PSP0201 Week 5 Writeup

Group Name: AIA

Members

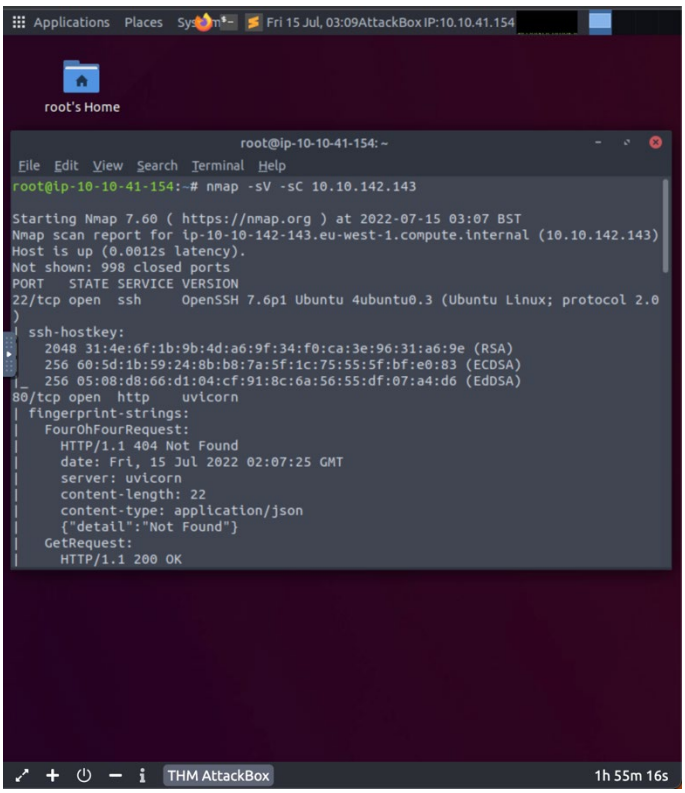
ID	Name	Role
1211103201	Muhammad Al-Amin Bin Mohd Marzuki	Leader
1211103217	Alif Durrani bin Zahari	Member
1211103140	Ahmad Nur Ikhwan Bin Hamid	Member
1211101810	Lim Jia Hao	Member

Day 16: Scripting – Help! Where is Santa?
Tools used: Firefox
Solution/walkthrough:

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

Ans: 80

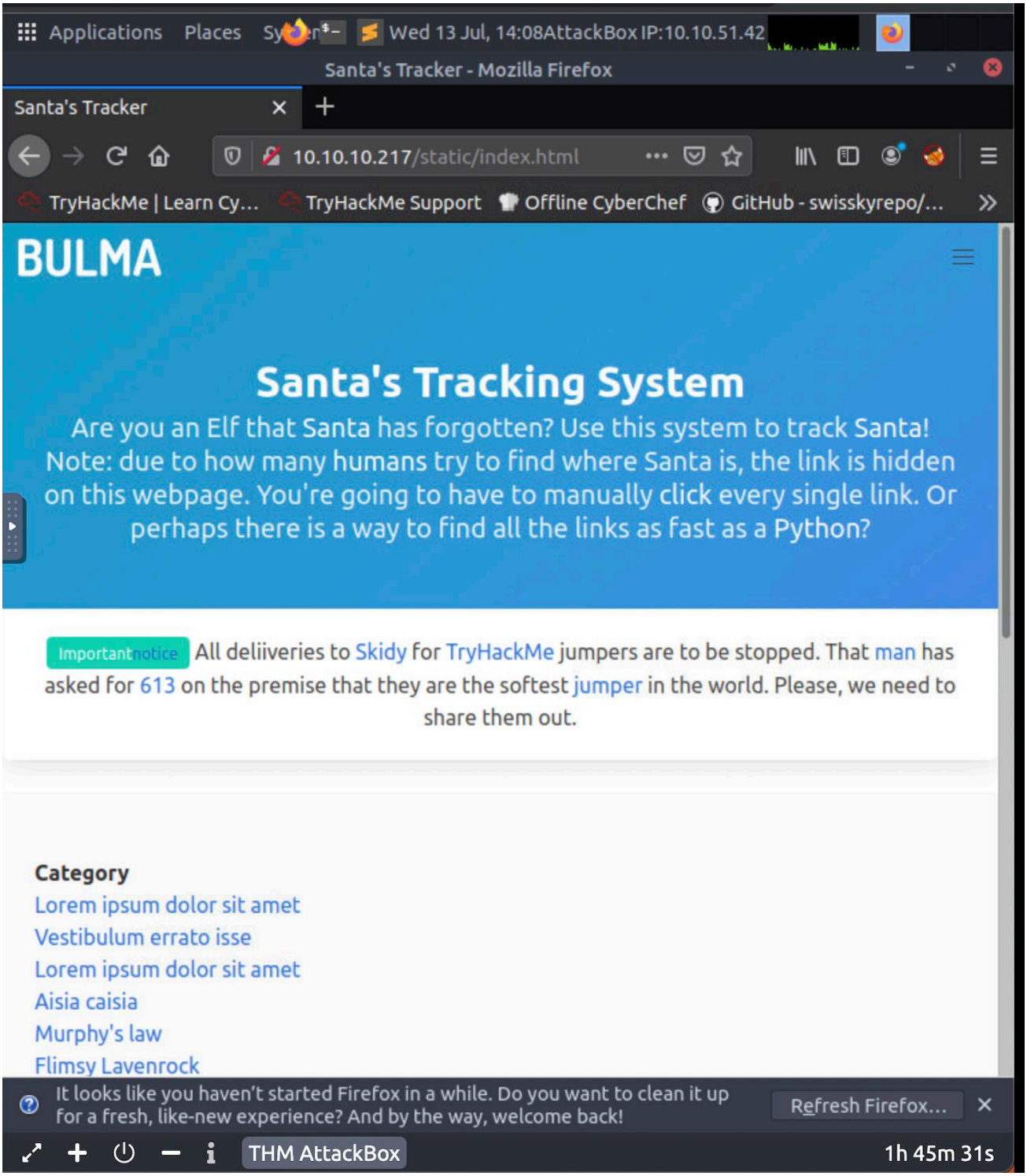
With the command of nmap -sC -sV [MACHINE_ID] to get all the ports and search for port with service http.



Question 2
What templates are being used?

ANS: BULMA

Enter the website given ([MACHINE_ID]/static/index.html) in the browser and will get the templates at the top left of the website.



Question 3

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

ANS: /api/

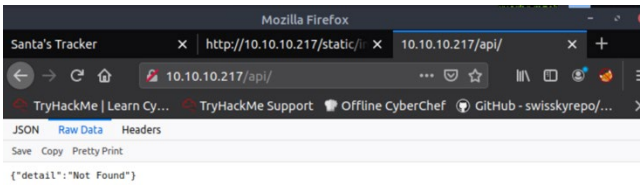
View the page source in the website that we visit just now and get the directory of api.

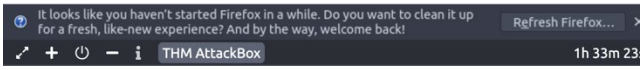
Question 4

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

ANS: {"detail":"Not Found"}

Enter [MACHINE_ID]/api/ in the browser without any API key and will get the raw data.



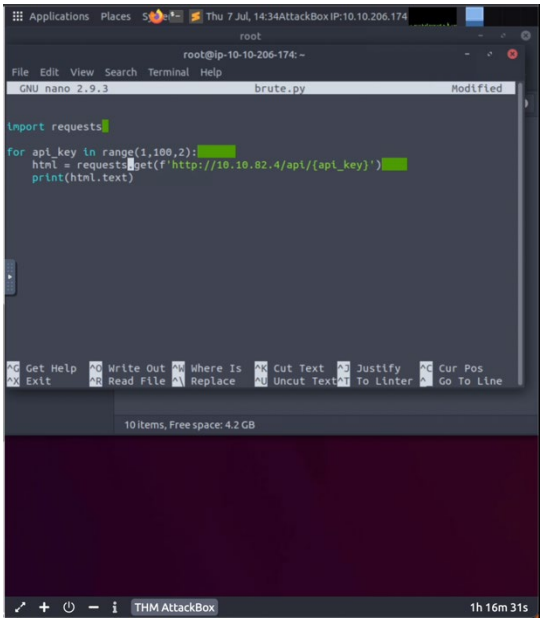


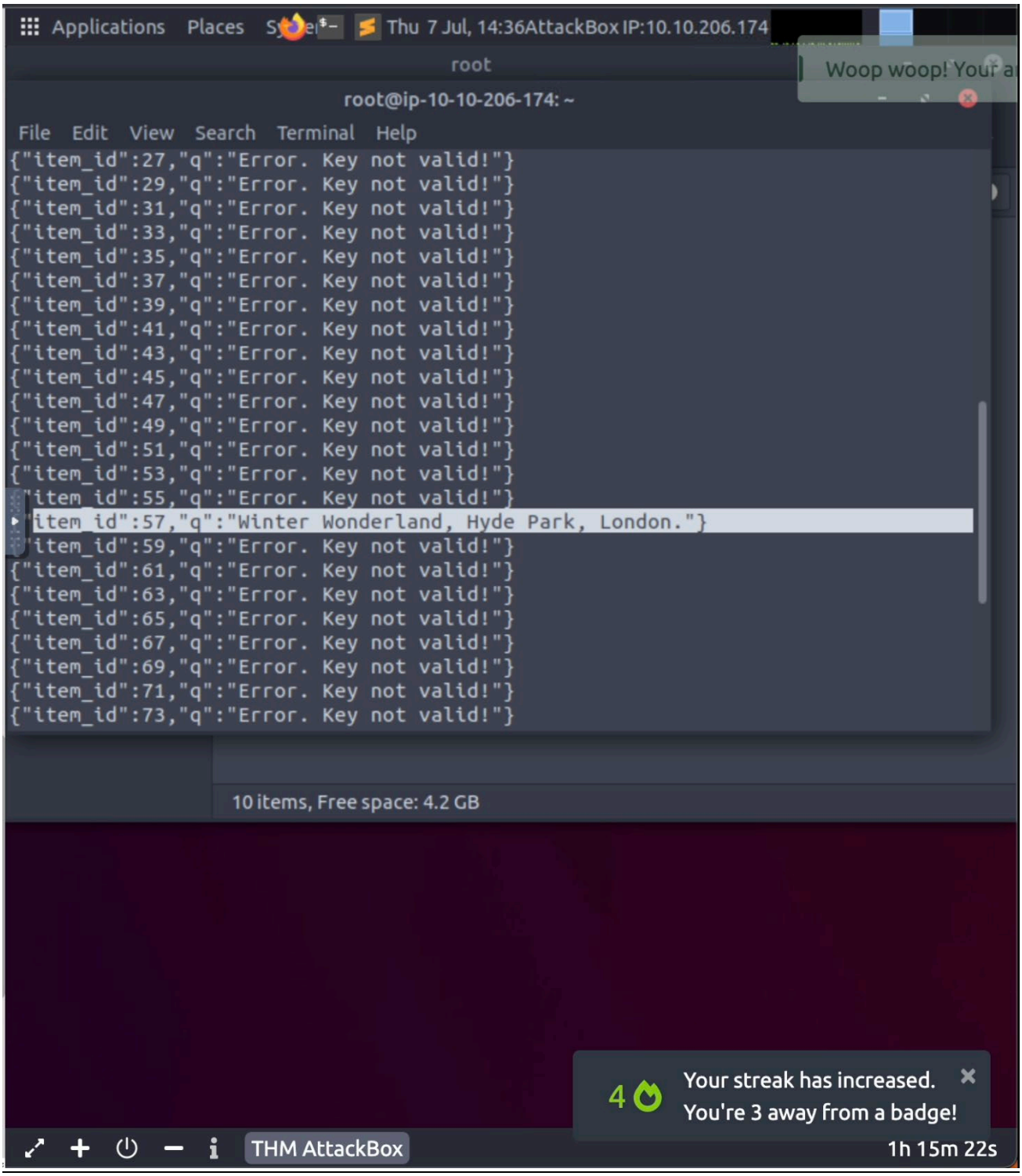
Question 5

Where is Santa right now?

ANS: Winter Wonderland, Hyde Park, London

Create an empty python file and edit it with the code below and enter the command of ‘python3 [FILENAME].py’ after saving the file to get the where is Santa right now.



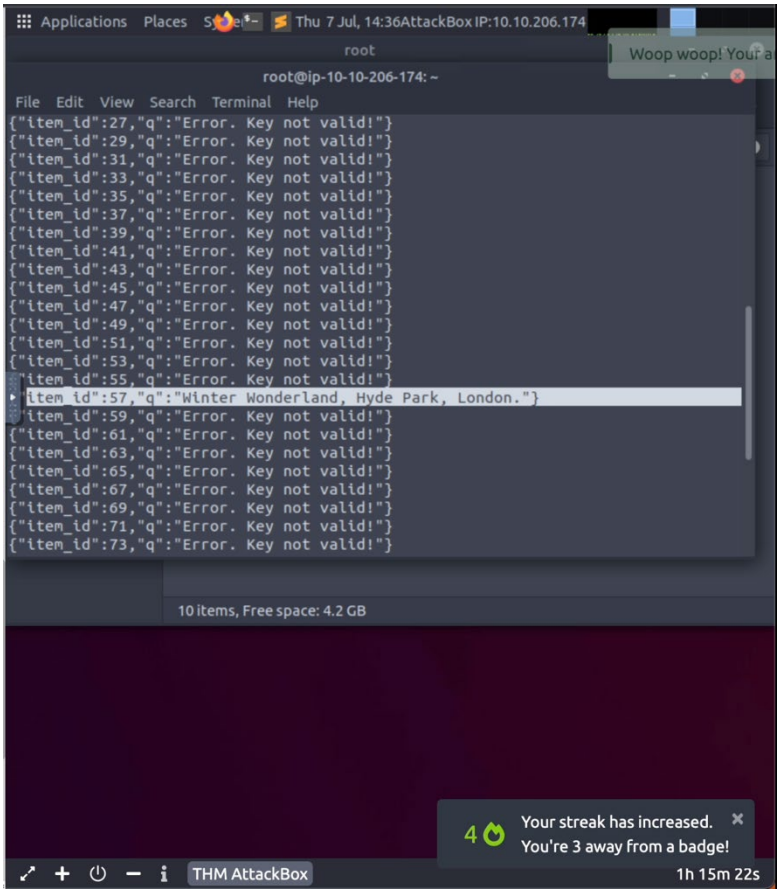


Question 6

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)

ANS: 57

Create an empty python file and edit it with the code below and enter the command of ‘python3 [FILENAME].py’ after saving the file to get the correct API key.



Thought Process/Methodology:

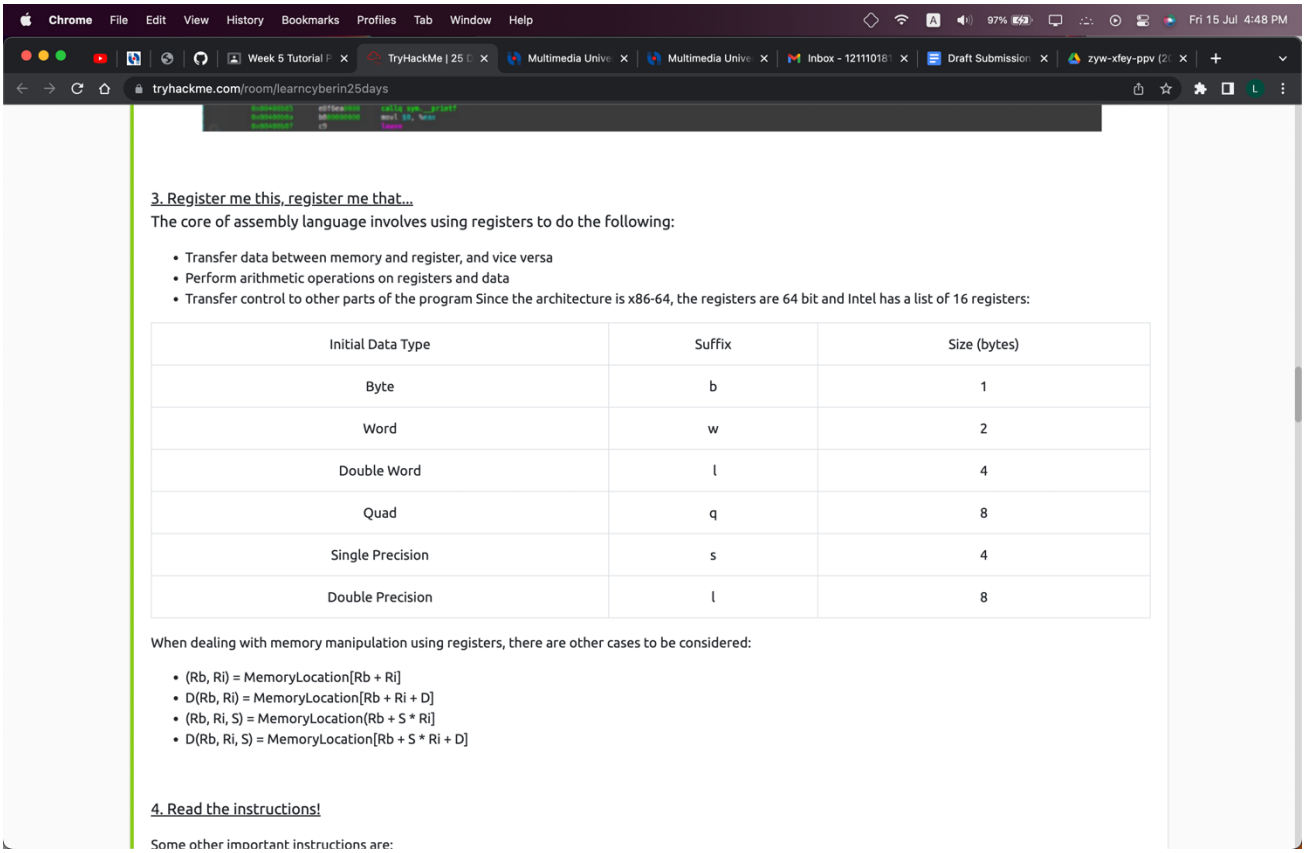
Firstly, in order to get the port number of http service, we need to use nmap command. The templates can get it from the website given ([MACHINE_ID]/static/index.html) and view the page source to get the directory of API in the source code. Next, we enter [MACHINE_ID]/api/ which means without parameter entered and get the raw data. Besides, we need to create a py file and edit it by the command nano. We need to import the library of ‘Request’ in the code. The sample code is provided in the image above. Finally, we just need to run the file by using the command ‘python3 [filename].py’ in order to get the correct API key follow by the place that Santa are right now.

