PSP0201 Week 5 Writeup

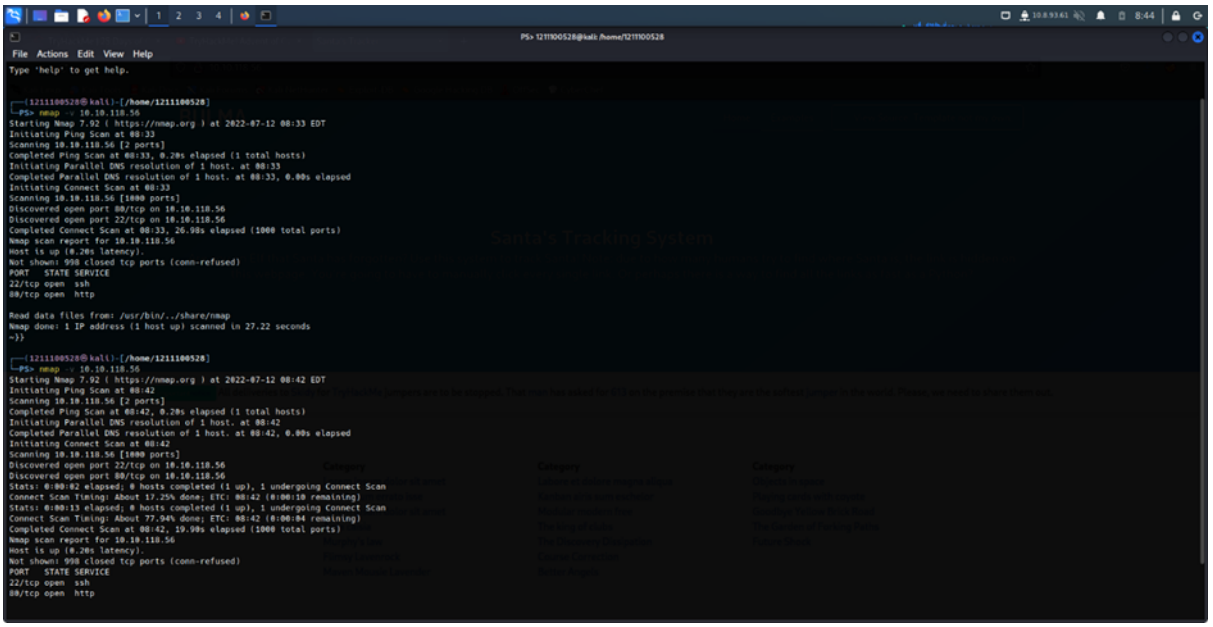
Group Name : Mali Pape

Members:

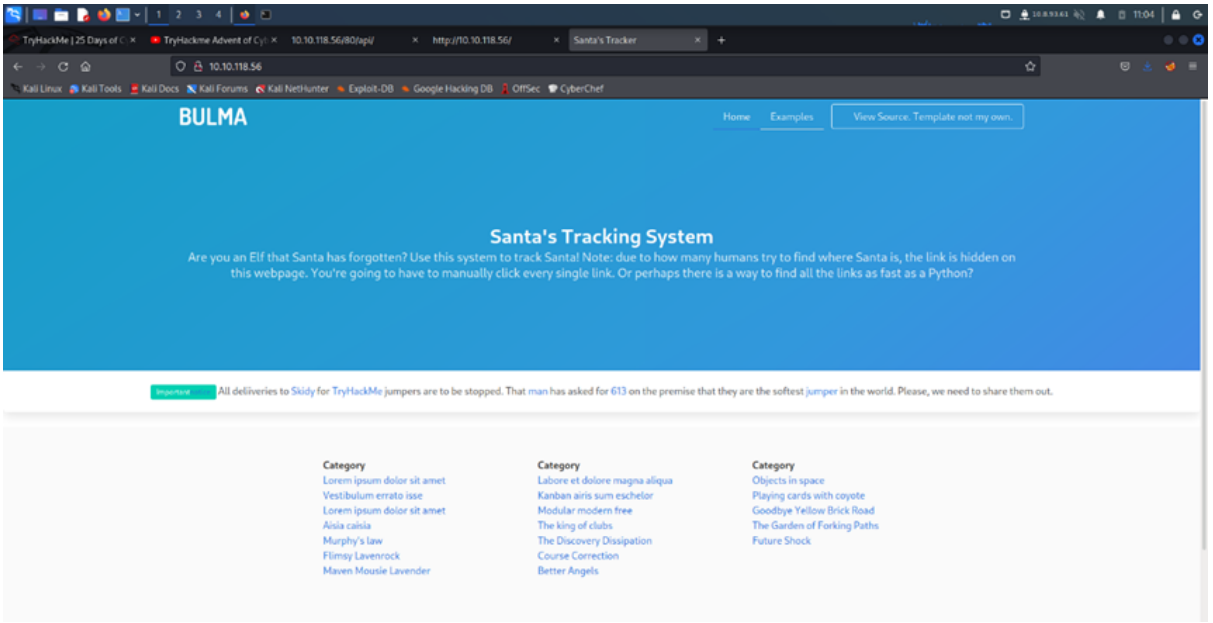
ID	Name	Role
1211102895	Muhammad Irfan Bin Mohd Nazri	Leader
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazariee	Member
1211103634	Ho Tian Ming	Member
1211101035	Mohamad Zuhir Bin Mohamad Zailani	Member

Day 16 - (scripting) Help! Where's is santa
Tools used: Kali Linux, Firefox, Terminal, Nano, Python
Solution/walkthrough:

Question 1:



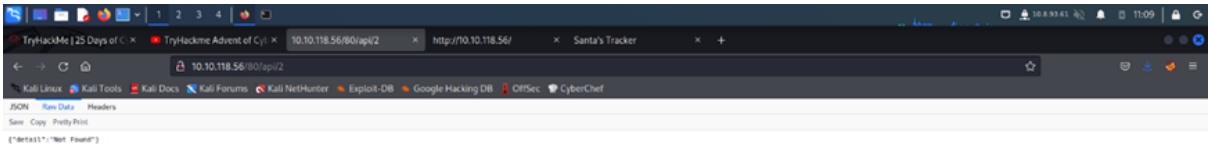
Utilise nmap with the address we just got. Obtaining the port number to launch the API is the next step.
Question 2:



Get the template name by going to the URL page.

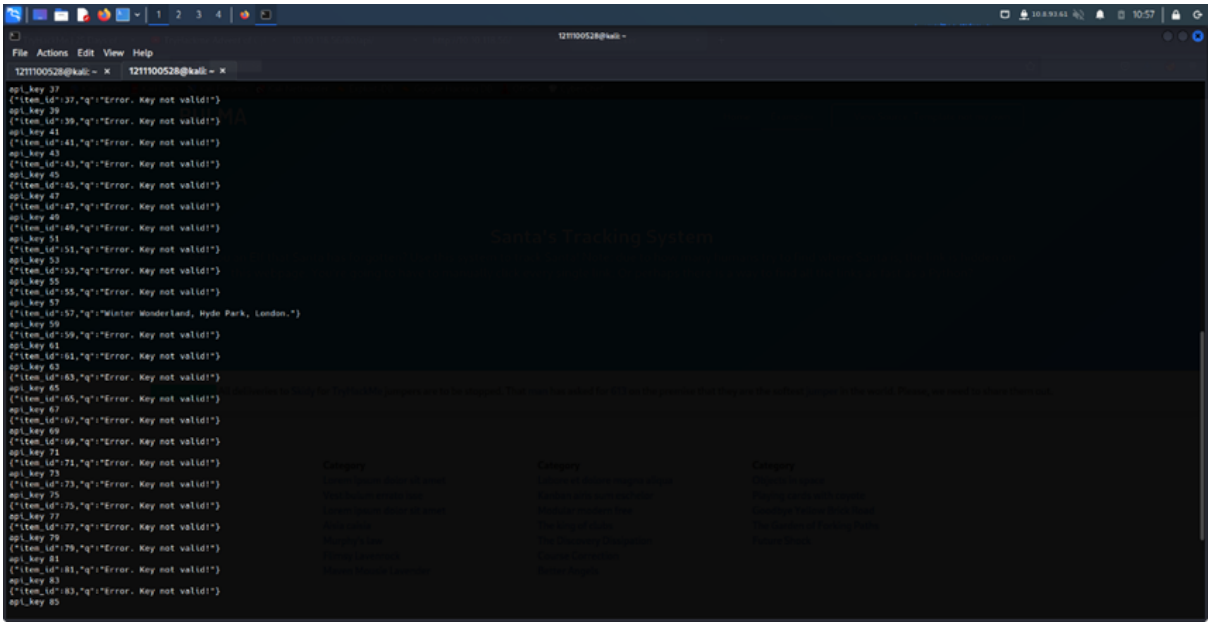
Question 3:
For this question, we can get the answer by putting "/api/" to the url and port number.

Question 4:



We must enter the url code along with the port number and api in order to visit this page. The RAW Data tab will then open.

Question 5&6



The brute.py method and the nano app should be used to locate the address, and python commands should then be used to obtain the location address and the appropriate api key in front of the address.

