

PSP0201

Week 5

Writeup

Group Name: Stellar

Members

ID	Name	Role
1211101145	Nurul Humairah binti Mohamad Kamaruddin	Leader
1211101216	Fatin Qistina binti Kamarul Irman	Member
1211102030	Ilyana Sofiya binti Muhammad Najeli	Member
1211103480	Nurul Afiqah binti Ismail	Member

Day 16: Scripting – Help! Where is Santa?

Tools used: Kali Linux, Firefox, Python

Solution/walkthrough:

Question 1

The port number for the web server is **80**.

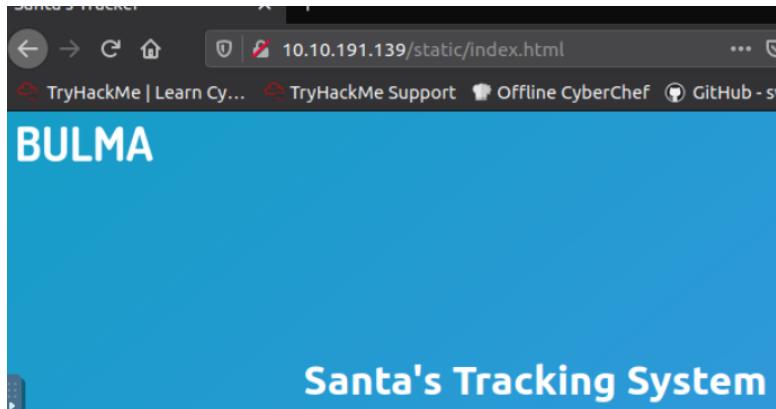
```
root@ip-10-10-51-244: ~
File Edit View Search Terminal Help
root@ip-10-10-51-244:~# nmap 10.10.68.126

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-13 09:42 BST
Nmap scan report for ip-10-10-68-126.eu-west-1.compute.internal (10.10.68.126)
Host is up (0.00097s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:F1:66:F5:49:DF (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
root@ip-10-10-51-244:~#
```

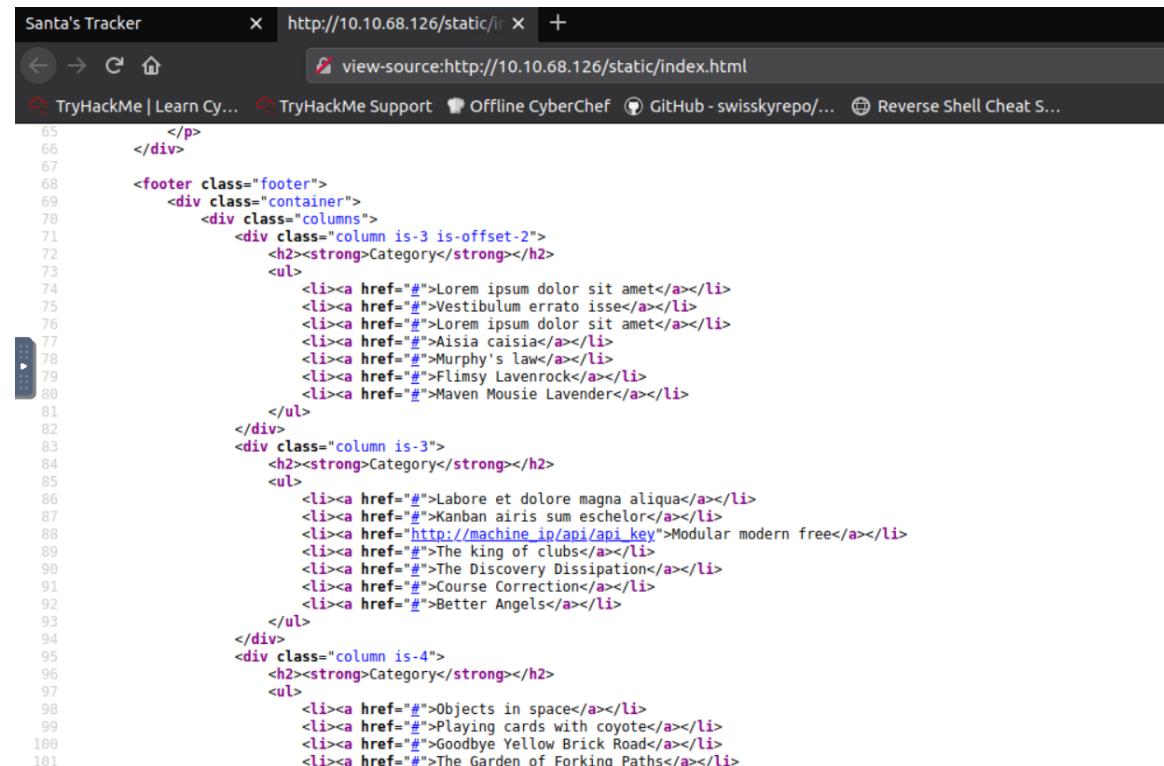
Question 2

The templates being used are **BULMA**.



Question 3

Without using enumerations tools such as Dirbuster, the directory for the API is `/api/`.

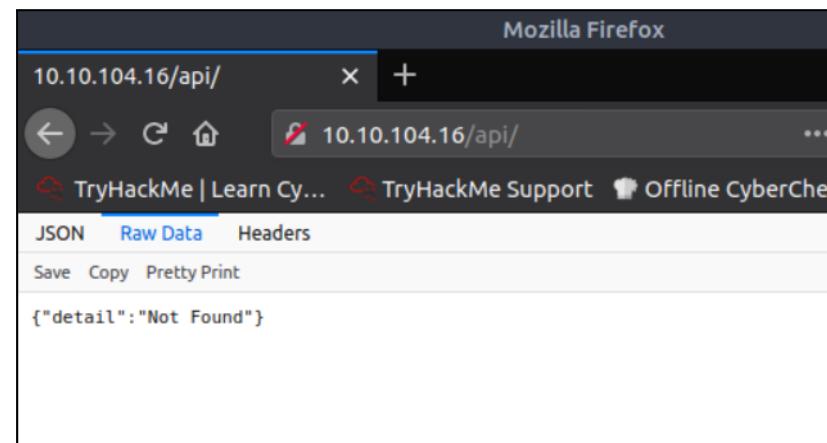


```
65      </p>
66      </div>
67
68  <footer class="footer">
69    <div class="container">
70      <div class="columns">
71        <div class="column is-3 is-offset-2">
72          <h2><strong>Category</strong></h2>
73          <ul>
74            <li><a href="#">Lorem ipsum dolor sit amet</a></li>
75            <li><a href="#">Vestibulum errato isse</a></li>
76            <li><a href="#">Lorem ipsum dolor sit amet</a></li>
77            <li><a href="#">Alisia caisia</a></li>
78            <li><a href="#">Murphy's law</a></li>
79            <li><a href="#">Flimsy Lavenrock</a></li>
80            <li><a href="#">Maven Mousie Lavender</a></li>
81          </ul>
82        </div>
83        <div class="column is-3">
84          <h2><strong>Category</strong></h2>
85          <ul>
86            <li><a href="#">Labore et dolore magna aliqua</a></li>
87            <li><a href="#">Kanban airis sum eschelor</a></li>
88            <li><a href="http://machine_ip/api/api_key">Modular modern free</a></li>
89            <li><a href="#">The king of clubs</a></li>
90            <li><a href="#">The Discovery Dissipation</a></li>
91            <li><a href="#">Course Correction</a></li>
92            <li><a href="#">Better Angels</a></li>
93          </ul>
94        </div>
95        <div class="column is-4">
96          <h2><strong>Category</strong></h2>
97          <ul>
98            <li><a href="#">Objects in space</a></li>
99            <li><a href="#">Playing cards with coyote</a></li>
100           <li><a href="#">Goodbye Yellow Brick Road</a></li>
101           <li><a href="#">The Garden of Forking Paths</a></li>
102         </ul>
103       </div>
104     </div>
105   </div>
106 
```

