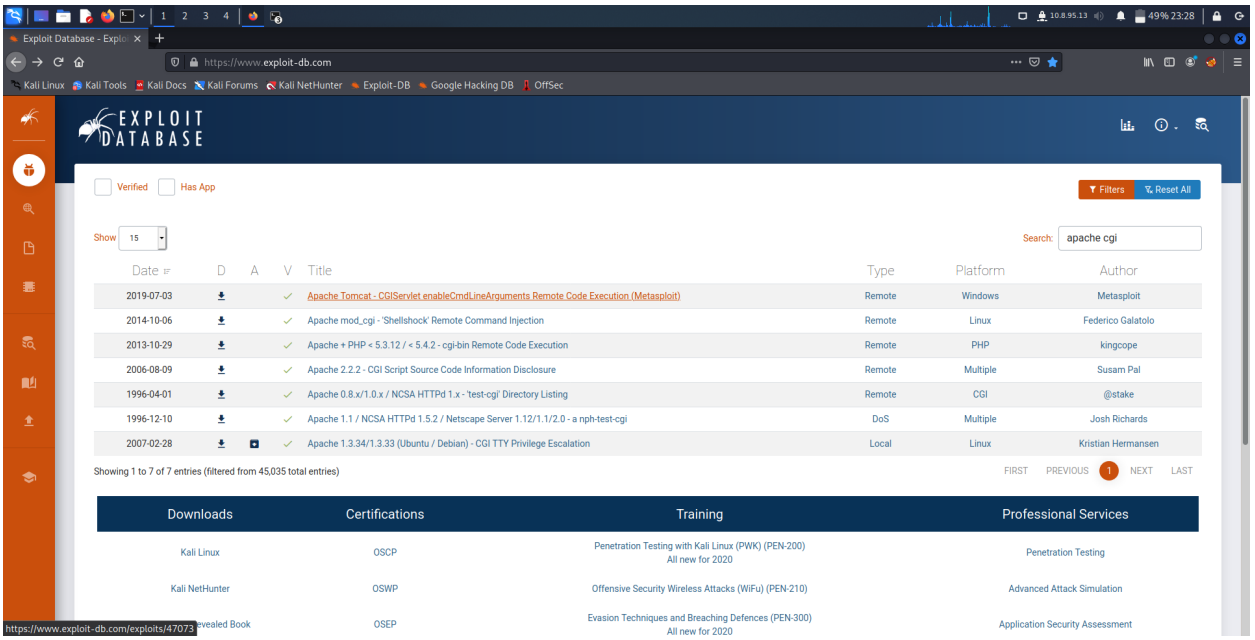


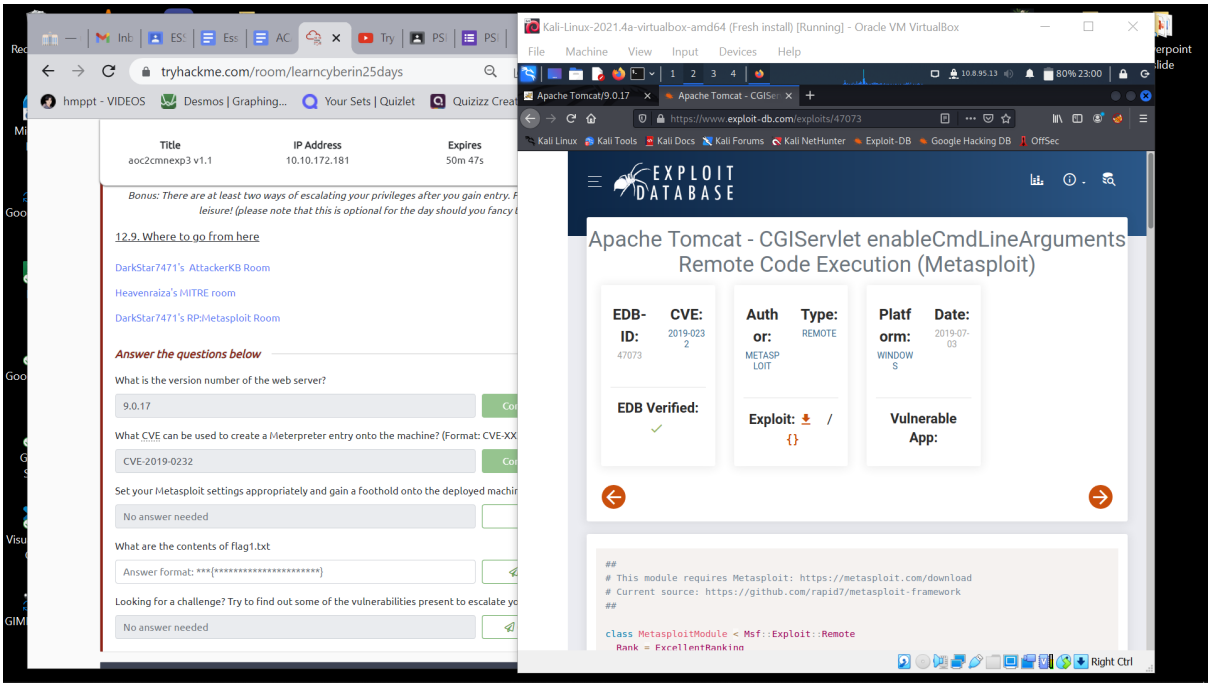
Question 2

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

ans : CVE-2019-0232

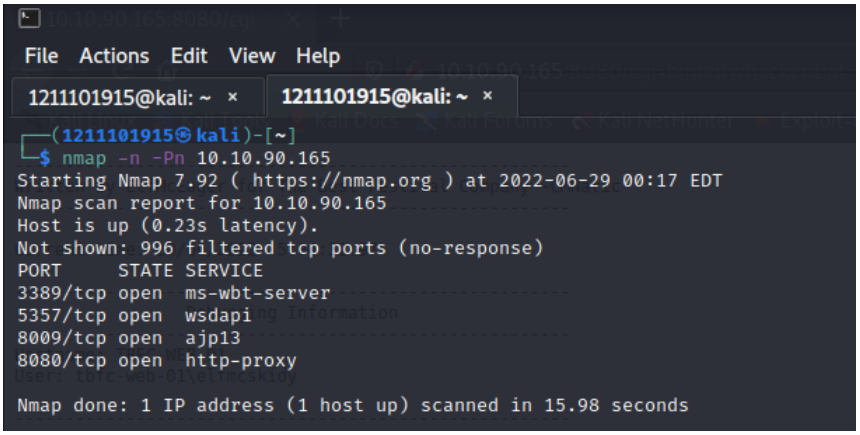
To get the CVI we open exploit database and search **apache cgi, and clicked on the first row**

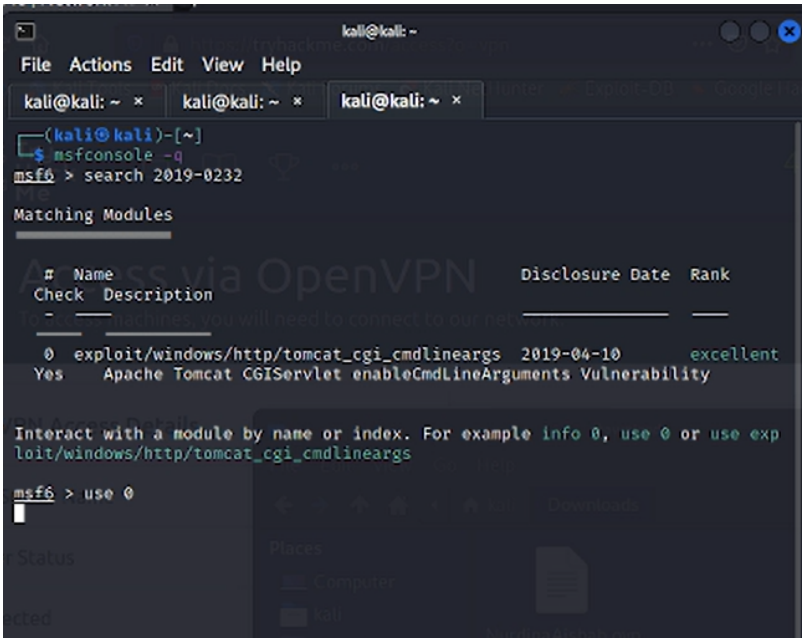


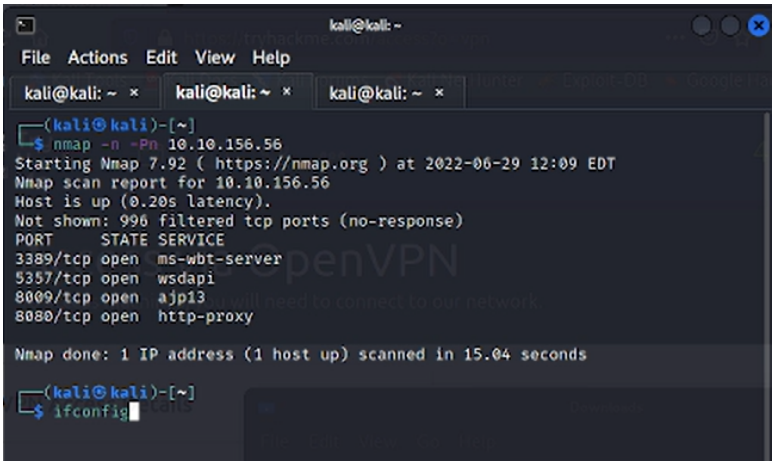


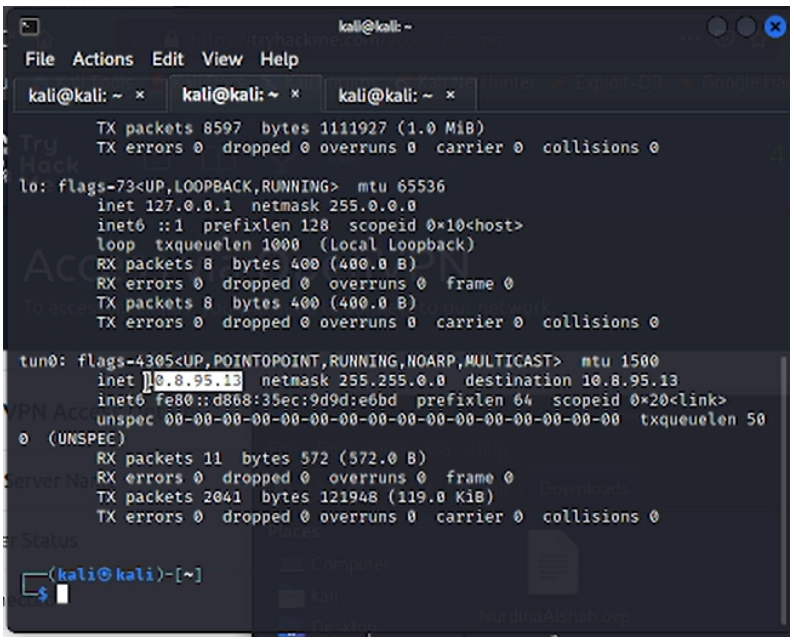
Question 3

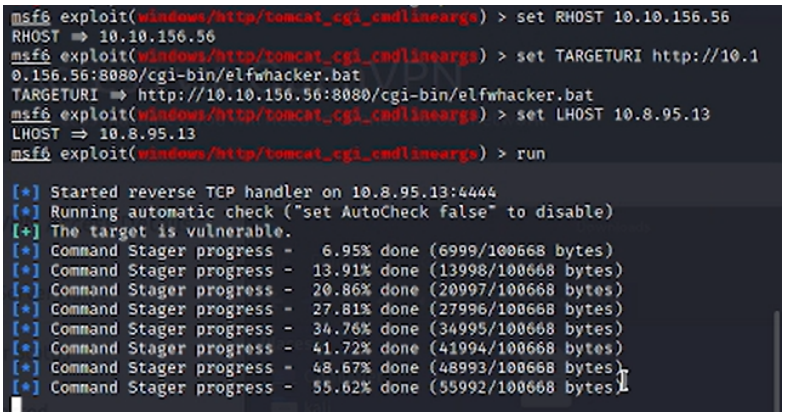
Set your Metasploit settings appropriately and gain a foothold onto the deployed machine.





