

# 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

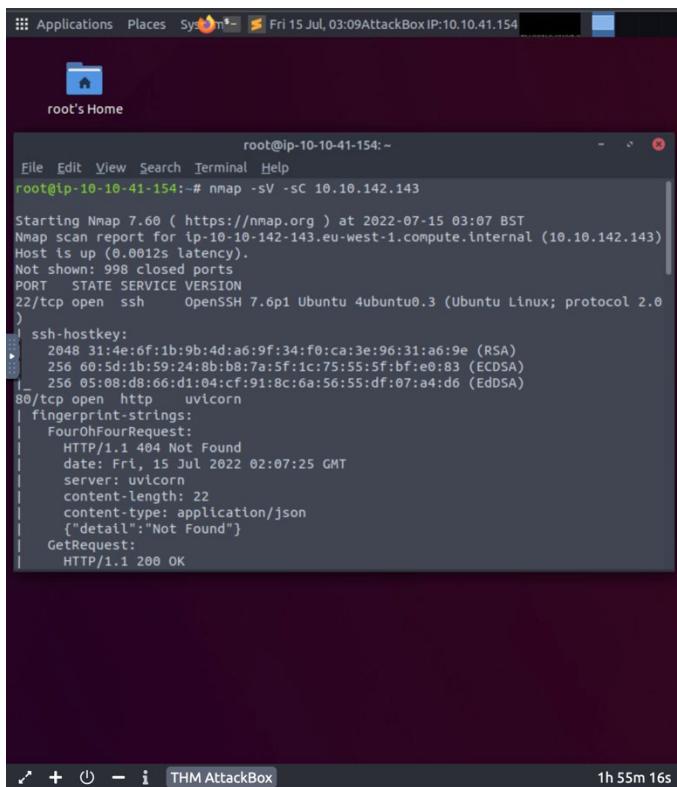
**Solution/walkthrough:**

### **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.



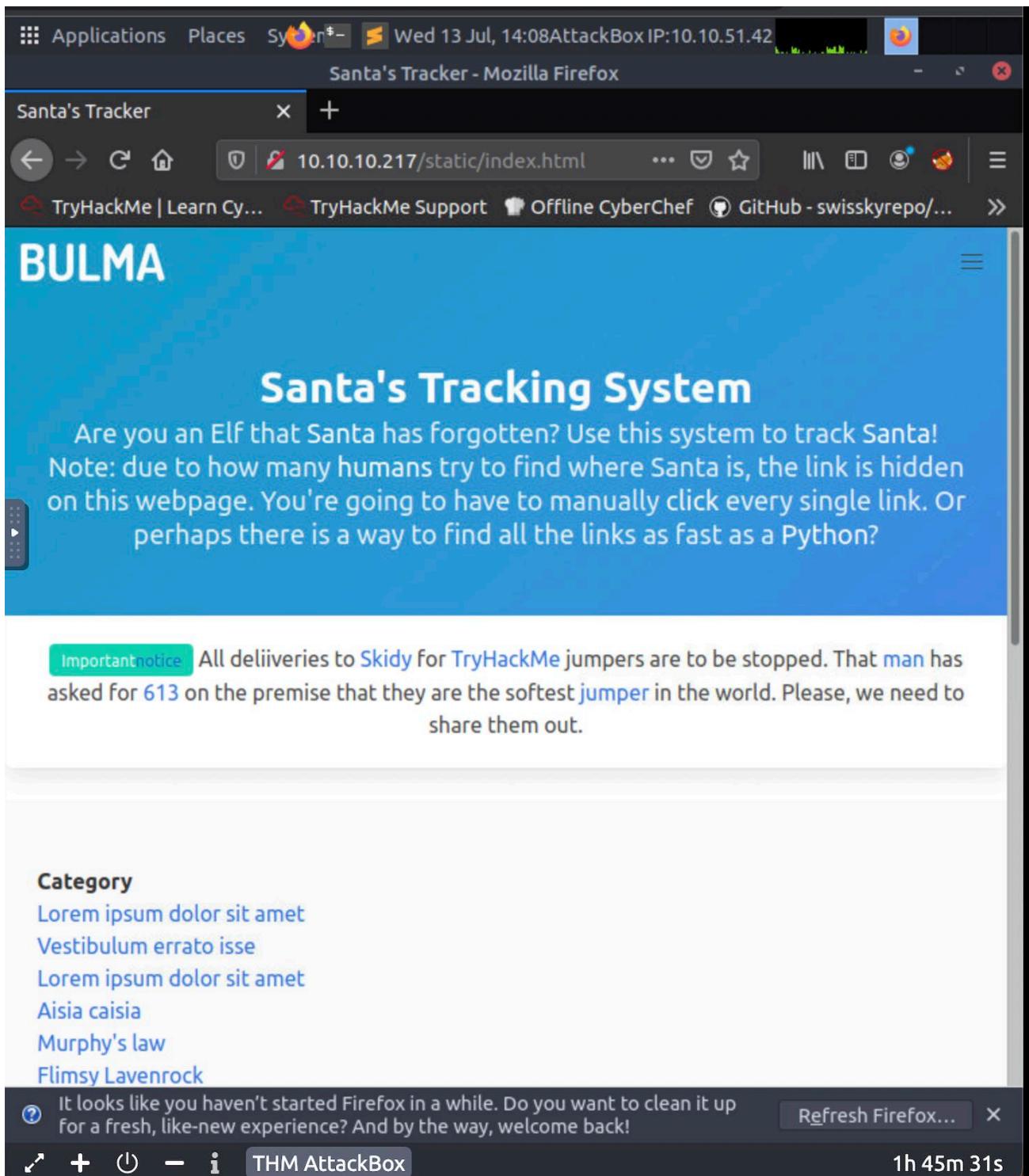
```
root@ip-10-10-41-154: ~
File Edit View Search Terminal Help
root@ip-10-10-41-154:~# nmap -sV -sC 10.10.142.143
Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-15 03:07 BST
Nmap scan report for ip-10-10-142-143.eu-west-1.compute.internal (10.10.142.143)
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
           ssh-hostkey:
             2048 31:4e:6f:1b:9b:4d:a6:9f:34:f0:ca:3e:96:31:a6:9e (RSA)
             256 00:5d:1b:59:24:8b:b6:7a:5f:1c:75:55:5f:bf:e0:83 (ECDSA)
             256 05:08:d8:66:d1:04:cf:91:8c:6a:56:55:df:07:a4:d6 (EdDSA)
80/tcp    open  http    uicorn
           fingerprint-strings:
             FourOhFourRequest:
               HTTP/1.1 404 Not Found
               date: Fri, 15 Jul 2022 02:07:25 GMT
               server: uicorn
               content-length: 22
               content-type: application/json
               {"detail":"Not Found"}
             GetRequest:
               HTTP/1.1 200 OK
```