Thought process/Methodology:

In order to access the IP address, we must first launch the machine and open the webpage. Next, we must use the nmap method to open the terminal and obtain the port number. The website can then be accessed by utilising both the IP address and

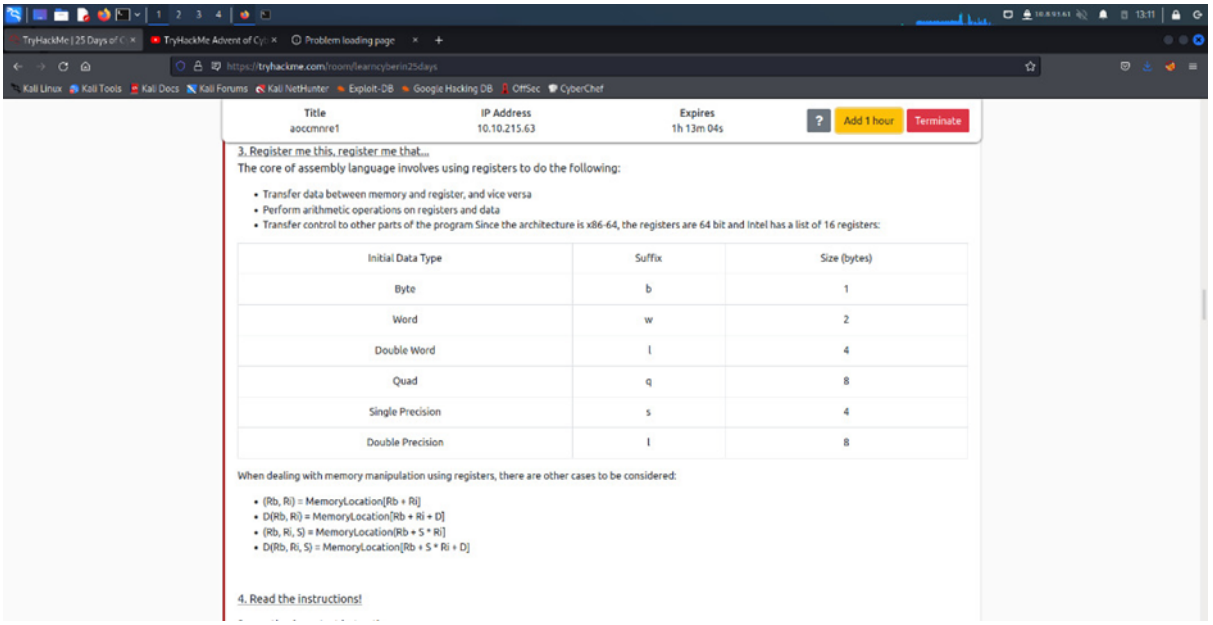
the port number. After that, we can add "/api/" to the url to enter the api secret page and obtain a wealth of data, including raw data. Finally, we need to utilise the brute technique using the python language as a command to acquire the stuff we want, which includes Santa's location address and the api key.

Day 17- [reverse engineering] ReverseELFneering

Tools used: Kali Linux, Firefox, Terminal.

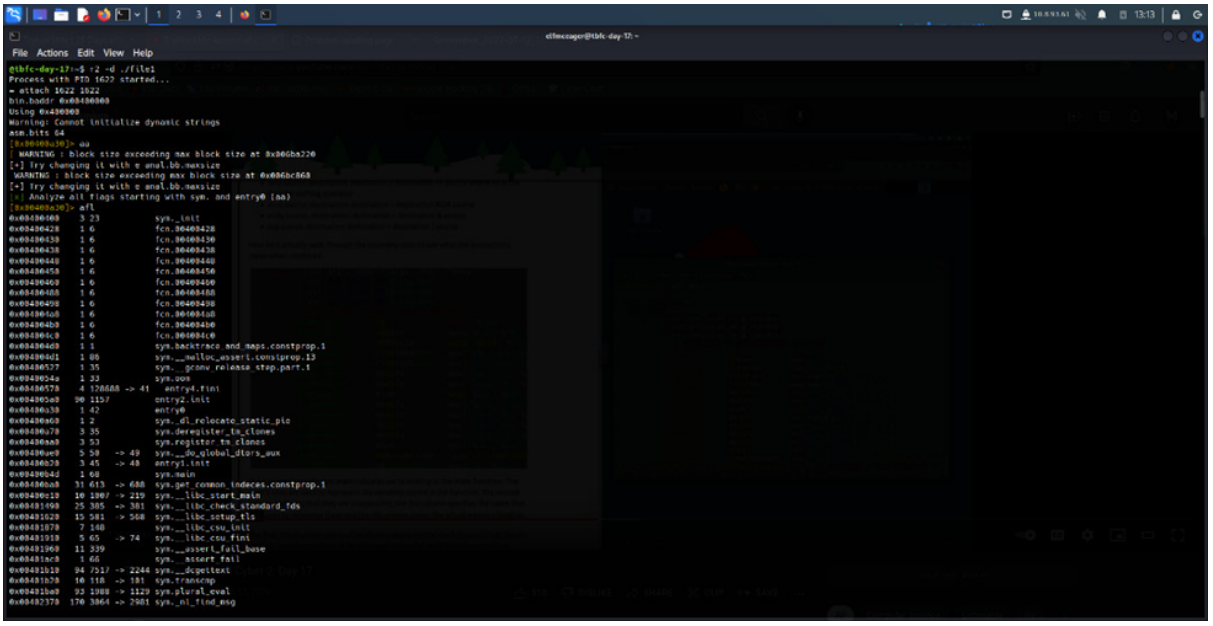
Solution/walkthrough:

Question 1:



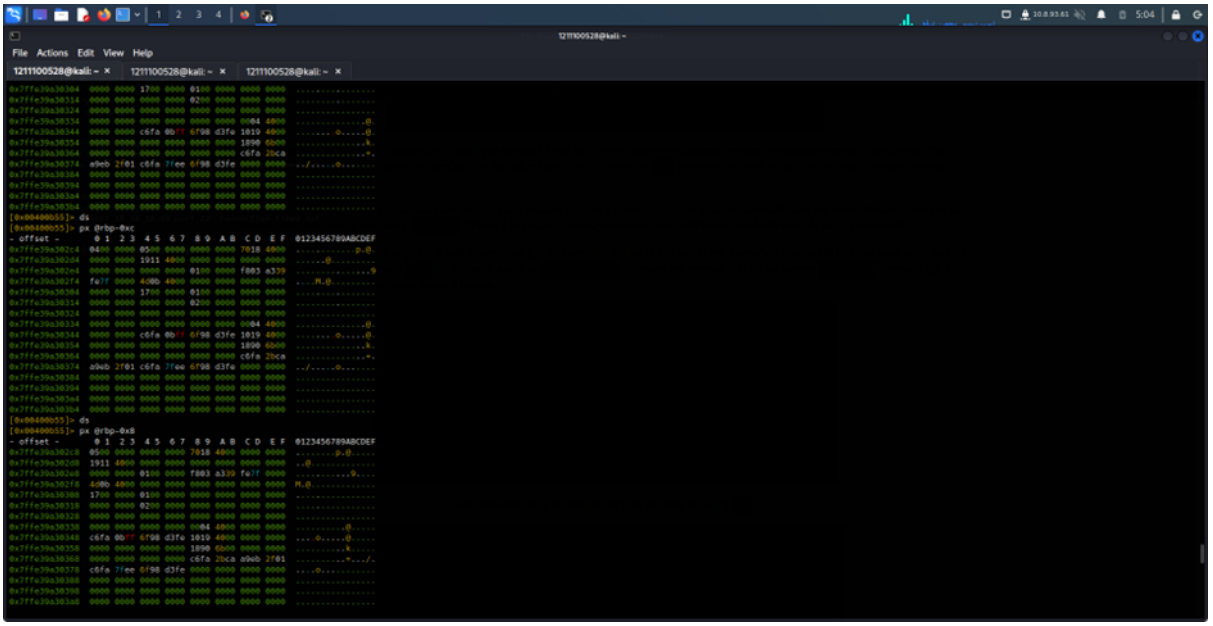
We can find the answer in tryhackme.

Question 2:



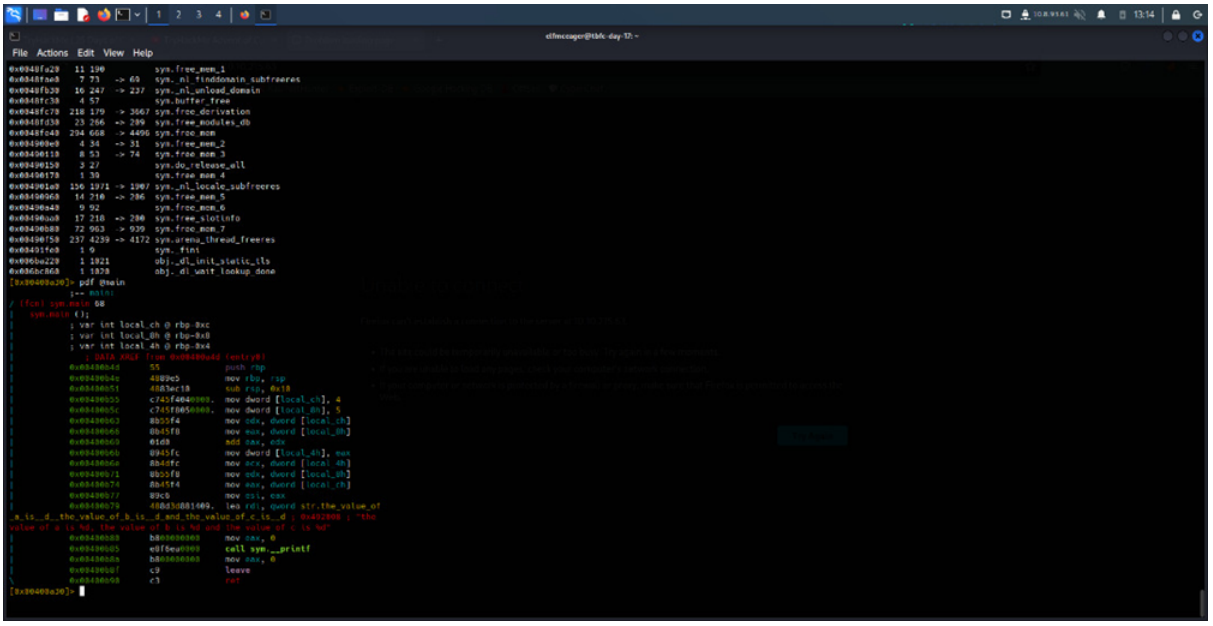
The command **"aa"** must be entered in radare2 in order to analyse the programme.