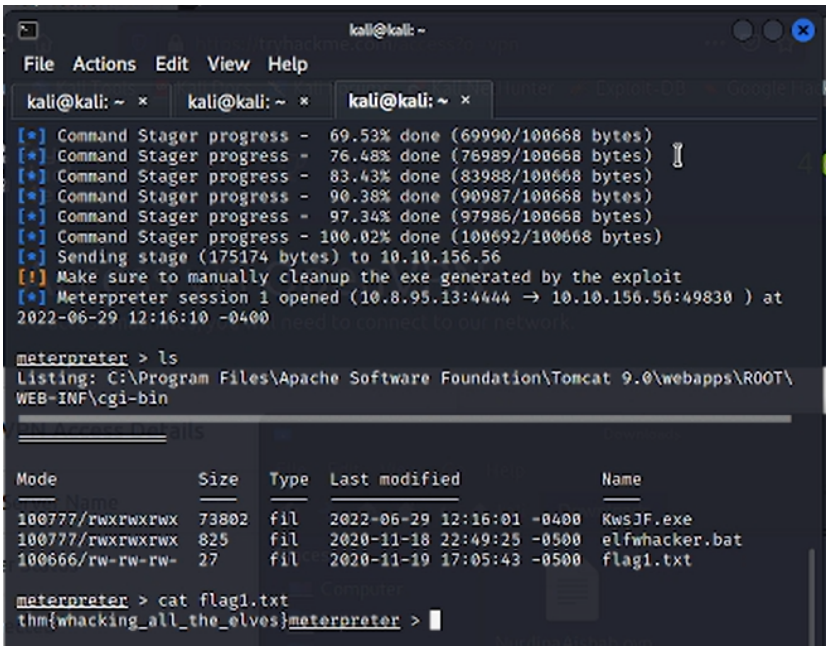






Question 4 : What are the contents of flag1.txt?

ans : thm{whacking_all_the_elves}



The Thought Process

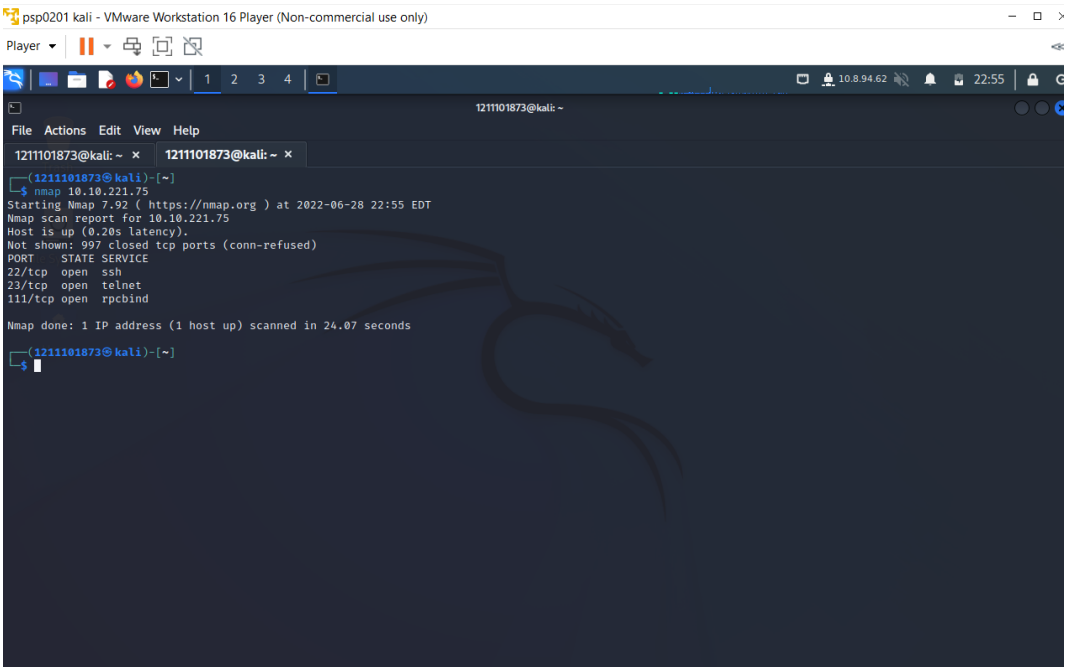
Once we opened kali, we opened the terminal and used nmap to find out what port the webserver **10.10.156.56** was running on. Then we visited the application and found the installation version. Then we search up its CVE to create a Meterpreter entry onto the machine, the CVE can be found by searching “apache cgi” in the exploit database on FireFox. After that, to gain a foothold onto the deployed machine,we opened a new tab and we typed in msfconsole -q to work with the Metasploit Framework and search up the CVE. Then we set RHOST and TARGETURI http://10.10.156/56:8080/cgi-ben/elfwhacker.bat. At this point we typed in ifconfig on the previous tab and there it listed tun0 with an ip address **10.8.95.13.** With this ip address we set LHOST and use command ‘ls’ to list files. Type “run” and we get a list of command stager progress with one line that stated **“The Target is Vulnerable”** to get inside we type ‘ls’ and 1 file with the name **“flag1.txt”** appeared. To print the context we typed in “cat flag1.txt” and a flag **thm{whacking_all_the_elves}** appeared.

Day 13 : Networking Coal for Christmas

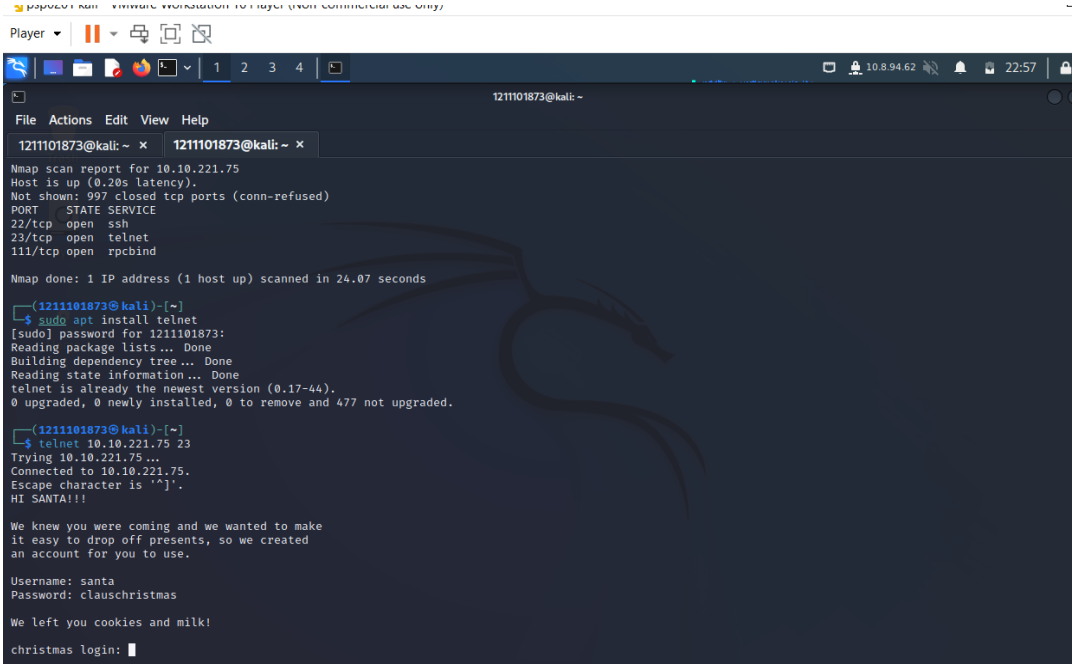
Tools used: Kali Linux, Firefox

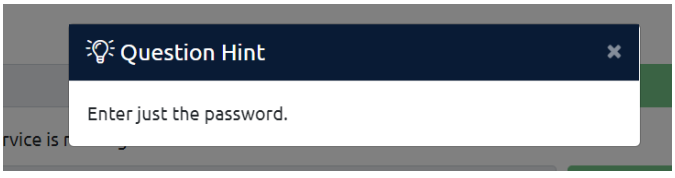
Solution:

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

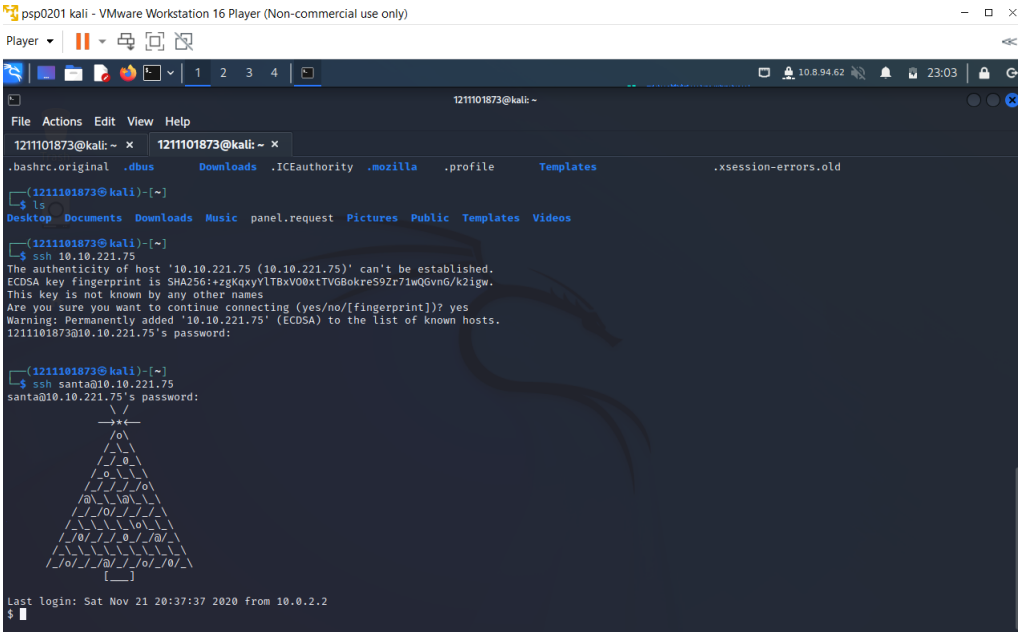


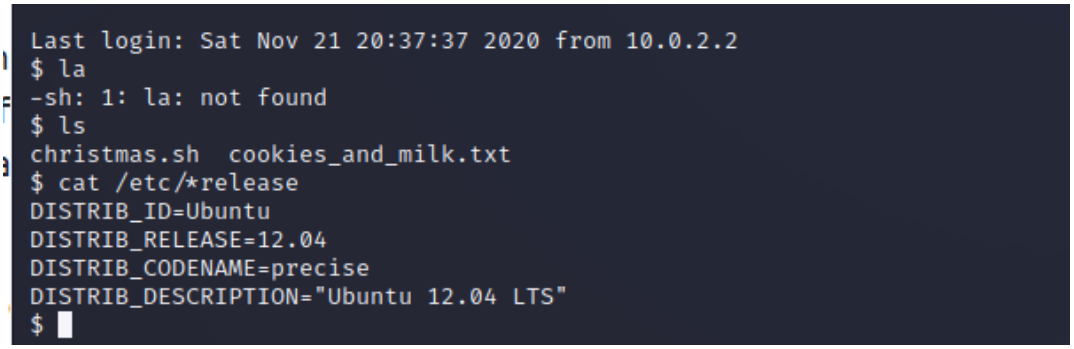
Question 2: What credential was left for you?