### **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 enumeration 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.

```
http://10.10.10.217/static/index.html - Mozilla Firefox
Santa's Tracker × http://10.10.10.217/static/in X +
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/...
<li><a href="#">Lorem ipsum dolor sit amet</a></li>
<li><a href="#">Aisia caisia</a></li>
<li><a href="#">Murphy's law</a></li>
<li><a href="#">Flimsy Lavenrock</a></li>
<li><a href="#">Maven Mousie Lavender</a></li>
</ul>
</div>
<div class="column is-3">
<h2><strong>Category</strong></h2>
<ul>
<li><a href="#">Labore et dolore magna aliqua</a></li>
<li><a href="#">Kanban airis sum eschelor</a></li>
<li><a href="http://machine_ip/api/api_key">Modular modern free</a></li>
<li><a href="#">The king of clubs</a></li>
<li><a href="#">The Discovery Dissipation</a></li>
<li><a href="#">Course Correction</a></li>
<li><a href="#">Better Angels</a></li>
</ul>
</div>
<div class="column is-4">
<h2><strong>Category</strong></h2>
<ul>
<li><a href="#">Objects in space</a></li>
<li><a href="#">Playing cards with coyote</a></li>
<li><a href="#">Goodbye Yellow Brick Road</a></li>
<li><a href="#">The Garden of Forking Paths</a></li>
<li><a href="#">Future Shock</a></li>
</ul>
</div>
<div class="content has-text-centered">
<p>
<a class="icon" href="https://github.com/BulmaTemplates/bulma-templates">
<i class="fa fa-github"></i>
</a>
</p>
<div class="control level-item">
<a href="https://github.com/BulmaTemplates/bulma-templates">
<div class="tags has-addons">
<span class="tag is-dark">Bulma Templates</span>
<span class="tag is-info">MIT license</span>
</div>

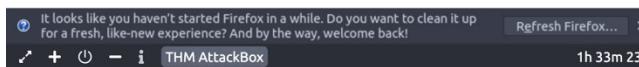
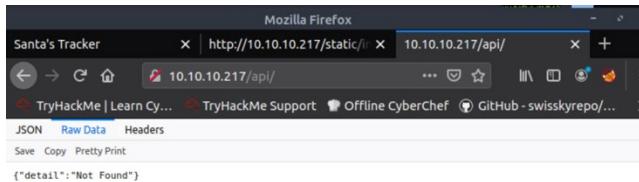
```

#### 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.

A screenshot of a terminal window titled 'root@ip-10-10-206-174:~'. The window shows a Python script named 'brute.py' being edited in nano. The script contains the following code:

```
import requests
for api_key in range(1,100,2):
    html = requests.get('http://10.10.82.4/api/{api_key}')
    print(html.text)
```

The terminal also displays the system status at the bottom: '10 items, Free space: 4.2 GB'.

```
root@ip-10-10-206-174:~
```

```
File Edit View Search Terminal Help
{"item_id":27,"q":"Error. Key not valid!"}
 {"item_id":29,"q":"Error. Key not valid!"}
 {"item_id":31,"q":"Error. Key not valid!"}
 {"item_id":33,"q":"Error. Key not valid!"}
 {"item_id":35,"q":"Error. Key not valid!"}
 {"item_id":37,"q":"Error. Key not valid!"}
 {"item_id":39,"q":"Error. Key not valid!"}
 {"item_id":41,"q":"Error. Key not valid!"}
 {"item_id":43,"q":"Error. Key not valid!"}
 {"item_id":45,"q":"Error. Key not valid!"}
 {"item_id":47,"q":"Error. Key not valid!"}
 {"item_id":49,"q":"Error. Key not valid!"}
 {"item_id":51,"q":"Error. Key not valid!"}
 {"item_id":53,"q":"Error. Key not valid!"}
 {"item_id":55,"q":"Error. Key not valid!"}
▶ "item_id":57,"q":"Winter Wonderland, Hyde Park, London."
 {"item_id":59,"q":"Error. Key not valid!"}
 {"item_id":61,"q":"Error. Key not valid!"}
 {"item_id":63,"q":"Error. Key not valid!"}
 {"item_id":65,"q":"Error. Key not valid!"}
 {"item_id":67,"q":"Error. Key not valid!"}
 {"item_id":69,"q":"Error. Key not valid!"}
 {"item_id":71,"q":"Error. Key not valid!"}
 {"item_id":73,"q":"Error. Key not valid!"}
```

10 items, Free space: 4.2 GB

4 🔥 Your streak has increased. ✕  
You're 3 away from a badge!

### 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.

The screenshot shows a terminal window titled 'root' with the command 'root@ip-10-10-206-174: ~'. The terminal displays a JSON-like list of items, mostly containing errors, except for one item which is highlighted in yellow: {"item\_id":57,"q":"Winter Wonderland, Hyde Park, London."}. Below the terminal, a status bar indicates '10 items, Free space: 4.2 GB'. At the bottom right, a notification box says 'Your streak has increased. You're 3 away from a badge!' with a timer showing '1h 15m 22s'.

```
{"item_id":27,"q":"Error. Key not valid!"}
{"item_id":29,"q":"Error. Key not valid!"}
{"item_id":31,"q":"Error. Key not valid!"}
{"item_id":33,"q":"Error. Key not valid!"}
{"item_id":35,"q":"Error. Key not valid!"}
{"item_id":37,"q":"Error. Key not valid!"}
{"item_id":39,"q":"Error. Key not valid!"}
{"item_id":41,"q":"Error. Key not valid!"}
{"item_id":43,"q":"Error. Key not valid!"}
{"item_id":45,"q":"Error. Key not valid!"}
{"item_id":47,"q":"Error. Key not valid!"}
{"item_id":49,"q":"Error. Key not valid!"}
{"item_id":51,"q":"Error. Key not valid!"}
{"item_id":53,"q":"Error. Key not valid!"}
{"item_id":55,"q":"Error. Key not valid!"}
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
{"item_id":59,"q":"Error. Key not valid!"}
{"item_id":61,"q":"Error. Key not valid!"}
{"item_id":63,"q":"Error. Key not valid!"}
{"item_id":65,"q":"Error. Key not valid!"}
{"item_id":67,"q":"Error. Key not valid!"}
{"item_id":69,"q":"Error. Key not valid!"}
{"item_id":71,"q":"Error. Key not valid!"}
{"item_id":73,"q":"Error. Key not valid!"}
```

### 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	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Word	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Double Word	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Quad	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Single Precision	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Double Precision	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

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

3. Log into your instance using the following information.

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

0x00400060	8945TC	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 (0x400b4d)
    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 .....0.....|0.
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')

The screenshot shows a terminal window titled "root@ip-10-10-3-231:~". The window contains the following command-line session:

```
root@ip-10-10-3-231:~# echo '10.10.16.29' > ip.txt
root@ip-10-10-3-231:~# cat ip.txt
10.10.16.29
root@ip-10-10-3-231:~# ssh ip.txt
ssh: Could not resolve hostname ip.txt: Name or service not known
root@ip-10-10-3-231:~# ssh elfmceager@10.10.16.29
The authenticity of host '10.10.16.29 (10.10.16.29)' can't be established.
ECDSA key fingerprint is SHA256:XrBuXSQs0wRKhvVRdrSfE/0F5ccAZQiXAhMhzB1dV7U.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.16.29' (ECDSA) to the list of known hosts.
elfmceager@10.10.16.29's password: [REDACTED]
```

The terminal window is part of a desktop environment, with a "root's Home" folder icon visible in the top-left corner. The bottom of the screen shows the THM AttackBox interface with icons for file operations and a timer indicating 1h 14m 50s.

