PSP0201 Week 5 Writeup

Group Name: Gold
Members:

ID	Name	Role
1211101707	Nur’aina Binti Ikhwan Moeid	Leader
1211103984	Nur Afreen Junaidah Binti Noorul Mohamed Eliyas	Member
1211101519	Aisyah Binti Ahmad Komarolaili	Member
1211102590	Nur Hanisah Binti Mohd Pauzi	Member

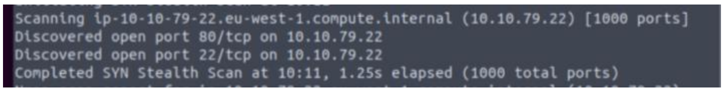
Day 16: Scripting - Help! Where is Santa?

Tools used: THM AttackBox, Firefox, Python

Solution/walkthrough:

Question 1

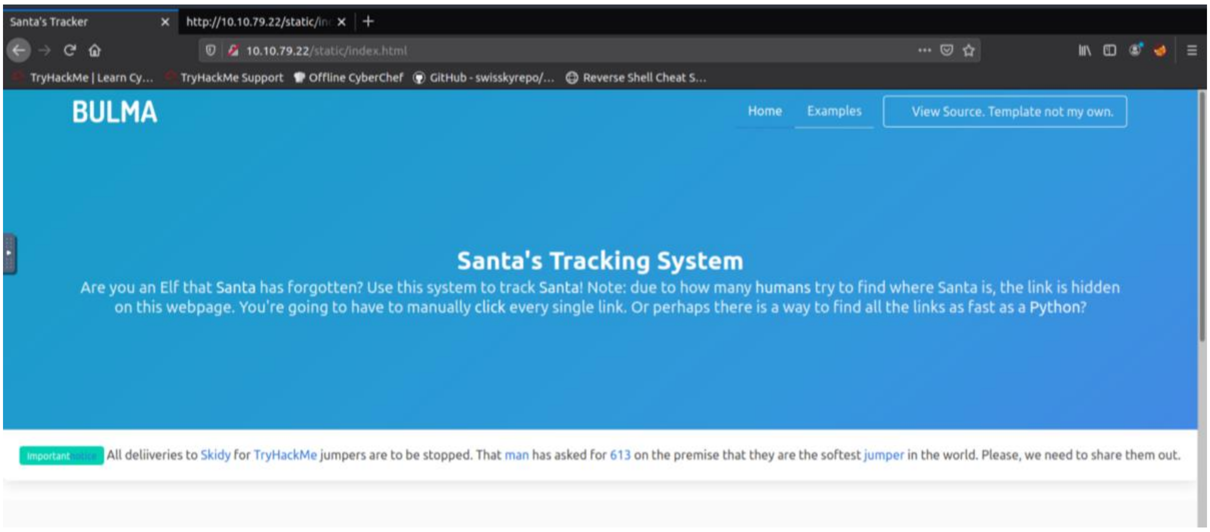
What is the port number for the web server? -80



```
Scanning ip-10-10-79-22.eu-west-1.compute.internal (10.10.79.22) [1000 ports]
Discovered open port 80/tcp on 10.10.79.22
Discovered open port 22/tcp on 10.10.79.22
Completed SYN Stealth Scan at 10:11, 1.25s elapsed (1000 total ports)
```

Question 2

What templates are being used? -BULMA



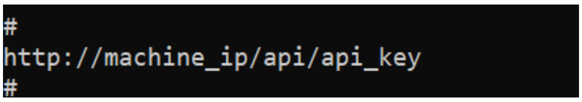
Santa's Tracking System

Are you an Elf that Santa has forgotten? Use this system to track Santa! Note: due to how many humans try to find where Santa is, the link is hidden on this webpage. You're going to have to manually click every single link. Or perhaps there is a way to find all the links as fast as a Python?

Important notice All deliiveries to Skidy for TryHackMe jumpers are to be stopped. That man has asked for 613 on the premise that they are the softest jumper in the world. Please, we need to share them out.