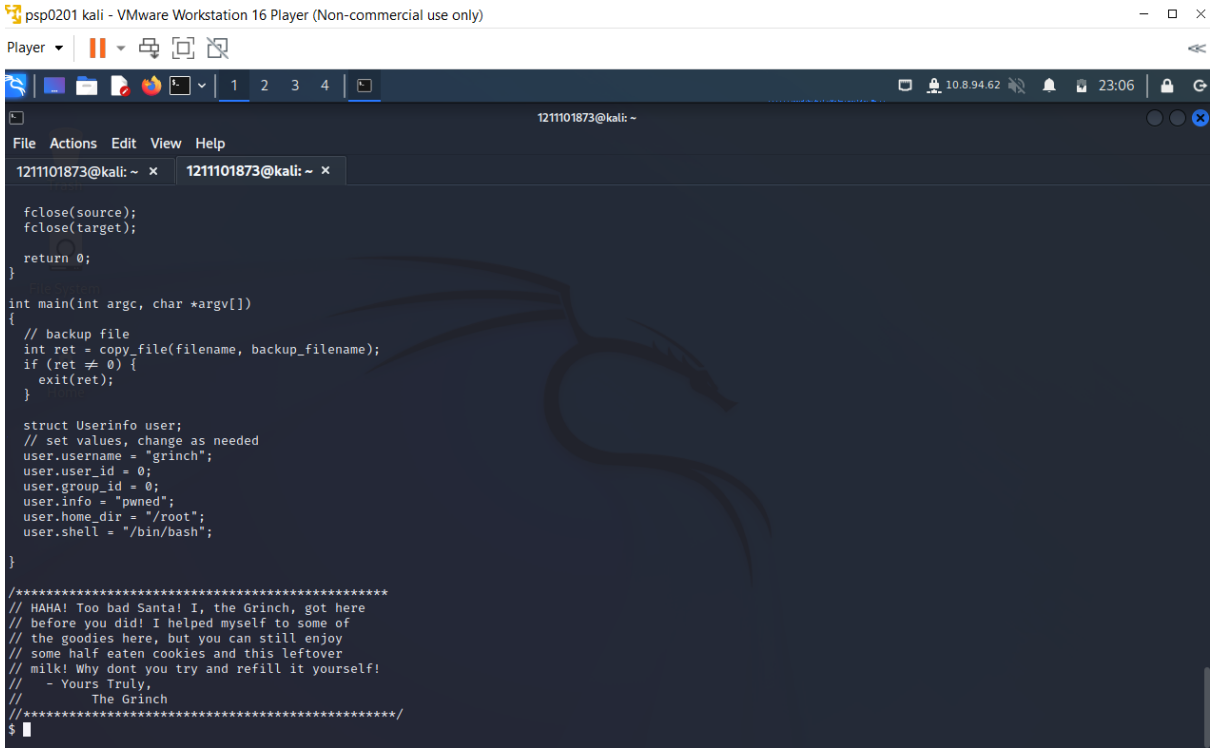


Question 3:What distribution of Linux and version number is this server running?

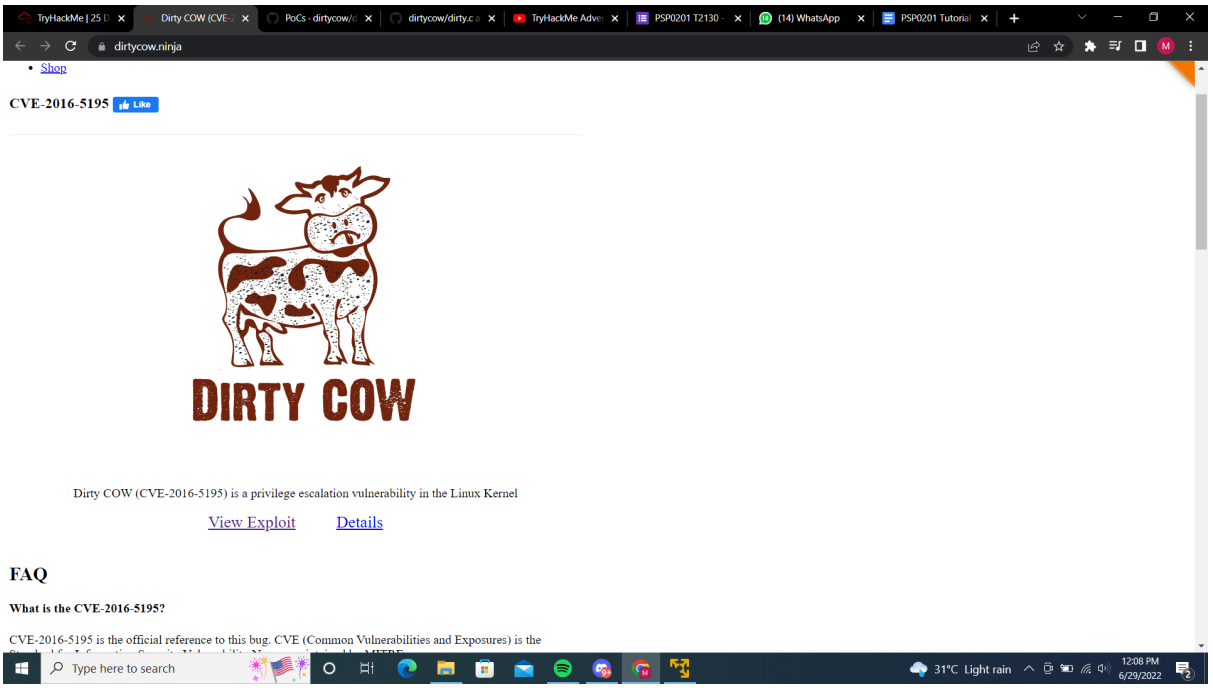


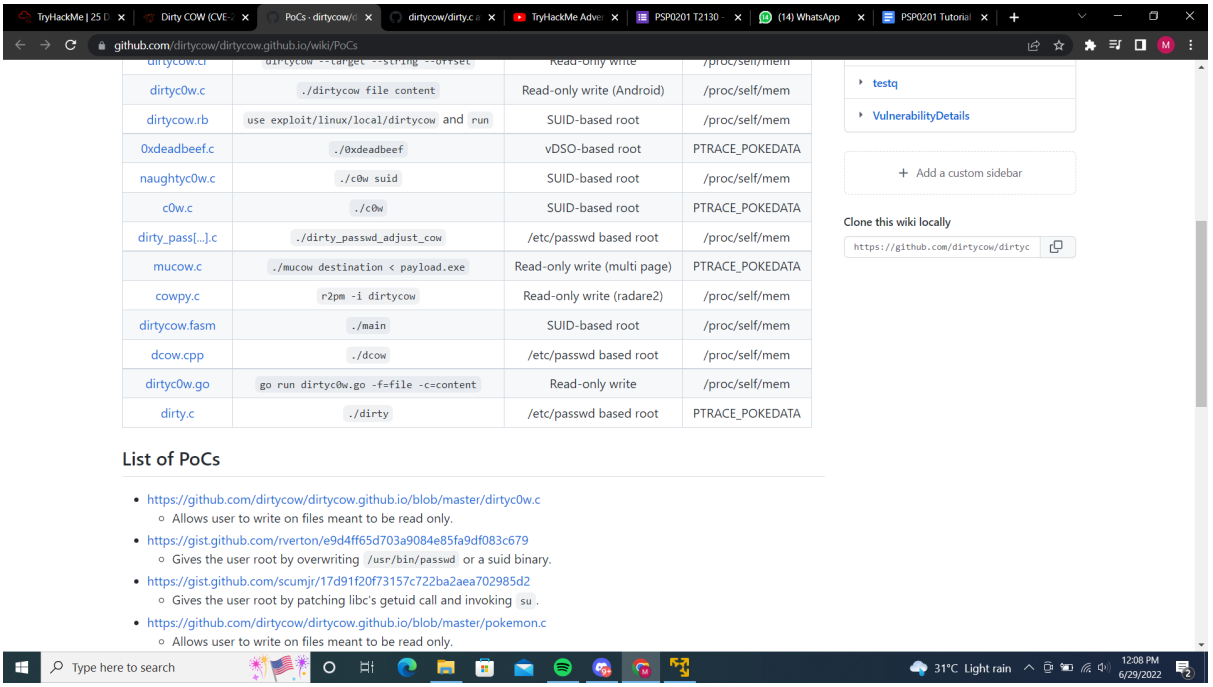


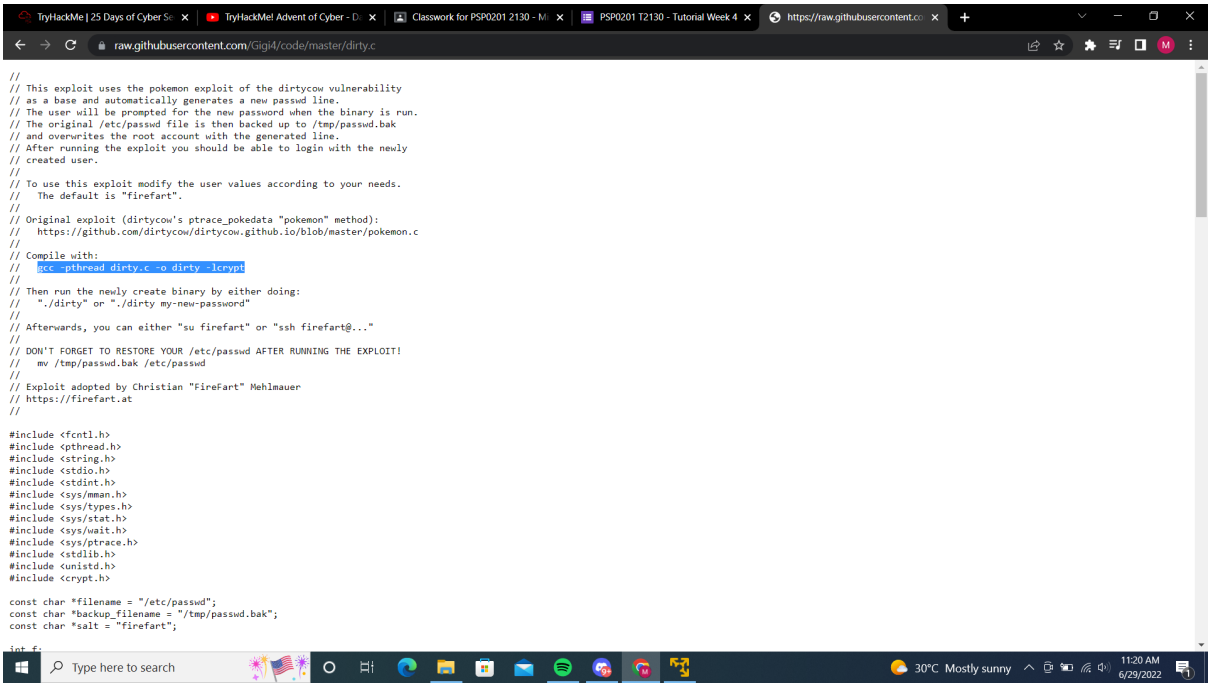
Question 4: Who got here first?



