

PSP0201

Week 5

Write Up

Group Name : Espada

Student ID	Name
1211103094	Muhammad Irfan Bin Zulkifli
1211103424	Muhammad Afiq Danish Bin Sunardi
1211103147	Ahmad Haikal Bin Emran

Day 16 - Scripting - Help! Where is Santa?

Tools used: Kali linux, firefox, python

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

Answer: 80

Launch the machine and we get the IP address of the machine. Scan the IP address using NMAP to detect port used by the web server. We get port 80. We search on the firefox by using `10.10.205.36:80` and landed on Santa Tracking System.

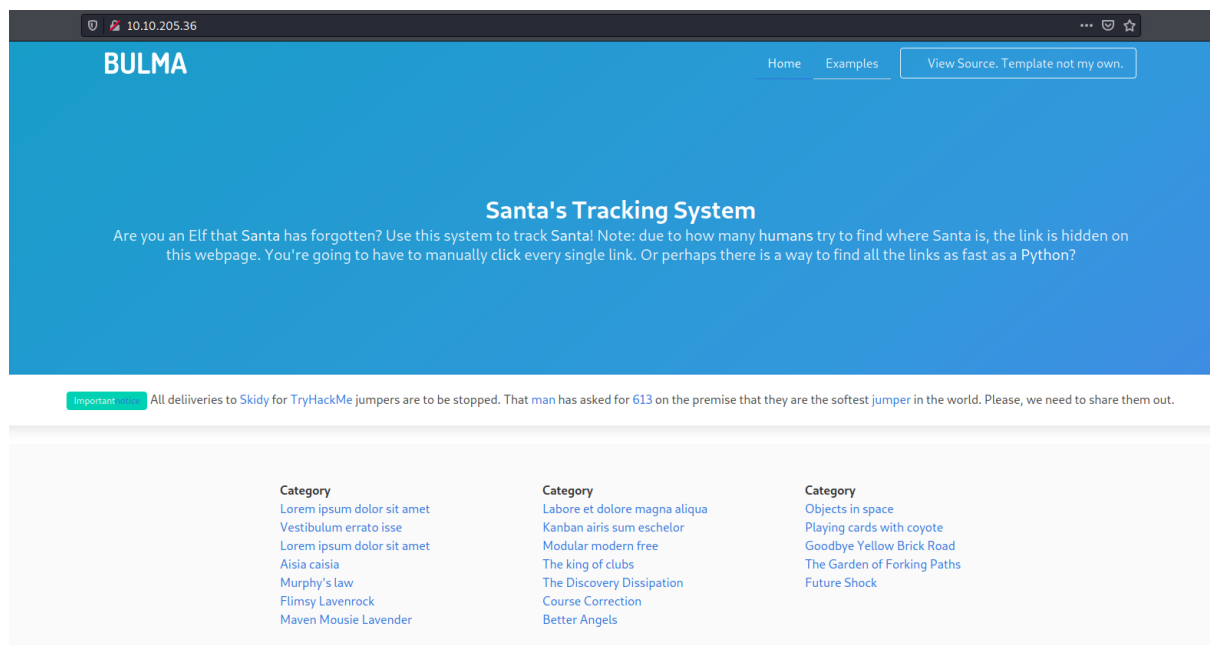
```
(kali㉿kali)-[~]
$ nmap 10.10.205.36
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-04 10:02 EDT
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 39.43% done; ETC: 10:03 (0:00:14 remaining)
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 66.75% done; ETC: 10:03 (0:00:07 remaining)
Nmap scan report for 10.10.205.36
Host is up (0.24s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 22.33 seconds
```

Q2: What templates are being used?

We can see the name of the templates appeared on the left top website page.

Answer: Bulma



Q3: Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)

Answer: /api/

We view the source code of the page and search for link that have API in it. Then we saw the link. As the question want the answer without the API key, we just give the API directory

```
<li><a href="#">Kanban airis sum eschelor</a></li>
<li><a href="http://machine_ip/api/api_key">Mod</li>
<li><a href="#">The king of clubs</a></li>
```

However, we also can get the directory using python that we learned from day 15.

We copy and paste the code from day 15 into file that we named as day16.py. After that we change the URL in the html variable into our target machine IP address included with the port number. In the code, we stated in that we find all link using attribute tag `<a>` using soup method called `find_all` stored in the `links` variable.

Something very cool you can do with these 2 libraries is the ability to extract all links on a webpage.

```
# 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('testurl.com')

# this parses the webpage into something that beautifulsoup can read over
soup = BeautifulSoup(html, "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 variable
links = soup.find_all('a href')
for link in links:
    # prints each link
    print(link)
```

```
# 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://10.10.205.36:80')

# 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 li>
links = soup.find_all('a')
for link in links:
    # prints each link
    print(link)
```

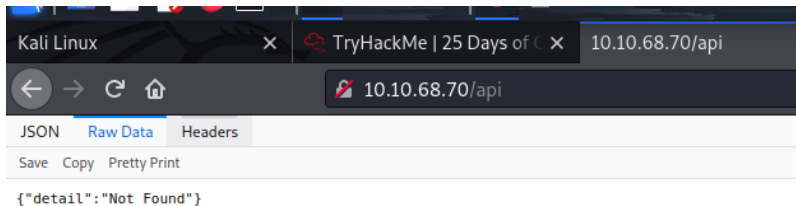
And then, we run the python code we just created for us to see if there is any API directory. As expected, there is it the directory.

```
(kali@kali)-[~]  
$ python3 day16.py
```

```
<a href="http://machine_ip/api/api_key">Modular modern free</a>
```

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

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



Q5: Where is Santa right now?

Answer: Winter Wonderland, Hyde Park, London

We get the answer through API key iteration in question 4

```
api_keys 55  
{"item_id":55,"q":"Error. Key not valid!"}  
api_keys 57  
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}  
api_keys 59  
{"item_id":59,"q":"Error. Key not valid!"}
```

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 (10.10.205.36)

Answer: 57

To find the correct API keys, we create another python file named findAPI.py and still be using requests libraries. We will iterate through 1 to 100 to find the correct API keys using the hint given which is the number must be odd. We create for loop and api_keys variable with range 1 to 100 with 2 steps every iteration since we want to use odd number only. Then we print out the html.text to see if the API key match or not. Then we see through the result and manage to see that 57 is the correct api key.

```
findAPI.py
File Edit Search Options Help
#!/usr/bin/env python3
import requests

for api_keys in range(1,100,2):
    print(f'api_keys {api_keys}')
    html = requests.get(f'http://10.10.205.36:80/api/{api_keys}')
    print(html.text)

api_keys 55
{"item_id":55,"q":"Error. Key not valid!"}
api_keys 57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
api_keys 59
{"item_id":59,"q":"Error. Key not valid!"}
```

Thought / methodology process:

Firstly, we launch the machine and we get the IP address of the machine. Scan the IP address using NMAP to detect port used by the web server. We get port 80. We search on the firefox by using `10.10.205.36:80` and landed on Santa Tracking System. From that we understand that port 80 is being used for the web application. After that we open the web application using the IP address given. As requested, we need to find the API directory. We view the source code of the page and search for link that have API in it. Then we saw the link of the API directory in the web application. However, we also can get the directory using python that we learned from day 15. We copy and paste the code from day 15 into file that we named as day16.py. After that we change the URL in the html variable into our target machine IP address included with the port number. In the code, we stated in that we find all link using attribute tag `<a>` using soup method called `find_all` stored in the `links` variable. To find the correct API keys, we create another python file named findAPI.py and still be using requests libraries. We will iterate through 1 to 100 to find the correct API keys using the hint given which is the number must be odd. We create for loop and api_keys variable with range 1 to 100 with 2 steps every iteration since we want to use odd number only. Then we print out the html.text to see if the API key match or not. Then we see through the result and manage to see that 57 is the correct api key. From that we also can see the location of the Santa which is Winter Wonderland, Hyde Park, London.

