PSP0201

Week 5

Writeup

Group Name: SupremeChickens

Members

ID	Name	Role
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	Member
1211101198	Fam YI Qi	Member
1211103978	Yong Dick Shen	Member

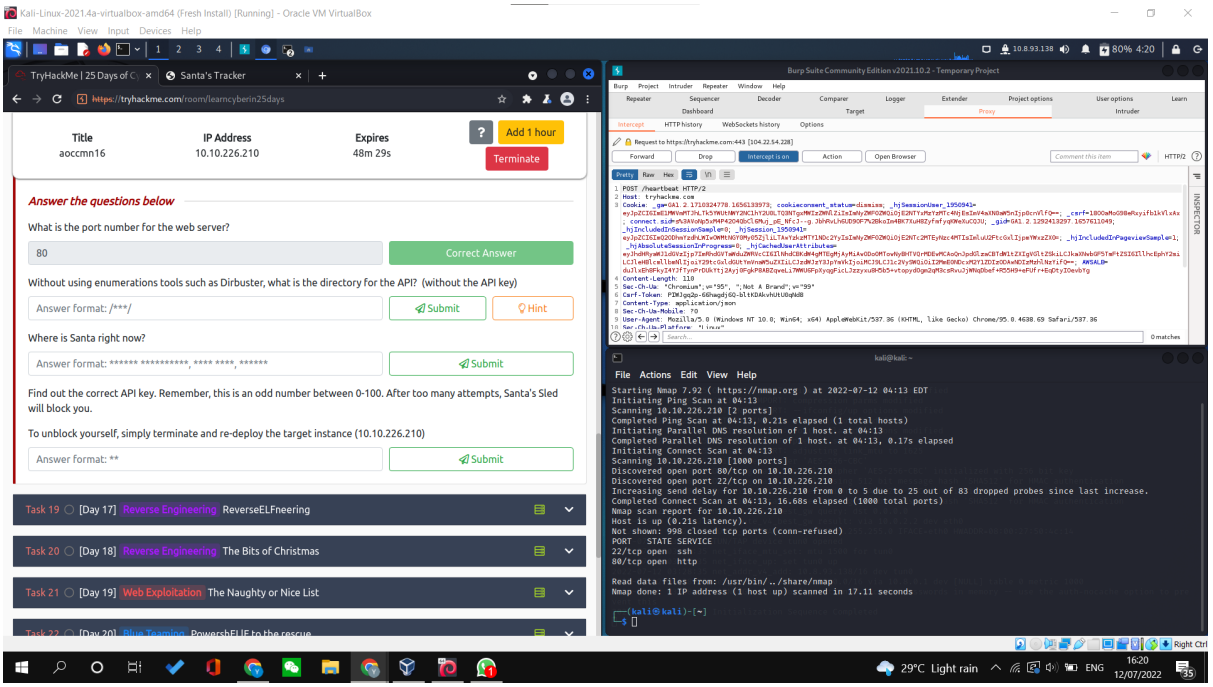
Day 16: Scripting – Help! Where is Santa!

Tools used: Kali Linux, Chrome

Solution/walkthrough: John Hammond

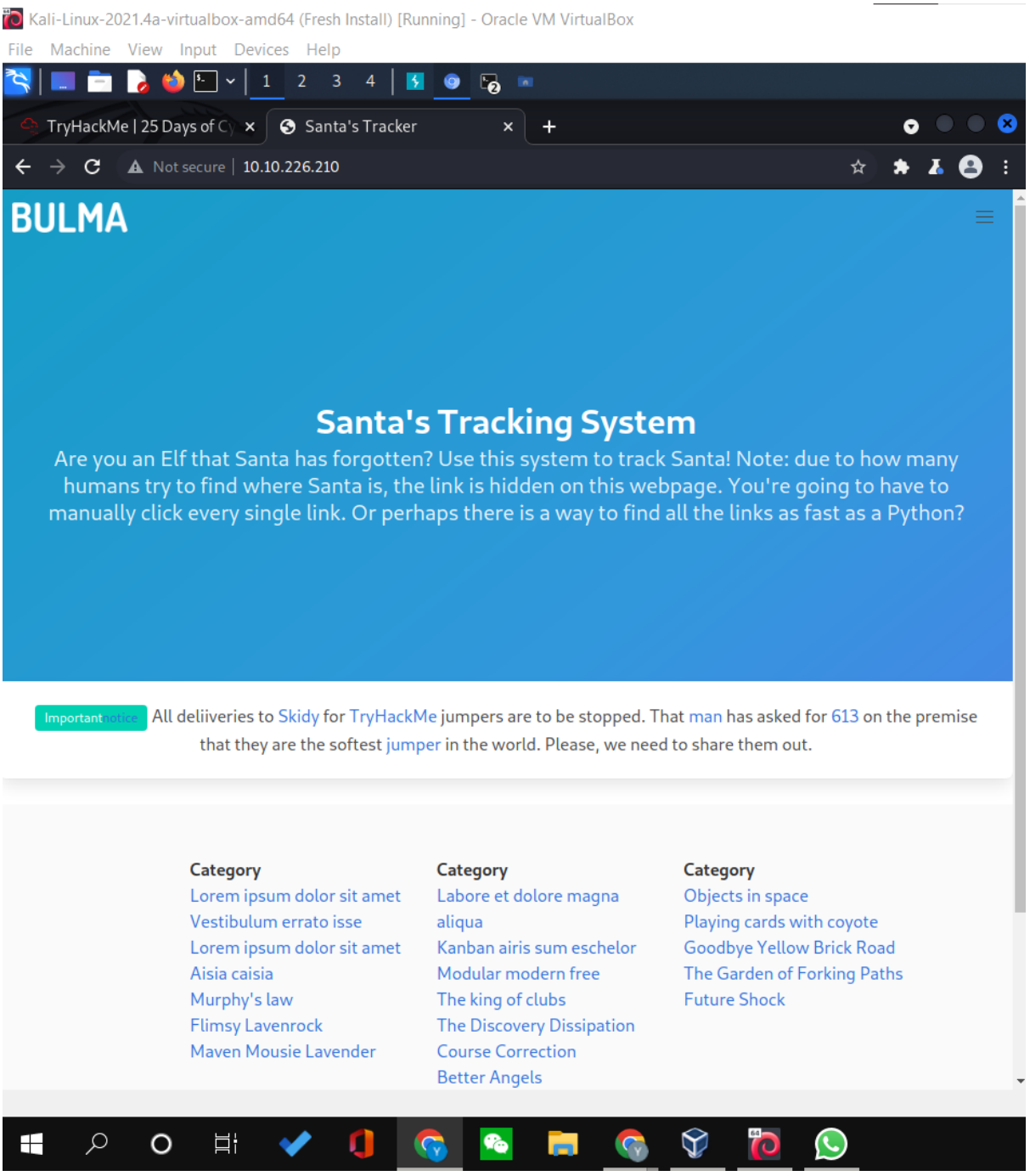
Question 1

What is the port number for the web server?



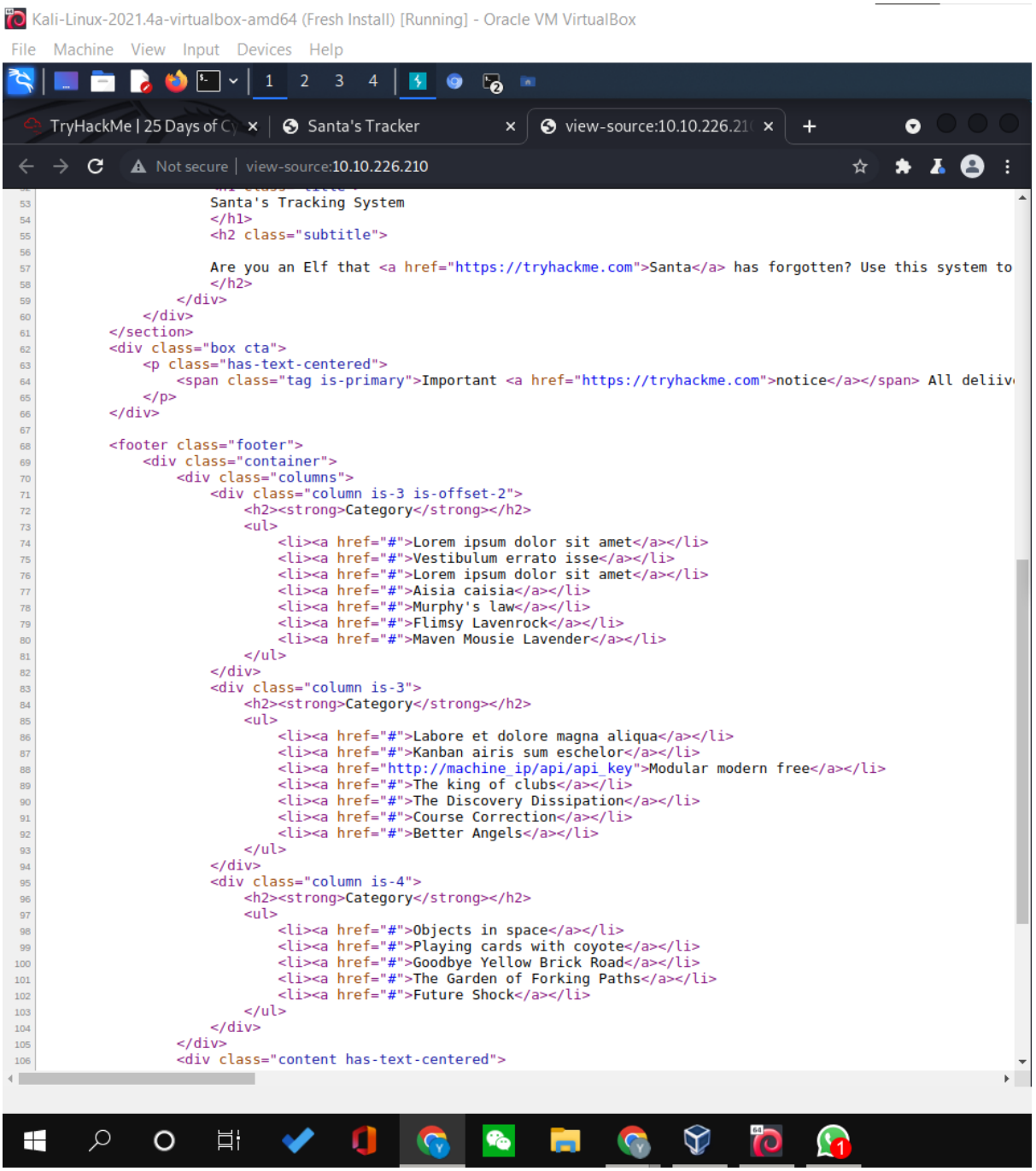
Question 2

What templates are being used?