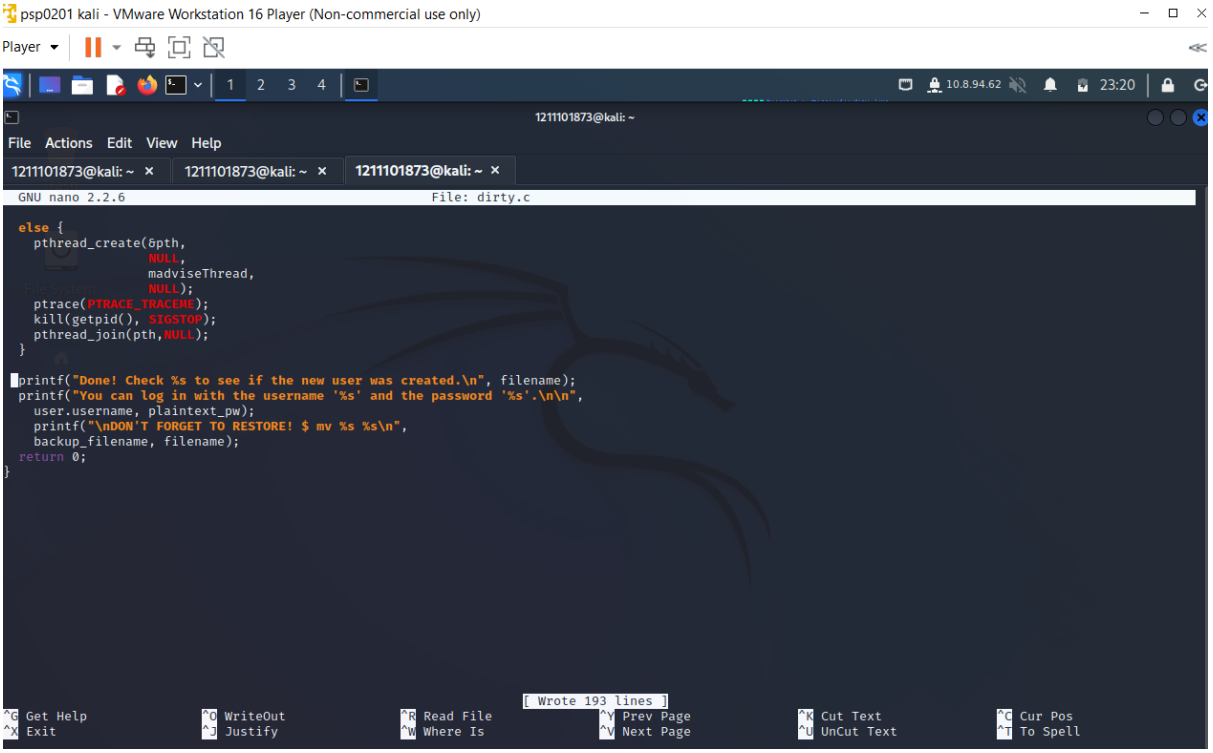
<u>Question 5</u>: What is the verbatim syntax you can use to compile, taken from the real C source code comments?





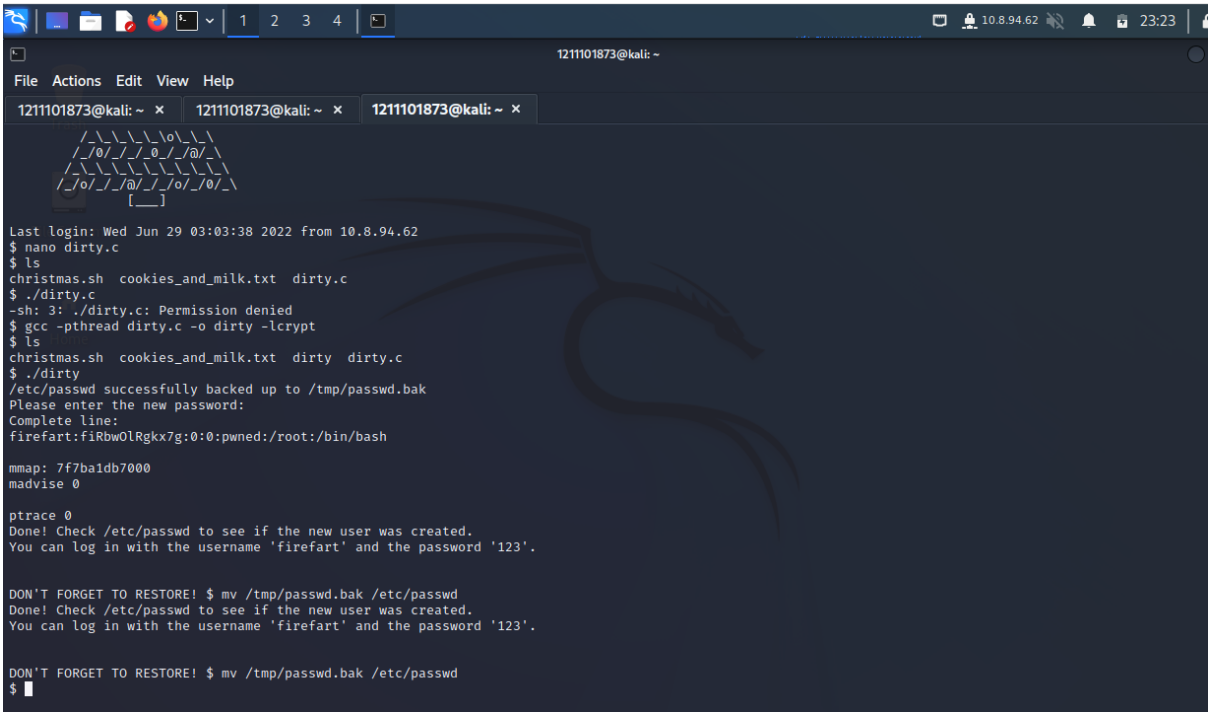


Question 6: What "new" username was created, with the default operations of the real C source code?



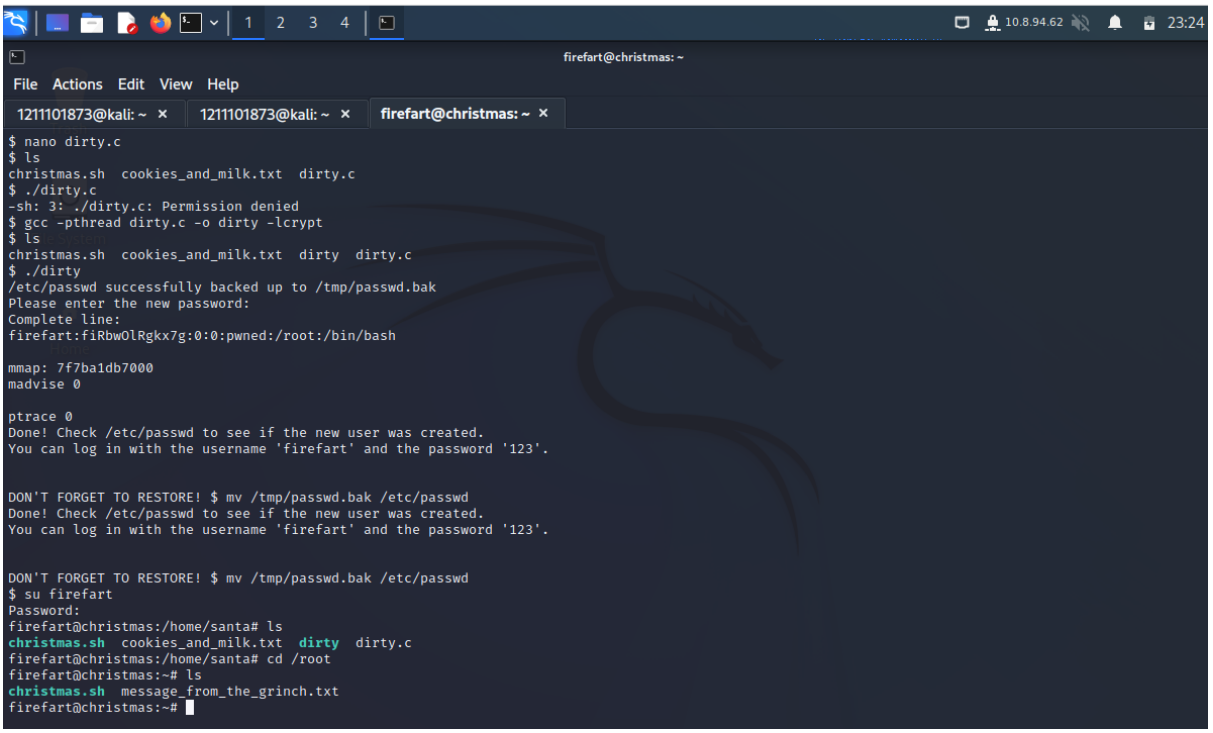
psp0201 kali - VMware Workstation 16 Player (Non-commercial use only)

Player

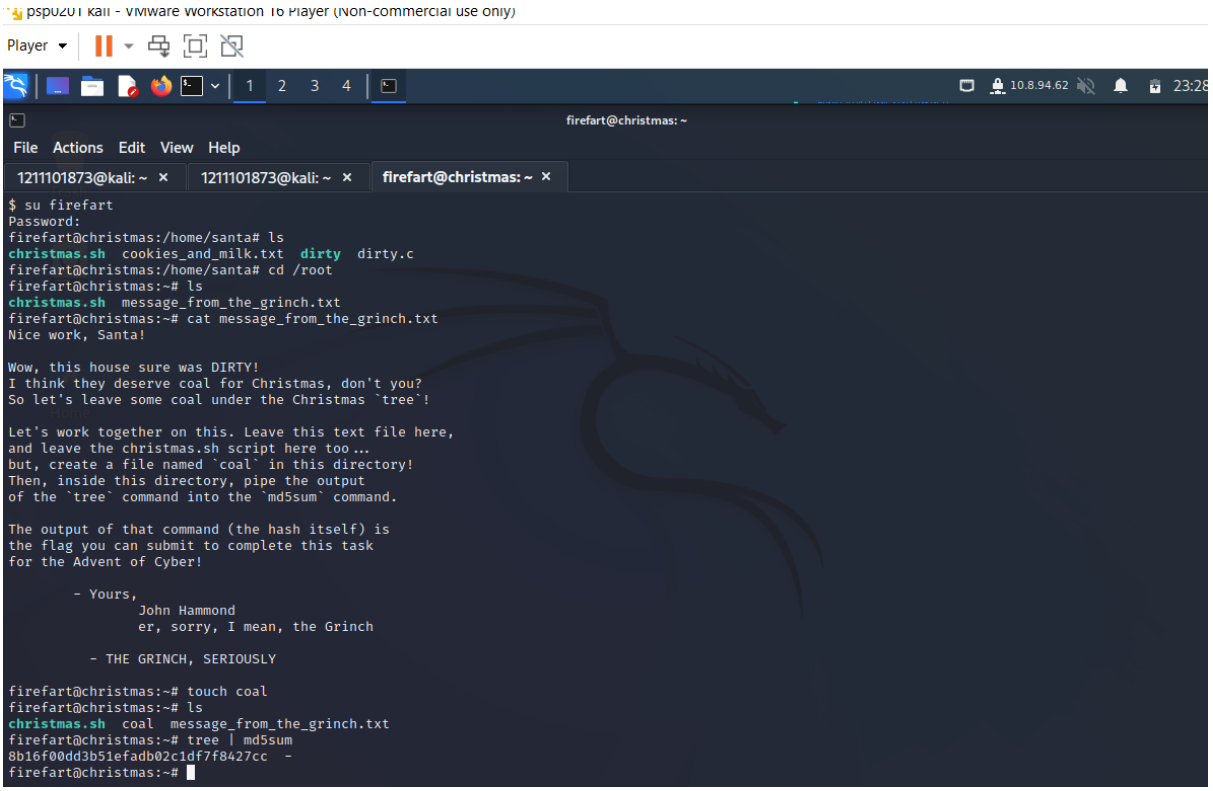


psp0201 kali - VMware Workstation 16 Player (Non-commercial use only)

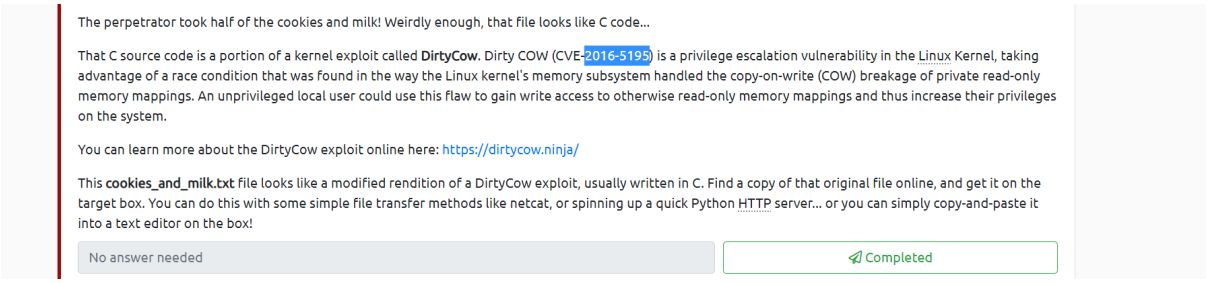
Player



Question 7: What is the MD5 hash output?



