

PSP0201

WEEK 5

WRITE UP

ID	NAME	ROLE
1211102582	AMEER IRFAN BIN NORAZIMAN	LEADER
1211101873	MUHAMMAD NABEEL SHAMIME BIN KHAEROZI	MEMBER
1211102269	MUHAMMAD ANIQ SYAHMI BIN SHAHARIL	MEMBER
1211101915	NURDINA AISHAH BINTI KASUMA SATRIA	MEMBER

Day 16 - Help? Where is Santa?

Tools Used: Kali Linux, Firefox, Terminal

Solutions:

Question 1

Start the terminal in Kali and use nmap ip address to find the port number.

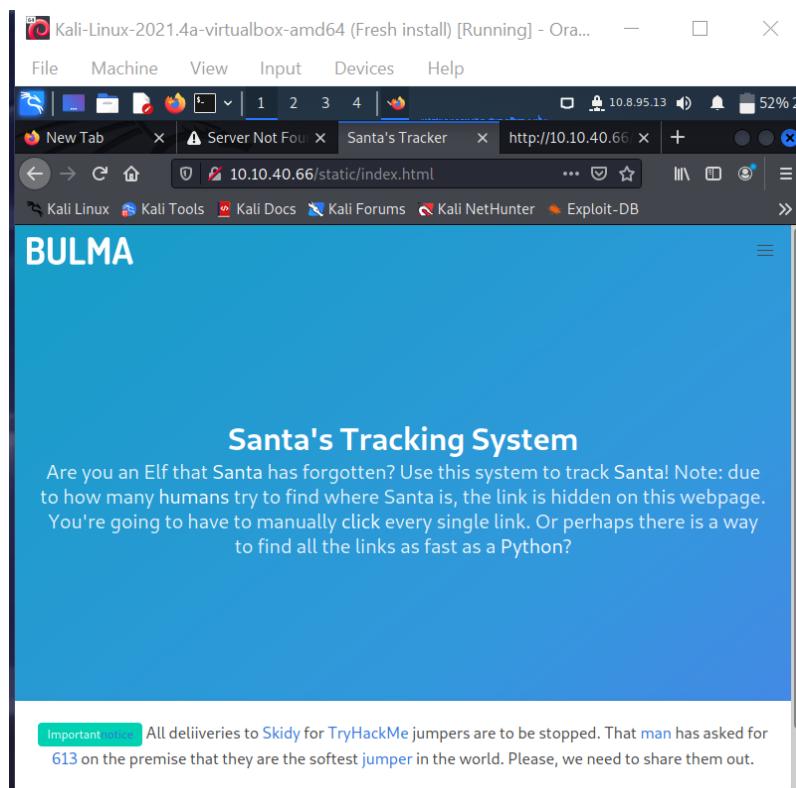
```
(kali㉿kali)-[~]
└─$ nmap 10.10.40.66
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-11 23:32 EDT
Nmap scan report for 10.10.40.66
Host is up (0.21s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 38.01 seconds

(kali㉿kali)-[~]
└─$ █ home
```

Question 2

Paste the webpage link given by Santa in FireFox.



Question 3

Clicked on the hidden link in Santa webpage

The screenshot shows a Firefox browser window running on a Kali Linux host. The title bar indicates the session is a 'Fresh install [Running] - Oracle VM VirtualBox'. The address bar shows the URL 10.10.223.233/api/. The main content area displays the 'Santa's Tracking System' page. The page has a blue header with the title 'Santa's Tracking System'. Below the header, there is a message: '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?'. A green 'Important' button contains the text: 'All deliveries 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.' Below this message, there are three columns of categories:

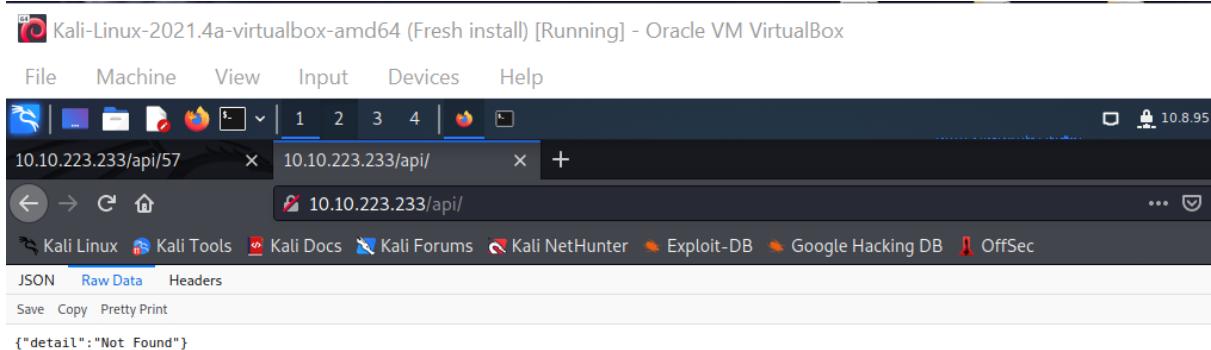
Category	Category	Category
Lorem ipsum dolor sit amet	Labore et dolore magna aliqua	Objects in space
Vestibulum errato isse	Kanban airis sum eschelor	Playing cards with coyote
Lorem ipsum dolor sit amet	Modular modern free	Goodbye Yellow Brick Road
Aisia caisia	The king of clubs	The Garden of Forking Paths
Murphy's law	The Discovery Dissipation	Future Shock
Flimsy Lavenrock	Course Correction	
Maven Mousie Lavender	Better Angels	

At the bottom of the page, there are two buttons: 'Bulma Templates' and 'MIT license'.

The screenshot shows a Firefox browser window running on a Kali Linux host. The title bar indicates the session is a 'Fresh install [Running] - Oracle VM VirtualBox'. The address bar shows the URL <http://10.10.40.66/static/index.html>. There are four tabs open, all showing a 'Server Not Found' error. The tabs are labeled 'New Tab', 'Server Not Found', 'Server Not Found', and 'http://10.10.40.66/static/'. The status bar at the bottom shows the IP address 10.8.95.13, battery level 49%, and time 23:43. The navigation bar includes icons for back, forward, search, and other browser functions. The bottom of the screen shows the Kali Linux desktop environment with various application icons.

Question 4

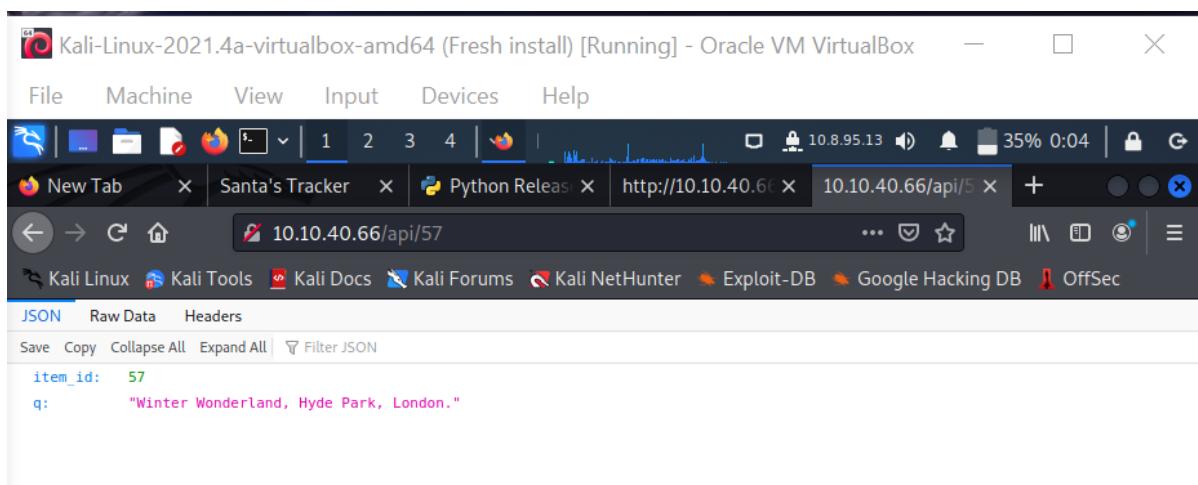
Delete the api_key at the end of the link and click enter,



```
{"detail": "Not Found"}
```

Question 5 and 6

Fill in the hidden link found in BULMA and as for the api key try and error any odd number from 1 till 100.



```
item_id: 57
q: "Winter Wonderland, Hyde Park, London."
```

The Thought Process

For day 16, as one of the Santa elves that got left behind, we had to find Santa's location. Luckily Santa has given a webpage "**10.10.40.66/static/index.html**" to help elves find their way back home. However Santa never told the elves the port number to the web server so we had to open the terminal and type in nmap (**10.10.40.66**), there were two ports 22 and 80, and we picked 80 as it uses http service. Then, we logged into FireFox and pasted the webpage given by Santa. We then saw the webpage template BULMA, somewhere in the web there's a hidden link, so we clicked one by one and eventually a link "machine_ip/api/api_key" appeared. Then we place our ip address (**10.10.40.66**) and as for the api_key we try and error to get the correct one. Finally Santa's location appeared, which is "Winter Wonderland, Hyde Park, London." As for question 4, to find the raw data we deleted the api-key and clicked the Raw Data tab and we used a new ip address (**10.10.223.233**) as we had trouble with the previous ip address when refreshing the page.

