

PSP0201

Week 5

Writeup

Group Name: F4urDeveloper

Members:

ID	NAME	ROLE
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	LEADER
1211104237	ALIA MAISARA BINTI SHAHRRIN	MEMBER
1211102287	TERRENCE CHENG	MEMBER
1211101153	MISCHELLE THANUSHA JULIUS	MEMBER

Day 16: Scripting Help! Where is Santa?

Tools used: THM Attackbox

Solution/walkthrough:

Question 1

What is the port number for the web server?

The screenshot shows a browser window with several tabs open. The active tab is 'tryhackme.com/room/learncyberin25days'. On the left, there's a challenge titled 'Where is Santa?' with a text area containing instructions about deploying a machine and finding an API key. Below the text is a decorative banner with the word 'SANTA' on it. There are input fields for answers and buttons for 'Correct Answer', 'Submit', and 'Hint'. The right side of the screenshot shows a terminal window titled 'root@ip-10-10-224-207: ~'. The terminal output shows a nmap scan of the target IP (10.10.250.91) which finds open ports 80/tcp (http) and 22/tcp (ssh). It also lists services as 'PORT STATE SERVICE' and provides MAC address information. The bottom of the terminal shows a list of challenges: 'Modular modern free', 'The king of clubs', 'The Discovery Dissipation', 'Course Correction', and 'Better Angels'. The status bar at the bottom of the terminal indicates '1h 38m 36s'.

The port number for this web server is 80.

Question 2

What templates are being used?

MERRY CHRISTMAS

Created by Bee.

Oh no! Santa 🎅 has taken off, leaving you – the faithful elves behind! Can you help find Santa's location?

Luckily, the elves are OSINT masters and remember a thing or two. Specifically, they remember:

- Santa has a webpage at 10.10.250.91/static/index.html to help lost elves find their way home. Santa never told the elves what port number the webserver is on. Can you find out?!
- This webpage has a link somewhere on it, hidden away so anyone that isn't an elf can't find it.
- Santa's Sled has an API we can talk too. The key for the API is between 0 and 100, and it's an odd number. But be careful! After an unknown number of attempts, Santa's Sled will ban your IP address.

Deploy the machine that is running Santa's Sled and allow a couple of minutes for the target (10.10.250.91) to start up. Using your Python skills from Day 15 to find the correct key for the API.

Watch John Hammonds video on solving this task!

Answer the questions below

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: 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.

Category: *Lorum ipsum dolor sit amet.*

THM AttackBox

1h 43m 01s

The template are being used is BULMA

Question 3

Without using enumeration tools such as Dirbuster, what is the directory for the API?

MERRY

Created by Bee.

Oh no! Santa 🎅 has taken off, leaving you – the faithful elves behind! Can you help find Santa's location?

Luckily, the elves are OSINT masters and remember a thing or two. Specifically, they remember:

- Santa has a webpage at 10.10.111.208/static/index.html to help lost elves find their way home. Santa never told the elves what port number the webserver is on. Can you find out?
- This webpage has a link somewhere on it, hidden away so anyone that isn't an elf can't find it.
- Santa's Sled has an API we can talk too. The key for the API is between 0 and 100, and it's an odd number. But be careful! After an unknown number of attempts, Santa's Sled will ban your IP address.

Deploy the machine that is running Santa's Sled and allow a couple of minutes for the target (10.10.111.208) to start up. Using your Python skills from Day 15 to find the correct key for the API.

Watch John Hammonds video on solving this task!

Answer the questions below

What is the port number for the web server?

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Save Page As...
Save Page to Pocket
Send Page to Device
View Background Image
Select All
View Page Source
View Page Info
Inspect Accessibility Properties
Inspect Element (Q)
Take a Screenshot

1h 54m 23s

MERRY

Created by Bee.

Oh no! Santa 🎅 has taken off, leaving you – the faithful elves behind! Can you help find Santa's location?

Luckily, the elves are OSINT masters and remember a thing or two. Specifically, they remember:

- Santa has a webpage at 10.10.111.208/static/index.html to help lost elves find their way home. Santa never told the elves what port number the webserver is on. Can you find out?
- This webpage has a link somewhere on it, hidden away so anyone that isn't an elf can't find it.
- Santa's Sled has an API we can talk too. The key for the API is between 0 and 100, and it's an odd number. But be careful! After an unknown number of attempts, Santa's Sled will ban your IP address.

Deploy the machine that is running Santa's Sled and allow a couple of minutes for the target (10.10.111.208) to start up. Using your Python skills from Day 15 to find the correct key for the API.

Watch John Hammonds video on solving this task!

Answer the questions below

What is the port number for the web server?

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

1h 52m 06s

Question 4

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

The screenshot shows a browser window with the URL tryhackme.com/room/learnCyberin25days. The page displays Task 18 [Day 16] titled "Scripting Help! Where is Santa?". It includes a banner with the word "MERRY" and a "Start Machine" button. Below the banner, there is text about Santa's sleigh taking off and the elves needing help. A list of hints follows, mentioning a webpage at 10.10.155.162/static/index.html and an API key between 0 and 100. A note says that after 100 attempts, the sled will ban the IP address. A link to a video by John Hammonds is provided.

On the right side of the screenshot, a terminal window is open on the THM AttackBox with root privileges. The user is in a directory where a file named "key.py" exists. The terminal shows a Python script using the requests library to iterate through API keys from 1 to 100, sending requests to `http://10.10.155.162/api/{api_key}`. If an error is encountered in the response, it continues to the next key; otherwise, it breaks out of the loop. The script then sends a final request to `http://10.10.155.162/api/57`.

The screenshot shows the same browser window and challenge page as above. On the right, a Firefox developer tools window is open, specifically the "Raw Data" tab of the Network panel. It shows a single request to `http://10.10.155.162/api/57` with the following raw JSON response:

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

A message at the bottom of the Firefox window says, "It looks like you haven't started Firefox in a while. Do you want to download it now? Fresh like new experiences. And by the way, it's fast."

Question 5

Where is Santa right now?

The screenshot shows a browser window with the URL <tryhackme.com/room/learn cyberin25days>. The page displays Task 18 [Day 16] Scripting Help! Where is Santa?. Below the task title is a banner with the word "MERRY". A green button labeled "Start Machine" is visible. The text on the page says: "Created by Bee. Oh no! Santa 🎅 has taken off, leaving you – the faithful elves behind! Can you help find Santa's location? Luckily, the elves are OSINT masters and remember a thing or two. Specifically, they remember:

- Santa has a webpage at 10.10.155.162/static/index.html to help lost elves find their way home. Santa never told the elves what port number the webserver is on. Can you find out?!
- This webpage has a link somewhere on it, hidden away so anyone that isn't an elf can't find it.
- Santa's Sled has an API we can talk too. The key for the API is between 0 and 100, and it's an odd number. But be careful! After an unknown number of attempts, Santa's Sled will ban your IP address.

Deploy the machine that is running Santa's Sled and allow a couple of minutes for the target (10.10.155.162) to start up. Using your Python skills from Day 15 to find the correct key for the API.

Watch John Hammonds video on solving this task!

On the right, a terminal window titled "root@ip-10-10-215-125: ~" shows a Python script named "key.py":

```
import requests

target_ip = '10.10.155.162'

for api_key in range(1,100,2):
    print(f'API Key: {api_key}')
    response = requests.get(f'http://[{target_ip}]/api/{api_key}')
    print(response.text)
```

The screenshot shows a browser window with the URL <tryhackme.com/room/learn cyberin25days>. The page displays Task 18 [Day 16] Scripting Help! Where is Santa? Below the task title is a banner with the word "MERRY". A green button labeled "Start Machine" is visible. The text on the page says: "Created by Bee. Oh no! Santa 🎅 has taken off, leaving you – the faithful elves behind! Can you help find Santa's location? Luckily, the elves are OSINT masters and remember a thing or two. Specifically, they remember:

- Santa has a webpage at 10.10.155.162/static/index.html to help lost elves find their way home. Santa never told the elves what port number the webserver is on. Can you find out?!
- This webpage has a link somewhere on it, hidden away so anyone that isn't an elf can't find it.
- Santa's Sled has an API we can talk too. The key for the API is between 0 and 100, and it's an odd number. But be careful! After an unknown number of attempts, Santa's Sled will ban your IP address.

Deploy the machine that is running Santa's Sled and allow a couple of minutes for the target (10.10.155.162) to start up. Using your Python skills from Day 15 to find the correct key for the API.

Watch John Hammonds video on solving this task!

On the right, a terminal window titled "root@ip-10-10-215-125: ~" shows the output of the "key.py" script:

```
API Key: 43
[{"item_id":43,"q":"Error. Key not valid!"}
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!"}]
```

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.

The screenshot shows a browser window with several tabs open. The main content area displays a challenge titled "Task 18 [Day 16] Scripting Help! Where is Santa?". It features a decorative banner with the word "MERRY" and a "Start Machine" button. Below the banner, there is a message from Bee: "Oh no! Santa 🎅 has taken off, leaving you – the faithful elves behind! Can you help find Santa's location?". Another message states: "Luckily, the elves are OSINT masters and remember a thing or two. Specifically, they remember:" followed by a bulleted list:

- Santa has a webpage at 10.10.155.162/static/index.html to help lost elves find their way home. Santa never told the elves what port number the webserver is on. Can you find out?!
- This webpage has a link somewhere on it, hidden away so anyone that isn't an elf can't find it.
- Santa's Sled has an API we can talk to. The key for the API is between 0 and 100, and it's an odd number. But be careful! After an unknown number of attempts, Santa's Sled will ban your IP address.

Below the list, there is a note: "Deploy the machine that is running Santa's Sled and allow a couple of minutes for the target (10.10.155.162) to start up. Using your Python skills from Day 15 to find the correct key for the API." A link "Watch John Hammonds video on solving this task!" is also present.

To the right of the browser, a terminal window is open with the command "root@ip-10-10-215-125: ~". The terminal shows a series of API requests and responses, all of which return an error message: "Error. Key not valid!". The responses are as follows:

```
API Key: 43 [{"item_id":43,"q":"Error. Key not valid!"}]  
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":"Error. Key not valid!"}]  
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!"}]
```

The terminal window has a status bar at the bottom indicating "THM AttackBox" and "1h 26m 40s".

