PSP0201

Week 5

Writeup

Group Name: Blessing Software

Members

ID	Name	Role
1211103213	Uwais	Leader
1211103184	Muzaffar	Member
1211103149	Dzakry Hariz	Member
1211102082	Thanussha	Member

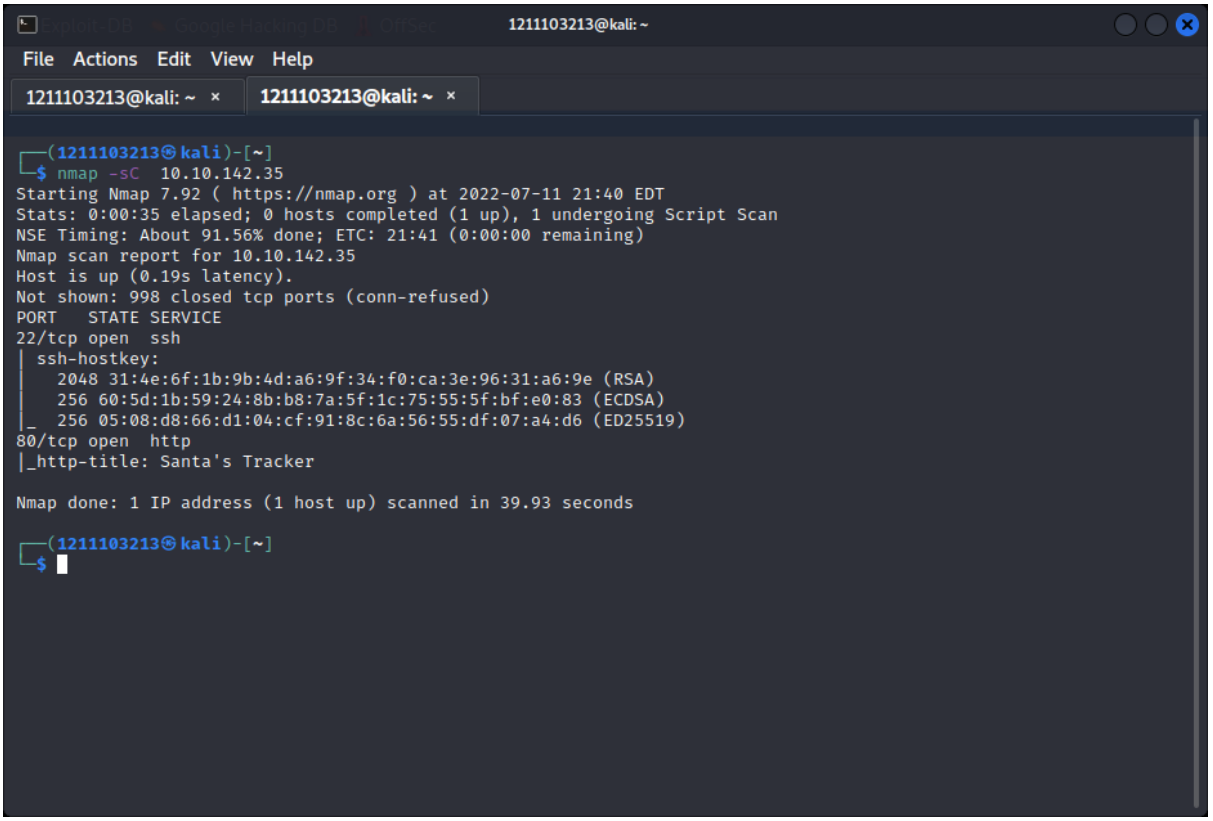
Day 16: Scripting – Help! Where is Santa?

Tools used: Kali Linux, Firefox, nmap, python3

Solution/walkthrough:

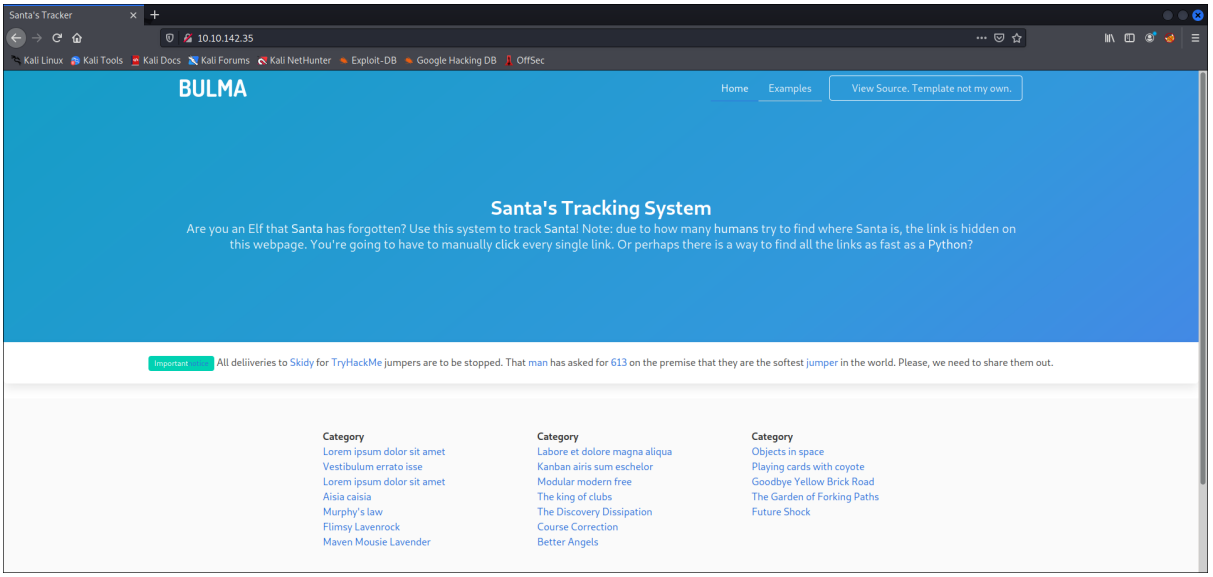
Question 1

Searched through the open ports using nmap.



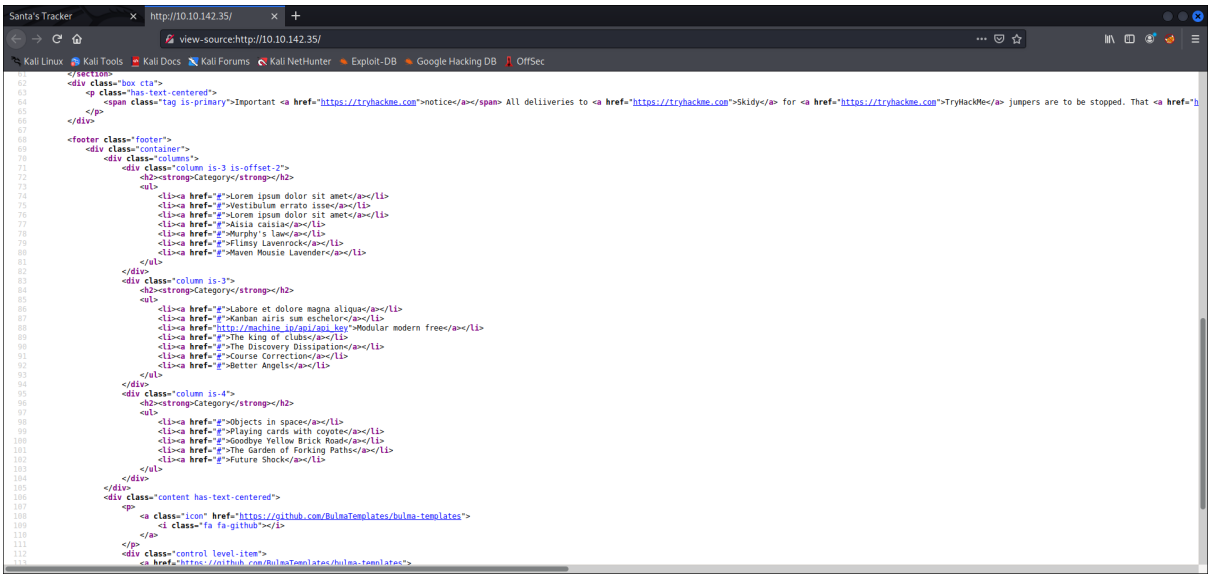
Question 2

Went to the website and looked for the template.