Day 12: Reverse Engineering – ReverseELFneering
Tools used: Firefox
Solution/walkthrough:

Question 1
Match the data type with the size in bytes:
ANS:

	1	2	4	8
Byte	◉	○	○	○
Word	○	◉	○	○
Double Word	○	○	◉	○
Quad	○	○	○	◉
Single Precision	○	○	◉	○
Double Precision	○	○	○	◉

Get the answer from the table above at THM website.



3. Register me this, register me that...

The core of assembly language involves using registers to do the following:

- Transfer data between memory and register, and vice versa
- 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]
- (Rb, Ri, S) = MemoryLocation(Rb + S * Ri]
- D(Rb, Ri, S) = MemoryLocation[Rb + S * Ri + D]

4. Read the instructions!

Some other important instructions are:

Question 2

What is the command to analyse the program in radare2?

Ans: aa

Get it from the text in THM website

IP Address: `10.10.16.29`

Username: elfmceager

Password: adventofcyber

Let's proceed to run through how Radare2 works exactly. Although you shouldn't do this if the program is unknown, it is safe for us to execute to 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?`

3. Computer says...Done?!

Once the analysis is complete, you would want to know where to start analysing from - most programs have an entry point defined as main. To find a list of the functions run: `afl`

```
[0x00400a30]> afl | grep main
```

Question 3

What is the command to set a breakpoint in radare2?

Ans : db

Get it from the text in THM website

```
0x00400b6b      8945fc          movl %eax, local_4h
0x00400b6e      8b4dfc          movl local_4h, %ecx
0x00400b71      8b55f8          movl local_8h, %edx
0x00400b74      8b45f4          movl local_ch, %eax
0x00400b77      89c6            movl %eax, %esi
0x00400b79      488d3d881409.   leaq str.the_value_of_a_i
0x00400b80      b800000000      movl $0, %eax
```

The line starting with sym.main indicates we're looking at the main function. The next 3 lines are used to represent the variables stored in the function. The 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.

```
0x00400a30]> pdf @main
            ;-- main:
(fcn) sym.main 68
  sym.main (int argc, char **argv, char **envp);
            ; var int local_ch @ rbp-0xc
            ; var int local_8h @ rbp-0x8
            ; var int local_4h @ rbp-0x4
            ; DATA XREF from entry0 (0x400a4d)
            0x00400b4d      55              pushq %rbp
            0x00400b4e      4889e5          movq %rsp, %rbp
            0x00400b51      4883ec10        subq $0x10, %rsp
            0x00400b55 b    c745f4040000.   movl $4, local_ch
```

Now that we've set a breakpoint, let's run the program using `dc`

Question 4

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

Ans: dc

Get it from the text in THM website

```
0x00400b55 b    c745f4040000.  movl $4, local_ch
```

Now that we've set a breakpoint, let's run the program using `dc`

```
[0x00400a30]> dc
hit breakpoint at: 400b55
[0x00400b55]> pdf
            ;-- main:
            ;-- rax:
/ (fcn) sym.main 68
|   sym.main (int argc, char **argv, char **envp);
|           ; var int local_ch @ rbp-0xc
|           ; var int local_8h @ rbp-0x8
|           ; var int local_4h @ rbp-0x4
|           ; DATA XREF from entry0 (0x400a4d)
|           0x00400b4d      55              pushq %rbp
|           0x00400b4e      4889e5          movq %rsp, %rbp
|           0x00400b51      4883ec10        subq $0x10, %rsp
```

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:

```
[0x00400b55]> px @ rbp-0xc
- offset -       0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x7ffc914f7bc4  0000 0000 1890 6b00 0000 0000 7018 4000  ......k.....p.@.
0x7ffc914f7bd4  0000 0000 1911 4000 0000 0000 0000 0000  ......@.........
0x7ffc914f7be4  0000 0000 0000 0000 0100 0000 f87c 4f91  .............|O.
0x7ffc914f7bf4  fc7f 0000 4d0b 4000 0000 0000 0000 0000  ....M.@.........
0x7ffc914f7c04  0000 0000 0600 0000 8e00 0000 8000 0000  ................
0x7ffc914f7c14  0a00 0000 0000 0000 0000 0000 0000 0000  ................
0x7ffc914f7c24  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x7ffc914f7c34  0000 0000 0000 0000 0000 0000 0004 4000  ..............@.
```

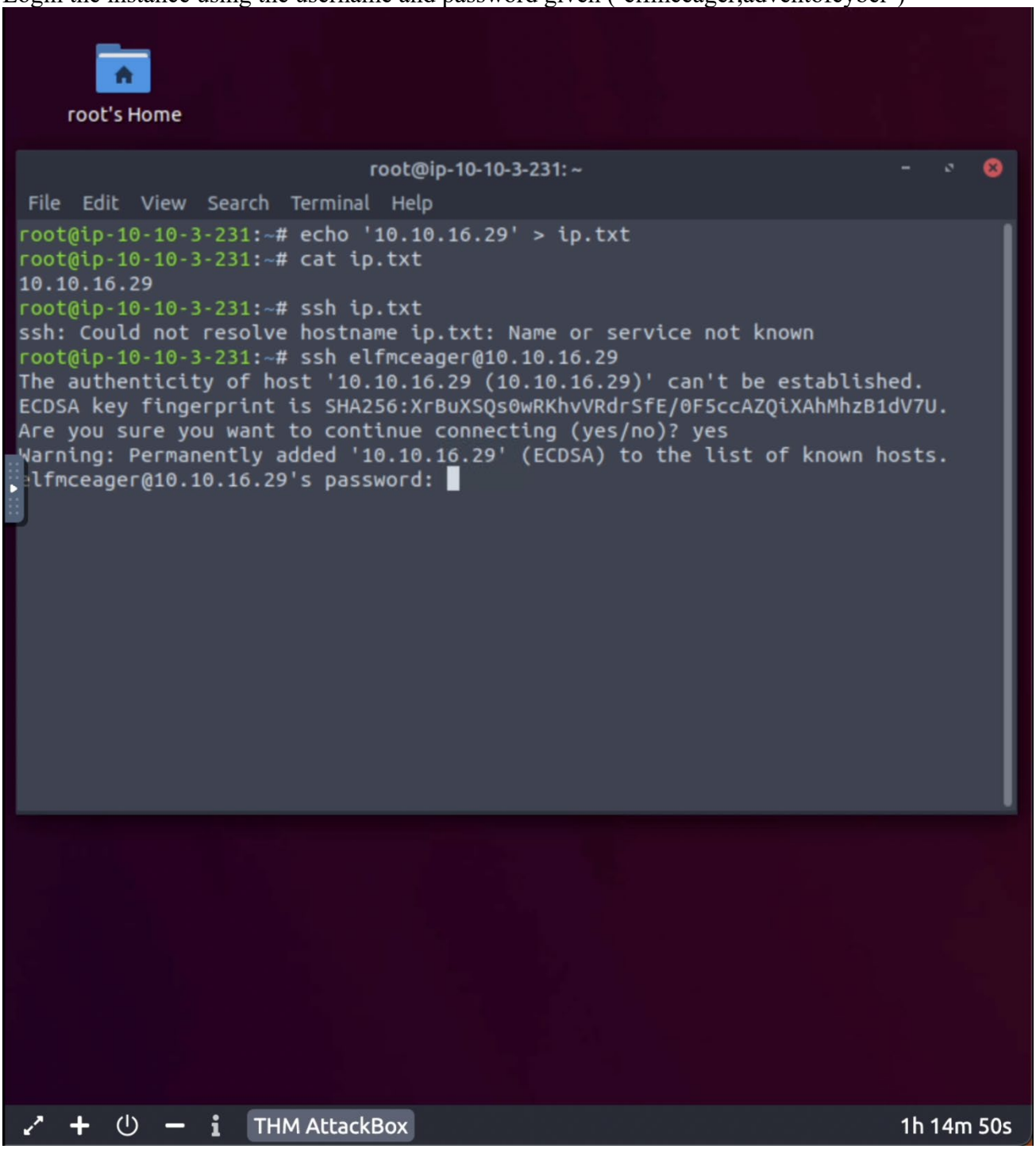
Question 5

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

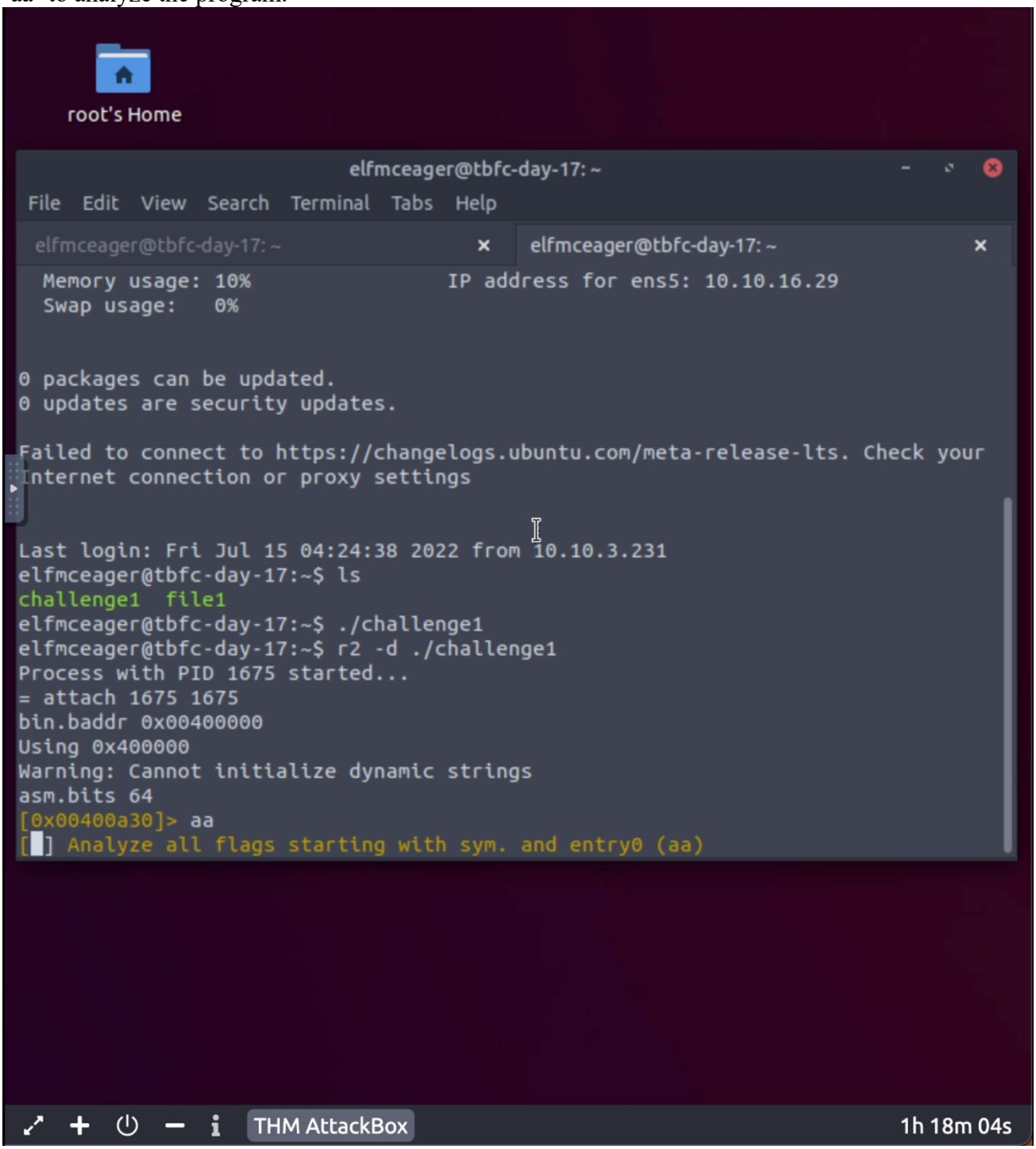
Answer as a numerical digit.

Ans: 1

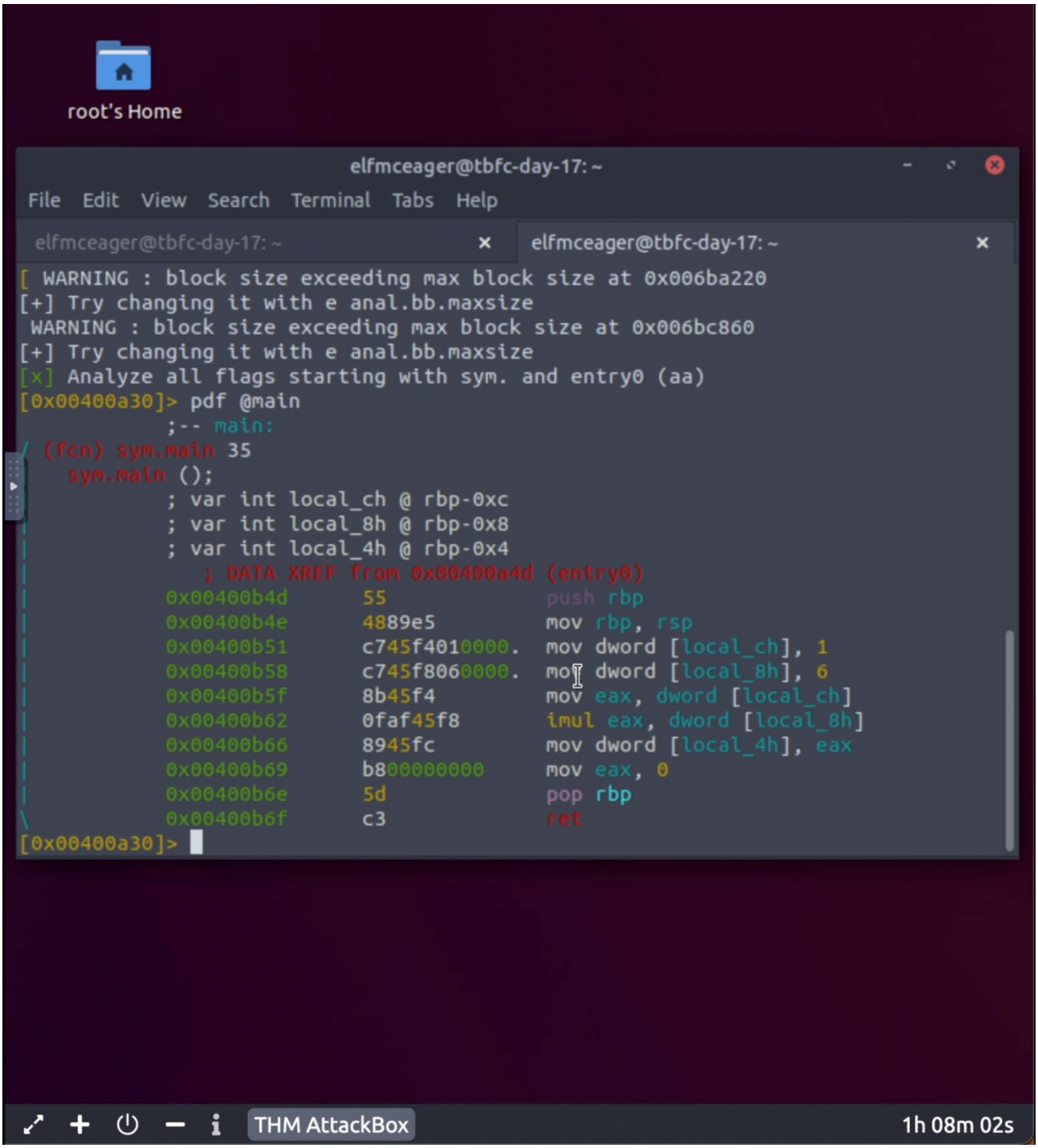
Login the instance using the username and password given (‘elfmceager,adventofcyber’)



Get the file inside by using ‘ls’ command and run the radare command ‘r2 -d ./challenge1’ follow by ‘aa’ to analyze the program.