"#">>Labore et dolore magna aliqua
"#">>Kanban airis sum eschelor
"http://machine_ip/api/api_key">Modular modern free
"#">>The king of clubs
"#">>The Discovery Dissipation
"#">>Course Correction
"#">>Better Angels

Question 4

The Raw Data that was returned if no parameters are entered are `{"detail": "Not Found"}`.



```
10.10.104.16/api/
```

Mozilla Firefox

10.10.104.16/api/

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef

JSON Raw Data Headers

Save Copy Pretty Print

```
{"detail": "Not Found"}
```

Question 5

Right now, Santa is at Winter Wonderland, Hyde Park and London.

```
root@ip-10-10-51-244:~# nano apibruter.py
root@ip-10-10-51-244:~# python3 apibruter.py
{"item_id":1,"q":"Error. Key not valid!"}
root@ip-10-10-51-244:~#
```

```
root@ip-10-10-51-244:~#
File Edit View Search Terminal Help
GNU nano 2.9.3 apibruter.py
#!/usr/bin/env python3

import requests

api_key = 1
html = requests.get(f'http://10.10.68.126:80/api/{api_key}')
print(html.text)
```

```
root@ip-10-10-51-244:~#
File Edit View Search Terminal Help
GNU nano 2.9.3 apibruter.py Modified
#!/usr/bin/env python3

import requests

for api_key in range(1,100,2):
    print(f'api_key {api_key}')
    html = requests.get(f'http://10.10.68.126:80/api/{api_key}')
    print(html.text)
```

```
root@ip-10-10-51-244:~# python3 apibruter.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!"}
```

```
{"item_id":51,"q":"Error. Key not valid!"}
api_key 53
{"item_id":53,"q":"Error. Key not valid!"}
api_key 55
{"item_id":55,"q":"Error. Key not valid!"}
api_key 57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
api_key 59
{"item_id":59,"q":"Error. Key not valid!"}
api_key 61
{"item_id":61,"q":"Error. Key not valid!"}
api_key 63
{"item_id":63,"q":"Error. Key not valid!"}
```

Question 6

The correct API key is **57**.

```
{"item_id":51,"q":"Error. Key not valid!"}
api_key 53
{"item_id":53,"q":"Error. Key not valid!"}
api_key 55
{"item_id":55,"q":"Error. Key not valid!"}
api_key 57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
api_key 59
{"item_id":59,"q":"Error. Key not valid!"}
api_key 61
{"item_id":61,"q":"Error. Key not valid!"}
api_key 63
{"item_id":63,"q":"Error. Key not valid!"}
```

Thought Process/Methodology:

First, question 1 asks for the port number we should use. As we learn before an easy way to scan the IP address to obtain the port number is by using Nmap. We'll need to write nmap Machine_ip. It will show which port numbers are available and which one we can use. According to the scan results, we need to use port 80 as it is open and not secured. Next is question 2, which wants to know what templates are being used on the website. We can see the answers on the left side of the website which is BULMA. Question 3, asks for the API directory. So, just go to the website, right-click, and chose the view page source. As it says on the website, there are a lot of hidden links on the website and we need to find a different link from the others. Later we'll be able to see the links which are http://machine_ip/api/api_key and as we can see here the directory for the API should be /api/. Moving on, question 4 wants to know the Raw Data that was returned if no parameters are entered. We can simply use the links that we've found earlier by inserting our machine IP address and deleting the api_key part. Search in firefox using the links that we've modified earlier, click on the Raw Data tab and we've found the answer which is {"detail": "Not Found"}. Question 5 then ask for the Santa locations right now while question 6 wants to know the correct API key. To solve both of these questions, we'll be applying the python knowledge we've learned before. Now, open a text editor such as nano in the terminal, and create a new file with python extension. Now, type import requests which is the library we need to download from day 15. We'll need to use loops to brute force into the website by trying all numbers from 1 to 100 that is odd numbers. Using for loops, set the range (1,100,2), and for every API key, we'll make it print the API key so that we know which one is successful. Also, do a get request for the link that was given in the task and print the results. Lastly, we need to type python3 file_name.py in the terminal and we'll see a list of attempts starting from number 1 and most of them will say that the key is not valid which means that was not the API key we wanted. Scroll until we found an API key that results in a successful attempt which is number 57. It will say where is Santa right now and in this case, Santa is at Winter Wonderland, Hyde Park, and London.

Day 17: Reverse Engineering – ReverseELFneering

Tools used: Terminal Emulator

Solution/walkthrough:

Question 1

Match the data type with the size in bytes:

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 command to analyse the program in radare2 is **aa**.

```
[0x00400a30]> aa
[ WARNING : block size exceeding max block size at 0x006ba220
[+] Try changing it with e anal.bb.maxsize
WARNING : block size exceeding max block size at 0x006bc860
[+] Try changing it with e anal.bb.maxsize
[x] Analyze all flags starting with sym. and entry0 (aa)
```

Question 3

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

```
0x7ffd92660fac 0000 0000 0000 0000 0000 0000 0000 0000 ..... .
[0x00400b5f]> ds
[0x00400b5f]> db 0x00400b69
[0x00400b5f]> pdf @ main
;-- main:
;-- main:          sym.main
/_ (fcn) sym.main 35
| sym.main ();
| ; var int local_ch @ rbp-0xc    switch to main_get_area
| ; var int local_8h @ rbp-0x8   get_d1_main_map
| ; var int local_4h @ rbp-0x4   switch to main_wget_area
| ; DATA XREF from 0x00400a4d (entry0)
| 0x00400b4d 55 push rbp
| 0x00400b4e 489e5 mov rbp, rsp
| 0x00400b51 c745f4010000. mov dword [local_ch], 1
| 0x00400b58 4845f4 mov dword [local_8h], 6
| 0x00400b5f b 8b45f4 mov eax, dword [local_8h]
| 0x00400b62 0faf45f8 imul eax, dword [local_8h]
| 0x00400b66 8945fc mov dword [local_4h], eax
As seen here, we can see that the value of local_ch is 1. Let's verify this by running the command
;-- rip;where pdf means print disassembly function. Doing so will give us the following
command: ;-- rip;where pdf means print disassembly function. Doing so will give us the following
view: 0x00400b69 b b800000000 Let's see what happens when we run this command
;-- rip;where pdf means print disassembly function. Doing so will give us the following
view: 0x00400b6c 5d pop rbp
\ 0x00400b6f c3 ret
```

Question 4

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

```
[0x00400a30]> dc
hit breakpoint at: 400b5f
```

Question 5

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

```
| 0x00400b4e 489e5 mov rbp, rsp
| 0x00400b51 c745f4010000. mov dword [local_ch], 1
| 0x00400b58 c745f8060000. mov dword [local_8h], 6
```


Thought Process/Methodology:

Firstly, we did SSH into the terminal with the username elfmceager and the password adventofcyber. We used radare2 to enter debug mode to learn more about the file. We did this using r2 -d ./challenge1. When we were inside debug mode, we did a full analysis of the file using the aa command. Next we search for main that most executable programs have an entry point. We did this using the alf command and then filtered the results with grep. The final command will be alf | grep main. We took a closer look at it using the print disassembly function(pdf). The command will be pdf @ main. Then we can see there were the Assembly instructions for the main function. Next, we need to find the value of local_ch when its corresponding movl instruction. We used db to put a breakpoint at address 0x00400b5f so the command will become db 0x00400b5f. Then we ran pdf @ main again to see the breakpoint set correctly. Next, we ran the program using dc and we received a message that we had stopped at the breakpoint set. Then, we analyse the contents of local_ch with the command px @ rbp-0xc. The value we saw is 1. Next, to find the value of eax at the first imul instruction, we used ds to move the next line and then used dr to see the value of eax. We saw that the value is 6. Lastly, to find the value of local_4h before the eax is set to 0, we used ds again to move the next line and then we ran px @ rbp-0x4. The value we saw is 6.