Thought Process/Methodology:

As for question 1, simply type in nmap (ip address) and run to get the port number for the web server. For question 2, go to firefox n type in (ip address : port number) to get the template that has been used for Santa's Tracking System. Next, for question 3, go to the template as in question 2 and right click on that page and search for view page source to find out the directory for API as per highlighted above. As for question 4, to find the RAW data type in the code in nano key.py as above and go to firefox and type in (ip address/api/57) to find the RAW data. For question 5 and 6 , type in the code as above and enter python3 key.py to find where was Santa as well as the correct API key(which is an odd number between 1-100).

Day 17: Reverse Engineering] ReverseELFneering

Tools used: THM Attackbox

Solution/walkthrough:

Question 1

Match the data type with the size in bytes:

3. Register me this, register me that...

The core of assembly language involves using registers to do the following:

- Transfer data between memory and register, and vice versa
- Perform arithmetic operations on registers and data
- Transfer control to other parts of the program Since the architecture is x86-64, the registers are 64 bit and Intel has a list of 16 registers:

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

When dealing with memory manipulation using registers, there are other cases to be considered:

- (Rb, Ri) = MemoryLocation[Rb + Ri]
- D(Rb, Ri) = MemoryLocation[Rb + Ri + D]
- (Rb, Ri, S) = MemoryLocation(Rb + S * Ri)
- D(Rb, Ri, S) = MemoryLocation[Rb + S * Ri + D]

Question 2

What is the command to analyse the program in radare2?

The best way to actually start explaining assembly is by diving in. We'll be using `radare2` to do this - `radare2` is a framework for reverse engineering and analysing binaries. It can be used to disassemble binaries(translate machine code to assembly, which is actually readable) and debug said binaries(by allowing a user to step through the execution and view the state of the program).

Luckily for us, everything we need has been provided to you via an Instance that you can deploy and log into:

1. Press the "Deploy" button on the top-right of this task
2. Wait for the IP address of the target Instance to display
3. Log into your Instance using the following information:

IP Address: **10.10.96.155**

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*'t be happening like so:

```
ashu@ashu-Inspiron-5379:~/T/c/christmas-re> ./file1
the value of a is 4, the value of b is 5 and the value of c is 9
```

The above program shows that there are 3 variables(a, b, c) where c is the sum of a and b.

```
elfmceager@tbfc-day-17:~$ ls
challenge1  file1
elfmceager@tbfc-day-17:~$ ls - lsa
ls: cannot access '-': No such file or directory
ls: cannot access 'lsa': No such file or directory
elfmceager@tbfc-day-17:~$ ls -lSa
total 1684
        4 drwxr-xr-x 4 elfmceager elfmceager    4096 Dec 16  2020 .
        4 drwxr-xr-x 3 root      root          4096 Dec 16  2020 ..
        0 lrwxrwxrwx 1 elfmceager elfmceager     9 Dec 16  2020 .bash_hist
        4 -rw-r--r-- 1 elfmceager elfmceager   220 Apr  4  2018 .bash_logo
ut
        4 -rw-r--r-- 1 elfmceager elfmceager   3771 Apr  4  2018 .bashrc
        4 drwx----- 2 elfmceager elfmceager  4096 Dec 16  2020 .cache
828 -wxr-xr-x 1 elfmceager elfmceager 844648 Dec 16  2020 challenge1
828 -wxr-xr-x 1 elfmceager elfmceager 844736 Dec 16  2020 file1
        4 drwx----- 3 elfmceager elfmceager  4096 Dec 16  2020 .gnupg
        4 -rw-r--r-- 1 elfmceager elfmceager   807 Apr  4  2018 .profile
        0 -rw-r--r-- 1 elfmceager elfmceager     0 Dec 16  2020 .sudo_as_a
dmin_successful
elfmceager@tbfc-day-17:~$ ./file1
the value of a is 4, the value of b is 5 and the value of c is 9
elfmceager@tbfc-day-17:~$
```

THM AttackBox 1h 50m 26s

The best way to actually start explaining assembly is by diving in. We'll be using **radare2** to do this - **radare2** is a framework for reverse engineering and analysing binaries. It can be used to disassemble binaries(translate machine code to assembly, which is actually readable) and debug said binaries(by allowing a user to step through the execution and view the state of the program).

Luckily for us, everything we need has been provided to you via an Instance that you can deploy and log into:

1. Press the "Deploy" button on the top-right of this task
2. Wait for the IP address of the target Instance to display
3. Log into your Instance using the following information:

IP Address: **10.10.96.155**

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 ~/U/c/christmas-re> ./file1
the value of a is 4, the value of b is 5 and the value of c is 9
```

The above program shows that there are 3 variables(a, b, c) where c is the sum of a and b.

The command to analyse the program in radare2 is aa.

Question 3

What is the command to set a breakpoint in radare2?

The screenshot shows a browser window with several tabs open. The active tab is 'tryhackme.com/room/learncyberin25days'. On the left, there's a challenge section with instructions:

2. use `ds` to move through instructions and check the values of registers and memory
3. If you make a mistake, you can always reload the program using the `ood` command

Below these instructions is a link: "You may find this [radare2 cheatsheet](#) useful in your adventures..."

6. Challenge

Use your new-found knowledge of Radare2 to analyse the "challenge1" file in the Instance **10.10.34.229** 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

The right side of the screenshot shows a terminal window titled "App" with the command `db 0x00400b55` entered. The output shows assembly code for the `main` function, with the instruction at address `0x00400b55` highlighted in red. The assembly code includes local variables `local_ch`, `local_8h`, and `local_4h`.

At the bottom of the terminal window, it says "THM AttackBox" and shows a timer: "32m 48s".

The command to set a breakpoint in radare2 is **db 0x00400b55**.

Question 4

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

The screenshot shows a browser window with several tabs open. The active tab is 'tryhackme.com/room/learncyberin25days'. The page contains instructions for using Radare2, a link to a cheatsheet, and a challenge section. The challenge asks to analyze a file named 'challenge1' attached to the task. Below the challenge are three questions with answer input fields and 'Correct Answer' buttons.

Challenge Instructions:

2. use `ds` to move through instructions and check the values of registers and memory
3. If you make a mistake, you can always reload the program using the `ood` command

You may find this [radare2 cheatsheet](#) useful in your adventures...

6. Challenge

Use your new-found knowledge of Radare2 to analyse the "challenge1" file in the Instance **10.10.34.229** 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

The terminal window on the right shows assembly code for the 'main' function of 'challenge1'. It includes comments for local variables and sections like .data and .text. A breakpoint is set at address 400b55. The assembly code includes instructions for pushing rbp, mov rbp, rsp, and various moves and adds involving eax, edx, and local_4h.

The command to execute the program until hit the breakpoint is **dc**.

Question 5

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

The screenshot shows a browser window with several tabs open. The active tab is a challenge page from tryhackme.com. The challenge asks about the value of local_ch when its corresponding movl instruction is called (first if multiple). It provides three hints:

2. use ds to move through instructions and check the values of register and memory
3. if you make a mistake, you can always reload the program using the `od` command

Below the hints, a link to a Radare2 cheatsheet is provided.

6. Challenge

Use your new-found knowledge of Radare2 to analyse the "challenge1" file in the Instance `10.10.34.229` 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

To the right of the browser is a terminal window titled "App" showing a root shell on an Ubuntu 18.04.5 LTS system. The user has run commands to echo "10.10.34.229" into a target.txt file, cat the file, and ssh into the box. They also checked system information and tried to connect to changelogs.ubuntu.com.

The screenshot shows a browser window with several tabs open. The active tab is a challenge page from tryhackme.com. The challenge asks about the value of local_ch when its corresponding movl instruction is called (first if multiple). It provides three hints:

2. use ds to move through instructions and check the values of register and memory
3. if you make a mistake, you can always reload the program using the `od` command

