

# 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

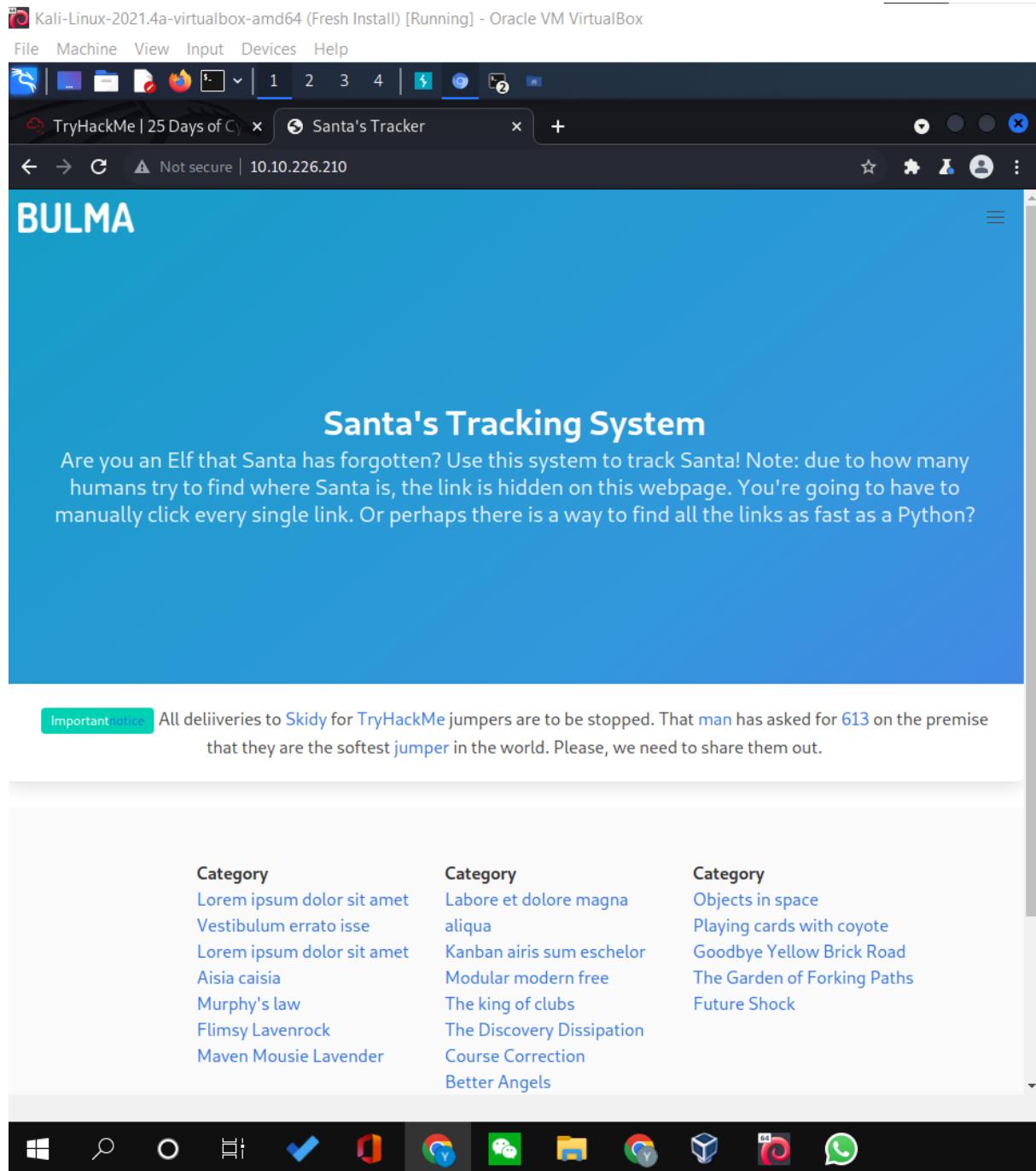
## Solution/walkthrough: John Hammond

## 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)

Kali-Linux-2021.4a-virtualbox-amd64 [Fresh Install] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | 25 Days of C | Santa's Tracker | view-source:10.10.226.210

Not secure | view-source:10.10.226.210

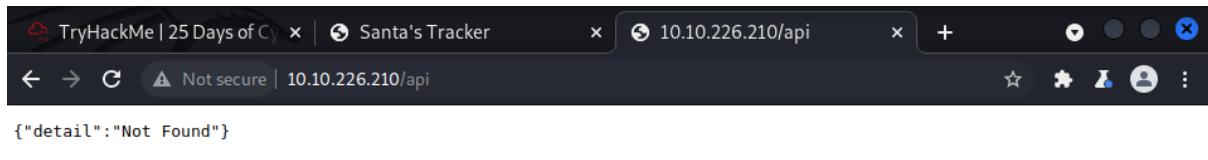
```
53     

# Santa's Tracking System


54
55     <h2 class="subtitle">
56
57         Are you an Elf that <a href="https://tryhackme.com">Santa</a> has forgotten? Use this system to
58             </h2>
59         </div>
60     </div>
61 </section>
62 <div class="box cta">
63     <p class="has-text-centered">
64         <span class="tag is-primary">Important <a href="https://tryhackme.com">notice</a></span> All deliv-
65             </p>
66 </div>
67
68 <footer class="footer">
69     <div class="container">
70         <div class="columns">
71             <div class="column is-3 is-offset-2">
72                 <h2><strong>Category</strong></h2>
73                 <ul>
74                     <li><a href="#">Lorem ipsum dolor sit amet</a></li>
75                     <li><a href="#">Vestibulum errato isse</a></li>
76                     <li><a href="#">Lorem ipsum dolor sit amet</a></li>
77                     <li><a href="#">Aisia caisia</a></li>
78                     <li><a href="#">Murphy's law</a></li>
79                     <li><a href="#">Flimsy Lavenrock</a></li>
80                     <li><a href="#">Maven Mousie Lavender</a></li>
81                 </ul>
82             </div>
83             <div class="column is-3">
84                 <h2><strong>Category</strong></h2>
85                 <ul>
86                     <li><a href="#">Labore et dolore magna aliqua</a></li>
87                     <li><a href="#">Kanban airis sum eschelor</a></li>
88                     <li><a href="http://machine_ip/api/api_key">Modular modern free</a></li>
89                     <li><a href="#">The King of clubs</a></li>
90                     <li><a href="#">The Discovery Dissipation</a></li>
91                     <li><a href="#">Course Correction</a></li>
92                     <li><a href="#">Better Angels</a></li>
93                 </ul>
94             </div>
95             <div class="column is-4">
96                 <h2><strong>Category</strong></h2>
97                 <ul>
98                     <li><a href="#">Objects in space</a></li>
99                     <li><a href="#">Playing cards with coyote</a></li>
100                    <li><a href="#">Goodbye Yellow Brick Road</a></li>
101                    <li><a href="#">The Garden of Forking Paths</a></li>
102                    <li><a href="#">Future Shock</a></li>
103                </ul>
104            </div>
105        </div>
106        <div class="content has-text-centered">
```