Question 3

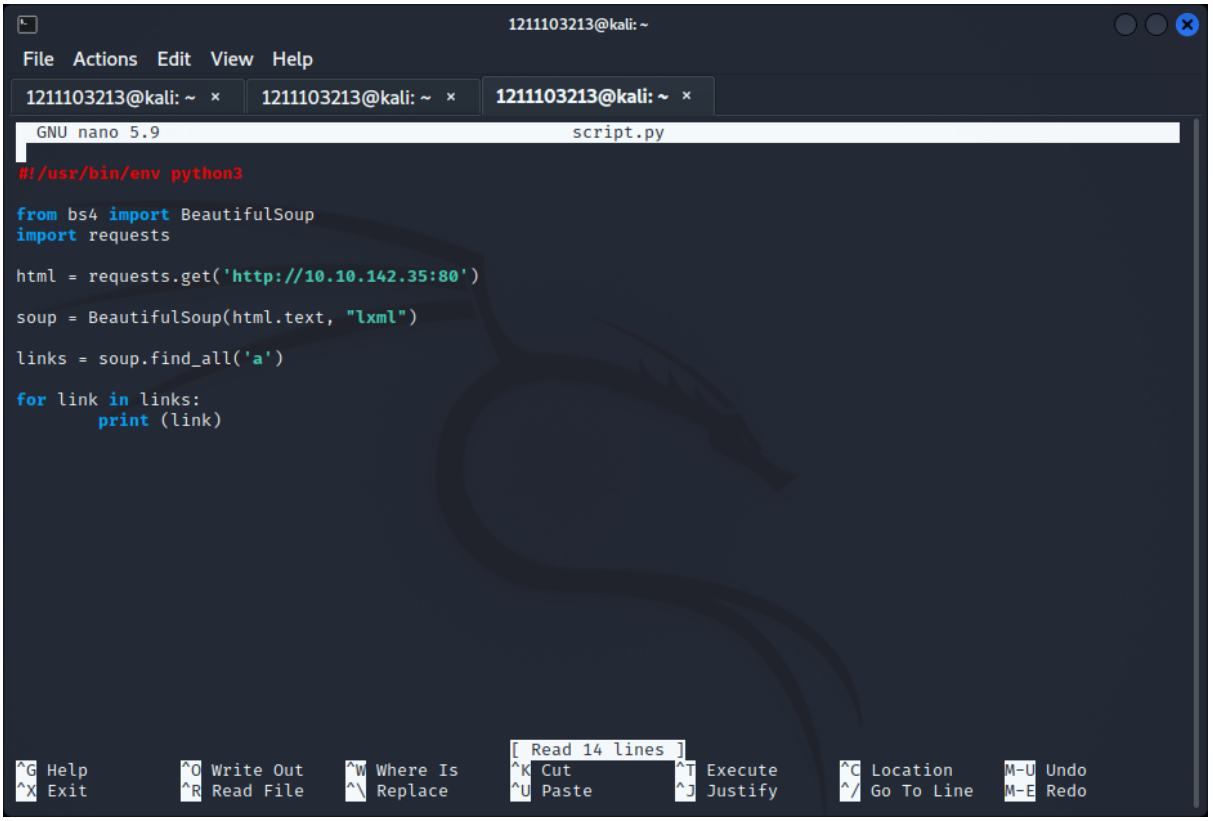
Viewed the page source and looked for the directory.

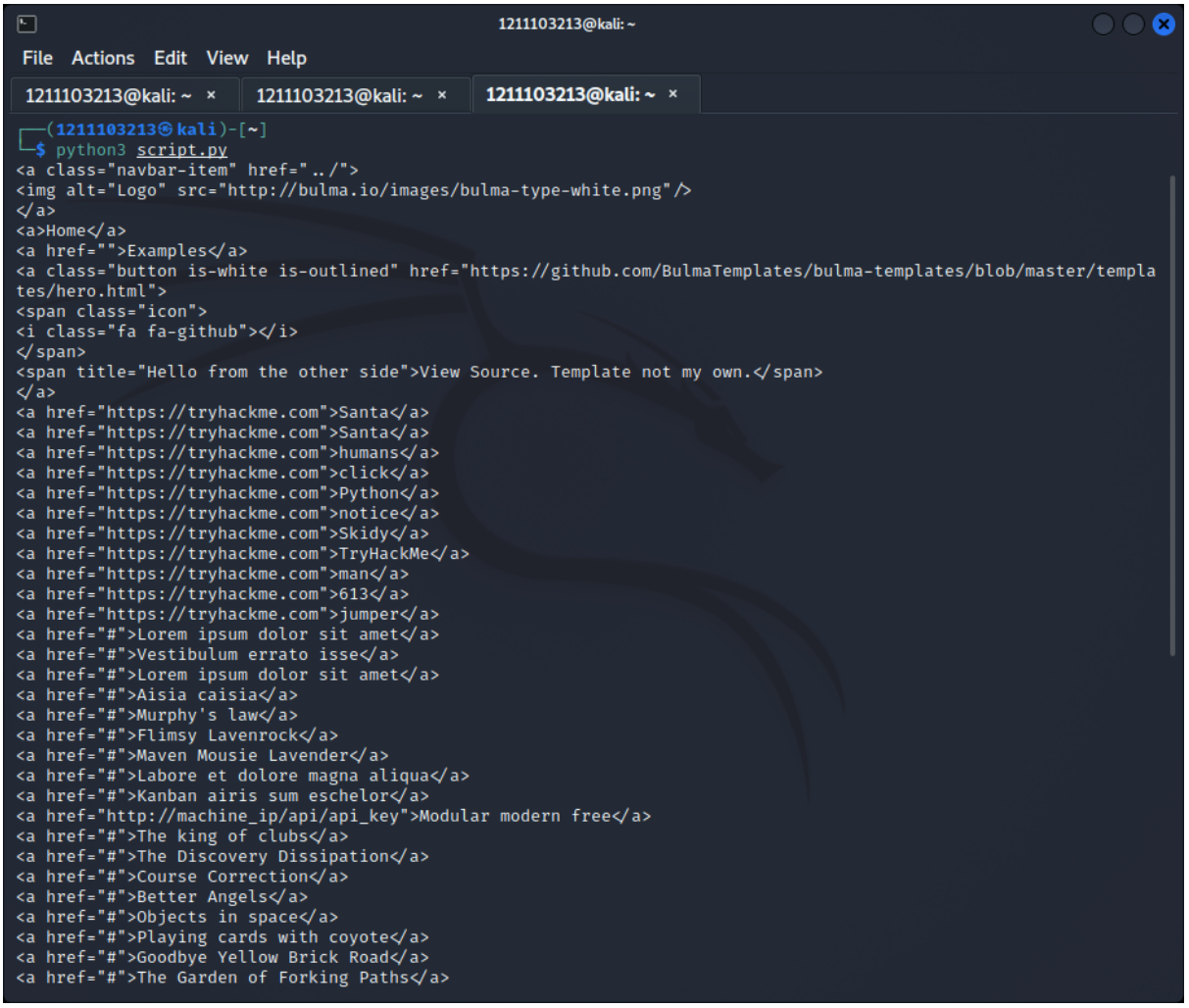



```
<div class="column is-3">
    <h2><strong>Category</strong></h2>
    <ul>
        <li><a href="#">Labore et dolore magna aliqua</a></li>
        <li><a href="#">Kanban airis sum eschelor</a></li>
        <li><a href="http://machine_ip/api/api_key">Modular modern free</a></li>
        <li><a href="#">The king of clubs</a></li>
        <li><a href="#">The Discovery Dissipation</a></li>
        <li><a href="#">Course Correction</a></li>
        <li><a href="#">Better Angels</a></li>
    </ul>
```

OR

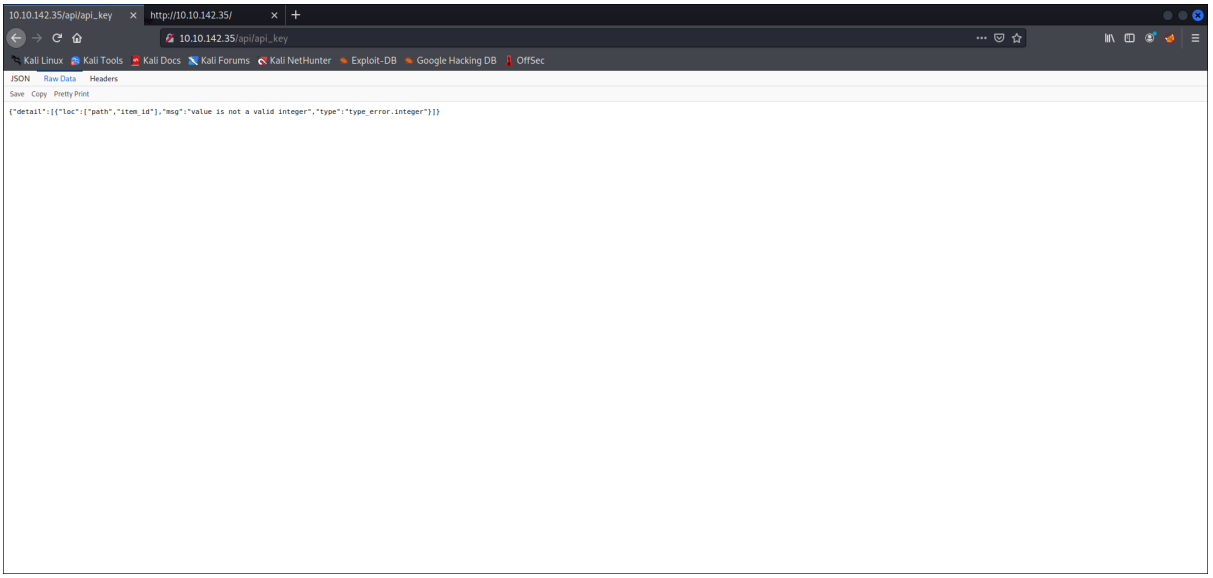
Used python scripting to search through the website for links.


