PSP0201
WEEK 5
WRITEUP

Group Name: Draco Malfoy

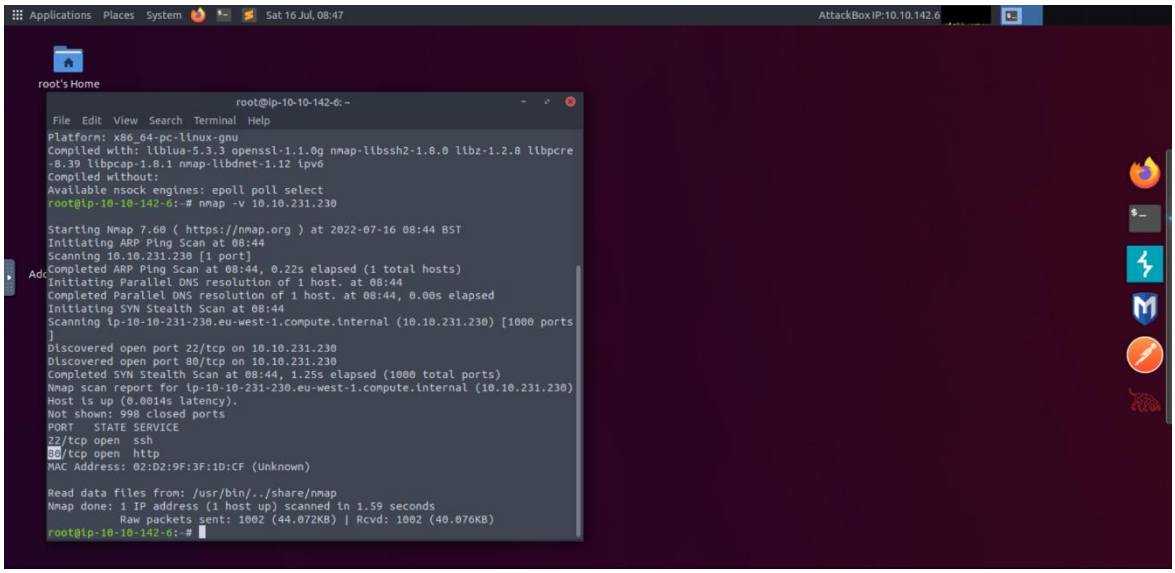
Aqra Alisa binti Rashidi	1211103093
Nurul Aqilah binti Mohd Shariff	1211103097
Nur Inqsyira binti Zamri	1211103098
Siti Nur Amirah binti Zuraihan	1211102093

Day 16: Help! Where is Santa?

Tools: firefox, nmap python3, requests, sublime text

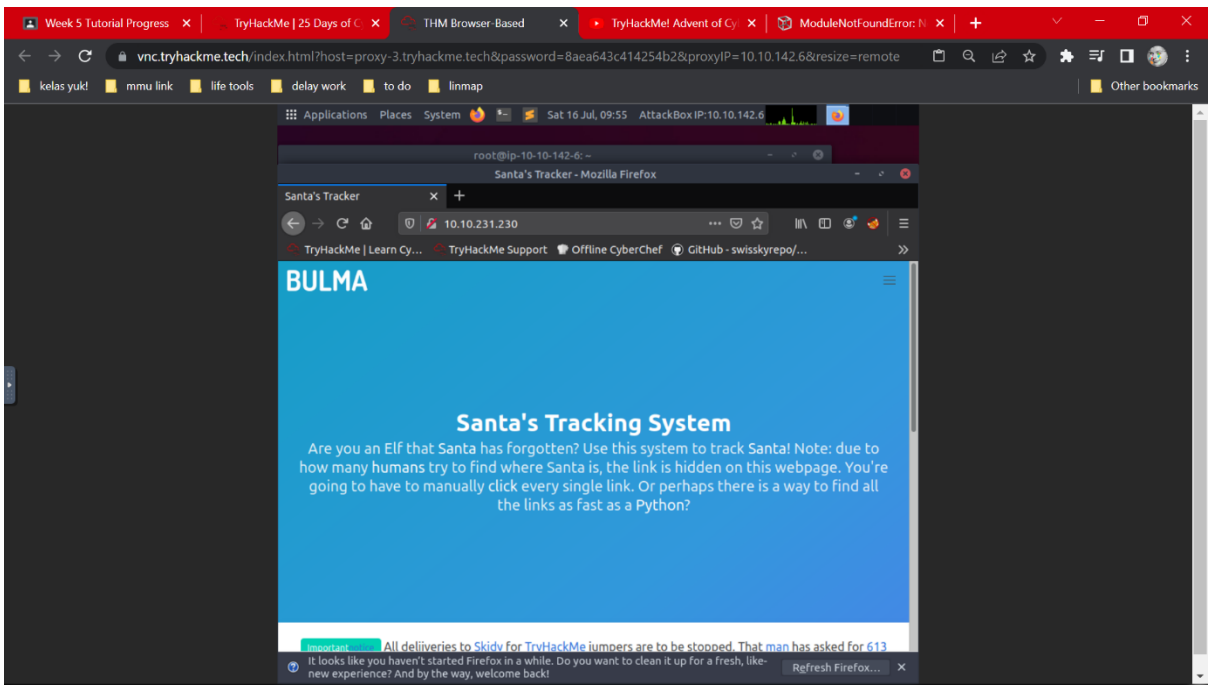
Q1: What is the port number for the web server?

=80



Q2: What templates are being used?

=BULMA

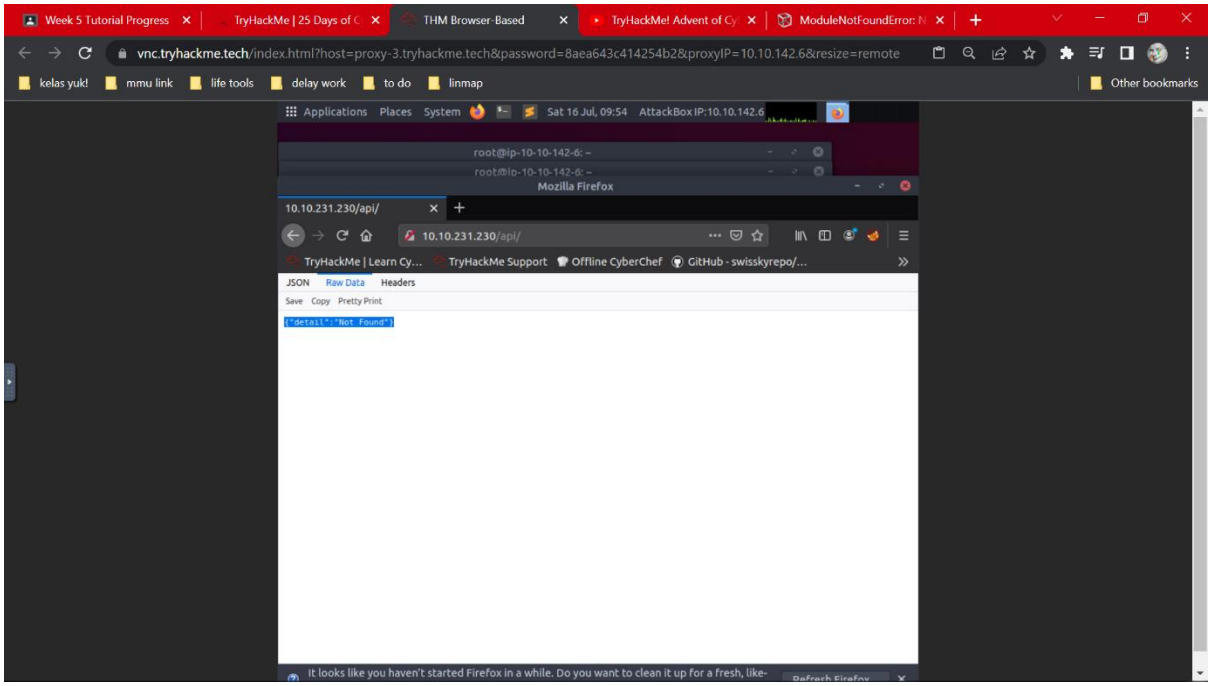


Q3: Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)

=/api/

Q4: Go the API endpoint. What is the Raw Data returned if no parameters are entered?

= {"detail":"Not Found"}

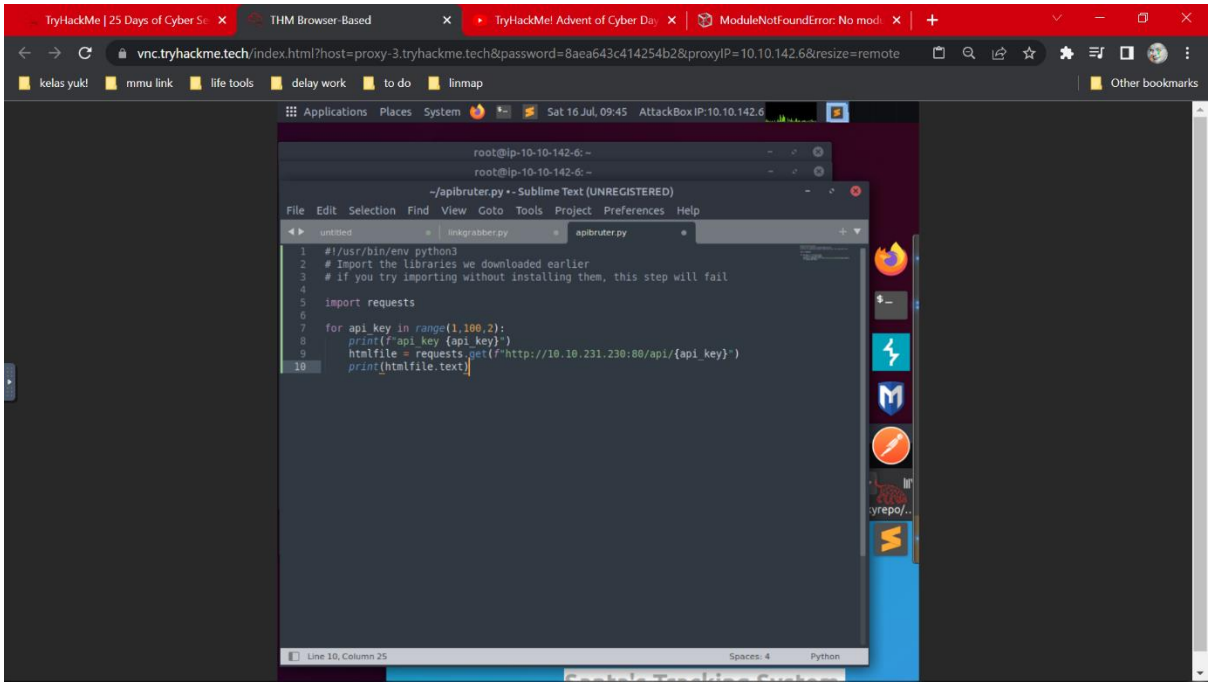


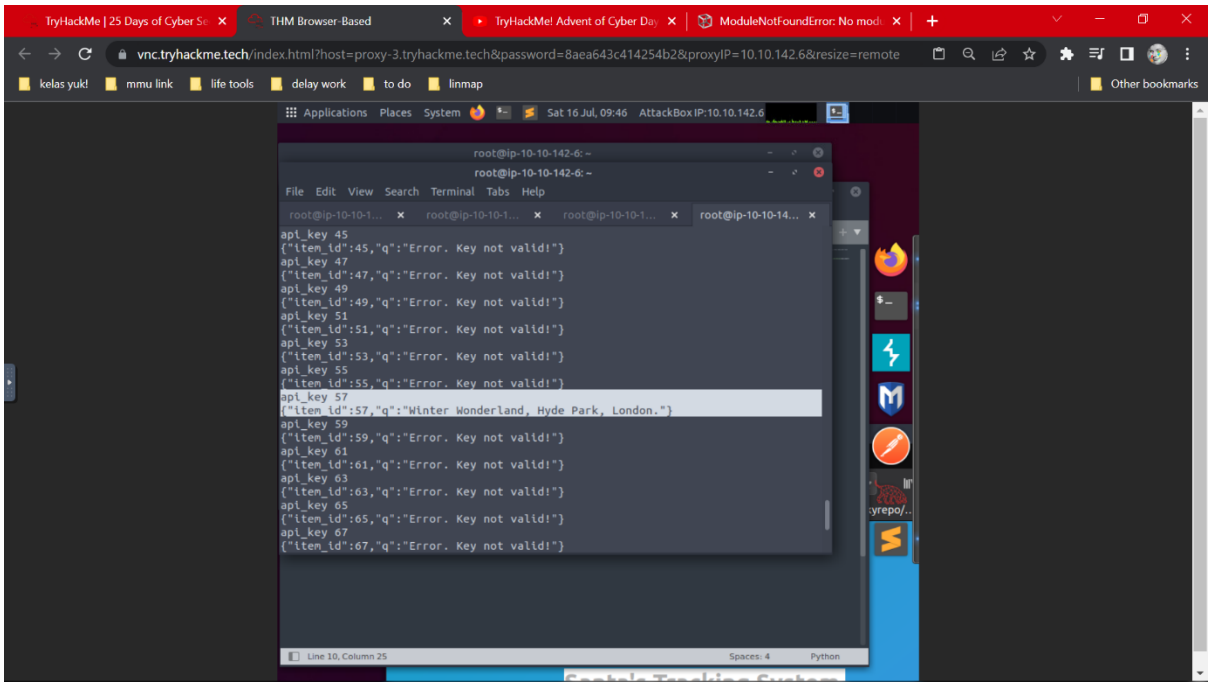
Q5: Where is Santa right now?

