PSP0201

Week 5

Write-up

Group Name: **PennCake**

ID	Name	Role
1211103144	Vaarindran Nyenasegran	Leader
1211103222	Asyrani Syazwan Yuhanis	Member
1211104230	Nur Aisyah Nabila Nahar	Member
1211101169	Tengku Alyssa Sabrina Tengku Erwin Martino	Member

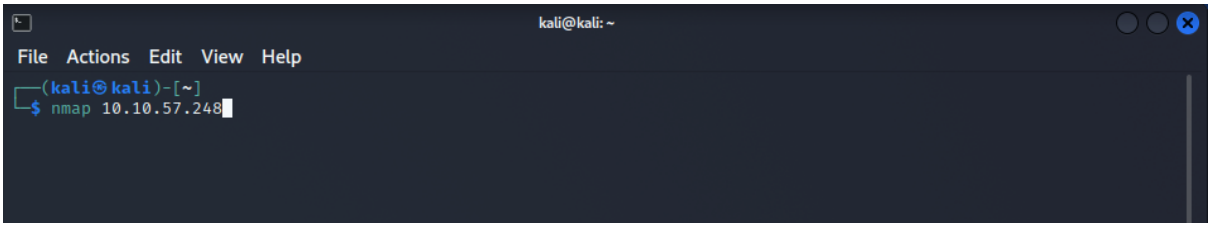
Day 16: Scripting - Help! Where is Santa?

Tools used: Kali Linux, Terminal, Mozilla Firefox

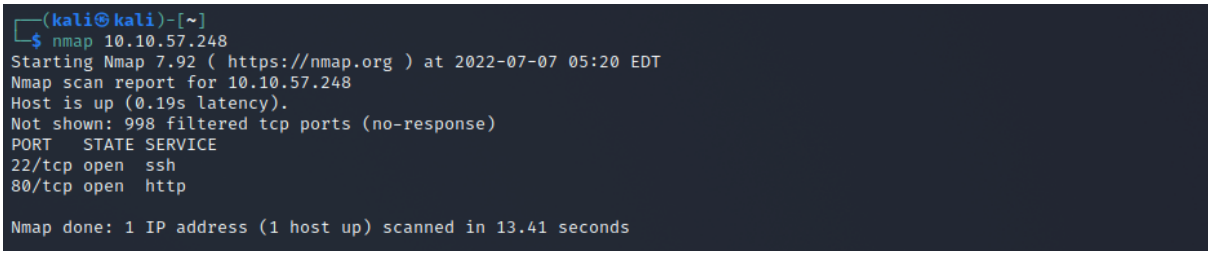
Solution/walkthrough:

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

Firstly, we need to set up nmap for the target IP Address. We can set it up by using the following command.



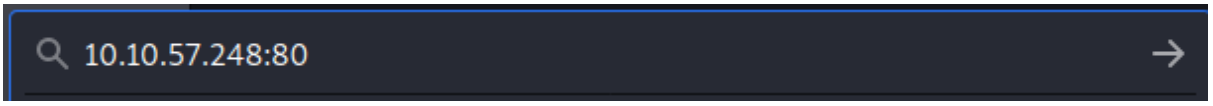
Wait for a bit and the port will be shown to us. From there, we can see that port **80** is for a **http** service.



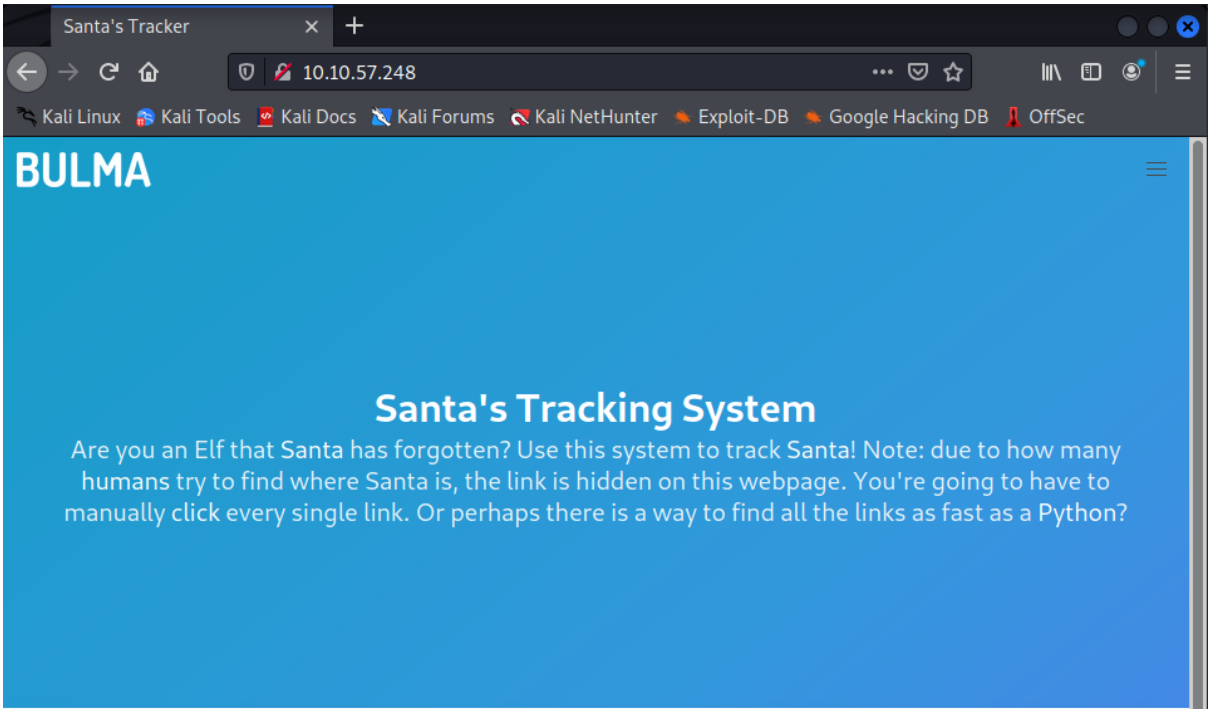
Answer: 80

Question 2:What templates are being used?

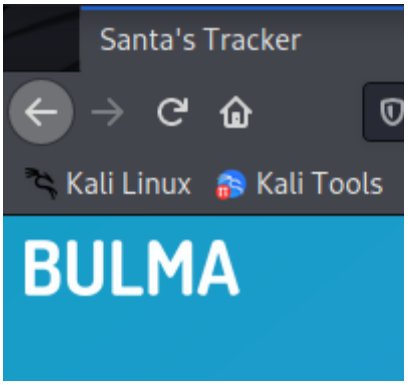
Enter the IP address with the port we want to use to access the website that we want to go to.



We will be brought to a website called “Santa’s Tracker”.



On the corner of the website, the template that it used is **BULMA**.



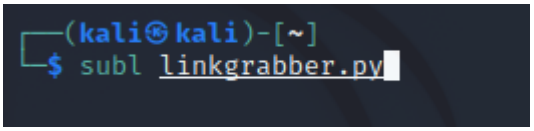
Answer: BULMA

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

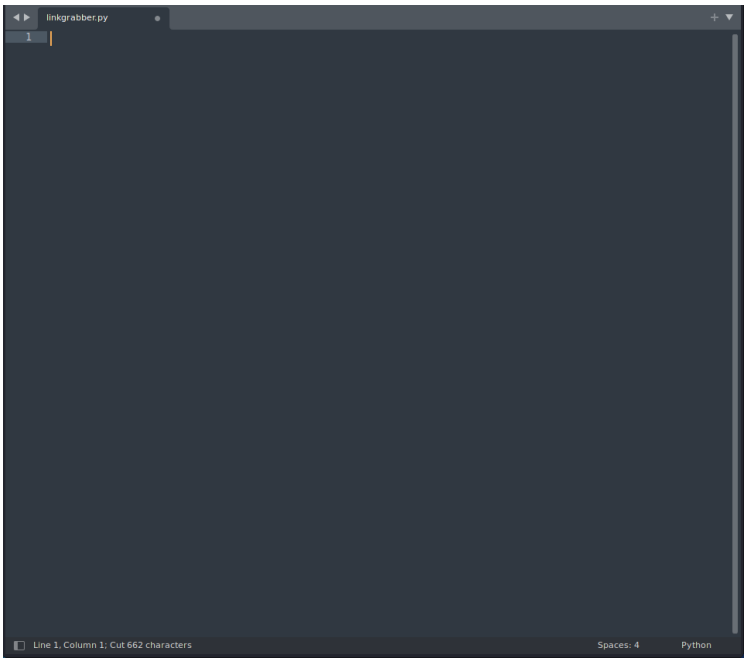
From the Python script from Day 15, we can reuse it and help us find the directory.

```
# Import the libraries we downloaded earlier
# if you try importing without installing them, this step will fail
from bs4 import BeautifulSoup
import requests

# replace testurl.com with the url you want to use.
# requests.get downloads the webpage and stores it as a variable
html = requests.get('testurl.com')

# this parses the webpage into something that beautifulsoup can read over
soup = BeautifulSoup(html, "lxml")
# lxml is just the parser for reading the html

# this is the line that grabs all the links # stores all the links in the links variable
links = soup.find_all('a href')
for link in links:
    # prints each link
    print(link)
```

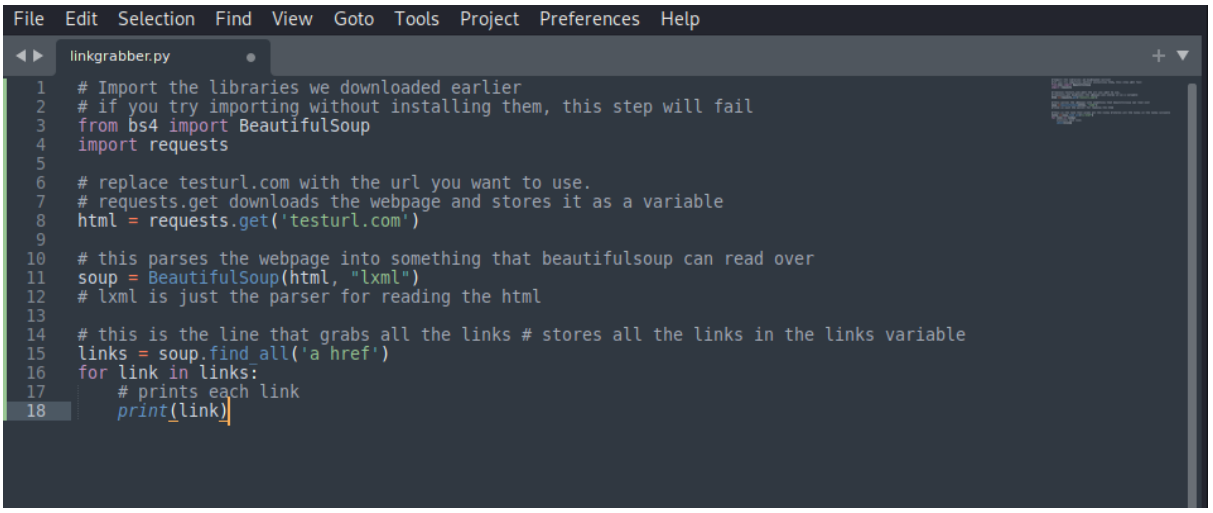
We need to paste the script into a sublime text editor. So we can use the command **subl** and the name, we also need to make sure it's a Python file by putting **.py** in the end of the name.



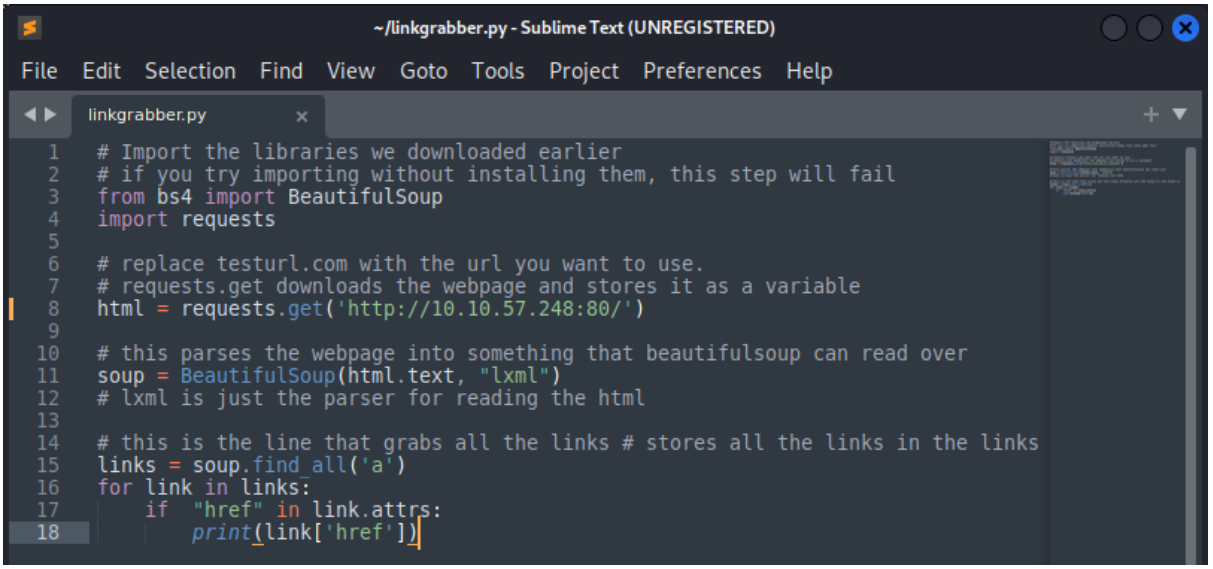
It will open a sublime text editor tab.



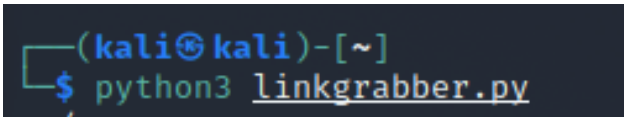
Then, we can paste the Python script into it.



Now, we need to change the script a bit so that it can find the link for us.



Next, we need to go to the terminal to execute the script. We can execute it by using the command **python3 name.py**.



Thus, it will run and list out all the links from the Santa's Tracker.

```
┌──(kali㉿kali)-[~]
└─$ python3 linkgrabber.py
../

https://github.com/BulmaTemplates/bulma-templates/blob/master/templates/hero.html
https://tryhackme.com
https://tryhackme.com
https://tryhackme.com
https://tryhackme.com
https://tryhackme.com
https://tryhackme.com
https://tryhackme.com
https://tryhackme.com
https://tryhackme.com
https://tryhackme.com
https://tryhackme.com
#
#
#
#
#
#
#
#
#
http://machine_ip/api/api_key
#
#
#
#
#
#
#
#
#
https://github.com/BulmaTemplates/bulma-templates
https://github.com/BulmaTemplates/bulma-templates
```

There, we can find the link we want to obtain. We can see that the directory of the API is **/api/**.

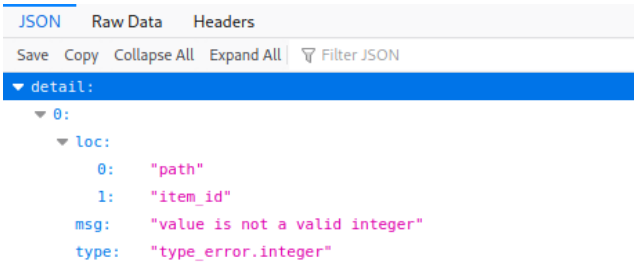
```
#
http://machine_ip/api/api_key
#
```

Answer: /api/

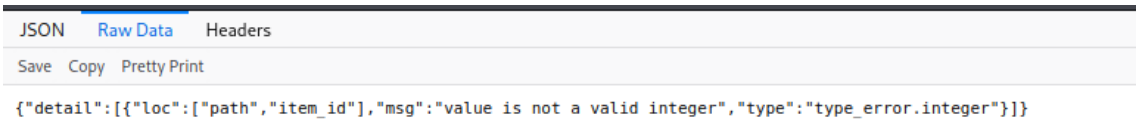
Question 4: Go to the API endpoint. What is the Raw Data returned if no parameters are entered?

