PSP0201

Week 5

Writeup

Group Name: F4urDeveloper

Members:

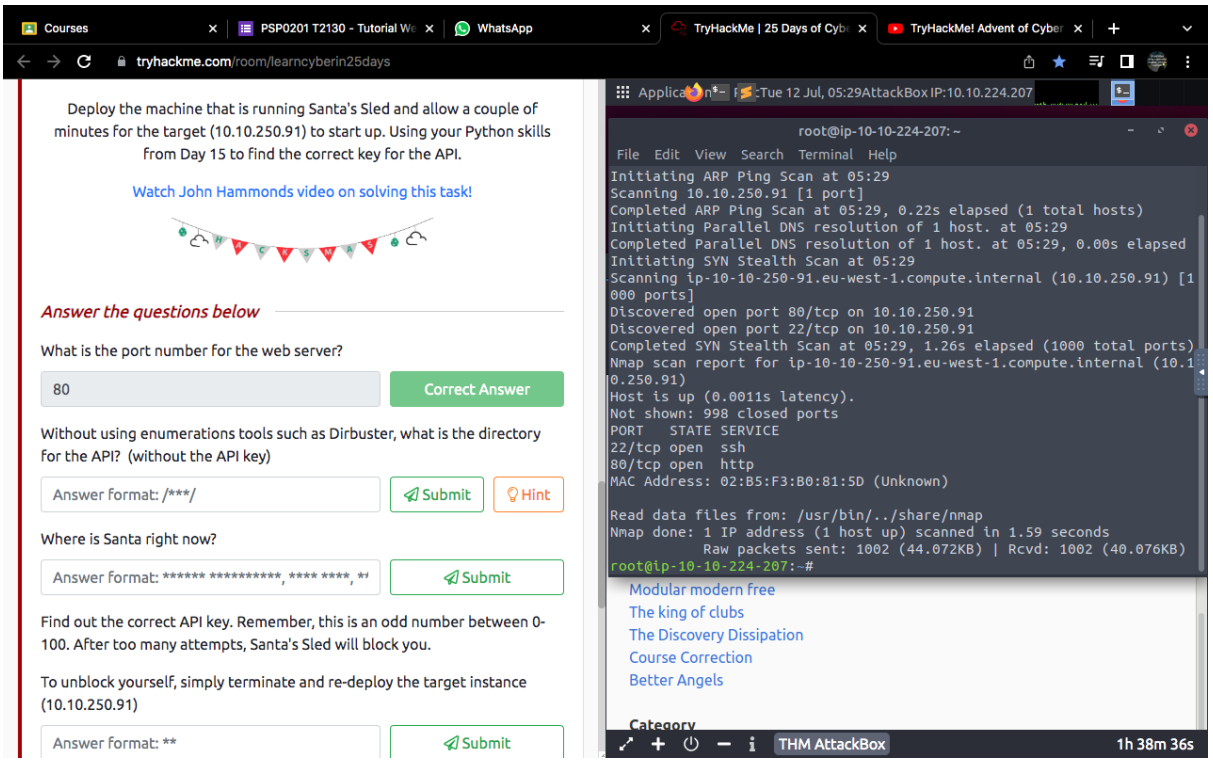
ID	NAME	ROLE
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	LEADER
1211104237	ALIA MAISARA BINTI SHAHRIN	MEMBER
1211102287	TERRENCE CHENG	MEMBER
1211101153	MISCHELLE THANUSHA JULIUS	MEMBER

Day 16:Scripting Help! Where is Santa?

Tools used: THM Attackbox

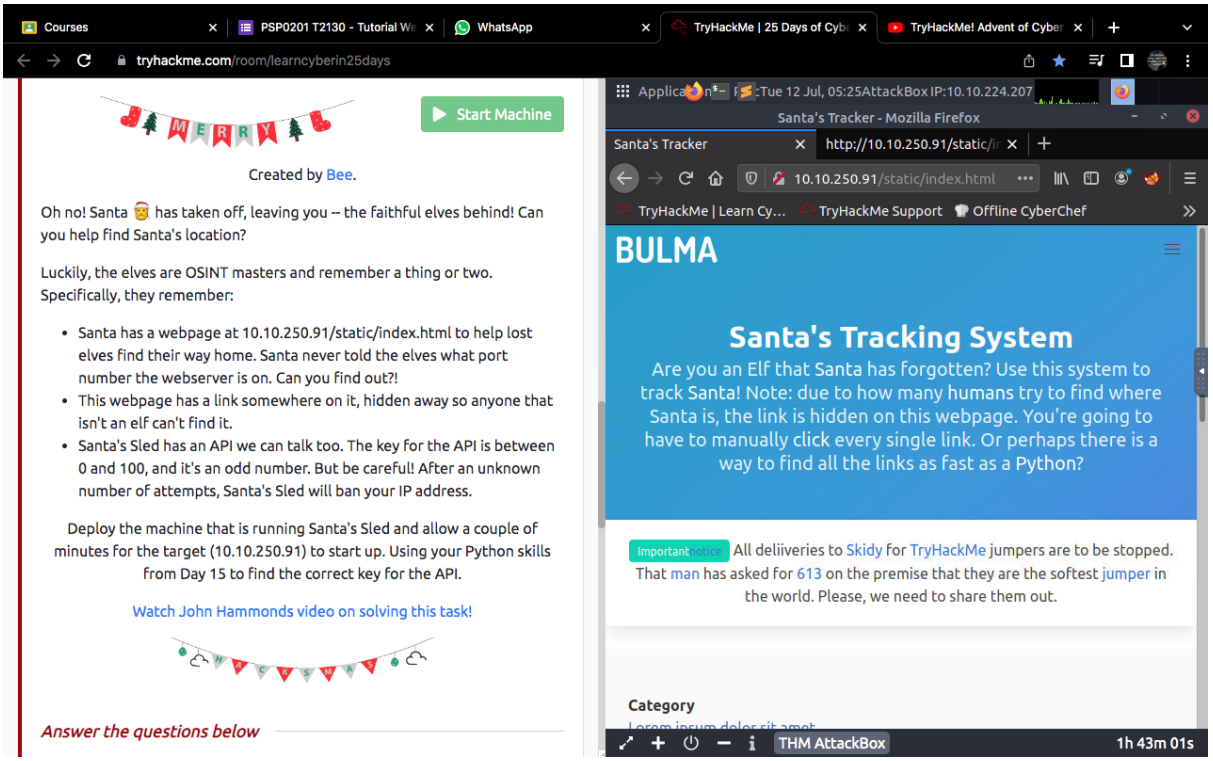
Solution/walkthrough:

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



The port number for this web server is 80.

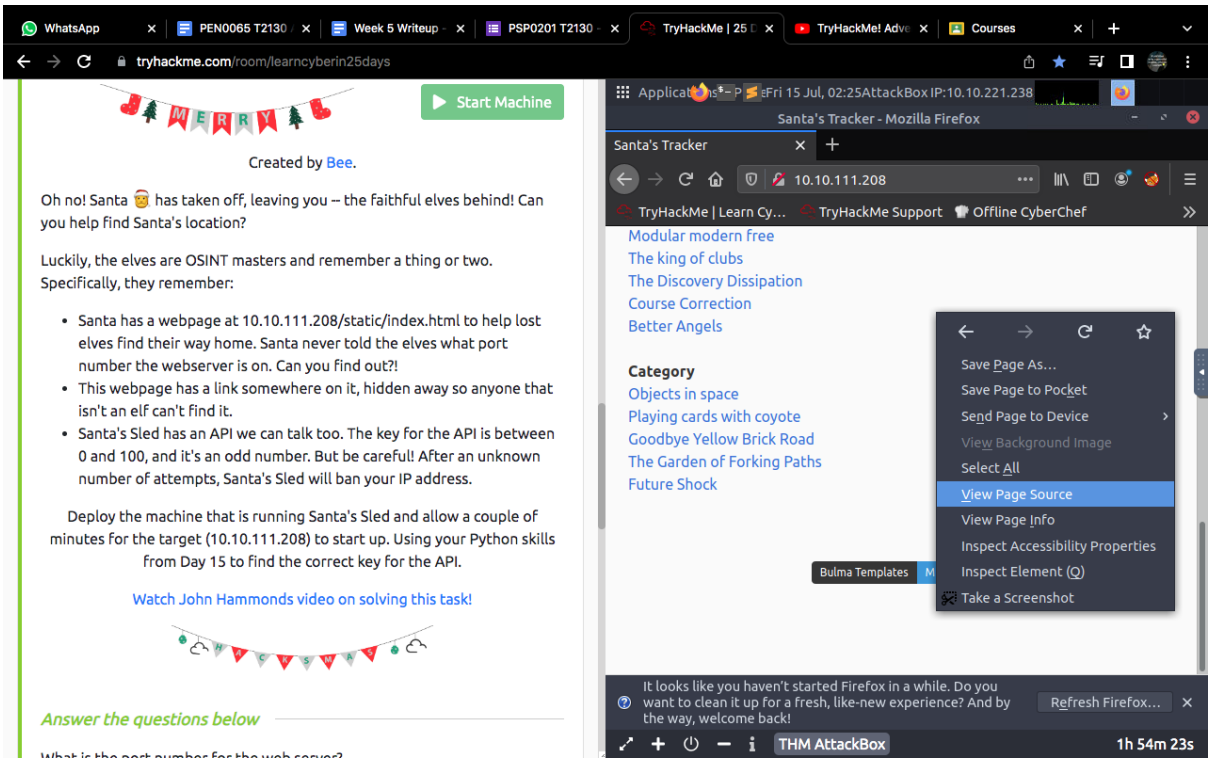
Question 2
What templates are being used?

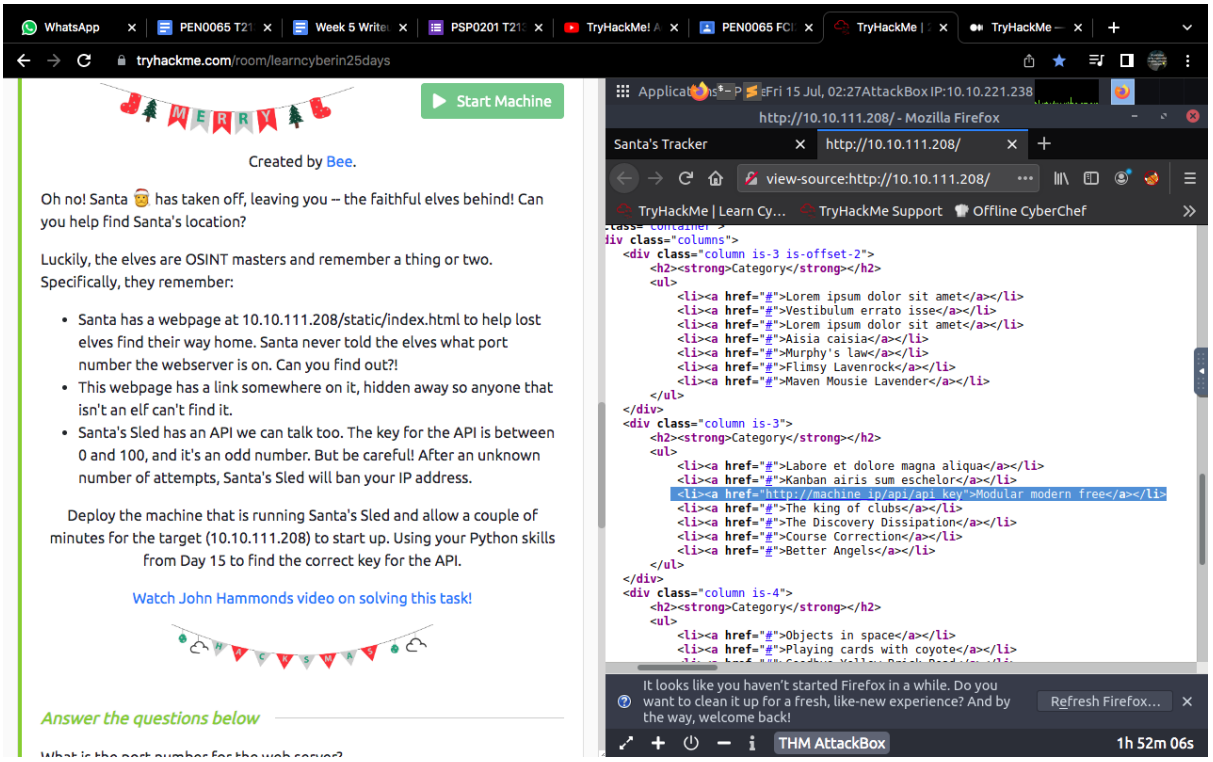


The template are being used is BULMA

Question 3

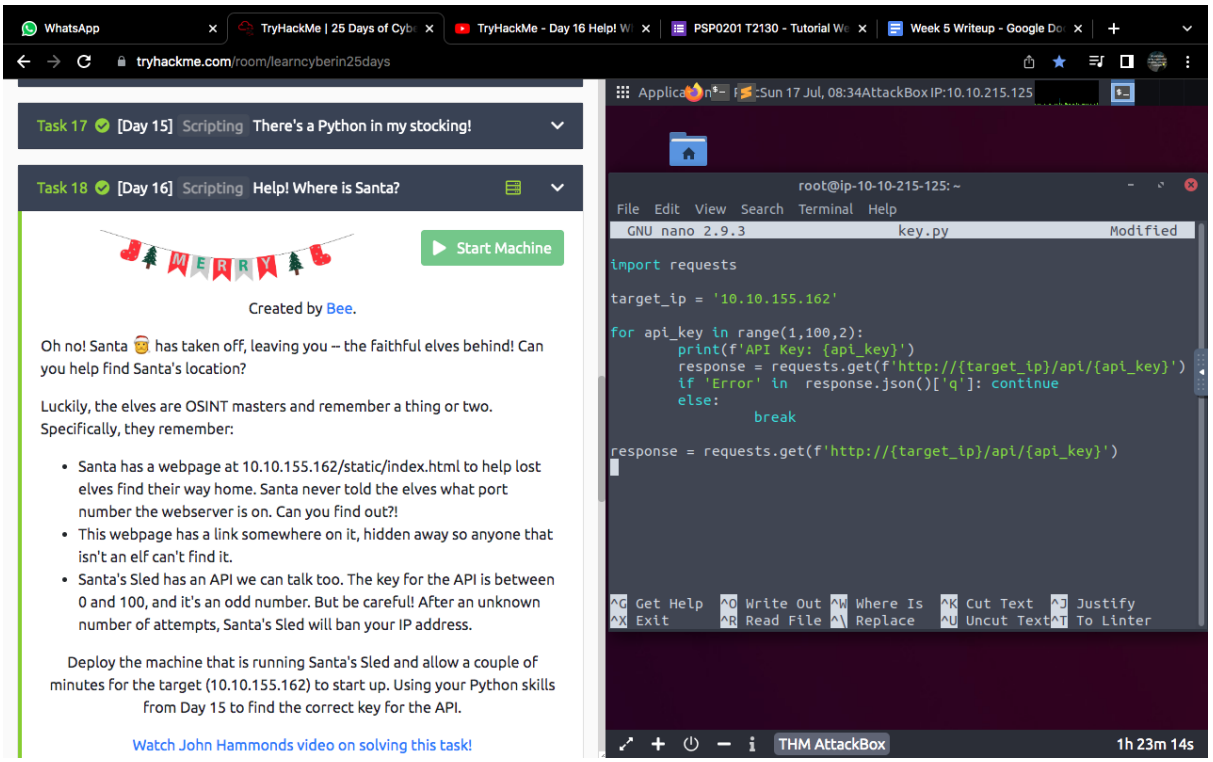
Without using enumeration tools such as Dirbuster, what is the directory for the API?

