

# PSP0201

## Week 5

## Write Up

Group name: Code Blu

ID	Name	Role
1211103236	Tang Yu Xuan	Leader
1211102879	Koh Jia Jie	Member
1211101196	Tan Hui Jeen	Member
1211100571	Teh Yvonne	Member

## Day 16: Help! Where is Santa?

Tools Used: Kali Linux

Solution / Walkthrough:

Question 1: What is the port number for the web server?

In the terminal, we use nmap to scan the network with the ‘-v’ tag (verbose mode) and the given ip address (10.10.5.107) to check for the port number. Here, we are able to find that the port number for the web server is **80**.

```
kali㉿kali:[~]
$ nmap -v 10.10.5.107
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-07 02:29 EDT
Initiating Ping Scan at 02:29
Scanning 10.10.5.107 [2 ports]
Completed Ping Scan at 02:29, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:29
Completed Parallel DNS resolution of 1 host. at 02:29, 0.01s elapsed
Initiating Connect Scan at 02:29
Scanning 10.10.5.107 [1000 ports]
Discovered open port 22/tcp on 10.10.5.107
Discovered open port 80/tcp on 10.10.5.107
Increasing send delay for 10.10.5.107 from 0 to 5 due to max_successful_tryno
increase to 4
Increasing send delay for 10.10.5.107 from 5 to 10 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.10.5.107 from 10 to 20 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 10.10.5.107 from 20 to 40 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.10.5.107 from 40 to 80 due to max_successful_tryno
increase to 5
Completed Connect Scan at 02:30, 61.12s elapsed (1000 total ports)
Nmap scan report for 10.10.5.107
Host is up (0.19s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 61.40 seconds
[~] $
```

Question 2: Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)

After entering the webpage: 10.10.5.107:80, we are able to view the source code and look for the directory for the API , which is /api/ as seen below.

```
<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>
```

Question 3: Where is Santa right now?

After typing in the below codes in Python, specifying the range of API keys is between 1 to 100 and is an odd number, we are able to find the location of Santa: **Winter Wonderland, Hyde Park, London**.

```
#!/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://10.10.5.107:80/api/{api_key}')
    print(html.text)
```

```
api_key 45
{"item_id":45,"q":"Error. Key not valid!"}
api_key 47
{"item_id":47,"q":"Error. Key not valid!"}
api_key 49
{"item_id":49,"q":"Error. Key not valid!"}
api_key 51
{"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
```

Question 4: 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 (10.10.14.113)

We are also able to identify the API key is **57** after finding Santa's location.

```
api_key 45
{"item_id":45,"q":"Error. Key not valid!"}
api_key 47
{"item_id":47,"q":"Error. Key not valid!"}
api_key 49
{"item_id":49,"q":"Error. Key not valid!"}
api_key 51
{"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
```

### Through process/ methodology:

Firstly, we typed in “nmap -v 10.10.5.107” to find the port number for the web server. After running it successfully, we are able to enter the webpage with the port number, “10.10.5.107:80”. Here, we found the directory for the API by right clicking to view source code or by using Python with Libraries which was learnt on day 15. Next, we found Santa’s

location using Python by specifying the range of API keys is from 1 to 100 and it is an odd number. Lastly, the API key was shown when we searched for Santa's location.