Question 8: What is the CVE for DirtyCow?



The Throughout Process:

For the first step, we follow the instructions that were given in the tryhackme to deploy the machine and run the command nmap **<IP_ADDRESS>**. From there, we can see that the old, deprecated protocol and service that were running was **telnet**. Next, we tried to connect to the service by running the command **telnet MACHINE_IP**. We did not include the port from nmap scan because the default port for telnet is 23. From there, we received the username and also the password for the christmas login, which the credential that was left for us was the password itself, **clauschristmas**. Next, we tried to login to the christmas login by running the command "**ssh santa@MACHINE_IP**" . We use "santa" just to specify that we are santa and not the kali account. When we were logged in, we simply run the command "**cat /etc/*release**" to receive the distribution of Linux and version number that the server is running. From there, we get that the distribution of Linux and the version number that the server was running is **Ubuntu 12.04**. Next, we found out that there was a file named "**cookies_and_milk.txt**" by running the command "**ls**". So, we tried to see what was in the file, there was a message that said that the **grinch** got here first! Next, for question 5, we got the verbatim syntax that we can use to compile by researching on the DirtyCow link that was provided in the notes. We are required to add a file named "**dirty.c**" into the system, which we added by using "**nano**". From the link, we took the codes for link "**dirty.c**" and pasted it in the file. Next, we ran the verbatim syntax , then "**./dirty**" and we inserted a new password for "**firefart**". And lastly, for the MD5 hash output, we followed the instructions to change the user account to a new user account and own the server. For that, we run the command "**su firefart**" and run the command "**cd /root**" to own the server. We noticed that there was a message left for us by the grinch. We followed grinch's instructions and run the command "**tree | md5sum**" to get the hash.

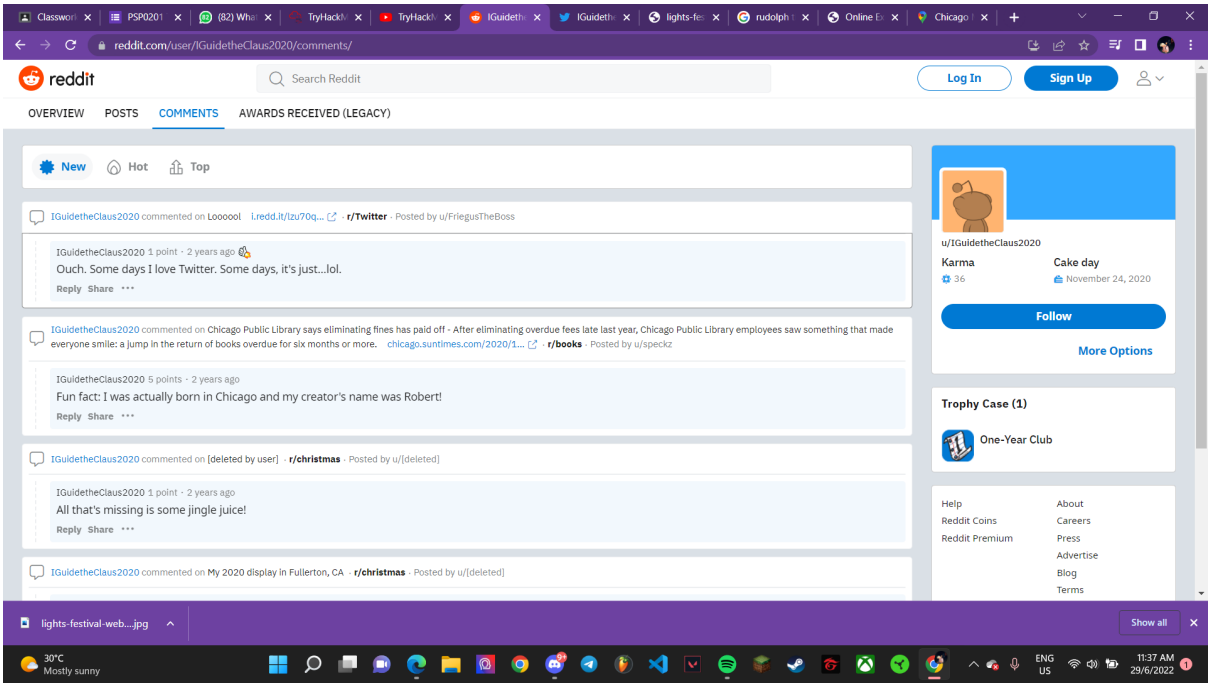
Day 14 : Where's Rudolph?

Tools used: Browser, Firefox

Solution:

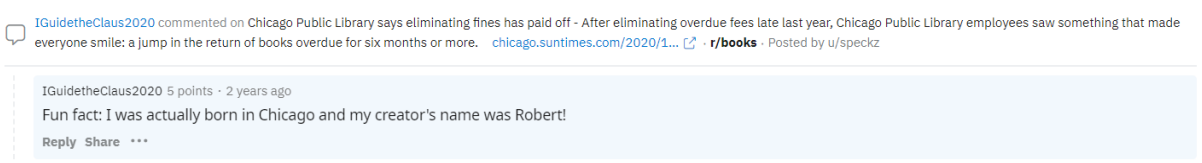
Question 1: What URL will take me directly to Rudolph's Reddit comment history?

Search ***IGuidetheClass reddit*** at browser, then go to comment and copy URL ***https://www.reddit.com/user/IGuidetheClaus2020/comments/***



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

According to Rudolph, he was born in CHICAGO

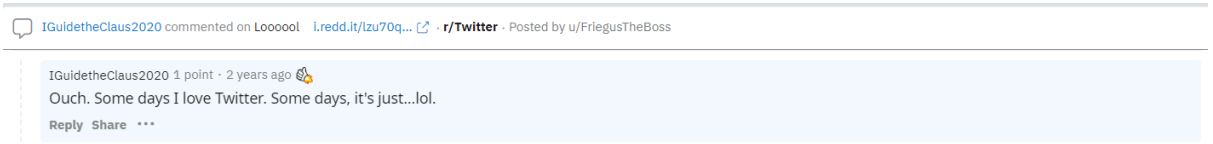


Question 3: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?

Answer : May

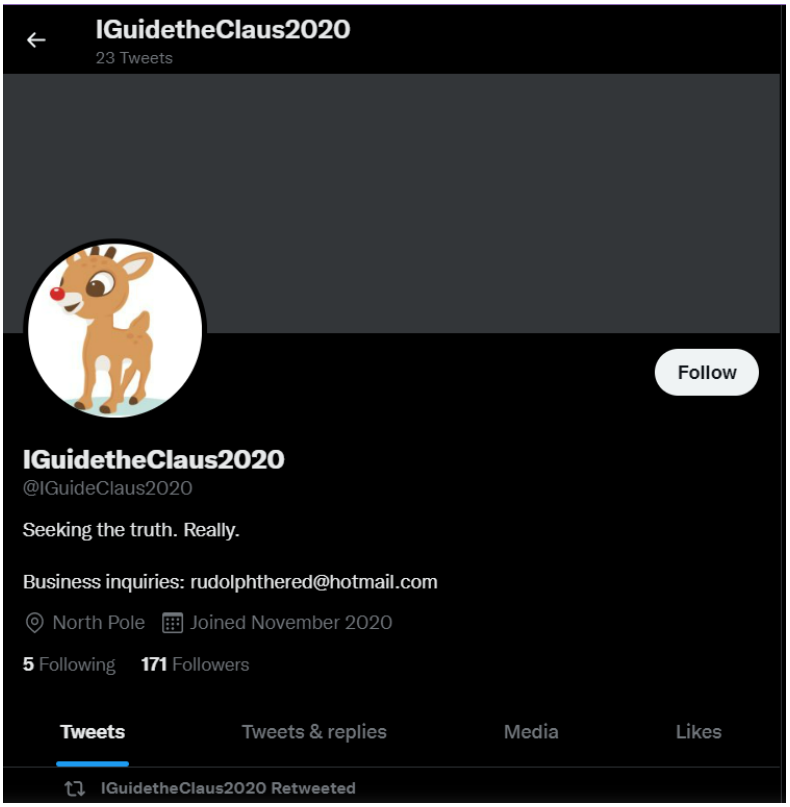
Question 4: On what other social media platform might Rudolph have an account?

Answer: Twitter



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

Answer: IGuideClaus2020

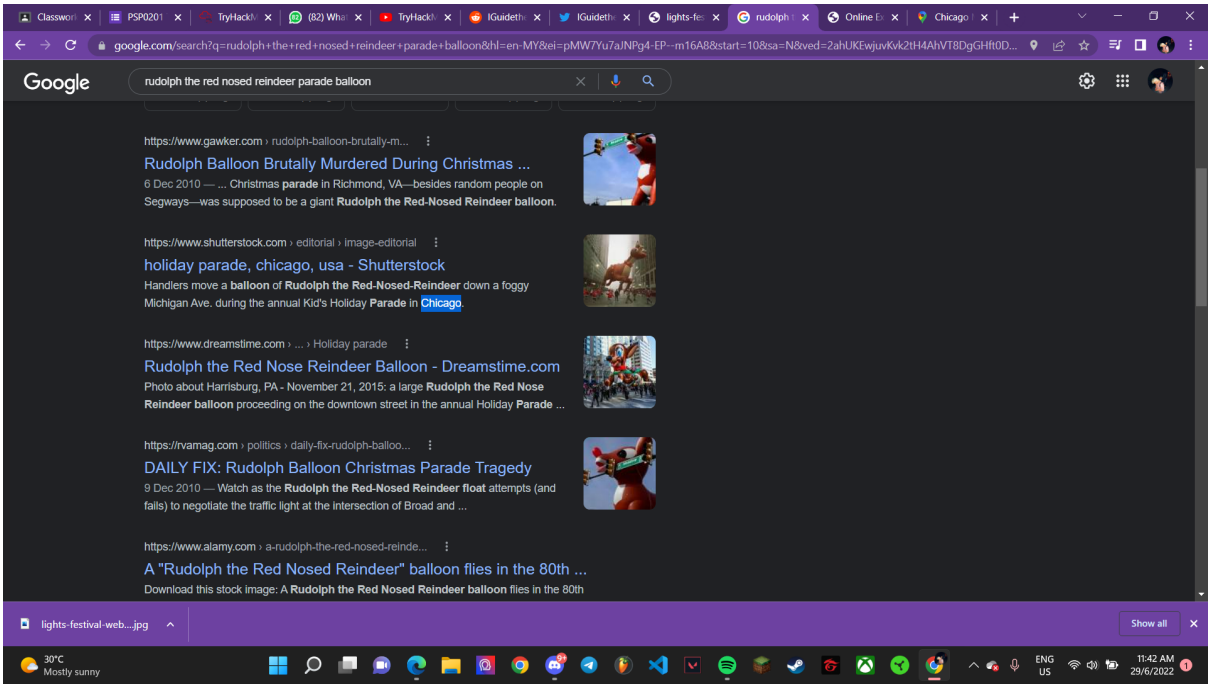


Question 6: What appears to be Rudolph's favorite TV show right now?