Examine the assembly code at main by running the code ‘pdf @main’ which means print disassembly function and we will get the answer for question 5 which is 1 from the source code below.

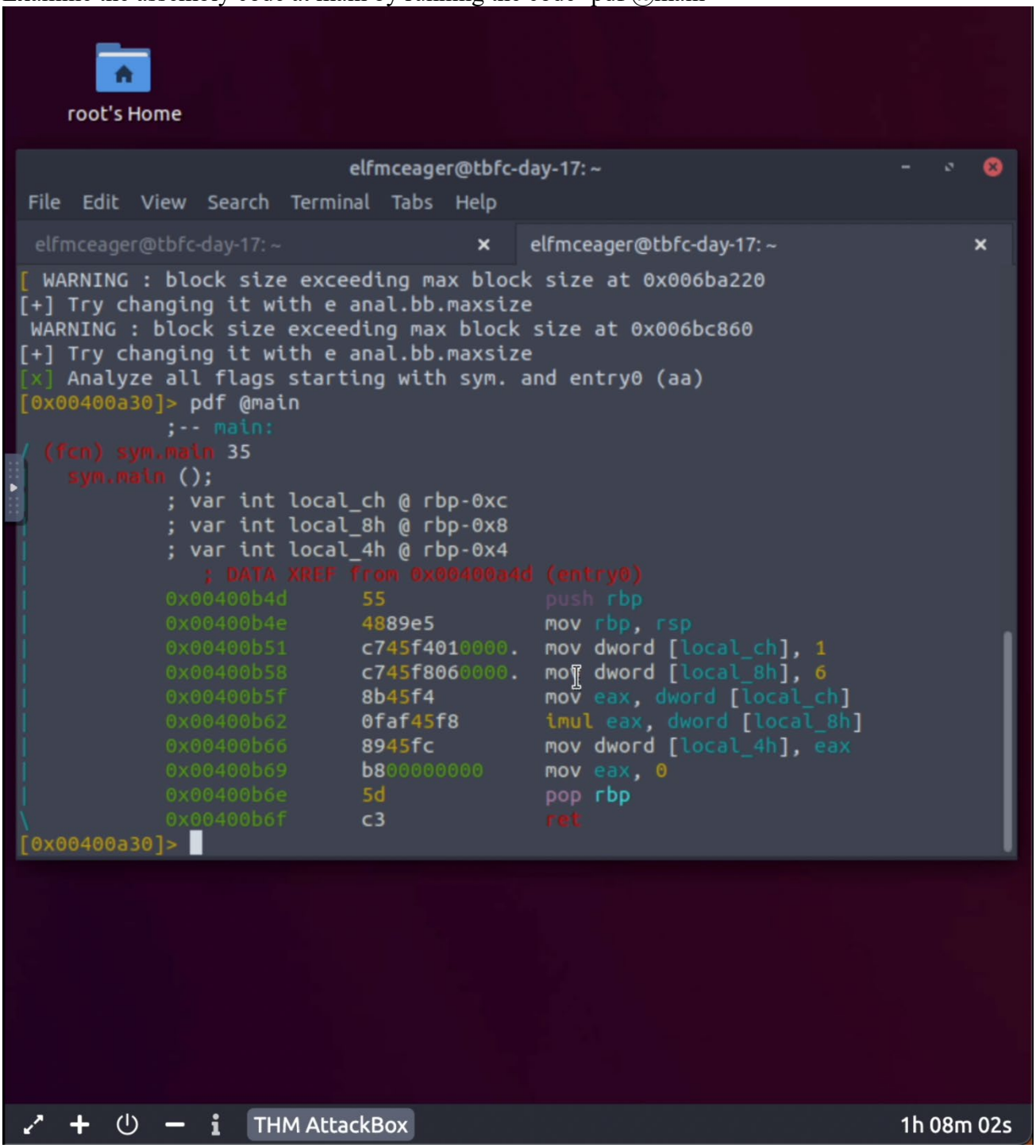


Question 6

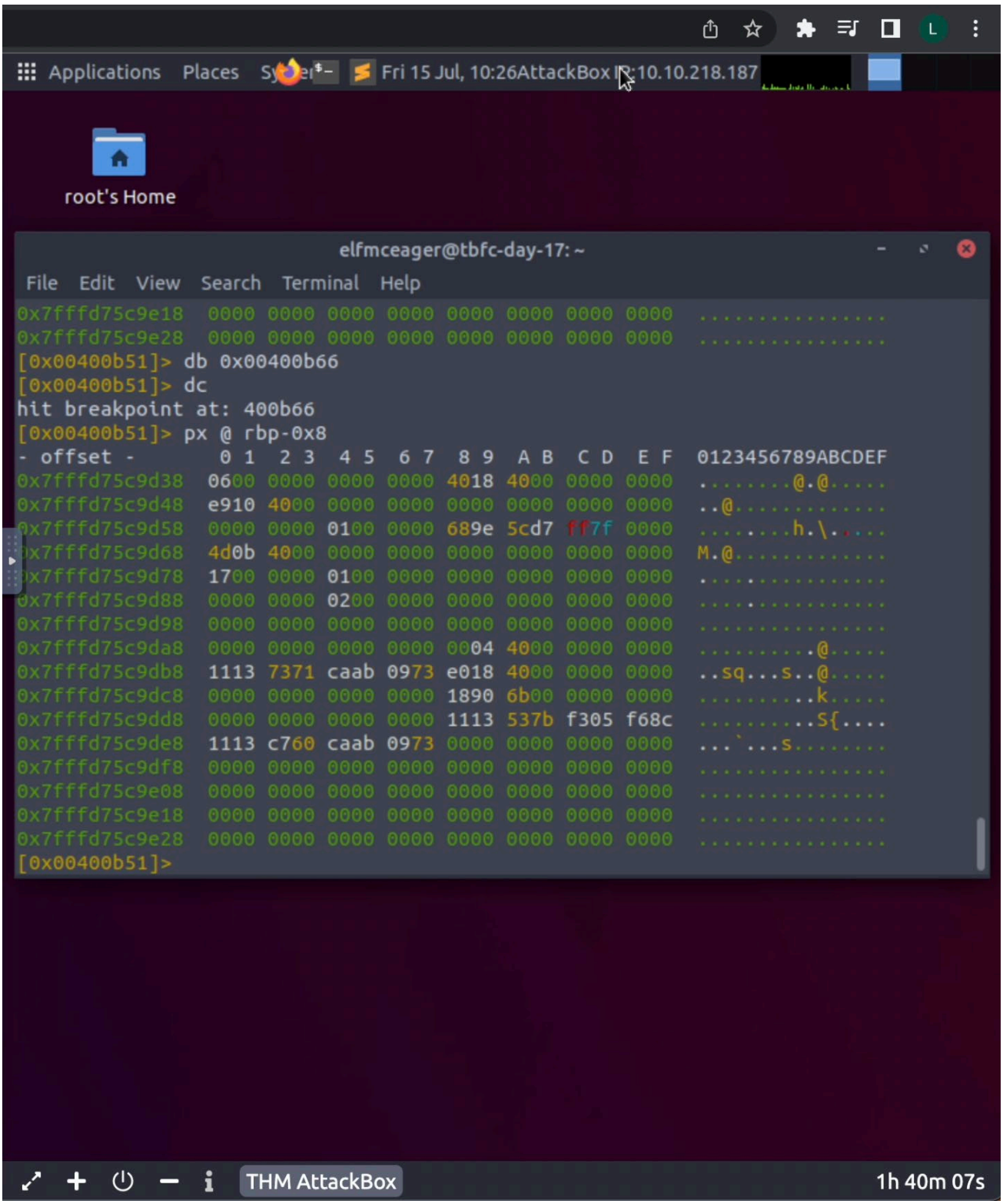
What is the value of eax when the imull instruction is called?

Ans: 6

Examine the assembly code at main by running the code ‘pdf @main’



Set the breakpoint on the memory address by using the command ‘db 0x00400b66’ and run the command ‘dc’ to execute the program until hitting the breakpoint. Next, in order to view the contents of the local_8h cause the imull eax is in local_8h by using the command ‘px @ rbp-0x8’ and get the answer at the first line first one which is 0600.

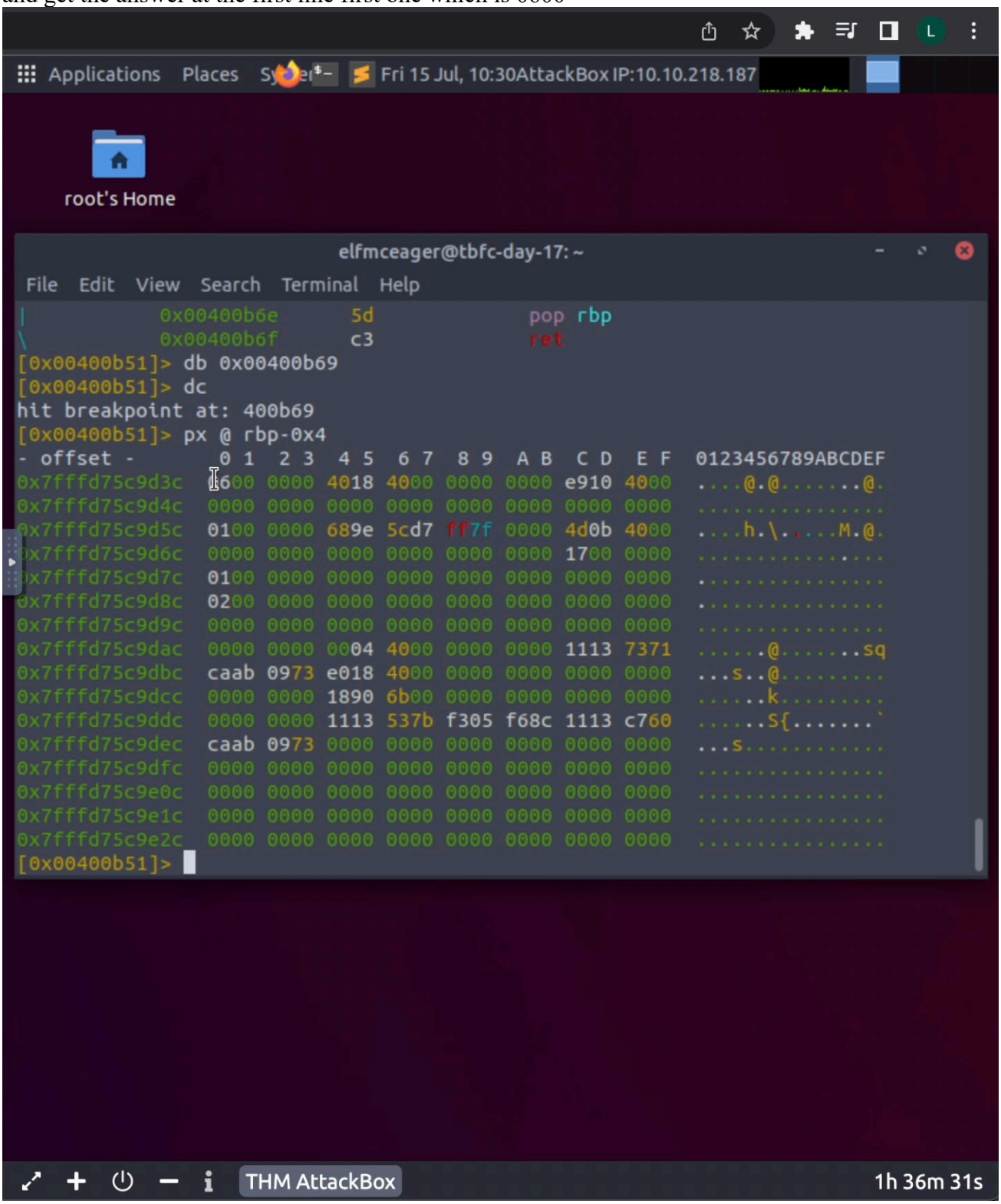


Question 7

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

Ans: 6

Set the breakpoint on the memory address by using the command ‘db 0x00400b69’ which return there ‘mov eax, 0’ and run the command ‘dc’ to execute the program until hitting the breakpoint. Next, in order to view the contents of the local_4h we will be using the command ‘px @ rbp-0x4’ and get the answer at the first line first one which is 0600

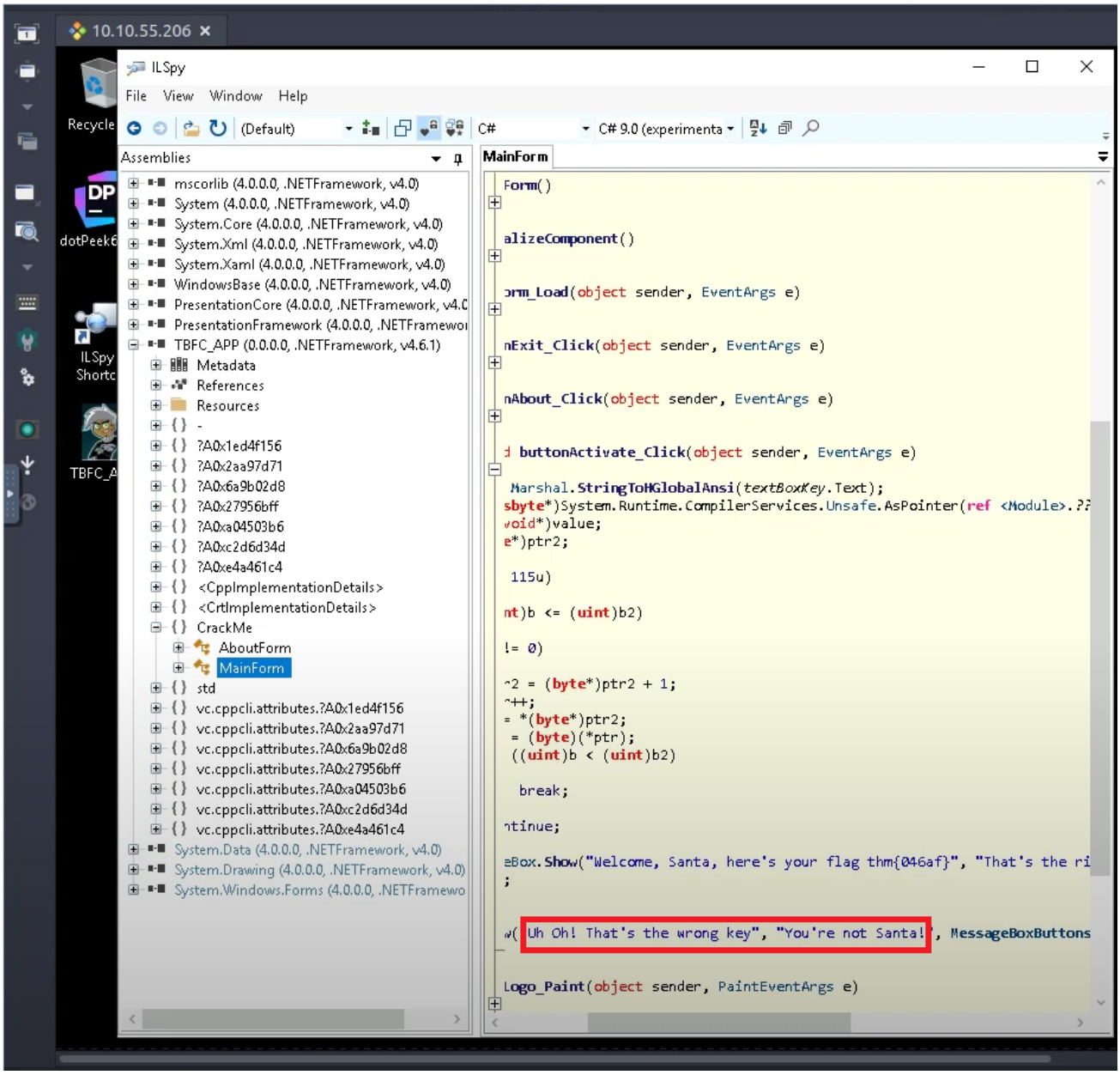


Thought Process/Methodology:

Firstly ,login the instance using the username and password given ('elfmceager,adventofcyber'). Get the file inside by using 'ls' command and run the radare command 'r2 -d ./challenge1' follow by 'aa' to analyze the program. Examine the assembly code at main by running the code 'pdf @main' which means print disassembly function and we will get the answer for question 5 which is 1 from the source code below. Examine the assembly code at main by running the code 'pdf @main' Set the breakpoint on the memory address by using the command 'db 0x00400b66' and run the command 'dc' to execute the program until hitting the breakpoint. Next, in order to view the contents of the local_8h cause the imull eax is in local_8h by using the command 'px @ rbp-0x8' and get the answer at the first line first one which is 0600. Set the breakpoint on the memory address by using the command 'db 0x00400b69' which return there 'mov eax, 0' and run the command 'dc' to execute the program until hitting the breakpoint. Finally, in order to view the contents of the local_4h, we will be using the command 'px @ rbp-0x4' and get the answer at the first line first one which is 0600.