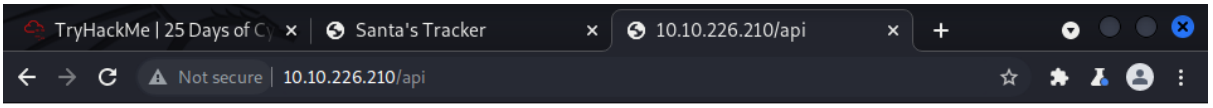
Question 3

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



Question 4

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



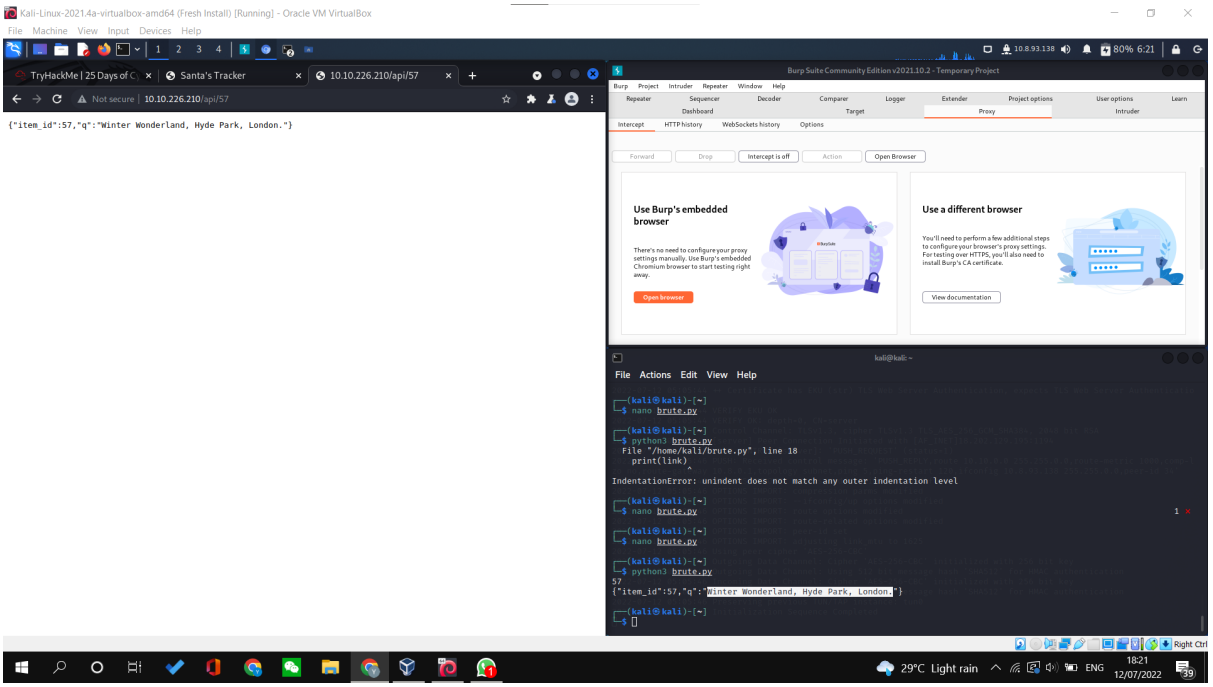
{"detail":"Not Found"}

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)



Thought Process/Methodology:

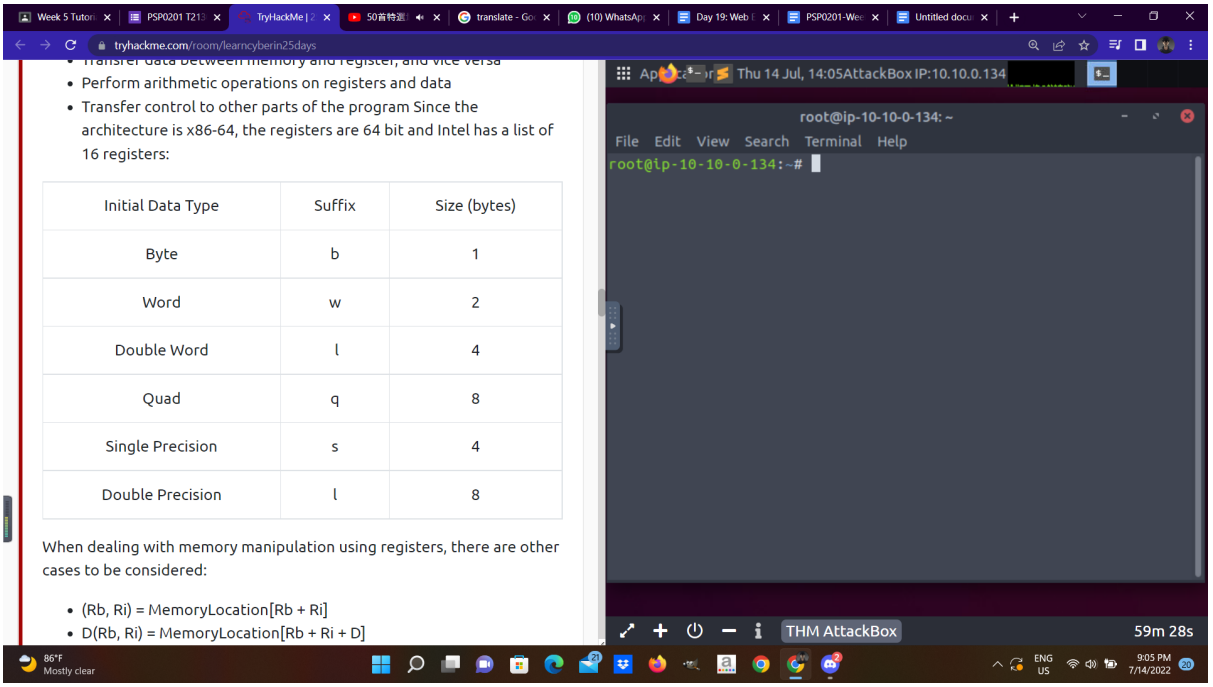
Having accessed the target machine, We were shown Santa's Tracking System. Then, we used nmap in verbose mode with my IP address and viewed the needed information. Next, we used the touch command to create a file (brute.py) and modify it. After that, we used python3 to run brute.py. After it found Santa's location, we typed the api into the url.

Day 17 [Reverse Engineering] ReverseELFneering

Tools used: Kali Linux, Chrome

Solution/walkthrough: Darkstar

Question 1



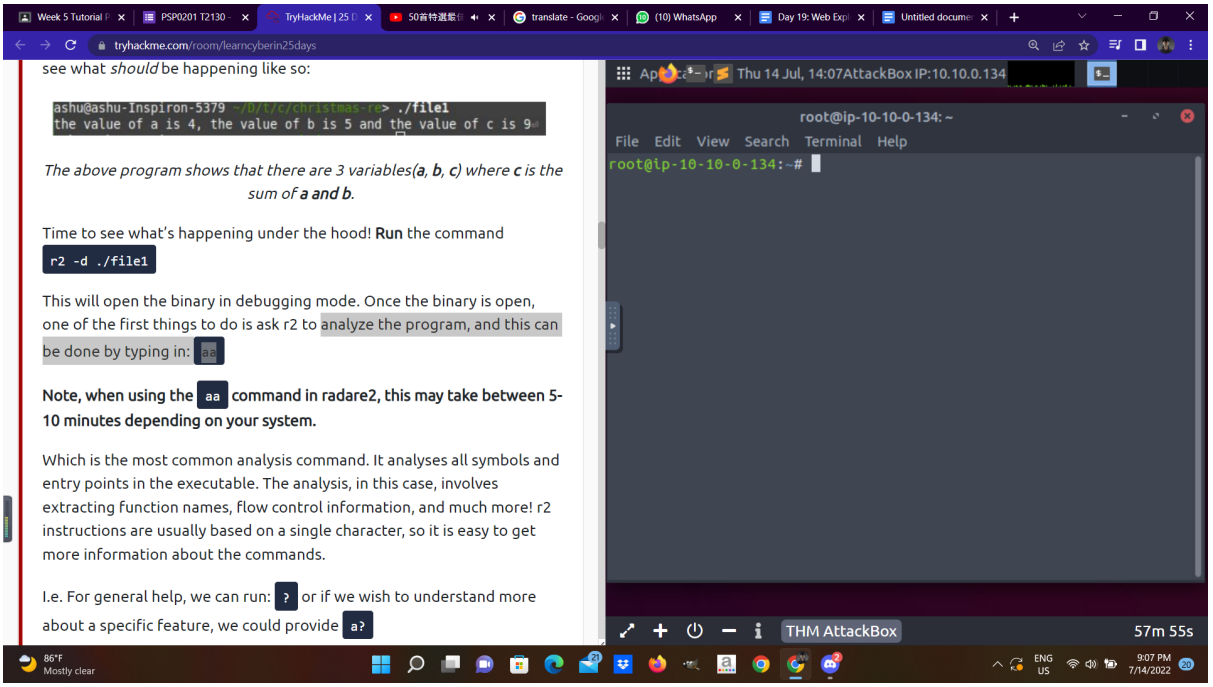
- Perform arithmetic operations on registers and data
- Transfer control to other parts of the program Since the architecture is x86-64, the registers are 64 bit and Intel has a list of 16 registers:

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

When dealing with memory manipulation using registers, there are other cases to be considered:

- (Rb, Ri) = MemoryLocation[Rb + Ri]
- D(Rb, Ri) = MemoryLocation[Rb + Ri + D]

Question 2



see what *should* be happening like so:

```
ashu@ashu-Inspiron-5379 ~/D/t/c/Christmas-re> ./file1
the value of a is 4, the value of b is 5 and the value of c is 9
```

*The above program shows that there are 3 variables(**a, b, c**) where **c** is the sum of **a and b**.*

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

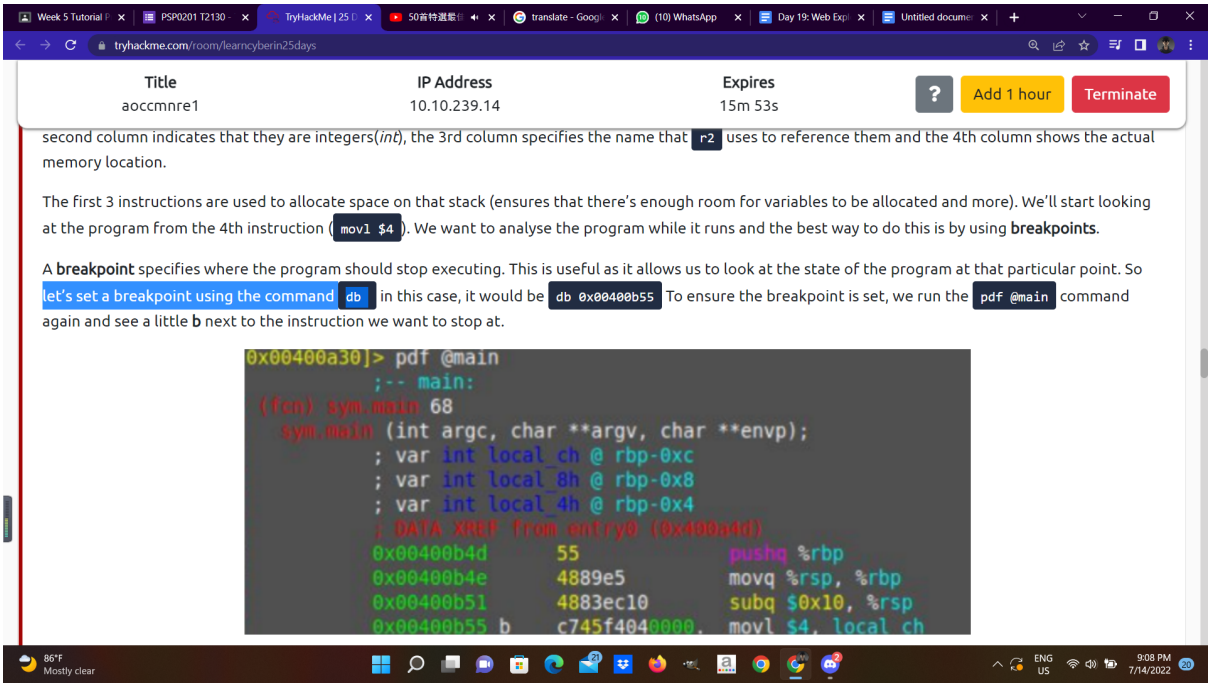
This will open the binary in debugging mode. Once the binary is open, one of the first things to do is ask r2 to analyze the program, and this can be done by typing in: `aa`

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

Which is the most common analysis command. It analyses all symbols and entry points in the executable. The analysis, in this case, involves extracting function names, flow control information, and much more! r2 instructions are usually based on a single character, so it is easy to get more information about the commands.