1211103213@kali: ~
File Actions Edit View Help
1211103213@kali: ~
1211103213@kali: ~
1211103213@kali: ~
GNU nano 5.9 script.py
#!/usr/bin/env python3
from bs4 import BeautifulSoup
import requests
html = requests.get('http://10.10.142.35:80')
soup = BeautifulSoup(html.text, "lxml")
links = soup.find_all('a')
for link in links:
print (link)
[Read 14 lines]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo



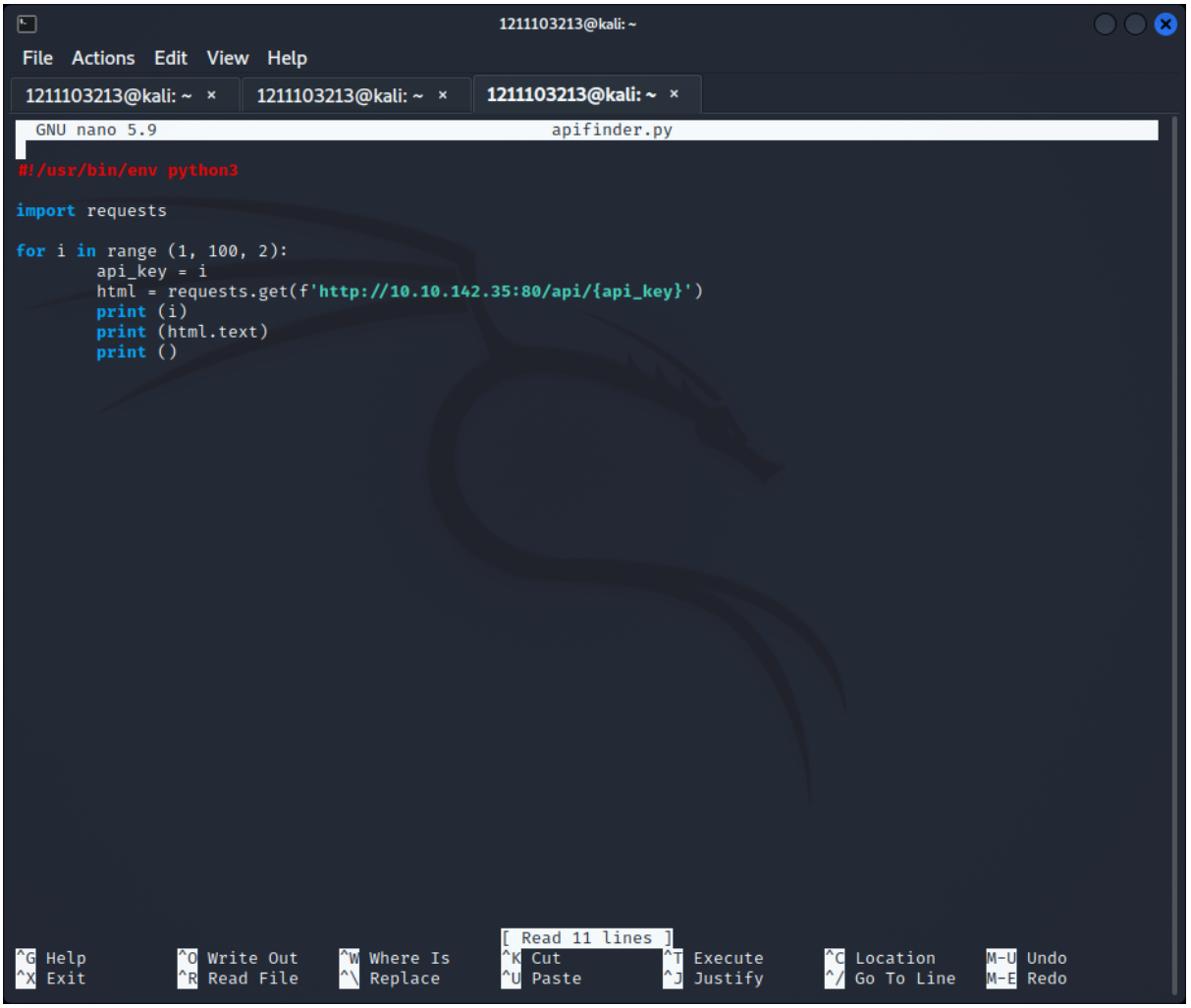
Question 4

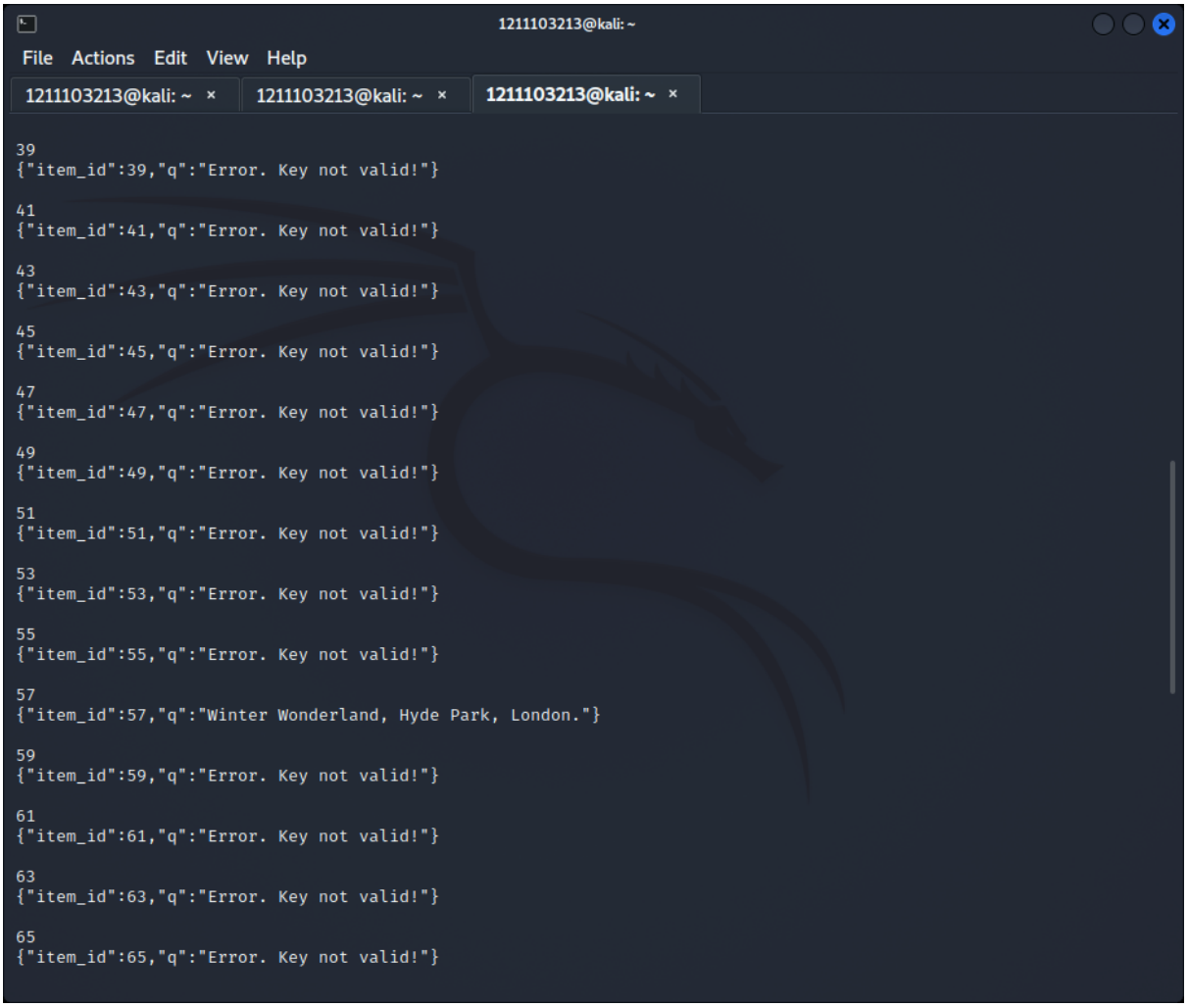
Went to the API endpoint from the last question, and looked to the Raw Data section.



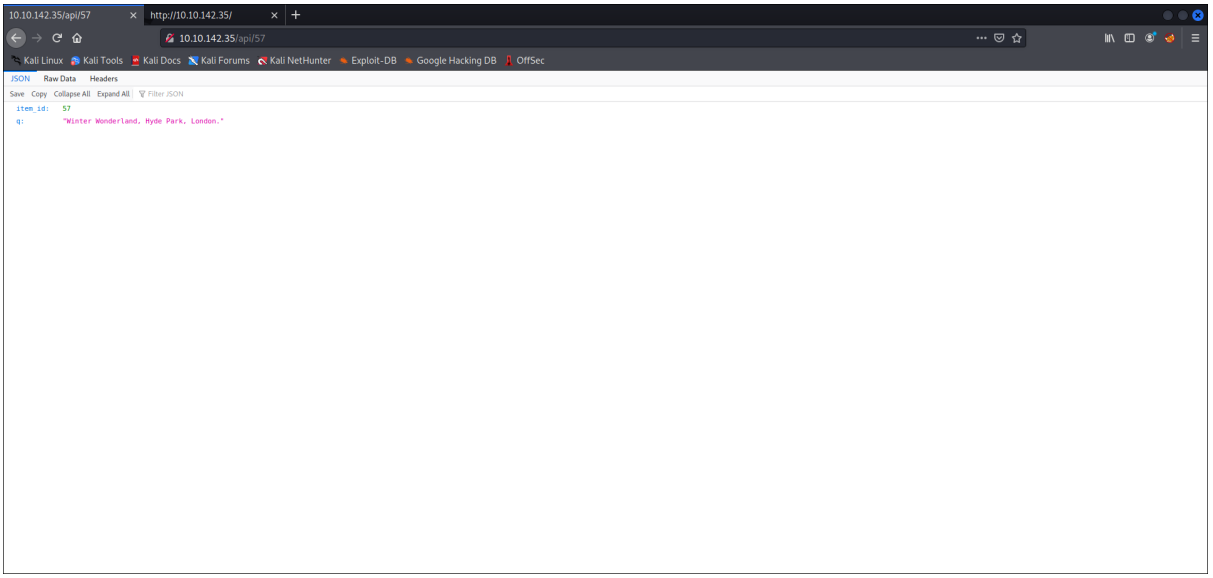
Question 5 and 6

Used python scripting to find the API key.





Got Santa’s location using the correct API key.



Thought Process/Methodology:

We used nmap scripts to search for any open ports to look for the website. After getting it, we looked for the template and went into the page source for hints on the API key. We decided to use python scripting to automate the search for the API directory, and then to automate the search for the API keys. Through this, our IP address wouldn't get blocked. Finally, we got the API key and Santa's location.

Day 17: Reverse Engineering – ReverseELFneering

Tools used: Kali Linux, radare2

Solution/walkthrough:

Question 1

Referred to the notes given in TryHackMe.

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

Referred to the notes given in TryHackMe.

This will open the binary in debugging mode. Once the binary is open, one of the first things to do is ask r2 to analyze the program, and this can be done by typing in: `aa`

Question 3

Referred to the notes given in TryHackMe.