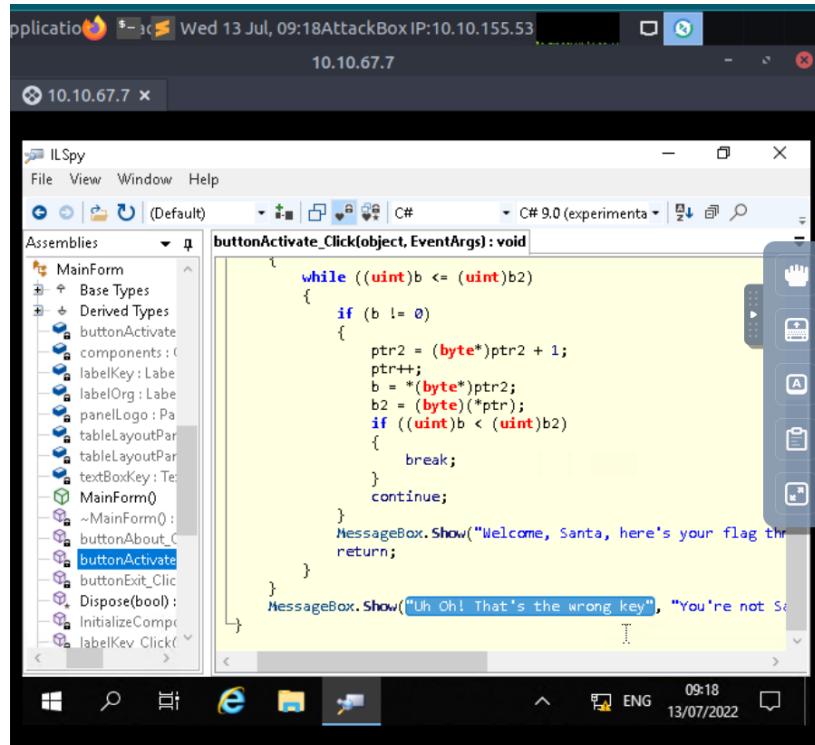
Day 18: Reverse Engineering – The Bits of Christmas

Tools used: Kali Linux, Firefox, ILSpy, Remmina

Solution/walkthrough:

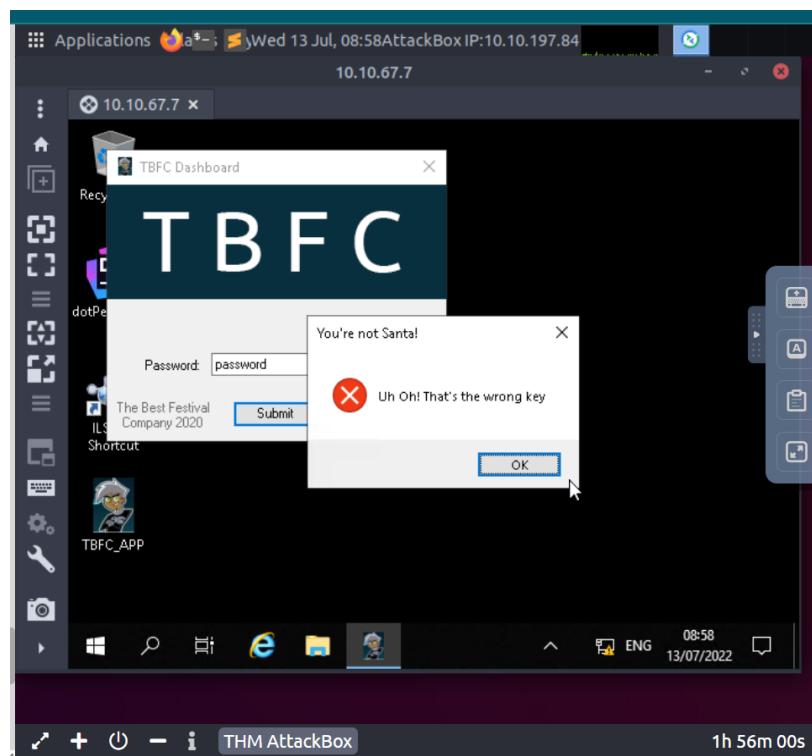
Question 1

The message that shows up if we enter the wrong password for TBFC_APP is **Uh Oh! That's the wrong key .**



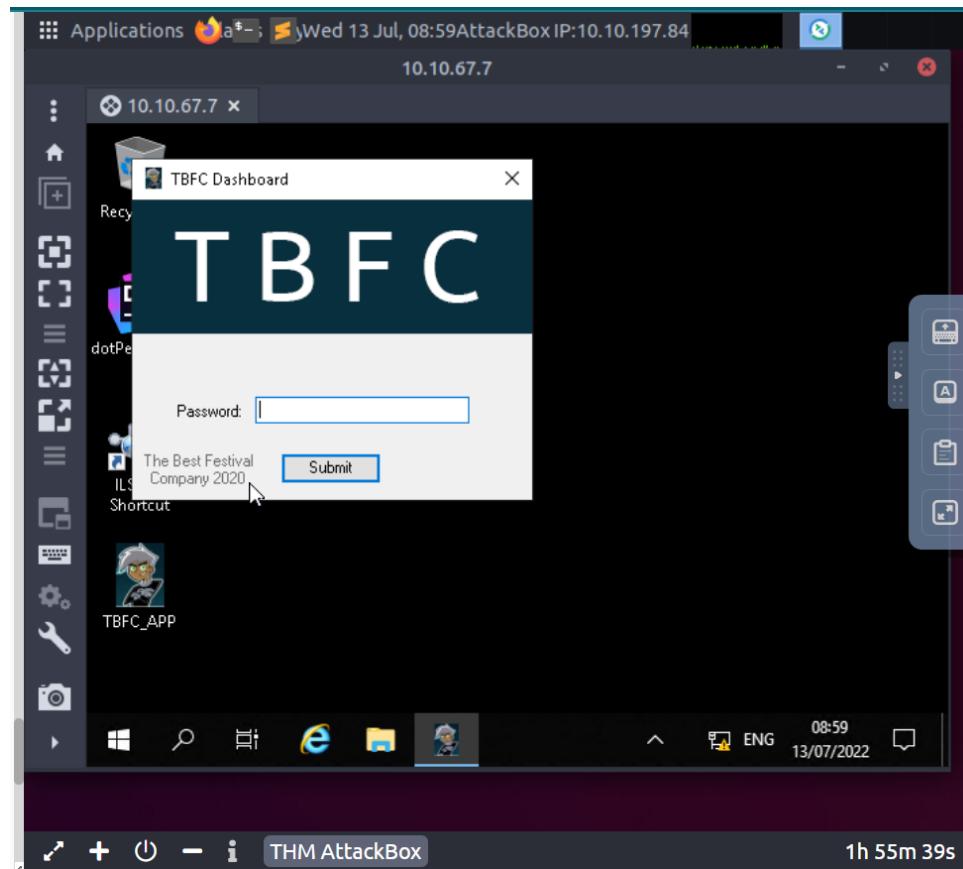
ILSpy window showing the C# code for the `buttonActivate_Click` method. The code reads bytes from memory starting at `ptr2` until it finds a match for `b2`. If no match is found, it displays an error message.

```
buttonActivate_Click(object, EventArgs) : void
{
    while ((uint)b <= (uint)b2)
    {
        if (b != 0)
        {
            ptr2 = (byte*)ptr2 + 1;
            ptr++;
            b = *(byte*)ptr;
            b2 = (byte)(*ptr);
            if ((uint)b < (uint)b2)
            {
                break;
            }
            continue;
        }
        MessageBox.Show("Welcome, Santa, here's your flag the");
        return;
    }
    MessageBox.Show("Uh Oh! That's the wrong key", "You're not Santa!");
}
```



