

# PSP0201

## Week 5

# Report

Group Name : Cipher

Members :

ID	Name	Role
1211103064	MUHAMAD AIMAN BIN MOHD EHWAL	Leader
1211103085	MUHAMMAD FARID BIN JAYATAN	Member
1211103373	MUHAMMAD ALIF BIN KHABALI	Member
1211103451	ARIF MUHRIZ BIN SYAMSUL FOZY	Member

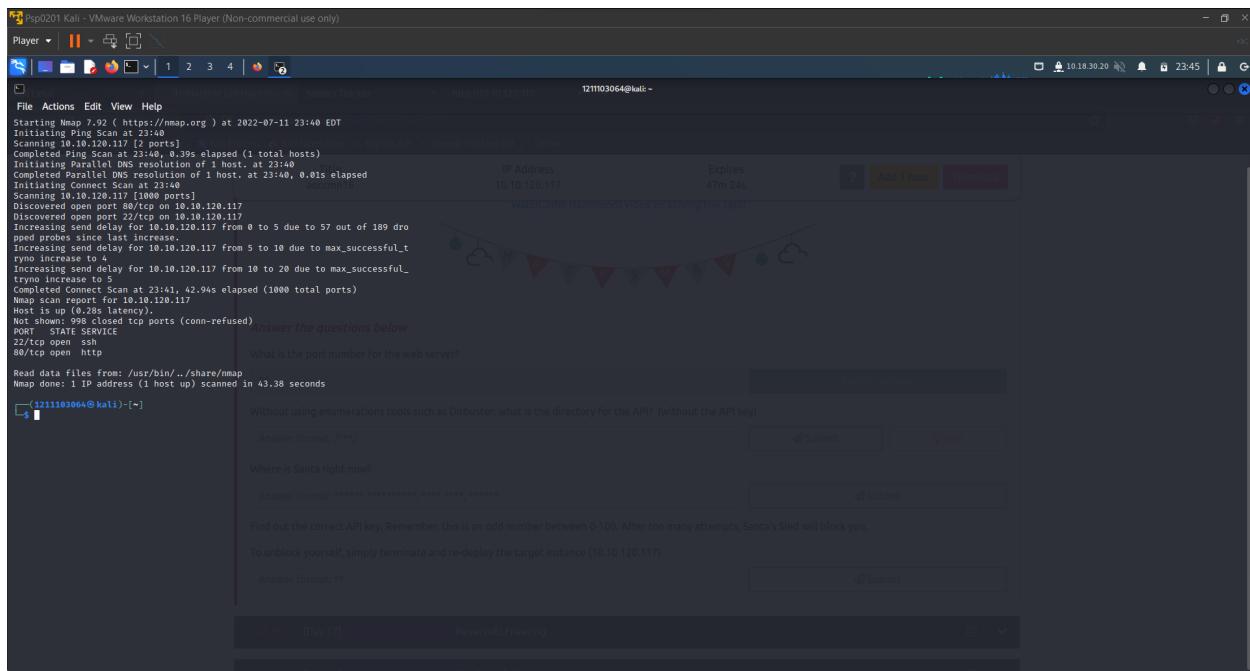
# Day 16 : Help! Where is Santa?

**Tool Used :** Kali Linux, Firefox, Attackbox, Sublime Text, Nmap, Python3

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

**Answer : 80**

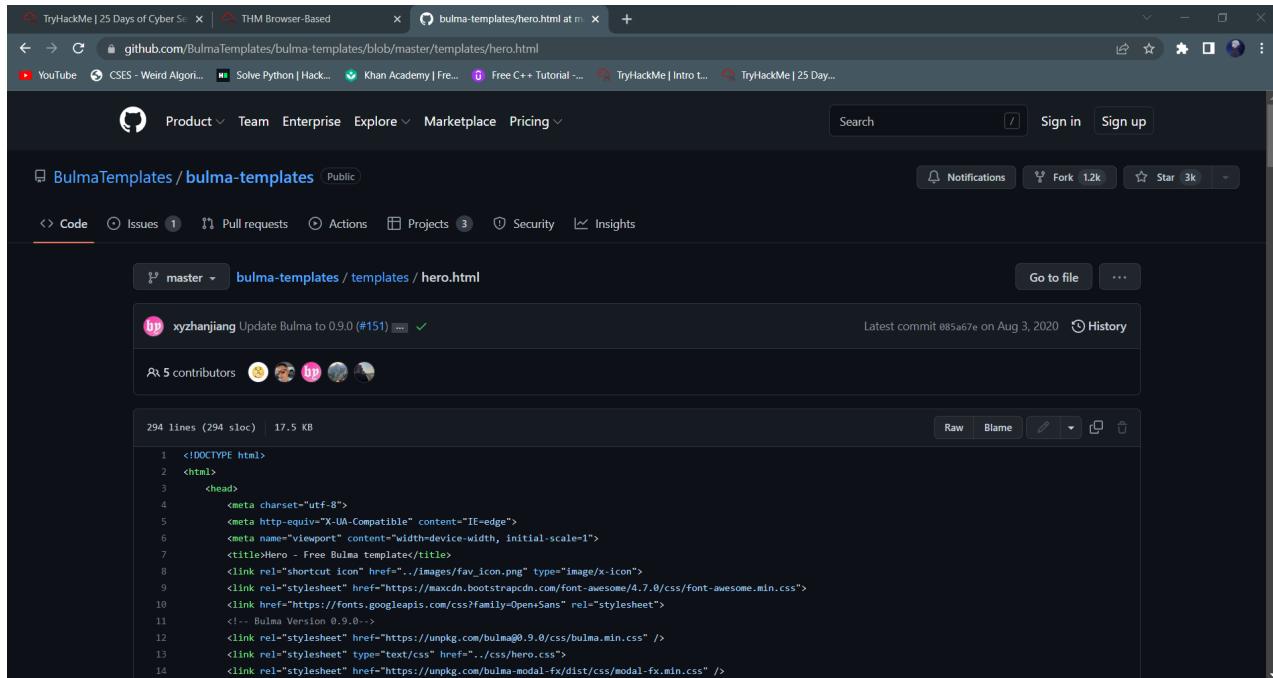
We got the answer by using nmap to scan the MACHINE\_IP and got the information that we need from it.



```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-11 23:40 EDT
[...]
Completed Ping Scan at 23:40, 0.3% elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 23:40
Completed Parallel DNS resolution of 1 host at 23:40, 0.01s elapsed
Initiating Connect Scan at 23:40
Scanning 10.10.120.117 [1000 ports]
Discovered open port 80/tcp on 10.10.120.117
Discovered closed port 22/tcp on 10.10.120.117
Increasing send delay for 10.10.120.117 from 0 to 5 due to 57 out of 189 dropped probes since last increase.
Increasing send delay for 10.10.120.117 from 5 to 10 due to max_successful_tries increased to 4.
Increasing send delay for 10.10.120.117 from 10 to 20 due to max_successful_tries increased to 10.
Completed Connect Scan at 23:41, 42.94s elapsed (1000 total ports)
Nmap scan report for 10.10.120.117
Host is up (0.28s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 43.38 seconds
[211103064@kali:~]
```