Question 3:



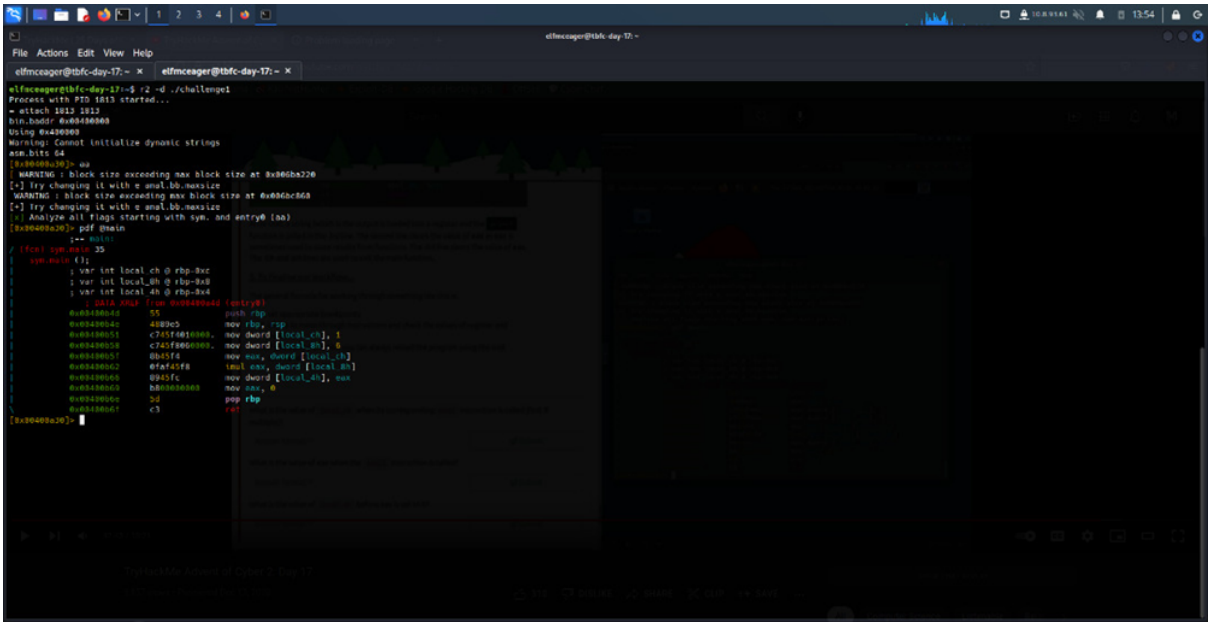
The command **"db"** would be used to set a breakpoint in radare2.

Question 4:



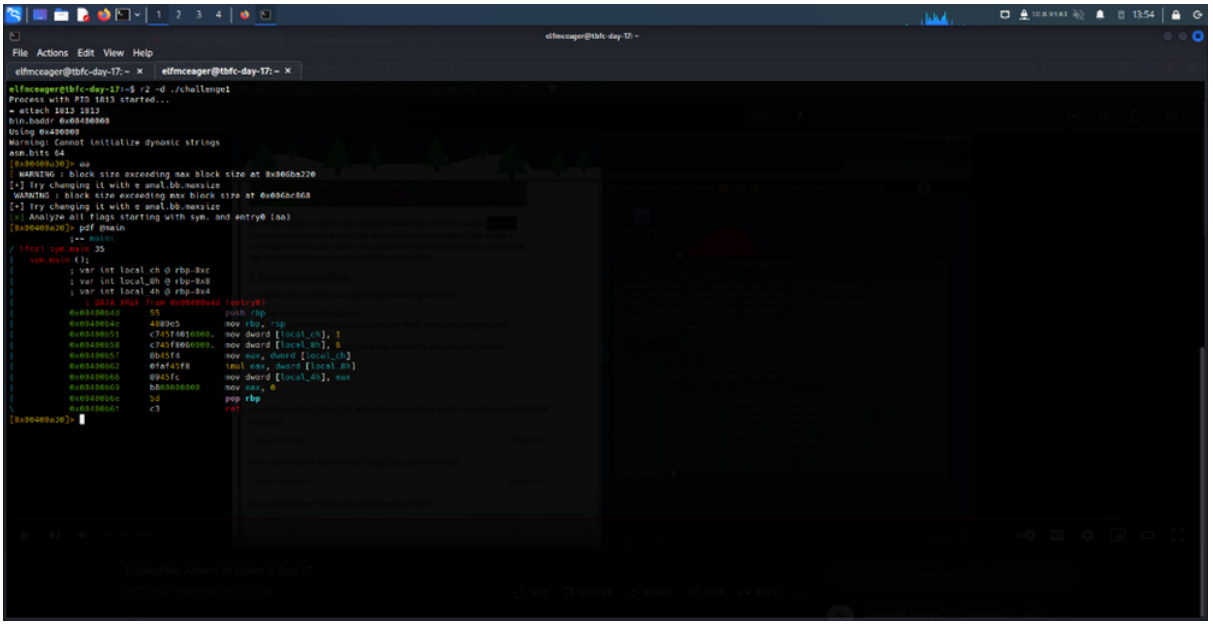
The command **"pdf @main"** is what we'll need to run the programme until we reach a breakpoint.

Question 5:



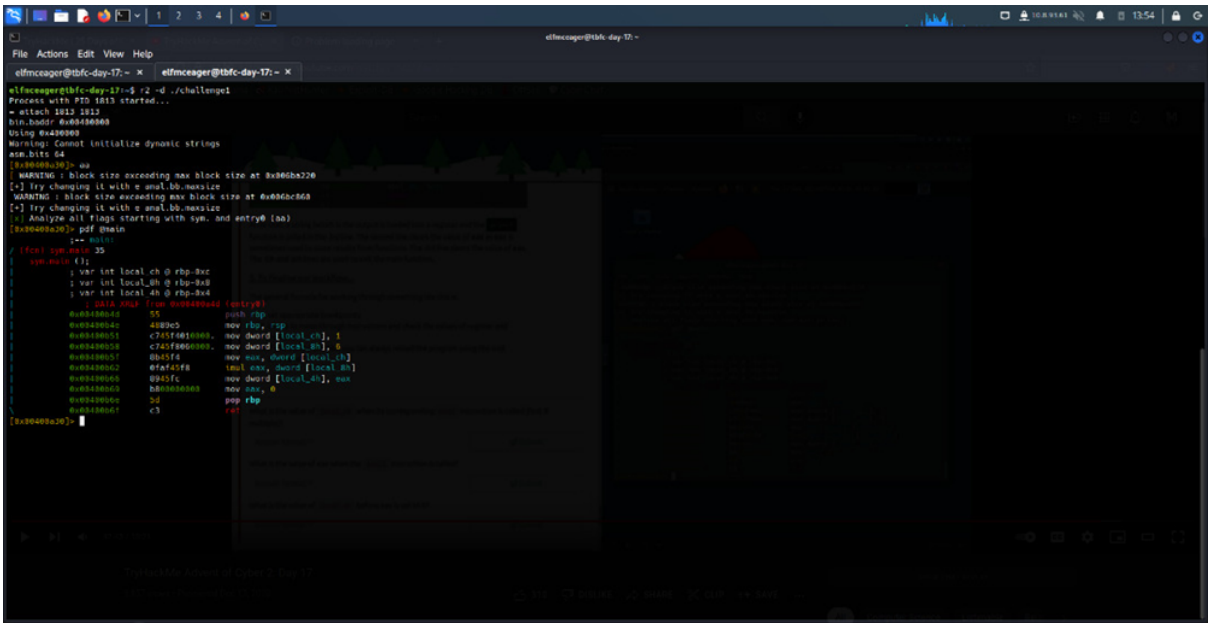
The value of local ch when the movl instruction that corresponds to it is called **"1"** as in the digit.

Question 6:



when the imull instruction is referred to as **"6"** as in the numeral digit, the value of eax.

Question 7:



Before eax is set to 0, local 4h would have the value **"6."**

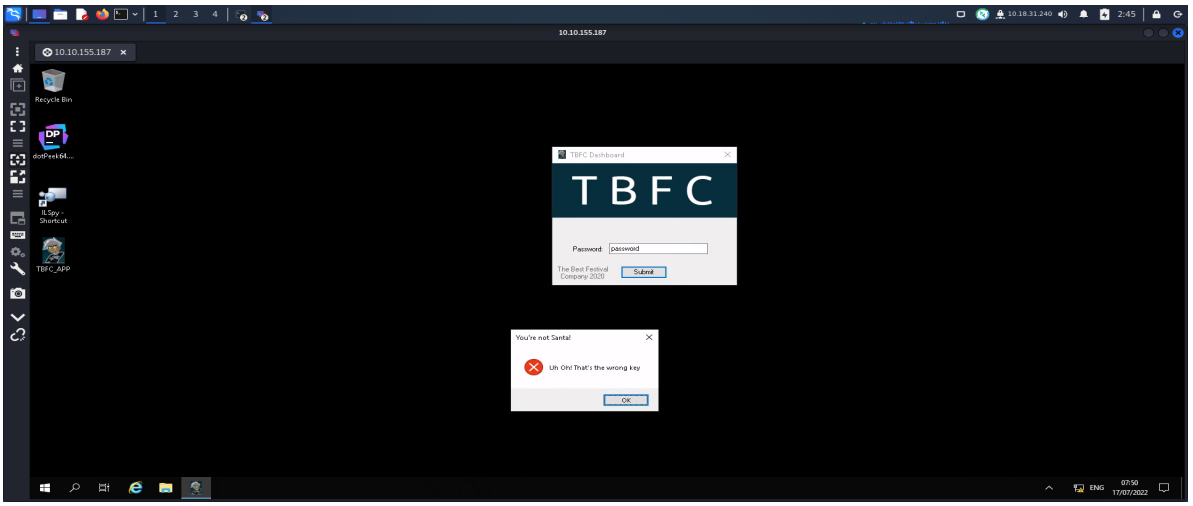
Thought process/Methodology:

Using the commands "nmap" and "cat target.txt" to target the web page, we must first connect the terminal to the website that we wish to view. To use Radare2 to enter the binary debugging mode, we only need to access the page using the username and password that were provided. The command "aa" can then be used to begin analysing the r2 programme. Once the analysis is finished, we must determine where to begin the analysis as a starting point, which is done by using the command

"afl." After determining the main function, we can use the command "pdf @main" to view the assembly code. Then

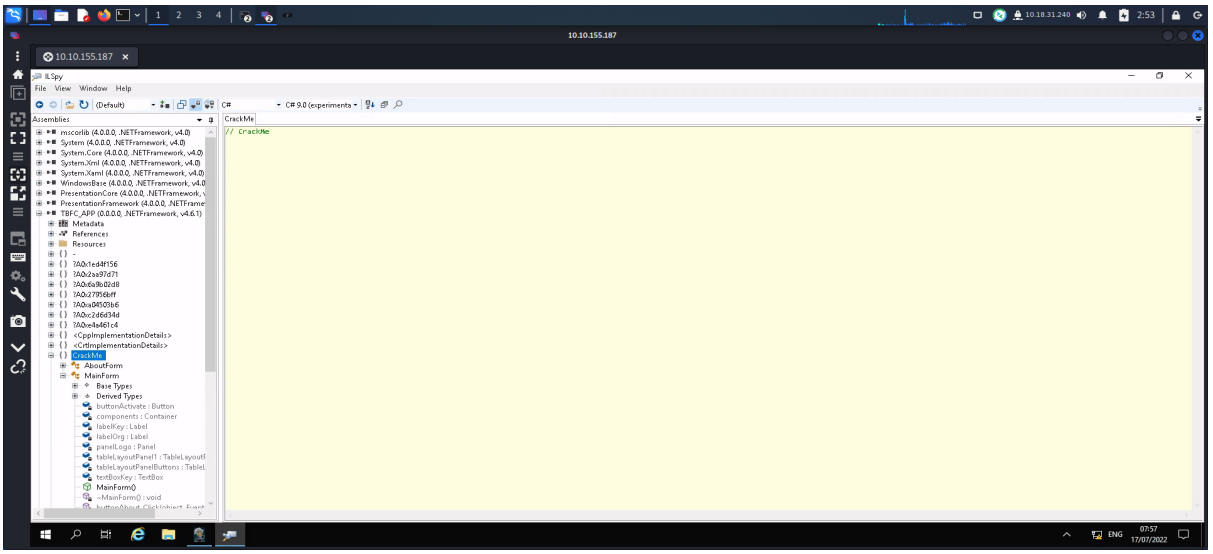
Day 18- [reverse engineering] The Bits of Christmas
Tool used: Kali Linux, Remmina
Solution/walkthrough:

Question 1&2:



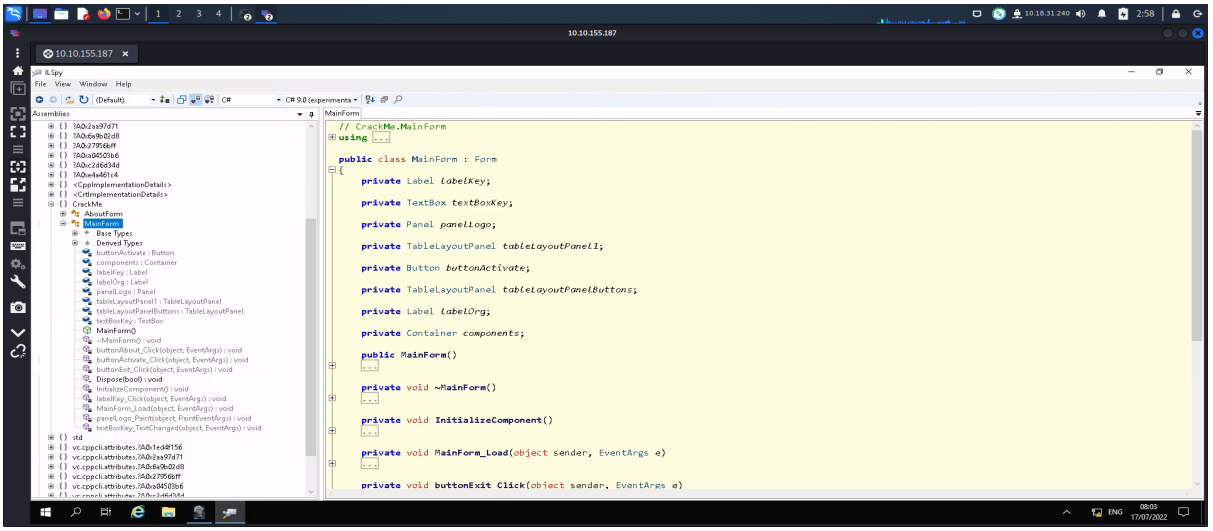
Open the remmina and open the TBFC and insert a random password. For question 2, The answer is beside the submit button.

Question 3:



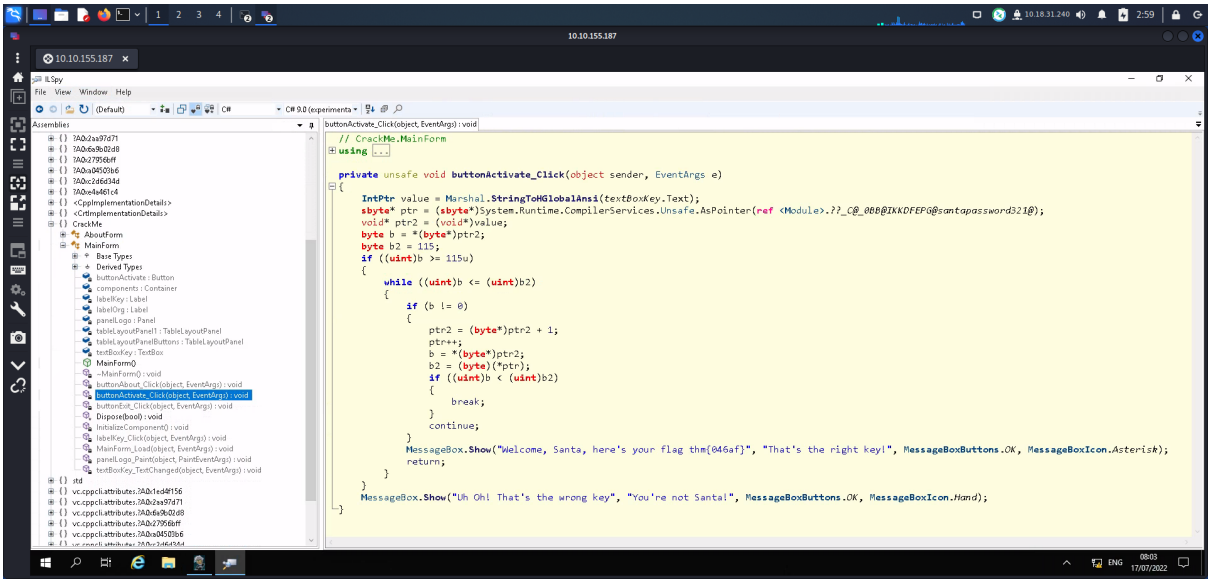
Open the IL Spy and click file and open the TBFC_App. Then find the special one that is CrackMe.

Question 4:



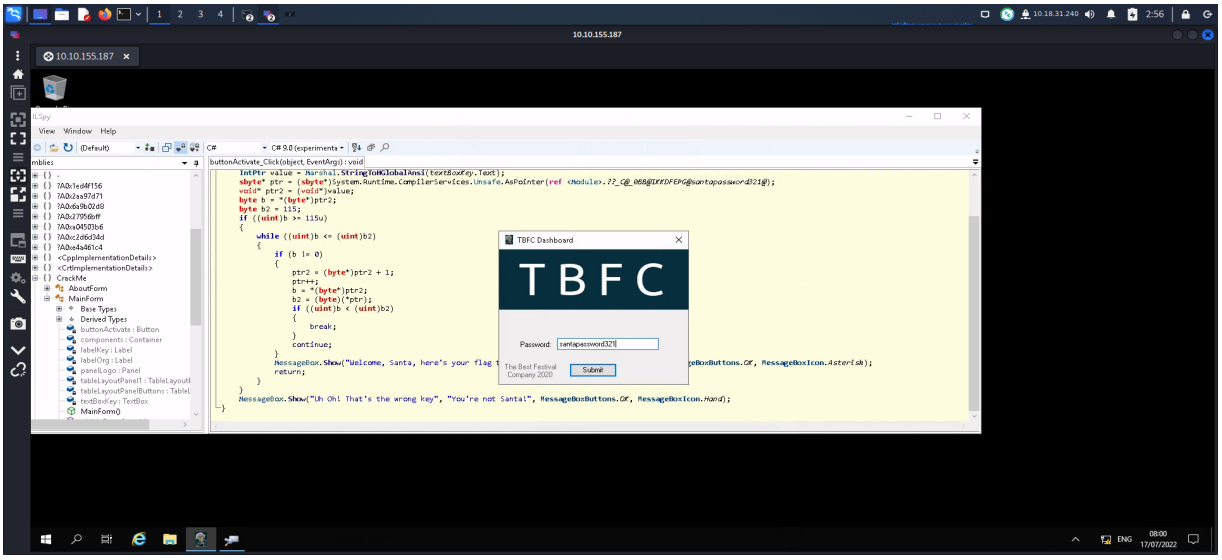
Click the CrackMe and then find MainForm

