PSP0201 WEEKLY REPORT

Group name: Apocalypse

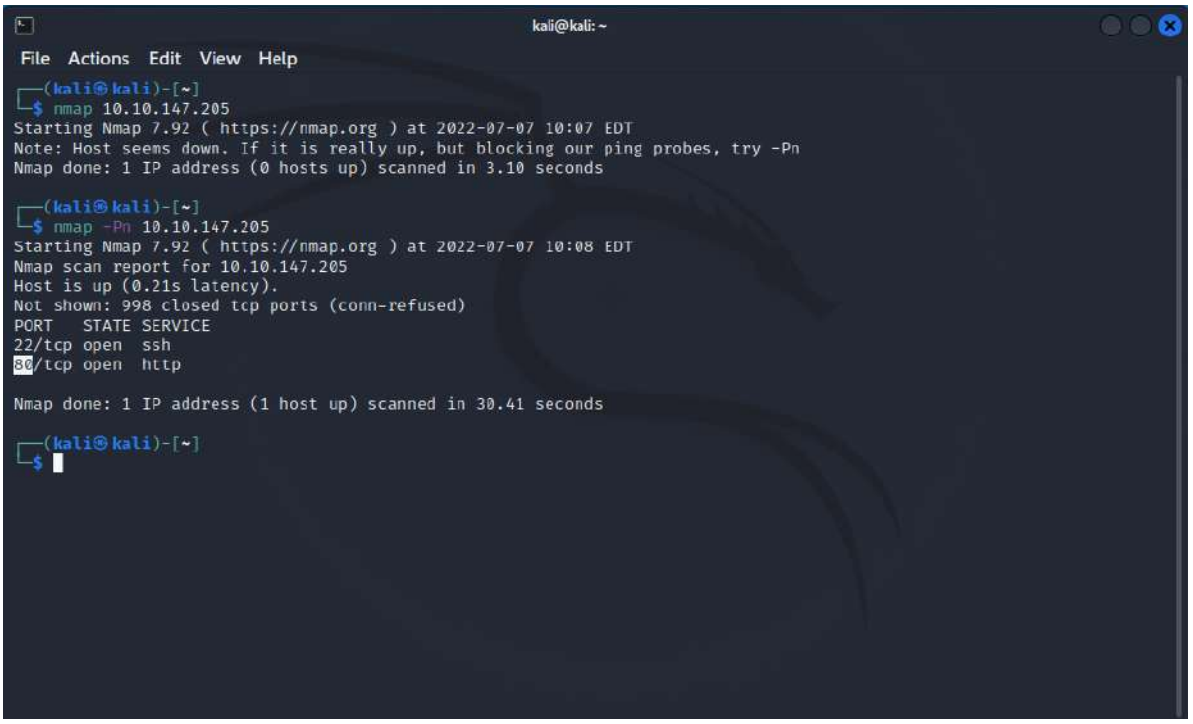
Members

ID	NAME	ROLE
1211103698	UMMI SYAHIRAH BINTI MUHAMMAD ROZAIDEE	LEADER
1211103293	FARAH FAMILA BINTI YAHYA	MEMBER
1211102031	NOR ALIAH SYUHAIDAH BINTI SHARUDDIN	MEMBER
1211101673	NURUL MANJA MURNIRA NAJWA BINTI MALIKI	MEMBER

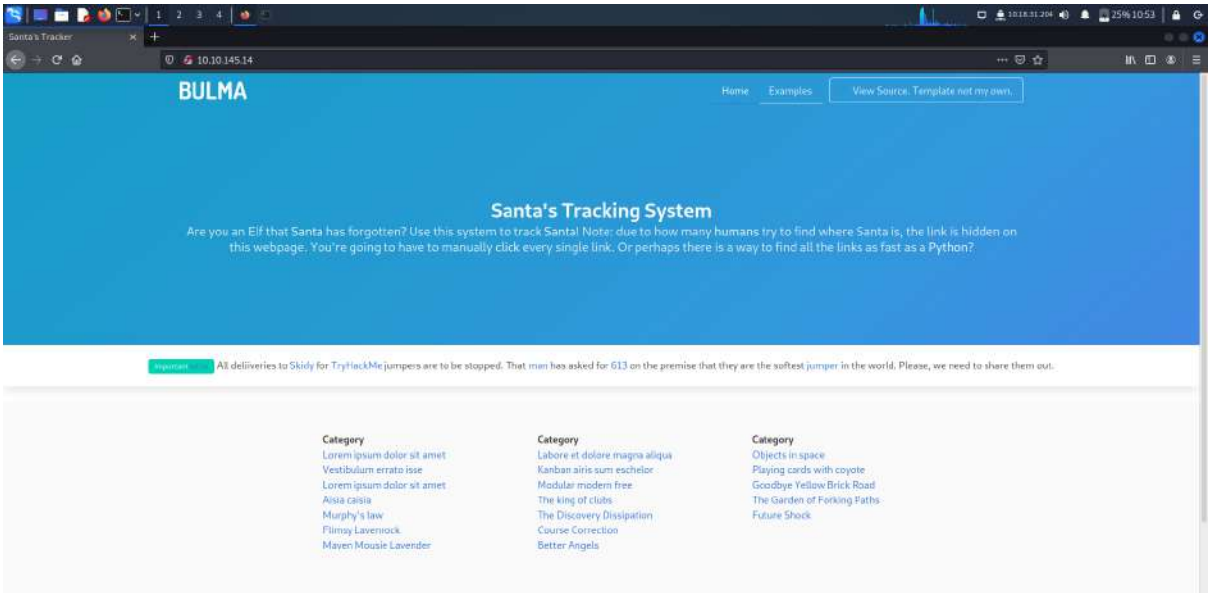
DAY 16 : [Scripting] Help! Where is Santa?

Tools used : Kali Linux, Firefox, Python3,

Question 1



Question 2

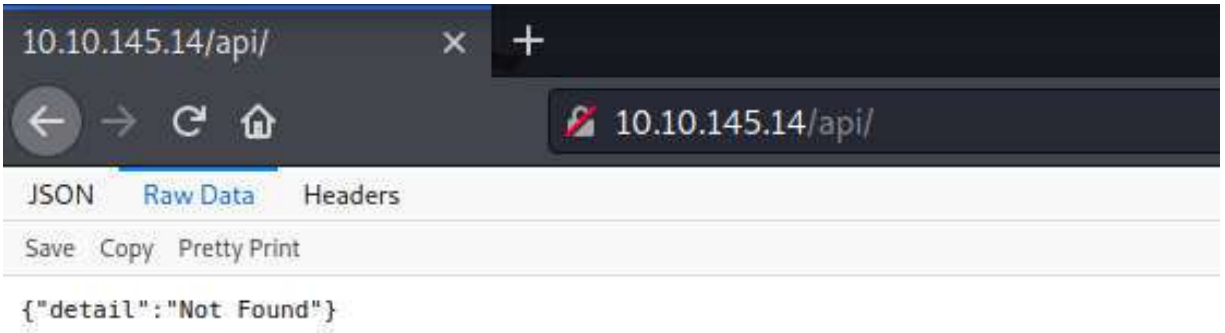


Question 3

Paste the Ip address on firefox and go to web consoles.

```
<footer class="footer">
    <div class="container">
        <div class="columns">
            <div class="column is-3 is-offset-2">
                <h2><strong>Category</strong></h2>
                <ul>
                    <li><a href="#">Lorem ipsum dolor sit amet</a></li>
                    <li><a href="#">Vestibulum errato isse</a></li>
                    <li><a href="#">Lorem ipsum dolor sit amet</a></li>
                    <li><a href="#">Aisia caisia</a></li>
                    <li><a href="#">Murphy's law</a></li>
                    <li><a href="#">Flimsy Lavenrock</a></li>
                    <li><a href="#">Maven Mousie Lavender</a></li>
                </ul>
            </div>
            <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>
            </div>
            <div class="column is-4">
                <h2><strong>Category</strong></h2>
                <ul>
                    <li><a href="#">Objects in space</a></li>
                    <li><a href="#">Playing cards with coyote</a></li>
                    <li><a href="#">Goodbye Yellow Brick Road</a></li>
                    <li><a href="#">The Garden of Forking Paths</a></li>
                    <li><a href="#">Future Shock</a></li>
                </ul>
            </div>
        </div>
        <div class="content has-text-centered">
            <p>
                <a class="icon" href="https://github.com/BulmaTemplates/bulma-templates">
                    <i class="fa fa-github"></i>
                </a>
            </p>
            <div class="control level-item">
                <a href="https://github.com/BulmaTemplates/bulma-templates">
                    <div class="tags has-addons">
                        <span class="tag is-dark">Bulma Templates</span>
                        <span class="tag is-info">MIT license</span>
                    </div>
```

Question 4



Question 5

Install pyhton3 on the terminal.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ pip3 install requests beautifulsoup4
Command 'pip3' not found, but can be installed with:
sudo apt install python3-pip
Do you want to install it? (N/y)y
sudo apt install python3-pip
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-wheel
The following NEW packages will be installed:
  python3-pip python3-wheel
0 upgraded, 2 newly installed, 0 to remove and 1377 not upgraded.
Need to get 1,387 kB of archives.
After this operation, 7,405 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-wheel all 0.37.1-2 [31.6 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 python3-pip all 22.1.1+dfsg-1 [1,355 kB]
Fetched 1,387 kB in 2s (774 kB/s)
Selecting previously unselected package python3-wheel.
(Reading database ... 268454 files and directories currently installed.)
Preparing to unpack .../python3-wheel_0.37.1-2_all.deb ...
Unpacking python3-wheel (0.37.1-2) ...
Selecting previously unselected package python3-pip.
Preparing to unpack .../python3-pip_22.1.1+dfsg-1_all.deb ...
Unpacking python3-pip (22.1.1+dfsg-1) ...
Setting up python3-wheel (0.37.1-2) ...
Setting up python3-pip (22.1.1+dfsg-1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for kali-menu (2021.4.2) ...

┌──(kali㉿kali)-[~]
└─$ 
                                                                    127 ✗
```

Type nano script.py and type the command to track the santa. Save the file and the file name is *script.py.*

```
kali@kali: ~
File  Actions  Edit  View  Help
  GNU nano 5.9                          script.py *
from b54 import BeautifulSoup
import requests

for dupa in range(1,100,2):
        print (f"{dupa}")
        html = requests.get(f'http://10.10.147.205/api/{dupa}')
        print (html.text)

Save modified buffer?
 Y Yes
 N No          ^C Cancel
```

Last but not least, you can track the location of the santa.

```
{"item_id":37,"q":"Error. Key not valid!"}
39
{"item_id":39,"q":"Error. Key not valid!"}
41
{"item_id":41,"q":"Error. Key not valid!"}
43
{"item_id":43,"q":"Error. Key not valid!"}
45
{"item_id":45,"q":"Error. Key not valid!"}
47
{"item_id":47,"q":"Error. Key not valid!"}
49
{"item_id":49,"q":"Error. Key not valid!"}
51
{"item_id":51,"q":"Error. Key not valid!"}
53
{"item_id":53,"q":"Error. Key not valid!"}
55
{"item_id":55,"q":"Error. Key not valid!"}
57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
59
{"item_id":59,"q":"Error. Key not valid!"}
61
```

Question 6