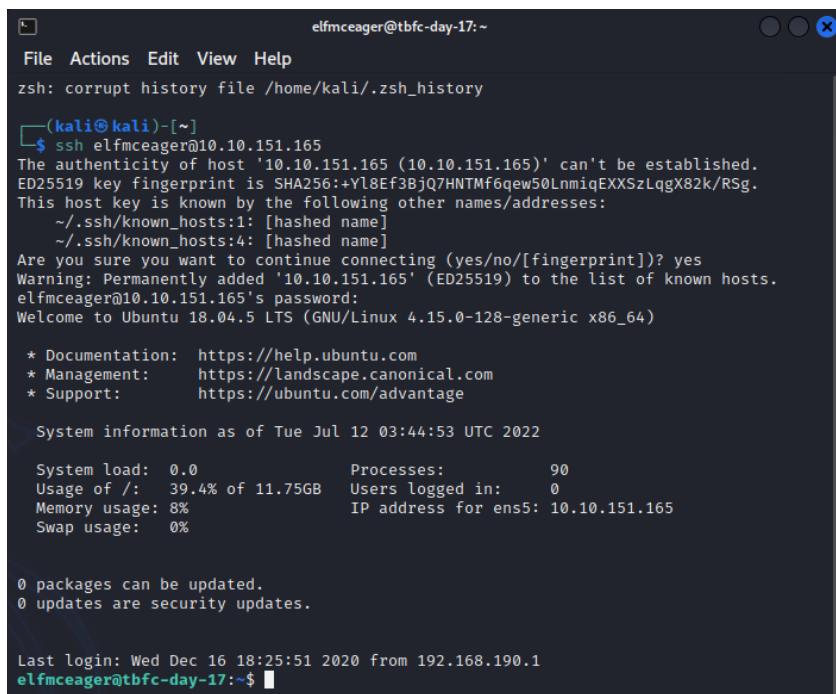
## Day 17: ReverseELFneering

Tools Used: Kali Linux

Solution / Walkthrough:

Question 1: What is the value of local\_ch when its corresponding movl instruction is called (first if multiple)?

Using ssh and the password given (adventofcyber), we logged in as elfmceager. We were able to see the folder “challenge1” and ran the following command to open the binary in debugging mode. After this, we used “aa” to analyse the program. To find a list of the functions, we ran the command “afl | grep main”. Then, we examine the assembly code at main by running the command “pdf @main”. From here, we are able to see that the value **1** is copied into local\_ch.



```
elfmceager@tbfc-day-17:~$ 
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history

└─(kali㉿kali)-[~]
$ ssh elfmceager@10.10.151.165
The authenticity of host '10.10.151.165 (10.10.151.165)' can't be established.
ED25519 key fingerprint is SHA256:+Yl8Ef3BjQ7HNTMf6qew50LnmiqEXXSzLqgX82k/RSg.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.151.165' (ED25519) to the list of known hosts.
elfmceager@10.10.151.165's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-128-generic x86_64)

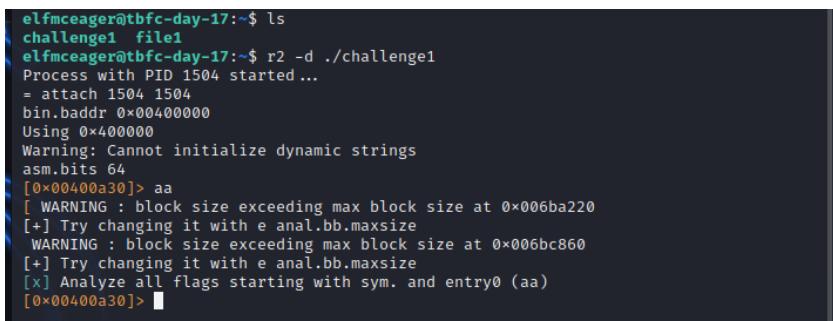
 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Tue Jul 12 03:44:53 UTC 2022

System load: 0.0          Processes:      90
Usage of /: 39.4% of 11.75GB   Users logged in:    0
Memory usage: 8%           IP address for ens5: 10.10.151.165
Swap usage:  0%

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

Last login: Wed Dec 16 18:25:51 2020 from 192.168.190.1
elfmceager@tbfc-day-17:~$
```



```
elfmceager@tbfc-day-17:~$ ls
challenge1
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1504 started ...
= attach 1504 1504
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[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)
[0x00400a30]>
```

```
[0x00400a30]> afl | grep main
0x00400b4d 1 35      sym.main
0x00400de0 10 1007 → 219 sym._libc_start_main
0x00403840 39 661 → 629 sym._nl_find_domain
0x00403ae0 308 5366 → 5301 sym._nl_load_domain
0x00415ef0 1 43      sym._IO_switch_to_main_get_area
0x0044ce10 1 8       sym._dl_get_dl_main_map
0x00470430 1 49      sym._IO_switch_to_main_wget_area
0x0048f9f0 7 73 → 69 sym._nl_finidomain_subfreeres
0x0048fa40 16 247 → 237 sym._nl_unload_domain
[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]
```