I.e. For general help, we can run: `?` or if we wish to understand more about a specific feature, we could provide `a?`

Question 3

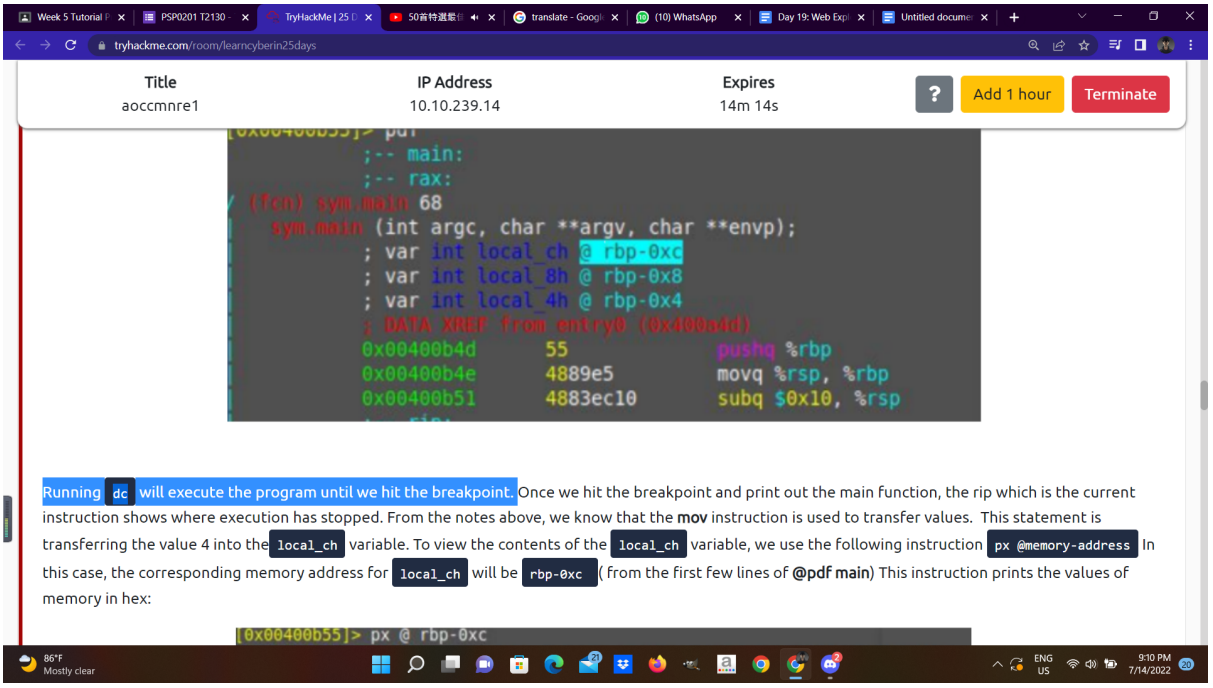


second column indicates that they are integers(*int*), the 3rd column specifies the name that `r2` uses to reference them and the 4th column shows the actual memory location.

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**.

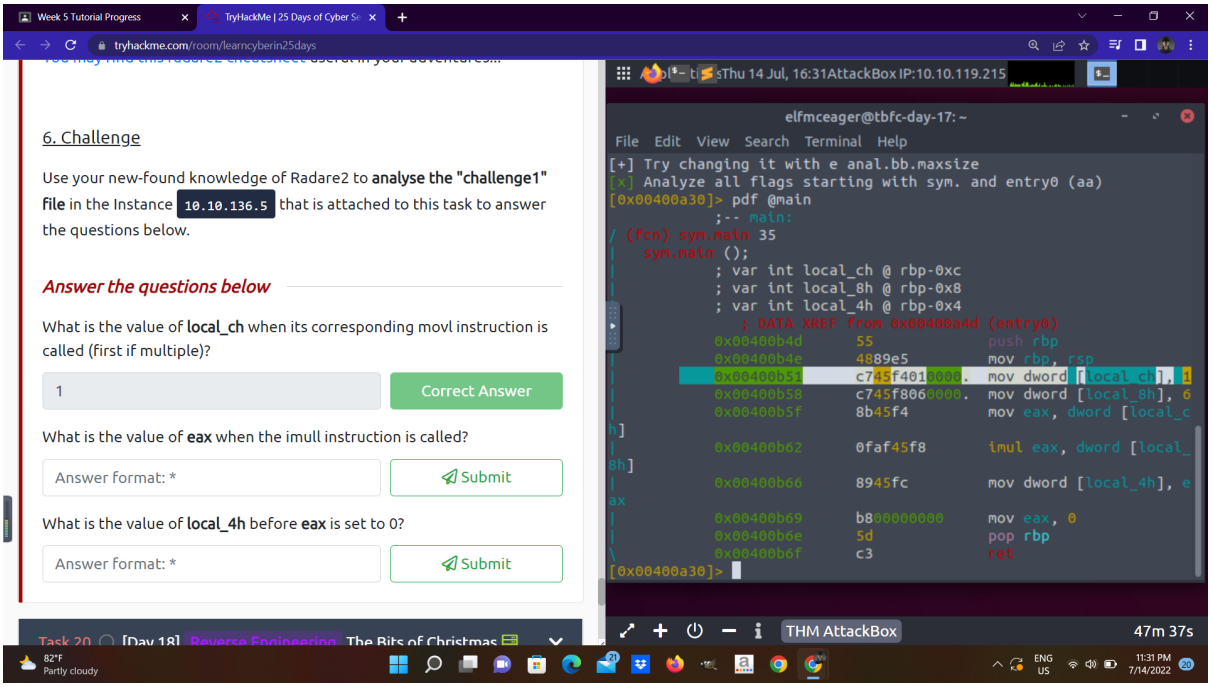
A **breakpoint** specifies where the program should stop executing. This is useful as it allows us to look at the state of the program at that particular point. So let's set a breakpoint using the command `db` in this case, it would be `db 0x00400b55` To ensure the breakpoint is set, we run the `pdf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

Question 4

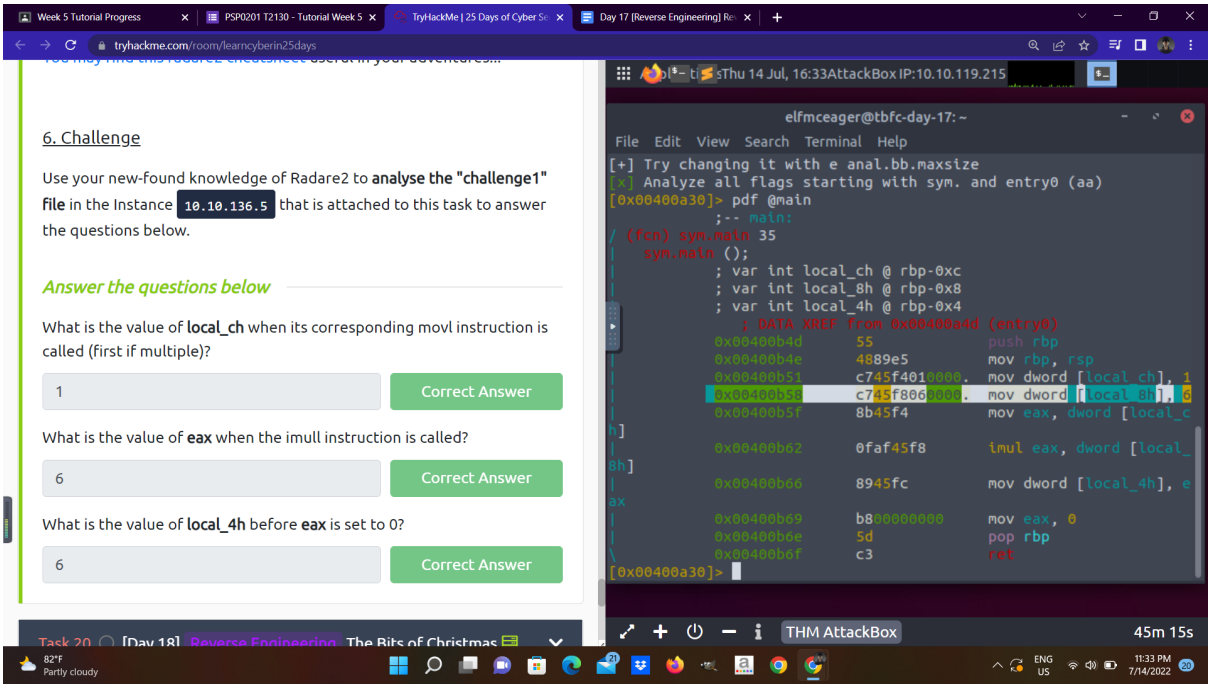


Running `dc` will execute the program until we hit the breakpoint. Once we hit the breakpoint and print out the main function, the rip which is the current instruction shows where execution has stopped. From the notes above, we know that the **mov** instruction is used to transfer values. This statement 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:

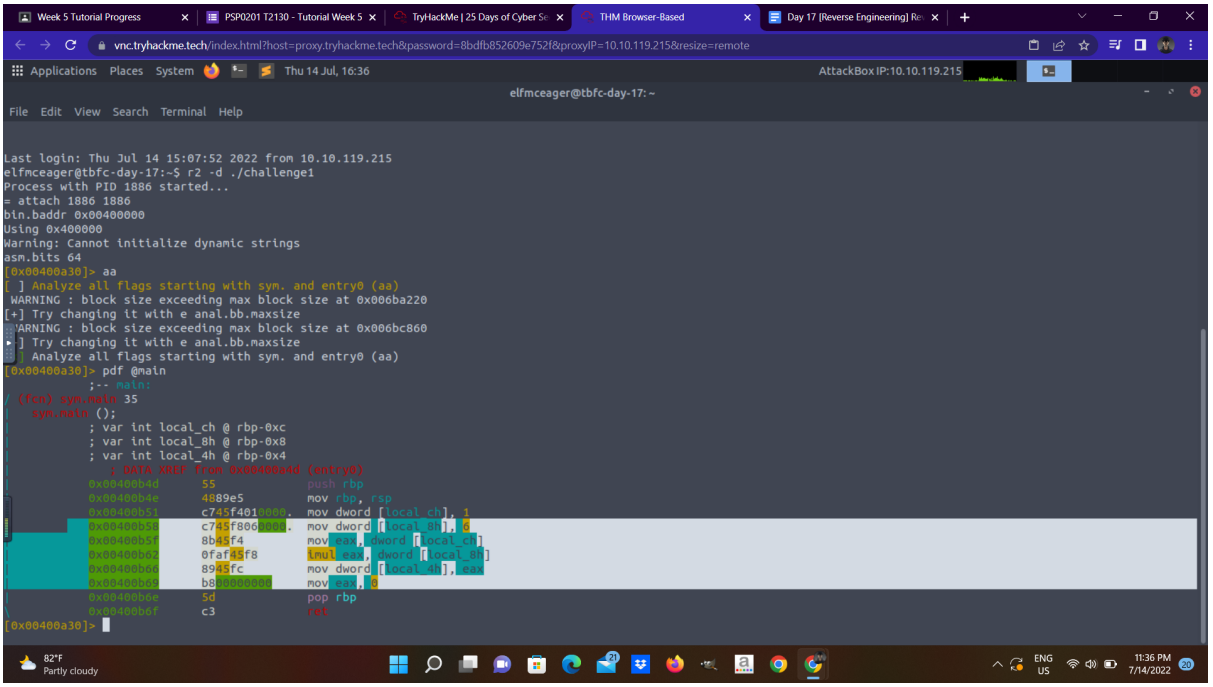
Question 5



Question 6



Question 7



Solution: open the command prompt ,try to login as user ‘elfmceager’. After that, run the command “r2 -d ./challenge1” then type ‘aa’ and wait for a while until ‘[0x00400a30]>’ appear .Next, type the command “pdf @main”.All the answer shown.

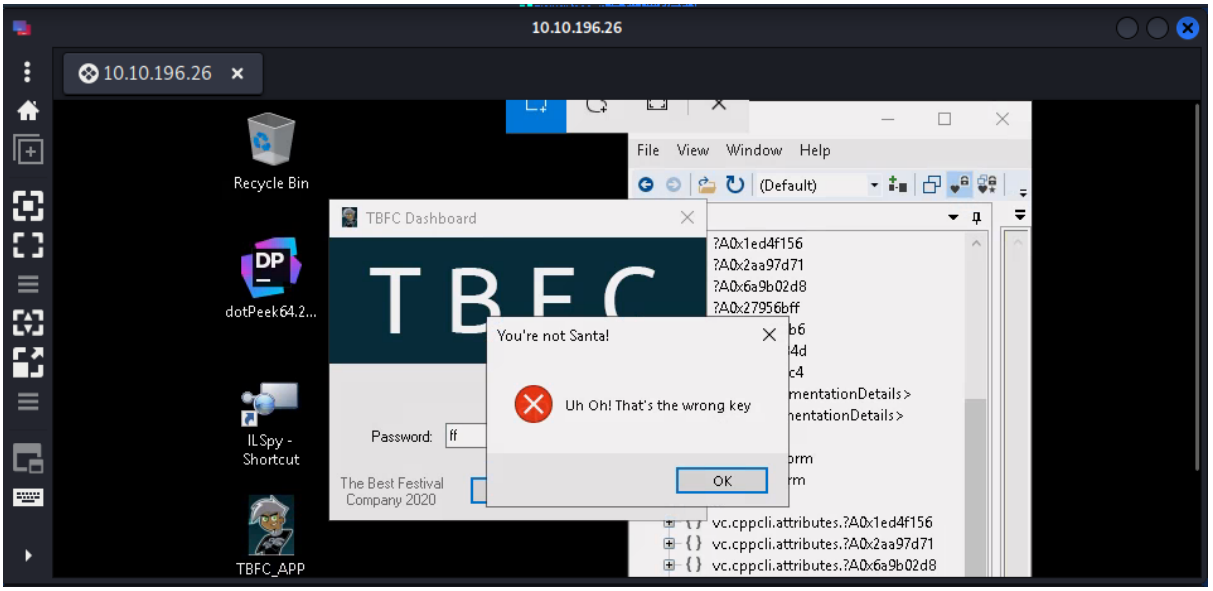
Day 18: Reverse Engineering - The Bits of Christmas

Tools used: Kali Linux, Chrome

Solution/walkthrough: John Hammond

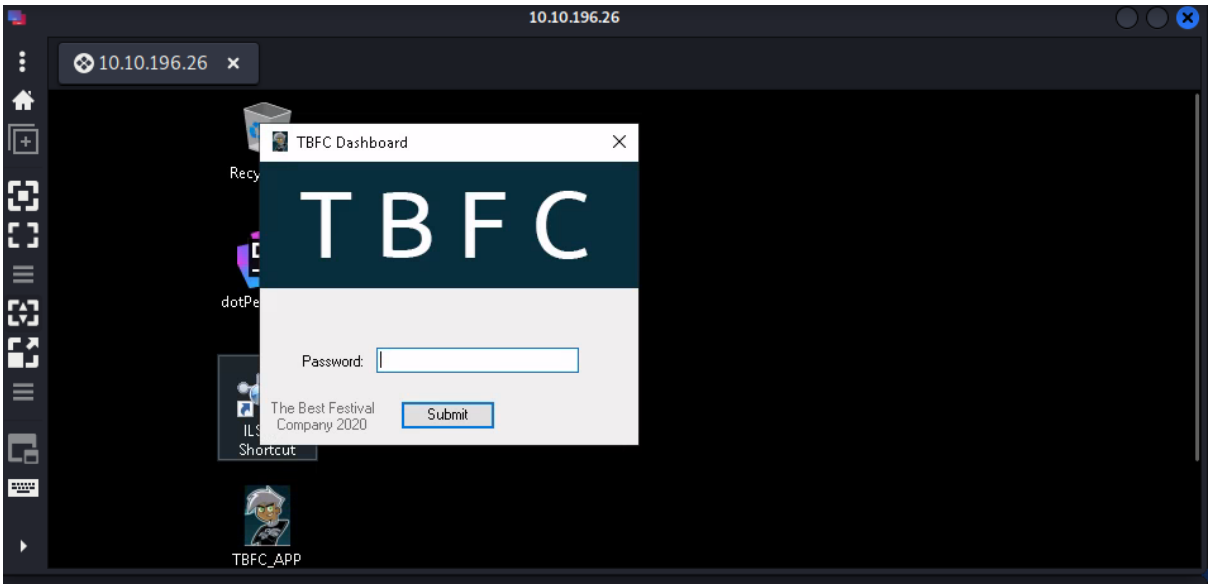
Question 1

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



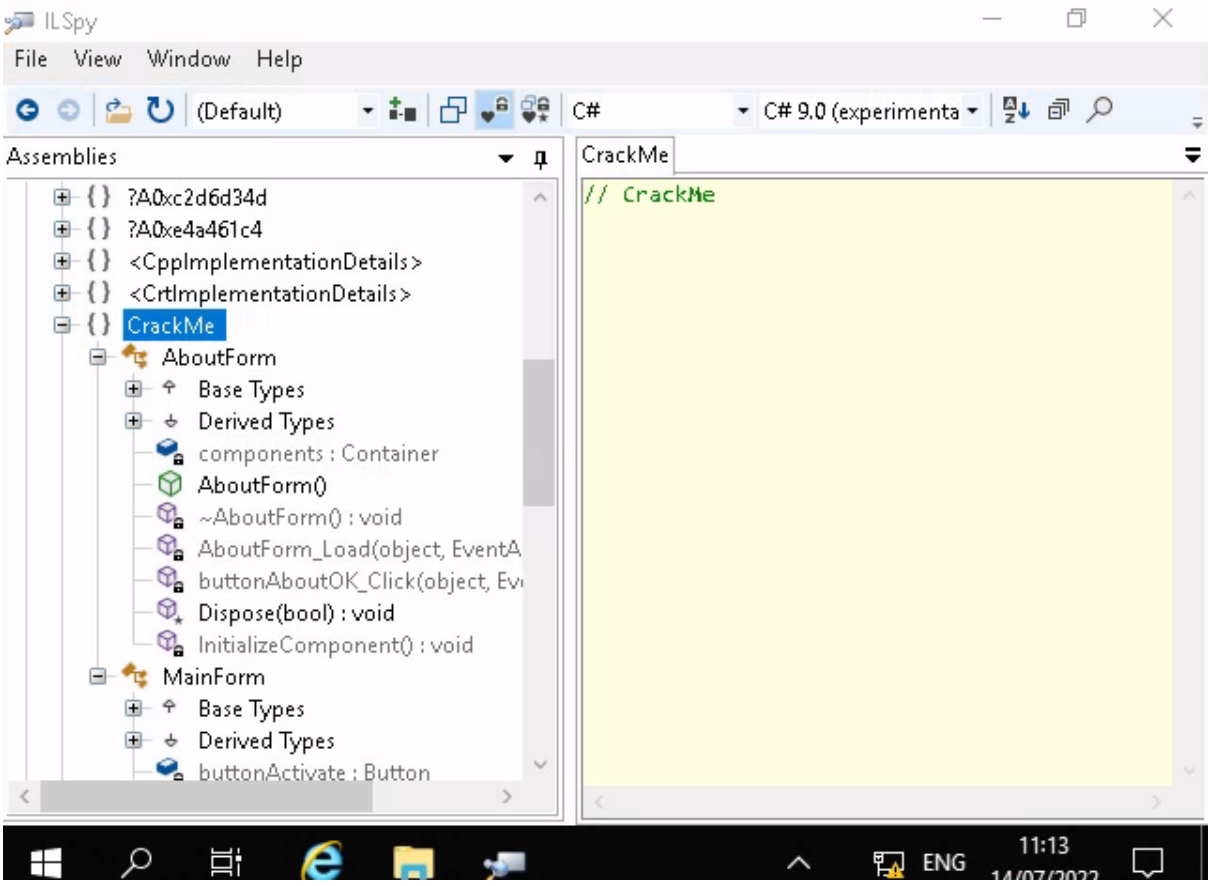
Question 2

What does TBFC stand for?