## Question 4

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



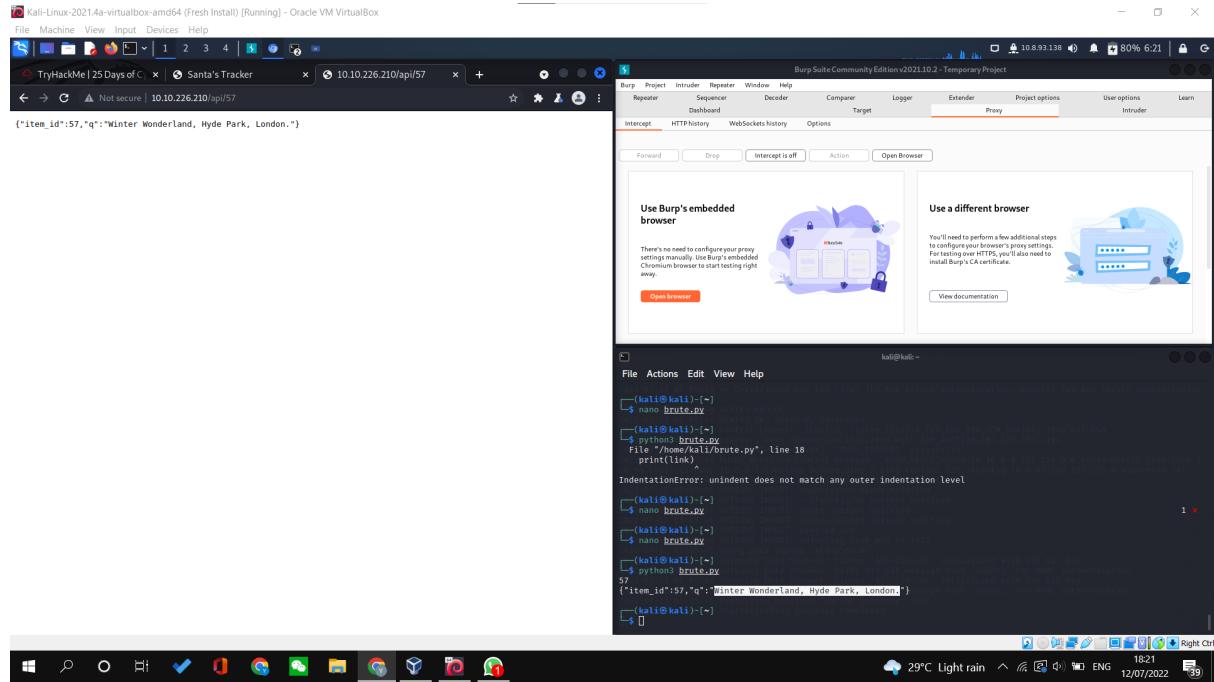
### Question 5

Where is Santa right now? (Tick all correct answers.)

```
kali@kali: ~
File Actions Edit View Help
2022-07-12 03:05:46 * Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
[(kali㉿kali)-[~]]$ nano brute.py
2022-07-12 03:05:46 VERIFY EKU OK
[(kali㉿kali)-[~]]$ python3 brute.py
2022-07-12 03:05:46 Control Channel: TLSv1.3, cipher TLS_AES_256_GCM_SHA384, 2048 bit RSA
2022-07-12 03:05:46 File "/home/kali/brute.py", line 18 [er]: 'PUSH_REQUEST' (status=1)
2022-07-12 03:05:46 print(link)
2022-07-12 03:05:46 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route-metric 1000,comp-1
2022-07-12 03:05:46 no router gateway 10.8.0.1,topology subnet,ping 5,ping-restart 120,ifconfig 10.8.93.138 255.255.0.0,peer-id 34'
IndentationError: unindent does not match any outer indentation level
2022-07-12 03:05:46 OPTIONS IMPORT: compression parms modified
[(kali㉿kali)-[~]]$ nano brute.py
2022-07-12 03:05:46 OPTIONS IMPORT: --ifconfig/up options modified
2022-07-12 03:05:46 OPTIONS IMPORT: route options modified
2022-07-12 03:05:46 OPTIONS IMPORT: route-related options modified
[(kali㉿kali)-[~]]$ nano brute.py
2022-07-12 03:05:46 OPTIONS IMPORT: peer-id set
2022-07-12 03:05:46 Using peer cipher 'AES-256-CBC'
[(kali㉿kali)-[~]]$ python3 brute.py
2022-07-12 03:05:46 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2022-07-12 03:05:46 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."} message hash 'SHA512' for HMAC authentication
2022-07-12 03:05:46 Preserving previous TUN/TAP instance: tun0
[(kali㉿kali)-[~]] Initialization Sequence Completed
[(kali㉿kali)-[~]]$
```

### 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

The screenshot shows a browser window with a table of initial data types and their sizes, and a terminal window showing a root shell on an AttackBox.

**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:

- $(Rb, Ri) = \text{MemoryLocation}[Rb + Ri]$
- $D(Rb, Ri) = \text{MemoryLocation}[Rb + Ri + D]$

THM AttackBox

### Question 2

The screenshot shows a browser window with a program output and a terminal window showing a root shell on an AttackBox.

