PSP0201

Week 5

Writeup

Group Name: WakuWaku

Members

ID	Name	Role
1211103115	Azri Syahmi Bin Azhar	Leader
1211103233	Muhammad Amir Adib Bin Mohd Aminuddin	Member
1211103419	Muhammad Afif Jazimin Bin Idris	Member
1211103284	Miteshwara Rao A/L Subramaniam	Member

Day 16: Scripting – Help! Where is Santa?

Tools used: Kali Linux, Firefox, Terminal

Solution/walkthrough:

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

Answer: 80

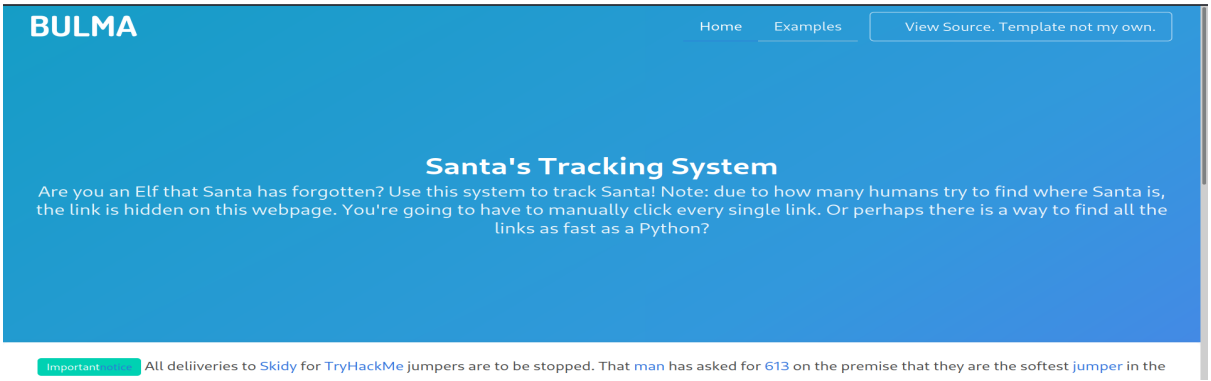
Open the terminal and then just run the command 'nmap -v {machine_ip}', the type of ports will then be displayed.

```
┌──(1211103233㉿kali)-[~]
└─$ nmap -v 10.10.90.84
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-15 05:00 EDT
Initiating Ping Scan at 05:00
Scanning 10.10.90.84 [2 ports]
Completed Ping Scan at 05:00, 0.21s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:00
Completed Parallel DNS resolution of 1 host. at 05:00, 0.01s elapsed
Initiating Connect Scan at 05:00
Scanning 10.10.90.84 [1000 ports]
Discovered open port 80/tcp on 10.10.90.84
Discovered open port 22/tcp on 10.10.90.84
Increasing send delay for 10.10.90.84 from 0 to 5 due to max_successful_tryno increase to 4
Increasing send delay for 10.10.90.84 from 5 to 10 due to max_successful_tryno increase to 5
Increasing send delay for 10.10.90.84 from 10 to 20 due to max_successful_tryno increase to 6
Increasing send delay for 10.10.90.84 from 20 to 40 due to max_successful_tryno increase to 7
Completed Connect Scan at 05:01, 29.71s elapsed (1000 total ports)
Nmap scan report for 10.10.90.84
Host is up (0.21s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 30.05 seconds
```

Question 2: What templates are being used?

Answer: BULMA

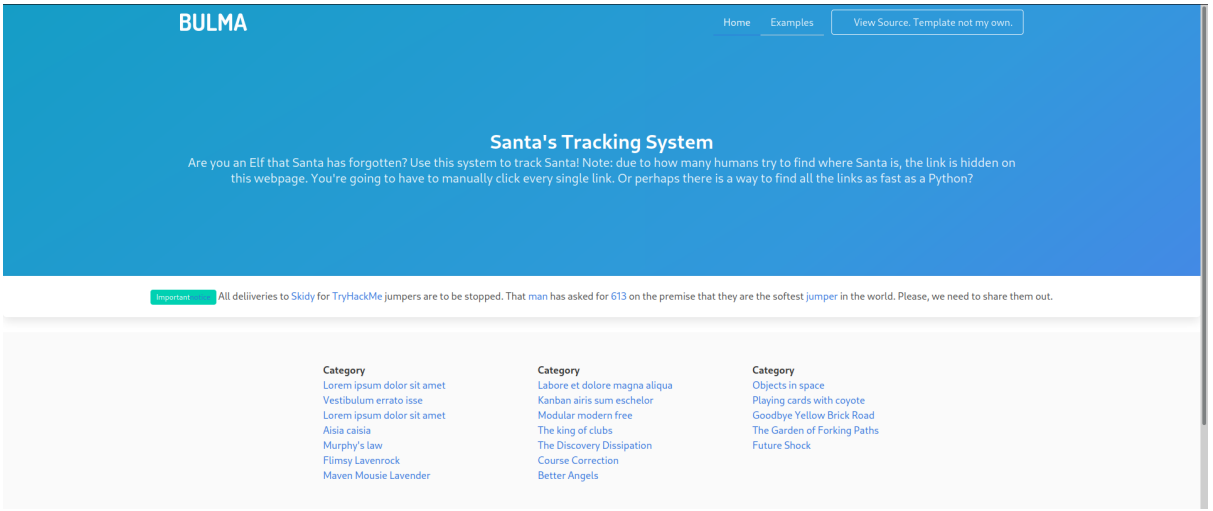
First, go to 'machine_ip:port/static/index.html'. To know what kind of template is being used, just simply look at the top left of the page.



Question 3: Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)

Answer: /api/

Firstly, I tried hovering over each link(blue text) to see the URL it's directing.

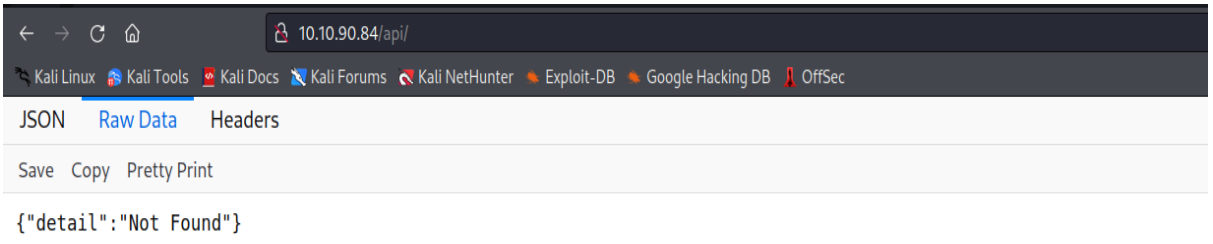


After that, I found this URL in the 'Modular modern free' text. Thus, the answer would be '/api/'

Question 4: Go the API endpoint. What is the Raw Data returned if no parameters are entered?

Answer: {"detail":"Not Found"}

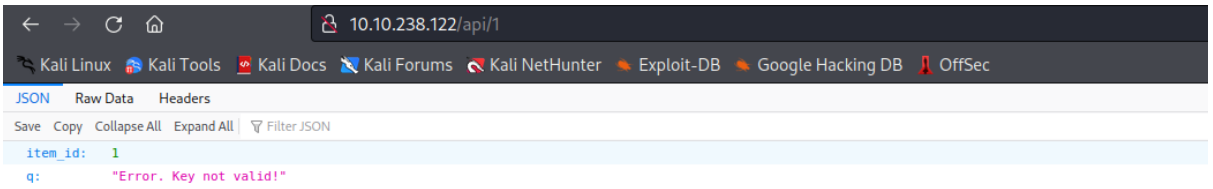
Just simply type in the value of each variable of 'machine_ip/api/api_key' from the previous question, but in this question, it says don't enter the parameter which refers to the 'api_key'. So in this case, we just have to type in 'machine_ip/api/' as there is no parameter. Then insert it in the URL box in your browser. The content of the redirected page will be the answer.



Question 5: Where is Santa right now? (Tick all correct answers.)