```
67
{"item_id":67,"q":"Winter Wonderland, Hyde Park, London."}
59
```

Methodology/Thought Process:

Port number of the website server can be found by using the terminal and using the “Nmap” method. Nmap for network discovery and security auditing. The installation of python3 in the terminal can use any tools converted to Python 3 containing only scripts.

DAY 17: [REVERSE ENGINEERING] ReverseELFneering

Tools used: Kali Linux

Question 1
The answer can be found 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

The answer can be found 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`

Note, when using the `aa` command in radare2, this may take between 5-10 minutes depending on your system.

Which is the most common analysis command. It analyses all symbols and entry points in the executable. The analysis, in this case, involves extracting function names, flow control information, and much more! r2 instructions are usually based on a single character, so it is easy to get more information about the commands.

Question 3

The answer can be found 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.

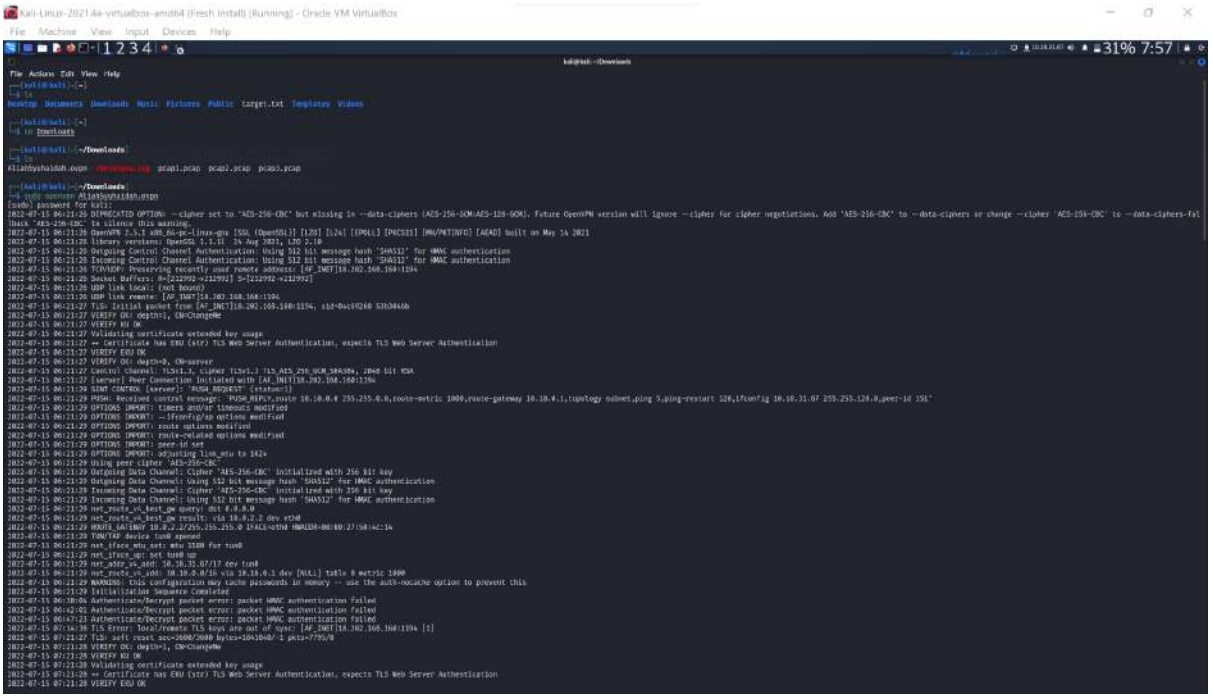
Question 4

The answer can be found in TryHackMe.

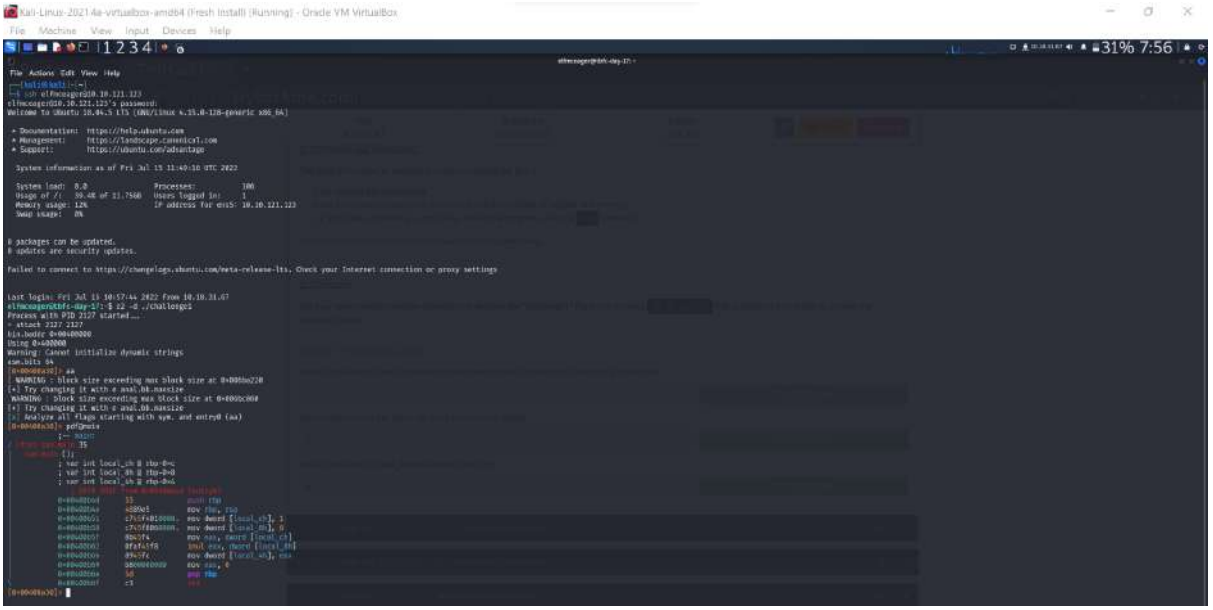
Running `dc` will execute the program until we hit the breakpoint

Question 5,6,7

Access machine using vpn.



Run the command **ssh elfmceager [IP Address]** and the password is **adventofcyber.** Run the command **r2 -d ./challenge > aa > pdf@main.**



Methodology/Thought Process:

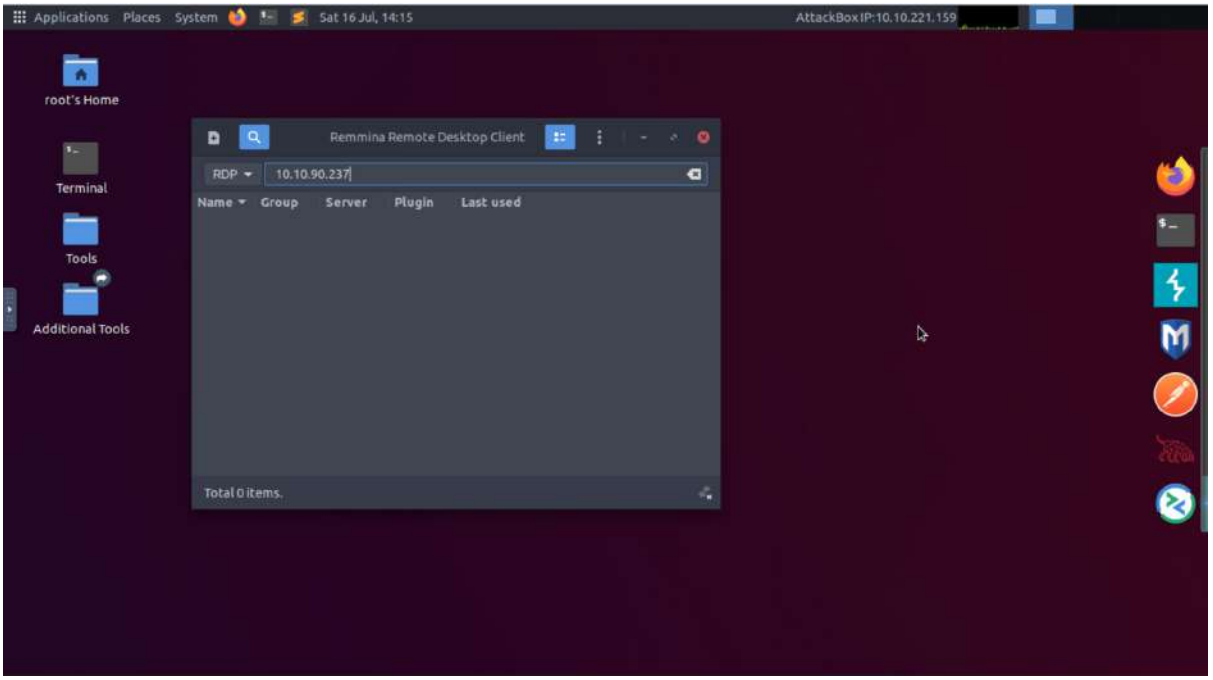
Answers for question 1-4 can be found in TryHackMe Day 17 material. Answers for 5-7, access machine using vpn. Open another terminal and use ssh to access the system by command **ssh elfmceager [IP Address]**, and fill the password with **adventofcyber.** After that run the command **r2 -d ./challenge1.** Run the command **aa** to identify the program in radare2. Next, run the command **pdf@main** to examine the assembly code. The answer for question 5 is just straightforward which is **1**. For question 6, the answer is **6. 1 X 6 =6.** The answer for question 7 is **6.**

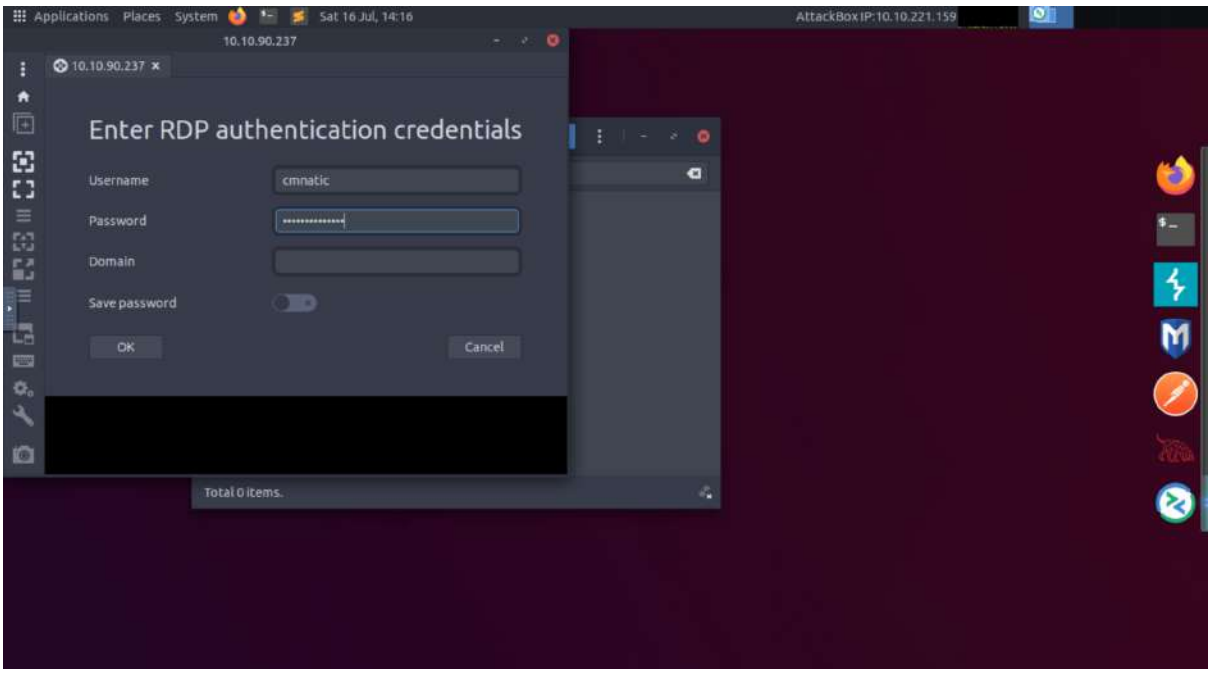