Below the hints, a link to a Radare2 cheatsheet is provided.

6. Challenge

Use your new-found knowledge of Radare2 to analyse the "challenge1" file in the Instance `10.10.34.229` 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

To the right of the browser is a terminal window titled "App" showing a root shell on an Ubuntu 18.04.5 LTS system. The user has run ls, l -ls, and ./challenge1. They also attempted to attach to PID 2054.

You may find this [radare2 cheatsheet](#) useful in your adventures...

6. Challenge

Use your new-found knowledge of Radare2 to analyse the "challenge1" file in the instance **10.10.34.229** 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

Task 20 [Day 18] Reverse Engineering The Bits of Christmas 29m 38s

The value of local_ch when its corresponding movl instruction is called 1

Question 6

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

You may find this [radare2 cheatsheet](#) useful in your adventures...

6. Challenge

Use your new-found knowledge of Radare2 to analyse the "challenge1" file in the Instance **10.10.34.229** 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

Task 20 [Day 18] Reverse Engineering The Bits of Christmas 29m 38s

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?

The screenshot shows a browser window with several tabs open. The active tab is 'tryhackme.com/room/learnCyberIn25days'. The page contains instructions for using radare2, a link to a cheatsheet, and a challenge section for question 6. The challenge asks to analyze the 'challenge1' file attached to the task. A terminal window titled 'elfmceager@tbfc-day-17: ~' is running radare2 on the file. The terminal output shows assembly code and command history related to analyzing the program. The browser task bar at the bottom indicates 'Task 20 [Day 18] Reverse Engineering: The Bits of Christmas'.

The value of local_4h before eax is set to 0 is 6.

Thought Process/Methodology:

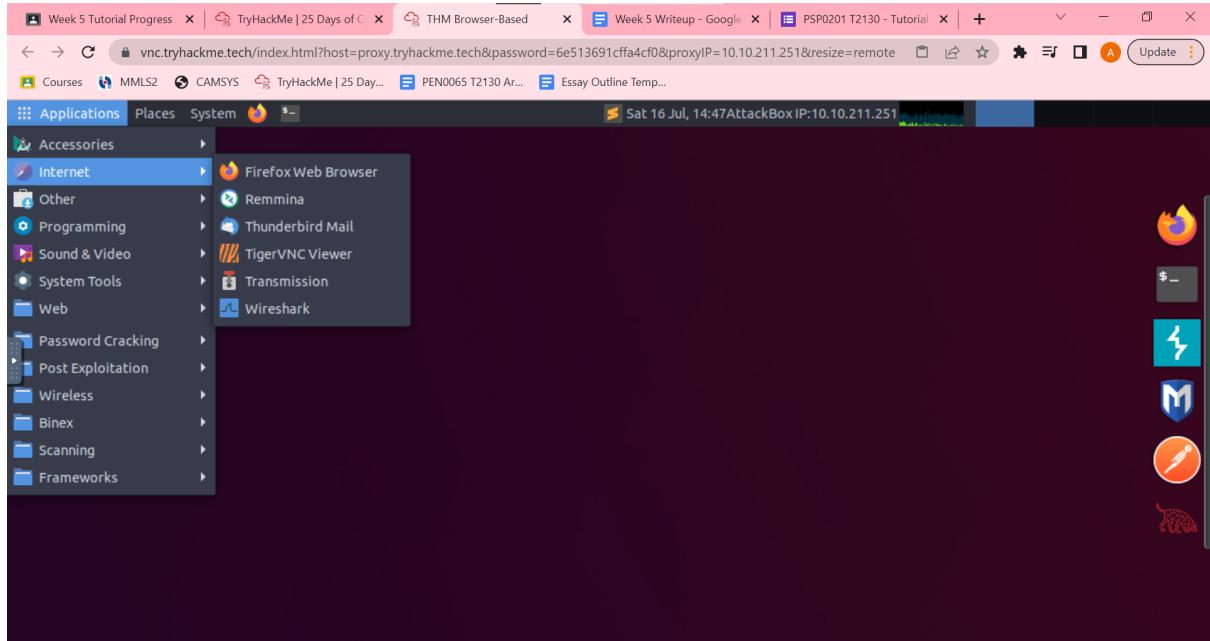
As for question 1, the data types is as above . For question 2, to find the command that analyse the program in radare2, simply press ssh elfmceager@(ip address), ls, ls -lisa , ./file1, r2 -d ./file 1 and lastly press aa. Next for question 3, press afl | grep main and db 0x00400b55 and pdf @main to set a breakpoint to radare2. For question 4, simply enter dc to execute the program till we hit a breakpoint. For question 5, open a new terminal and replace ./file 1 to ./challenge 1 to all 3 values which are the values of local_ch when its corresponding movl instruction is called, the value of eax when the imul instruction is called and the value of local_4h before eax is set to 0.

Day 18 : Reverse Engineering - The Bits of Christmas

Tools : Attackbox THM, Chrome

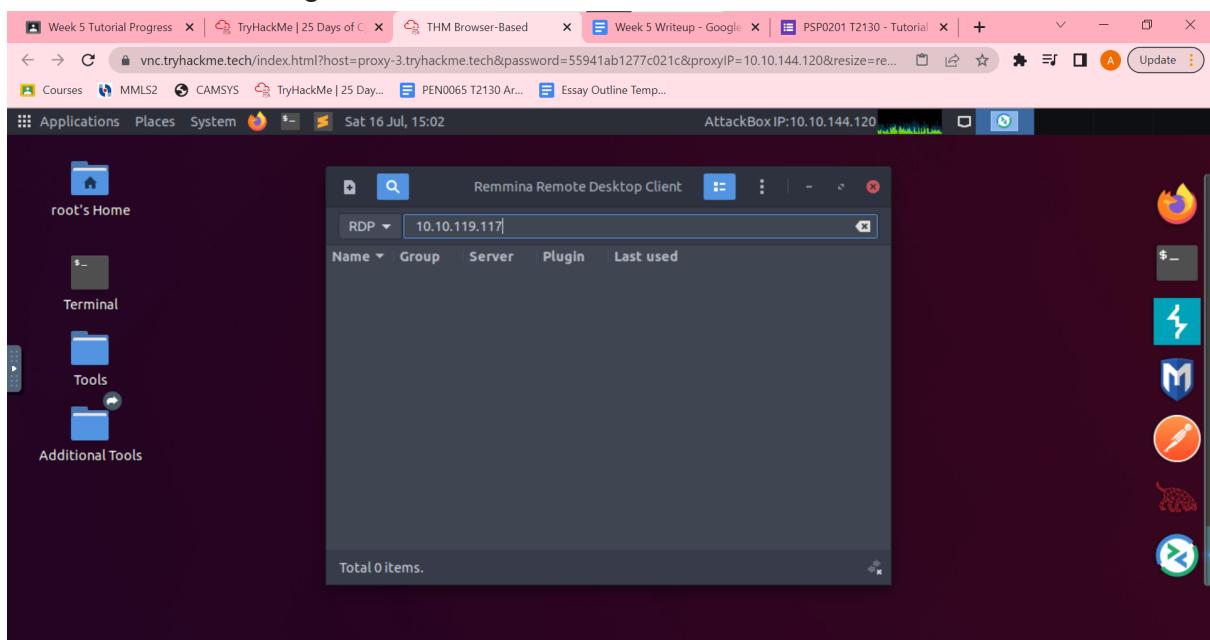
Solutions / Walkthrough :

Deploy the THM Attackbox and machine and open the application to open Remmina.

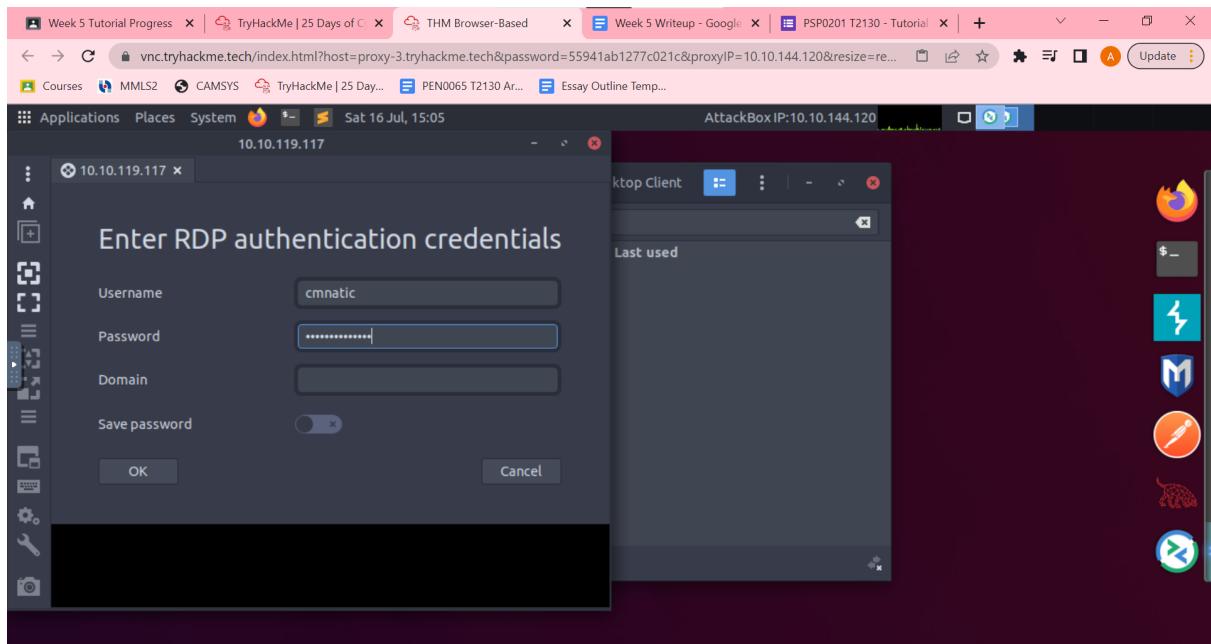


Q1: What is the message that shows up if you enter the wrong password for TBFC_APP?

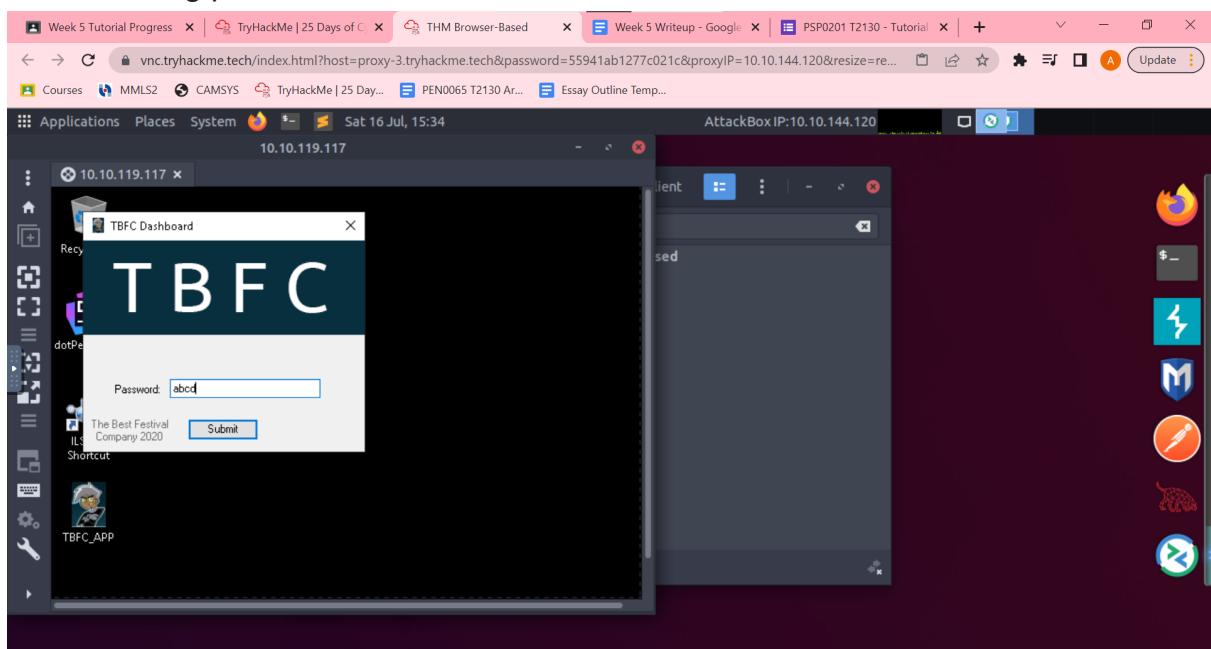
Enter the IP address given.



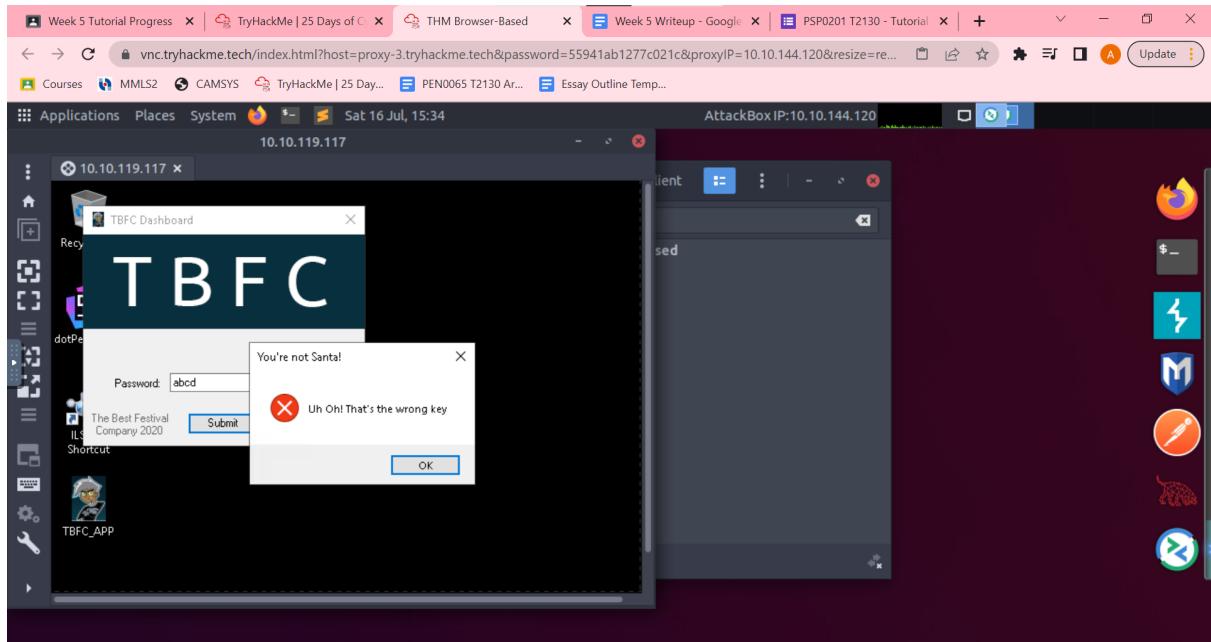
Enter the username and password.



Enter a wrong password.

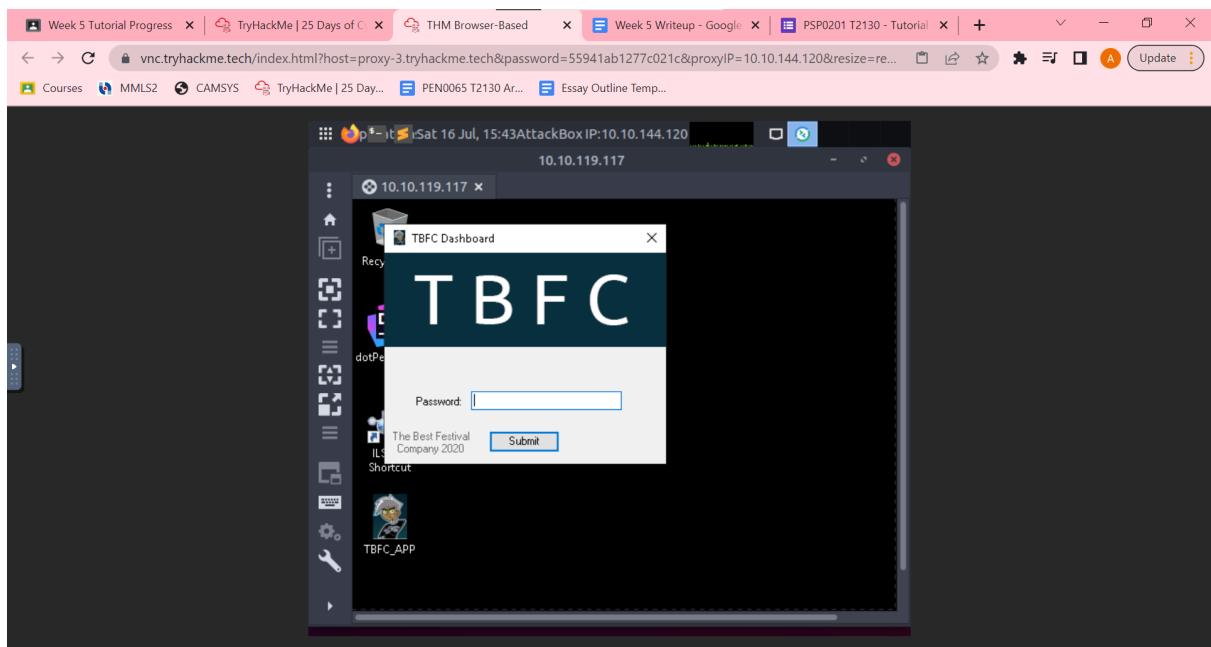


The message that shows up is Uh Oh! That's the wrong key



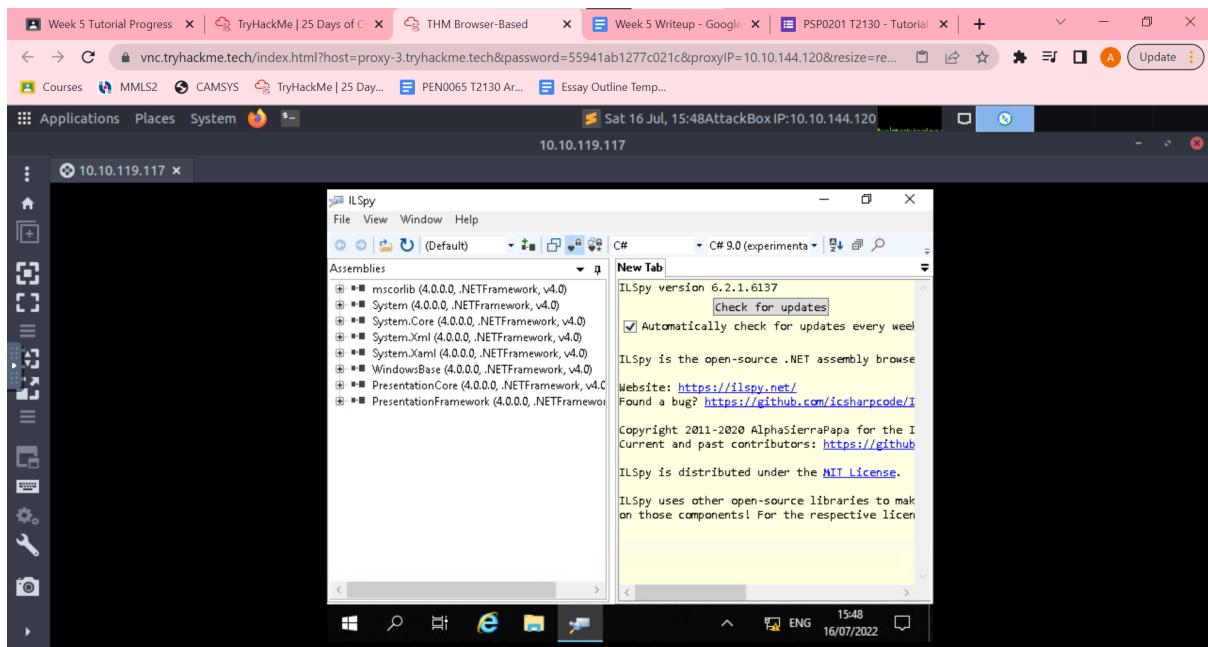
Q2: What does TBFC stand for?

The Best Festival Company

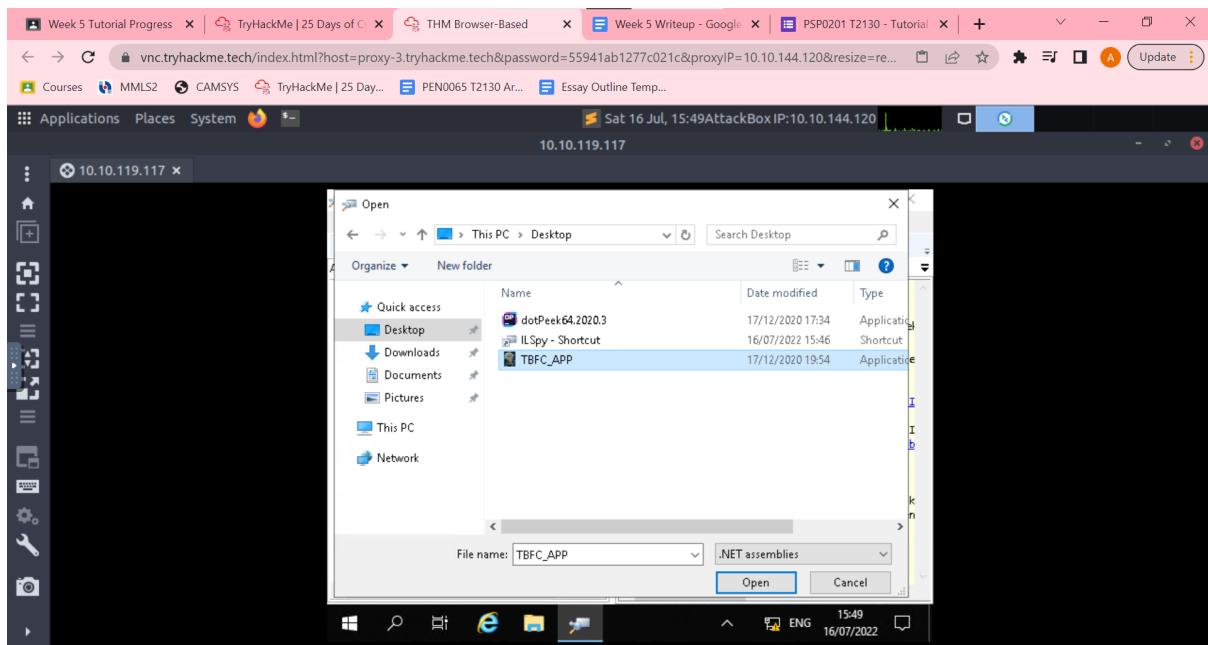


Q3: Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?

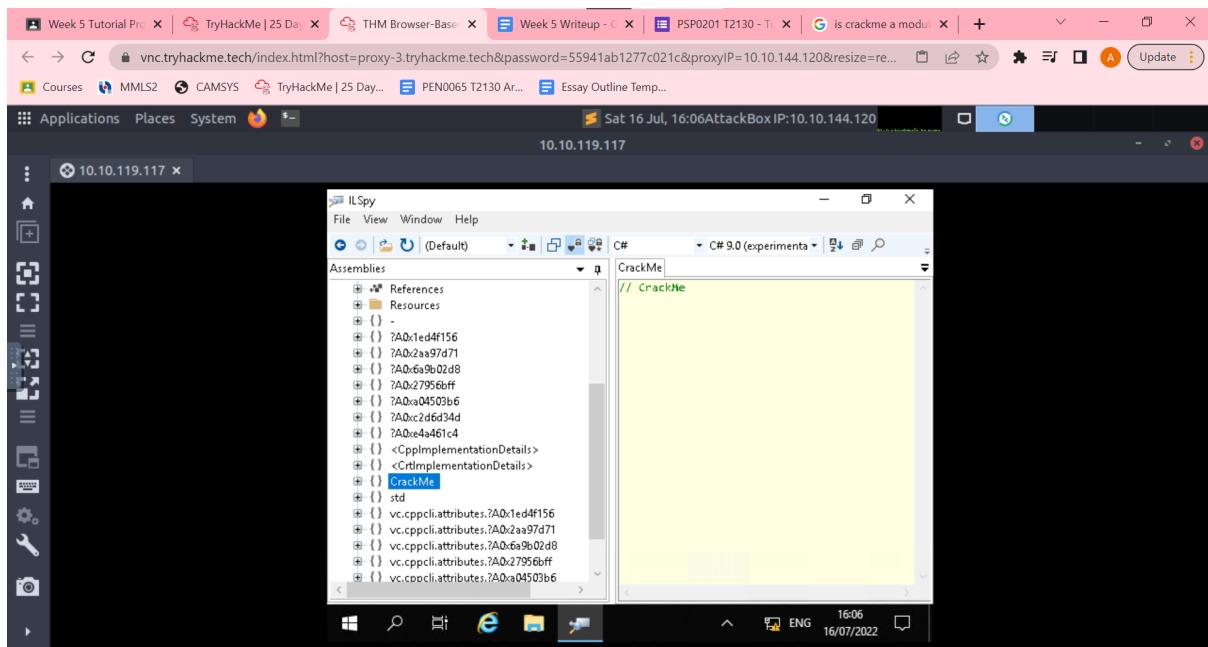
Open ILSpy



Open TBFC-App in ILSpy

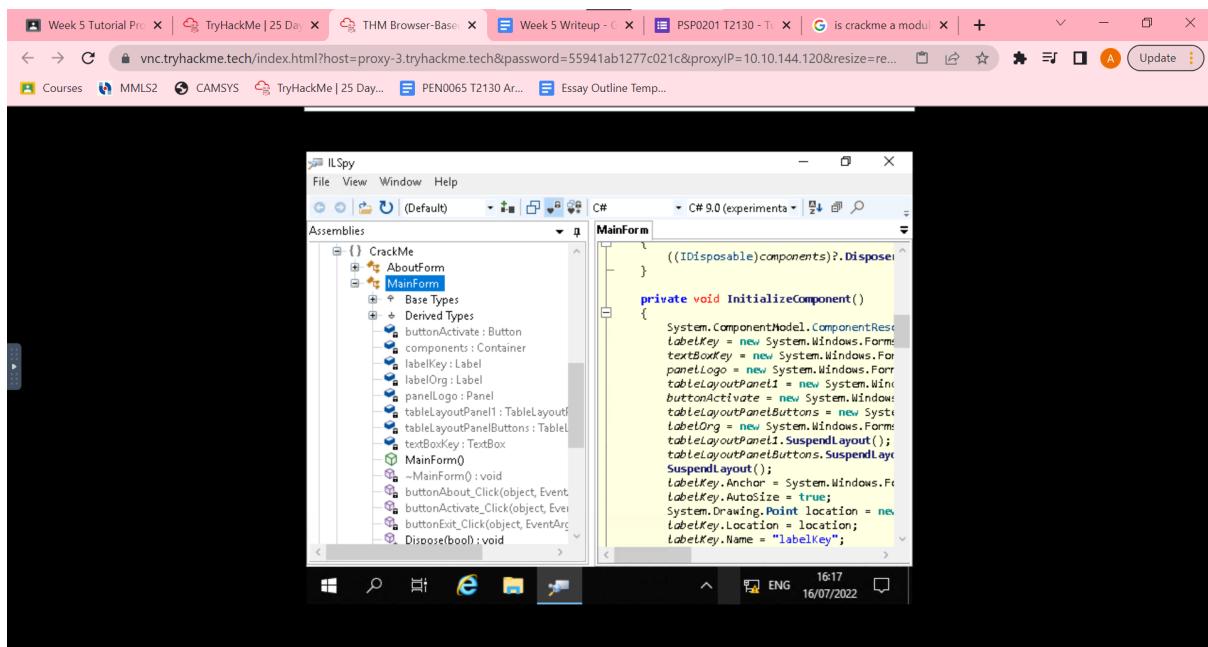


Decompile the TBFC-App and the answer is CrackMe



Q4: Within the module, there are two forms. Which contains the information we are looking for?

MainForm



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

buttonActivate_Click

The screenshot shows the IL Spy application interface. The left pane displays the assembly structure for the 'CrackMe' module, including types like MainForm, AboutForm, and various derived types. The right pane shows the decompiled C# code for the `buttonActivate_Click` event handler. The code uses unsafe pointers to manipulate memory, specifically comparing a value at address 0x115 against a loop counter `b`. The assembly code corresponds to the decompiled C#.