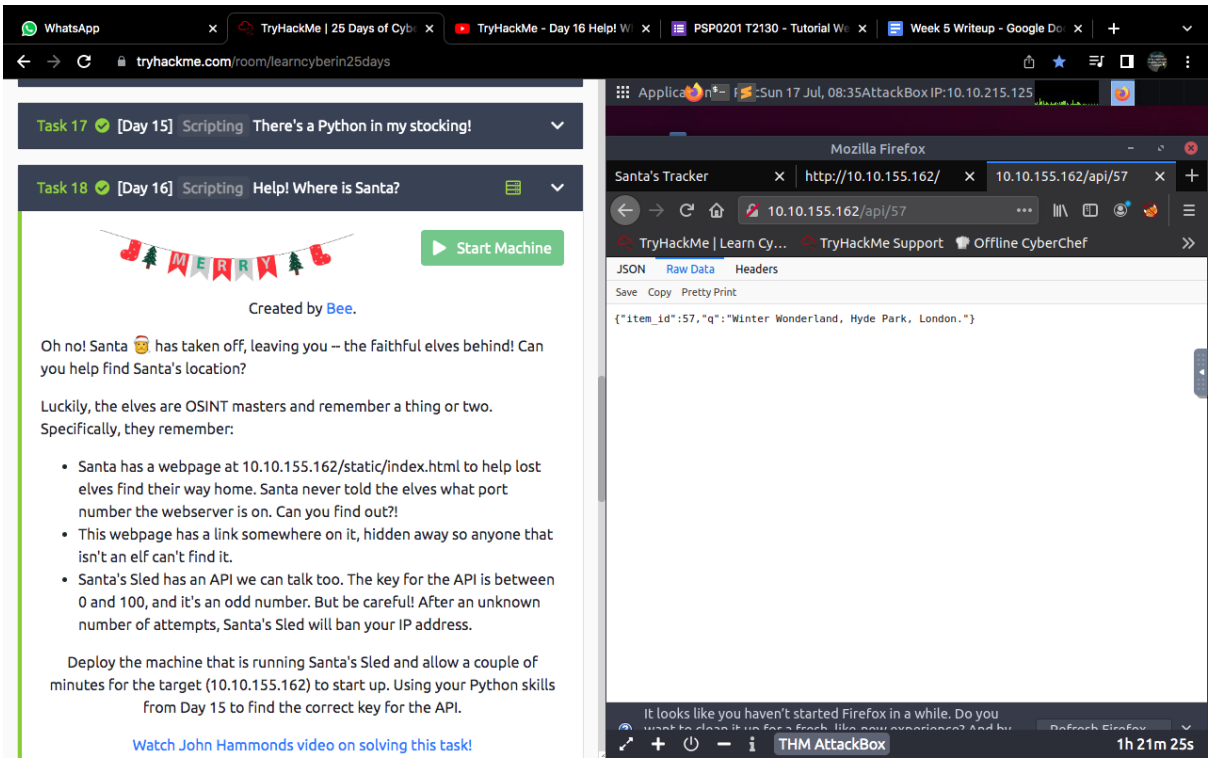




Question 4

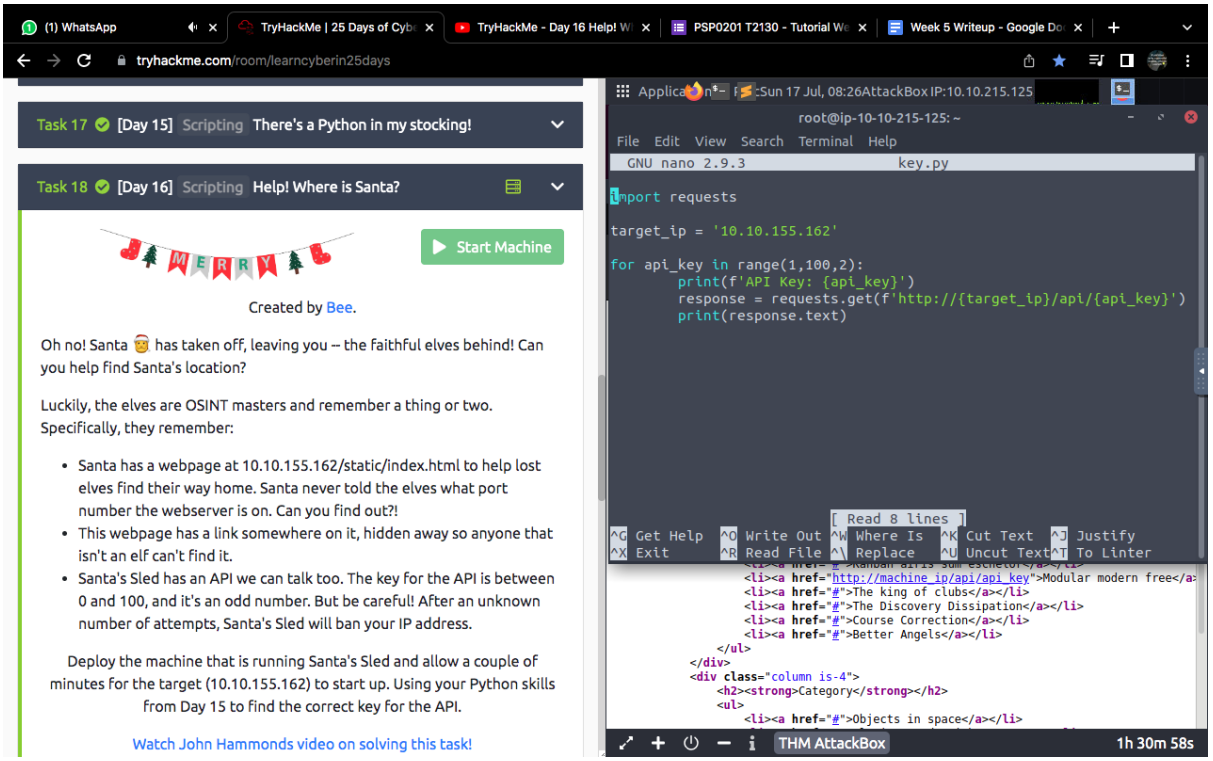
Go the API endpoint. What is the Raw Data returned if no parameters are entered?

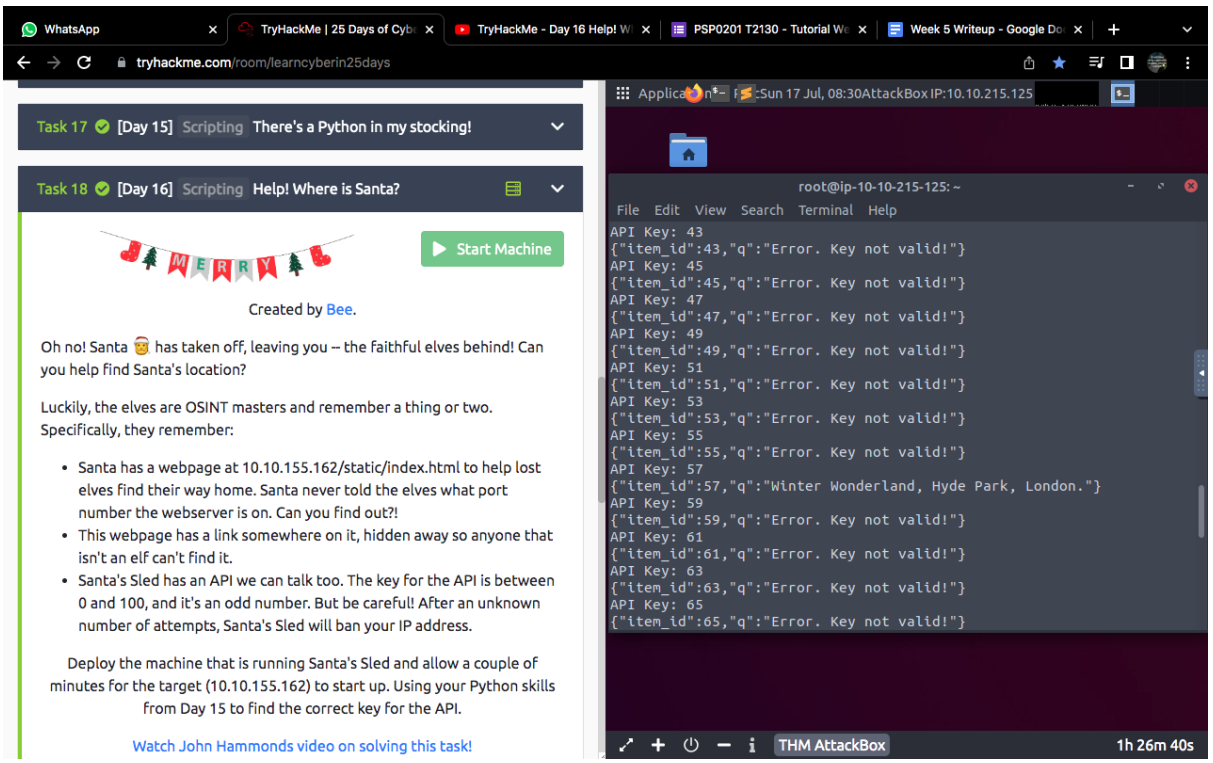




Question 5

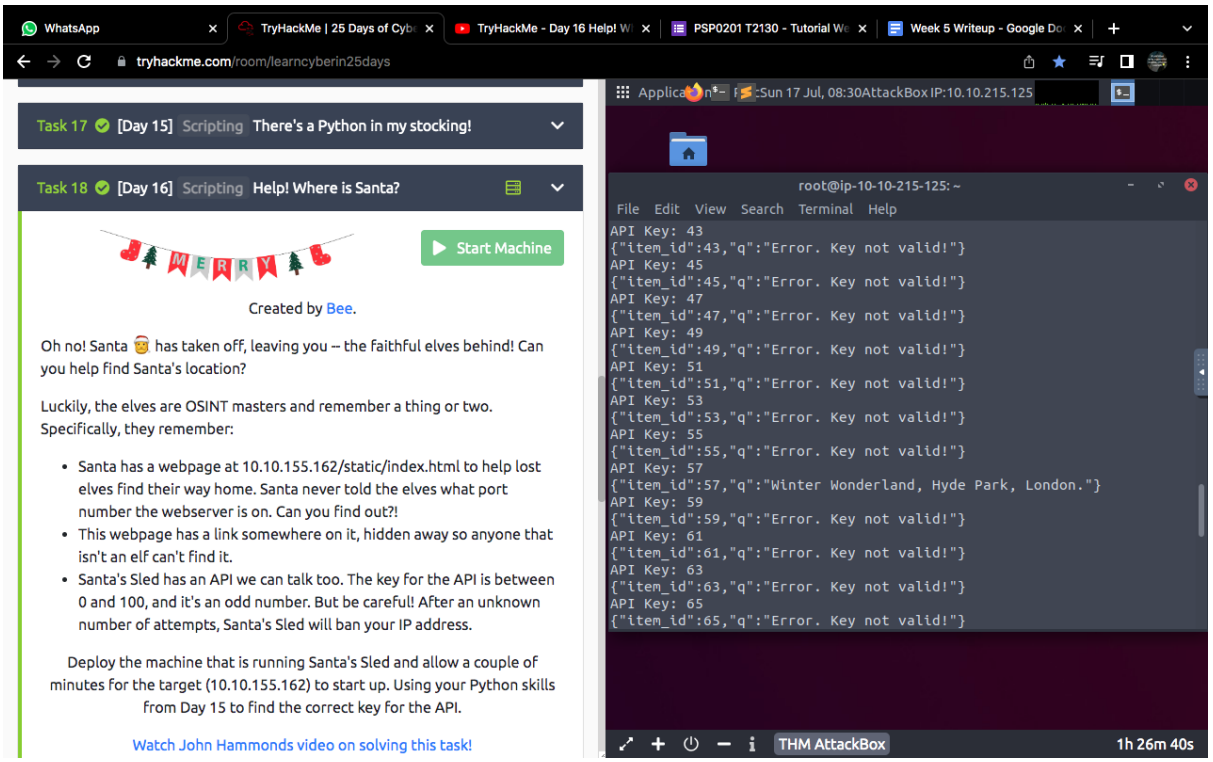
Where is Santa right now?





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.



Thought Process/Methodology:

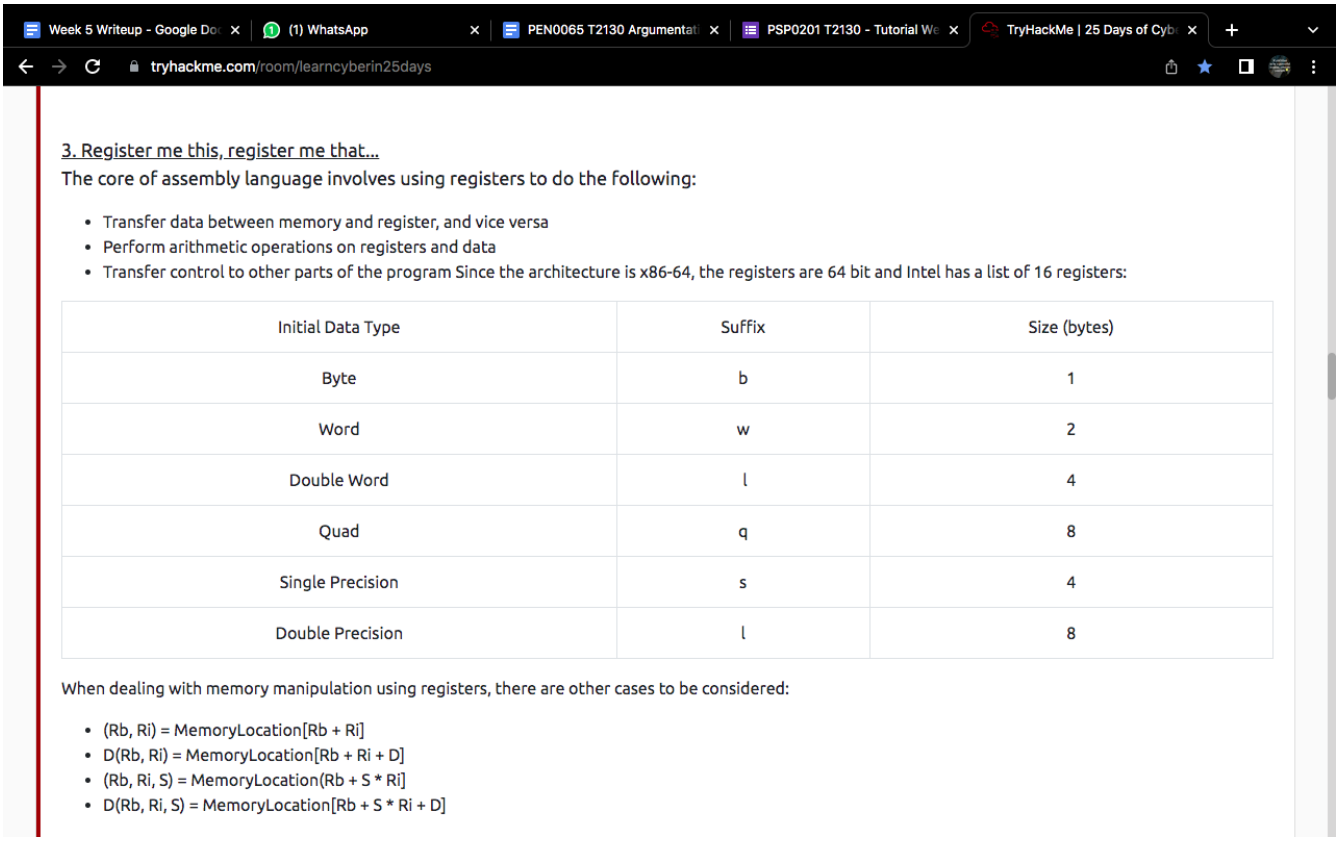
As for question 1, simply type in nmap (ip address) and run to get the port number for the web server. For question 2, go to firefox n type in (ip address : port number) to get the template that has been used for Santa's Tracking System. Next, for question 3, go to the template as in question 2 and right 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:

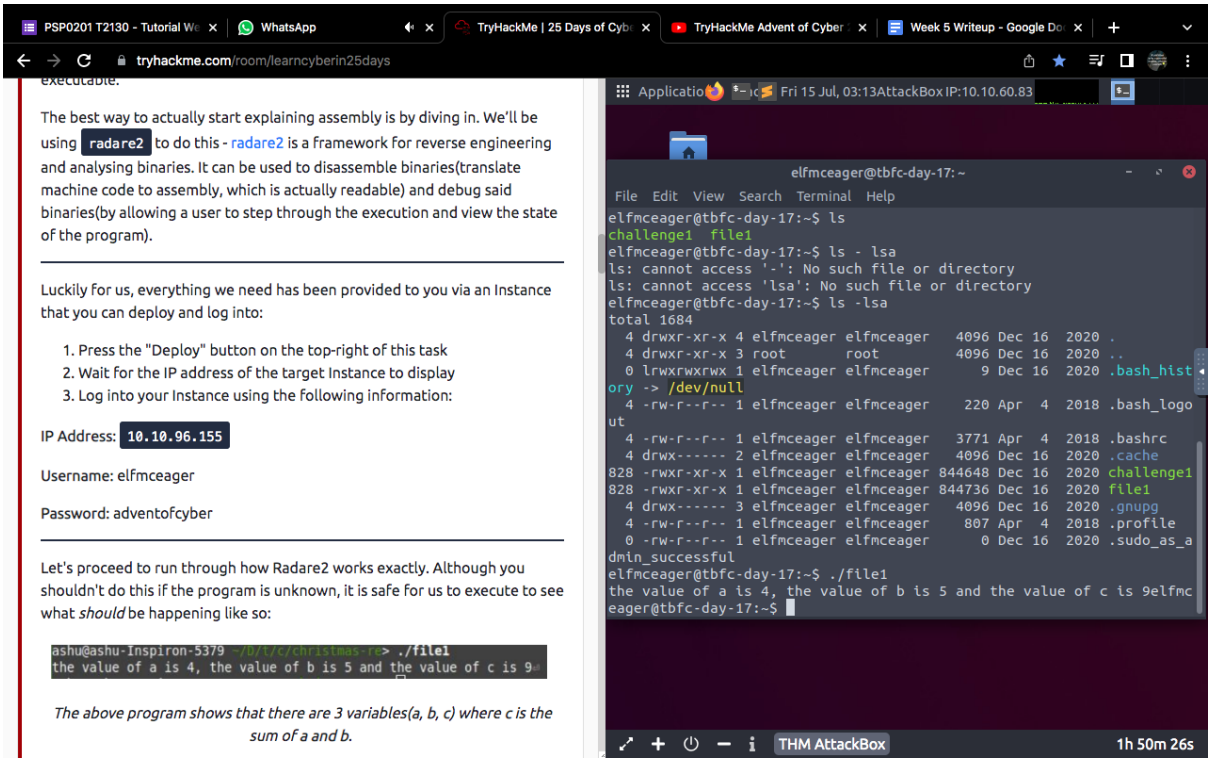
Initial Data Type	Suffix	Size (bytes)
Byte	b	1
Word	w	2
Double Word	l	4
Quad	q	8
Single Precision	s	4
Double Precision	l	8

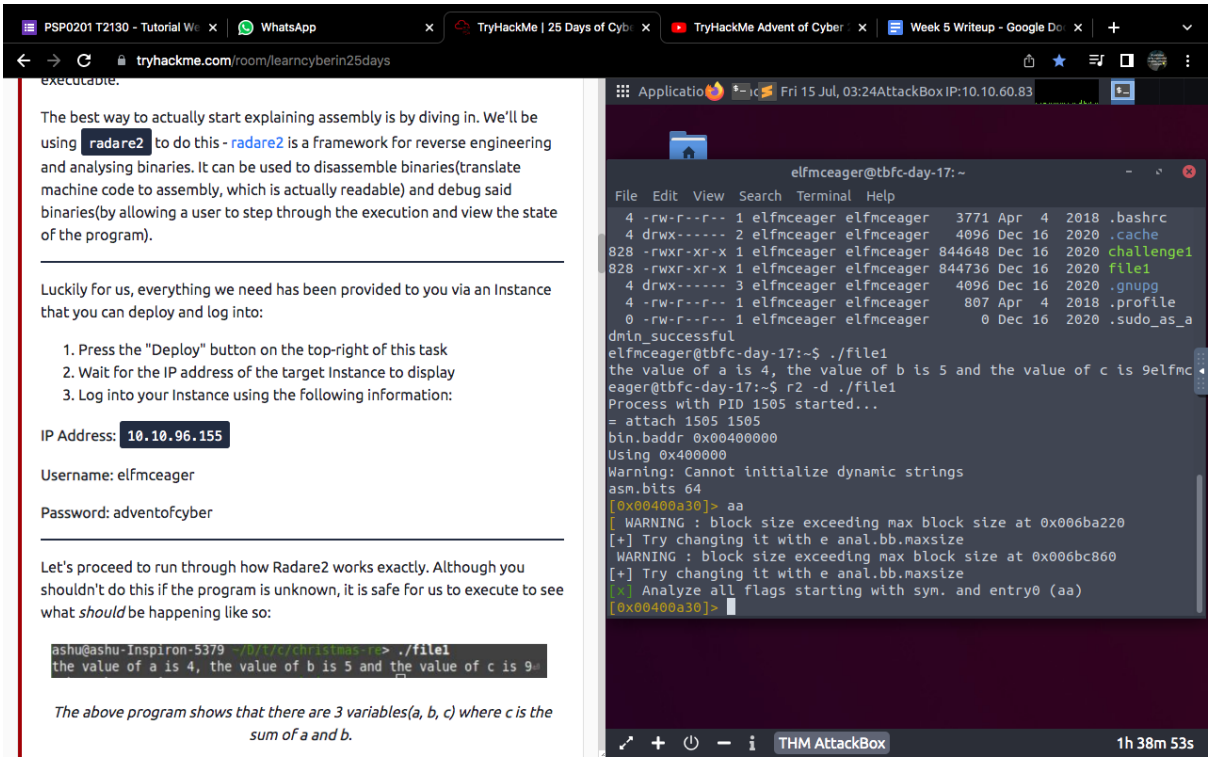
When dealing with memory manipulation using registers, there are other cases to be considered:

- (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?

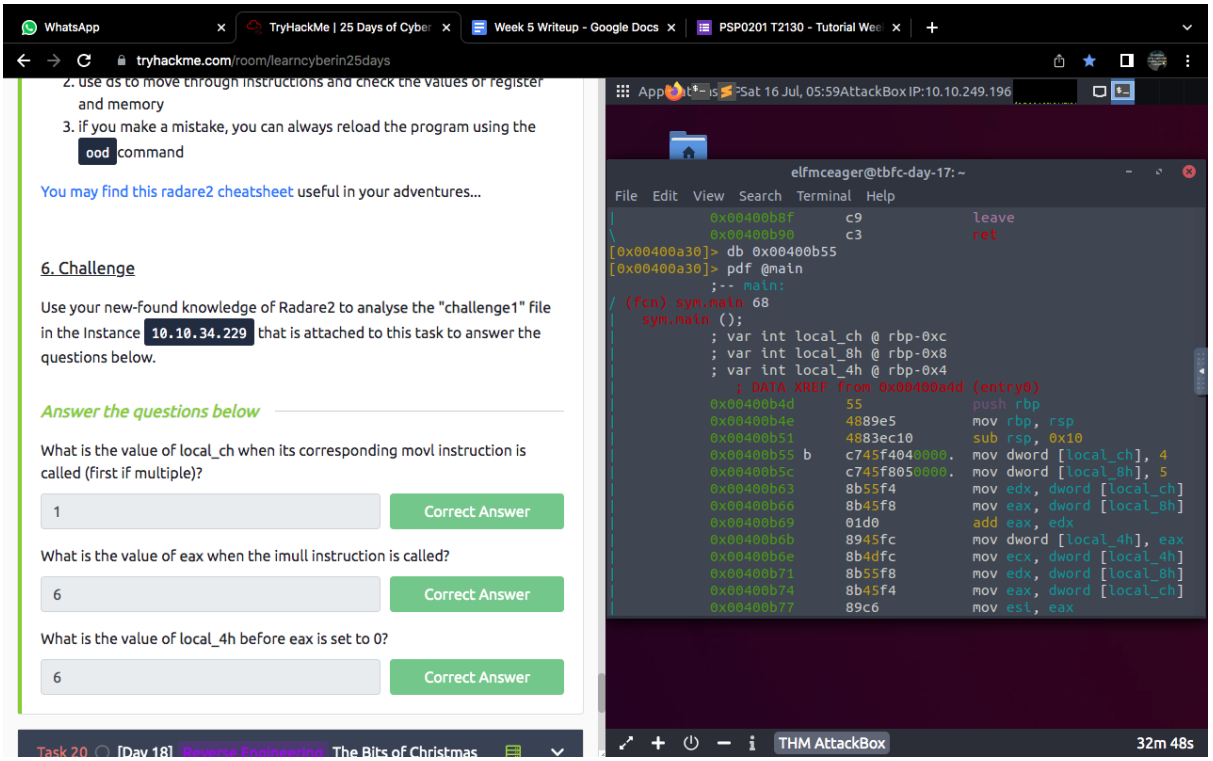




The command to analyse the program in radare2 is aa.

Question 3

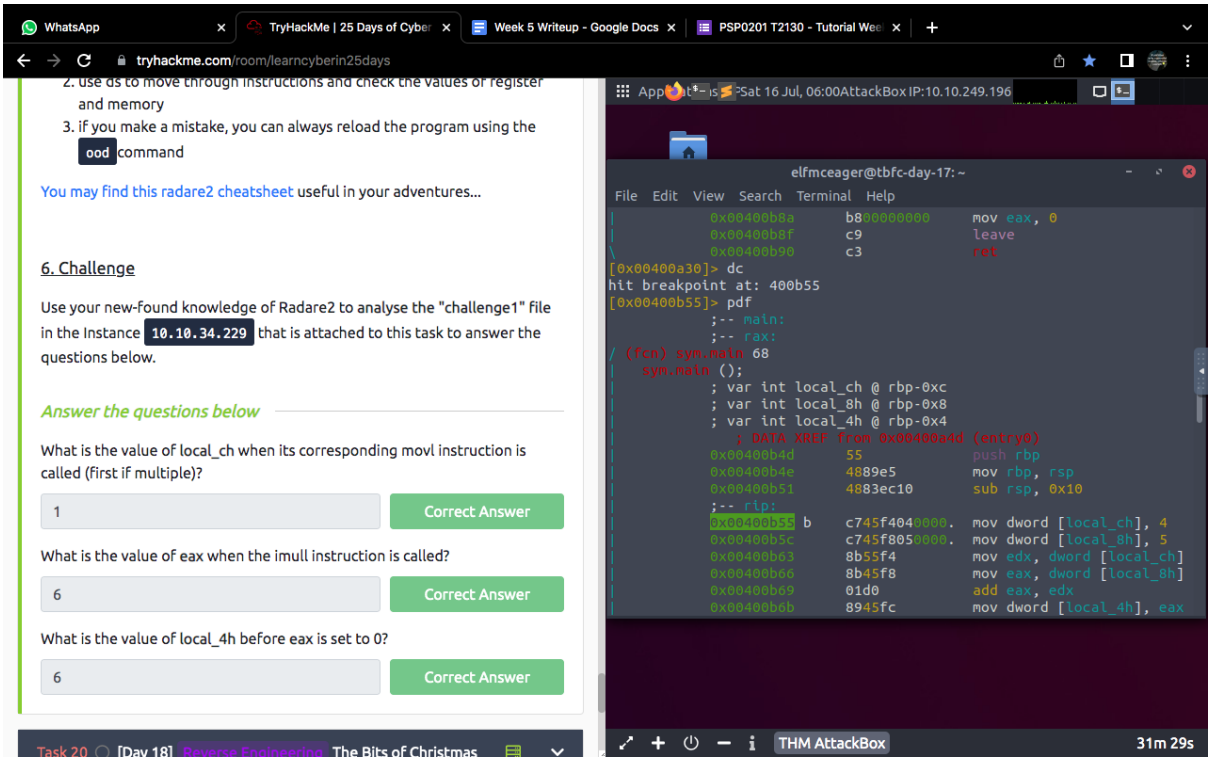
What is the command to set a breakpoint in radare2?



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

Question 4

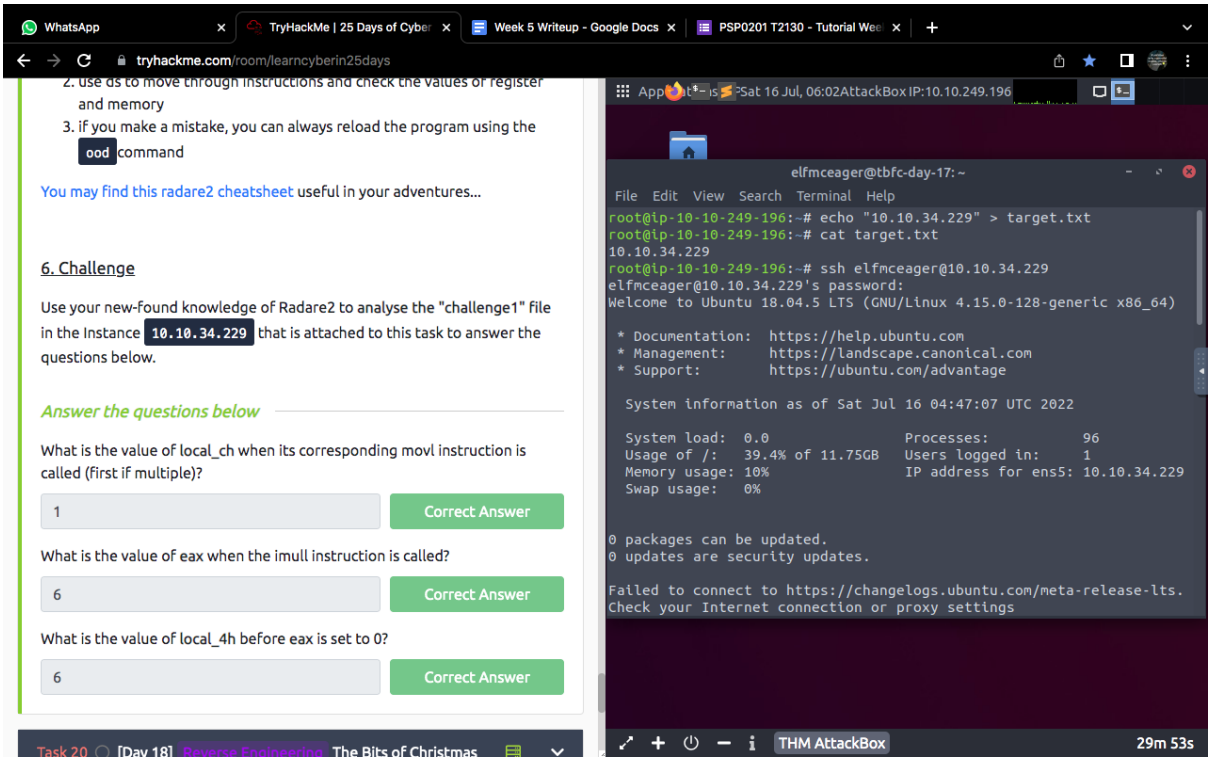
What is the command to execute the program until we hit a breakpoint?