see what should be happening like so:

```
ashu@ashu-Inspiron-5379:~/Desktop$ ./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`

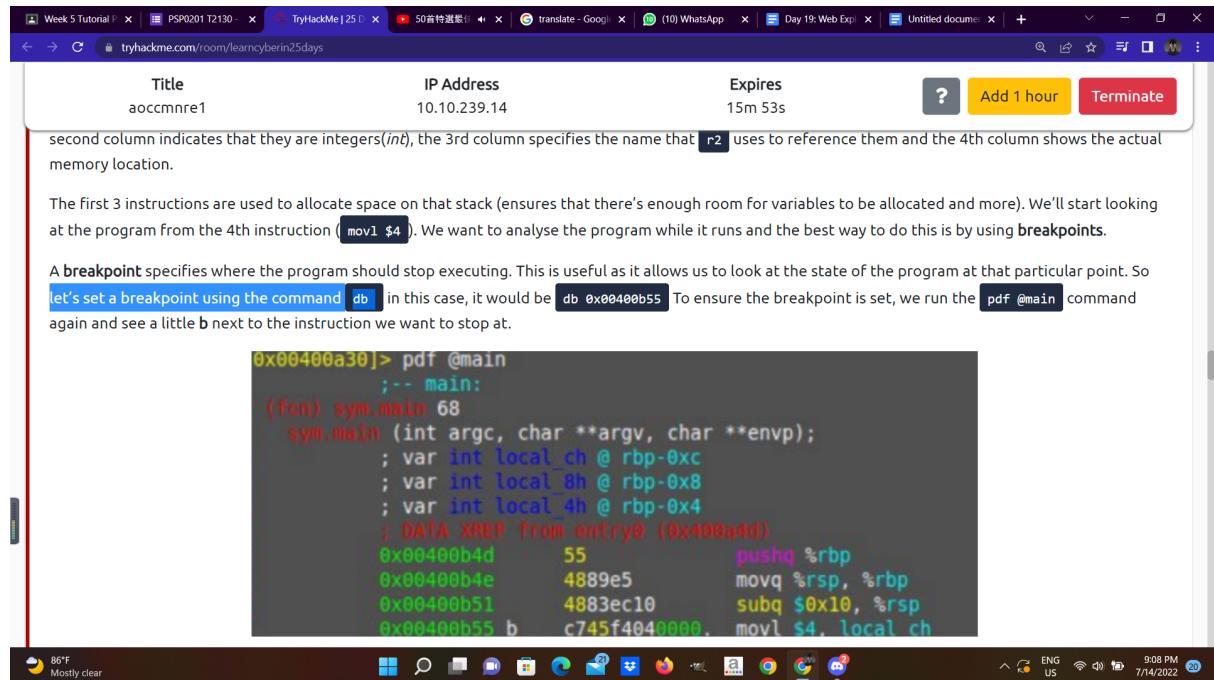
Note, when using the `aa` command in radare2, this may take between 5-10 minutes depending on your system.

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?`

THM AttackBox

## Question 3



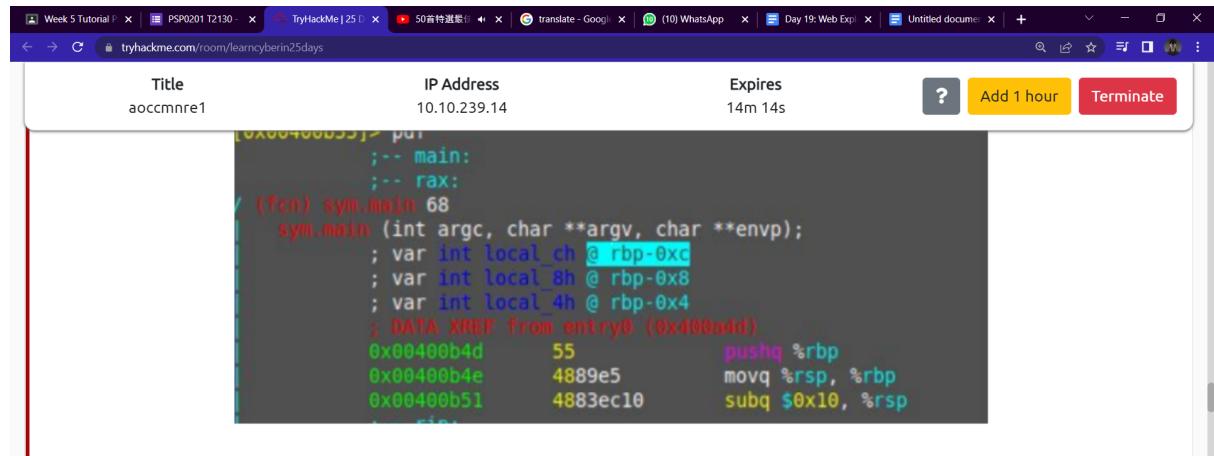
second column indicates that they are integers(`int`), the 3rd column specifies the name that `r2` uses to reference them and the 4th column shows the actual memory location.

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.

```
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
```

## Question 4



```
[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
0x00400b55: 00 00 00 00 00 00 00 00
```

## Question 5

**6.Challenge**

Use your new-found knowledge of Radare2 to analyse the "challenge1" file in the Instance **10.10.136.5** that is attached to this task to answer the questions below.

**Answer the questions below**

What is the value of **local\_ch** when its corresponding movl instruction is called (first if multiple)?

Correct Answer

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

Submit

What is the value of **local\_4h** before **eax** is set to 0?

Submit

```

[+] 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
  0x00400b54  c745f8060000  mov dword [local_8h], 6
  0x00400b5f  b845f4      mov eax, dword [local_c]
  ...
  0x00400b62  0faf45f8    imul eax, dword [local_
  0x00400b66  8945fc      mov dword [local_4h], e
  0x00400b69  b800000000  mov eax, 0
  0x00400b6e  5d          pop rbp
  0x00400b6f  c3          ret
[0x00400a30]>

```

Task 20 [Day 18] Reverse Engineering The Bits of Christmas 47m 37s  
82°F Partly cloudy

## Question 6

**6.Challenge**

Use your new-found knowledge of Radare2 to analyse the "challenge1" file in the Instance **10.10.136.5** that is attached to this task to answer the questions below.

**Answer the questions below**

What is the value of **local\_ch** when its corresponding movl instruction is called (first if multiple)?

Correct Answer

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

Correct Answer

What is the value of **local\_4h** before **eax** is set to 0?

Correct Answer

```

[+] 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
  0x00400b54  c745f8060000  mov dword [local_8h], 6
  0x00400b5f  b845f4      mov eax, dword [local_c]
  ...
  0x00400b62  0faf45f8    imul eax, dword [local_
  0x00400b66  8945fc      mov dword [local_4h], e
  0x00400b69  b800000000  mov eax, 0
  0x00400b6e  5d          pop rbp
  0x00400b6f  c3          ret
[0x00400a30]>

```

Task 20 [Day 18] Reverse Engineering The Bits of Christmas 45m 15s  
82°F Partly cloudy

## Question 7

The screenshot shows a terminal window with several tabs open. The current tab displays assembly code from address 0x00400a30 to 0x00400a4d. The assembly code includes instructions like push rbp, mov dword [local\_8], and mov byte [local\_4]. The terminal also shows command-line interactions with the debugger.

