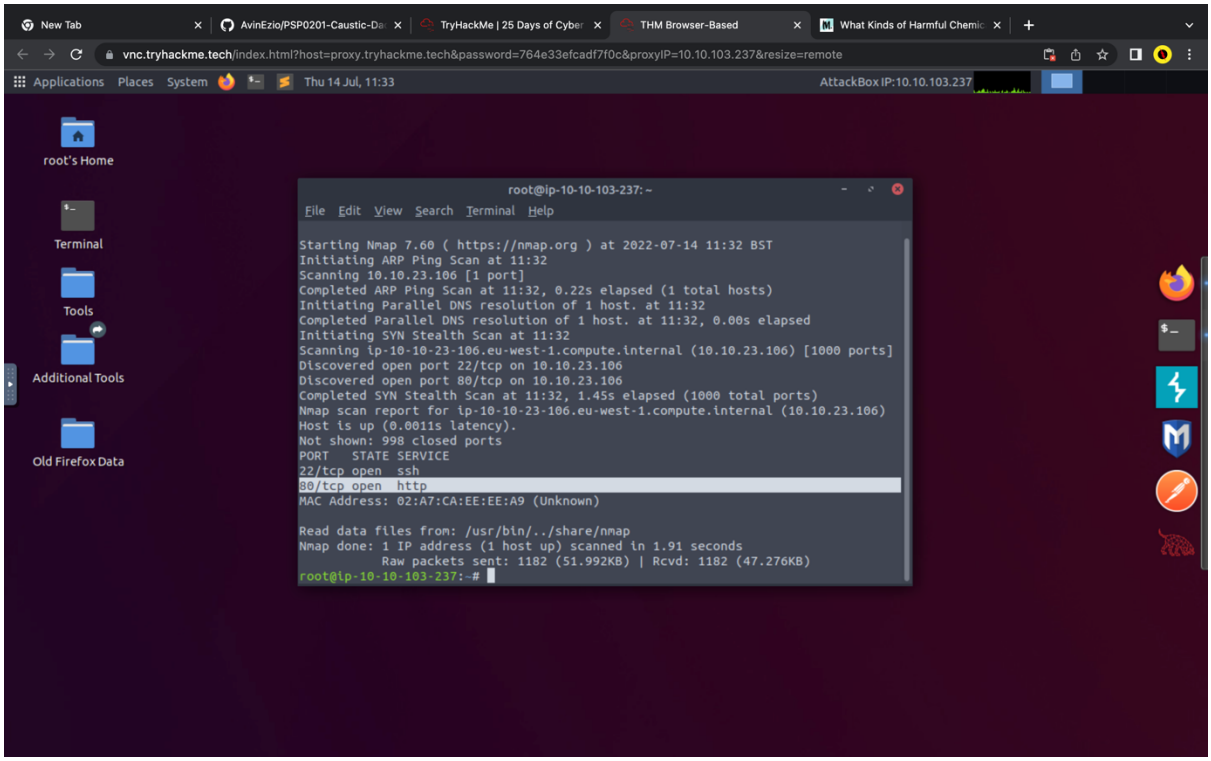
PSP0201
WEEK 5
Write Up

Group members	ID
1)Nevendra Eravanan	1211101778
2) Avinnaesh A/L G Baramesvaran	1211101658
3) Arvind A/L Krishna Kumar	1211101977

Day 16 – {Scripting} Help! Where is Santa?
Tools used: Kali linux, Firefox, Terminal

Question 1: What is the port number for the web server?

- Open terminal and run a nmap scan with verbose on the machine ip.
- nmap -v 10.10.23.106
- the open ports will be listed below.

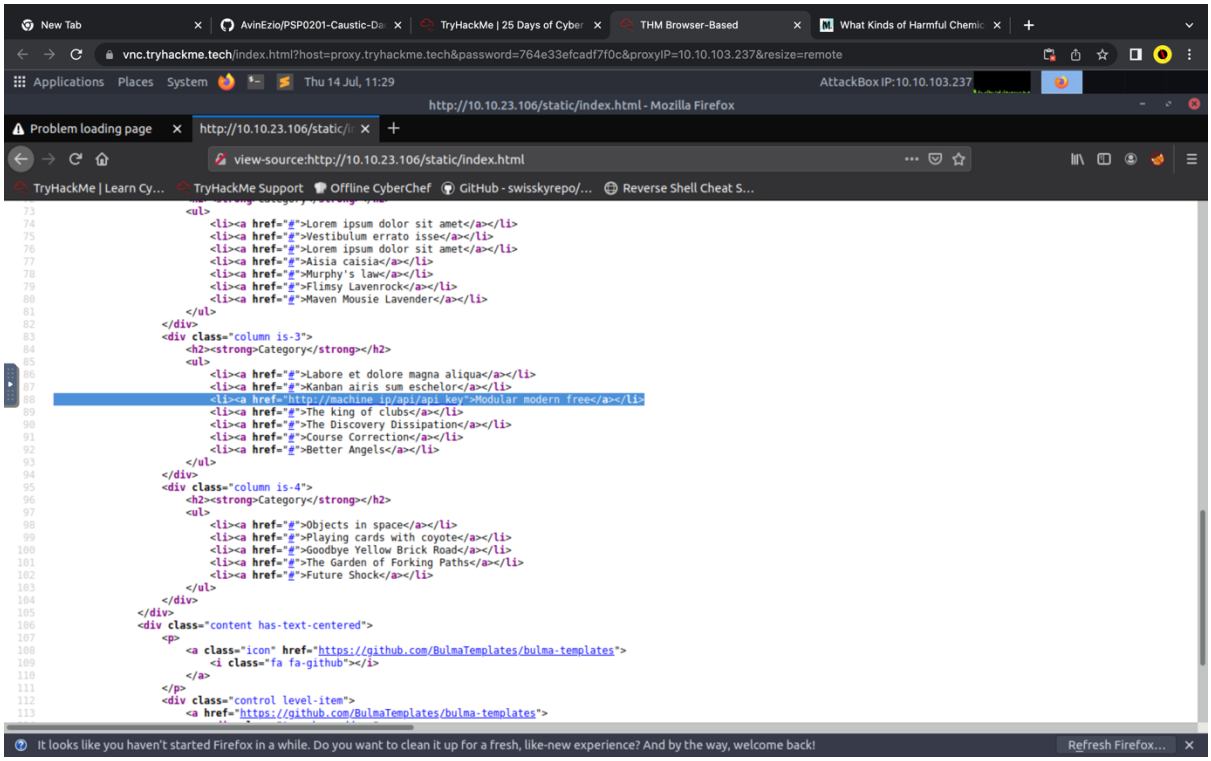


Question 2: What templates are being used?

- The templates being used can be seen on the top left corner of the website.

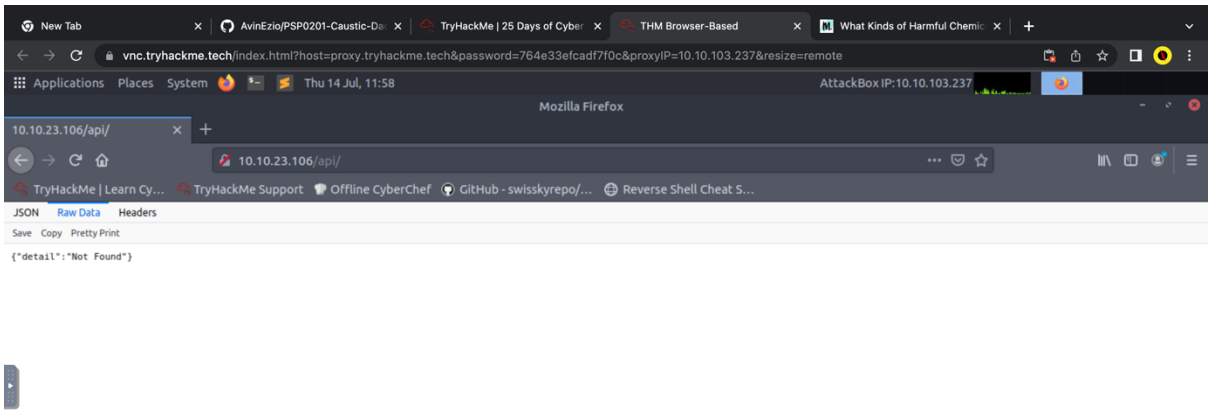
Question 3: Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)

- Open Firefox browser and search for the URL machine_ip/static/index.html
- Right click and view the page source.
- Scroll down to find the api directory.



Question 4: Go the API endpoint. What is the Raw Data returned if no parameters are entered?

- Open a new tab on Firefox and search for machine_ip/api/
- Navigate to the Raw Data tab.

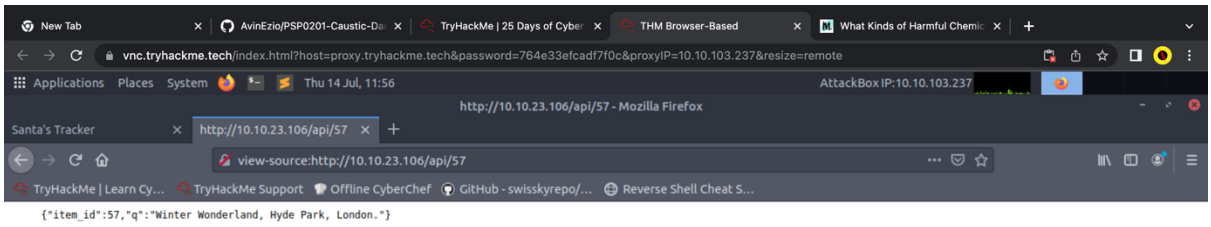


Question 5: Where is Santa right now? (Tick all correct answers.)