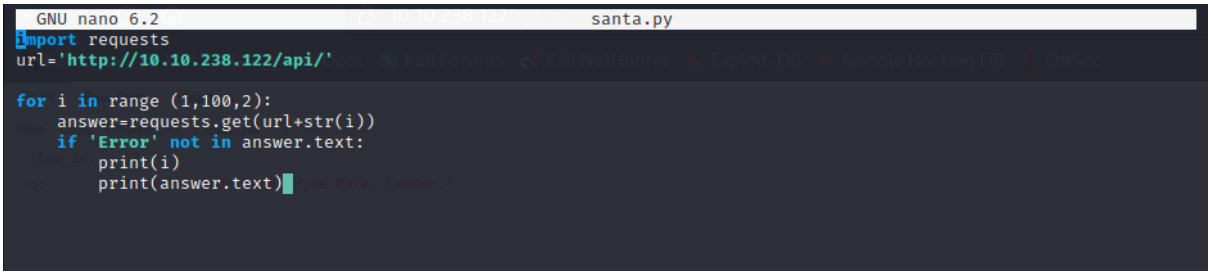
Answer: Winter Wonderland, Hyde Park, London

First, let's understand what 'machine_ip/api/api_key' URL will actually show if it actually has a parameter. It will show you as below, which 'item_id' refers to api_key (parameter) that we inserted which is 1 and q is some kind of message. From this, we can assume that q will show us Santa's location if we got the parameter(api_key) correct.

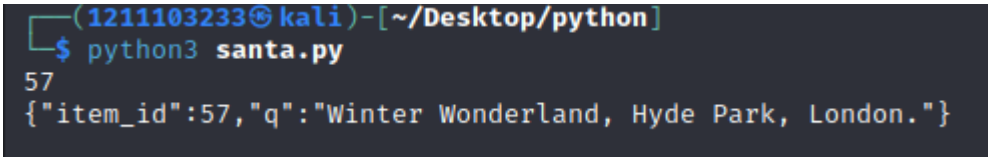


Then, I enter the Desktop/python directory, create a non-existing file and named it as 'santa.py' and enter the file.

After entering the 'santa.py', I typed in a python command as below and save it



Then, I tried running the python file and the results are shown as below which gives both the api_key(value) and the q message or location of Santa.

- 

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.

Answer: 57

The process to get the answer to this question is the same as question 6.

```
┌──(1211103233㉿kali)-[~/Desktop/python]
└─$ python3 santa.py
57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
```

Thought Process/Methodology:

For question 1, we have to use the 'nmap -v {machine_ip}' command in the terminal to identify the port for a certain host. The reason behind this is that with nmap, server administrators can easily identify hosts and services, look for security flaws, and check for open ports. The "-v" flag will provide additional information about the completed scan of the targeted host.

For question 2, after obtaining the port, add the port in the given URL which is 'machine_ip:port/static/index.html' and search it in the URL box. You should be redirected to the page and to know what kind of template is being used, just simply look at the top left of the page.

For question 3, I tried hovering each blue text(links) on that page which its URL appears at the bottom left corner until I found a URL showing 'machine_ip/api/api_key' at the text 'Modular modern free'.

For question 4, Just simply type in the value of each variable of 'machine_ip/api/api_key' from the previous question, but in this question, it says don't enter the parameter which refers to the 'api_key'. So in this case, we just have to type in 'machine_ip/api/' as there is no parameter. Then insert it in the URL box in your browser. The content of the redirected page will be the answer.

Questions 5 and 6 are related to each other and the answer for both questions would appear simultaneously after undergoing only one process. First, let's understand what 'machine_ip/api/api_key' URL will actually show if it actually has a parameter. It will show you as below, which 'item_id' refers to api_key(parameter) that we inserted which is 1 and q is some kind of message. From this, we can assume that q will show us Santa's location if we got the parameter(api_key) correct. Then I enter the 'Desktop/python' directory using the command 'cd' which is a shell command that is used to switch the current working directory. After that, I created an empty python file while in that directory using the 'touch' command which is to create a file without any contents in it. Then, I opened up the santa.py file using the nano command which its function is as so. After that, I filled up the santa.py file using the 'nano' command. The content of it is python commands like below.

First, I import the requests module as it allows to send HTTP requests using Python. The HTTP request returns a Response Object with all the response data (content, encoding, status, etc). Santa's location information is in one of the api_key between 1 and 100, and the hint it gave api_key is an odd number. So I use the 'for' loop in the 1 and 100 range with 2 as its step to obtain an odd number and ultimately find the correct api_key. Then, I use the requests function to send the HTTP request to my targetted host and added it with the str(i) so that it can iterate through all the possibilities to find the api_key value. As the wrong api_key will give the message 'Error', so I put in the command `if 'Error' not in answer.text:` as I wanted the correct output which it doesn't contain 'Error' in it. Then, I print 'answer.text'. The answer will then be displayed with both the api_key value and Santa's location.

Day 17: Reverse Engineering – ReverseELFneering

Tools used: Attackbox, terminal

Solution/walkthrough:

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

Answer: Byte-1, Word-2, Double Word-4, Quad-8, Single Precision-4, Double Precision-8

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?

Answer: aa

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`

Question 3: What is the command to set a breakpoint in radare2?

Answer: 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 `db 0x00400b55` To ensure the breakpoint is set, we run the `pdf @main` command again and see a little **b** next to the instruction we want to stop at.

Question 4: What is the command to execute the program until we hit a breakpoint?

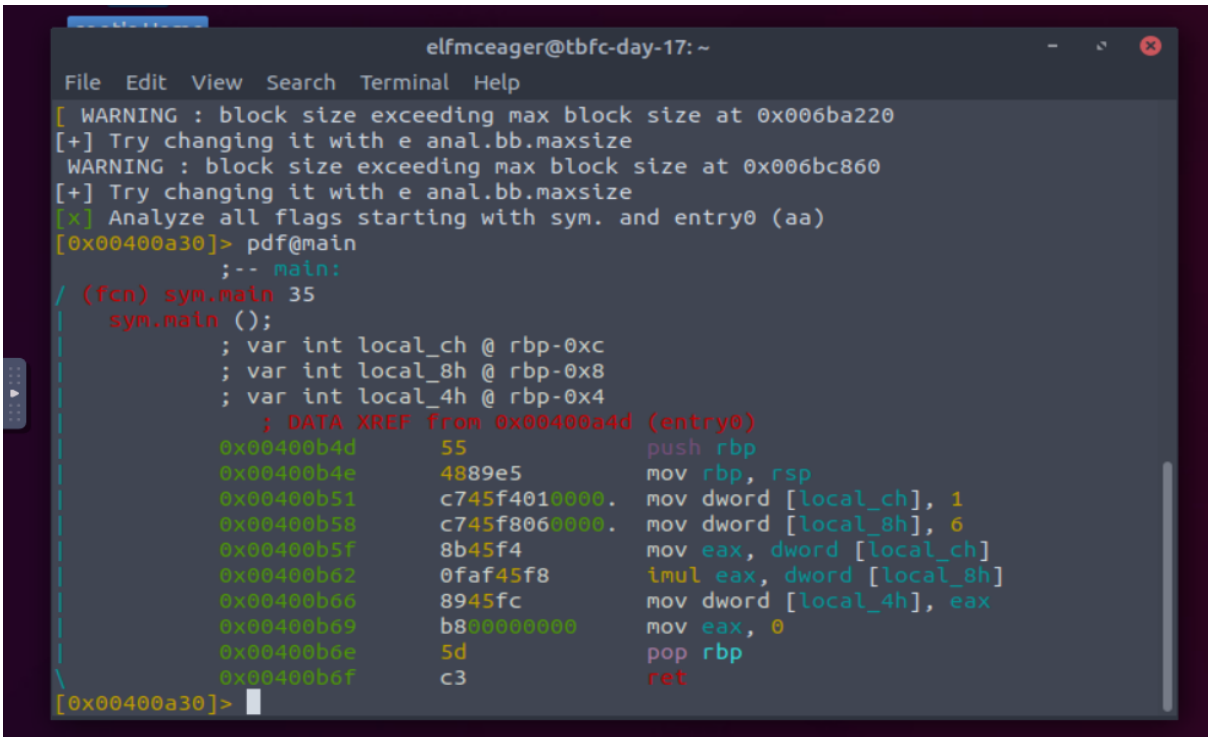
Answer: dc

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

Question 5: What is the value of local_ch when its corresponding movl instruction is called (first if multiple)?