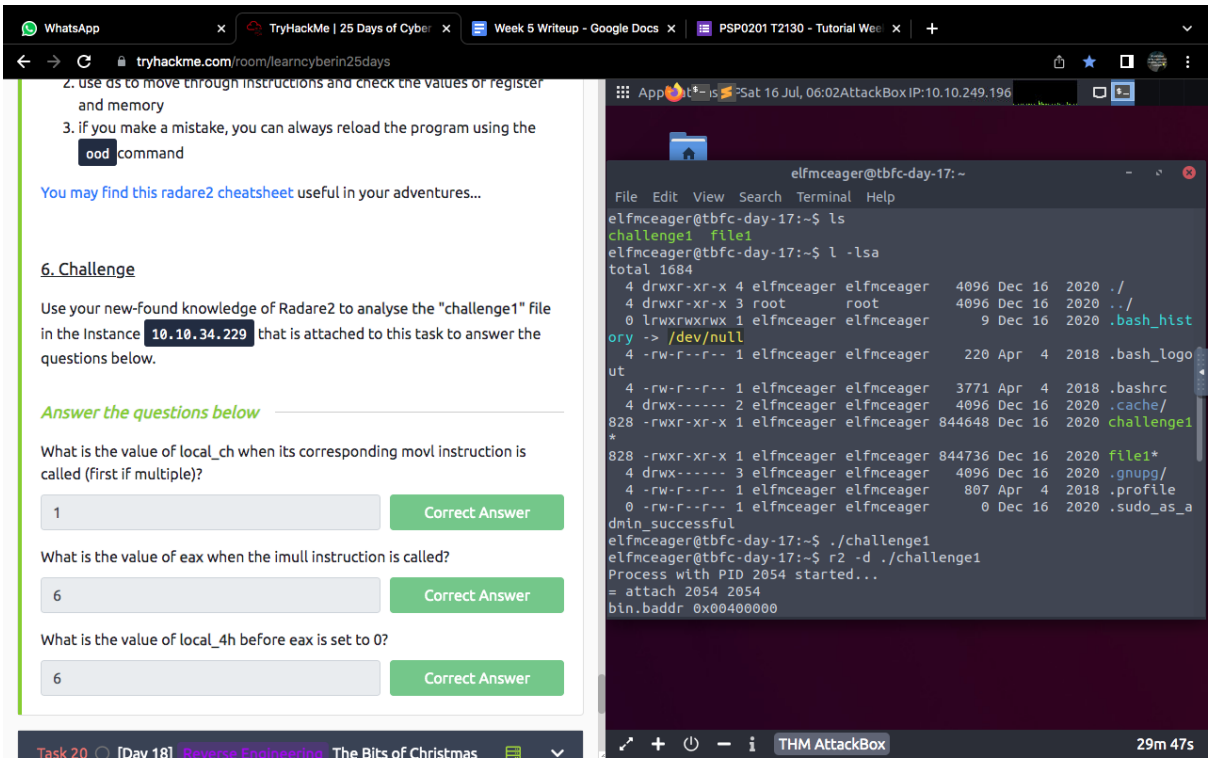


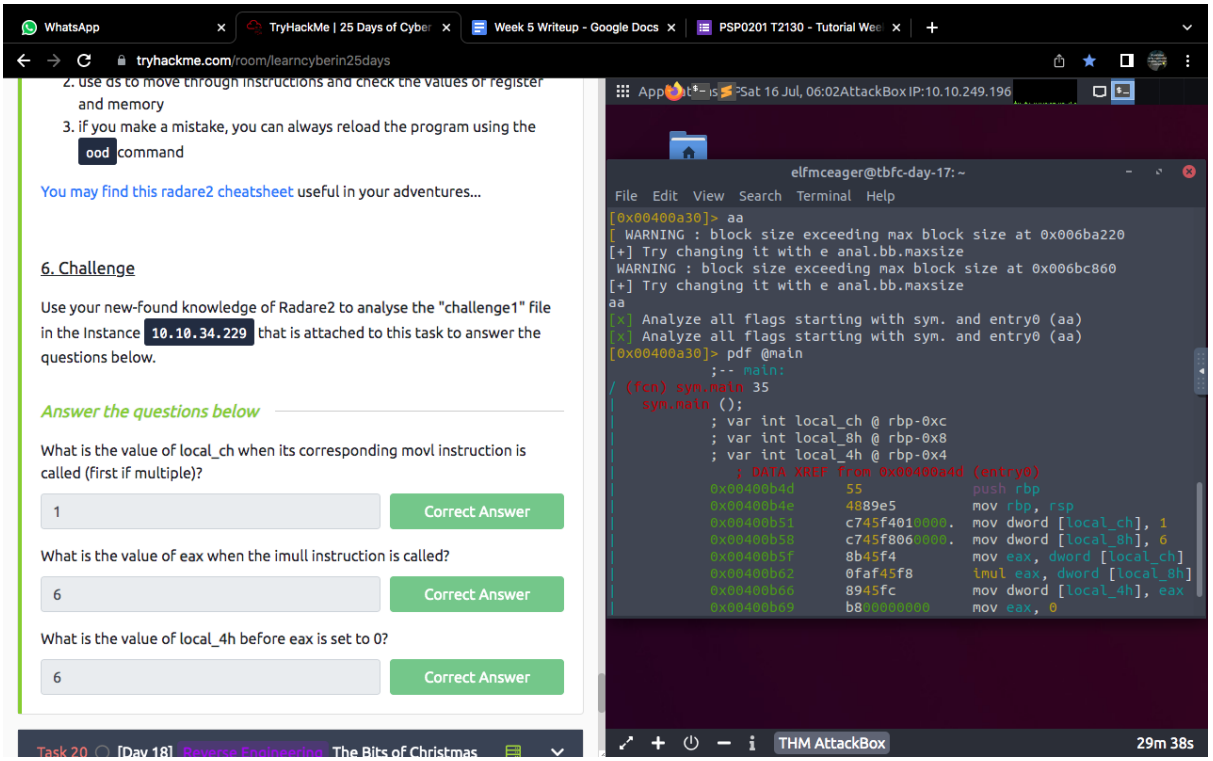
The command to execute the program until hit the breakpoint is dc.

Question 5

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



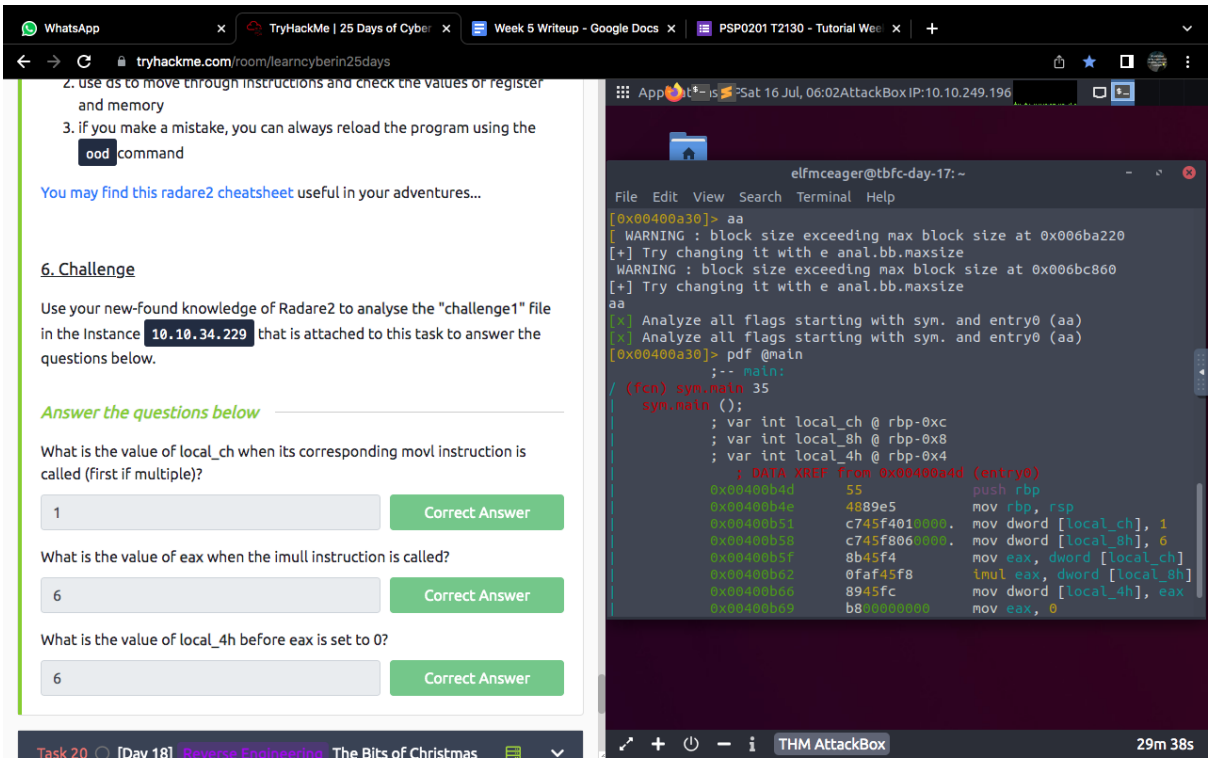




The value of local_ch when its corresponding movl instruction is called 1

Question 6

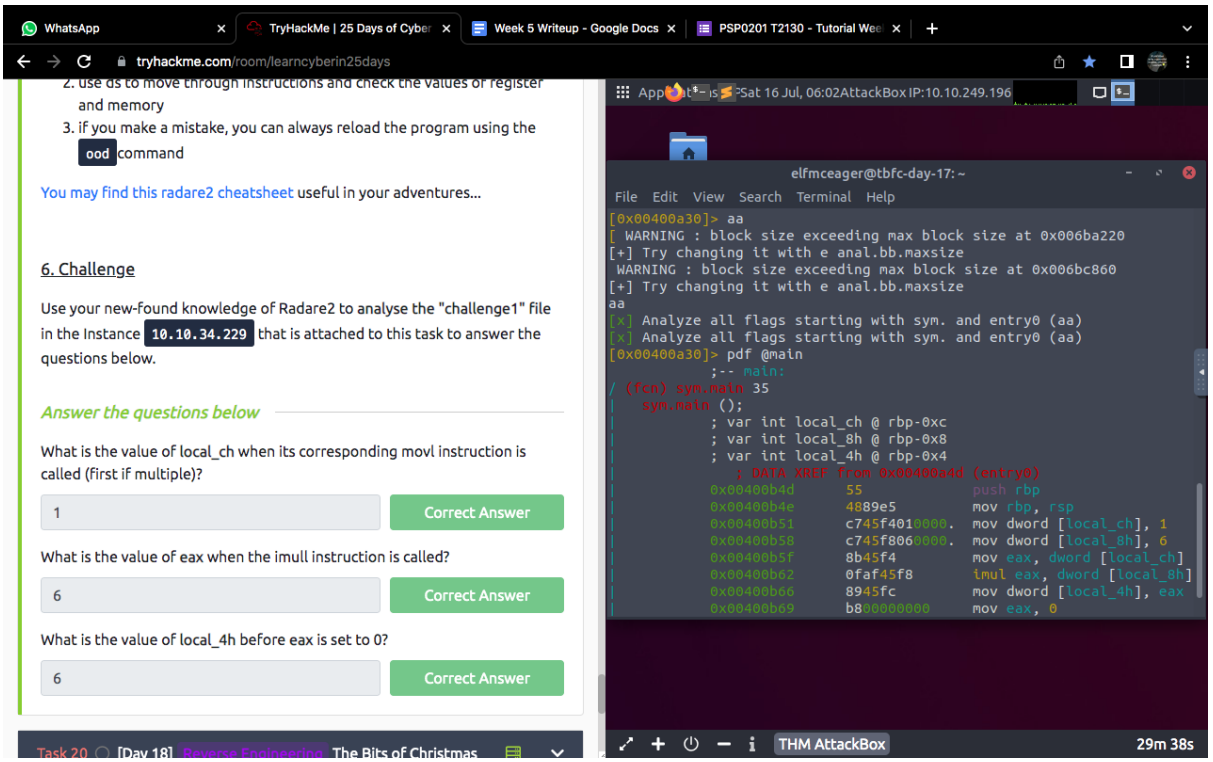
What is the value of eax when the imull instruction is called?



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

Thought Process/Methodology:

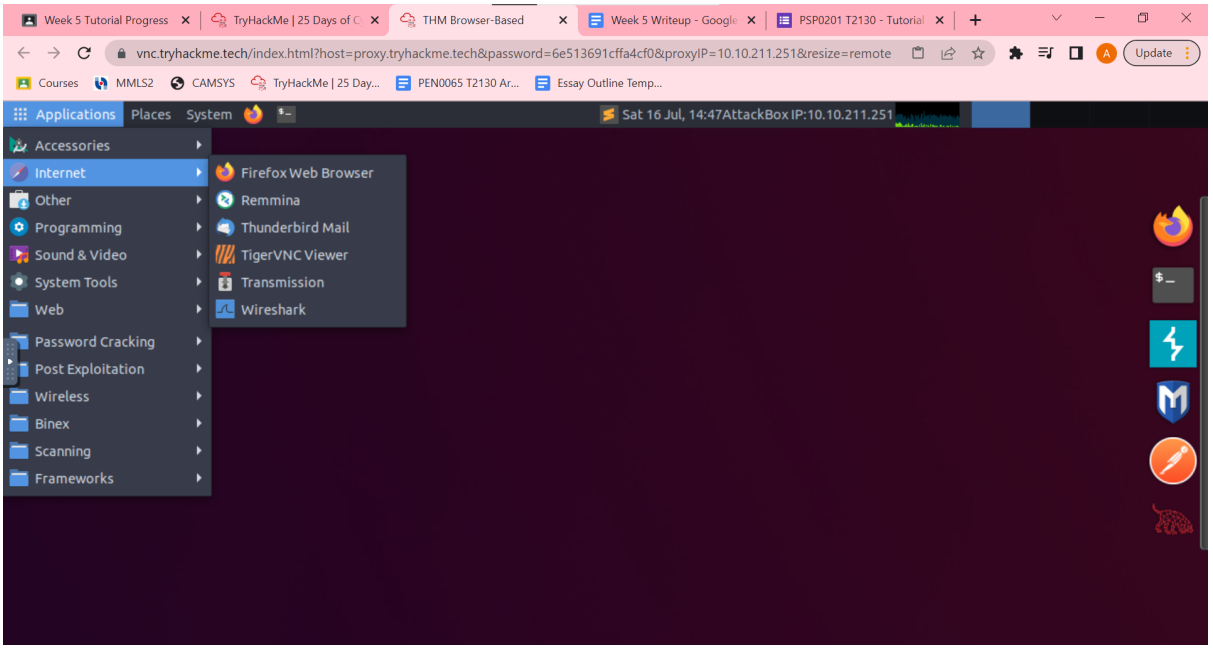
As for question 1, the data types is as above . For question 2, to find the command that analyse the program in radare2, simply press ssh elfmceager@(ip address), ls, ls -lsa , ./file1, r2 -d ./file 1 and lastly press aa. Next for question 3, press afl | grep main and db 0x00400b55 and pdf @main to set 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

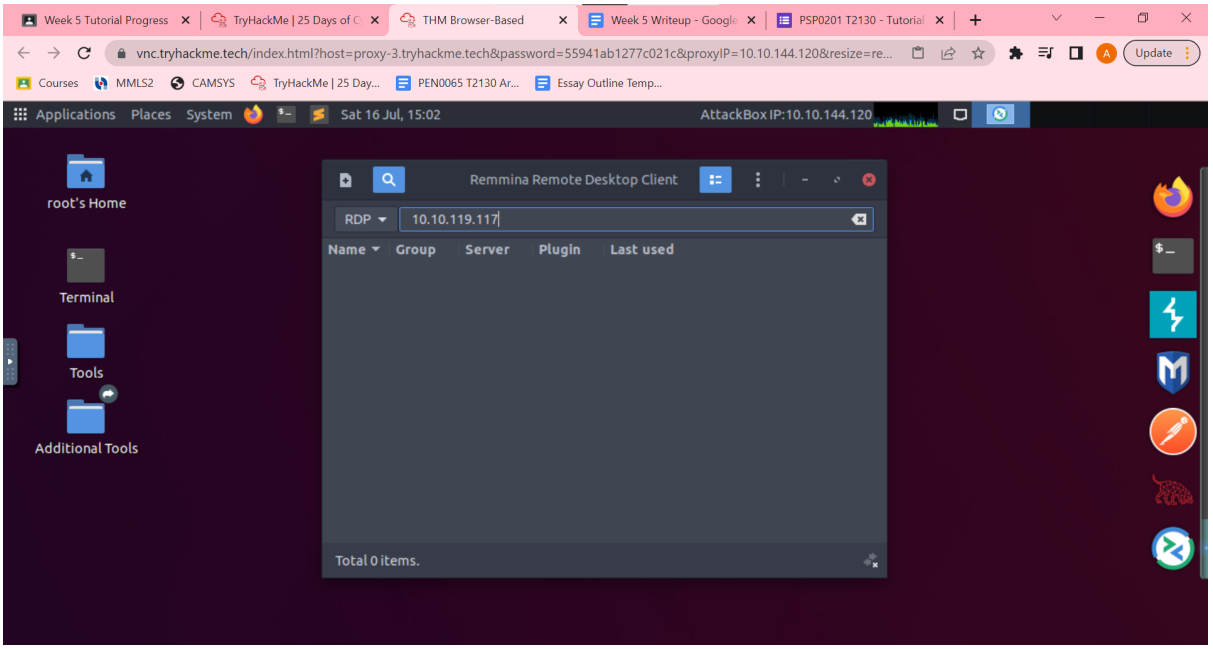
Solutions / Walkthrough :

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

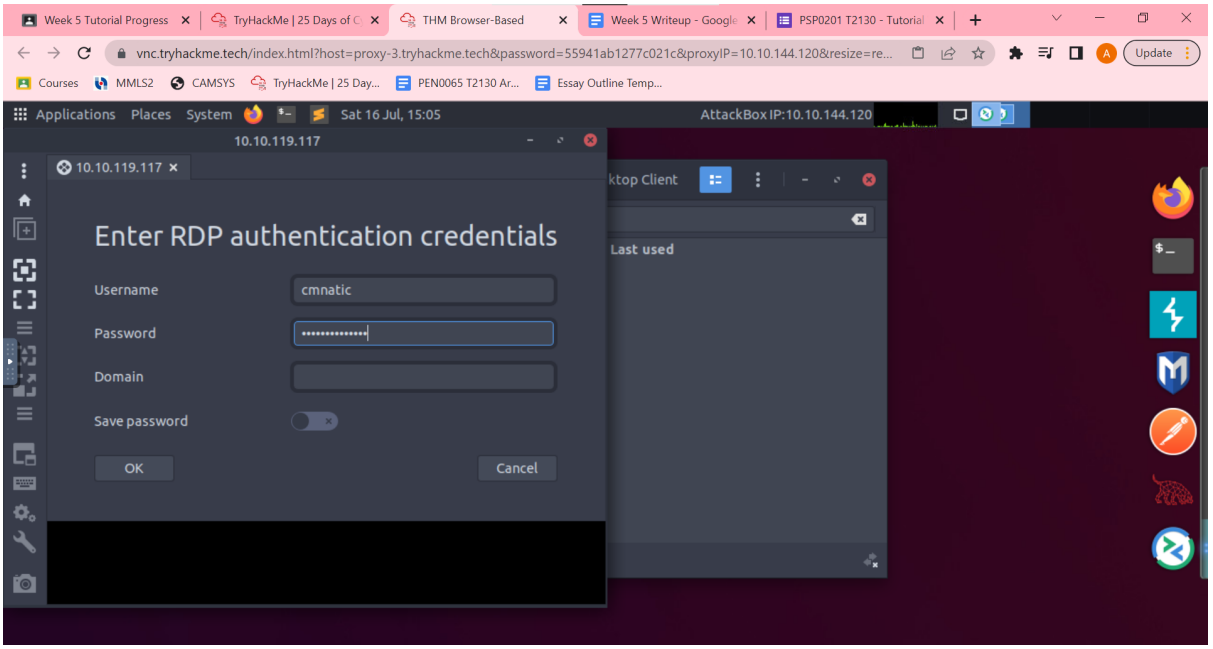


Q1: What is the message that shows up if you enter the wrong password for TBFC_APP?