Question 3

Without using enumerations tools such as Dirbuster, what is the directory for the API? - /api/

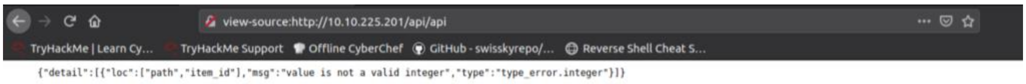


```
#
http://machine_ip/api/api_key
#
```

Question 4

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

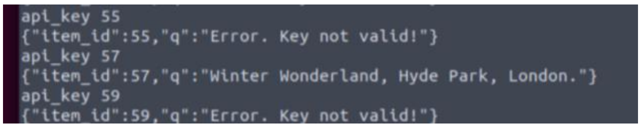
- {"detail":[{"loc":["path","item_id"],"msg":"value is not a valid integer","type":"type_error.integer"}]}



```
{"detail":[{"loc":["path","item_id"],"msg":"value is not a valid integer","type":"type_error.integer"}]}
```

Question 5

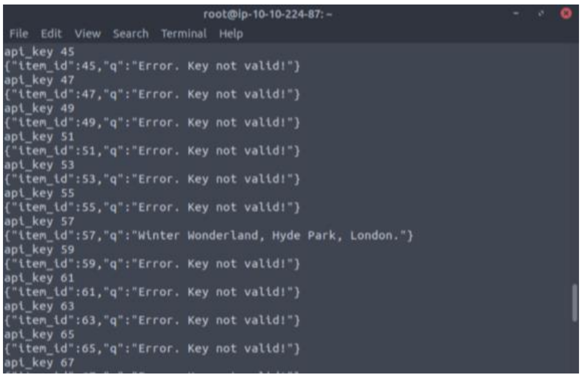
Where is Santa right now? -Winter Wonderland, Hyde Park, London



```
api_key 55
{"item_id":55,"q":"Error. Key not valid!"}
api_key 57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
api_key 59
{"item_id":59,"q":"Error. Key not valid!"}
```

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) -57



```
api_key 45
{"item_id":45,"q":"Error. Key not valid!"}
api_key 47
{"item_id":47,"q":"Error. Key not valid!"}
api_key 49
{"item_id":49,"q":"Error. Key not valid!"}
api_key 51
{"item_id":51,"q":"Error. Key not valid!"}
api_key 53
{"item_id":53,"q":"Error. Key not valid!"}
api_key 55
{"item_id":55,"q":"Error. Key not valid!"}
api_key 57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
api_key 59
{"item_id":59,"q":"Error. Key not valid!"}
api_key 61
{"item_id":61,"q":"Error. Key not valid!"}
api_key 63
{"item_id":63,"q":"Error. Key not valid!"}
api_key 65
{"item_id":65,"q":"Error. Key not valid!"}
api_key 67
```

Thought Process/ Methodology:

Firstly, we're using nmap in the terminal to find the open ports using syntax `nmap <ip address>`. Next, we opened the developer tools in th web browser followed by tab elements.We look for the hint through the source code; `http://machine_ip/api/api_key.` After that, we're using python `python3 <script name>` to look out for all the HTML links in the website. From there, we modified the script and continue to run it. Then using the library request, we create a script and save it as "apibrute.py" and run `python3 apibrute.py` there, we found santa's location and the API key.

