PSP0201

Week 5

Write-up

Group Name: Bubble Buddies

Student ID	Name	Role
1211103286	Ahmad Danish Izzuddin Bin Mohd Anas Zahari	Group Leader
1211101384	Ahmad Luqman Bin Zakarani	Member
1211103223	Amirah Hakimah binti Masri	Member
1211103656	Adlin Sofea Binti Adam Saffian	Member

Day 16 : Help! Where is Santa?

Tools used: Kali, Python, Nmap

Solution/walkthrough:

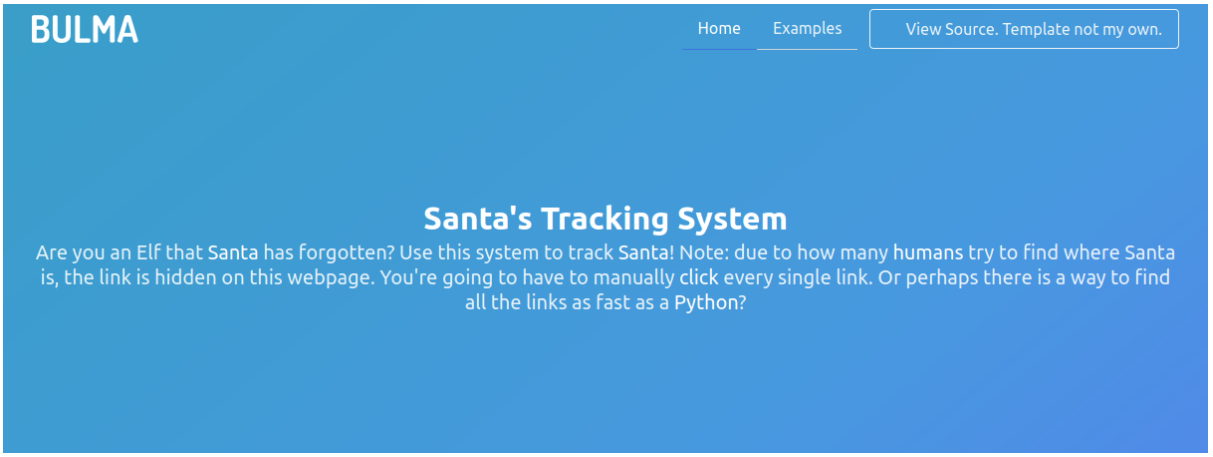
Q1: What is the port number for the web server?

Answer : 80

```
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Q2: What templates are being used?

Answer : BULMA



Q3: Without using enumeration tools such as Dirbuster, what is the directory for the API?

Answer : /api/

```
<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>
```

find_link.py find_api.py

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

# replace testurl.com with the url you want to use.
# requests.get downloads the webpage and stores it as a variable
html = requests.get('http://10.10.143.116:80')

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

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