DAY 18: [REVERSE ENGINEERING] The Bits of Christmas

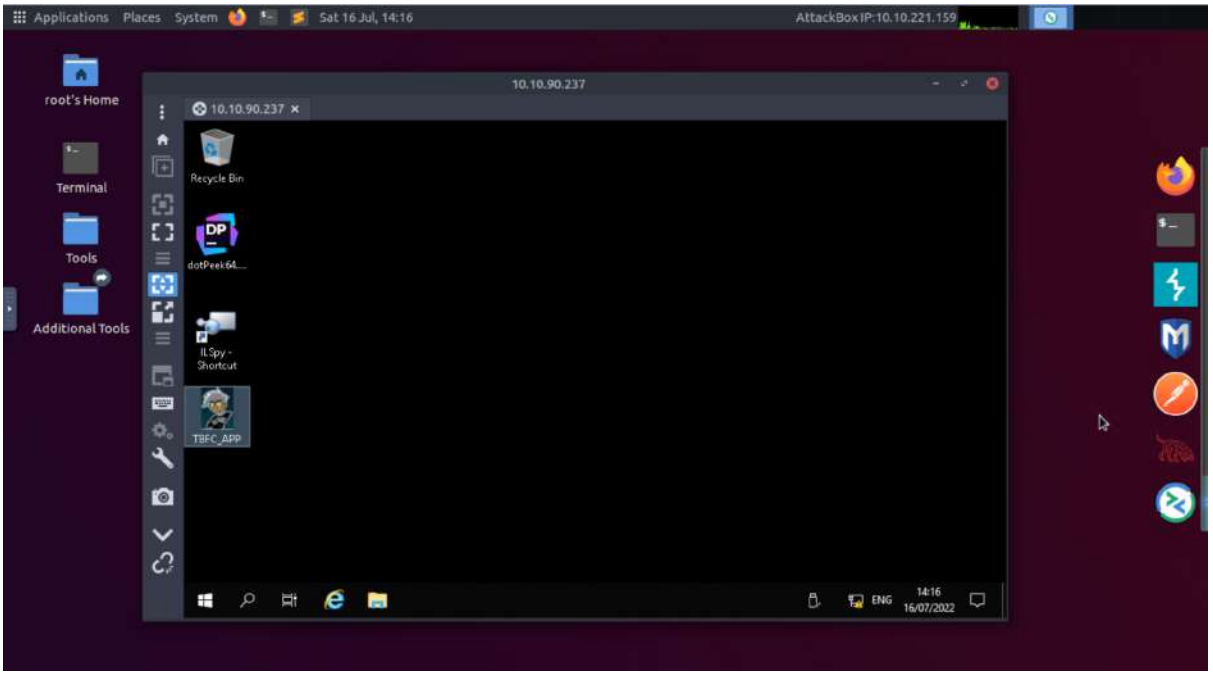
Tools used: Kali Linux

Question 1

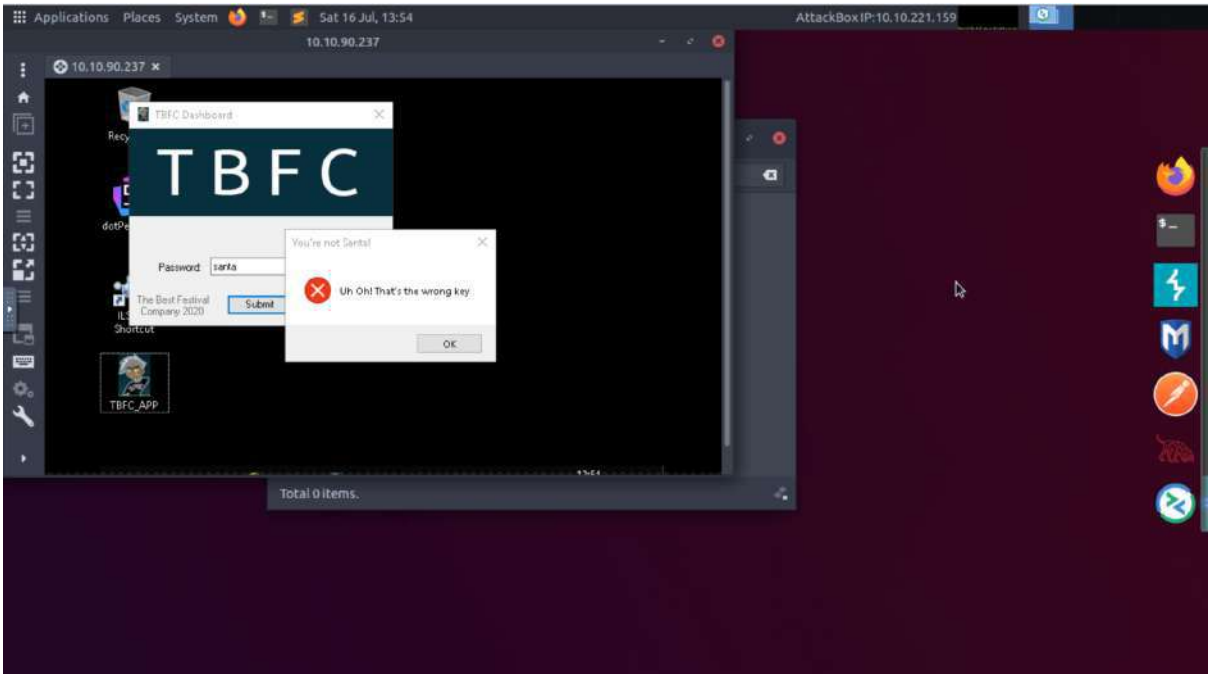
Open Remmina on your machine and put in the IP address provided by TryHackMe. Enter the username and password as provided by TryHackMe and then open the TBFC_APP already installed on Remmina.





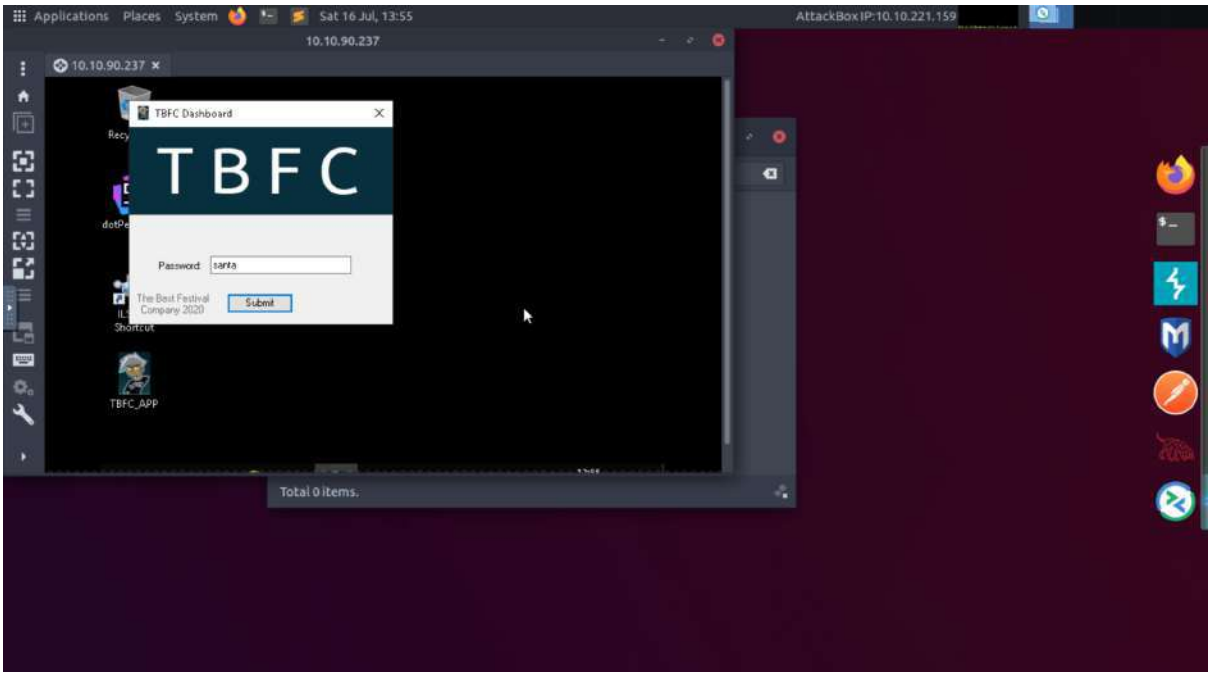


Put in any password and copy the message on the feedback returned.



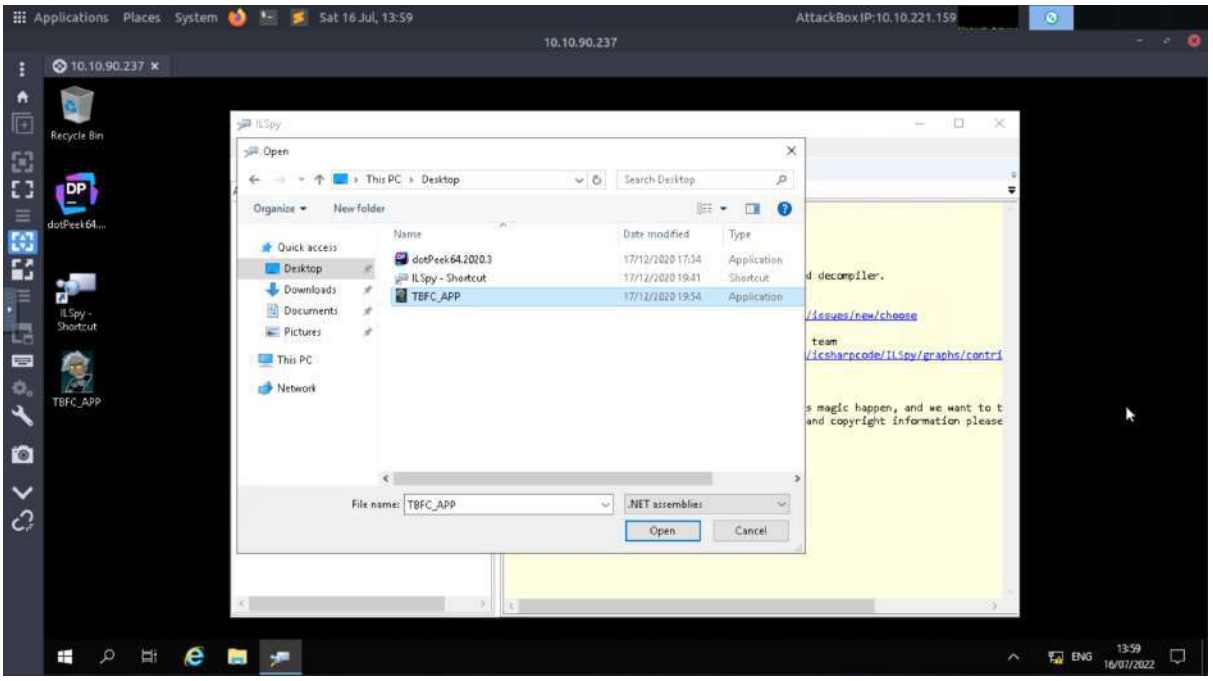
Question 2

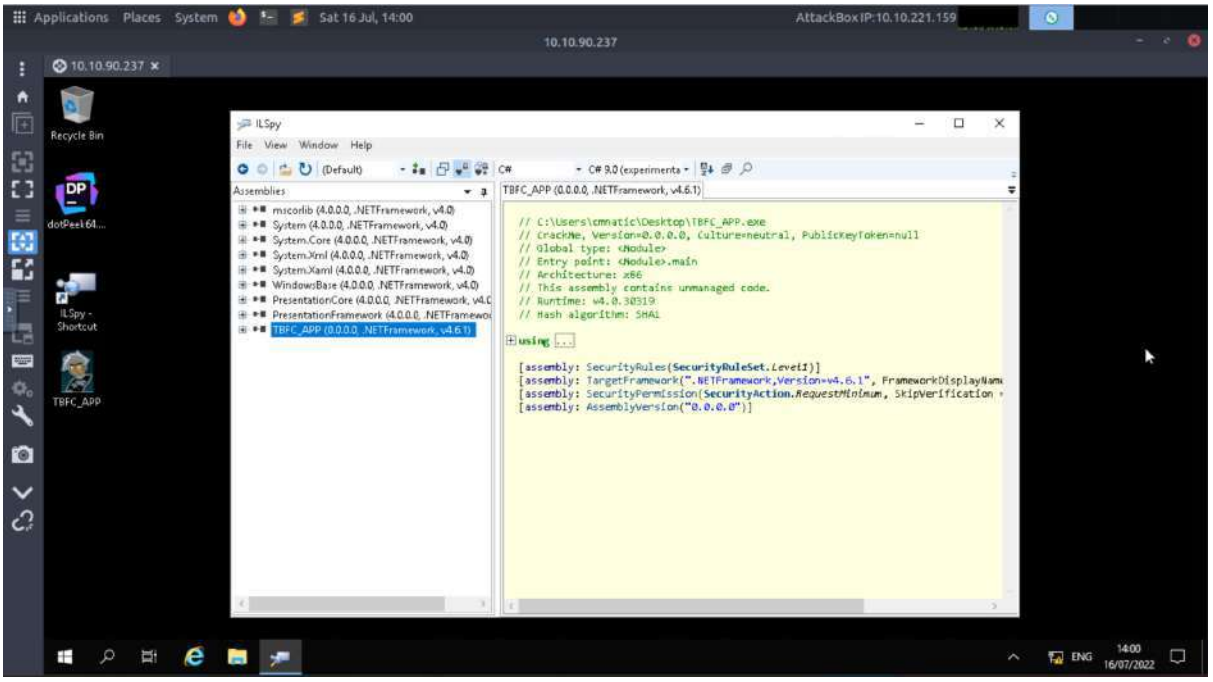
The meaning of TBFC is available on the dashboard of TBFC_APP.

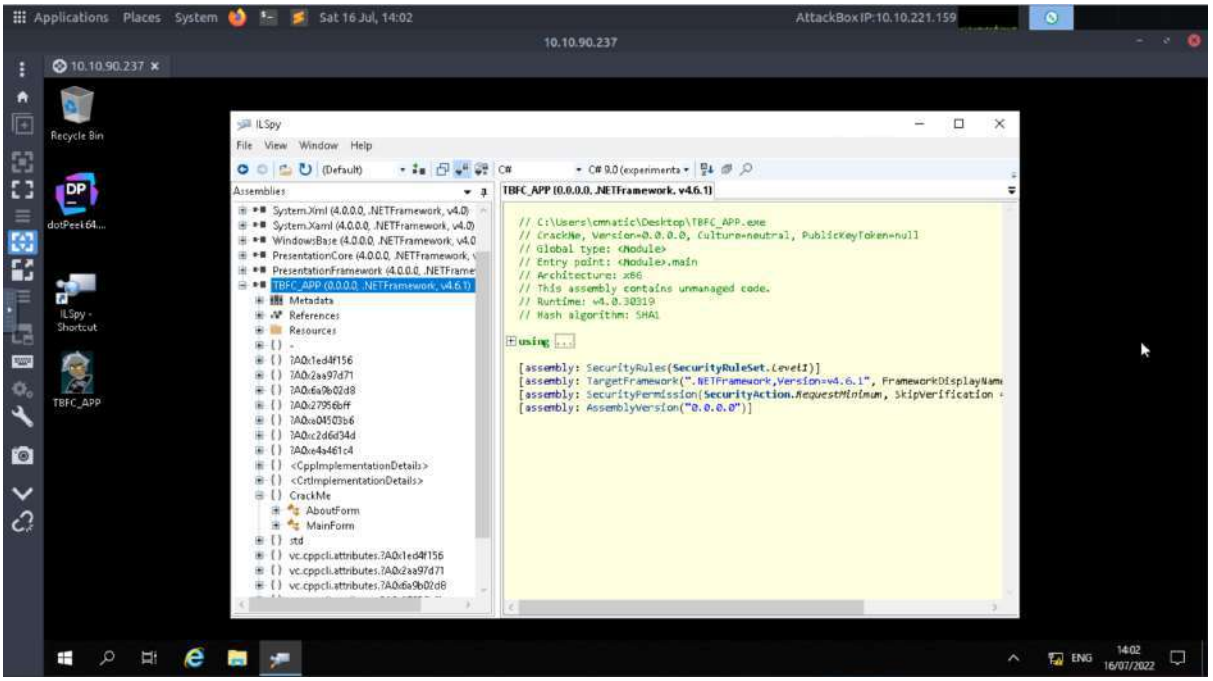


Question 3

Open ILSpy and then open TBFC_APP on ILSpy to decompile the code of the application. Once it's been decompiled, search for the module that stands out.

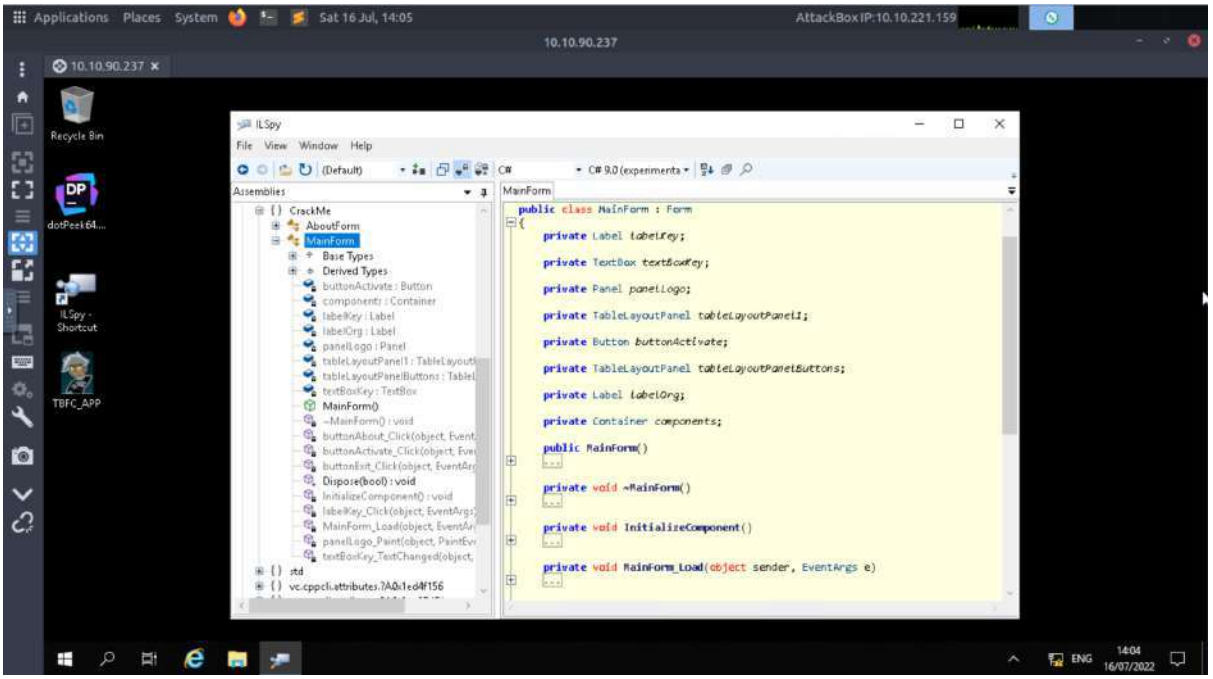



Applications Places System
Sat 16 Jul, 14:00
AttackBox IP:10.10.221.159
10.10.90.237
Recycle Bin
dotPeek64...
ILSpy - Shortcut
TBFC_APP
ILSpy
File View Window Help
Assemblies
mscorlib (4.0.0.0, .NETFramework, v4.0)
System (4.0.0.0, .NETFramework, v4.0)
System.Core (4.0.0.0, .NETFramework, v4.0)
System.Xml (4.0.0.0, .NETFramework, v4.0)
System.Xaml (4.0.0.0, .NETFramework, v4.0)
WindowsBase (4.0.0.0, .NETFramework, v4.0)
PresentationCore (4.0.0.0, .NETFramework, v4.0
PresentationFramework (4.0.0.0, .NETFramewo
TBFC_APP (0.0.0.0, .NETFramework, v4.6.1)
// C:\Users\cmnatic\Desktop\TBFC_APP.exe
// CrackMe, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null
// Global type: <Module>
// Entry point: <Module>.main
// Architecture: x86
// This assembly contains unmanaged code.
// Runtime: v4.0.30319
// Hash algorithm: SHA1
using ...
[assembly: SecurityRules(SecurityRuleSet.Level1)]
[assembly: TargetFramework(".NETFramework,Version=v4.6.1", FrameworkDisplayNam
[assembly: SecurityPermission(SecurityAction.RequestMinimum, SkipVerification
[assembly: AssemblyVersion("0.0.0.0")]
ENG
14:00
16/07/2022


Applications Places System
Sat 16 Jul, 14:02
AttackBox IP:10.10.221.159
10.10.90.237
Recycle Bin
dotPeek64...
ILSpy - Shortcut
TBFC_APP
ILSpy
File View Window Help
Assemblies
System.Xml (4.0.0.0, .NETFramework, v4.0)
System.Xaml (4.0.0.0, .NETFramework, v4.0)