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

The screenshot shows a terminal window titled 'elfmceager@tbfc-day-17: ~'. The window has two tabs: one for memory usage and swap usage, and another for network information. Below these, system status messages are displayed, including '0 packages can be updated.' and '0 updates are security updates.' A message about failed internet connection is also present. The main part of the terminal shows the user's session:

```
Last login: Fri Jul 15 04:24:38 2022 from 10.10.3.231
elfmceager@tbfc-day-17:~$ ls
challenge1 file1
elfmceager@tbfc-day-17:~$ ./challenge1
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1675 started...
= attach 1675 1675
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[0x00400a30]> aa
[ ] Analyze all flags starting with sym. and entry0 (aa)
```

The bottom of the terminal shows the THM AttackBox interface with a timer of '1h 18m 04s'.

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.

The screenshot shows a terminal window titled "elfmceager@tbfc-day-17: ~". The window contains assembly code for the main function:

```
[WARNING : block size exceeding max block size at 0x006ba220
[+] Try changing it with e anal.bb.maxsize
WARNING : block size exceeding max block size at 0x006bc860
[+] Try changing it with e anal.bb.maxsize
[x] Analyze all flags starting with sym. and entry0 (aa)
[0x00400a30]> pdf @main
;-- main:
(fcn) sym.main 35
sym.main ();
    ; var int local_ch @ rbp-0xc
    ; var int local_8h @ rbp-0x8
    ; var int local_4h @ rbp-0x4
        ; DATA XREF from 0x00400a4d (entry0)
0x00400b4d      55          push rbp
0x00400b4e      4889e5       mov rbp, rsp
0x00400b51      c745f4010000. mov dword [local_ch], 1
0x00400b58      c745f8060000. mov dword [local_8h], 6
0x00400b5f      8b45f4       mov eax, dword [local_ch]
0x00400b62      0faf45f8     imul eax, dword [local_8h]
0x00400b66      8945fc       mov dword [local_4h], eax
0x00400b69      b800000000  mov eax, 0
0x00400b6e      5d          pop rbp
0x00400b6f      c3          ret
[0x00400a30]>
```

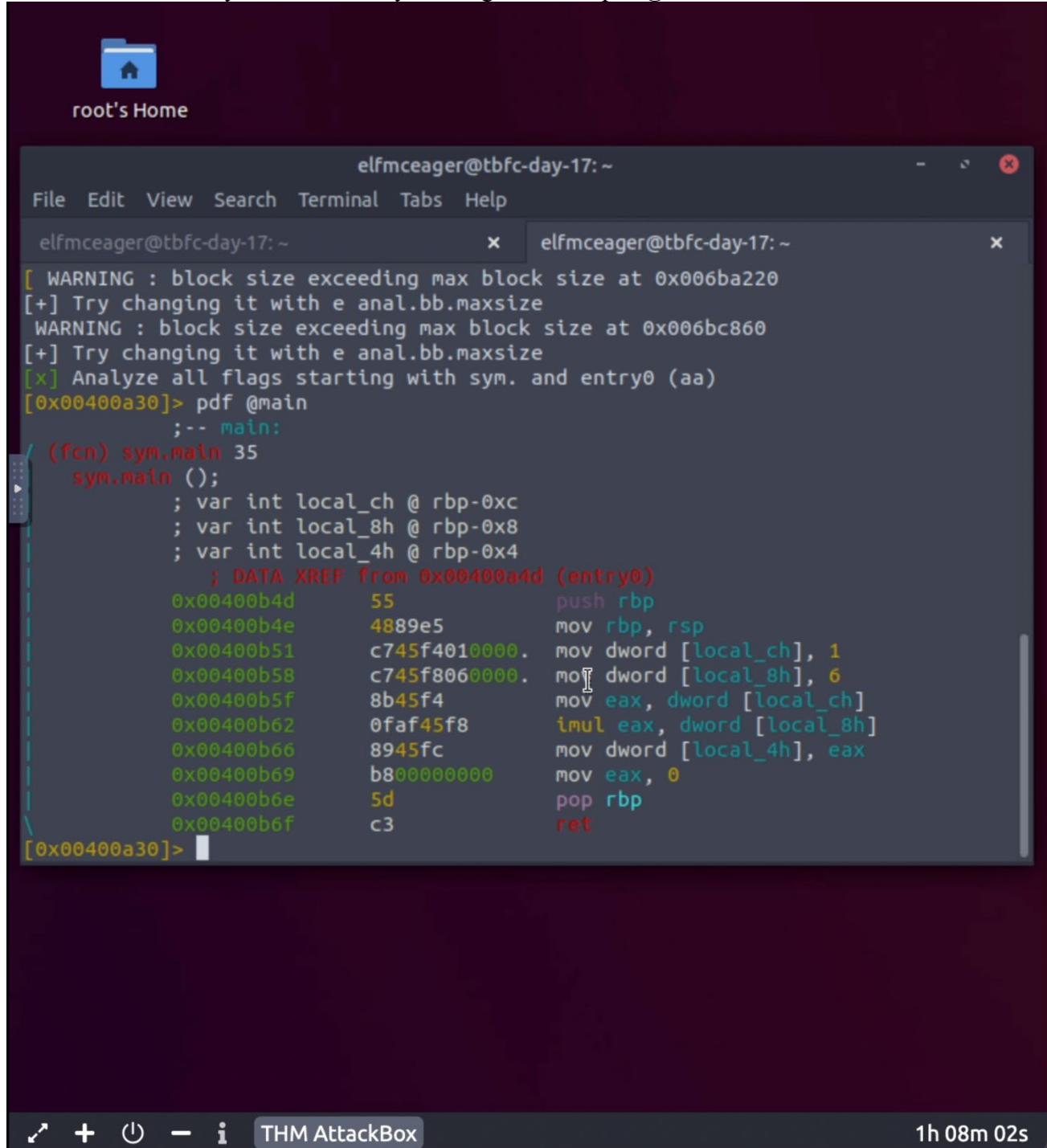
The terminal window has two tabs, both labeled "elfmceager@tbfc-day-17: ~". The status bar at the bottom shows "THM AttackBox" and "1h 08m 02s".