&

Question 6: Find out the correct API key. Remember, this is an odd number between 0-100. After too many attempts, Santa's Sled will block you. To unblock yourself, simply terminate and re-deploy the target instance (10.10.94.92)

- Open a new tab on the browser.
- Search for the URL machine_ip/api/api_key
- The correct api_key is obtained by trial and error by entering different odd numbers between 1 and 100.
- Once give access the location of Santa will be displayed.
- The api_key number is 57



Thought process / Methodology

We first ran a nmap scan with verbose to display all the open ports. Then, we opened Firefox and viewed the source page to obtain the api key and the api directory. To get access to Santa's location, we randomly entered odd numbers from 1 to 100 to find the correct api key value.

Day 17: Reverse Engineering- ReverseELFneering

Tools Used: Try Hack me Attack Box

Solution/Walkthrough:

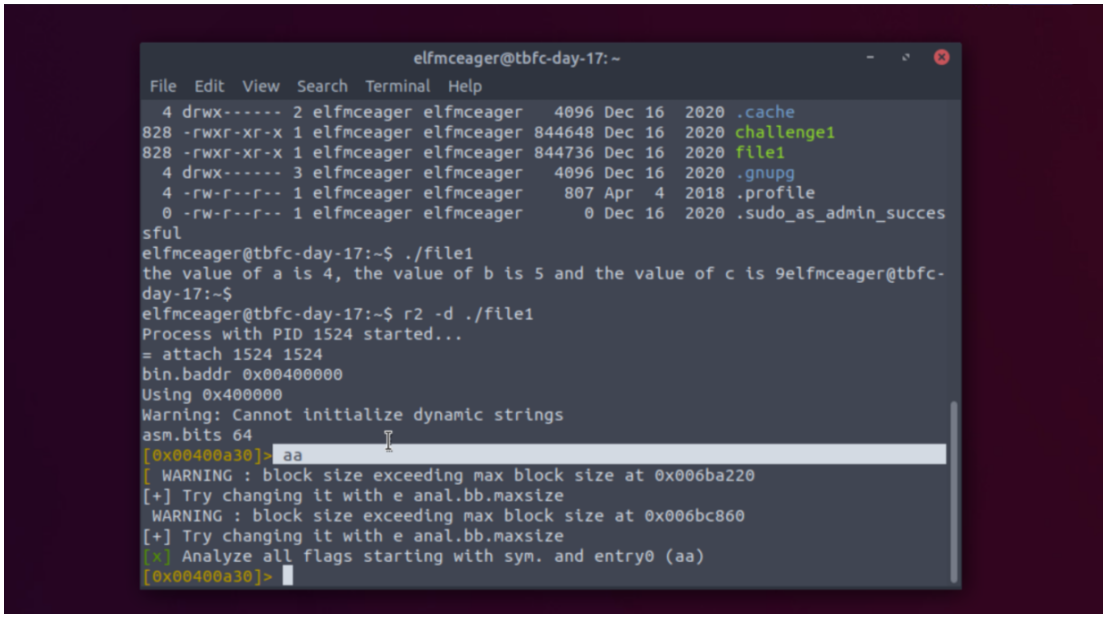
Question 1

Matching the data types along with the size in bytes.

Initial Data Type	Suffix	Size (bytes)
Byte	b	1
Word	w	2
Double Word	l	4
Quad	q	8
Single Precision	s	4
Double Precision	l	8

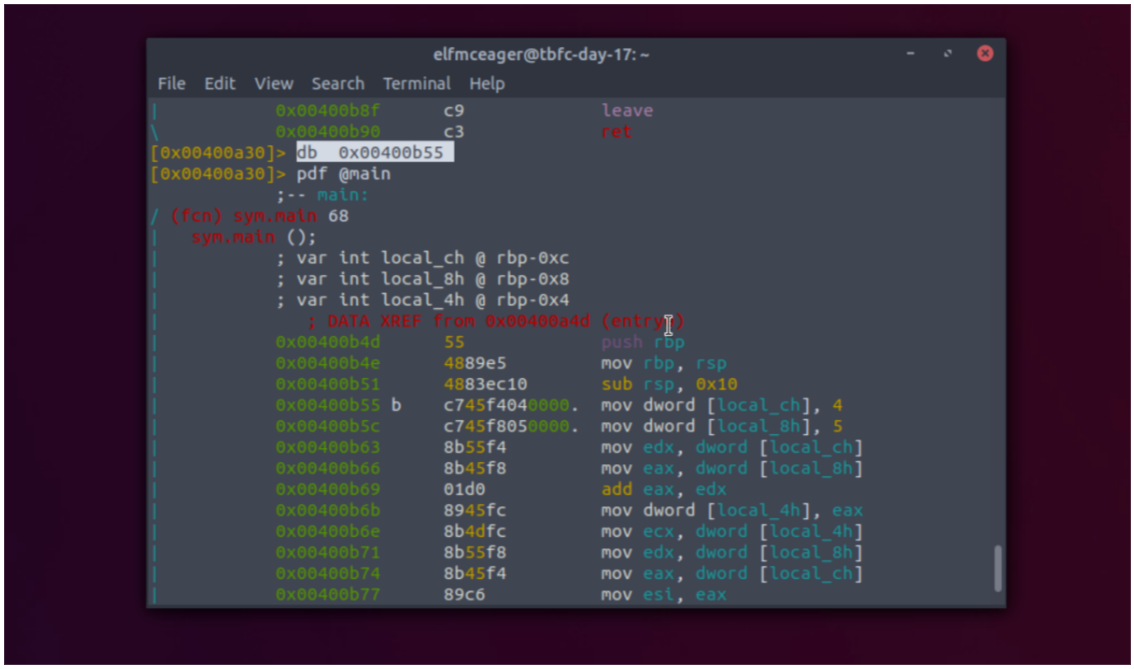
Question 2

Entering the required command to analyse the program in radare2, which is **"aa"**.



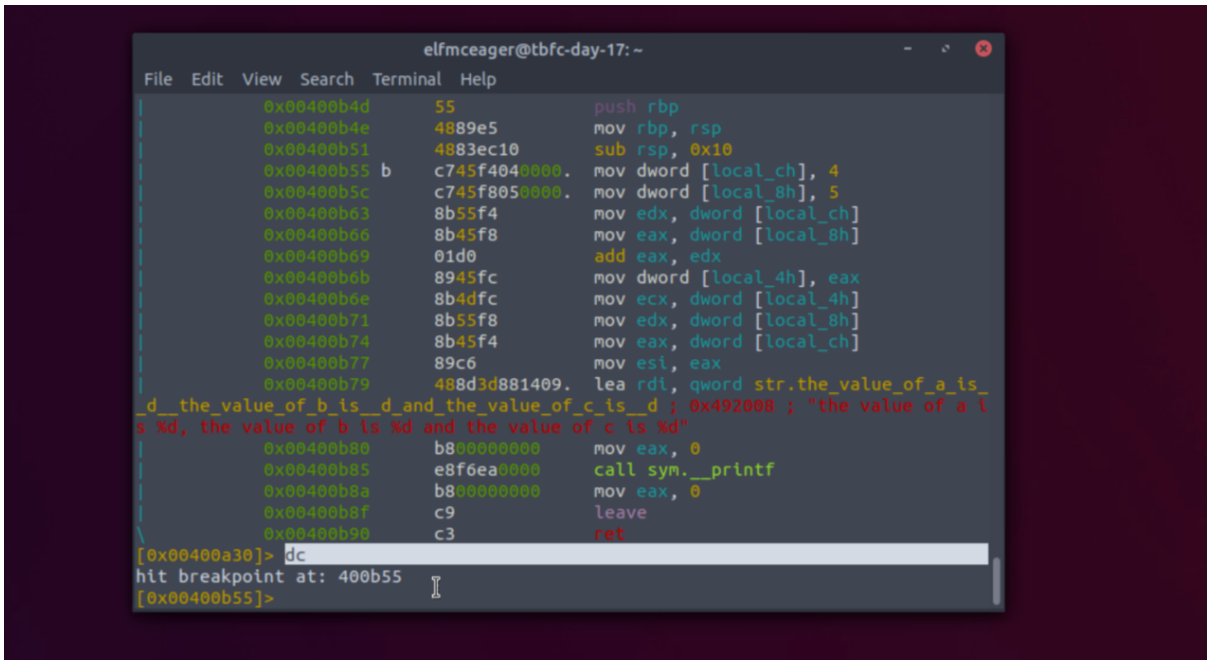
Question 3

Putting in the command **"db"** to set a breakpoint in radare2.



