PSP0201
WEEKLY WRITE UP
WEEK 4
GROUP 7

Group Name : Sang Haekeo (The Hackers)

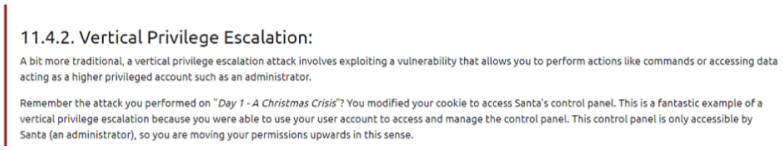
Sang
- Taken from a Malay word , sang , meaning ‘the’

Haekeo
- Taken from a Korean word , 해커 , meaning ‘hacker’
-

ID	NAME	ROLE
1211102162	AMILIA NADZEERA BINTI BAHARUDIN	Leader
1211100930	KU NAJWA SYAUQINA BINTI KU AZRIN	Member
1211101693	SAVITHA MURUGUMUNISEGARAN	Member

Day 11 : The Rogue Gnome

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

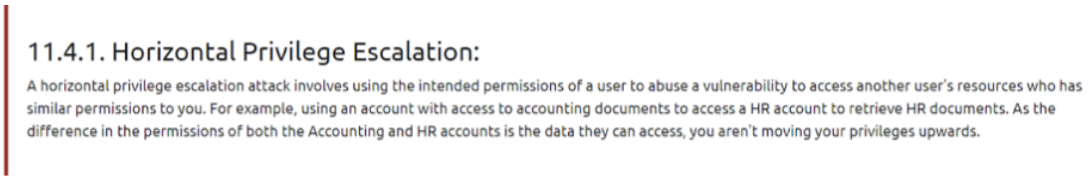


11.4.2. Vertical Privilege Escalation:

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.

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.

Q2&3: 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?

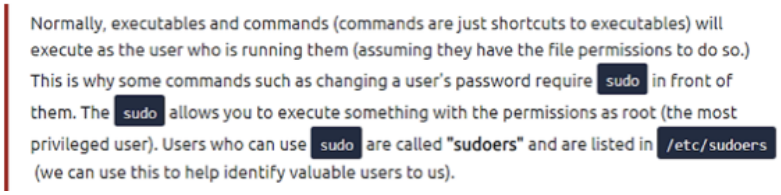


11.4.1. Horizontal Privilege Escalation:

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.

A2&3: Horizontal

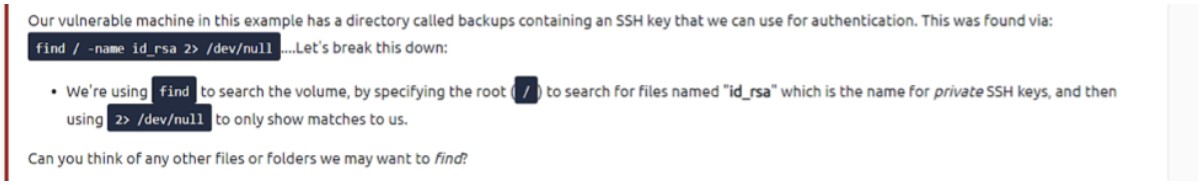
Q4 : What is the name of the file that contains a list of users who are a part of the sudo group?



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).

A4 : sudoers

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



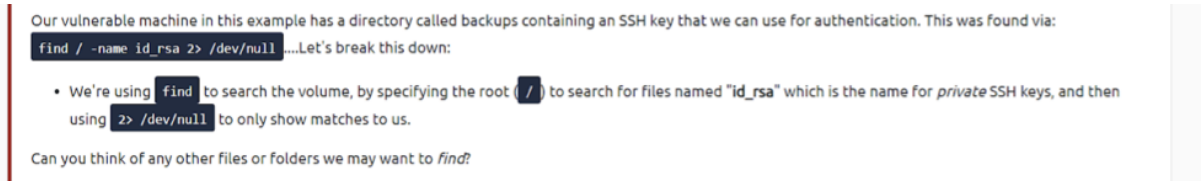
Our vulnerable machine in this example has a directory called backups containing an SSH key that we can use for authentication. This was found via: `find / -name id_rsa 2> /dev/null` ....Let's break this down:

- 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*?

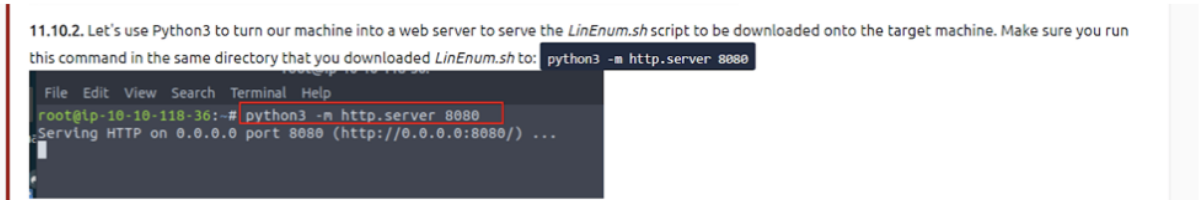
A5: find/ -name id_rsa 2> /dev/null

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?