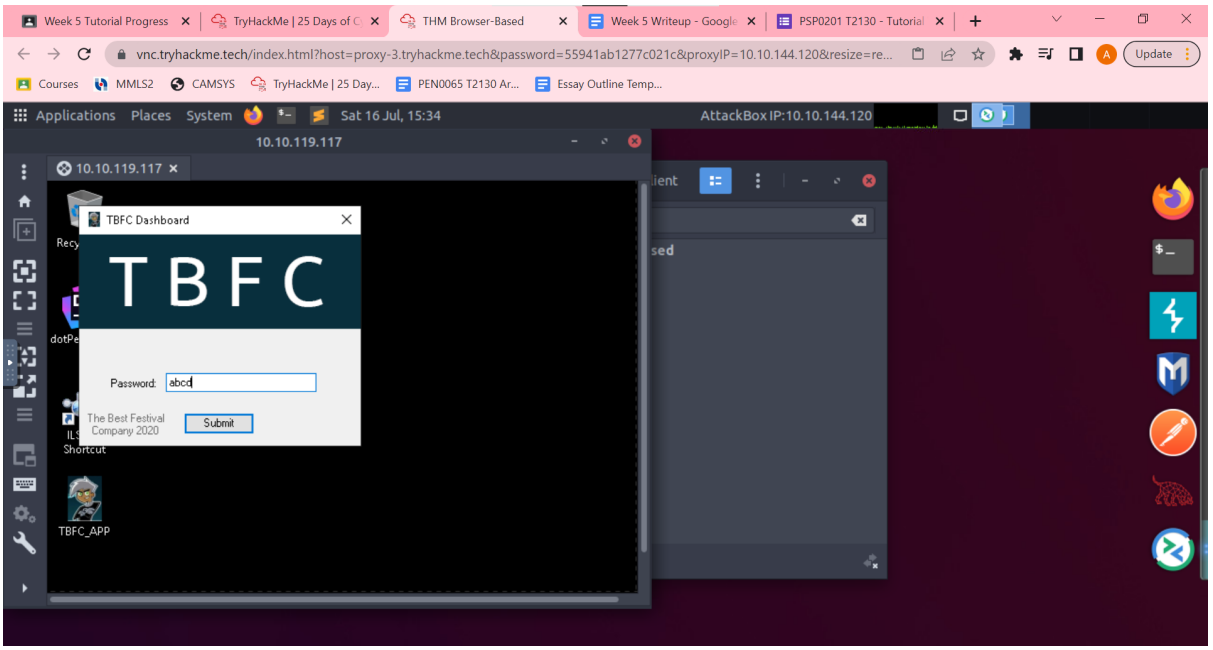
Enter the IP address given.



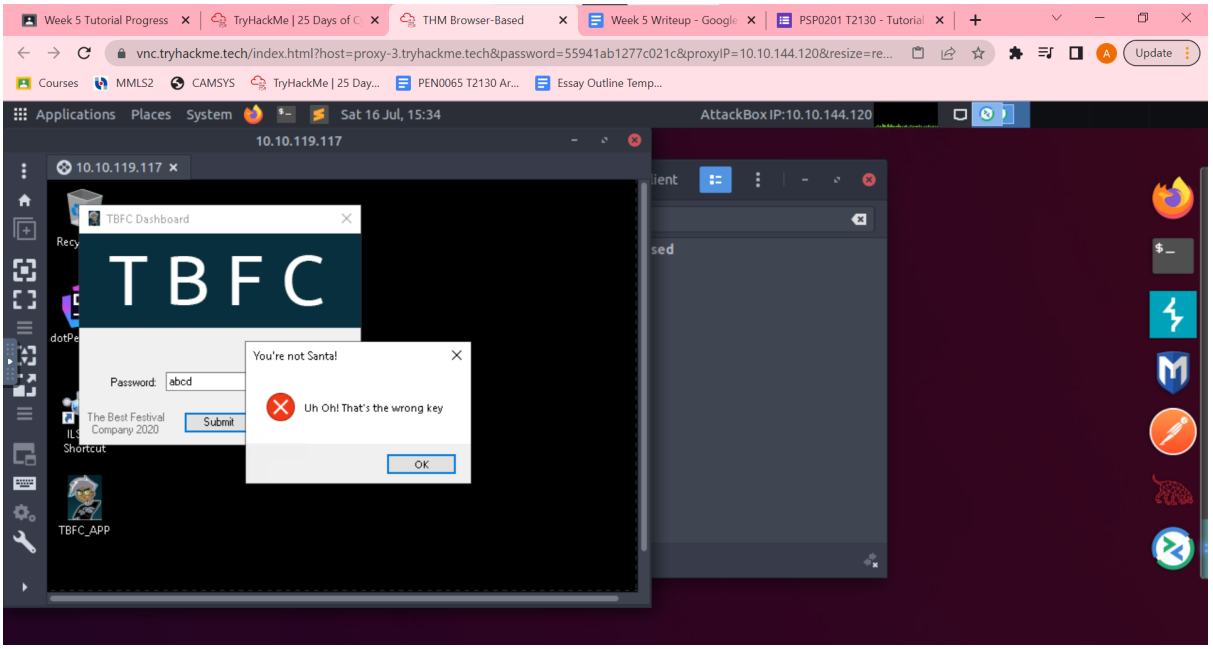
Enter the username and password.



Enter a wrong password.

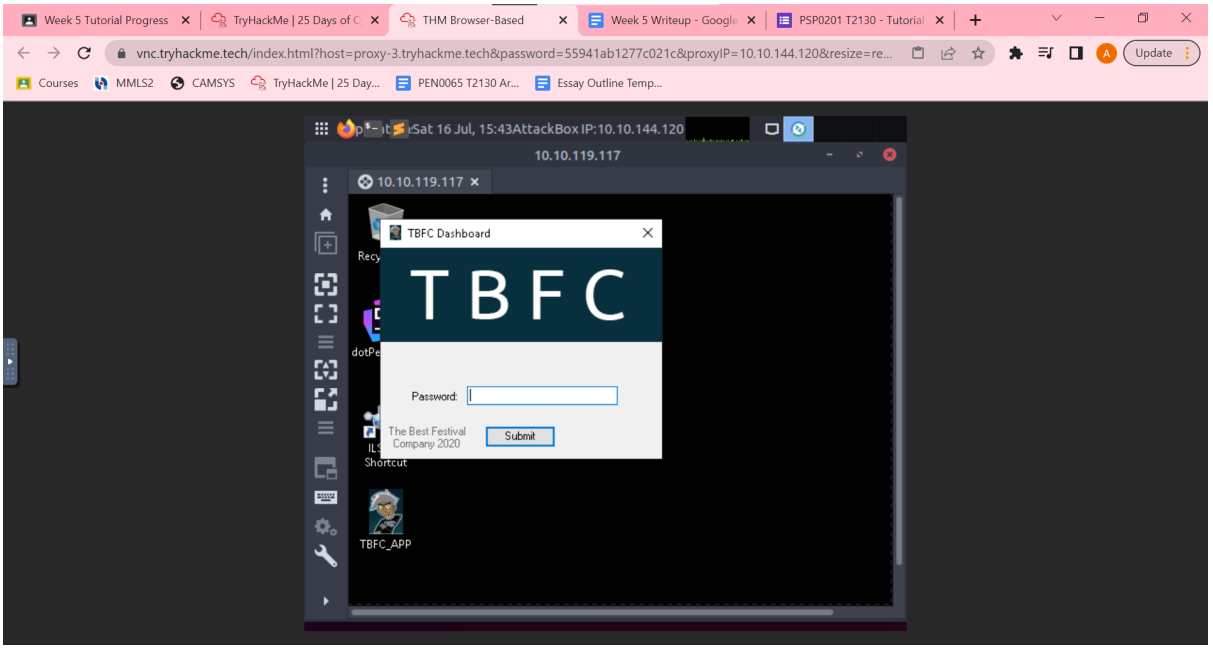


The message that shows up is Uh Oh! That's the wrong key



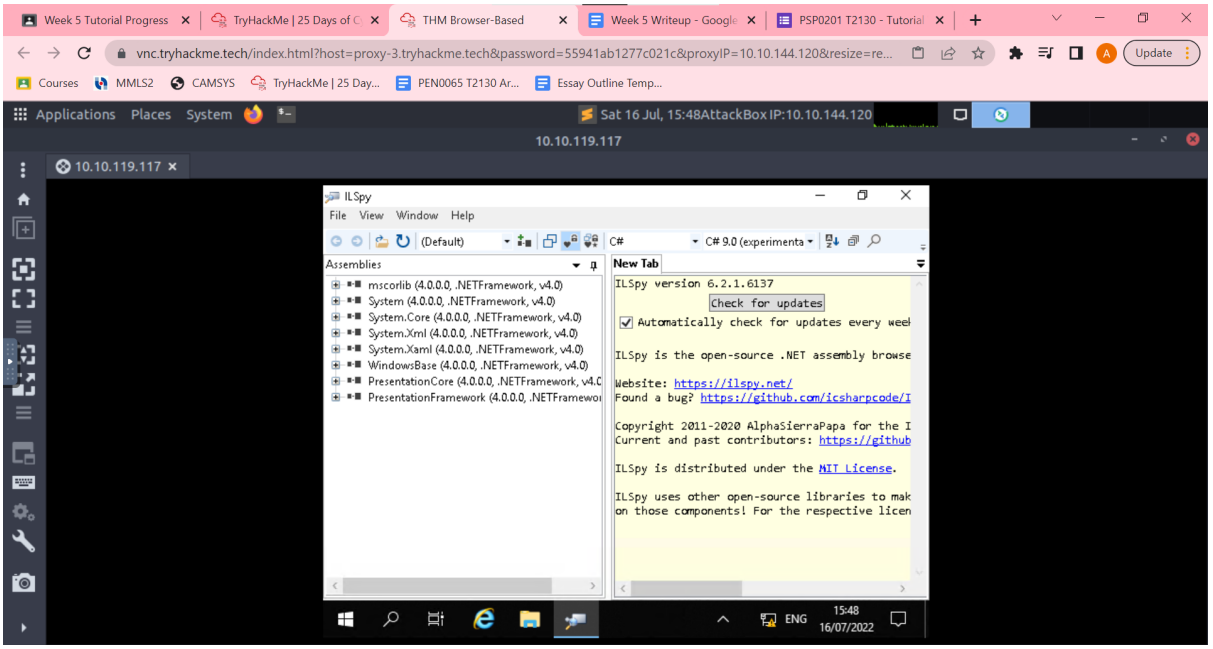
Q2: What does TBFC stand for?

The Best Festival Company

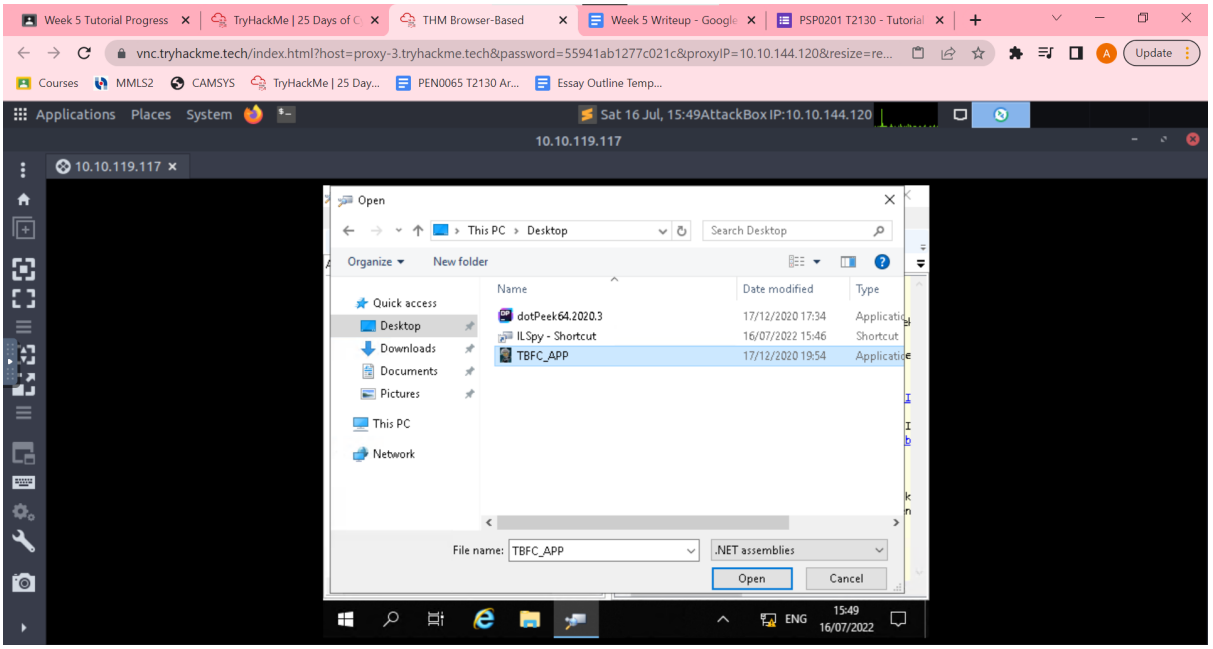


Q3: Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?