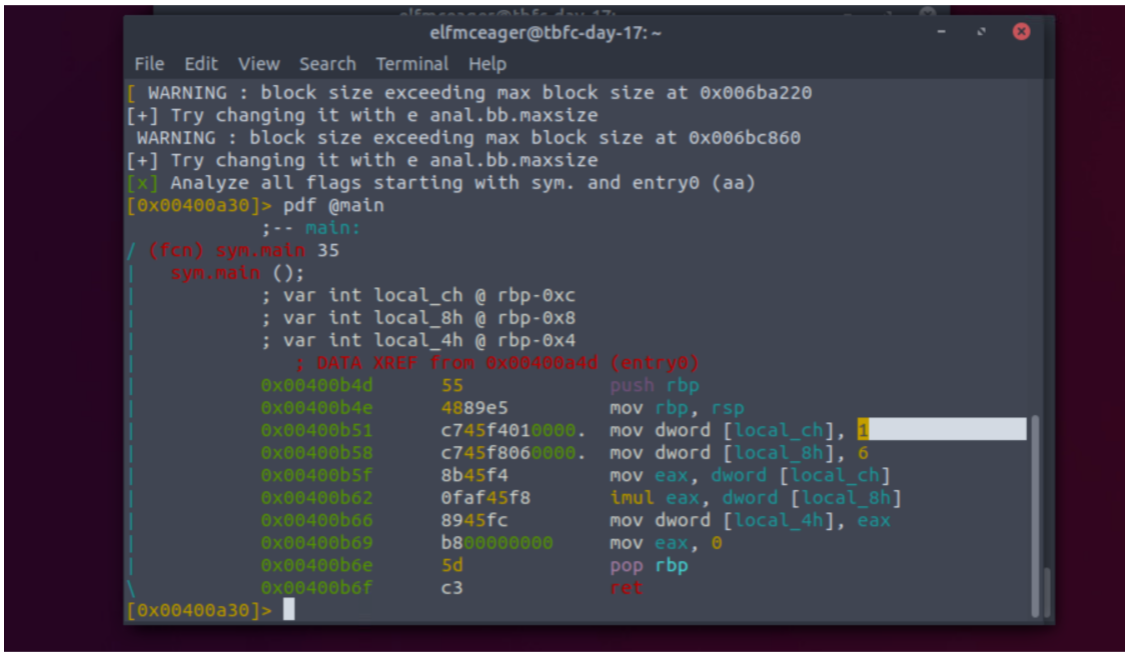
Question 4

Using the command **“dc”** to execute the program until we hit a breakpoint



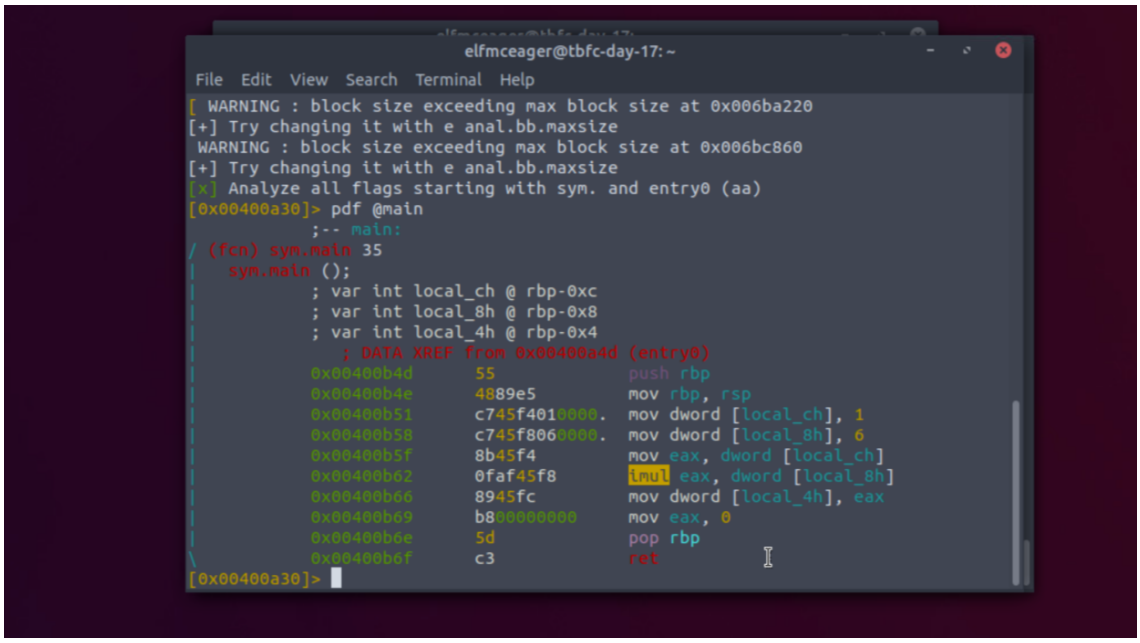
Question 5

Entering the command **“pdf @main”** to Identify the value of local_ch when its corresponding movl instruction is called (first if multiple), which turns out to be **“1”**



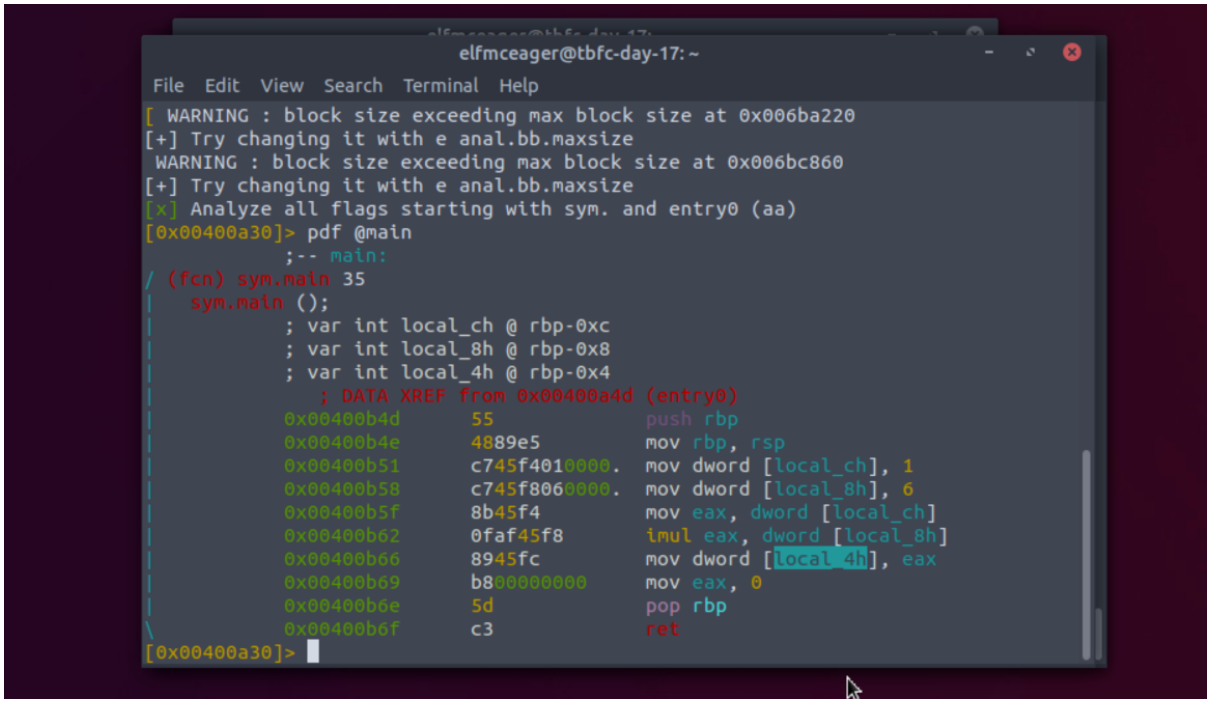
Question 6

By doing some calculation we were able to get to know the value of eax when the imull instruction is called, which is **“6”**



Question 7

Identifying the value of local_4h before eax is set to 0 by calculating. Thus the value is **"6"**



Thought Process/Methodology:

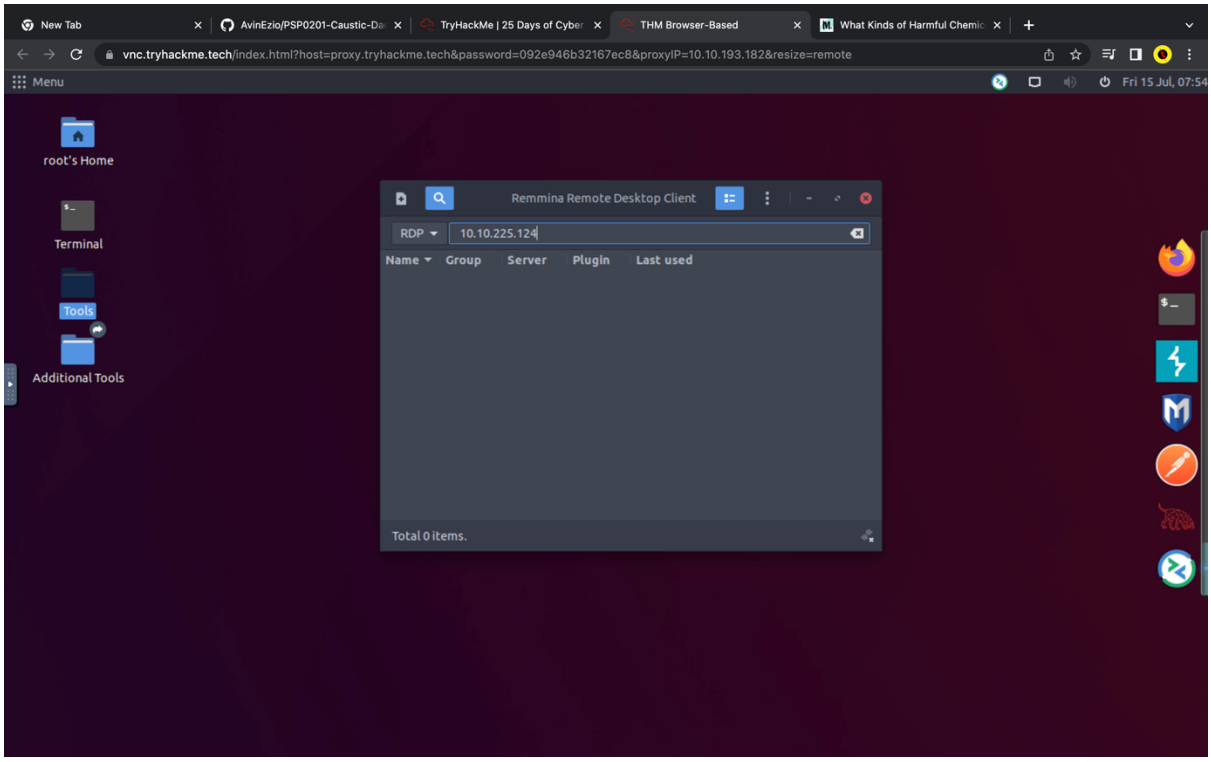
We started by reading through the instructions that have been provided by Try Hack Me, where we got to know that a table have been provided answering the very first question, after done reading the table we then answered the question. Moving on, we identified and entered the command to analyse the program in radare2 which is **"aa"** for the second question. Then, we moved on by putting in the command **"db"** to set a breakpoint in radare2. We typed in the command **"dc"** in order to execute the program until it hits a breakpoint. Then we moved on by entering the command **"pdf @main"** to get the value of local_ch when its corresponding movl instruction is called (first if multiple), which turns out to be **"1"**. Then we calculated what is the value of eax when the imull instruction is called, which turns out to be **"6"**. Finally, we calculated the value of local_4h before eax is set to 0, which then gives us a value of**"6"**.