## Question 2 : What templates are being used?

### Answer : Bulma

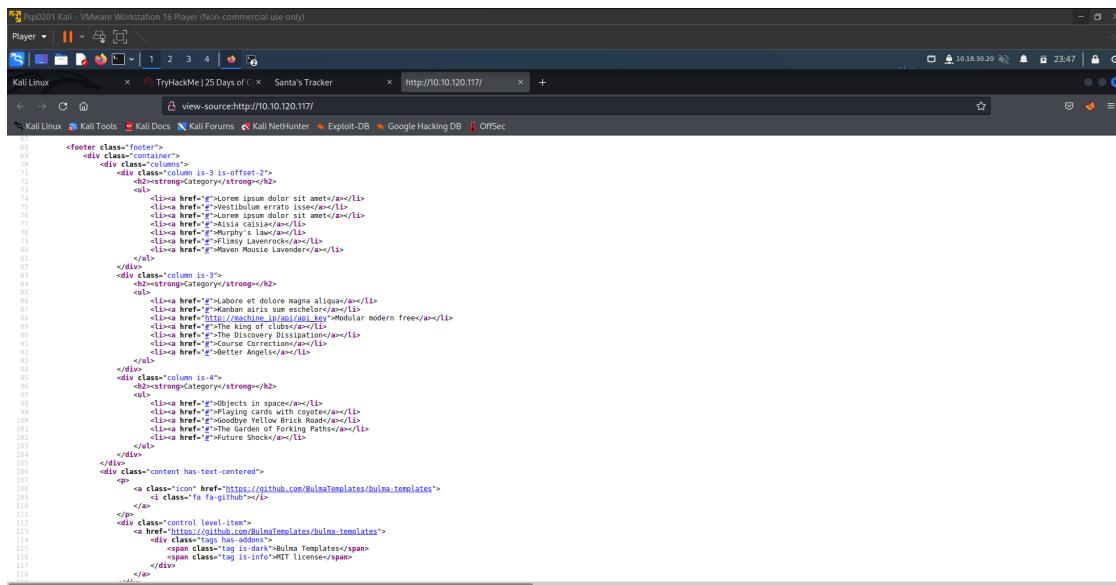


The screenshot shows a GitHub repository page for 'bulma-templates/bulma-templates'. The file 'hero.html' is displayed, containing the following code:

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta charset="utf-8">
5     <meta http-equiv="X-UA-Compatible" content="IE=edge">
6     <meta name="viewport" content="width=device-width, initial-scale=1">
7     <title>Hero - Free Bulma template</title>
8     <link rel="shortcut icon" href="../images/fav_icon.png" type="image/x-icon">
9     <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css">
10    <link href="https://fonts.googleapis.com/css?family=Open+Sans" rel="stylesheet">
11    <!-- Bulma Version 0.9.0 -->
12    <link rel="stylesheet" href="https://unpkg.com/bulma@0.9.0/css/bulma.min.css" />
13    <link rel="stylesheet" type="text/css" href="..css/hero.css">
14    <link rel="stylesheet" href="https://unpkg.com/bulma-modal-fx/dist/css/modal-fx.min.css" />
```

## Question 3 : Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)

### Answer : /api/

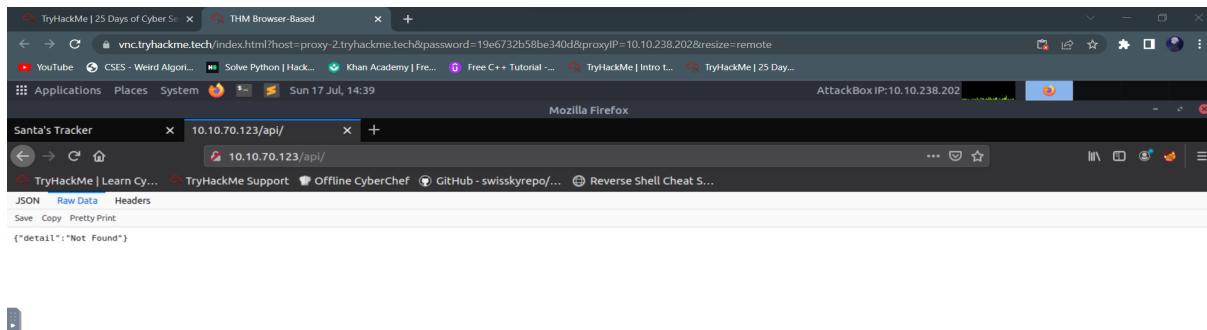


The screenshot shows a terminal window on Kali Linux displaying the source code of a webpage at <http://10.10.120.117/>. The code includes the following links:

- [Santa's Tracker](#)
- [Murphy's Law](#)
- [Tinley Lavenderock](#)
- [Maven Mouse Lavenderock](#)
- [Westbulium errato isse](#)
- [Lore ipsum dolor sit amet](#)
- [The King of clubs](#)
- [Course Correction](#)
- [Better Angels](#)
- [Labore et nisi magna aliqua](#)
- [Modular modern free](#)
- [The Garden of Forking Paths](#)
- [Future Shock](#)

**Question 4 :** Go to the API endpoint. What is the Raw Data returned if no parameters are entered?

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



**Question 5 :** Where is Santa right now?

**Answer :** Winter Wonderland, Hyde Park, London

A screenshot showing a web browser and a Sublime Text code editor side-by-side. The browser window on the left displays a challenge page from TryHackMe. It includes a list of tasks, a note about deploying the machine, a video link, and a question asking for the port number. A red box highlights the answer '80'. Below the browser is a form for the question 'Where is Santa right now?' with an input field containing '/api/' and a 'Submit' button. The Sublime Text editor on the right shows a Python script named 'santalocation.py' with the following code:

```
import requests
for api_key in range(1,100,2):
    print(f"api key {api_key}")
    html = requests.get(f"http://10.10.120.117:88/api/{api_key}")
    print(html.text)
```

The status bar at the bottom of the Sublime Text window shows 'AttackBox IP:10.10.146.86'.

Santa's Sled has an API we can talk too. The key for the API is between 0 and 100, and it's an odd number. But be careful! After an unknown number of attempts, Santa's Sled will ban your IP address.

Deploy the machine that is running Santa's Sled and allow a couple of minutes for the target (10.10.120.117) to start up. Using your Python skills from Day 15 to find the correct key for the API.

[Watch John Hammonds video on solving this task!](#)

**Answer the questions below**

What is the port number for the web server?

[Correct Answer](#)

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

[Correct Answer](#) [Hint](#)

Where is Santa right now?

[Submit](#)

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.

**Question 6 : 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 (MACHINE\_IP)**

## Answer : 57

Santa's Sled has an API we can talk too. The key for the API is between 0 and 100, and it's an odd number. But be careful! After an unknown number of attempts, Santa's Sled will ban your IP address.

Deploy the machine that is running Santa's Sled and allow a couple of minutes for the target (10.10.120.117) to start up. Using your Python skills from Day 15 to find the correct key for the API.

[Watch John Hammonds video on solving this task!](#)

**Answer the questions below**

What is the port number for the web server?

[Correct Answer](#)

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

[Correct Answer](#) [Hint](#)

Where is Santa right now?

[Submit](#)

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.

Santa's Sled has an API we can talk too. The key for the API is between 0 and 100, and it's an odd number. But be careful! After an unknown number of attempts, Santa's Sled will ban your IP address.

Deploy the machine that is running Santa's Sled and allow a couple of minutes for the target (10.10.120.117) to start up. Using your Python skills from Day 15 to find the correct key for the API.

[Watch John Hammonds video on solving this task!](#)

**Answer the questions below**

What is the port number for the web server?

[Correct Answer](#)

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

[Correct Answer](#) [Hint](#)

Where is Santa right now?

[Submit](#)

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.

File Edit View Search Terminal Help  
 {"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  
 {"item\_id":63,"q":"Error. Key not valid!"}  
 api\_key 65  
 {"item\_id":65,"q":"Error. Key not valid!"}  
 api\_key 67  
 {"item\_id":67,"q":"Error. Key not valid!"}  
 api\_key 69  
 {"item\_id":69,"q":"Error. Key not valid!"}  
 api\_key 71

Category  
 Lorem ipsum dolor sit amet

root@lp-10-10-146-86:~

THM AttackBox 41m 21s

## Thought Process / Methodology :

Firstly, we used **nmap** to get the port number for the web server and then we visited the website by using the **MACHINE\_IP:80** (80 is the port number) to get the name of the templates that are being used on the webpage. We figured out the directory of the API by using the **view page source** and without using any enumerations tools. After that, we simply go to the API endpoint of the website to see the Raw Data returned if no parameters are entered and we saw that the Raw Data returned **{"detail": "Not Found"}**. Lastly, we used some simple coding to get the answers for both question 5 and 6.

## Day 17 : ReverseELFneering

**Tool Used :** Kali Linux, Firefox, Attackbox,

**Question 1 :** Match the data type with the size in bytes:

**Answer :**

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

**Answer :**

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

**Question 3 :** What is the command to set a breakpoint in radare2?

**Answer :**

A breakpoint specifies where the program should stop executing. This is useful as it allows us to look at the state of the program at that particular point. So let's set a breakpoint using the command db in this case, it would be db 0x00400b55 To ensure the breakpoint is set, we run the pdf @main command again and see a little b next to the instruction we want to stop at.

**Question 4 :** What is the command to execute the program until we hit a breakpoint?

**Answer :**

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 the `mov` instruction is used to transfer values. This statement is

**Question 5 :** What is the value of `local_ch` when its corresponding `movl` instruction is called (first if multiple)?

**Answer :**

```
(kali㉿kali)-[~]
$ ssh elfmceager@10.10.94.22
The authenticity of host '10.10.94.22 (10.10.94.22)' 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:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.94.22' (ED25519) to the list of known hosts.
elfmceager@10.10.94.22'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 Sun Jul 17 12:52:22 UTC 2022
System load:  0.0          Processes:      92
Usage of /:   39.4% of 11.756GB  Users logged in:  0
Memory usage: 8%           IP address for ens5: 10.10.94.22
Swap usage:   0%
0 packages can be updated.
0 updates are security updates.

When we examine the contents of
This is the file used as an example
you have not read through this and

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

The other is called **challenge1** and

```
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1564 started...
= attach 1564
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]> 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_fnddomain_subfreeres
0x0048fa40    16 247  → 237 sym._nl_unload_domain
```

```
[0x00400a30]> db 0x00400b5f
[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 b 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]> dc
hit breakpoint at: 400b5f
[0x00400b5f]> px @ rbp-0xc
- offset - 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0x7ffd370a5464 0100 0000 0600 0000 0000 0000 4018 4000 .....@. 6 7 8 9 A B C D E F
0x7ffd370a5474 0000 0000 e910 4000 0000 0000 0000 0a37 .....@. 0000 0000 0000 4018 4000
0x7ffd370a5484 0000 0000 0000 0100 0000 9855 0a37 .....@. 0000 0000 0000 4018 4000
0x7ffd370a5494 fd7f 0000 4d0b 4000 0000 0000 0000 .....M. 0. 0000 0109 0000 ade2 7764
0x7ffd370a54a4 0000 0000 1700 0000 0100 0000 0000 0000 .....@. 0000 0000 0000 4000 0000
0x7ffd370a54b4 0000 0000 0000 0000 0200 0000 0000 0000 .....@. 0000 5500 0000 5000 0000
0x7ffd370a54c4 0000 0000 0000 0000 0000 0000 0000 0000 .....@. 0000 0000 0000 0000 0000
0x7ffd370a54d4 0000 0000 0000 0000 0000 0004 4000 .....@. 0000 0000 0000 0004 4000
0x7ffd370a54e4 0000 0000 102e 6c0f 2915 abae e018 4000 .....L. ) ..@. 2294 3125 6c1b e018 4000
0x7ffd370a54f4 0000 0000 0000 0000 0000 1890 6b00 .....k. 0000 0000 0000 1890 0000
0x7ffd370a5504 0000 0000 0000 0000 0000 102e ec96 .....@. 0000 0000 0001 4441 8267
0x7ffd370a5514 bd7b 5151 102e d81e 2915 abae 0000 0000 .{QQ. ....} .....@. 0000 0000 0000 0000
```