From the link, we can use it to find the raw data.

The link will lead to a page that lists out the JSON and Raw Data.



Go to the **Raw Data** tab to get the answer.

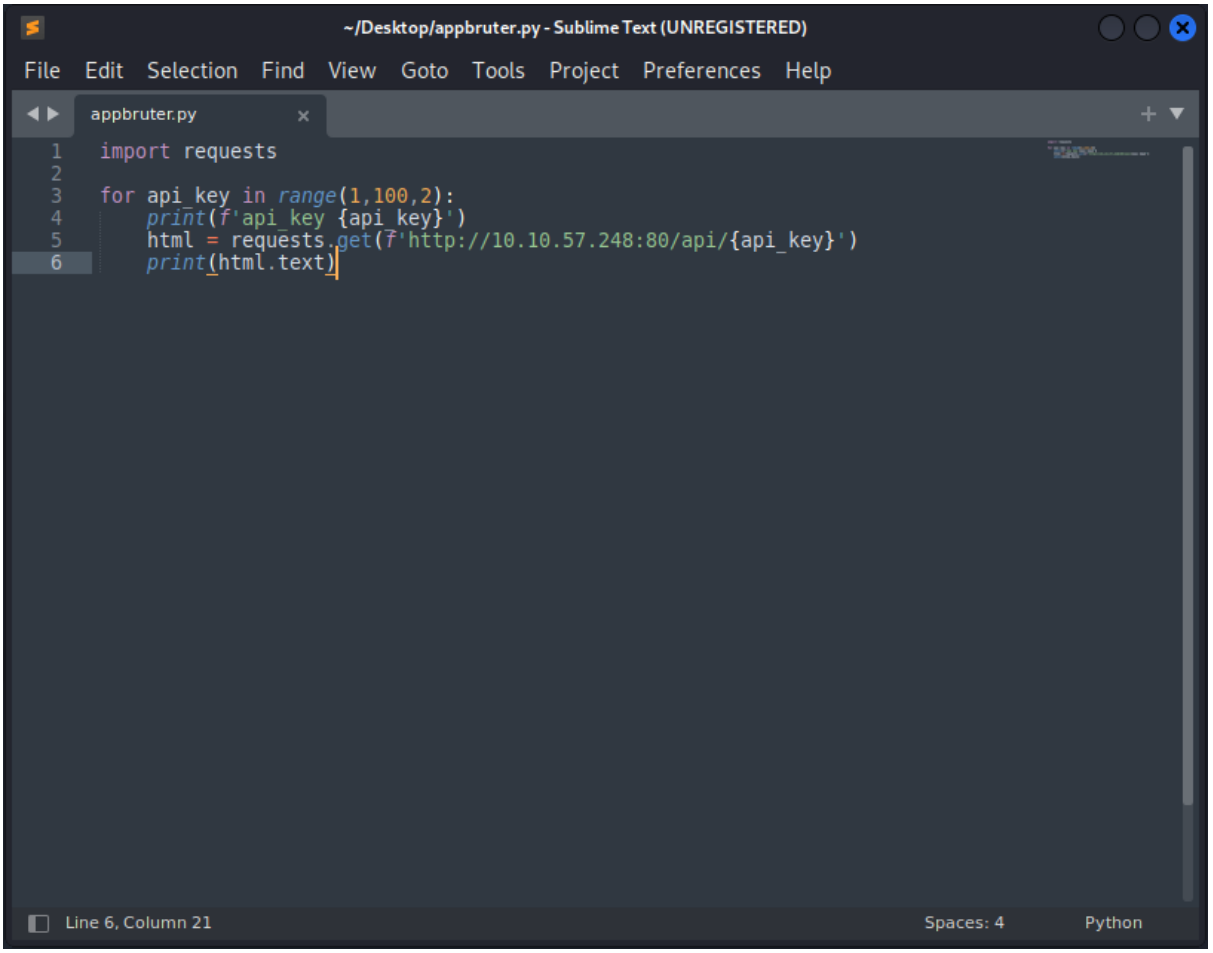


Answer: {"detail":[{"loc":["path","item_id"],"msg":"value is not a valid integer","type":"type_error.integer"}]}

Question 5: Where is Santa right now?

To find Santa's location, we need to make a Python programme that can detect the location of Santa.

We need to get another Sublime Text Editor. We need to have a script that continuously repeats itself with a new number until it finds Santa's location.



Now, we can run it by using the command **python3 name.py**.

When it is run, it will repeat itself with a new number until it finds the location.

```
┌──(kali㉿kali)-[~]
└─$ python3 appbruter.py
api_key 1
{"item_id":1,"q":"Error. Key not valid!"}
api_key 3
{"item_id":3,"q":"Error. Key not valid!"}
api_key 5
{"item_id":5,"q":"Error. Key not valid!"}
api_key 7
{"item_id":7,"q":"Error. Key not valid!"}
api_key 9
{"item_id":9,"q":"Error. Key not valid!"}
api_key 11
{"item_id":11,"q":"Error. Key not valid!"}
api_key 13
{"item_id":13,"q":"Error. Key not valid!"}
api_key 15
{"item_id":15,"q":"Error. Key not valid!"}
api_key 17
{"item_id":17,"q":"Error. Key not valid!"}
api_key 19
{"item_id":19,"q":"Error. Key not valid!"}
api_key 21
{"item_id":21,"q":"Error. Key not valid!"}
api_key 23
{"item_id":23,"q":"Error. Key not valid!"}
api_key 25
{"item_id":25,"q":"Error. Key not valid!"}
api_key 27
{"item_id":27,"q":"Error. Key not valid!"}
api_key 29
{"item_id":29,"q":"Error. Key not valid!"}
```

Then, when the correct number is keyed in, it will list Santa's location.

```
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
```

Answer: Winter Wonderland, Hyde Park, London

Question 6: Find out the correct API key. Remember, this is an odd number between 0-100. After too many attempts, Santa's Sled will block you. To unblock yourself, simply terminate and re-deploy the target instance

From the last question, the correct API Key is **57**.

```
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
```

Answer: 57

Thought Process/Methodology:

With the given IP Address, we can find the port that is open by using **nmap**. There, only 2 ports are open and one of them has a service of **http**. Now, we know the correct port is **80**. Hence, we use the port along with the IP Address to access the website which is **Santa's Tracker**. The first thing we can see in the website is the template used which is **BULMA**. Next, we need to find the directory of the API. We can easily go to **"View Page Source"** and find the link that leads to the directory. However, we can also use Python to obtain the directory. Firstly, we can use the script that has been given to us in the TryHackMe website on **Day 15**. Secondly, we need to paste the script in a **Sublime Text Editor** and make it a **Python file** by using the **.py** on the end of the name of the file. Next, we need to modify the script a bit to have a programme that can help us filter out all the links that are in the website. Now, we can run the Python script by using the command **python3 name.py**. It will filter out the links and we can identify the correct link that has the directory we need which is **/api/**. From the link we obtained from the Python script, we can also obtain the **Raw Data**. Use the link with the IP Address that TryHackMe has provided. There, we can obtain the **Raw Data** which is **{"detail":[{"loc":["path","item_id"],"msg":"value is not a valid integer","type":"type_error.integer"}]}**. After that, we need to find **Santa's location**. We can find the location by using **Python**. We need to make a Python script that can continuously repeat itself until it finds the correct API key and lists out the location. We can do this by making a loop. After finishing the script, run it and it will continuously repeat the programme until it finds the correct API key. The correct API key is **57** and Santa's location is **Winter Wonderland, Hyde Park, London**.

Day 17: Reverse Engineering - ReverseELFneering

Tools used: AttackBox, Terminal

Solution/walkthrough:

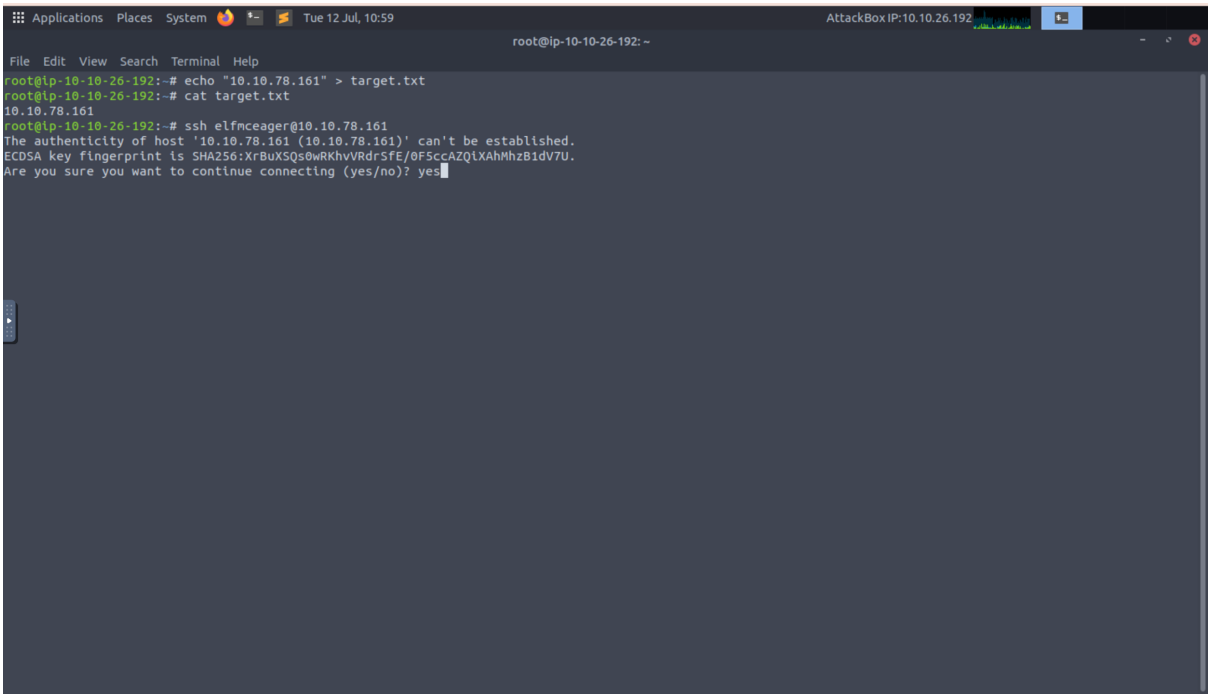
Question 1: Match the data type with size of bytes

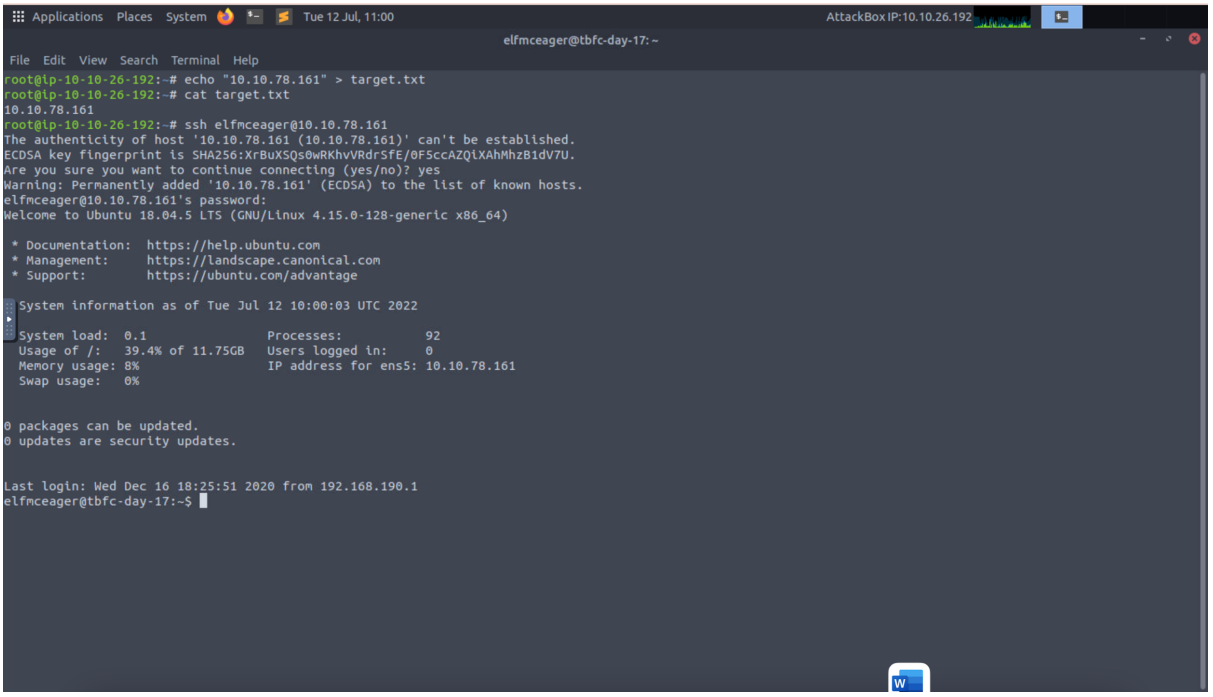
Answer :

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

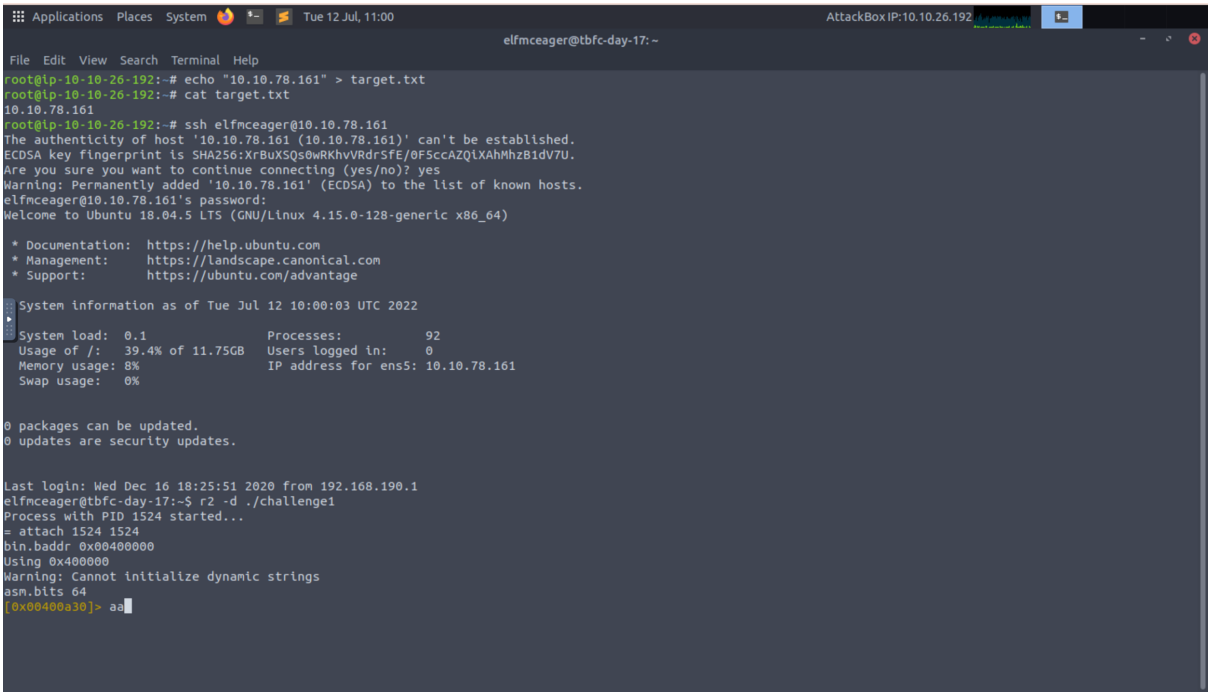
Question 2: What is the command to analyse the program in radare2?