A **breakpoint** specifies where the program should stop executing. This is useful as it allows us to look at the state of the program at that particular point. So let's set a breakpoint using the command `db` in this case, it would be `db 0x00400b55` To ensure the breakpoint is set, we run the `pdf @main` command again and see a little **b** next to the instruction we want to stop at.

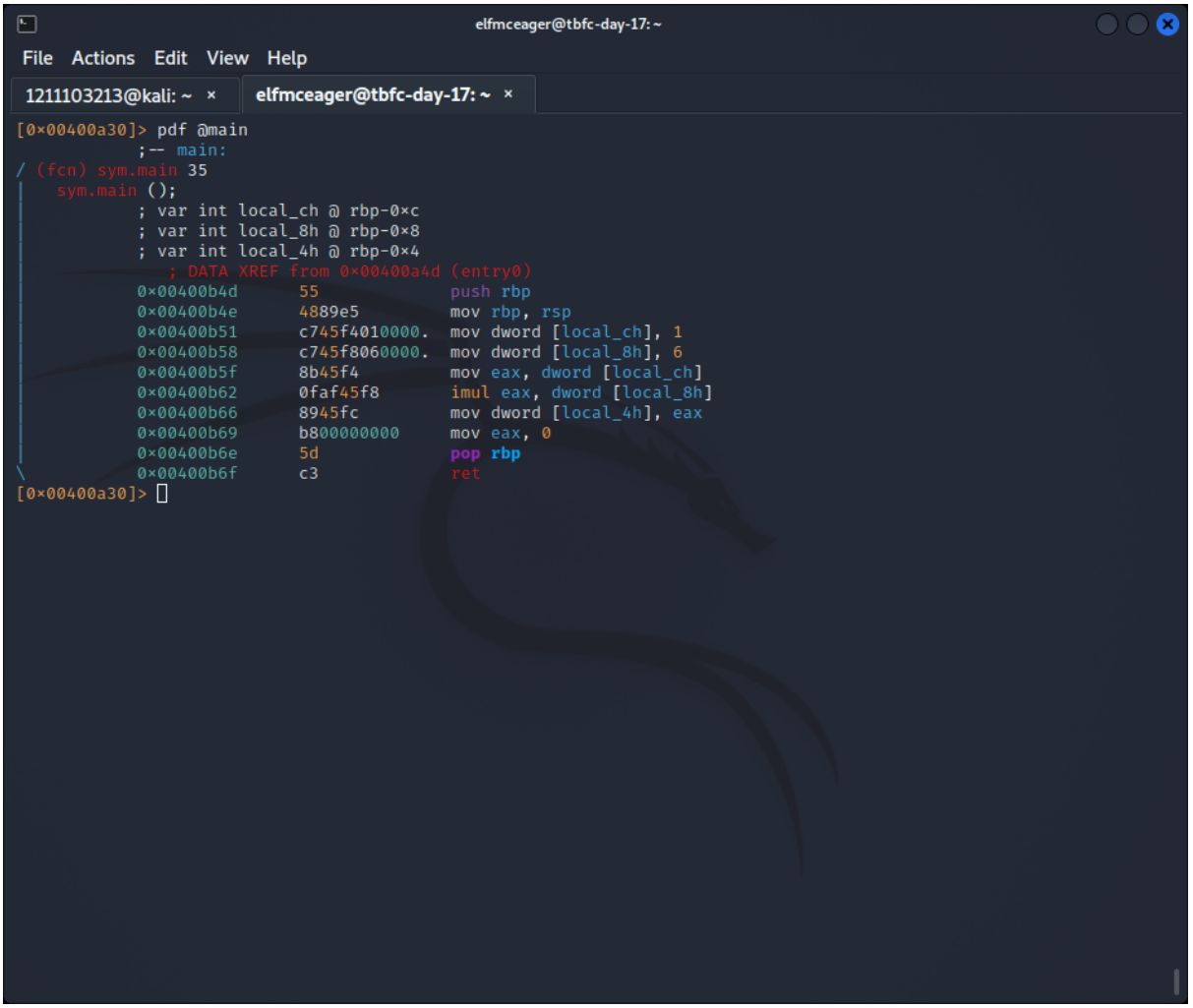
Question 4

Referred to the notes given in TryHackMe.

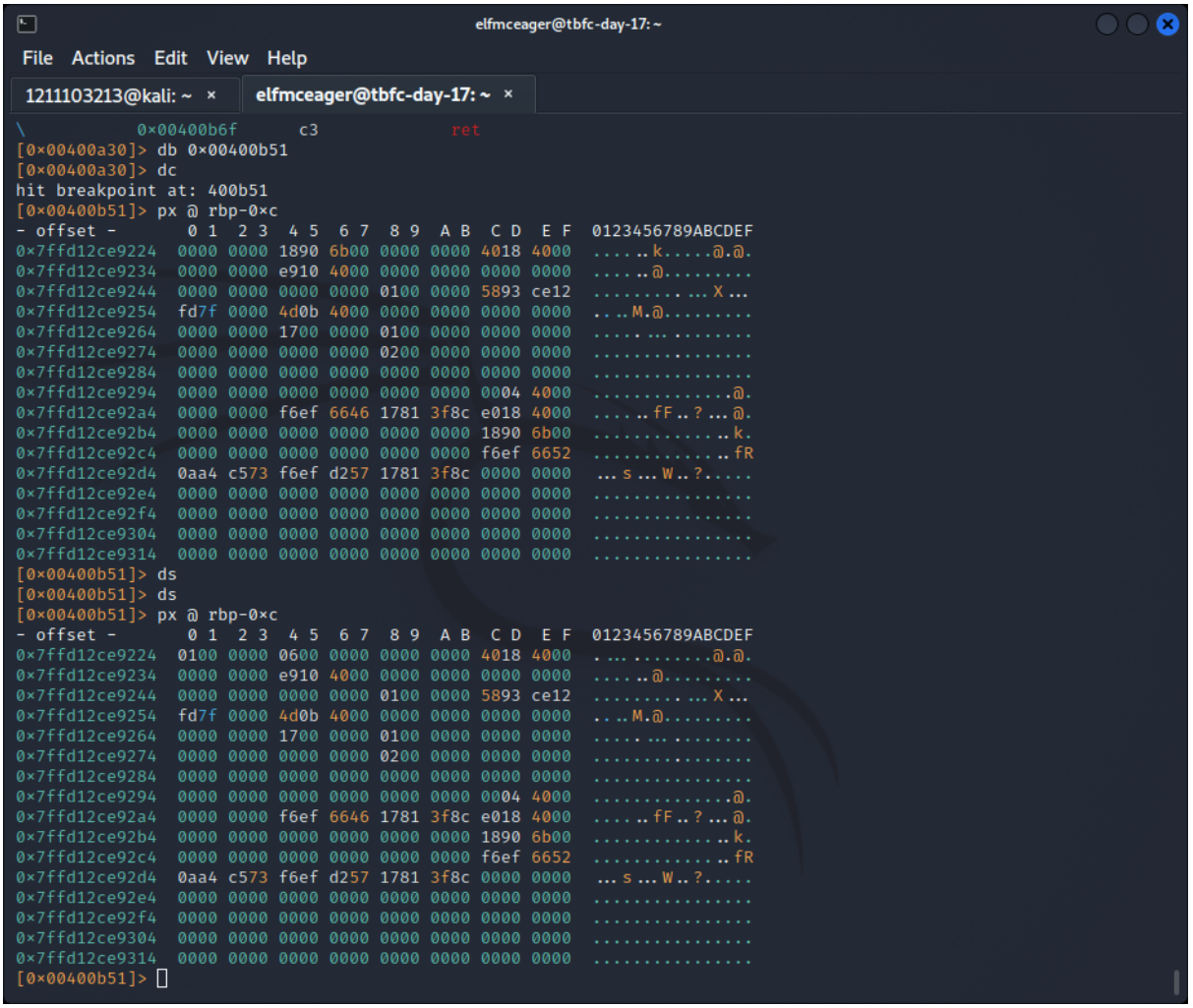
Running `dc` will execute the program until we hit the breakpoint. Once we hit the breakpoint and print out the main function, the rip which is the current instruction shows where execution has stopped. From the notes above, we know that the **mov** instruction is used to transfer values. This statement is

Question 5

Analyzed the file, and examined the code.