Day 18: **Reverse Engineering The Bits Of Christmas**

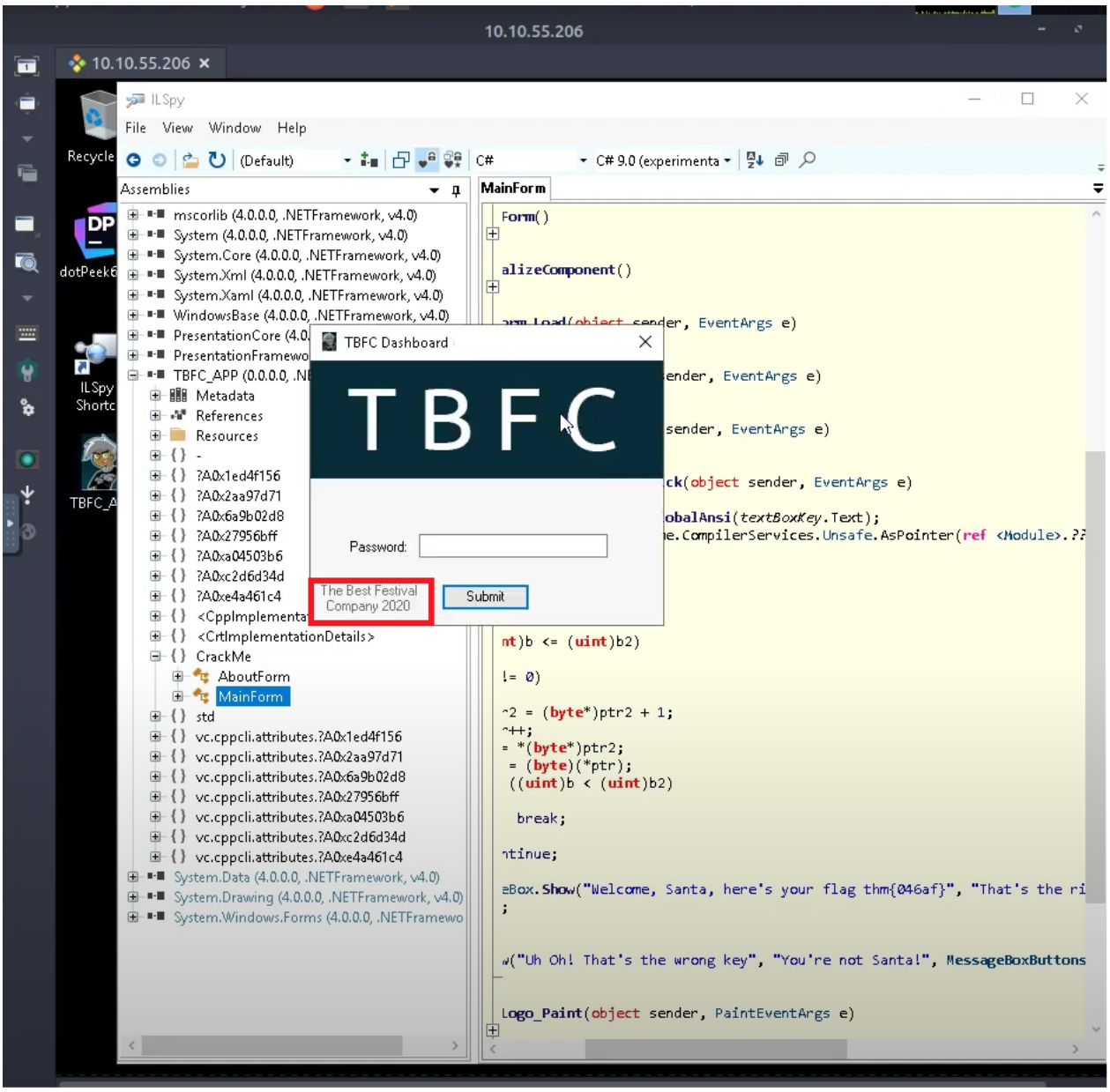
Q1: What is the message that shows up if you enter the wrong password for TBFC_APP?*
Follow the casing displayed on the message.



Ans: Uh Oh! That's the wrong key

It stated both inside the code and when you type in the wrong password.

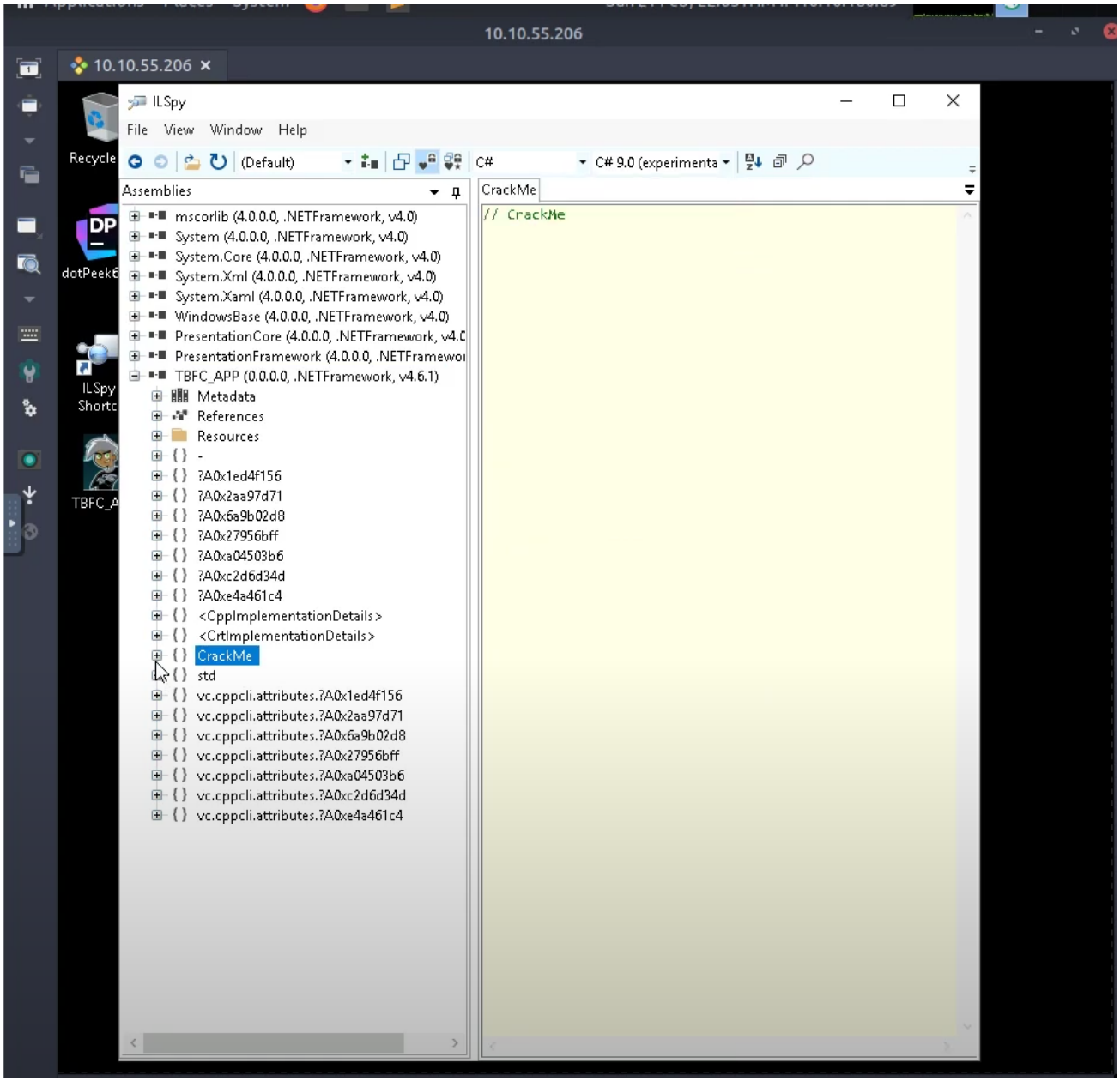
Q2: What does TBFC stand for?*



Ans: The Best Festival Company

Open the App and it is displayed at the bottom left corner.

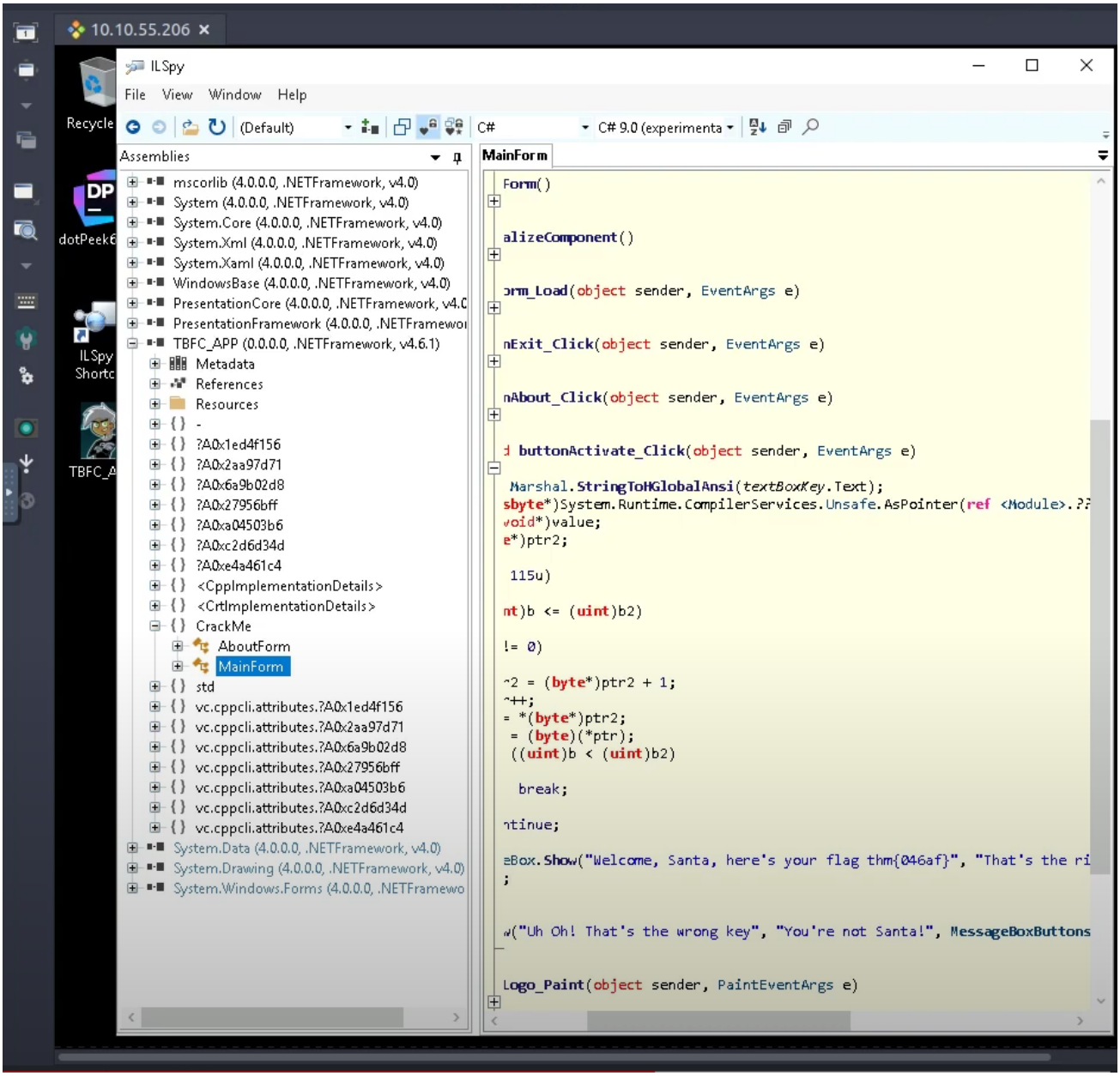
Q3: Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?



Ans: CrackMe

Seems to be quite fishy.

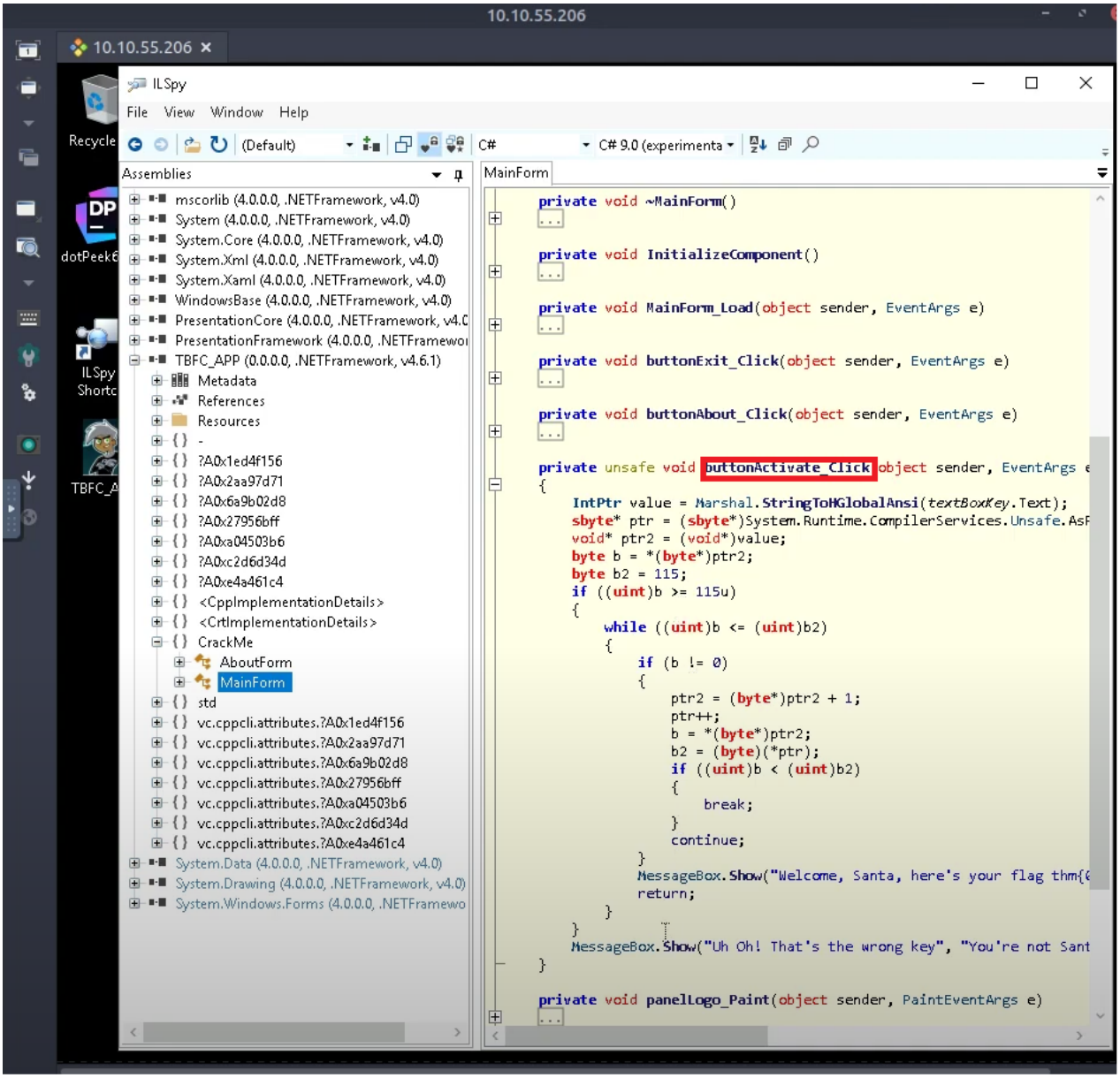
Q4: Within the module, there are two forms. Which contains the information we are looking for?



