PSP0201

WEEK 5

WRITE-UP

GROUP NAME : PELITA

ID	Name	Role
1211102057	Muhammad Syahir Nazreen Bin Abdul Hamid	Leader
1211101935	Mohamed Imran Bin Mohamed Yunus	Member
1211103220	Muhammad Firzan Ruzain Bin Firdus	Member
1211102060	Farris Aiman Bin Mohd Harris	Member

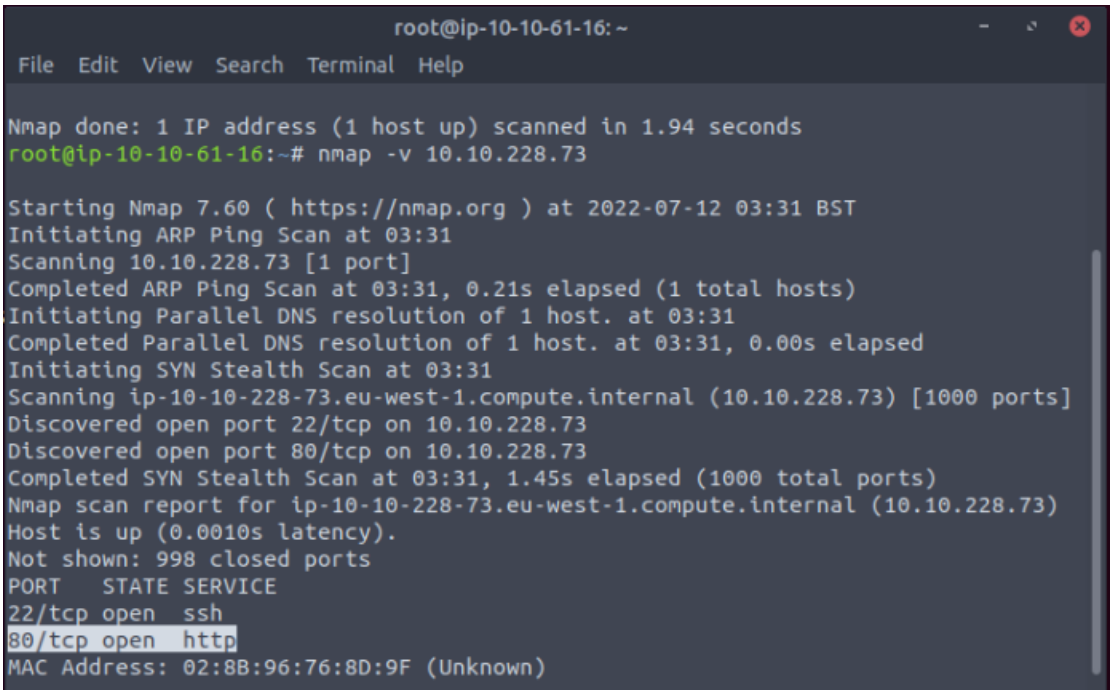
DAY 16: Help! Where is Santa?

Tools used: Kali, Nmap

Solution/walkthrough:

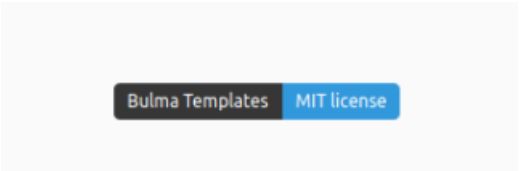
Question 1

Connected to Nmap in order to find the website port. The port number is **80.**



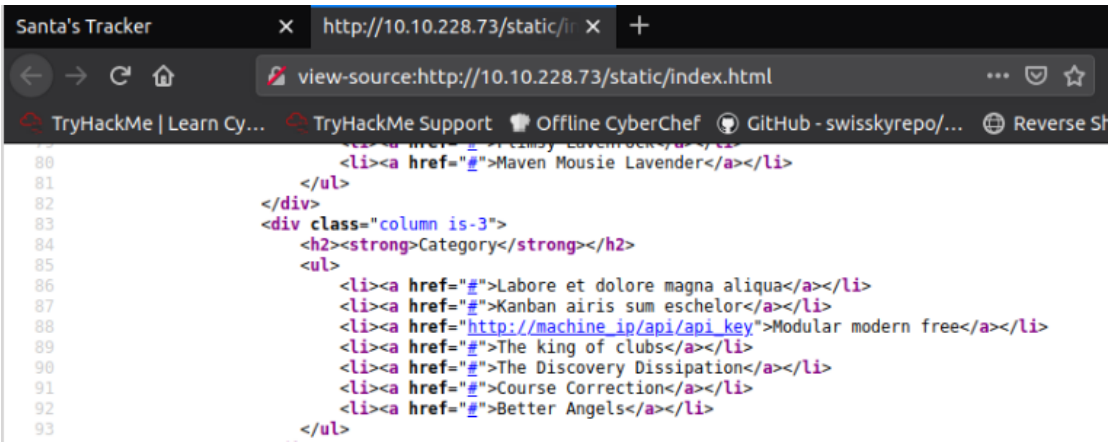
Question 2

Bulma is the template used for the website. It can be found at the bottom of the website.



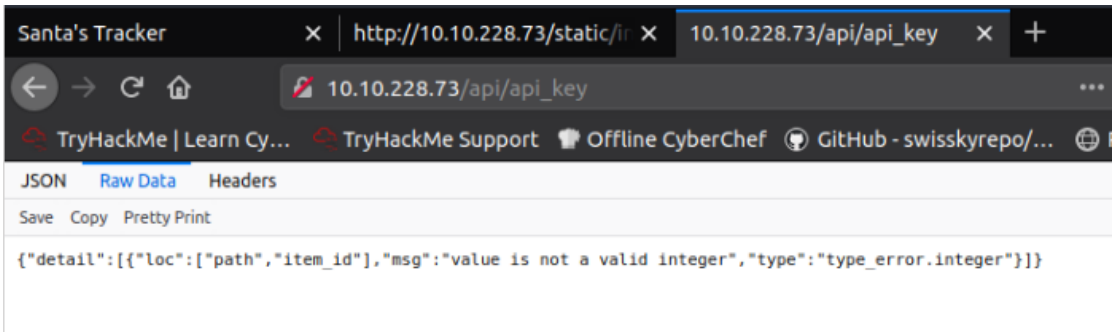
Question 3

The directory for the API can be found in the page source of the website. It is **/api/** .