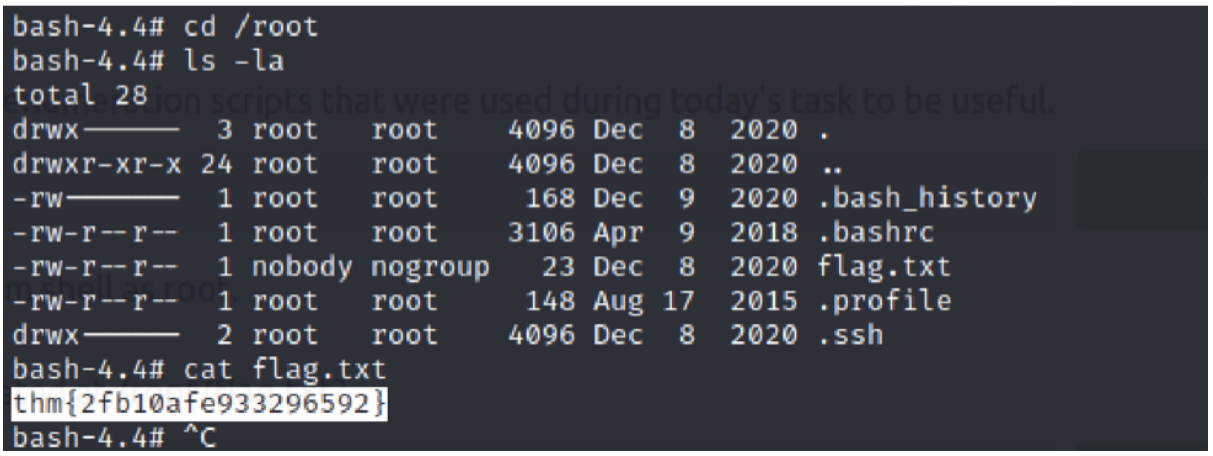
A6: chmod +x find.sh

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: python3 -m http.server 9999

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



A8: thm{2fb10afe933296592}

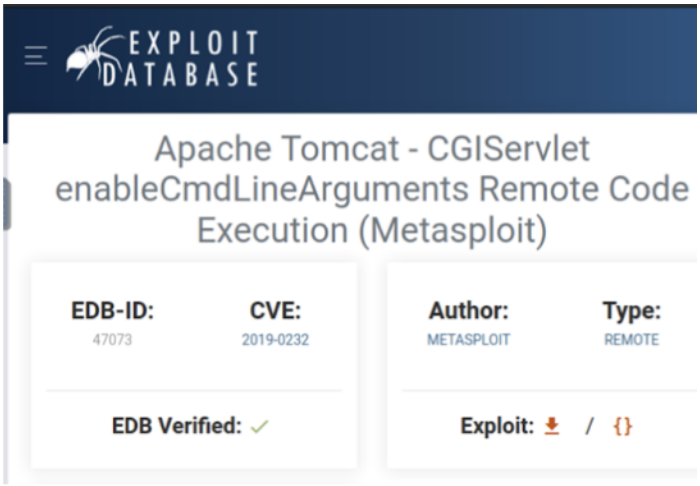
Day 12 : Ready , set , elf

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

```
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Apache Tomcat/9.0.17
1 service unrecognized despite returning data. If you know the service/version
```

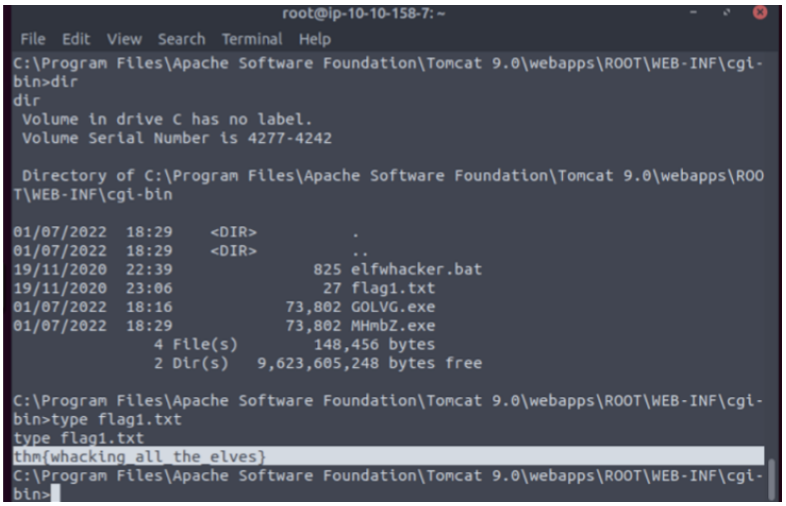
A1: 9.0.17

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



A2: CVE-2019-0232

Q3: What are the contents of flag1.txt ?



