

PSP0201

WEEK 5

Write Up

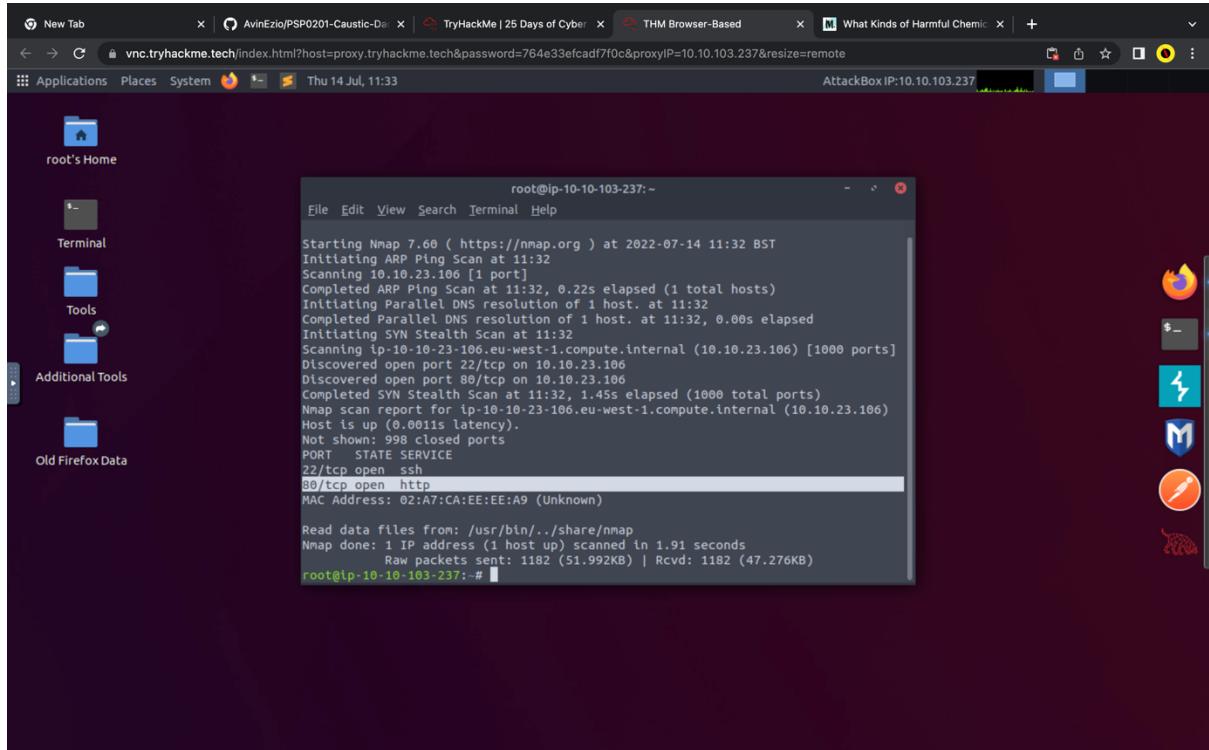
Group members	ID
1)Nevendra Eravanan	1211101778
2) Avinnaesh A/L G Baramesvaran	1211101658
3) Arvind A/L Krishna Kumar	1211101977

Day 16 – {Scripting} Help! Where is Santa?

Tools used: Kali linux, Firefox, Terminal

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

- Open terminal and run a nmap scan with verbose on the machine ip.
- nmap -v 10.10.23.106
- the open ports will be listed below.



The screenshot shows a Kali Linux desktop environment. In the center, a terminal window displays the output of an Nmap scan. The output shows the following details:

```
root@ip-10-10-103-237:~# Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-14 11:32 BST
Initiating ARP Ping Scan at 11:32
Scanning 10.10.23.106 [1 port]
Completed ARP Ping Scan at 11:32, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:32
Completed Parallel DNS resolution of 1 host. at 11:32, 0.00s elapsed
Initiating SYN Stealth Scan at 11:32
Scanning lp-10-10-23-106.eu-west-1.compute.internal (10.10.23.106) [1000 ports]
Discovered open port 22/tcp on 10.10.23.106
Discovered open port 80/tcp on 10.10.23.106
Completed SYN Stealth Scan at 11:32, 1.45s elapsed (1000 total ports)
Nmap scan report for ip-10-10-23-106.eu-west-1.compute.internal (10.10.23.106)
Host is up (0.0011s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:A7:CA:EE:EE:A9 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.91 seconds
Raw packets sent: 1182 (51.992KB) | Rcvd: 1182 (47.276KB)
```

Question 2: What templates are being used?