Day 17 - Reverse engineering - ReverseELFneering

Tools used: Kali linux, firefox

Q1: Match the data type with the size in bytes:

Answer:

Byte: 1 byte

Word: 2 bytes

Double Words: 4 bytes

Quad: 8 bytes

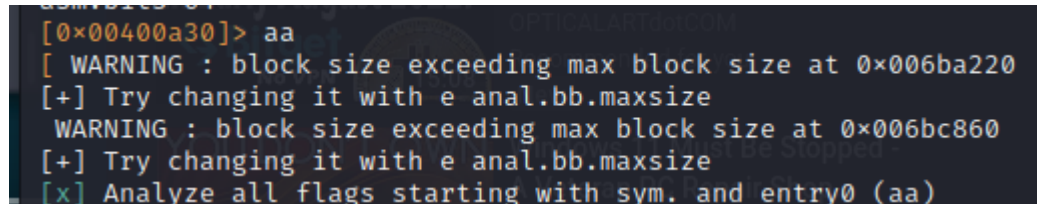
Single Precision: 4 bytes

Double Precision: 8 bytes

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

Answer: aa

We run aa command to analyze the programme



```
[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)
```

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

Answer: db

We run the db command to set the breakpoint on the wanted instruction.

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

Answer: dc

We run the dc command to execute the programme until we hit the breakpoint that we already set up.

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

Answer: 1

Connect to the IP address using ssh. Use the password given in tryhackme.

```
(kali@kali)-[~]
$ ssh elfmceager@10.10.67.211
elfmceager@10.10.67.211's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-128-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Tue Jul  5 04:07:43 UTC 2022

System load:  0.0               Processes:           104
Usage of /:   39.4% of 11.75GB   Users logged in:    1
Memory usage: 12%              IP address for ens5: 10.10.67.211
Swap usage:   0%

⇒ There is 1 zombie process.

0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Tue Jul  5 02:38:33 2022 from 10.8.94.82
```

Using ls command, we can see challenge1 file then we run r2 -d ./challenge1 command to open binary in debugging mode.

```
elfmceager@tbfc-day-17:~$ ls
challenge1 e file1
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1828 started...
= attach 1828 1828
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
```

Run aa command to ask r2 analyze the programme

```
[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)
```

Run afl command to see the function and we can see sys.main function


```

[0x00400a30]> afl
0x00400b20  3 45 → 40  entry1.init
0x00400b4d  1 35      sym.main

```

Then we run pdf @main command to see the assembly code. Then we can see that local_ch value is 1.

```

[0x00400a30]> pdf @main
;-- main:
/ (fcn) sym.main 35
  sym.main ();
    ; var int local_ch @ rbp-0xc
    ; var int local_8h @ rbp-0x8
    ; var int local_4h @ rbp-0x4
    ; DATA XREF from 0x00400a4d (entry0)
0x00400b4d  55          push rbp
0x00400b4e  4889e5      mov rbp, rsp
0x00400b51  c745f4010000. mov dword [local_ch], 1
0x00400b58  c745f8060000. mov dword [local_8h], 6
0x00400b5f  8b45f4      mov eax, dword [local_ch]
0x00400b62  0faf45f8    imul eax, dword [local_8h]
0x00400b66  8945fc      mov dword [local_4h], eax
0x00400b69  b800000000  mov eax, 0
0x00400b6e  5d          pop rbp
0x00400b6f  c3          ret

```

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

Answer: 6

We can see that imul instruction run on 5th instruction. Imul is an instruction that will multiply the source and destination. In this case we can see that eax is the source and local_8h is the destination. If the value of eax which is previously assigned as 1 taken from local_ch multiply with local_8h value which is 6, we will get the product is 6.

```

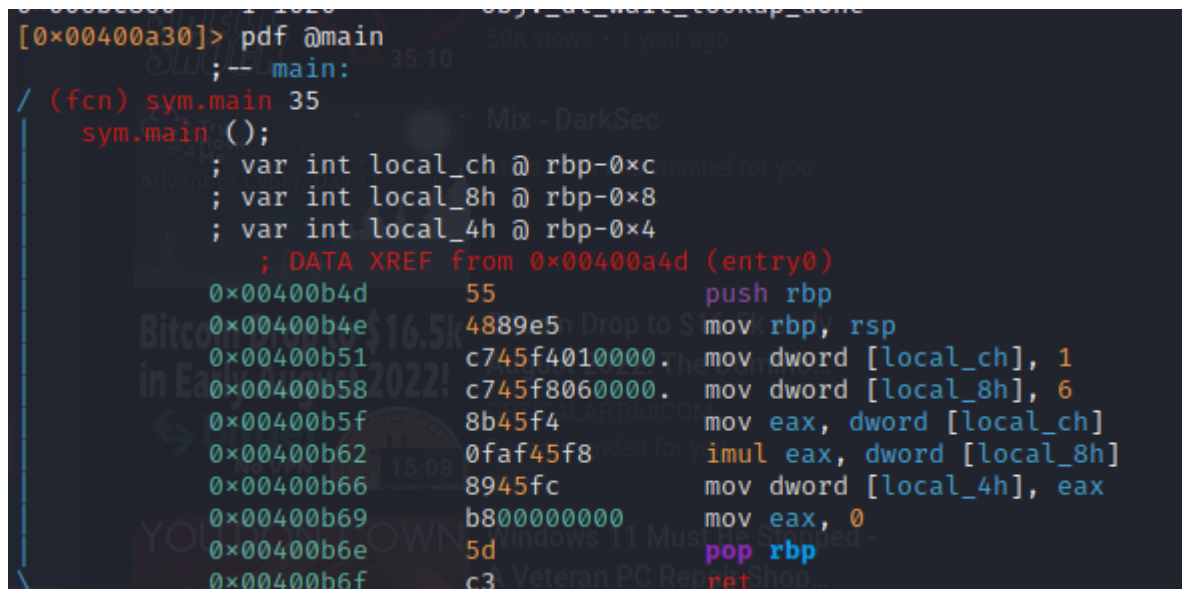
[0x00400a30]> pdf @main
;-- main:
/ (fcn) sym.main 35
  sym.main ();
    ; var int local_ch @ rbp-0xc
    ; var int local_8h @ rbp-0x8
    ; var int local_4h @ rbp-0x4
    ; DATA XREF from 0x00400a4d (entry0)
0x00400b4d  55          push rbp
0x00400b4e  4889e5      mov rbp, rsp
0x00400b51  c745f4010000. mov dword [local_ch], 1
0x00400b58  c745f8060000. mov dword [local_8h], 6
0x00400b5f  8b45f4      mov eax, dword [local_ch]
0x00400b62  0faf45f8    imul eax, dword [local_8h]
0x00400b66  8945fc      mov dword [local_4h], eax
0x00400b69  b800000000  mov eax, 0
0x00400b6e  5d          pop rbp
0x00400b6f  c3          ret

```


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

Answer: 6

We can see that the instruction that eax set to 0 is on the 6th instruction. Right before it we can see that one instruction happen which is the value of eax which is right at that moment is 6 copied into local_4h variable. So we can know that at that moment before it is set to 0, the value of eax is still 6.



```
[0x00400a30]> pdf @main
-- main:
/ (fcn) sym.main 35
sym.main();
; var int local_ch @ rbp-0xc
; var int local_8h @ rbp-0x8
; var int local_4h @ rbp-0x4
; DATA XREF from 0x00400a4d (entry0)
0x00400b4d 55 push rbp
0x00400b4e 4889e5 mov rbp, rsp
0x00400b51 c745f4010000 mov dword [local_ch], 1
0x00400b58 c745f8060000 mov dword [local_8h], 6
0x00400b5f 8b45f4 mov eax, dword [local_ch]
0x00400b62 0faf45f8 imul eax, dword [local_8h]
0x00400b66 8945fc mov dword [local_4h], eax
0x00400b69 b800000000 mov eax, 0
0x00400b6e 5d pop rbp
0x00400b6f c3 ret
```