### 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’



The screenshot shows a terminal window titled 'elfmceager@tbfc-day-17: ~' displaying assembly code. The code is for the 'main' function, which has a size of 35 bytes. It starts with a push rbp instruction, followed by mov rbp, rsp, and then initializes three local variables: local\_ch (dword [local\_ch]), local\_8h (dword [local\_8h]), and local\_4h (dword [local\_4h]). The local\_8h variable is initialized to 6. Subsequent instructions include imul eax, dword [local\_8h], mov dword [local\_4h], eax, and finally pop rbp and ret.

```
[WARNING : block size exceeding max block size at 0x006ba220
[+] Try changing it with e anal.bb.maxsize
WARNING : block size exceeding max block size at 0x006bc860
[+] Try changing it with e anal.bb.maxsize
[x] Analyze all flags starting with sym. and entry0 (aa)
[0x00400a30]> pdf @main
;-- main:
(fcn) sym.main 35
sym.main () {
    ; var int local_ch @ rbp-0xc
    ; var int local_8h @ rbp-0x8
    ; var int local_4h @ rbp-0x4
        ; DATA XREF from 0x00400a4d (entry0)
    0x00400b4d      55          push rbp
    0x00400b4e      4889e5       mov rbp, rsp
    0x00400b51      c745f4010000. mov dword [local_ch], 1
    0x00400b58      c745f8060000. mov dword [local_8h], 6
    0x00400b5f      8b45f4       mov eax, dword [local_ch]
    0x00400b62      0faf45f8     imul eax, dword [local_8h]
    0x00400b66      8945fc       mov dword [local_4h], eax
    0x00400b69      b800000000  mov eax, 0
    0x00400b6e      5d          pop rbp
    0x00400b6f      c3          ret
[0x00400a30]>
```

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.

Applications Places Syntex Fri 15 Jul, 10:26 AttackBox IP: 10.10.218.187

root's Home

```
elfmceager@tbfc-day-17:~
```

File Edit View Search Terminal Help

```
0x7ffffd75c9e18 0000 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0x7ffffd75c9e28 0000 0000 0000 0000 0000 0000 0000 0000 0000 .....  
[0x00400b51]> db 0x00400b66  
[0x00400b51]> dc  
hit breakpoint at: 400b66  
[0x00400b51]> px @ rbp-0x8  
- offset - 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF  
0x7ffffd75c9d38 0600 0000 0000 0000 4018 4000 0000 0000 .....@. @.....  
0x7ffffd75c9d48 e910 4000 0000 0000 0000 0000 0000 0000 .....@.....  
0x7ffffd75c9d58 0000 0000 0100 0000 689e 5cd7 ff7f 0000 .....h.\.....  
0x7ffffd75c9d68 4d0b 4000 0000 0000 0000 0000 0000 0000 M. @.....  
0x7ffffd75c9d78 1700 0000 0100 0000 0000 0000 0000 0000 .....  
0x7ffffd75c9d88 0000 0000 0200 0000 0000 0000 0000 0000 .....  
0x7ffffd75c9d98 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0x7ffffd75c9da8 0000 0000 0000 0000 0004 4000 0000 0000 .....@.....  
0x7ffffd75c9db8 1113 7371 caab 0973 e018 4000 0000 0000 .....sq..s.@.....  
0x7ffffd75c9dc8 0000 0000 0000 0000 1890 6b00 0000 0000 .....k.....  
0x7ffffd75c9dd8 0000 0000 0000 0000 1113 537b f305 f68c .....S{.....  
0x7ffffd75c9de8 1113 c760 caab 0973 0000 0000 0000 0000 .....`..s.....  
0x7ffffd75c9df8 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0x7ffffd75c9e08 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0x7ffffd75c9e18 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0x7ffffd75c9e28 0000 0000 0000 0000 0000 0000 0000 0000 .....  
[0x00400b51]>
```

### **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

The screenshot shows a terminal window titled 'elfmceager@tbfc-day-17: ~'. The window contains the following assembly code:

```
File Edit View Search Terminal Help
[0x00400b51]> db 0x00400b69
[0x00400b51]> dc
hit breakpoint at: 400b69
[0x00400b51]> px @ rbp-0x4
- offset -
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0x7ffd75c9d3c 600 0000 4018 4000 0000 0000 e910 4000 .....@.0.....@.
0x7ffd75c9d4c 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x7ffd75c9d5c 0100 0000 689e 5cd7 ff7f 0000 4d0b 4000 ....h.\...M.@
0x7ffd75c9d6c 0000 0000 0000 0000 0000 0000 1700 0000 .....
0x7ffd75c9d7c 0100 0000 0000 0000 0000 0000 0000 0000 .....
0x7ffd75c9d8c 0200 0000 0000 0000 0000 0000 0000 0000 .....
0x7ffd75c9d9c 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x7ffd75c9dac 0000 0004 4000 0000 0000 1113 7371 .....@....sq
0x7ffd75c9dbc caab 0973 e018 4000 0000 0000 0000 0000 ...s.0...
0x7ffd75c9dcc 0000 0000 1890 6b00 0000 0000 0000 0000 .....k...
0x7ffd75c9ddc 0000 0000 1113 537b f305 f68c 1113 c760 .....S{...
0x7ffd75c9dec caab 0973 0000 0000 0000 0000 0000 0000 ...s...
0x7ffd75c9dfc 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x7ffd75c9e0c 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x7ffd75c9e1c 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x7ffd75c9e2c 0000 0000 0000 0000 0000 0000 0000 0000 .....
[0x00400b51]>
```

The terminal window is part of a desktop environment, with a menu bar and a taskbar at the top. The taskbar shows 'Applications', 'Places', 'System', 'Fri 15 Jul, 10:30 AttackBox IP:10.10.218.187', and other icons. The bottom of the screen shows a dock with icons for a browser, file manager, terminal, and others. The status bar at the bottom right says '1h 36m 31s'.