```
┌──(12111013845㉿kali)-[~/room/day16]
└─$ python3 find_link.py | uniq
../
https://github.com/BulmaTemplates/bulma-templates/blob/master/templates/hero.html
https://tryhackme.com
#
http://machine_ip/api/api_key
#
https://github.com/BulmaTemplates/bulma-templates
```

Q4: Go to the API endpoint. What is the Raw Data returned if no parameters are entered?

Answer : {"detail":"Not Found"}

JSON Raw Data Headers

Save Copy Pretty Print

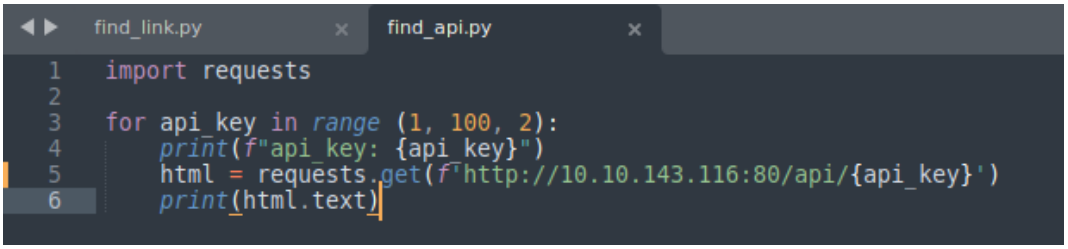
```
{"detail":"Not Found"}
```

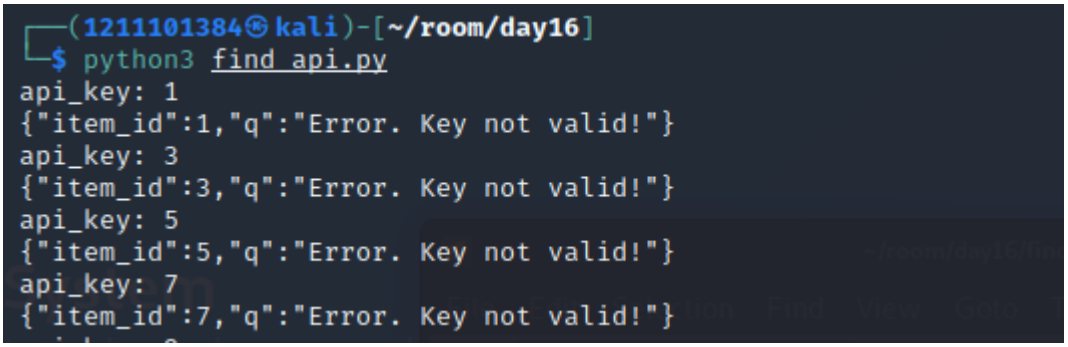
Q5: Where is Santa right now?

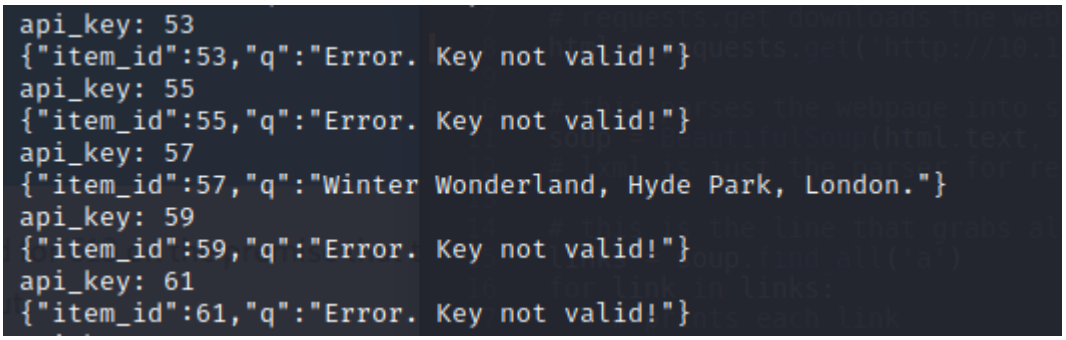
Answer : Winter Wonderland, Hyde Park, London

Q6: Find out the correct API key. Remember, this is an odd number between 0-100. After too many attempts, Santa's Sled will block you. To unblock yourself, simply terminate and re-deploy the target instance (10.10.94.92)

Answer : 57







Thought Process/Methodology:

First and foremost we run nmap to search for the server port on Kali Linux by scanning the IP Address. That is how we find the port number of the web server. After that, we go to the web browser, search for "`MACHINE_IP:port`". By viewing the page source we can find the api link. From there we use the Python script that we learn from day 15. We try to find the api key using Python script with the condition "odd number within 1-100". Therefore we could figure out the correct api link and santa current location.

Day 17 : ReverseELFneering

Tools used: Kali, Radare2

Solution/walkthrough:

Q1: Match the data type with the size in bytes

Data byte	1	2	4	8
Byte	☑	☐	☐	☐
Word	☐	☑	☐	☐
Double Word	☐	☐	☑	☐
Quad	☐	☐	☐	☑
Single Precision	☐	☐	☑	☐
Double Precision	☐	☐	☐	☑

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

Q2: What is the command to analyse the program in radare2?

Answer : aa

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`

Q3: What is the command to set a breakpoint in radare2?

Answer : db

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

Q4: What is the command to execute the program until we hit a breakpoint?

Answer : dc

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

Q5: What is the value of local_ch when its corresponding movl instruction is called (first if multiple)?

Answer : 1