Echo “10.10.78.161” > target.txt command was used to display lines of text or string which are passed as arguments on the command line. Then, **cat target.txt** command and **ssh elfmceager@10.10.78.161** was used.

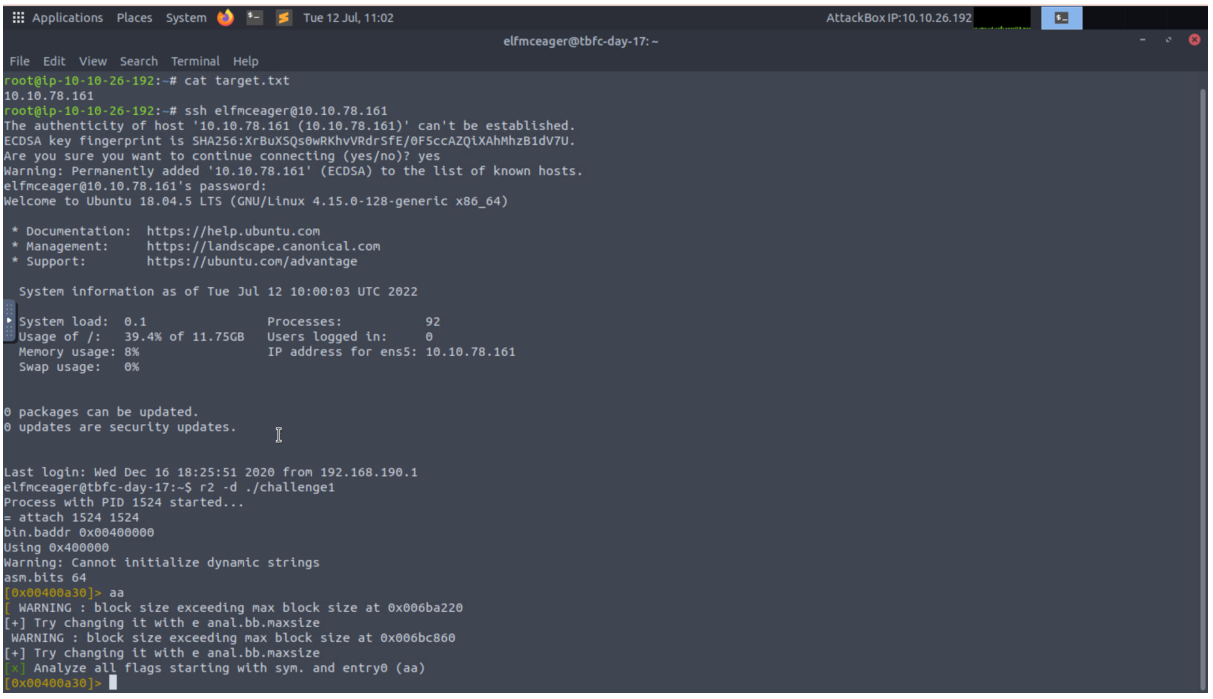




r2 -d ./challenge1 was used to open the binary in debugging mode.



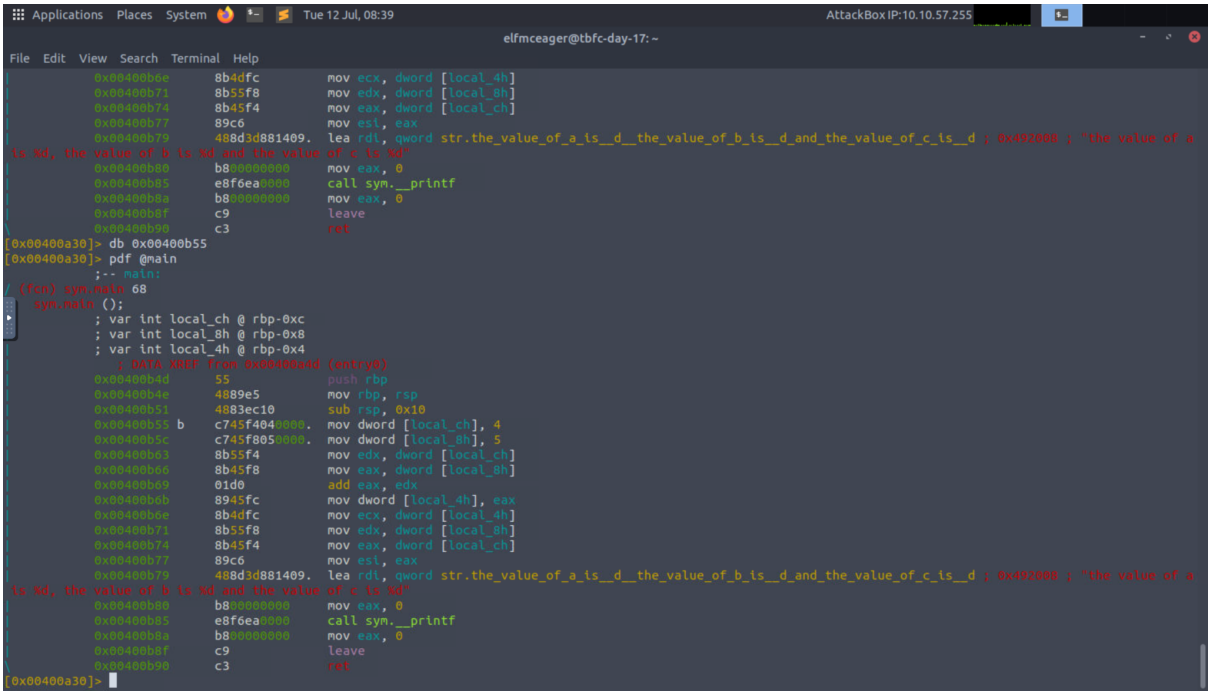
aa command was used to analyze the program.



Answer: aa

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

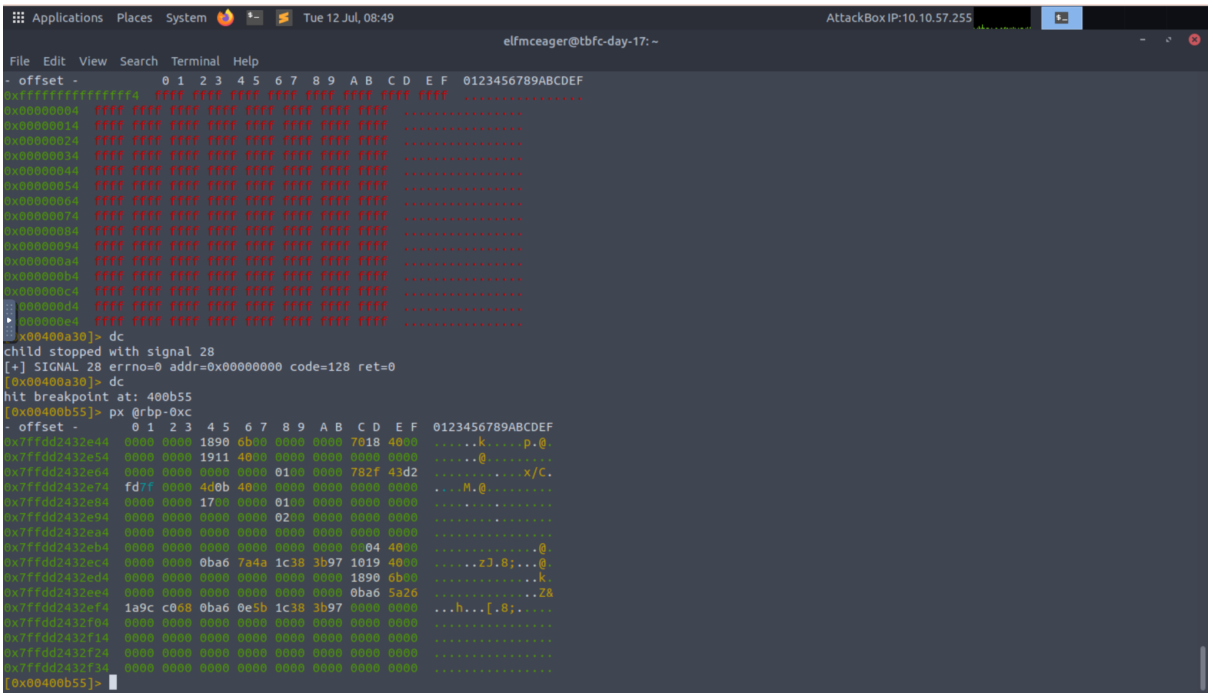
The **db** command was used to set a breakpoint.



Answer: db

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

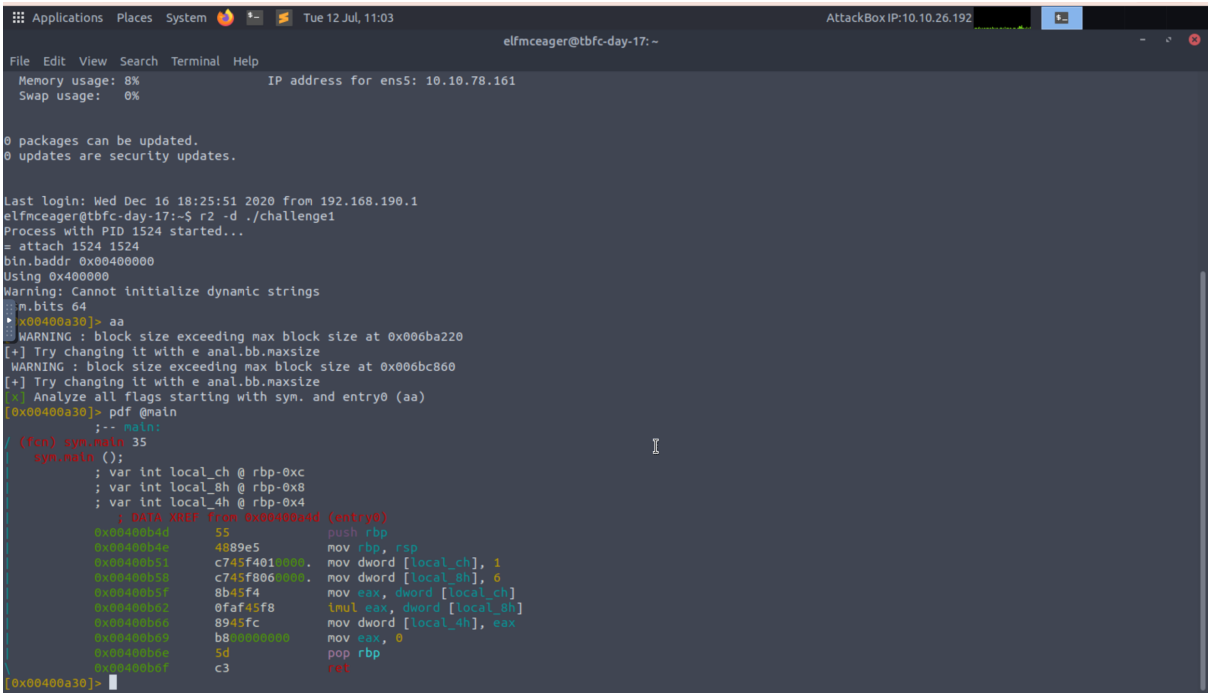
We used **dc** command to execute the program until it hit the breakpoint that was set previously.



Answer: dc

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

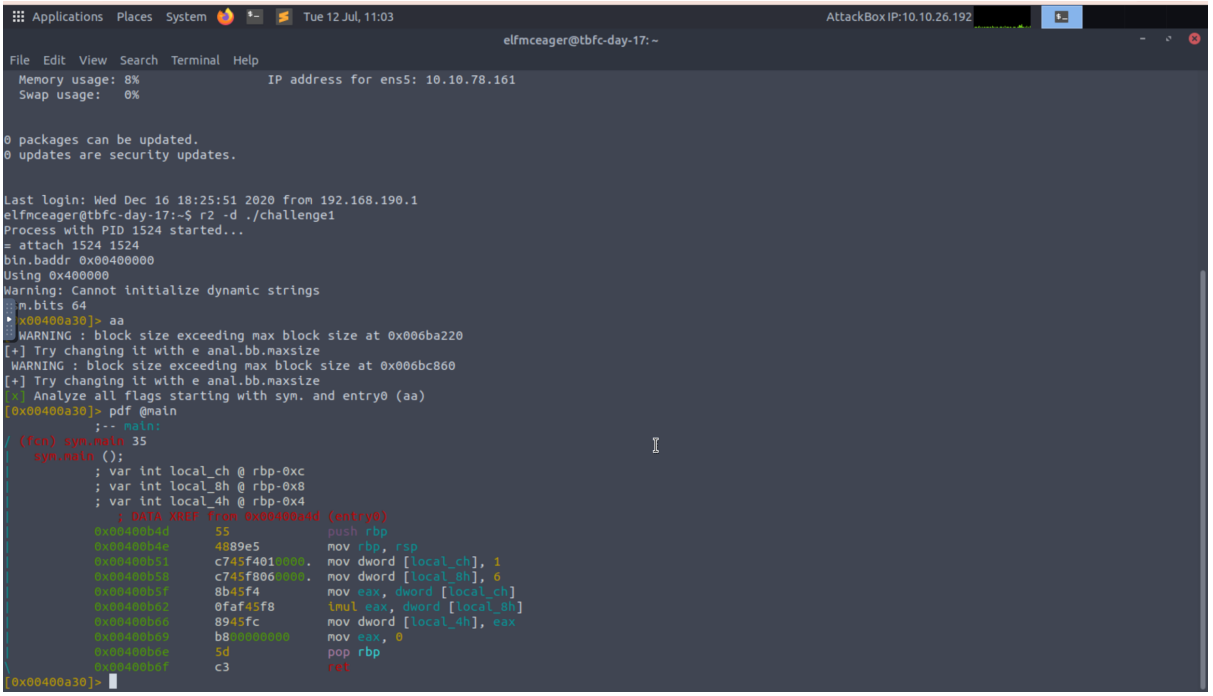
By using pdf @main, the value of local_ch could be seen.



Answer: 1

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

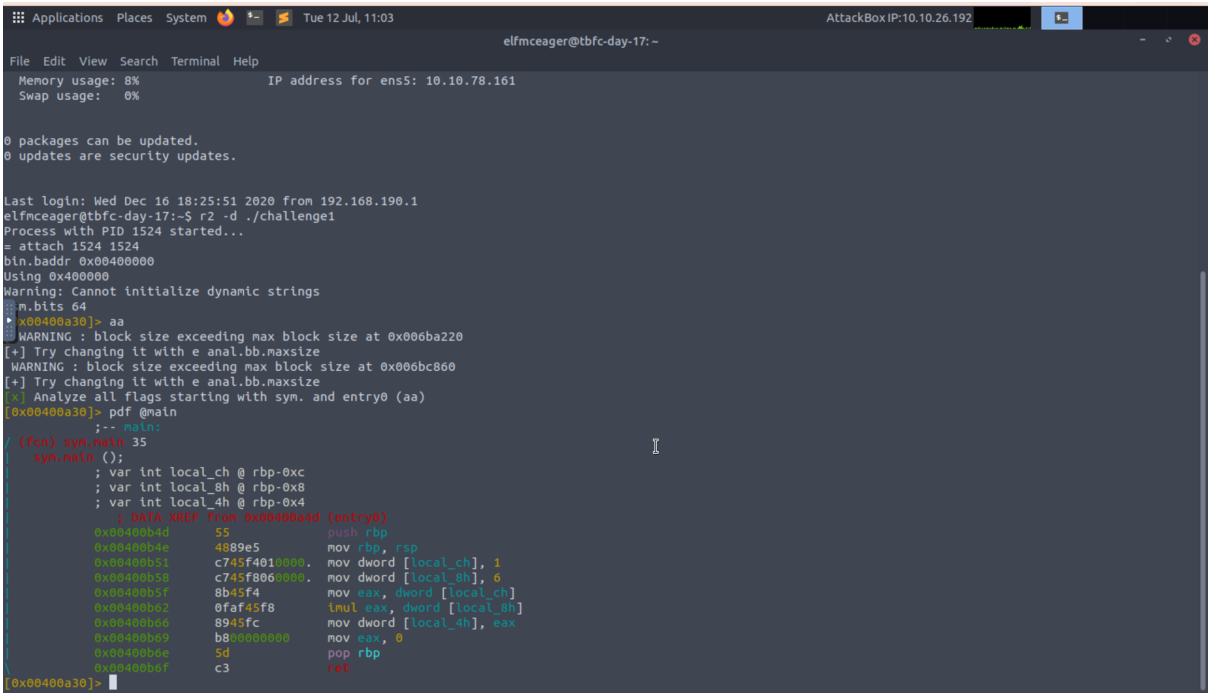
dword = 6 , eax = 1. Thus, 6x1=6



Answer: 6

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

dword = 6 , eax = 1. Thus, 6x1=6



Answer: 6

Thought Process/Methodology:

To start the task, **echo "10.10.78.161" > target.txt** and **cat target.txt** was used. Then, **ssh elfmceager@10.10.78.161** was used to log in. Then, password is required to connect to Ubuntu which we used **adventofcyber** . Next to start the challenge, **r2 -d ./challenge** was used. Then, we used **aa** command to analyze the program. After analyzing the program, **pdf @main** was used to examine the assembly code at main. Then, we used **db** command to set a breakpoint and **dc** command to execute the program until it hit the breakpoint.