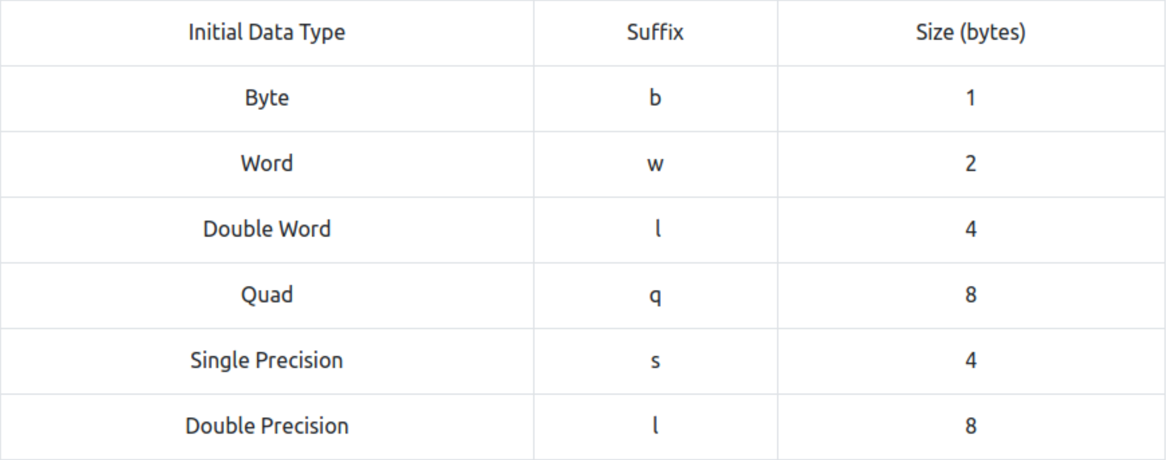
Day 17 - [Reverse Engineering] ReverseELFneering

Tools used: THM AttackBox, Firefox

Solution/walkthrough:

Question 1

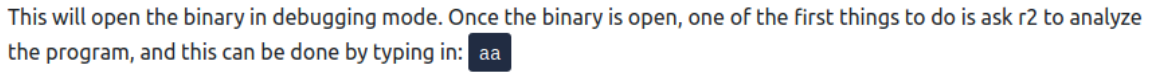
Match the data type with the size in bytes:



Initial Data Type	Suffix	Size (bytes)
Byte	b	1
Word	w	2
Double Word	l	4
Quad	q	8
Single Precision	s	4
Double Precision	l	8

Question 2

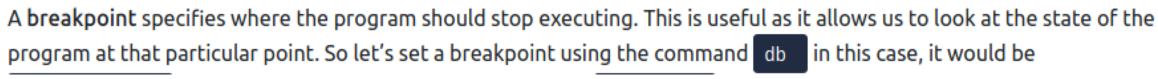
What is the command to analyse the program in radare2? - aa



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`

Question 3

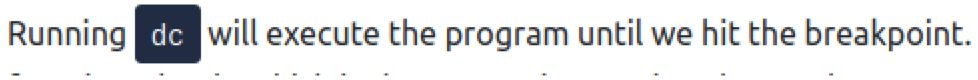
What is the command to set a breakpoint in radare2? - db



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

Question 4

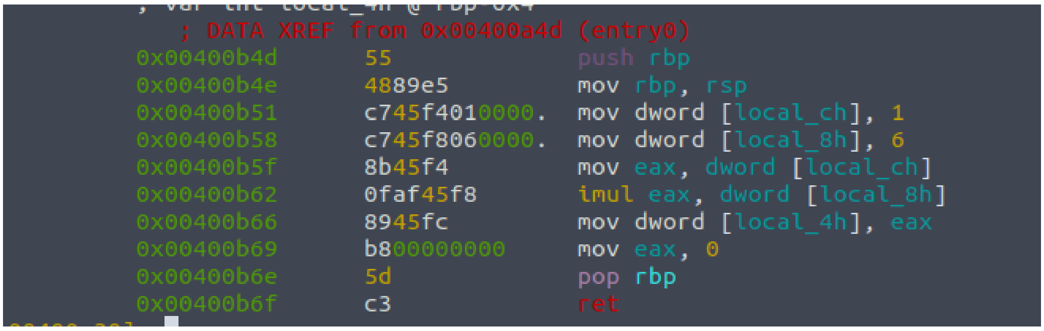
What is the command to execute the program until we hit a breakpoint? - dc



Running `dc` will execute the program until we hit the breakpoint.