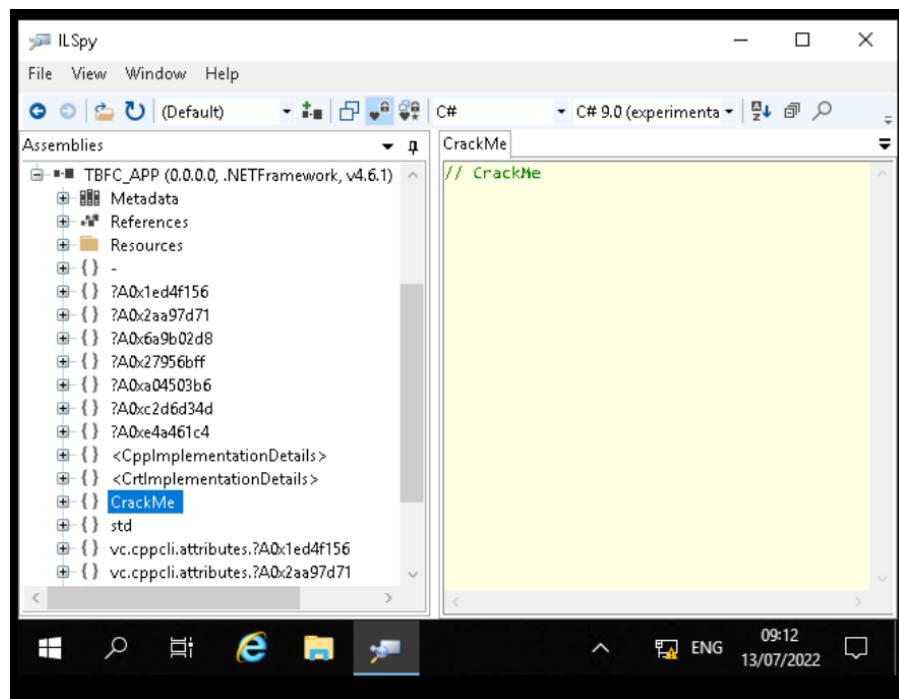
Question 2

TBFC stands for **The Best Festival Company**.



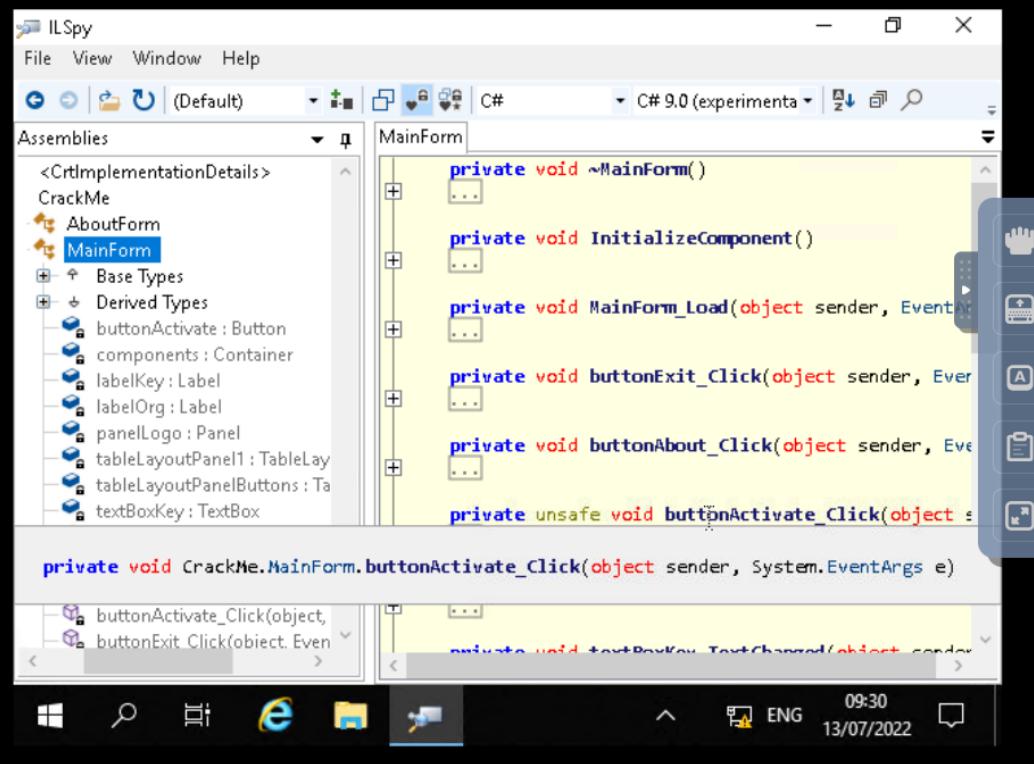
Question 3

Decompile the TBFC_APP with ILSpy. The module that catches our attention is **CrackMe**.



Question 4

Within the module, there are two forms. **MainForm** contains the information we are looking for.

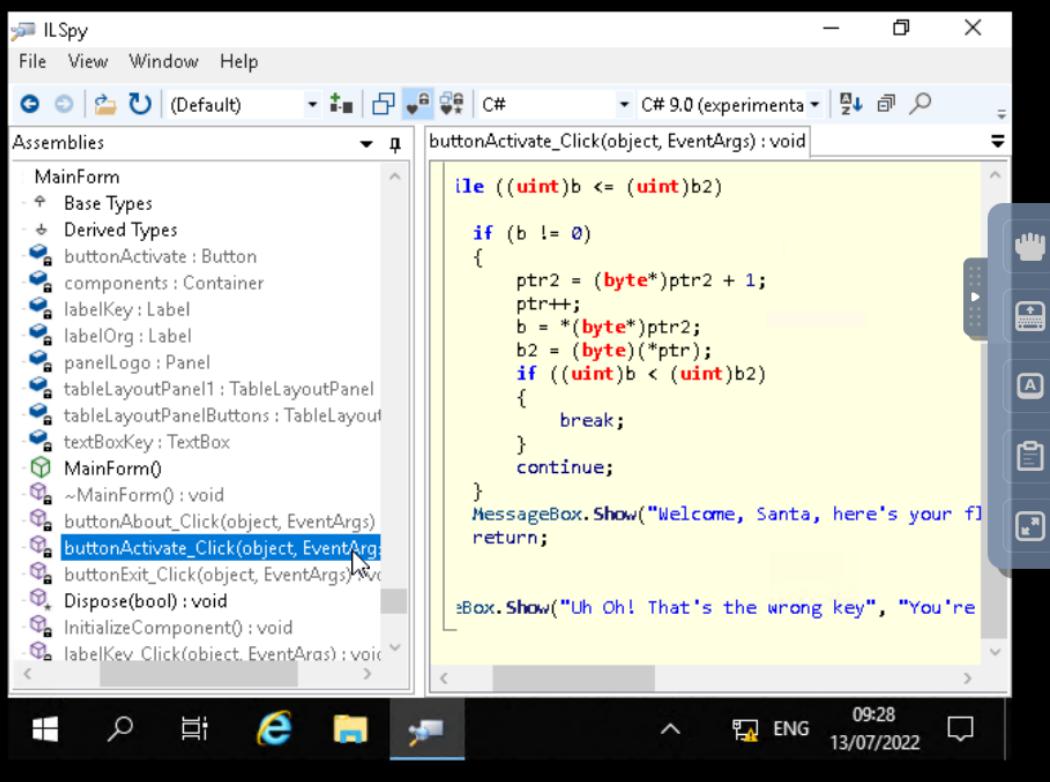


The screenshot shows the ILSpy interface. The left pane displays the assembly structure under 'CrackMe'. The 'MainForm' assembly is selected, showing its class hierarchy and member list. The right pane shows the decompiled C# code for the **MainForm** class. The code includes several event handlers and a method named **buttonActivate_Click**. A tooltip or context menu is visible over the **buttonActivate_Click** method, indicating it is the target of interest.

```
private void ~MainForm()
...
private void InitializeComponent()
...
private void MainForm_Load(object sender, EventArgs e)
...
private void buttonExit_Click(object sender, EventArgs e)
...
private void buttonAbout_Click(object sender, EventArgs e)
...
private unsafe void buttonActivate_Click(object sender, EventArgs e)
...
private void CrackMe.MainForm.buttonActivate_Click(object sender, System.EventArgs e)
...
private void buttonActivate_Click(object, EventArgs)
private void buttonExit_Click(object, EventArgs)
...
private void buttonAbout_Click(object, EventArgs)
private void buttonActivate_Click(object, EventArgs)
private void buttonExit_Click(object, EventArgs)
private void Dispose(bool)
private void InitializeComponent()
private void labelKey_Click(object, EventArgs)
```

Question 5

The form from Q4 will contain the information we are seeking is **buttonActivate_Click**.