### Question 2: What is the value of eax when the imull instruction is called?

The value 6 is copied into local\_8h. Next, the value in local\_ch, 1 is copied into eax. We are able to obtain the value of eax by multiplying the value in local\_8h with eax, which is 6 multiplied by 1, hence eax has the value **6** now.

```
[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]
```

### Question 3: What is the value of local\_4h before eax is set to 0?

The value in eax, **6** is copied to local\_4h.

```
[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
[0x00400a30]>
```

### Through process/ methodology:

After logging in to elfmceager with the password given (adventofcyber), we can open the binary in debugging mode of the folder “challenge1” and analyse the program. After the analysis is done, we found the functions containing “main”. Lastly, by using “pdf @main” we are able to examine the assembly code.

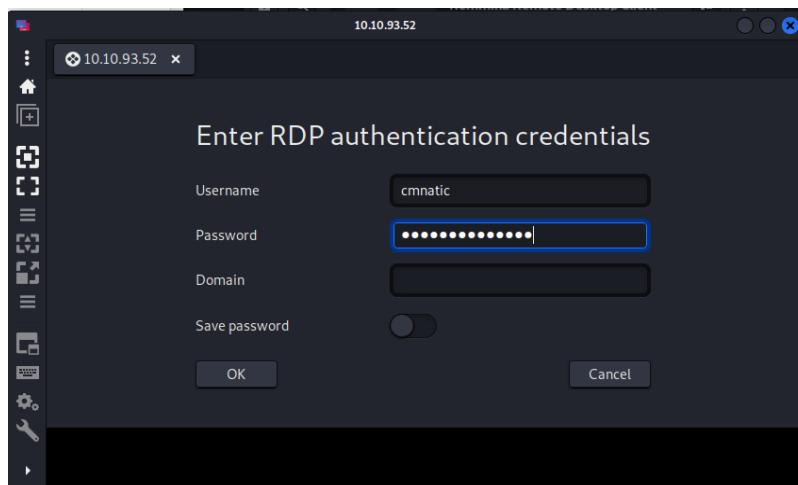
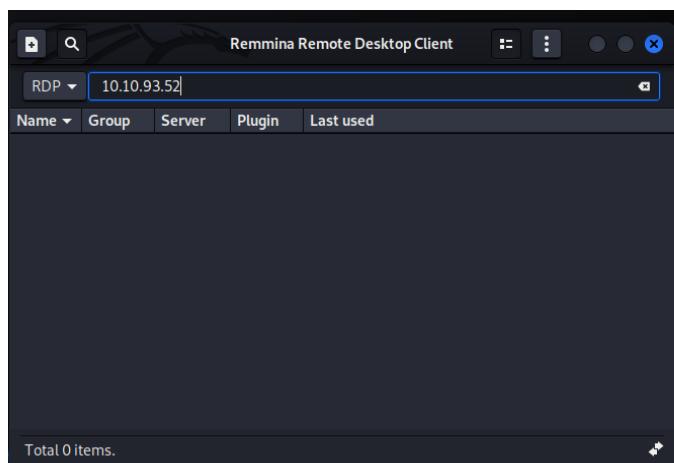
## Day 18: The Bits of Christmas