Ans: MainForm

The information we are looking for is indide the MainForm File.

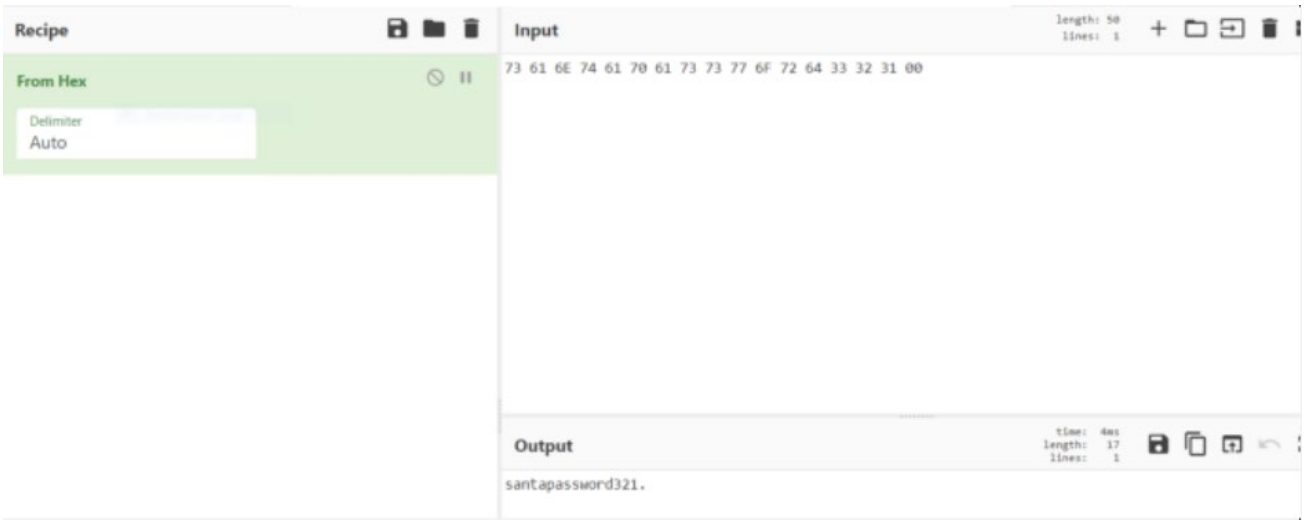
Q5: Which method within the form from Q4 will contain the information we are seeking?



Ans: buttonActivate_Click

The App runs on the buttonActivate, as stated in the public class MainForm. Scroll down and we can see the buttonActivate_Click

Q6: What is Santa's password?*

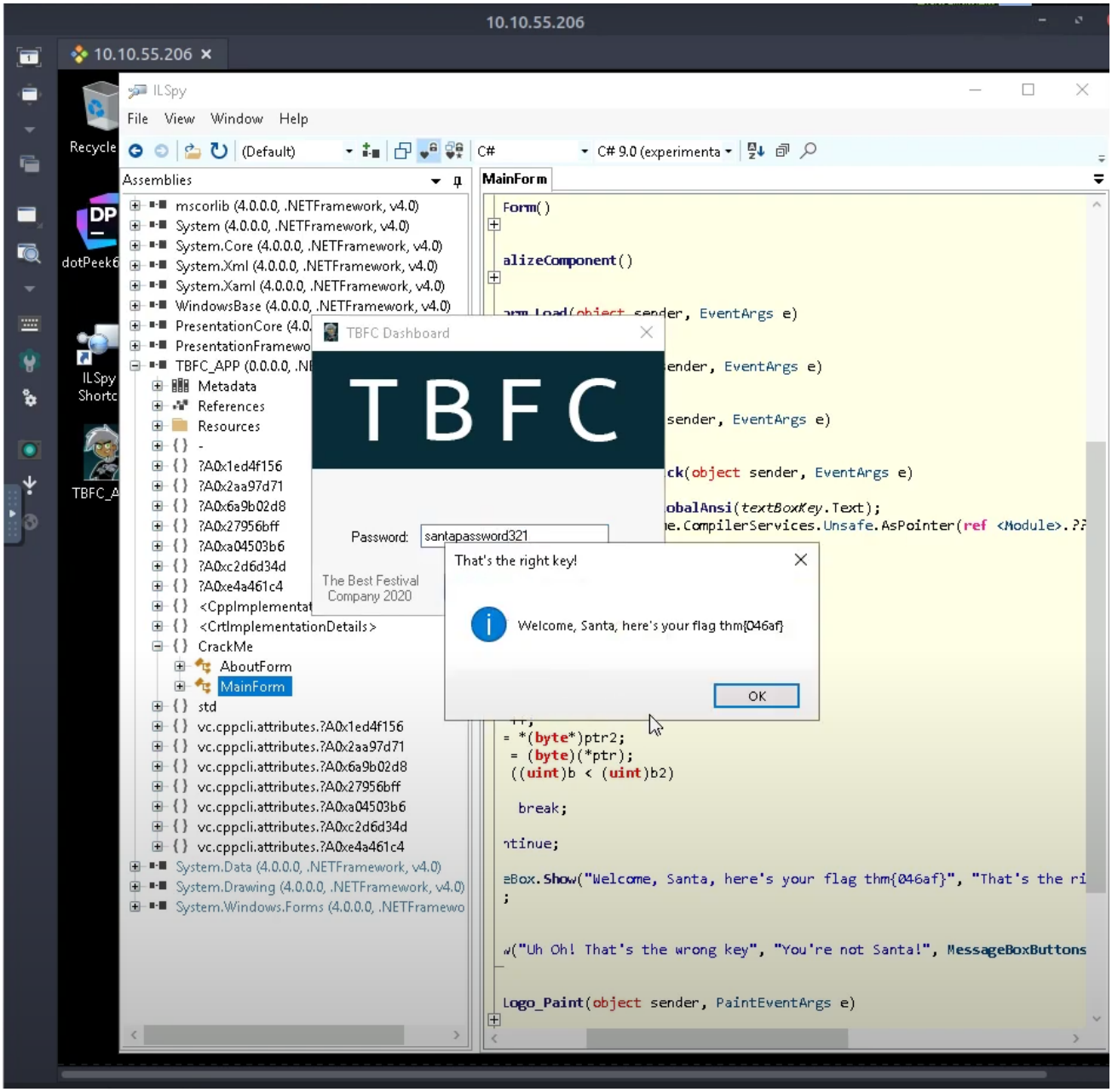


Ans: santapassword321

Use from hex in cyberchef, it will decode the code hence giving santa's Password which is santapassword321.

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

Copy and paste from THM



Ans: thm{046af}

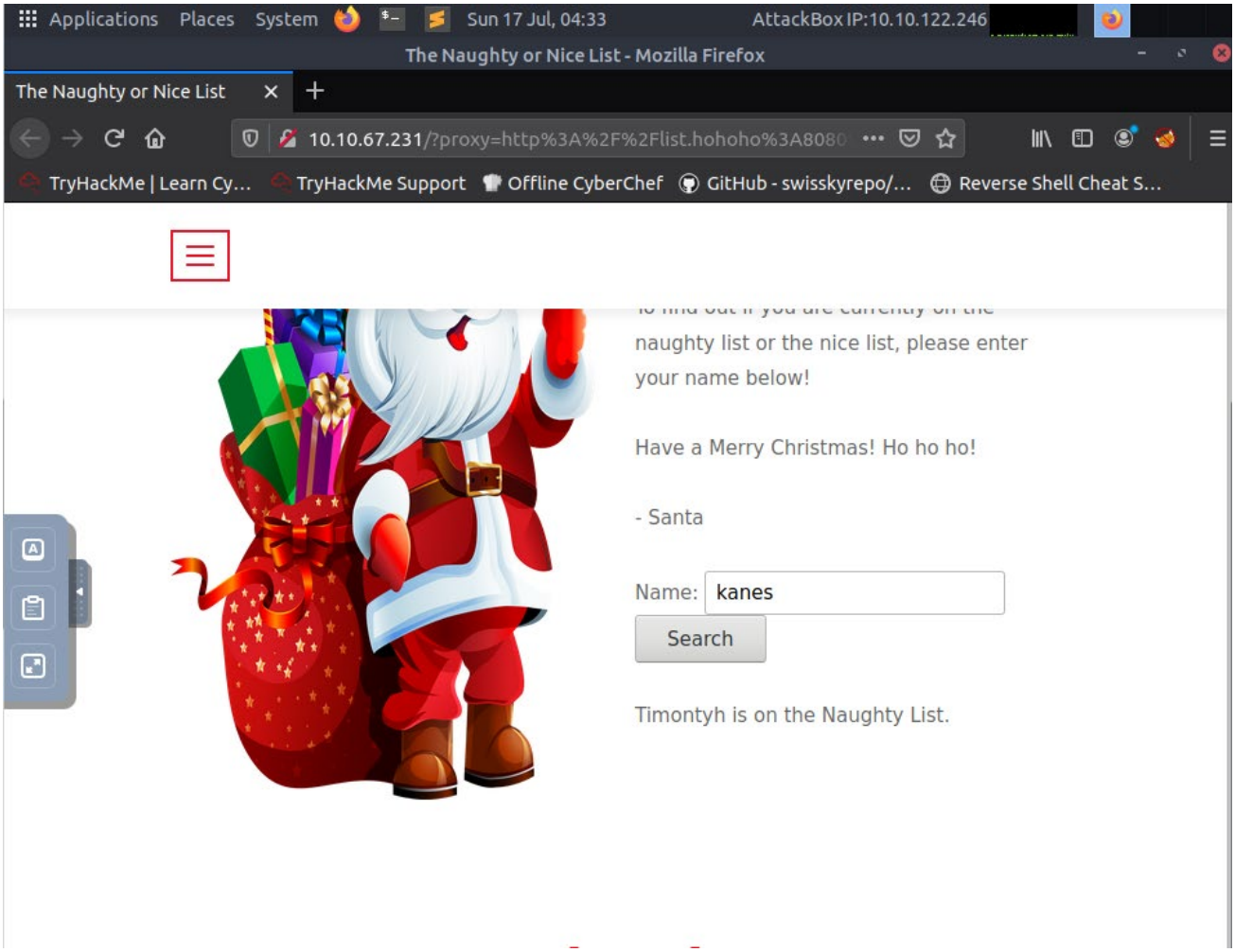
With the password obtain from cyberchef, enter the password in TBFC_APP

Methodology

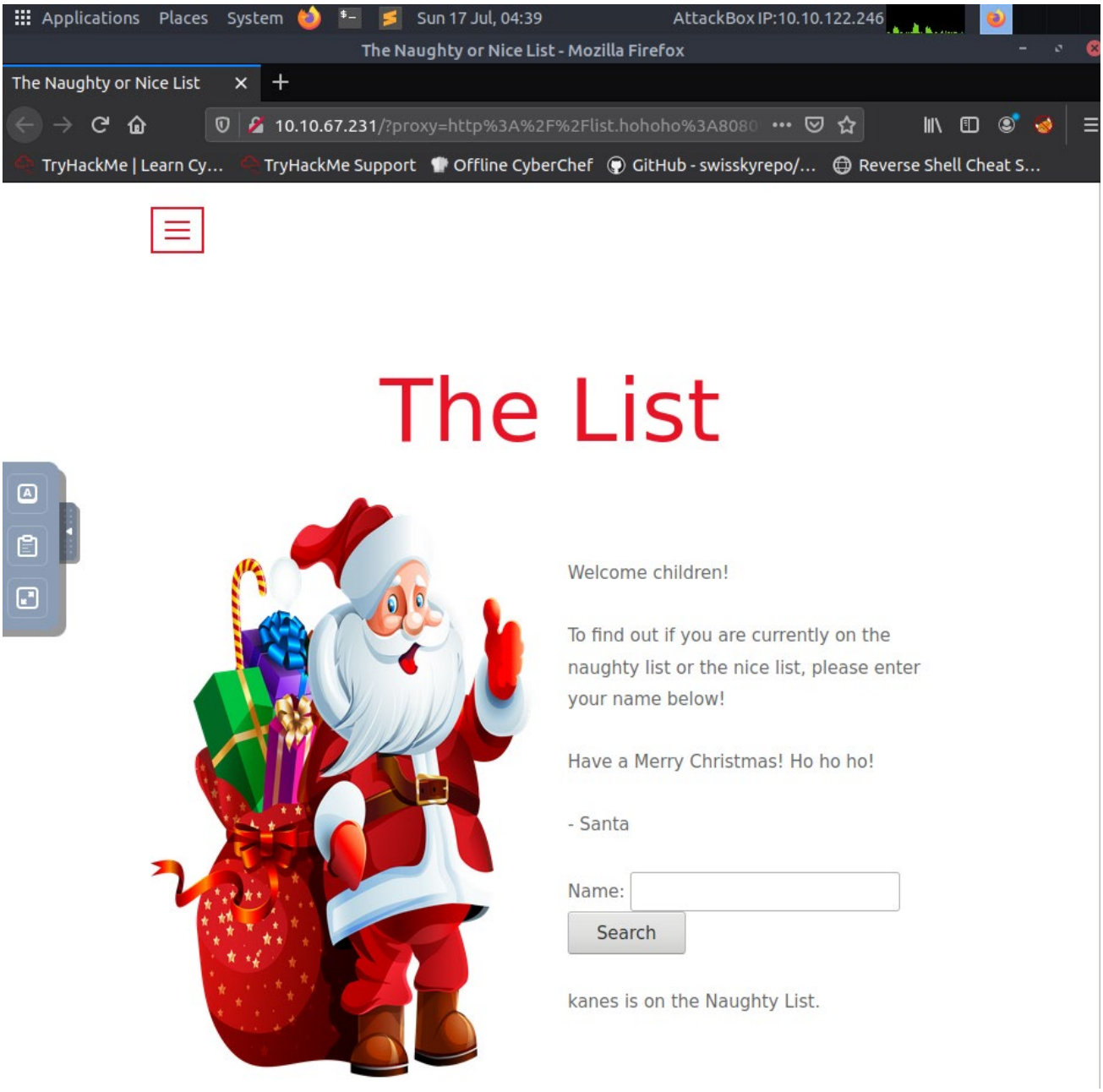
Open ILspy and deploy and in it open TBFC file. Then, access the CrackMe file inside the TBFC_APP file. After that, access the MainForm. Based on the File, to activatition of the App runs on the Source code in buttonActivation_Click. In cybercgef, Take "_c@_0BB@IKKDFEPG@santapassword321" in the format to hexadecimal and decode the code. The output will lead to Santa's password which is santapassword321. With Santa's Password, open TBFC_APP and place the password than capture the flag.