A3: thm{whacking_all_the_elves}

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

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.158.7      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

A4: LHOST , LPORT

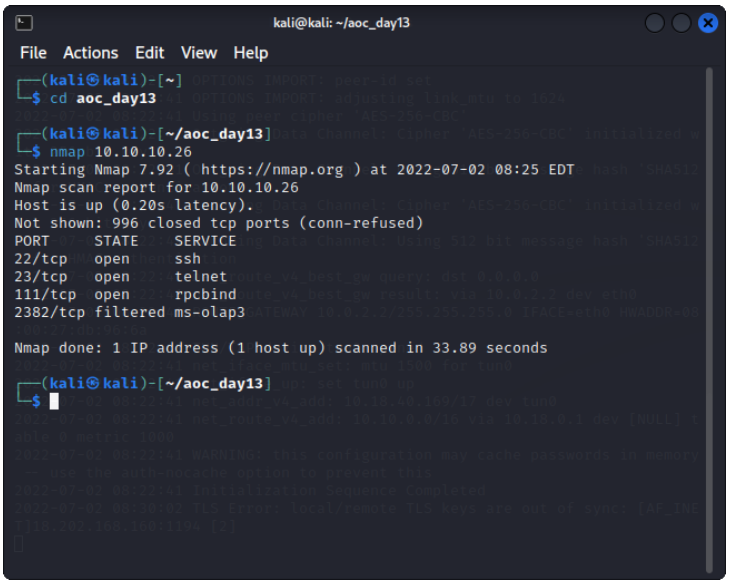
Thought process/methodology

We used the nmap tool on metasploit to enumerate the webserver to get the version number. With the information given , we browsed it on google where we found the CVE that can be used for the Metapreter entry onto the machine. On Metasploit Framework we use a search command and look up the exploit module and ran the exploit to create the session. We then execute a command shell followed by command dir to get the contents of flag1.txt.

DAY 13 – NETWORKING: COAL FOR CHRISTMAS

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

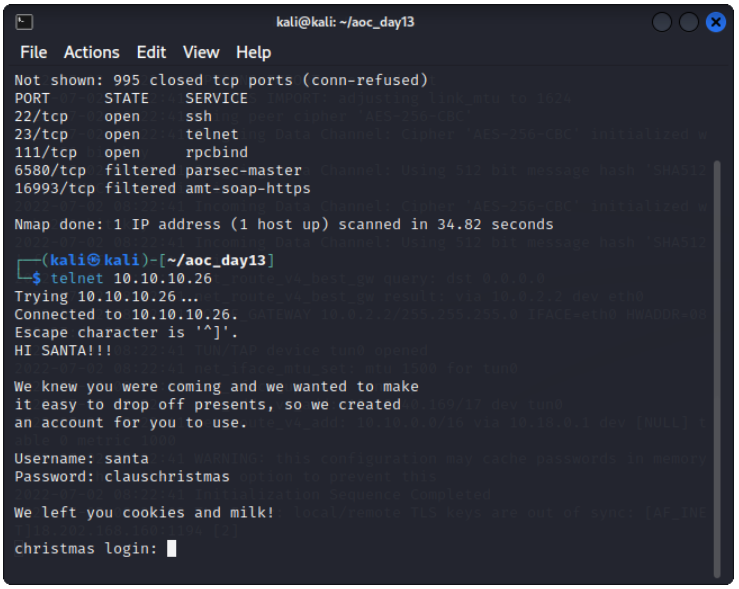
telnet



QUESTION 2 : What credential was left for you?

clauschristmas

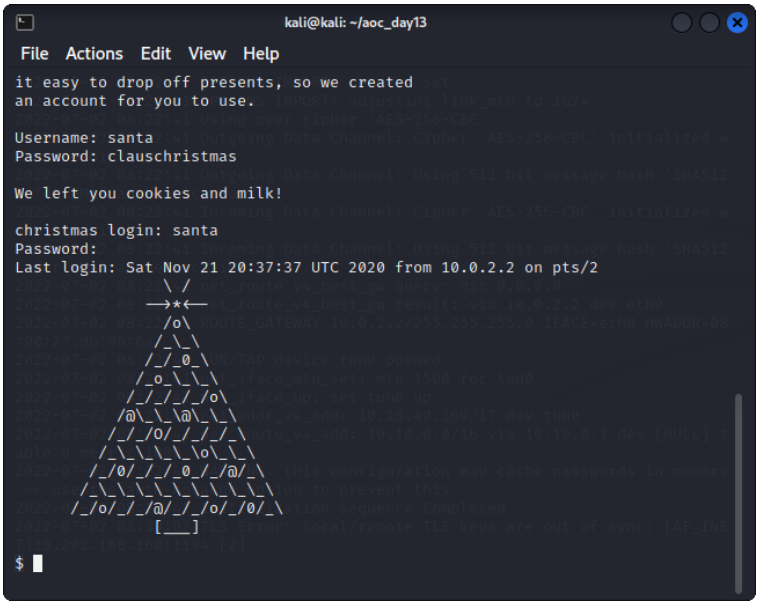
connect to the service with the standard command-line client netcat with syntax : telnet 10.10.10.26 (the ip address).



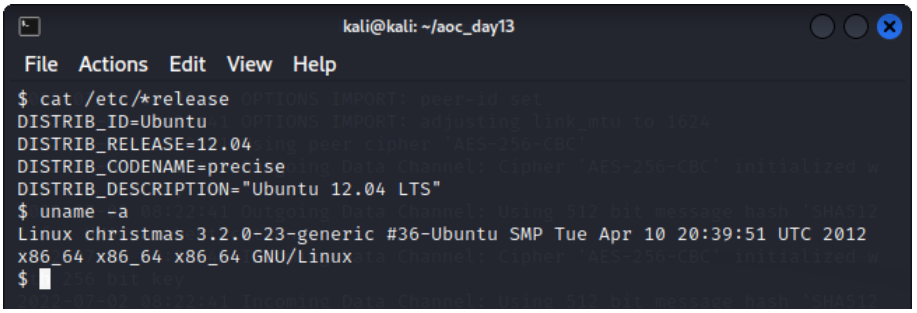
QUESTION 3 : What distribution of Linux and version number is this server running?