Question 5

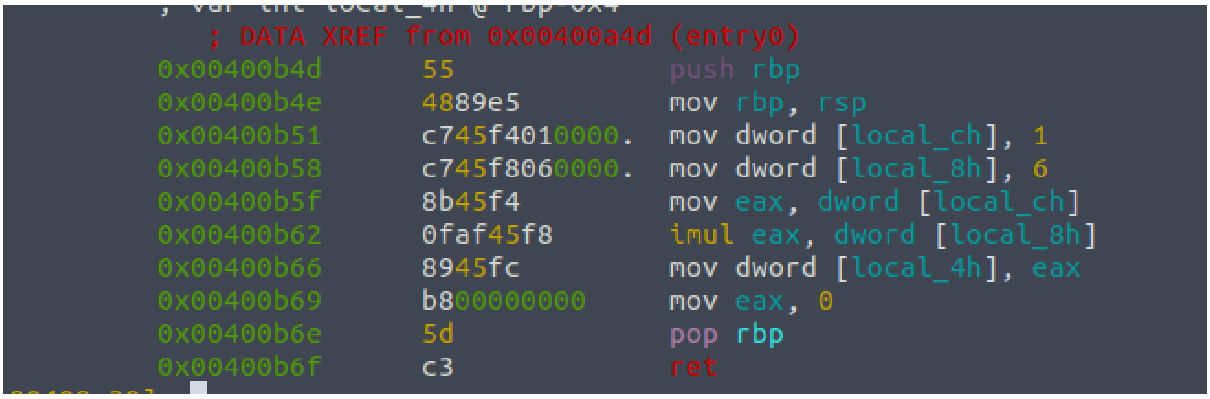
What is the value of local_ch when its corresponding movl instruction is called (first if multiple)? - 1



```
          ; 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
```

Question 6

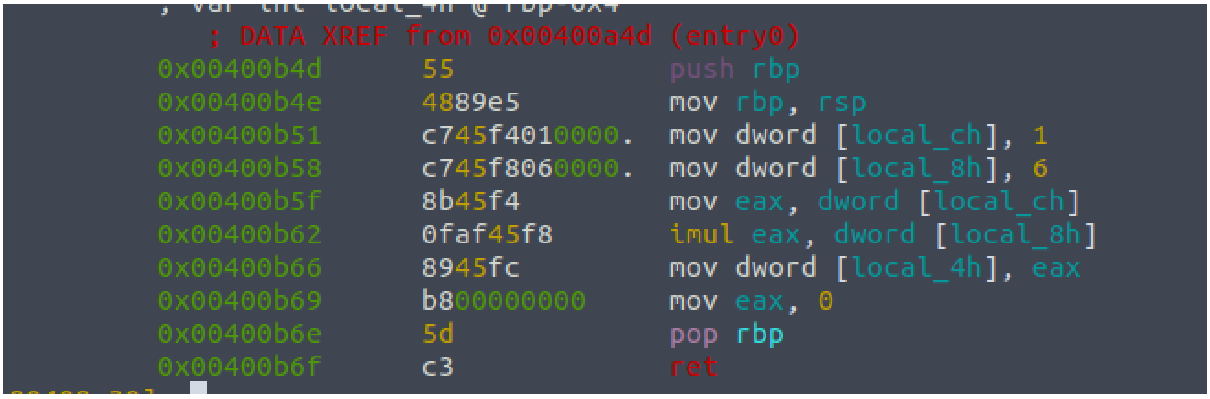
What is the value of eax when the imull instruction is called? - 6



```
   ; 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
```

Question 7

What is the value of local_4h before eax is set to 0? - 6



```
   ; 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
```

Thought Process/ Methodology:

We’re using a secure shell(ssh) in the terminal with an ip address given such as `<ssh elfmceager@ip address>`and inserted the password given which is adventofcyber. Then, 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`. 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`. As seen here, there actually is a function at main. Let’s examine the assembly code at main by running the command `pdf @main` Where pdf means print disassembly function.