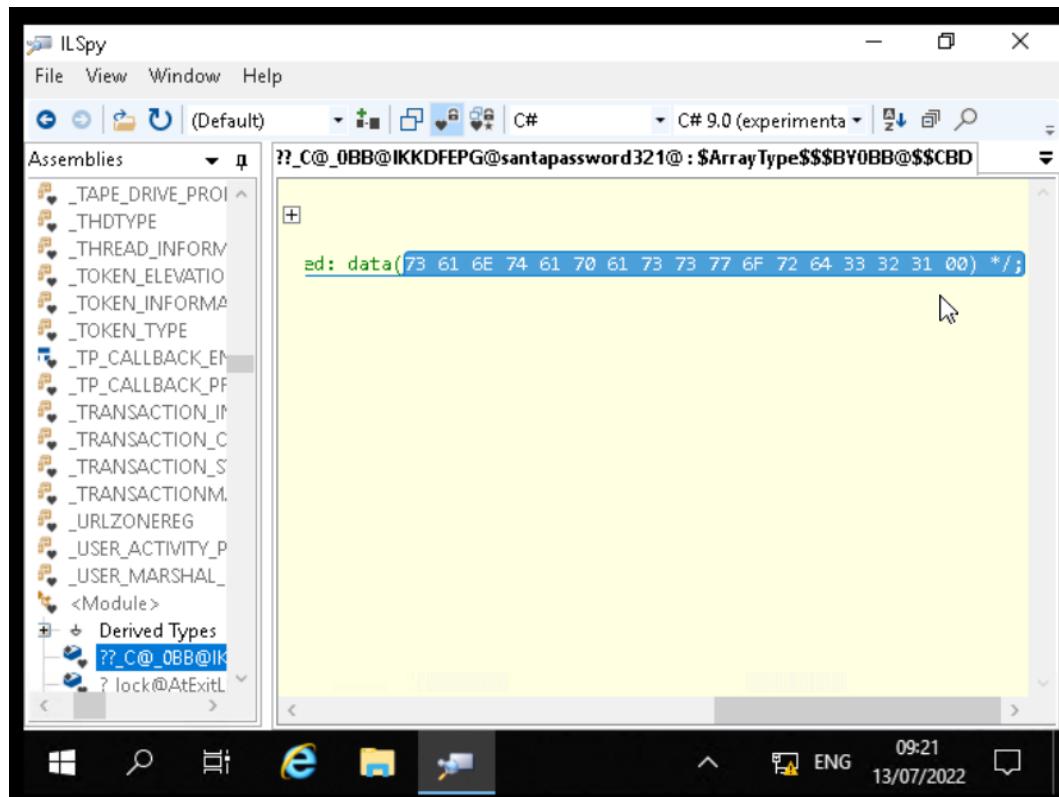
The screenshot shows the ILSpy interface with the **buttonActivate_Click** method highlighted in the code editor. The left pane shows the assembly structure, and the right pane displays the decompiled C# code for the **buttonActivate_Click** method. The code contains a loop that compares **b** and **b2**, and a message box is shown if the condition is met.

```
if ((uint)b <= (uint)b2)
{
    if (b != 0)
    {
        ptr2 = (byte*)ptr2 + 1;
        ptr++;
        b = *(byte*)ptr2;
        b2 = (byte)(*ptr);
        if ((uint)b < (uint)b2)
        {
            break;
        }
        continue;
    }
    MessageBox.Show("Welcome, Santa, here's your f");
    return;
}

MessageBox.Show("Uh Oh! That's the wrong key", "You're
```

Question 6

Santa's password is **santapassword321**.



From To

Hexadecimal Text

Paste hex numbers or drop file

```
73 61 6e 74 61 70 61 73 73 77 6f 72 64 33 32 31
```

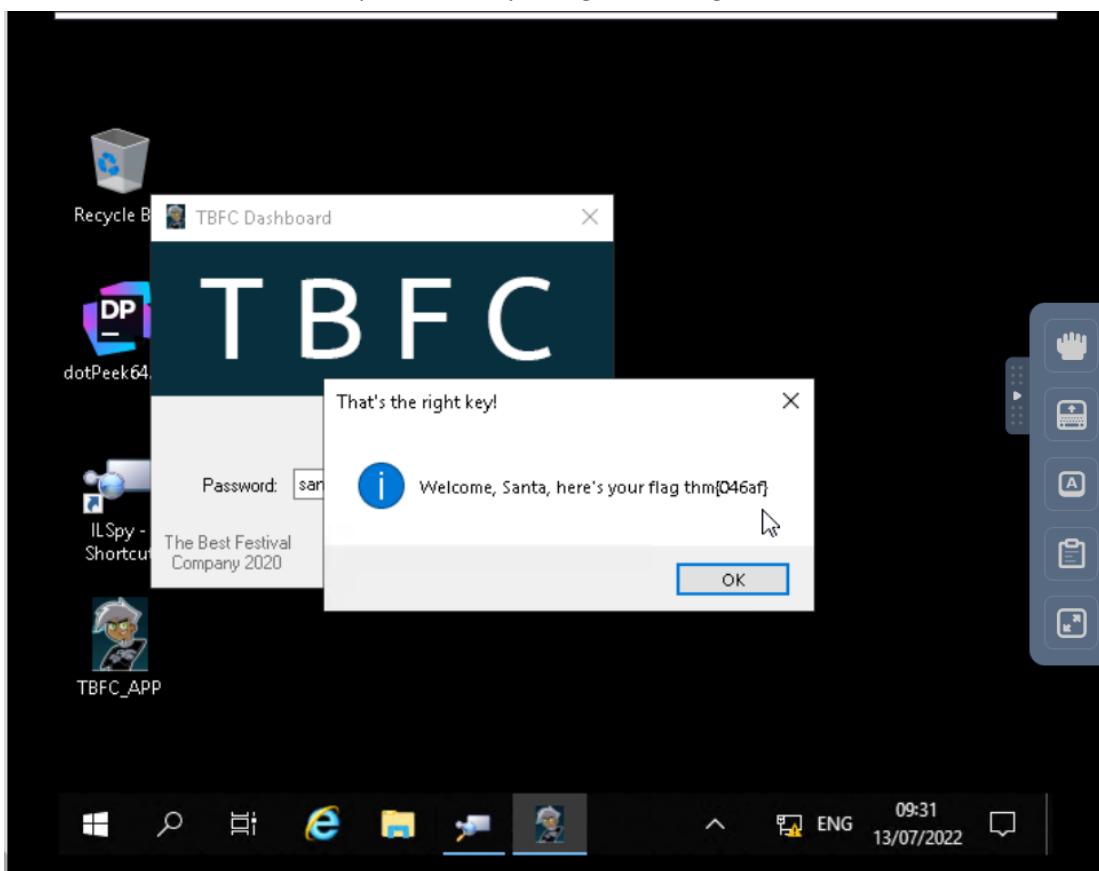
Character encoding

ASCII

santapassword321

Question 7

Now that we've retrieved this password, try to login. The flag is **thm{046af}** .