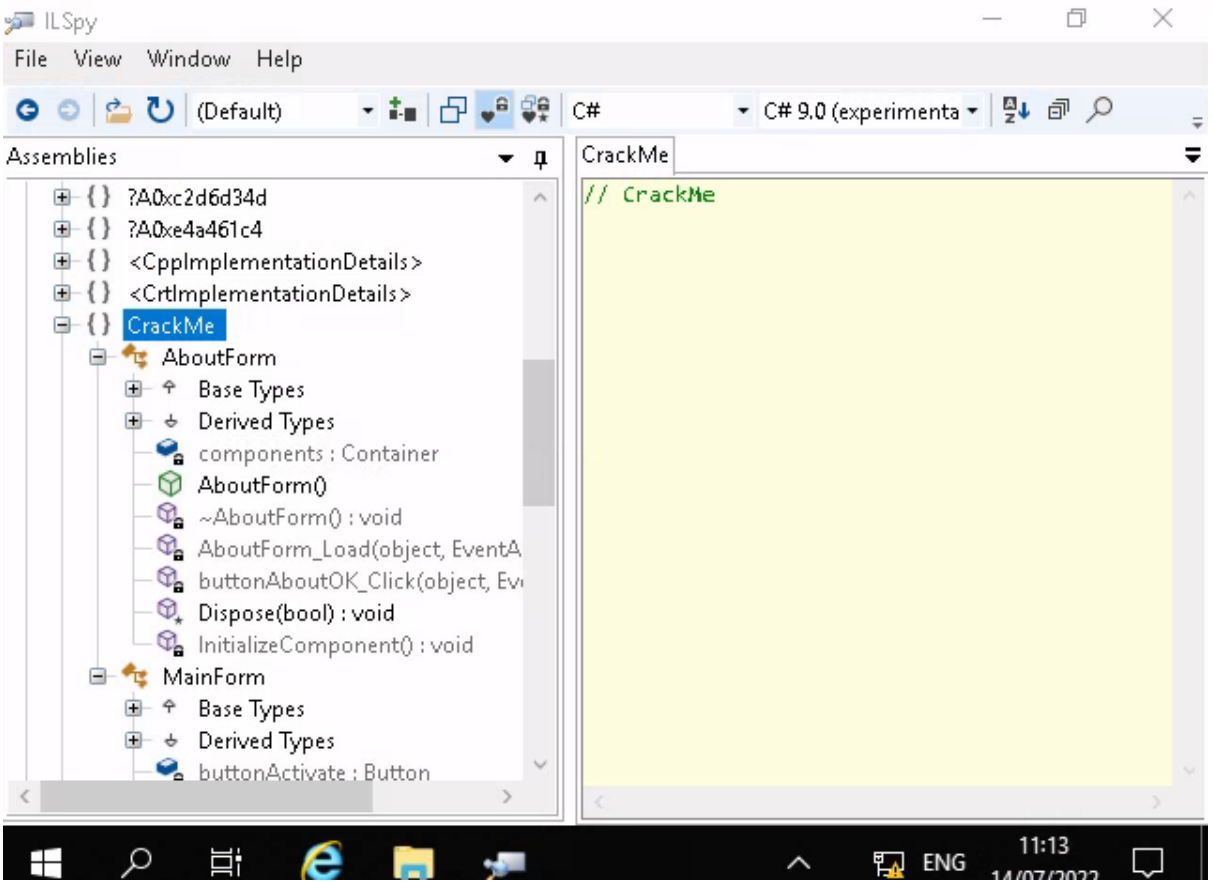
Question 3

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



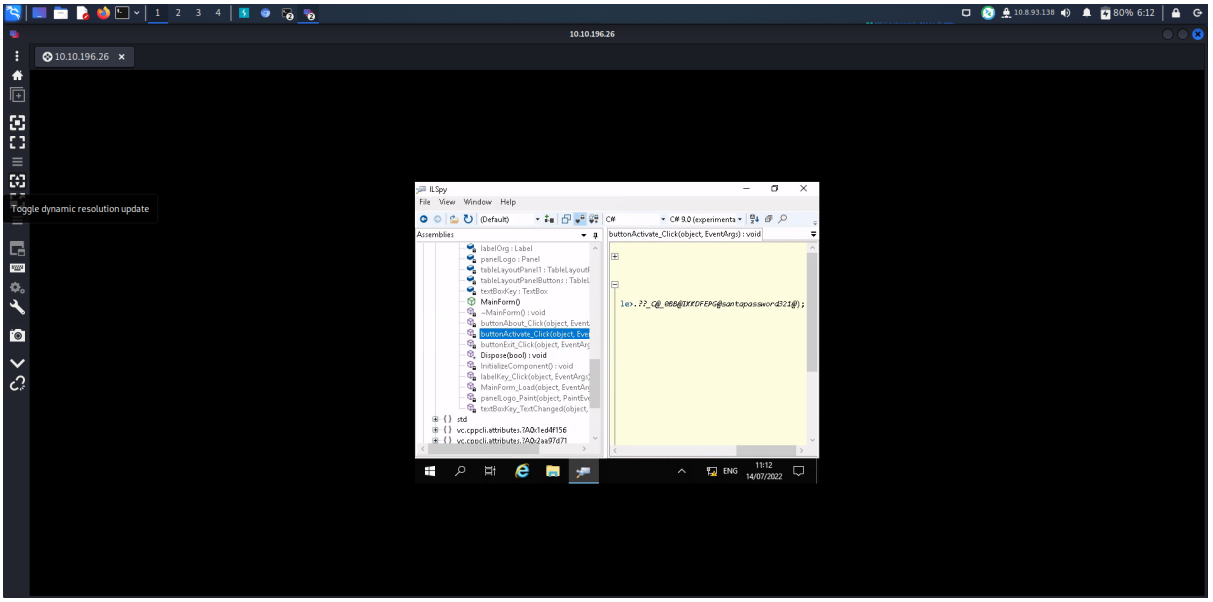
Question 4

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



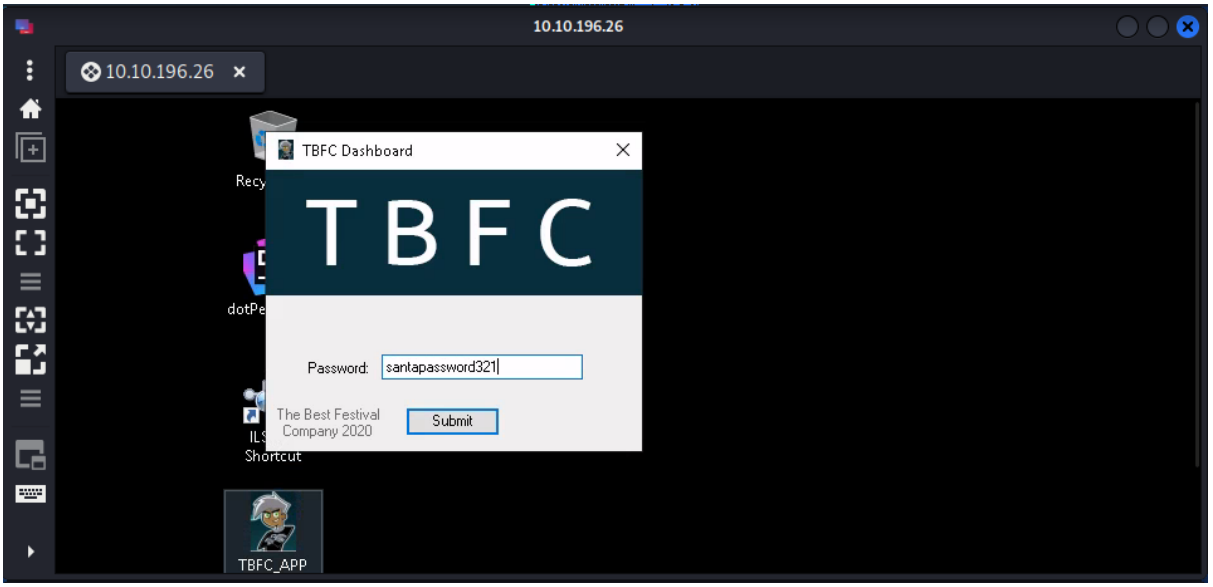
Question 5

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



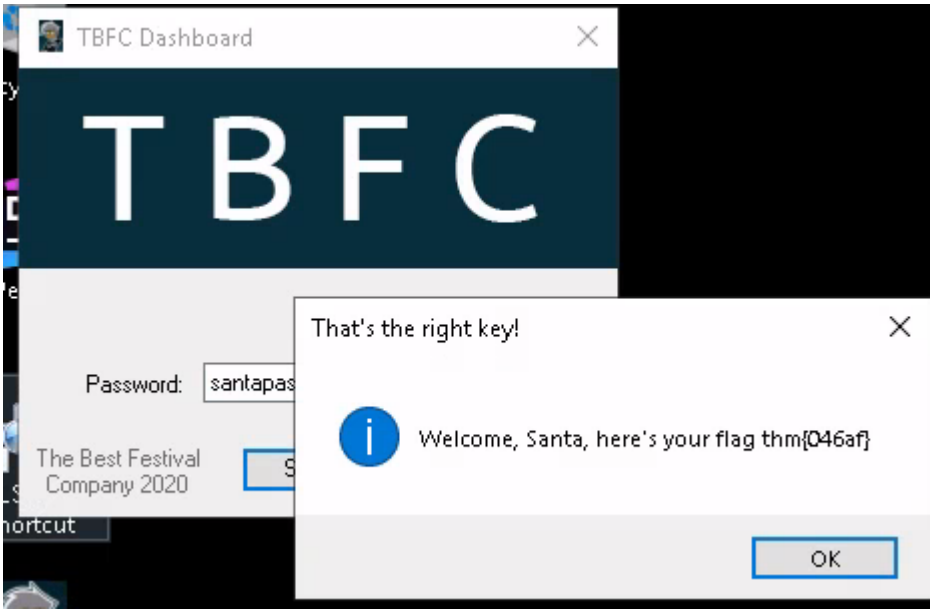
Question 6

What is Santa's password?