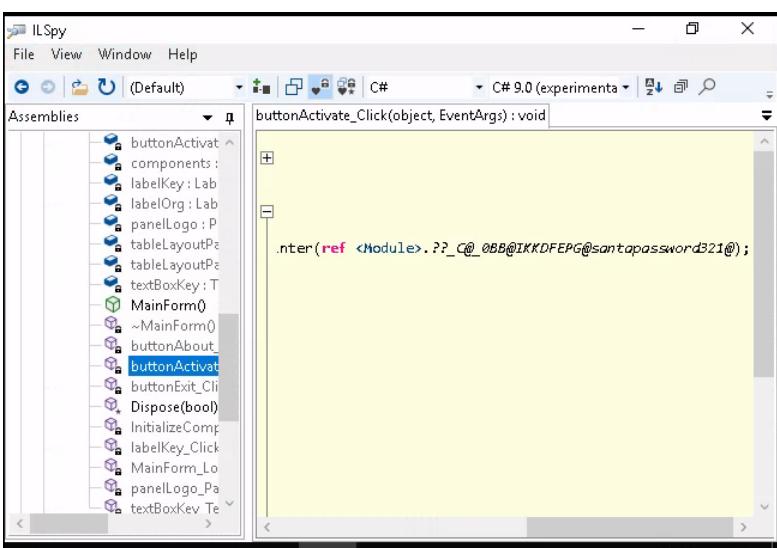
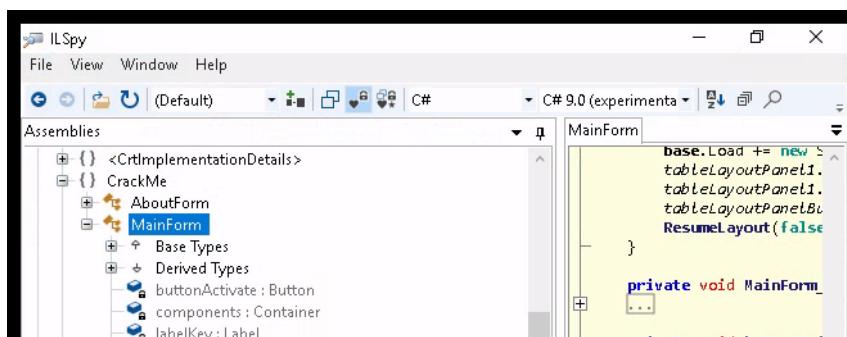
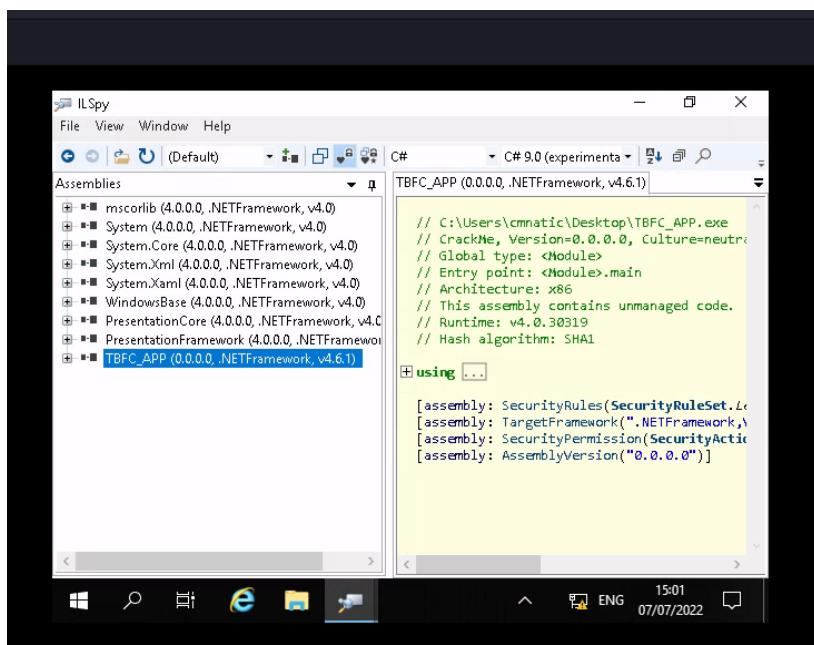
**Tools Used:** Kali Linux, Remmina, ILSpy