Answer: 1

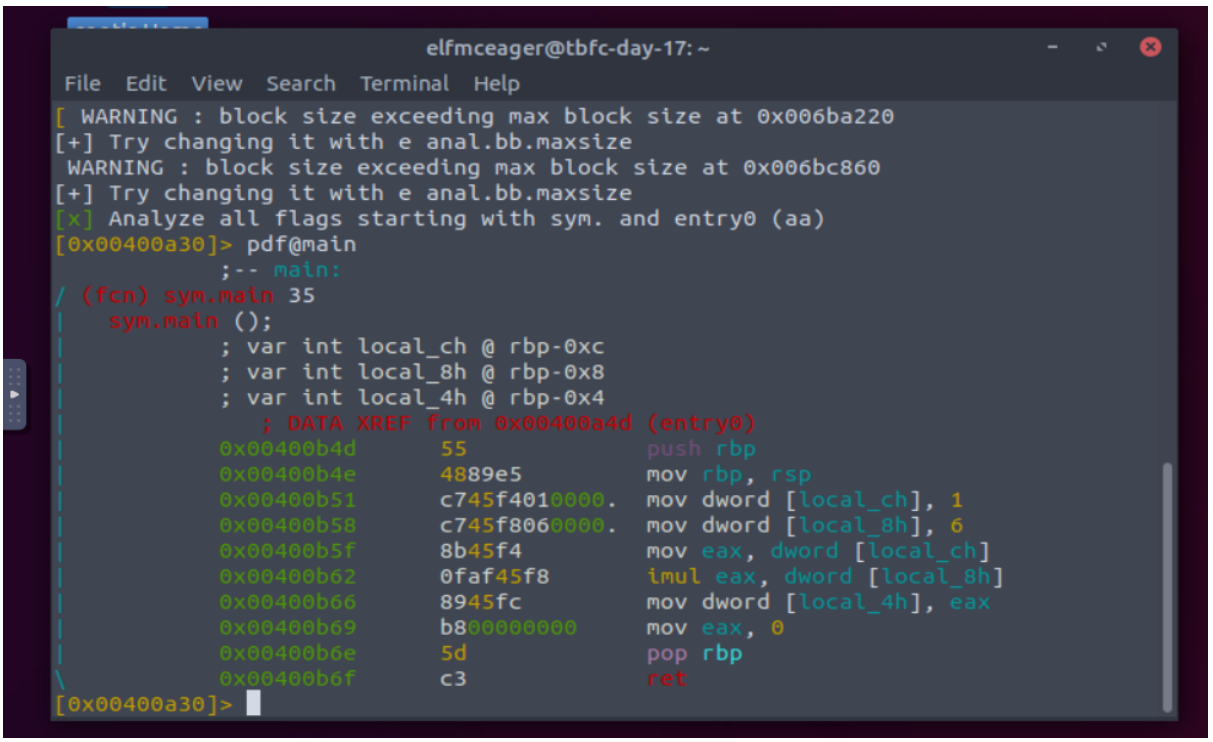
Type "r2 -d ./challenge1" after logging in. Then, use the command "aa". Then, use the command "pdf@main". We can see that the first value of local_ch when its corresponding movl instruction is called is 1.



Question 6: What is the value of eax when the imull instruction is called?*

Answer: 6

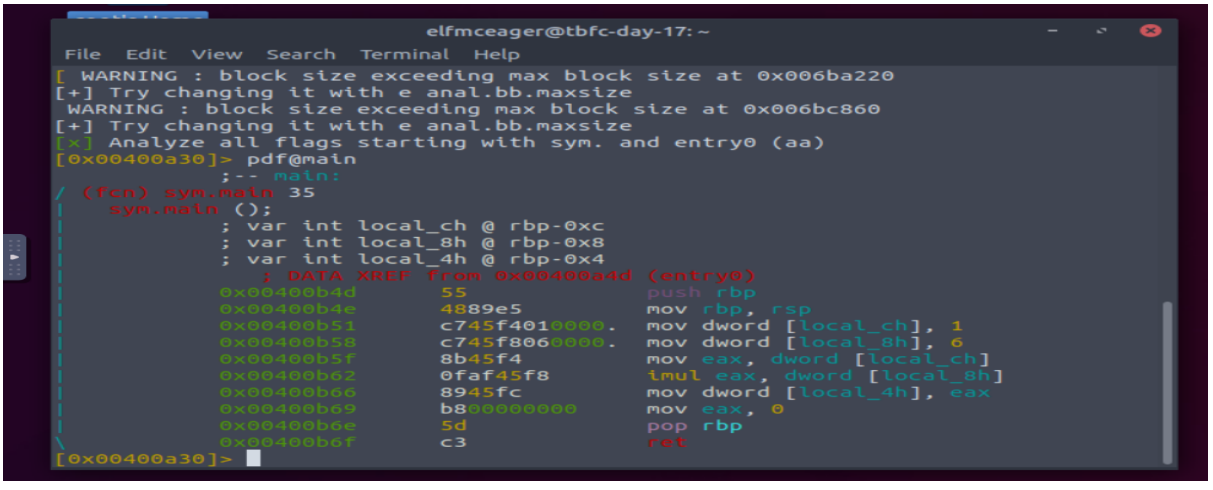
Type "r2 -d ./challenge1" after logging in. Then, use the command "aa". Then, use the command "pdf@main". It shows that the value is 6.



Question 7: What is the value of local_4h before eax is set to 0?

Answer: 6

Type "r2 -d ./challenge1" after logging in. Then, use command "aa". Then, use the command "pdf@main". We can see that before eax is set to 0, it is 6.



Thought Process/Methodology:

Open the terminal and log into the instance by using the command "ssh elfmceager@10.10.21.185" and enter the password. When we use the command "ls" to see what file is there, there will be "challenge1 file1". Use the command "-lsa" and then run the file1 by using the command "./file1". Next up, run the command "r2 -d ./file1". It will open the binary in debugging mode. We can analyze the program by typing "aa".We have to wait for about 10 minutes for the program to be analyzed. Then, we can use command "afl" so that we can get a function list. Find the function for "main", copy the function and paste it onto the terminal. We can examine the assembly code at main by running the command "pdf @main". First of all, we want to analyze the 4th instruction. We want to analyze the program while it runs, so we have to use breakpoint so that breakpoint will specify where the program should stop executing. To set the breakpoint at instruction 4, use the command "db 0x00400b55" (the function of instruction 4). To see whether the breakpoint is set or not, we can use the command "pdf @main" again and we'll see there's a little b next to the instruction we want to stop at. Next, run the program using the command "dc". The mov instruction is used to transfer values. It transfers the value 4 into the local_ch variable. To view the content, we can use the command "px @rbp-0xc" (the memory-address can be obtained from the first few lines of pdf@main). Looks like the variable currently doesn't have anything stored in it because it's just 0000. Use command "ds" so that it steps the execution to the next instruction. Use the command "px @rbp-0xc" again. Now we can see the first 2 bytes have the value 4. If we do the same process for the next instruction, we can see that the variable local_8h has a value of 5. Next, go to the instruction "movl local_8h, %eax" by using the command "ds". When we have reached the instruction, use the command "dr". We can see the content of eax.

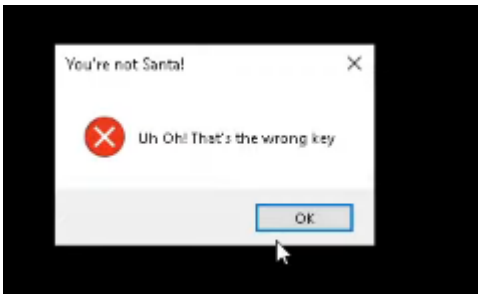
Day 18: Reverse Engineering – The Bits of Christmas

Tools used: attackbox, firefox, ILSPY

Solution/walkthrough:

Question 1: What is the message that shows up if you enter the wrong password for TBFC_APP?