WindowsBase (4.0.0.0, .NETFramework, v4.0
PresentationCore (4.0.0.0, .NETFramework,
PresentationFramework (4.0.0.0, .NETFrame
TBFC_APP (0.0.0.0, .NETFramework, v4.6.1)
Metadata
References
Resources
{} -
{} ?A0x1ed4f156
{} ?A0x2aa97d71
{} ?A0x6a9b02d8
{} ?A0x27956bff
{} ?A0xa04503b6
{} ?A0xc2d6d34d
{} ?A0xe4a461c4
{} <CppImplementationDetails>
{} <CrtImplementationDetails>
{} CrackMe
AboutForm
MainForm
{} std
{} vc.cppcli.attributes.?A0x1ed4f156
{} vc.cppcli.attributes.?A0x2aa97d71
{} vc.cppcli.attributes.?A0x6a9b02d8
TBFC_APP (0.0.0.0, .NETFramework, v4.6.1)
// C:\Users\cmnatic\Desktop\TBFC_APP.exe
// CrackMe, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null
// Global type: <Module>
// Entry point: <Module>.main
// Architecture: x86
// This assembly contains unmanaged code.
// Runtime: v4.0.30319
// Hash algorithm: SHA1
using ...
[assembly: SecurityRules(SecurityRuleSet.Level1)]
[assembly: TargetFramework(".NETFramework,Version=v4.6.1", FrameworkDisplayNam
[assembly: SecurityPermission(SecurityAction.RequestMinimum, SkipVerification
[assembly: AssemblyVersion("0.0.0.0")]
ENG
14:02
16/07/2022

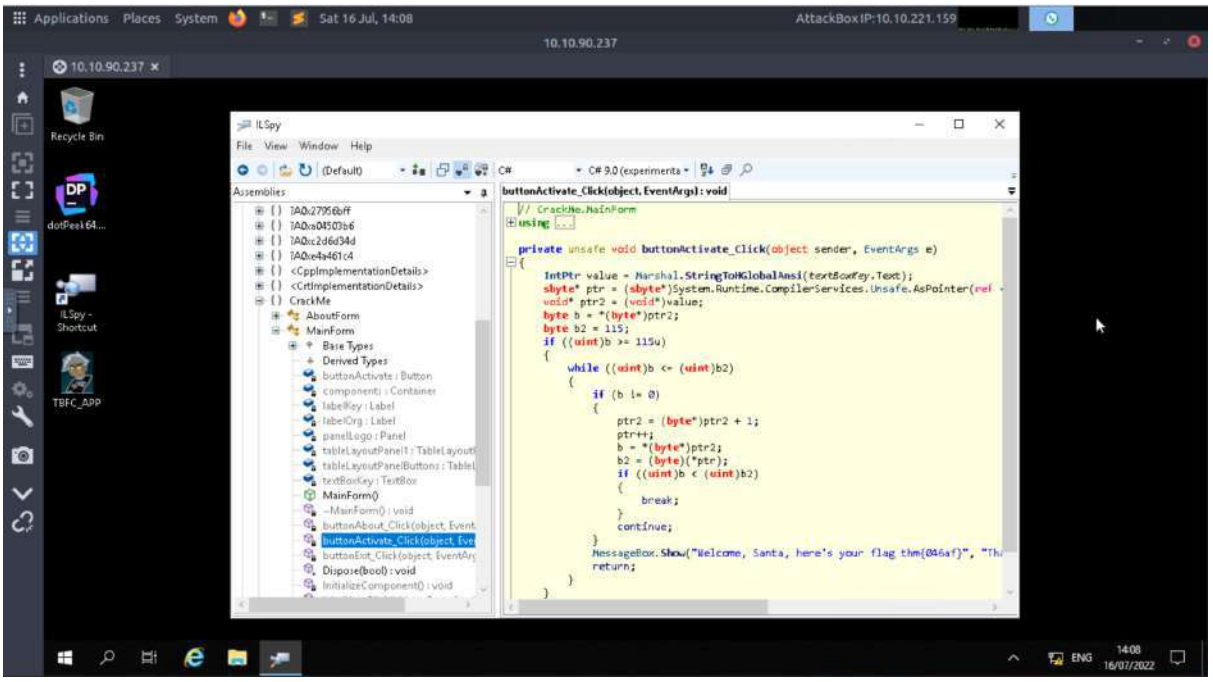
Question 4

Check through both options under CrackMe and look for the one that will provide information on the data input.



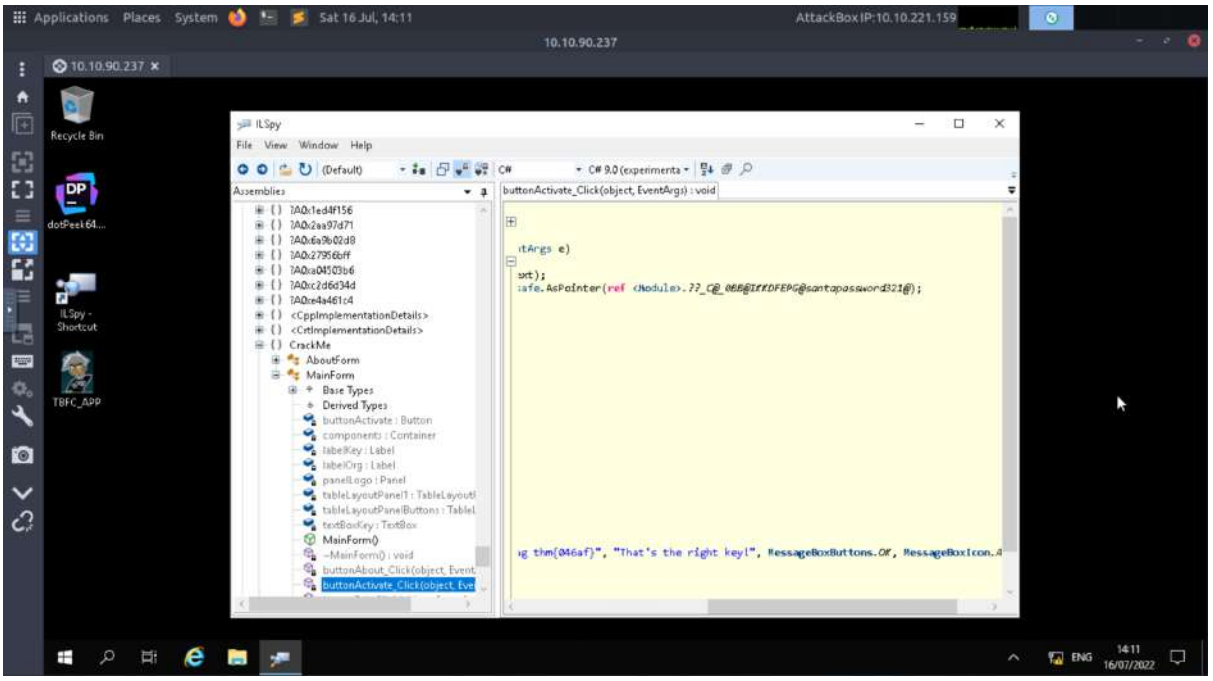
Question 5

Look through the methods under MainForm and find the one that provides information on the login data input.



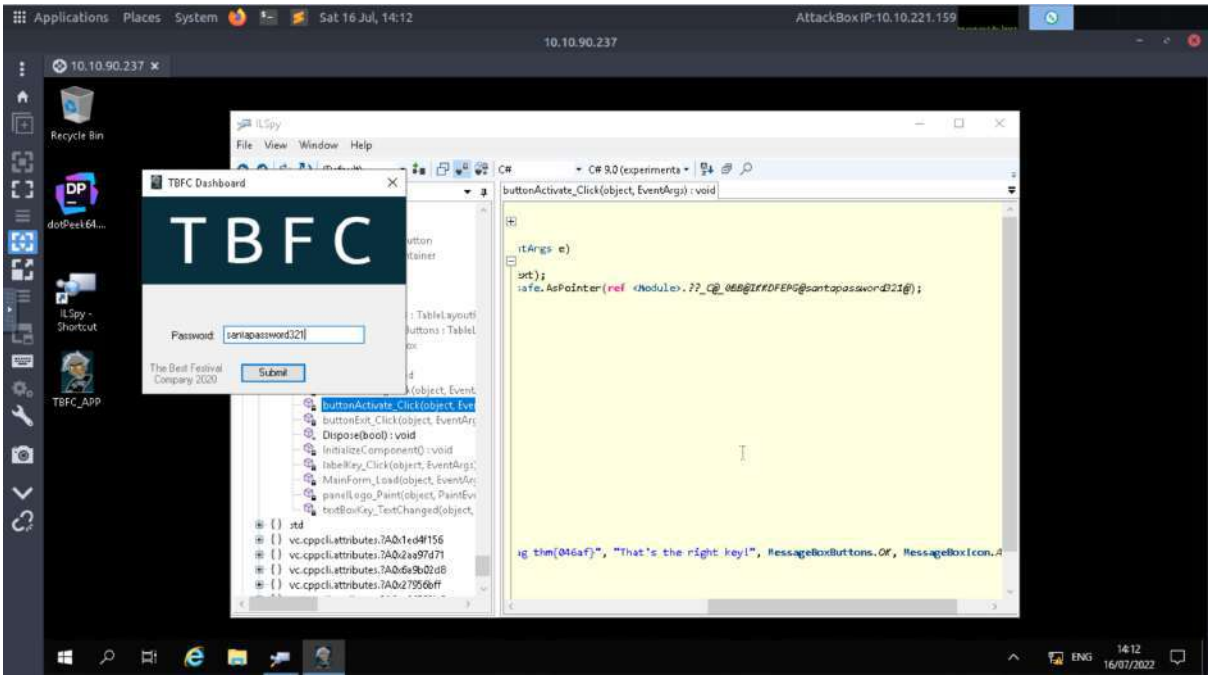
Question 6

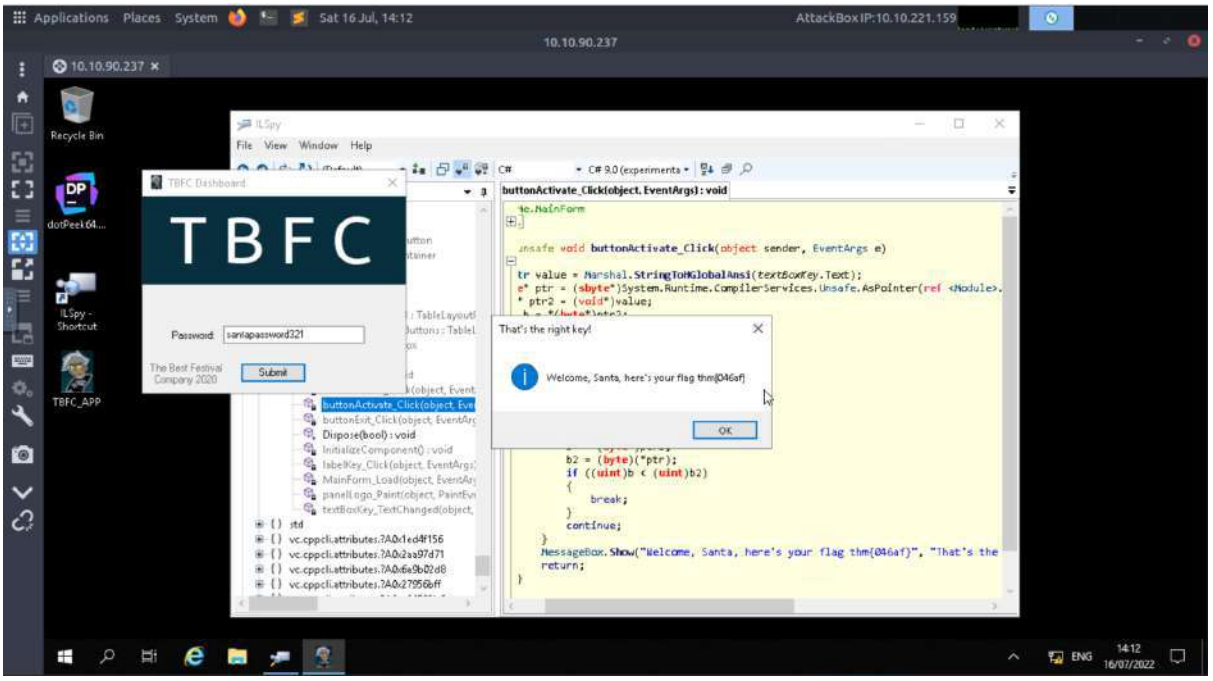
Once the login data input has been found, obtain the password to login to TBFC_APP.



Question 7

Open the TBFC_APP again and login with the correct password. The flag will then be returned.





Methodology/Thought Process:

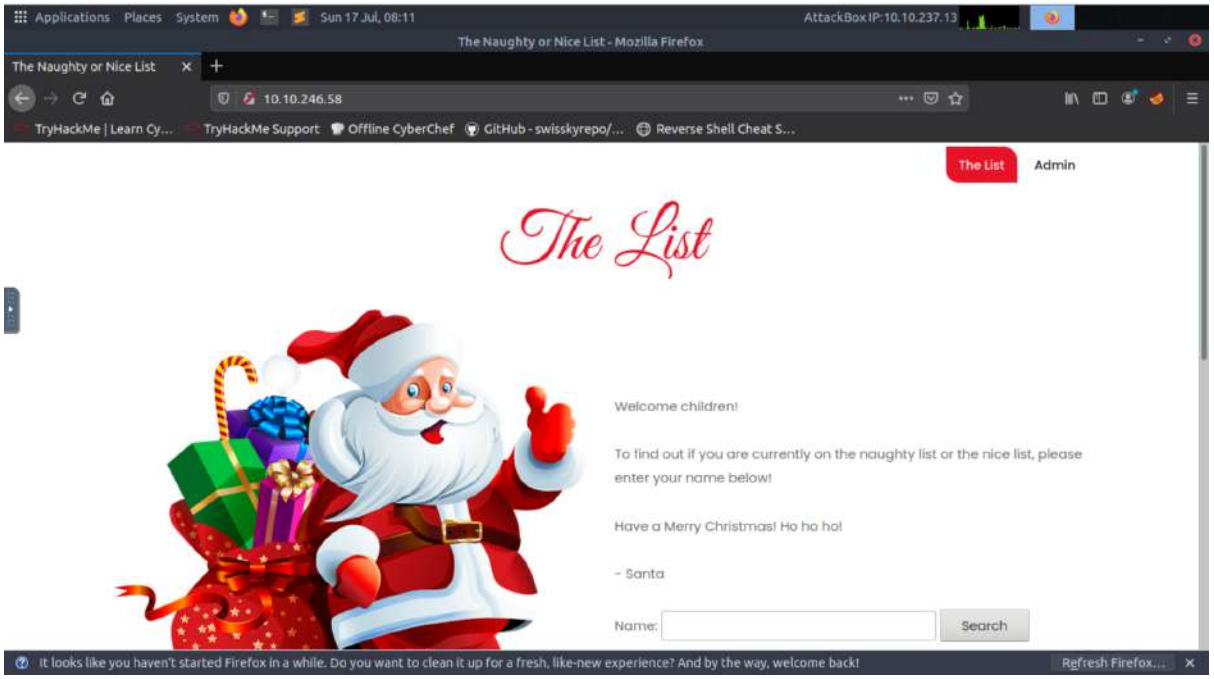
Open Remmina and put in the IP address that had been provided by TryHackMe. Once it's opened, we put in the username and password as provided by TryHackMe which will open the desktop to Remmina. Then, we opened the TBFC_APP that was available on Remmina's desktop. To decompile the code of TBFC_APP, we opened ILSpy and chose the TBFC_APP file. Once its code was decompiled, we looked through the modules