Thought / methodolgy process:

Firstly, we connect to the IP address using ssh using the password given in tryhackme. Using ls command, we can see challenge1 file then we run r2 -d ./challenge1 command to open binary in debugging mode. Then, we run aa command to ask r2 analyze the programme. After that, we run afl command to see the function and we can see sys.main function. Then we run pdf @main command to see the assembly code. For the question 5, we can see that local_ch value is 1. We can identify the answer by observing the third line of instruction where we can see the instruction assigned the value number 1 to the local_ch variable. For the question 6, We can see that imul instruction run on 5th instruction. Imul is an instruction that will multiply the source and destination. In this case we can see that eax is the source and local_8h is the destination. If the value of eax which is previously assigned as 1 taken from local_ch multiply with local_8h value which is 6, we will get the product is 6. Lastly, for the question 7, we can see that the instruction that eax set to 0 is on the 6th instruction. Right before it we can see that one instruction happen which is the value of eax which is right at that moment is 6 copied into local_4h variable. So we can know that at that moment before it is set to 0, the value of eax is still 6.

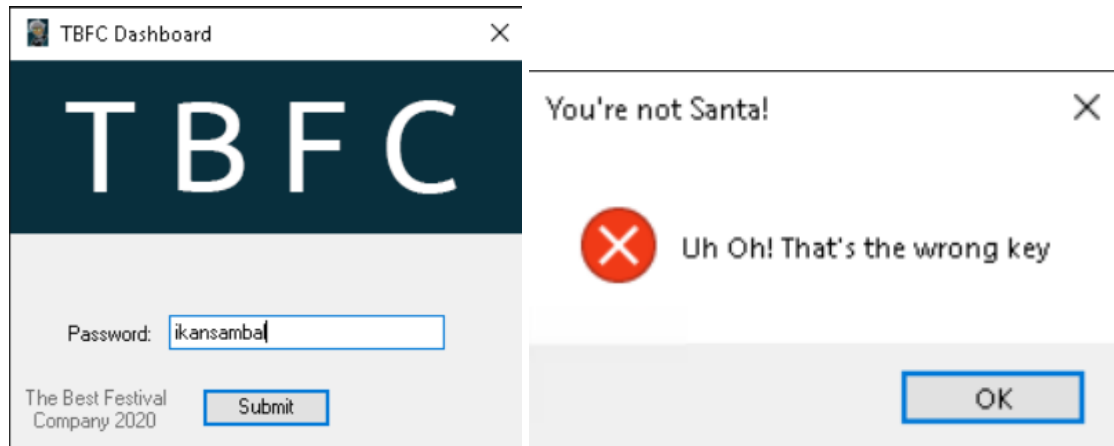
Day 18 - Reverse engineering - The Bits of Christmas

Tools used: Attackbox, Remmina

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

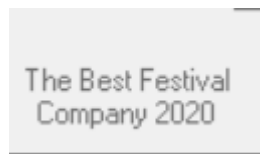
As we enter the random password which is "ikansamba", another window popped out and displayed the message.



Q2: What does TBFC stand for?

Answer: The Best Festival Company

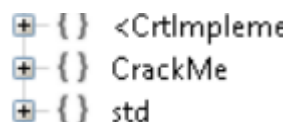
The answer can be seen from the left bottom of the app dashboard. The year omitted



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

Answer: CrackMe

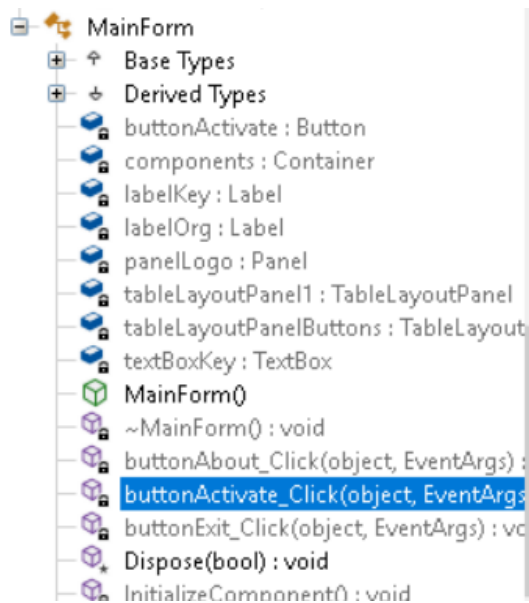
Among others module displayed with somewhat random characters, CrackMe module catch our attention as it names brings some meanings.



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

Answer: MainForm

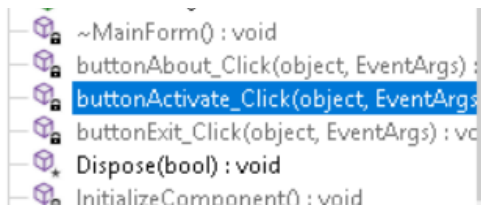
As we see through the MainForm, we can see there is the function named buttonActivate where we could assume it is the button used in the TBFC password insertion form.



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

Answer: buttonActivate_Click

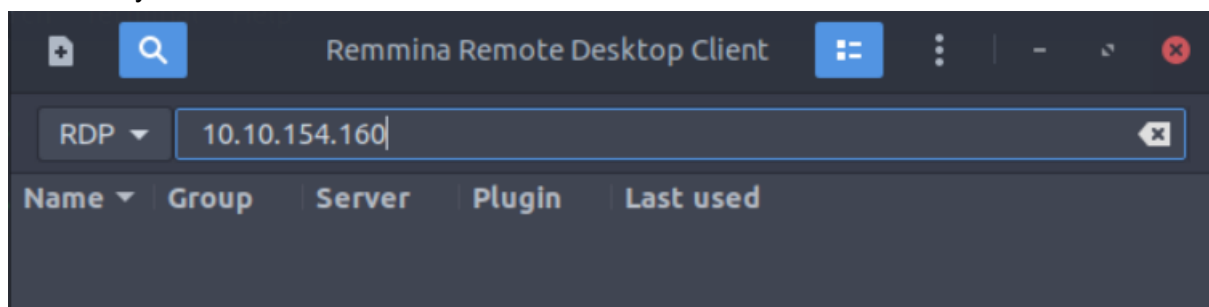
As we see through the MainForm, we can see there is the function named buttonActivate where we could assume it is the button used in the TBFC password insertion form.

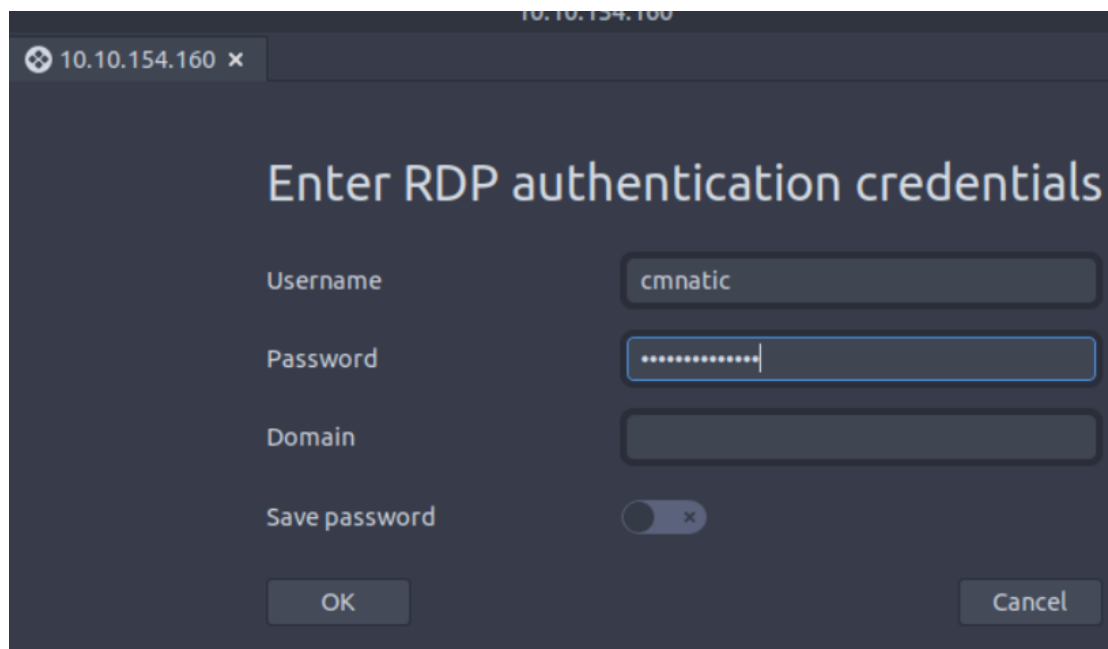


Q6: What is Santa's password?