Ubuntu 12.04

Now login with username and password given.



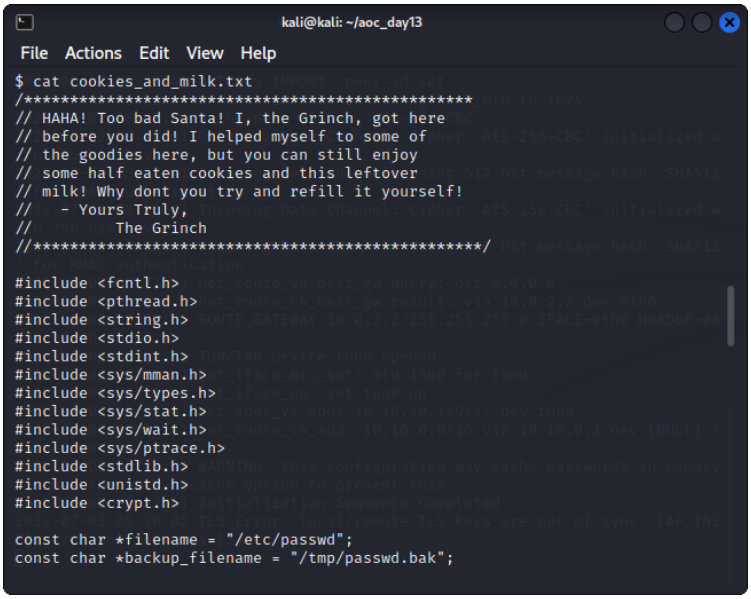
Using command cat /etc/*release to get information on distribution of linux.



QUESTION 4 : Who got here first?

grinch

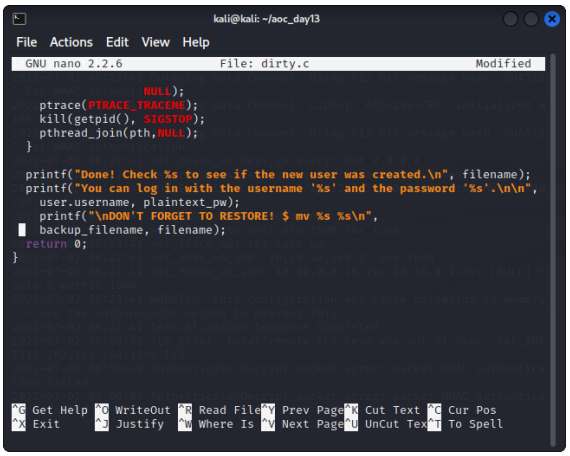
using cat command to look at the cookies and milk left by server, cat cookies_and_milk.txt



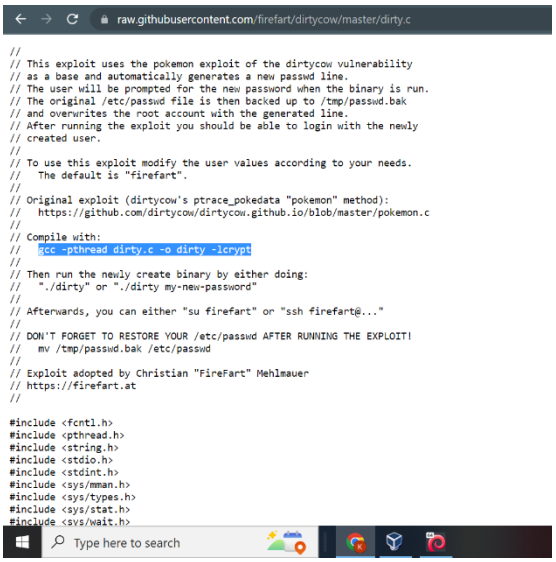
QUESTION 5 : What is the verbatim syntax you can use to compile, taken from the real C source code comments?

gcc -pthread dirty.c -o dirty -lcrypt

Find a copy of that original file online, copy-and-paste it into a text editor on the box.



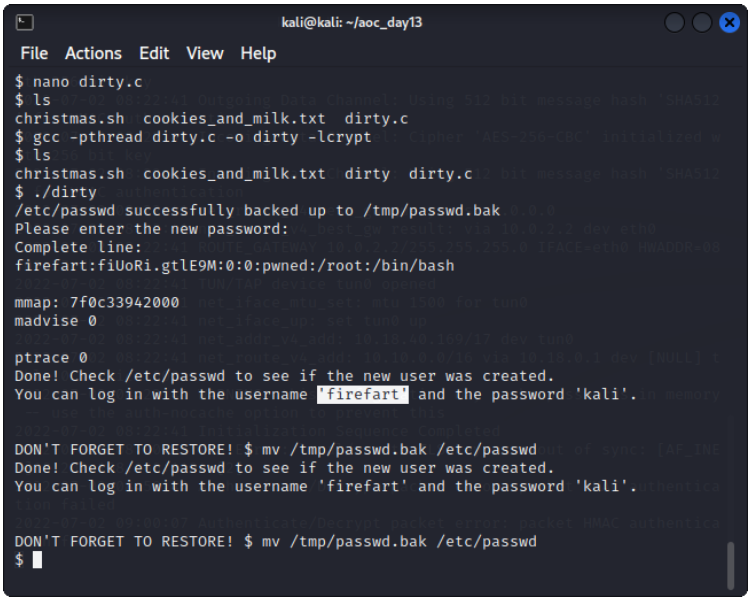
You can get the verbatim syntax from Dirtycow code.