and found that CrackMe stood out as it was unlike the other modules. Under the CrackMe module, we searched through the forms. The MainForm holds information regarding the data input, which is what we're looking for to get the login information. After going through the methods in the MainForm, we found that the buttonActivate_Click method had information about the login data input. In the code of that method, we found the password for TBFC_APP which is santapassword321. Then, we login to TBFC_APP using the password we found and the flag thm{046af} was returned.

DAY 19: [WEB EXPLOITATION] The Naughty or Nice List

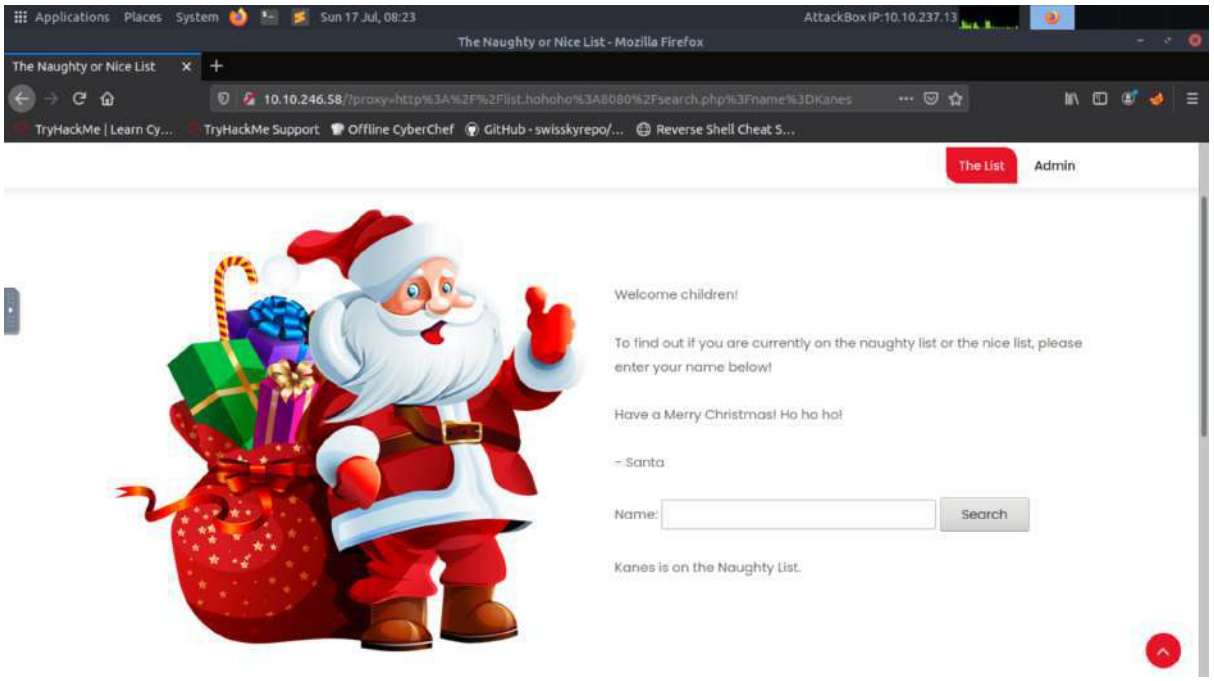
Tools used: Mozilla Firefox

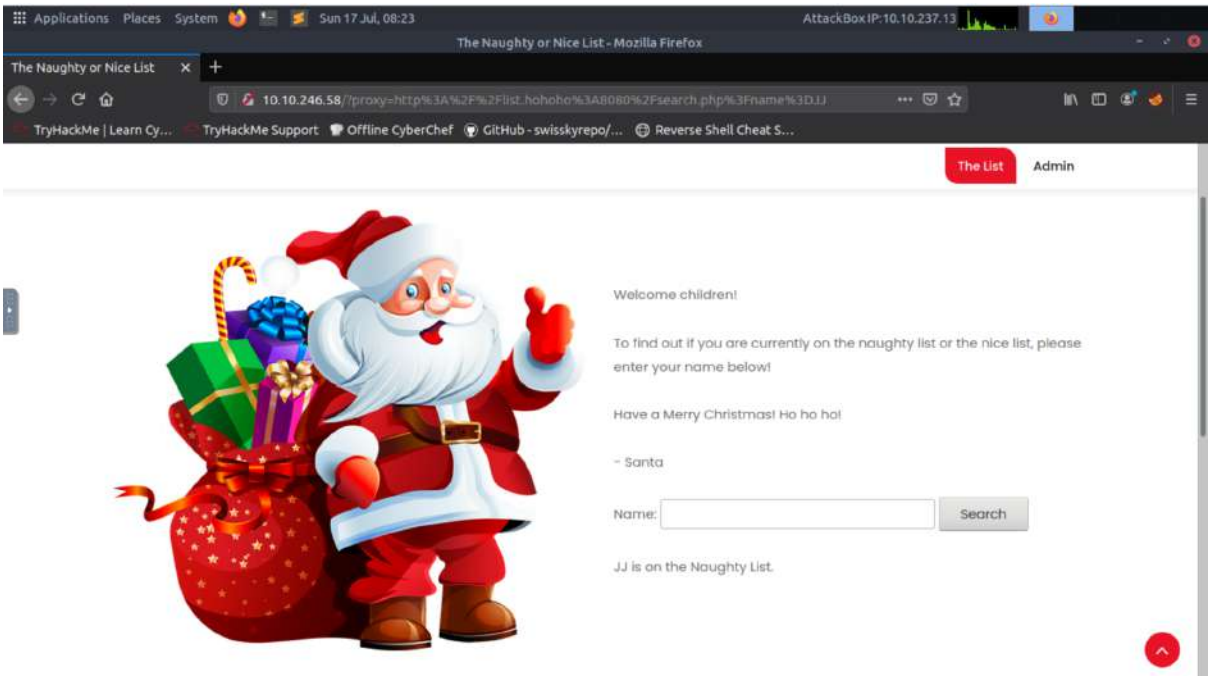
Question 1

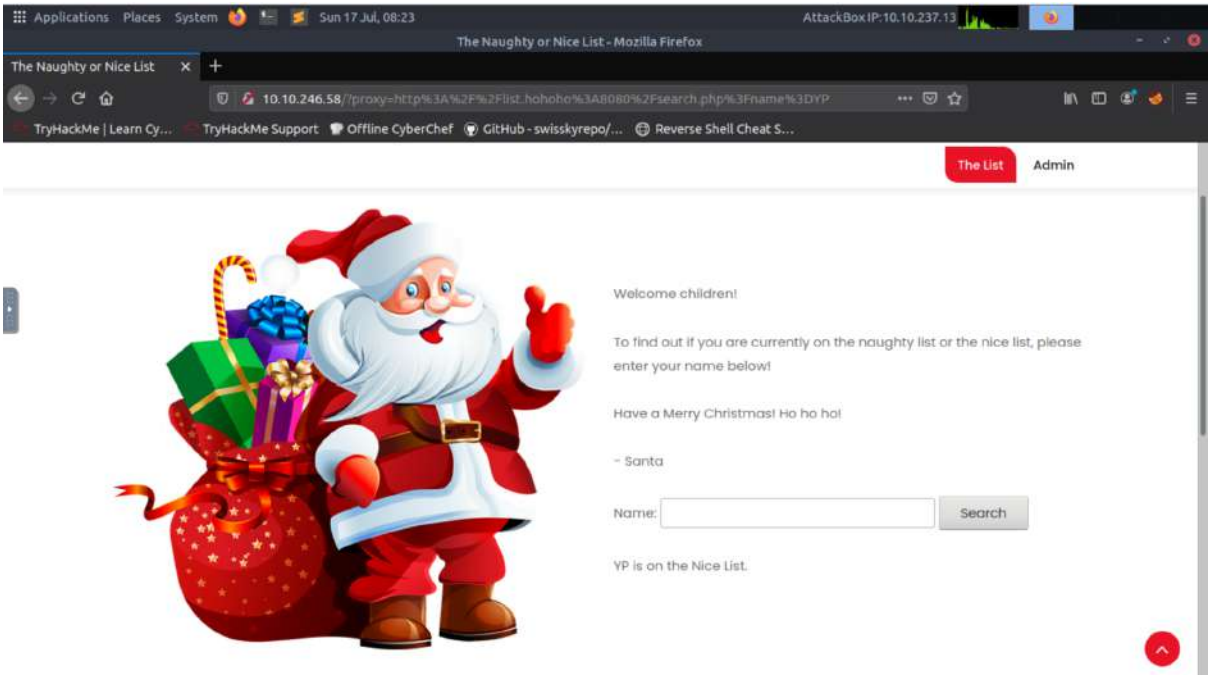
Open the website by using the IP address provided by TryHackMe

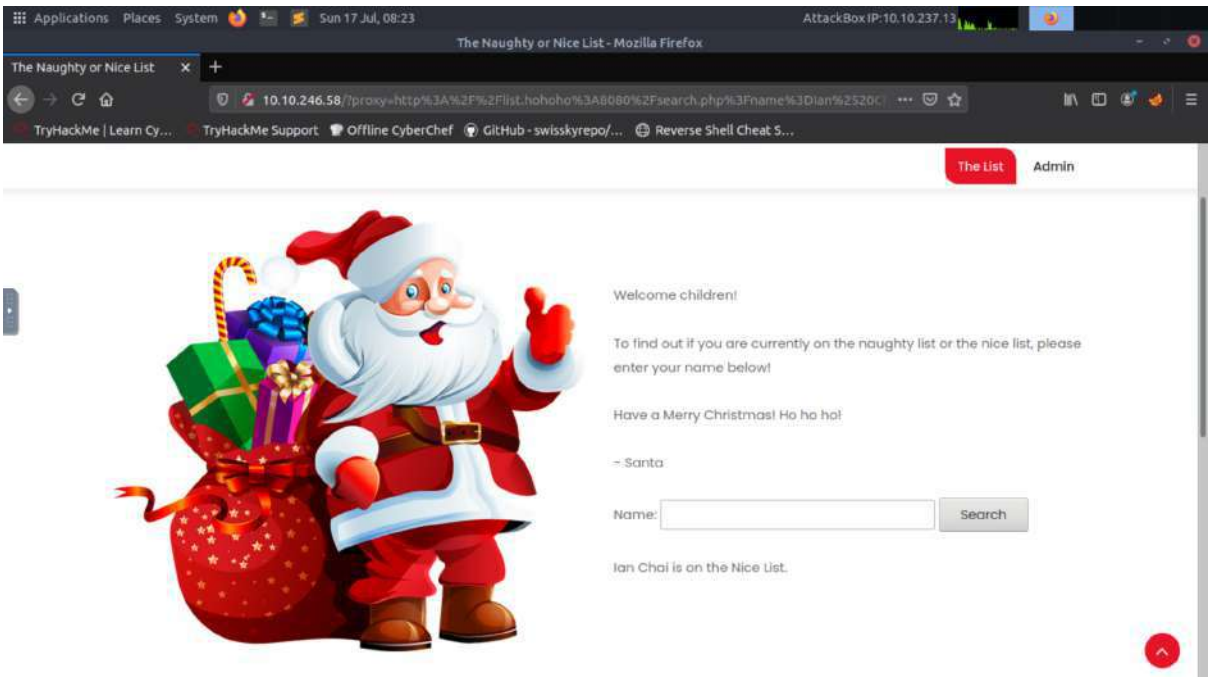


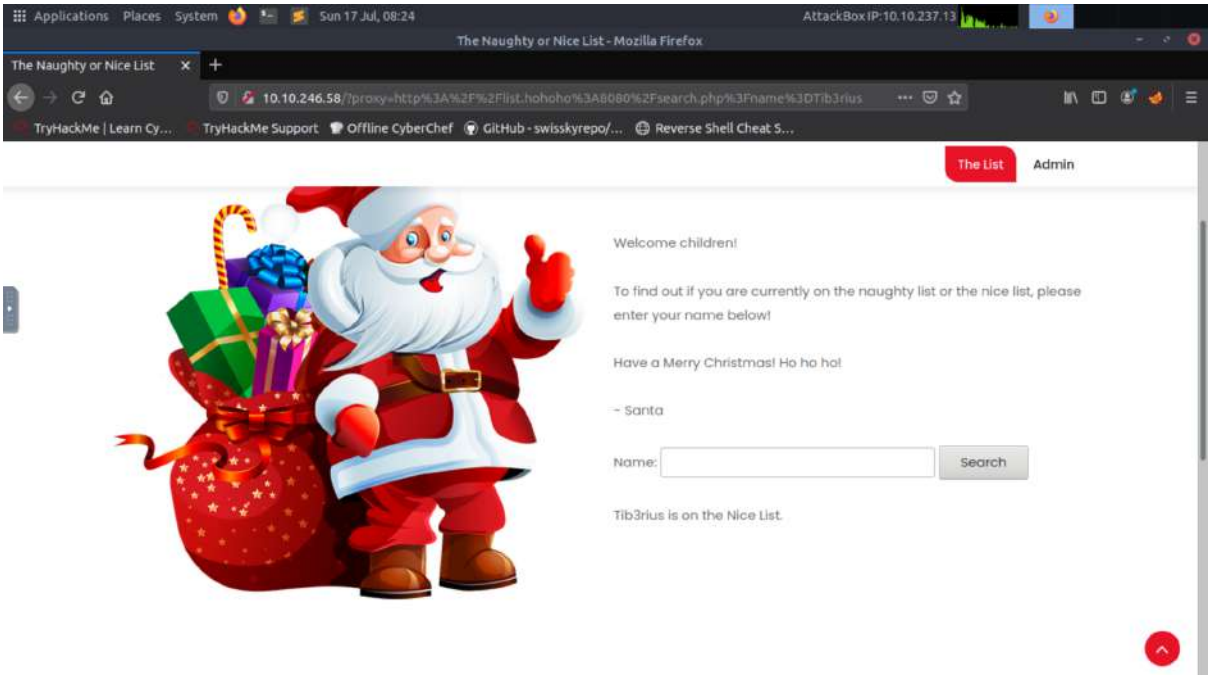
Once the page has loaded, scroll down to find the name search box and search the names given to see if they are on the naughty or nice list.

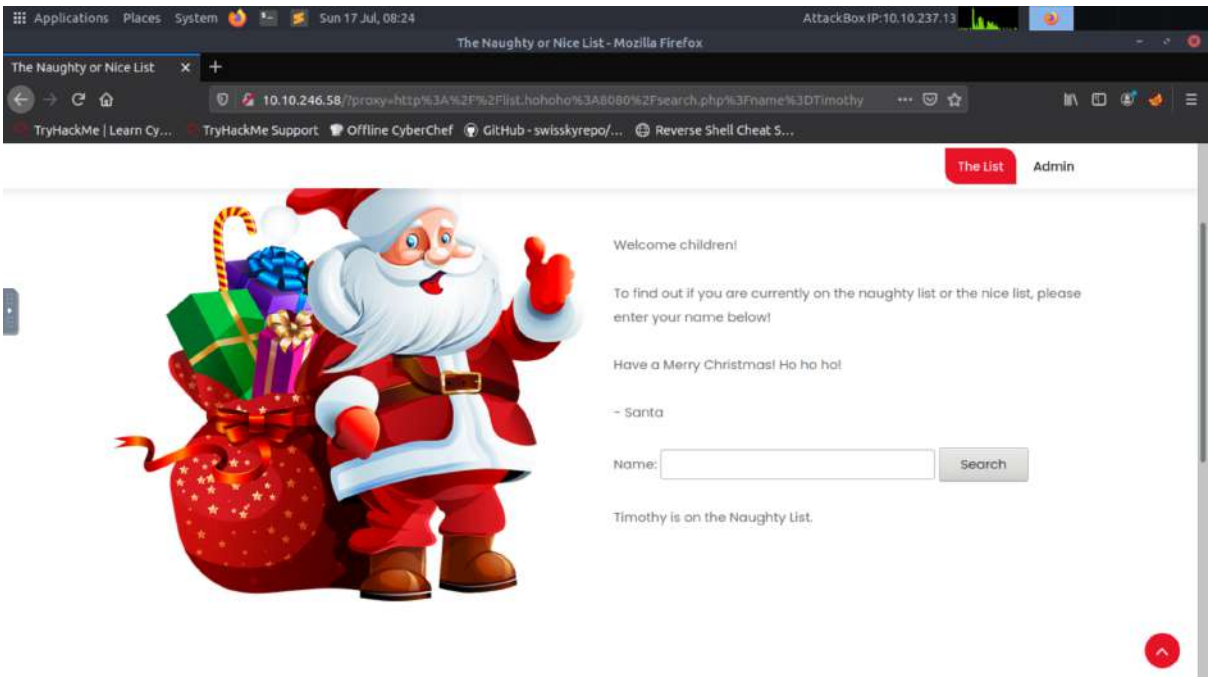



Applications Places System
Sun 17 Jul, 08:23
AttackBox IP: 10.10.237.13
The Naughty or Nice List - Mozilla Firefox
The Naughty or Nice List
10.10.246.58/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DJJ
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Reverse Shell Cheat S...
The List
Admin
Welcome children!
To find out if you are currently on the naughty list or the nice list, please enter your name below!
Have a Merry Christmas! Ho ho ho!
- Santa
Name:
Search
JJ is on the Naughty List.


Applications Places System
Sun 17 Jul, 08:23
AttackBox IP: 10.10.237.13
The Naughty or Nice List - Mozilla Firefox
The Naughty or Nice List
10.10.246.58/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DYP
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Reverse Shell Cheat S...
The List
Admin
Welcome children!
To find out if you are currently on the naughty list or the nice list, please enter your name below!
Have a Merry Christmas! Ho ho ho!
- Santa
Name:
Search
YP is on the Nice List.

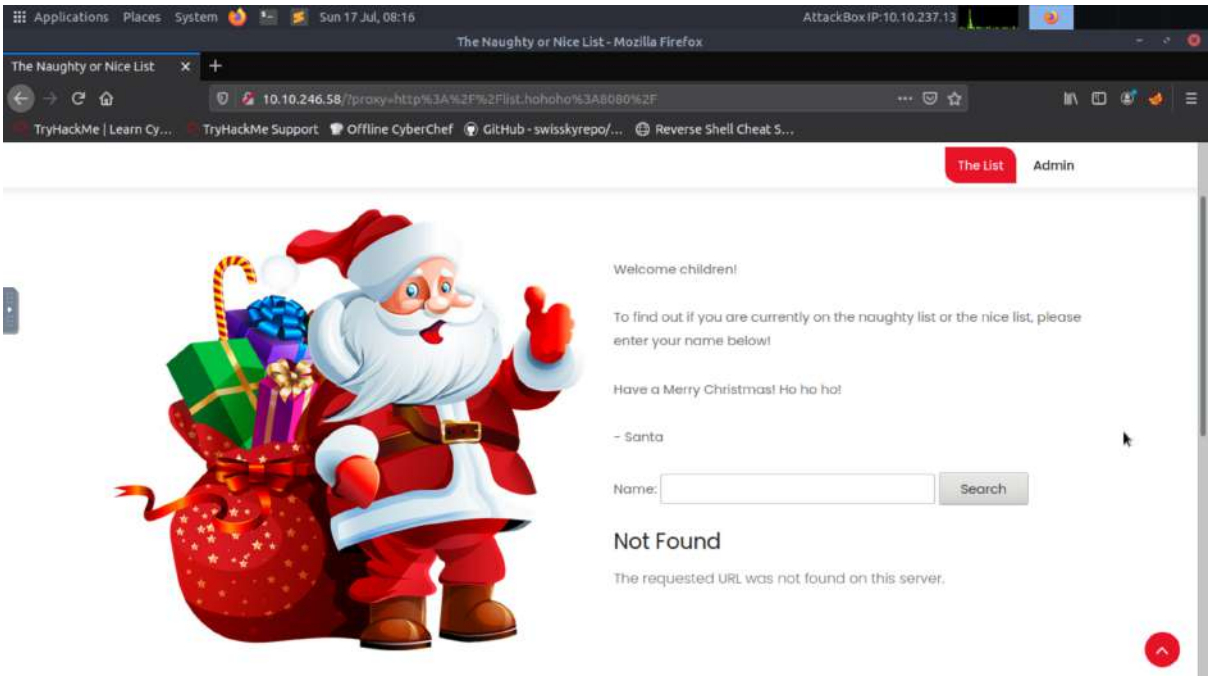

Applications Places System
Sun 17 Jul, 08:23