- The templates being used can be seen on the top left corner of the website.

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

- Open Firefox browser and search for the URL machine_ip/static/index.html
- Right click and view the page source.
- Scroll down to find the api directory.

```

73      <ul>
74        <li><a href="#">Lorem ipsum dolor sit amet</a></li>
75        <li><a href="#">Liberum errato isse</a></li>
76        <li><a href="#">Lorem ipsum dolor sit amet</a></li>
77        <li><a href="#">Aisia caisia</a></li>
78        <li><a href="#">Murphy's law</a></li>
79        <li><a href="#">Flimsy Lavenrock</a></li>
80        <li><a href="#">Maven Mousie Lavender</a></li>
81      </ul>
82    </div>
83    <div class="column is-3">
84      <strong>Category</strong></h2>
85      <ul>
86        <li><a href="#">Labore et dolore magna aliqua</a></li>
87        <li><a href="http://machine_ip/api/key">Modular modern free</a></li>
88        <li><a href="#">The King of clubs</a></li>
89        <li><a href="#">The Discovery Dissipation</a></li>
90        <li><a href="#">Course Correction</a></li>
91        <li><a href="#">Better Angels</a></li>
92      </ul>
93    </div>
94    <div class="column is-4">
95      <strong>Category</strong></h2>
96      <ul>
97        <li><a href="#">Objects in space</a></li>
98        <li><a href="#">Playing cards with coyote</a></li>
99        <li><a href="#">Goodbye Yellow Brick Road</a></li>
100       <li><a href="#">The Garden of Forking Paths</a></li>
101       <li><a href="#">Future Shock</a></li>
102     </ul>
103   </div>
104 </div>
105 <div class="content has-text-centered">
106   <p>
107     <a class="icon" href="https://github.com/BulmaTemplates/bulma-templates">
108       <i class="fa fa-github"></i>
109     </a>
110   </p>
111 <div class="control level-item">
112   <a href="https://github.com/BulmaTemplates/bulma-templates">
113

```

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

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

- Open a new tab on Firefox and search for machine_ip/api/
- Navigate to the Raw Data tab.

```

10.10.23.106/api/

```

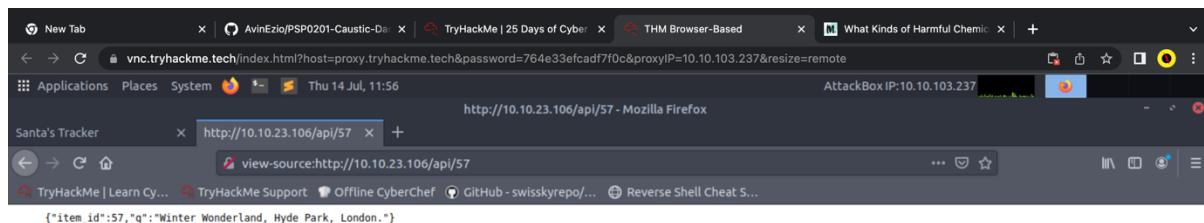
JSON	Raw Data	Headers
Save	Copy	Pretty Print
{"detail": "Not Found"}		

Question 5: Where is Santa right now? (Tick all correct answers.)

&

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 (10.10.94.92)

- Open a new tab on the browser.
- Search for the URL machine_ip/api/api_key
- The correct api_key is obtained by trial and error by entering different odd numbers between 1 and 100.
- Once give access the location of Santa will be displayed.
- The api_key number is 57



Thought process / Methodology

We first ran a nmap scan with verbose to display all the open ports. Then, we opened Firefox and viewed the source page to obtain the api key and the api directory. To get access to Santa's location, we randomly entered odd numbers from 1 to 100 to find the correct api key value.

Day 17: Reverse Engineering- ReverseELFneering

Tools Used: Try Hack me Attack Box

Solution/Walkthrough:

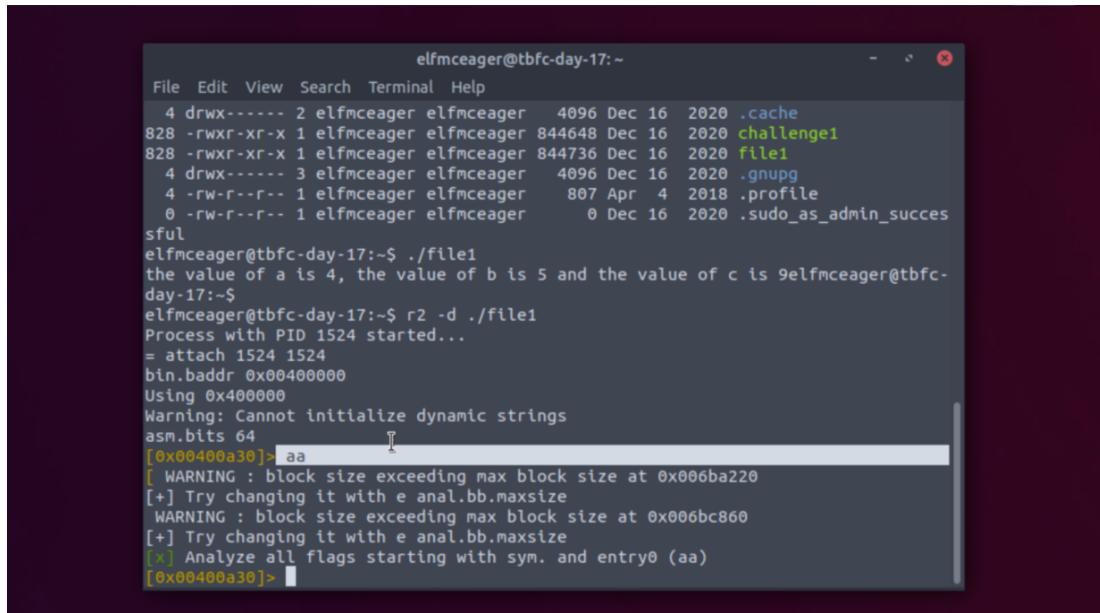
Question 1

Matching the data types along with the size in bytes.

Initial Data Type	Suffix	Size (bytes)
Byte	b	1
Word	w	2
Double Word	l	4
Quad	q	8
Single Precision	s	4
Double Precision	l	8

Question 2

Entering the required command to analyse the program in radare2, which is “aa”.



```
elfmceager@tbfc-day-17:~
```

```
File Edit View Search Terminal Help
```

```
4 drwx----- 2 elfmceager elfmceager 4096 Dec 16 2020 .cache
828 -rwxr-xr-x 1 elfmceager elfmceager 844648 Dec 16 2020 challenge1
828 -rwxr-xr-x 1 elfmceager elfmceager 844736 Dec 16 2020 file1
4 drwx----- 3 elfmceager elfmceager 4096 Dec 16 2020 .gnupg
4 -rw-r--r-- 1 elfmceager elfmceager 807 Apr  4 2018 .profile
0 -rw-r--r-- 1 elfmceager elfmceager     0 Dec 16 2020 .sudo_as_admin_sucessful
```

```
elfmceager@tbfc-day-17:~$ ./file1
the value of a is 4, the value of b is 5 and the value of c is 9elfmceager@tbfc-day-17:~$
```

```
elfmceager@tbfc-day-17:~$ r2 -d ./file1
Process with PID 1524 started...
= attach 1524 1524
bin.baddr 0x04000000
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]>
```

Question 3

Putting in the command “db” to set a breakpoint in radare2.

```
elfmceager@tbfc-day-17: ~
File Edit View Search Terminal Help
0x00400b8f    c9      leave
0x00400b90    c3      ret
[0x00400a30]> db 0x00400b55
[0x00400a30]> pdf @main
;-- main:
(fcn) sym.main 68
sym.main ();
; var int local_ch @ rbp-0xc
; var int local_8h @ rbp-0x8
; var int local_4h @ rbp-0x4
; DATA XREF from 0x00400a4d (entry)
0x00400b4d    55      push rbp
0x00400b4e    4889e5   mov rbp, rsp
0x00400b51    4883ec10 sub rsp, 0x10
0x00400b55 b   c745f4040000. mov dword [local_ch], 4
0x00400b5c    c745f8050000. mov dword [local_8h], 5
0x00400b63    8b55f4    mov edx, dword [local_ch]
0x00400b66    8b45f8    mov eax, dword [local_8h]
0x00400b69    01d0      add eax, edx
0x00400b6b    8945fc    mov dword [local_4h], eax
0x00400b6e    8b4dfc    mov ecx, dword [local_4h]
0x00400b71    8b55f8    mov edx, dword [local_8h]
0x00400b74    8b45f4    mov eax, dword [local_ch]
0x00400b77    89c6      mov esi, eax
```