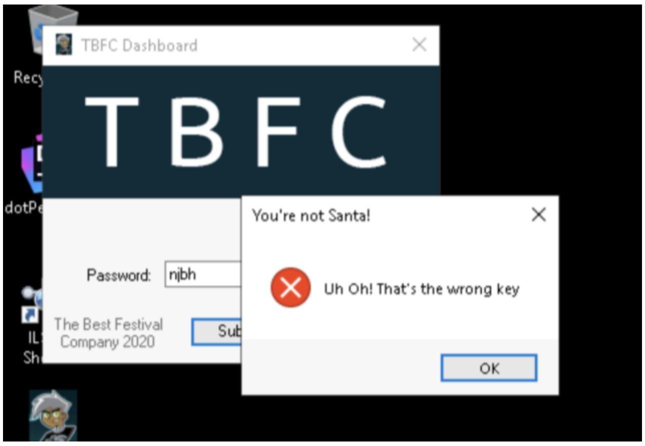
Day 18:Reverse Engineering - The Bits of Christmas

Tools used: THM AttackBox, Firefox, Cyberchef, Remmina, TBFC_APP

Solution/walkthrough:

Question 1

What is the message that shows up if you enter the wrong password for TBFC_APP? - Uh Oh! That's the wrong key



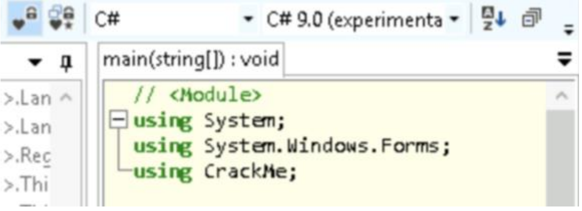
Uh Oh! That's the wrong key

Question 2

What does TBFC stand for? - The Best Festival Company

Question 3

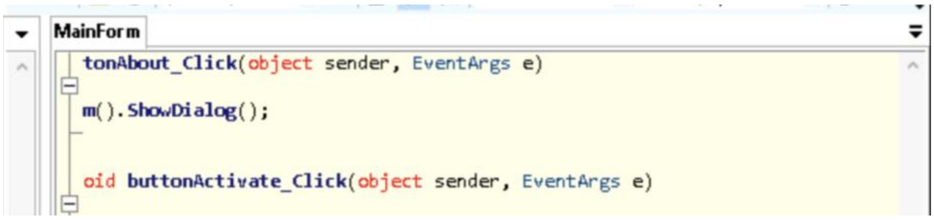
Decompile the TBFC_APP with ILSpy. What is the module that catches your attention? - CrackMe



```
// <Module>
using System;
using System.Windows.Forms;
using CrackMe;
```

Question 4

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



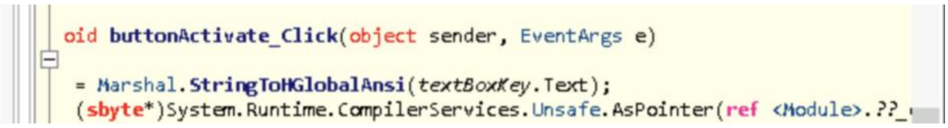
```
tonAbout_Click(object sender, EventArgs e)

m().ShowDialog();


oid buttonActivate_Click(object sender, EventArgs e)
```

<u>Question 5</u>

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

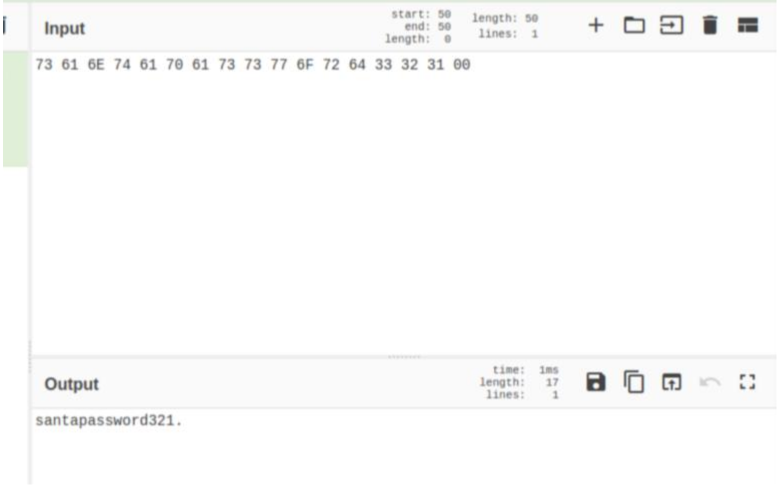


```
oid buttonActivate_Click(object sender, EventArgs e)

 = Marshal.StringToHGlobalAnsi(textBoxKey.Text);
 (sbyte*)System.Runtime.CompilerServices.Unsafe.AsPointer(ref <Module>.??_
```