```

ILSpy
File View Window Help
C# C# 9.0 (experiments)
buttonActivate_Click(object, EventArgs): void
private unsafe void buttonActivate_Click(object
{
    IntPtr value = Marshal.StringToGlobalAllocAnsi("Santa");
    byte* ptr = (byte*)System.Runtime.InteropServices.Marshal.PtrToStringAnsi(value);
    void* ptr2 = (void*)value;
    byte b = *(byte*)ptr;
    byte b2 = 115;
    if ((uint)b >= 115u)
    {
        while ((uint)b < (uint)b2)
        {
            if (b != 0)
            {
                ptr2 = (byte*)ptr2 + 1;
                ptr += 1;
                b = *(byte*)ptr2;
                b2 = *(byte*)(ptr);
                if ((uint)b < (uint)b2)
                    r
}
}
}
}

```

Q6: What is Santa's password?

Copy the hexadecimal number from

<Module>.??_C@_0BB@!KKDFEPPG@santapassword321@

The screenshot shows the IL Spy application interface. The left pane displays the assembly structure for a different module, listing various Windows kernel structures like _TOKEN_TYPE, _TP_CALLBACK_ENVIRON_V3, etc. The right pane shows the decompiled C# code for a constructor or static initializer. It contains a string literal `t supported: data(73 61 6E 74 61 70 61 73 73)`, which is likely the password in hex format.