= { Winter Wonderland, Hydre Park, London }

Q6: Find out the correct API key. Remember, this is an odd number between 0-100

=57





Methodology (Day16):

To begin with, we scanned for available port using nmap. Turns out, it shows port: 80. We then continue browsing to the firefox and finds out BULMA as the template used. Next, we go to /api/ default and heads to raw tab to get the raw data. Moreover, we use python3 to find out the correct API key by creating apibruter.py file for the python code. Open the file using command “python3 our-file-name” and we now obtain the correct API key as well as the location of Santa.

Day 17: Reverse ELFneering

Tools: terminal, ssh radare2

Q1: Match the 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

Q2: What is the command to analyse the program in radare2?

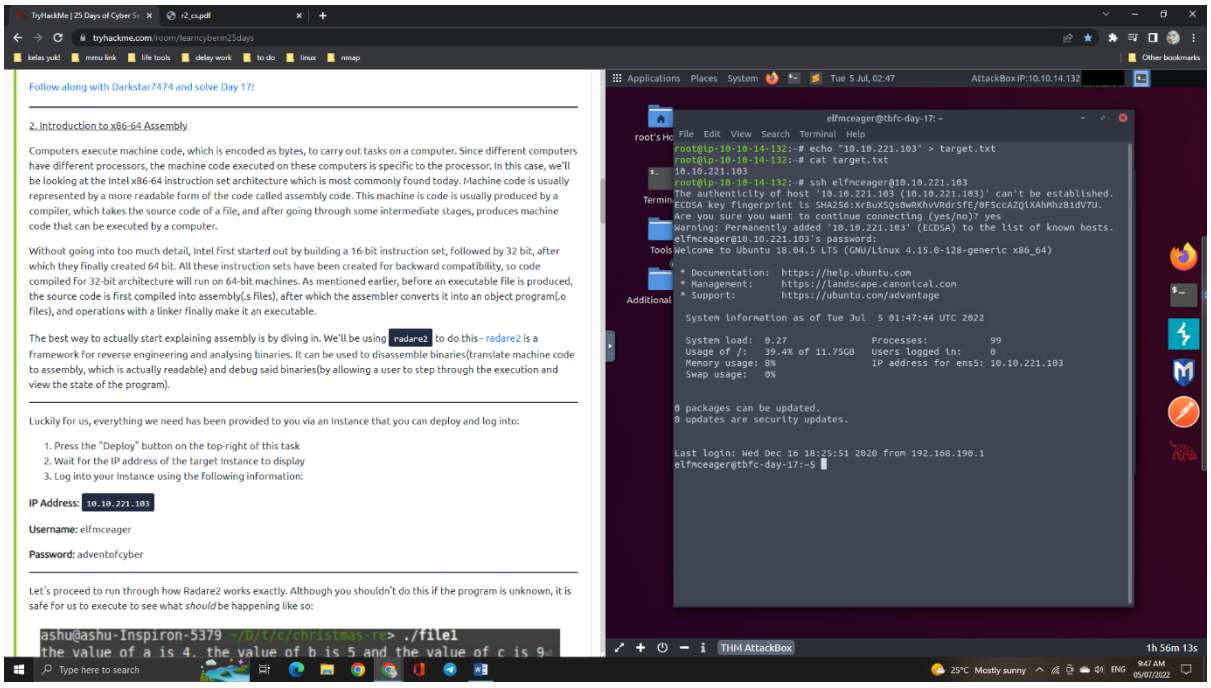
= aa

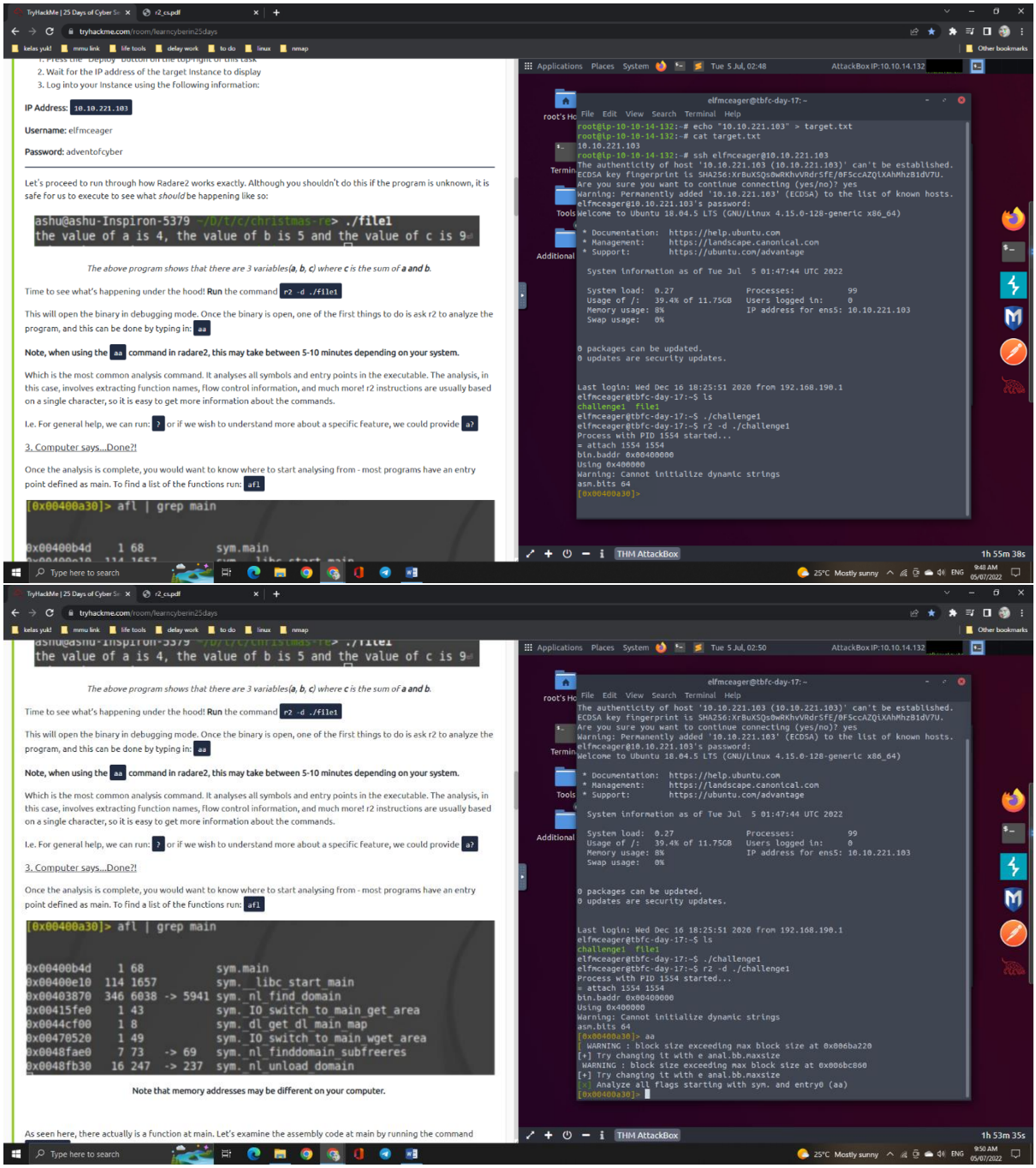
Q3: What is the command to set a breakpoint in radare2?

=db

Q4: What is the command to execute the program until we hit a breakpoint?

=dc





Q5: What is the value of local_ch when its corresponding movl instruction is called (first if multiple)?