<u>Question 6</u>

What is Santa's password? - santapassword321

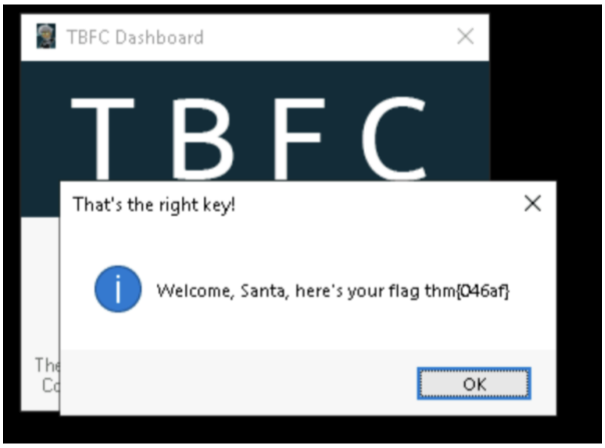


```
73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31 00
```

```
santapassword321.
```

<u>Question 7</u>

Now that you've retrieved this password, try to login...What is the flag? - thm{046af}



That's the right key!

Welcome, Santa, here's your flag thm{046af}

Thought Process/ Methodology:

After we opened TBF_APP, we tried entering the wrong password to find the message. Then, we decompile TBFC_APP with ILSpy. Now we can see some of the source codes behind the application. We can find all sorts of information and even passwords. After we found santa's password, we can now decode using cyberchef. Then we can get the flag by successfully login into the TBFC_APP.

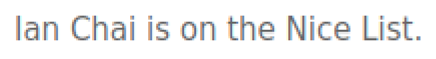
Day 19: [Web Exploitation] The Naughty or Nice List

Tools used: THM Attackbox, Firefox

Solution/walkthrough:

Question 1

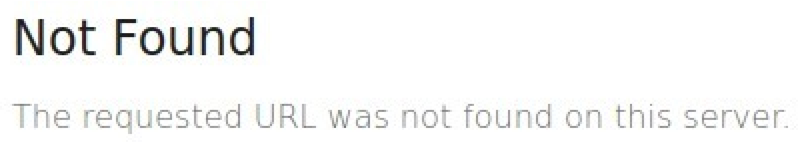
Which list is this person on?



Ian Chai is on the Nice List.

Question 2

What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"? - Not Found. The requested URL was not found on this server.

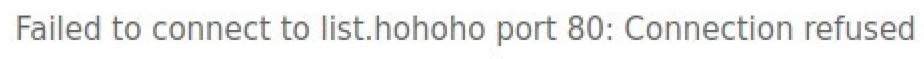


Not Found

The requested URL was not found on this server.

Question 3

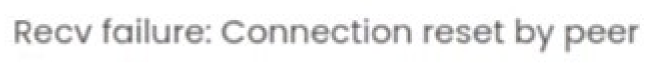
What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"? -Failed to connect to list.hohoho port 80: Connection refused



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

Question 4

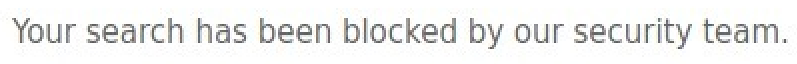
What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"? -Recv failure: Connection reset by peer



Recv failure: Connection reset by peer

Question 5

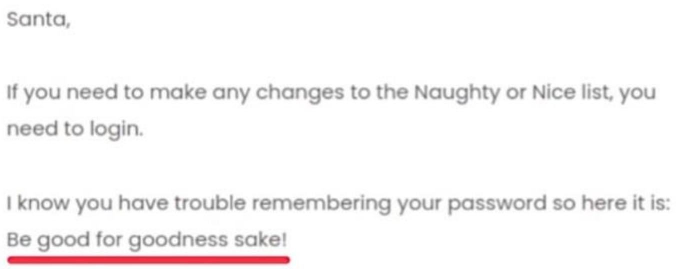
What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"? -Your search has been blocked by our security team.