Question 4

Using the command “dc” to execute the program until we hit a breakpoint

```
elfmceager@tbfc-day-17: ~
File Edit View Search Terminal Help
0x00400b4d    55      push rbp
0x00400b4e    4889e5   mov rbp, rsp
0x00400b51    4883ec10 sub rsp, 0x10
0x00400b55 b   c745f4040000. mov dword [local_ch], 4
0x00400b5c    c745f8050000. mov dword [local_8h], 5
0x00400b63    8b55f4    mov edx, dword [local_ch]
0x00400b66    8b45f8    mov eax, dword [local_8h]
0x00400b69    01d0      add eax, edx
0x00400b6b    8945fc    mov dword [local_4h], eax
0x00400b6e    8b4dfc    mov ecx, dword [local_4h]
0x00400b71    8b55f8    mov edx, dword [local_8h]
0x00400b74    8b45f4    mov eax, dword [local_ch]
0x00400b77    89c6      mov esi, eax
0x00400b79    488d3d881409. lea rdi, qword str.the_value_of_a_is_
d__the_value_of_b_is_d_and_the_value_of_c_is_d ; 0x492008 ; "the value of a i
s %d, the value of b is %d and the value of c is %d"
0x00400b80    b800000000  mov eax, 0
0x00400b85    e8f6ea0000  call sym.__printf
0x00400b8a    b800000000  mov eax, 0
0x00400b8f    c9      leave
0x00400b90    c3      ret
[0x00400a30]> dc
hit breakpoint at: 400b55
```

Question 5

Entering the command “pdf @main” to Identify the value of local_ch when its corresponding movl instruction is called (first if multiple), which turns out to be “1”

```
elfmceager@tbfc-day-17:~
```

```
File Edit View Search Terminal Help
```

```
[ 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]> 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
```

Question 6

By doing some calculation we were able to get to know the value of eax when the imull instruction is called, which is “6”

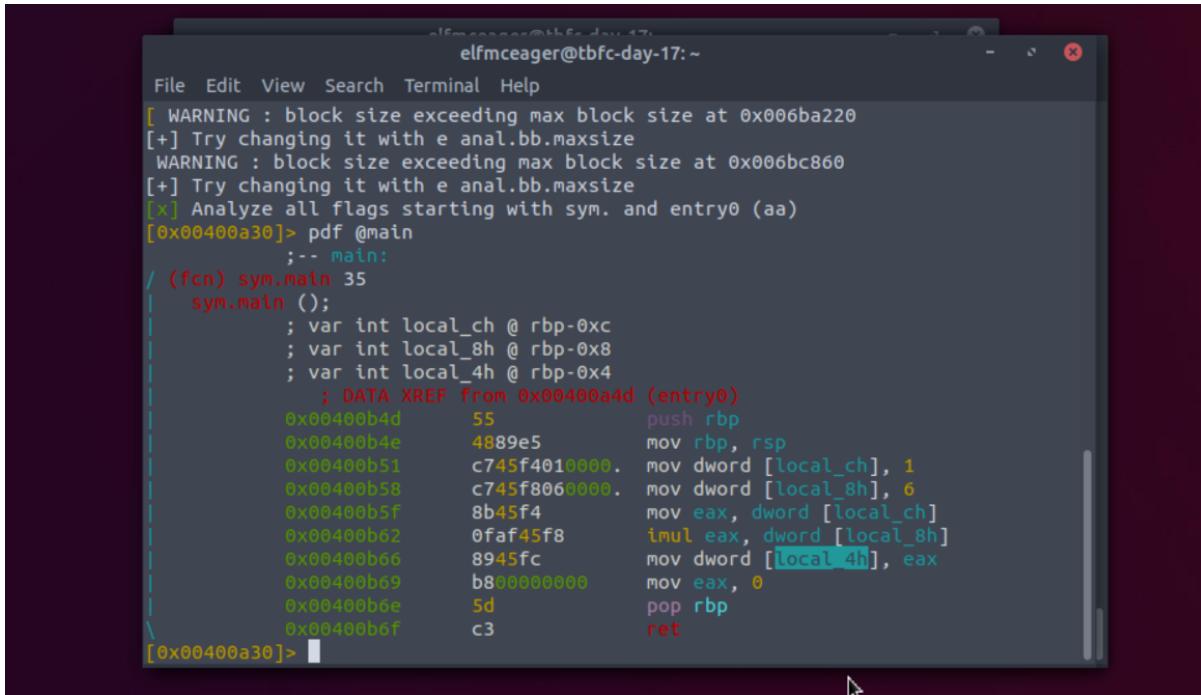
```
elfmceager@tbfc-day-17:~
```

```
File Edit View Search Terminal Help
```

```
[ 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]> 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
```