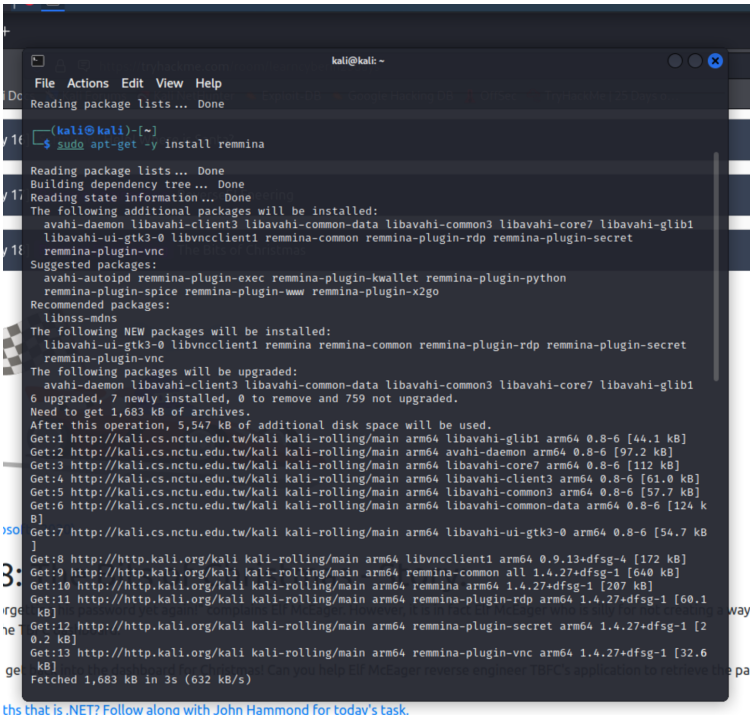
Day 18 : Reverse Engineering - The Bits of Christmas

Tools used: Kali Linux, Remmina, ILSpy, TBFC_APP, OpenVPN, FireFox, Command Prompt

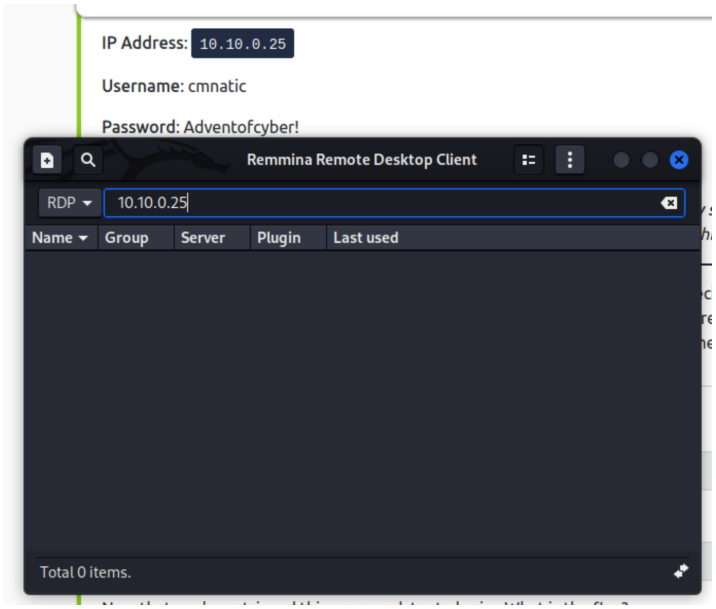
Solution/walkthrough:

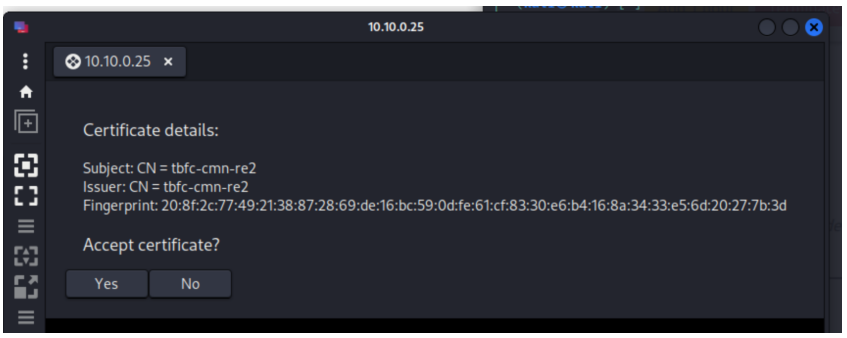
Question 1: What is the message that shows up if you enter the wrong password for TBFC_APP?

Install remmina using the command **sudo apt-get -y install remmina** .

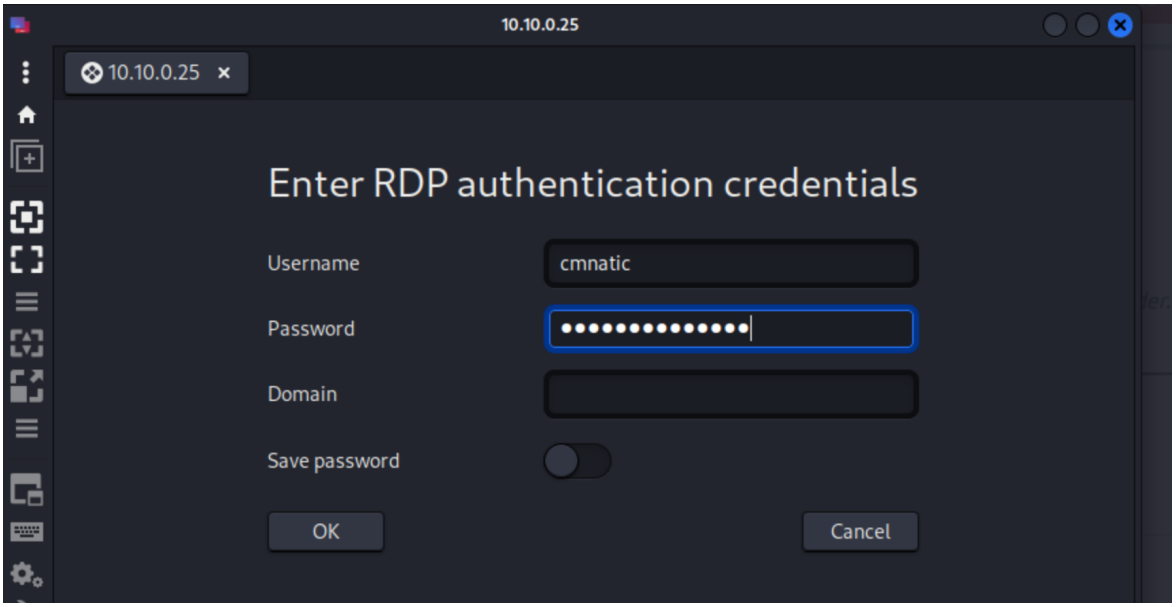


After installation has completed, open remmina and type in the machine instance IP address.

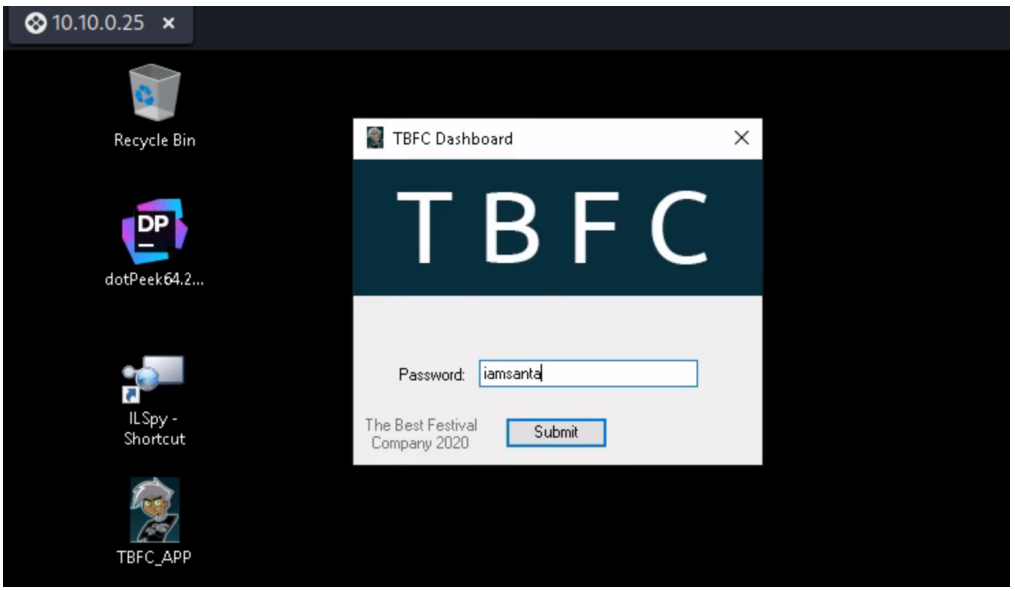




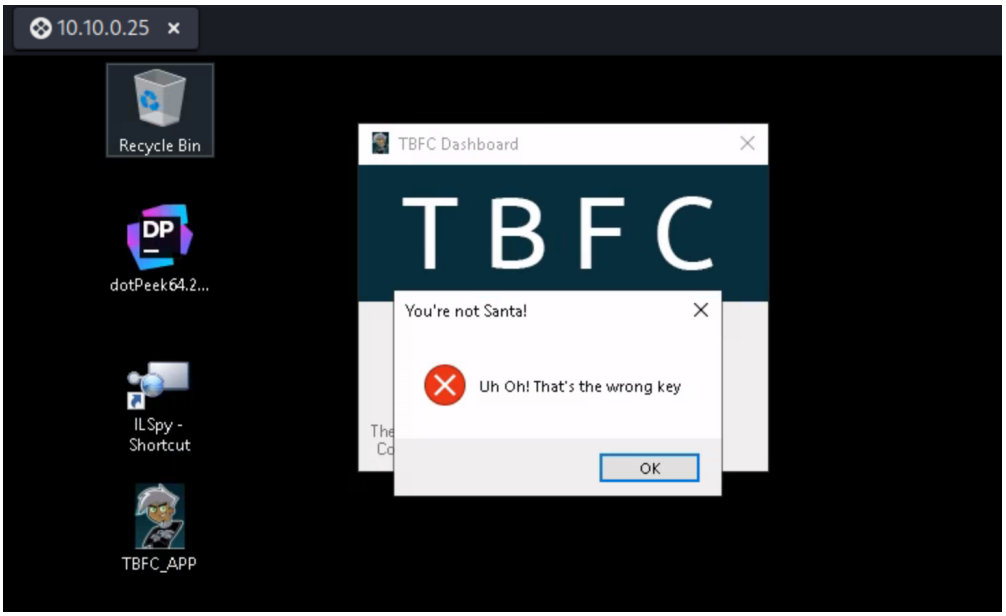
Insert the username and password given in tryhackme.



Click on the TBFC_App and insert the password.



The error message will be displayed on the screen.



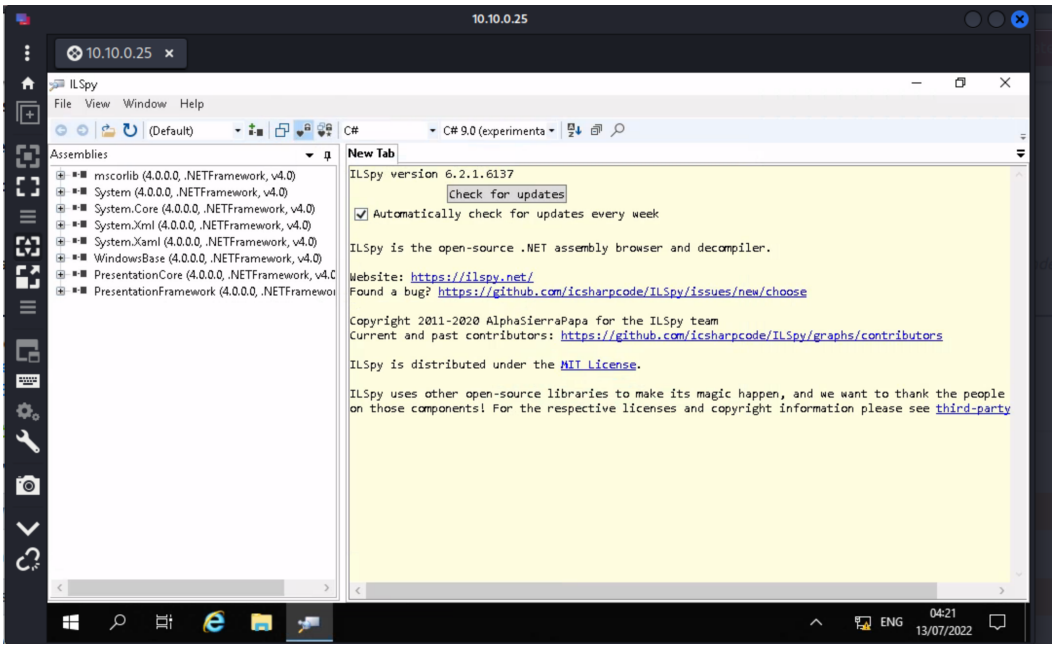
Answer: <u>Uh Oh! That's the wrong key</u>

Question 2: What does TBFC stand for?