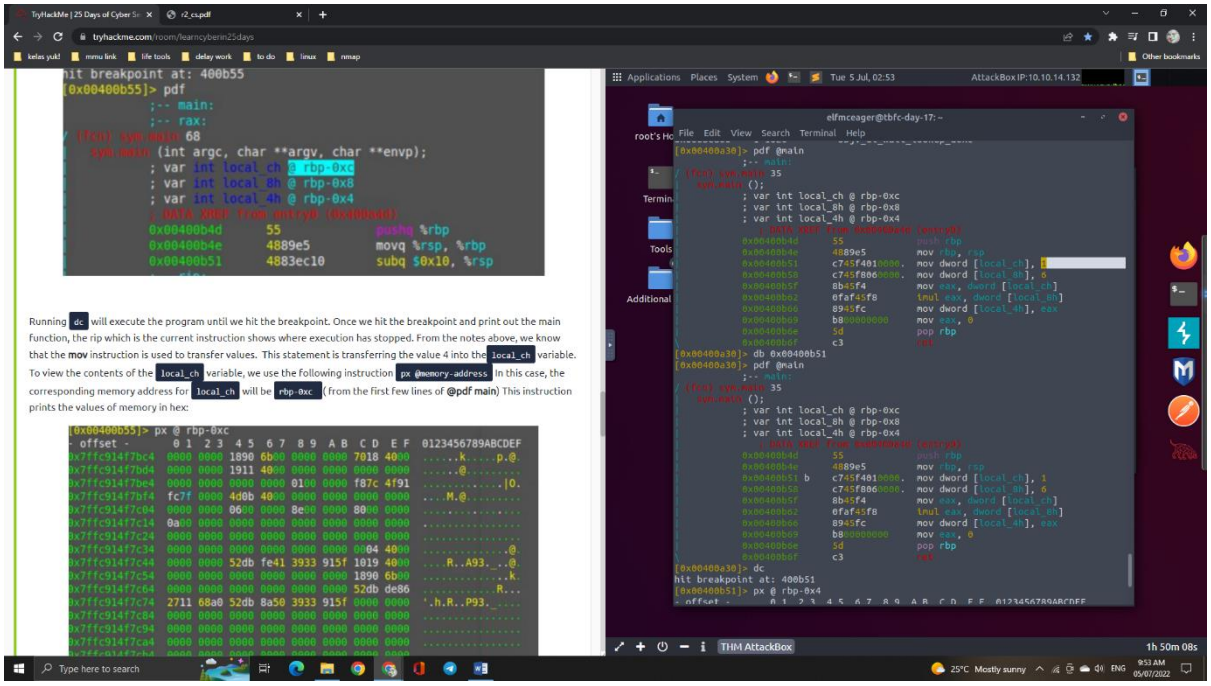
= 1

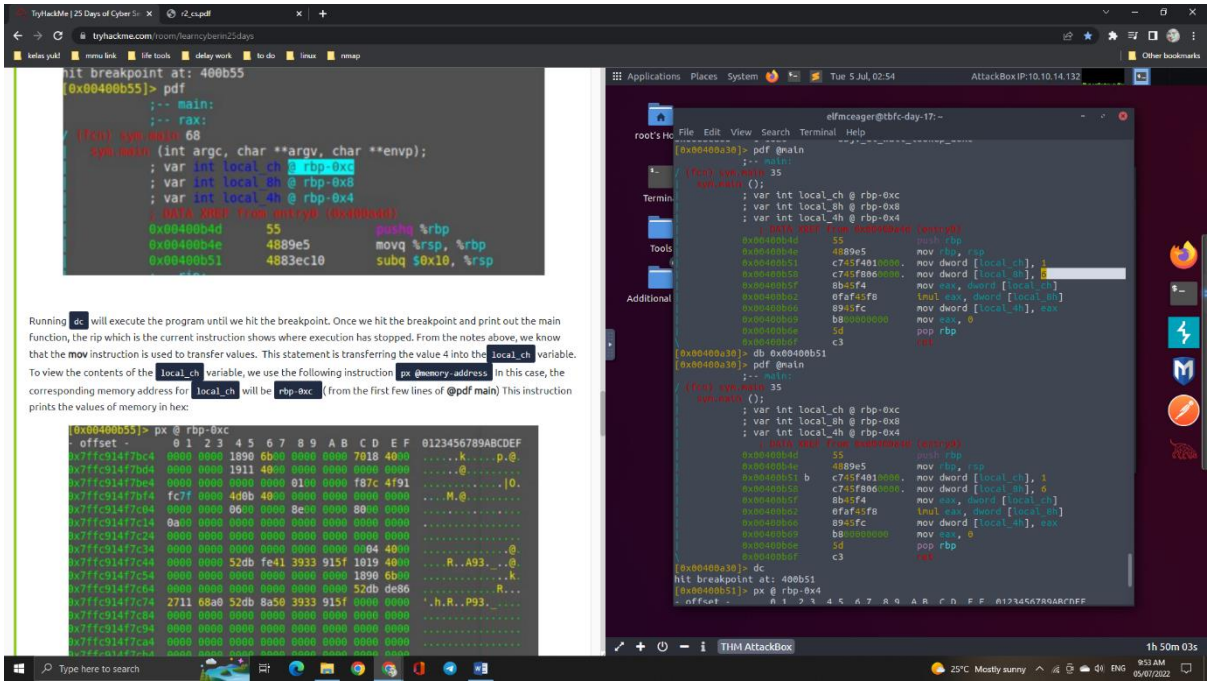
Q6: What is the value of eax when the imull instruction is called?

=6

Q7: What is the value of local_4h before eax is set to 0?

=6





Methodology (Day17):

First, we login using ssh with the information provided. We then get the list of programme using ls command. Then, we analyse the programme (challenge1) using aa command. Next,

we are using pdf@main command to examine the assembly code at main. After that, we are supposed to get the answer for the rest of question by reading the current assembly code.

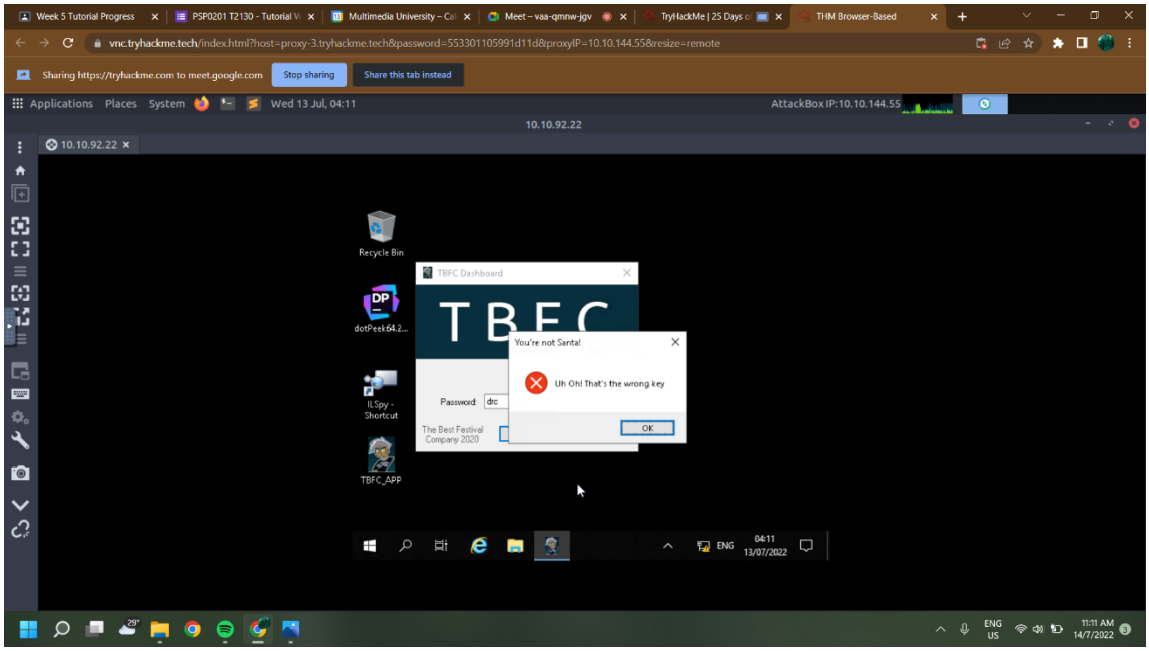
DAY 18: [Reverse Engineering] The Bits of Christmas

Tools: Attackbox

Question 1

Q1: What is the message that shows up if you enter the wrong password for TBFC_APP?

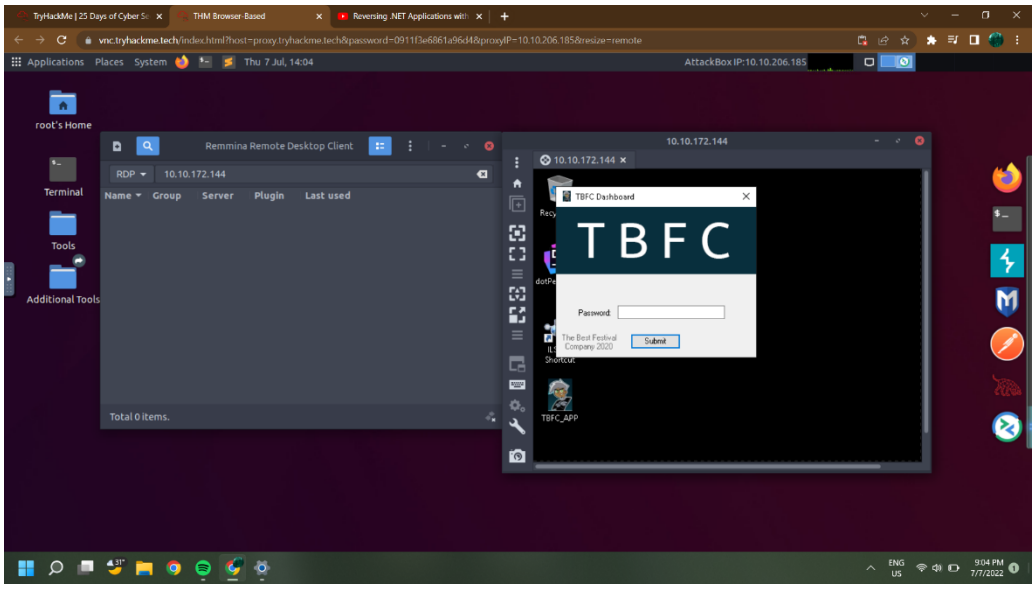
= Uh Oh! That's the wrong key



Question 2

Q2: What does TBFC stand for?

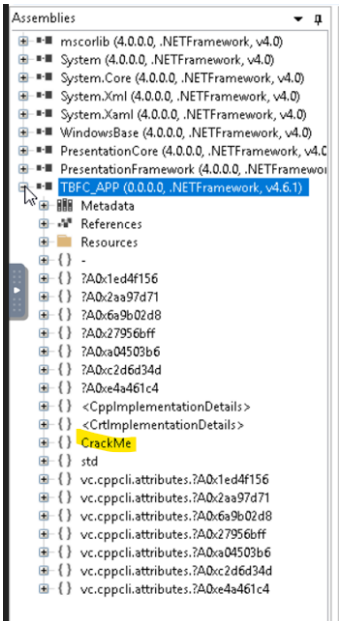
= The Best Festival Company



Question 3

Q3: Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?

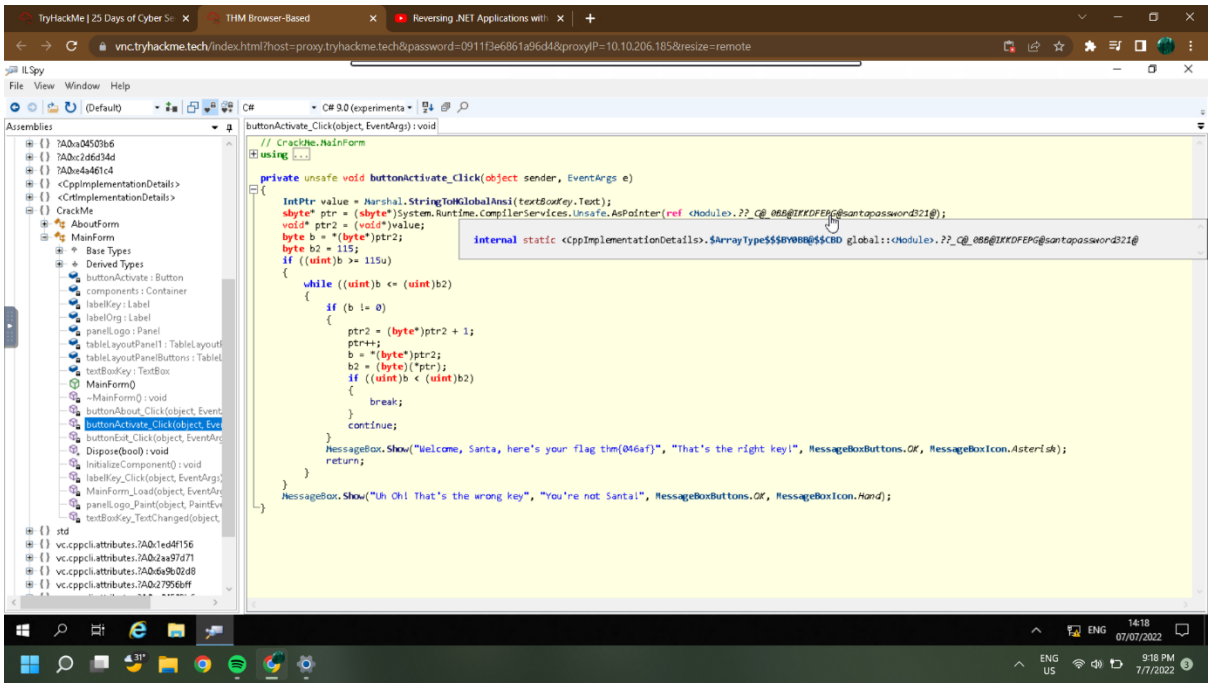
=CrackMe



Question 4

Q4: Within the module, there are two forms. Which contains the information we are looking for?