Day 18 – {Reverse Engineering} The Bits of Christmas

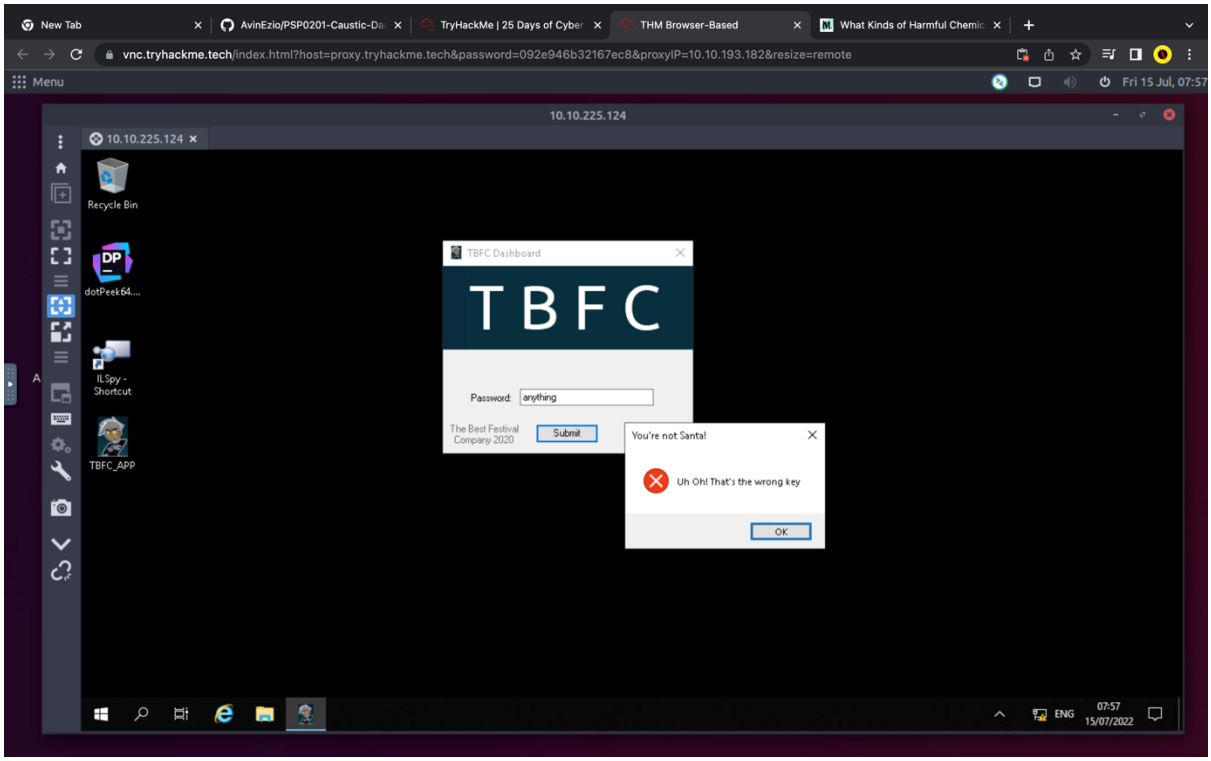
Tools used: Kali linux, Windows, Firefox, CyberChef

Question 1: What is the message that shows up if you enter the wrong password for TBFC_APP?

- Navigate to the apps tab and open Remmina.
- Enter the machine ip and enter.



- Enter the username and password which is given in the task description.
- Once logged in, open the TBFC app.
- Enter anything as the password to display the message.

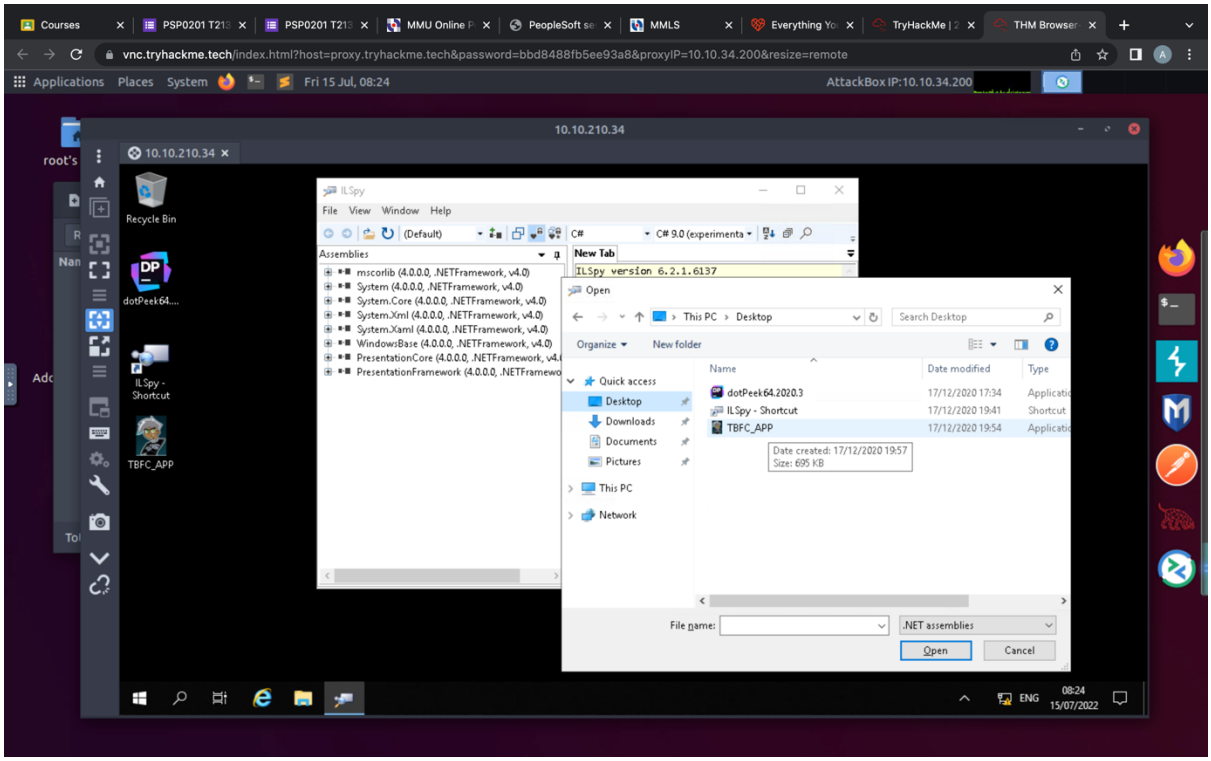


Question 2: What does TBFC stand for?

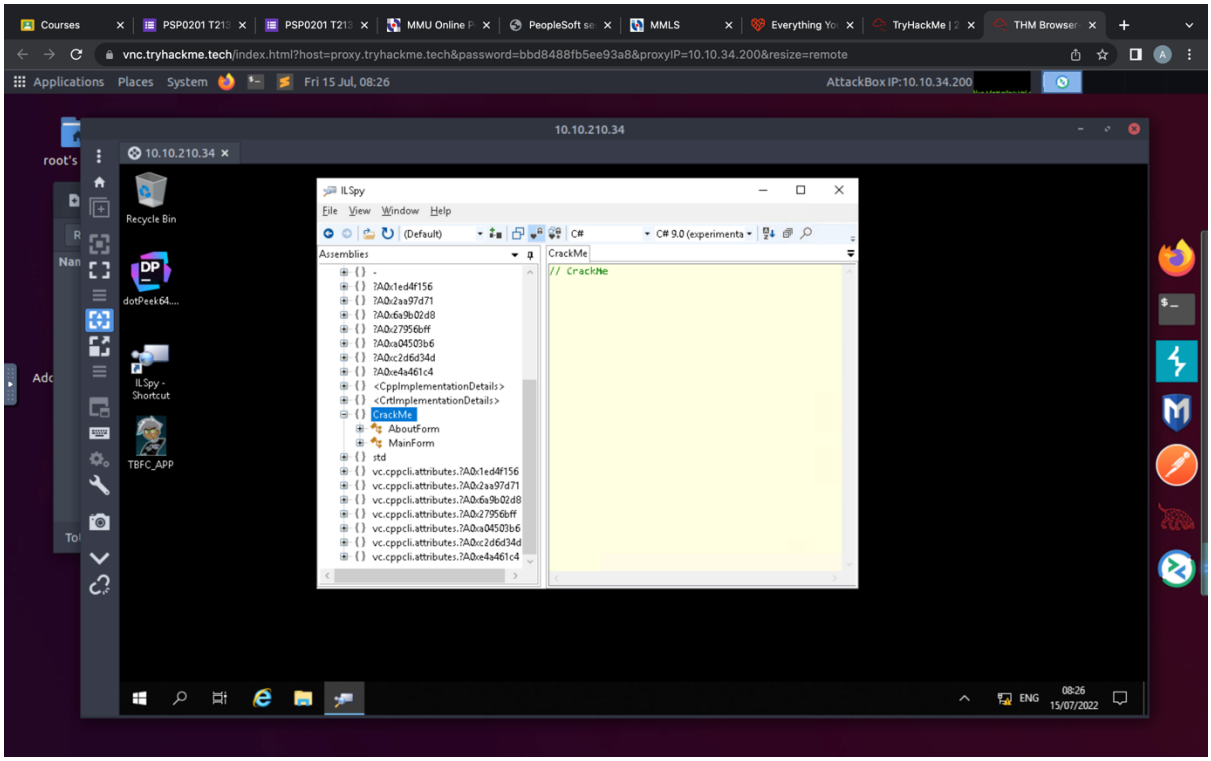
- The full name of the app can be found at the bottom left of the app window.

Question 3: Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?

- Open the ILSpy using the shortcut in the desktop page.
- Navigate to the file tab at the top, and open the TBFC app



- Find for the Crack Me module.