```

Last login: Thu Jul 14 15:07:52 2022 from 10.10.119.215
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1886 started...
= attach 1886 1886
bln.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[0x00400a30]> aa
[!] Analyze all flags starting with sym. and entry0 (aa)
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
[!] Analyze all flags starting with sym. and entry0 (aa)
[0x00400a30]> pdf @main
;-> main:
/ (cn) 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)
0x00400040      55          push rbp
0x00400041      4899e5     mov rbp, rsp
0x00400042      c745f4010000  mov dword [local_ch], 1
0x00400043      c745f8060000  mov dword [local_8h], 0
0x00400044      b844f4        mov byte [local_4h], 0
0x00400045      0f7f00000000  lmul eax, word [local_8h]
0x00400046      8941fc        mov dword [local_4h], eax
0x00400047      b80000000000  mov byte [local_4h], 0
0x00400048      5d          pop rbp
0x00400049      c3          ret
[0x00400a30]>

```

**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.

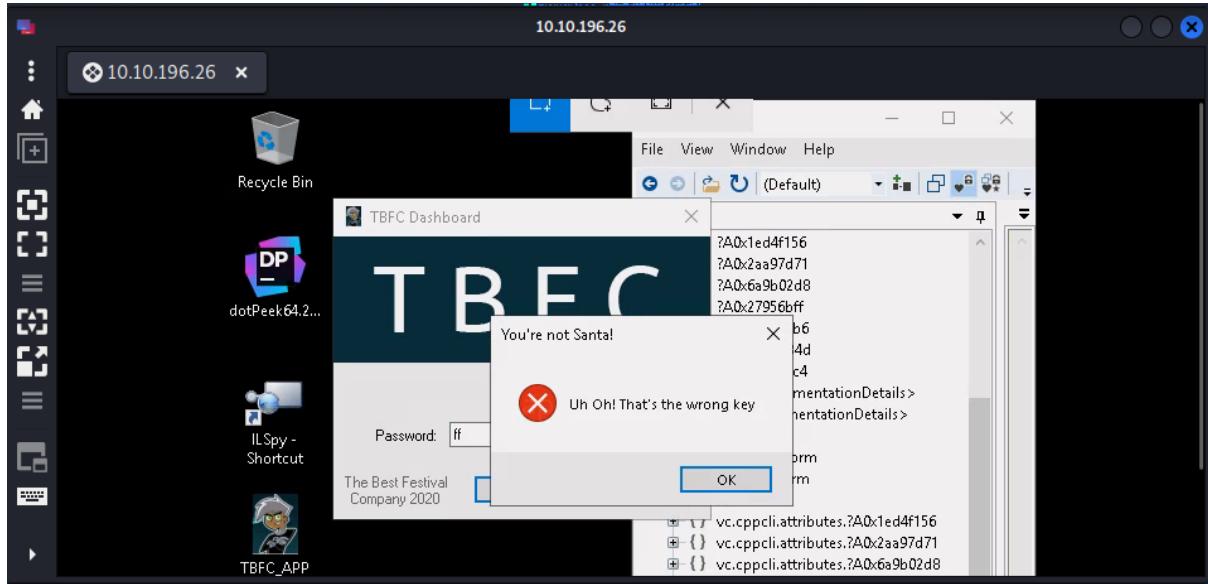
## Day 18: Reverse Engineering - The Bits of Christmas

**Tools used:** Kali Linux, Chrome

**Solution/walkthrough:** John Hammond

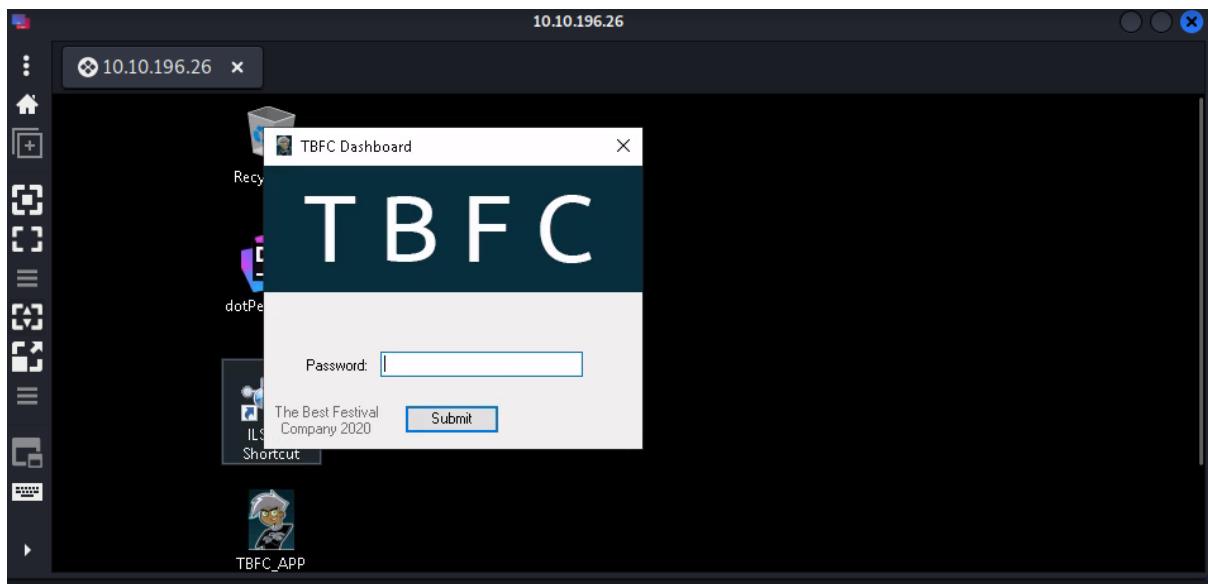
### Question 1

What is the message that shows up if you enter the wrong password for TBFC\_APP?



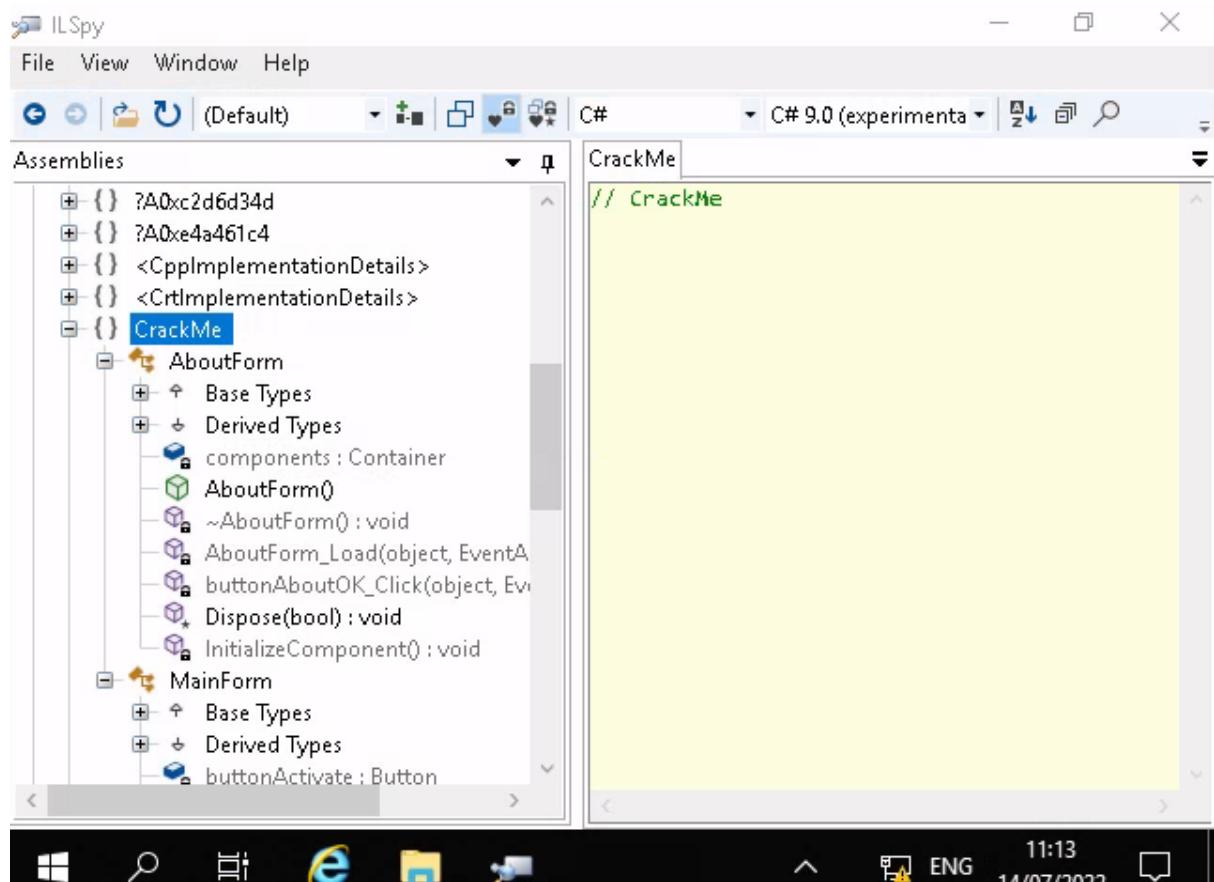
## Question 2

What does TBFC stand for?