**Question 6 :** What is the value of eax when the imull instruction is called?

**Answer :**

```
[0x00400b5f]> ds
[0x00400b5f]> dr
rax = 0x00000006
rbx = 0x00400400
rcx = 0x0044b9a0
rdx = 0x7ffd370a55a8
r8 = 0x01000000
r9 = 0x006bb8e0
r10 = 0x00000015
r11 = 0x00000000
r12 = 0x004018e0
r13 = 0x00000000
r14 = 0x006b9018
r15 = 0x00000000
rsi = 0x7ffd370a5598
rdi = 0x00000001
rsp = 0x7ffd370a5470
rbp = 0x7ffd370a5470
rip = 0x00400b66
```

**Question 7 :** What is the value of local\_4h before eax is set to 0?

## **Answer :**

[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_fnddomain_subfreeres
0x0048fa40  16 247 → 237  sym._nl_unload_domain
```

The first challenge question asks us what the value of **local\_ch** is at address **0x00400b5f**. Now when we can run **db** and **dc** at this location we can use **db** and **dc** to point set correctly.

[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]> db 0x00400b69

[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
```

Lastly, we want to find the value of **local\_4h** before the **eax** is set to 0. We can do this by setting a breakpoint at instruction **0x00400b69**. Use the **dc** command to get to that point and then use the **dc** command to look at the memory of **local\_4h** with **px @ rbp-0x4**. The value here is **1**.

[0x00400a30]> dc

hit breakpoint at: 400b69

[0x00400b69]> px @ rbp-0x4

- offset -	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0x7ffc4983de5c	0600	0000	4018	4000	0000	0000	e910	4000	.	...	0.0.	.....	0.0.	.	.	.	0123456789ABCDEF
0x7ffc4983de6c	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
0x7ffc4983de7c	0100	0000	88df	8349	fctf	0000	4d0b	4000	.	...	I.	..	M.	0.	.	.	0000
0x7ffc4983de8c	0000	0000	0000	0000	0000	0000	0000	1700	0000	.	.....	.....	.....	.....	.....	.....	0000
0x7ffc4983de9c	0100	0000	0000	0000	0000	0000	0000	0000	0000	.	.....	.....	.....	.....	.....	.....	0000
0x7ffc4983deac	0200	0000	0000	0000	0000	0000	0000	0000	0000	.	.....	.....	.....	.....	.....	.....	0000
0x7ffc4983debc	0000	0000	0000	0000	0000	0000	0000	0000	0000	.	.....	.....	.....	.....	.....	.....	0000
0x7ffc4983dec0	0000	0000	0004	4000	0000	0000	f286	0656	.	...	0.	..	V	.	.	.	0000
0x7ffc4983dedc	1b7c	70e3	e018	4000	0000	0000	0000	0000	0000	p p	0.	..	0.	.	.	.	0000

## **Thought Process / Methodology :**

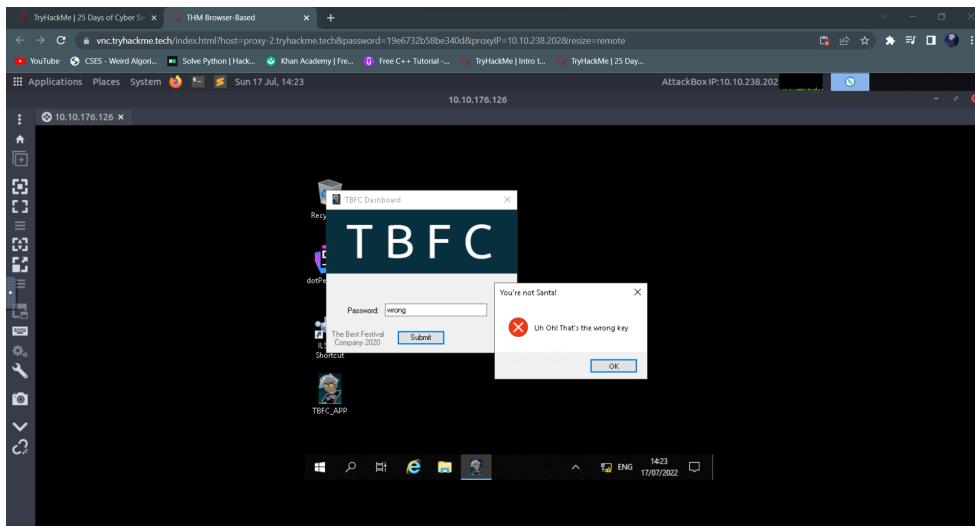
In the terminal , run ssh mceager@[machine\_IP] then enter the password.  
Use aa to analyze. Then pick db to breakpoint . pdf@main to check the  
breakpoint then dc to execute. Px

## Day 18 : The Bits Of Christmas

**Tool Used :** Kali Linux, Firefox, Attackbox, Remmina, ILSpy, TBFC\_app, CyberChef

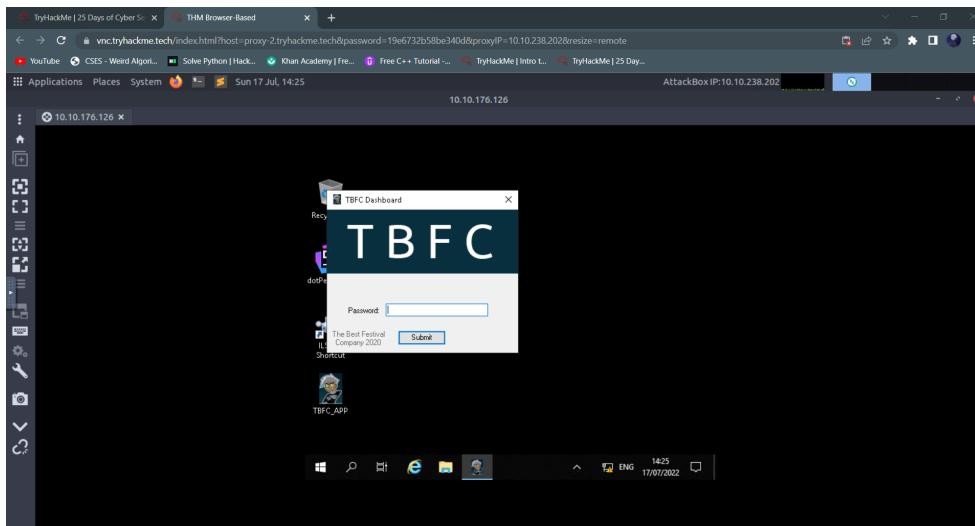
**Question 1 :** What is the message that shows up if you enter the wrong password for TBFC\_APP?