Answer: Uh Oh! That's the wrong key



open the tbfc app and enter a random password which has to be wrong and this message will be displayed

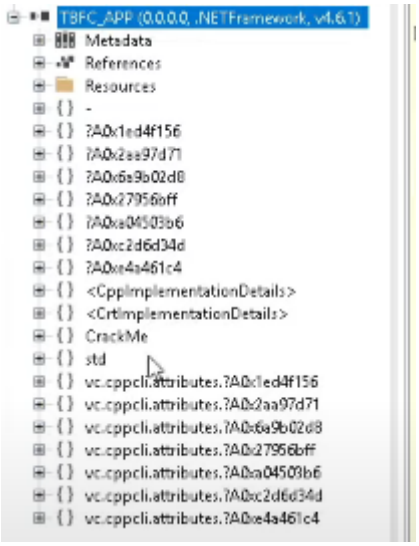
Question 2:What does TBFC stand for?

Answer: The Best Festival Company

when we open the app we can see the company name at the bottom left of the app dashboard

Question 3: Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?

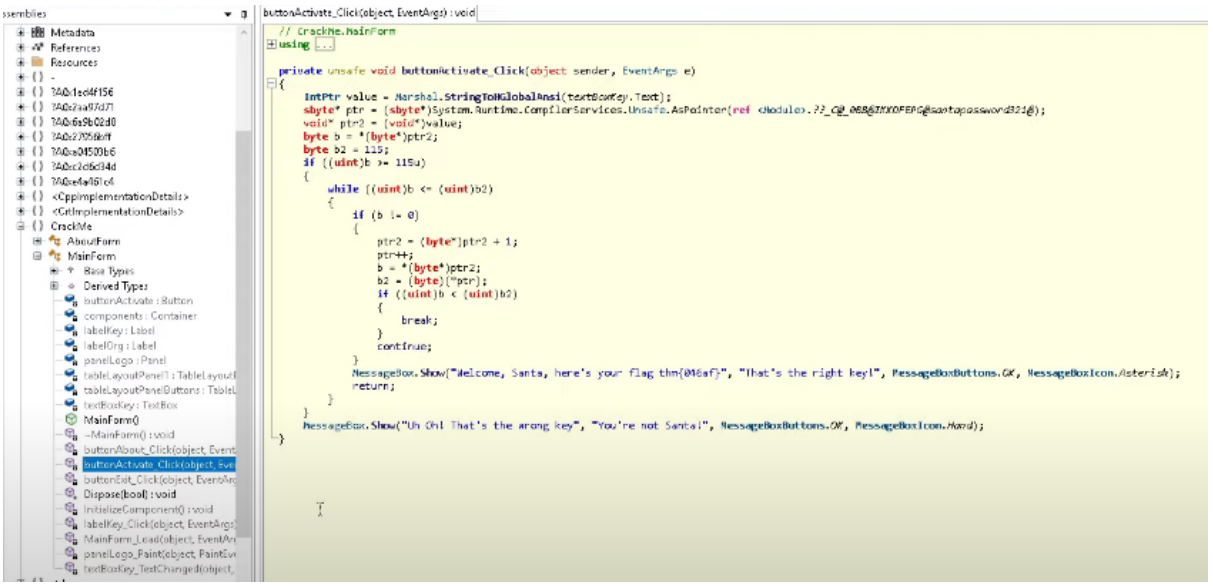
Answer: CrackMe



most of the files are almost named in the same format except for the file CrackMe

Question 4: Within the module, there are two forms. Which contains the information we are looking for?

Answer: MainForm



after going through both forms we can see that MainForm has the actual details we need like santa's password and thm flag

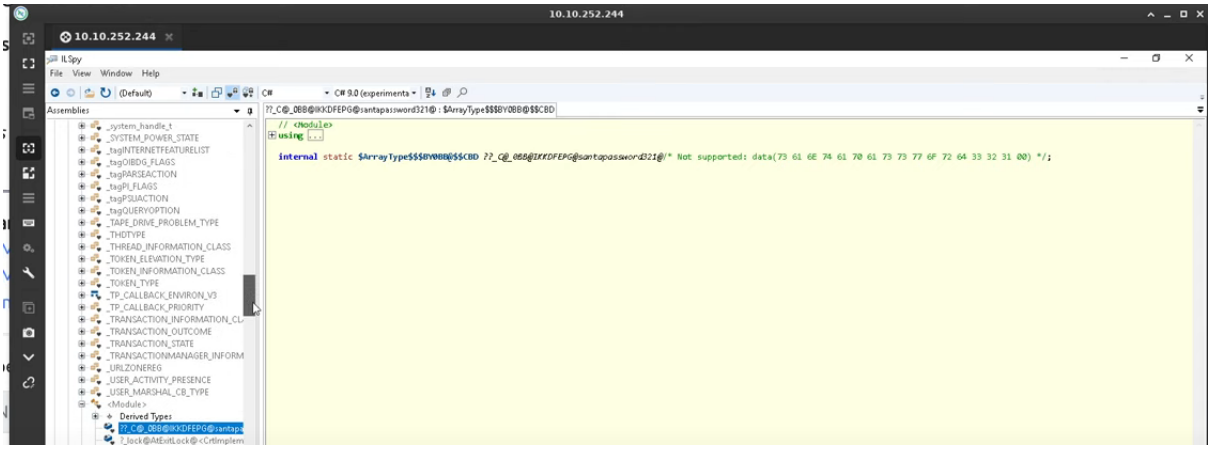
Question 5: Which method within the form from Q4 will contain the information we are seeking?

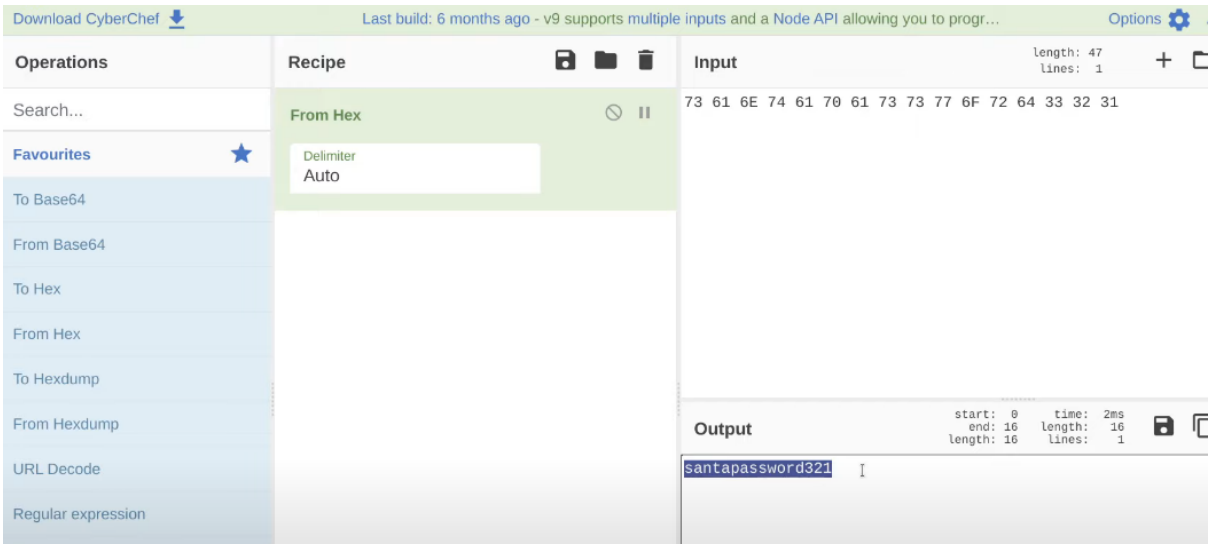
Answer: buttonActivate_Click

buttonActivate_Click has the thm flag

Question 6:What is Santa's password?