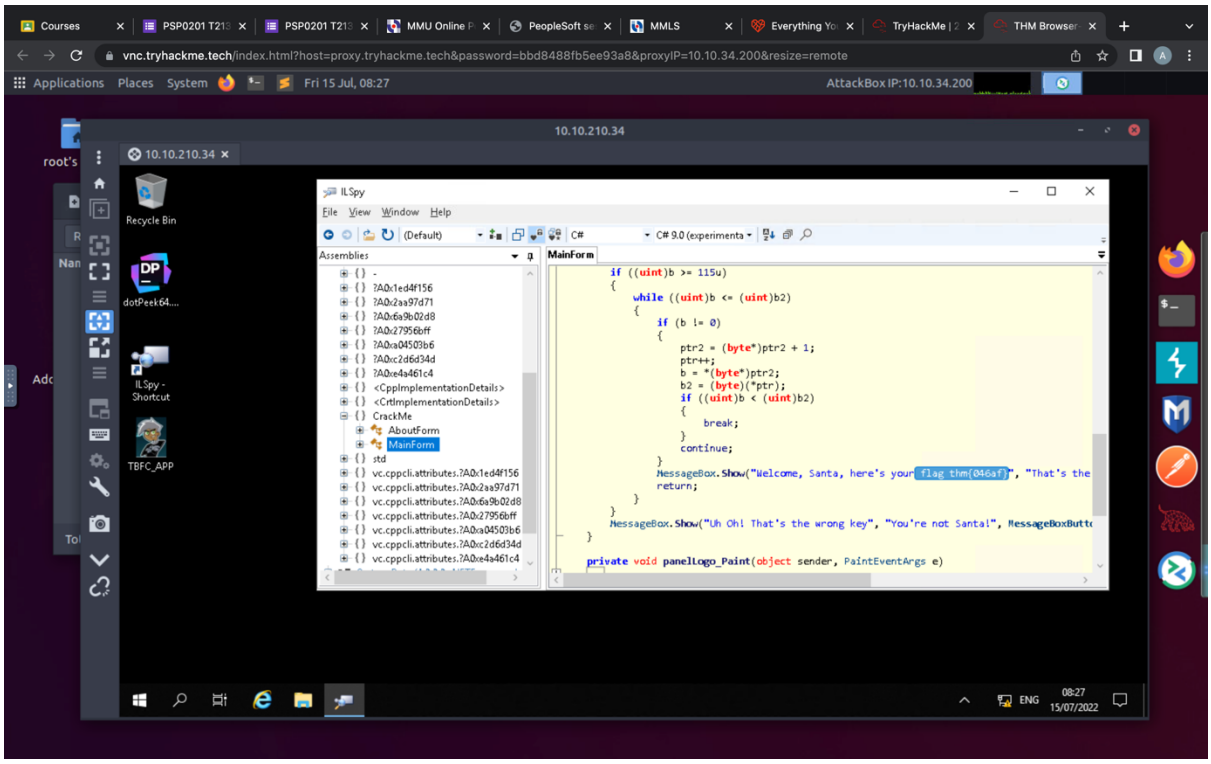


Question 4: Within the module, there are two forms. Which contains the information we are looking for?

- To find the Santa's password and the flag, we have to search in the MainForm.

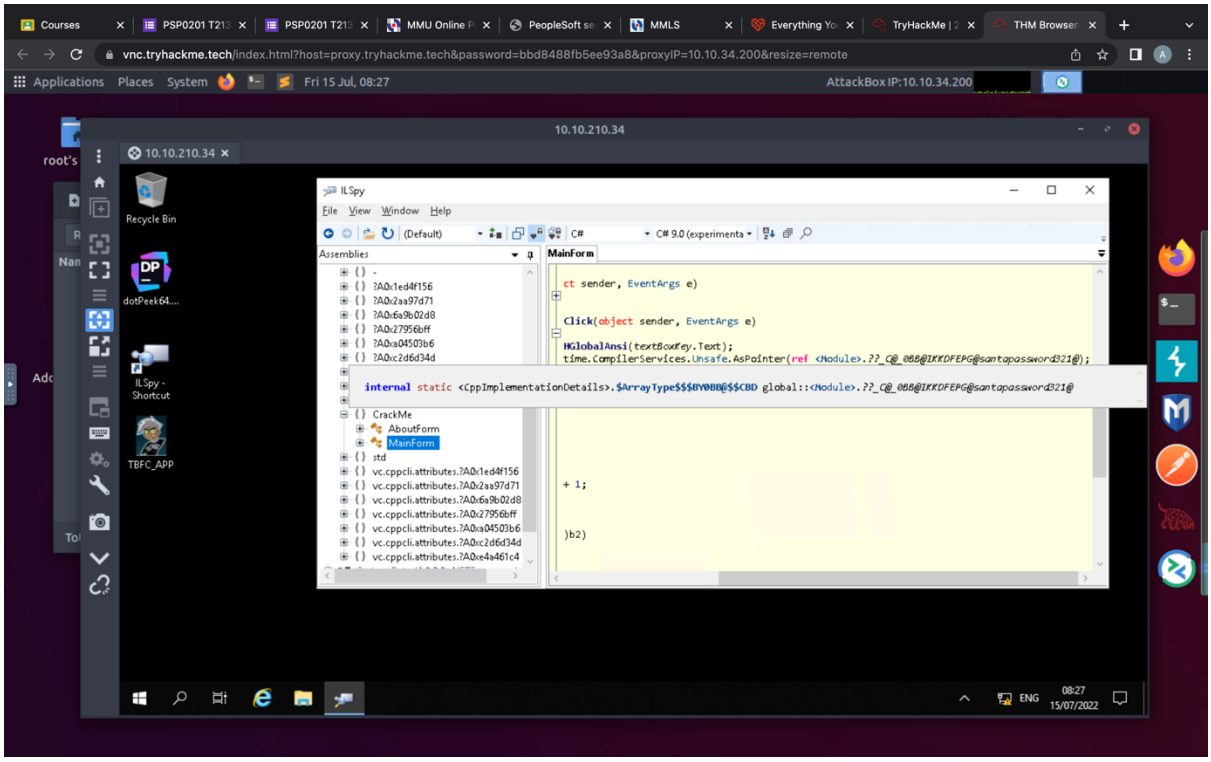
Question 5: Which method within the form from Q4 will contain the information we are seeking?

- Scroll through the MainForm and search for the activate button to find Santa's password and the flag.

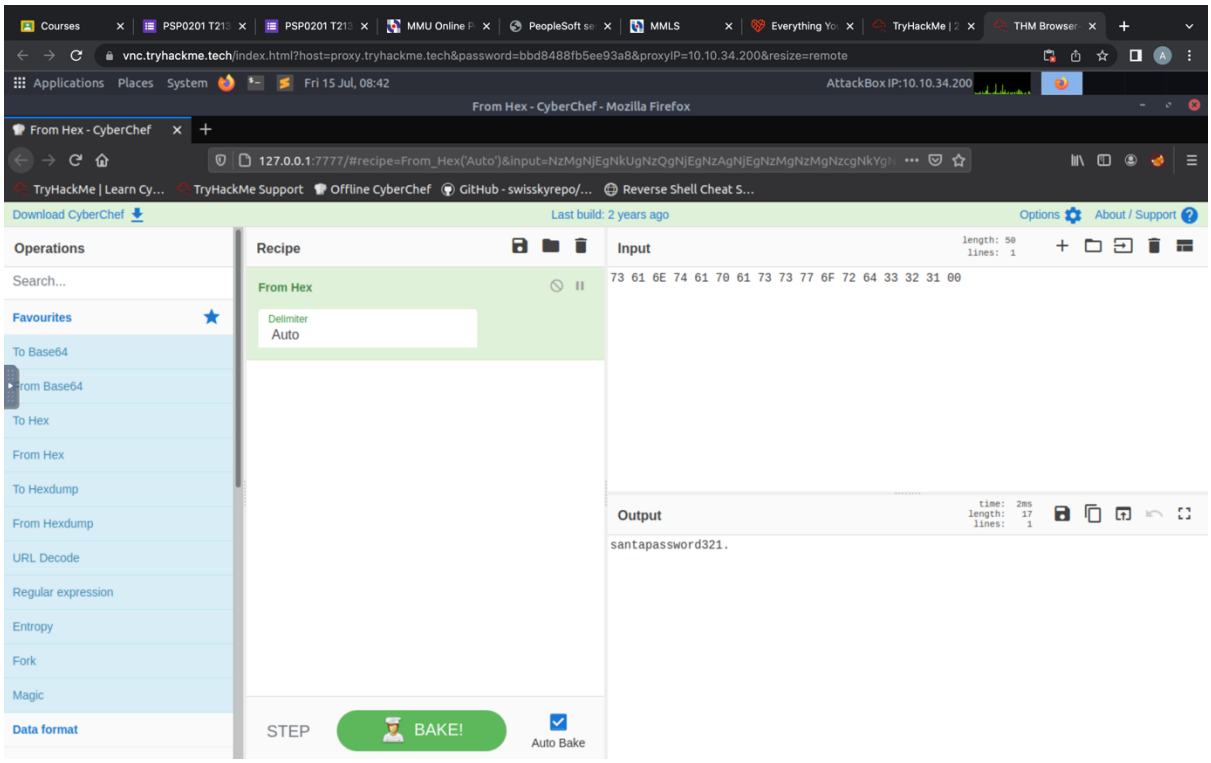


Question 6: What is Santa's password?

- In the MainForm, find for the password module and double click on it.