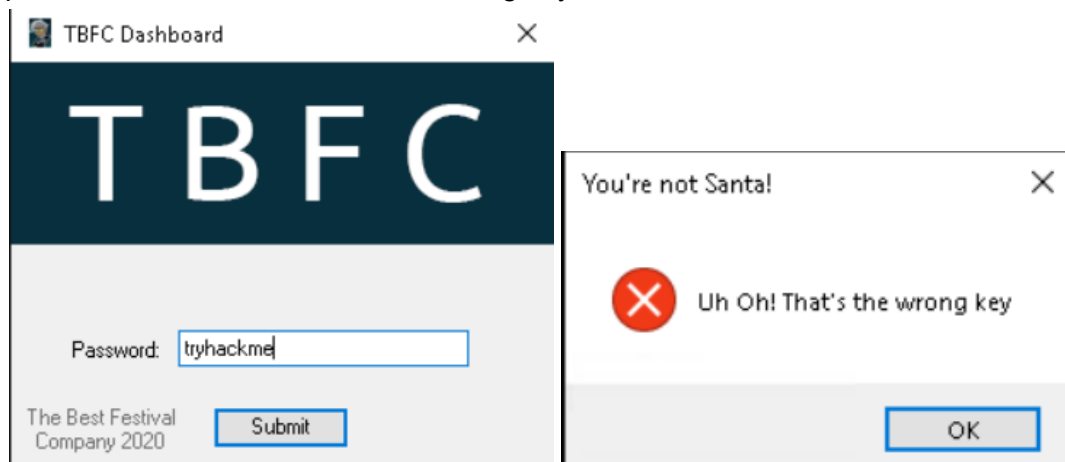
Answer: santapassword321

Open Attackbox and activate the machine. On the attackbox, launch the remmina to connect to the IP address given. Use the provided username which is cmnatic and password which is Adventofcyber!.

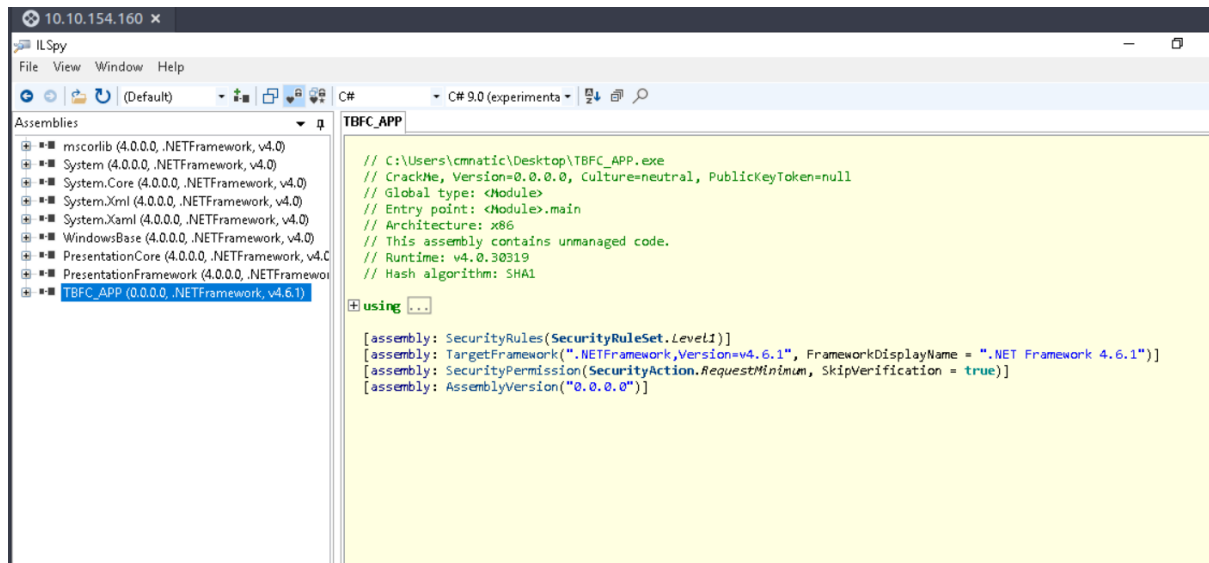




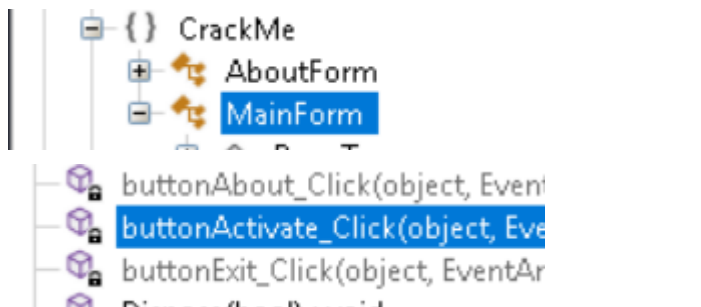
Then we can see TBFC application on the desktop. Once open it, we try to insert random password and it told that it was a wrong key.



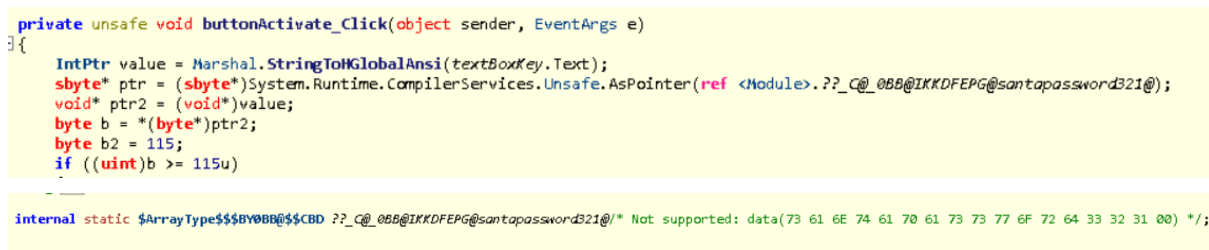
Then on the remote desktop, open the ILSpy application and then open the TBFC application on it to explore the santa password.