Day 17 - ReverseELFneering

Tools Used: Kali Linux, Firefox, Terminal

Solutions:

Question 1

Match the data type with the size in bytes:

tryhackme.com/room/learnyberin25days



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:

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

4. Read the instructions!

Some other important instructions are:

- $\text{leaq source, destination}$: this instruction sets destination to the address denoted by the expression in source

Question 2:

What is the command to analyse the program in radare2?(aa)

The screenshot shows a Kali Linux desktop environment with several open windows. One window displays search results from exploit-db for the exploit 'christmas-re'. The results show a title 'aoccmnre1', IP address '10.10.161.208', and expiration time '1h 22m 03s'. Another window shows a terminal session with Radare2 running on the exploit file. The terminal output includes assembly code and strings like 'they finally created 64 bit. All these', 'the value of a is 4, the value of b is 5 and the value of c is 9'. A tooltip in the top right corner of the terminal window says 'Add 1 hour'.

Without going into too much detail, instruction sets have been created and an executable file is produced, the linker finally makes operations with a linker finally makes

The best way to actually start exploiting binaries is to do this - radare2 is a framework for reverse engineering and analysing binaries. It can be used to disassemble them, analyze assembly which is actually readable, and debug said binaries by allowing a user to step through the execution.

Luckily for us, everything we need is already there:

1. Press the "Deploy" button on the exploit-db page.
2. Wait for the IP address of the exploit instance.
3. Log into your instance using the provided credentials.

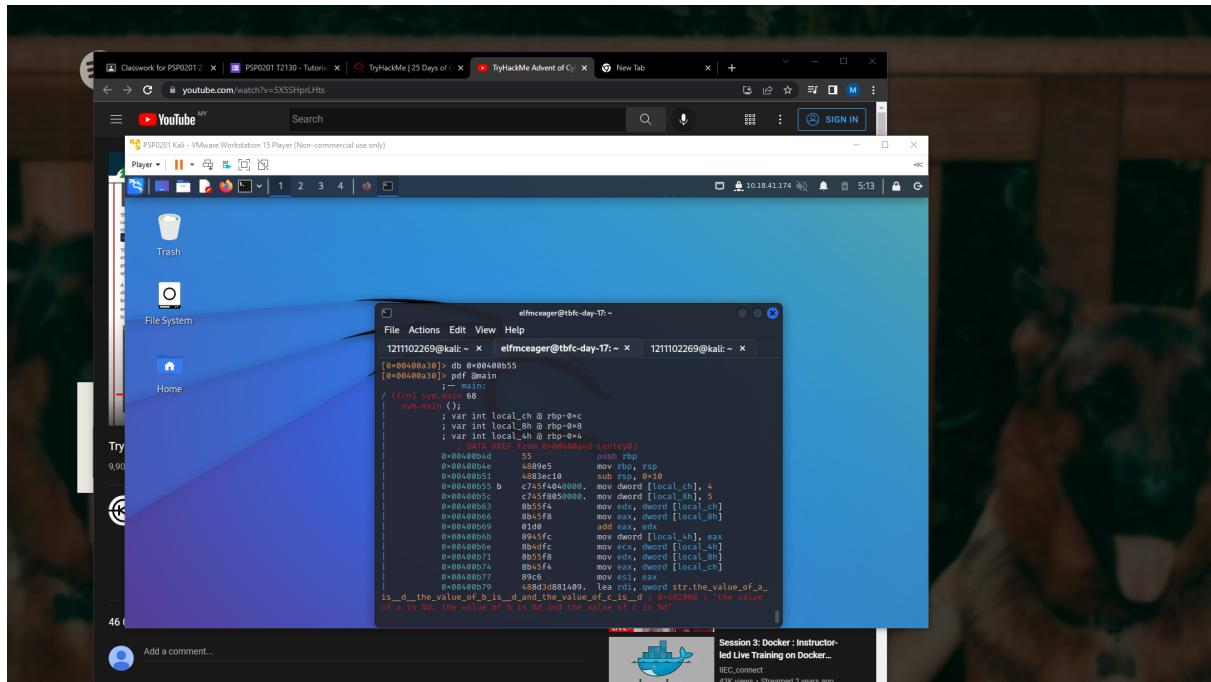
IP Address: 10.10.161.208
Username: elfmceager
Password: adventofcyber