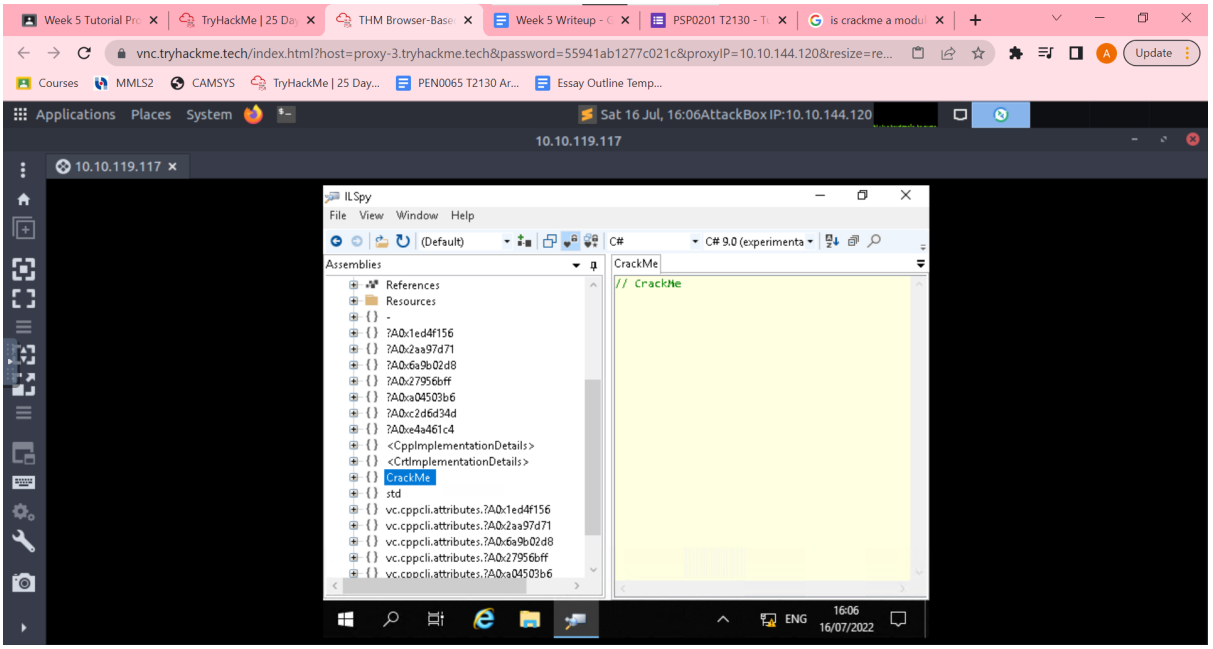
Open ILSpy



Open TBFC-App in ILSpy

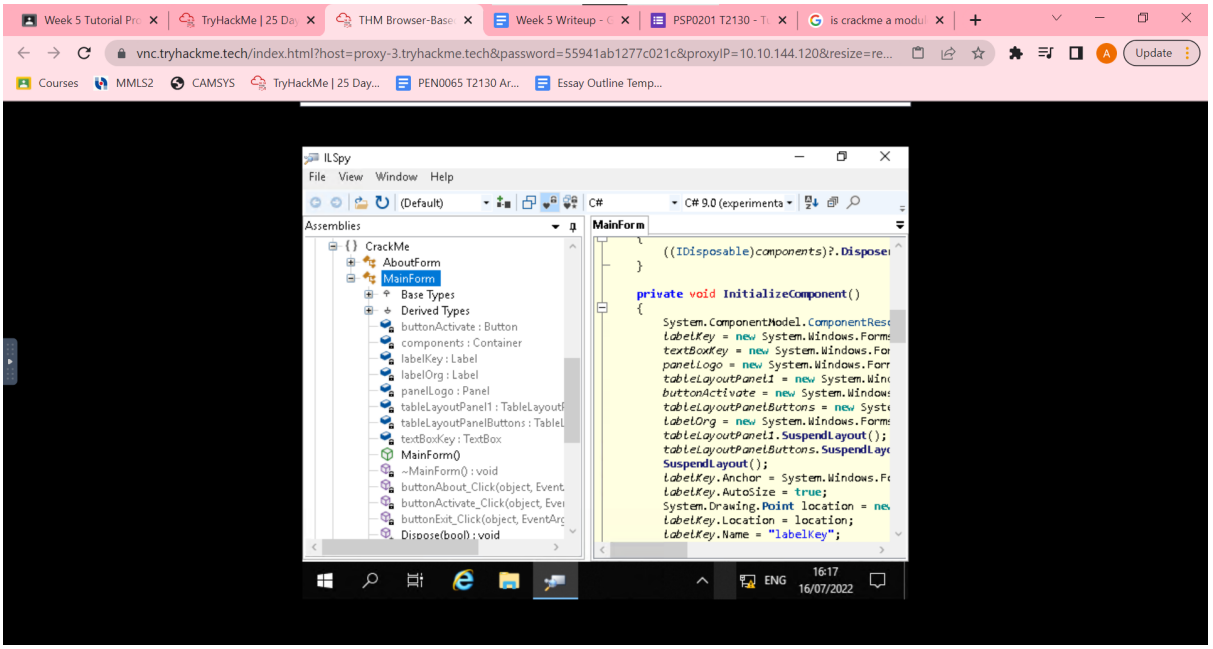


Decompile the TBFC-App and the answer is CrackMe



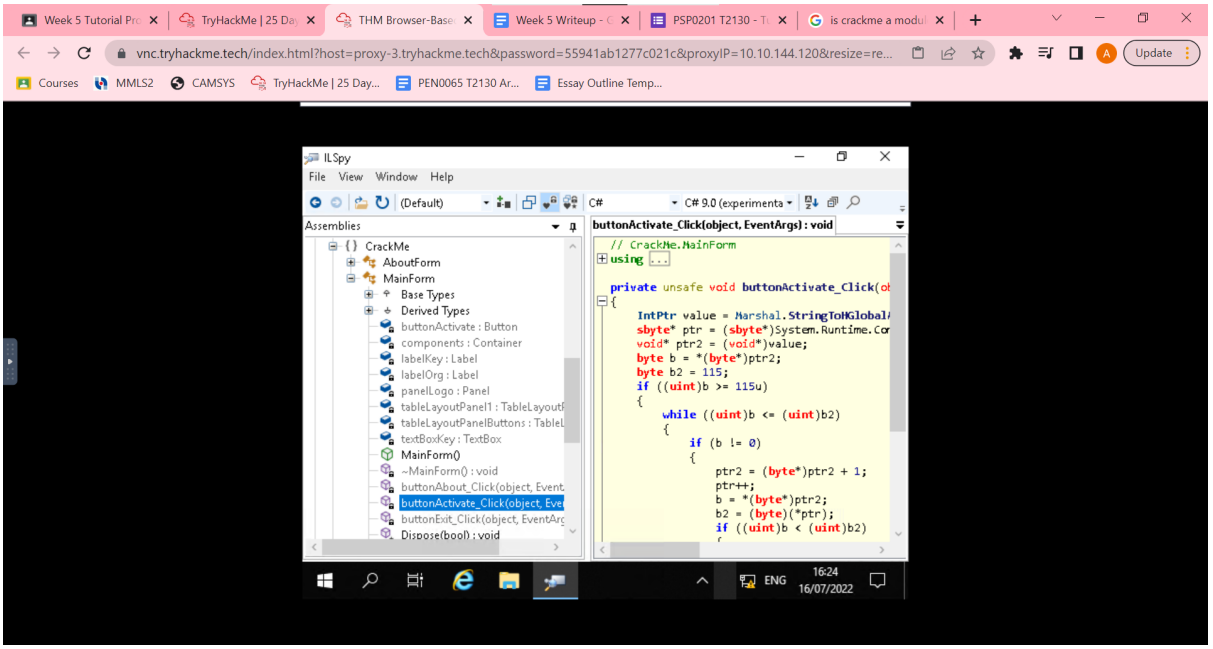
Q4: Within the module, there are two forms. Which contains the information we are looking for?

MainForm



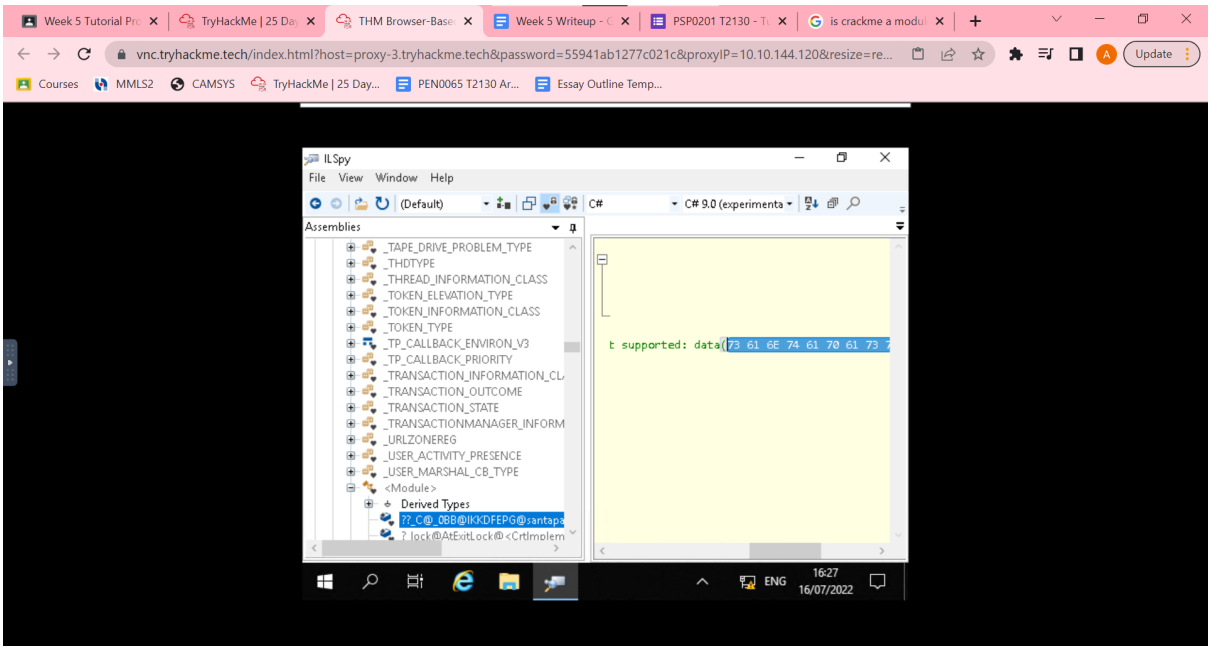
Q5: Which method within the form from Q4 will contain the information we are seeking?

buttonActivate_Click

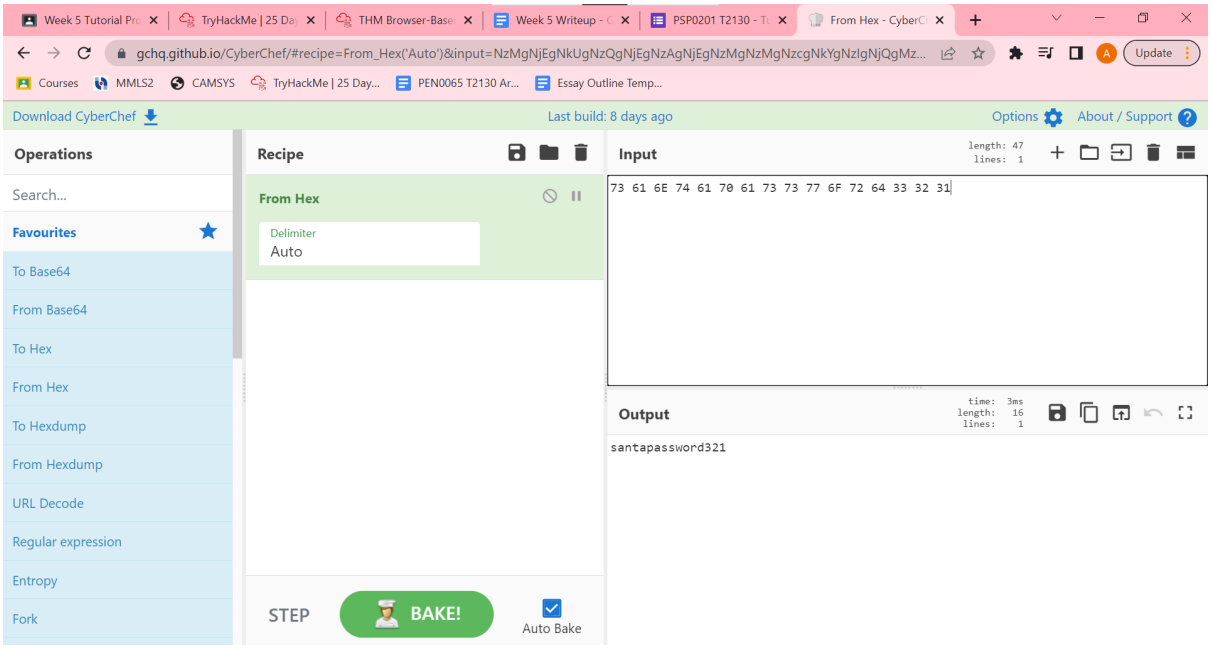


Q6: What is Santa's password?

Copy the hexadecimal number from <Module>.??_C@_0BB@IKKDFEPG@santapassword321@

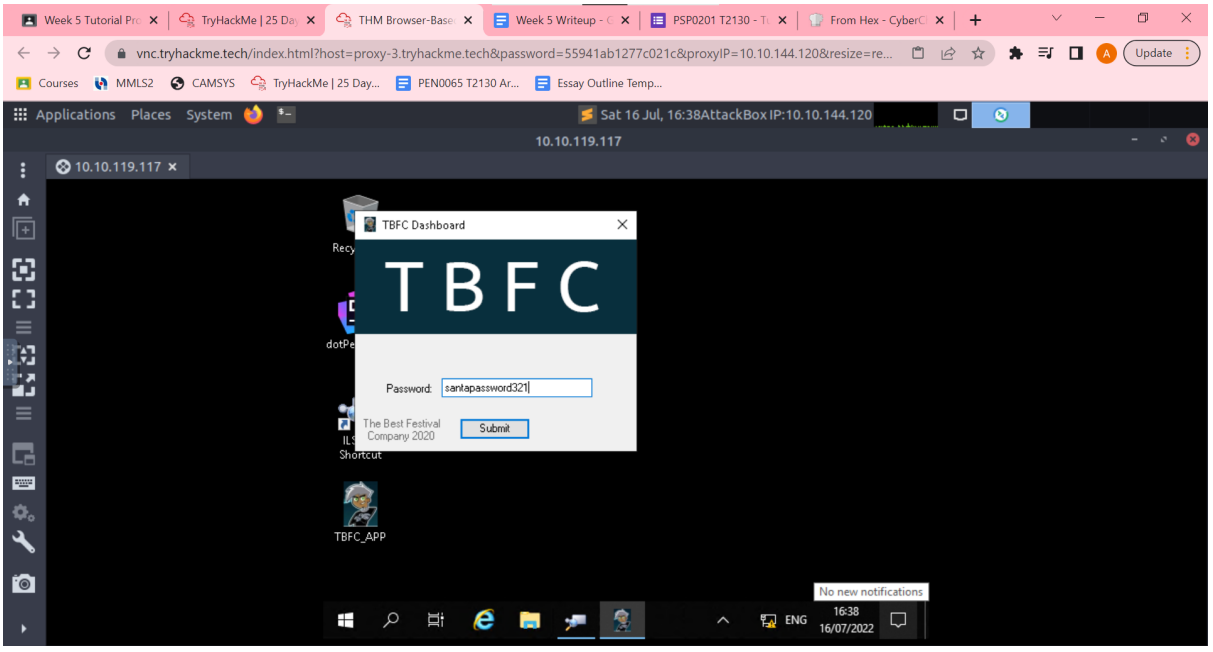


Paste into Cyberchef and the password santapassword321

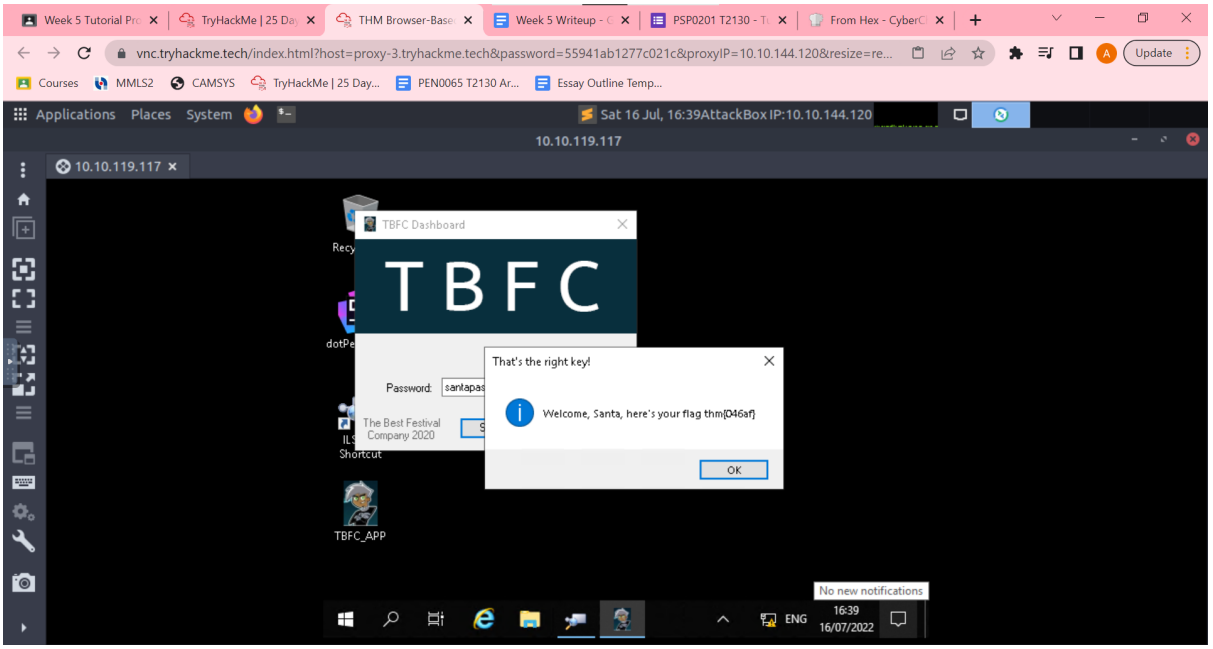


Q7: Now that you've retrieved this password, try to login...What is the flag?