Answer: bachelorette

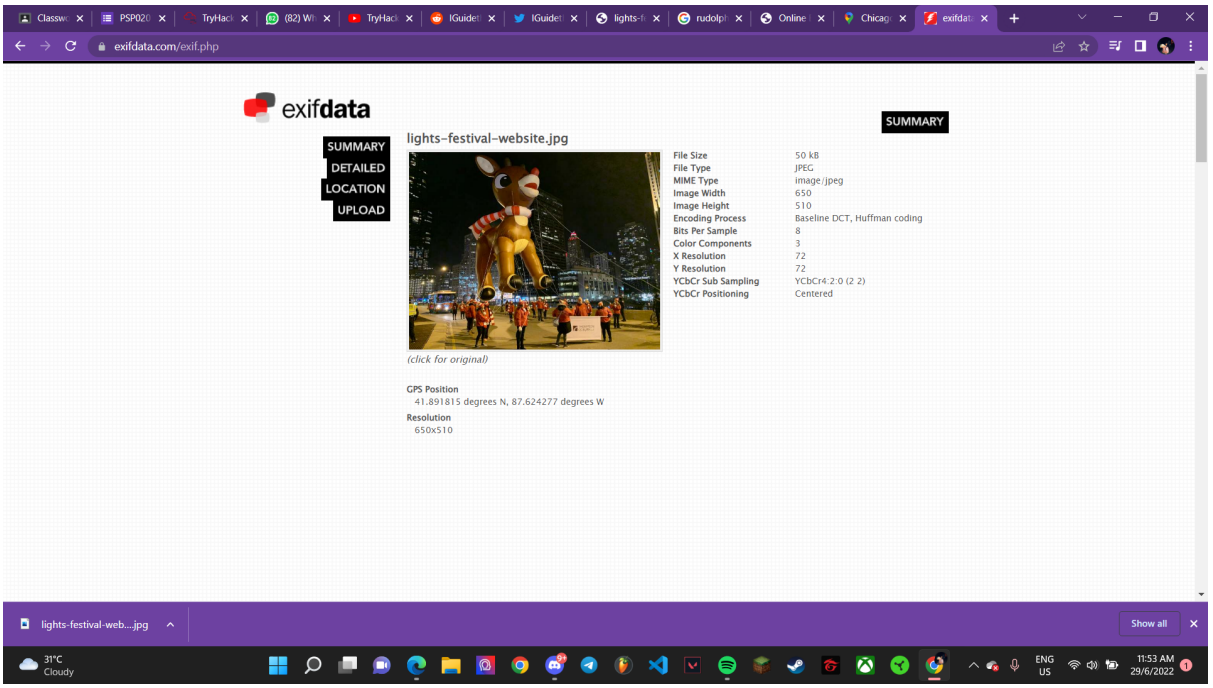
Question 7: Based on Rudolph's post history, he took part in a parade. Where did the parade take place?

Answer: Chicago



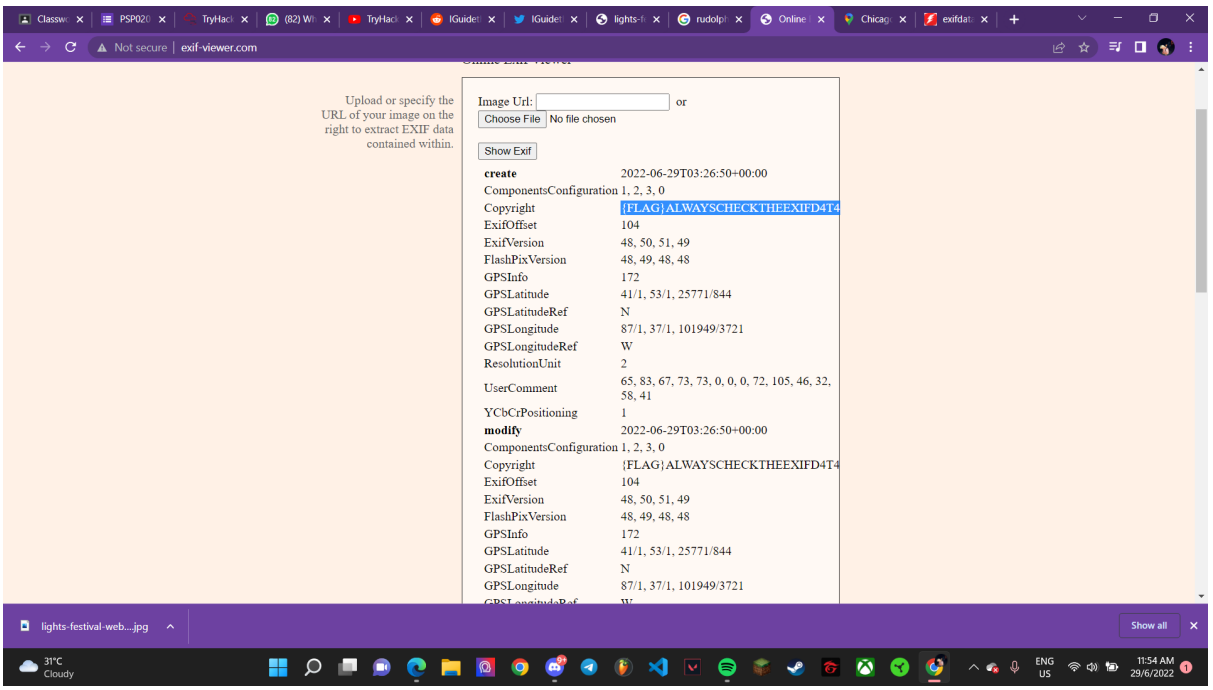
Question 8: Okay, you found the city, but where specifically was one of the photos taken?

Answer: 41.891815 ,-87.624277



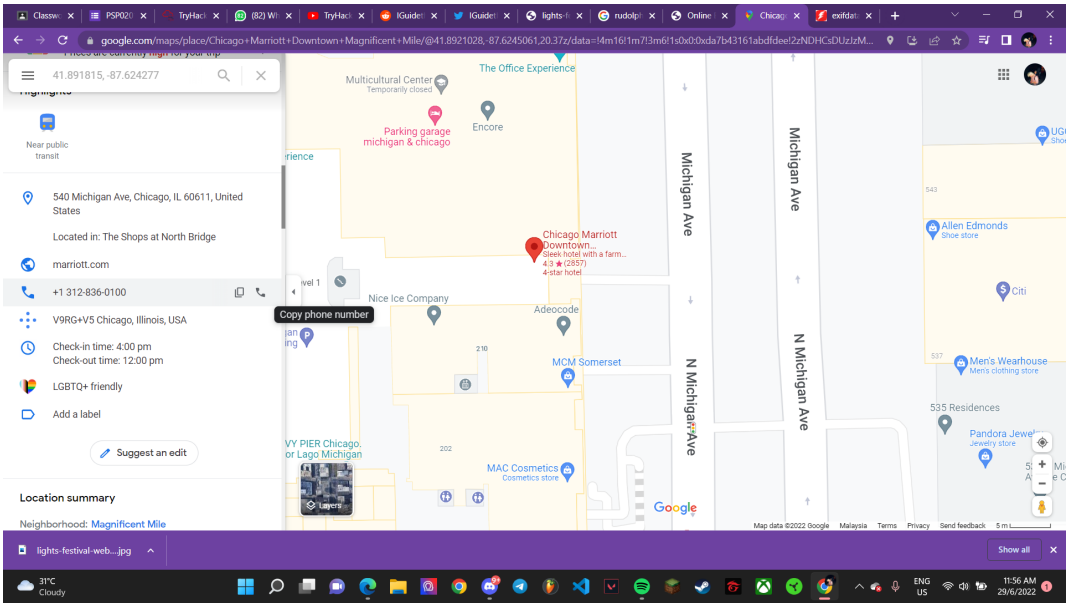
Question 9: Did you find a flag too?

Answer: {FLAG}ALWAYSCHECKTHEEXIFD4T4



Question 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



The Throughout Process

To identify typical crucial processes in an OSINT study, this assignment was developed. For question 1 we were told to find the Url about Rudolph's Reddit comment history? We use ***https://www.reddit.com/user/IGuidetheClaus2020/comments/*** to find the answer.

For the question 2, it told us to know where Rundolph born. We searched in the browser that Rundolph was born in ***Chicago***. For question 3, Google tells us that Rundolph's last name is ***May.*** For question 4, Rudolph might have a profile on another social media network is ***Tweeter.*** IGuideClaus2020 is Rudolph's username on that platform. ***Bachelorette*** looks to be Rudolph's current favourite television programme. For question 9, we use exifdata to find the flag which is {FLAG}ALWAYSCHECKTHEEXIFD4T4. For the last question, based on the totality of the data gathered. Rudolph is probably in Chicago and is staying at a hotel on Magnificent Mile, the street numbers of the hotel address is ***540*** that we can found it through google map

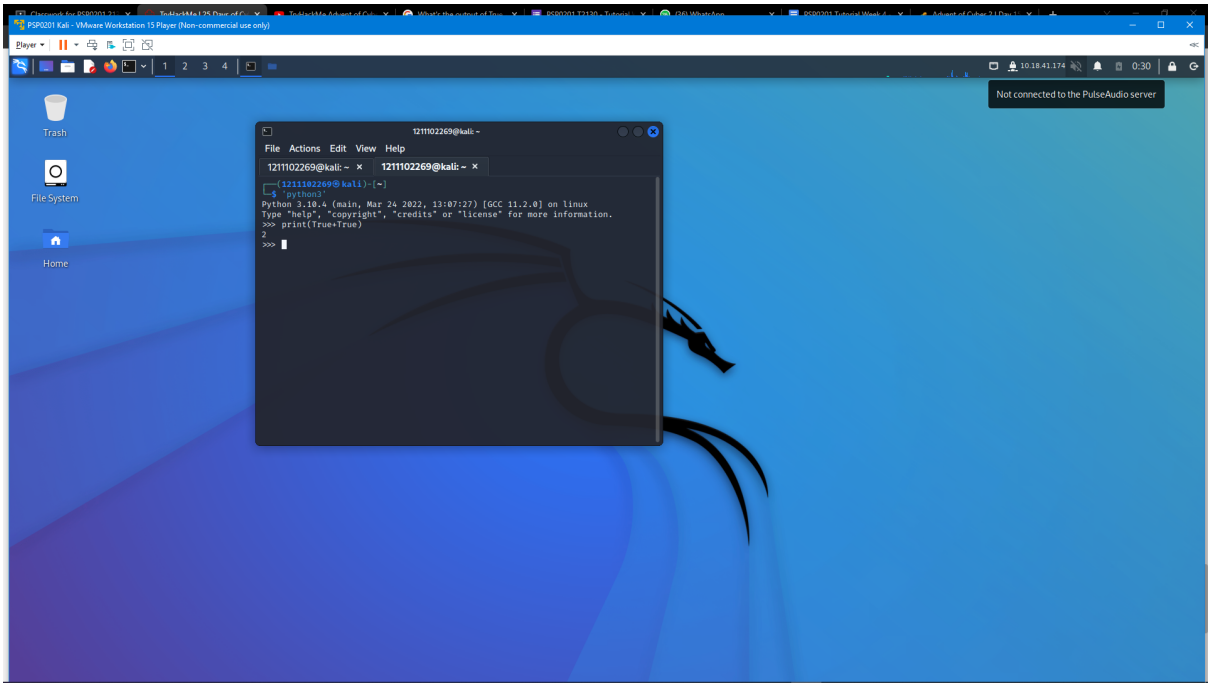
Day 15 :There's Python in my stocking!