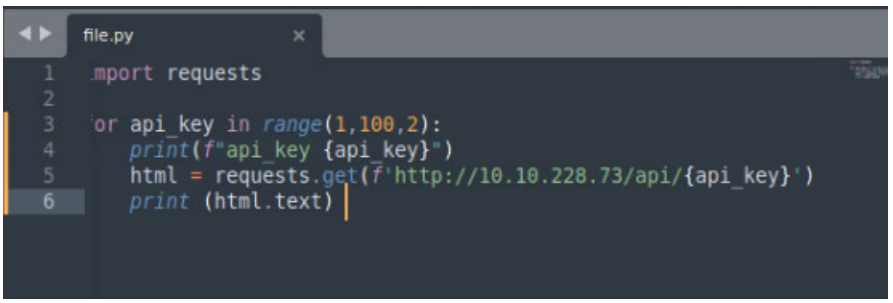
Question 4

The raw data of API endpoint if no parameter is entered.

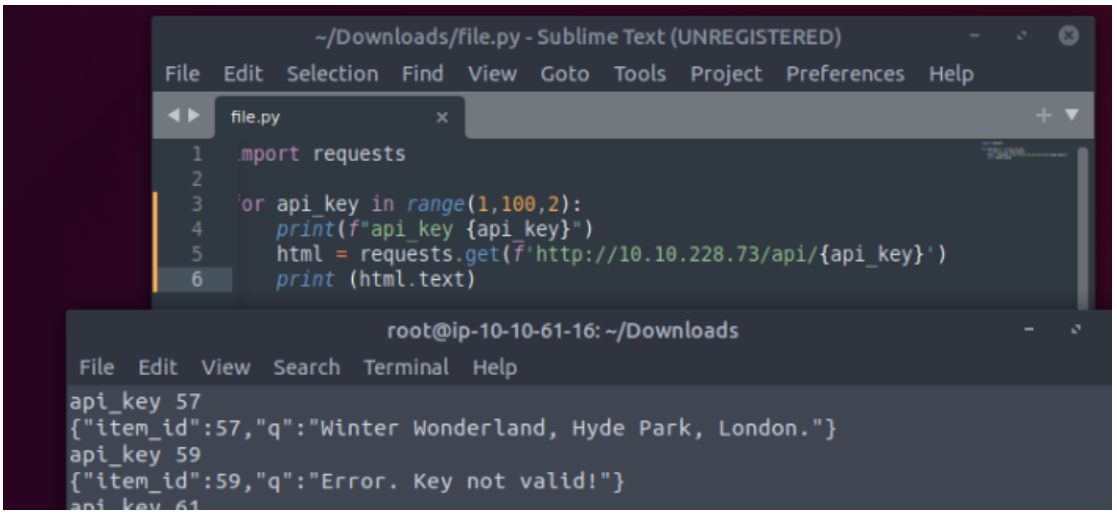


Question 5

Created a python file, **file.py**. Entered the needed code to find the API key and Santa's whereabouts.

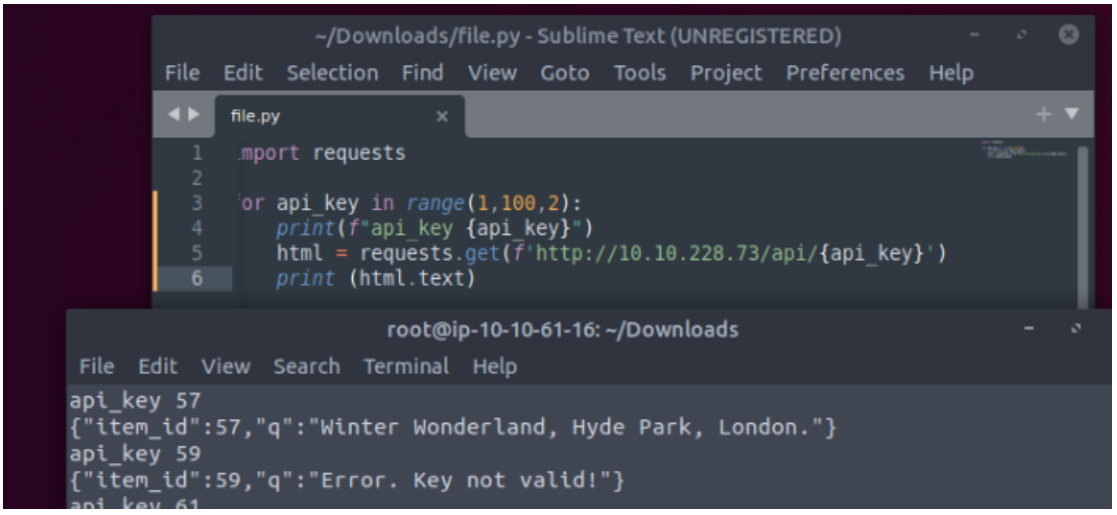


Run the python file on the terminal. Santa is at **Winter Wonderland, Hyde Park, London**.



Question 6

The API key is **57**.



Thought Process/Methodology:

Connected to Santa's webpage at **10.10.228.73/static/index.html** . In order to find the port number, we connected to the nmap and used the -v parameter for higher verbosity. Executed the code **nmap -v 10.10.228.73**. The port number of the web server is **80**. The template of the Santa's can be found at the bottom of the page. Viewed the page resource of Santa's website to find the API directory. It is **/api/**. Open the API link with the machine port to see the raw data if no parameter is entered. The next thing is we created a python file to find the API key and Santa's whereabouts. Put in the necessary code and execute it through the terminal. Santa is at **Winter Wonderland, Hyde Park, London** and the API key is **57**.

Day 17 : Reverse Engineering ReverseELFneering

Tools Used : Kali, ssh

Solution/walkthrough:

Question 1

Data type 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

The command to analyse the program in radare2 is **aa**

Time to see what's happening under the hood! **Run** the command `r2 -d ./file1`

This will open the binary in debugging mode. Once the binary is open, one of the first things to do is ask r2 to analyze the program, and this can be done by typing in: `aa`

Note, when using the `aa` command in radare2, this may take between 5-10 minutes depending on your system.

Question 3

The command to set a breakpoint in radare2 is **db**

The first 3 instructions are used to allocate space on that stack (ensures that there's enough room for variables to be allocated and more). We'll start looking at the program from the 4th instruction (`movl $4`). We want to analyse the program while it runs and the best way to do this is by using **breakpoints**.