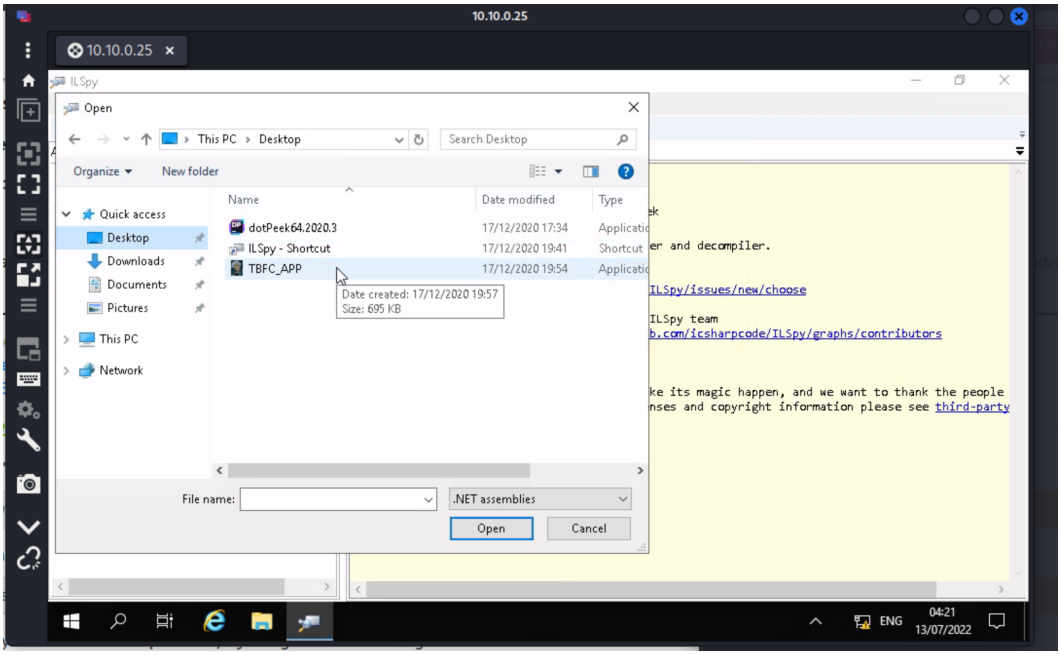
Answer: <u>The Best Festival Company</u>

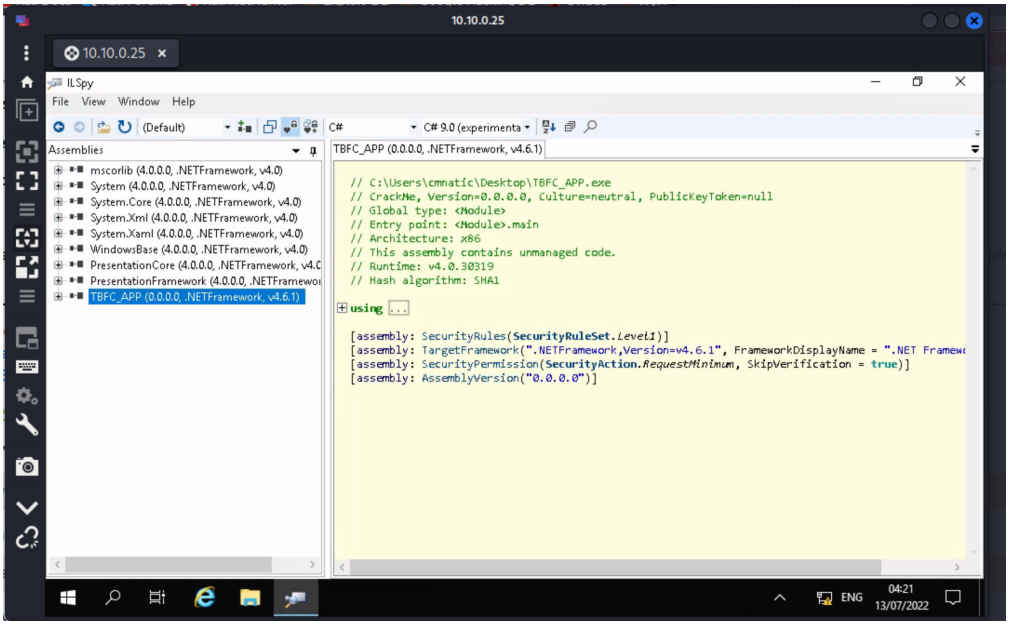
Question 3: Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?

Click on ILSpy from the desktop.

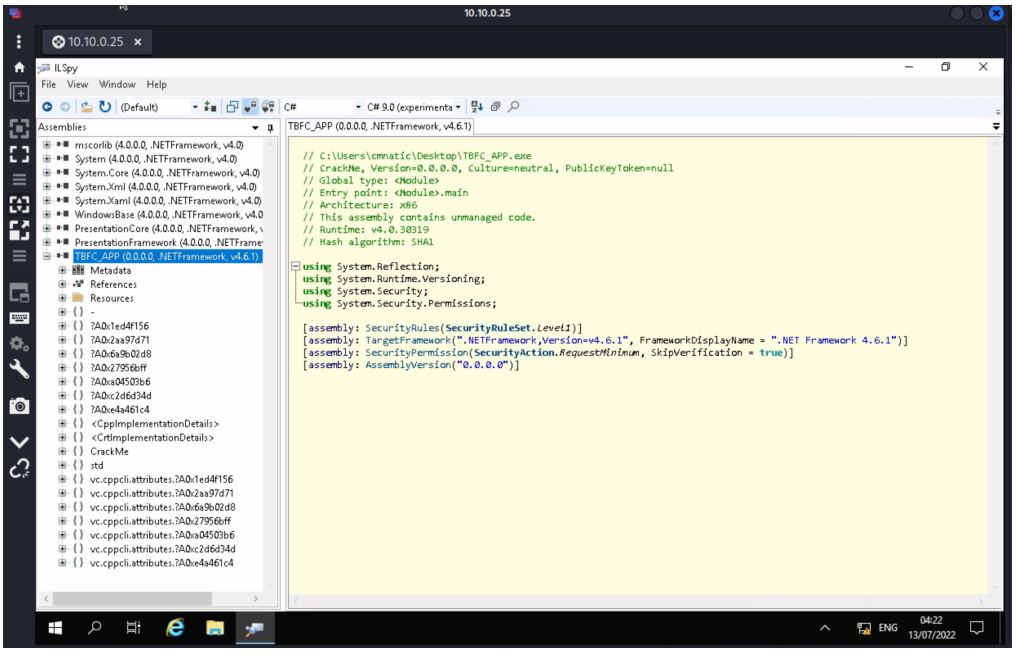


Open the TBFC_APP from ILSpy.

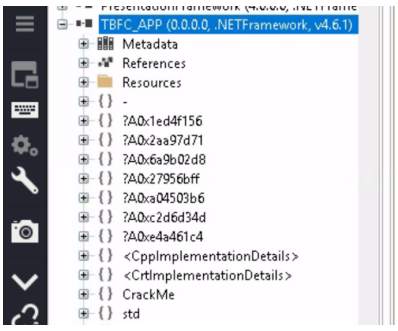




Click on the plus button to expand the TBFC_APP assemblies.



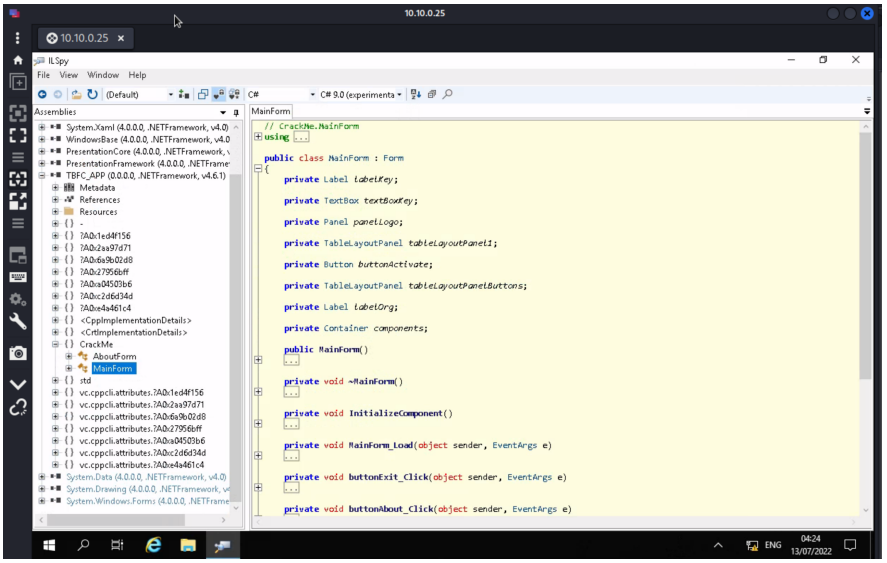
The module **CrackMe** can be seen.



Answer: CrackMe

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

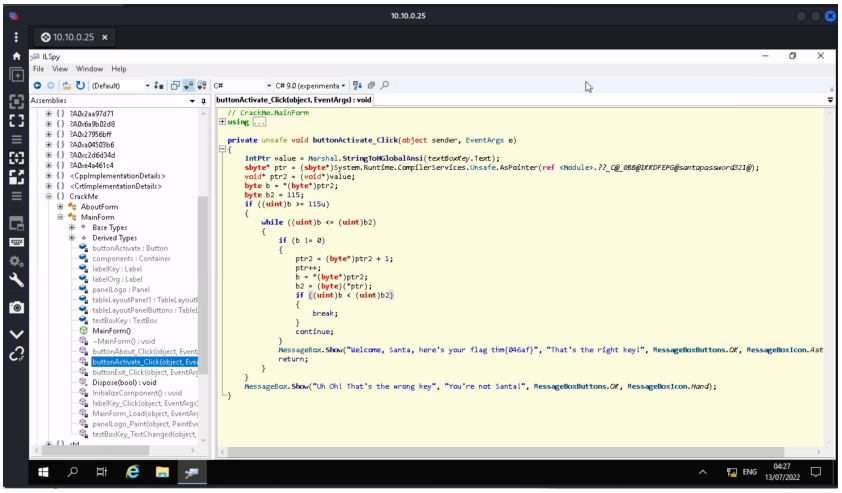
Expand the CrackMe module by clicking on the plus sign. The MainForm contains information that we are looking for.



Answer: MainForm

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

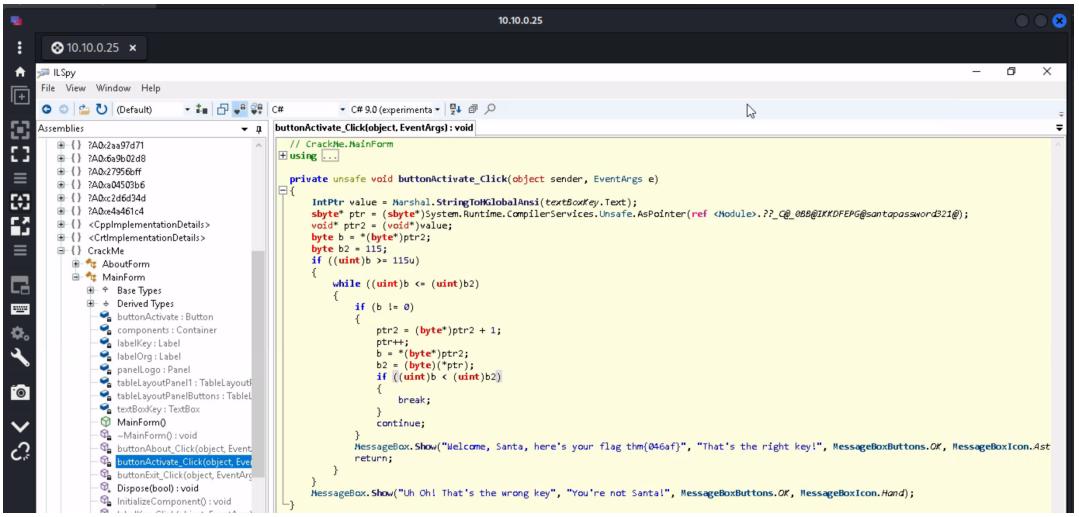
Expand the MainForm by clicking on the plus sign. The buttonActivate method will contain the information.



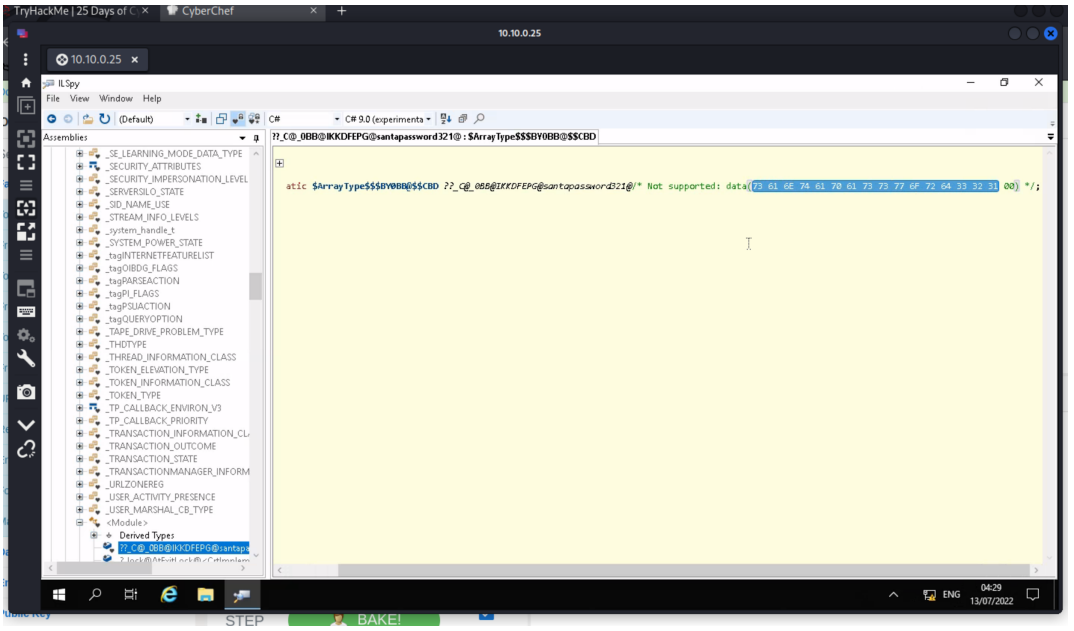
Answer: buttonActivate_click

Question 6: What is Santa's password?

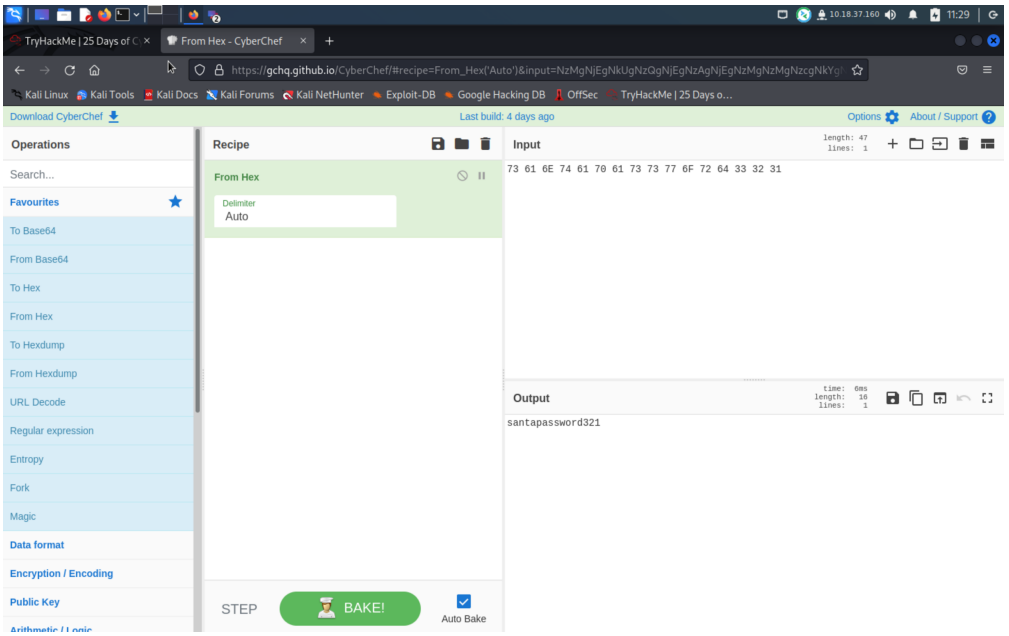
Click on the santapassword to retrieve the hexadecimal form.



Copy the hexadecimal value and paste it into cyberchef.com .