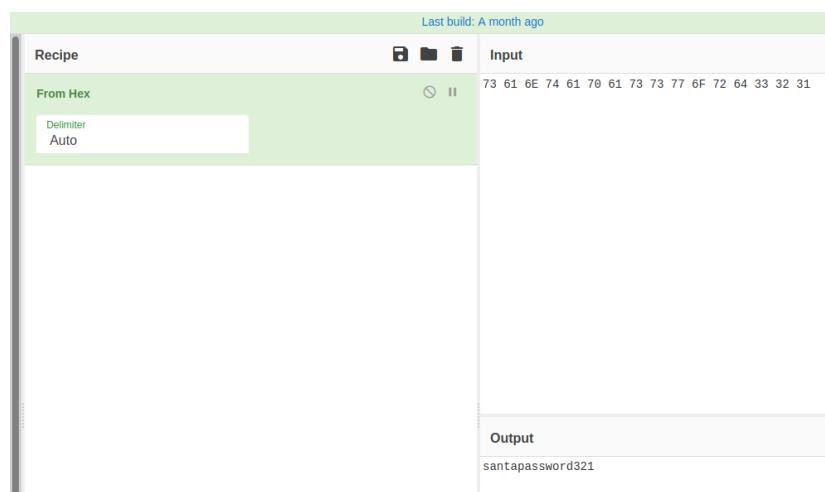
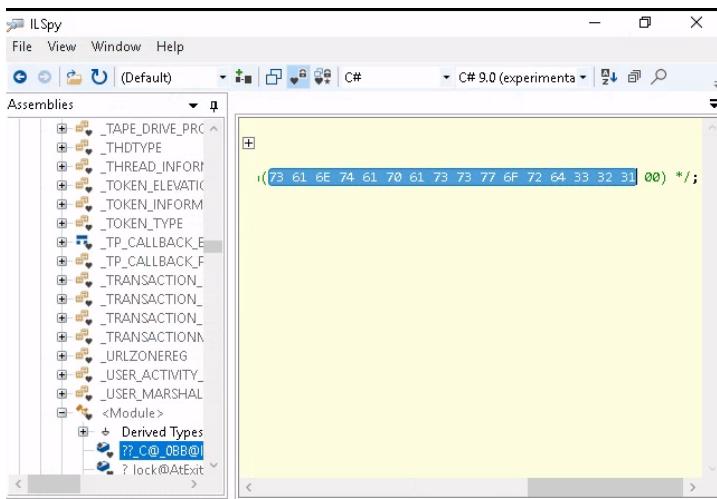
Solution / Walkthrough:

### Question 1: What is Santa's password?

Using Remmina, we type in the IP address given into the RDP. A pop up screen will appear asking for the username: “cmnatic” and the password: “Adventofcyber!”. After clicking ILSpy, we opened TBFC\_APP from the Desktop. From here, we clicked the “+” button to view more details. We are able to see “CrackMe” and under it, we can see the details of “MainForm”. In the “MainForm”, we clicked into “buttonActivate...” to view it and double clicked into the “santapassword321” and copied the values. We then used Cyberchef to convert the hexadecimal values, which indeed showed Santa’s password to be “santapassword321”.

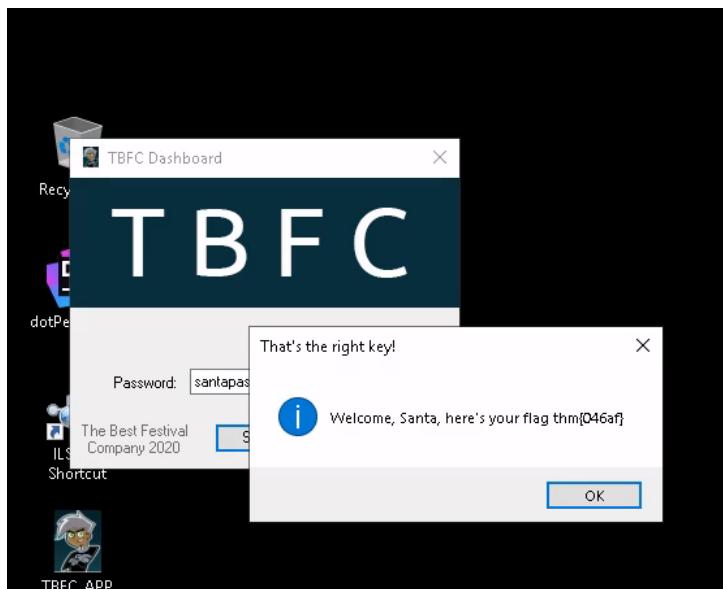






Question 2: Now that you've retrieved this password, try to login...What is the flag?