**Answer :** Uh Oh! That's the wrong key



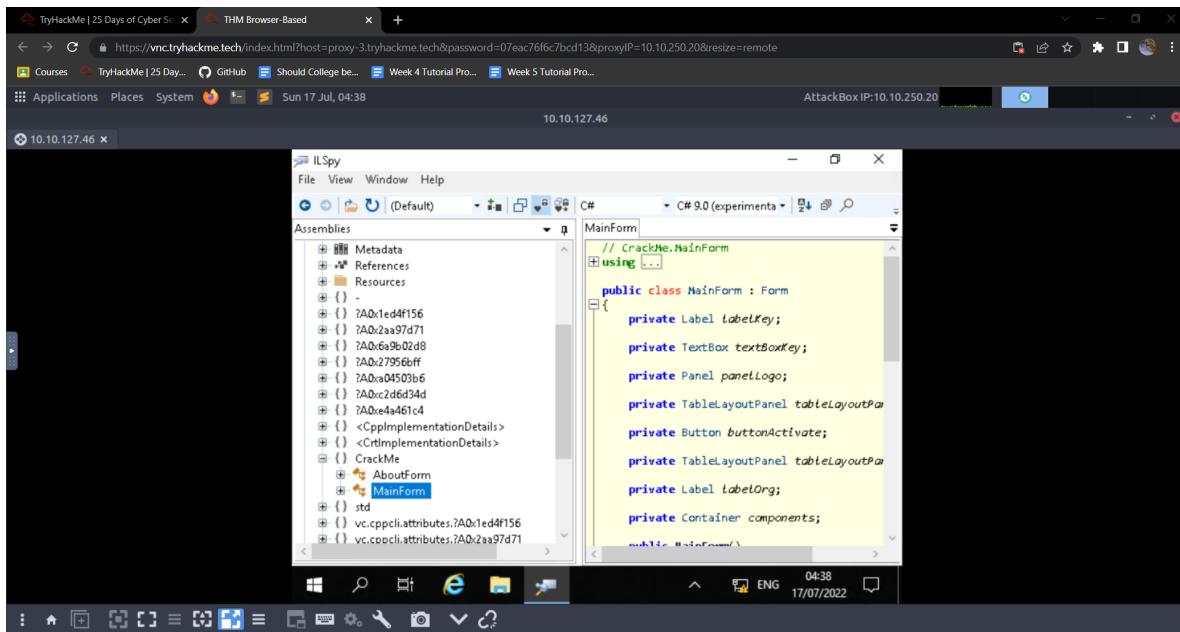
**Question 2 :** What does TBFC stand for?

**Answer :** The Best Festival Company



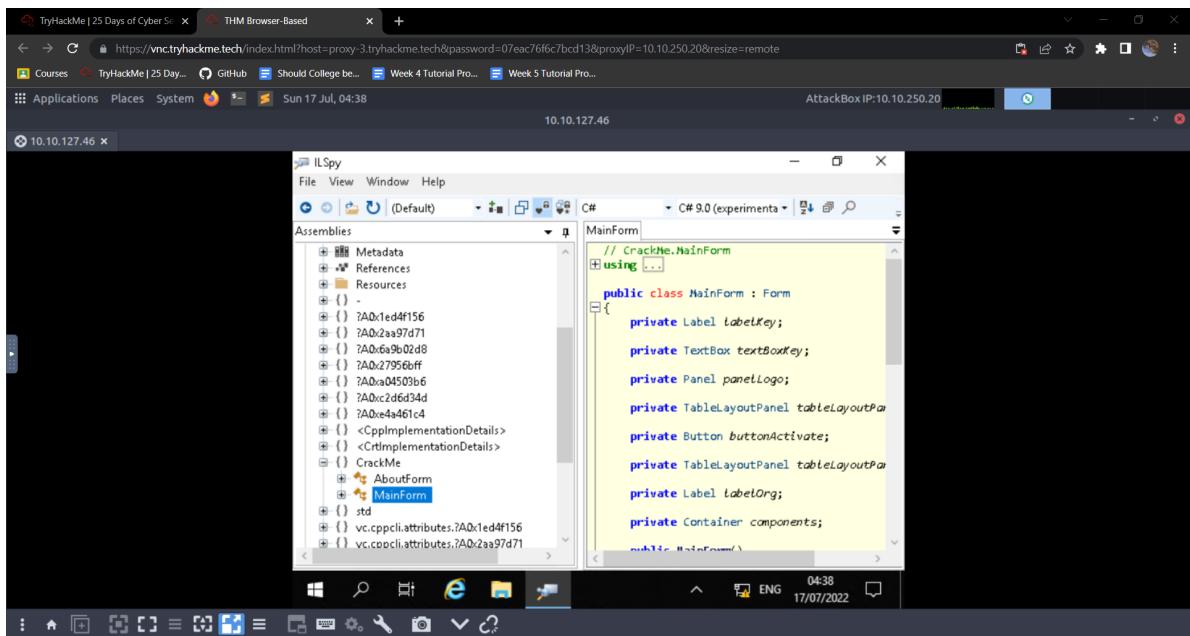
**Question 3 :** Decompile the TBFC\_APP with ILSpy. What is the module that catches your attention?

**Answer : CrackMe**



**Question 4 :** Within the module, there are two forms. Which contains the information we are looking for?

**Answer : MainForm**



The screenshot shows the IL Spy application running in a browser window. The title bar says "IL Spy" and the menu bar includes "File", "View", "Window", and "Help". The toolbar has icons for opening files, saving, and searching. The code editor is displaying C# 9.0 code for a "MainForm" class. The code includes imports for "System", "System.Windows.Forms", and "CrackMe". It defines several private fields: "labelKey", "textBoxKey", "panelLogo", "tableLayoutPanel1", "buttonActivate", "tableLayoutPanel2", "labelOrg", and "components". A constructor "public MainForm()" is also present. The assembly tree on the left shows the "CrackMe" project with "MainForm" selected.