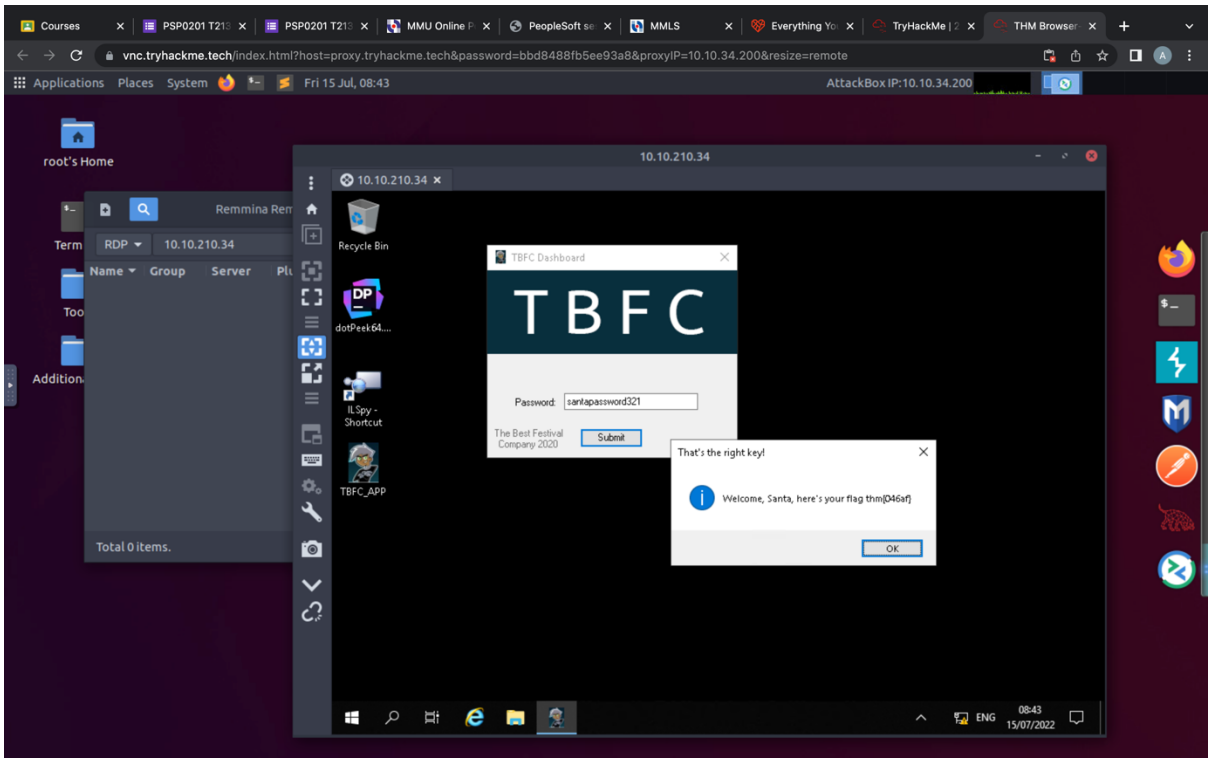


- Once redirected to Derived Types, copy the hexadecimal value displayed.
- Open Firefox and search for CyberChef.
- Paste the hex value in the input section and set the Recipe as From Hex.



Question 7: Now that you've retrieved this password, try to login...What is the flag?

- Copy the output value from CyberChef.
- Open the TBFC app and paste the password.
- The flag will be displayed once you have successfully logged in.



Thought process / Methodology

We first opened the Remmina app and type out the machine ip. Then we entered the username and password that was given in the task description. Once we launched the Windows. Then, we opened the TBFC app and entered anything as the password. After that we opened the ILSpy shortcut on the desktop page. We opened the TBFC app in the ILSpy and searched the CrackMe module for Santa's password and the flag. Once we found the hex value of Santa's password we opened CyberChef on Firefox to convert it into a string. We then opened the TBFC app again to use the correct password, we were greeted with a message and also the flag.

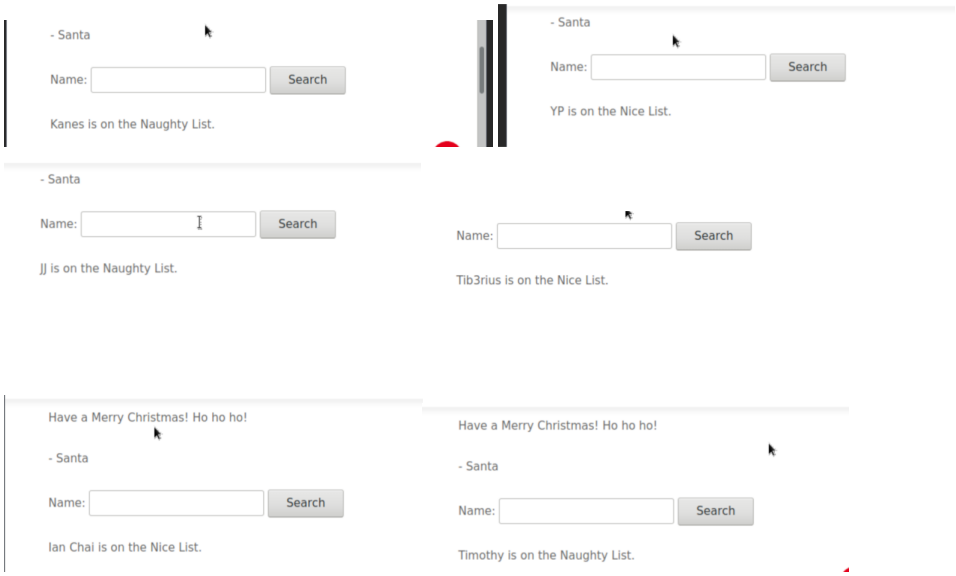
Day 19: Web Exploitation- The Naughty Or Nice List

Tools Used: Try Hack Me Attack Box, Firefox

Solutions/ Walkthrough:

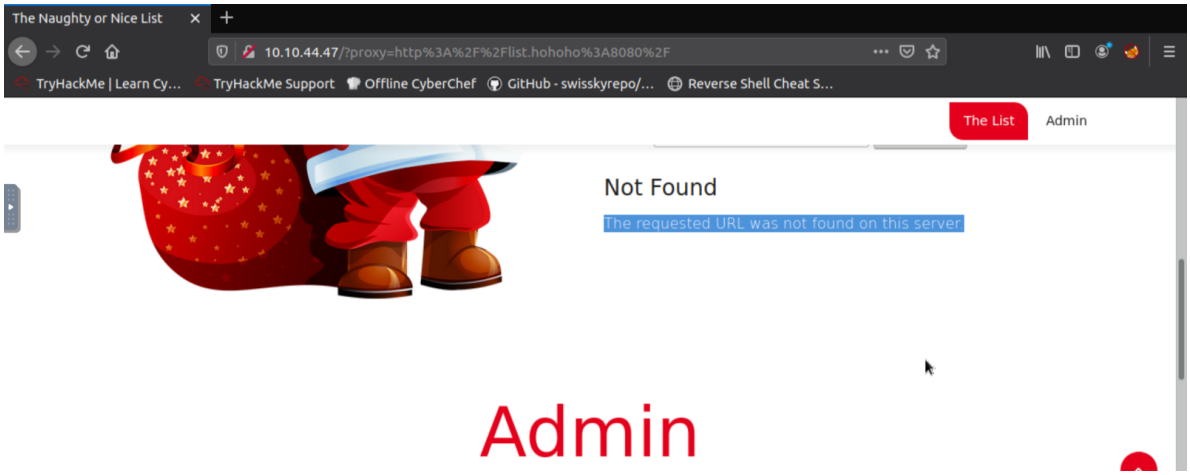
Question 1

Searching on the names given to state on which list their names are on.



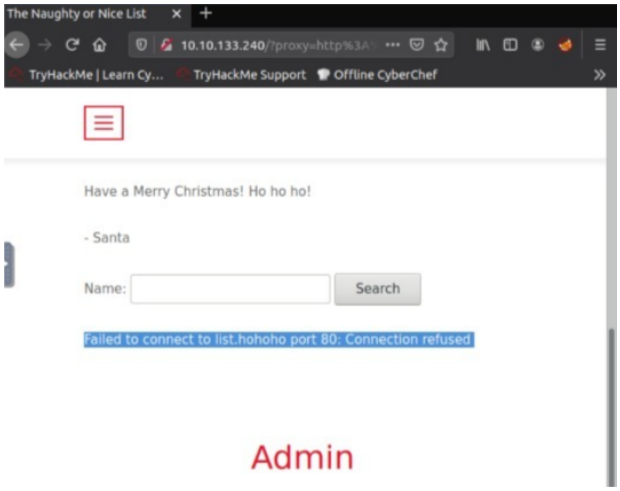
Question 2

Replacing the actual URL with the given URL to see what is displayed on the page.



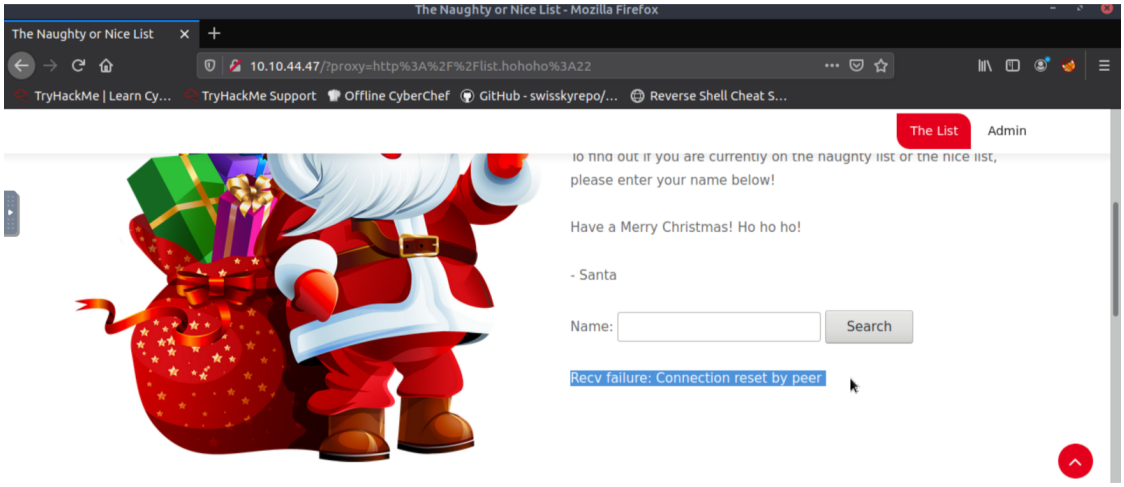
Question 3

Obtaining the message displayed on the page when we replaced the URLD with the given.