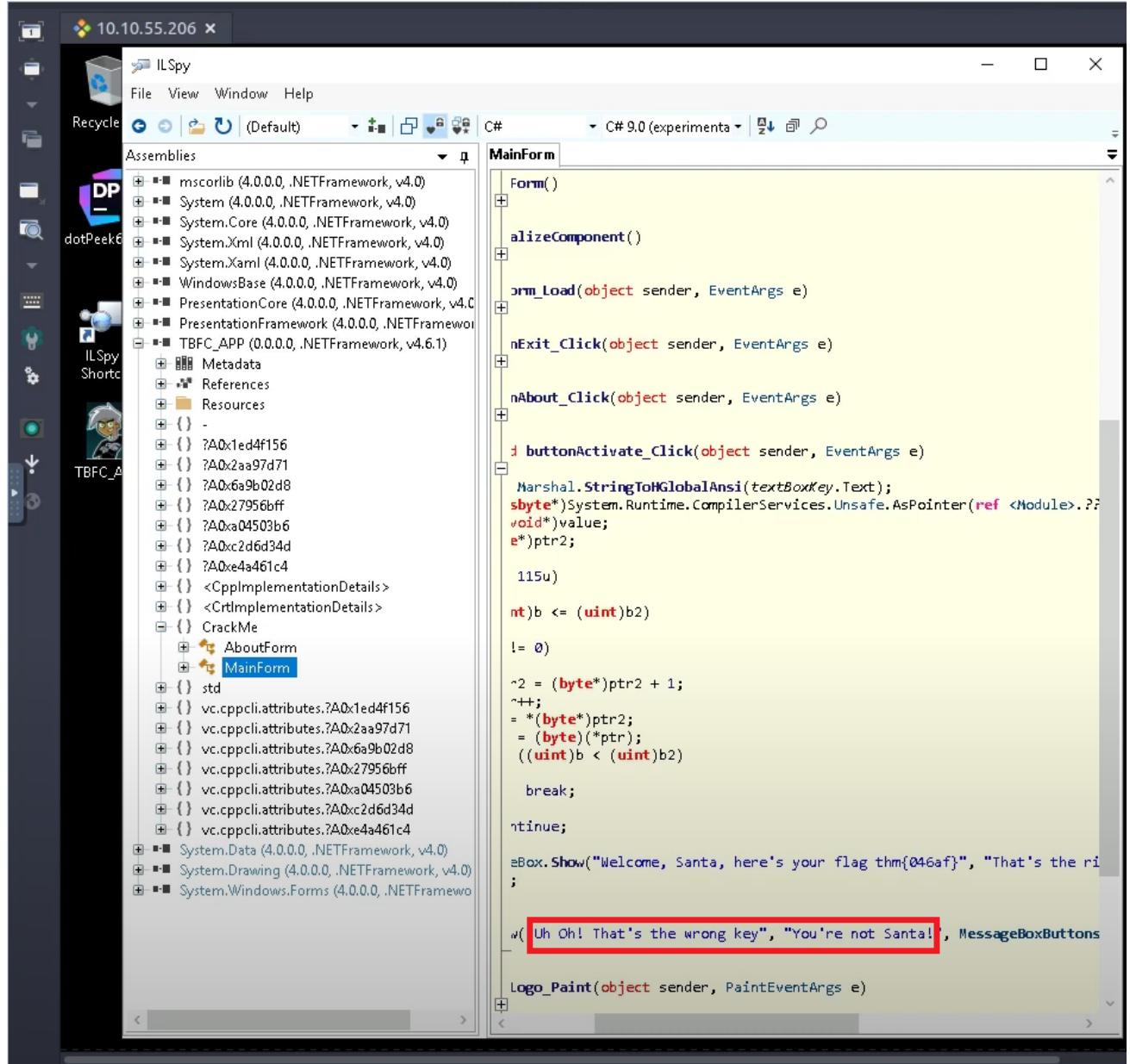
## **Thought Process/Methodology:**

**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.



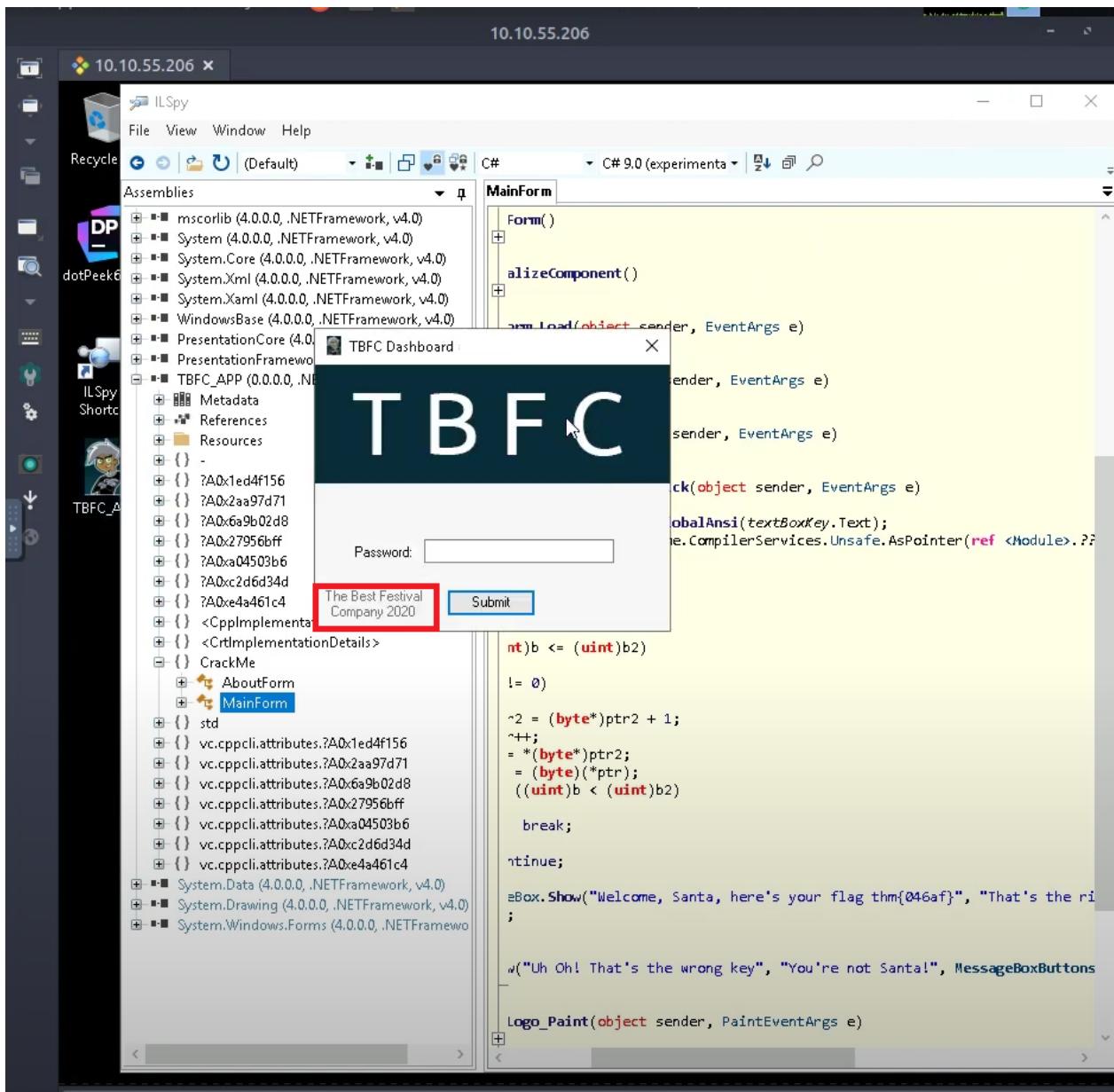
The screenshot shows the ILSpy interface with the assembly 'TBFC\_APP' loaded. The code editor displays the `MainForm.cs` file. A red box highlights the following line of code:

```
MessageBox.Show("Uh Oh! That's the wrong key", "You're not Santa!", MessageBoxButtons.OK);
```