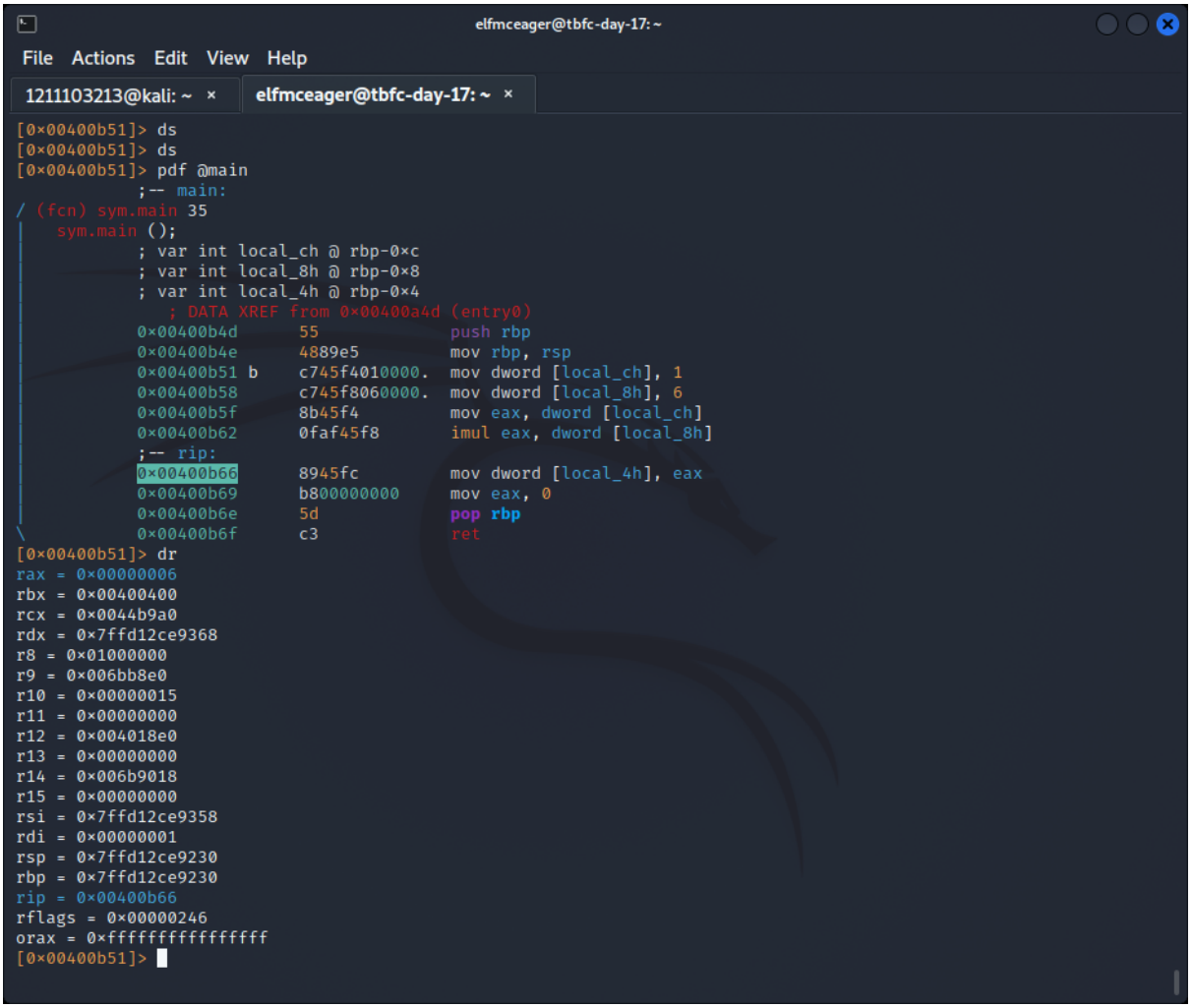


Set a breakpoint at the corresponding movl instruction to see the value change within local_ch.



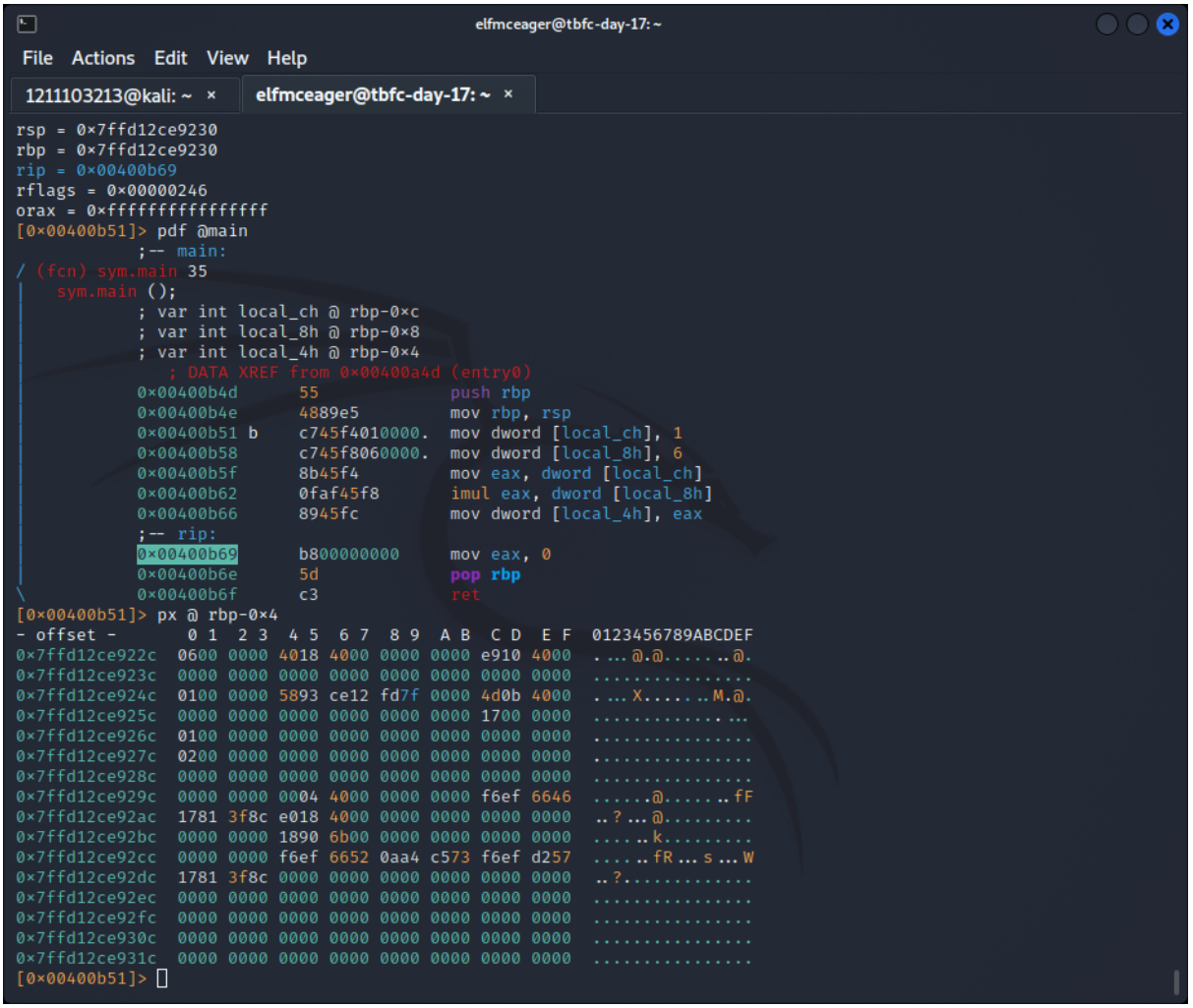
Question 6

Went to the step that has the imull instruction to pass it, and then checked the value of eax.



Question 7

Went before the step that sets eax as 0, and checked the value of local_4h.



Thought Process/Methodology:

Using the radare2 commands, we analysed the challenge1 file and its code. From pdf @main, we can see the steps and disassemble the functions step by step. We saw the 3rd instruction moved the value to local_ch. Using breakpoint, we ran the code right after that instruction and stopped it, followed by looking into the value of local_ch to see its current value. Then, using ds to proceed to the next steps, we went to the imull instruction. There, we ran dr to see the eax value. Finally, we went to the 8th instruction where we saw the eax value changing to 0. By not passing it, we could check the value of local_4h before that instruction is passed.

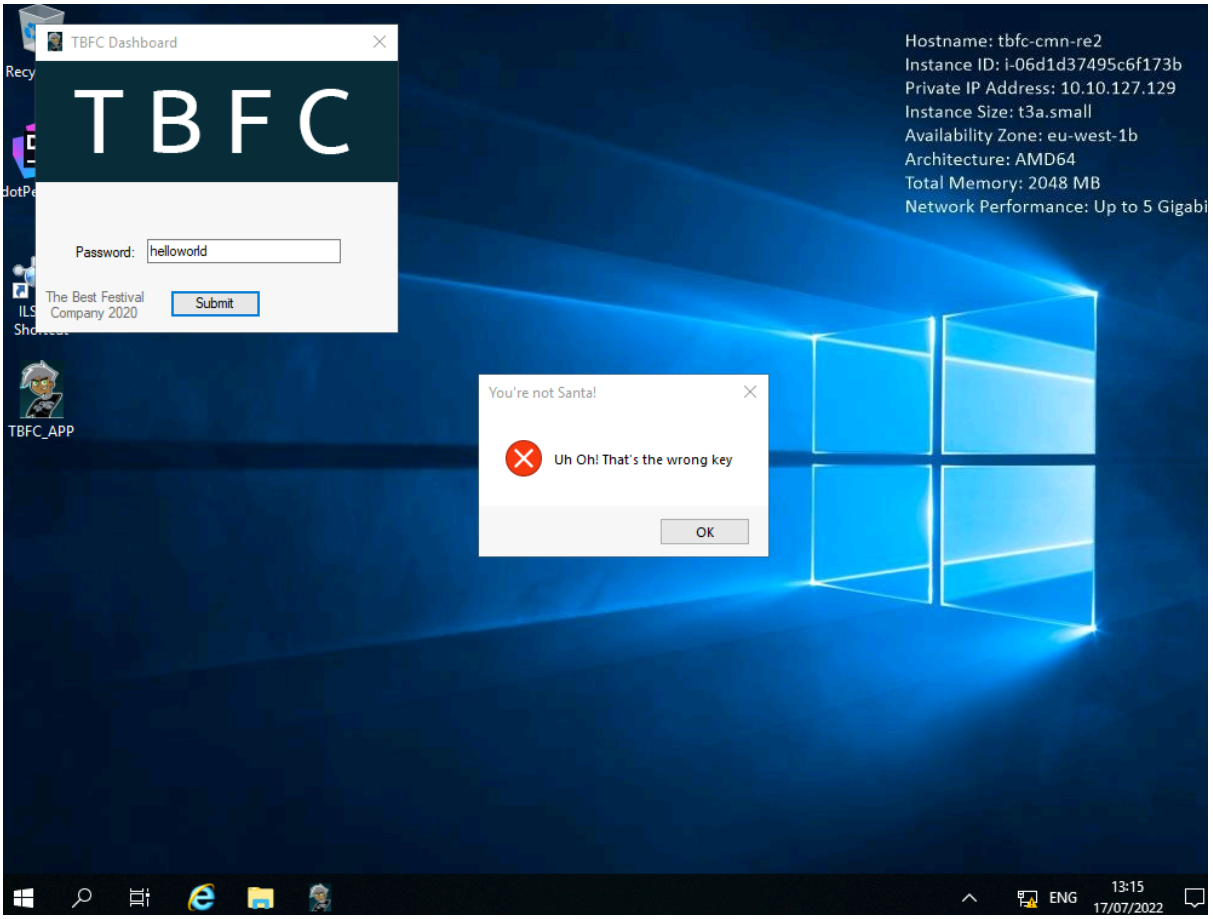
Day 18

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

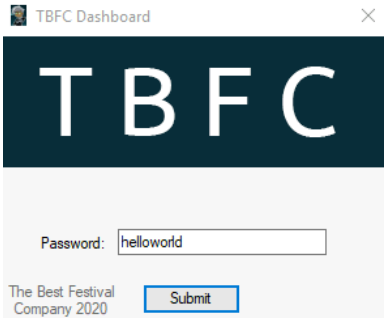
Question 1

Open the machine and click on TBFC_APP. Then, enter the wrong password.