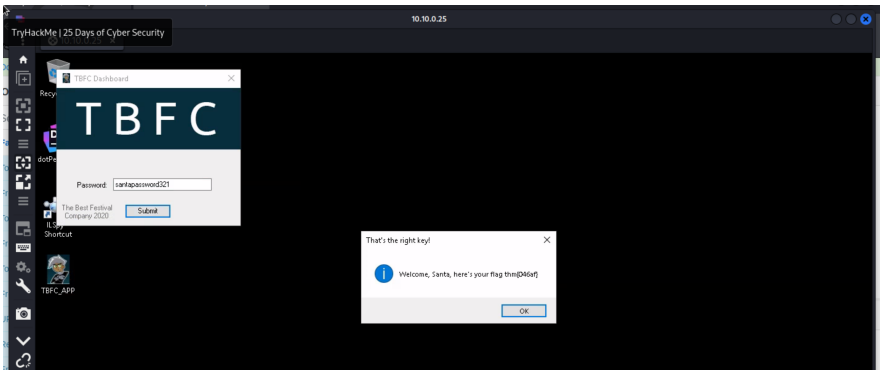
Convert the hexadecimal value.



Answer: santapassword321

Question 7: Now that you've retrieved this password, try to login...What is the flag?

Insert the password into the TBFC_APP. The flag will be displayed in the message box.



Answer: thm{046af}

Thought Process/Methodology:

To start this task, we installed remmina into Kali Linux by using the command **sudo apt-get install remmina** . Once the tool has been installed, we typed in the machine instance IP Address and we connected to the machine instance by using the username (**cmnatic**) and password (**Adventofcyber!**) given from the tryhackme website. After successfully connecting to the machine instance, we opened **TBFC_APP** and tried to guess the password. Unfortunately, an error message was displayed on the screen telling us we were not Santa after we entered the wrong password. Thus, we used **reverse engineering** using **ILSpy** to allow us to look at the source code of the application. Firstly, we opened the **TBFC_APP** in **ILSpy**. Once we opened it, we saw an interesting module named **CrackMe** . We clicked the plus sign to expand the module and found two forms (**AboutForm** and **MainForm**). After looking through the two forms, we eventually found that the **MainForm** had a **buttonActivate_Click**. When we clicked on it, we saw a susceptible string which could potentially be Santa's password. However, we were not sure of the specific string for the password. Hence, to confirm our suspicions, we clicked on the string (**santapassword**) and it brought us to the hexadecimal value of the string. We copied this value, and pasted it into **cyberchef** to convert it. After successfully converting the value, it gave us **santapassword321**. Therefore, we opened the **TBFC_APP** and entered the password. After successfully logging in, we were shown the flag **thm{046af}** .

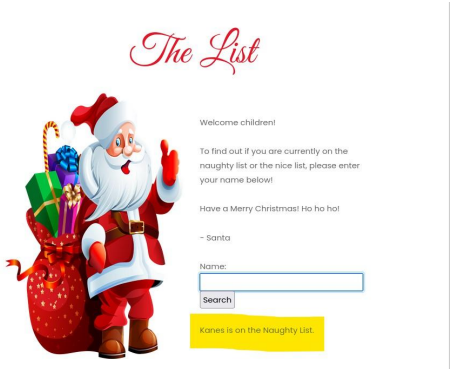
Day 19 : Web Exploitation—The Naughty or Nice List

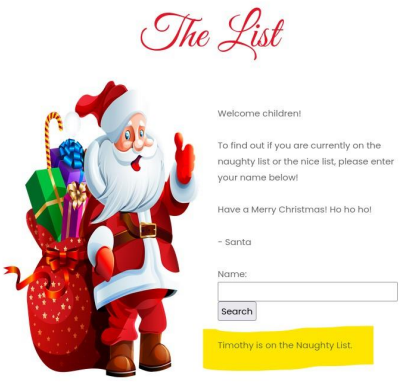
Tools used: WSL, Firefox, Notepad, Kali Linux

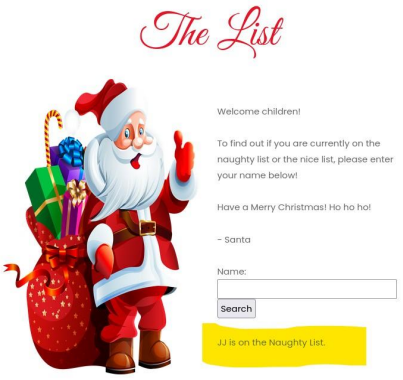
Solution/walkthrough:

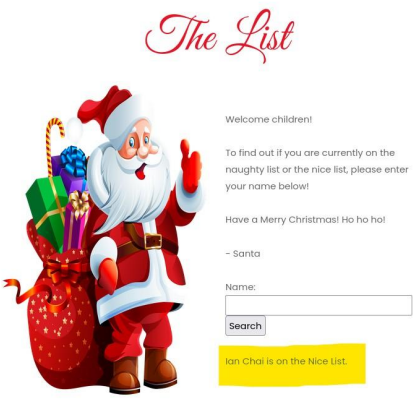
Question 1: Which list is this person on?

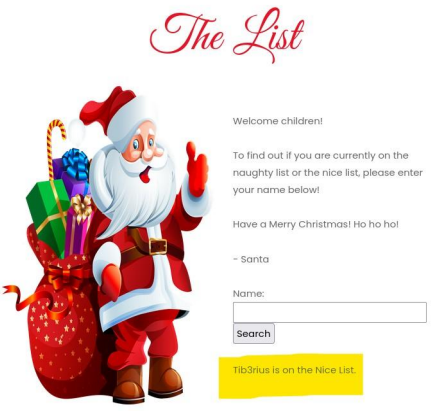
Start the machine and input the IP address given to your browser. Once you have successfully opened the website, input each name given into the list and observe the output given









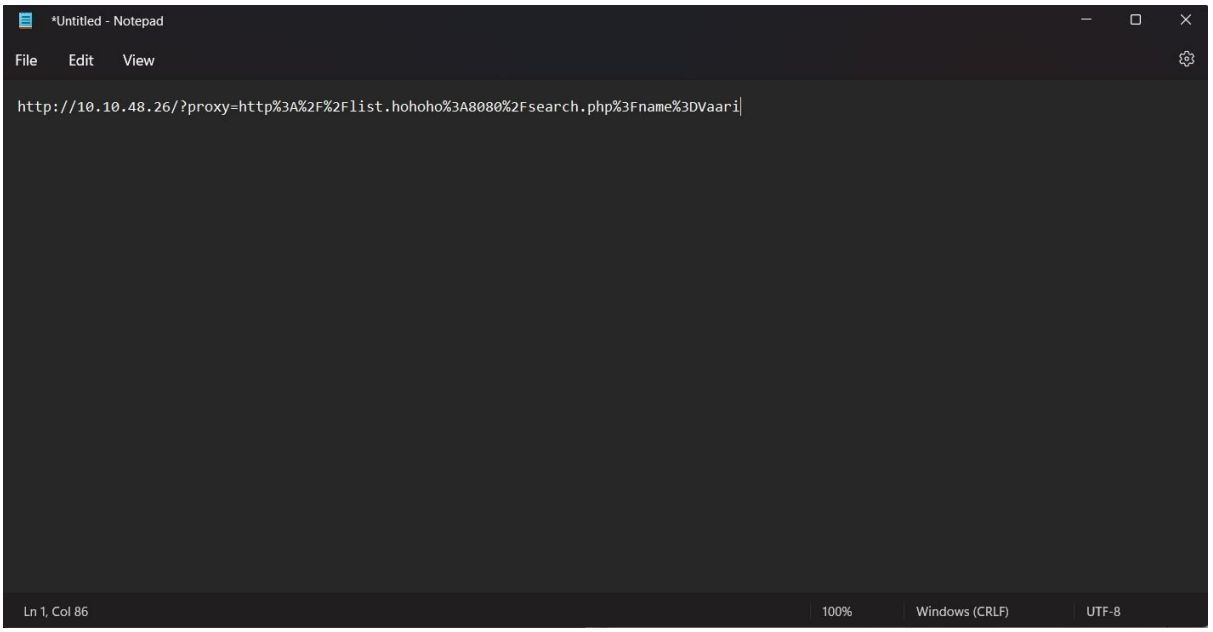


Answer:

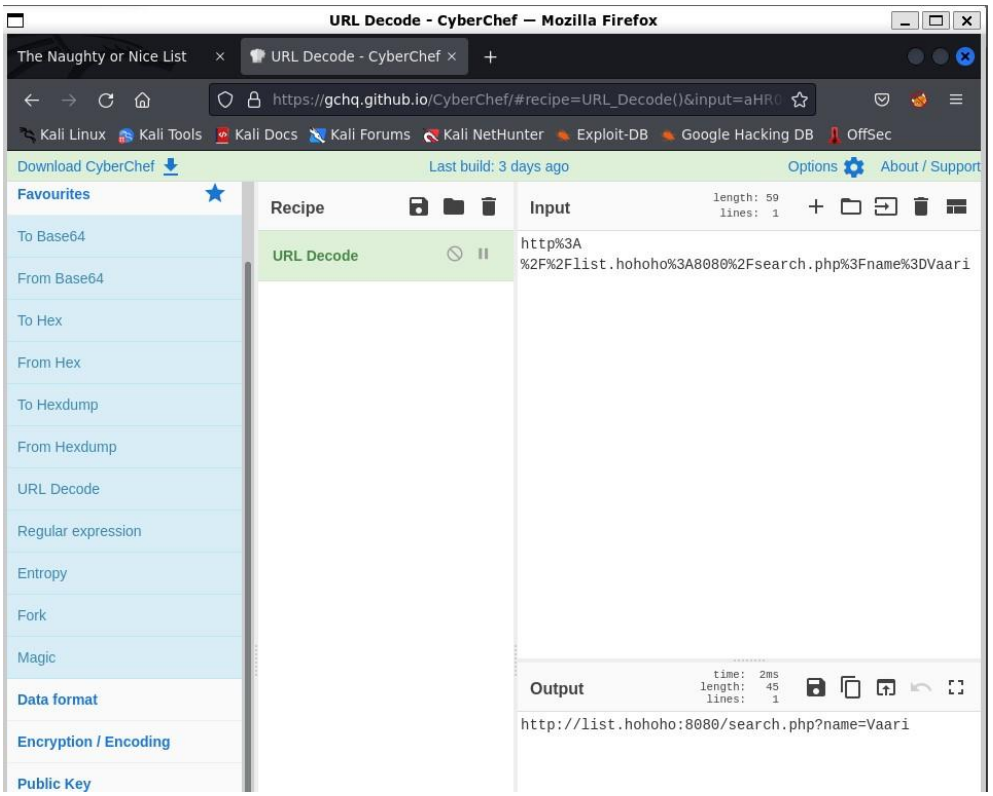
Name	Naughty or Nice
Ian Chai	***Nice***
Tib3rius	***Nice***
JJ	***Naughty***
Timothy	***Naughty***
YP	***Nice***
Kanes	***Naughty***

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

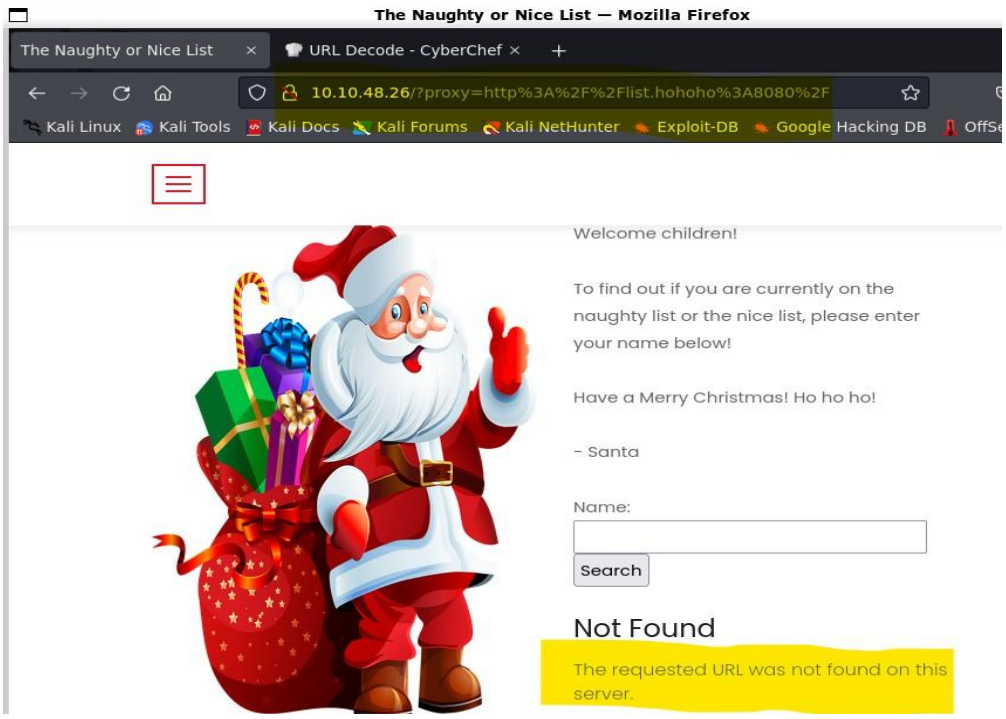
Copy the URL and paste it at your desired text editor



Open a new tab at your browser and search cyberchef, then decode it. Observe and understand the output given.



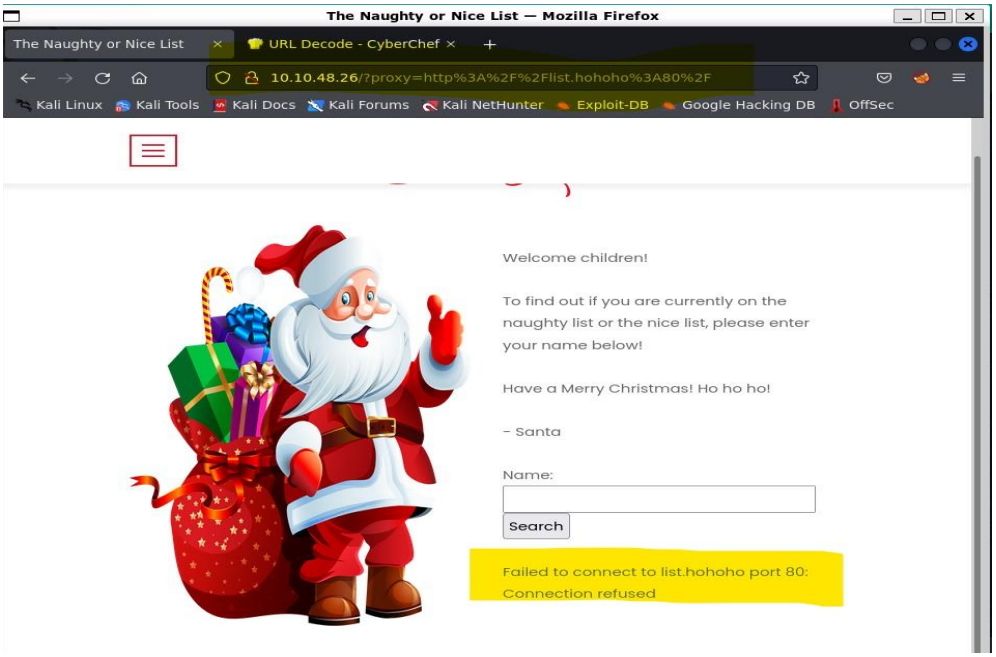
Now we got the idea on how the website fetch the data, alter the URL by replacing the "/?proxy…" to
"/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"? and observe the output.



Answer: 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"?