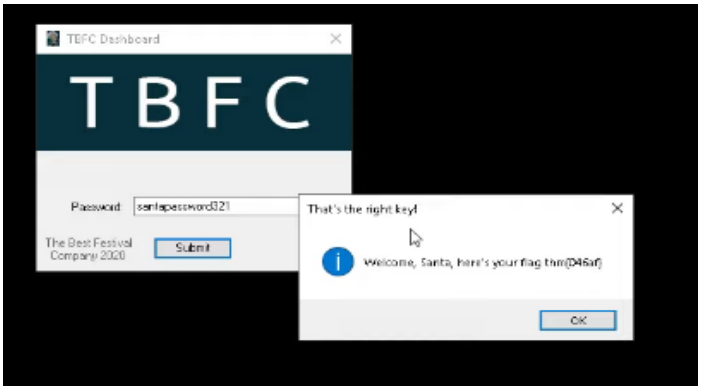
Answer: santapassword321





we can see in that file the row of numbers is hexadecimal so we used cyberchef to find the real password

Question 7:Now that you've retrieved this password, try to login...What is the flag?
Answer: thm{046af}



when we tried the password we got from cyberchef we managed to log in and get a flag

Thought Process/Methodology:

Firstly we open remina we logged in with the username and password that was given to us on tryhackme.After that we opened ilspy then we opened the file tfc_app on ilspy and we began browsing through the files and the CrackMe stood out from the others and we began exploring it had some information we needed from there we browsed through MainFormand there we found the password in hexadecimal form and the thm flag

Day 19: Web Exploitation – The Naughty or Nice List

Tools used: attackbox, firefox, tbfc-app

Solution/walkthrough:

Question 1: Which list is this person on?

Answer: Kanes - Naughty

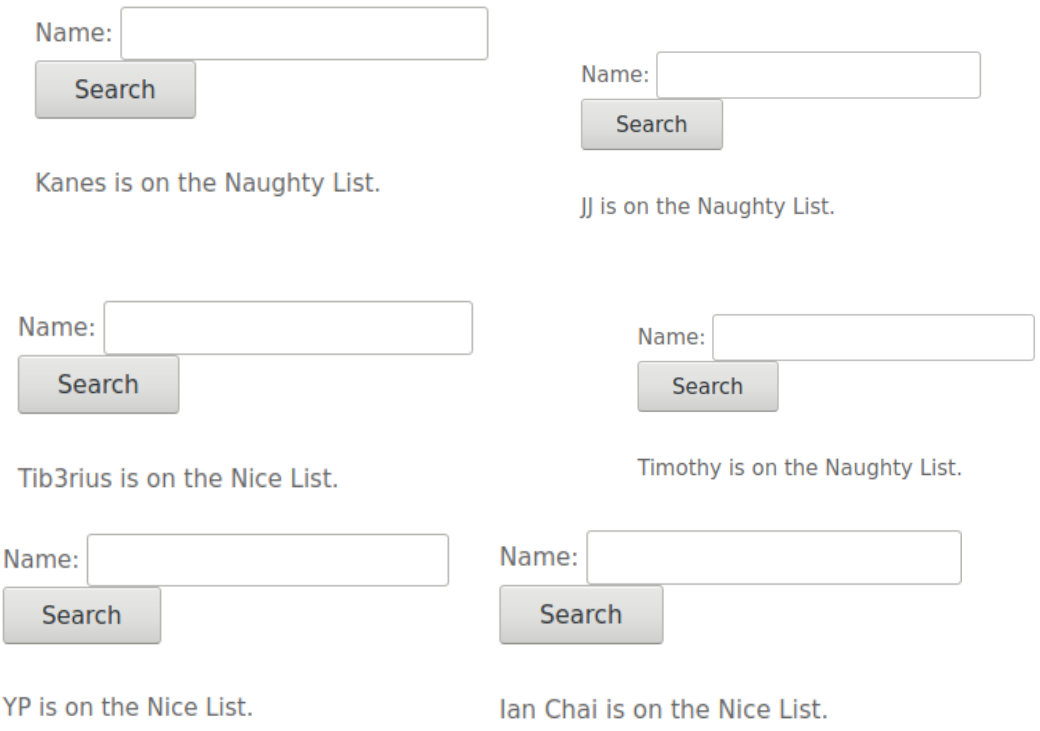
Tib3rius - Nice

Timothy - Naughty

Ian Chai - Nice

JJ - Naughty

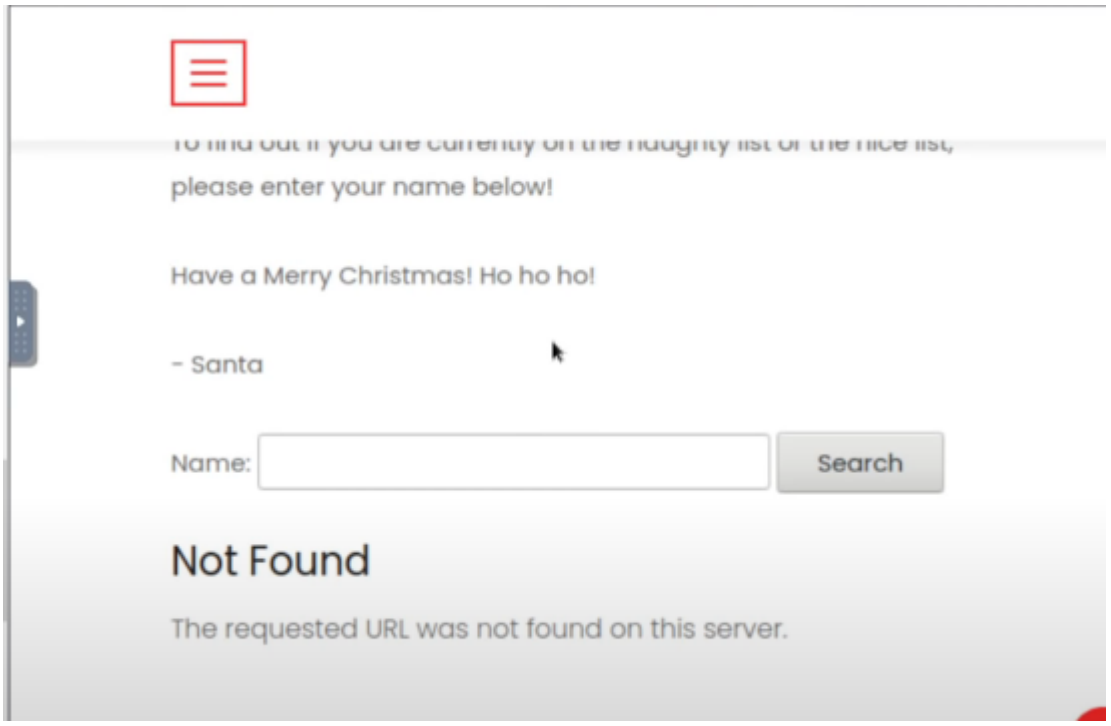
YP - Nice



when we type in the IP address on the attackbox firefox we can go to Santa's nice and naughty list we type in all the names and we will get the results