Tools used: Kali Linux, Firefox,Visual Studio Code

Solution:

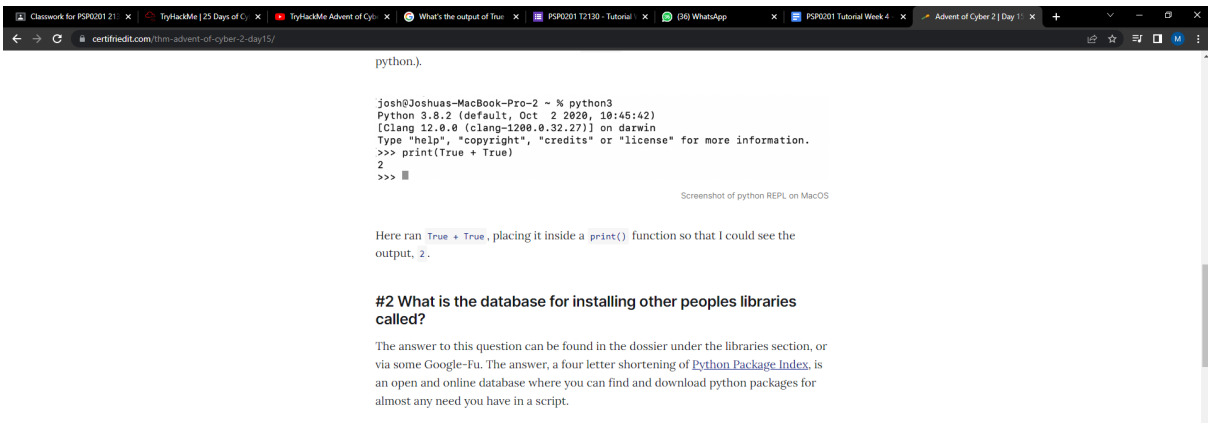
Question 1:What's the output of True+True?

Answer:2



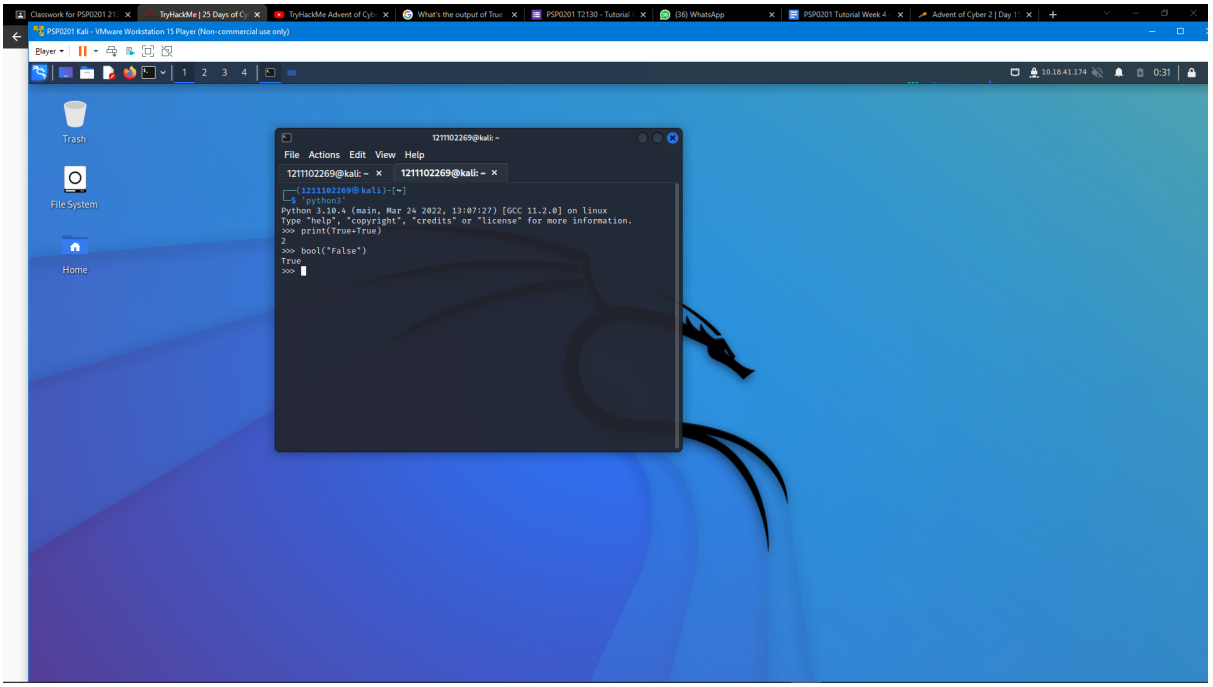
Question 2:What's the database for installing other peoples libraries called?

Answer:PyPi



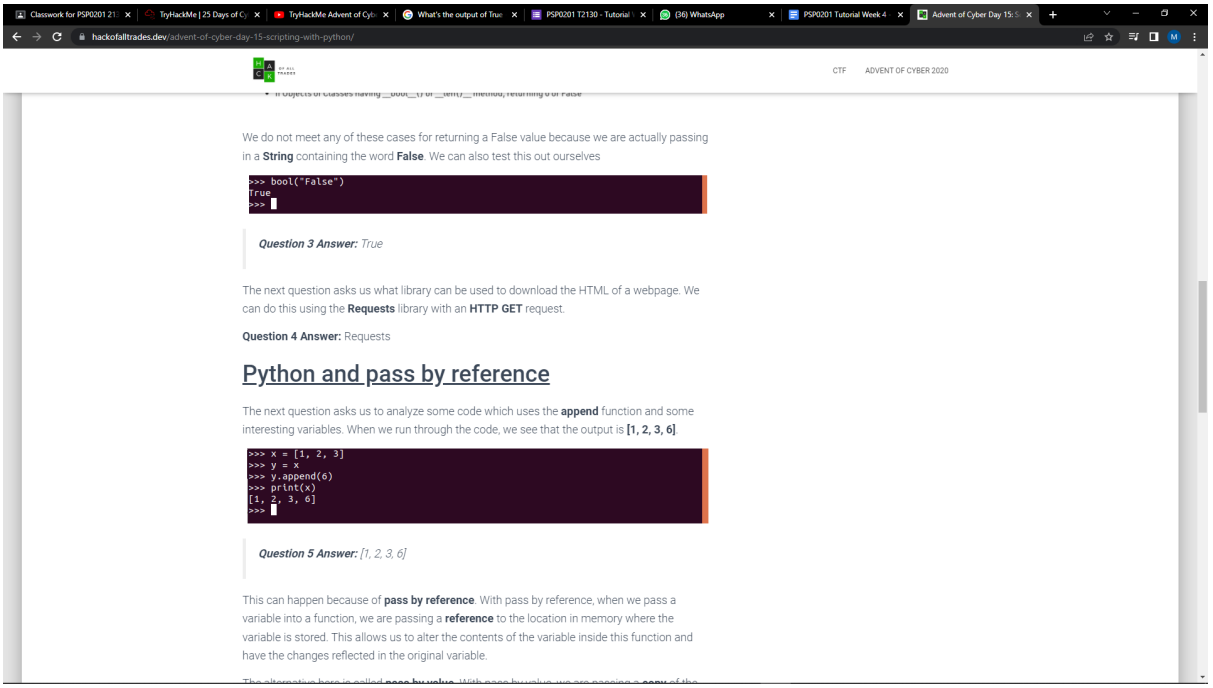
Question 3:What is the output of bool("False")?

Answer:True



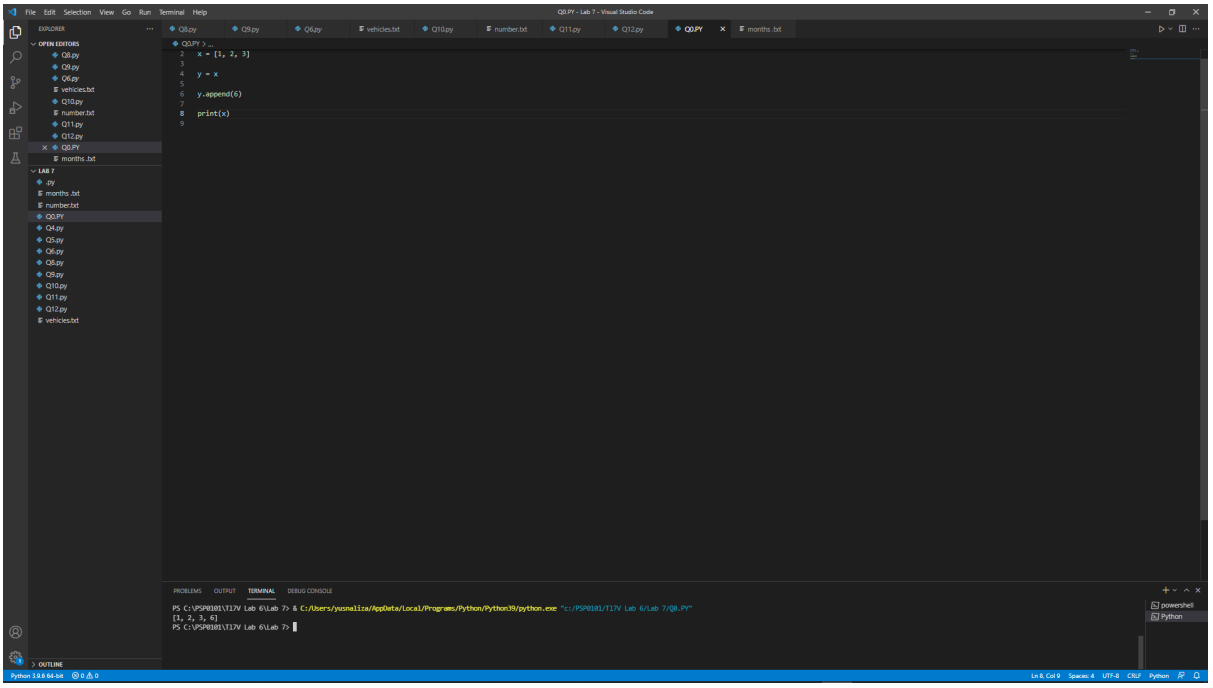
Question 4:What library lets us download the HTML of a webpage?