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
```

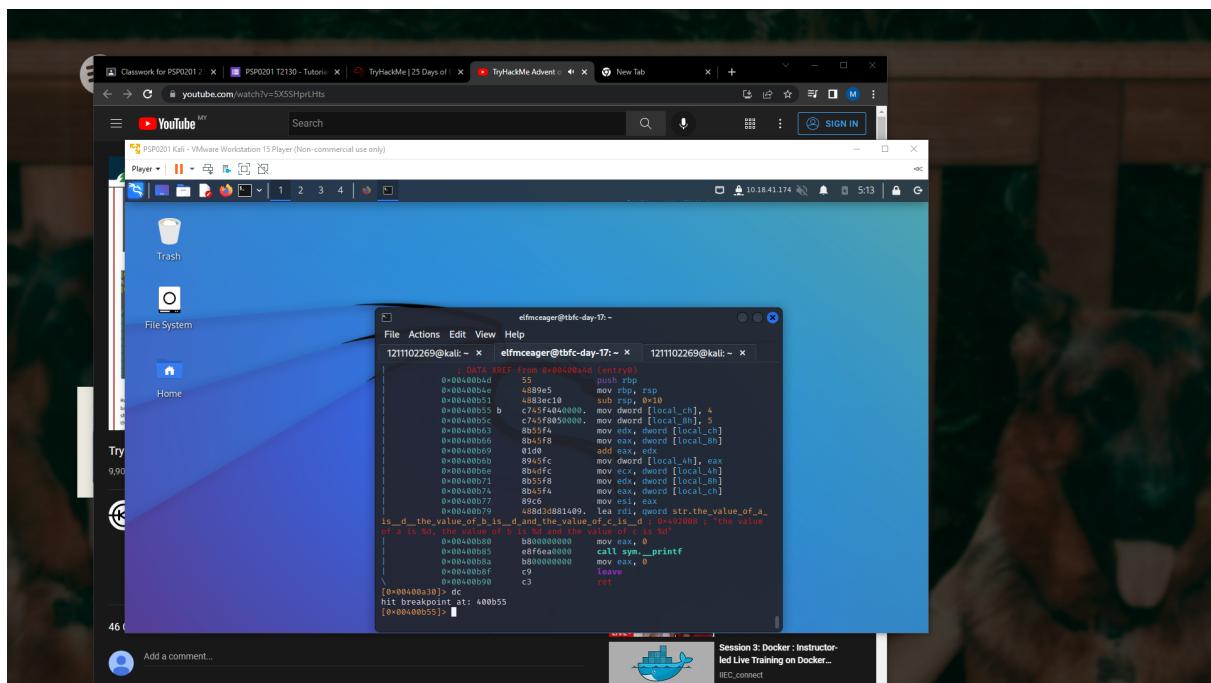
Question 3:

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



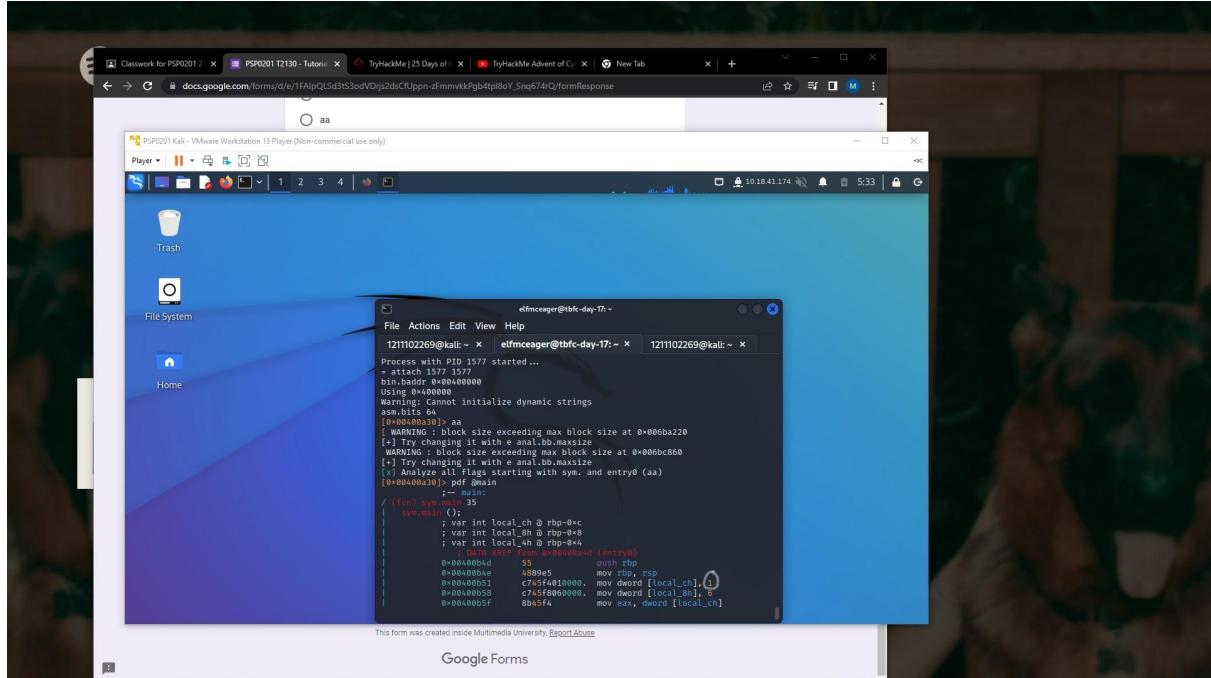
Question 4:

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



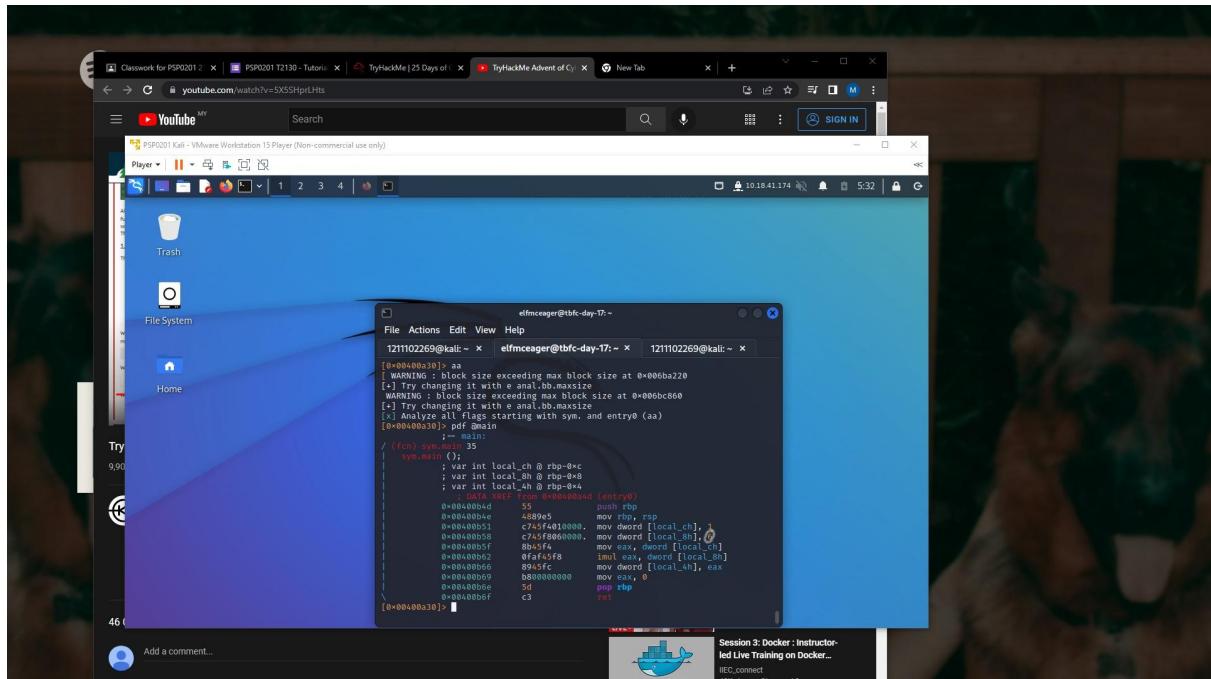
Question:5

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



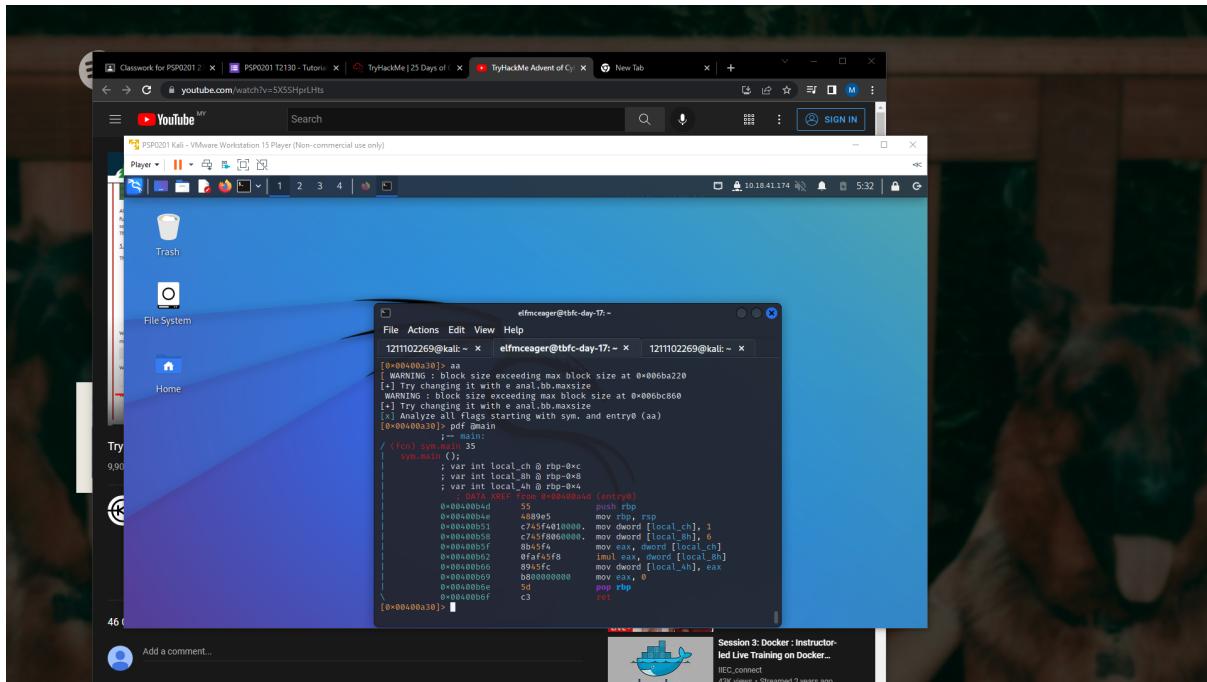
Question 6

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



Question 7:

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



The Thought Process

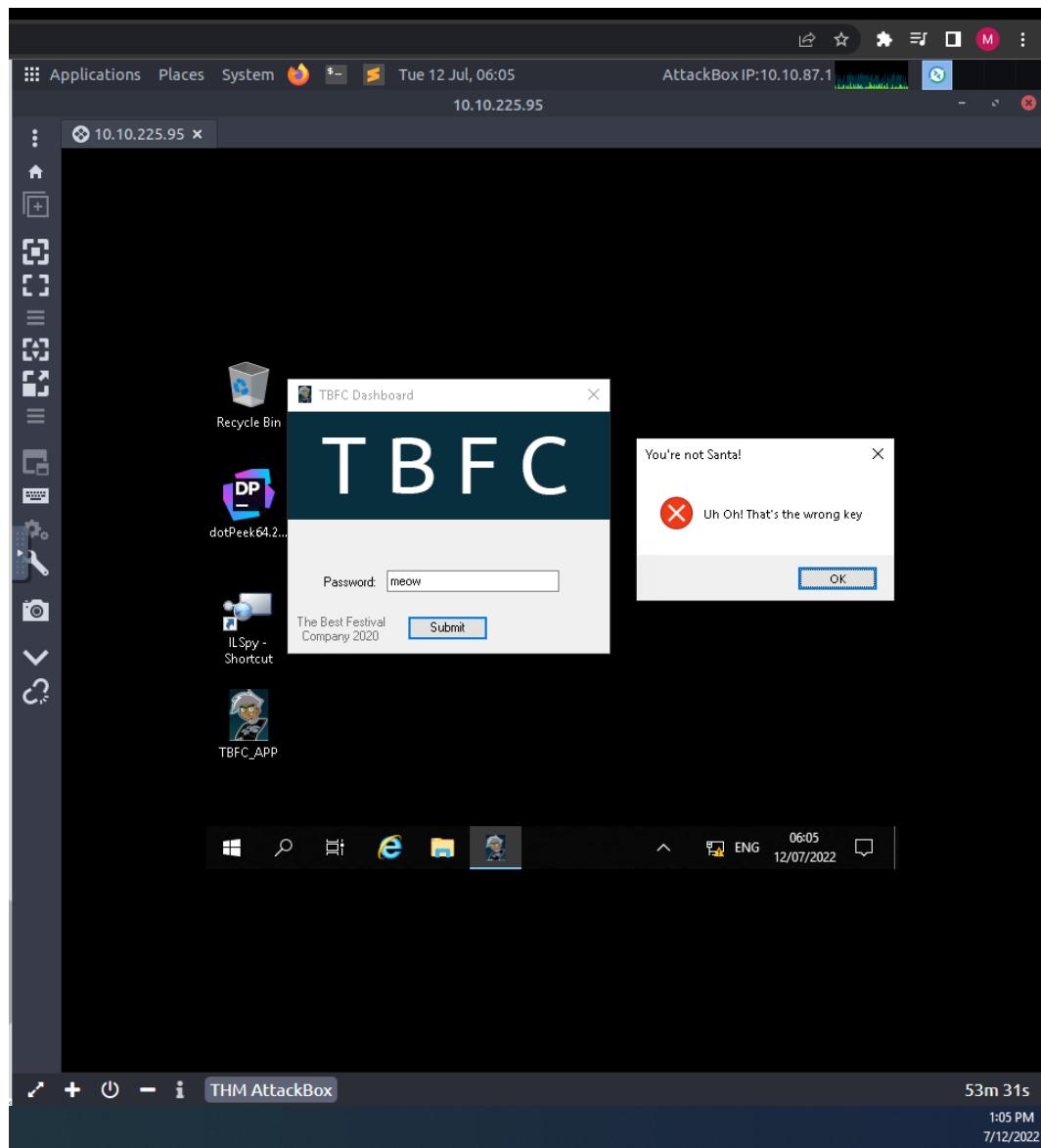
For Day 17, the match data type can be found at tryhackme website itself. To get the answer for the next question, we need to open the terminal because we need to login. For the login process, we need to open the terminal and key in the IP address that is given, the username and the password. Then, we need to run command `r2 - d ./file1`. This will open the binary in debugging mode. After that, just type `(aa)` command to analyse the program in radare2. For the next question, we need to run some commands to see how it works and get the answer. We run commands like `afl` to find a list of the functions. Then, we run the command `pdf@main`. From there, we start looking at the program from the 4th instruction(`movl $4`). We want to analyse the program while it runs. The best way to do it is by setting a breakpoint. So to set a breakpoint, we use command `(db)`. Since we want to look at the program