Login into TBFC-App



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

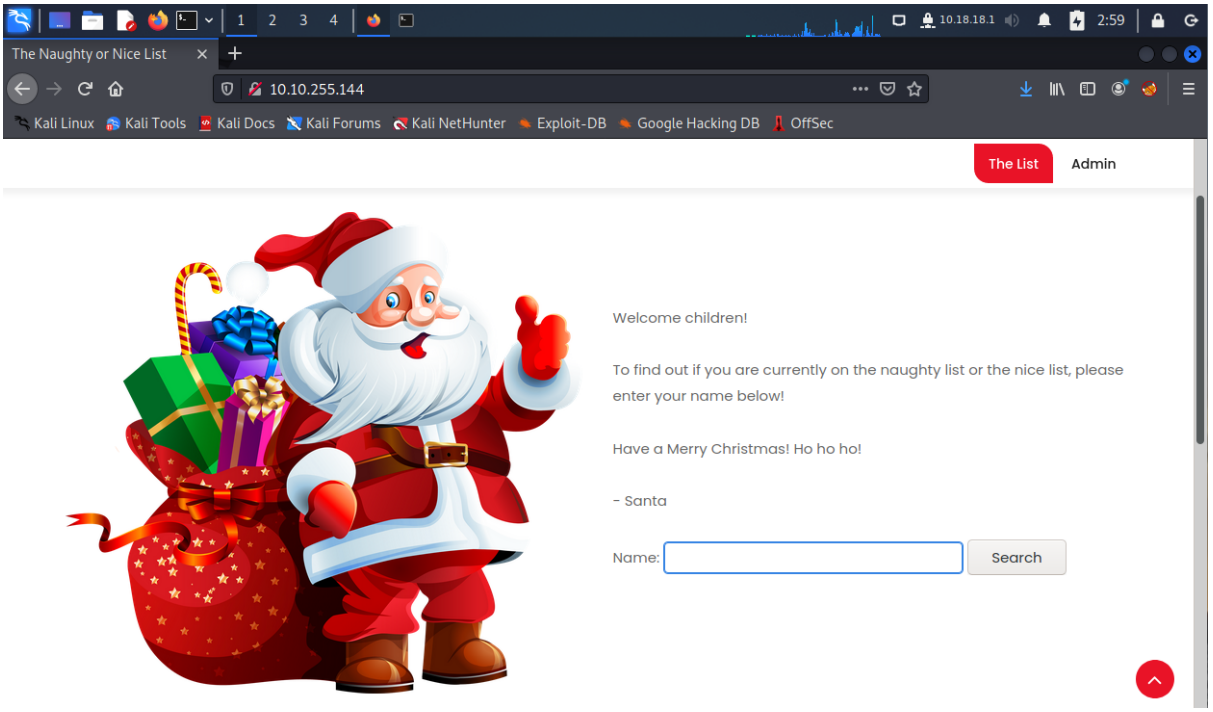
Tools used: THM Machine/Kali Linux/Mozilla Firefox

Solution/Walkthrough:

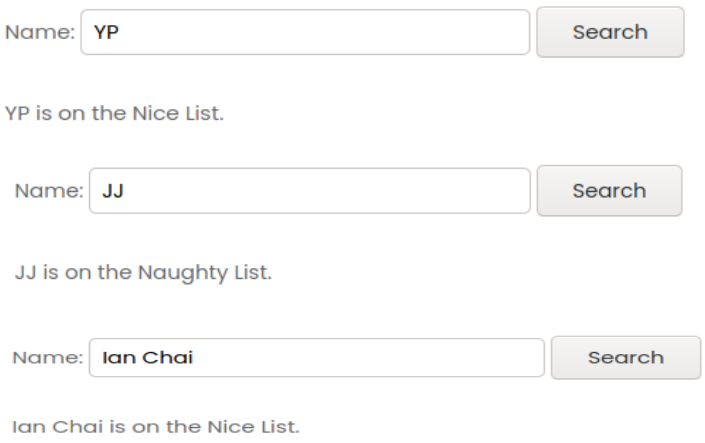
Question 1

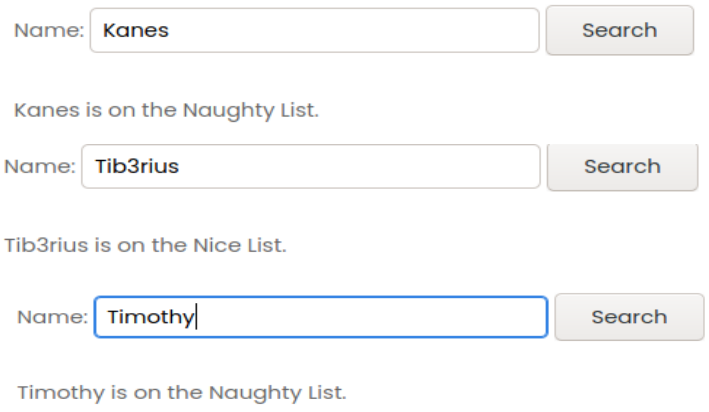
Which list is this person on?

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.

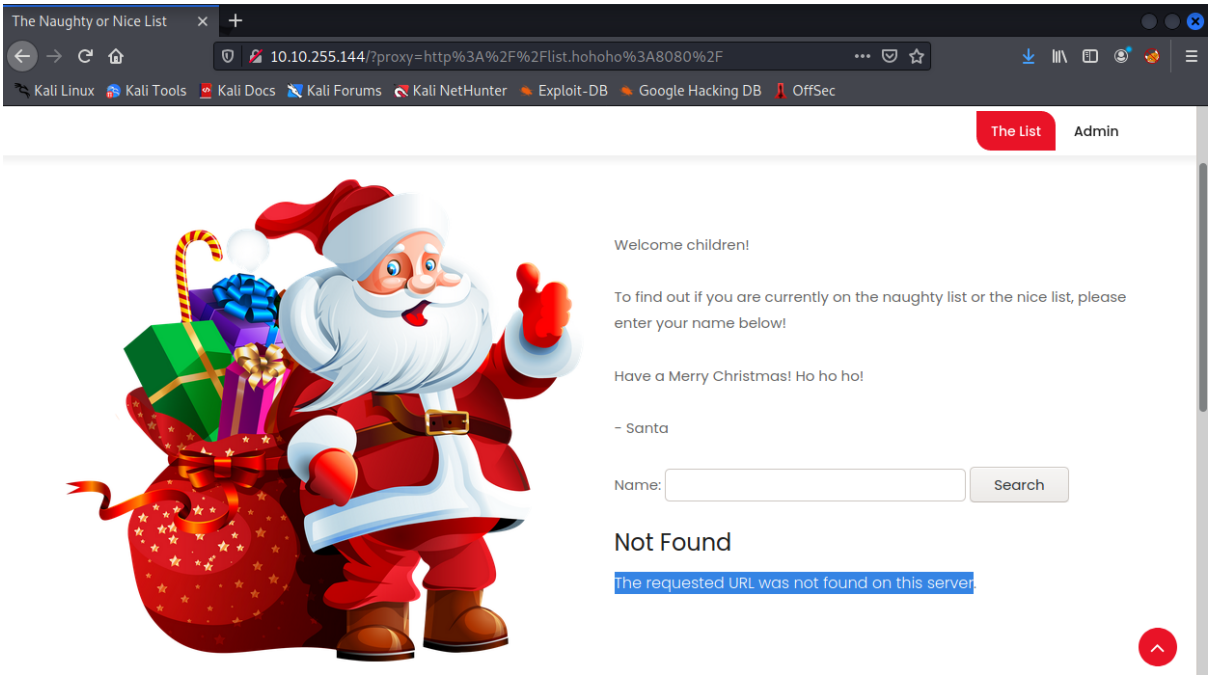




Question 2

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

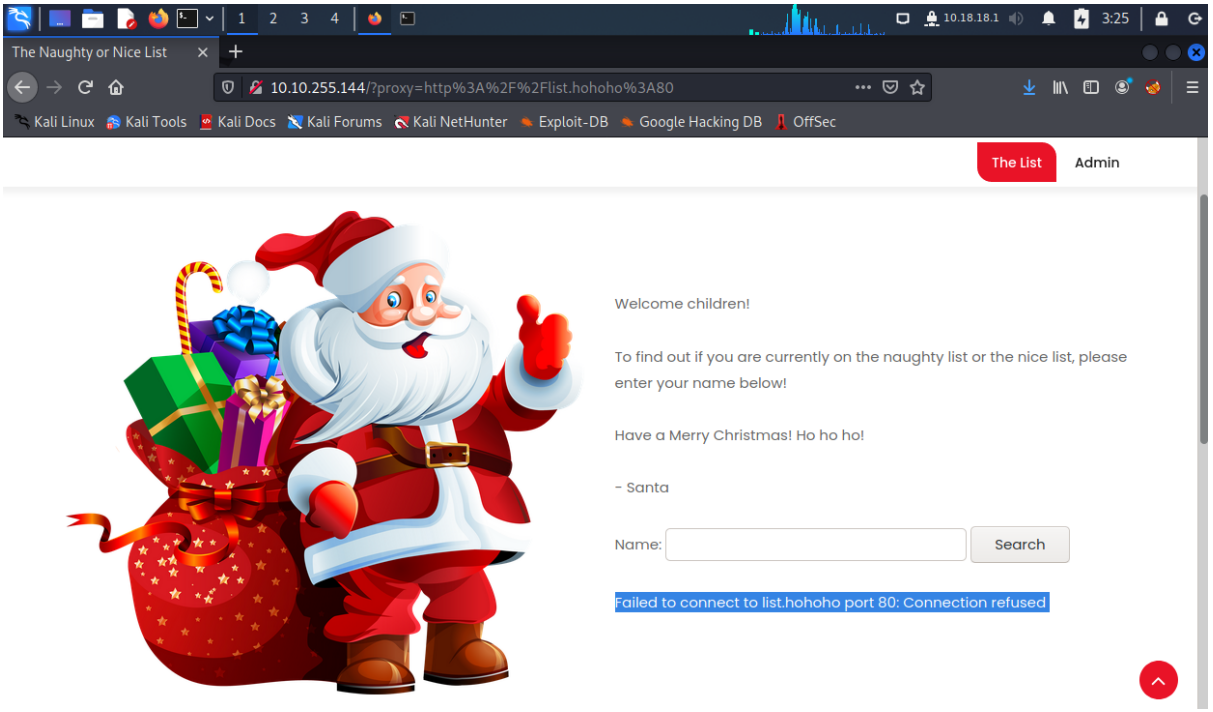
In order to see the message in the page, insert **"/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"** at the back of the IP address in the web browser. The message could be found displayed (Highlighted)



Question 3

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

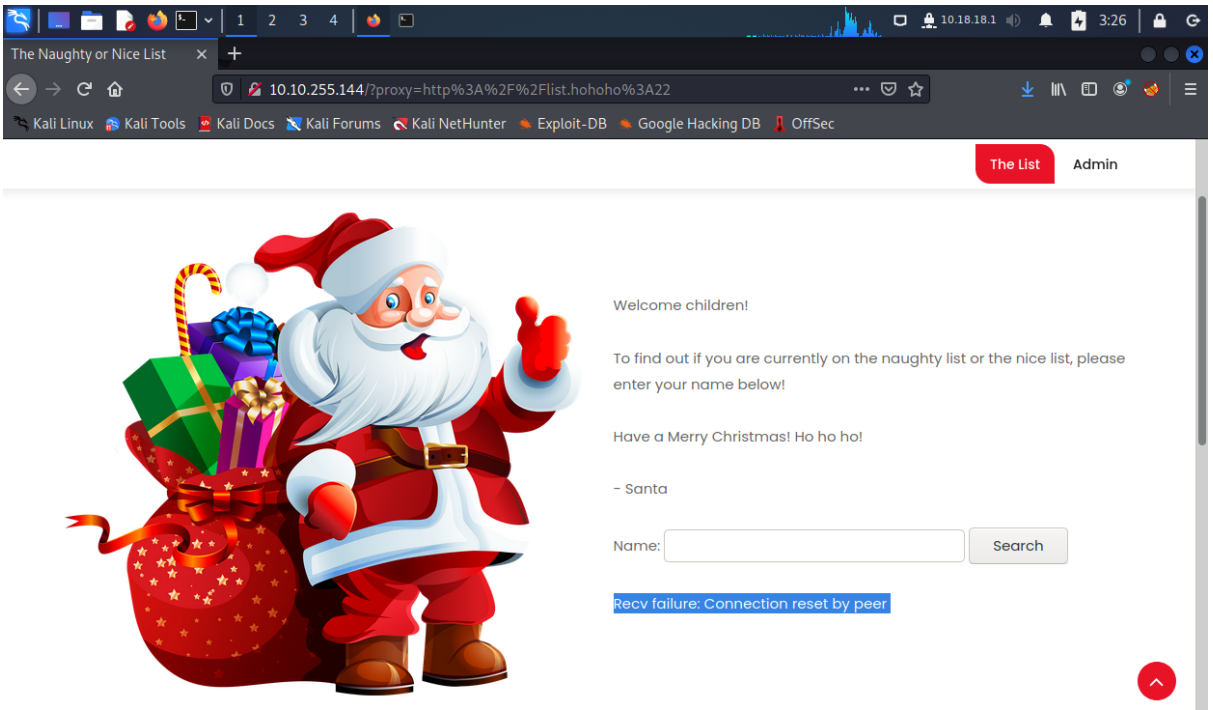
In order to see the message in the page, insert **"/?proxy=http%3A%2F%2Flist.hohoho%3A80"** at the back of the IP address in the web browser. The message could be found displayed (Highlighted)