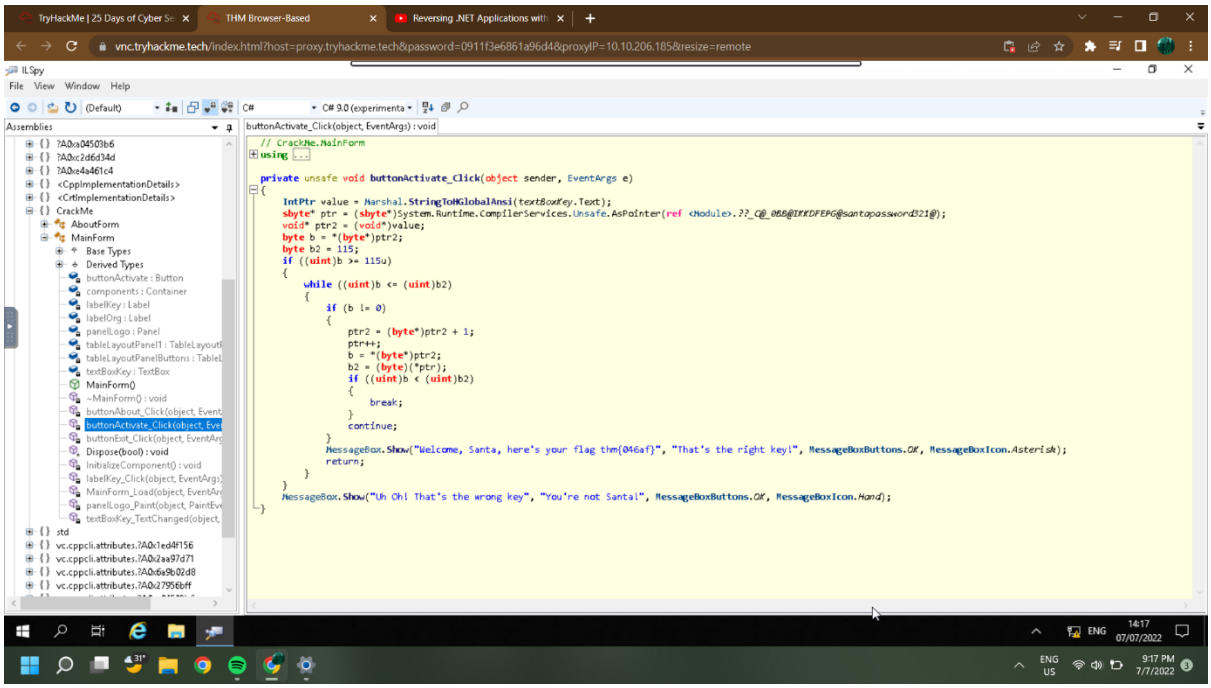
=MainForm



Question 5

Q5: Which method within the form from Q4 will contain the information we are seeking?

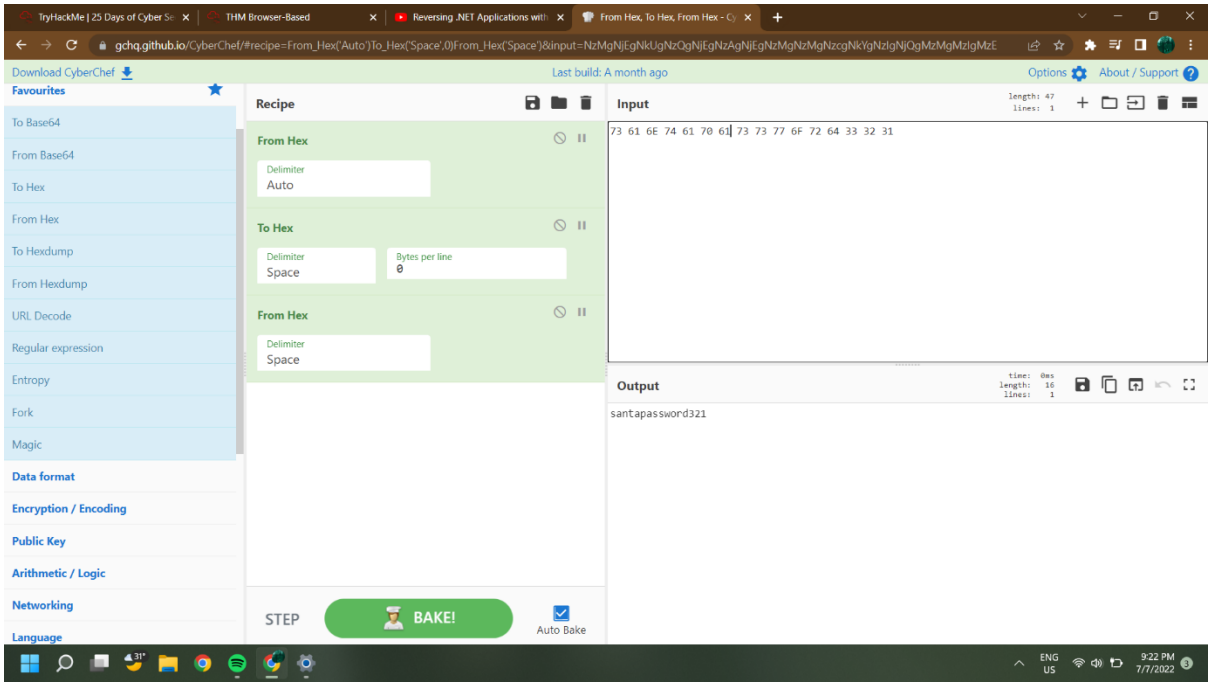
= buttonActivate_Click



Question 6

Q6: What is Santa's password?

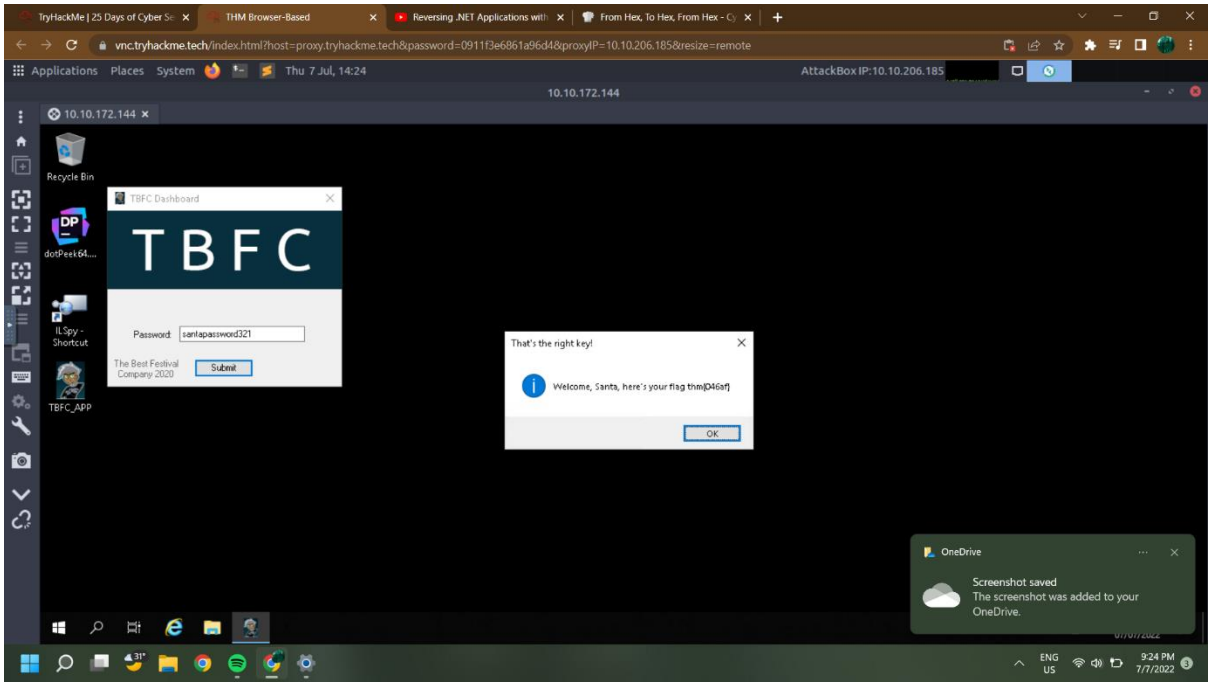
=santapassword321



Question 7

Q7: Now that you've retrieved this password, try to login...What is the flag?

= thm{046af}



Methodology (Day 18):

First and foremost, we deploy our machine and the respective AttackBox. Next, we navigate to the "Applications" tab on the AttackBox where "Remmina" is located in the "Internet" sub-menu. Reminna asked for a password to save sessions, we safely press "Cancel". Now we filled the IP address of the target Instance that we have deployed, input the Username and password provided and set the "Color depth" to "RemoteFX (32 bpp).

Username: cmnatic

Password: Adventofcyber!

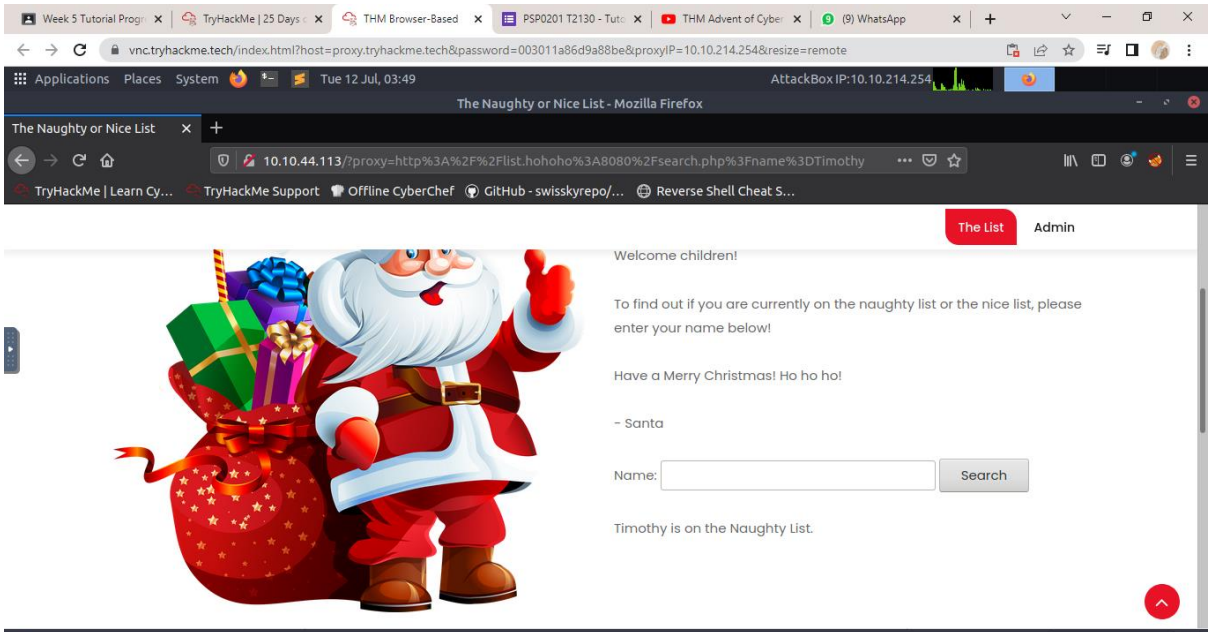
Subsequently, we open the TBFC App and tried to log in but failed. So we navigate to the ILSpy to do some hacking. We open the "TBFC_APP" application in ILspy and begin decompiling the code. In there, we successfully received the needed password and flag.