AttackBox IP:10.10.237.13
The Naughty or Nice List - Mozilla Firefox
The Naughty or Nice List
10.10.246.58/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3Dian%2520C
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Reverse Shell Cheat S...
The List
Admin
Welcome children!
To find out if you are currently on the naughty list or the nice list, please enter your name below!
Have a Merry Christmas! Ho ho ho!
- Santa
Name:
Search
Ian Chai is on the Nice List.


Applications Places System
Sun 17 Jul, 08:24
AttackBox IP:10.10.237.13
The Naughty or Nice List - Mozilla Firefox
The Naughty or Nice List
10.10.246.58/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DTib3rius
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Reverse Shell Cheat S...
The List
Admin
Welcome children!
To find out if you are currently on the naughty list or the nice list, please enter your name below!
Have a Merry Christmas! Ho ho ho!
- Santa
Name:
Search
Tib3rius is on the Nice List.



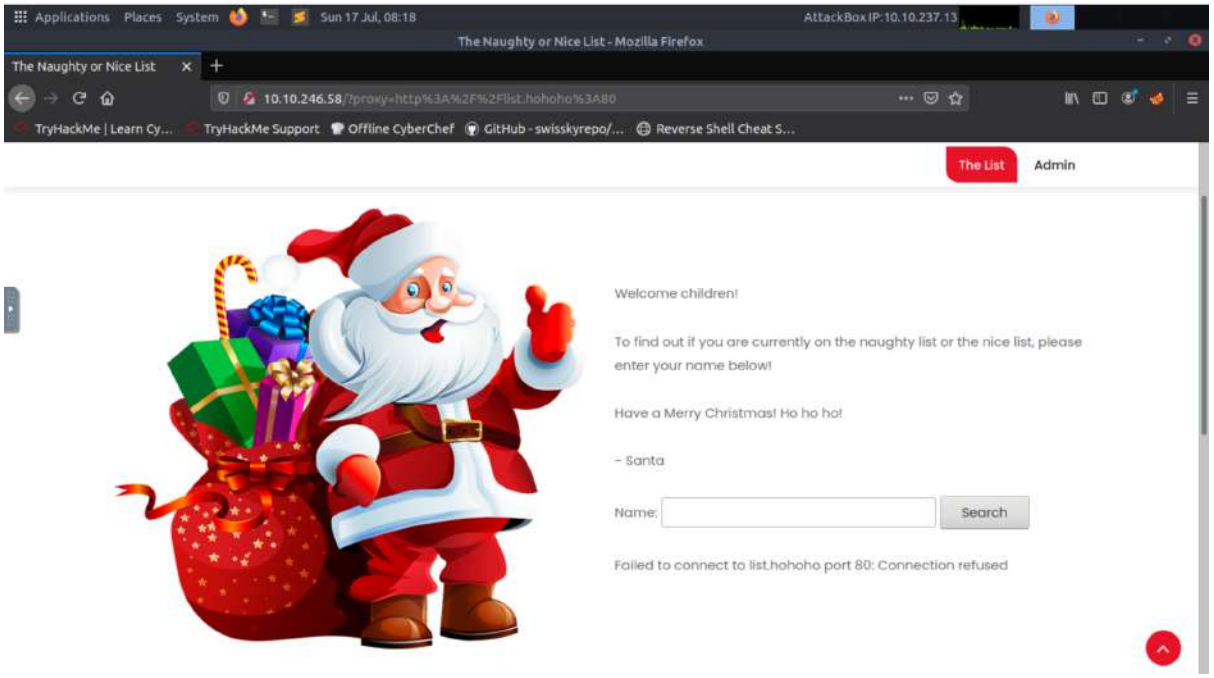
Question 2

Using the same IP address, browse to /?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F . A message will appear.



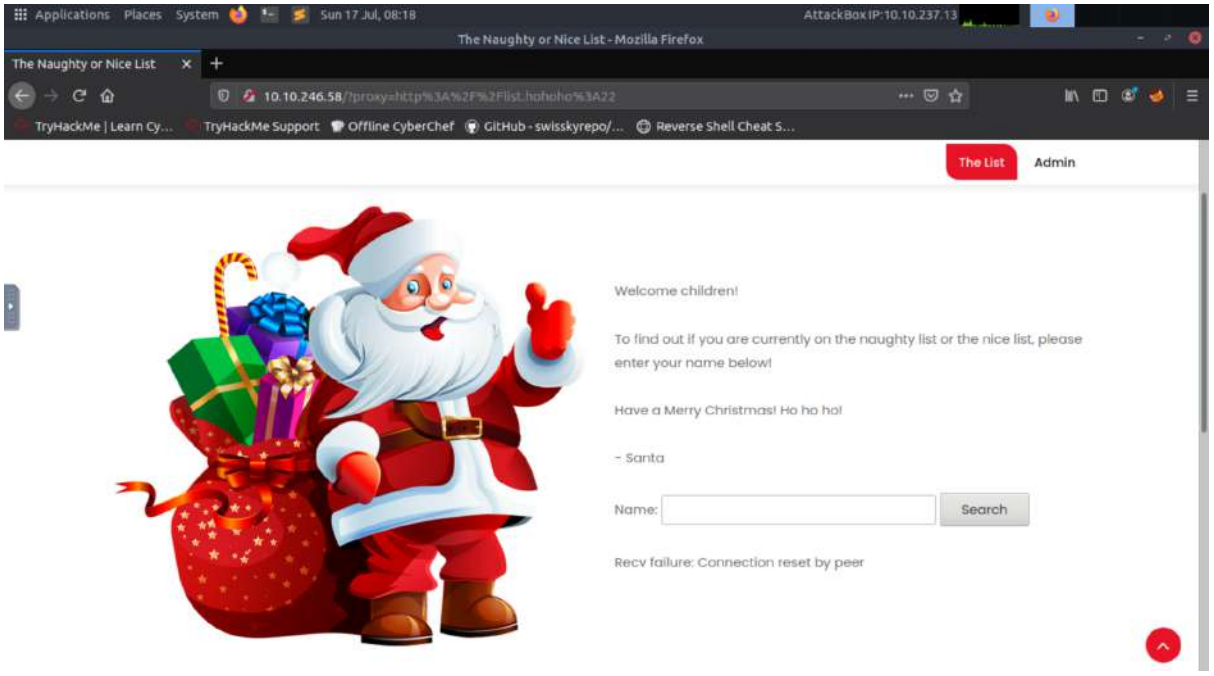
Question 3

Using the same IP address, browse to /?proxy=http%3A%2F%2Flist.hohoho%3A80 and copy the message returned.



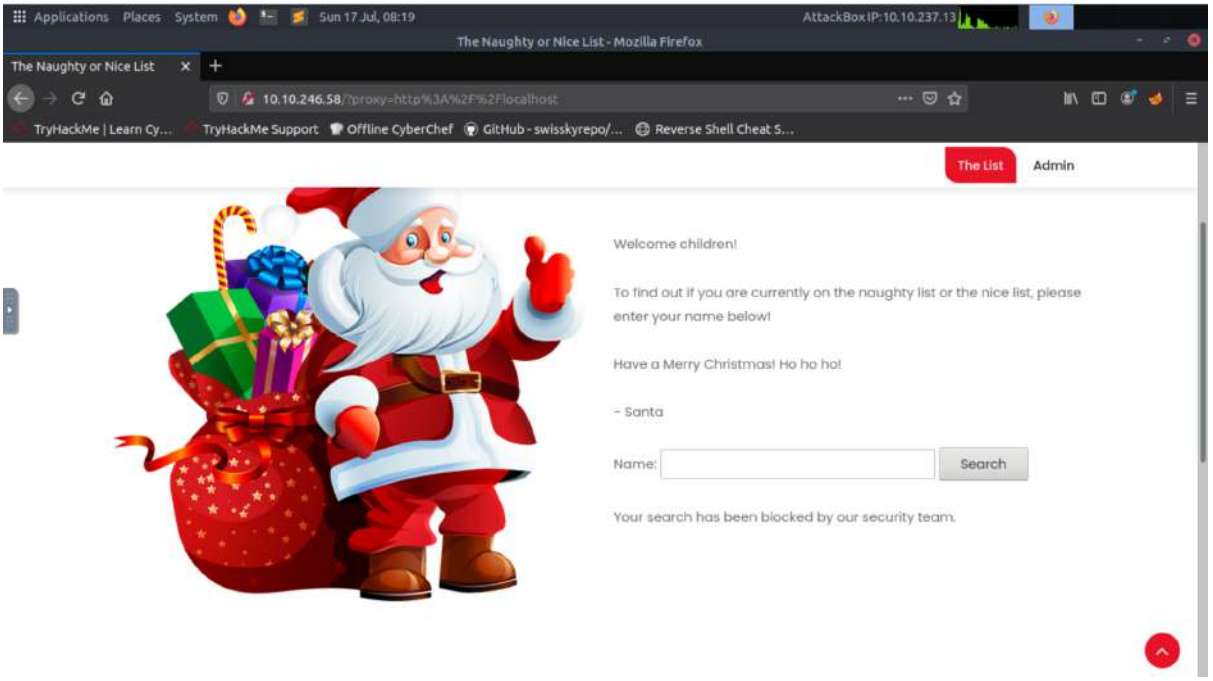
Question 4

Still on the same IP address, browse to /?proxy=http%3A%2F%2Flist.hohoho%3A22 instead.



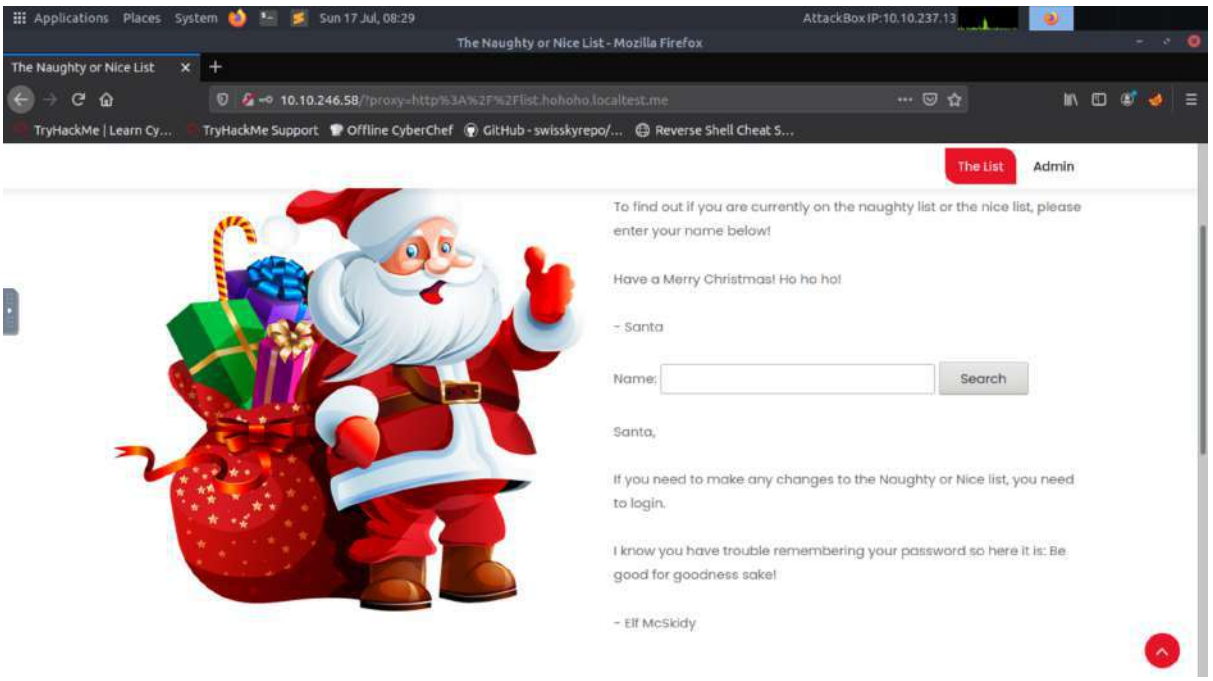
Question 5

Again, on the same IP address, browse to /?proxy=http%3A%2F%2Flocalhost .



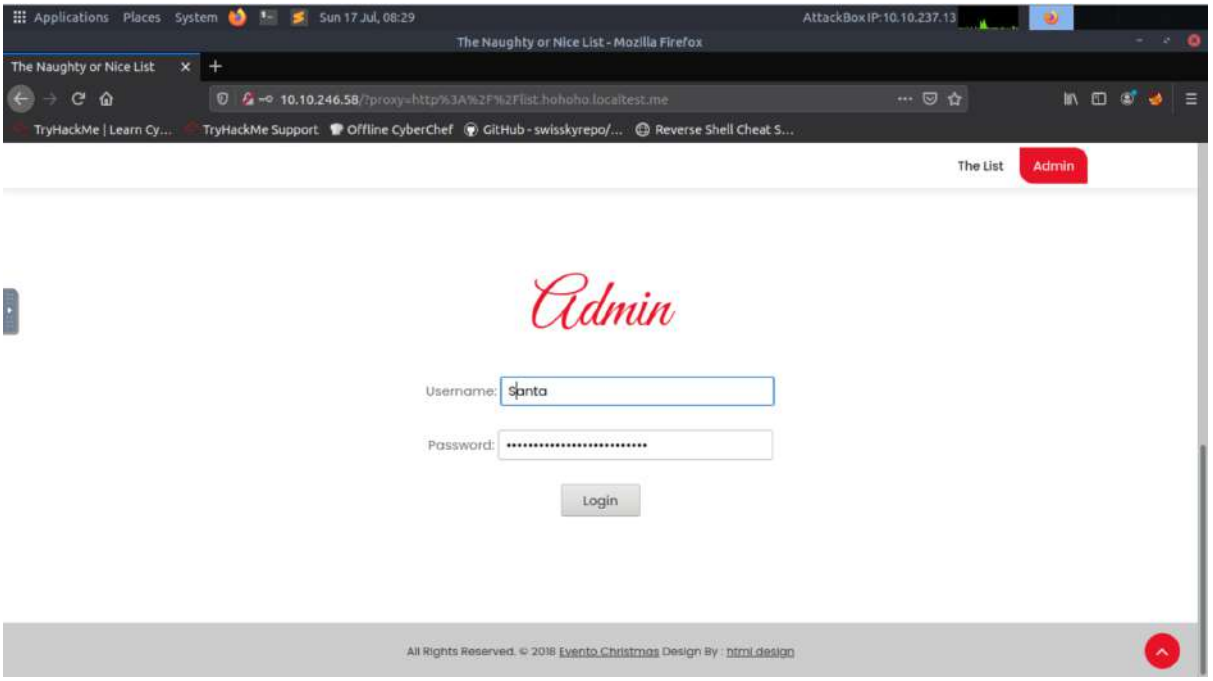
Question 6

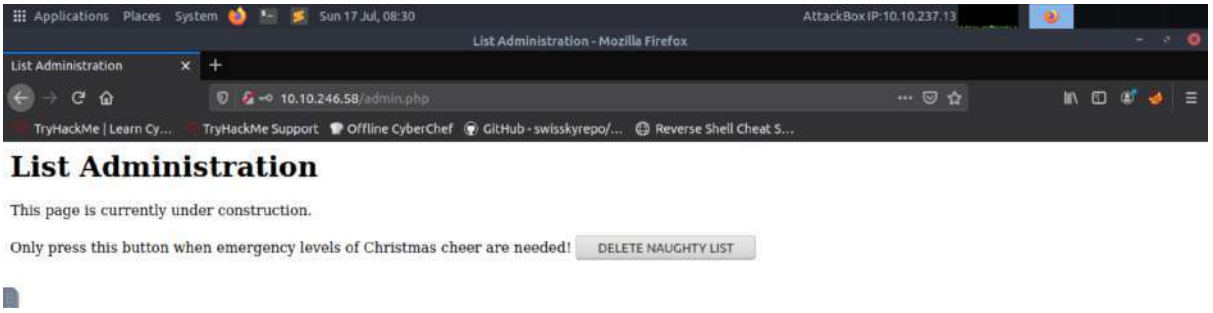
By changing the hostname in the URL to “list.hohoho.localtest.me” we can access local services. On the same IP address, browse to /?proxy=http%3A%2F%2Flist.hohoho.localtest.me . The feedback contains the password needed.

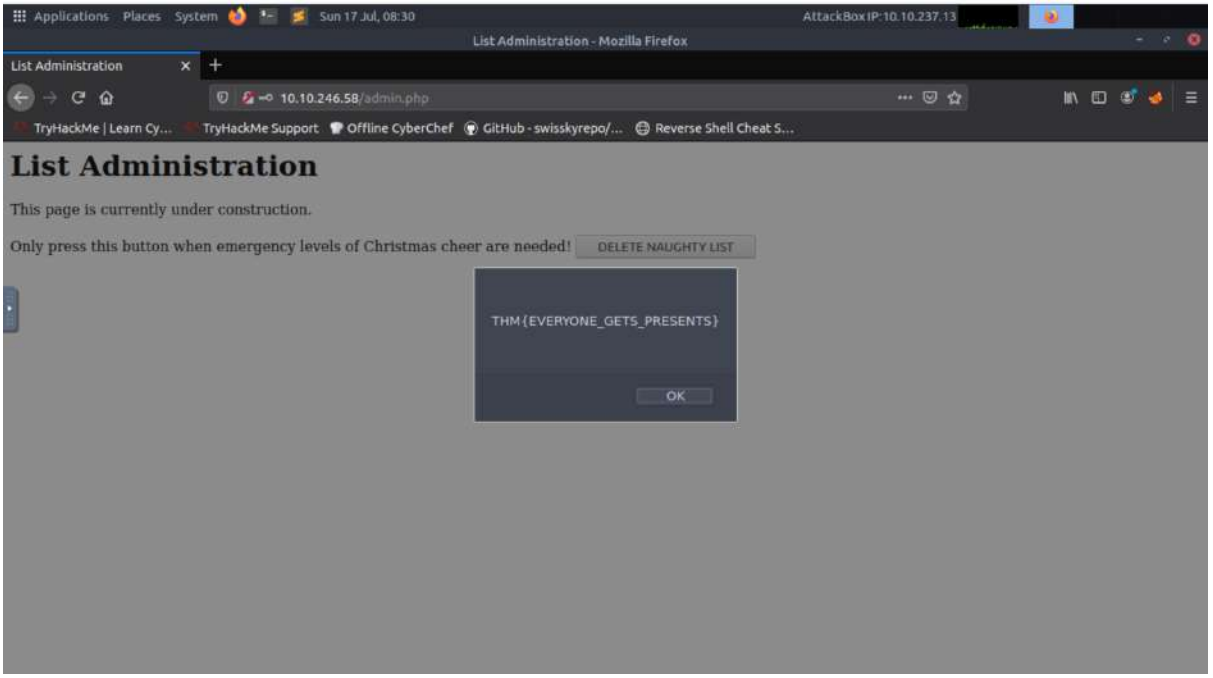


Question 7

Once we have the password, login to Santa's account to access the admin privileges. After we've managed to login, we can delete the naughty list and receive the flag for the challenge.







Methodology/Thought Process:

Open the website we want to exploit on a browser using the IP address provided by TryHackMe. On the home page, there's a name search box to see if a name is on the naughty or nice list. Check each name given to see if they are on the naughty or nice list. Then, we can try finding valid URLs for the site. On the same IP address, we tried browsing to **/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F** , **/?proxy=http%3A%2F%2Flist.hohoho%3A80 ,** and **/?proxy=http%3A%2F%2Flocalhost** to see if we can run them on the host. After trying these URLs, we noticed that the hostname needs to start with "list.hohoho" to bypass the check. By using **/?proxy=http%3A%2F%2Flist.hohoho.localtest.me** we were able to access local services and obtain the password to Santa's account. After obtaining Santa's password, we managed to login to Santa's account and access admin privileges such as deleting the naughty list. This way, we could obtain the flag for the challenge.

DAY20 : [BLUE TEAMING] PowershELIF to the rescue

Tools uses: Kali Linux

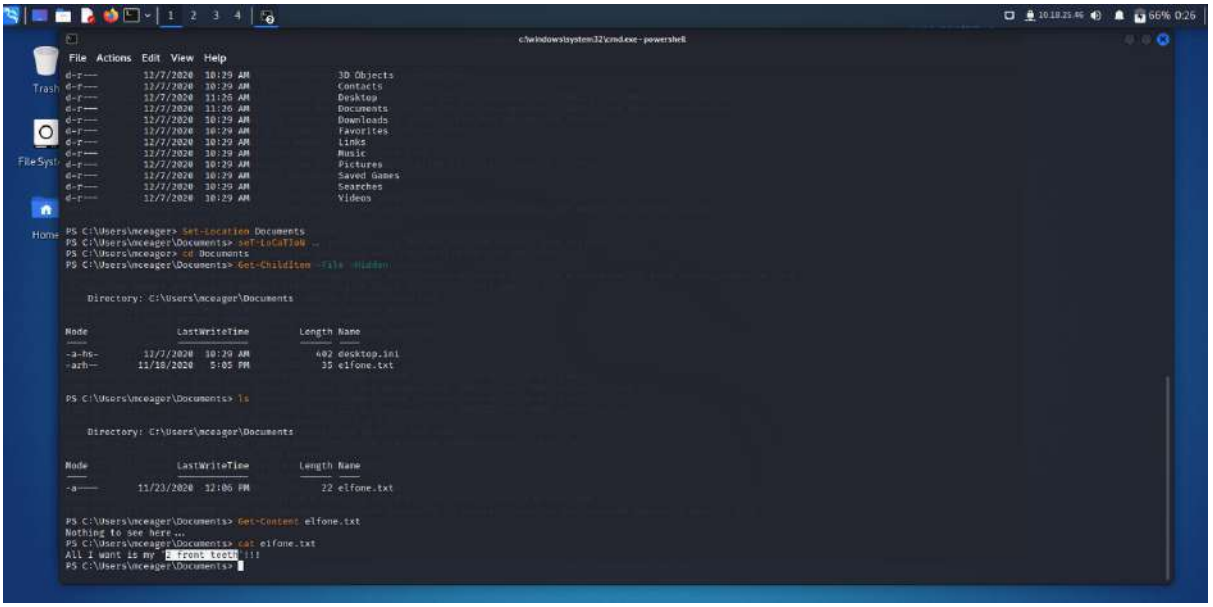
Question 1

At ssh manual, Parameter -l do:

debug_ssh	Specifies whether the legacy SSH client writes debug information into the `agent/logs/ssh.log` log file. This log file can get very large and should be reviewed frequently. The ServiceNow SSH client does not use this parameter.

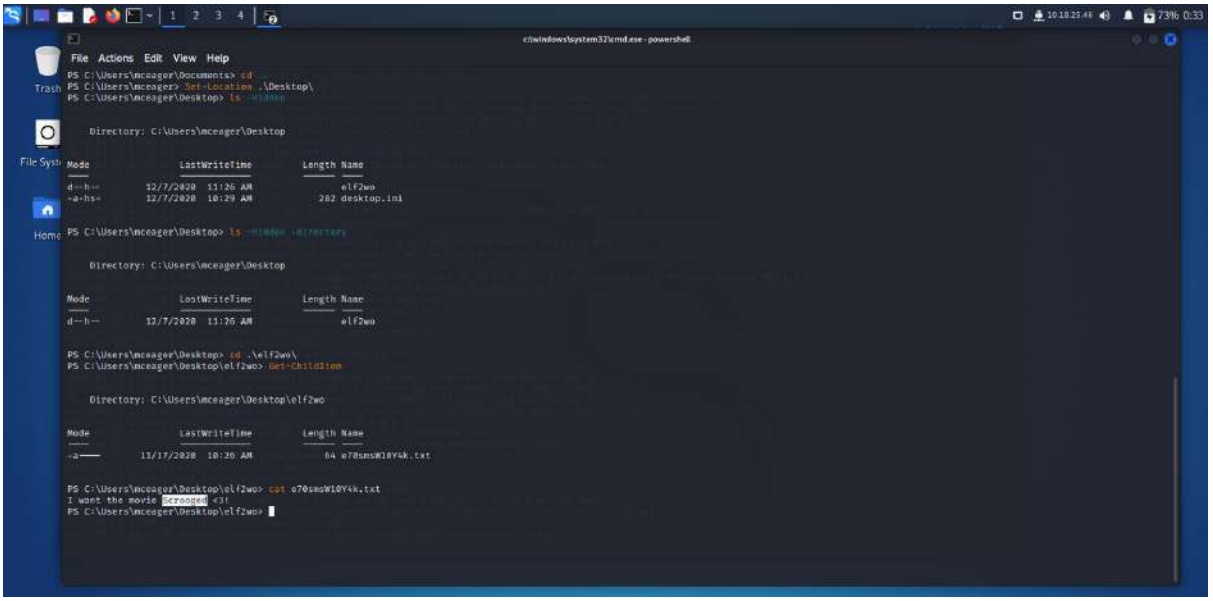
Question 2

Open terminal. Command SSH mceager and enter the password given. Enter the document and command **cat e1fone.txt**.



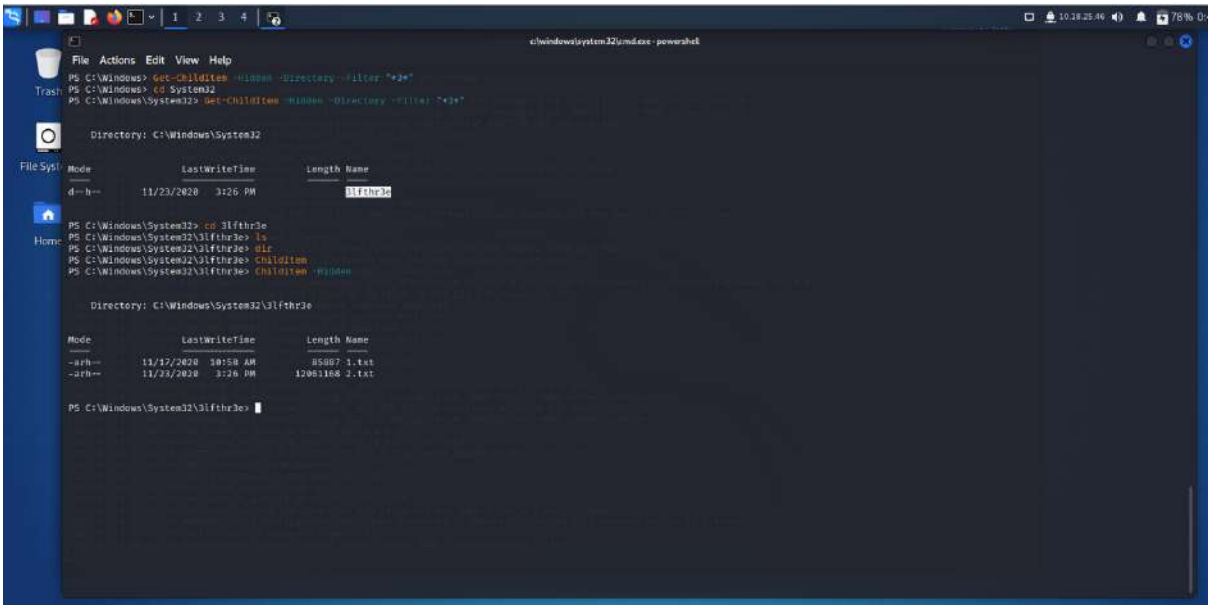
Question 3

Next, go to the desktop and enter the hidden elfwo directory. Command **cat e70smsW10Y4k.txt** at Get-ChildItem.



Question 4

Command **System32** and **Get-ChildItem -Hidden -Directory -Filter "*3*"** at the terminal.



Question 5

At 3lfthr3e file, command Get-Content 1.txt | Measure-Object from the first file.

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

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


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

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

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

Question 6

Command **(Get-Content 1.txt)[551,6991]** at 3lfthr3e file form file 1 .