After knowing the password, we can login to TBFC\_APP to get the flag, which is **thm{046af}**.



**Through process/ methodology:**

Having the password to open Remmina, we are able to open ILSpy from it. We then opened TBFC\_APP in ILSpy. From here, we found “CrackMe” to be unique and clicked on the “+” button. We clicked on “MainForm” and then “buttonActivate...” to view the details in it. In this file, we can see the password was given but was unsure, hence, we double clicked into the password and found hexadecimal values. We then convert them using Cyberchef which shows the password in String. After knowing the password, we are able to successfully login to TBFC\_APP using the password, which then shows us the flag.

## Day 19: The Naughty or Nice List

Tools Used: Kali Linux

Solution / Walkthrough:

Question 1: What is Santa's password?

After entering the website (10.10.196.151), we checked for different ports in order to get Santa's password, such as port 80, 22 and localhost, however, these did not work out. We then tried with "localhost.me". It showed a message with Santa's password, which is "Be good for goodness sake!"

The screenshot shows a Firefox browser window with the title "The Naughty or Nice List". The URL in the address bar is "10.10.196.151/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch". The page content includes a large illustration of Santa Claus carrying a sack of gifts. Text on the page says "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!", and "- Santa". There is a search form with a "Name:" input field and a "Search" button. At the bottom, it says "Tib3rius is on the Nice List.".

The Naughty or Nice List

URL Decode - CyberChef

10.10.196.151/?proxy=http%3A%2F%2Flist.hohoho%3A80%2F

The List Admin

# The List



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

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

The Naughty or Nice List

URL Decode - CyberChef

10.10.196.151/?proxy=http%3A%2F%2Flist.hohoho%3A22%2F

The List Admin

# The List



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

Recv failure: Connection reset by peer

The Naughty or Nice List

URL Decode - CyberChef

10.10.196.151/?proxy=http%3A%2F%2Flocalhost

The List Admin

# The List



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

Your search has been blocked by our security team.

The Naughty or Nice List

URL Decode - CyberChef

10.10.196.151/?proxy=http%3A%2F%2Flist.hohoho.localtest.me

The List Admin

# The List



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

Santa,

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

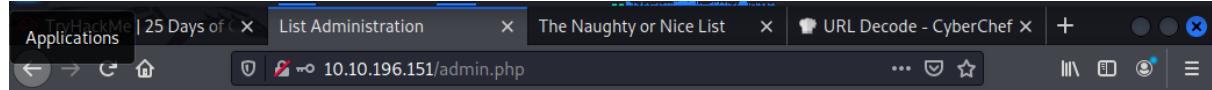
I know you have trouble remembering your password so here it is: Be good for goodness sake!

- Elf McSkidy

## Question 2: What is the challenge flag?

We logged in with the password given and typed in “Santa” as the username. After that, we deleted the naughty list which then displayed the flag:

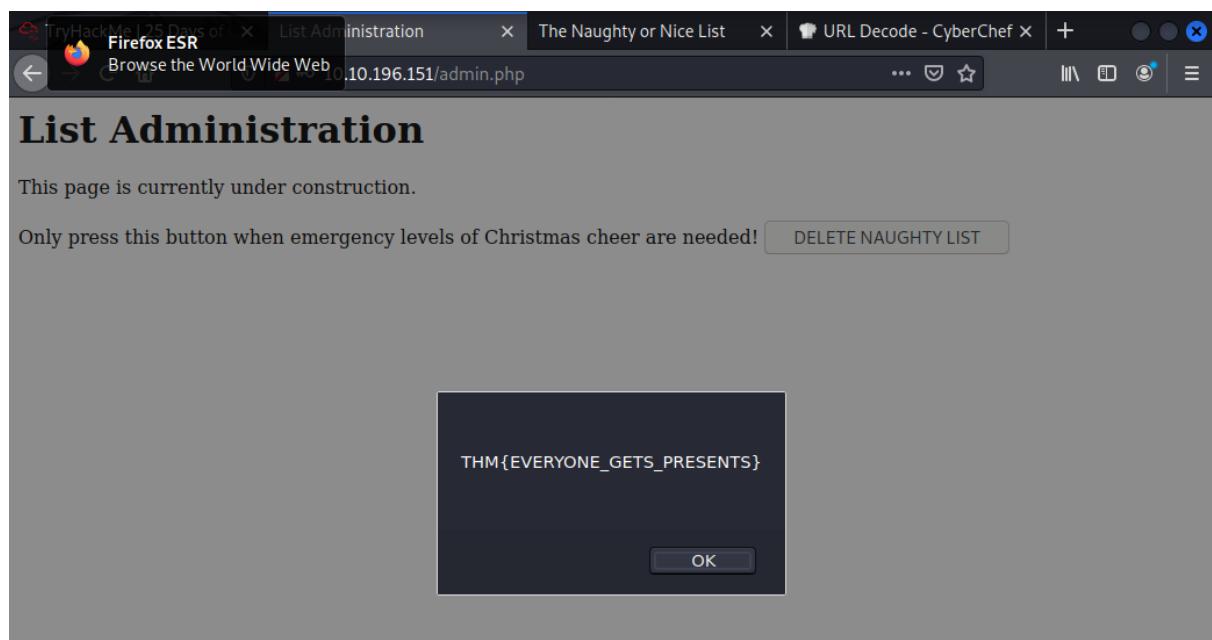
**THM{EVERYONE\_GETS\_PRESENTS}**



## List Administration

This page is currently under construction.

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



## Through process/ methodology:

In the webpage, we changed the port from 8080 to port 80, 22 and localhost. These ports did not work out, hence we tried it with “localtest.me”. This then displayed a message from Mc Skidy and Santa’s password. We logged into the admin page by using Santa as the username and the given password. From here, we were able to delete the naughty list, which then showed us the flag for this task.

## Day 20: Powershell to the rescue

Tools Used: Kali Linux

Solution / Walkthrough:

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

After typing in the following ssh command and password given (r0ckStar!), we typed in “powershell” and navigated to the Documents folder. Then, we used the commands below to find the hidden file. After finding the hidden file, we viewed the contents by using “Get-Content -Path e1fone.txt”, which displayed a message “All I want is my ‘2 front teeth’!!!”.

```
└─(root㉿kali)-[~]
# ssh -l mceager 10.10.188.101
The authenticity of host '10.10.188.101 (10.10.188.101)' can't be established
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.188.101' (ED25519) to the list of known hosts.
mceager@10.10.188.101's password:
└─[mceager@kali ~]#
```

```
c:\windows\system32\cmd.exe - powershell
File Actions Edit View Help
Microsoft Windows [Version 10.0.17763.737] Expires
(c) 2018 Microsoft Corporation. All rights reserved.

mceager@ELFSTATION1 C:\Users\mceager>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
You was left in one of the stockings that hints that the contents have been
PS C:\Users\mceager>
```

```
c:\windows\system32\cmd.exe - powershell
File Actions Edit View Help
IP Address Expires
PS C:\Users\mceager> Get-ChildItem -File -Hidden
Directory: C:\Users\mceager\Documents
Such as how many words are in the file and the exact positions for a particular word
Mode LastWriteTime Length Name
-a-hs- 12/7/2020 10:29 AM 402 desktop.ini
-arh-- 11/18/2020 5:05 PM 35 e1fone.txt
PS C:\Users\mceager>
```

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

Question 2: 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?