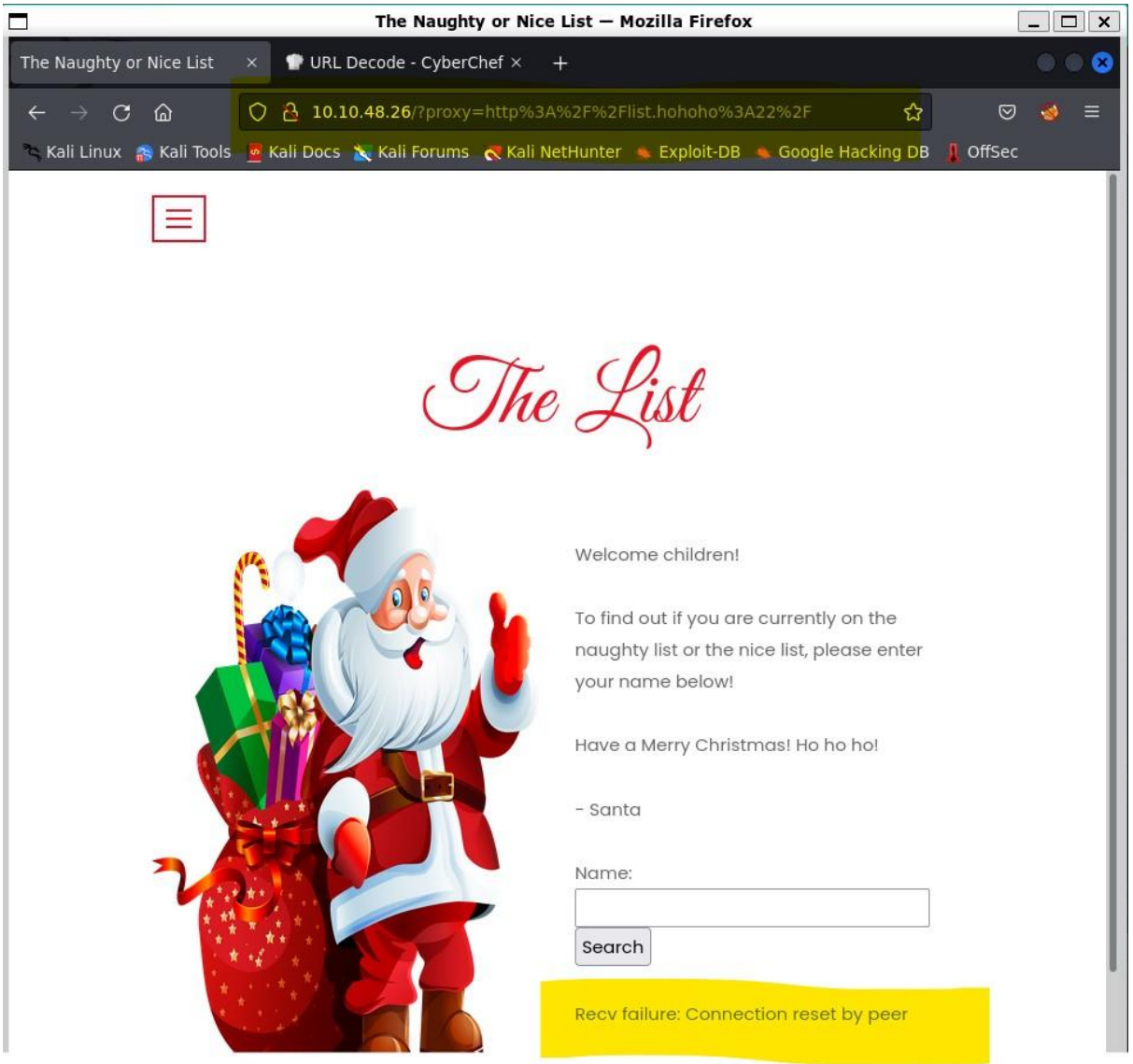
Replace “…/?proxy…” to “/?proxy=http%3A%2F%2Flist.hohoho%3A80" and observe the output.



Answer: 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"

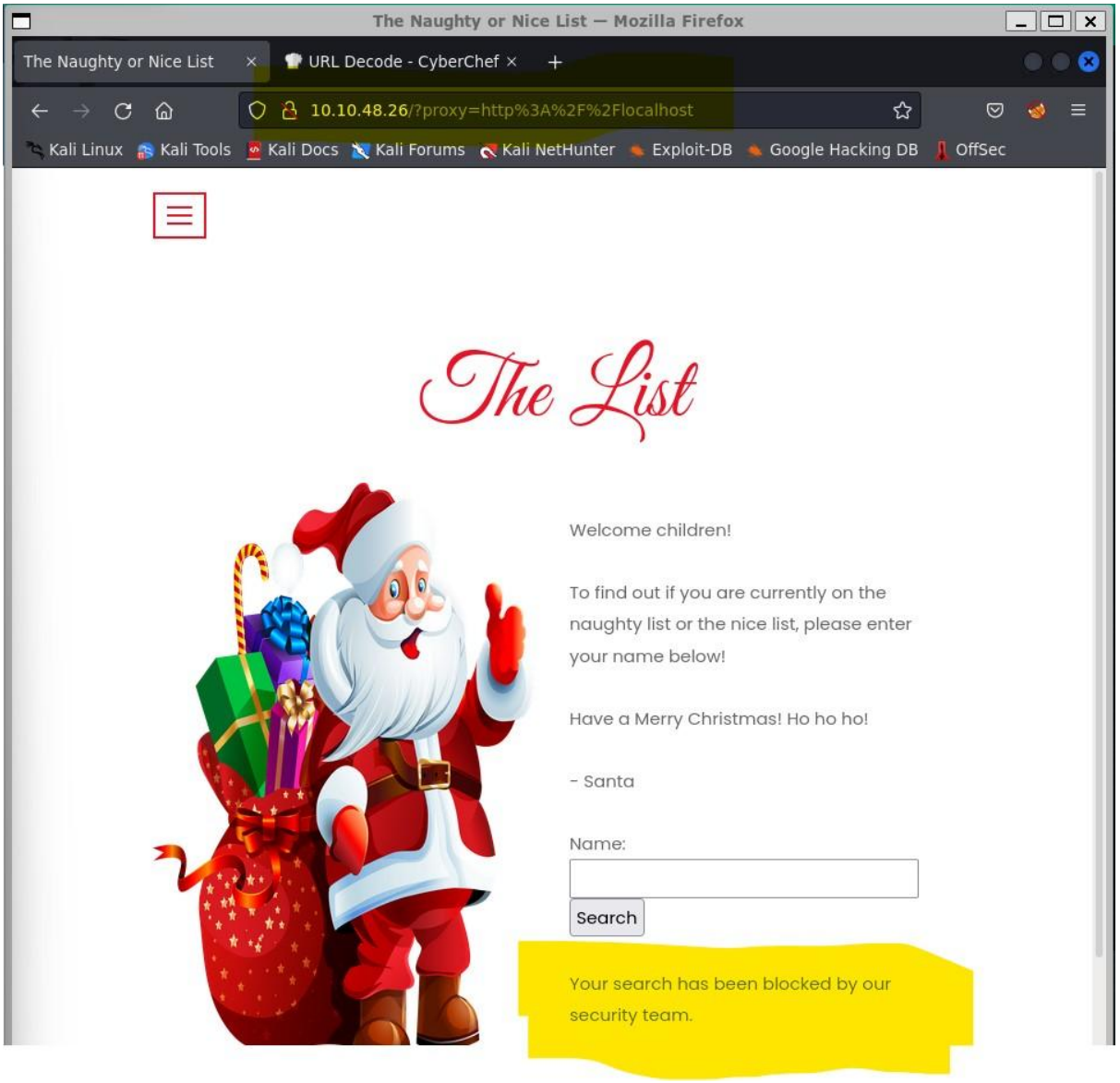
Replace "**.../?proxy...**" to "**/?proxy=http%3A%2F%2Flist.hohoho%3A22**" and observe the output.



Answer: Recv failure: Connection reset by peer

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

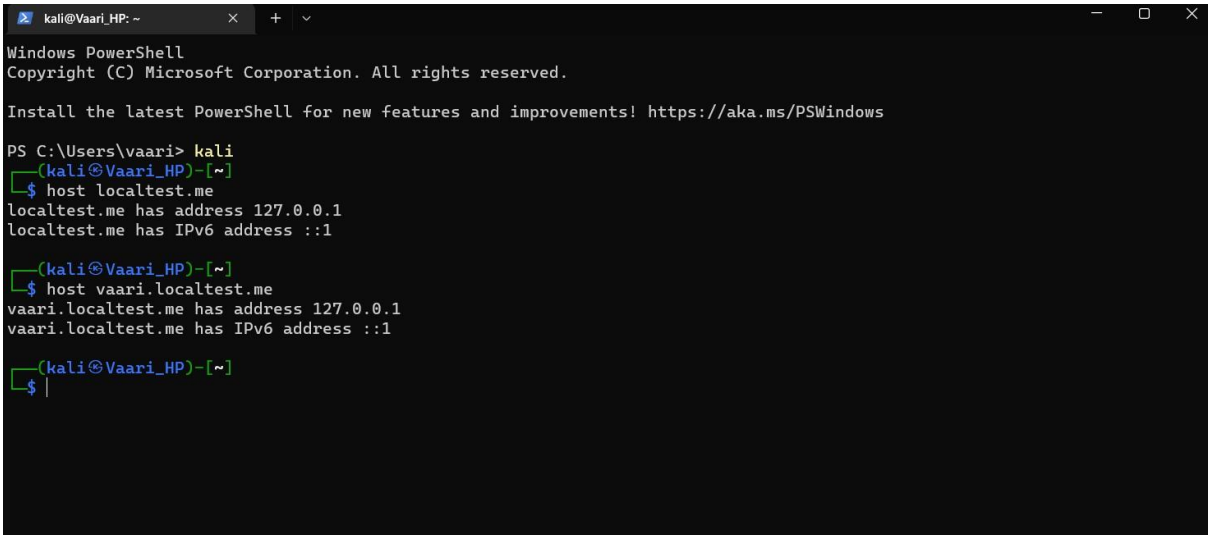
Replace “**.../?proxy...**” to “**/?proxy=http%3A%2F%2Flocalhost**" and observe the output.



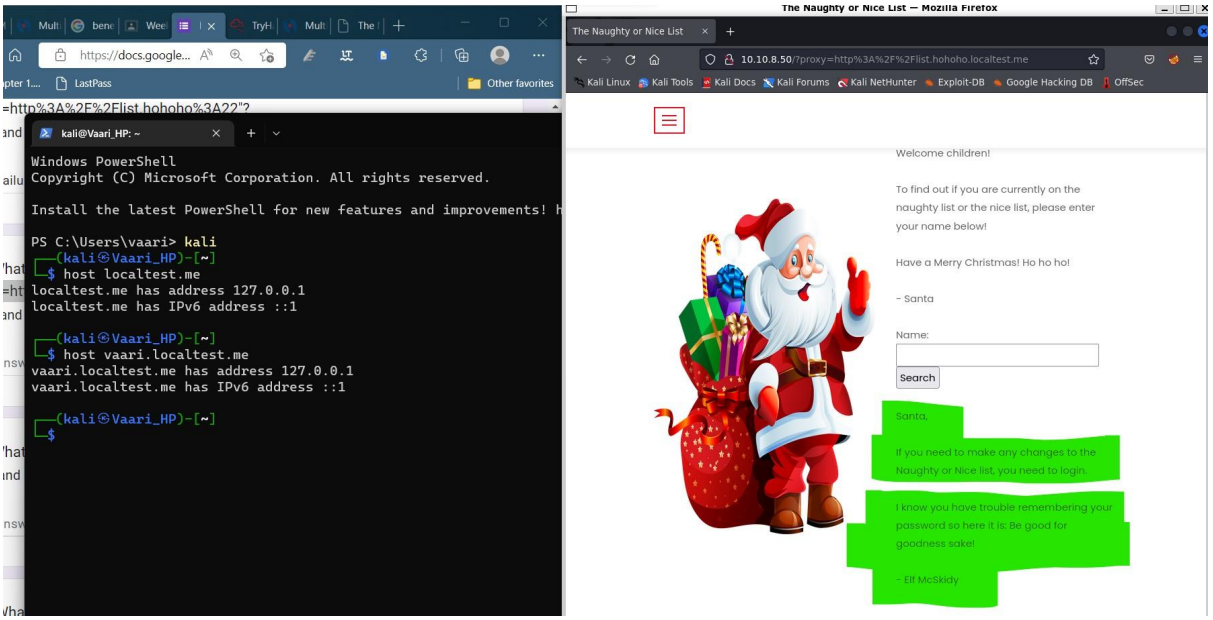
Answer: Your search had been blocked by our security team.

Question 6: What is Santa's password?

By taking advantage of DNS subdomain, we be using localtest.me as our DNS subdomain, list.hohoho.localtest.me



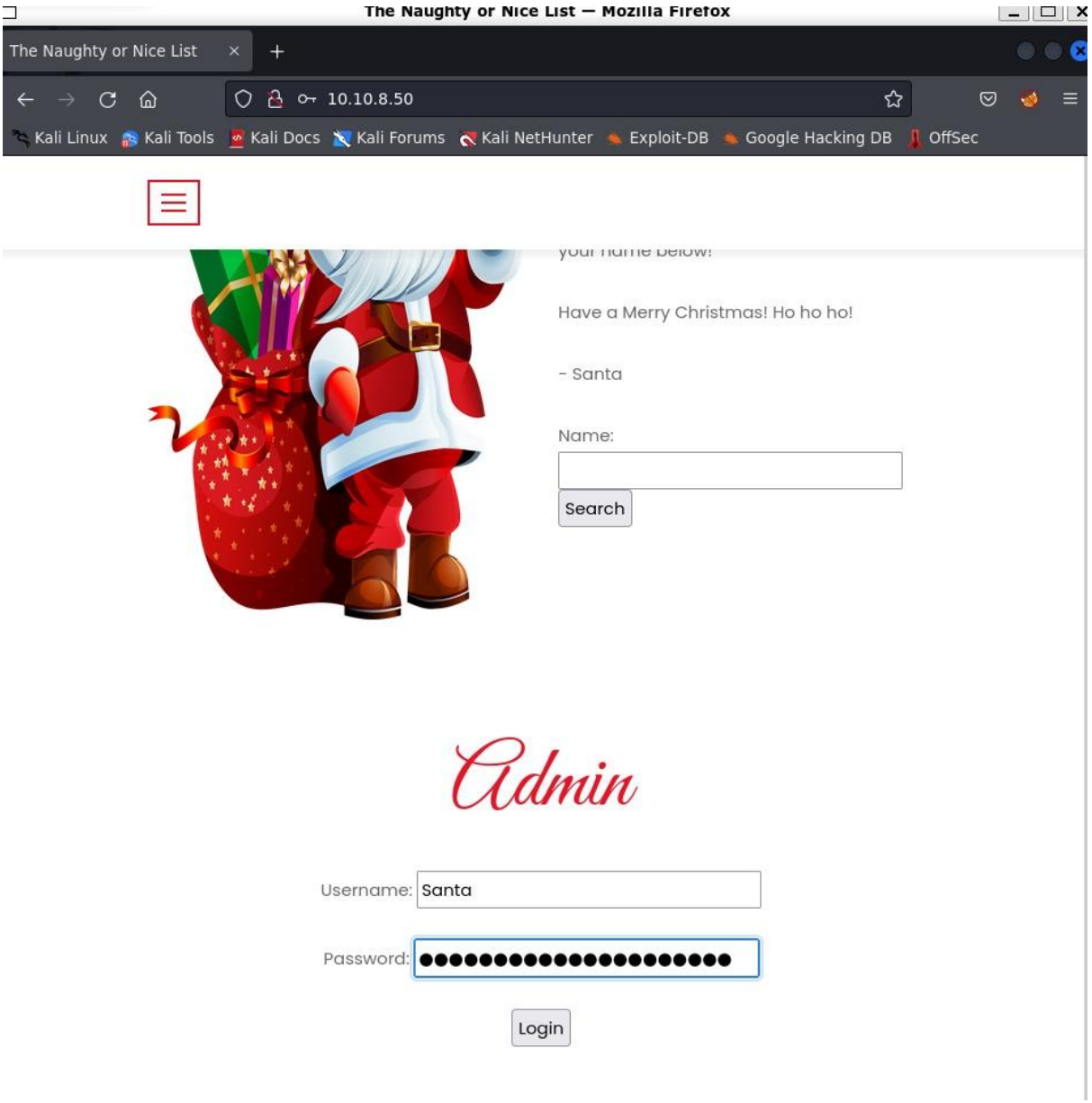
Replace **.../?proxy...** to **/?proxy=http%3A%2F%2Flist.hohoho.localtest.me** and analyse the output.