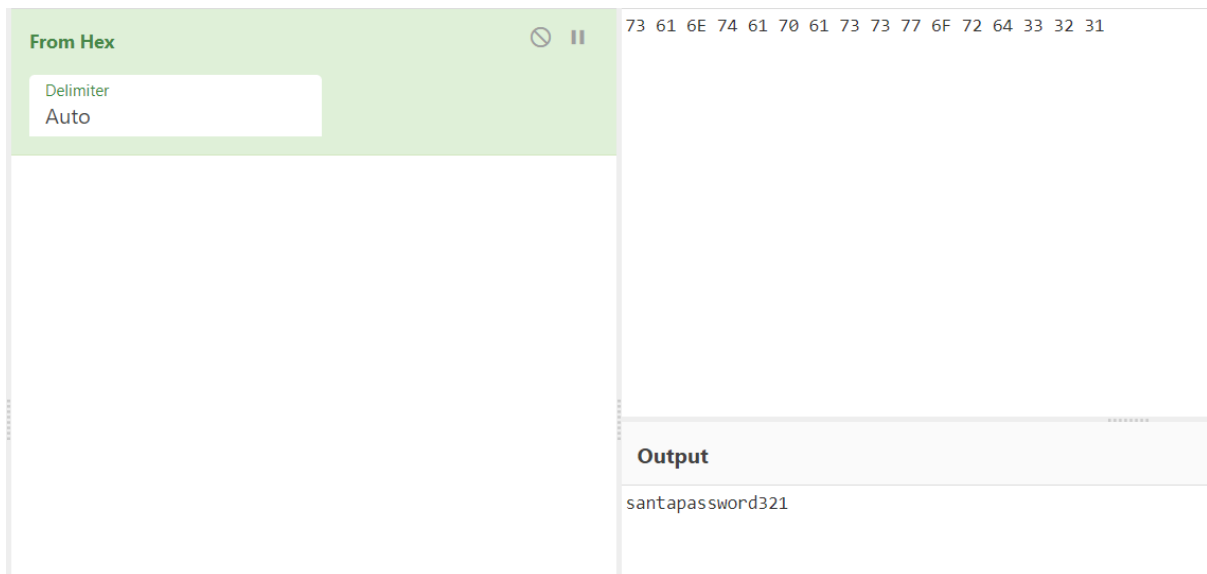
After expanding the application code, we can see one function that seems to be related to the password insertion form we meet earlier. Expand the function then we can see the buttonActivate_Click within it. We can assume that this maybe the button that appeared on the password insertion form we meet earlier. We then explore it a little.



At here, we can see the programme have ptr means that it is accepting string variable. Maybe this is place where the password are inserted into. We click the link that appeared when we hover on the @santapassword321@ and we were brought into other part of code where we can see hexadecimal assumed by how the code structured. We assuming that the hexadecimal is the password that santa used.



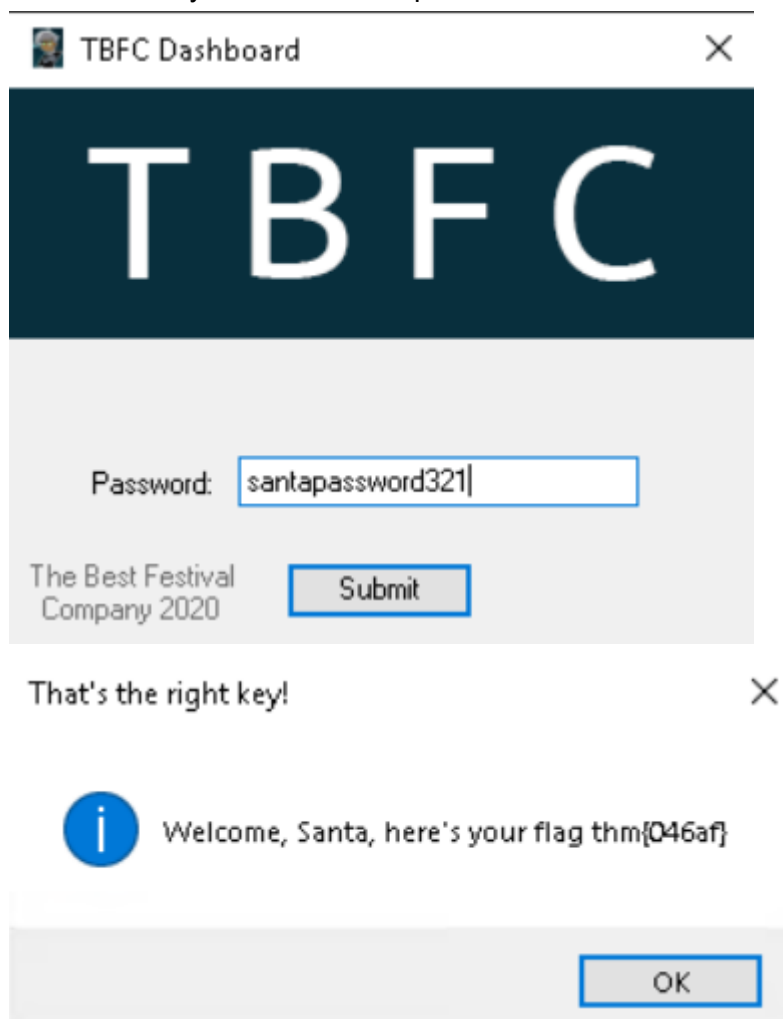
To be able get the real password used, we then we copy the hexadecimal code and paste it into cyberchef to translate it into readable text. Then we get the password that santa used to use which is **santapassword321**



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

Answer: thm{046af}

Use the password that we get from the ILspy, submit it then we shall get the flag indicates that we already use the correct password



Thought / methodology process:

Firstly, we open Attackbox and activate the machine. On the attackbox, launch the remmina to connect to the IP address given. Use the provided username which is cmnatic and password which is Adventofcyber!. Then we can see TBFC application on the desktop. Once open it, we try to insert random password and it told that it was a wrong key. Then on the remote desktop, open the ILspy application and then open the TBFC application on it to explore the santa password. After expanding the application code, we can see one function that seems to be related to the password insertion form we meet earlier. Expand the function then we can see the buttonActivate_Click within it. We can assume that this maybe the button that appeared on the password insertion form we meet earlier. We then explore it a little. At here, we can see the programme have ptr means that it is accepting string variable. Maybe this is place where the password are inserted into. We click the link that appeared when we hover on the @santapassword321@ and we were brought into other part of code where we can see hexadecimal assumed by how the code structured. We assuming that the hexadecimal is the password that santa used. To be able get the real password used, we then we copy the hexadecimal code and paste it into cyberchef to translate it into readable text. Then we get the password that santa used to use which is santapassword321. Use the password that we get from the ILspy, submit it then we shall get the flag indicates that we already use the correct password.