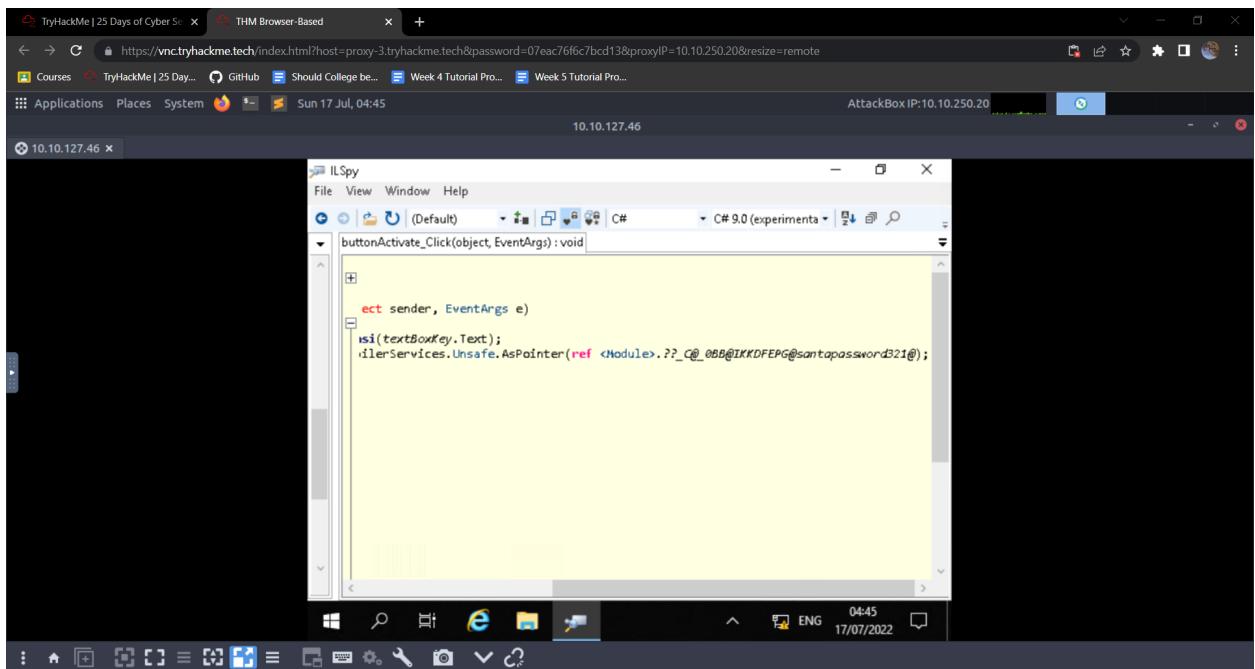
```
// CrackMe.MainForm
using System;
using System.Windows.Forms;
using CrackMe;

public class MainForm : Form
{
    private Label labelKey;
    private TextBox textBoxKey;
    private Panel panelLogo;
    private TableLayoutPanel tableLayoutPanel1;
    private Button buttonActivate;
    private TableLayoutPanel tableLayoutPanel2;
    private Label labelOrg;
    private Container components;

    public MainForm()
    {
        InitializeComponent();
    }
}
```

**Question 5 :** Which method within the form from Q4 will contain the information we are seeking?

**Answer : buttonActivate\_Click**



The screenshot shows the IL Spy application running in a browser window. The title bar says "IL Spy" and the menu bar includes "File", "View", "Window", and "Help". The toolbar has icons for opening files, saving, and searching. The code editor is displaying C# 9.0 code for the "buttonActivate\_Click" method. The method signature is "buttonActivate\_Click(object, EventArgs) : void". The body of the method contains code that reads the text from a text box and writes it to a file using a pointer to a module named "IKKDFEPG@santapassword321".

```
buttonActivate_Click(object, EventArgs) : void
{
    object sender, EventArgs e)
    {
        string text = textBoxKey.Text;
        IntPtr module = IntPtr.Zero;
        module = MarshalServices.Unsafe.AsPointer(ref module);
        module.WriteString(0, text);
    }
}
```

## Question 6 : What is Santa's password?

Answer : santapassword321

The screenshot shows a Windows desktop environment. In the foreground, there is a debugger window titled "ILSpy" running on "AttackBox IP:10.10.250.20". The code editor displays the following C# code:

```
??_C@_0BB@IKKDFEPG@santapassword321@ : $ArrayType$$$BY0BB@$ CBD
    '21@/* Not supported: data(73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31 00) */;
```

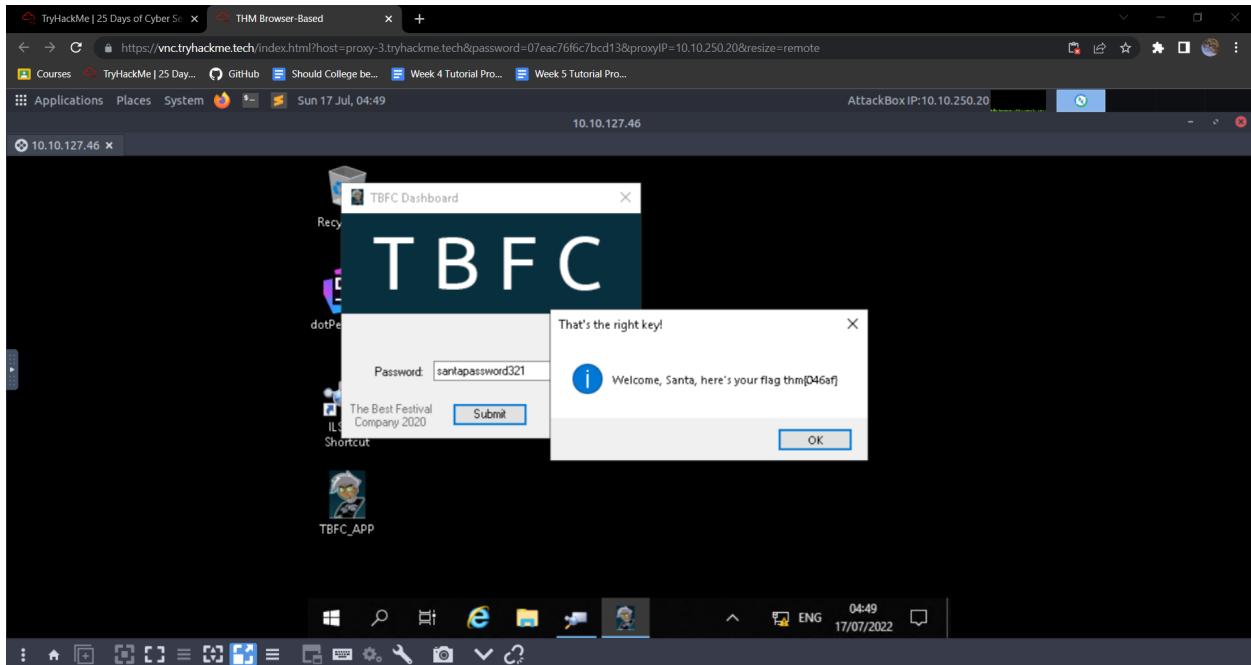
In the background, a Firefox browser window titled "THM Browser Based" is open, displaying the URL <https://vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=07eac76f6c7bcd13&proxyIP=10.10.250.20&resize=remote>. The status bar at the bottom of the browser window shows "17/07/2022 04:45".