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

firefart

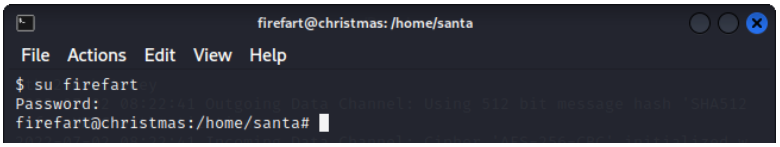
run the commands to compile the exploit, and run it.

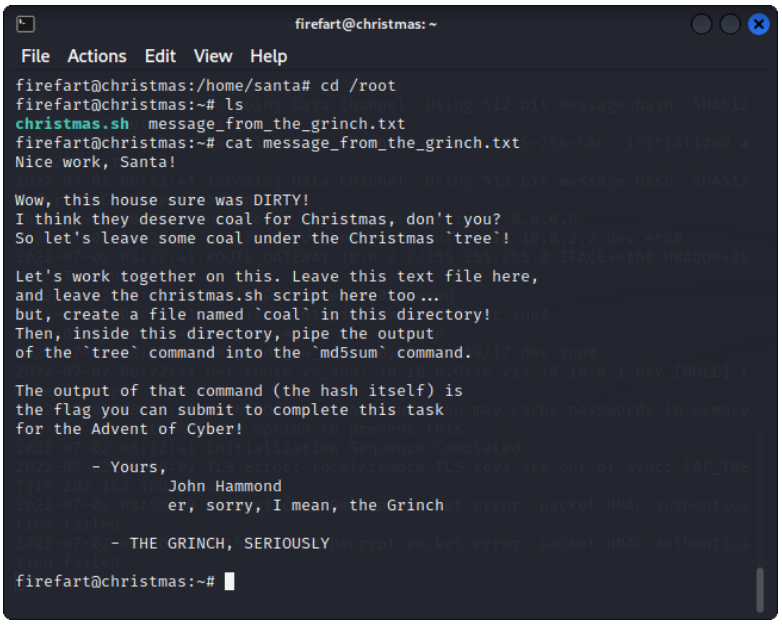


QUESTION 7 : What is the MD5 hash output?

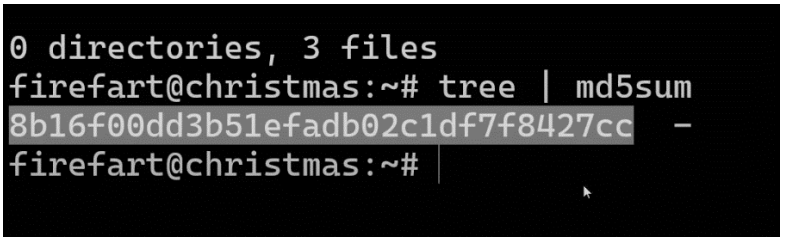
8b16f00dd3b51efadb02c1df7f8427cc

Switch the user into that new user account, using command su firefart and go to /root directory to own this server





Create a file named coal in the directory and pipe the output of the ‘tree’ command into the ‘md5sum’ command.



QUESTION 6 : What is the CVE for DirtyCow?