Thought Process/Methodology:

For Day 18, we opened up Remmina on the TryHackMe AttackBox and we connected to an IP address that has been given which is 10.10.67.7. After that, we key in the username and password for RDP authentication credentials and we are now connected. Then, we opened TBFC_APP and we saw TBFC which stands for The Best Festival Company 2020. On the side note, we opened ILSpy and had TBFC_APP loaded. Once we open it, we are asked to find Santa's password. After a bit of searching, there are components named 'CrackMe' which is a very weird name. We expand the thing, and inside it there is the MainForm() where the main function is. On the TBFC dashboard picture, the login mechanism is using a button to trigger the action and is also declared in the main function. After going through all the 'button' things, we arrived at 'buttonActivate_Click' and luckily the flag is hardcoded on the source code. In the same file, there is also Santa's password written on the code. After we click on that code, it displays the password that is formatted in hexadecimal. We use a converter to decode that. The password that we are expecting is santapassword123. Still on the same file, we can see the message that shows up if we enter the wrong password for TBFC_APP is Uh Oh! That's the wrong key. Now that we have retrieved the password, we try to login and the flag is revealed which is thm{046af}.

Day 19: Web Exploitation – The Naughty or Nice List

Tools used: Firefox, Sublime Text, Offline CyberChef

Solution/walkthrough:

Question 1

Which list is this person on?

Tib3rius - Nice



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:

Ian Chai is on the Nice List.

Ian Chai - Nice



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:

Ian Chai is on the Nice List.

YP - Nice



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.

Timothy - Naughty



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

Timothy is on the Naughty List.

Kanes - Naughty



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:

Kanes is on the Naughty List.

JJ - Naughty



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:

JJ is on the Naughty List.

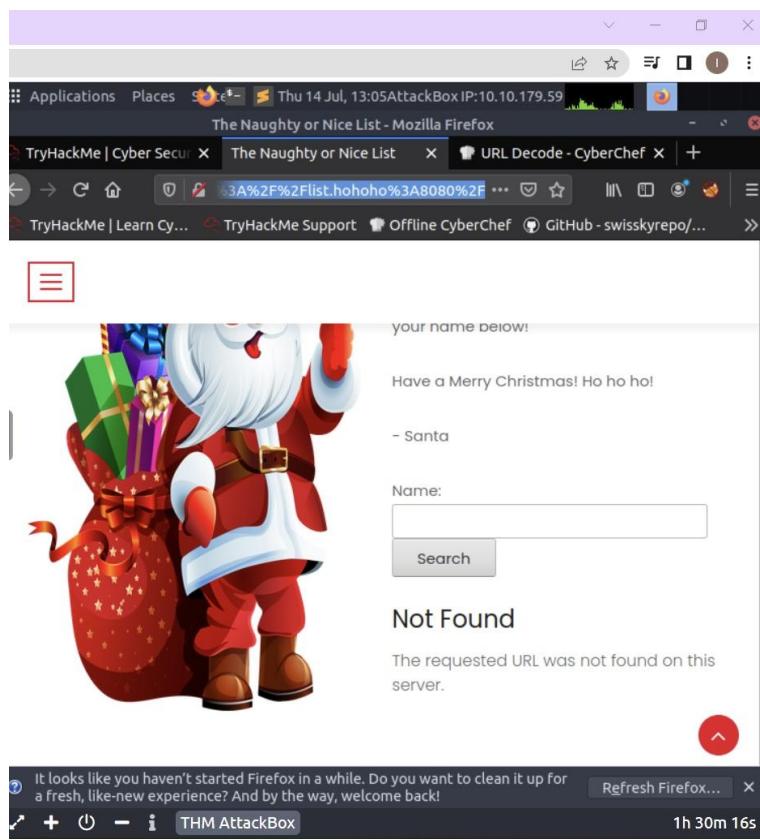
Question 2

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

Not Found. The requested URL was not found on this server.

The screenshot shows the CyberChef interface. In the Input field, the URL `http%3A%2F%2Flist.hohoho%3A8080%2F` is entered. The Output field shows the decoded result: `http://list.hohoho:8080/search.php?name=Ilyana`. The Firefox status bar at the bottom indicates "1h 50m 22s".

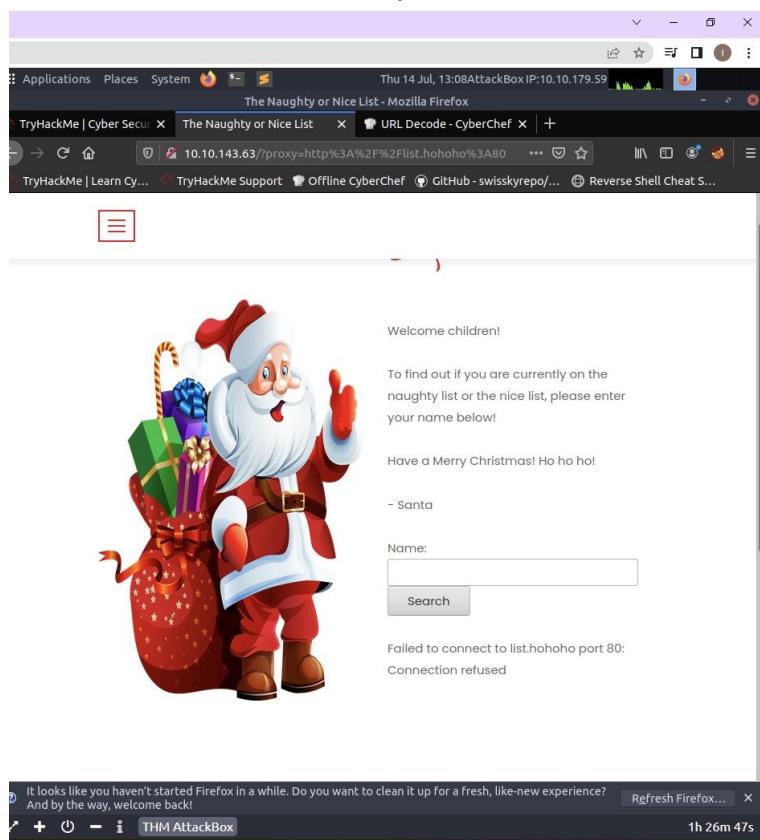
The screenshot also shows a terminal window with the command `http://10.10.143.63/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F` and the output `1 http://10.10.143.63/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fse 2 arch.php?name=Ilyana 3 http://list.hohoho:8080/search.php?name=Ilyana`.



Question 3

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

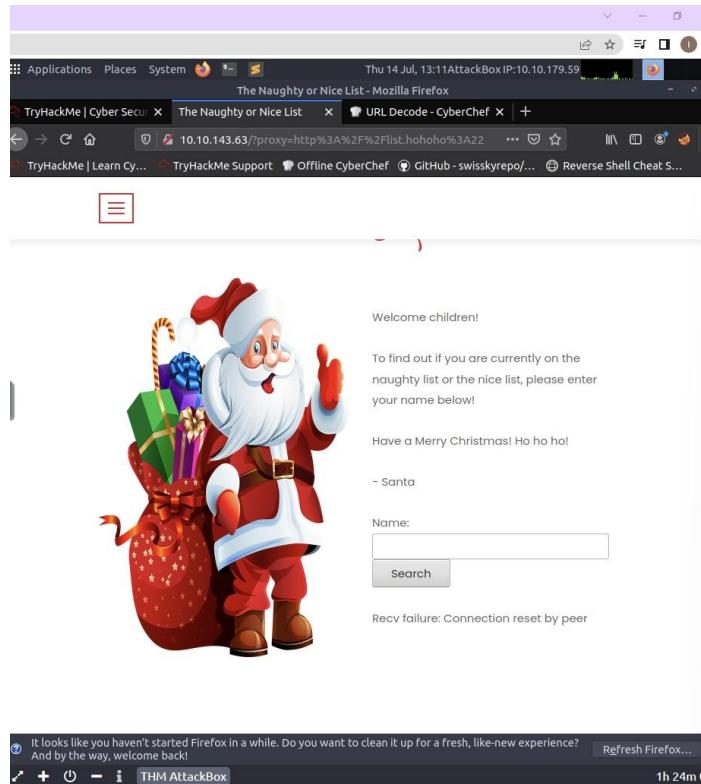
Failed to connect to list.hohoho port 80: Connection refused