Day 19: **Web Exploitation** The Naughty or Nice List

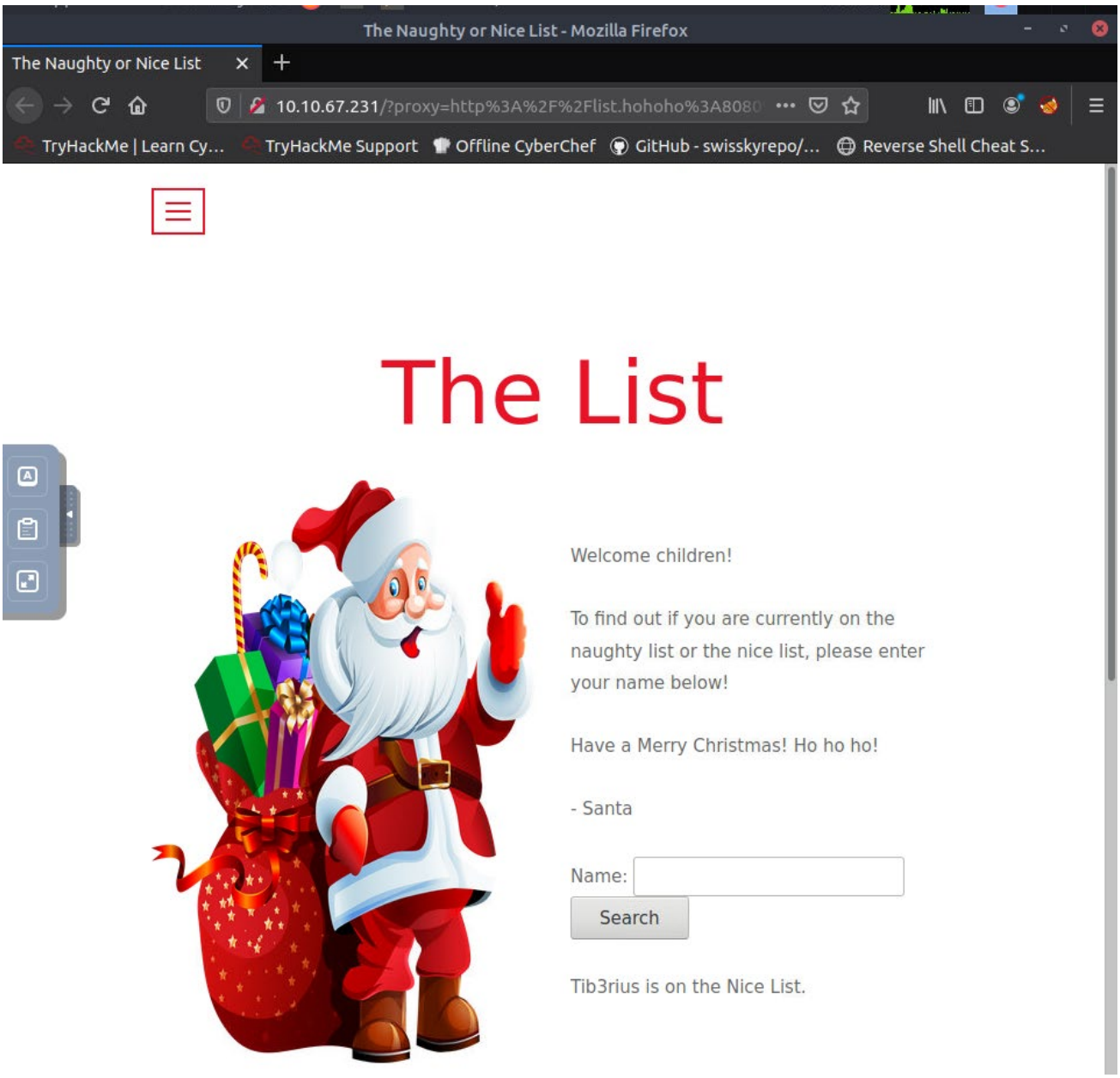
Q1: Which list is this person on?*
Select the proper words in the proper place of the command: [a] -c -z file,[b] http://[c].xyz/api.[d]?[e]=FUZZ



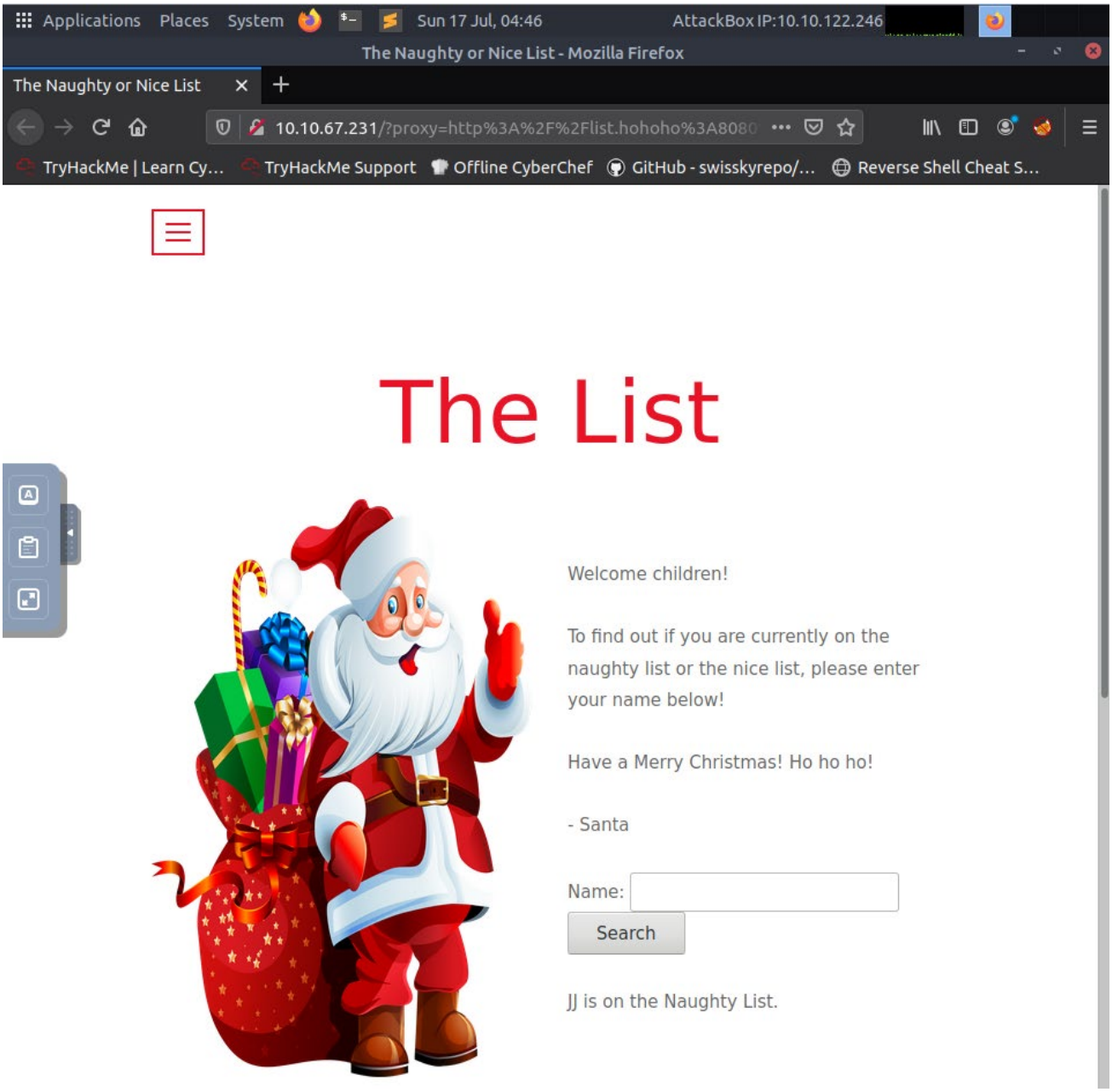
Timonty: Naughty



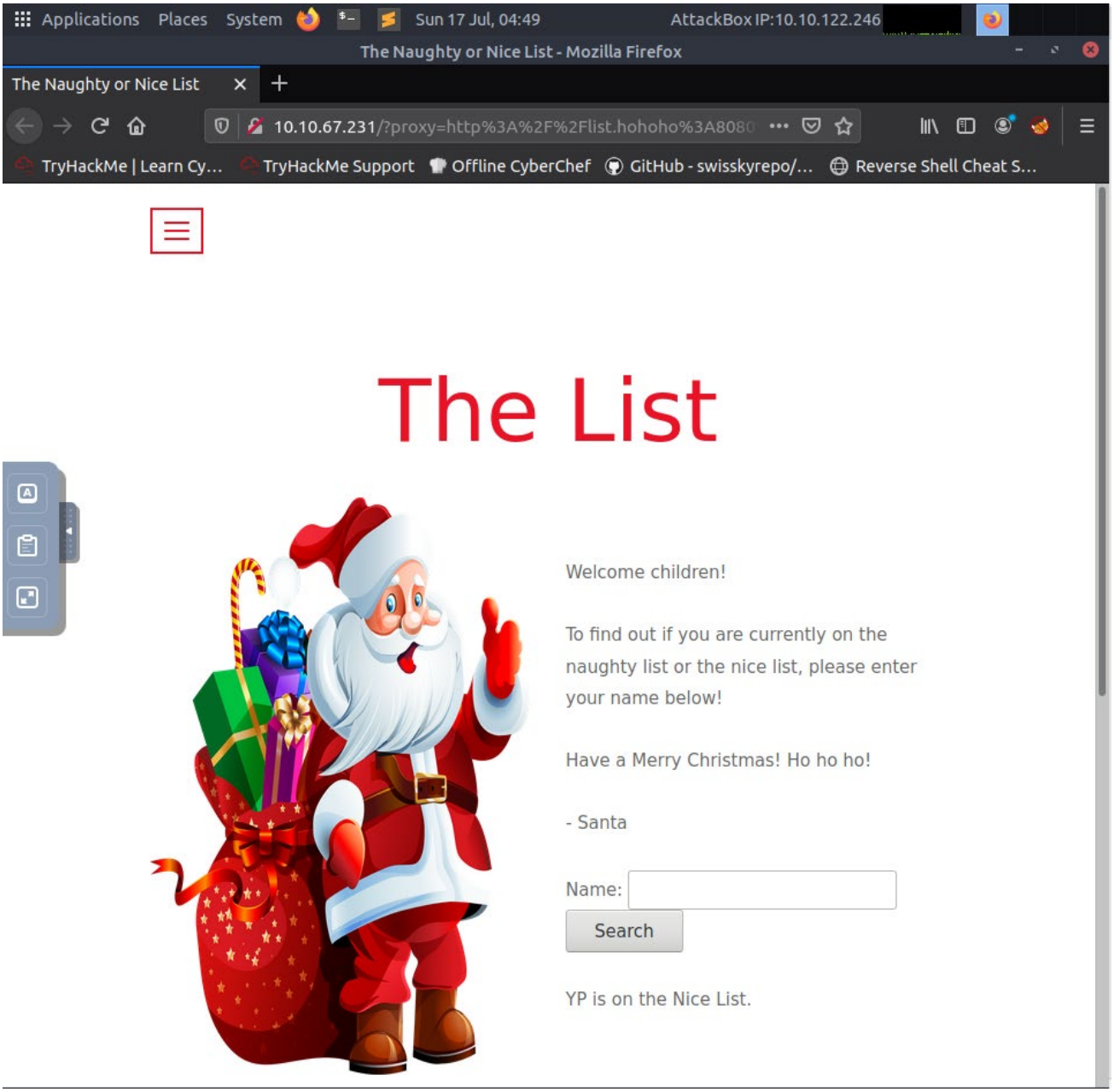
Kanes : Naughty



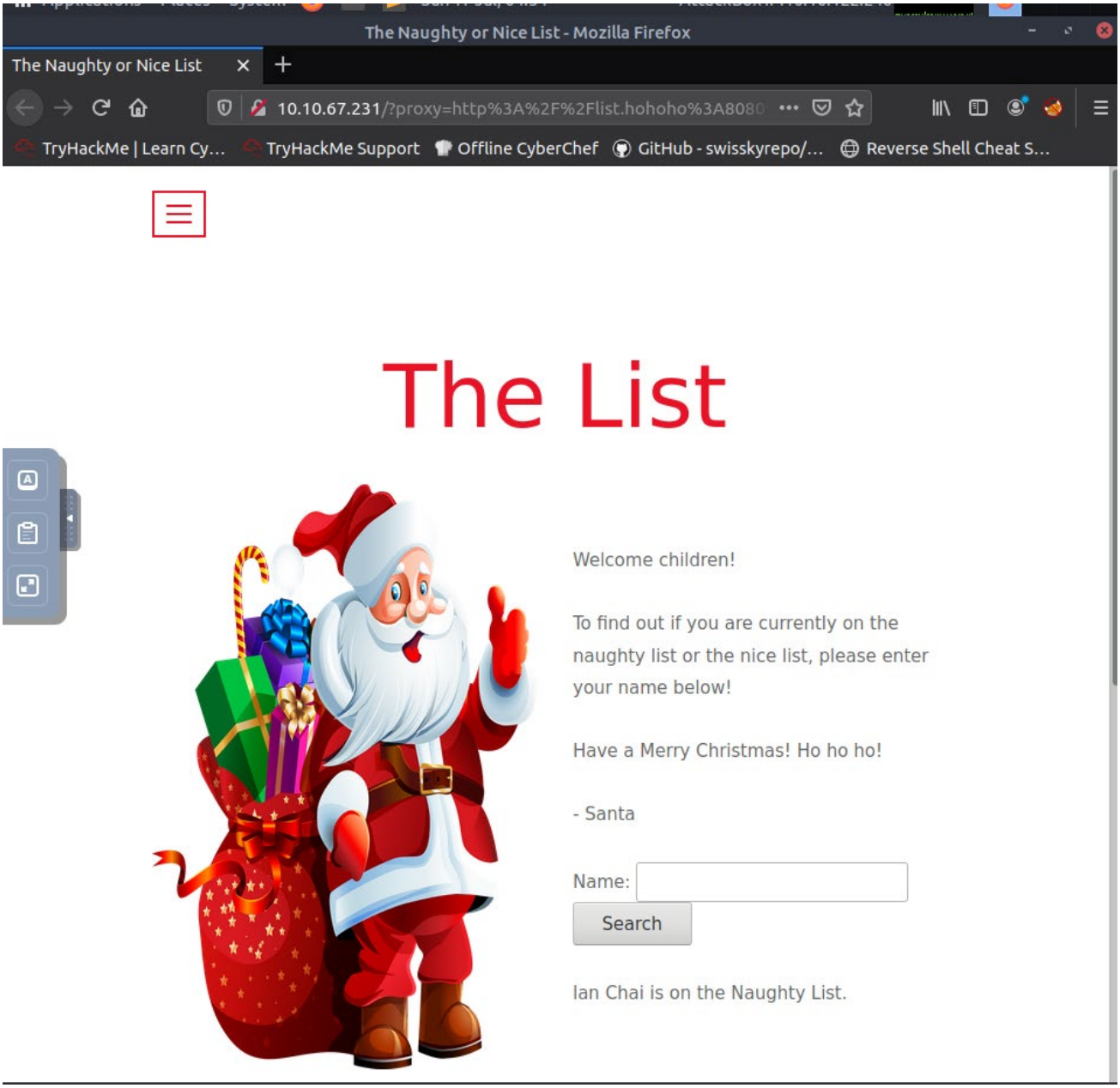
Tib3rius : Nice


Applications Places System Sun 17 Jul, 04:46 AttackBox IP:10.10.122.246
The Naughty or Nice List - Mozilla Firefox
The Naughty or Nice List
10.10.67.231/?proxy=http%3A%2F%2Flist.hohoho%3A8080
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...
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.

JJ: Naughty

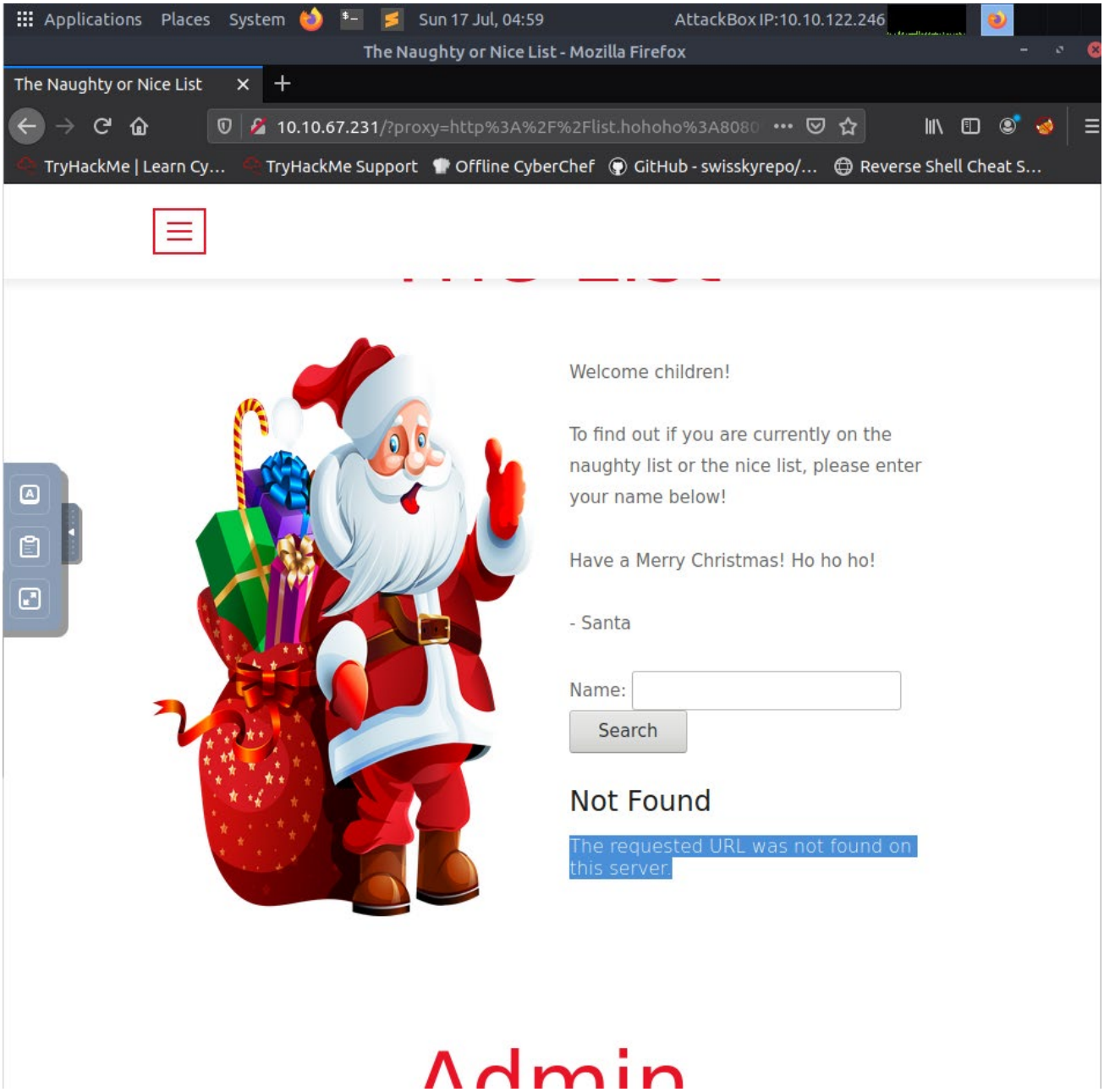

Applications Places System Sun 17 Jul, 04:49 AttackBox IP:10.10.122.246
The Naughty or Nice List - Mozilla Firefox
The Naughty or Nice List
10.10.67.231/?proxy=http%3A%2F%2Flist.hohoho%3A8080
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...
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.