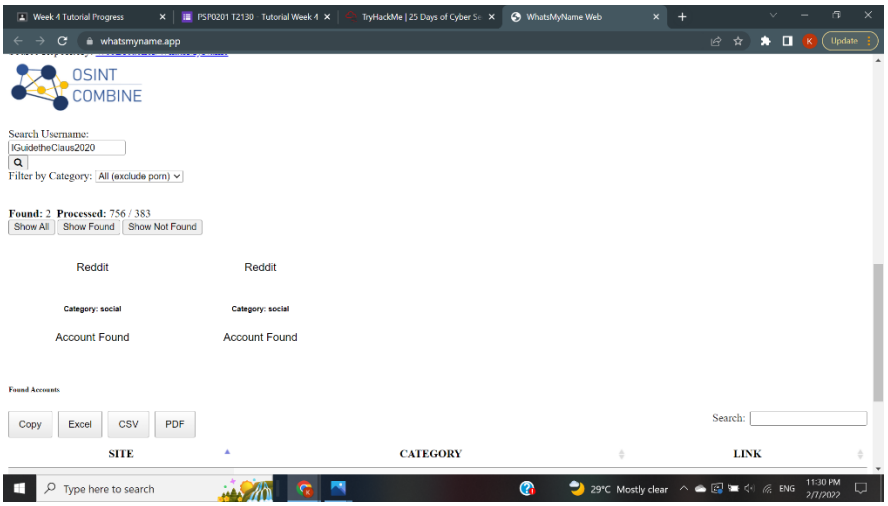
CVE-2016-5195

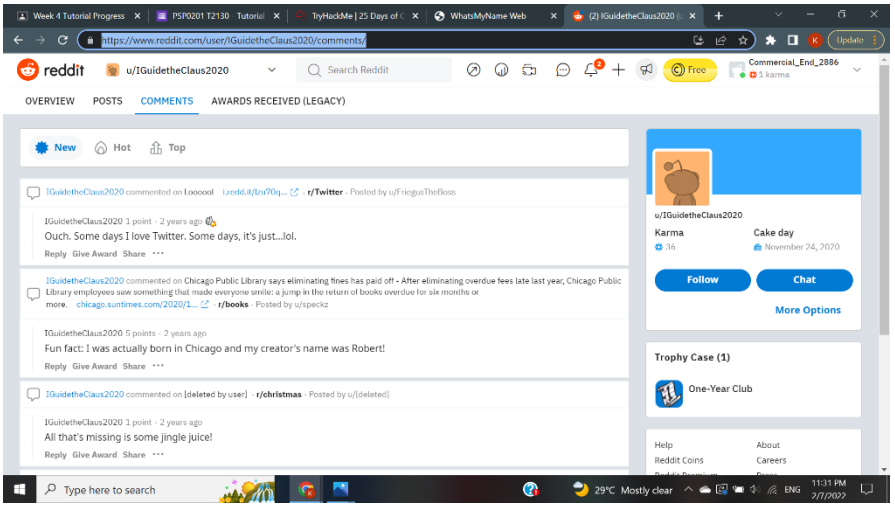
DAY 14 – OSINT: WHERE'S RUDOLPH?

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

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

search the given username on https://whatsmyname.app/ and we will find Rudolph's reddit. Once we get to the reddit account, go to comment and copy the link.

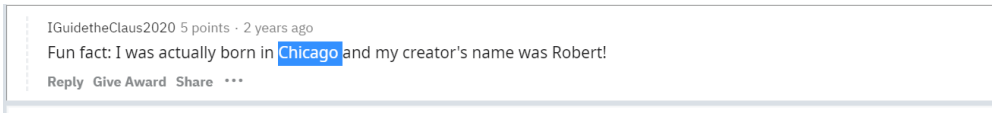




QUESTION 2: According to Rudolph, where was he born?

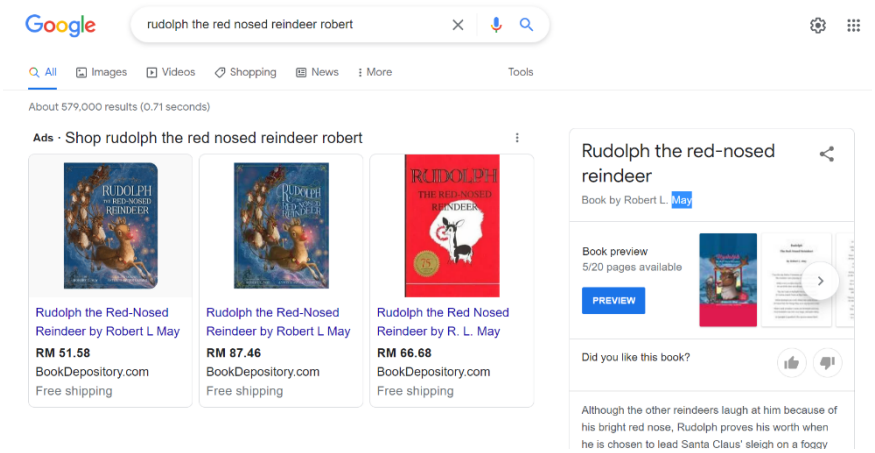
Chicago

We found out where he was born on one of his reddit comments.



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

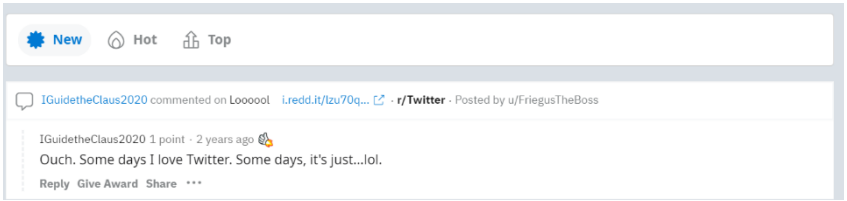
May

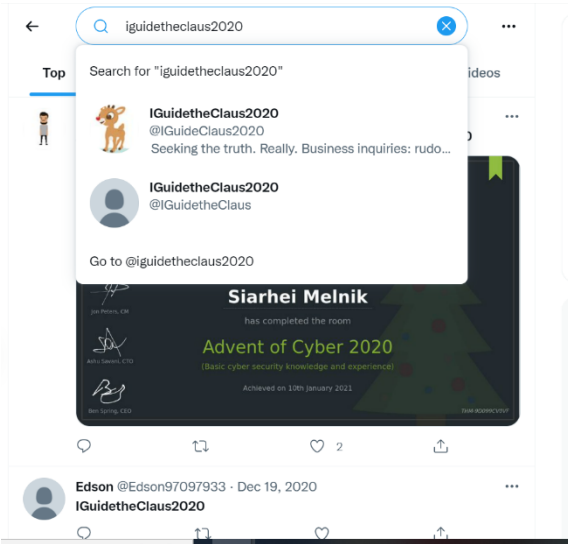


QUESTION 4: On what other social media platform might Rudolph have an account?

Twitter

We found out he has a twitter account from one of his comments on reddit and to confirm we search for him on twitter.