Question 4

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

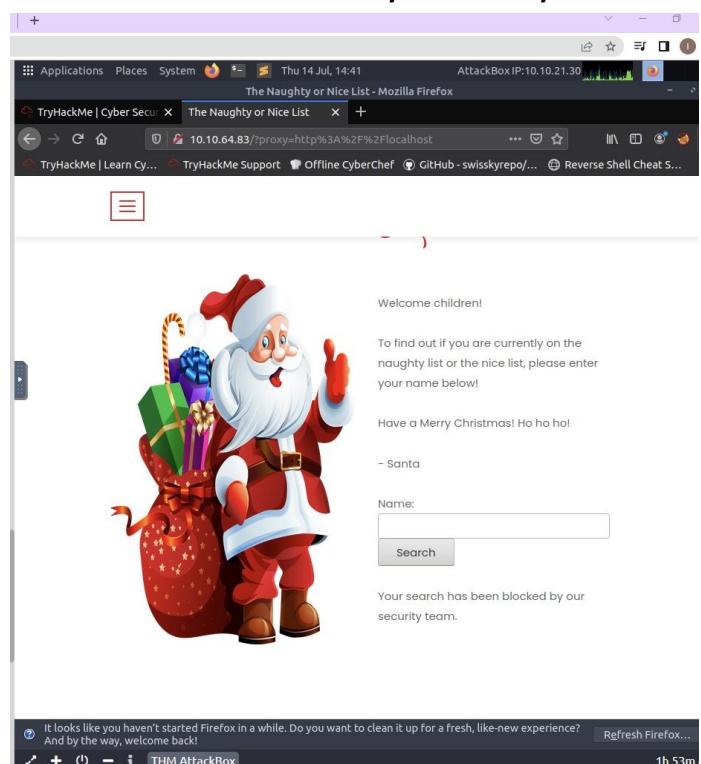
Recv failure: Connection reset by peer



Question 5

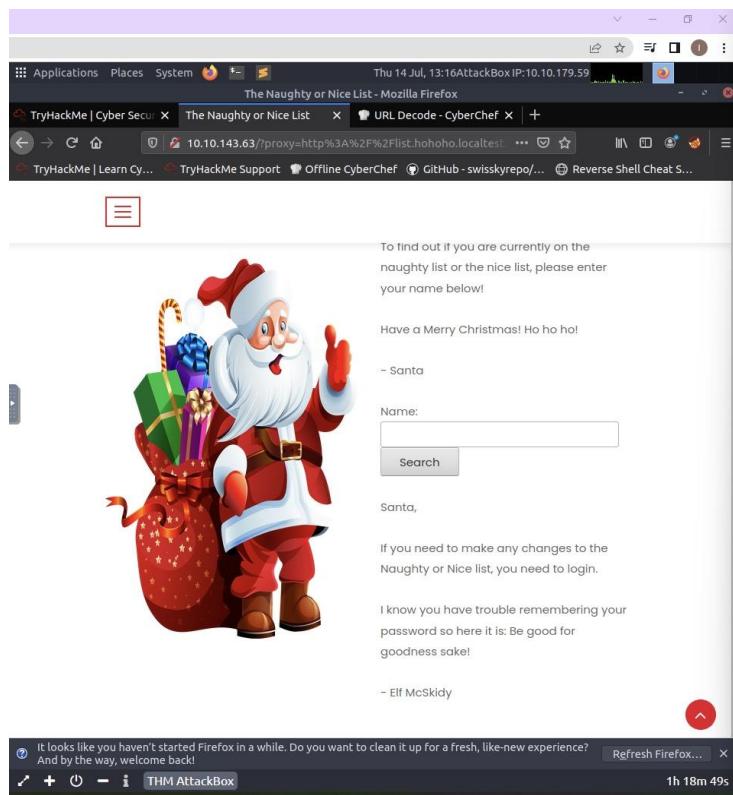
What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?

Your search has been blocked by our security team.



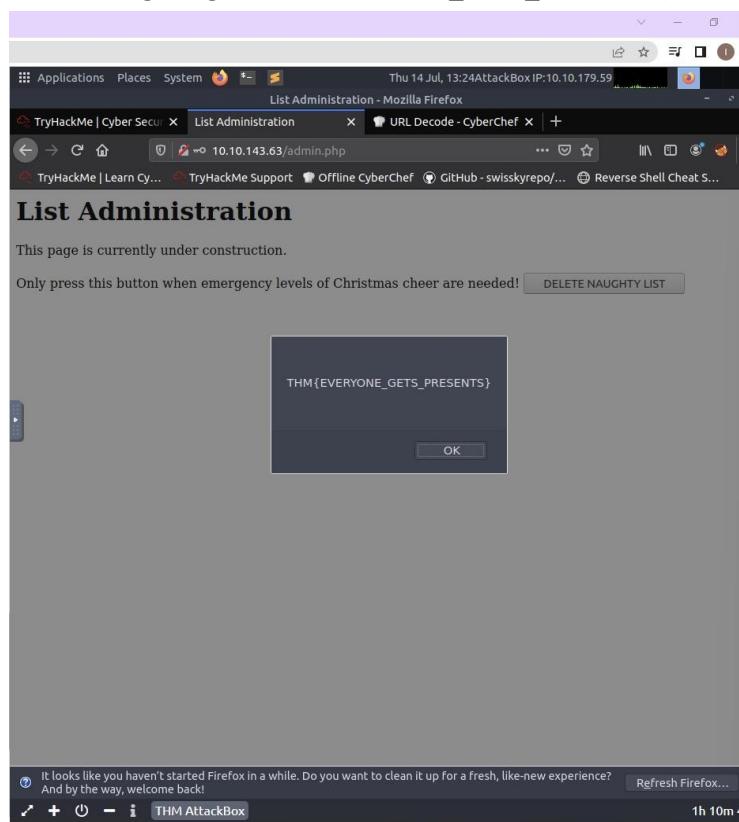
Question 6

Santa's password is **Be good for goodness sake!**



Question 7

The challenge flag is **THM{EVERYONE_GETS_PRESENTS}**



Thought Process/Methodology:

Firstly, once the VM is deployed, we connect to the web application by entering the IP address in firefox. Upon entry into the website, we can enter a name and check if that person is on the Naughty or Nice List. There is also an admin panel on the homepage. So we tried searching for the names **Tib3rius, Ian Chai, YP, Timothy, Kanes and JJ**. Therefore, we get to find out whether their names are on the Naughty List or the Nice List. Then, we enter the name Ilyana, and we notice that when we search for the name, there is a proxy parameter in the URL. Next, we open Sublime Text and paste the URL. Next, we copy `http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3Dillyana` and paste it into Offline Cyberchef. After we decode the URL, we get the decoded output which is <http://list.hohoho:8080/search.php?name=illyana> and we paste it back on Sublime Text. Since "list.hohoho" is not a valid hostname, it seems to be communicating with a backend service that takes the user's name and returns whether they are Naughty or Nice. We can take advantage of this by performing a SSRF (Server-Side Request Forgery) attack. Next, we try to fetch the root of the same site. We enter the url <http://10.10.143.63/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F> and we can see "**Not Found. The requested URL was not found on this server.**" This looks like a generic 404 message, which we were able to make the server request the modified URL and it returned the response. Next, we try changing the port number from 8080 to 80 and we can see there is "**Failed to connect to list.hohoho port 80: Connection refused**" messages are displayed which implies that port 80 is not open on list.hohoho. After that, we try to change the port number to 22 and now there is "**Recv failure: Connection reset by peer**" which implies that port 22 is open but was unable to understand what was sent. Next, we access services running locally on the server by replacing the list.hohoho hostname with "localhost" and we can see there is "**Your search has been blocked by our security team**" messages are displayed because the developer has added a check to ensure that the hostname provided begins with "list.hohoho" and any hostnames that do not will be blocked. We discovered that only the domain list.hohoho works, but perhaps we can try some different subdomains, which is localtest.me. The full URL is <http://10.10.143.63/?proxy=http%3A%2F%2Flist.hohoho.localtest.me>. This URL appears to respond with a message from Elf McSkidy containing a password to log into the admin which is "**Be good for goodness sake!**" We guessed the username and found out that the username is Santa and we logged in. Then, we delete the naughty list and the flag **THM{EVERYONE_GETS_PRESENTS}** appears.