from the 4th instruction, we type `db 0x0040b55` as shown on the screen. If we want to ensure that we already set the breakpoint, we can run the command `pdf@main` and we can see the breakpoint indicator(`b`). For the next question, we can continue from our exercise. We just simply run the command `(dc)`. We can see that it started to hit the breakpoint. From that, we know that command `(dc)` is used to hit a breakpoint. For question 5, we need to type command `r2 - d ./challenge1`. Then, we type command `pdf @ main`. From there, we can analyse the program and we can find the answer which is `(1)`. The next question, we need to do some multiplication. So, we are going to move the `1` to the `eax` and multiply it by `6`. For the last question, we just need to take the value from `eax` which is `(6)` and copy it.

Day 18 : The Bits of Christmas

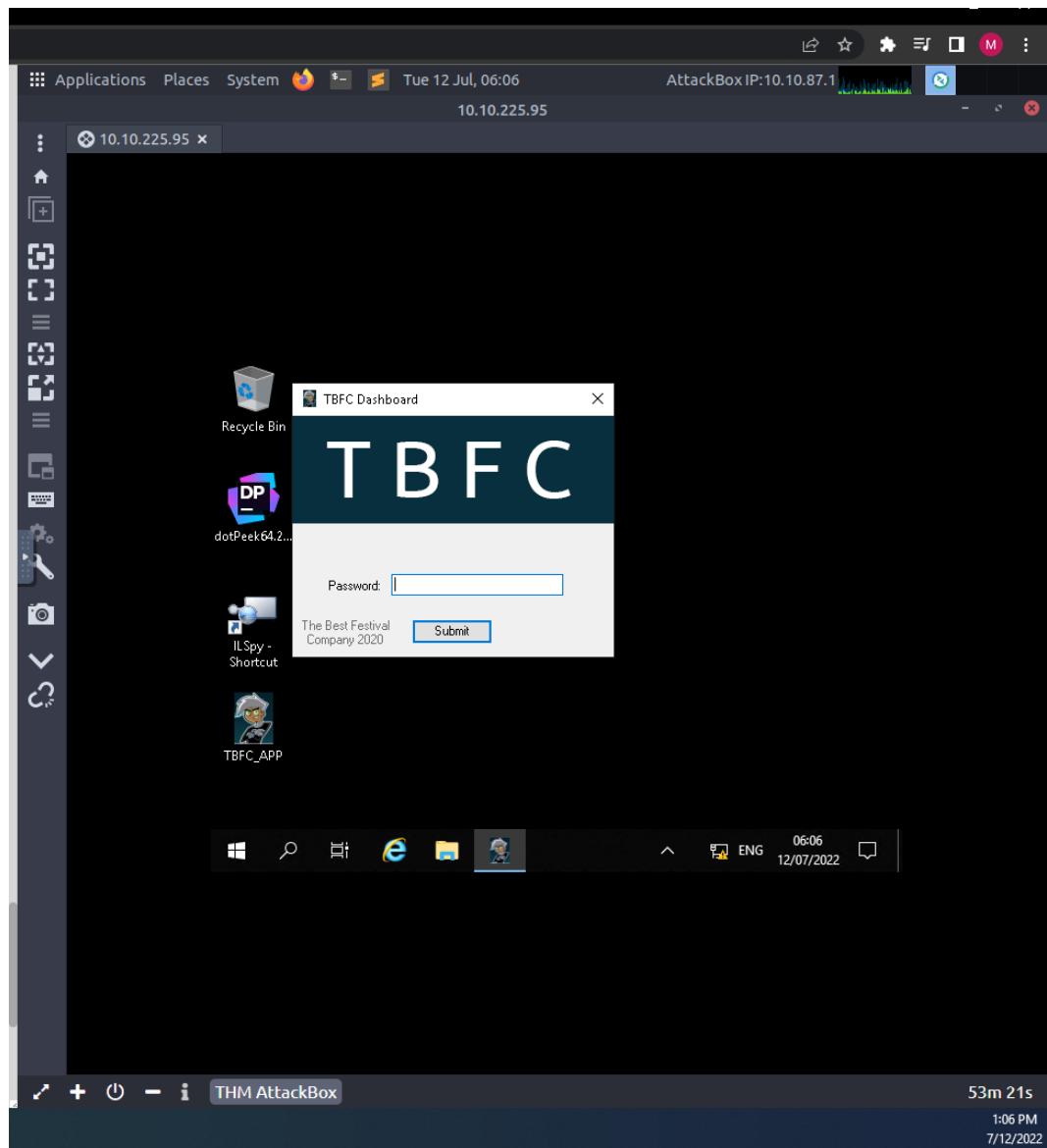
Tools used: TryHackMe, Firefox, Cyberchef

Solutions:

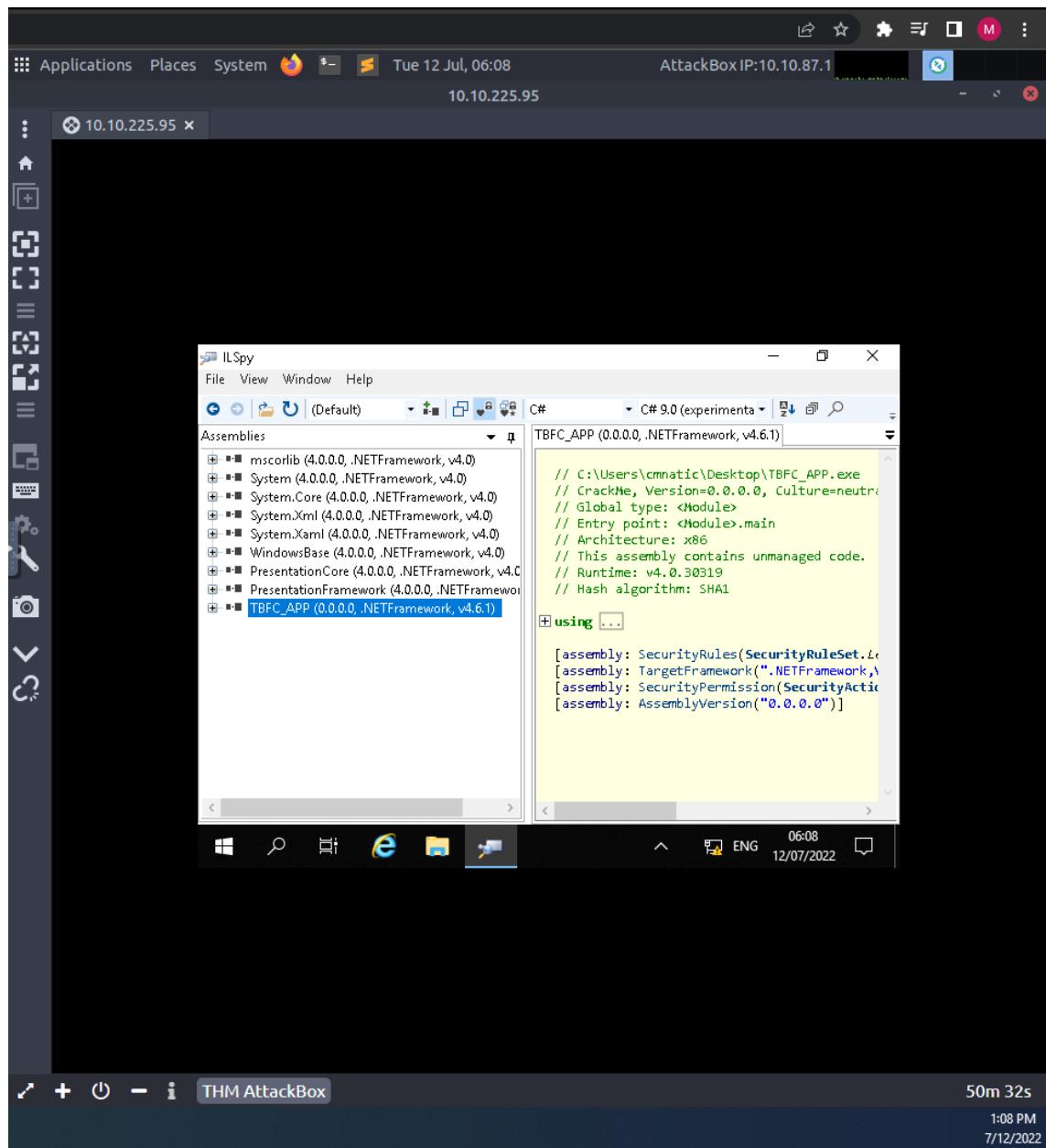
Question 1: The message that we received from TBC_APP when we entered the wrong password



Question 2: TBFC stands for The Best Festival Company



Question 3: The module that catches our attention (CrackMe)



The screenshot shows the ILSpy interface. The left pane displays a tree view of assembly symbols, including a node for 'CrackMe' which contains 'AboutForm' and 'MainForm'. The right pane shows the assembly manifest code for 'TBFC_APP'. The 'MainForm' symbol is highlighted in the manifest code, indicating it is the target for analysis.