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

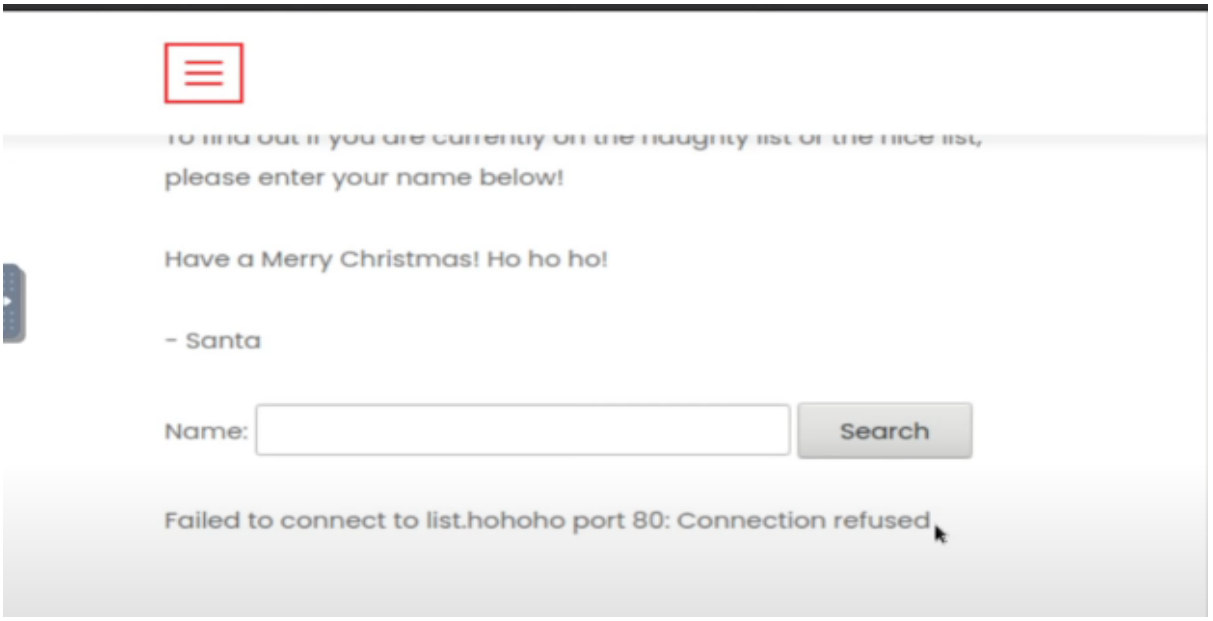
Answer: The requested URL was not found on this server.



when we changed the URL and removed some parts of it we go this message

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

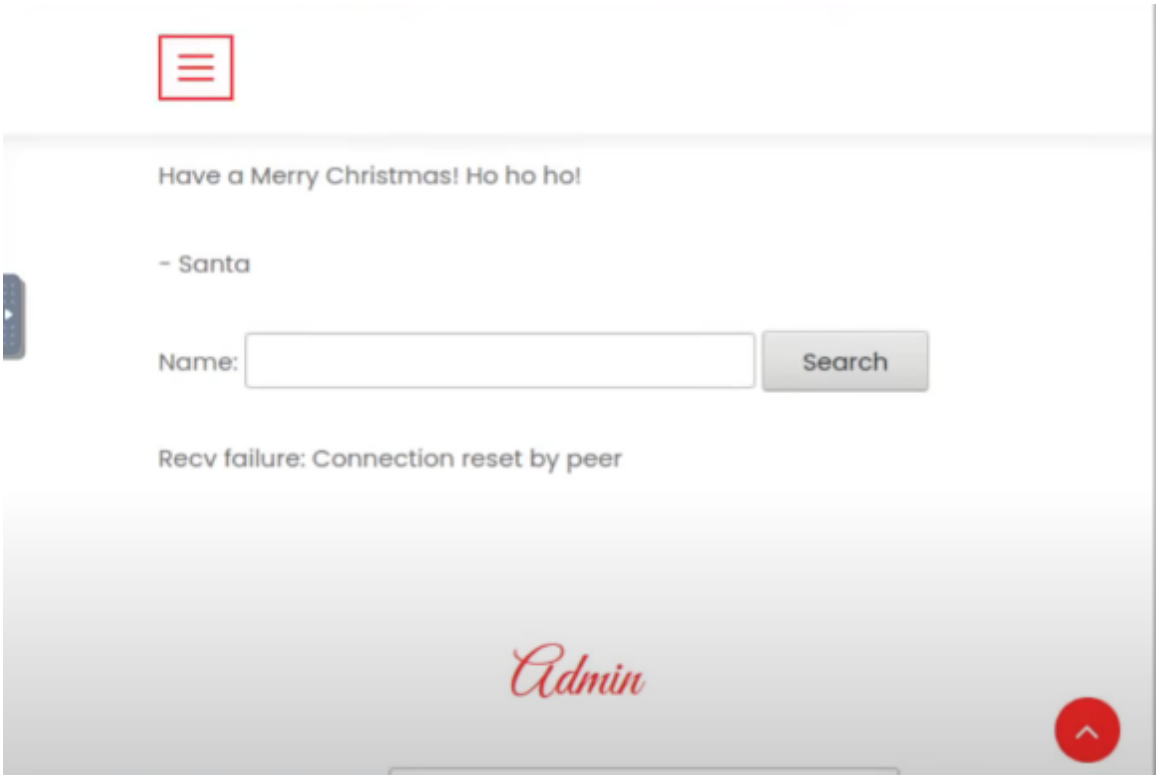
Answer: Failed to connect to list.hohoho port 80: Connection refused



when we try to change the port number form 8080 to 80 we failed to connect to that port

Question 4: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"?

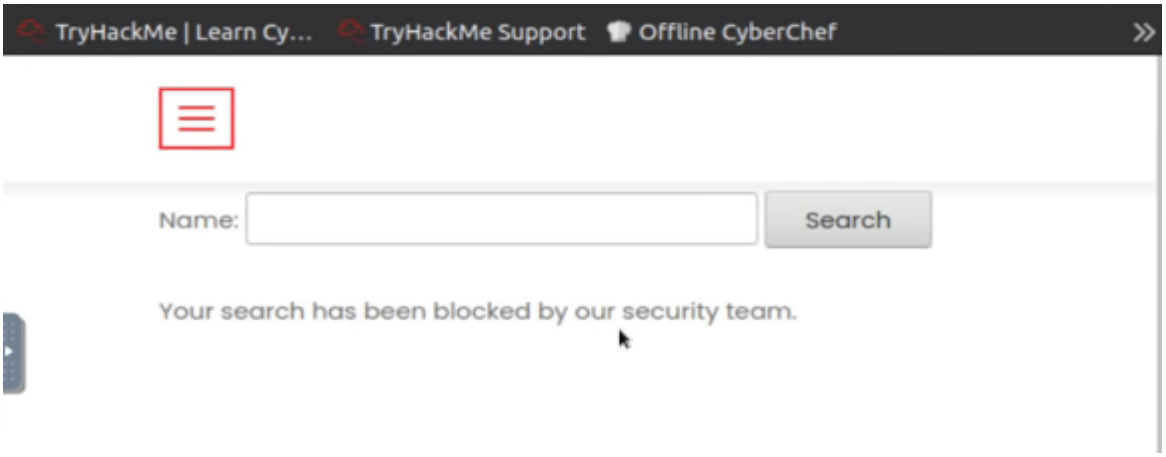
Answer: Recv failure: Connection reset by peer



when we changed it to port 22 we got another error message

Question 5: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?

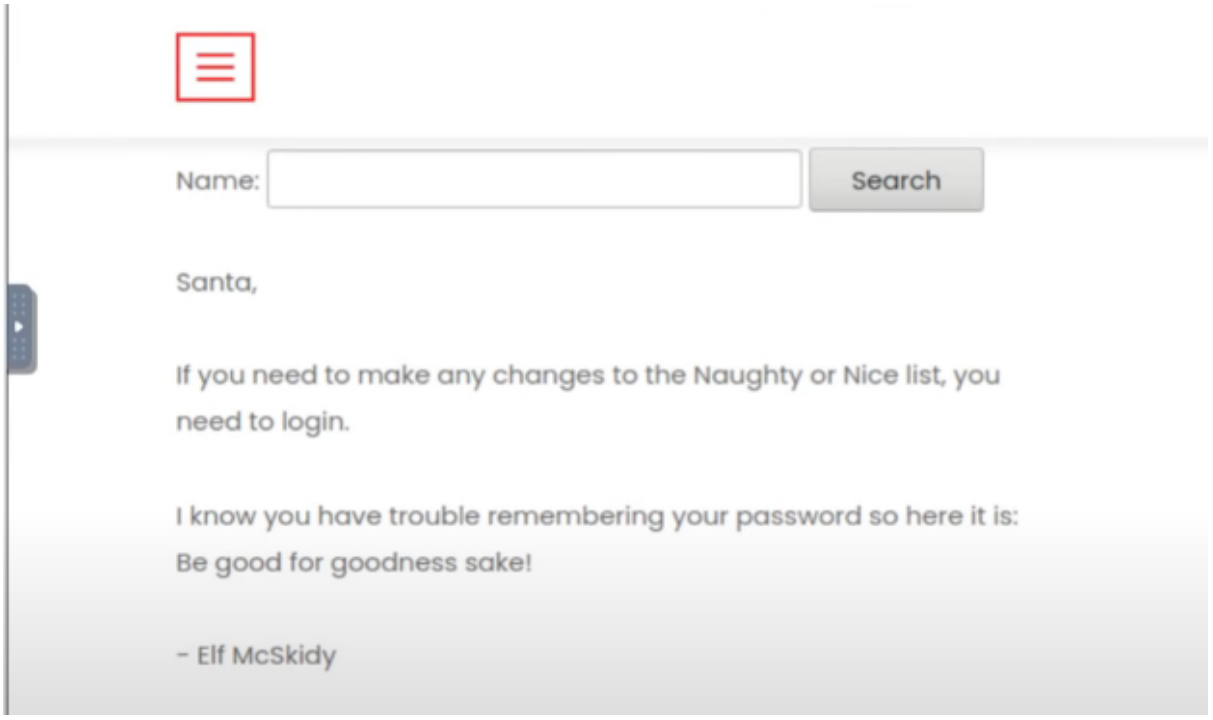
Answer: Your search has been blocked by our security team



when we removed list.hohoho from the URL. It instantly got blocked by the security