Question 5:



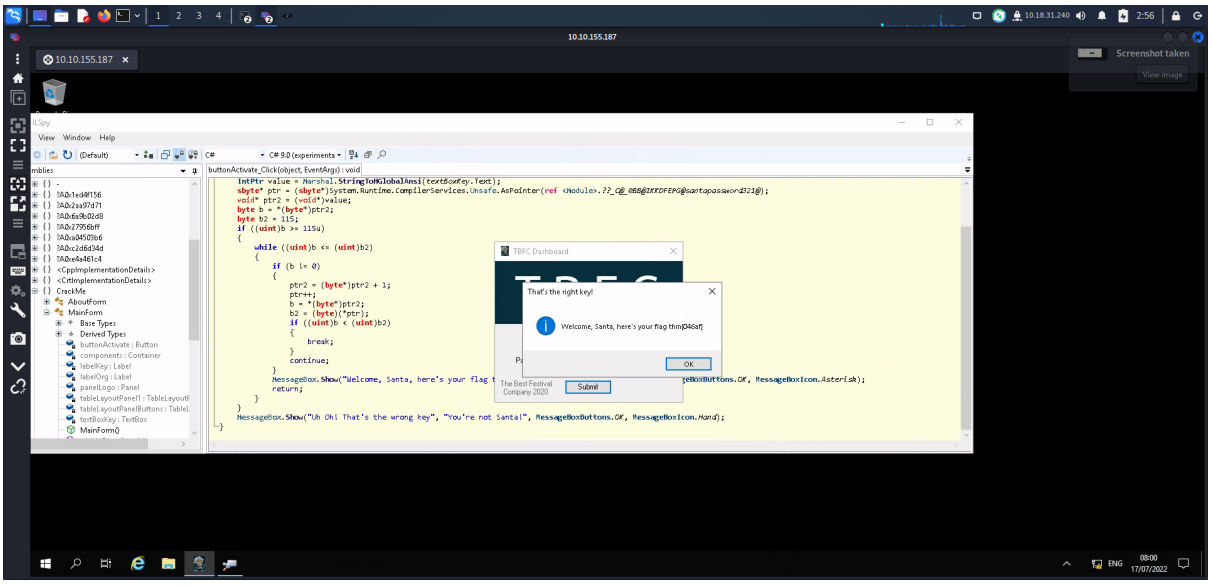
Find the buttonActivate_Click

Question 6:



Click the buttonActivate_Click and you will find the password on your right.

Question 7:



Enter the correct password and you will found the flag

Thought process/Methodology:

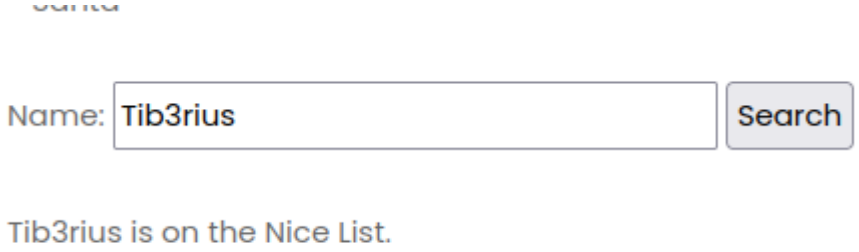
First of all, connect your vpn. Next, download remmina in your kali Linux. Then, open your remmina once it has downloaded completely. Enter your password when opening the remmina. Insert your ip address (website) in the RDP column. Then press enter. After that, it will appear a RDP authentication credentials. Now, Insert the username and password that are provided from the website. After filing the username and password, click ok. Wait for a while, the window machine will appear. Next, you will found out that there are recycle bin, dotPeek, IL Spy and TBFC_App on the desktop. Open the TBFC_App first. Next, insert a random password. Then it will tell you you're not a santa. To access the TBFC_App, you need to open IL Spy.

Next, you click file, click open, click desktop, click TBFC_App and lastly click open. The IL Spy will show a lot of line in the assemblies. Then, click the plus on CrackMe. It will show about form and main form. Click the plus on the main form, it will show more lines(reference to elements). Click the buttonActive_Click and see the source code (which are in the right with yellow page). You will found out the password in the line start with word sbyte*. Insert the password into the TBFC_App without the @ symbol. Lastly, press submit. Congratulations, you had found the flag.

Day 19- [Web exploitation] The Naughty or Nice List
Tool used: Kali Linux,
Solution/walkthrough:

Question 1:

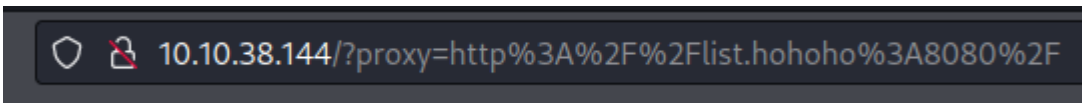
After we connect to the web app, we can search up names in the search bar to look for who is in the naughty or nice list. For example Tib3rius is on the nice list



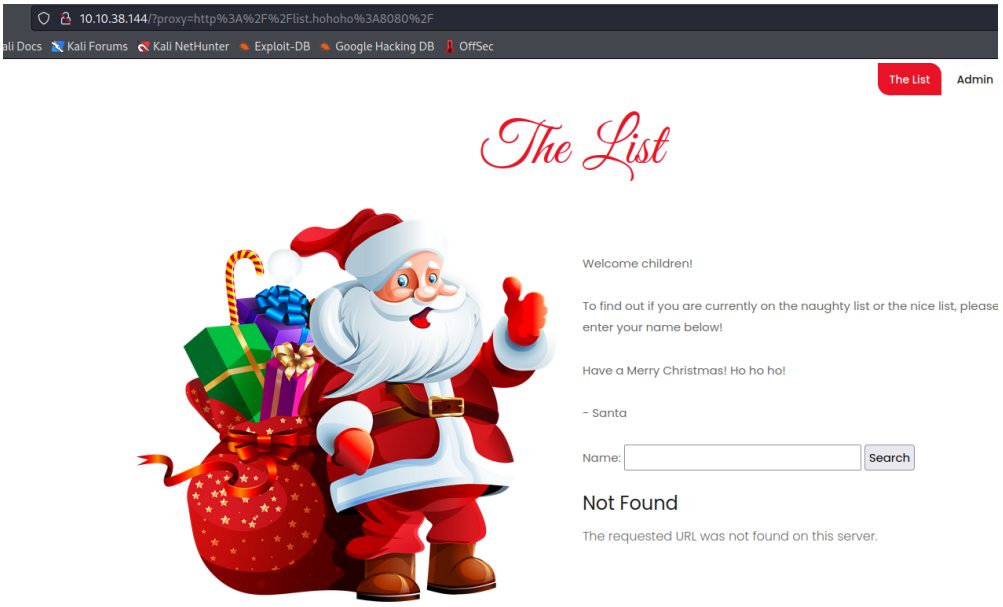
With this we can identify on which list Kanes, Timothy, YP, Ian Chai, and JJ are currently in

Question 2:

If we search up,



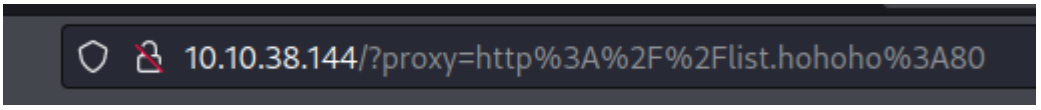
In the url, this page will appear



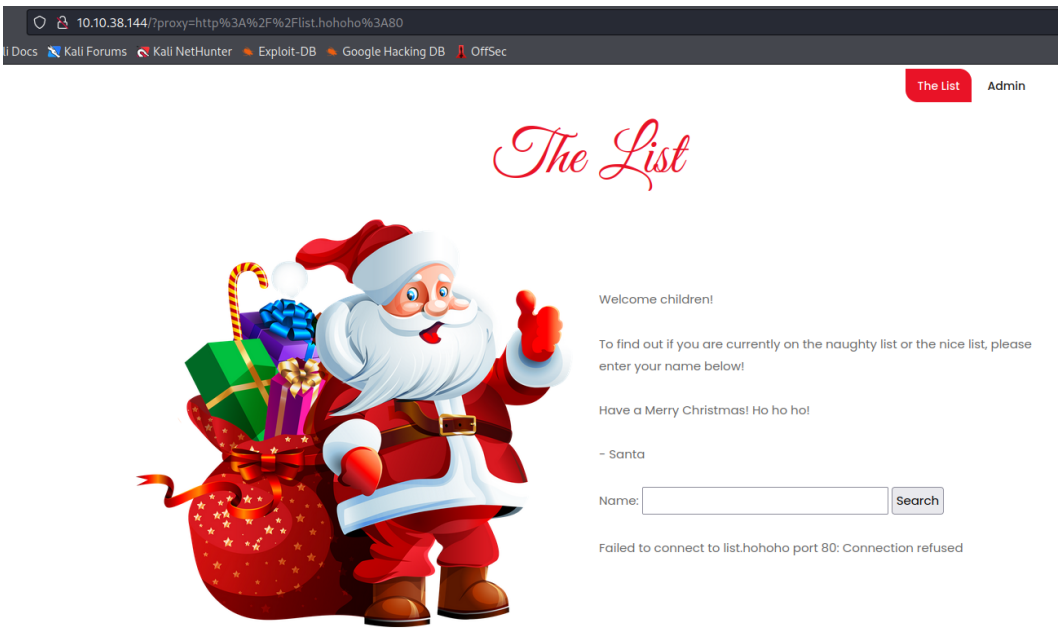
On the page, it displays the “Not Found” error.