```
0×00400b51      c745f4010000.  mov dword [local_ch], 1
```

Q6: What is the value of eax when the imul instruction is called?

Answer : 6

```
0×00400b58      c745f8060000.  mov dword [local_8h], 6
0×00400b5f      8b45f4         mov eax, dword [local_ch]
0×00400b62      0faf45f8       imul eax, dword [local_8h]
```

Q7: What is the value of local_4h before eax is set to 0?

Answer : 6

```
0×00400b66      8945fc         mov dword [local_4h], eax
0×00400b69      b800000000     mov eax, 0
```

Thought Process/Methodology:

First of all we login into the machine and write “ssh elfmceager@MACHINE_IP”. After that we used the command “`ls`” and found the “challenge1” file. From there we run the command “r2 -d ./challenge1” to open the file using Radare2. In the Radare2 environment, we run the command “`aa`” to analyse all flags starting with sym. After that, we run the command “pdf @main” to examine the code inside the main function.Before the instruction carried out a certain breakpoint is already being set. We use the command “dc” to execute the program until breakout and “px @memory-address” command being used to read the content in the variable. After that we use the command “ds” to proceed to the next one. The ds command allows us to put a value into the specified variable. Lastly, We use the “dr” command to make sure the values are accurate.

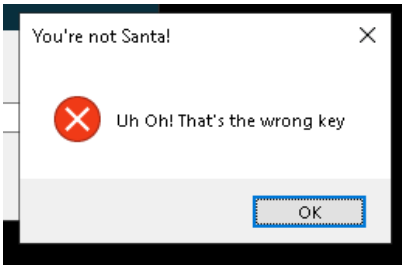
Day 18 : The Bits Of Christmas

Tools used: Remmina, TBFC, CyberChef, ILSpy, THM Attackbox

Solution/walkthrough:

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

Answer : Uh Oh! That's the wrong key

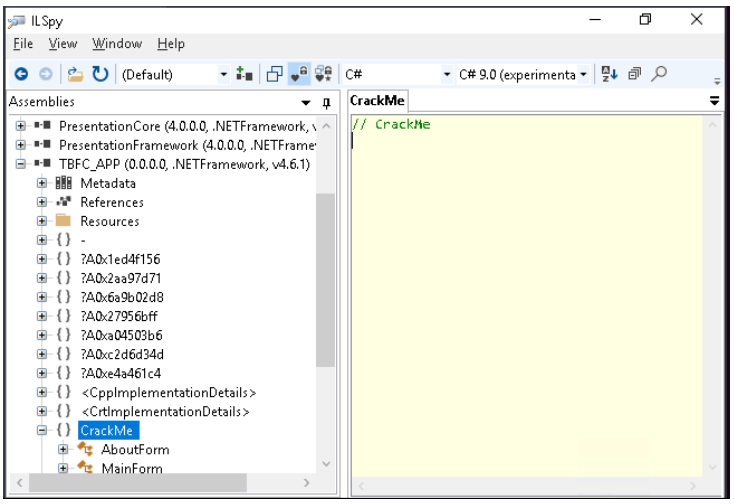


Q2: What does TBFC stand for?

Answer : The Best Festival Company

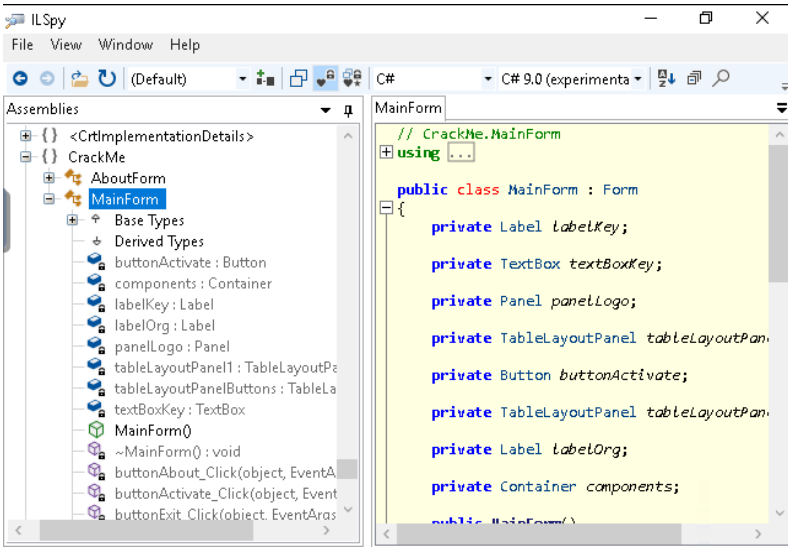
Q3: Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?

Answer : CrackMe



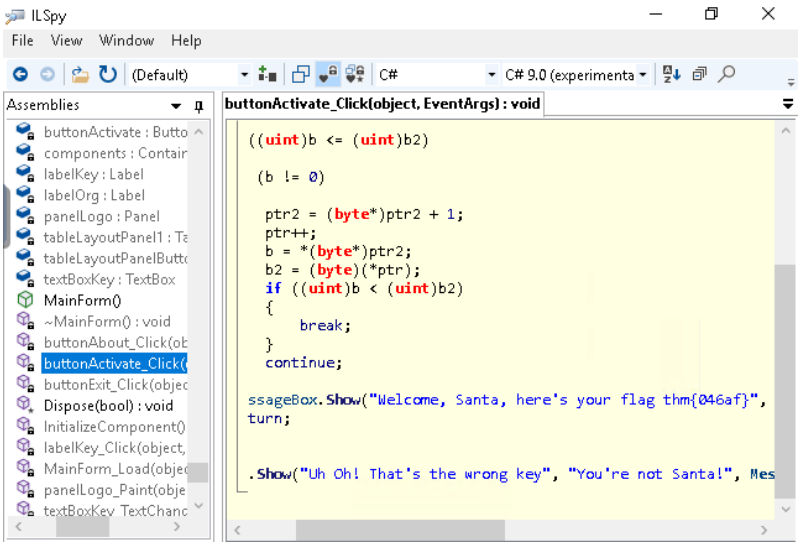
Q4: Within the module, there are two forms. Which contains the information we are looking for?

Answer : MainForm



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

Answer : buttonActivate_Click

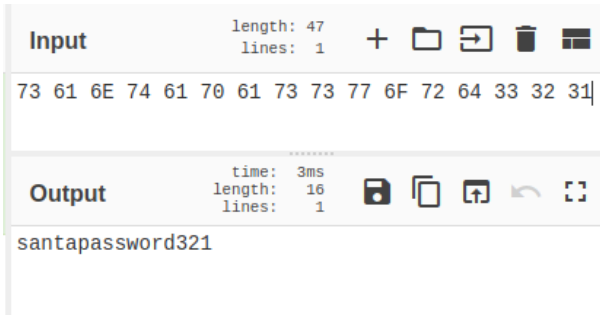


Q6: What is Santa's password?

Answer : santapassword321

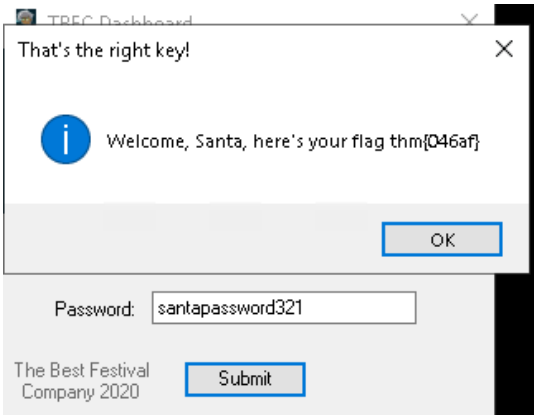
```
(ref <Module>.??_C@_0BB@IKKDFEPG@santapassword321@);
```