```
// C:\Users\cmnatic\Desktop\TBFC_APP.exe
// CrackMe, Version=0.0.0.0, Culture=neutral
// Global type: <Module>
// Entry point: <Module>.main
// Architecture: x86
// This assembly contains unmanaged code.
// Runtime: v4.0.30319
// Hash algorithm: SHA1

[using ...]

[assembly: SecurityRules(SecurityRuleSet.L
[assembly: TargetFramework(".NETFramework,\\
[assembly: SecurityPermission(SecurityAction
[assembly: AssemblyVersion("0.0.0.0")]
```

Question 4 : The form that contains information that we are looking for (MainForm)

This screenshot is identical to the one above, showing the ILSpy interface with the assembly manifest and the 'MainForm' symbol highlighted in the code view.

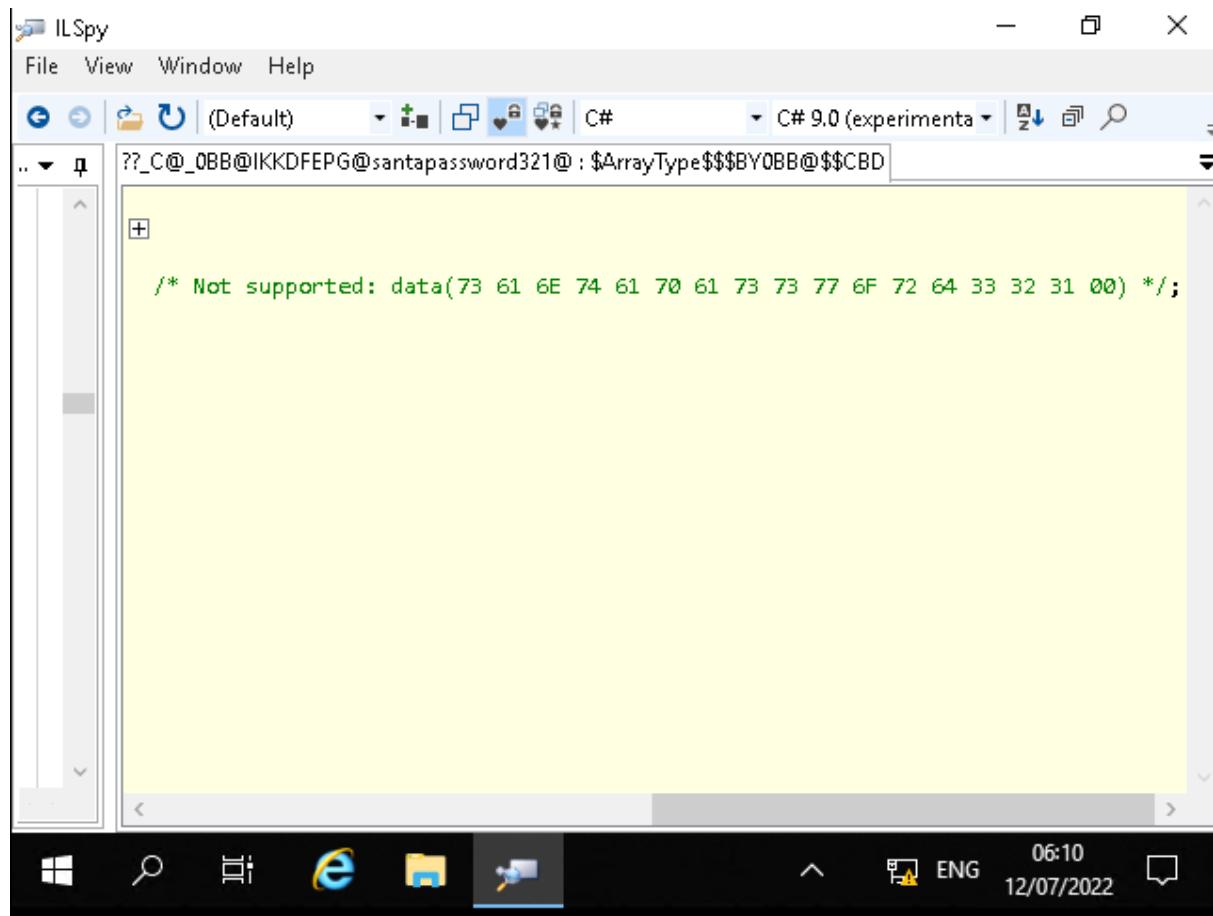
```
// C:\Users\cmnatic\Desktop\TBFC_APP.exe
// CrackMe, Version=0.0.0.0, Culture=neutral
// Global type: <Module>
// Entry point: <Module>.main
// Architecture: x86
// This assembly contains unmanaged code.
// Runtime: v4.0.30319
// Hash algorithm: SHA1