Question 6: What is Santa's password?

Answer: Be good for goodness sake!



when we got the right URL we found out Santa's password

Question 7:What is the challenge flag?

Answer: THM{EVERYONE_GETS_PRESENTS}

when we logged in to tbfc_app using santa's username and password we got this flag

Thought Process/Methodology:

Firstly we got to santa's naughty and nice list and the we tried different URL's to figure santa's password but it many got denied until we tried `http://MACHINE_IP/?proxy=http%3A%2F%2Flist.hohoho.localtest.me` which was the right one and we got santa's password with that URL with that password we headed to the tbfc_app to identify the flag with the right username and password we go the flag.

Day 20: Blue Teaming – PowershELlF to the rescue

Tools used: Attackbox, Terminal

Solution/walkthrough:

Question 1: Check the ssh manual. What does the parameter -l do?

Answer: login name

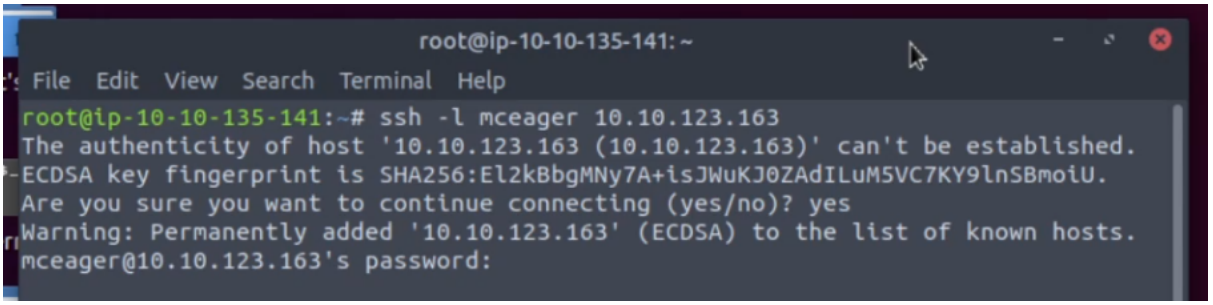
Open the terminal and use the man command to open the ssh manual.

```
-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.
```

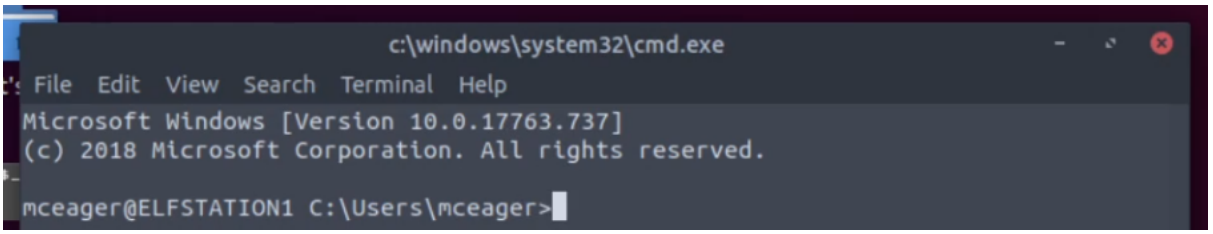
Question 2: Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

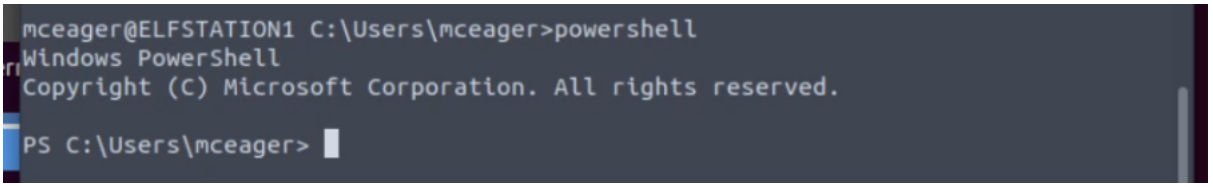
Answer: 2 front teeth

At the terminal, connect to the remote machine using SSH. Use the command `ssh -l mceager 10.10.123.163` and enter the password "r0ckStar!" as given by TryHackMe.



Once we successfully log in, launch PowerShell.





The first hidden elf file is within the Documents folder. Navigate to the Documents folder using the command `Set-Location .\Documents\` and search for the hidden file using `Get-ChildItem -Hidden`

```
PS C:\Users\mceager> Set-Location .\Documents\
PS C:\Users\mceager\Documents> Get-ChildItem -Hidden


    Directory: C:\Users\mceager\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--hsl        12/7/2020  10:28 AM                My Music
d--hsl        12/7/2020  10:28 AM                My Pictures
d--hsl        12/7/2020  10:28 AM                My Videos
-a-hs-        12/7/2020  10:29 AM            402 desktop.ini
-arh--       11/18/2020   5:05 PM             35 e1fone.txt
```

There's a file named e1fone.txt. Use the command `Get-Content -Path e1fone.txt` to read the content. Now, we have got what Elf 1 wants: 2 front teeth.

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

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?

Answer: Scrooged

Next, we need to find another file in a hidden folder on the Desktop. Navigate to the Desktop using `Set-Location` cmdlet and search for the hidden folder using `Get-ChildItem -Hidden`.

```
PS C:\Users\mceager\Documents> Set-Location ..\Desktop\.
PS C:\Users\mceager\Desktop> Get-ChildItem -Hidden


    Directory: C:\Users\mceager\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--        12/7/2020  11:26 AM                elf2wo
-a-hs-        12/7/2020  10:29 AM            282 desktop.ini
```

Now, we've got the hidden folder "elf2wo". Navigate to the folder. Using the `Get-ChildItem` cmdlet, we got a text file "e70smsW10Y4k.txt". Use `Get-Content e70smsW10Y4k.txt` to read the content. The name of the movie is "Scrooged".

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

Question 4: Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder?