A **breakpoint** specifies where the program should stop executing. This is useful as it allows us to look at the state of the program at that particular point. So let's set a breakpoint using the command `db` in this case, it would be `db 0x00400b55` To ensure the breakpoint is set, we run the `pdf @main` command again and see a little **b** next to the instruction we want to stop at.

Question 4

the command to execute the program until we hit a breakpoint is **dc**

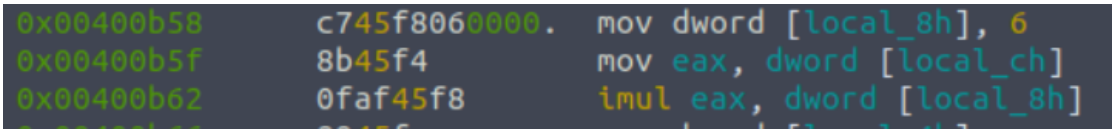
Running `dc` will execute the program until we hit the breakpoint. Once we hit the breakpoint and print out the main function, the rip which is the current instruction shows where execution has stopped. From the notes above, we know that the **mov** instruction is used to transfer values. This statement is transferring the value 4 into the `local_ch` variable. To view the contents of the `local_ch` variable, we use the following instruction `px @memory-address` In this case, the corresponding memory address for `local_ch` will be `rbp-0xc` (from the first few lines of **@pdf main**) This instruction prints the values of memory in hex:

Question 5

the value of local_ch when its corresponding movl instruction is called (first if multiple) **1**

Question 6

the value of eax when the imull instruction is **6**



Question 7

the value of local_4h before eax is set to 0 is **6**

Methodology/Explanation;

Firstly, I used the command echo “10.10.149.84” > target.txt to output the text. Then I entered the command **cat target.txt** to show the content of the file. I entered the command **ssh** elfmceager@10.10.149.84 and entered the password adventofcyber to log in to the remote machine. I used **ls** to list the file, which was **challenge1 file1.** i then entered the command **r2 -d ./challenge1** to enter the debug mode and after that i entered the command **aa** to analyse the program.

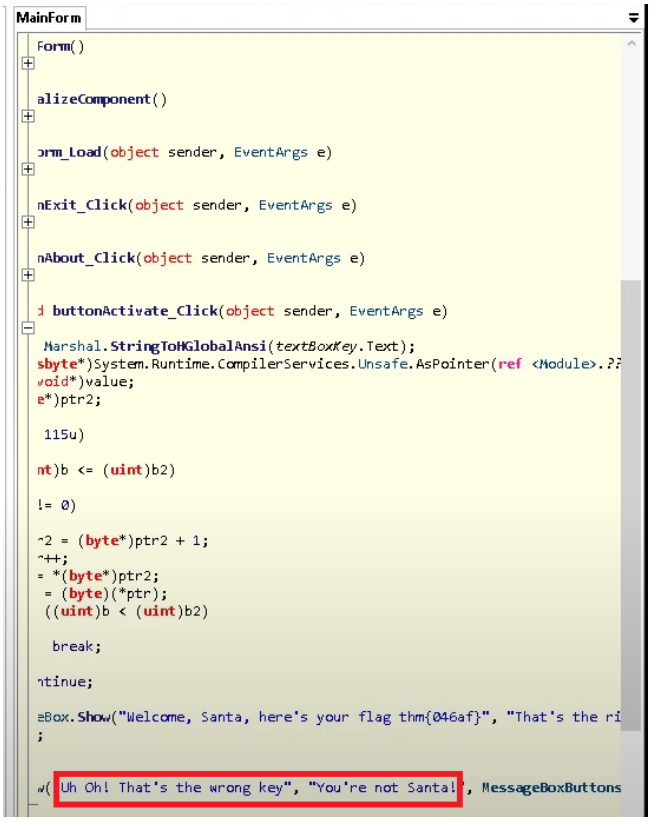
DAY 18: The bits of Christmas.

Tools used: Kali,

Solution/walkthrough:

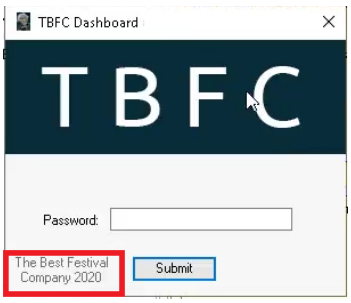
Question 1

Qs: What is the message that shows up if you enter the wrong password for TBFC_APP?*?
Answer: Uh Oh! That's the wrong key, You're not Santa!