Day 19 - Web Exploitation - The Naughty or Nice List

Tools used: Kali Linux, Firefox

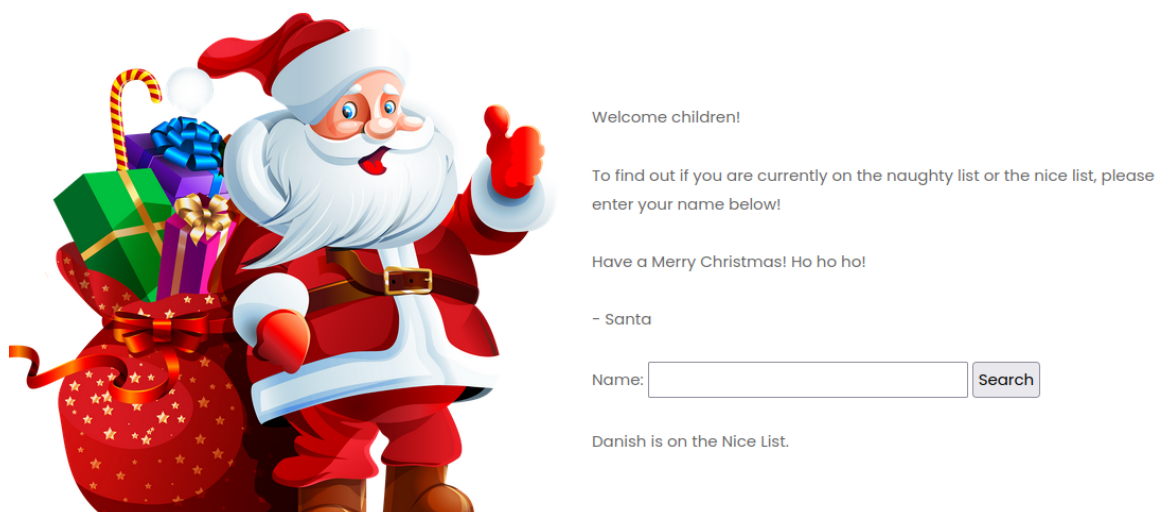
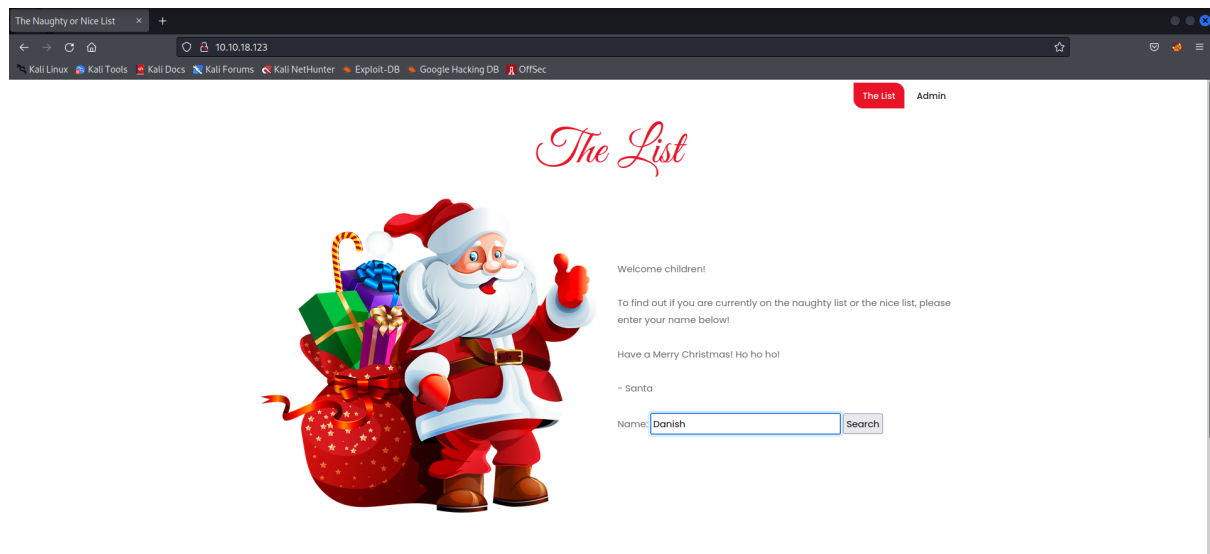
Q1: Which list is this person on?

Answer:

Naughty List - Timothy, JJ, Kanes, Ian Chai

Nice List - YP, Tib3rius

Open Firefox browser and search the IP address of the machine (**10.10.18.123**). The website will appear as below. Search for a random name to see if the website will respond to the names entered.



By the output above, we know that the name 'Danish' is on the Nice List. Then, try again this method to check for Timothy, JJ, YP, Tib3rius, Kanes, Ian Chai.

Name:

Search

Timothy is on the Naughty List.

Name:

Search

JJ is on the Naughty List.

Name:

Search

YP is on the Nice List.

Name:

Search

Tib3rius is on the Nice List.

Name:

Search

Kanes is on the Naughty List.

Name:

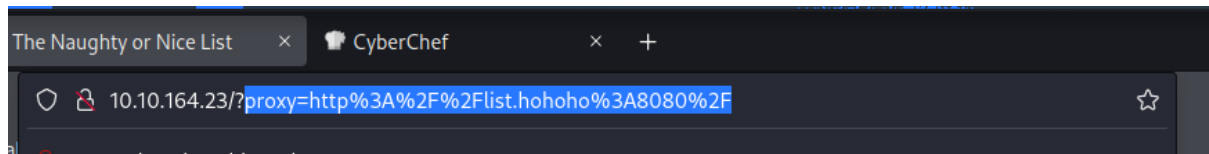
Search

Ian Chai is on the Naughty List.

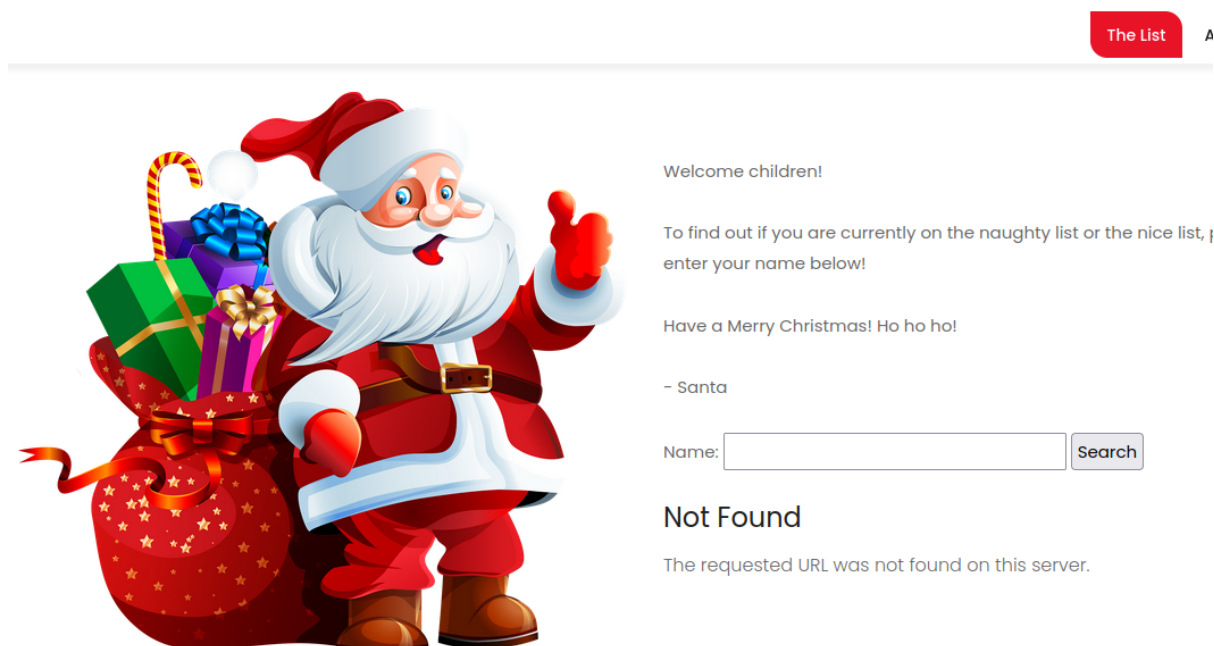
Q2: What is displayed on the page when you use
"/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?

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

Change the url in the search box by changing the proxy value to the
"/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?

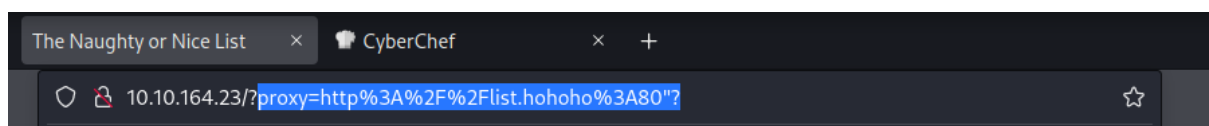


The website will give the result as below.



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
Change the url in the search box by changing the proxy value to the
"/?proxy=http%3A%2F%2Flist.hohoho%3A80"?



The website will give the result as below.



Welcome children!

To find out if you are currently on the naughty list or the nice list, enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

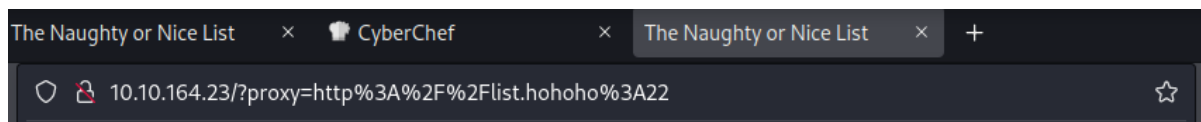
Name:

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

Change the url in the search box by changing the proxy value to the
"/?proxy=http%3A%2F%2Flist.hohoho%3A22"?