Answer: 3lfthr3e

Next, navigate to the Windows directory. Using the `Get-ChildItem` cmdlet, we'll see there are many files and directories.

```
File  Edit  View  Search  Terminal  Help
d-----         7/7/2022   4:19 PM                Temp
d-----         9/6/2019   5:31 PM                TextInput
d-----        9/15/2018  12:19 AM                tracing
d-----        9/15/2018  12:19 AM                twain_32
d-----        9/15/2018  12:19 AM                Vss
d-----        9/15/2018  12:19 AM                WaaS
d-----        9/15/2018  12:19 AM                Web
d-----        12/7/2020  11:16 AM                WinSxS
-a----        9/15/2018  12:12 AM          78848 bfsvc.exe
-a--s-         7/7/2022   4:09 PM          67584 bootstat.dat
-a----         9/6/2019   5:28 PM         232960 DfsrAdmin.exe
-a----         9/6/2019   5:30 PM           1315 DfsrAdmin.exe.config
-a----        11/23/2020   1:42 PM           1947 DtcInstall.log
-a----         9/6/2019   5:28 PM        4353016 explorer.exe
-a----         9/6/2019   5:29 PM        1071616 HelpPane.exe
-a----        9/15/2018  12:12 AM          18432 hh.exe
-a----        11/23/2020   1:42 PM           1378 lsasetup.log
-a----        9/15/2018  12:12 AM          43131 mib.bin
-a----         9/6/2019   5:29 PM         254464 notepad.exe
-a----         7/7/2022   4:06 PM          26238 PFRO.log
-a----        11/26/2020  11:32 AM          87616 PSSDNSVC.EXE
-a----         9/6/2019   5:29 PM         358400 regedit.exe
-a----        9/15/2018  12:13 AM          30931 ServerStandard.xml
```

So, we'll specify the folder we want using the command `Get-ChildItem -Directory -Hidden -Filter "*3*" -ErrorAction SilentlyContinue`. We'll get the folder "3lfthr3e" in the System32 directory.

```
PS C:\Windows> Get-ChildItem -Directory -Recurse -Hidden -Filter "*3*" -ErrorAction SilentlyContinue

    Directory: C:\Windows\System32

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

Question 5: How many words does the first file contain?

Answer: 9999

Navigate to the hidden folder and search for the hidden files for Elf 3 with the `Get-ChildItem` cmdlet. There are 2 files.

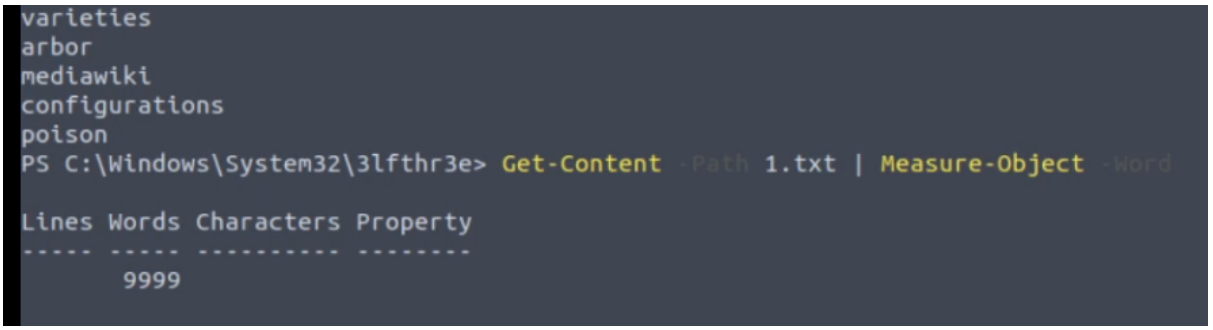
```
PS C:\Windows> Set-Location System32\3lfthr3e
PS C:\Windows\System32\3lfthr3e> Get-ChildItem
PS C:\Windows\System32\3lfthr3e> Get-ChildItem -Hidden


    Directory: C:\Windows\System32\3lfthr3e


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

If we try to read the content of the first file, it will show lines of words such as below:

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

```
File  Edit  View  Search  Terminal  Help
said
de
does
set
under
general
research
university
january
```

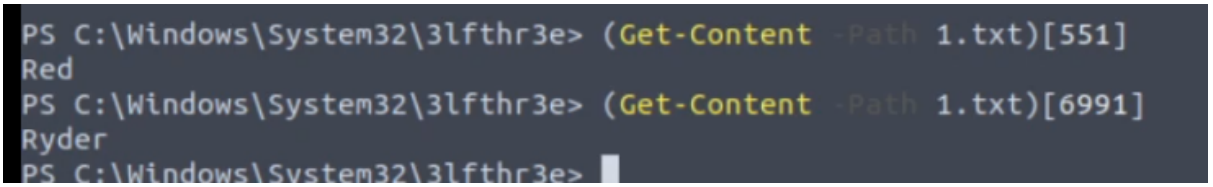
Use the `Get-Content` cmdlet and pipe the results to the `Measure-Object` cmdlet with the option `-Word` to get the number of words in “1.txt”.



Question 6: What 2 words are at index 551 and 6991 in the first file?

Answer: Red Ryder

To get the exact position of index 551 and 6991 in the first file, use the command `(Get-Content -Path 1.txt)[index]`.



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?

Answer: redryderbbgun

If we try to read the “2.txt” file, it shows endless lines of random characters such as below:

```
PS C:\Windows\System32\3lfthr3e> Get-Content 2.txt
```

```
File  Edit  View  Search  Terminal  Help
iphyhmutidftt
mroleufifksif
momcevfamyugf
tfrzwbouafxir
wtfuwjkaycokw
mmtmaxszexpob
tgtzhkaobuobi
uupqkbiwbqbvl
womifuthejclv
mprziudtonrgm
xukqalmtwzvdr
thyiydscjnjqc
suvndqzdfxjtz
rfyfxogqsdx
nbjkzgbwctx
kuvjufmkkvj
cpqekfzskklmm
```

We know that the real answer has the phrase “redryder” in it. So, we’ll use the command `Select-String -Path 2.txt -Pattern 'redryder'` to search for the exact string. Then, we now got the complete answer.

```
PS C:\Windows\System32\3lfthr3e> Select-String -Path 2.txt -Pattern 'redryder'

2.txt:558704:redryderbbgun
```

Thought Process/Methodology:

For this task, we need to remote into the workstation using PowerShell over SSH. To do this, we need to use the **ssh** command at the terminal. Use the **man** command to open the ssh manual to know how to log in as on the remote machine. Then, use the command **ssh -l** and complete the authentication based on what is given by TryHackMe. Once we successfully log in, launch PowerShell.

To search for the hidden file in the Documents folder, we must navigate to Documents. **Set-Location** cmdlet is used to change directories. Use the cmdlet to navigate there. The cmdlet **Get-ChildItem** functions the same as the **ls** command. It lists the contents of the current directory. Use the **Get-ChildItem** cmdlet with **-hidden** option to get only hidden items. We then saw a file named e1fone.txt. To read the contents of the file, use the **Get-Content** cmdlet. Now, we have got what Elf 1 wants: 2 front teeth.

Just now, we've searched for a hidden file. Now, we have to search for a hidden folder. It is located on the Desktop. Navigate there using **Set-Location** cmdlet and use **Get-ChildItem -hidden** to list all the hidden items. From that, we've got the hidden folder named 'elf2wo'. After we navigate to the hidden folder and listed all the contents, we got the text file 'e70smsW10Y4k.txt'. We've read the content of the file using the **Get-Content** cmdlet and got the name of the movie that Elf2 wanted; "Scrooged".

For question 4, navigate to the Windows directory to search for the hidden folder. Lists the items in the directory. Then we'll see many files and directories. It'll be time-consuming if we search each at a time. So, we'll use the **Get-Content** cmdlet with the option **-Directory -Hidden -Filter "*3*" -ErrorAction SilentlyContinue**. The option **-Directory -Hidden -Filter "*3*"** to specify the item we are searching is a hidden directory with "3" in its name. **-ErrorAction SilentlyContinue** is to make sure the command will be continuous even if it encounters an error. We'll get the folder "3lfthr3e" in the System32 directory.

Next, after we navigate to the folder and lists the content, we'll see text file "1.txt" and "2.txt". If we read the content of "1.txt", it'll be many lines of string. Counting it one by one will takes time. So, we'll use the **Get-Content** cmdlet and pipe the results to the **Measure-Object** cmdlet with the option **-Word**. This cmdlet will output the number of words contained within a file. The file contains 9999 words.

Question 6 is similar to the case of question 5. To count one by one until the index of 551 and 6991 will be time-consuming. So, we'll use the cmdlet **(Get-Content -Path 1.txt)[index]** to get the exact index of the file "1.txt". Index 551 outputs "Red" and index 6991 outputs "Ryder".

The answer to question 6 is just half of the phrase of what Elf3 wanted. The answer is in file “2.txt”. We know that the answer has the phrase “redryder” in it. To save time, we use the command **Select-String -Path 2.txt -Pattern ‘redryder’**. This command will search a particular file for the pattern “redryder”. This command outputs the complete answer; redryderbbgun.