```
>assword321@/* Not supported: data(73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31
```



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

Answer : thm{046af}



Thought Process/Methodology:

First of all we deployed TryHackMe attackbox and opened the tool remmina. After that we clicked the TBFC application and tried to write anything in the username and password section to know the messages it gave us if we login with the wrong one users.After that, we can find the full name of TBFC at the bottom left of the application. Next, we opened ILSpy to complete the second challenge. As our ILSpy does not have TBFC in it, we need to insert TBFC into ILSpy by going from File to Open to Desktop to TBFC and lastly Open. By doing that, it is the only way for us to proceed with the second challenge. First thing first, we clicked '+' button to get to know more files under Resources and looked at all the module names. We did the same thing at the CrackMe module, there are 2 modules which are MainForm and AboutForm. We explored both modules and we knew the MainForm contained the information we are looking for. As we were looking for a password, we looked at the method one by one and buttonActivate_Click gave us the information as it wrote the messages that will pop up if the password is correct or wrong. Furthermore it brought us to the password page. To get confirmation of the password, we copied the hexadecimal given and pasted it at CyberChef website.Therefore, by doing that we successfully got Santa's password. We use the correct password to login into TBFC and got our flag.

Day 19 : The Naughty or Nice List

Tools used: AttackBox

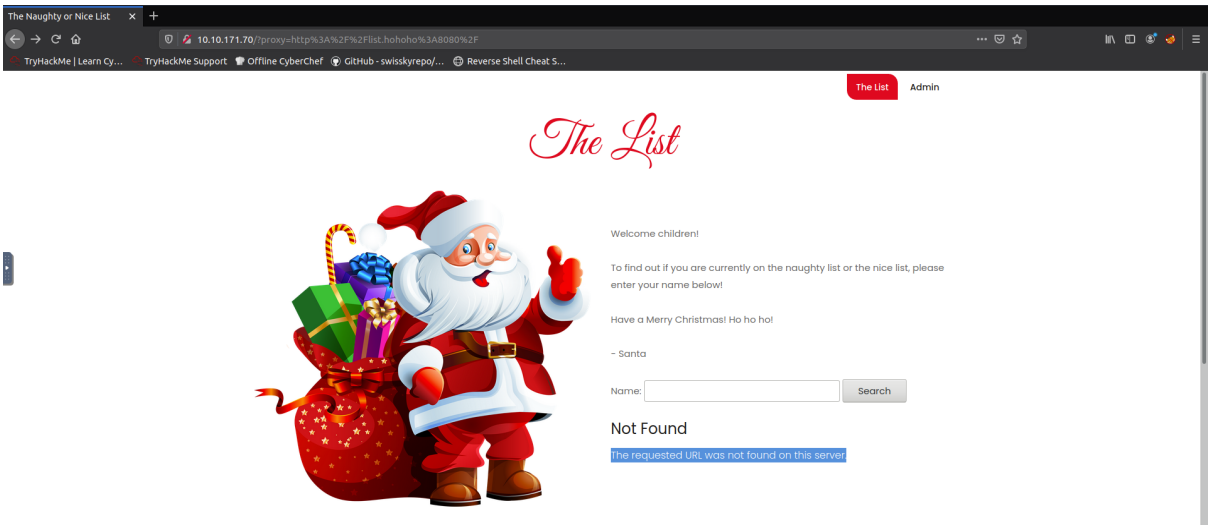
Solution/walkthrough:

Q1: Which list is this person on?

Name	Naughty	Nice
Timothy	☑	☐
JJ	☑	☐
Tib3rius	☐	☑
Kanes	☑	☐
YP	☐	☑
Ian Chai	☐	☑

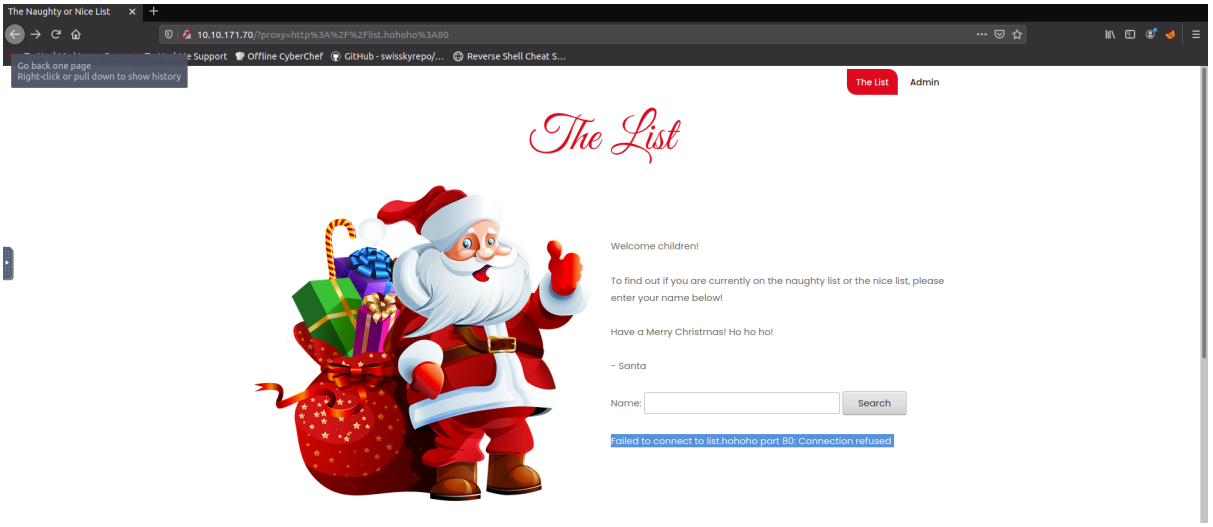
Q2: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?

Answer : The requested URL was not found on this server.



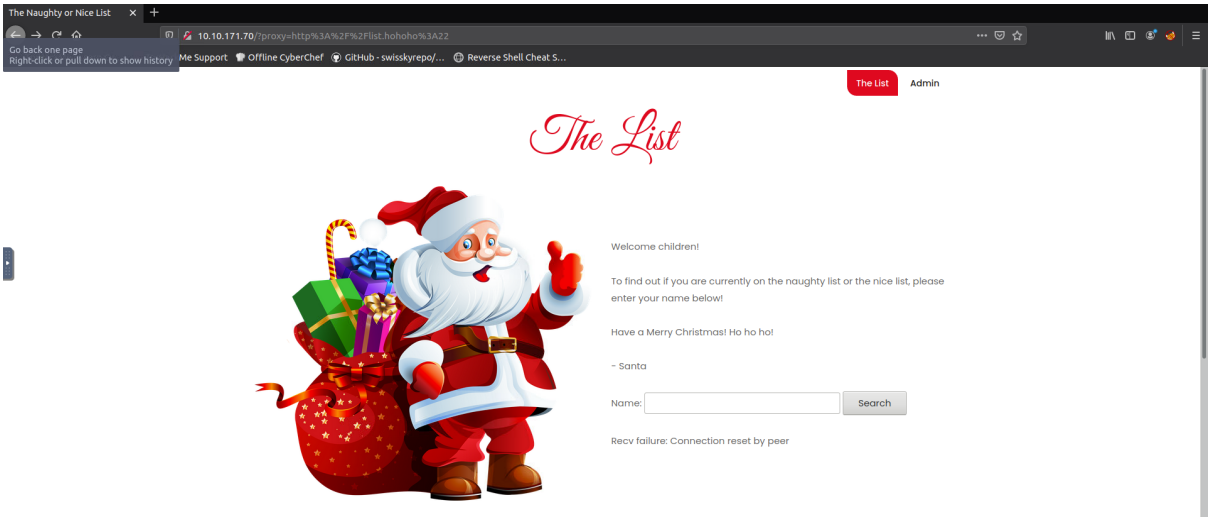
Q3: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"?

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



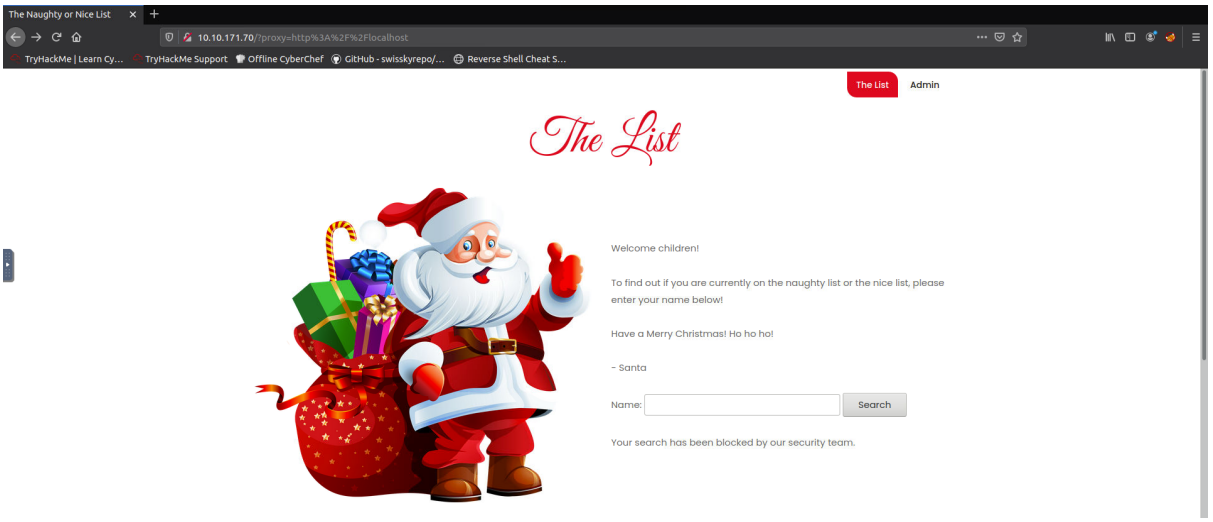
Q4: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"?

Answer : Recv failure: Connection reset by peer



Q5: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?

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



Q6: What is Santa's password?

Answer : Be good for goodness sake!

Santa,

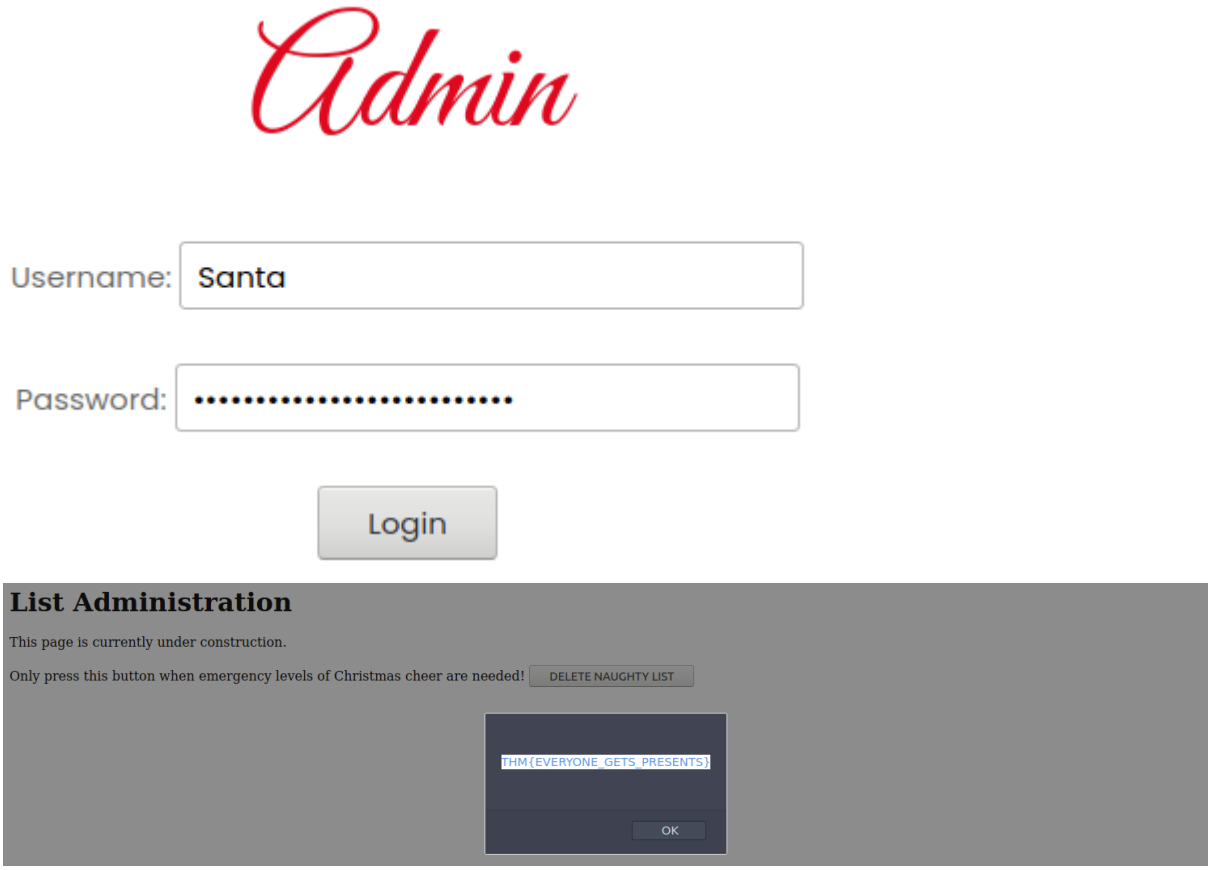
If you need to make any changes to the Naughty or Nice list, you need to login.

I know you have trouble remembering your password so here it is: Be good for goodness sake!

- Elf McSkidy

Q7: What is the challenge flag?

Answer : THM{EVERYONE_GETS_PRESENTS}



Thought Process/Methodology:

First and foremost, we use the IP address that is given and paste it at Mozilla Firefox. We enter each name to check whether they are in either the naugthy list or the nice list. After that, we deleted the parameter “search.php%3Fname%3DTimothy" and the website showed “The requested URL was not found on this server.” We know that “list.hohoho” is not a valid hostname because ``.hohoho" is not a top-level domain. We tried changing the port 8080 to 80, but the website still refuses to connect us to it. We then changed the port number to 22, which is the default SSH port, but it is still not working as sending an HTTP request to an SSH server will never work. We also tried to replace the “list.hohoho” hostname with "localhost" to try accessing the services running locally on the server, but there is a check implemented to ensure that the hostname provided starts with "list.hohoho", and will block any hostnames that don't. So now we know that the hostname has to start with "list.hohoho". We therefore set the hostname in the URL to "list.hohoho.localtest.me", and we can see a message Elf McSkidy left for Santa regarding his password. Afterwards, we log in as admin with the username “Santa” and the password “Be good for goodness sake!”. We got the flag by deleting the naughty list as instructed in the walkthrough.

Day 20 : PowershELIF To The Rescue

Tools used: Mozilla Firefox, Kali Linux

Solution/walkthrough:

Q1: Check the ssh manual. What does the parameter -l do?

Answer : local host

Q2: Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

Answer : 2 front teeth