Question 7

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



Thought Process/Methodology:

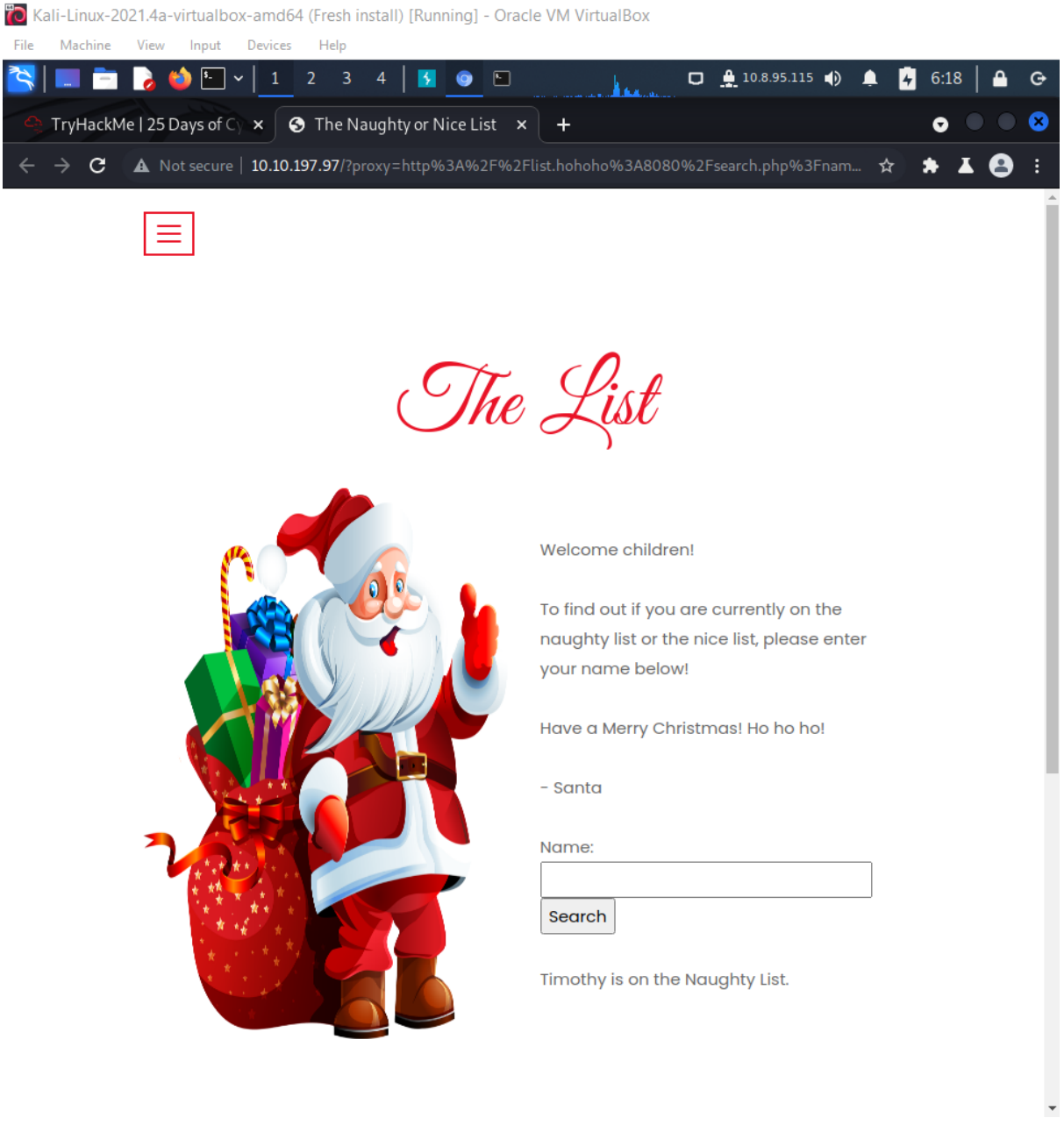
Having accessed the target machine, we opened remmina with my IP address and opened the TBFC_APP application in ILspy to decompile the code. We clicked into CrackMe and clicked the form to view the information we were looking for. After that, we clicked buttonActivate_Click to view Santa's password. Next, we keyed the password into the TBFC dashboard and we were shown the flag.

Day 19: Web Exploitation - The Naughty or Nice List

Tools used: Kali Linux, Chrome

Solution/walkthrough: -

Q1: Which list is this person on?



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | 25 Days of C

The Naughty or Nice List

Not secure | 10.10.197.97/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fnam...

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.

Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | 25 Days of C

The Naughty or Nice List

Not secure | 10.10.197.97/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fnam...

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.

Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 10.8.95.115 6:19

TryHackMe | 25 Days of C | The Naughty or Nice List

Not secure | 10.10.197.97/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fnam...

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.

Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | 25 Days of C

The Naughty or Nice List

Not secure | 10.10.197.97/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fnam...

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.

Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | 25 Days of C

The Naughty or Nice List

Not secure | 10.10.197.97/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fnam...

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!

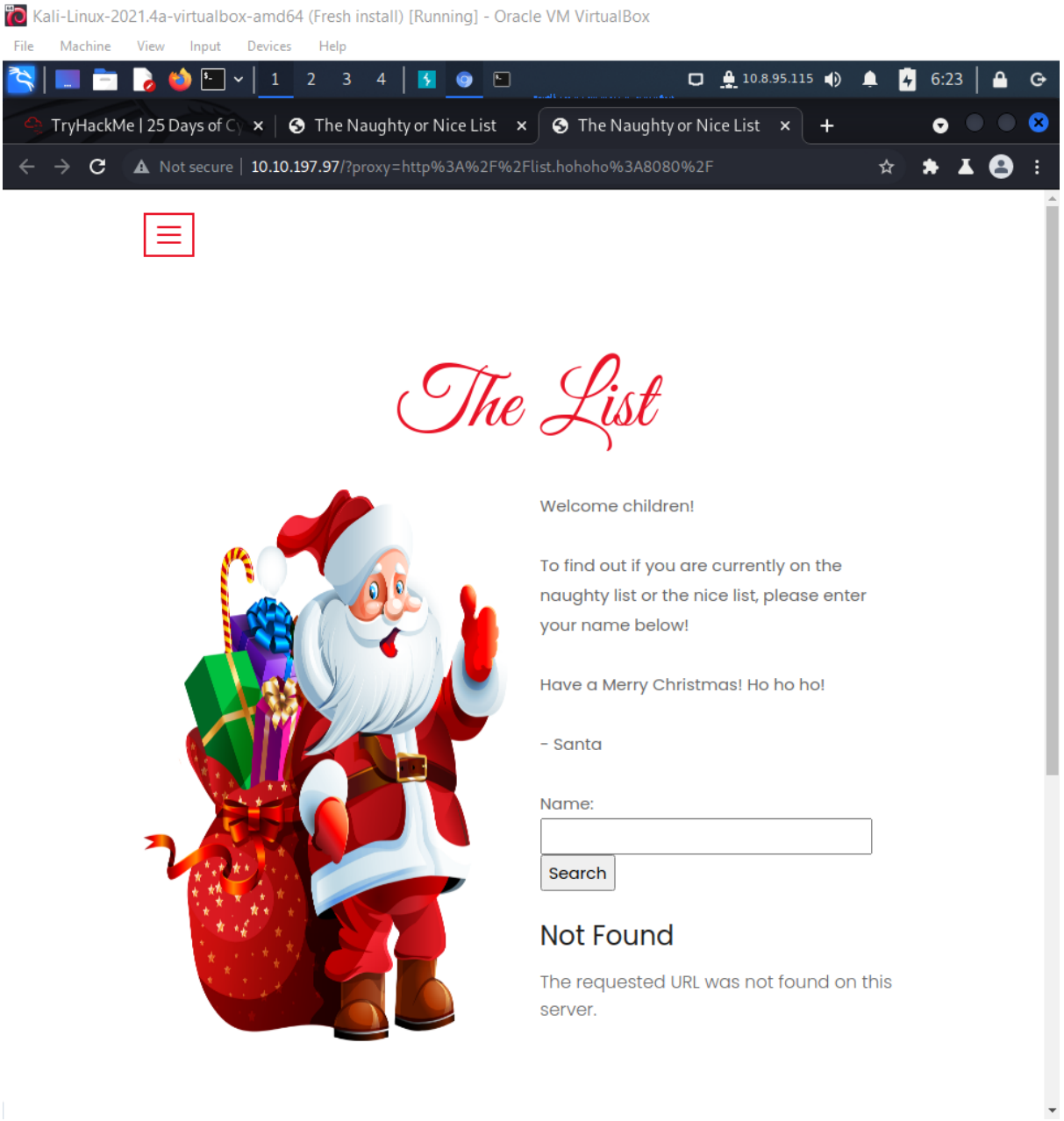
- Santa

Name:

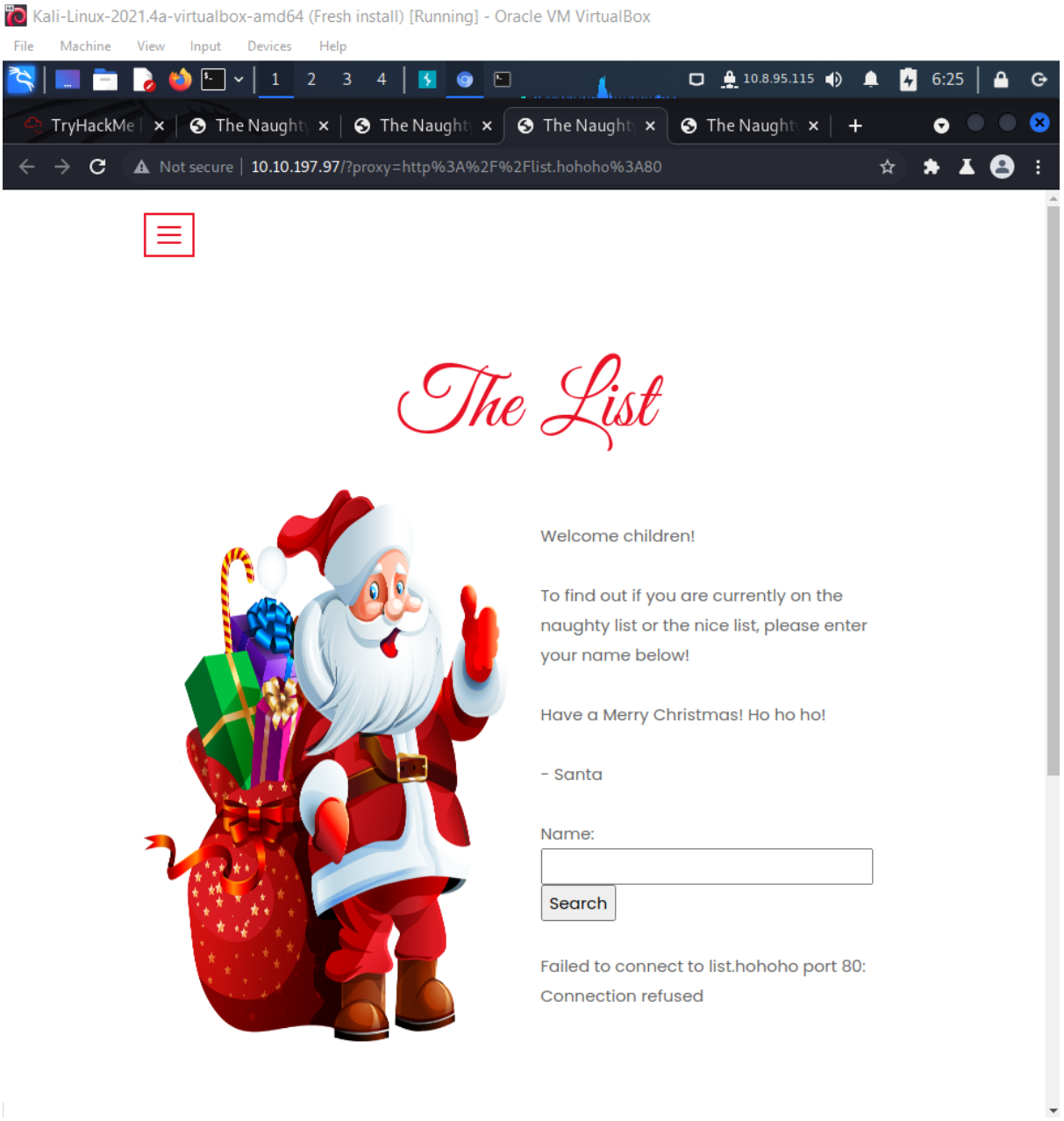
Search

Ian Chai is on the Nice List.