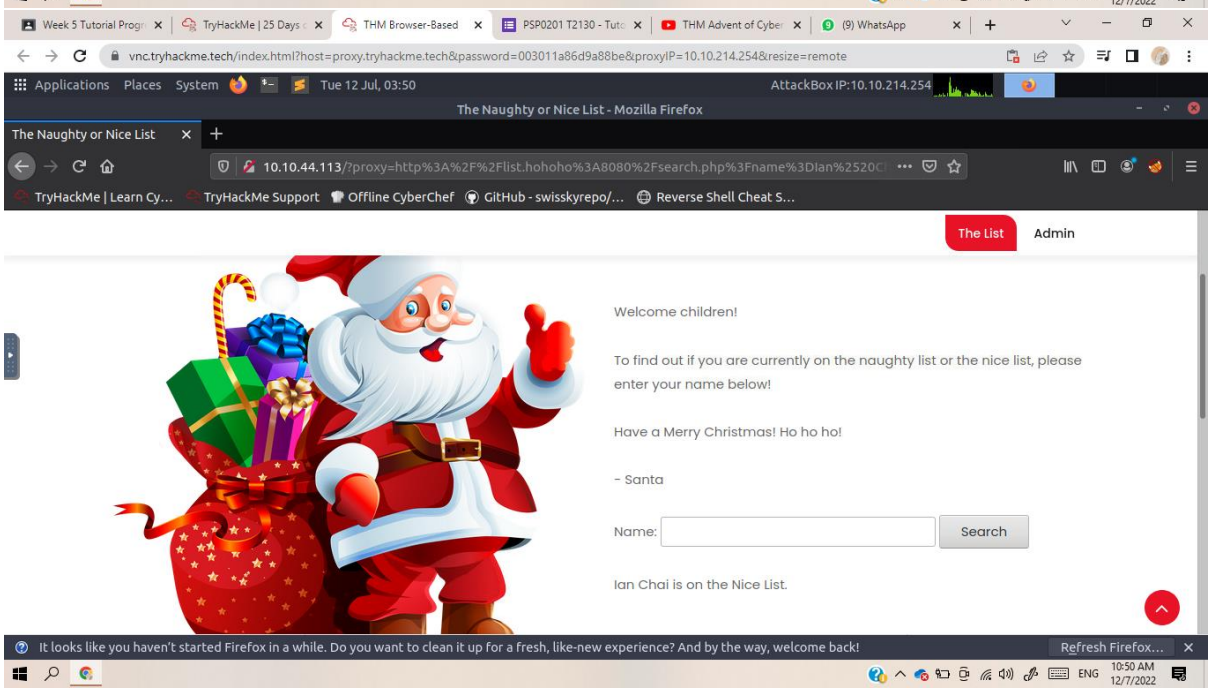
DAY 19 : [Web Exploitation] The Naughty or Nice List

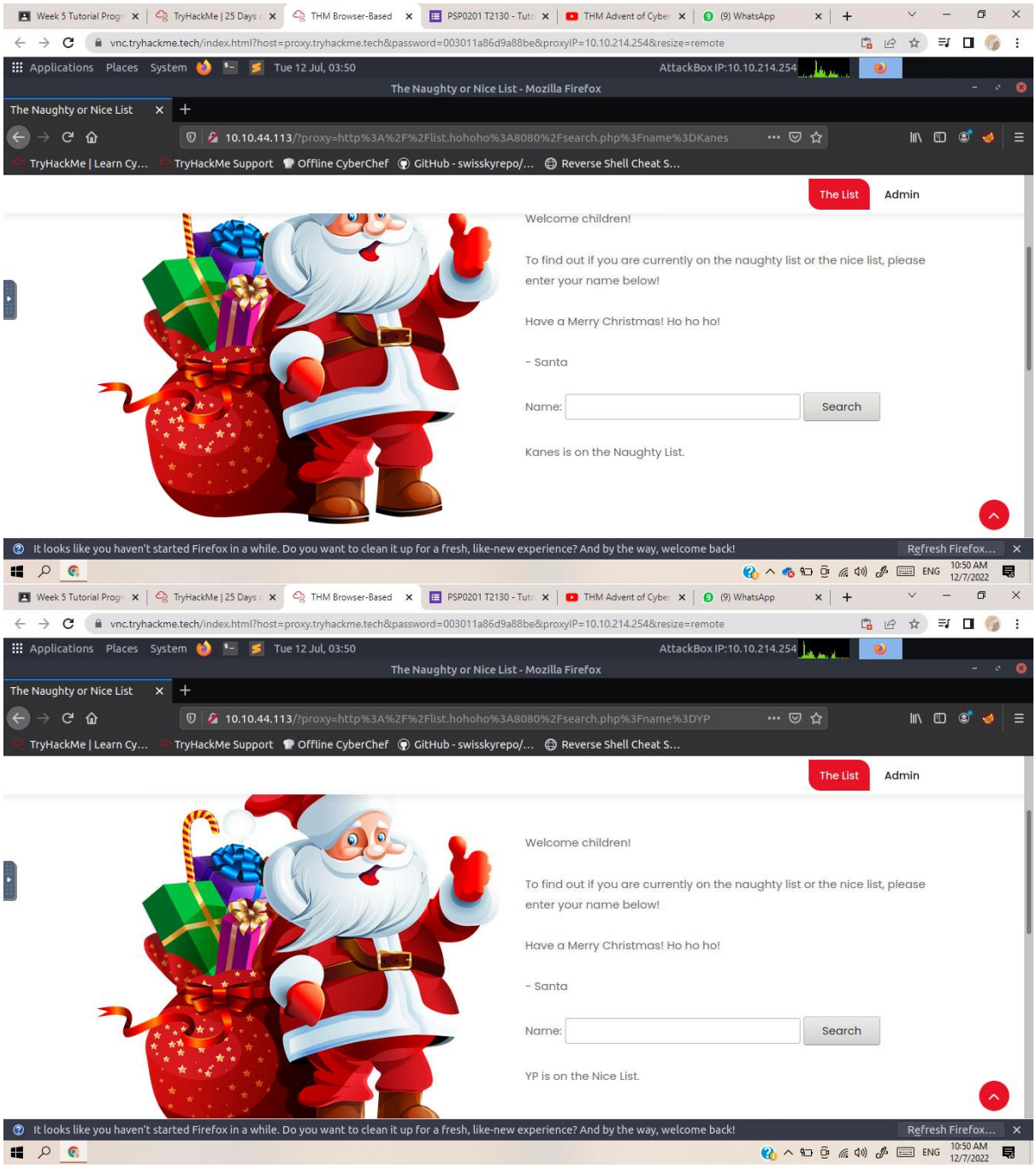
Tools : Firefox

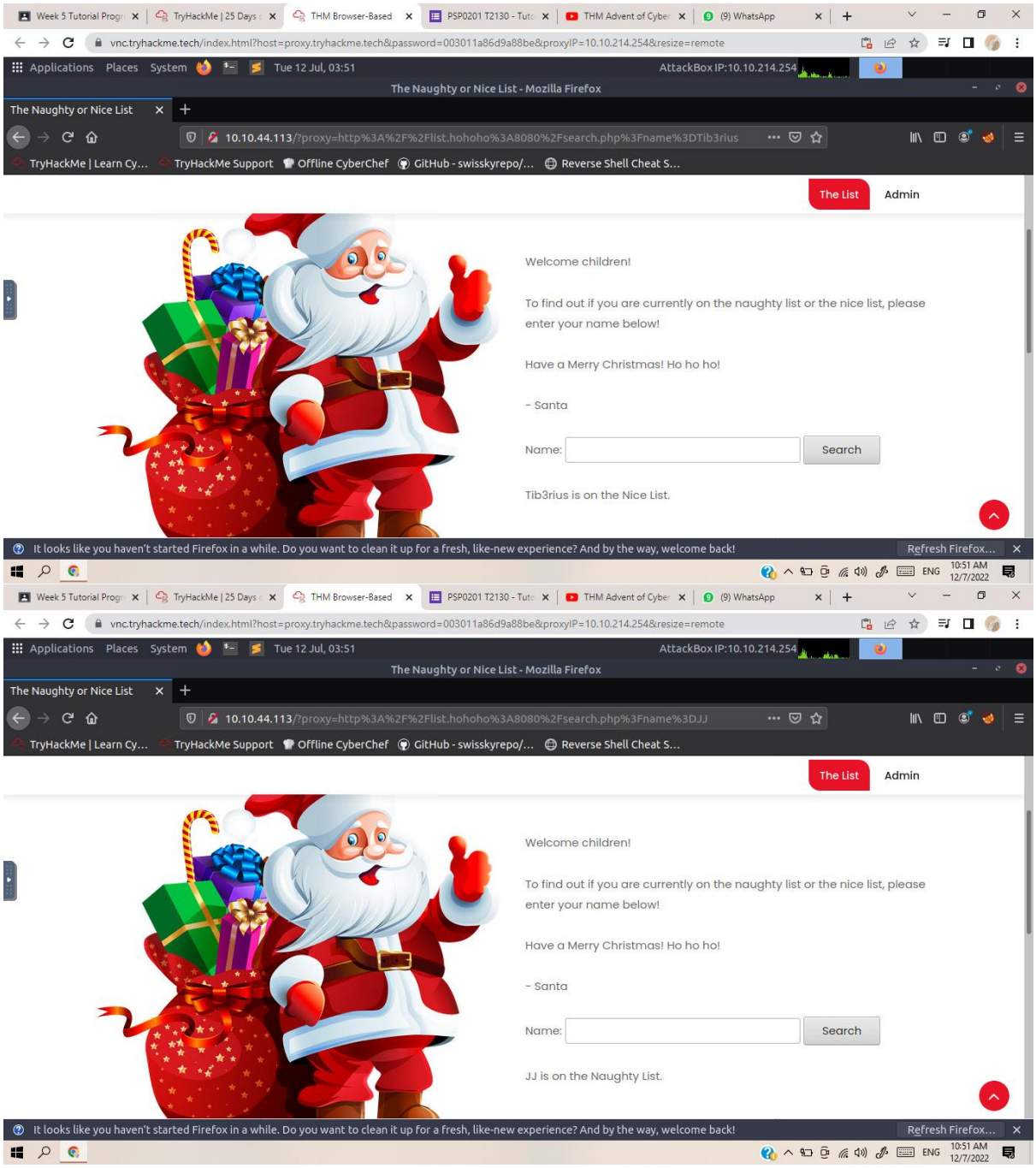
Question 1:

Q1: Which list is this person on?





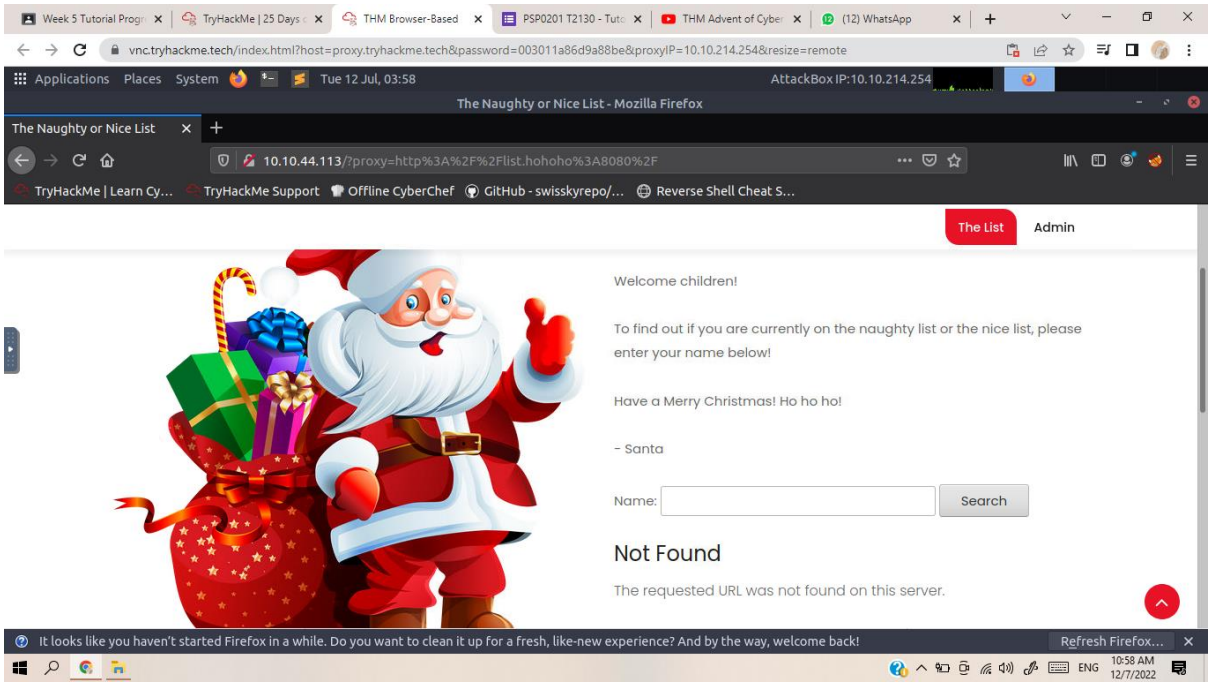

The Naughty or Nice List - Mozilla Firefox
10.10.44.113/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DKanes
The List
Admin
Welcome children!
To find out if you are currently on the naughty list or the nice list, please enter your name below!
Have a Merry Christmas! Ho ho ho!
- Santa
Name:
Search
Kanes is on the Naughty List.
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
The Naughty or Nice List - Mozilla Firefox
10.10.44.113/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DYP
The List
Admin
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.
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...