Ans: Uh Oh! That's the wrong key

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

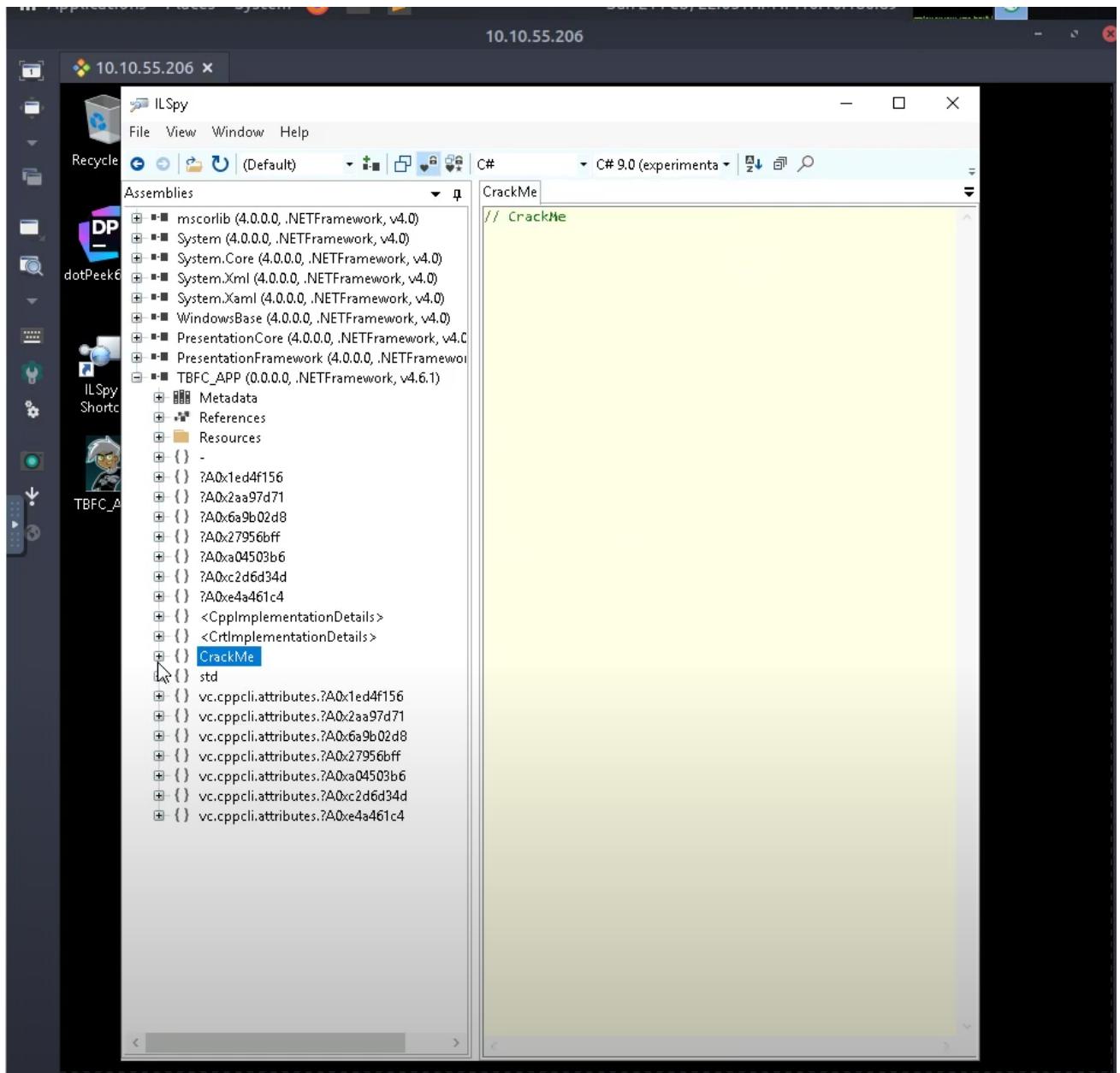
Q2: What does TBFC stand for?\*



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?

The screenshot shows the ILSpy decompiler interface. The left sidebar lists various assemblies loaded into memory, including mscorelib, System, System.Core, System.Xml, System.Xaml, WindowsBase, PresentationCore, PresentationFramework, and TBFC\_APP. The main window displays the decompiled code for the MainForm class. The code includes several methods: Form(), alizeComponent(), form\_Load, nExit\_Click, nAbout\_Click, buttonActivate\_Click, and Logo\_Paint. The buttonActivate\_Click method contains assembly-level code for marshaling strings and pointers, which is highlighted in the screenshot.

```
Form()
alizeComponent()

form_Load(object sender, EventArgs e)

nExit_Click(object sender, EventArgs e)

nAbout_Click(object sender, EventArgs e)

buttonActivate_Click(object sender, EventArgs e)
{
    Marshal.StringToGlobalAnsi(textBoxKey.Text);
    byte* value;
    void* ptr;
    ((void**)ptr) = value;
    ptr2 = (byte*)ptr + 1;
    ++ptr2;
    ((byte**)ptr2) = (byte)(*ptr);
    if ((uint)b < (uint)b2)
        break;
    continue;
}

MessageBox.Show("Welcome, Santa, here's your flag thm{046af}", "That's the right key");
if ("Uh Oh! That's the wrong key", "You're not Santa!", MessageBoxButtons.OK);

Logo_Paint(object sender, PaintEventArgs e)
```

Ans: MainForm

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

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

```
private void ~MainForm()
{
}

private void InitializeComponent()
{
}

private void MainForm_Load(object sender, EventArgs e)
{
}

private void buttonExit_Click(object sender, EventArgs e)
{
}

private void buttonAbout_Click(object sender, EventArgs e)
{
}

private unsafe void buttonActivate_Click(object sender, EventArgs e)
{
    IntPtr value = Marshal.StringToGlobalAnsi(textBoxKey.Text);
    sbyte* ptr = (sbyte*)System.Runtime.CompilerServices.Unsafe.AsF
    void* ptr2 = (void*)value;
    byte b = *(byte*)ptr2;
    byte b2 = 115;
    if ((uint)b >= 115u)
    {
        while ((uint)b <= (uint)b2)
        {
            if (b != 0)
            {
                ptr2 = (byte*)ptr2 + 1;
                ptr++;
                b = *(byte*)ptr2;
                b2 = *(byte*)(ptr);
                if ((uint)b < (uint)b2)
                {
                    break;
                }
                continue;
            }
            MessageBox.Show("Welcome, Santa, here's your flag thm{");
            return;
        }
        MessageBox.Show("Uh Oh! That's the wrong key", "You're not Sant
    }
}

private void panelLogo_Paint(object sender, PaintEventArgs e)
{
}
```