Question 3

For this question, we can insert this url



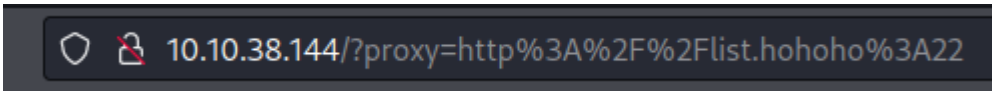
To get the respective page,



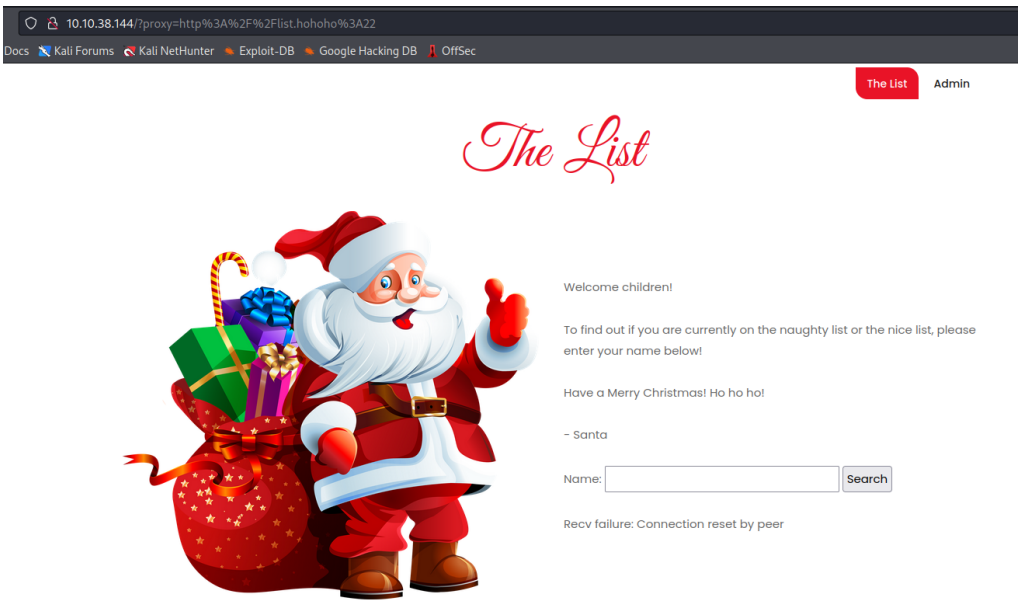
On the page it displays “Failed to connect to list.hohoho port 80: Connection refused

Question 4:

Next we can insert the url

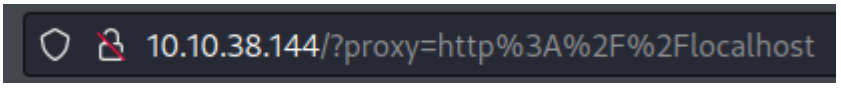


And we will get a new error message which is “Recv failure: Connection reset by peer ”

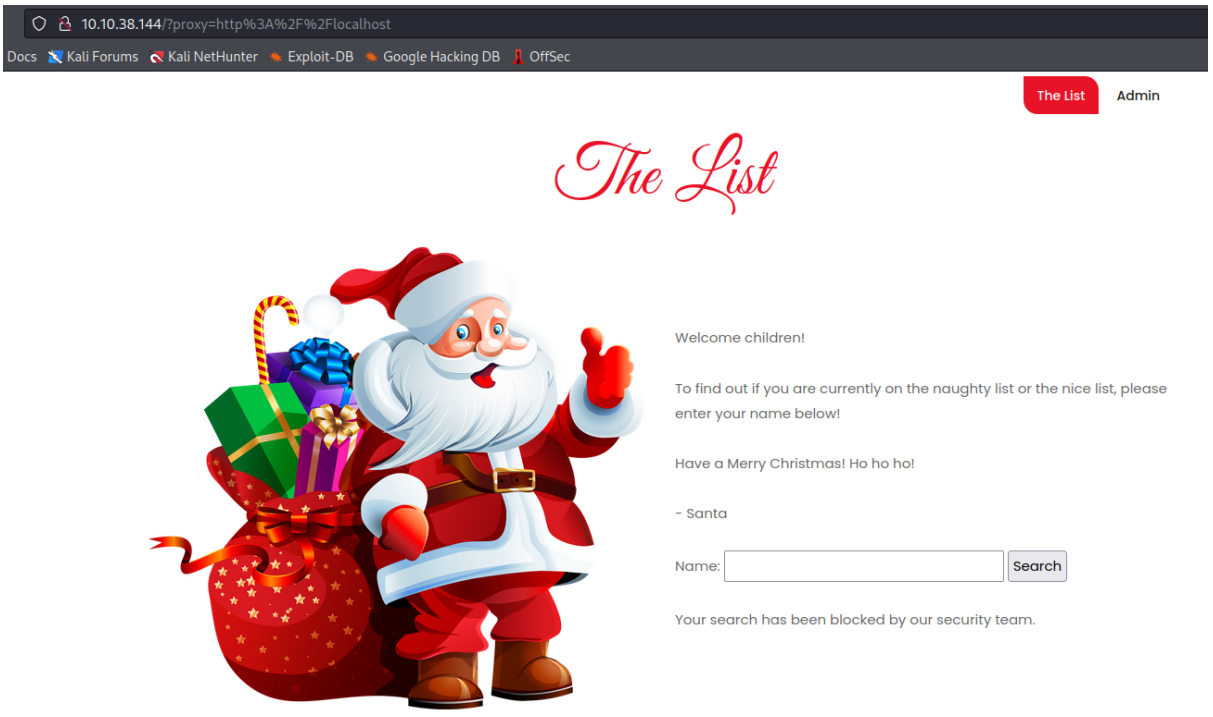


Question 5:

For the last url we need to search up,



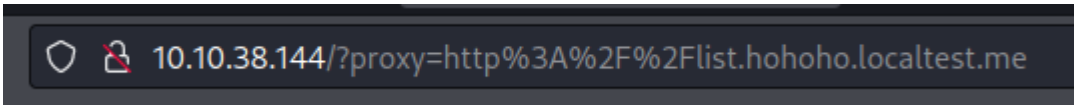
The page will display



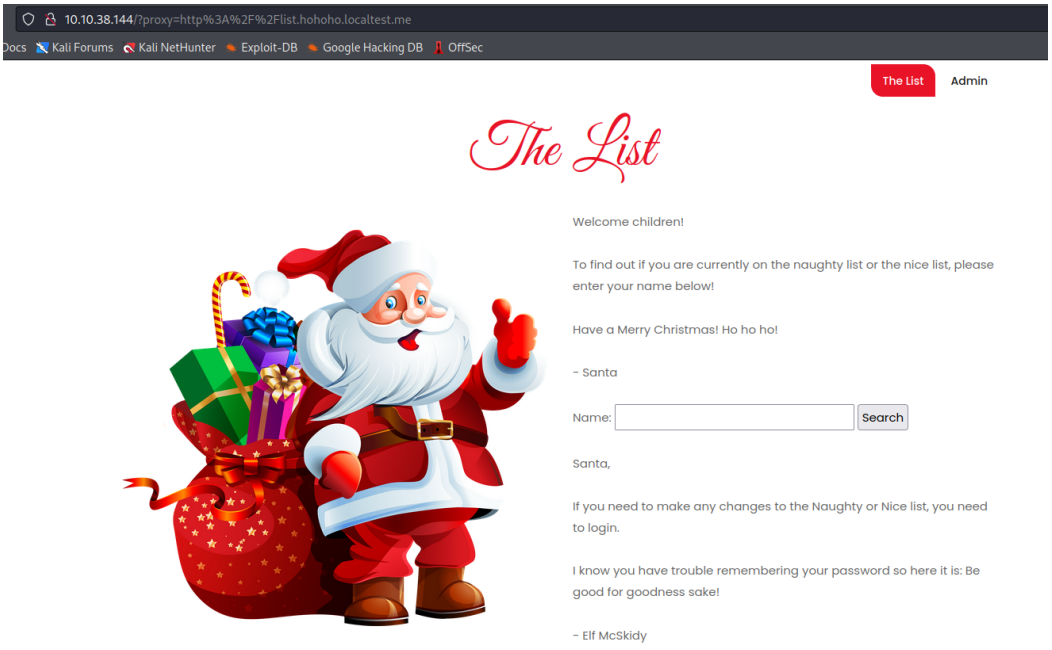
Where it says that pur search has been blocked by our security team

Question 6:

To get santa's password all we need to do is set the hostname in the URL to "list.hohoho.localtest.me"



After that, the page will display McSkidy's note to santa



In the notes McSkidy, have reminded santa of his password and thus we can use that to login with santa's account

Santa,

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

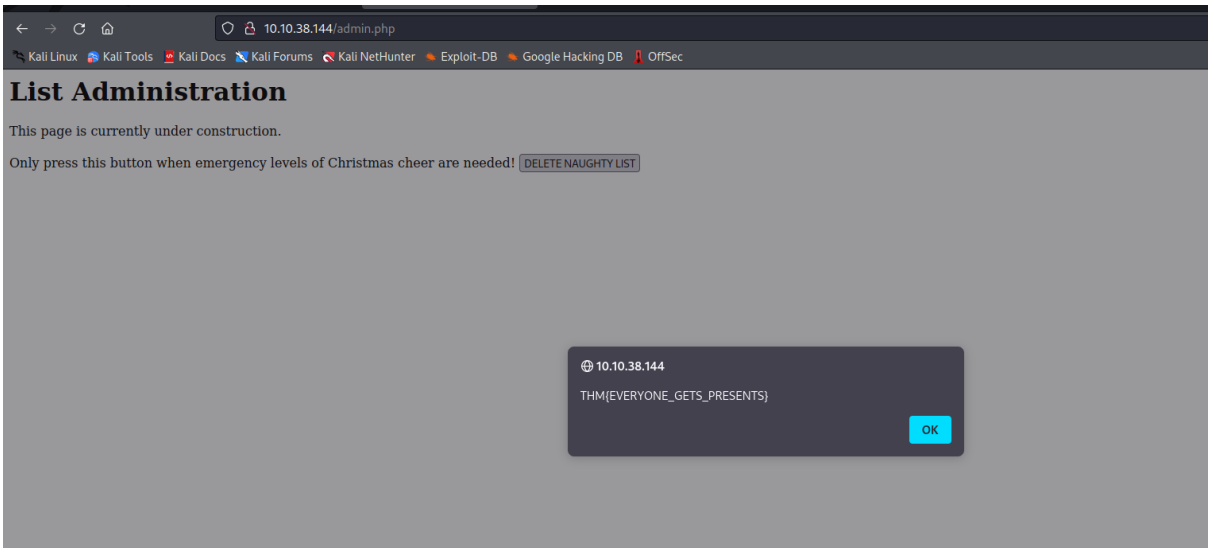
I know you have trouble remembering your password so here it is: Be good for goodness sake!