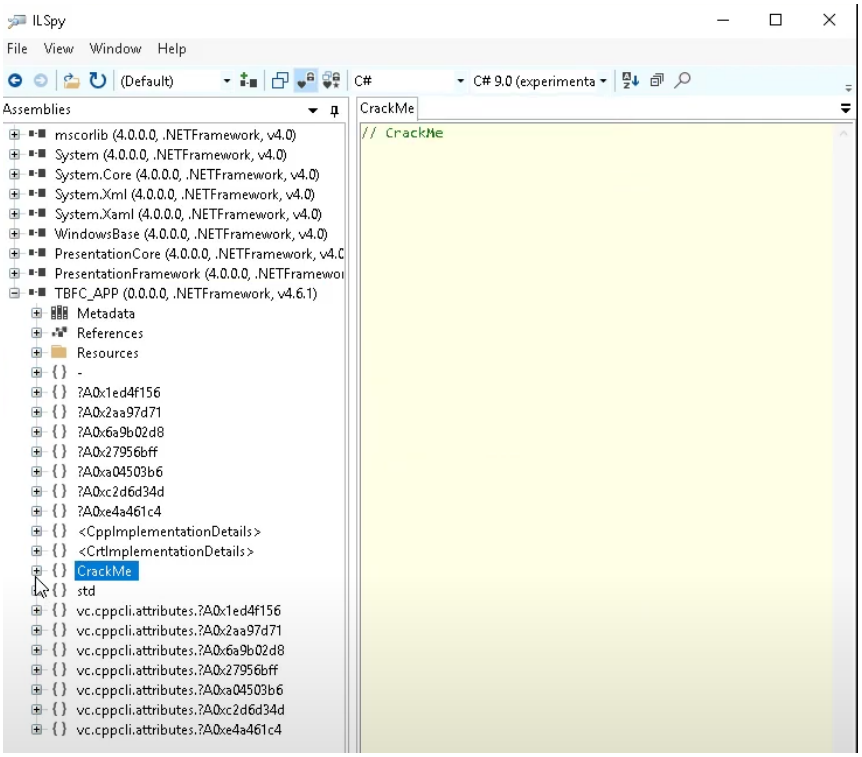
Question 2

Qs: What does TBFC stand for?
Answer: The Best Festival Company 2020



Question 3

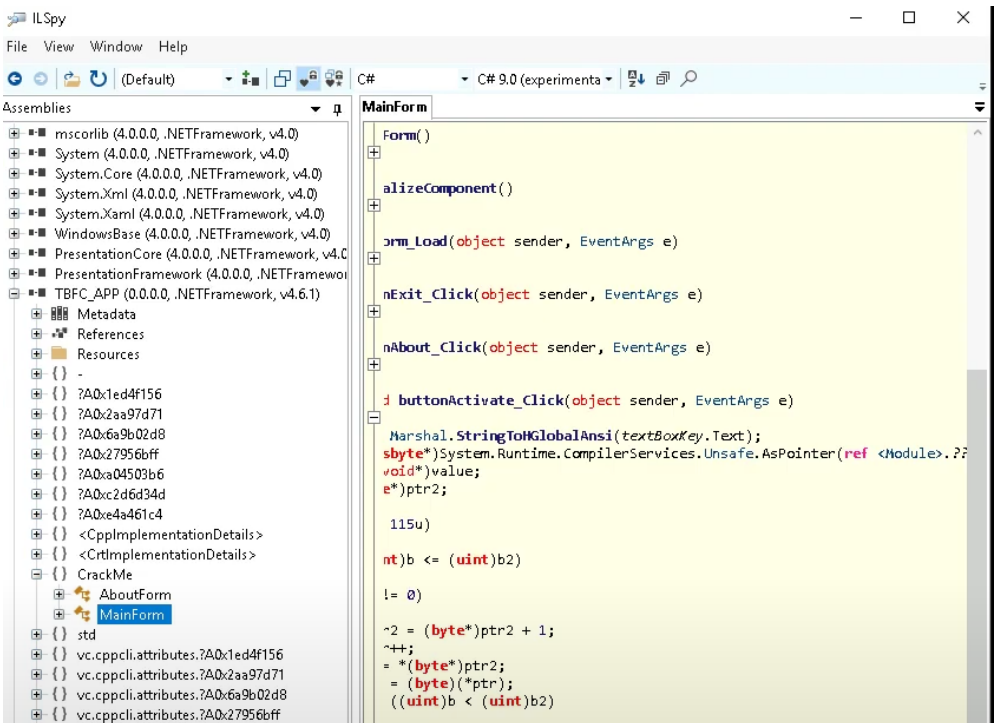
Qs: Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?
Answer: CrackMe



Question 4

Qs: Within the module, there are two forms. Which contains the information we are looking for?
Answer: MainForm

The answer is in MainForm file

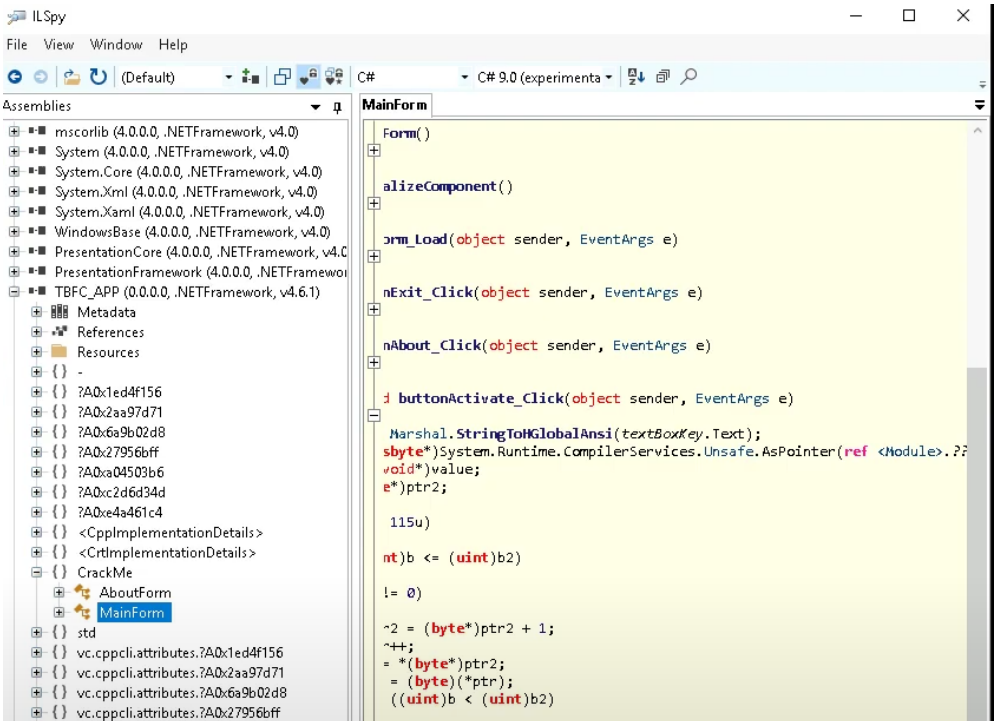


Question 5

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

Answer: buttonActivate_Click

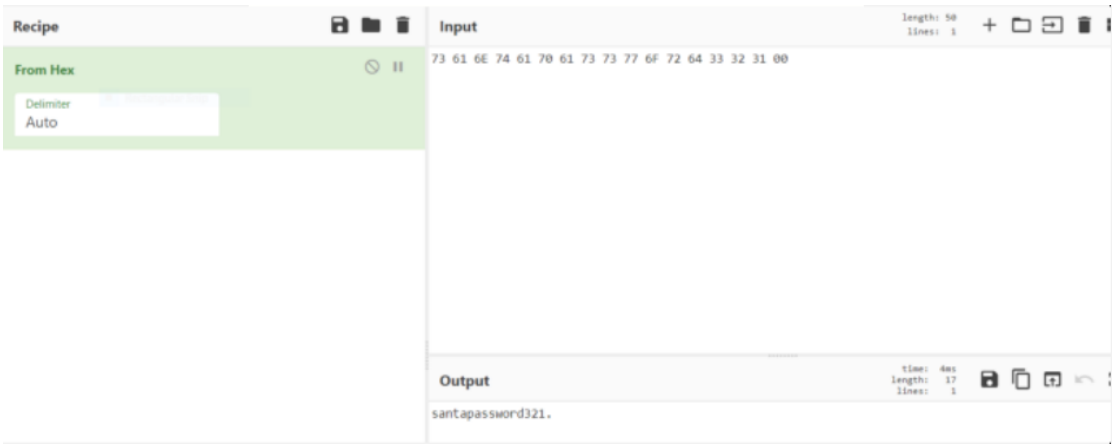
The app runs on buttonActivate_Click as we see on the MainForm