```

ILSpy
File View Window Help
C# C# 9.0 (experiments)
<Module> ??_C@_0BB@!KKDFEPPG@santapassword321@ {
    t supported: data(73 61 6E 74 61 70 61 73 73)
}

```

Paste into Cyberchef and the password santapassword321

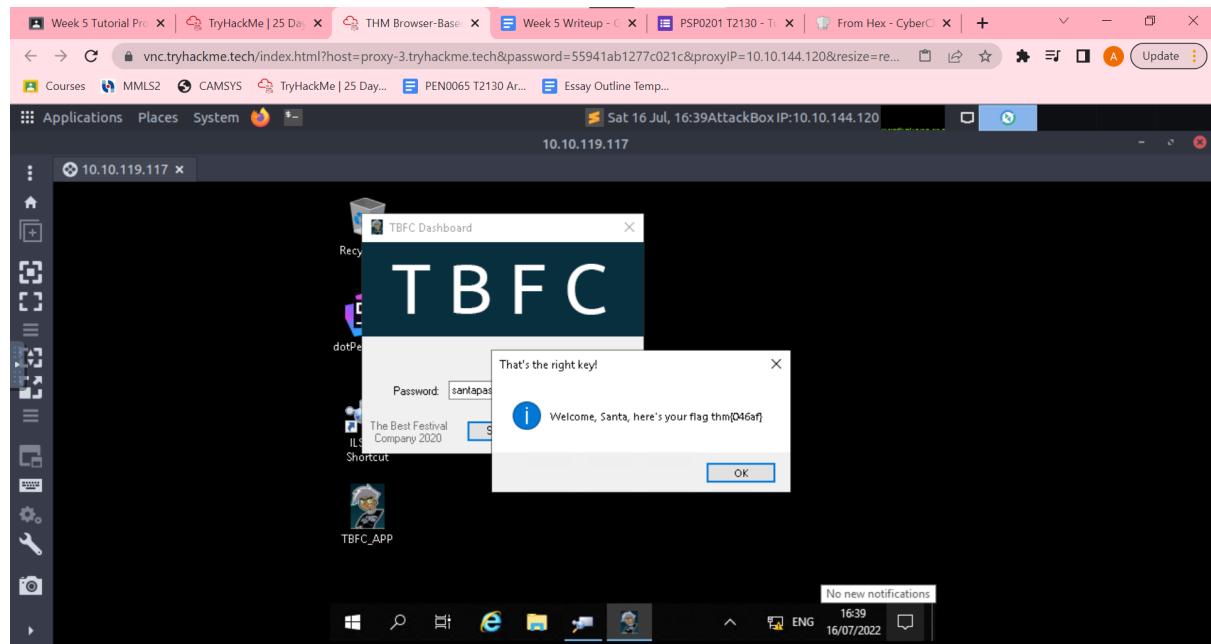
The screenshot shows the CyberChef interface. In the 'Input' section, the hex bytes `73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31` are pasted. The 'From Hex' recipe is selected. In the 'Output' section, the resulting password `santapassword321` is shown.

Q7: Now that you've retrieved this password, try to login...What is the flag?

Login into TBFC-App

The screenshot shows a Windows desktop environment. A browser window is open at `vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=55941ab1277c021c&proxyIP=10.10.144.120&resize=re...`. The taskbar shows the IP address `10.10.119.117`. A desktop icon for 'TBFC_APP' is visible. A tooltip for the icon reads: 'TBFC APP The Best Festival Company 2020 Shortcut'. A notification bar at the bottom right indicates 'No new notifications'.

The flag is thm{046af}



Thought Process/Methodology:

We can decompile an app through ILSpy if we open the application that we want to decompile in ILSpy. In ILSpy, we can see the modules that are inside the application that we decompiled, in this case it's TBFC. We can expand one by one module to see what is inside them. After a while of looking into each module, it is found that the CrackMe module is unique compared to others. After expanding the CrackMe module, it is found that there are 2 forms which are MainForm and AboutForm. After a while of digging up, it is found that the password for this application is in MainForm. We can then open TBFC-App and enter the password that we found.

Day 19: Web Exploitation - The Naughty or Nice List

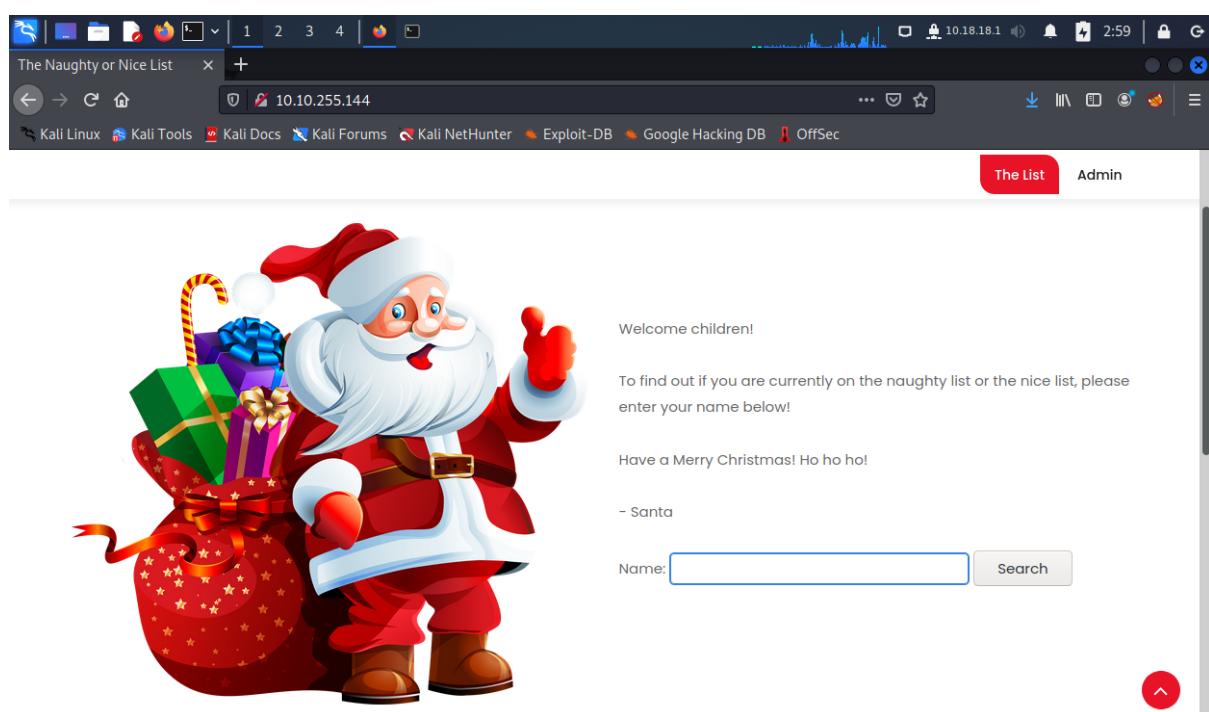
Tools used: THM Machine/Kali Linux/Mozilla Firefox

Solution/Walkthrough:

Question 1

Which list is this person on?

Deploy the machine and enter the IP address on the web browser. Insert the names so that we can know whether they are on the nice list or the naughty list.



We can see the people who are on the Nice list or the Naughty list.

Name:

YP is on the Nice List.

Name:

JJ is on the Naughty List.

Name:

Ian Chai is on the Nice List.

Name:

Kanes is on the Naughty List.

Name:

Tib3rius is on the Nice List.

Name:

Timothy is on the Naughty List.

Question 2

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

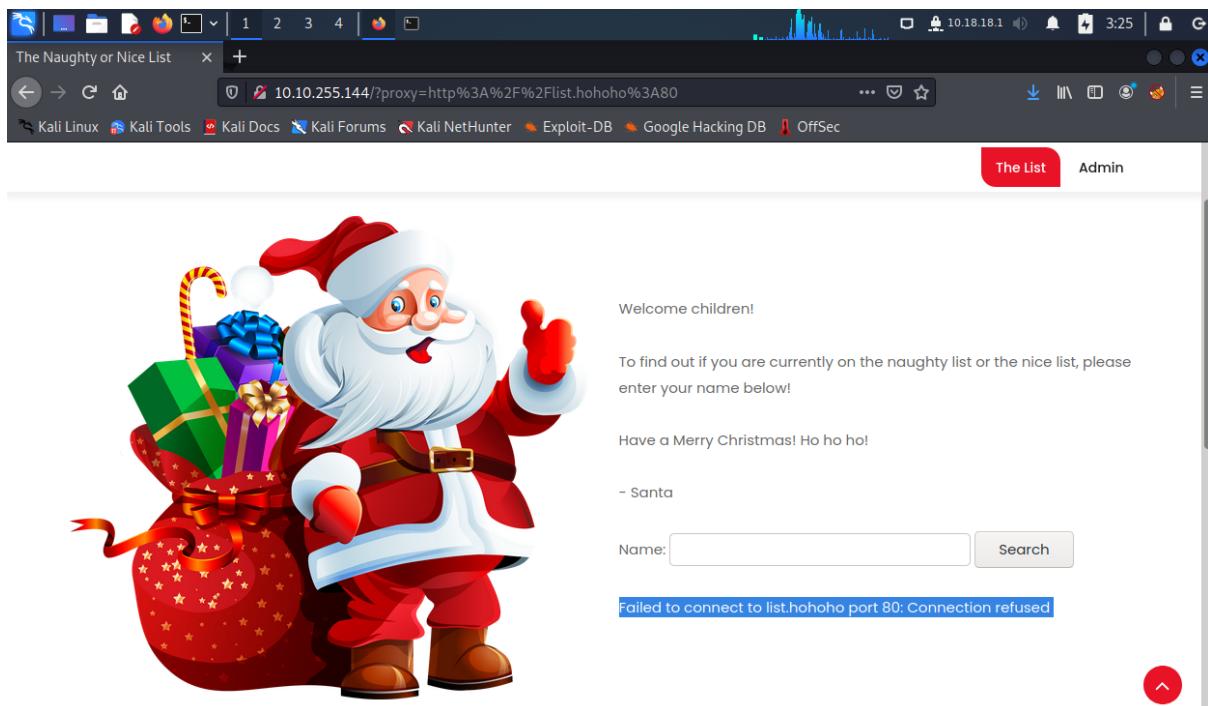
In order to see the message in the page, insert
"/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F" at the back of the IP address in the web browser. The message could be found displayed (Highlighted)

The screenshot shows a web browser window titled "The Naughty or Nice List". The URL bar contains "10.10.255.144/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F". The page features a large cartoon Santa Claus holding a bag full of wrapped gifts. To the right of Santa, there is text: "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", and a search form with a placeholder "Name:" and a "Search" button. Below the search form, the text "Not Found" is displayed, followed by the error message "The requested URL was not found on this server". A red circular arrow icon is in the bottom right corner of the browser window.

Question 3

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

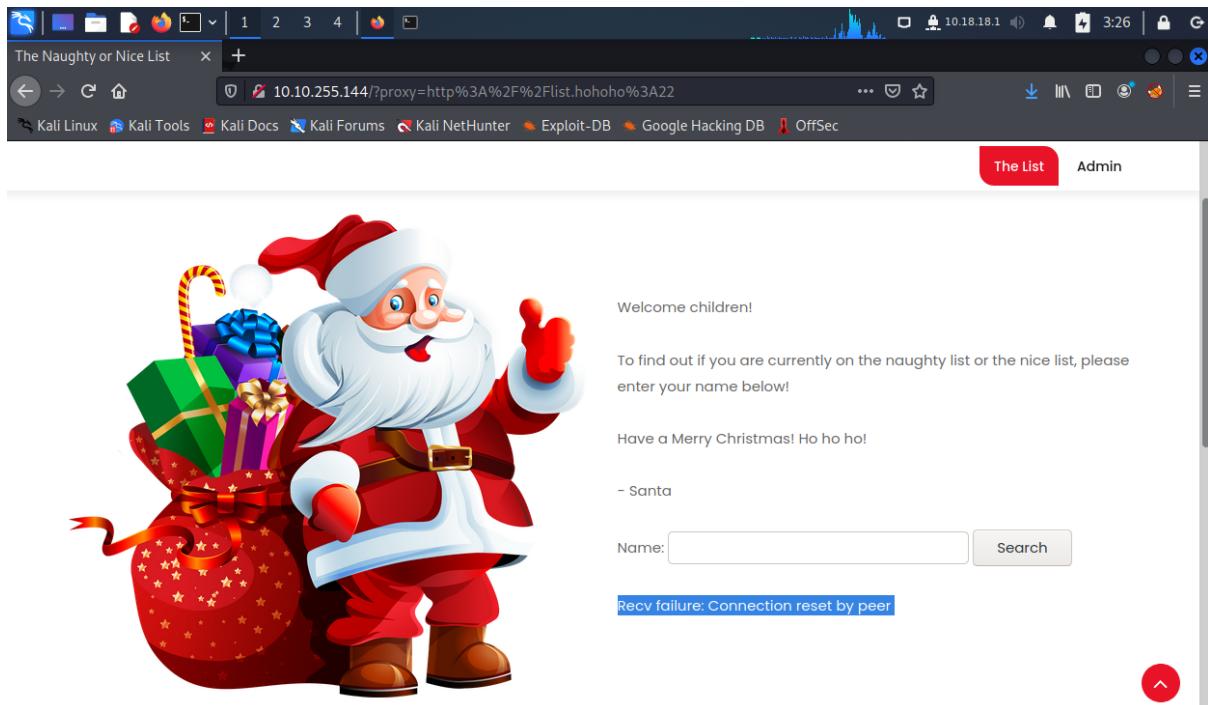
In order to see the message in the page, insert
"/?proxy=http%3A%2F%2Flist.hohoho%3A80" at the back of the IP address in the web browser. The message could be found displayed (Highlighted)



Question 4

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

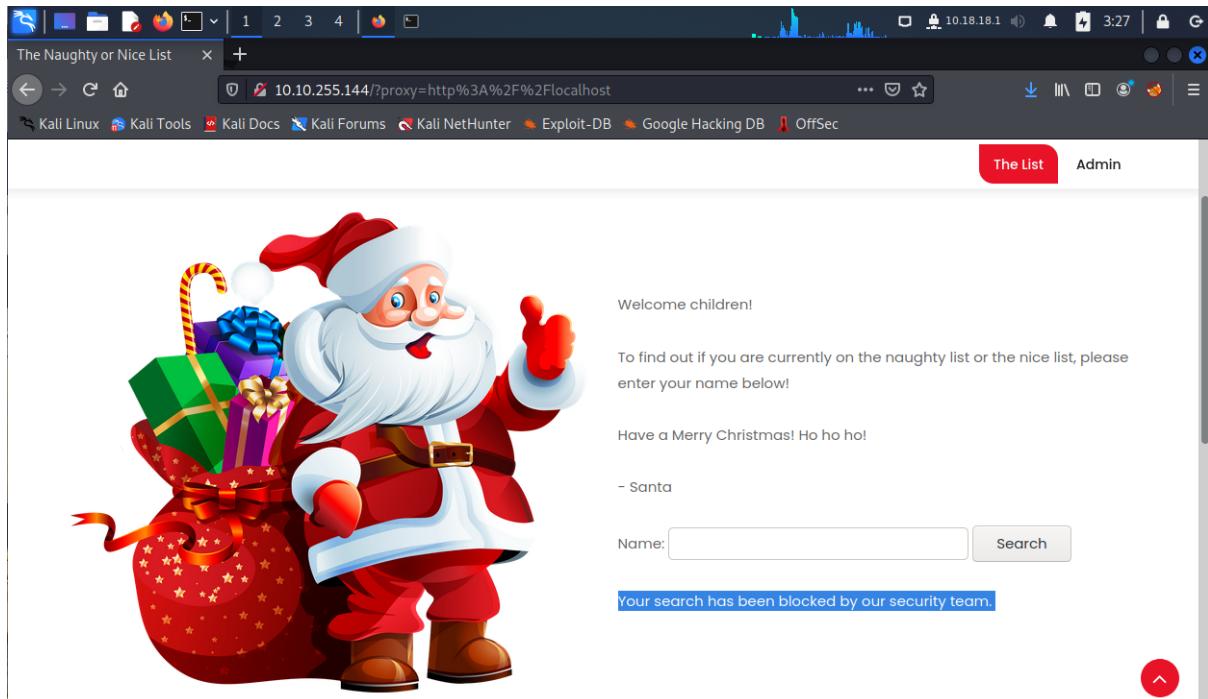
In order to see the message in the page, insert
"/?proxy=http%3A%2F%2Flist.hohoho%3A22" at the back of the IP address in the web browser. The message could be found displayed (Highlighted)



Question 5

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

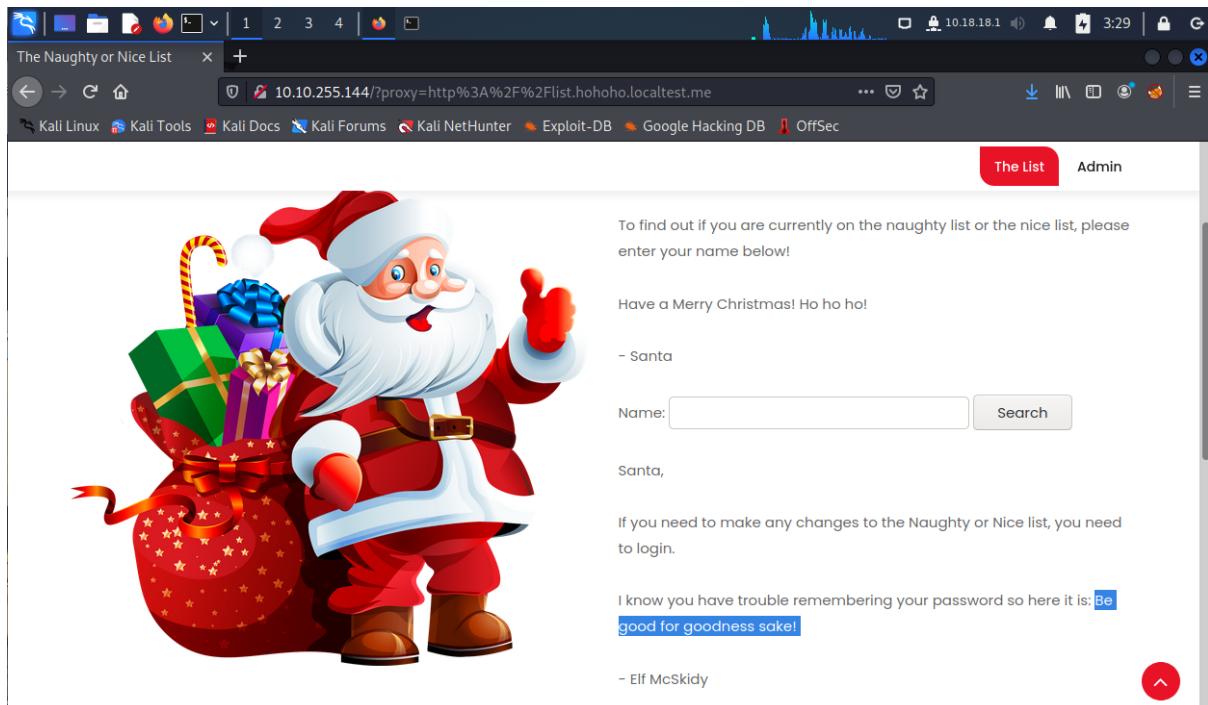
In order to see the message in the page, insert "?proxy=http%3A%2F%2Flocalhost" at the back of the IP address in the web browser. The message could be found displayed (Highlighted)



Question 6

What is Santa's password?

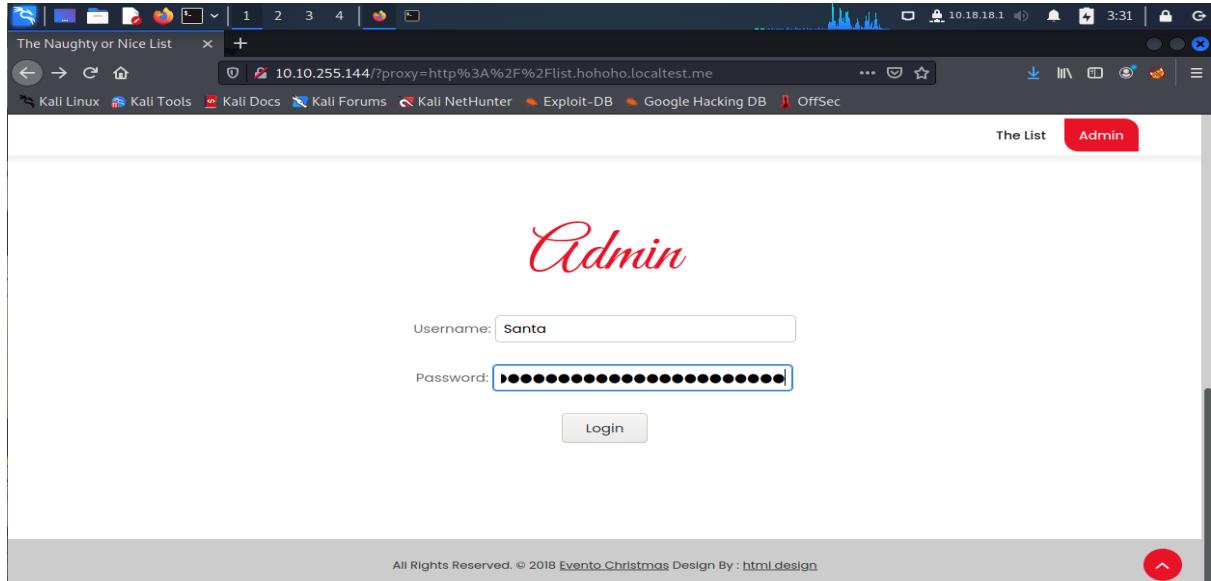
To bypass and check the local services, insert “/?proxy=http%3A%2F%2Flist.hohoho.localtest.me” at the back of the IP address in the web browser. Here we could find that the web server is running locally and there is a message left on the page. Santa’s password could be found in the message area. (Highlighted)



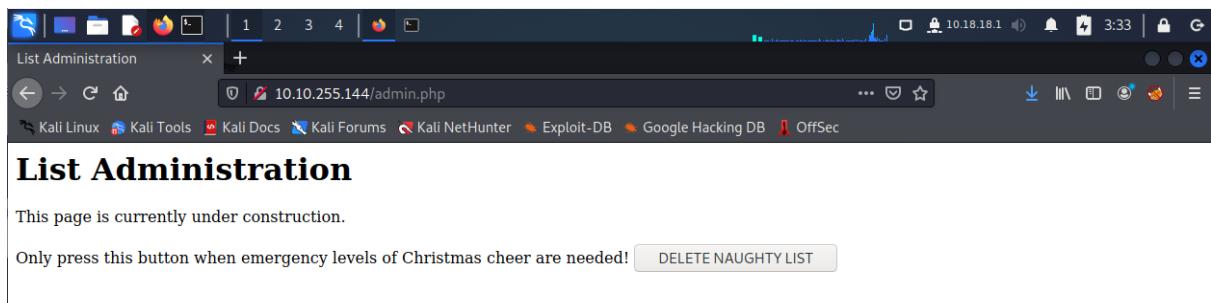
Question 7

What is the challenge flag?

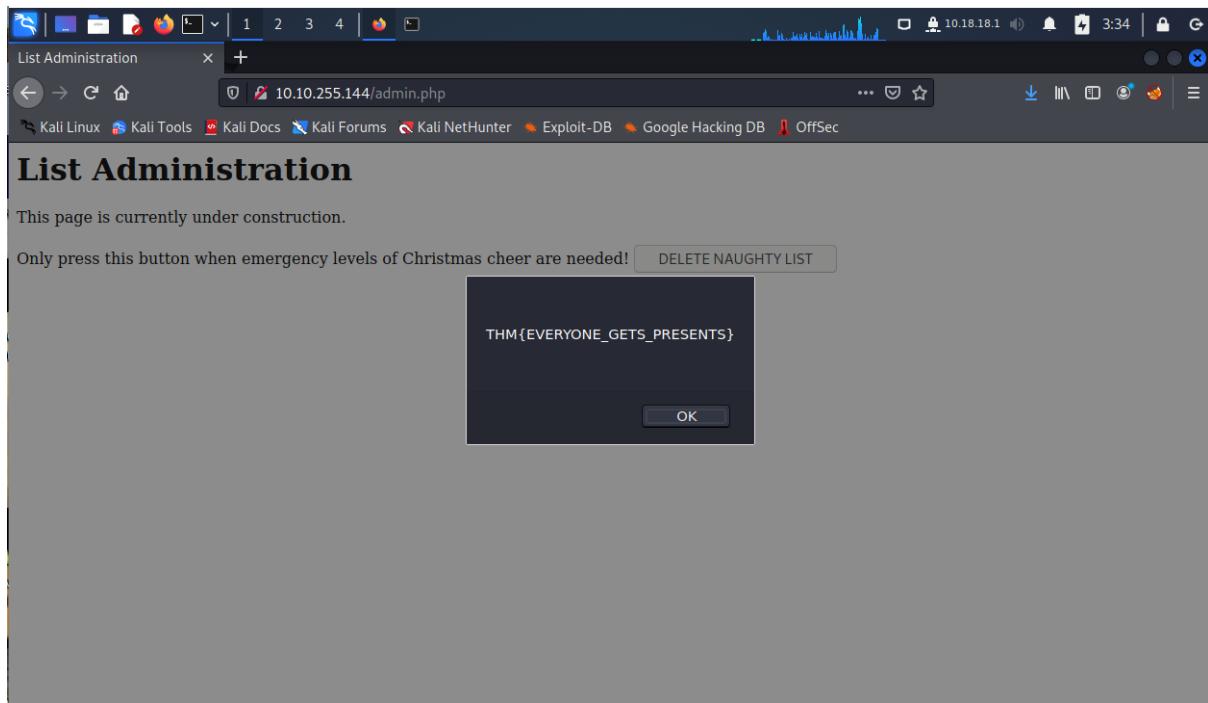
Click the “**Admin**” button on the top right corner of the page and we could find a login section to use from. Log in as Santa by using the provided credentials by entering the Username (**Santa**) and the Password (**Be good for goodness sake!**).



Looks like we have successfully logged in as Santa. We can see that this is an admin page.