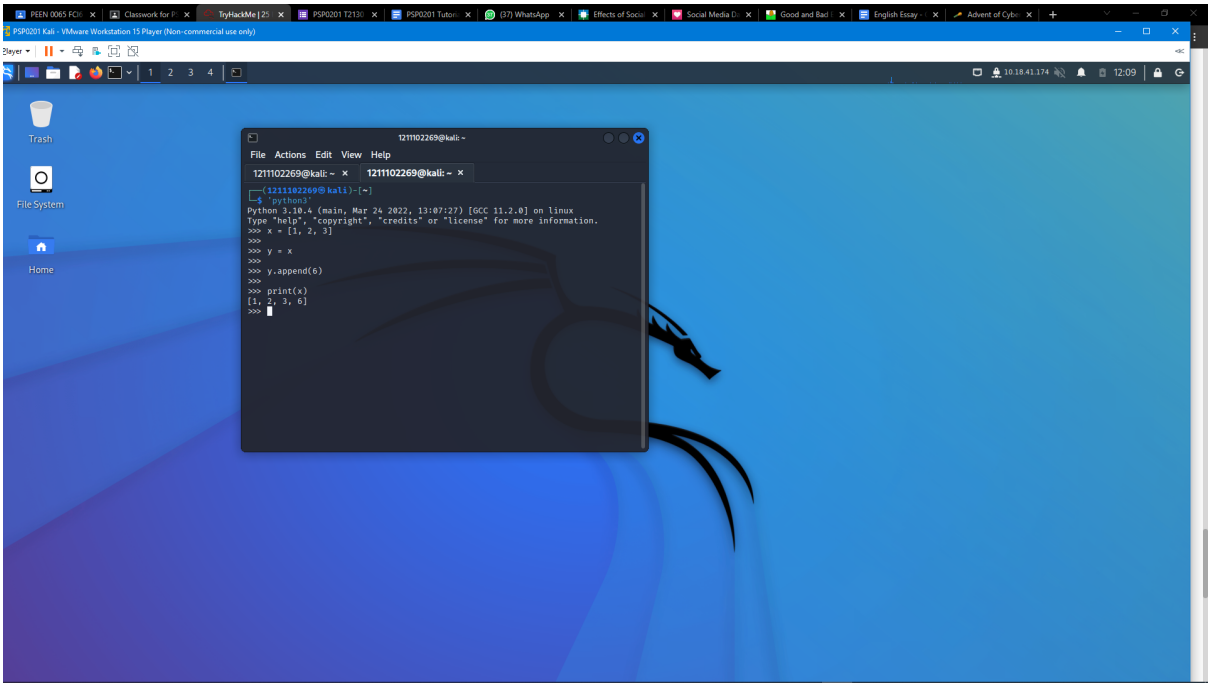
Answer:**Requests**



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

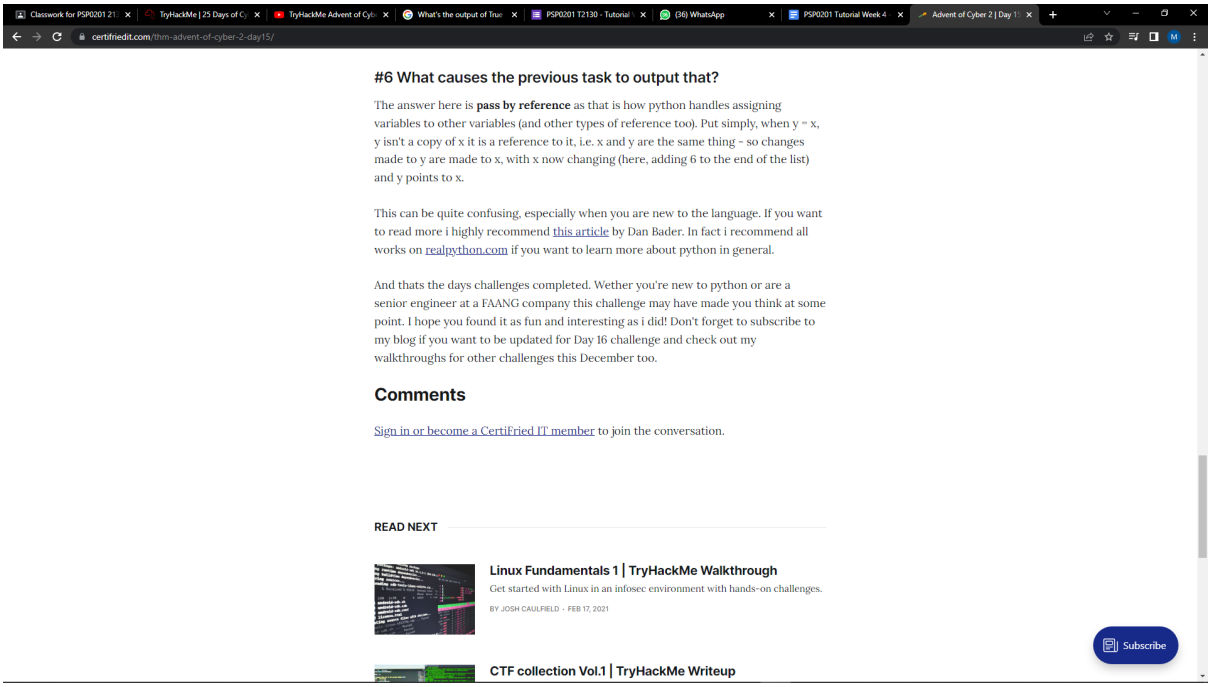
Answer:[1, 2, 3, 6]





Question 6: What causes the previous task to output that?

Answer:Pass by reference

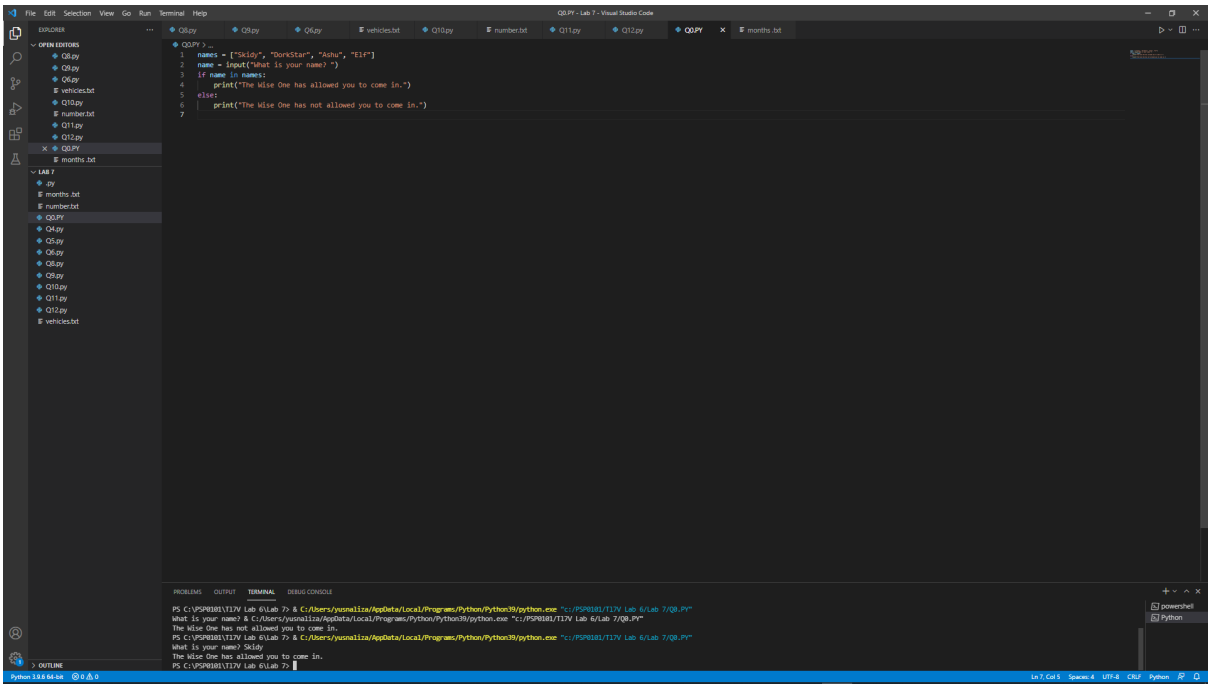


Examine the following code:

```
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.")
```

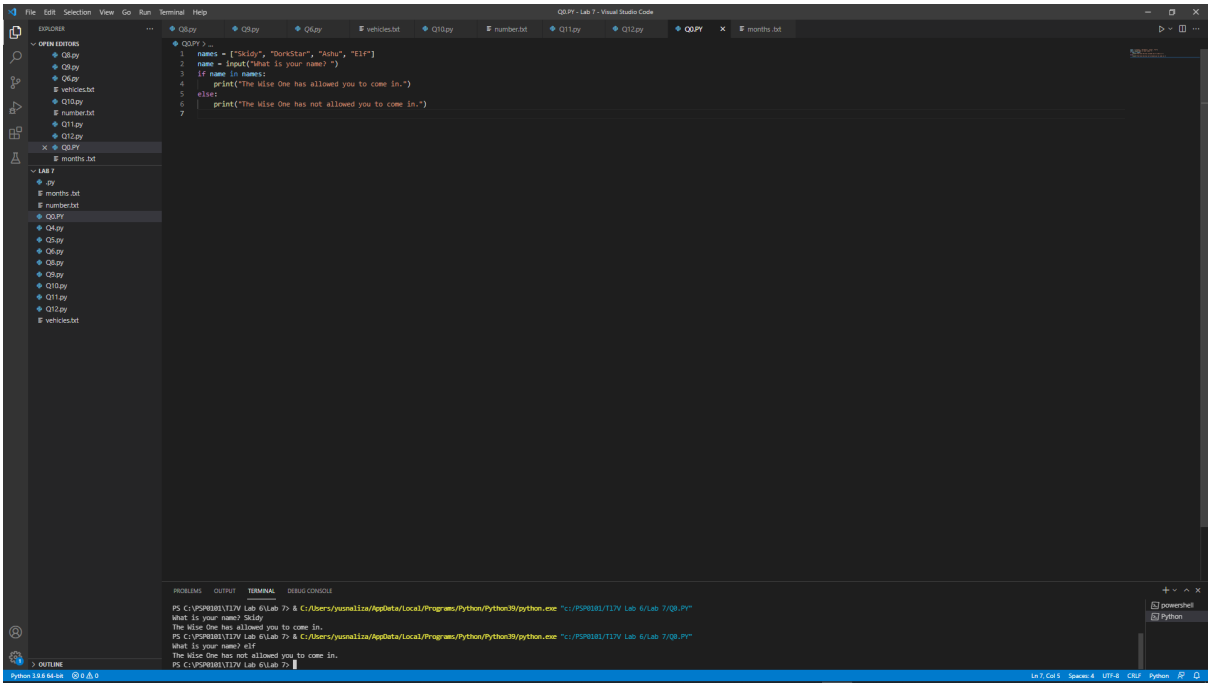
Question 7: if the input was "Skidy", what will be printed?

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



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

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



The Throughout Process

For the first step,you will need to activate your python.Load up the terminal and enter “pyhton3” . This will load an interactive editor for Python.For the first question,just simply type print(True+True).Then the answer will be print out.For the next question,u can just search it on internet since it is a general knowledge question.For the third question,just simply write bool(“False”) in the command and enter.You will get the answer.For the next question,its a general knowledge.You just need to search it up on google and will get the answer.For the question 5,I'm using both kali and visual studio code.The code has been given on the question.You just need to type `x = [1, 2, 3]`

```
y = x

y.append(6)

print(x)
```

And enter.Then you will get the answer.For question 6,its general knowledge.You can search it up on google and will get the answer.For question 7,i'm using Visual Studio Code.Firstly,you need to enter 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.")
```

And then,the system gonna ask,”What is your name?”.You will need to enter name “Skidy”.For the last question,same as before.Just change the name to “elf”.Then you will get the answer.