Question 6

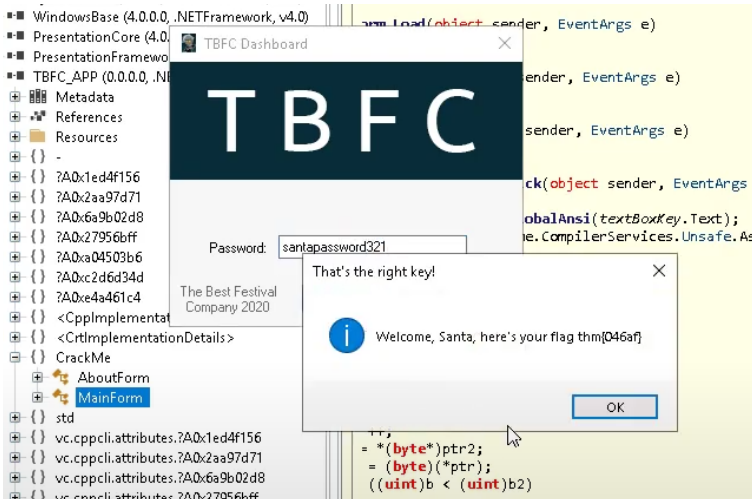
Qs: What is Santa's password?
Answer: santapassword321

Using hex from cyberchef, putting the input will give us Santa's password



Question 7

Qs: Now that you've retrieved this password, try to login...What is the flag?
Answer: thm{046af}



Thought Process/Methodology:

Open ILSpy, deploy and in it open the TBFC file. Next, access the CrackMe file inside the TBFC_APP file. After that, access the MainForm. Based on that file, the activation of the App runs on the source code buttonActivation_Click. Then, in cyberchef, Take("_c@_0BB@IKKDFEPG@santapassword321")in the format to hex and decode it.We will then be given the output that will lead to Santa's password which is santapassword321. With Santa's Password, open TBFC_APP and place the password to capture the flag.

DAY 19: The Naughty or Nice List

Tools used: Kali,

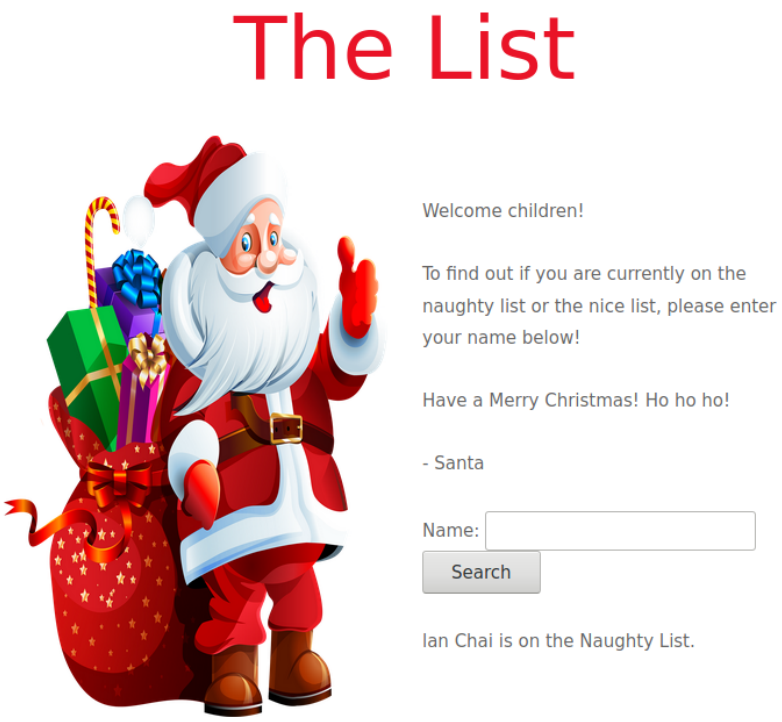
Solution/walkthrough:

Question 1

Qs: Which list is this person on?
Answers

Run the command (": [a] -c -z file,[b] http://[c].xyz/api.[d]?[e]=FUZZ
")

Only Tib3rius and YP are in the Nice list while the others are in the Naughty list



The List

Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name:

Search

JJ is on the Naughty List.

The List

Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name:

Search

YP is on the Nice List.

The List

Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name:

Search

Tib3rius is on the Nice List.

The List

Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name:

Search

kanes is on the Naughty List.

naughty list or the nice list, please enter
your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name: kanes

Search

Timontyh is on the Naughty List.

Question 2

Qs: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?

Answer :**Not Found. The requested URL was not found on this server.**

Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name:

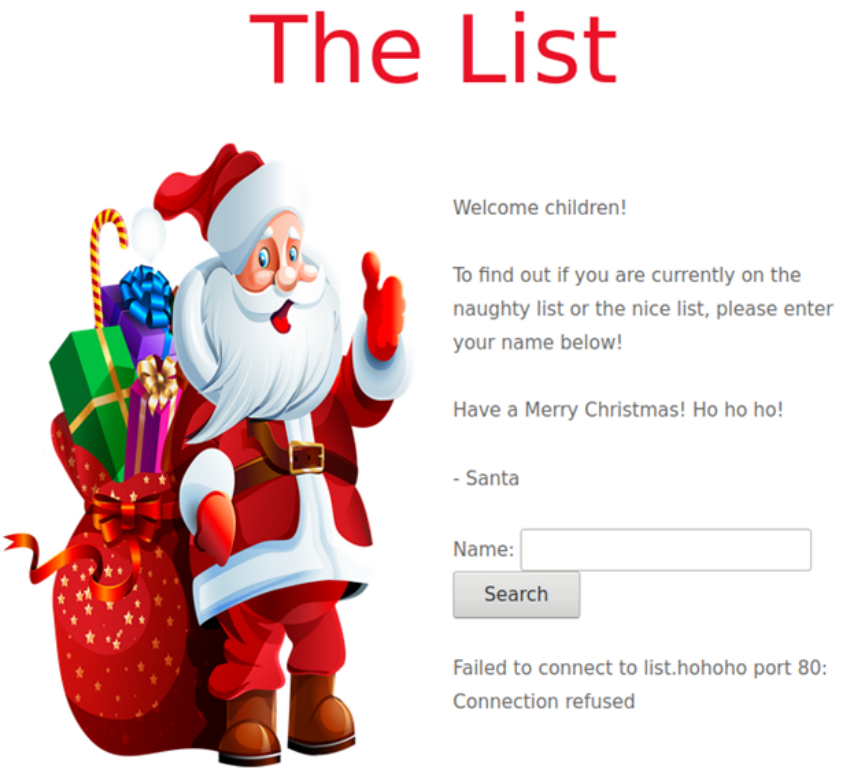
Search

Not Found

The requested URL was not found on this server.