The Naughty or Nice List - Mozilla Firefox
10.10.44.113/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DTib3rius
The List
Admin
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.
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
The Naughty or Nice List - Mozilla Firefox
10.10.44.113/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DJJ
The List
Admin
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.
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...

Question 2:

Q2: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?

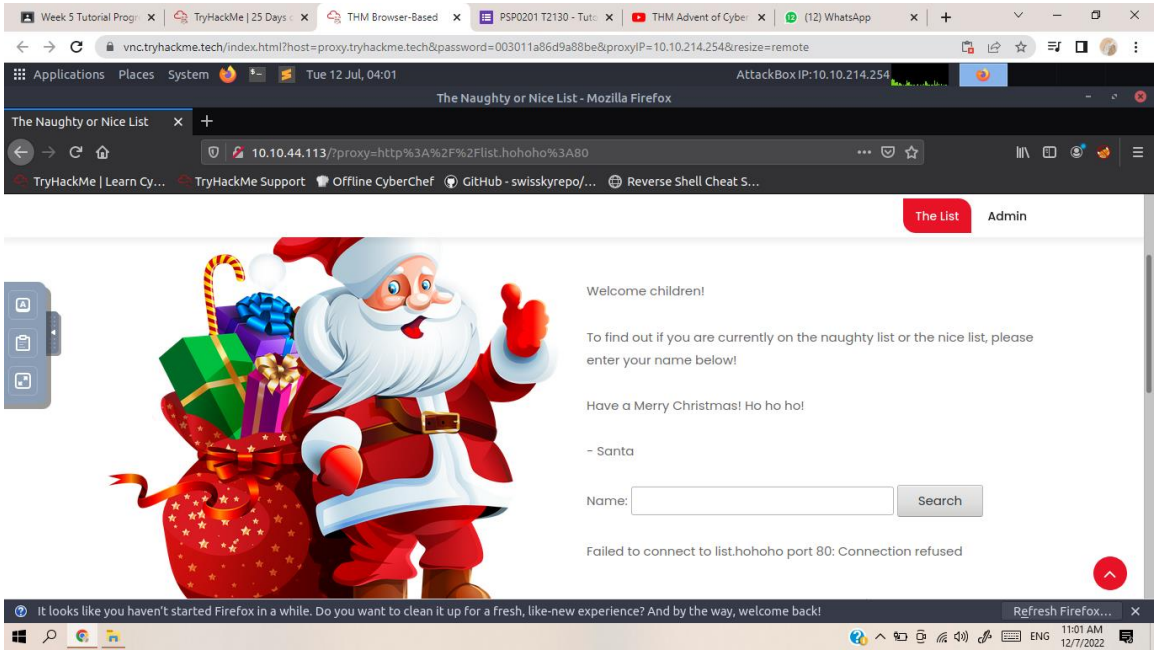
= The requested URL was not found on this server.



Question 3:

Q3: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"?

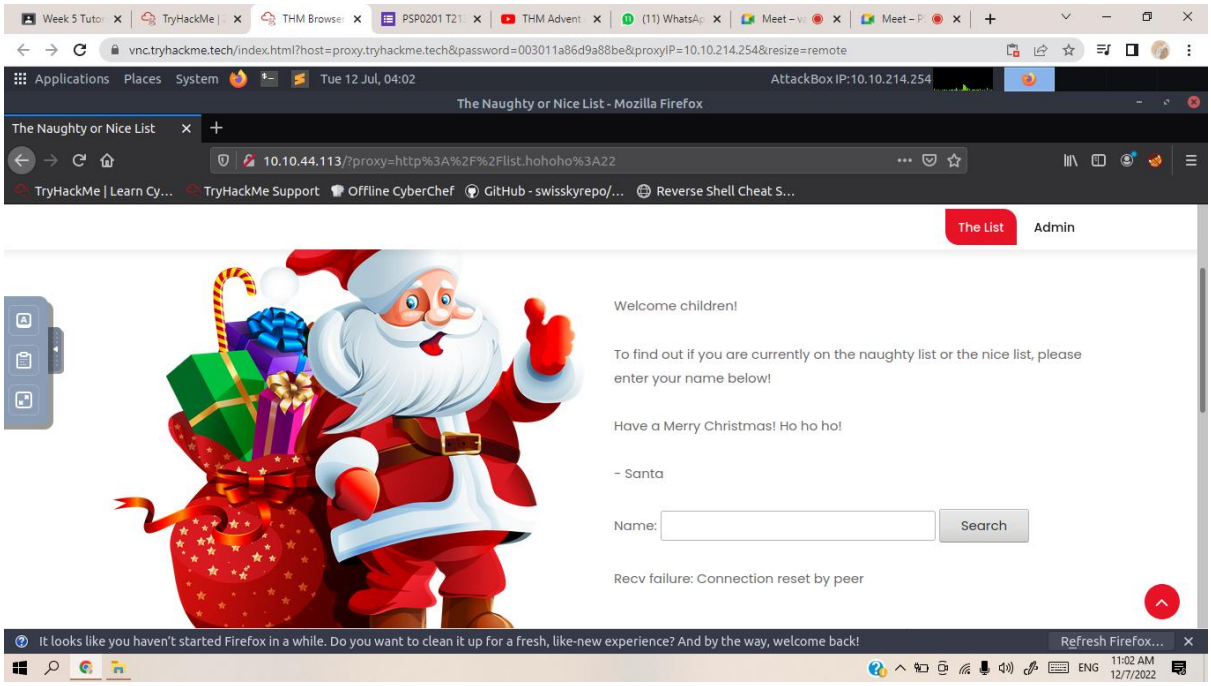
= Failed to connect to list.hohoho port 80: Connection refused



Question 4 :

Q4: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"?

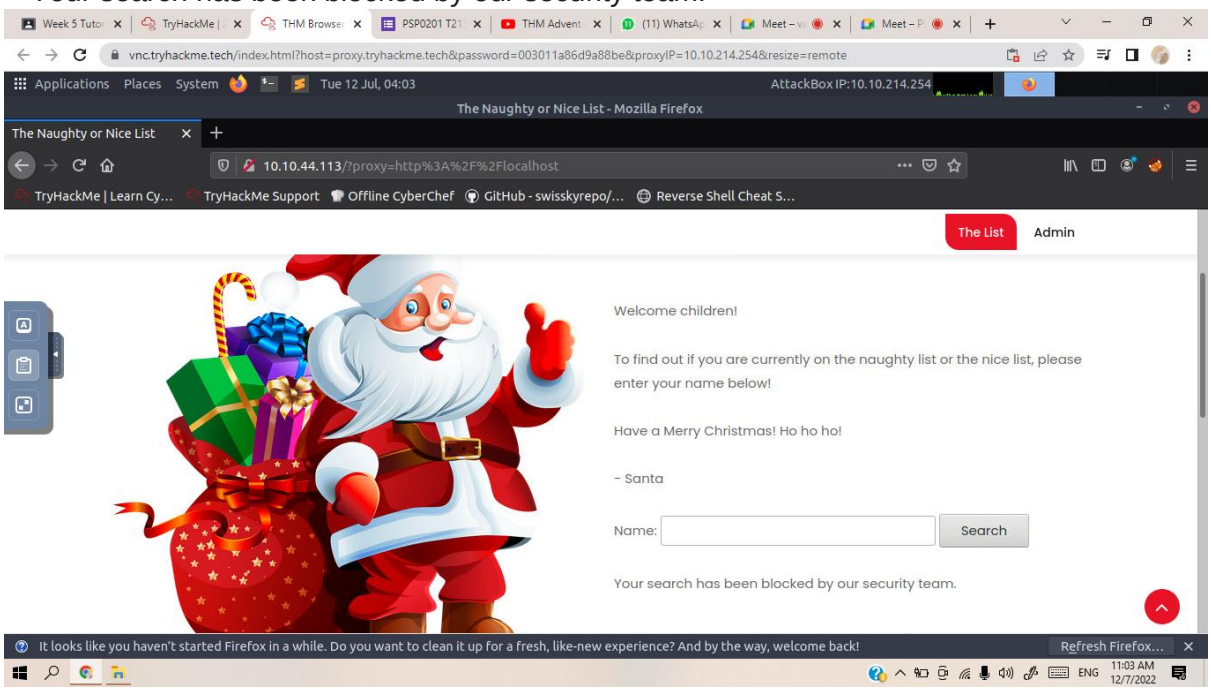
= Recv failure: Connection reset by peer



Question 5 :

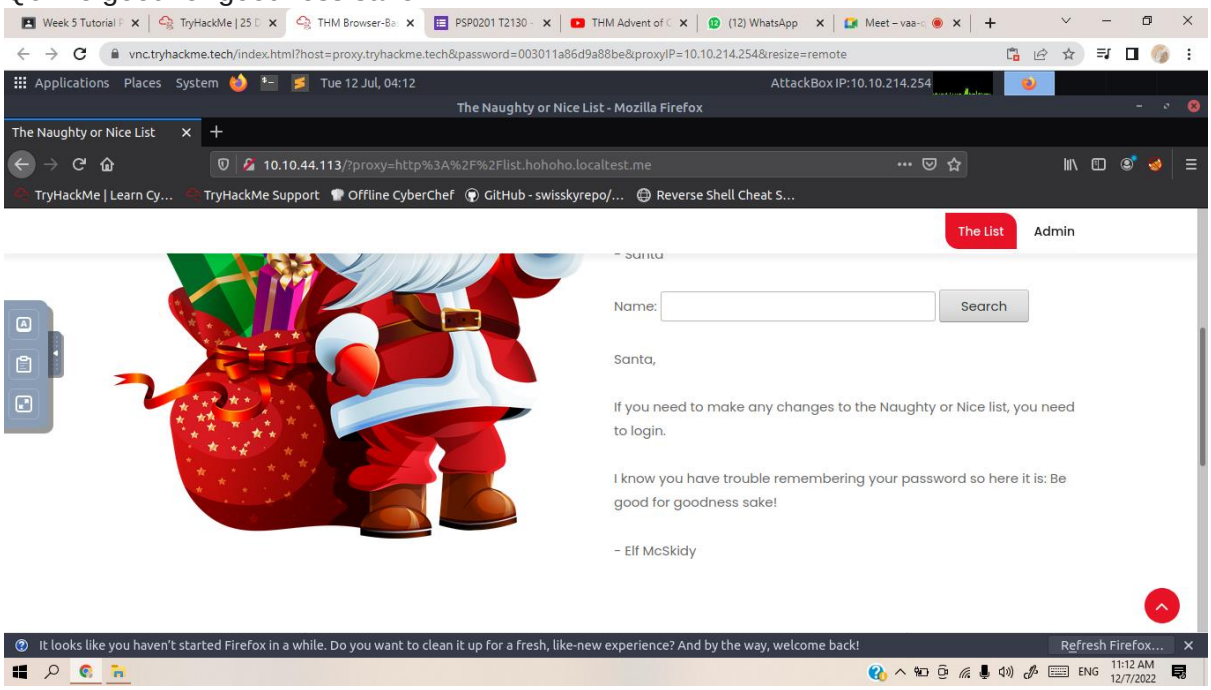
Q5: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?