[using ...]

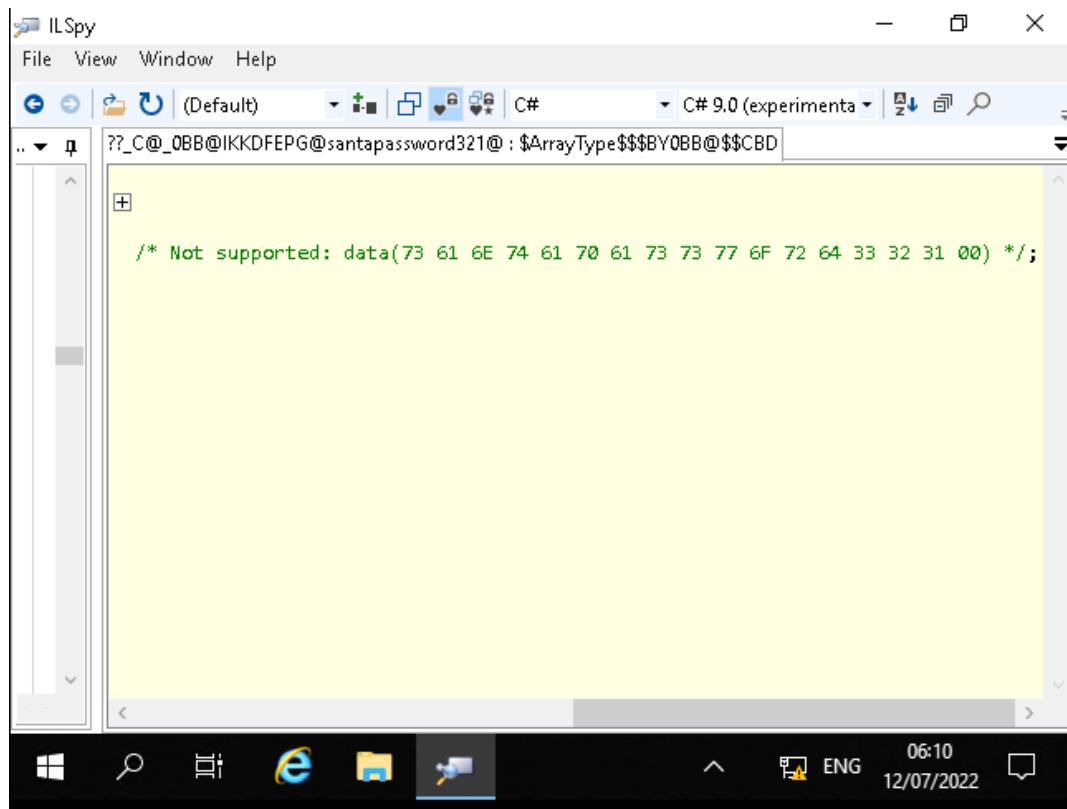
[assembly: SecurityRules(SecurityRuleSet.L
[assembly: TargetFramework(".NETFramework,\\
[assembly: SecurityPermission(SecurityAction
[assembly: AssemblyVersion("0.0.0.0")]
```

Question 5: The method that contains the information we seek
(buttonActivate_Click)

The picture below are in metod (**buttonActivate_click**)



Question 6: The Santa's password (**santapassword321**)

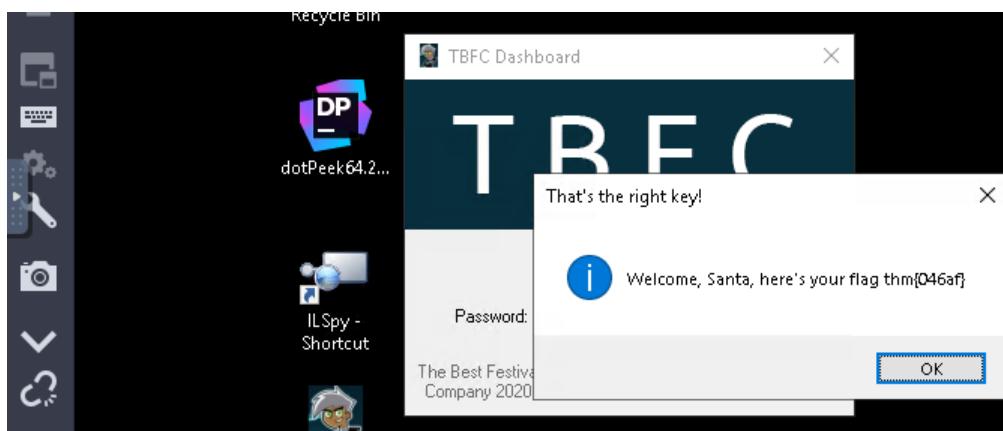


This screenshot shows a hex editor interface. At the top, it says "Last build: 4 days ago". The interface is divided into sections: "Recipe" (with "From Hex" selected), "Input", and "Output".

Input: The input section contains the hex bytes: 73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31 00.

Output: The output section displays the decoded string: santapassword321.

Question 7: The flag we received when we logged in (**thm{046af}**)



The Thought Process:

First of all, we open the Remmina on TryHackMe Attackbox to connect to the instance with the RDP client by referring to the notes that were provided in THM. Once we have done that, we open up ILSpy and decompile TBFC_APP. Then, we noticed there was a module called "**CrackMe**" that contained 2 forms which were "**AboutForm**" and "**MainForm**". We took a look at both forms and each form contained its own methods and information. In the end, we noticed that the method "**buttonActivate_Click**" in "**MainForm**" contained information that mentions "**santapassword321**". But before we took that as the password, we double clicked on it and noticed that there was data stored in Hexadecimal form. From there, we used CyberChef to decode the Hexadecimal code to achieve the password. Once we receive the password, we insert the password into the TBFC Dashboard to get the flag.

Day 19: The Naughty or Nice List

Tools Used: Kali Linux, Firefox

Solutions:

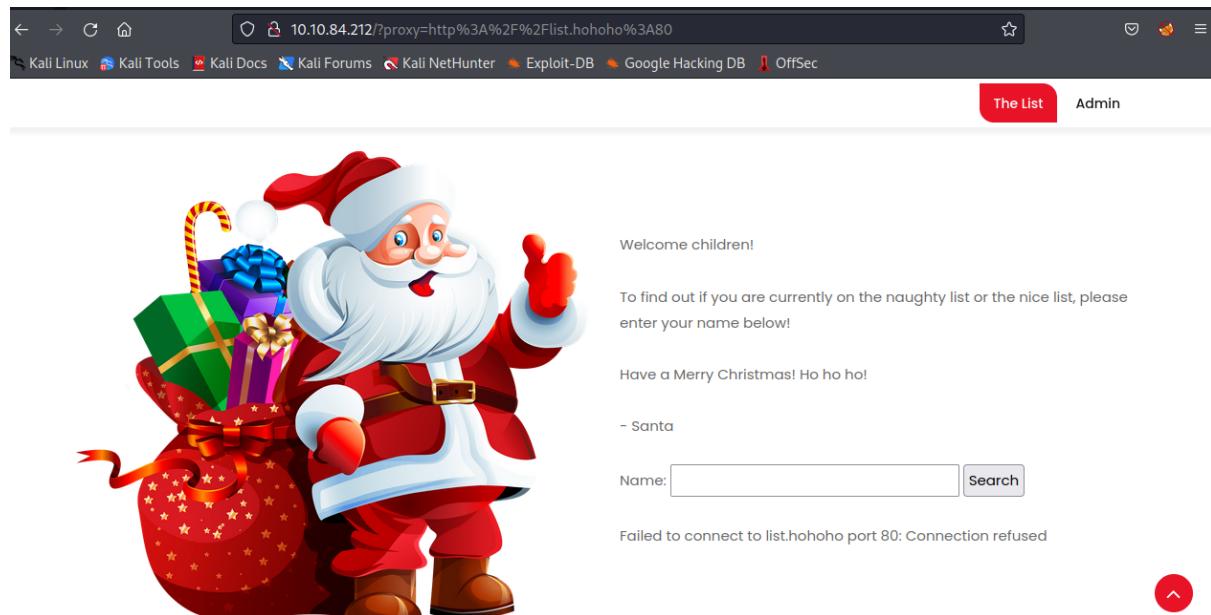
Question 1: The list for each person

The screenshot shows a web page titled "The Naughty or Nice List". At the top right are two buttons: "The List" (highlighted in red) and "Admin". The main content features a cartoon illustration of Santa Claus carrying a large sack of gifts. To the right of the illustration, the text "Welcome children!" is displayed. Below it, a message reads: "To find out if you are currently on the naughty list or the nice list, please enter your name below!". Underneath this is a signature from "Santa" and a search form with a placeholder "Name:" and a "Search" button. The search results show the message "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"?

The screenshot shows a web browser window with the URL "10.10.84.212/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F" in the address bar. The page content is identical to the first screenshot, featuring the "The Naughty or Nice List" header, the Santa illustration, and the search form. However, the search results now display the error message "Not Found" and "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"?