Question 3

Qs: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"?
Answer: **Failed to connect to list.hohoho port 80: Connection refused**



Question 4

Qs: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"
Answer: **Recv failure: Connection reset by peer**

The List

Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name:

Search

Recv failure: Connection reset by peer

Question 5

Qs: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?

Answer:Your search has been blocked by our security team.

The List

Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name:

Search

Your search has been blocked by our security team.

Question 6

Qs: What is Santa's password?
Answer: Be good for goodness sake!

- Santa

Name:

Search

Santa,

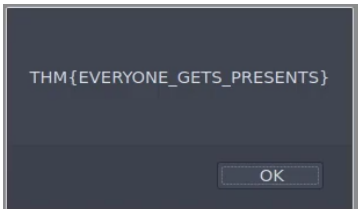
If you need to make any changes to the Naughty or Nice list, you need to login.

I know you have trouble remembering your password so here it is: Be good for goodness sake!

- Elf McSkidy

Question 7

Qs: What is the challenge flag?
Answer: THM{EVERYONE_GETS_PRESENTS}



Thought Process/Methodology:

Fetch the root of the site by browsing "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F".We will get the requested URL was not found on this server. Then try to change the port 8080 to something else like /?proxy=http%3A%2F%2Flist.hohoho%3A80 to see if can connect to any service running on the site. After doing so we will get Failed to connect to list.hohoho port 80:Connection refused. So then we try to change the port number to 22 and it will displayed Recv failure: Connection reset by peer which means the port 22 is open but it cannot understand what was being sent. So we will replaced to local . It turns out that the DNS only accepts subdomains that begins with list.hohoho, then we alter the list.hohoho to list.hohoho.localtest.me . After doing so we obtain the password. Then, enter the username and the password to access to the list of administration. Click on the delete naughty list button and capture the flag.

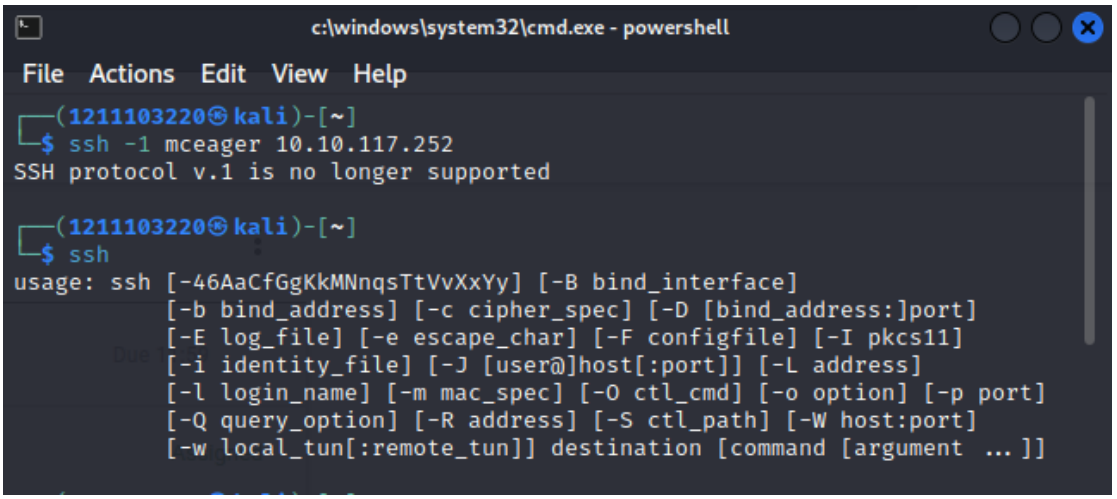
Day 20 - [Blue Teaming] PowershELlF to the rescue

Tools Used: Kali, ssh

Solution/Walkthrough:

Question 1

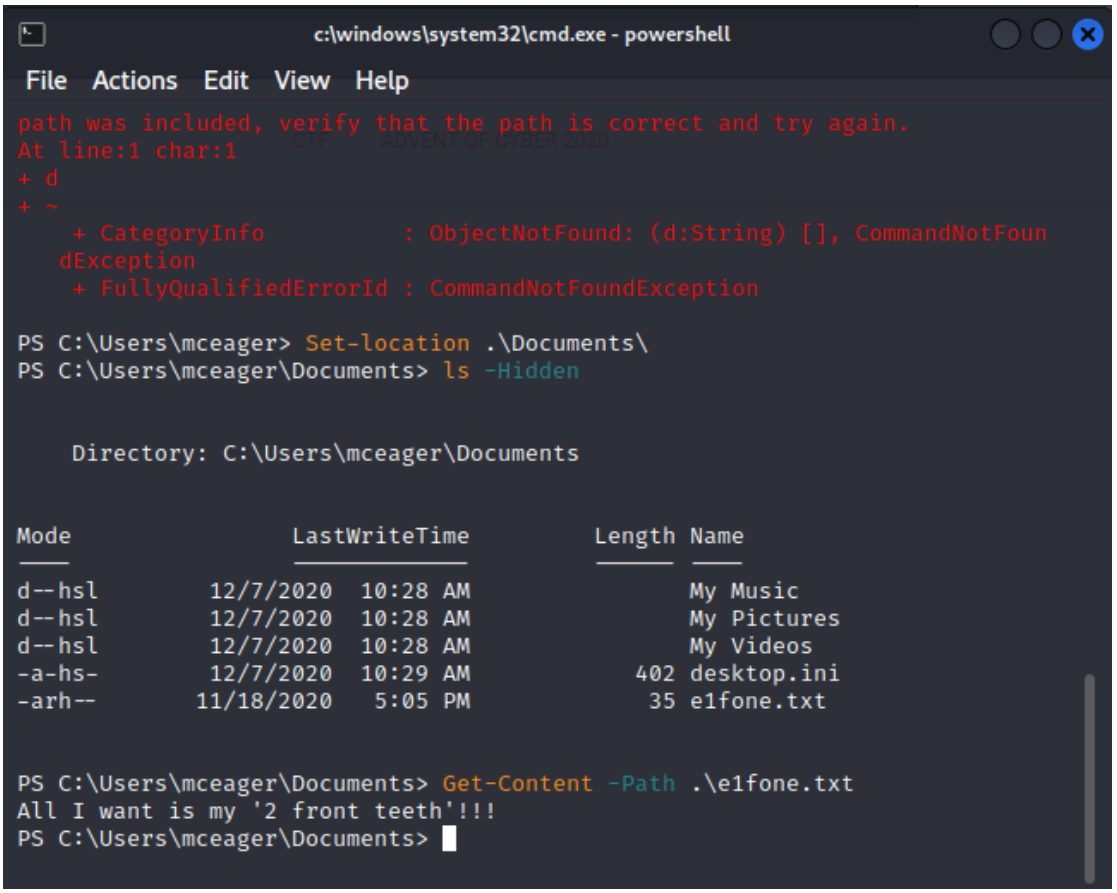
Check the ssh manual. What does the parameter -l do?