YP: Nice



Lan Chai: Naughty

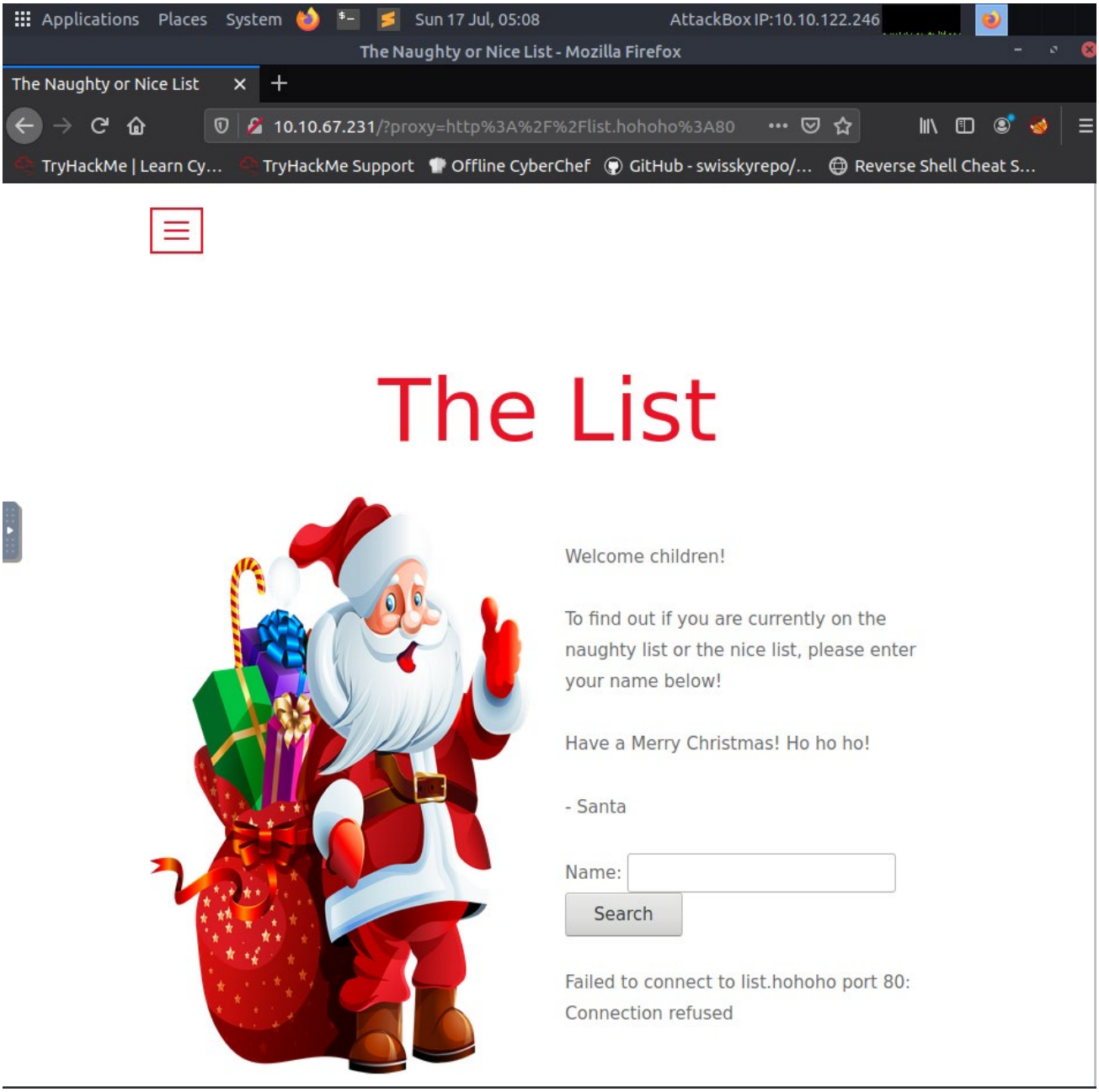
Q2: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?



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

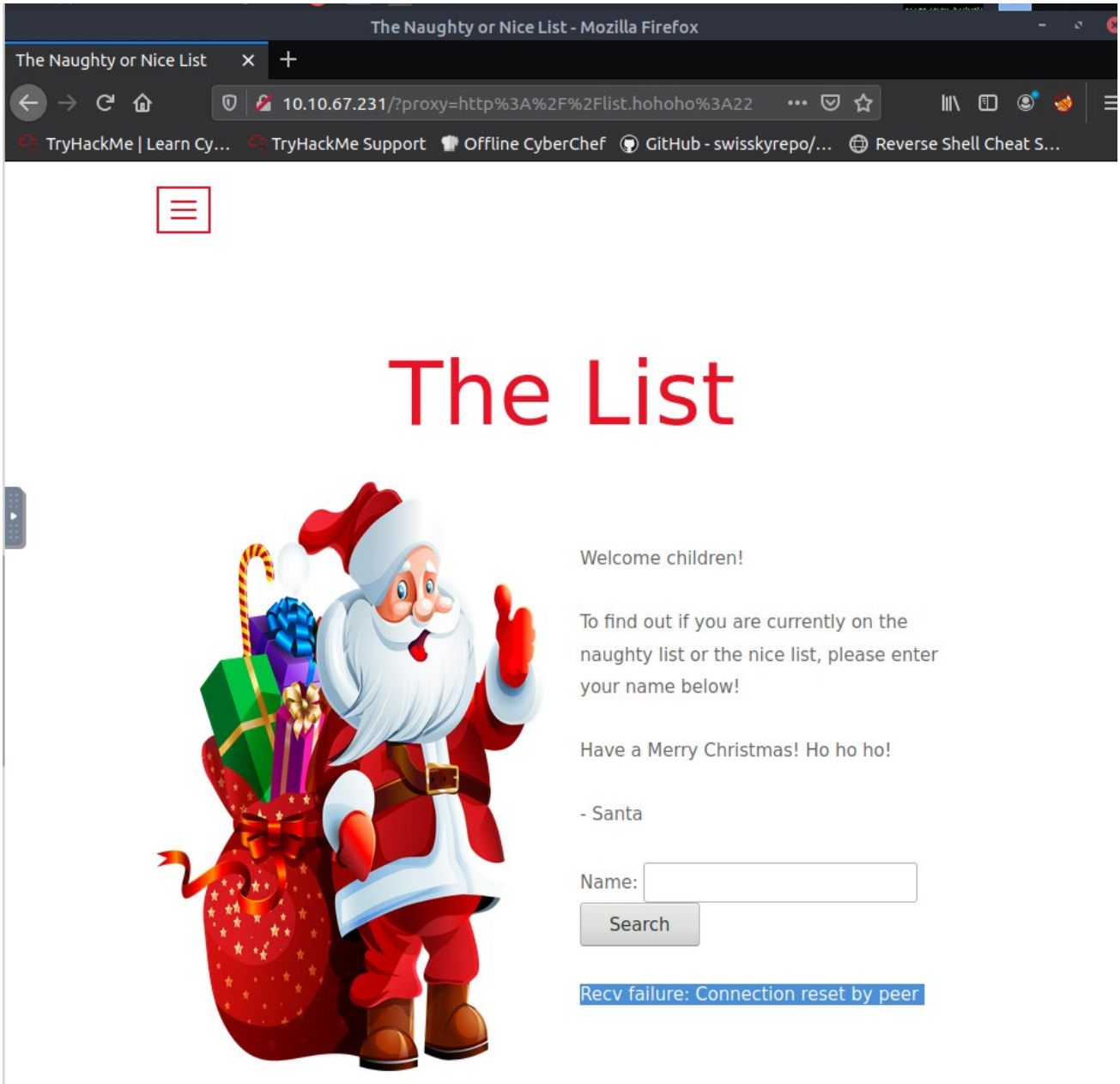
Q3: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"?*

Copy and paste from THM



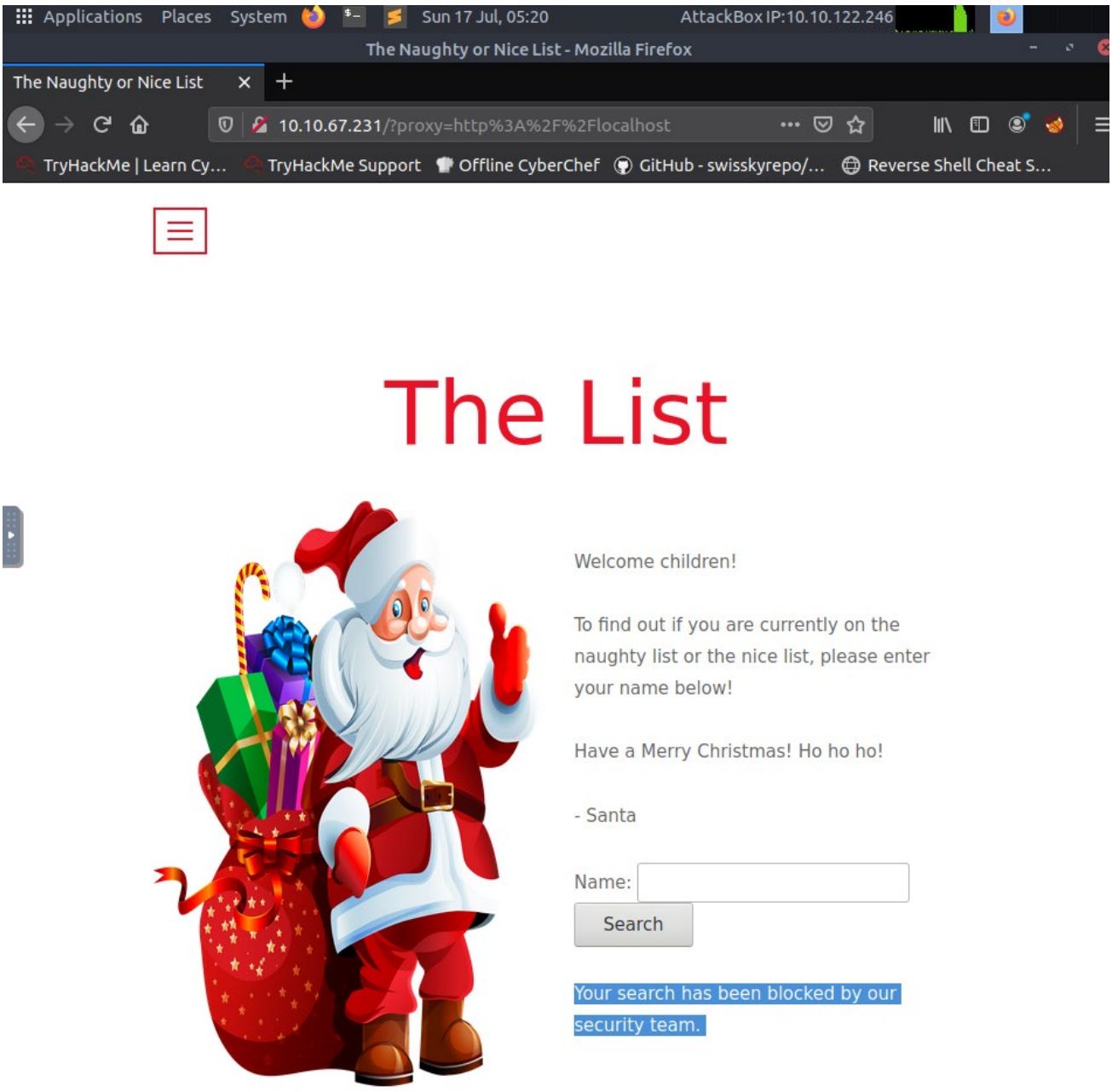
Ans: Failed to connect to list.hohoho port 80: Connection refused.

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



Ans: Recv failure: Connection reset by peer

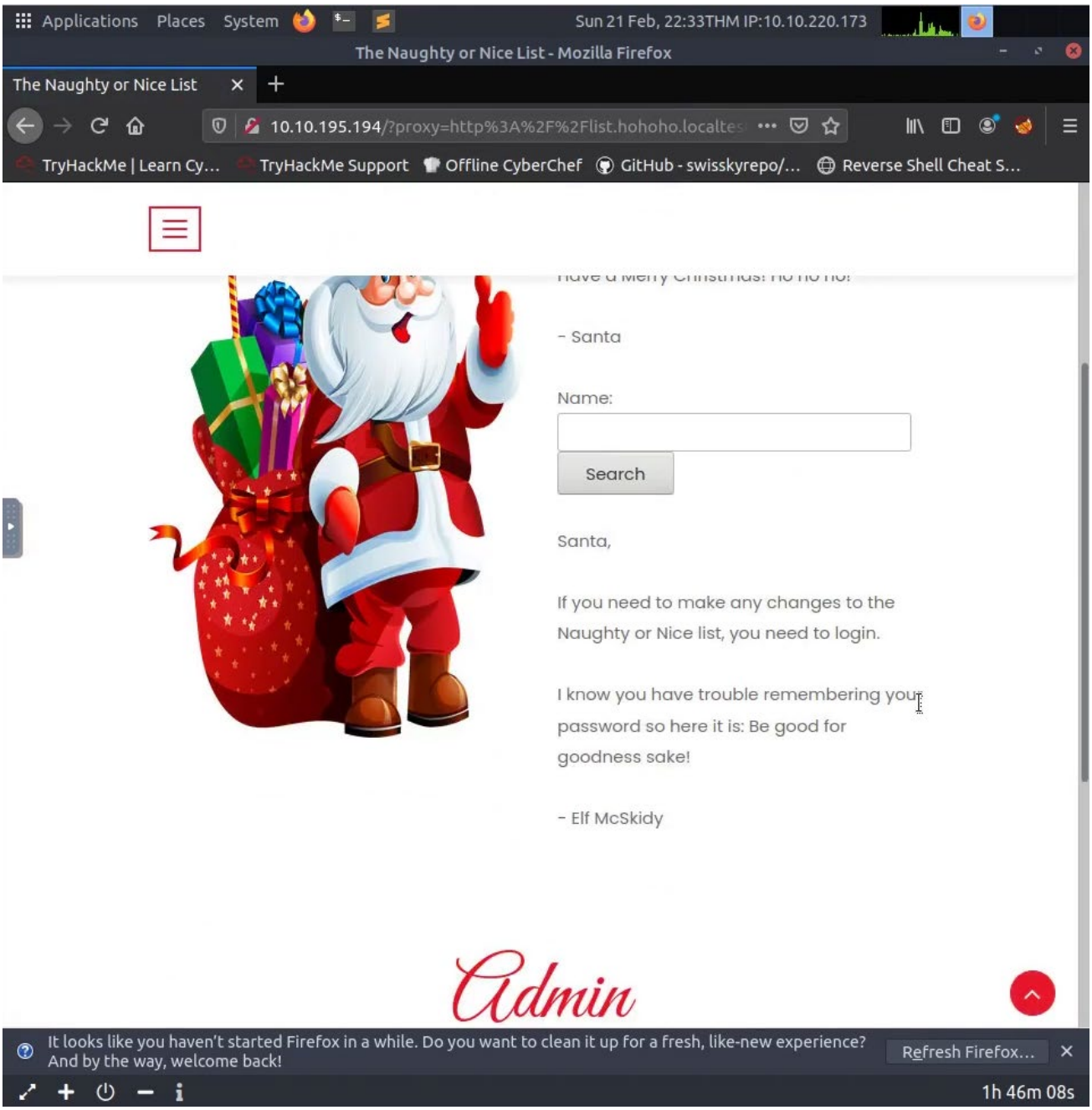
Q5: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?*
Copy and paste from THM