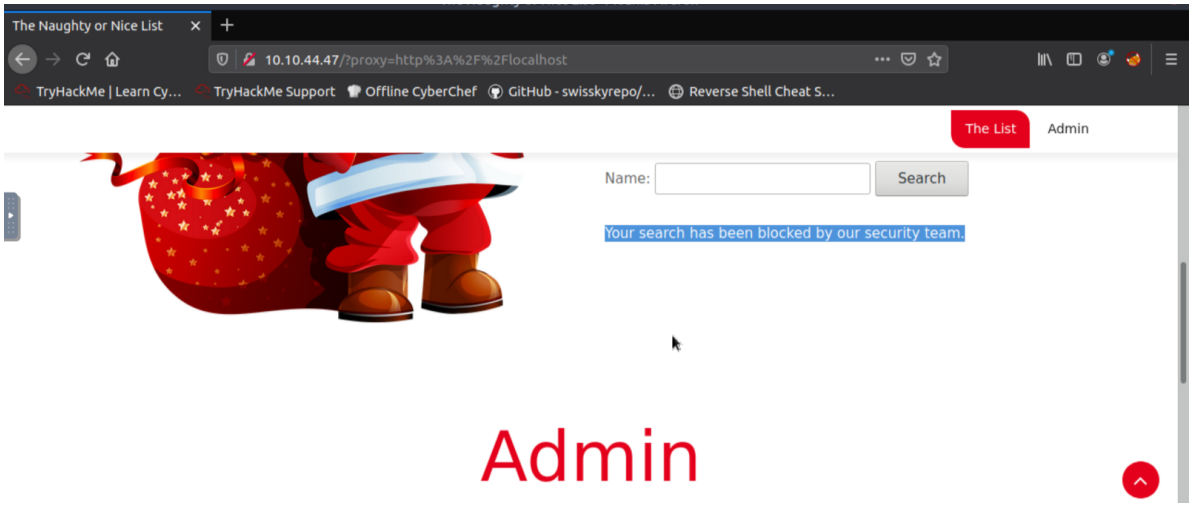
Question 4

Obtaining What is displayed on the page when the URL is replaced with the given.



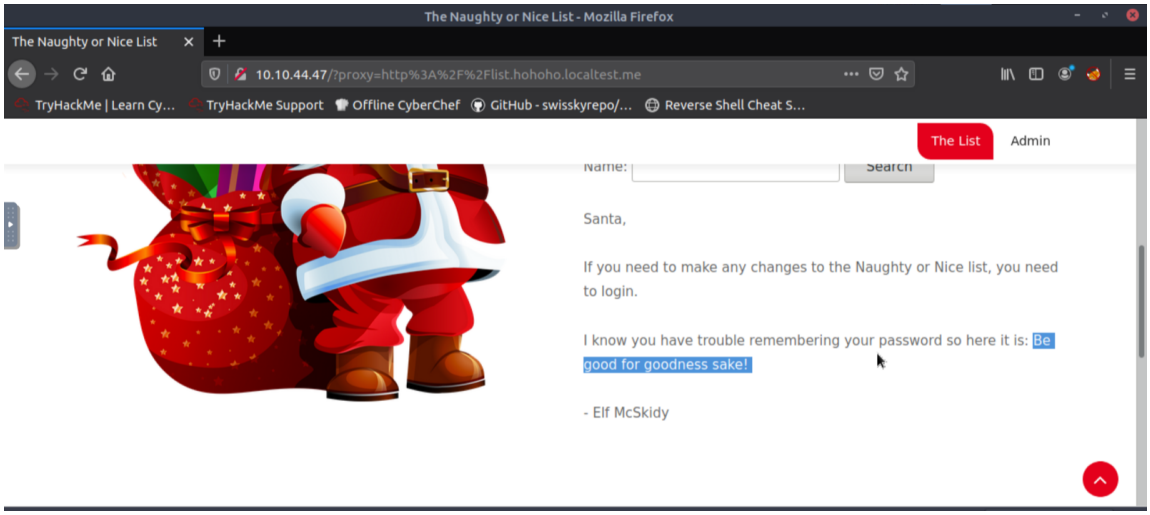
Question 5

Pasting the given URL to obtain what is displayed on the page.



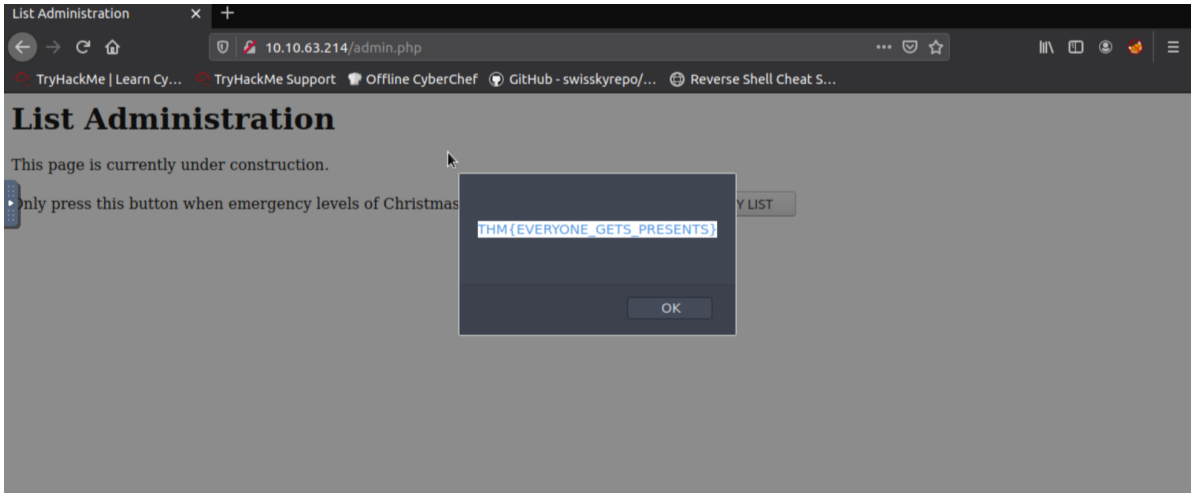
Question 6

Obtaining Santa's password by modifying the URL, by adding **".localtest.me"**



Question 7

Obtaining the challenge flag by signing into the admin account and deleting the naughty list.



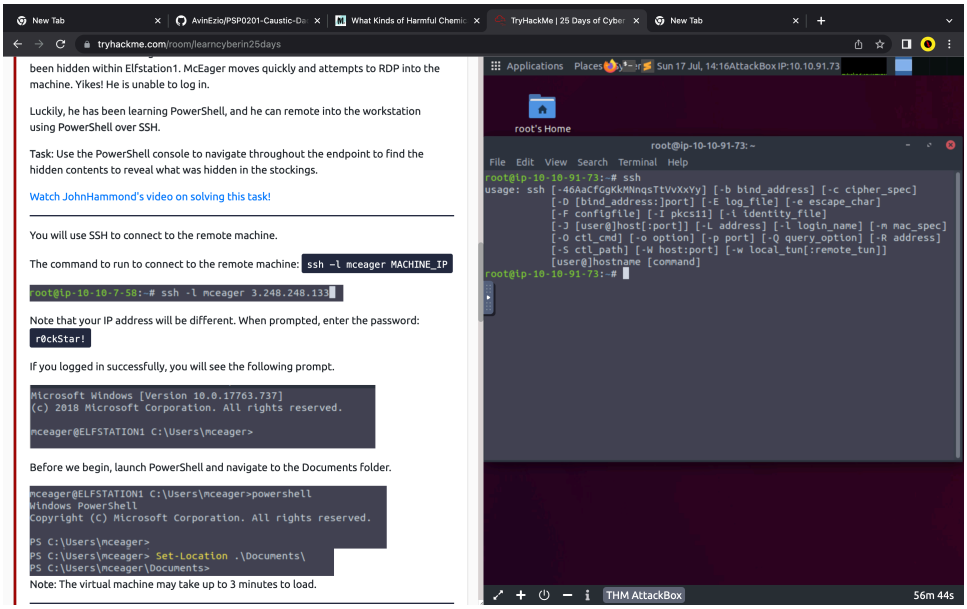
Thought Process/Methodology:

Starting off, we open Firefox and typed in the given IP address, we then proceeded to search on the given names on the naughty or nice list to check if their names were on the naughty or nice list. Moving on, we then replaced 4 different URL one at a time, with the existing one to acquire what is displayed on the page. Once we are done, we then moved on by modifying the URL by adding **".localtest.me"** to it, to obtain Santa's password. Finally, we log into the Amin's account and deleted the naughty list to get the challenge flag.