```
PS C:\Users\mceager\Documents> Get-Content e1fone.txt
All I want is my '2 front teeth'!!!
```

Q3: 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?

Answer :Scrooged

```
    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> Get-content e70smsW10Y4K.txt
I want the movie Scrooged <3!
PS C:\Users\mceager\Desktop\elf2wo>
```

Q4: Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder?

Answer :3lfthr3e

```
    Directory: C:\Windows\System32


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--        11/23/2020   3:26 PM                3lfthr3e
```

Q5: How many words does the first file contain?

Answer :9999

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


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

Q6: What 2 words are at index 551 and 6991 in the first file?

Answer : Red Ryder

```
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[551]
Red
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[551,6991]
Red
Ryder
```

Q7: 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?

Answer :redryderbbgun

```
PS C:\Windows\System32\3lfthr3e> Get-Content 2.txt | Select-String -Pattern "redryder"

redryderbbgun
```

Thought Process/Methodology:
First of all, we use the command “ssh -l mceager MACHINE_IP” and password “r0ckStar” to connect to the remote machine, after that we switch into the powershell to control and navigate the machine. After that to complete the task we use commands such as “Set-Location” to change the directory, “Get-ChildItem”cmdlet to enhance its capabilities further. We also use the command “hidden” and “filter” to find the hidden file more easily without having to go through every file there. Beside that, we use the command “Measure-Object” to calculate the number of content in the file. By using all this command, we complete all the tasks.