```
c:\windows\system32\cmd.exe - powershell
File  Actions  Edit  View  Help
hugo
wagner
constraint
groundwater
touched
strengthening
cologne
grip
wishing
ranger
smallest
insulation
newman
marsh
ricky
ctrl
scared
theta
infringement
bent
laos
subjective
monitors
asylum
lightbox
robbie
stake
cocktail
outlets
swaziland
varieties
arbor
mediawiki
configurations
poison
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[551]
Red
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[551,6991]
Red
Ryder
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[6991]
Ryder
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Select-Object -Index 551
Red
PS C:\Windows\System32\3lfthr3e>
```

Question 7

Command **Get-Content 2.txt | Select-String -Pattern “redryder”** at file 2.

Methodology/Thought Process:

Firstly, access the machine with open VPN. Next, we opened the terminal. SSH mceager was command and entered the password given. We entered the document and command **cat e1fone.txt**. Go to the desktop and enter the hidden elfwo directory. **cat e70smsW10Y4k.txt** was command at Get-ChildItem. Command **System32** and **Get-ChildItem -Hidden -Directory -Filter "*3*"** at the terminal. At 3lfthr3e file, we command Get-Content 1.txt | Measure-Object from the first file. Moving on to the next step, we command **(Get-Content 1.txt)[551,6991]** at 3lfthr3e file form file 1. Lastly, Command **Get-Content 2.txt | Select-String -Pattern "redryder"** at file 2 to get the final answer.