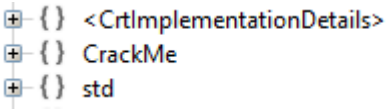
Question 2

Look at the bottom left corner of the application.



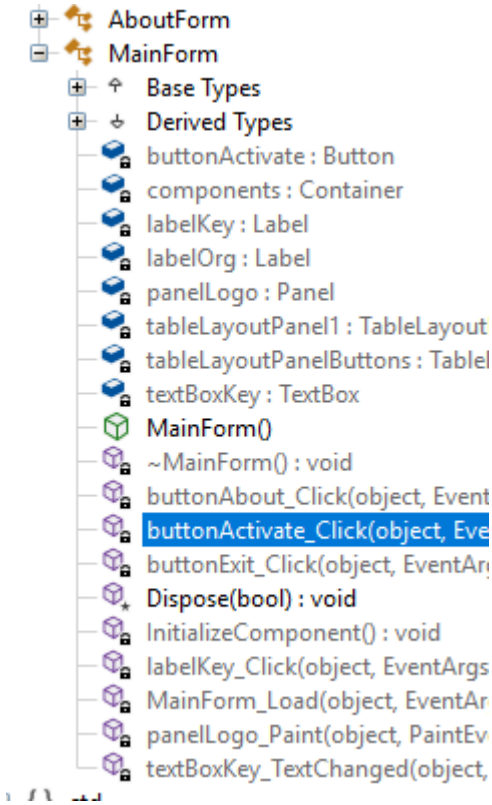
Question 3

Click on ILSpy. Look through TBFC_APP.



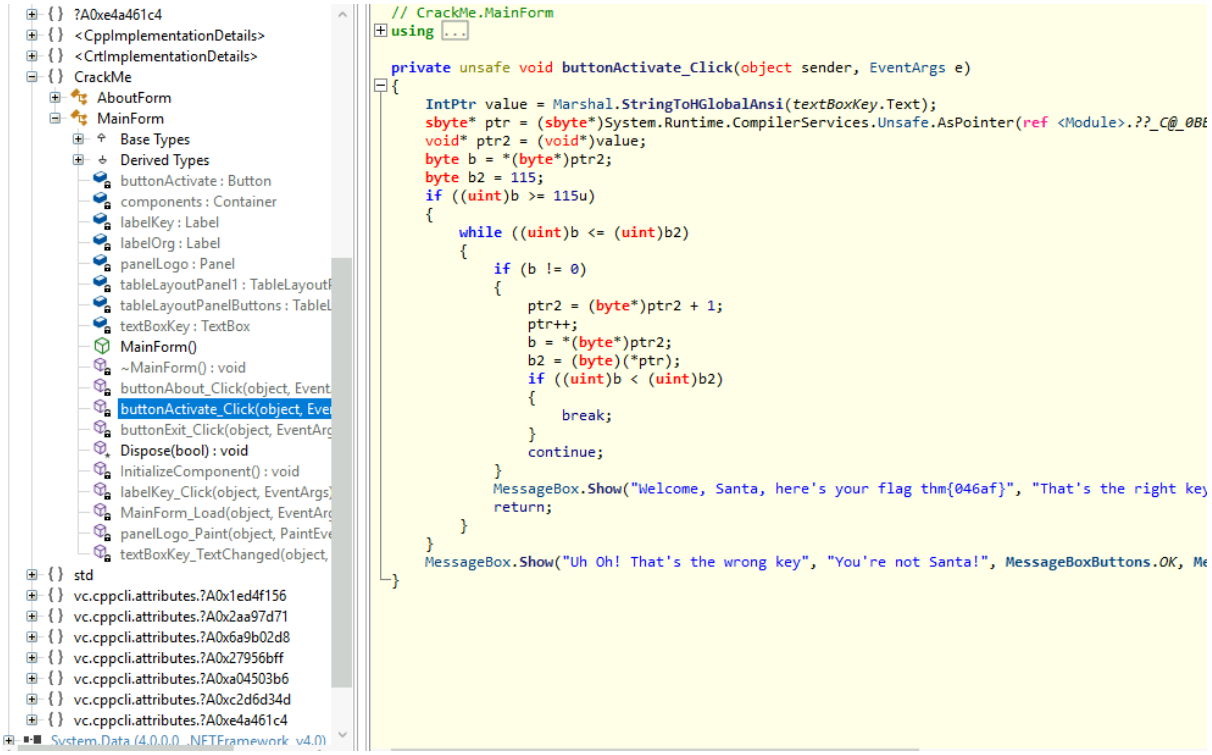
Question 4

Look on both forms.



Question 5

Click on the file that has connection to the password.



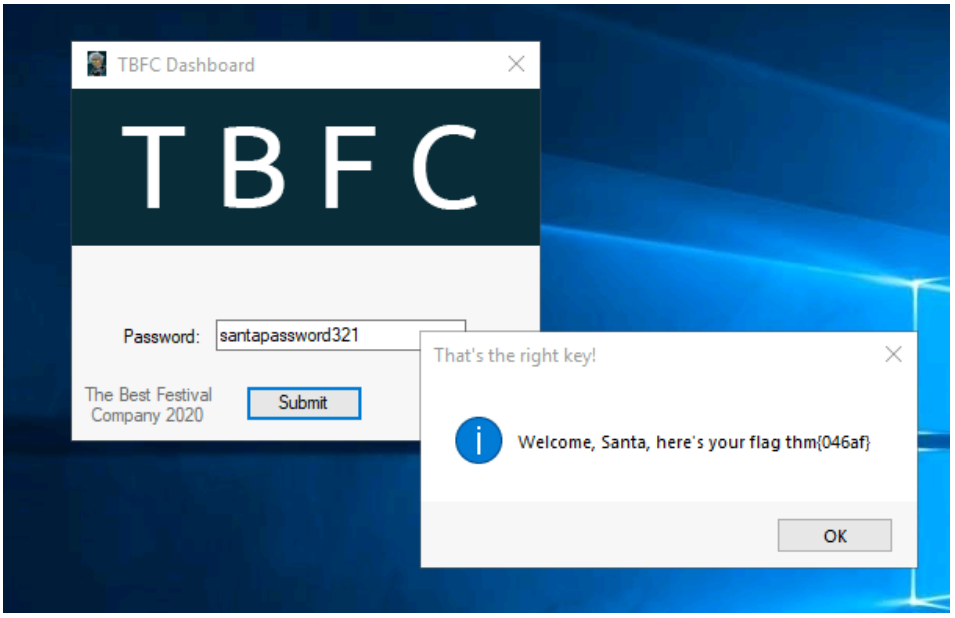
Question 6

Look for the password.

```
er(ref <Module>.??_C@_0BB@IKKDFEPG@santapassword321@);
```

Question 7

Enter the password on the TBFC_APP.



Thought process/Methodology:

Once we found the way to the machine, click on ILSpy and search for TBFC_APP. There, we found the file, CrackMe. We thought there is some connection of submit button with the password. Then, we searched for the button activation file and found the password. Ater entering the password on the application, we finally obtained the flag.

Day 19: Web Exploitation - The Naughty or Nice List

Tools used: Kali Linux, FireFox

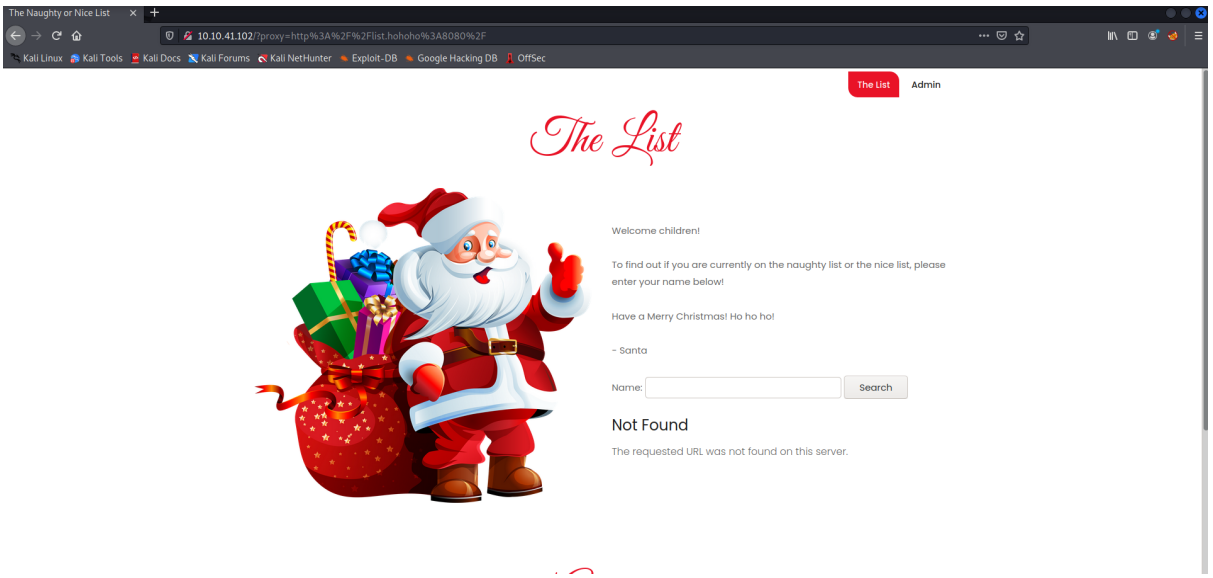
Solution/ Walkthrough:

Question 1

Search for every name in the list on the searchbar.