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?\*

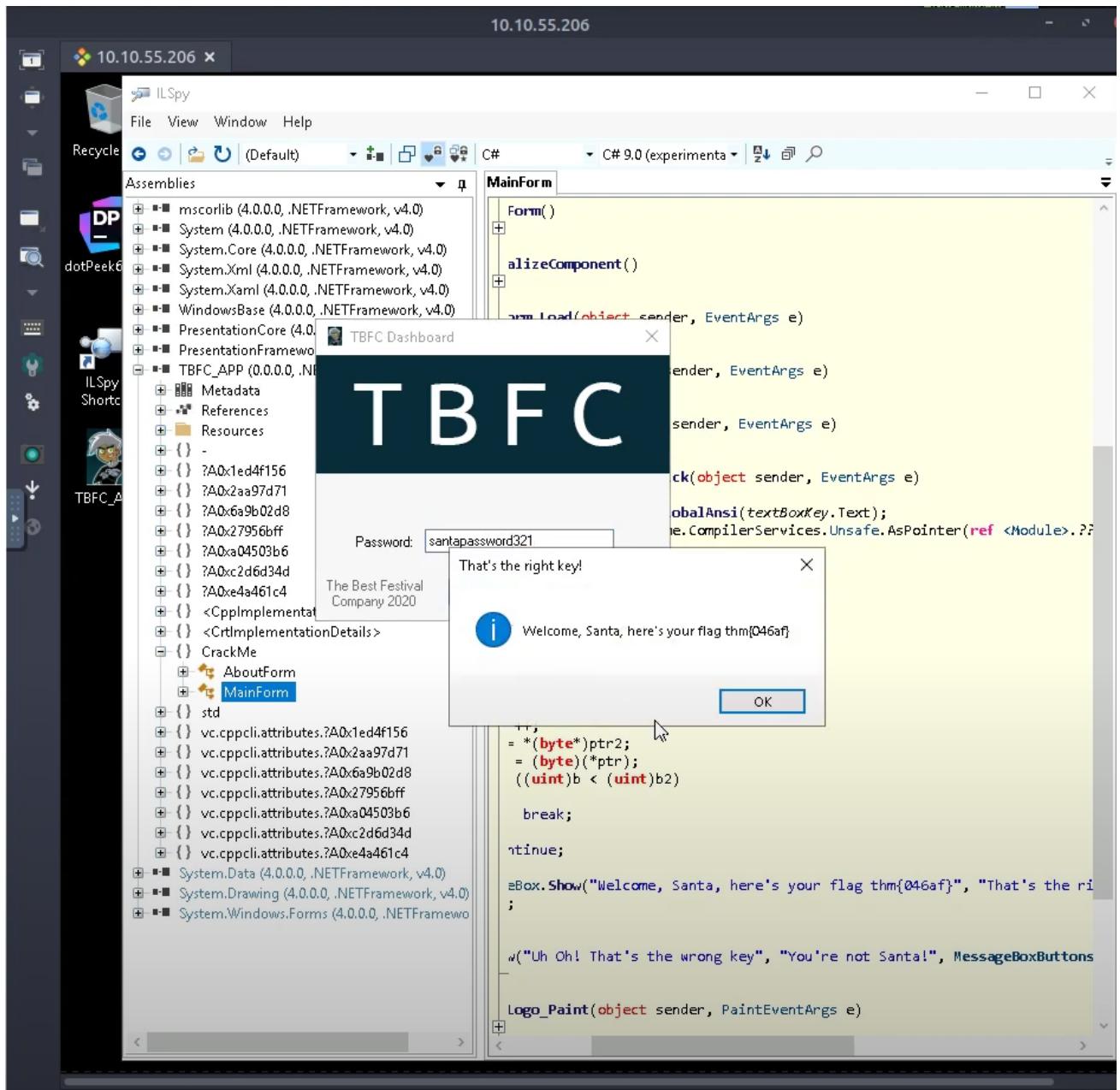
The screenshot shows the CyberChef interface. In the 'Input' section, the hex code '73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31 00' is pasted. In the 'Output' section, the resulting ASCII text 'santapassword321.' is displayed. The 'From Hex' tab is selected in the 'Recipe' sidebar.

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](http://[c].xyz/api.[d]?[e]=FUZZ)

The Naughty or Nice List - Mozilla Firefox

AttackBox IP:10.10.122.246

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...

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!

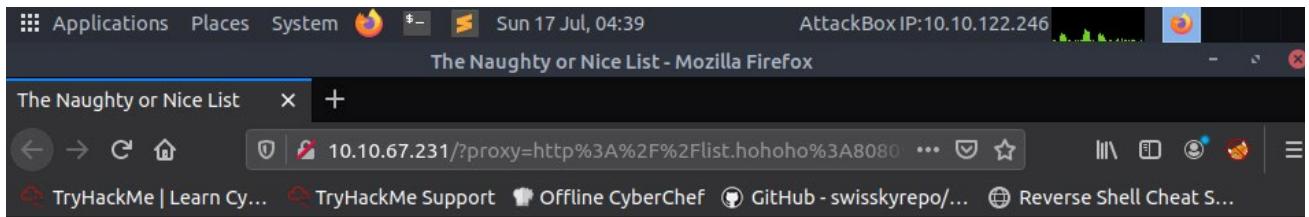
- Santa

Name:

Search

Timontyh is on the Naughty List.

Timontyh: Naughty



# 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:

kanes is on the Naughty List.

Kanes : Naughty

The Naughty or Nice List - Mozilla Firefox

The Naughty or Nice List X +

10.10.67.231/?proxy=http%3A%2F%2Flist.hohoho%3A8080 ... TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...

A cartoon illustration of Santa Claus. He is wearing his traditional red suit with white trim and a white beard. He is carrying a large sack filled with wrapped gifts, including one in green and one in purple. He is pointing his right index finger upwards towards the text "Welcome children!".

A vertical sidebar on the left side of the page containing three icons: a magnifying glass over a letter 'A', a clipboard with a document icon, and a square with a circular arrow icon.

# 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.

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...

A cartoon illustration of Santa Claus, wearing his red suit and hat, carrying a large sack filled with wrapped gifts. He is smiling and pointing upwards with his right hand.

# 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 Mozilla Firefox

The Naughty or Nice List - Mozilla Firefox

The Naughty or Nice List +

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

The Naughty or Nice List - Mozilla Firefox

The Naughty or Nice List +

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...

10.10.67.231/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F

A cartoon illustration of Santa Claus standing and pointing his right hand upwards. He is wearing his traditional red suit with white trim, a white beard, and a red hat. A large sack filled with wrapped gifts (blue, green, purple) is slung over his left shoulder.

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 Naughty List.

Lan Chai: Naughty

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

Sun 17 Jul, 04:59      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...

A cartoon illustration of Santa Claus standing and waving. He is wearing his traditional red suit with white trim, a white beard, and a red hat. He is carrying a large red sack filled with wrapped gifts, including one with a blue bow and another with a gold ribbon.

Welcome children!

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

Have a Merry Christmas! Ho ho ho!

- Santa

Name:

Search

Not Found

The requested URL was not found on this server.

Admin

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

Sun 17 Jul, 05:08      AttackBox IP:10.10.122.246

The Naughty or Nice List - Mozilla Firefox

The Naughty or Nice List    +

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

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

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

The Naughty or Nice List - Mozilla Firefox

The Naughty or Nice List +

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...

10.10.67.231/?proxy=http%3A%2F%2Flist.hohoho%3A22

A cartoon illustration of Santa Claus standing and pointing his right hand upwards. He is wearing his traditional red suit with white trim, a white beard, and a red hat. He is carrying a large red sack filled with wrapped gifts, including one green gift with a blue ribbon and another with a gold ribbon.

# The List

Welcome children!

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

Have a Merry Christmas! Ho ho ho!