Answer: **login name**

Question 2

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



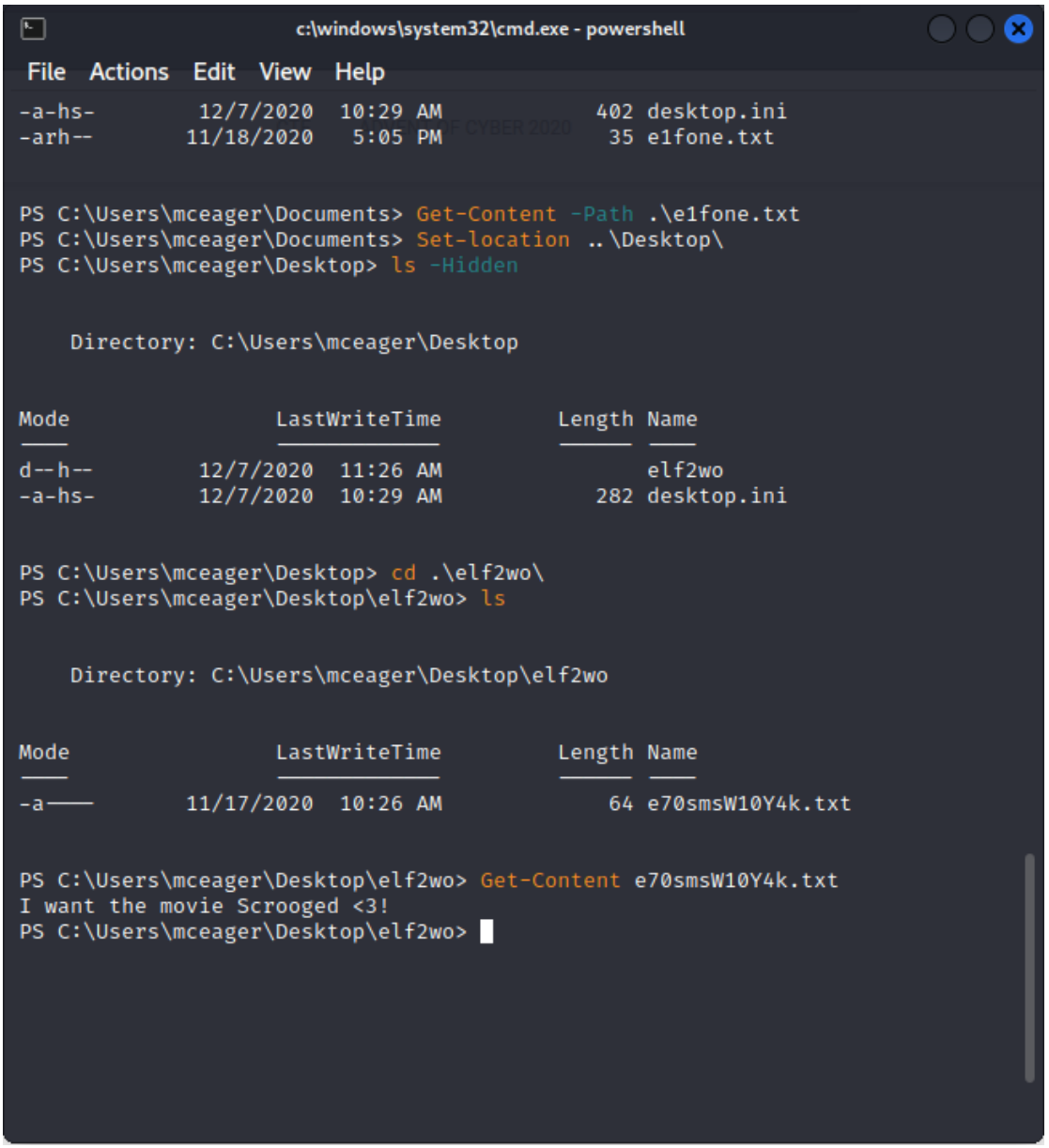
We can set the location to Documents Folder by the command "**Set-location .\Documents**\". Then, since the file is hidden, we can use command "**ls**" with the flag "**-Hidden**".

We can see there's a file named "**e1fone.txt**". With the command "**Get-Content -Path .\e1fone.txt**" we can open the file.

Answer: the elf wants **2 front teeth**

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?