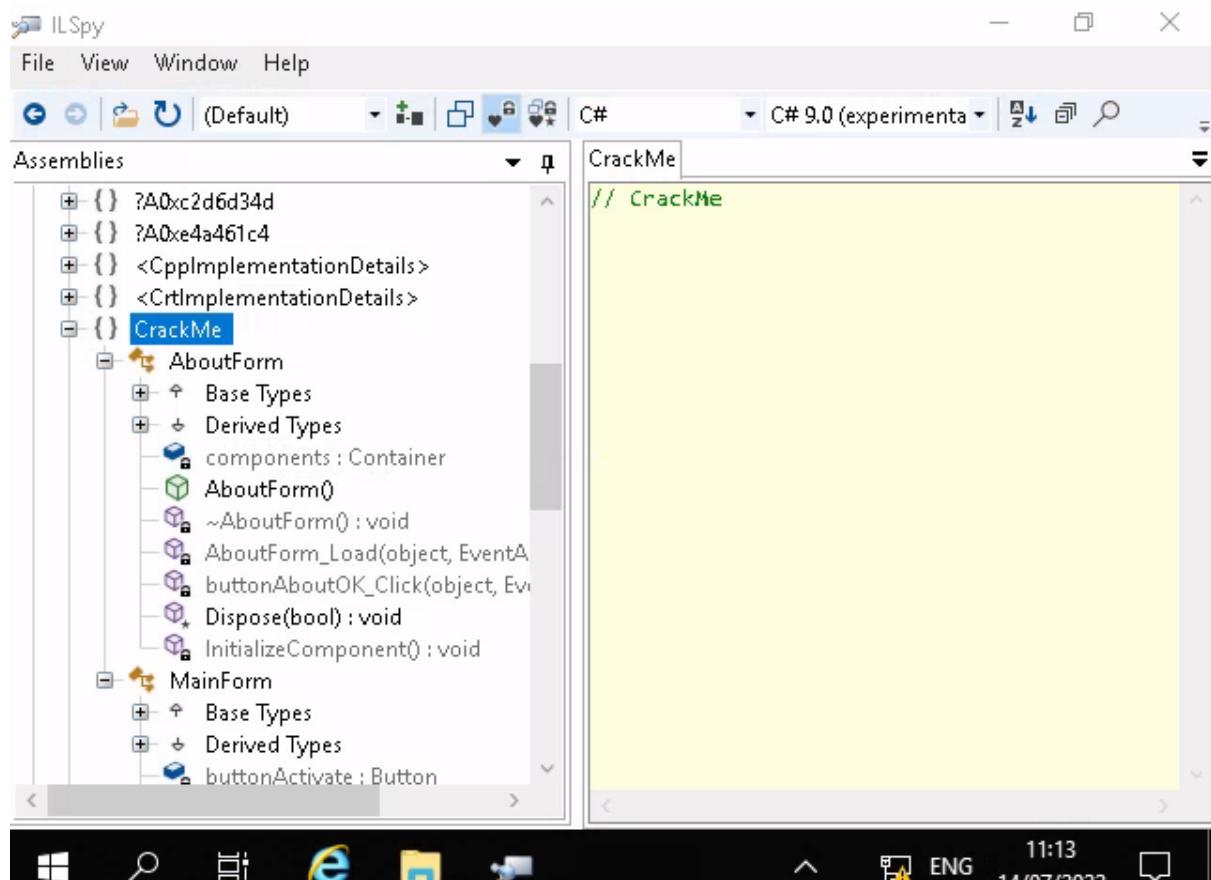
## Question 3

Decompile the TBFC\_APP with ILSpy. What is the module that catches your attention?



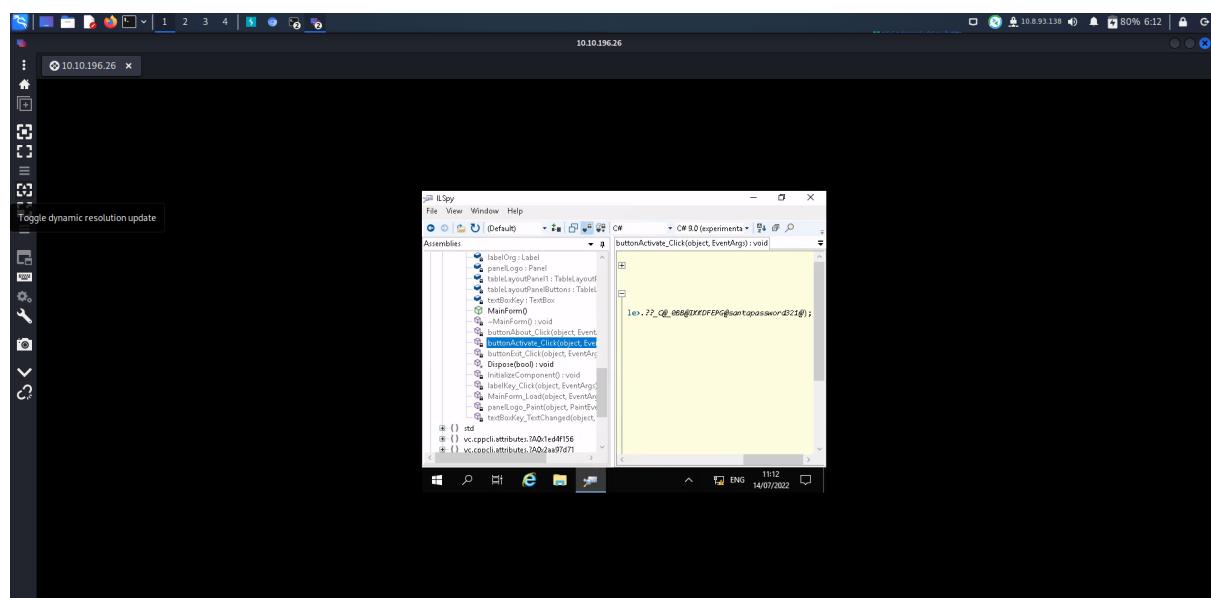
#### Question 4

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



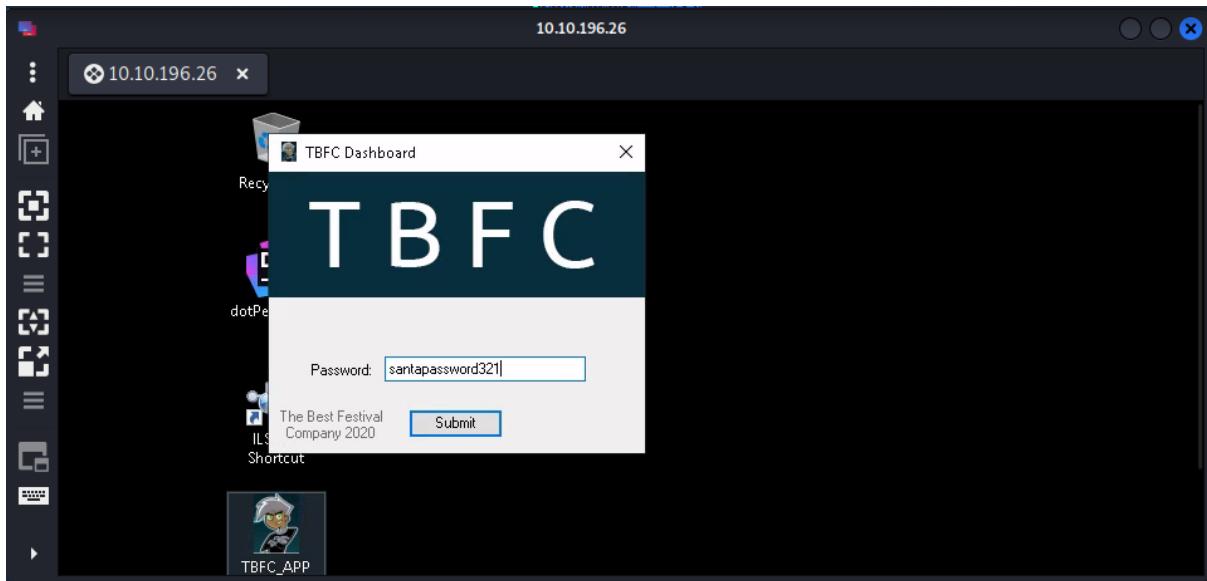
### Question 5

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



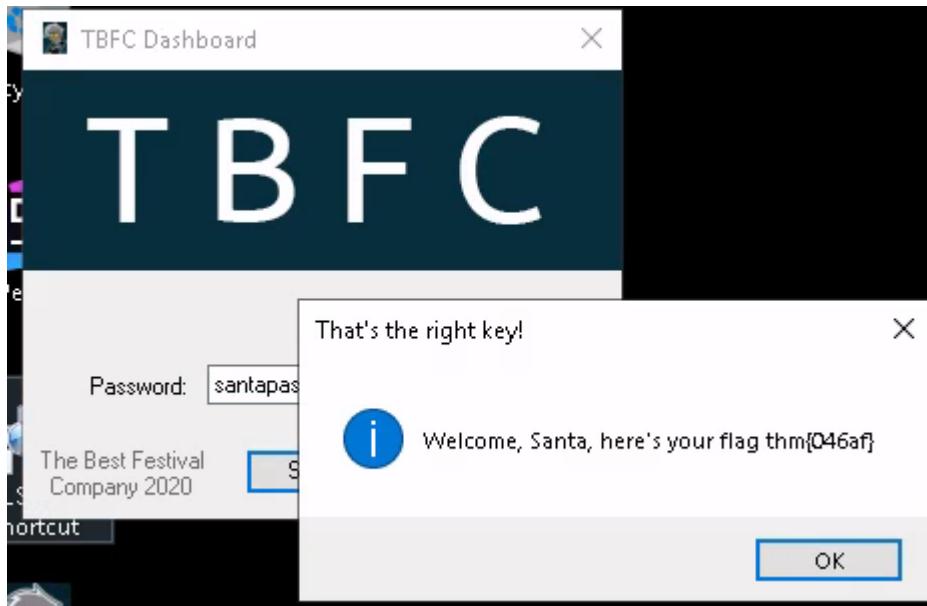
### Question 6

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 Cy The Naughty or Nice List +

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

 Welcome children!

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

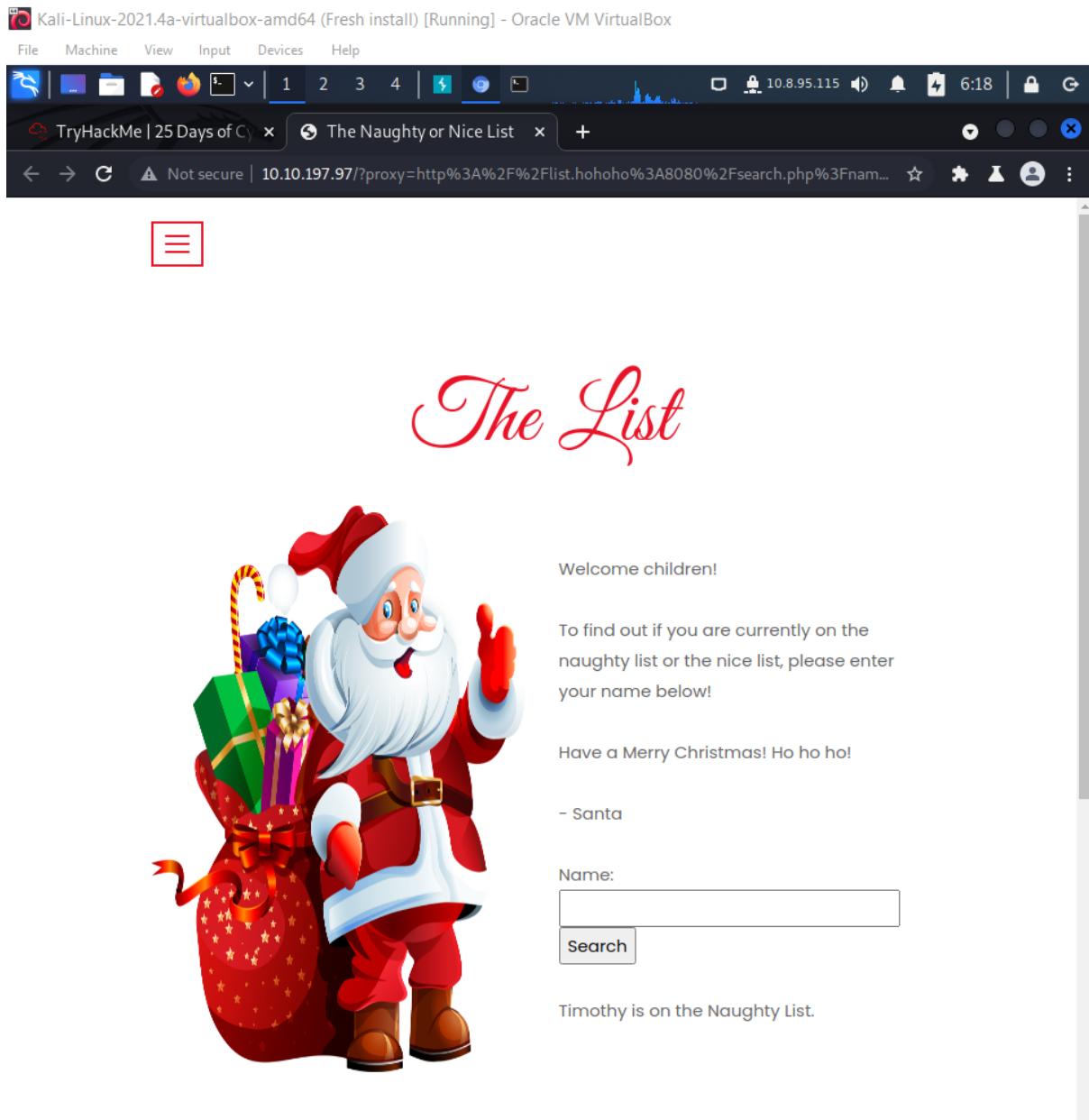
Have a Merry Christmas! Ho ho ho!

- Santa

Name:

Search

Timothy 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... ☆ 🔍 6:18



# 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:

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... ☆ 🔍 6:19



# The List



Welcome children!

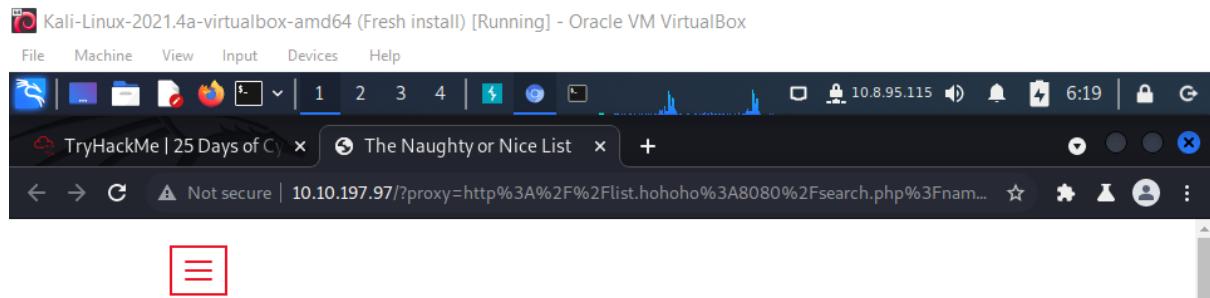
To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name:

YP is on the Nice List.



# The List



Welcome children!

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

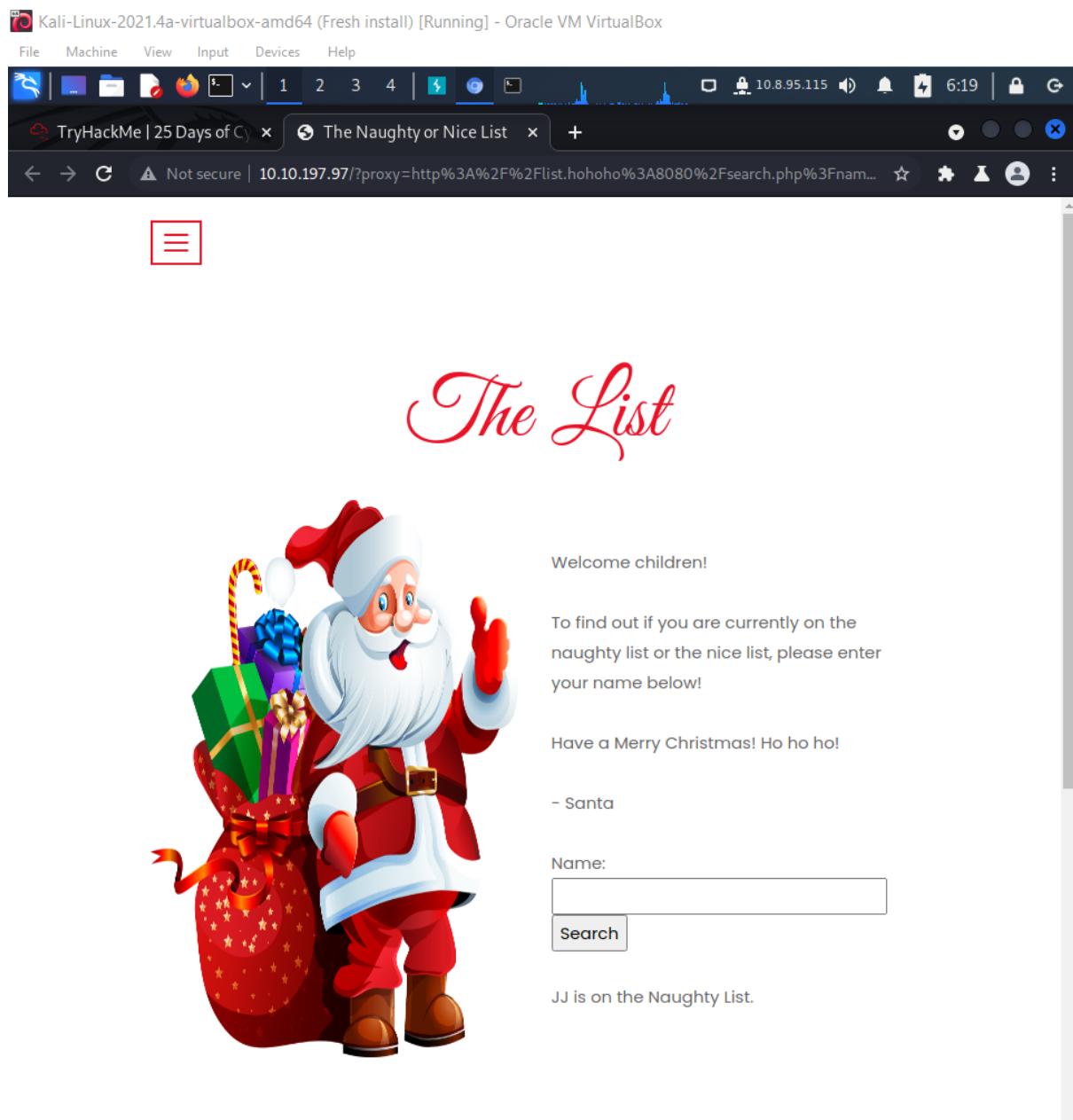
Have a Merry Christmas! Ho ho ho!

- Santa

Name:

Kanes is on the Naughty List.



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... ☆ 🔍 6:20