To find the challenge flag, click on the button which contains the text “**DELETE NAUGHTY LIST**” and a flag will be displayed on the page.



Thought Process/Methodology:

Deploy the machine and enter the IP address on the web browser. Insert the names on the search bar so that we can know whether they are on the nice list or the naughty list. To fetch the root of the same site, insert “/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F” at the back of the IP address in the web browser. The message “**The requested URL was not found on this server.**” could be found displayed. Next, insert “/?proxy=http%3A%2F%2Flist.hohoho%3A80” at the back of the IP address in the web browser. The message “**Failed to connect to list.hohoho port 80: Connection refused**” could be found, suggesting that port 80 is not open on list.hohoho. By inserting “/?proxy=http%3A%2F%2Flist.hohoho%3A22” at the back of the IP address in the web browser, the message “**Recv failure: Connection reset by peer**” could be found displayed which suggests that port 22 is open but did not understand what was sent. Insert “/?proxy=http%3A%2F%2Flocalhost” at the back of the IP address in the web browser. The message “**Your search has been blocked by our security team.**” could be found displayed. As the hostname simply needs to start with “list.hohoho” and to bypass and check the local services, insert “/?proxy=http%3A%2F%2Flist.hohoho.localtest.me” at the back of the IP address in the web browser. The web server should be running locally and there is a message left on the page by Elf McSkidy. Santa’s password could be found in the

message area. Log in as Santa on the admin page by using the provided credentials by entering the Username (**Santa**) and the Password (**Be good for goodness sake!**). On the admin page, the button which contains the text “**DELETE NAUGHTY LIST**” is shown. To find the challenge flag, click on it and a small window containing the challenge flag will appear.

Day 20: Blue Teaming - PowersELF to the rescue

Tools used: Kali Linux

Solution/Walkthrough:

Question 1:

Check the ssh manual. What does the parameter -I do?

In order to see the ssh manual, simply type in 'ssh' in the command prompt to identify the functionality of -I parameter.

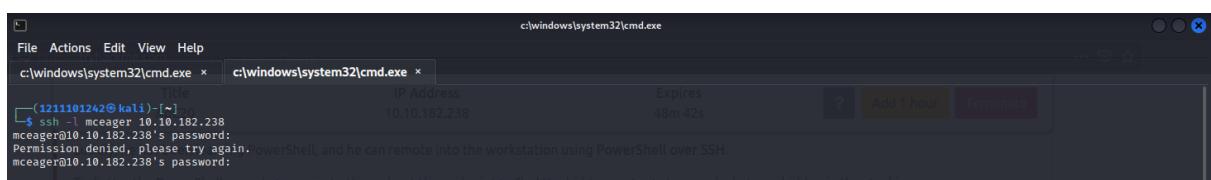


A terminal window titled '1211101242@kali:~'. The command 'ssh' is entered, followed by its usage information. The usage text includes options like '-B bind_interface', '-b bind_address', '-c cipher_spec', '-D [bind_address:]port', '-E log_file', '-e escape_char', '-F configfile', '-I pkcs11', '-i identity_file', '-l [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]', and destination [command].

Question 2:

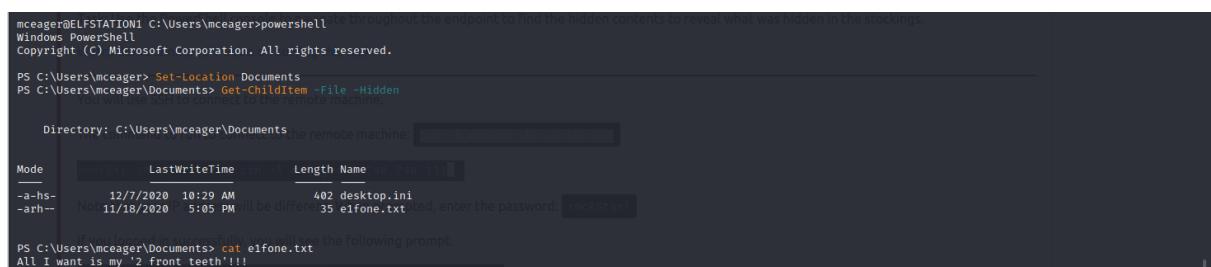
Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

Copy and paste the command given on THM into the command prompt to gain access to Mceager.



A terminal window titled '1211101242@kali:~'. The command 'ssh -l mceager 10.10.182.238' is entered. The response shows 'Permission denied, please try again.' followed by 'mceager@10.10.182.238's password:'.

Type in powershell after logging to Mceager. After doing so, type in Set-Location Documents to gain access to the Documents file. Type in Get-Children -File -Hidden to gain the name of the file needed for the question. Use cat e1fone.txt to gain access to the content of the file.



A PowerShell window titled 'Windows PowerShell' with the title bar 'c:\windows\system32\cmd.exe'. The command 'Set-Location Documents' is run, followed by 'Get-ChildItem -File -Hidden'. The output shows a table with columns 'Mode', 'LastWriteTime', 'Length', and 'Name'. One file, 'e1fone.txt', is listed with a length of 35 bytes. The command 'cat e1fone.txt' is then run, displaying the contents: '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?

Use “cd ..” to go back to the main page and proceed with using “Set-Location .\Desktop\” to gain access to Mceager’s Desktop. Use “ls” and “ls -Hidden” to gain access to the files available in Mceager’s Desktop. Use cd .\elf2wo\ and use “Get-ChildItem” to gain access to the files under elf2wo. Use cat e70smsW10Y4k.txt to gain access to the content of the file.

The screenshot shows a Windows PowerShell window titled 'c:\windows\system32\cmd.exe - powershell'. The session starts with 'PS C:\Users\mceager\Documents> cd ..' followed by 'PS C:\Users\mceager> Set-Location .\Desktop\'. Then, 'ls' and 'ls -Hidden' commands are run to list files. The output shows a hidden folder named 'elf2wo' and a file named 'desktop.ini'. Next, 'cd .\elf2wo\' is entered, followed by 'Get-ChildItem'. The output lists a file named 'e70smsW10Y4k.txt'. Finally, 'cat e70smsW10Y4k.txt' is run, displaying the text 'I want the movie Scrooged <3!'. The PowerShell interface includes tabs for 'File', 'Actions', 'Edit', 'View', and 'Help', and status bars for 'IP Address' (10.10.182.238), 'Expires' (22m 44s), and connection details.

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)

Use cd :\Windows to go to Mceager’s Windows