- Santa

Name:

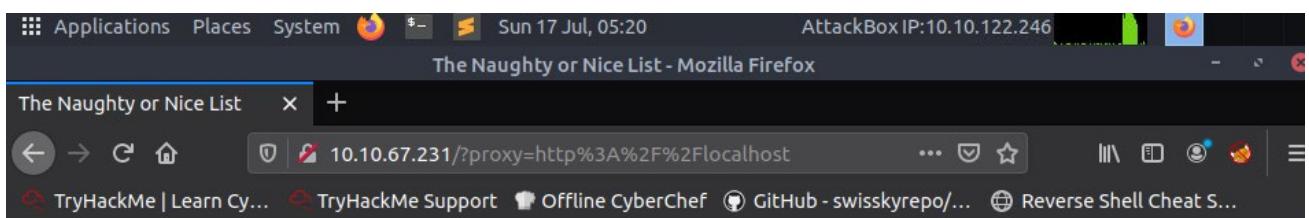
Search

Recv failure: Connection reset by peer

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



# 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!

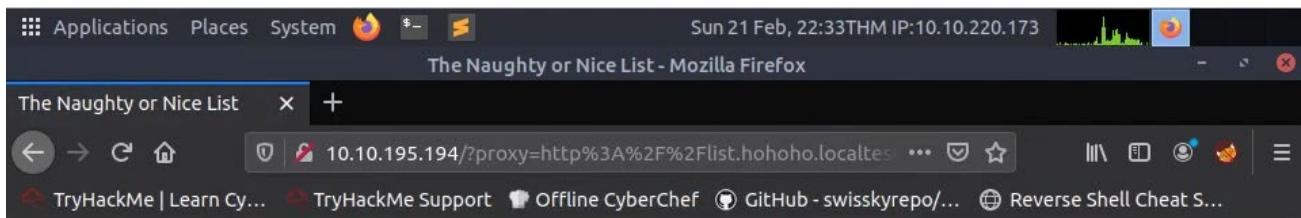
- Santa

Name:

Your search has been blocked by our security team.

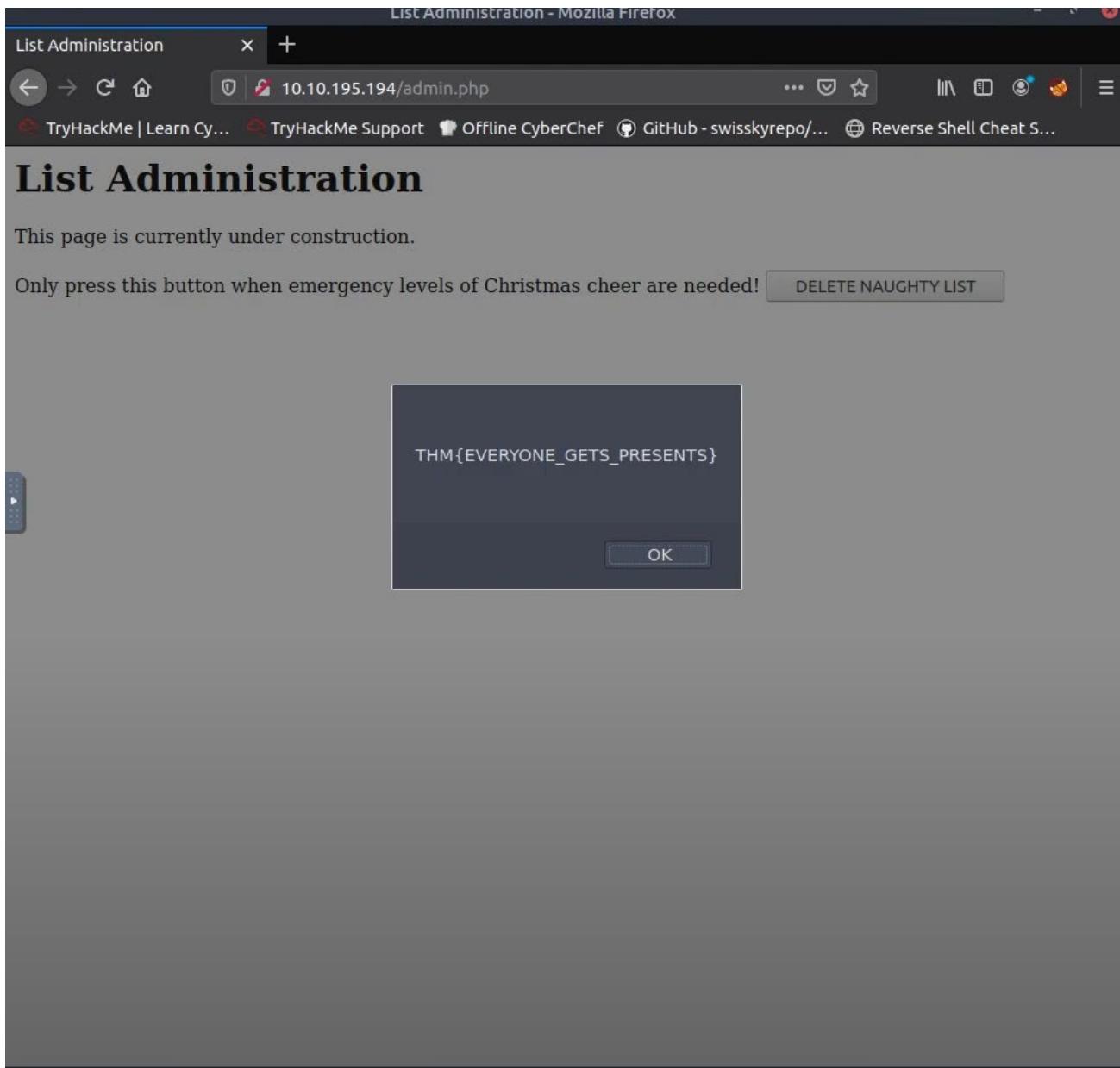
Ans : Your search has been blocked by our security team.

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 button and capture the flag.

## Day 20: Blue Teaming Powershell 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

The screenshot shows a Windows PowerShell window titled 'c:\windows\system32\cmd.exe - powershell'. The session starts with an SSH connection to a host at IP 10.10.233.125, where the user 'mceager' is logged in. The user then navigates to the 'Documents' folder and uses the 'Get-ChildItem -File -Hidden' cmdlet to find hidden files. A table is displayed showing two files: 'desktop.ini' and 'elfone.txt'. Finally, the user reads the content of 'elfone.txt' using the 'Get-Content' cmdlet.

```
root@ip-10-10-233-232:~# ssh -l mceager 10.10.233.125
mceager@10.10.233.125's password:

Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

mceager@ELFSTATION1 C:\Users\mceager>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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 elfone.txt

PS C:\Users\mceager\Documents> Get-Content elfone.txt
```

```

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> Get-Content e1fone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\Documents>

```

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

```

c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Help

Directory: C:\Users\mceager\Desktop

Mode                LastWriteTime          Length Name
----                -----          ----  --
d--h--        12/7/2020 11:26 AM           elf2wo

PS C:\Users\mceager\Desktop> Set-Location .\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> Get-Content e70smsW10Y4k.txt
I want the movie Scrooged <3!
PS C:\Users\mceager\Desktop\elf2wo>

```

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
----                -              -          -
d--h--       11/17/2020   10:58 AM        85887 1.txt
d--h--       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.