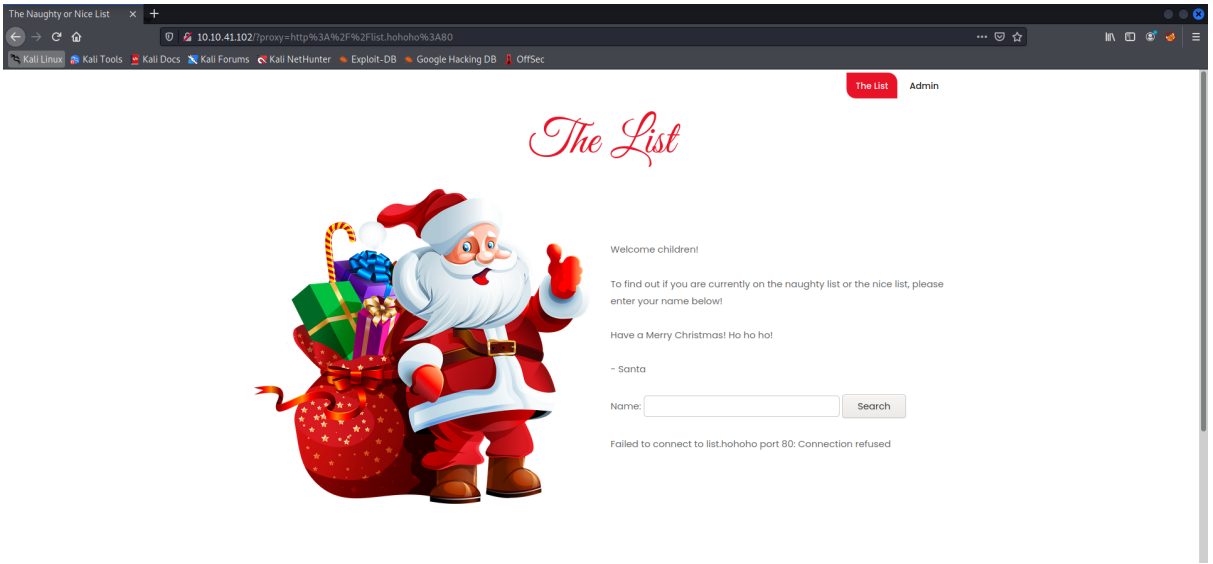
Question 2

Copy and paste “/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F” on the browser.



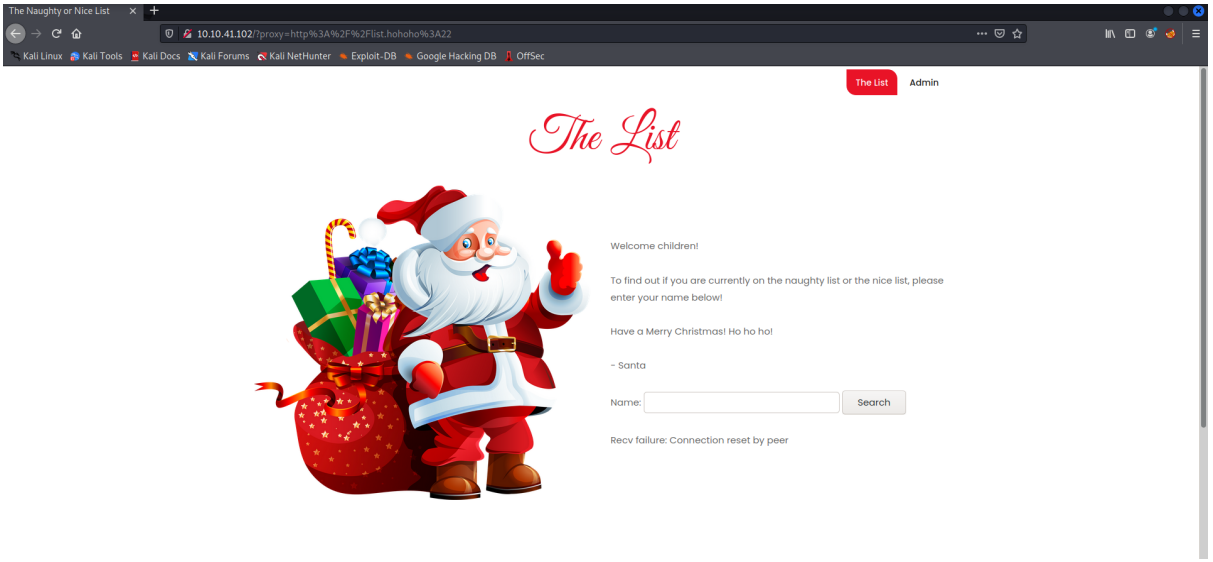
Question 3

Paste "/?proxy=http%3A%2F%2Flist.hohoho%3A80"? on the browser.



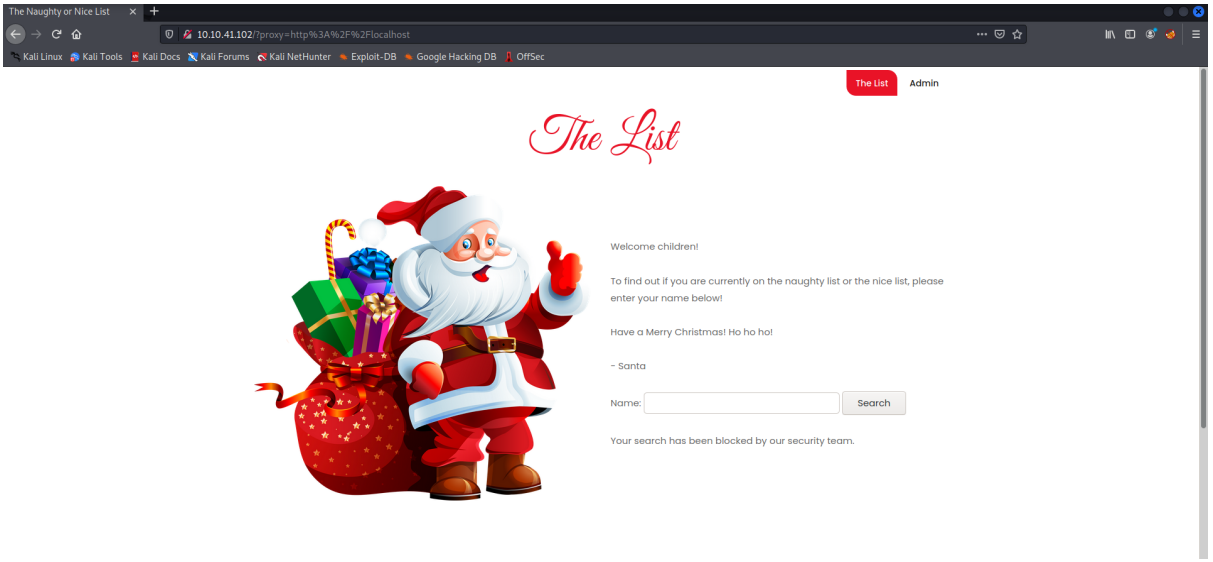
Question 4

Paste "/?proxy=http%3A%2F%2Flist.hohoho%3A22" on the browser.



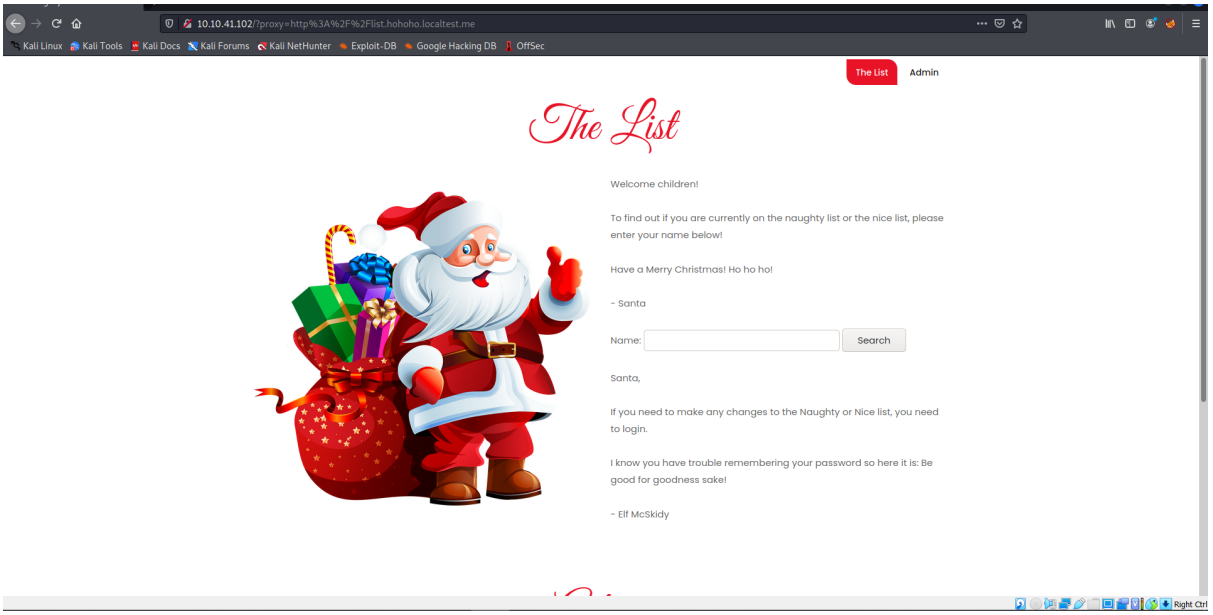
Question 5

Paste "/?proxy=http%3A%2F%2Flocalhost" on the browser.