The website will give the result as below.



Welcome children!

To find out if you are currently on the naughty list or the nice list, enter your name below!

Have a Merry Christmas! Ho ho ho!

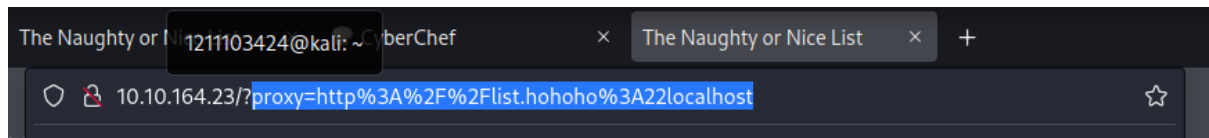
- Santa

Name:

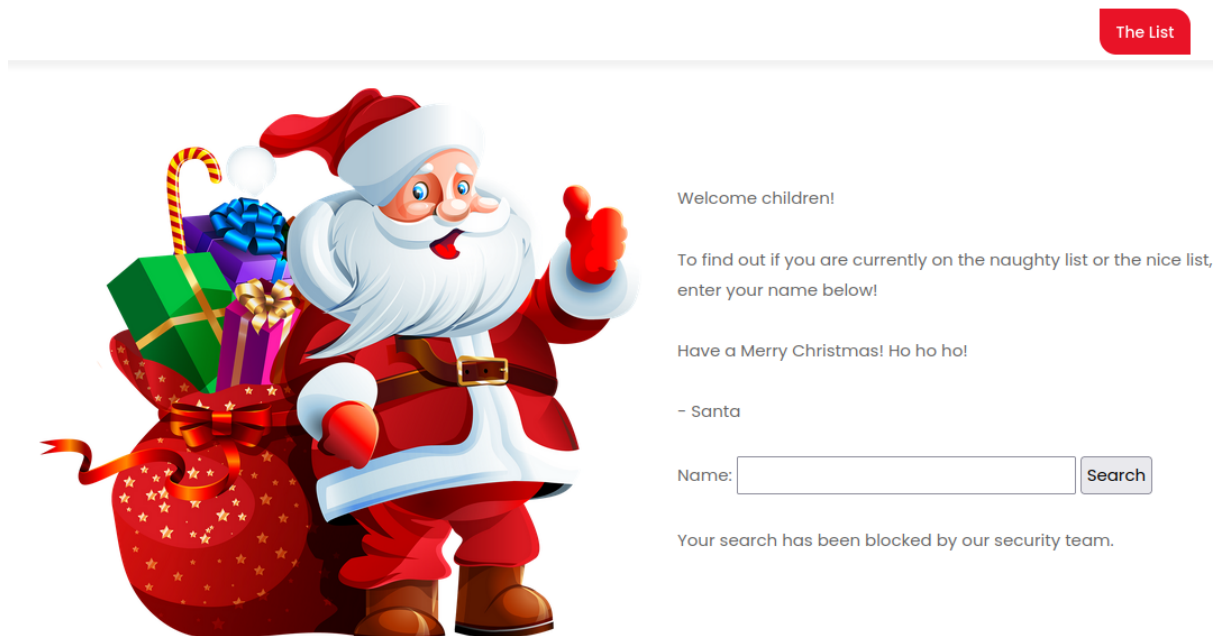
Recv failure: Connection reset by peer

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.
Change the url in the search box by changing the proxy value to the
"/?proxy=http%3A%2F%2Flocalhost"?

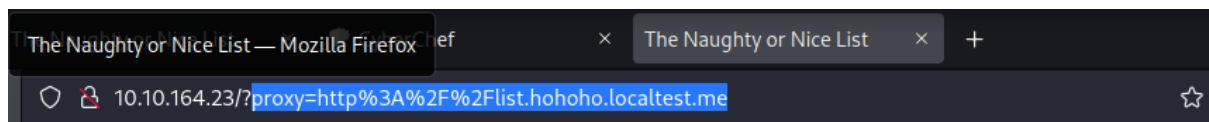


The website will give the result as below.



Q6: What is Santa's password?

Answer: Be good for goodness sake!
Change the url in the search box by changing the proxy value to the
"/?proxy=http%3A%2F%2Flist.hohoho.localtest.me"?



The website will give the result as below.



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:

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

Now, we are given the greetings from Elf Mcskidy and information which is the password of the admin account.

Q7: What is the challenge flag?

Answer: THM{EVERYONE_GETS_PRESENTS}

Go to the admin section at the website then enter the required username(**Santa**) and password(**Be good for goodness sake!**). Log in to the designated location.

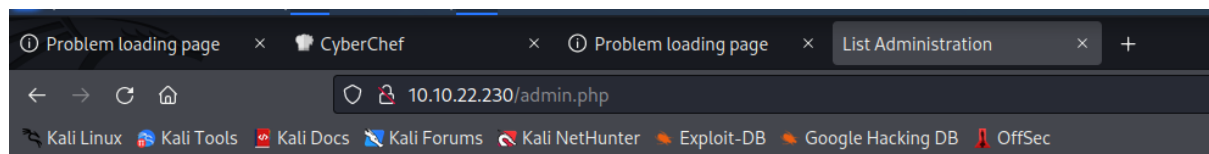
Admin

Username:

Password:

After that, the website will direct us to the admin.php page which contains of List Administration. It also stated that the page is under construction. There is a button

called 'Delete Naughty List' which has the command to delete the naughty list. Click that button.

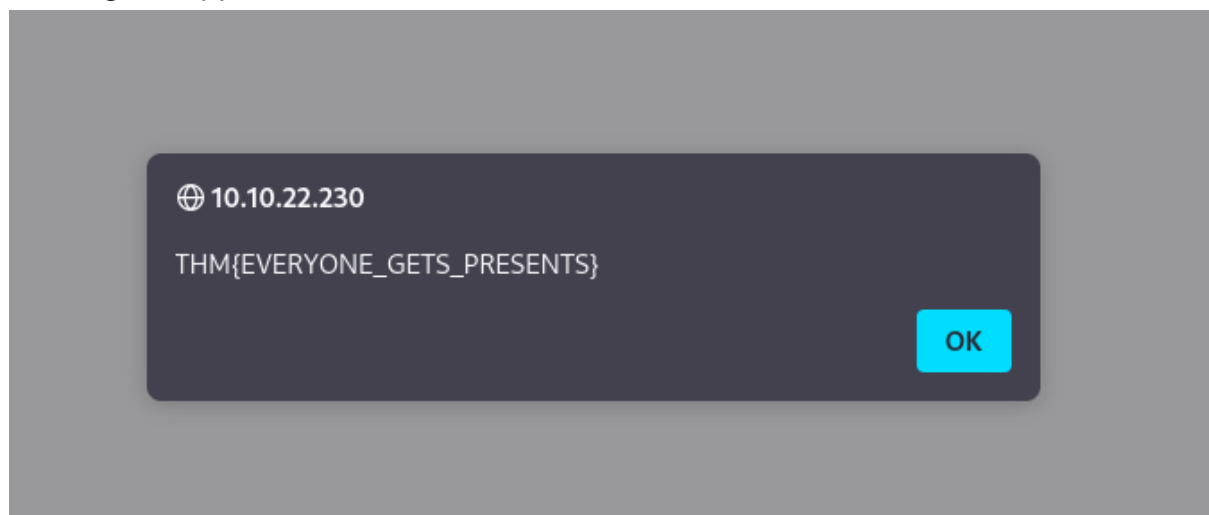


List Administration

This page is currently under construction.

Only press this button when emergency levels of Christmas cheer are needed!

The flag will appeared as below.