Your search has been blocked by our security team.

Question 6

What is Santa's password? -Be good for goodness sake!



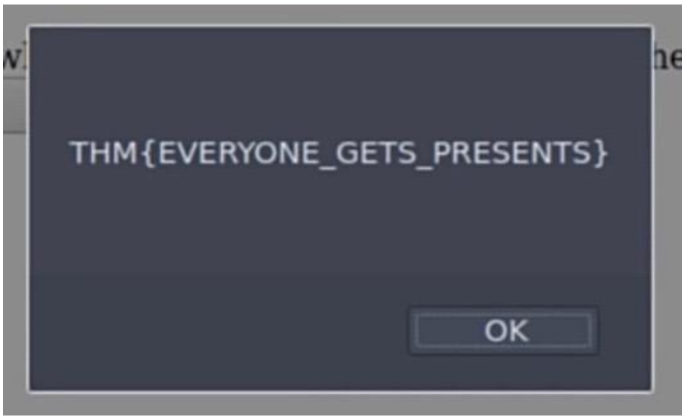
Santa,

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!

Question 7

What is the challenge flag? -THM{EVERYONE_GETS_PRESENTS}



THM{EVERYONE_GETS_PRESENTS}

Thought Process/ Methodology:

We start by entering the given IP Address in the search bar which will lead us to access Santa’s Naughty List or Nice List where we can enter names to check whether they are in Santa’s Naughty List or Nice List. Then, we replace the URL with the given replacements which will lead us to different pages. Next, to find out Santa’s password, we start by modifying the URL with `localtest.me` which will lead us to a message left by Santas’s Elf that contains Santa’s password. Lastly, we are able to login to Admin which will display the challenge flag.

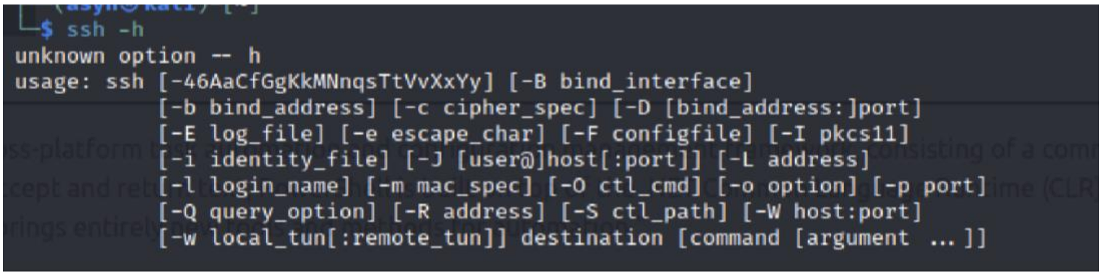
Day 20: [Blue Teaming] PowershELIF to the rescue

Tools used: THM AttackBox, PowerShell, SSH

Solution/walkthrough:

Question 1

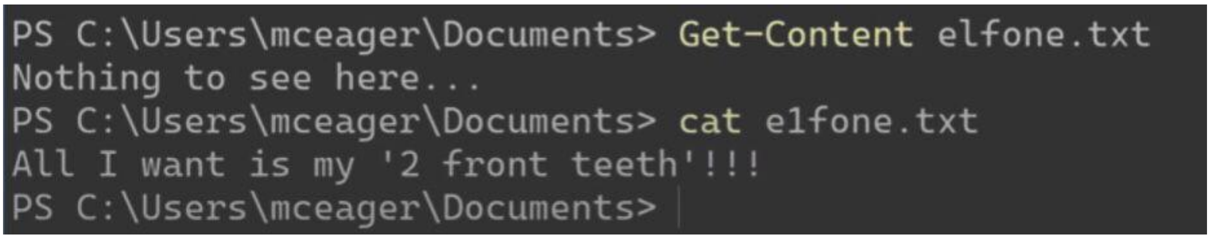
Check the ssh manual. What does the parameter -l do? - login name



```
└─$ ssh -h
unknown option -- h
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-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 [argument ...]]
```