- Elf McSkidy

Question 7:

To get the challenge flag, we must first login in the admin section using santa's account

From there, we need to delete the naughty list and the flag will appear afterwards.



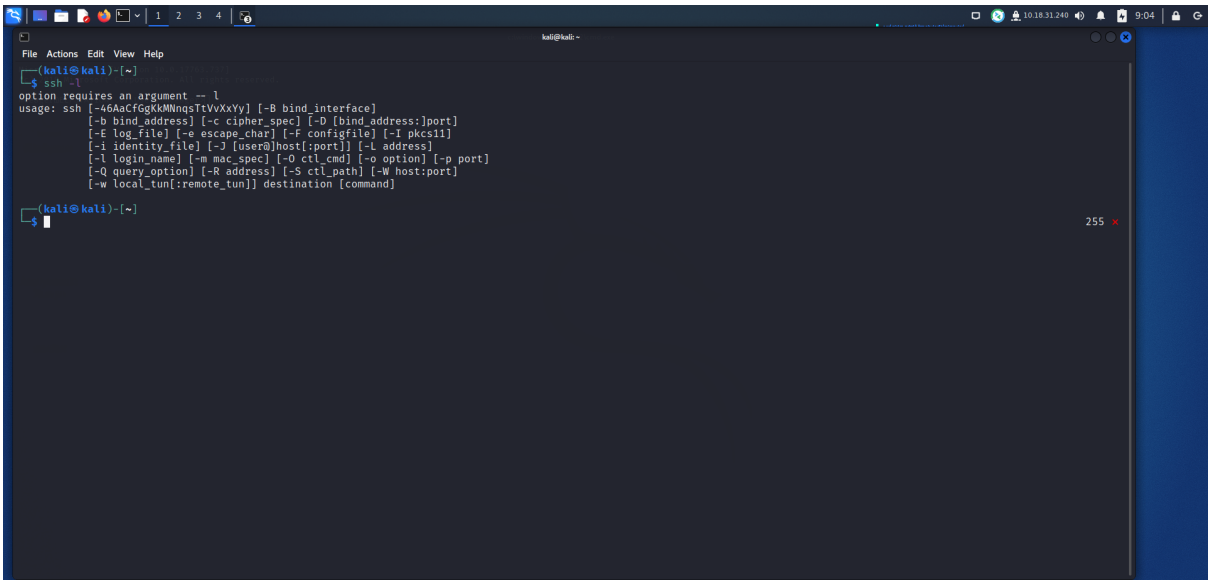
Thought Process / Methodology :

Once we open kali linux we can connect to the webapp. After that, in the website there's a search bar and inside we can search up a name. For example if we search up Tib3rius, it will tell us that the name is in the nice list. In the URL the hostname is

“list.hohoho” which is not a valid hostname. First we can browse “http://10.10.38.144/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F “ to get the root of the same site. In the place where it originally says “Tib3rius is on the nice list”it instead said “Not Found. The requested URL was not found on this server.”. This seems like an error so we can try other methods like changing the port number from 8080 to just 80, or changing the port number to 22 which is the default SSH port, or even access services running locally on the server by replacing the “list.hohoho” with “localhost”. Unfortunately, each of them comes up with a different error every time. The last thing that we could do is by creating our own domain. We can set the hostname in the URL to “list.hohoho.localtest.me”. Afterwards, we could access a message from Elf McSkidy that contained Santa's passwords. With this, we can now log in as admin using santa’s account and delete the naughty list to get the challenge flag.

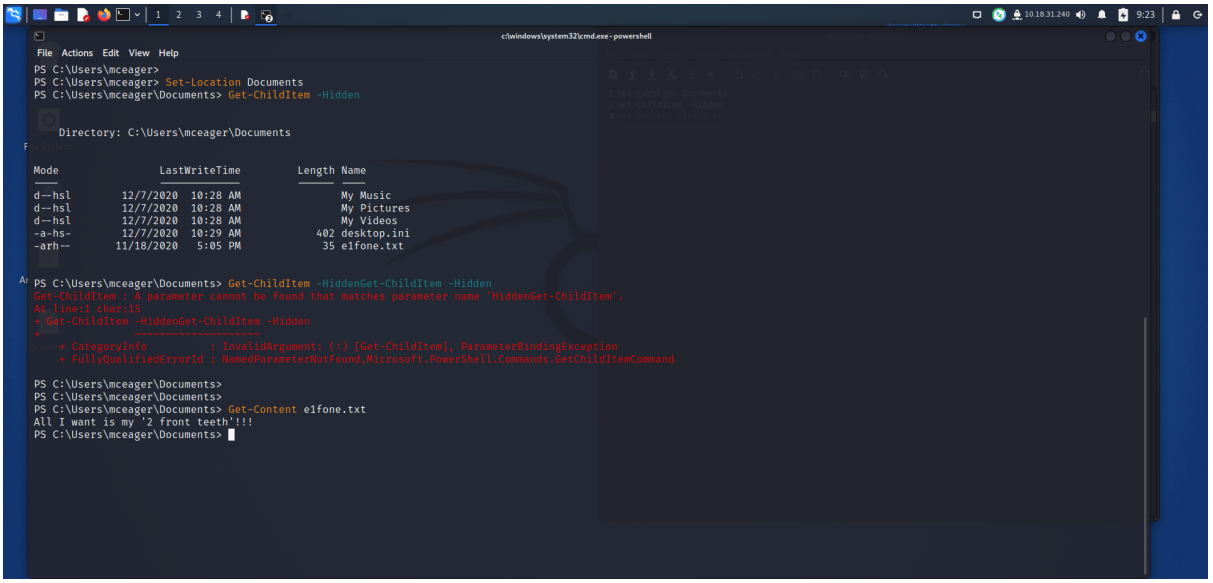
Day 20- [Blue Teaming] PowershELIF to the rescue
Tool used: Kali Linux
Solution/walkthrough:

Question 1:



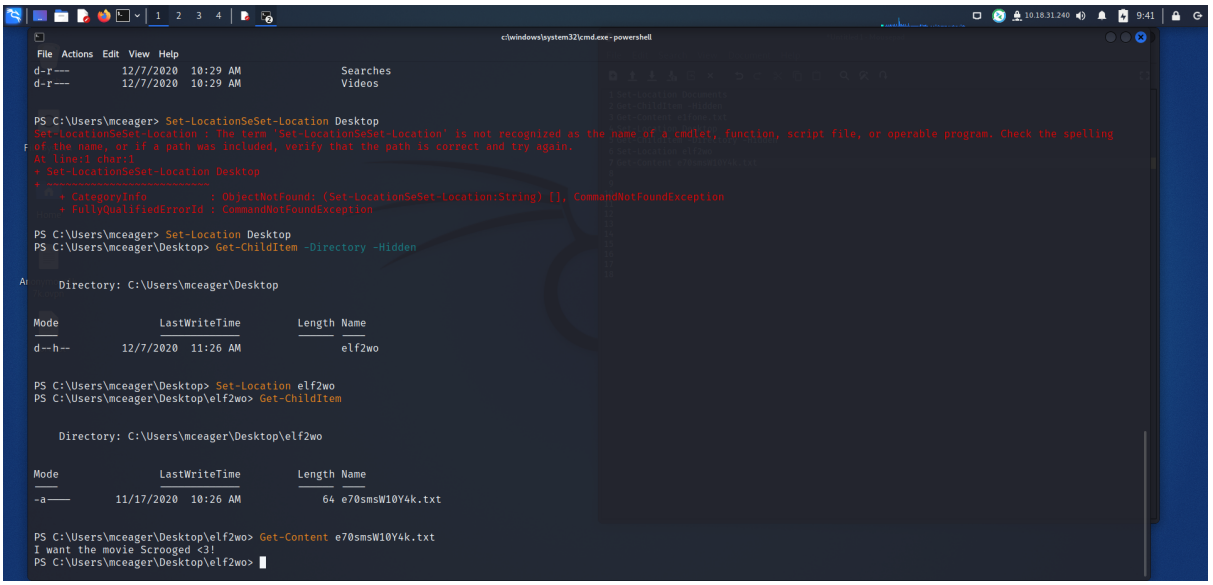
Open the terminal Type ssh -l and you search for it

Question 2:



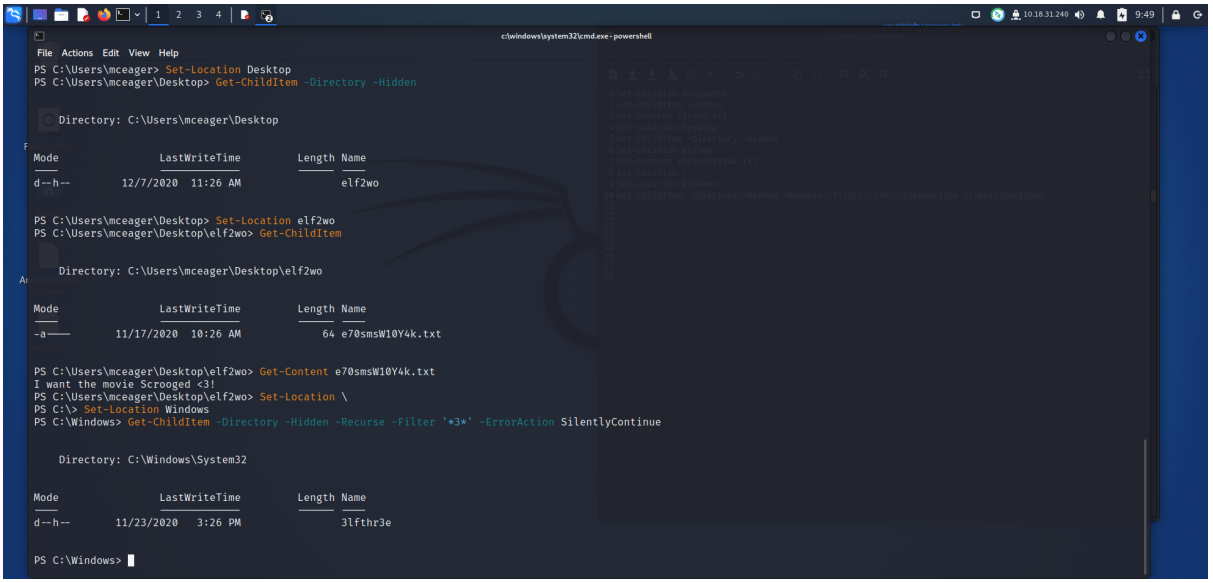
In the powershell, Type Set-Location Documents, then type Get-ChildItem -Hidden. You will set the list. Type Get-Content elfone.txt and you will get the answer.

Question 3:



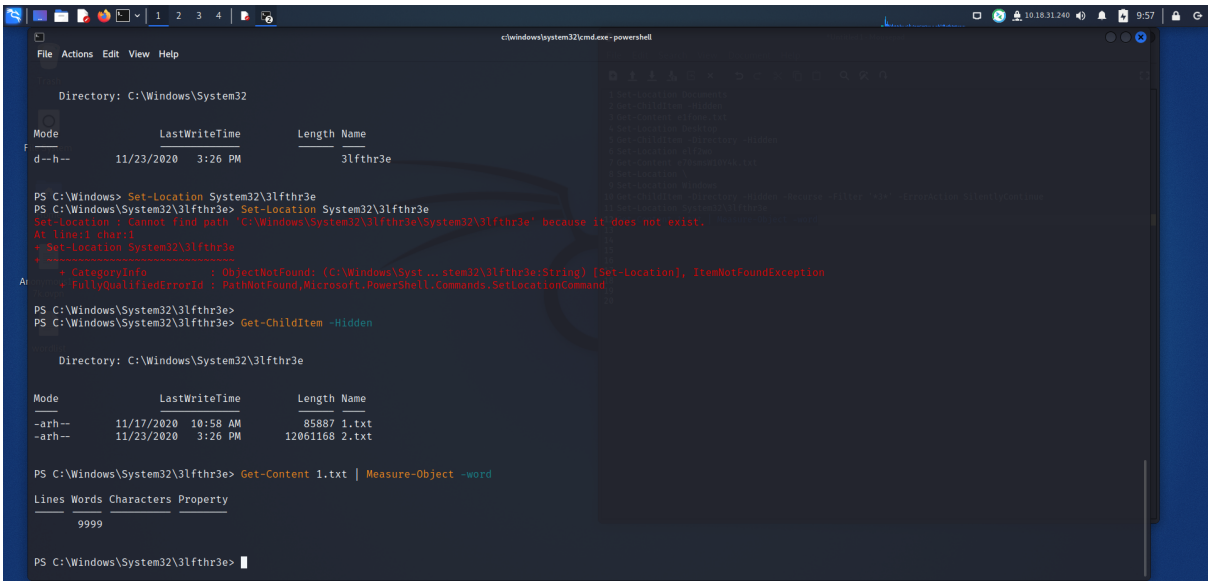
Set your directory to desktop, and find the hidden folder for elf 2. Read the content of the file by using Get-Content.

Question 4:



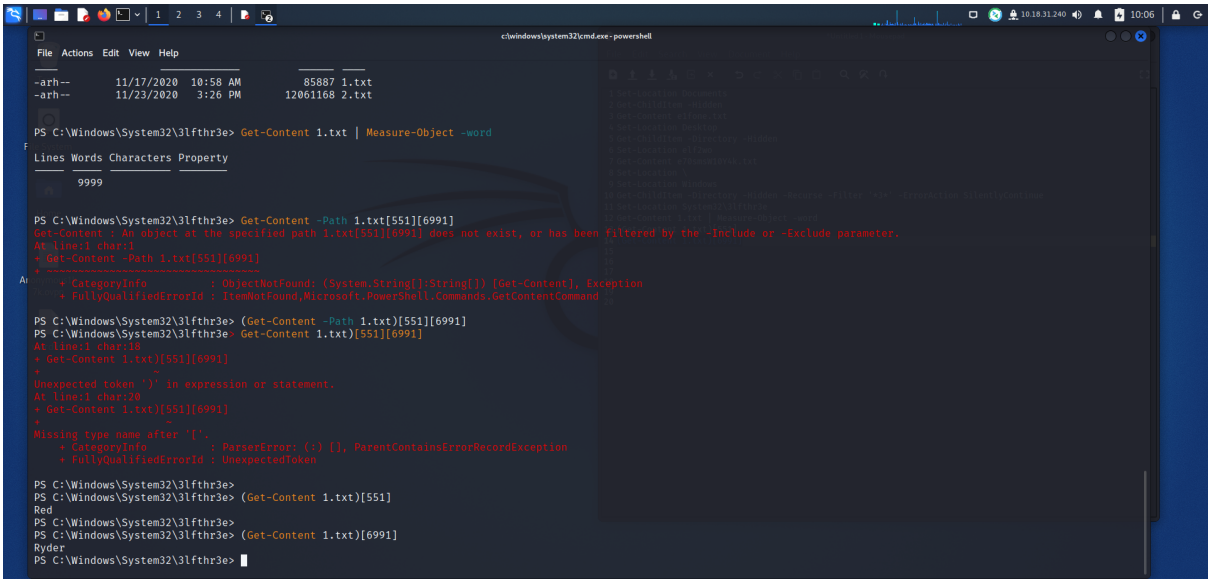
Set your directory to Window,then and find the hidden folder for Elf 3 by typing Get-ChildItem -Directory -Hidden -Recurse -Filter '*3*' -ErrorAction SilentlyContinue

Question 5:



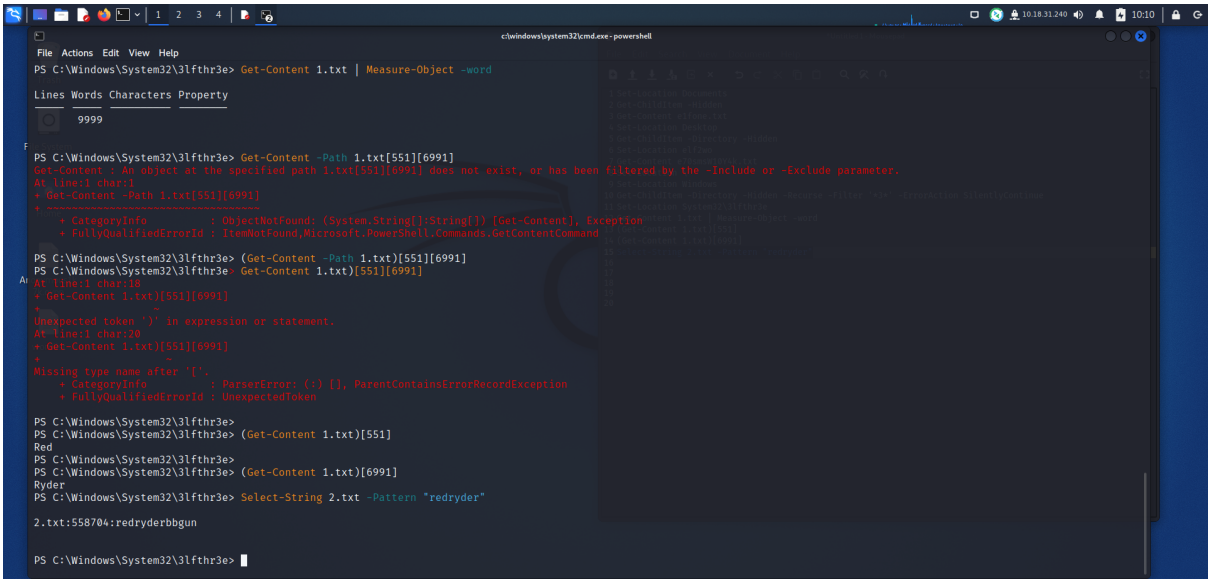
After found out the folder, Set you directory to the hidden folder, and get the number of words by typing Get-Content 1.txt | Measure-Object -word

Question 6:



To find the word, type (Get-Content 1.txt)[551] and (Get-Content 1.txt)[6991]

Question 7:



To find the answer, type Select-String 2.txt -Pattern "redryder"

Thought Process / Methodology :

Use PowerShell to first reveal the majority of files within documents, including hidden files. To complete this work, we were required to locate the concealed content in the subject file, Elf. We can locate the file's location and specific contents using the command directory list. As a result, there are several hidden folder names that can be accessed by various command directories. The last two words, which were from the index numbers 551 and 6991, are displayed in the first and second files respectively. Finally, utilising PowerShell inside the Concealed Files module, we

were able to complete the entire file directory and any content that was hidden therein.