Thought / methodology process:

Open Firefox browser and search the IP address of the machine (**10.10.18.123**). The website to check the status of names, either naughty or nice list. Search for names (Timothy, JJ, YP, Tib3rius, Kanes,Ian Chai) to check the name status. Now, we can know the name in which list. After that, change the url in the search box by changing the proxy value to the **"/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?**. This output will appear - The requested URL was not found on this server. Change the url in the search box by changing the proxy value to the **"/?proxy=http%3A%2F%2Flist.hohoho%3A80"?**. This output will appear - Failed to connect to list.hohoho port 80: Connection refused. Change the url in the search box by changing the proxy value to the **"/?proxy=http%3A%2F%2Flist.hohoho%3A22"?**. The output will appear - Recv failure: Connection reset by peer. Change the url in the search box by changing the proxy value to the **"/?proxy=http%3A%2F%2Flocalhost"?**. The output will appear - Your search has been blocked by our security team. Next, Change the url in the search box by changing the proxy value to the **"/?proxy=http%3A%2F%2Flist.hohoho.localtest.me"?**. The website will show the

greeting from Elf Mcskidy to santa. It also tells us the password of the admin account. After that, log in to the admin.php by entering the username (**Santa**) and Password(**Be good for goodness sake!**). We will be directed to the **List Administration** page. Click the 'Delete Naughty List' to delete the names in the naughty list. The flag will that we want will appeared.

Day 20 - Blue Teaming - Powershell to the rescue

Tools used: Kali linux, Firefox

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

Answer: login name

In the terminal, we run the command `ssh -help` to see the command related to the ssh connection. We can see there is `-l` parameter functioned as login name.

```
(kali㉿kali)-[~]  
$ ssh -help  
unknown option -- h  
usage: ssh [-46AaCfGgKkMnqsTtVvXxYy] [-B bind_interface]  
          [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]  
          [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]  
          [-i identity_file] [-J [user@]host[:port]] [-L address]  
          [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]  
          [-Q query_option] [-R address] [-S ctl_path] [-W host:port]  
          [-w local_tun[:remote_tun]] destination [command]
```

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

Connect to the IP address given using SSH command which `ssh -l mceager 10.10.78.104` and then open the powershell by typing the powershell on the command prompt.

```
mceager@ELFSTATION1 C:\Users\mceager>powershell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
PS C:\Users\mceager> █
```

Go to the Documents folder and then search for the hidden file by typing this command `Get-ChildItem -file -Hidden`. We can see one of the files is `e1fone.txt`. But if we search for the unhidden file, we can see that the file is spelled `elfone.txt`. If we run the `cat elfone.txt` command we can see what elf 1 wants which is 2 front teeth.

```

PS C:\Users\mceager> cd .\Documents\
PS C:\Users\mceager\Documents> Get-ChildItem -file -Hidden
want?

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 elfone.txt

PS C:\Users\mceager\Documents> cat elfone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\Documents>

```

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

Then, we go to the desktop directory. We need to search for the hidden directory. We run the same command as before but change the -file to the -Directory. The full command is `Get-ChildItem -Directory -Hidden`. We can see there is elf2wo folder. As we go deeper into that folder, we can see there is also a text file. We see the contents of the file by run the cat command on that file. The movie is Scrooged.

```

PS C:\Users\mceager\Documents> cd..
PS C:\Users\mceager> cd .\Desktop\
PS C:\Users\mceager\Desktop> Get-ChildItem -Directory -hidden

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> ls

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>

```

Q4: Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder? (This command will take a while)

Answer: 3lfthr3e

Go to the Windows\System32 folder since there is where windows file stored. We need to use -Filter command in order to find for the hidden folder because there is too many folder in that folder. The full command that we use is `Get-ChildItem -Hidden -Filter "*3*"`

```
mceager@ELFSTATION1 C:\Users\mceager>cd C:\Windows
mceager@ELFSTATION1 C:\Windows>cd system32
mceager@ELFSTATION1 C:\Windows\System32>
```

```
PS C:\Windows\System32> Get-ChildItem -Hidden -Filter "*3*"

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

We find for the hidden file in that folder. We found there is 1.txt and 2.txt file within it. We need to find the number of words in the first file. To find it, we run the command `Get-Content -Path 1.txt | Measure-Object -Word` command then we can see there is 9999 words in there.

```
PS C:\Windows\System32> cd .\3lfthr3e\  
PS C:\Windows\System32\3lfthr3e> ls  
PS C:\Windows\System32\3lfthr3e> Get-ChildItem -Hidden  
  
Directory: C:\Windows\System32\3lfthr3e  
  
Mode                LastWriteTime         Length Name  
----                -  
-arh--            11/17/2020  10:58 AM           85887 1.txt  
-arh--            11/23/2020   3:26 PM        12061168 2.txt  
  
PS C:\Windows\System32\3lfthr3e> Get-Content -Path 1.txt | Measure-Object -Words  
rdn to the Administrator's desktop.  
  
Lines Words Characters Property  
-----  
9999
```

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

Answer: Red Ryder

To find the exact words on the particular index given, we run this command `(Get-Content -Path 1.txt)[551,6991]` and we got the answer for both index.

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

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? (use spaces when submitting the answer)

Answer: red ryder bbgun

To get the full answer in second file., we run the following command `Get-Content -Path 2.txt | Select-String -Pattern 'redryder'`. Then, we can see the answer.

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

Thought / methodology process:

Firstly, we connect to the mceager account through SSH by using `ssh -l mceager 10.10.78.104` command. Then we open the powershell on that account by typing the powershell on the command prompt. Go to the Documents folder by typing `cd .\Documents\` and then search for the hidden file by typing this command

`Get-ChildItem -file -Hidden`. `Get-ChildItem` command works same as `ls` command on linux but it is used on powershell with many other option such as we did which is to find the hidden file using the `-file` and `-Hidden` parameter on the command. We can see one of the file is `elfone.txt`. But if we search for the unhidden file, we can see that the file is spelled `elfone.txt`. If we run the `cat elfone.txt` command we can see what elf 1 want which is 2 front teeth. Then, we go to the desktop directory. We need to search for the hidden directory. We run the same command as before but change the `-file` to the `-Directory`. The full command is `Get-ChildItem -Directory -Hidden`. In this case, it is the same as the one we used on the previous command which is to find the hidden file, but this time we change the parameter to the `-Directory` instead because we want to find the hidden directory. We can see there is `elf2wo` folder. As we go deeper into that folder, we can see there is also a text file. We see the contents of the file by run the `cat` command on that file. The movie is `Scrooged`. Then, we go to the `Windows\System32` using the `cd C:\windows\system32` command since `system32` is the folder that contains information about windows OS. We need to use `-Filter` command in order to find for the hidden folder because there is too many folder in that folder. The full command that we use is `Get-ChildItem -Hidden -Filter "*3*"`. The filter parameter used to find all the folder that contains character "3" in it since we want to find the file for elf3. As the previous folder for elf 1 and elf 2, their folder must have character 1 and 2 indicated their own file. Then, we found the folder named `3lfthr3e`. In that folder, we find for the hidden file in that folder using the `Get-ChildItem -Hidden` command. We found there is `1.txt` and `2.txt` file within it. We need to find the number of words in the first file. To find it, we run the command `Get-Content -Path 1.txt | Measure-Object -Word` command then we can see there is 9999 words in there. We can pipe the result to find the specific result as we did to find the number of words in the `1.txt` file. To find the exact words on the particular index given, we run this command `(Get-Content -Path 1.txt)[551,6991]` and we got the answer for both index. We provide the index to get the exact string on that particular index.

To get the full answer in second file., we run the following command `Get-Content -Path 2.txt | Select-String -Pattern 'redryder'`. Then, we can see the answer which is `red ryder bbgun`. For this time, we use the `Select-String` command to find the particular things that we want. For this task we want to find the word `redryder` from the previous file. That is why we use the `Select-String` command followed by the `-Pattern` parameter to specify the patter that we want which is `redryder`.