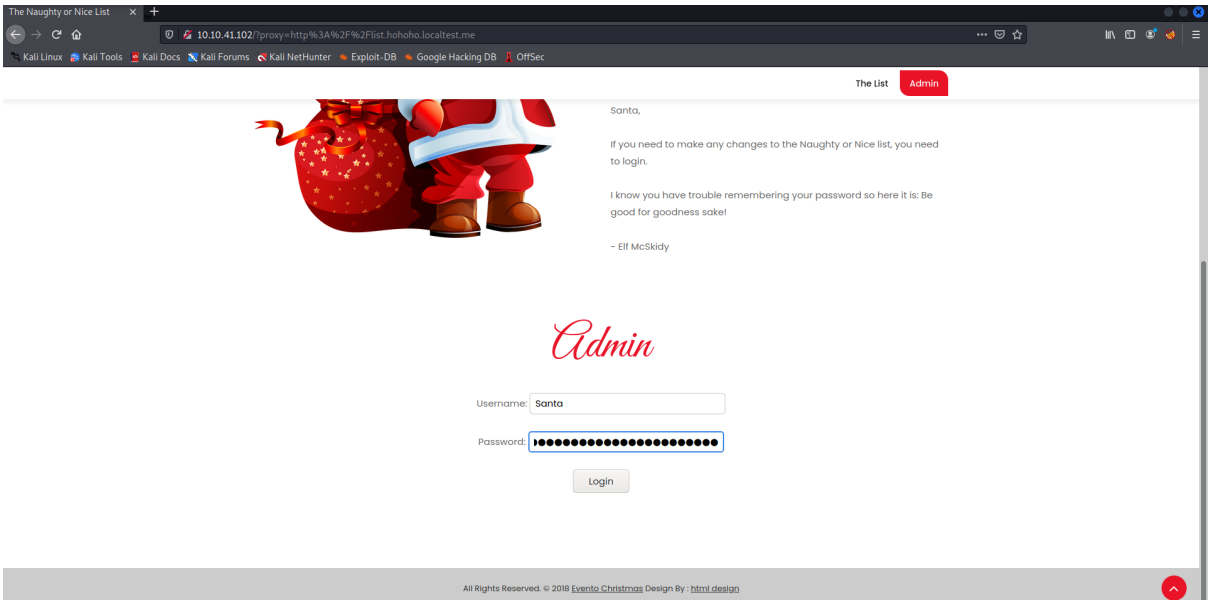
Question 6

Set the hostname in the URL to "list.hohoho.localtest.me". Look for the password.

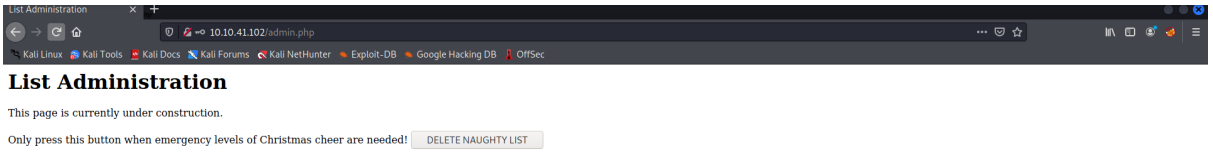


Question 7

Guess the username and enter the password.



Delete the naughty list.



Thought process/Methodology:

To begin with, we entered the Ip address given and directed to the website. When we search a name in the search bar, the page is loaded and told whether the name is on the Naughty list or Nice list. We noticed the URL had changed and we tried to fetch the root, but it gave us a 404 message. We tried to change the port to 80 but the connection was refused. When we switched the port to 22, we got this message; "Recv failure: Connection reset by peer". We tried to run the server locally, but it got blocked by the security team. Although it was unfortunate, we noticed that we can take advantage of DNS subdomains and create our own domain. So, we used the localtest.me and it brought us to the password. After guessing the username and entering the password at the admin login page, it brought us to the list administration. There, we can delete the Naughty list and get the flag.

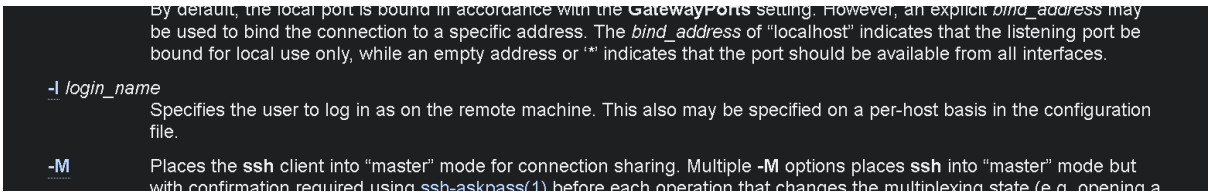
Day 20 : Blue Teaming - PowershELlF to the rescue

Tools used: Kali Linux, Firefox, SSH

Solution/walkthrough:

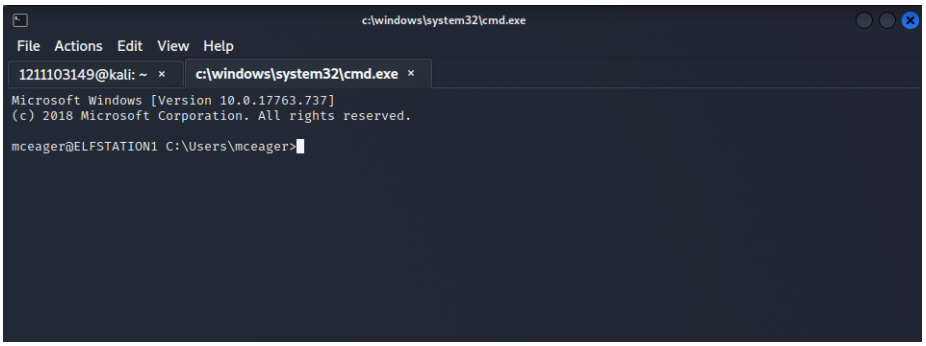
Question 1

Search for -l in the SHH manual

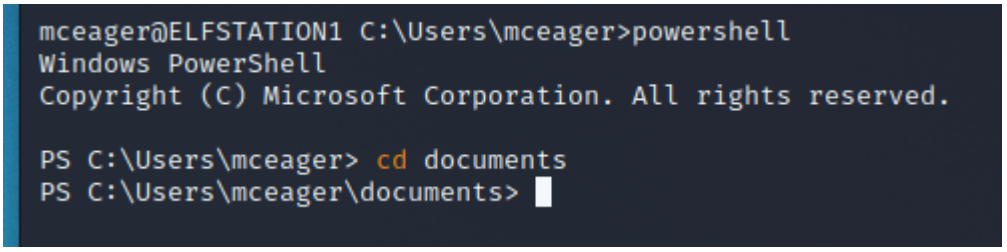


Question 2

Enter the command and password given to login.



Startup powershell and got to documents



Using some commands we can get to the hidden files. catscan the contents to get the answer

```
PS C:\Users\mceager> cd documents
PS C:\Users\mceager\documents> get-childitem -file -hidden


    Directory: C:\Users\mceager\documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a-hs-         12/7/2020  10:29 AM            402 desktop.ini
-arh--        11/18/2020   5:05 PM             35 e1fone.txt


PS C:\Users\mceager\documents> get-content e1fone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\documents>
```

Question 3

Go into desktop to find the elf2wo file

```
PS C:\Users\mceager\documents> cd ..
PS C:\Users\mceager> cd desktop
PS C:\Users\mceager\desktop> ls -hidden


    Directory: C:\Users\mceager\desktop


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


PS C:\Users\mceager\desktop>
```

Cat the file to get the answer

```
PS C:\Users\mceager\desktop> cd .\elf2wo\
PS C:\Users\mceager\desktop\elf2wo> get-childitem


    Directory: C:\Users\mceager\desktop\elf2wo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         11/17/2020  10:26 AM             64 e70smsW10Y4k.txt


PS C:\Users\mceager\desktop\elf2wo> cat e70smsW10Y4k.txt
I want the movie Scrooged <3!
PS C:\Users\mceager\desktop\elf2wo>
```

Question 4

Go into system 32 in windows

```
PS C:\Users\mceager> cd C:/Windows
PS C:\Windows> cd system32
PS C:\Windows\system32>
```

Using filter to easily find the hidden file

```
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

change the directory to the file and get the contents with -hidden

```
PS C:\Windows\system32> cd 3lfthr3e
PS C:\Windows\system32\3lfthr3e> ls -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
```

Use the command from THM to get the number of words in the first file

```
PS C:\Windows\system32\3lfthr3e> cat 1.txt | Measure-object -Word

Lines Words Characters Property
----- ----- ---------- --------
       9999


PS C:\Windows\system32\3lfthr3e>
```

Question 6

Use command from THM to get the exact position we want

```
PS C:\Windows\system32\3lfthr3e> (cat 1.txt)[551]
Red
PS C:\Windows\system32\3lfthr3e> (cat 1.txt)[6991]
Ryder
PS C:\Windows\system32\3lfthr3e>
```

Question 7

Use the command from THM to search for string only with redryder in them to get the answer

```
PS C:\Windows\system32\3lfthr3e> cat 2.txt | select-string -Pattern "redryder"

redryderbbgun


PS C:\Windows\system32\3lfthr3e>
```

Thought Process/Methodology:

Using the command given in THM, we were able to get into the windows machine. Using commands we can search for items in a file to get the answer and using filters we can narrow down the search to hidden items,the number of the index and a specific string