A cartoon illustration of Santa Claus standing and pointing his right hand towards the viewer. He is wearing his traditional red suit with white trim, a white beard, and a red hat. A large sack filled with wrapped gifts is slung over his shoulder.

*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:

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"?

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

File Machine View Input Devices Help

TryHackMe | 25 Days of Cy x The Naughty or Nice List x The Naughty or Nice List x + 10.8.95.115 6:23 Not secure | 10.10.197.97/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F



# 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:

## 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"?

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

File Machine View Input Devices Help

TryHackMe | The Naught | The Naught | The Naught | The Naught | +

Not secure | 10.10.197.97/?proxy=http%3A%2F%2Flist.hohoho%3A80

10.8.95.115 6:25



*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



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

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

File Machine View Input Devices Help

TryHackMe | The Naught | The Naught | The Naught | The Naught | +

Not secure | 10.10.197.97/?proxy=http%3A%2F%2Flist.hohoho%3A22

6:25

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

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

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

File Machine View Input Devices Help

TryHackMe | The Nau... | +

Not secure | 10.10.197.97/?proxy=http%3A%2F%2Flocalhost

6:26

The screenshot shows a web browser window on a Kali Linux virtual machine. The address bar displays the URL `10.10.197.97/?proxy=http%3A%2F%2Flocalhost`. The page content features a large red title "The List". To the left of the text is a cartoon illustration of Santa Claus carrying a large sack filled with wrapped gifts. On the right side of the title, there is a "Welcome children!" message and a form for entering a name to check the naughty or nice list. Below the form, a note states that the search has been blocked by the security team. The browser interface includes a menu bar, a toolbar with various icons, and a status bar at the bottom.

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

Your search has been blocked by our security team.

### Q3: What is Santa's password?

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

File Machine View Input Devices Help

Try! x | The x | List x | +

Not secure | 10.10.197.97/?proxy=http%3A%2F%2Flist.hohoho.localtest.me

6:33

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

Santa,

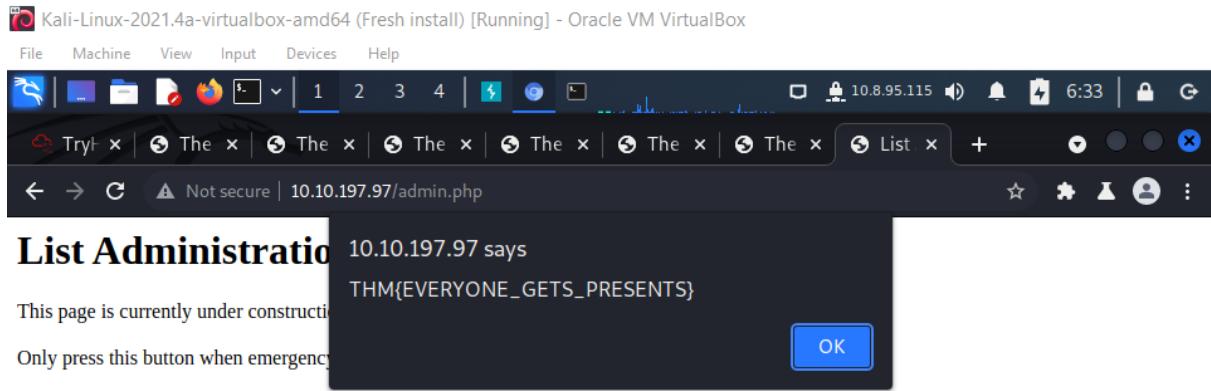
If you need to make any changes to the Naughty or Nice list, you need to login.

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

- Elf McSkidy



### 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?

```
(kali㉿kali)-[~]
$ ssh -l mceager 10.10.93.214
^C  PowershELIF to the rescue

(kali㉿kali)-[~]
$ ssh --help
unknown option --help. The contents within the stockings have been removed. A clue
usage: ssh [-46AaCcGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
(kali㉿kali)-[~]
$ sudo apt-get install remmina
```

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

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?

```
File Actions Edit View Help https://tryhackme.com/room/16788  
Directory: C:\Windows\system32\3lfthr3e Watch John Hammond's video on how to connect to this machine via SSH to connect to this machine.  
  
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 Note that your IP address will be  
Average :  
Sum : If you logged in successfully, you  
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)

```
+-----+ Expired Machine
Unexpected token 'get-content' in expression or statement.
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorReco
rdException
+ FullyQualifiedErrorId : UnexpectedToken

PS C:\Windows\system32\3lfthr3e> get-content 2.txt | select-string -Pattern
"redryner"
PS C:\Windows\system32\3lfthr3e> Get-Content 2.txt | Select-String -Pattern
"veryder"
PS C:\Windows\system32\3lfthr3e> get-content 2.txt | select-string -Pattern
"redryder"
redryderbbgun
```

### 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.