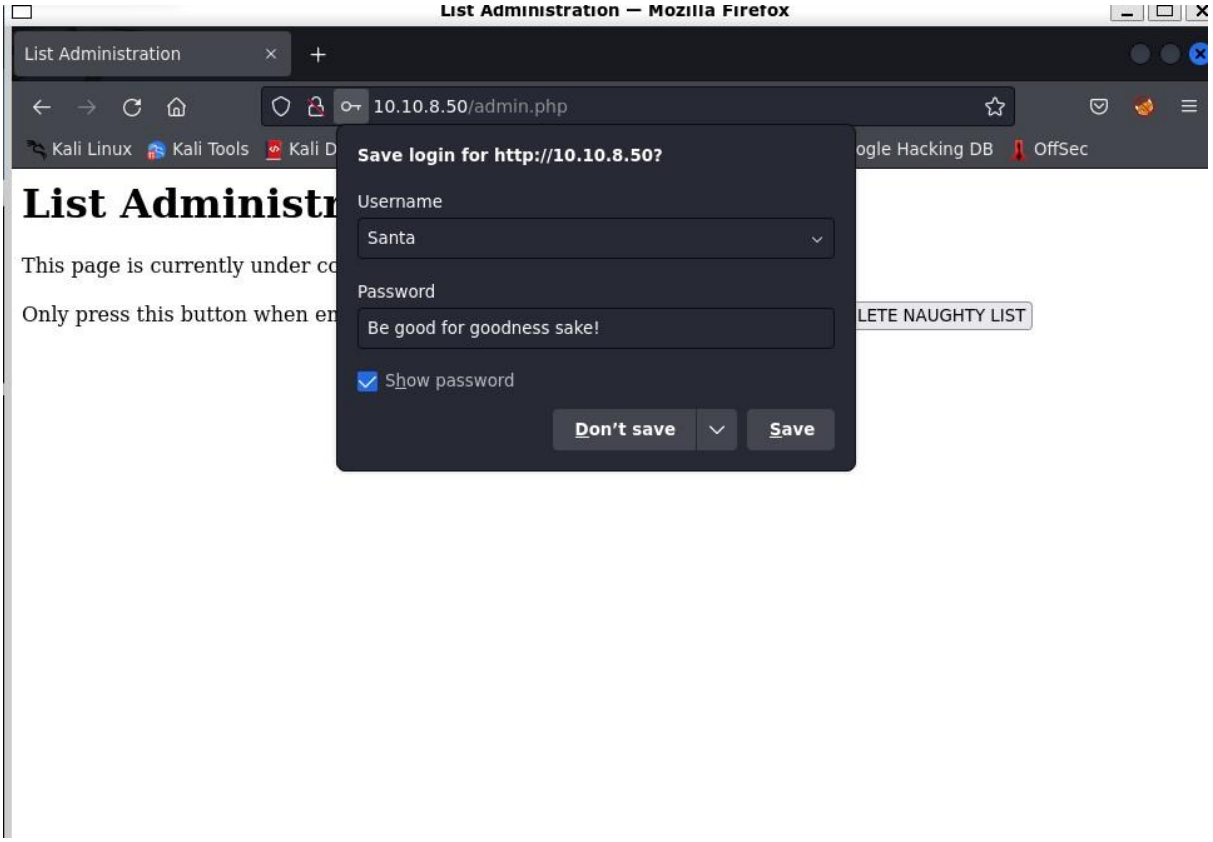
Answer: Be good for goodness sake!

Question 7: What is the challenge flag?

Go to admin page and enter Santa's credentials.



Once we have successfully figured out and logged into the web application as Santa, we can delete the naugthy list.



Click the 'Delete Naughty List' button to delete the list

Observe the output once you have successfully deleted the naughty list.

Answer: THM{EVERYONE_GETS_PRESENTS}

Thought Process/Methodology:

Once we have successfully started the machine, input the IP address of the machine into our browser. We are greeted with a web application where we can check whether we are in Santa's Nice or Naughty list. From Google forms, we can input the names given into the search box and observe the output. By entering the names given, we can observe that the URL changes. Then, we copied the entire IP address and pasted it into our desired text editor. Afterwards, we decided to copy "**/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%...**" and paste it into CyberChef and decode the URL. By decoding the URL, we can observe that there is a back-end machine (list.hohoho) where the data is fetched and sent to the web app. We can find ports and valid URLs for the back-end machine. By changing the port number to 80 from altering the URL to "**.../?proxy=http%3A%2F%2Flist.hohoho%3A80**", We can observe that the message states "**Failed to connect to list.hohoho port 80: Connection refused**" which means **port 80** is not open on the back-end machine. By changing the port number to **22** we can observe that the message changes to "**Recv failure: Connection reset by peer**" which means **port 22 is open** but it did not understand what was being sent because sending an **HTTP request** to an **SSH server** isn't a viable option. We can also try changing the **list.hohoho** hostname with localhost and observe the output. By changing it, we can observe that there is a message returned states "**Your search has been blocked by our security team**." To find out Santa's credentials, we can simply bypass the backend machine by taking advantage of **DNS subdomains** in which we will be using **localtest.me** which resolves every subdomain to **127.0.0.1.** To do so, we can alter the website to "**.../?proxy=http%3A%2F%2Flist.hohoho.localtest.me**". When we observe the output, we can see that we have successfully discovered Santa's password. All we have to do is, go to the admin login and type the username: **Santa** and password: **Be good for goodness sake!** . Once we have successfully logged into the backend system we can finally delete the naughty list.

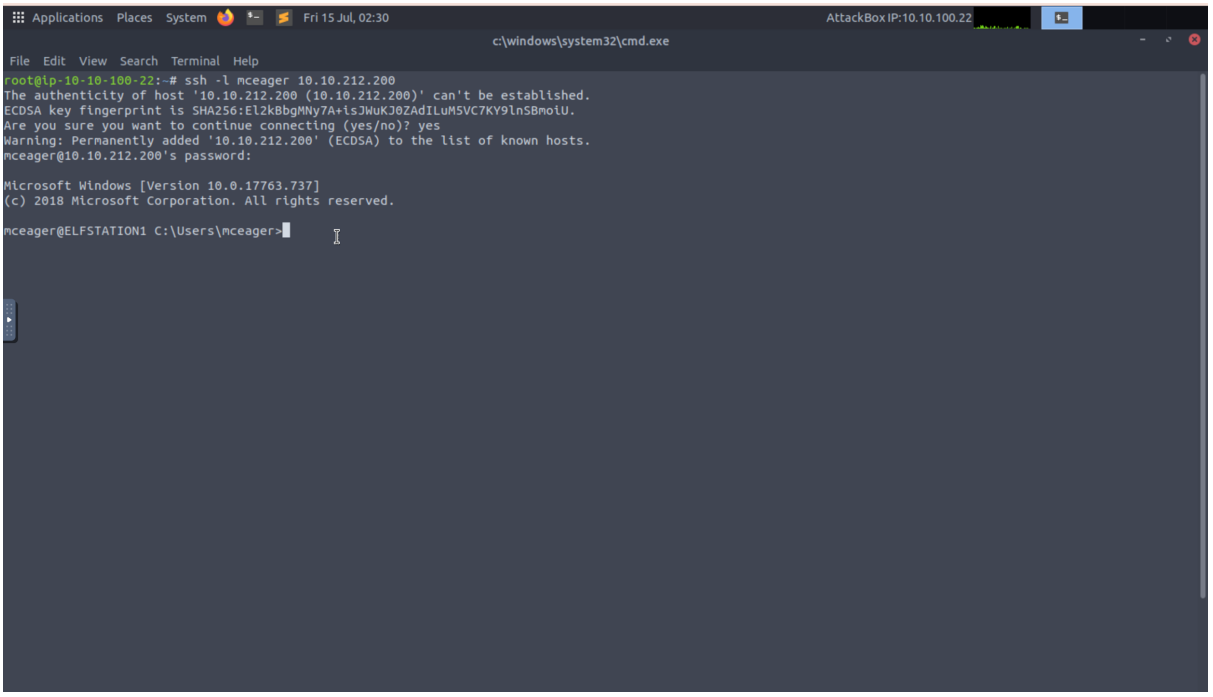
Day 20: Blue Teaming - PowershELlF to the rescue

Tools used: AttackBox, Terminal

Solution/walkthrough:

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

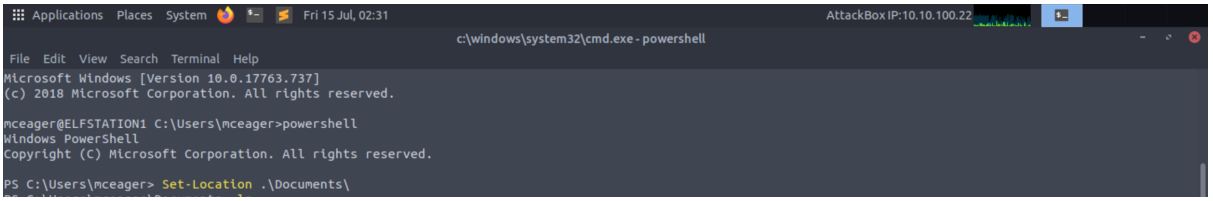
The -l command is used to specify our username and the hostname that we are connecting to.



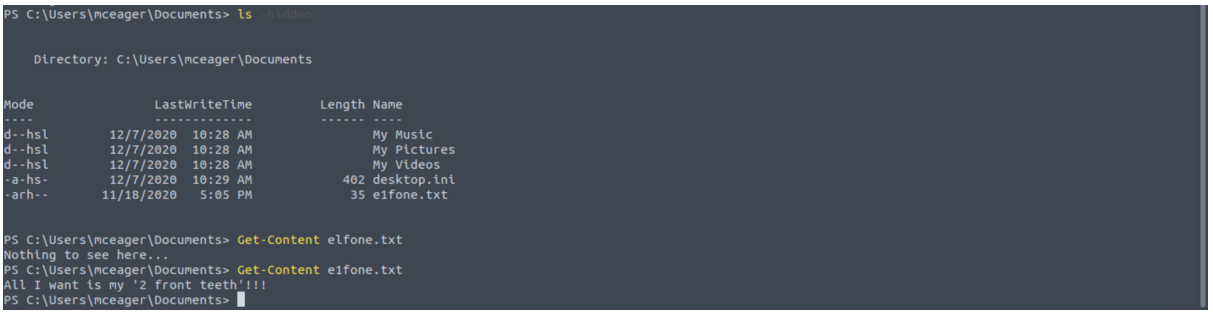
Answer: login name

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

Set-Location is used to set the working location to the Documents location.



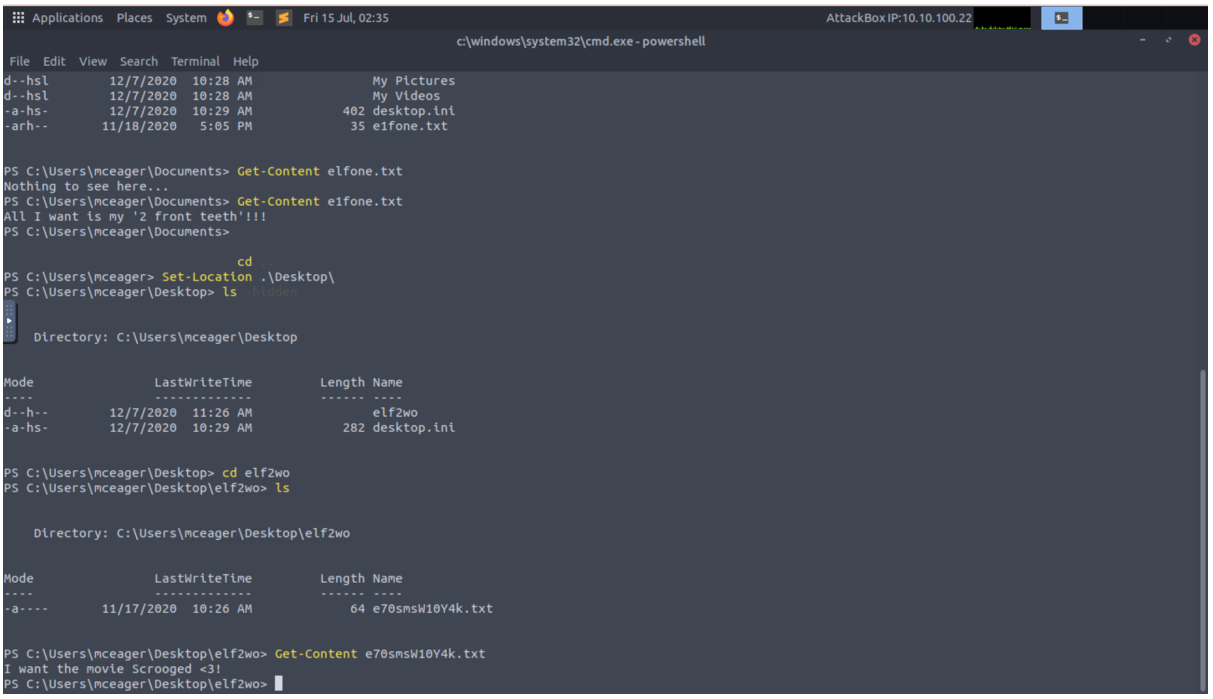
Get-Content is used to see the contents of the file.



Answer: <u>2 front teeth</u>

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?

Set-Location is used again to set working location to Desktop. **ls -Hidden** is used to get the list of the hidden folders. The content of the hidden folder can be found using **cd** command. Then, **Get-Content** is used to see the contents of the file.



Answer: <u>Scrooged</u>

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)

From Users directory, we changed to Windows directory by using **cd C:/Windows** command.

By using **cd System32**, we went into the System32 directory to get the list of hidden folders

Using the **ls -Hidden** command, the hidden folders can be found.

Answer: 3lfthr3e

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

By using **cd 3lfthr3e**, we get to change directory to the hidden folder which is the 3lfthr3e. Then, we used **Get-ChildItem -hidden** command to get the hidden items in the folder. The list can be found then. For this question, **Get-Content 1.txt | Measure-Object -word** is used to get the number of words that the file contains.

Answer: 9999

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

For this question, **(Get-Content 1.txt)[551,6991]** is used to get the words at index 551 and 6691 in the 1.txt file. Then, the words can be seen.

Answer: 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)

We used Get-Content 2.txt | Select-String -Pattern “redryder” to see what does Elf 3 want. Then, the words can be seen.

Answer: redryderbbgun

Thought Process/Methodology:

To start the task, we used **ssh -l mceager 10.10.212.200** to login name. Then, we used **Set-Location .\Documents** to set working locations to Documents. After that, to list out the hidden files in the Documents, **ls -Hidden** command was used and the list could be seen. Next, we used **Get-Content e1fone.txt** to get the content of the file to answer the question given. For the next task, the working location was changed from Documents to Desktop by using **Set-Location .\Desktop** and **ls -Hidden** was used to get the list of hidden folders. By using **cd** command, we got into the folder and **ls** command was used to list out the files from the folder. To see the content of the folder, **Get-Content e70smsW10Y4k.txt** . The answer for the question can be seen which is in the form of sentence **I want the movie Scrooged <3!** . Next task, to change from Users to Windows, **cd C:/Windows** was used and **cd System32** to get into the System32 folder. The **ls -Hidden** command again was used to list out the hidden folders and 3lfthr3e could be seen. We got into the folder by using **cd 3lfthr3e** command and **Get-ChildItem -Hidden** to get the list of the files inside the folder. Then, to get the number of words contained in the 1.txt file, **Get-Content 1.txt | Measure-Object -word** was used. The answer 9999 can be seen. After that, **(Get-Content 1.txt)[551,6991]** was used to see the words at index 551 and 6991 which are Red and Ryder. Next, **Get-Content 2.txt | Select-String -Pattern “redryder”** was used to get the items that Elf 3 wants which is redryderbbgun that could be seen next.