Question 4

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

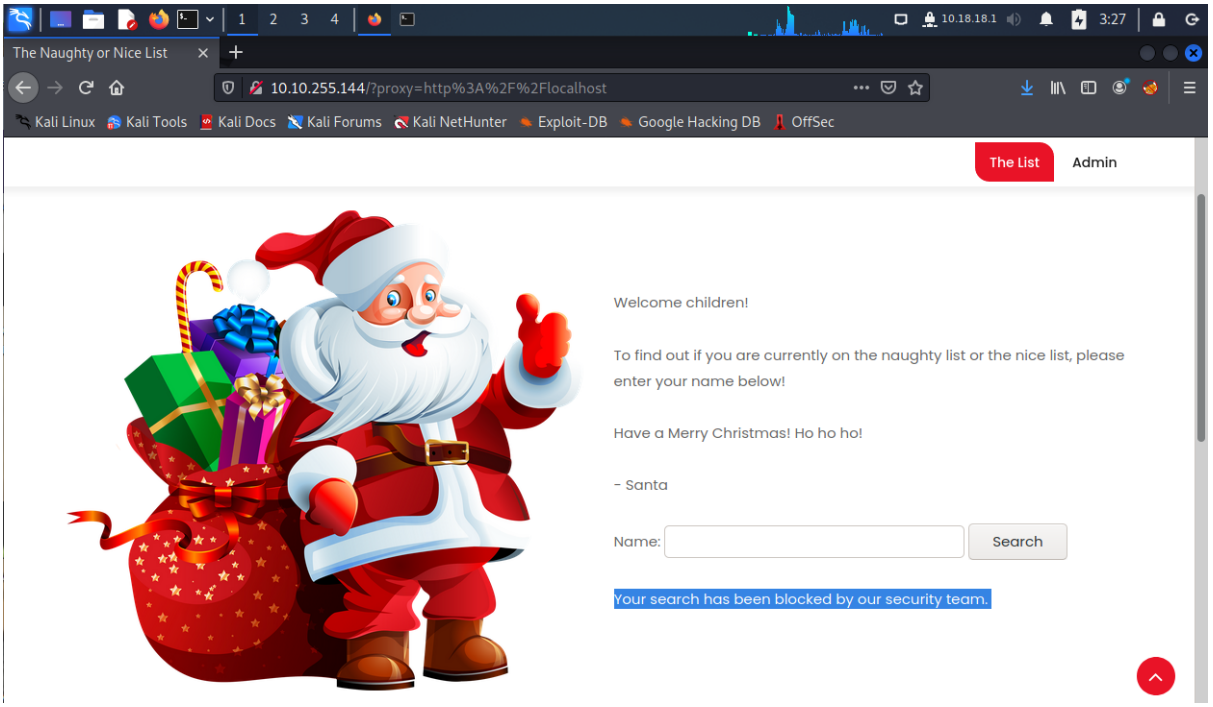
In order to see the message in the page, insert **"/?proxy=http%3A%2F%2Flist.hohoho%3A22"** at the back of the IP address in the web browser. The message could be found displayed (Highlighted)



Question 5

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

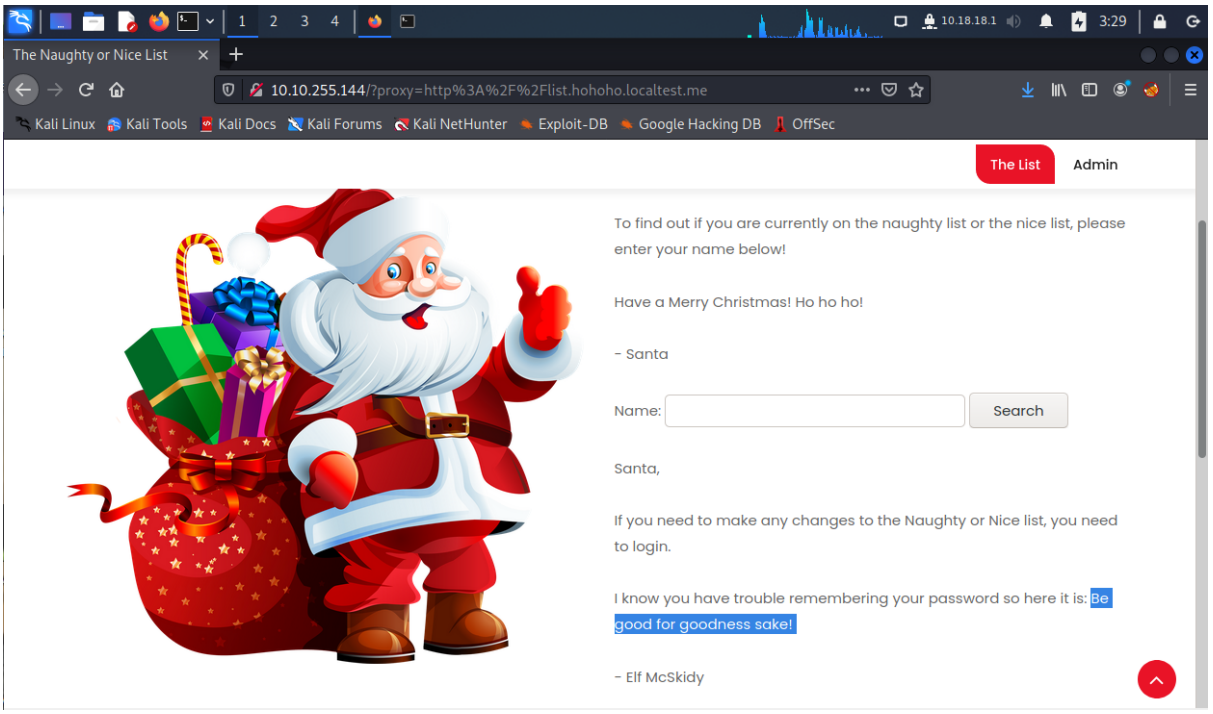
In order to see the message in the page, insert **"/?proxy=http%3A%2F%2Flocalhost"** at the back of the IP address in the web browser. The message could be found displayed (Highlighted)



Question 6

What is Santa's password?

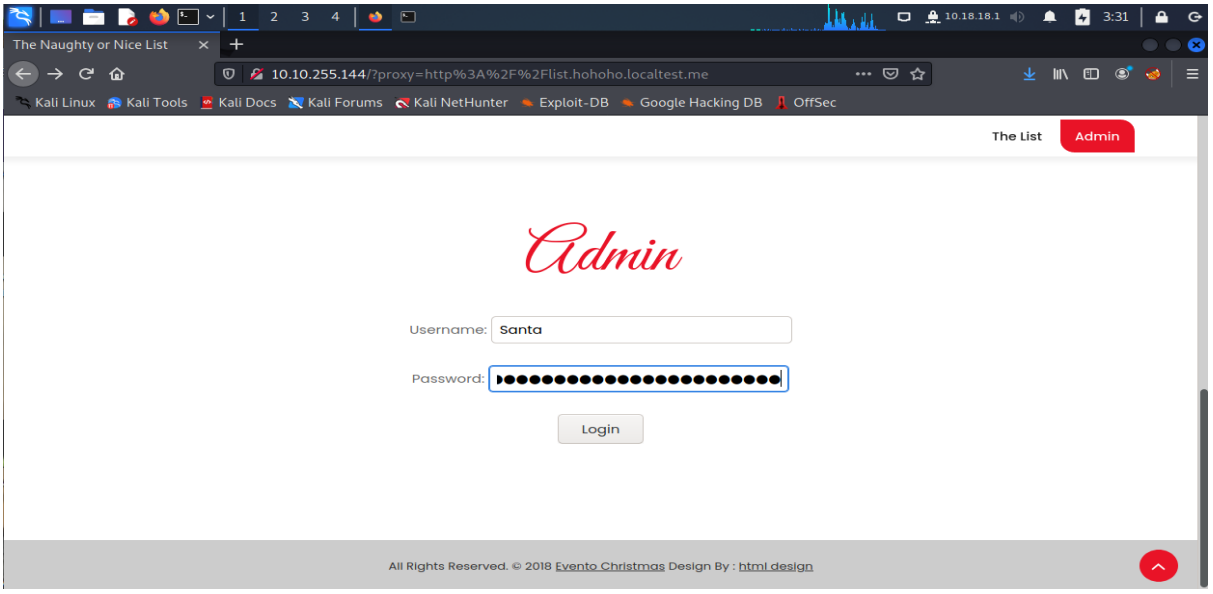
To bypass and check the local services, insert **"/?proxy=http%3A%2F%2Flist.hohoho.localtest.me"** at the back of the IP address in the web browser. Here we could find that the web server is running locally and there is a message left on the page. Santa's password could be found in the message area.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



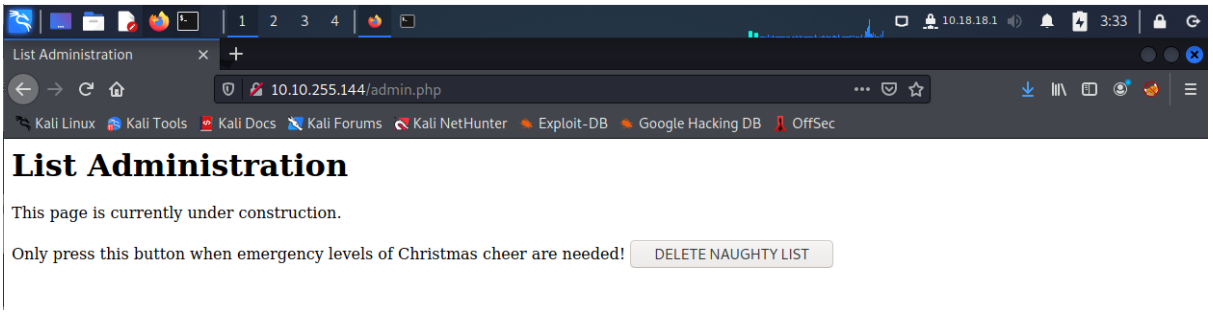
Question 7

What is the challenge flag?

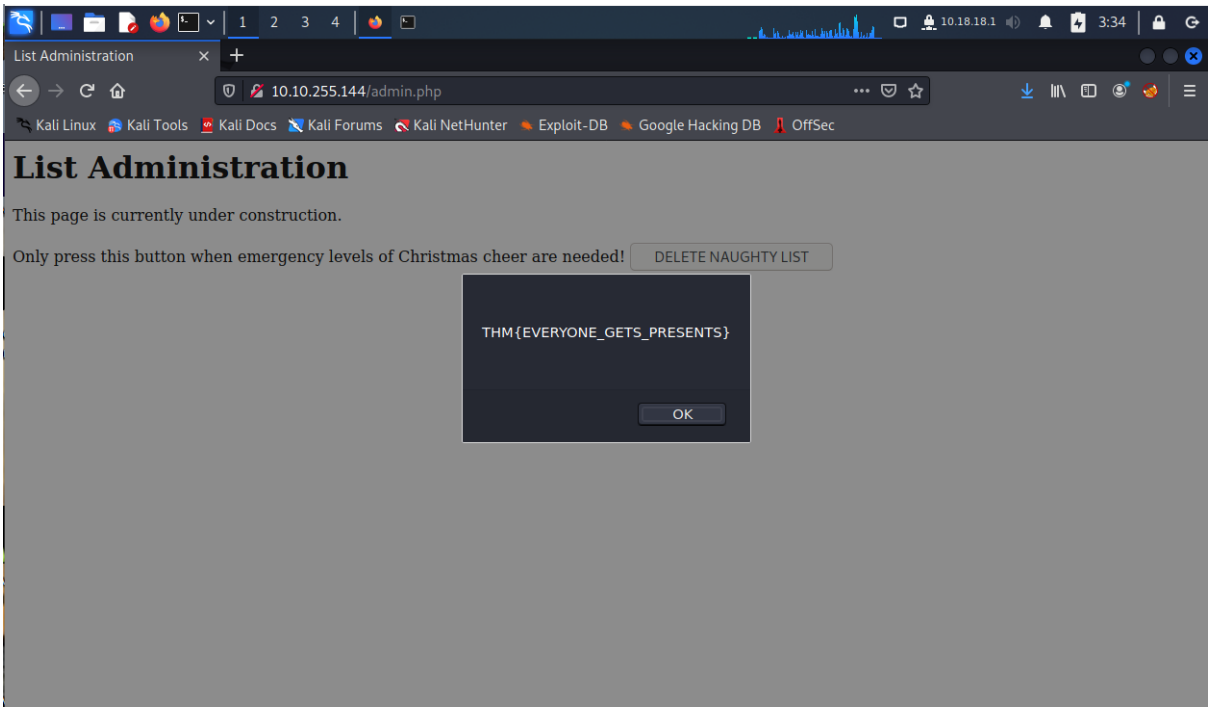
Click the **"Admin"** button on the top right corner of the page and we could find a login section to use from. Log in as Santa by using the provided credentials by entering the Username **(Santa)** and the Password **(Be good for goodness sake!).**



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 - PowersELIF to the rescue

Tools used: Kali Linux

Solution/Walkthrough:

Question 1:

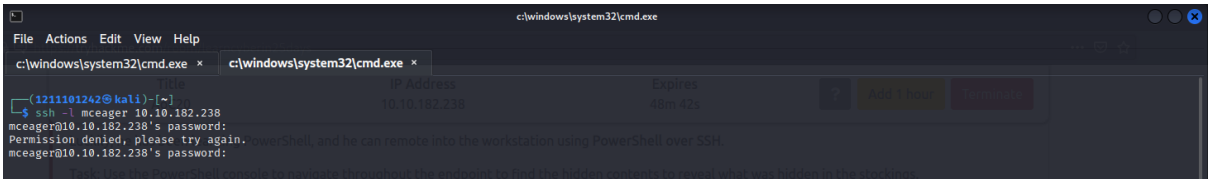
Check the ssh manual. What does the parameter -l do?

In order to see the ssh manual, simply type in ‘ssh’ in the command prompt to identify the functionality of -l parameter.

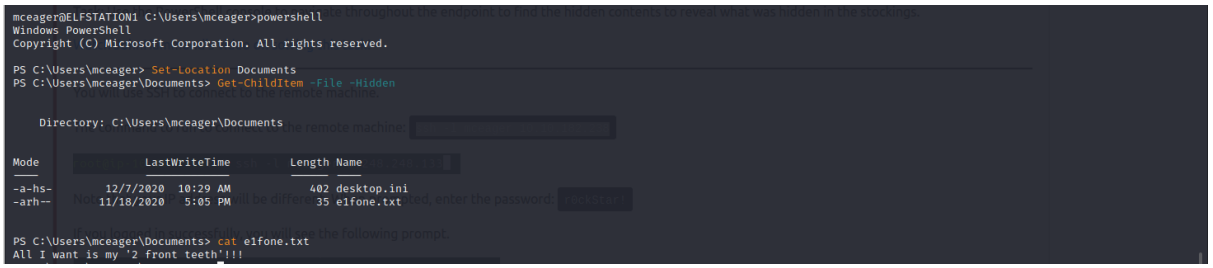
Question 2:

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.



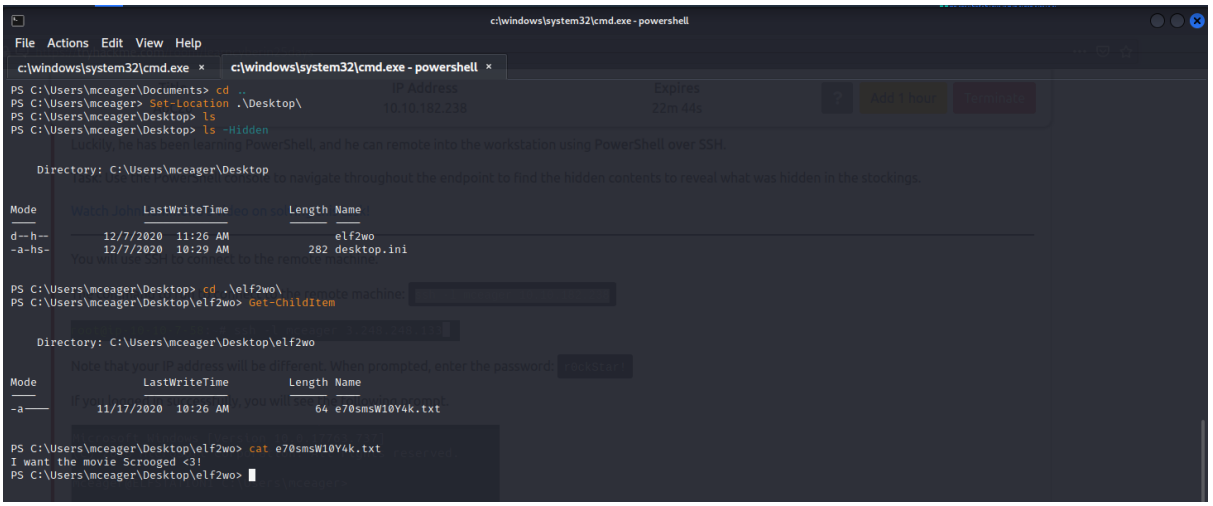
Type in powershell after logging to Mceager. After doing so, type in Set-Location Documents to gain access to the Documents file. Type in Get-Children -File -Hidden to gain the name of the file needed for the question. Use cat e1fone.txt to gain access to the content of the file.



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.



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

Use cd System32 to go to Windows’s System32

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


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
----                 -------------         ------ ----
-arh--        11/17/2020  10:58 AM          85887 1.txt
-arh--        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-Connect 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 of 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-Connect 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.