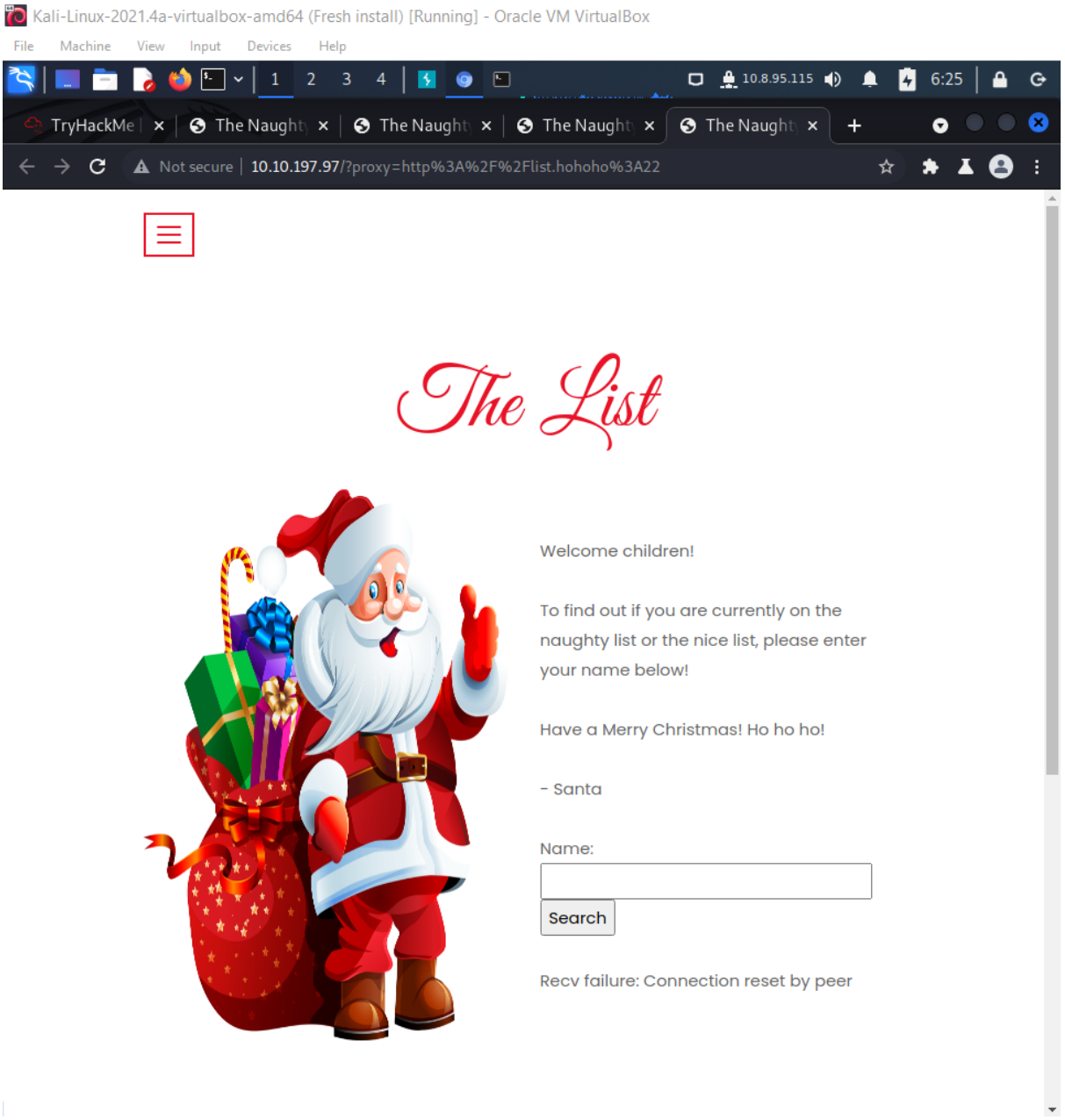
Q2: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?



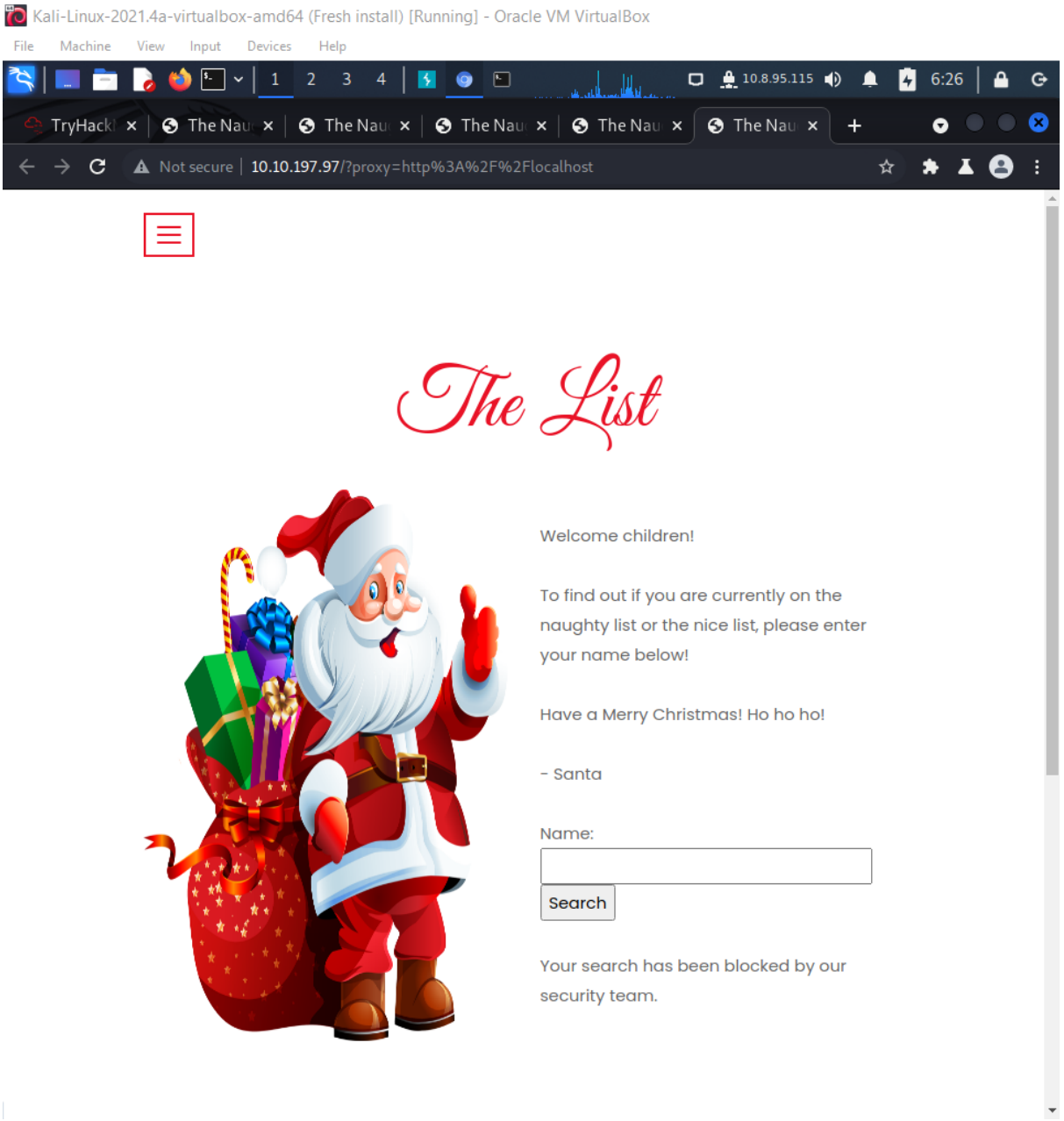
Q3: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"?



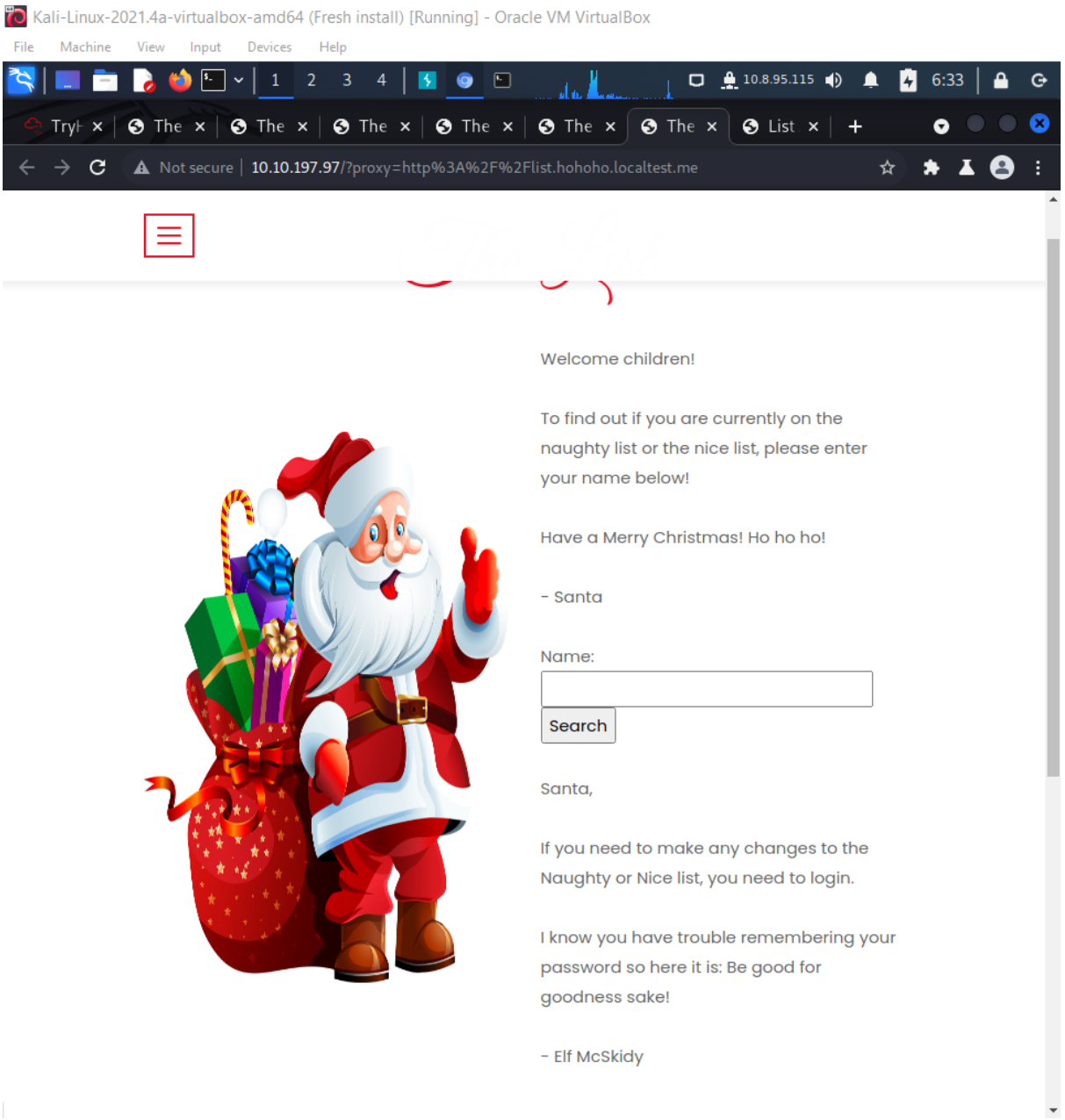
Q4: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"?