The screenshot shows the CyberChef interface with the title "From Hex - CyberChef - Mozilla Firefox". The "Input" field contains the hex dump: "73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31". The "Output" field shows the converted string: "santapassword321". The "Operations" sidebar on the left includes options like "From Hex", "To Hex", "From Base64", and "To Base64".

**Question 7 :** Now that you've retrieved this password, try to login...What is the flag?

**Answer : thm{046af}**



### Thought Process / Methodology :

Firstly, we used Remmina to connect to the instance. We put the MACHINE\_IP, username which is **cmnatic** and password which is **Adventofcyber!**. After log in into the Remote Desktop Protocol (RDP). We open the **TBFC\_APP** and we put the incorrect password to see the message that shows up if you enter the wrong password. We knew that **TBFC** stands for **The Best Festival Company** by looking at the App Dashboard. After that we decompiled **TBFC\_APP** with **ILSpy** and a module titled **CrackMe** caught our attention because of the unique name. Within the module, we found two forms which are **AboutForm** and **MainForm**. After looking through both forms, we found that **MainForm** contains the information that we are looking for. We found that the method **buttonActivate\_Click** contains all the information that we are seeking. Lastly, we used **CyberChef** to get Santa's password and then we logged in by using the password to get the flag.

## Day 19 : The Naughty or Nice List

**Tool Used :** Kali Linux, Firefox, Attackbox

**Question 1 :** Which list is this person on?

**Answer :**

Q1: Which list is this person on? \*

6 points

Select the proper words in the proper place of the command: [a] -c -z file,[b]  
http://[c].xyz/api.[d]?[e]=FUZZ

	Naughty	Nice
YP	<input checked="" type="radio"/>	<input type="radio"/>
Timothy	<input checked="" type="radio"/>	<input type="radio"/>
JJ	<input type="radio"/>	<input checked="" type="radio"/>
Ian Chai	<input type="radio"/>	<input checked="" type="radio"/>
Kanes	<input checked="" type="radio"/>	<input type="radio"/>
Tib3rius	<input type="radio"/>	<input checked="" type="radio"/>

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

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

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

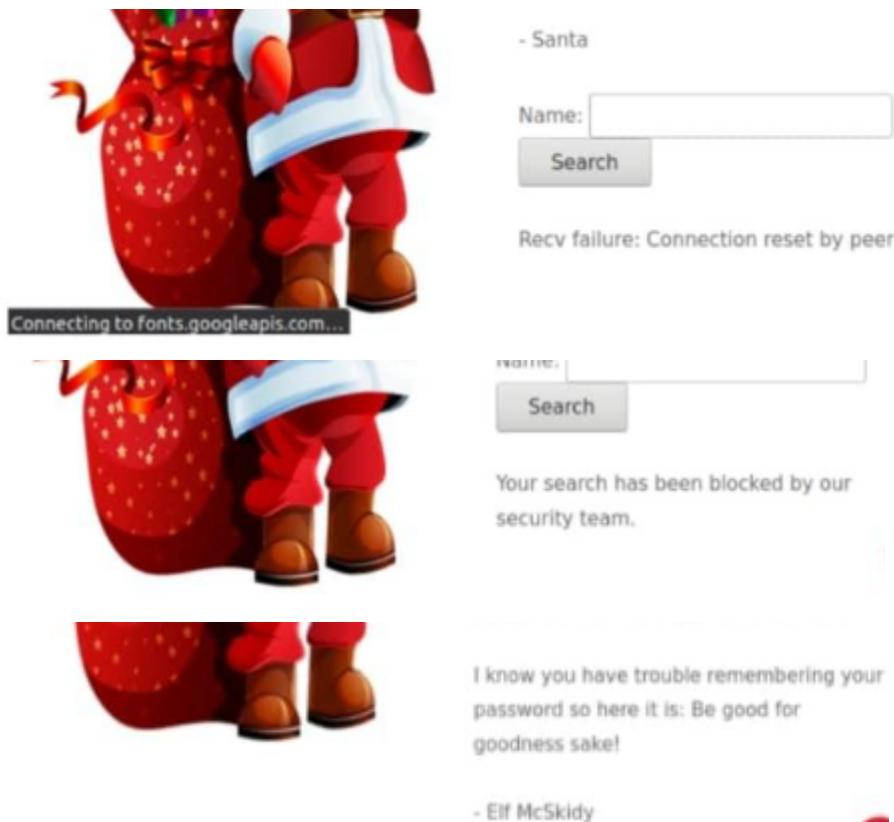
**Answer : Failed to connect to list.hohoho port 80:  
Connection refused**

**Question 4 :** What is displayed on the page when you use "?/proxy=http%3A%2F%2Flist.hohoho%3A22"?

**Answer : Recv failure: Connection reset by peer**

**Question 5 :** What is displayed on the page when you use "?/proxy=http%3A%2F%2Flocalhost"?

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



**Question 6 : What is Santa's password?**

**Answer : Be good for goodness sake!**

**Question 7 : What is the challenge flag?**

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

**Thought Process / Methodology :**

Using the provided URL, we should begin by retrieving the site's root, but instead we receive the message "Not Found. The server could not find the requested URL. This generic 404 message demonstrates that we were successful in getting the server to request our altered URL. The notification now reads "Failed to connect to list" after we attempt altering the port number. port 80: "hohoho: Connection denied." We attempted changing the port to 22, which is the standard SSH port, since neither of those solutions worked. Reception failure: Connection reset by peer\* is now the message. Port 22 did open, but it did not comprehend the message, therefore this indicates. We can also try substituting "localhost" or "127.0.0.1" for the list.hohoho hostname, but it prevents us from conducting a search. This is due to a check that the developer has set up that immediately rejects any hostname that doesn't begin with list.hohoho. To avoid that check, we simply use a hostname that does not begin with list.hohoho, in this case "list.hohoho.localtest.me". Success! It is effective. This allowed us to locate Santa's username, which was contained in Elf McSkidy's message.