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

@IGuideClaus2020

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

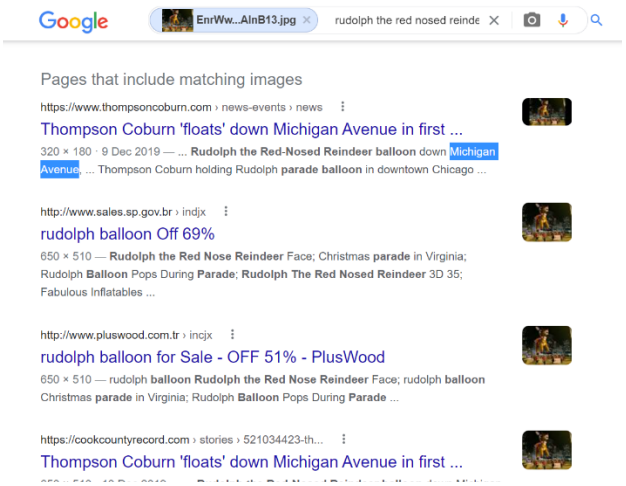
Bachelorette

From his twitter account, we can see he tweets and retweets about this show a lot.

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

Chicago

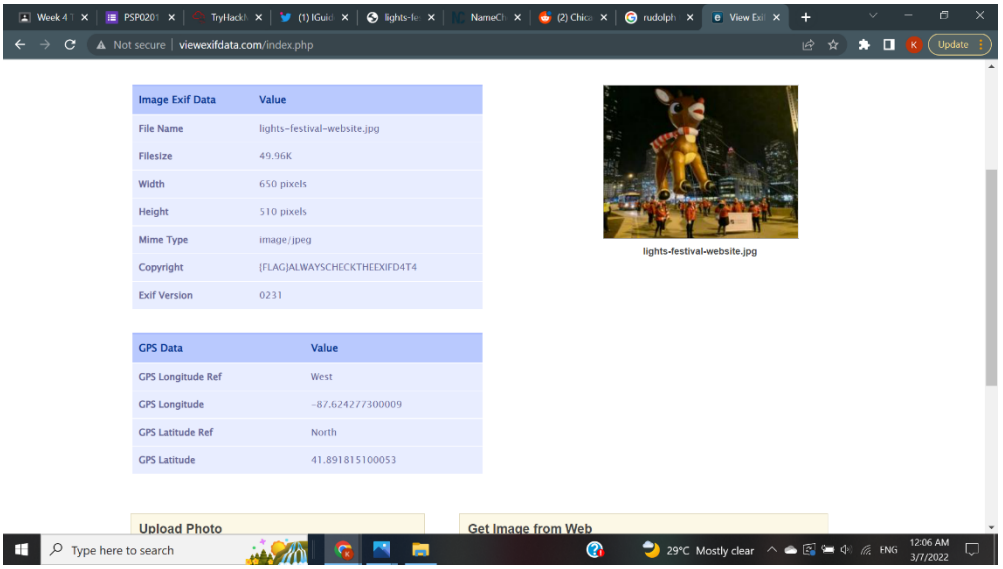
Using the image he uploaded during the parade, we can reverse image search on google. We found out that it was in Chicago.



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

41.891815, -87.624277

Usite sites like viewexifdata.com we can find the exif data of the image uploaded by Rudolph in higher resolution on twitter.



QUESTION 9: Did you find a flag too?

{FLAG}ALWAYSCHECKTHEEXIFD4T4

Image Exif Data	Value
File Name	lights-festival-website.jpg
Filesize	49.96K
Width	650 pixels
Height	510 pixels
Mime Type	image/jpeg
Copyright	{FLAG}ALWAYSCHECKTHEEXIFD4T4
Exif Version	0231

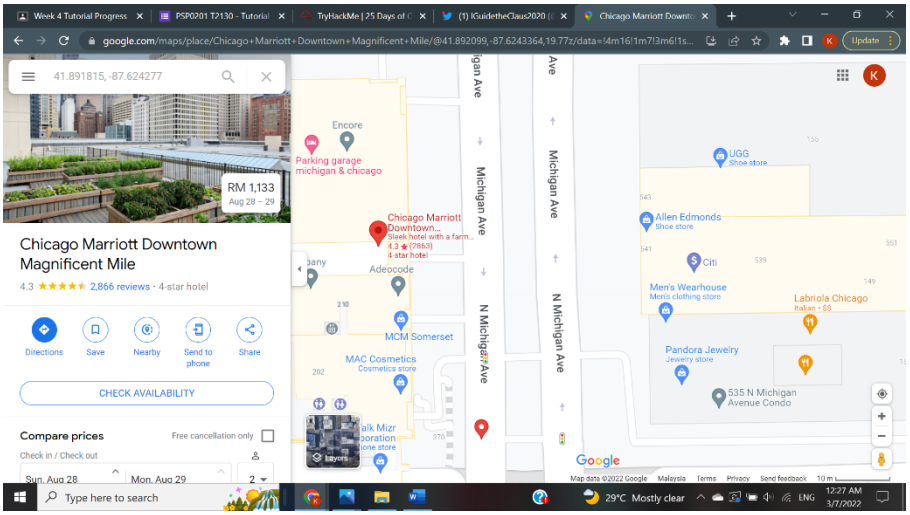
GPS Data	Value
GPS Longitude Ref	West
GPS Longitude	-87.624277300009
GPS Latitude Ref	North
GPS Latitude	41.891815100053