```
PS C:\Users\mceager\Desktop\elf2wo> cd C:\Windows  
PS C:\Windows>
```

Use cd System32 to go to Windows’s System32

```
PS C:\Windows> cd System32  
PS C:\Windows\System32> ls
```

Use the following command to gain access to the hidden folder for Elf 3

```
PS C:\Windows\System32> Get-ChildItem -Hidden -Directory -Filter "*3*"
Directory: C:\Windows\System32\3lfthr3e

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

Question 5:

How many words does the first file contain?

Continue the work from previous question by typing in cd 3lfthr3e go into its path. After doing so, use “Get-ChildItem -Hidden” to gain access to the files available under 3lfthr3e. In order to identify the word count, use “Get-Content 1.txt | Measure-Object”. It should be 9999 as shown in the image below.

```
PS C:\Windows\System32> cd 3lfthr3e
PS C:\Windows\System32\3lfthr3e> Get-ChildItem -Hidden
Directory: C:\Windows\System32\3lfthr3e

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

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

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

Question 6:

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

Use the following command “(Get-Content 1.txt)[551,6991]” to gain the words at the specific index given in the question.

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

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)

Use the following command “Get-Content 2.txt | Select-String -Pattern "redryder"” to get the answer.

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

Thought Process/Methodology:

As for question 1, in order to see the ssh manual, simply type in 'ssh' in the command prompt to identify the functionality of -l parameter. As for question 2, start off by coping and pasting the command given on THM into the command prompt to gain access to Mceager. After doing so, proceed by typing in powershell after logging to Mceager. Next, type in Set-Location Documents to gain access to the Documents file. The final step for this question can be done by continuing to type in Get-Children -File -Hidden to gain the name of the file needed for the question. Use cat e1fone.txt to gain access to the content of the file. As for question 3, use "cd .." to go back to the main page and proceed with using "Set-Location .\Desktop\" to gain access to Mceager's Desktop. Use "ls" and "ls -Hidden" to gain access to the files available in Mceager's Desktop. Use cd .\elf2wo\ and use "Get-ChildItem" to gain access to the files under elf2wo. Use cat e70smsW10Y4k.txt to gain access to the content of the file. As for question 4, use cd :\Windows to go to Mceager's Windows and then use cd System32 to go to Windows's System32 follow up by using the following command to gain access to the hidden folder for Elf 3 which is "Get-ChildItem -Hidden -Directory -Filter "*3*". As for question 5, continue the work from previous question by typing in cd 3lfthr3e go into its path. After doing so, use "Get-ChildItem -Hidden" to gain access to the files available under 3lfthr3e. In order to identify the word count, use "Get-Content 1.txt | Measure-Object". It should be 9999 as shown in the image below. As for question 6, use the following command "(Get-Content 1.txt)[551,6991]" to gain the words at the specific index given in the question. Lastly, as for question 7, use the following command "Get-Content 2.txt | Select-String -Pattern "redryder"" to get the answer.