Day 20: Blue Teaming – Powershell to the rescue

Tools used: Terminal Emulator

Solution/walkthrough:

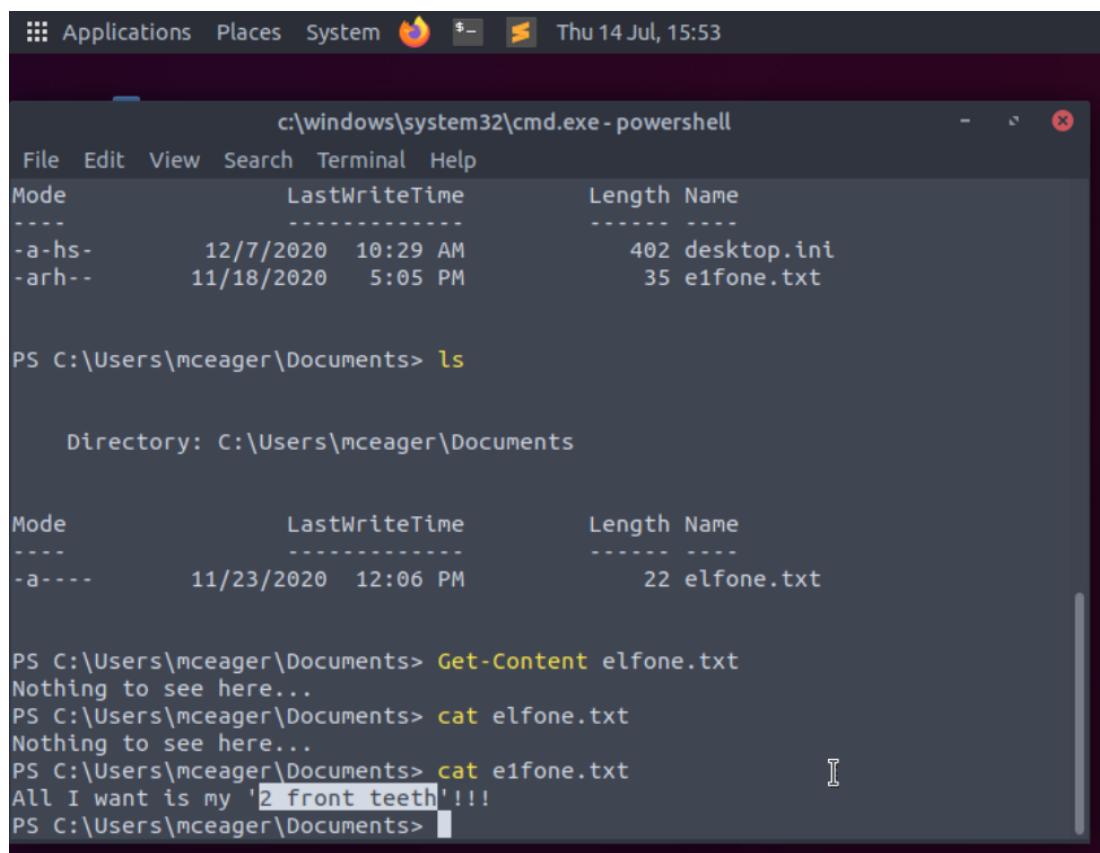
Question 1

The parameter -l is used for the login name.

```
-l login_name
      Specifies the user to log in as on the remote machine. This also
      may be specified on a per-host basis in the configuration file.
```

Question 2

Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want **2 front teeth**.



The screenshot shows a terminal window titled 'c:\windows\system32\cmd.exe - powershell'. The window contains the following command-line session:

```
c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Help
Mode           LastWriteTime          Length Name
----           -----              ---- -
-a-hs-         12/7/2020 10:29 AM       402 desktop.ini
-arh--        11/18/2020 5:05 PM        35 efone.txt

PS C:\Users\mceager\Documents> ls

Directory: C:\Users\mceager\Documents

Mode           LastWriteTime          Length Name
----           -----              ---- -
-a---         11/23/2020 12:06 PM        22 elfone.txt

PS C:\Users\mceager\Documents> Get-Content elfone.txt
Nothing to see here...
PS C:\Users\mceager\Documents> cat elfone.txt
Nothing to see here...
PS C:\Users\mceager\Documents> cat efone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\Documents>
```

Question 3

The name of that movie that Elf 2 wants is **Scrooged**.

```
c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Help
Directory: C:\Users\mceager\Desktop

Mode LastWriteTime Length Name
---- ----- ----- --
d--h-- 12/7/2020 11:26 AM elf2wo

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

Search the Windows directory for a hidden folder that contains files for Elf 3. The name of the hidden folder is **3lfthr3e**.

```
File Edit View Search Terminal Help
c:\windows\system32\cmd.exe - powershell
-a--- 9/15/2018 12:12 AM 606720 Windows.UI.Xaml.Resources.r
s3.dll
-a--- 9/15/2018 12:12 AM 792992 winsqlite3.dll
-a--- 9/6/2019 5:28 PM 366592 Wldap32.dll
-a--- 9/15/2018 12:12 AM 17408 wowreg32.exe
-a--- 9/15/2018 12:12 AM 434952 ws2_32.dll
-a--- 9/15/2018 12:12 AM 66560 wsnmp32.dll
-a--- 9/15/2018 12:12 AM 18944 wsock32.dll
-a--- 9/15/2018 12:12 AM 64792 wtsapi32.dll
-a--- 9/15/2018 12:12 AM 143360 xwtpw32.dll

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

The first file contains **9999** words.

```
c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Help
arbor
mediawiki
configurations
poison
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

The 2 words at index 551 and 6991 in the first file are **Red Ryder**.

```
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. Elf 3 want **redryderbbgun**.

```
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[551,6991]
Red
Ryder
PS C:\Windows\System32\3lfthr3e> Get-Content 2.txt | Select-String -Pattern "redryder"
redryderbbgun
```

Thought Process/Methodology:

For Day 20, we used PowerShell over SSH to connect to the remote machine. The command that we use to run to connect to the remote machine is ssh -l mceager 10.10.206.66. For Question1, parameter -l used for the login name. When prompted, enter the password r0ckStar! and once we have logged in successfully, we will begin to launch PowerShell and navigate to the Documents folder. To access the 'Documents' directory we can use powershell command - Set-Location Documents. After that, we can list the directory contents with command Get-ChildItem. Based on Question 2, we need to find the hidden elf file so in order to display only the hidden files, we can use the additional flag Get-ChildItem -Hidden -File. As a result, it shows us "e1fone.txt". To display the content of a file, in powershell we use command Get-Content e1fone.txt and it shows that he wants his 2 front teeth. Next, same as before, we navigated into the Desktop directory and listed all the contents inside it. But since the thing that we are looking for is a directory, we used another flag on our powershell command Get-ChildItem -Hidden -Directory. We navigated into the 'elf2wo' directory and listed the directory's content inside. There is a file 'e70smsW10Y4k.txt' in it. We see the file content using cat e70smsW10Y4k.txt. In the file, Elf 2 wants to watch a movie called "Scrooged". In John's walkthrough video, he is searching the file on C:\Windows\System32 and we are going to do the same. The command that we'll using is Get-ChildItem -Hidden -Filter "*3*". The command will display us the hidden content of the directory where it shows 3lfthr3e. For Question 5, we navigated into the directory '3lfthr3e', and list the file inside. There are two files by the name of '1.txt' and '2.txt'. To count the all words from file 1.txt, we can use the Measure-Object with flag -Word which input piped from Get-Content. It shows that the first file contains 9999 words. To find the 2 words at index 551 and 6991 in the first file, the command that we use is (Get-Content 1.txt)[551,6991] and the results are Red Ryder. For the last question, the command that we'll be using is Select-String -Pattern "redryder". It shows that Elf 3 want redryderbbgun.