Day 20 [Blue Teaming] PowershELlF to the rescue

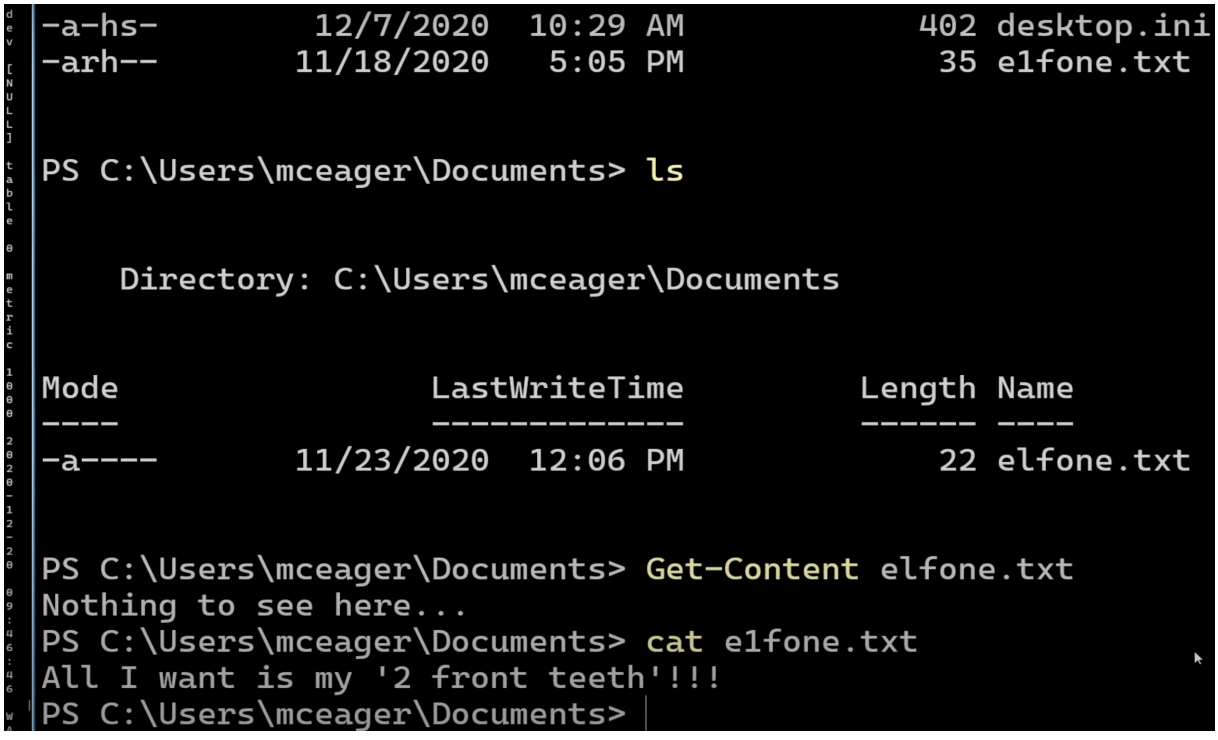
Question 1 : Check the ssh manual. What does the parameter -l do?

In the terminal, type out ssh to display all the functions of each parameter.



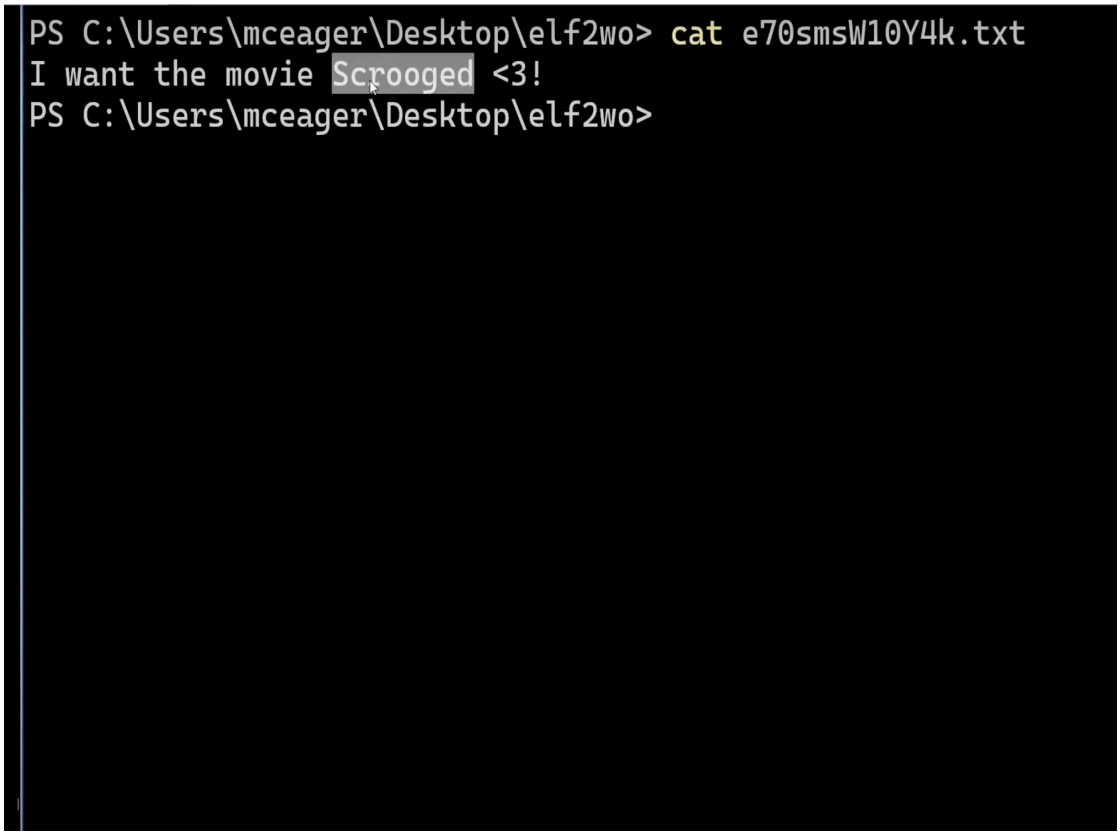
Queation 2 : Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

After finding out the e1fone.txt file as the hidden file go ahead and cat the elfone.txt file and it will reveal the answer as shown below.



Question 3 : Search on the desktop for a hidden folder that contains the file for Elf 2. Read the contents of this file. What is the name of that movie that Elf 2 wants?

After finding the hidden elf2 file go ahead and find the e70smsW10y4k.txt. Find the contents of this file and cat the e70smsW10y4k.txt and it will show the answer.



Question 4 : Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder? (This command will take a while)

```
PS C:\Windows\System32> Get-ChildItem -Hidden -Directory -Filt


    Directory: C:\Windows\System32


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--        11/23/2020   3:26 PM                3lfthr3e


PS C:\Windows\System32>
```

Use hidden directory to find the elf 3 file.

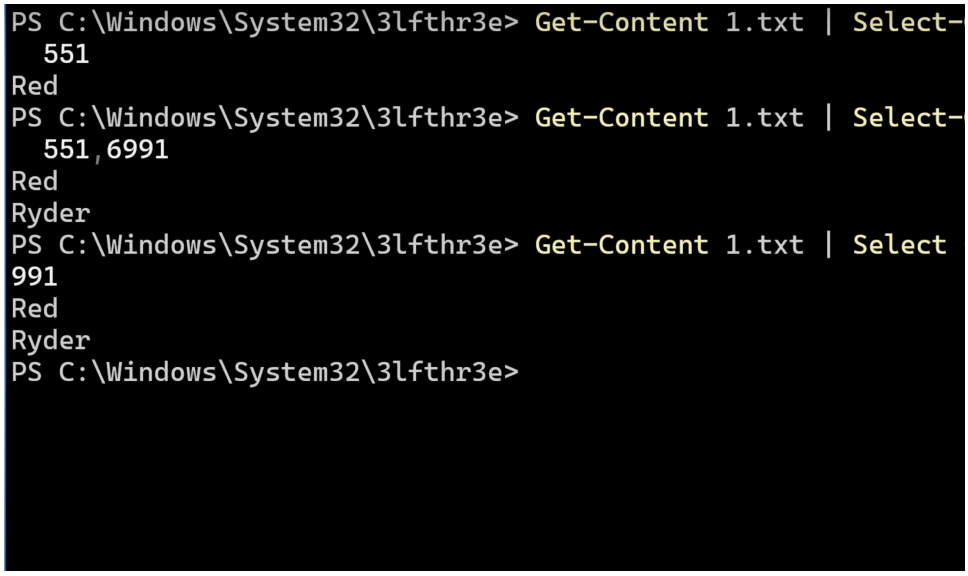
Question 5 : How many words does the first file contain?

After finding the 1.txt file go ahead and get content and it should load up a bunch of words on your screen and after this you can measure object and it should come up to 9999 words.

```
Count    : 9999
Average  :
Sum      :
Maximum  :
Minimum  :
Property :


PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Measure-Ob


Lines Words Characters Property
----- ----- ---------- --------
       9999


PS C:\Windows\System32\3lfthr3e>
```

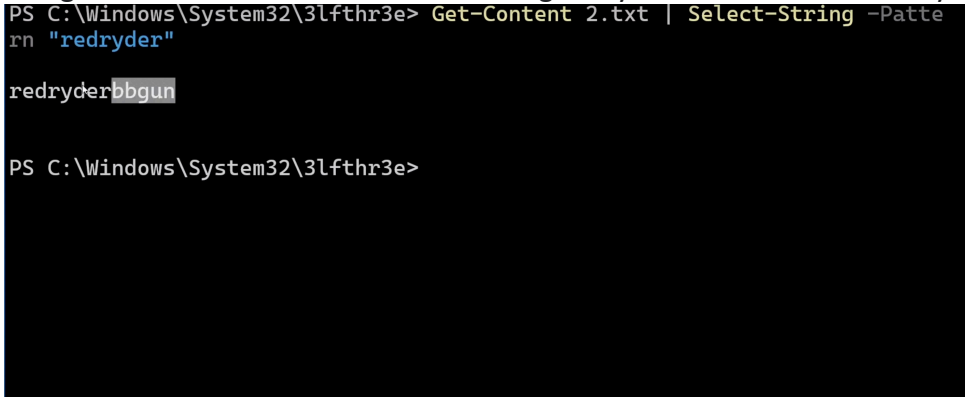
Question 6 : What 2 words are at index 551 and 6991 in the first file?

Use get content 1.txt and get 551 which will show red and then find the word 6991 and it will show ryder thus making the answer red ryder.



Question 7 : This is only half the answer. Search in the 2nd file for the phrase from the previous question to get the full answer. What does Elf 3 want? (use spaces when submitting the answer)?

Use get content 2.txt and and select string redryder and it should show you the answer



Thought Process and Methodlogy

To finish day 20 I first started with typing out ssh to display all the functions of each parameter. I then, found out the e1fone.txt file as the hidden file go ahead and cat the elfone.txt file and it will reveal the answer as shown. I continued by, finding the hidden elf2 file go ahead and find the e70smsW10y4k.txt. Find the contents of this file and cat the e70smsW10y4k.txt and it will show the answer. After that I used hidden directory to find the elf 3 file. After finding the 1.txt file go ahead and get content and it should load up a bunch of words on your screen and after this you can measure object and it should come up to 9999 words. Use get content 1.txt and get 551 which will show red and then find the word 6991 and it will show ryder thus making the answer red ryder. And finally, Use get content 2.txt and and select string redryder and it should show you the answer