Welcome children!

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

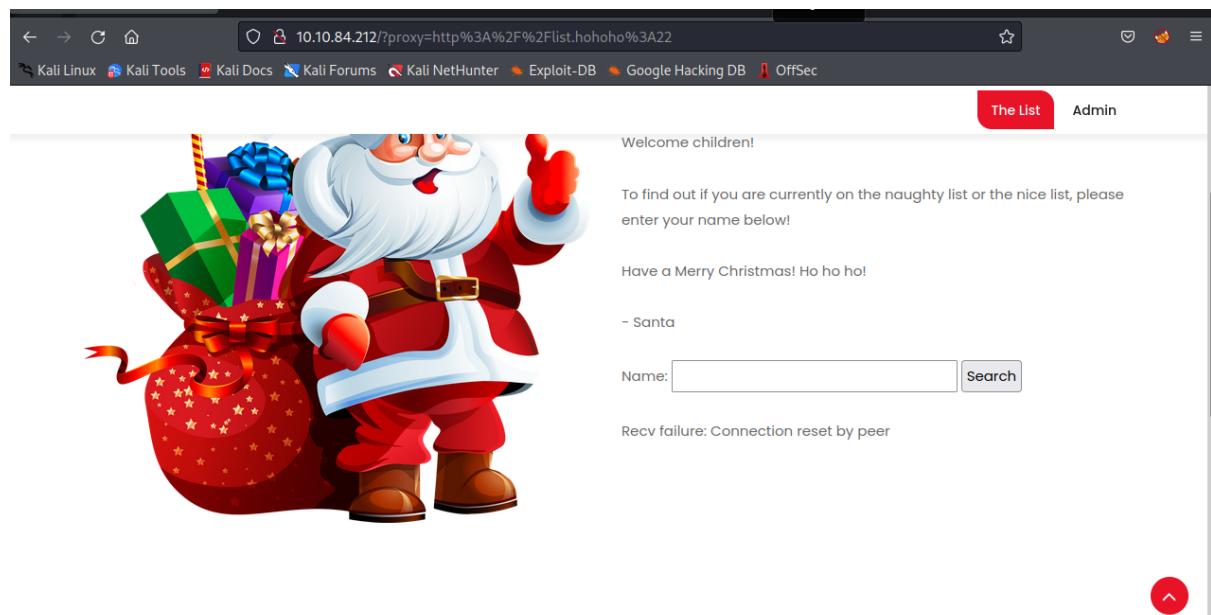
Have a Merry Christmas! Ho ho ho!

- Santa

Name:

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"?



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:

Recv failure: Connection reset by peer

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

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.

Question 6: The Santa's Password

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.

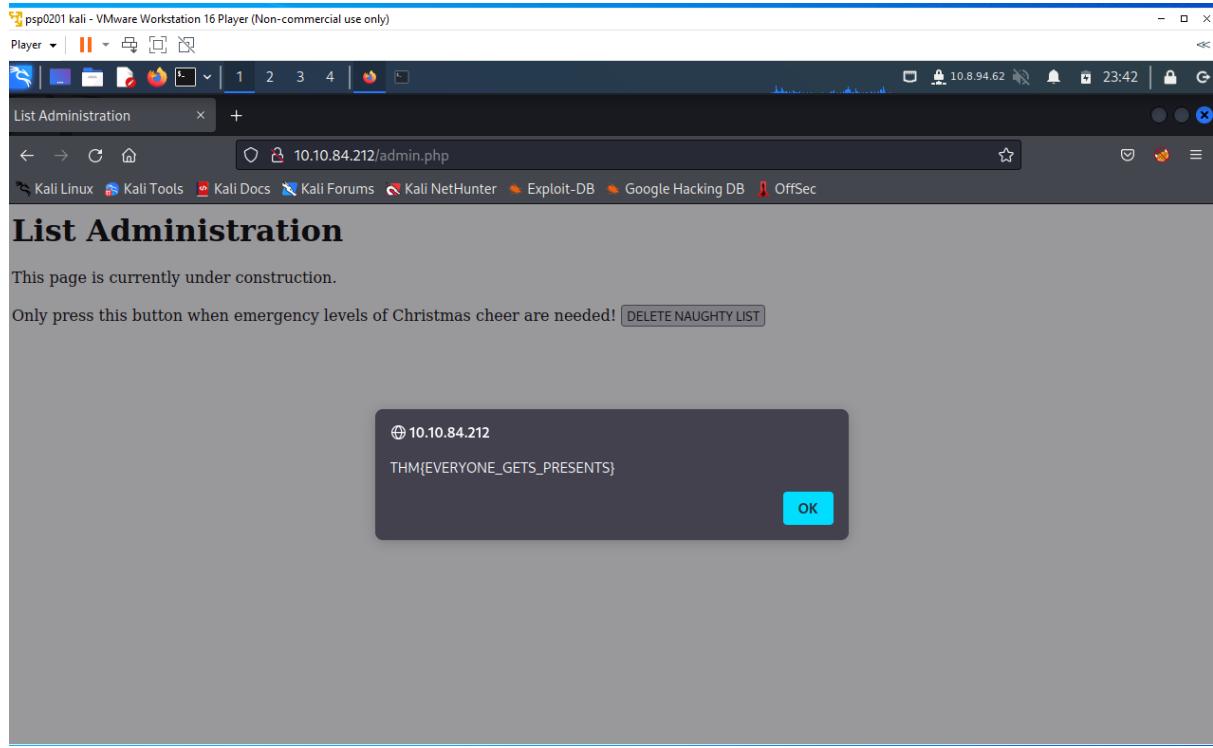
I know you have trouble remembering your password so here it is: Be good for goodness sake!

- Elf McSkidy

Question 7: The challenge flag

The screenshot shows a Firefox browser window titled "psp0201 kali - VMware Workstation 16 Player (Non-commercial use only)". The address bar contains the URL "10.10.84.212/?proxy=http%3A%2F%2Flist.hohoho.localtest.me". The page title is "Admin". The content area displays a red "Admin" logo at the top, followed by a form with fields for "Username" (containing "Santa") and "Password" (containing a long string of black dots). A "Login" button is below the password field. At the bottom of the page, a footer reads "All Rights Reserved. © 2018 Evento Christmas Design By : html design".

The screenshot shows a Firefox browser window titled "psp0201 kali - VMware Workstation 16 Player (Non-commercial use only)". The address bar contains the URL "10.10.84.212/admin.php". The page title is "List Administration". The content area displays the text "This page is currently under construction." and a button labeled "Only press this button when emergency levels of Christmas cheer are needed! [DELETE NAUGHTY LIST]".



The Thought Process

For day 19, first, we started the machine and inserted the ip address into the search bar and then the website appeared. To answer question 1, we just simply insert the names into the “Name” search bar to see whether the name is in naughty list or nice list. Next, For questions 2,3,4 and 5, we just simply insert the parameters that were given in each question into the search bar. From there, the answer for the questions will appear on the page. Next, for question 6, we need to search for Santa’s password. To achieve that, according to the notes in tryhackme, we can easily bypass it by setting the hostname in the URL to “list.hohoho.localtest.me”. This is because the hostname needs to be started with “list.hohoho”. Once we have done that, we can see on the page that the password was given. From there, we logged in via the admin section, and then we clicked the “**DELETE NAUGHTY LIST**” button to receive the flag.

Day 20: Powershell to rescue

Tools Used: Kali Linux, Firefox

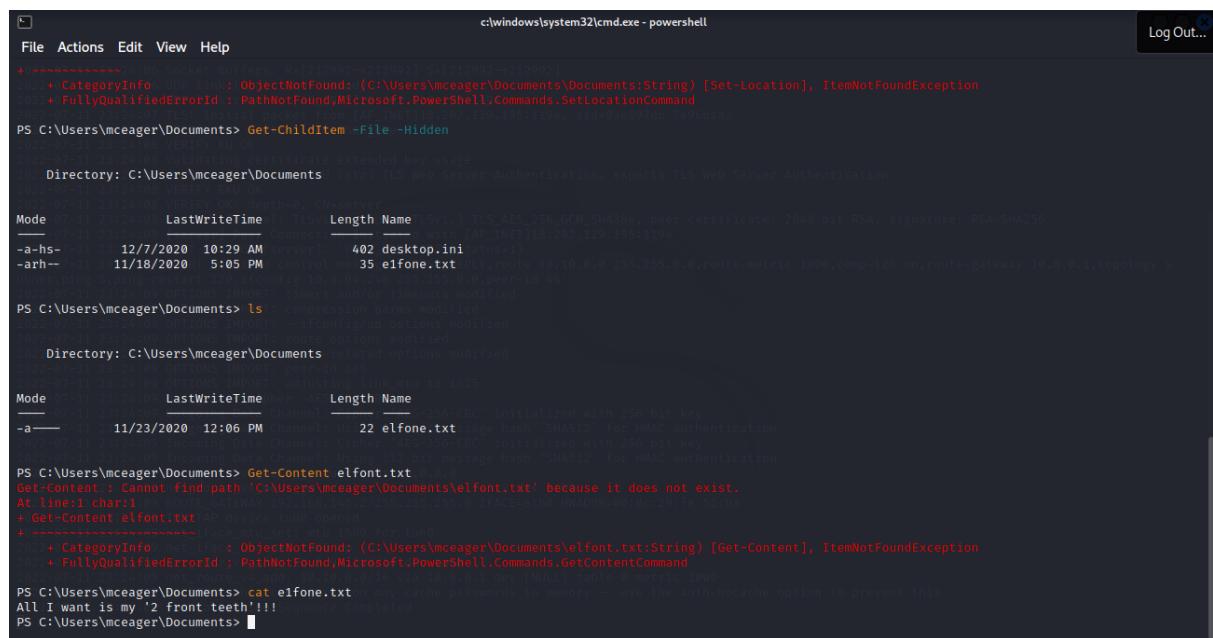
Solutions:

Question 1:

The parameter -l do that checked in ssh manual is **login name**

Question 2

The first hidden elf file within the Documents folder that Elf 1 wants is **2 front teeth**.