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

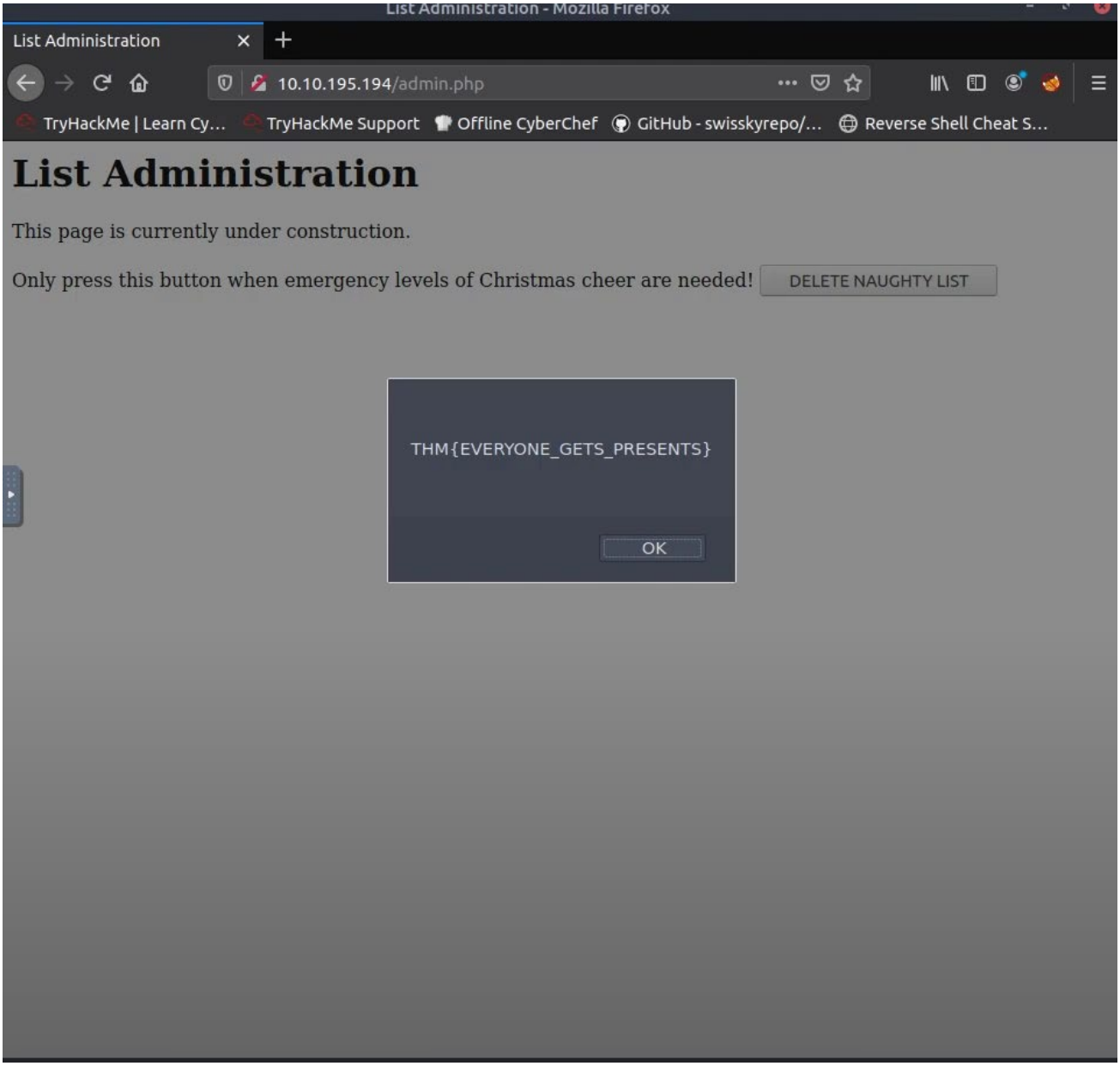
Q6: What is Santa's password?*

copy and paste from THM.



Ans: Be good for goodness sake!

Q7: What is the challenge flag?*



Ans: THM{EVERYONE_GETS_PRESENTS}

Methodology

First fetch the root of the site by browsing "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F". Unfortunately, we get Not Found. The requested URL was not found on this server. Then try to change 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. Then, we get Failed to connect to list.hohoho port 80:Connection refused. After that we try to change the port number to 22 and it displayed Recv failure: Connection reset by peer which means the port 22 is open but cannot understand what was sent(Sending HTTP request to SSH server). Than we 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 . Then bingo password obtain. Then, enter the username and the password to access the list administration. Lastly press the delete naughty list buton and capture the flag.

Day 20: Blue Teaming PowershELlF to the rescue

Tools used: Firefox
Solution/walkthrough:

Question 1

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

Ans: login name

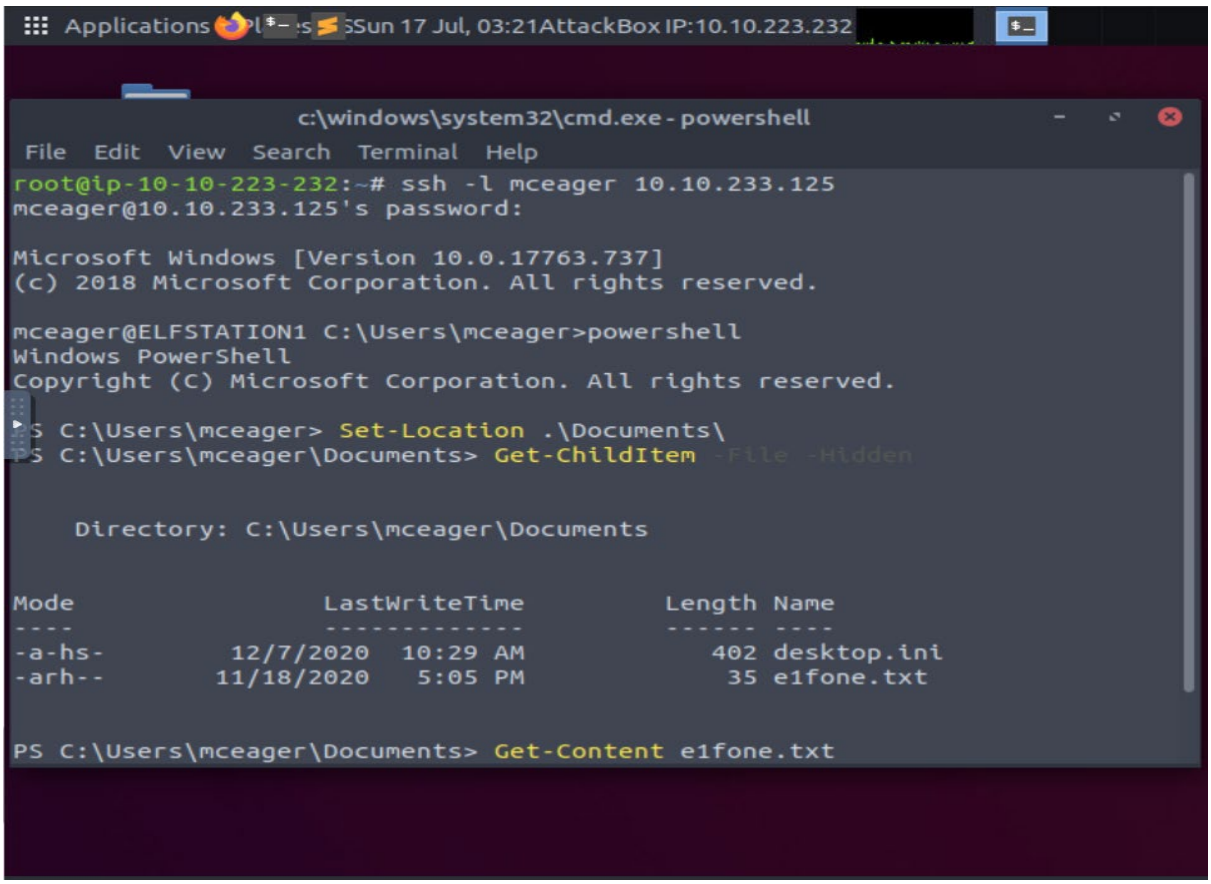
```
-l login_name
        Specifies the user to log in as on the remote machine.  This also may be specified on a per-host
        basis in the configuration file.
```

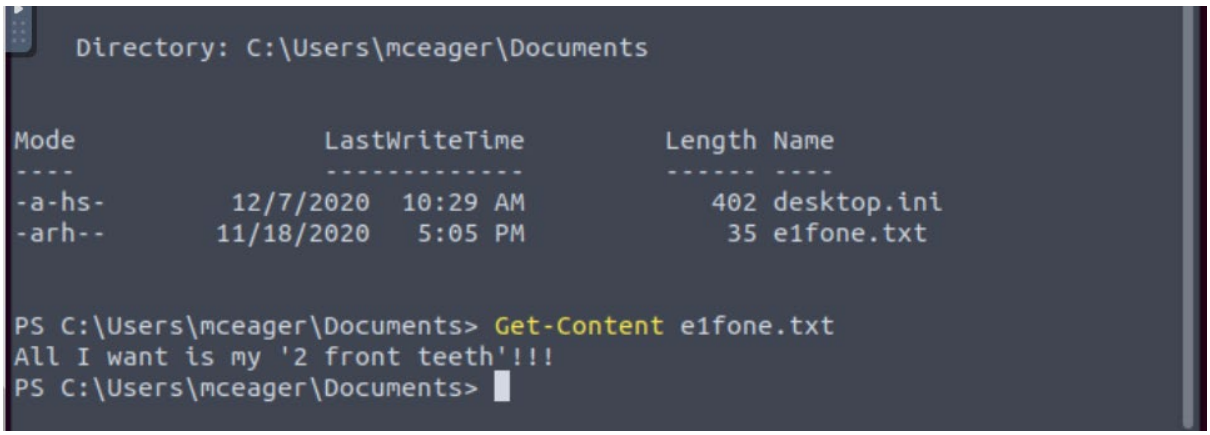
Search “ssh -l” command in google.

Question 2

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

Ans: 2 front teeth



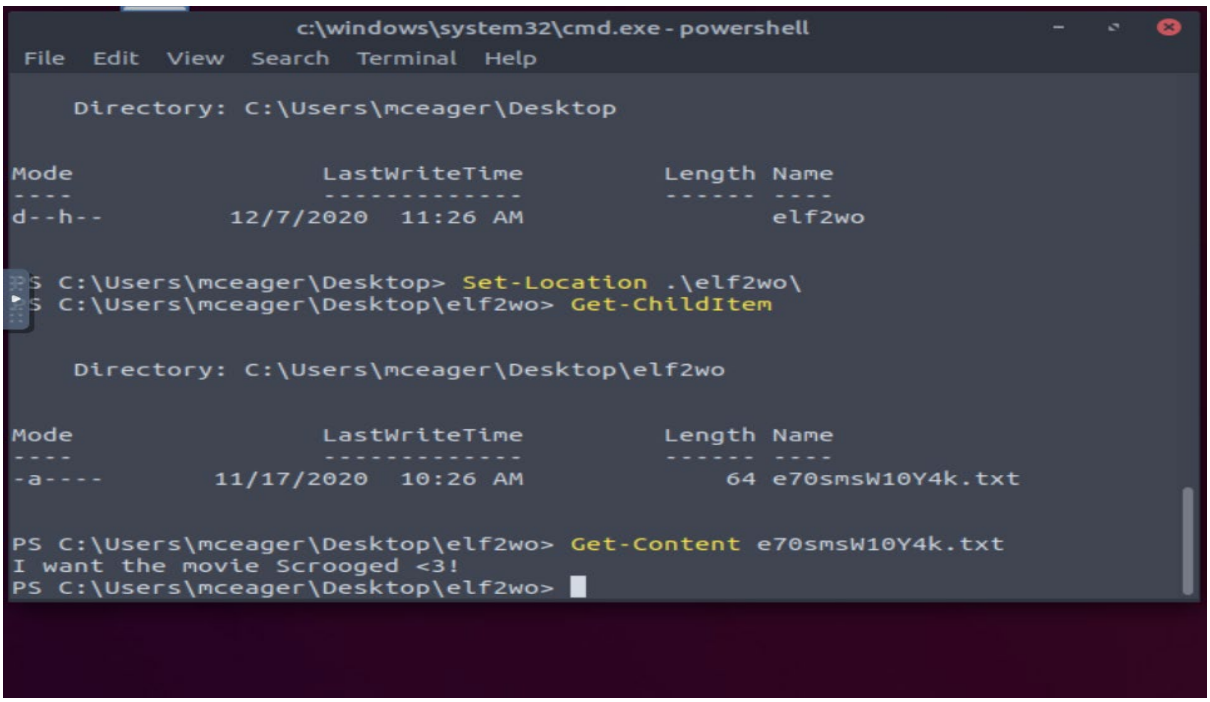


Input command (ssh -l mceager [MACHINE_IP]) to connect to the remote machine. Input yes to continue connecting and enter password [r0ckStar1!]. Launch powershell and input the command (Set-Location .\Documents\) to navigate to the Documents folder. Then, use command (Get-ChildItem -File -Hidden) to list the hidden files and input (Get-Content e1fone.txt) to see the content.

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?

Ans: Scrooged



Input (Set-Location ..). Then, navigate to the desktop. Use the command (Get-ChildItem -Hidden -Directory) to search the hidden folder. Then, set the location to elf2wo by entering (Set-Location .\elf2wo\) and (Get-ChildItem) to list down the file. To see the content, input (Get-Content e70smsW10Y4k.txt).

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)

Ans: 3lfthr3e

```
PS C:\Users\mceager> Set-Location C:/Windows
PS C:\Windows> Set-Location  System32
PS C:\Windows\System32> Get-ChildItem -Hidden -Directory -Filter "*3*"


    Directory: C:\Windows\System32


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

Navigate to the windows and then to System32. Input command (Get-ChildItem -Hidden -Directory -Filter “*3*”) to search the folder name that includes the number 3.

Question 5

How many words does the first file contain?

Ans: 9999

```
c:\windows\system32\cmd.exe - powershell
File  Edit  View  Search  Terminal  Help
PS C:\Windows\System32> Set-Location 3lfthr3e
PS C:\Windows\System32\3lfthr3e> Get-ChildItem -Hidden


    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 :
```

Navigate to the 3lfthr3e folder. Then, list the files in the folder. Input command (Get-Content 1.txt | Measure-Object) to count the number of words in the file.

Question 6

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

Ans: Red Ryder

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

Input command ((Get-Content 1.txt)[551]) to see the word at index 551. For index 6991, you can change the number in the square bracket.

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)

Ans: red ryder bb gun

```
PS C:\Windows\System32\3lfthr3e> Get-Content 2.txt | Select-String -Pattern
 "redryder"

redryderbbgun
```

Input command (Get-Content 2.txt | Select-String -Pattern “redryder”) to search a particular file for the pattern redryder.

Thought Process/Methodology:

Firstly, you can search parameter -l do in google. Then, input command (ssh -l mceager [MACHINE_IP]) in terminal. Key in the password given (r0ckStar!). Launch powershell and navigate to the documents folder using the Set-Location command. Then, use command (Get-ChildItem -File -Hidden) to list the hidden files and input (Get-Content e1fone.txt) to see the content. Next, navigate to the desktop folder and input command (Get-ChildItem -Hidden -Directory). Navigate to the elf2wo folder and use the Get-Content command to view the contents of the txt file. Next, navigate to the windows and then to System32. Input command (Get-ChildItem -Hidden -Directory -Filter “*3*”) to search the folder name that includes the number 3. Next, navigate to the 3lfthr3e folder. Then, list the files in the folder. Input command (Get-Content 1.txt | Measure-Object) to count the number of words in the file. Next, input command ((Get-Content 1.txt)[551]) to see the word at index 551. For index 6991, you can change the number in the square bracket. For the last question, input command (Get-Content 2.txt | Select-String -Pattern “redryder”) to search a particular file for the pattern redryder.