We redirected to the Desktop and searched for the hidden folder. In the hidden folder, we were able to find a file and view it, showing a message “I want the movie Scrooged <3!”.

```

PS C:\Users\mceager\Documents> cd ..
PS C:\Users\mceager> Set-Location Desktop          32m 46s
PS C:\Users\mceager\Desktop> ls
PS C:\Users\mceager\Desktop> ls -Hidden

numerical value that is the location of the string within the file. Since in
the Fc Directory: C:\Users\mceager\Desktop at the correct position.

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

```

```

PS C:\Users\mceager\Desktop> cd .\elf2wo\
PS C:\Users\mceager\Desktop\elf2wo> Get-ChildItem
Location -Path c:\users\administrator\desktop will change your lo
Directory: C:\Users\mceager\Desktop\elf2wo

You can use the Set-Location cmdlet.
Mode                LastWriteTime      Length Name
-a----          11/17/2020  10:26 AM          64 e70smsW10Y4k.txt

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

```

### Question 3: Search the Windows directory for a hidden folder that contains files for Elf 3.

#### What is the name of the hidden folder?

We directed to Windows and searched for the hidden folder in System32 by filtering it. To make it easier, we included the “-Hidden -Directory” commands, which then showed “3lfthr3e”.

```

PS C:\Users\mceager\Desktop\elf2wo> cd C:/Windows
PS C:\Windows> cd System32
PS C:\Windows\System32> Get-ChildItem -Filter "*3*"
You can use the Set-Location cmdlet.
Directory: C:\Windows\System32
Location -Path c:\users\administrator\desktop will change your lo
Mode                LastWriteTime      Length Name
-a----          9/15/2018  12:12 AM        659720 advapi32.dll
-a----          9/15/2018  12:13 AM         2560 advapi32res.dll
-a----          9/15/2018  12:12 AM        79872 avicap32.dll
-a----          9/15/2018  12:12 AM       115712 avifil32.dll
-a----          9/15/2018  12:12 AM       293344 cfgmgr32.dll
-a----          9/15/2018  12:12 AM         73728 clfsfw32.dll
-a----          9/15/2018  12:12 AM        37888 cmcfg32.dll
-a----          9/15/2018  12:12 AM       556032 cmdial32.dll
-a----          9/15/2018  12:12 AM         51712 cmdl32.exe
-a----          9/15/2018  12:12 AM        43008 common32.exe

```

```

PS C:\Windows\System32> Get-ChildItem -Hidden -Directory -Filter "*3*"
You can use the Get-Help cmdlet to obtain more information about a specific cmd
Directory: C:\Windows\System32
Mode                LastWriteTime      Length Name
d--h--           11/23/2020   3:26 PM          3lfthr3e

```

### Question 4: How many words does the first file contain?

We viewed the folder and found two hidden files. We then typed in the following commands to get the words count for the first file, which is 9999.

```

PS C:\Windows\System32> cd 3lfthr3e
PS C:\Windows\System32\3lfthr3e> Get-ChildItem -Hidden
You can use the Get-Help cmdlet to obtain more information about a specific cmdlet.
  Directory: C:\Windows\System32\3lfthr3e

Mode                LastWriteTime         Length Name
-->---->           11/17/2020 10:58 AM      85887 1.txt
-->---->           11/23/2020 3:26 PM     12061168 2.txt

hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Measure-Object -Word
Lines Words Characters Property
----- ----- ----- -----
9999
hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

```

### Question 5: What 2 words are at index 551 and 6991 in the first file?

To get the words in the respective indexes, we typed in the commands below, which displayed “**Red**” at index 551 and “**Ryder**” at index 6991.

```

PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[551]
Red
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[6991]
Ryder
story for a hidden folder that contains files for Elf 3. What does Elf 3 want?
PS C:\Windows\System32\3lfthr3e>

```

### Question 6: 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?

We used the command below to search for the particular file by including “redryder”. It then displayed **red ryder bb gun**.

```

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

```

### Through process/ methodology:

We first typed in the ssh command and the password. After gaining access, we launched powershell and directed it to Documents. In the Documents, we searched for the hidden file and viewed the contents which displayed a message saying Elf 1 wants its 2 front teeth. Next, we directed to Desktop to search for the hidden folder and viewed the file in it, showing a message about Elf 2 wanting the movie Scrooged. Lastly, we directed to Windows, then to System32. We searched for the hidden folder by filtering it, including a string that contains “3”. After finding the hidden folder, we got the words count for the first hidden file. In this file, we were able to know the words on index 551 and 6991. The next step was to find the phrase from the second hidden file. We simplified the searching process which then displayed the phrase.