## Day 20 : PowershELIF to the rescue

**Tool Used :** Kali Linux, Firefox, Windows Powershell

**Question 1 :** Check the ssh manual. What does the parameter -l do?

**Answer : 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 configura-
    tion 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?

**Answer : 2 front teeth**

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

PS C:\Users\mceager\Documents> ls -Hidden
Next, go back to the
Location ..\Desktop

Directory: C:\Users\mceager\Documents
PS C:\Users\mceager\Documents>
PS C:\Users\mceager\Deskt

Mode                LastWriteTime         Length Name
-->---->----->----->----->
d--hsl      12/7/2020 10:28 AM          0 My Music
d--hsl      12/7/2020 10:28 AM          0 My Pictures
d--hsl      12/7/2020 10:28 AM          0 My Videos
-a-hs-     12/7/2020 10:29 AM        402 desktop.ini
-arh--    11/18/2020  5:05 PM         35 efone.txt

Now we can search
for the file 'elf2'
in the directory ..\D
esktop\My Pictures\

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

**Question 3 :** 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**

```
PS C:\Users\mceager\Desktop> ls -Hidden
Location ..\Desktop\

Directory: C:\Users\mceager\Desktop
PS C:\Users\mceager\Documents> Set-Content
PS C:\Users\mceager\Desktop>

Mode          LastWriteTime
--           --
d--h--       12/7/2020 11:26 AM
-a-hs-       12/7/2020 10:29 AM

Length Name
Now we can search for the hid
elf2wo
directo282 desktop.ini.
PS C:\Users\mceager\Desktop> ls -Hidden
PS C:\Users\mceager\Desktop> cd ..\elf2wo\
PS C:\Users\mceager\Desktop\elf2wo> ls -Hidden
PS C:\Users\mceager\Desktop\elf2wo>

Mode          LastWriteTime
--           --
d--h--       12/7/2020 11:26 AM
-a-hs-       12/7/2020 10:29 AM

Length Name
PS C:\Users\mceager\Desktop>
PS C:\Users\mceager\Desktop> ls -Hidden
PS C:\Users\mceager\Desktop> cd ..\elf2wo\
PS C:\Users\mceager\Desktop\elf2wo>

Mode          LastWriteTime
--           --
-a-hs-       11/17/2020 10:26 AM

Length Name
When we search the documents
we read the contents of this file
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>
```

## Question 4 : Search the Windows directory for a hidden folder t

Answer : 3lfthr3e

```
Directory: C:\Windows\System32
Mode                LastWriteTime
--h--          11/23/2020  3:26 PM
--h--          11/23/2020  2:26 PM

Directory: C:\Windows\System32\3lfthr3e
Mode                LastWriteTime
--arh--        11/17/2020  10:58 AM
--arh--        11/23/2020  3:26 PM

Length   Name
----- 
      85887  1.txt
  12061168  2.txt
      11/23/2020
      11/23/2020
```

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

## Question 5 : How many words does the first file contain?

Answer : 9999

```
PS C:\Users\mceager\Desktop\elf2wo> Get-Content C:\Windows\System32\3lfthr3e\1.txt | Measure-Object -Word
Lines Words Characters Property
--- --- --- ---
 9999
```

Question 4 Answer: 9999

## Question 6 : What 2 words are at index 551 and 6991 in the first file?

Answer : Red Ryder

```
PS C:\Users\mceager\Desktop\elf2wo> (Get-Content C:\Windows\System32\3lfthr3e\1.txt)[551]
Red
PS C:\Users\mceager\Desktop\elf2wo> (Get-Content C:\Windows\System32\3lfthr3e\1.txt)[6991]
Ryder
PS C:\Users\mceager\Desktop\elf2wo>
```

Answer the questions below

Search for the first hidden elf file with

**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. What does Elf 3 want? (use spaces when submitting the answer)

## Answer : Red Ryder BB Gun

```
PS C:\Users\mceager\Desktop\elf2wo> (Get-Content C:\Windows\System32\3lfthr3e\1.txt)[551]
Red
PS C:\Users\mceager\Desktop\elf2wo> (Get-Content C:\Windows\System32\3lfthr3e\1.txt)[6991]
Ryder
PS C:\Users\mceager\Desktop\elf2wo>
```

After finding the total number of words, we want to find specific words in the file with the command `(Get-Content C:\Windows\System32\3lfthr3e\1.txt)[index]` where index is the location of the word we want to find. We can use this to find **551** and **6991**.

```
PS C:\Users\mceager\Desktop\elf2wo> (Get-Content C:\Windows\System32\3lfthr3e\1.txt)[551]
Red
PS C:\Users\mceager\Desktop\elf2wo> (Get-Content C:\Windows\System32\3lfthr3e\1.txt)[6991]
Ryder
PS C:\Users\mceager\Desktop\elf2wo> ■
```

*Question 5 Answer: Red Ryder*

Finally, we want to search the second file for the phrase from the previous question with the command `Select-String -Path C:\Windows\System32\3lfthr3e\2.txt -Pattern 'redryder'`

```
PS C:\Users\mceager\Desktop\elf2wo> Select-String -Path C:\Windows\System32\3lfthr3e\2.txt
C:\Windows\System32\3lfthr3e\2.txt:558784:redryderbbgun
PS C:\Users\mceager\Desktop\elf2wo> ■
```

*Question 5 Answer: Red Ryder bb Gun*

```
> Select-String -Path C:\Windows\System32\3lfthr3e\2.txt -Pattern 'redryder'
```

```
C:\Windows\System32\3lfthr3e\2.txt:558704:redryderbbgun
```

## **Thought Process / Methodology :**

In the terminal , run ssh -l mceager [machine\_IP] then enter password r0ckStar! . After that, type cd Documents then type powershell. Type ls -Hidden to find text file, e1fone.txt. Then , cd desktop and run ls -Hidden again to find elf2wo directory. cd .\elf2wo\ then ls -Hidden then ls again . found a file . Then Get-Content [file name]. Run Get-ChildItem -Path / -Recurse -Hidden -ErrorAction SilentlyContinue to find system32 and find a directory. Two files in the directory . Get-Content

C:\Windows\System32\3lfthr3e\1.txt | Measure-Object -Word and get answer 9999.TType (Get-Content

C:\Windows\System32\3lfthr3e\1.txt)[index] where index is the location of the word we want to find. We can use this to find 551 and 6991 .Lastly, Select-String -Path C:\Windows\System32\3lfthr3e\2.txt -Pattern 'redryder' to get last answer.