```
c:\windows\system32\cmd.exe - powershell
File Actions Edit View Help
+-----+----+----+----+----+----+
+ CategoryInfo : ObjectNotFound: ((C:\Users\mceager\Documents:String) [Set-Location], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
PS C:\Users\mceager\Documents> Get-ChildItem -File -Hidden
Directory: C:\Users\mceager\Documents
Mode                LastWriteTime     Length Name
-a---             12/23/2020  12:06 PM          22 elfone.txt
PS C:\Users\mceager\Documents> ls
Directory: C:\Users\mceager\Documents
Mode                LastWriteTime     Length Name
-a---             11/23/2020  12:06 PM          22 elfone.txt
PS C:\Users\mceager\Documents> Get-Content elfont.txt
Get-Content : Cannot find path 'C:\Users\mceager\Documents\elfont.txt' because it does not exist.
At line:1 char:1  + GET-CONTENT C:\Users\mceager\Documents\elfont.txt
+-----+----+----+----+----+----+
+ CategoryInfo : ObjectNotFound: ((C:\Users\mceager\Documents\elfont.txt:String) [Get-Content], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand
PS C:\Users\mceager\Documents> cat elfone.txt
cat: elfone.txt: may cache passwords in memory -- use the auth-nocache option to prevent this
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\Documents>
```

Question 3

The name of that movie is **Scrooged**.



```
PS C:\Users\mceager\Desktop\elf2wo> cat ^C
cat: ^C: may cache passwords in memory -- use the auth-nocache option to prevent this
PS C:\Users\mceager\Desktop\elf2wo> cat e70smsW10Y4k.txt
cat: e70smsW10Y4k.txt: may cache passwords in memory -- use the auth-nocache option to prevent this
I want the movie Scrooged <3!
PS C:\Users\mceager\Desktop\elf2wo>
```

Question 4

The name of the hidden folder is **3lfthr3e**.

```
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

PS C:\Windows\System32> cd 3lfthr3e
PS C:\Windows\System32\3lfthr3e>
```

Question 5

First file contains **9999**.

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

Count      : 9999
Average    :
Sum        :
Maximum    :
Minimum    :
Property   :
```

Question 6

2 words are at index 551 and 6991 in the first file is ***Red Ryder***.

```
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Select-Object -Index  
551  
Red  
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Select-Object -Index  
551,6991  
Red  
Ryder  
PS C:\Windows\System32\3lfthr3e> |
```

Question 7

Answer is ***redryderbbun***.

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

Throughout Process

In order to open the powershell and obtain the IP address, we first deploy the computer. Using ssh, we log in as meagre and start the powershell. The Get-Childitem command with the -Hidden argument is then used to view what is hidden inside the Documents folder after using the cd command to navigate there. There, we discovered a "elfone.txt" file belonging to elf 1. We may view the file's content using the cat tool. The Get-Childitem command with the -Hidden argument is then used to find the hidden folder after changing the location to Desktop using the cd command. Then, using the cd command once more, we are in the elf2wo folder after discovering a folder with that name. The movie title that elf 2 requests is revealed when we use the Get-Childitem command to locate a file with the name e70smsW10Y4k.txt. Then we use the cd command to move the directory to Windows and the cd command once again to enter system32. The hidden folder with the name 3lfthr3e is then located using the Get-Childitem command with the -Hidden, -Directory, and -Filter "*3" option. The 3lfthr3e folder is then entered using the cd command, and the files in the folder are then visible using the Get-Childitem command with the -Hidden argument. The first file's contents are then seen using the Get-Content command, and the number of words it contains is determined by piping the output to Measure-Object with the -Word argument. Using the Get-Content argument in a bracket to open the first file and the index enclosed in square brackets, we can view the precise location in this file. Then, by opening the second file with the Get-Content command and piping the output to Select-String with the -Pattern "redryder" option, we can determine what elf 3 is looking for.