= Your search has been blocked by our security team.



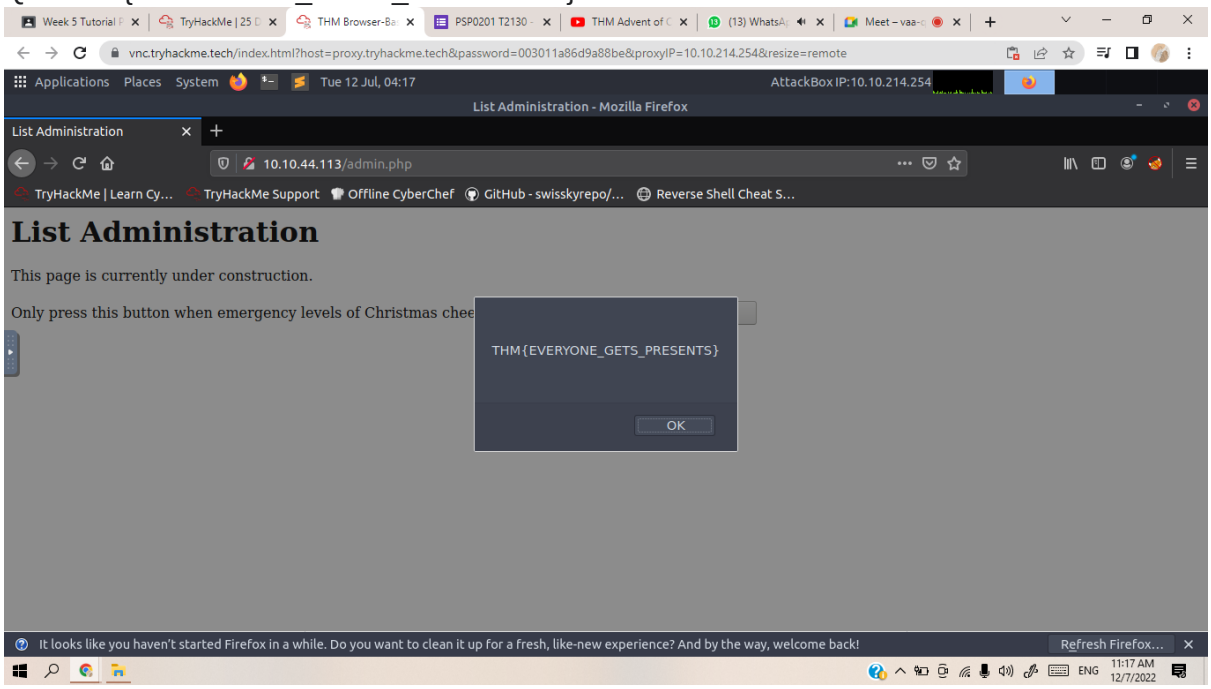
Question 6 : What is Santa's password?

Q6: Be good for goodness sake!



Question 7 : What is the challenge flag?

Q7: THM{EVERYONE_GETS_PRESENTS}



Methodology: (Day 19)

First, we deploy our machine and attackbox. We started the progress by inserted IP address and we were shown The Naughty or Nice List page. We search which list is Timothy, Ian Chai, Kanes, YP, Tib3rius and JJ on. Then, we insert the URL given to look up what displayed on pages. After that, we try localtest.me to find out admin password and log in. We have to delete the naughty list to get the challenge flag.

Day 20: PowershELIF to rescue

Tools: terminal, ssh

Question 1

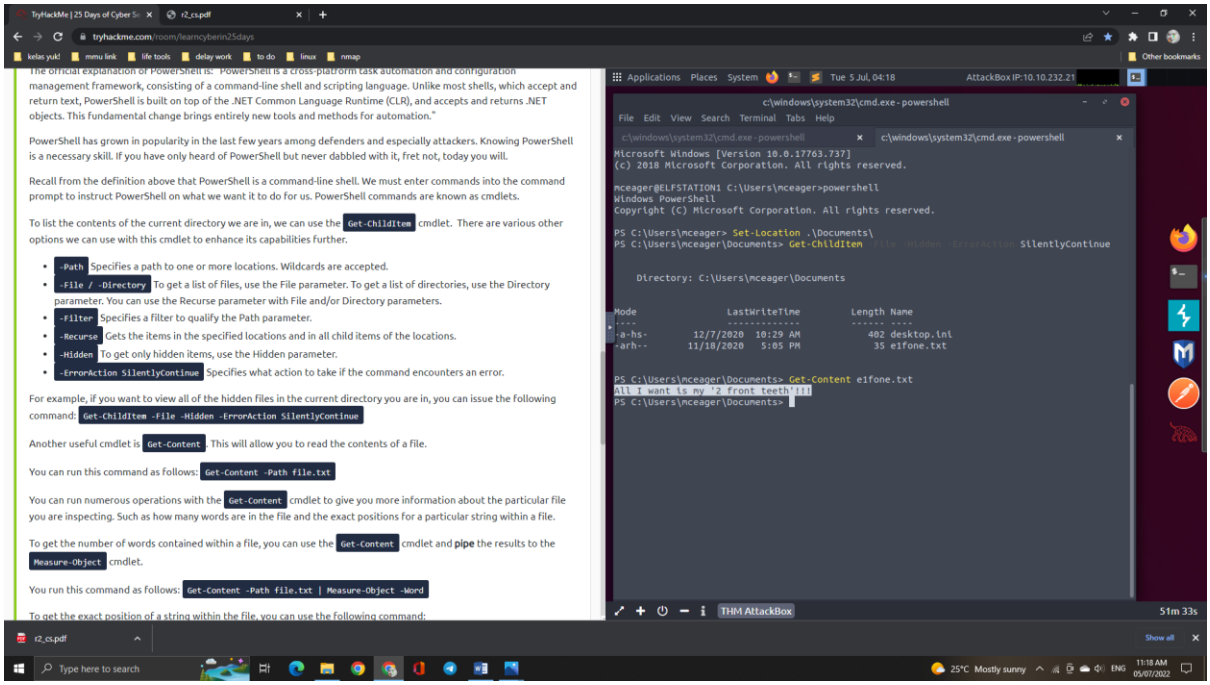
Q1: Check the ssh manual. What does the parameter -l do?

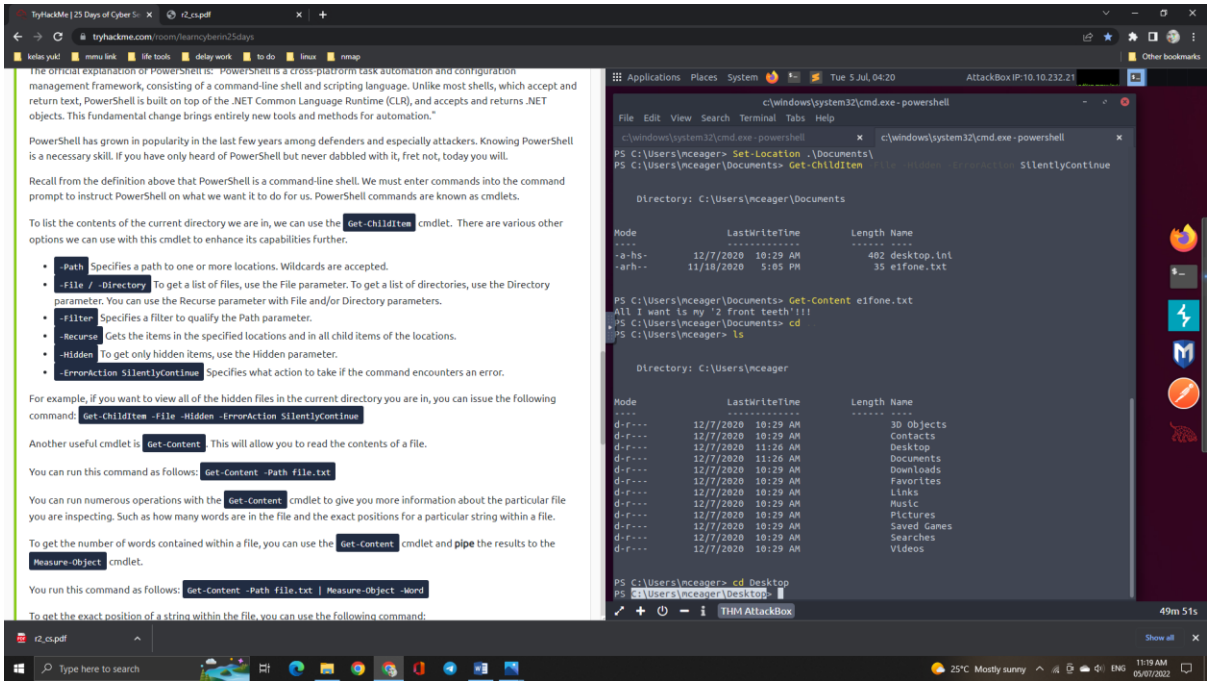
= login name

Question 2

Q2: Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

= 2 front teeth

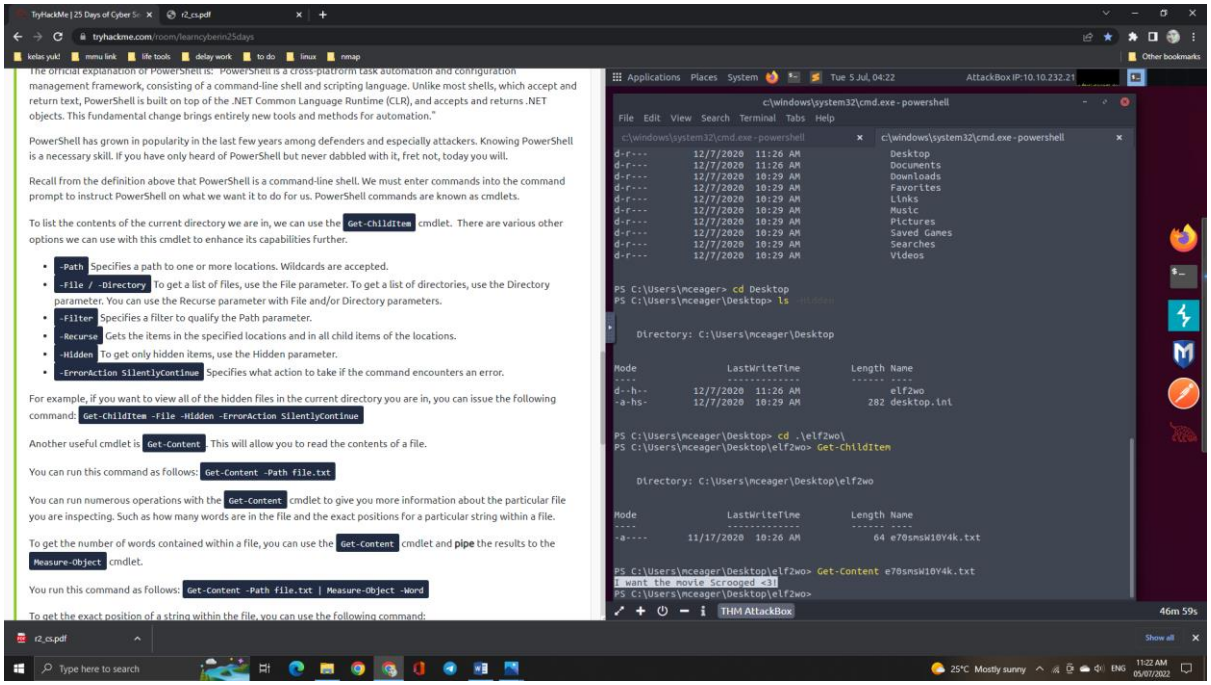




Question 3

Q3: 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?