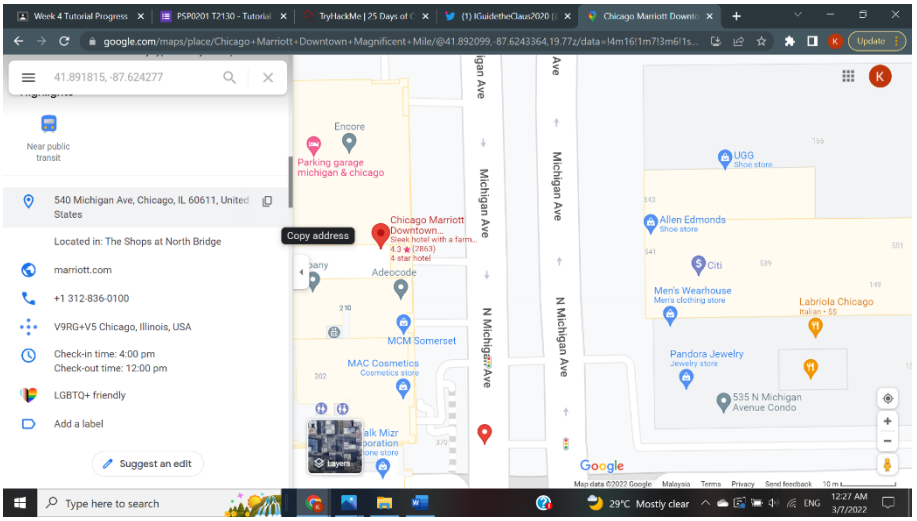
lights-festival-website.jpg

Q11: Based on all the information gathered. It's likely that Rudolph is in the Windy City and is staying in a hotel on Magnificent Mile. What are the street numbers of the hotel address?

540

From one of his tweets, he is staying at Marriott hotel. Copy paste the exact location of the parade on google and open google maps. And tap on the Marriott hotel nearby and we will get the street number.





Thought Process/Methodology:

We search the given username on sites like https://whatsmyname.app/ and we will find Rudolph's reddit. Once we get to the reddit account, go to comment and copy the link. We found out where he was born on one of his reddit comments. Using google to find out Robert's full name. We found out he has a twitter account from one of his comments on reddit and to confirm we search for him on twitter and get his username. From his twitter account, we can see he tweets and retweets about the show Bachelorette a lot. Using the image he uploaded during the parade, we can reverse image search on google. We found out that it was in Chicago. Usite sites like viewexifdata.com we can find the exif data of the image uploaded by Rudolph in higher resolution on twitter so we can know the exact location of the parade and get the flag. From one of his tweets, he is staying at Marriott hotel therefore copy paste the exact location of the parade on google and open google maps. And tap on the Marriott hotel nearby and we will get the street number.

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

Question 1

What's the output of True + True?

Answer: 2

Python states that True + True equals 2, which is illogical given that booleans can be added, concatenated, or combined in any way.

```
$ python
Python 3.9.0 (default, Oct  7 2020, 23:09:01)
[GCC 10.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> True + True
2
```

The True boolean would therefore appear to be truthy as well as one, and the False boolean would appear to be false as well as zero. So when there is a + operation between booleans, they opted to cast True as one. And therefore 1 + 1 Equals 2. This is foolish and perplexing.

In Ruby, true + true generates an error as intended:

```
$ irb
irb(main):001:0> true + true
Traceback (most recent call last):
        4: from /usr/bin/irb:23:in `<main>'
        3: from /usr/bin/irb:23:in `load'
        2: from /usr/lib/ruby/gems/2.7.0/gems/irb-1.2.7/exe/irb:11:in `<top (required)>'
        1: from (irb):1
NoMethodError (undefined method `+' for true:TrueClass)
```

because booleans, which make more sense and are anticipated, do not provide the + operator.

Question 2

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

Answer: pypi

It is known as pypi in Python and rubygems in Ruby.

Question 3

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

Answer: true

A string converted to a boolean in Python is always regarded truthy, hence the result will always be true. Additionally, an empty string is regarded as false and returns false.

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

PHP has the same bizarre behaviour.

As opposed to this less evident behaviour, ruby allows you to verify whether an object is empty and returns a boolean, which makes more sense:

```
irb(main):001:0> "noraj".empty?
=> false
irb(main):002:0> "".empty?
=> true
irb(main):003:0> [0].empty?
=> false
irb(main):004:0> [].empty?
```

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?

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

Answer: [1, 2, 3, 6]

In python:

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

This code also functions in Ruby:

```
irb(main):001:0> x = [1, 2, 3]
=> [1, 2, 3]
irb(main):002:0> y = x
=> [1, 2, 3]
irb(main):003:0> y.append(6)
=> [1, 2, 3, 6]
irb(main):004:0> print(x)
[1, 2, 3, 6]=> nil
irb(main):005:0> x
=> [1, 2, 3, 6]
```

Question 6

What causes the previous task to output that?

Answer: pass by reference

Thought Process/Methodology:

This problem involves Python boolean logic. In general, thinking through straightforward issues like this may be a useful approach to grasp how a programming language operates. However, if this is our first time using Python, it is best to run a line of code to see the results.

Python may be run in two different ways: using scripts (as described in the dossier) or the REPL (Read Evaluate Print-Loop). Despite its confusing name, REPL essentially implies that each line is executed when users press enter and that all variables, data structures, and functions are stored in memory until the shell is closed. Using the REPL instead of writing a script, in our experience, is faster for straightforward problems like this as all the work can be done at once.