Question 2

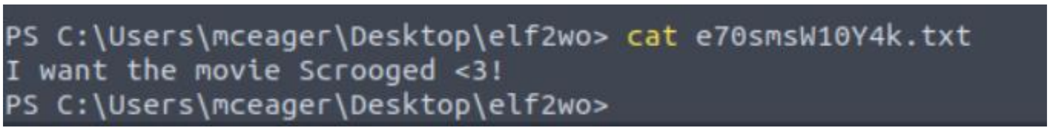
Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want? -2 front teeth



```
PS C:\Users\mceager\Documents> Get-Content elfone.txt
Nothing to see here...
PS C:\Users\mceager\Documents> cat e1fone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\Documents>
```

Question 3

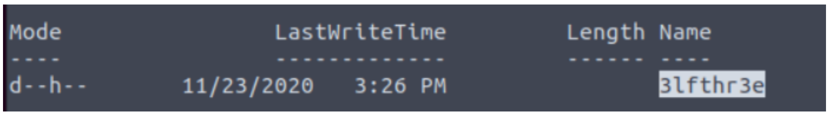
Search on the desktop for a hidden folder that contains the file for Elf 2. Read the contents of this file. What is the name of that movie that Elf 2 wants? -Scrooged



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

Question 4

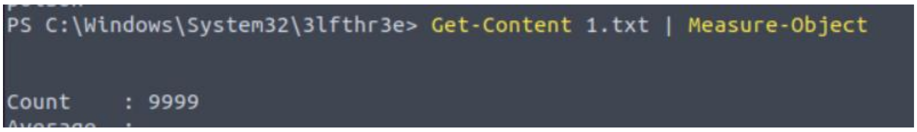
Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder? (This command will take a while) - 3lfthr3e



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

Question 5

How many words does the first file contain? -9999

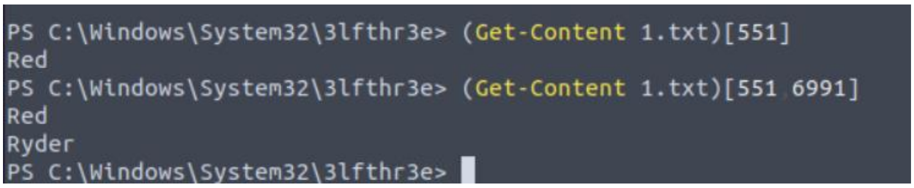


```
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Measure-Object


Count    : 9999
```

Question 6

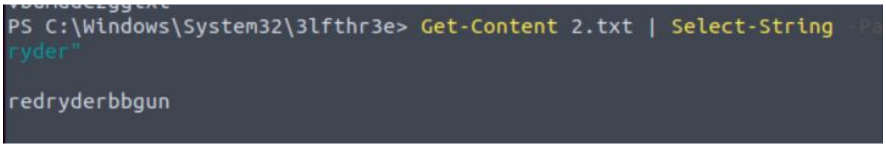
What 2 words are at index 551 and 6991 in the first file? -Red Ryder



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

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) -red ryder bbgun



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

redryderbbgun
```

Thought Process/ Methodology:

First, we launched PowerShell and navigate to the Documents folder.We use powershell command to access the 'Documents' directory. After we done navigate into the directory, we can see a list of the directory contents with `Get-ChildItem` but the result of this command doesn't require the results we want. Then, we add additional flags; `Get-ChildItem -Hidden -File` to specifies the command. Then, we use command `Get-Content` to see the content of the file and found what elf1 want. Next, we navigate into Desktop directory where it listed all the contents inside it using powershell command; `Get-ChildItem -Hidden -Directory` and navigate into 'elf2wo' directory. Next, we're looking for a a hidden folder that contains files for Elf 3 using command `Get-ChildItem -Hidden -Filter '*3*'`

We navigate into th efile we found earlier and list the file inside. Using `Measure-Object` cmdlet with flag `-Word` to count all the words. Then we use the common that has been provided `(Get-Content .\1.txt)[551, 6991]` to find the 2 words in the first file.For the last question, we use command `Select-String <path/filename> -Pattern 'redryder'` to get the full answer.