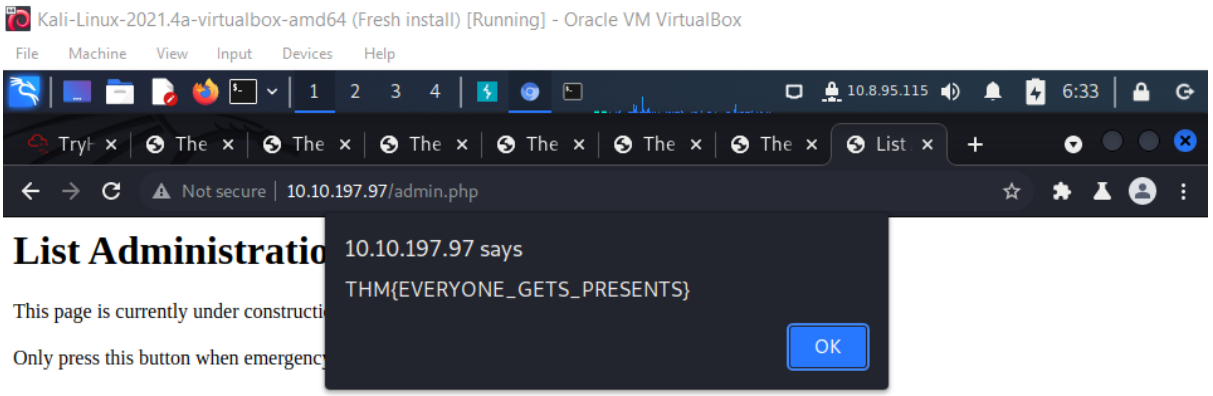
Q5: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?



Q3: What is Santa's password?



Q4: What is the challenge flag?



Thought Process/Methodology:

Having accessed the target machine, the title page shows ‘The Naughty or Nice List’. It provides the blank for us to fill in the name to check whether the name is under ‘Naughty List’ or ‘Nice List’. We type in the names one by one to check which list the children are in. Then, we go to ‘http://10.10.197.97/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F’, ‘http://10.10.197.97/?proxy=http%3A%2F%2Flist.hohoho%3A80’, ‘http://10.10.197.97/?proxy=http%3A%2F%2Flist.hohoho%3A22’, ‘http://10.10.197.97/?proxy=http%3A%2F%2Flocalhost’ to check what is displayed on the pages. Afterwards, we go to ‘http://10.10.197.97/?proxy=http%3A%2F%2Flist.hohoho.localtest.me’, and it shows the

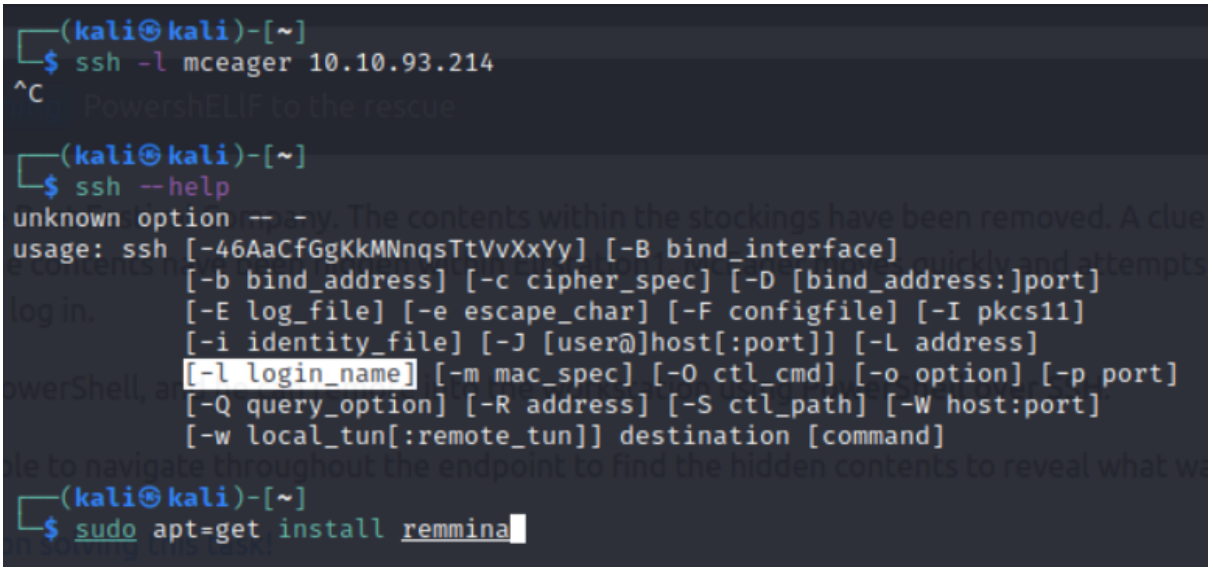
message from Elf McSkidy which contains the password of the admin (Be good for goodness sake!) . We guess the username correctly (Santa) and key in the password, it leads us to the admin.php, and there is a button for us to delete naughty list. We press the button, and it shows the flag to us (THM{EVERYONE_GETS_PRESENTS}).

Day 20 Blue Teaming - PowershELIF to the rescue

Tools used: Kali Linux, Powershell

Solution/Walkthrough: John Hammond

Question1 : Check the ssh manual. What does the parameter -l do?



Question2 : Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

```
PS C:\Users\mceager> Get-ChildItem


    Directory: C:\Users\mceager


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        12/7/2020  10:29 AM                3D Objects
d-r---        12/7/2020  10:29 AM                Contacts
d-r---        12/7/2020  11:26 AM                Desktop
d-r---        12/7/2020  11:26 AM                Documents
d-r---        12/7/2020  10:29 AM                Downloads
d-r---        12/7/2020  10:29 AM                Favorites
d-r---        12/7/2020  10:29 AM                Links
d-r---        12/7/2020  10:29 AM                Music
d-r---        12/7/2020  10:29 AM                Pictures
d-r---        12/7/2020  10:29 AM                Saved Games
d-r---        12/7/2020  10:29 AM                Searches
d-r---        12/7/2020  10:29 AM                Videos


PS C:\Users\mceager> Set-Location Documents
PS C:\Users\mceager\Documents> get-childitem -File -Hidden


    Directory: C:\Users\mceager\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a-hs-        12/7/2020  10:29 AM            402 desktop.ini
-arh--       11/18/2020   5:05 PM             35 e1fone.txt


PS C:\Users\mceager\Documents> cat e1fone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\Documents> @s
```

Question3: 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?

```
PS C:\Users\mceager\Desktop> cd .\elf2wo\
PS C:\Users\mceager\Desktop\elf2wo> get-childitem


    Directory: C:\Users\mceager\Desktop\elf2wo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/17/2020  10:26 AM             64 e70smsW10Y4k.txt


PS C:\Users\mceager\Desktop\elf2wo> cat e70smsW10Y4k.txt
I want the movie Scrooged <3!
PS C:\Users\mceager\Desktop\elf2wo>
```

Question4: 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)

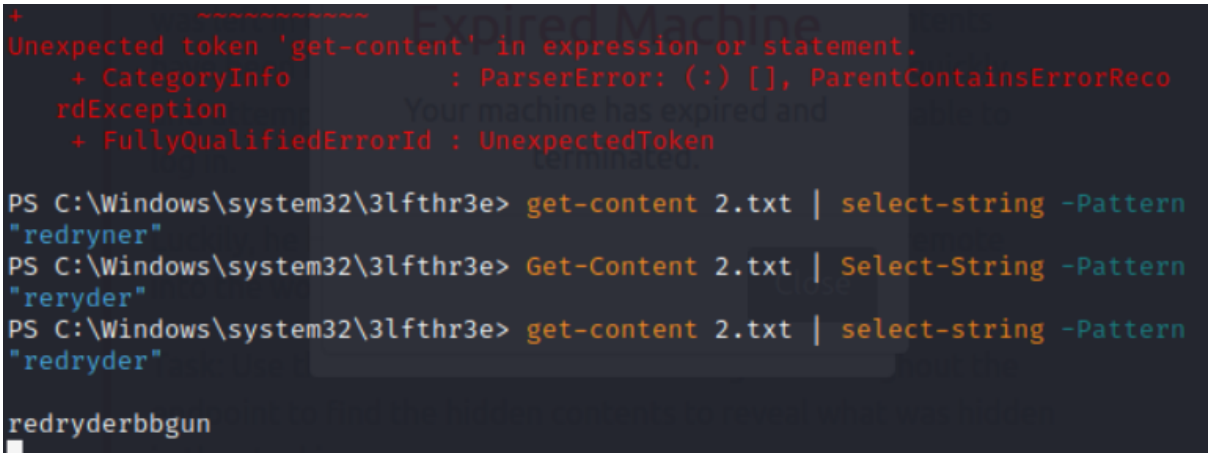
Question5: How many words does the first file contain?

```
    Directory: C:\Windows\system32\3lfthr3e


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-arh--        11/17/2020  10:58 AM          85887 1.txt
-arh--        11/23/2020   3:26 PM       12061168 2.txt


PS C:\Windows\system32\3lfthr3e> get-content 1.txt | measure-object


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


PS C:\Windows\system32\3lfthr3e>
```

Question5: What 2 words are at index 551 and 6991 in the first file?

```
PS C:\Windows\system32\3lfthr3e> (Get-Content -Path 1.txt)[551,6991]
Red
Ryder
PS C:\Windows\system32\3lfthr3e>
```

Question6: 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)



Thought Process/Methodology:

For Question1, using the parameter --help we can know what parameter -l do. After that we connect to the mceager remote machine then to the powershell. After that we set-location to the documents directory and u the get-childitem cmdlet with -file and -Hidden to search for what the elf1 wants. After that, we use the same method we used at elf1 to elf2 and 3.For q3, we use get-content filename | measure objects to know how many words are in the file. To find the index 551 and 6991 , we use (getcontent -Path filename)[indexnumber] to search for the index. For q6 to find what elf3 wants in the second file, we use select-string"xxx"to search through the second file to find the related phrase.