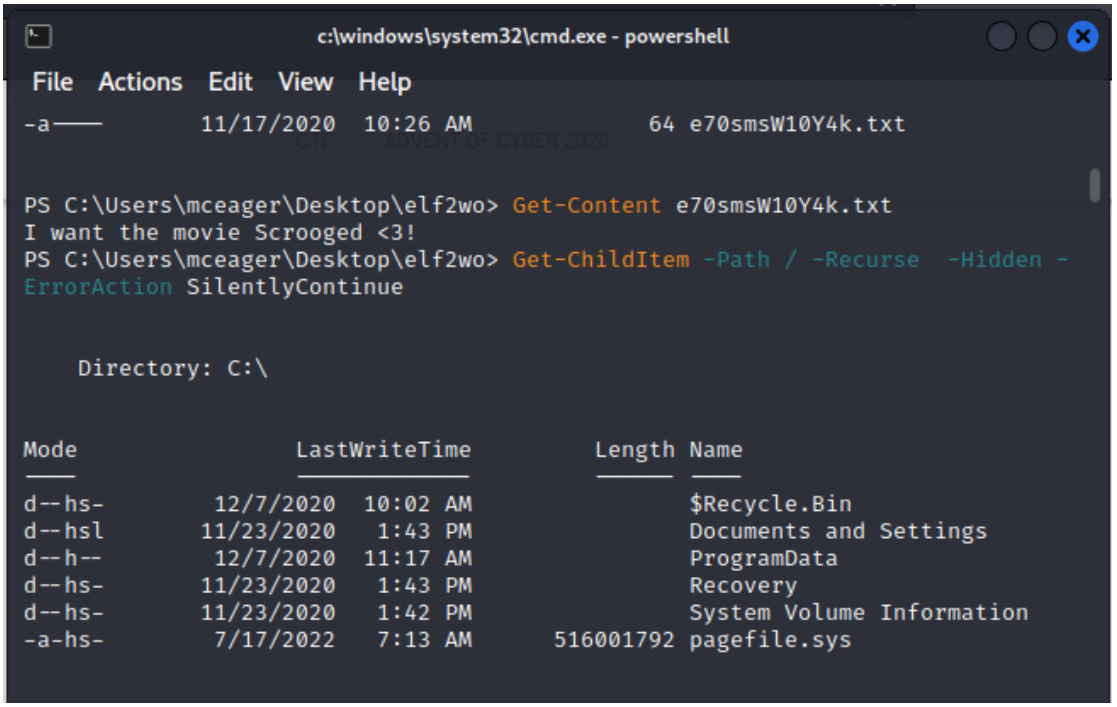


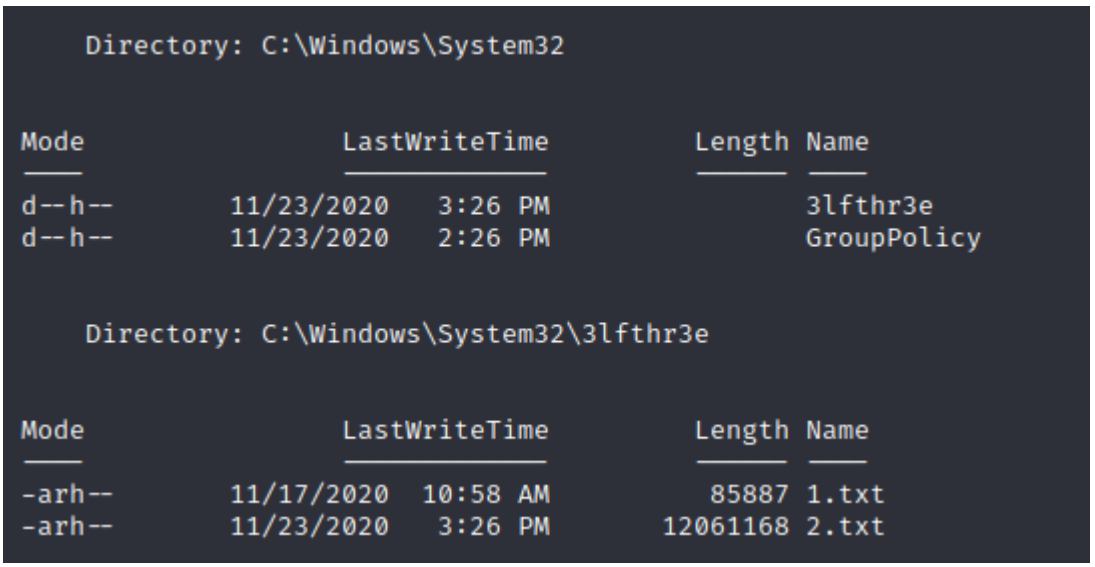
We can repeat the same step as the previous question.

Answer: the movie that the elf wants is **Scrooged**

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)





We searched through the entire directory of the drive, and we can see there is a folder name "**3lfthr3e"**.

Question 5

How many words does the first file contain?

```
PS C:\Users\mceager\Desktop\elf2wo> Get-Content C:\Windows\System32\3lfthr3e\
1.txt | Measure-Object -Word

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


PS C:\Users\mceager\Desktop\elf2wo>
```

With the command "**Measure-Object**" we can get the total number of words along with the flag "**-Word**"

Answer: **9999**

Question 6

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

```
PS C:\Users\mceager\Desktop\elf2wo> (Get-Content C:\Windows\System32\3lfthr3e
\1.txt)[551]
Red
PS C:\Users\mceager\Desktop\elf2wo> (Get-Content C:\Windows\System32\3lfthr3e
\1.txt)[6991]
Ryder
PS C:\Users\mceager\Desktop\elf2wo>
```

By using the concept of array through the entire file we can get the exact word for the specific index.

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)

```
PS C:\Users\mceager\Desktop\elf2wo> Select-String -Path C:\Windows\System32\3
lfthr3e\2.txt -Pattern 'redryder'

C:\Windows\System32\3lfthr3e\2.txt:558704:redryderbbgun


PS C:\Users\mceager\Desktop\elf2wo>
```

We can select the exact string from the entire file with the command "**Select-String**" and then with the flag **-Pattern** along side with the string we want which is "**redryder**"

Answer: **Red Ryder bb Gun**

Thought Process/Methodology:

We can check the ssh manual by type in "**ssh**" into the terminal and we can see the parameter -i is for **login name**. In order to find the hidden elf file within the Documents folder, we need to set the location to the Documents folder first. This can be done by using the command "**Set-location .\Documents\"**. Then since the file is hidden we use the "**ls**" common with the parameter "**-Hidden**". We then see the list of files and one of them is named "**e1fone.txt**". With the command "**Get-Content**" we can open the file. We found out the elf wants **2 front teeth**. To search the hidden folder that contains the file for Elf 2 in the desktop we repeat the same steps as before. Set the location to Desktop and get the list of hidden files and folders. We found a hidden folder with a text file inside. Then we got the movie that the elf wants is **Scrooged**. For elf 3 we have to search the entire directory for the hidden folder. For that we use the command "**Get-ChildItem -path / -recurse -Hidden -ErrorAction SilentlyContinue**". From scrolling through the output we can see a folder named "**3lfthr3e"**. This folder contains 2 files. The first file has **9999** words that can be obtained with the command, "**Measure-Object"** along with the parameter **-Word**. To find the words at index 551 and 6991 we use the concept of array through the entire file. At index 551 we get **Red** and at 6991 we get **Ryder**. This is only half the answer. We can search in the 2nd file for the phrase "redryder" to get the full answer. With the command "**Select-String**" along with parameter **-Pattern** we can get the specific string. Finally we got the full answer which is "**Red Ryder bb Gun"**