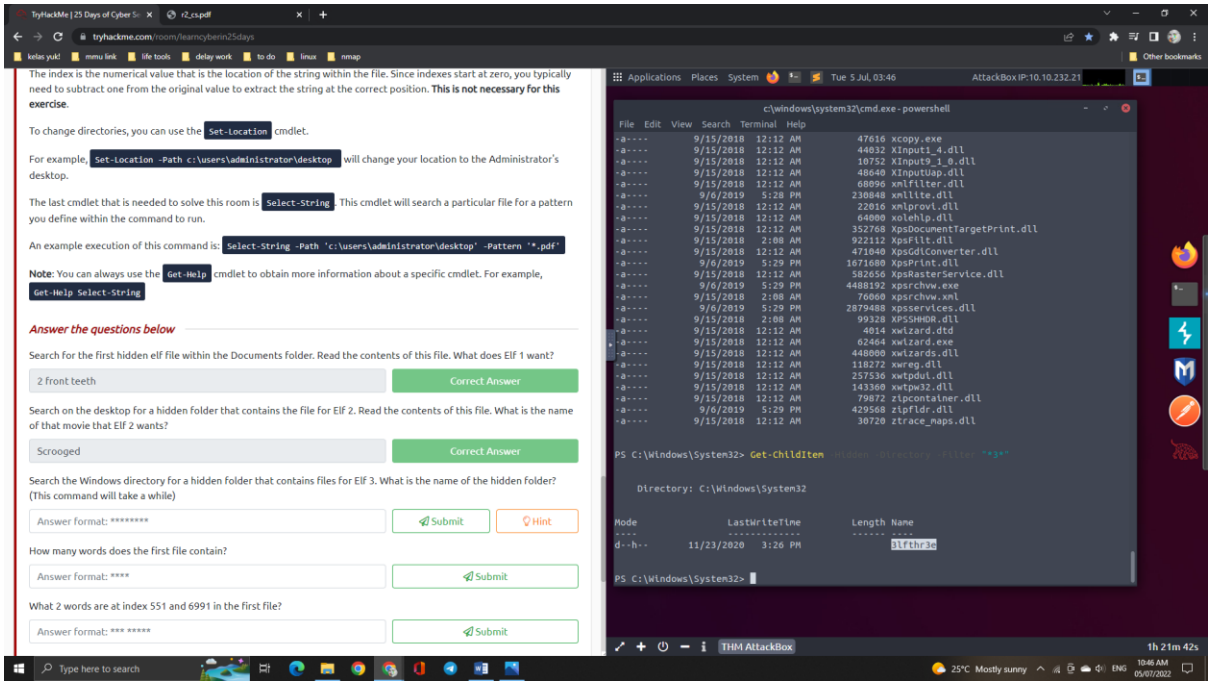
=Scrooged



Question 4

Q4: Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder?

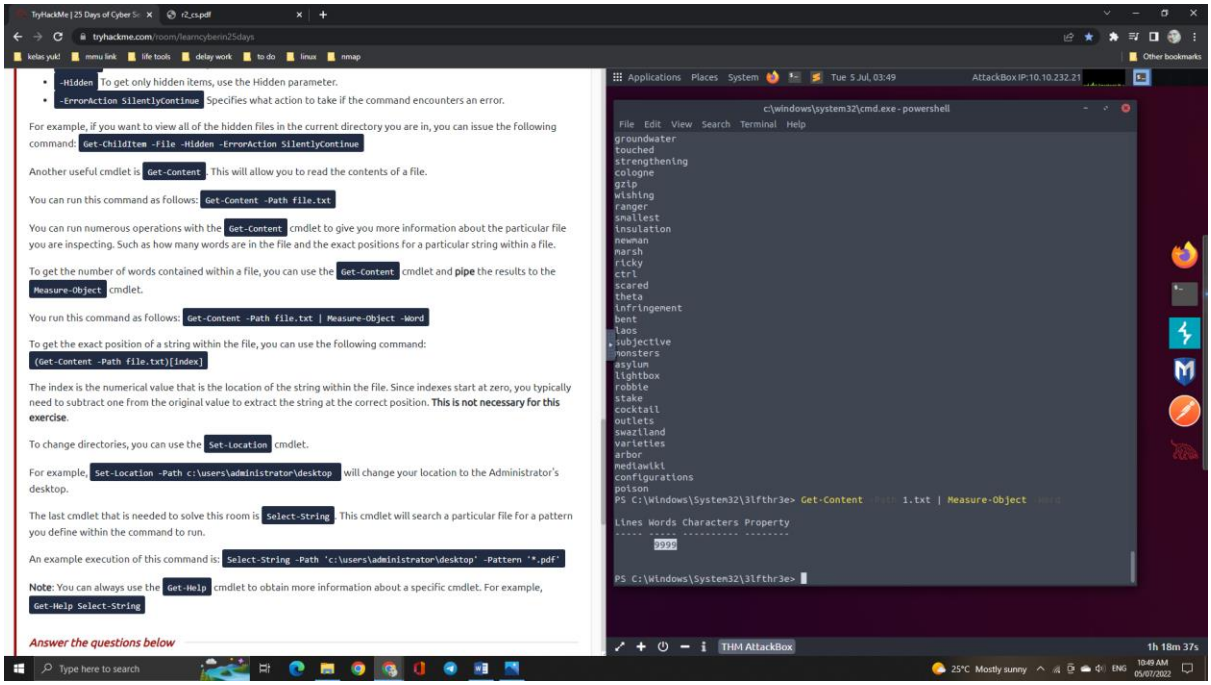
= 3lfthr3e



Question 5

Q5: How many words does the first file contain?

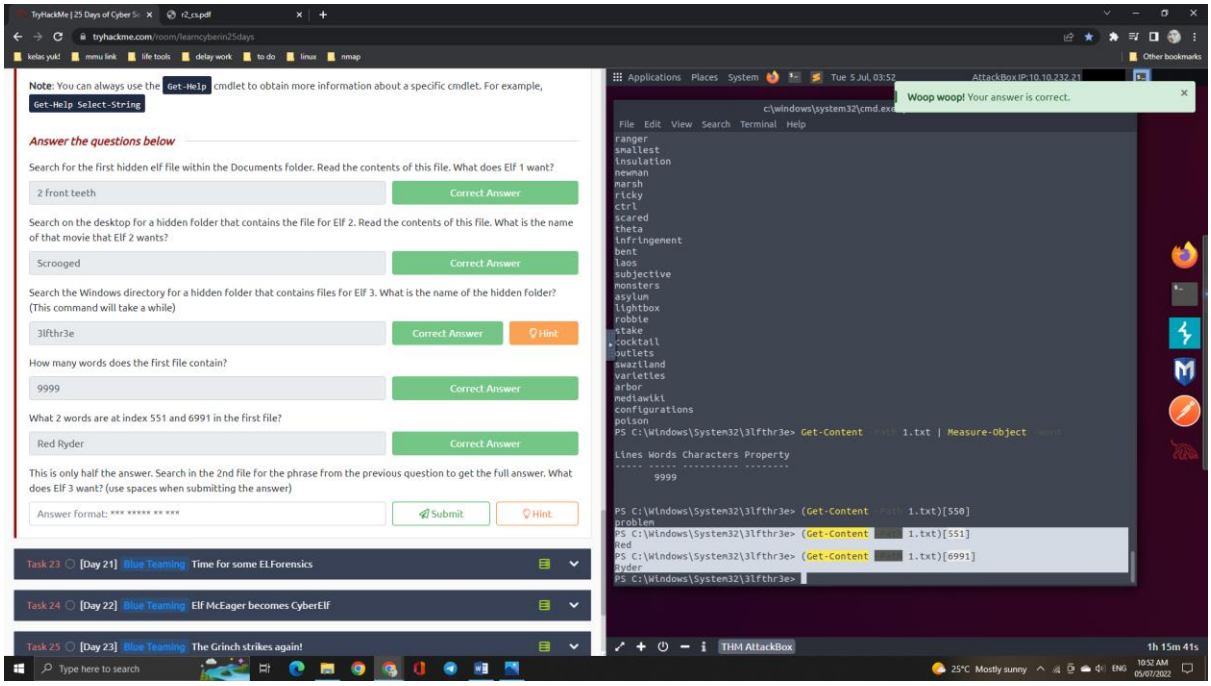
=9999



Question 6

Q6: What 2 words are at index 551 and 6991 in the first file?

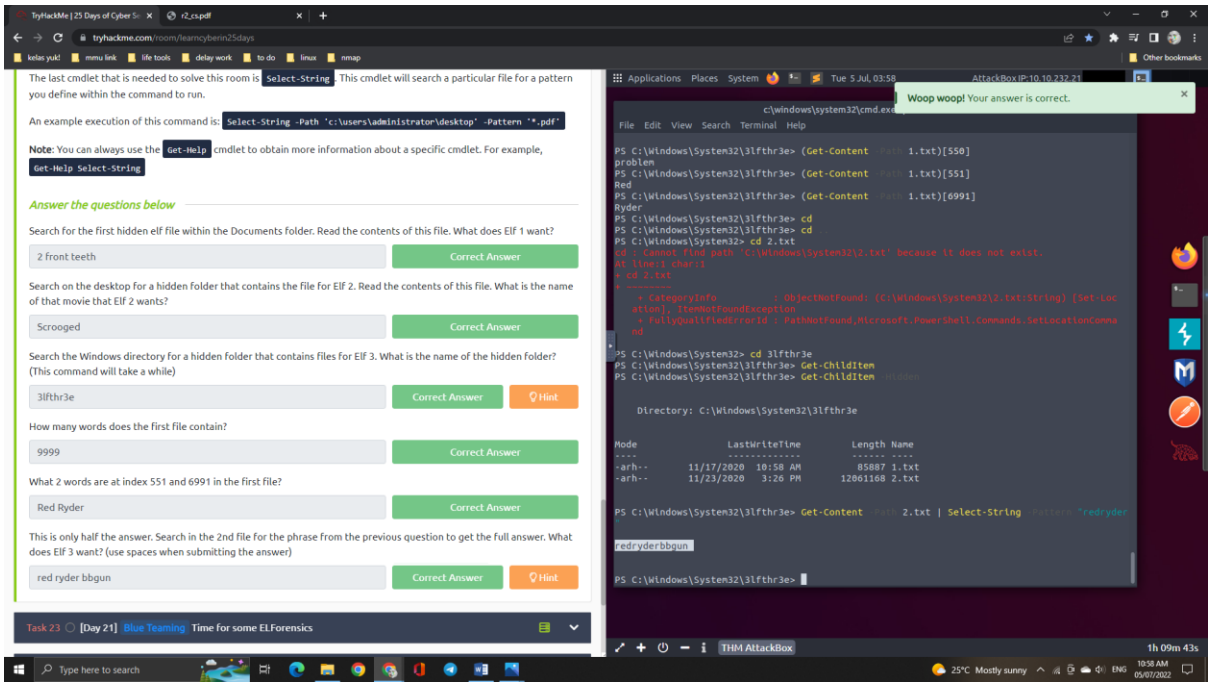
=Red Ryder



Question 7

Q7: 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?

=redryderbbgun



Methodology (Day20):

To begin with, we use SSH to connect to the remote machine using respective command. Then, continue by inserting the password as provided. First, we navigate to the Documents folder and using “Get-ChildItem -File -Hidden -ErrorAction SilentlyContinue” command to see the list of hidden folder. Next we use “Get-Content -Path e1fone.txt” command to access the contents of the file. Moving to the next task, we navigate to the Desktop folder. Using the same steps, we access the contents of the file that has been stored there. After that, we navigate to the Windows directory, “C:\Windows\System32”. To see the name of hidden folder, we use Get-ChildItem -Hidden -Directory -Filter “*3*” command. Then, proceeds with “Get-Content -Path 1.txt | Measure-Object -Word” command to get the number of words contained in that file. We also use “(Get-Content -Path 1.txt)[index] “ command to get exact position of a word within the file. Last, we use “Get-Content -Path 1.txt | Select-String -Pattern “redryder” “ command to get the full answer.