Question 7

Identifying the value of local_4h before eax is set to 0 by calculating. Thus the value is “6”



The screenshot shows a terminal window titled "elfmceager@tbfc-day-17:~". The command "pdf @main" has been run, displaying the assembly code for the main function. The assembly code includes instructions for initializing local variables (local_ch, local_8h, local_4h) and setting up stack frames. The value of local_4h is explicitly shown as 1. The assembly code is as follows:

```
[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
[*] Analyze all flags starting with sym. and entry0 (aa)
[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]>
```

Thought Process/Methodology:

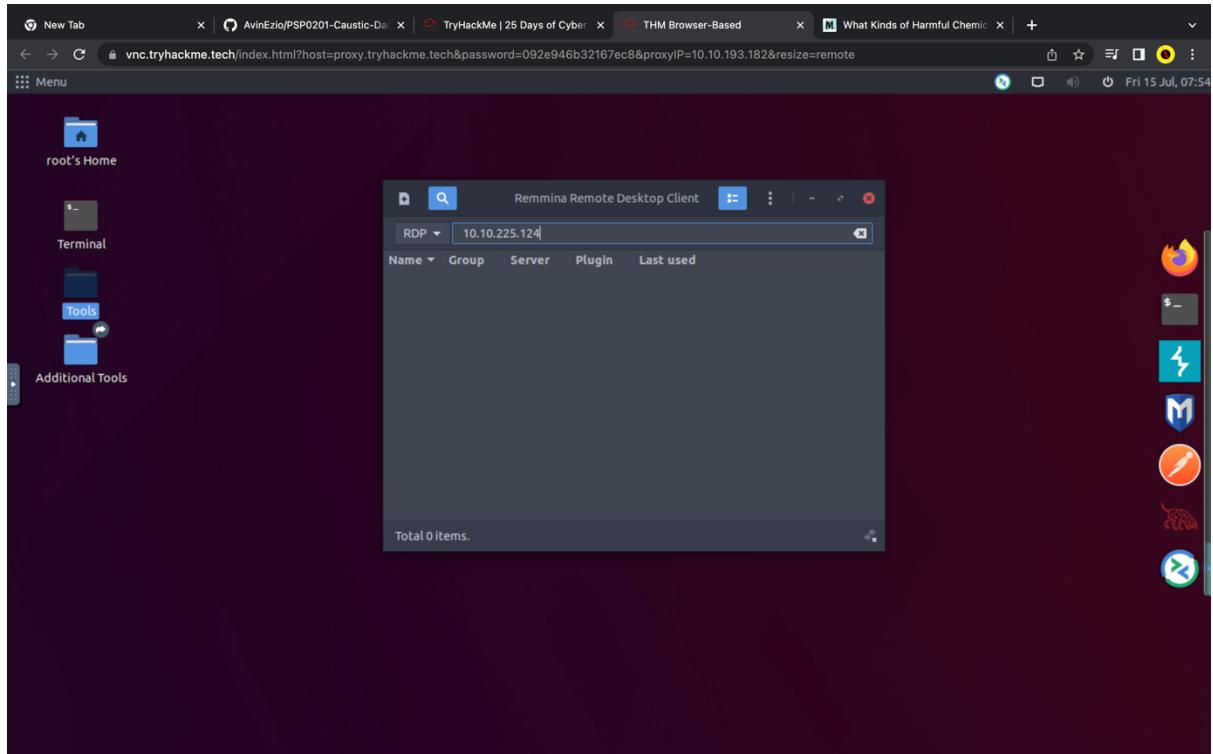
We started by reading through the instructions that have been provided by Try Hack Me, where we got to know that a table have been provided answering the very first question, after done reading the table we then answered the question. Moving on, we identified and entered the command to analyse the program in radare2 which is “aa” for the second question. Then, we moved on by putting in the command “db” to set a breakpoint in radare2. We typed in the command “dc” in order to execute the program until it hits a breakpoint. Then we moved on by entering the command “pdf @main” to get the value of local_ch when its corresponding movl instruction is called (first if multiple), which turns out to be “1”. Then we calculated what is the value of eax when the imull instruction is called, which turns out to be “6”. Finally, we calculated the value of local_4h before eax is set to 0, which then gives us a value of “6”.

Day 18 – {Reverse Engineering} The Bits of Christmas

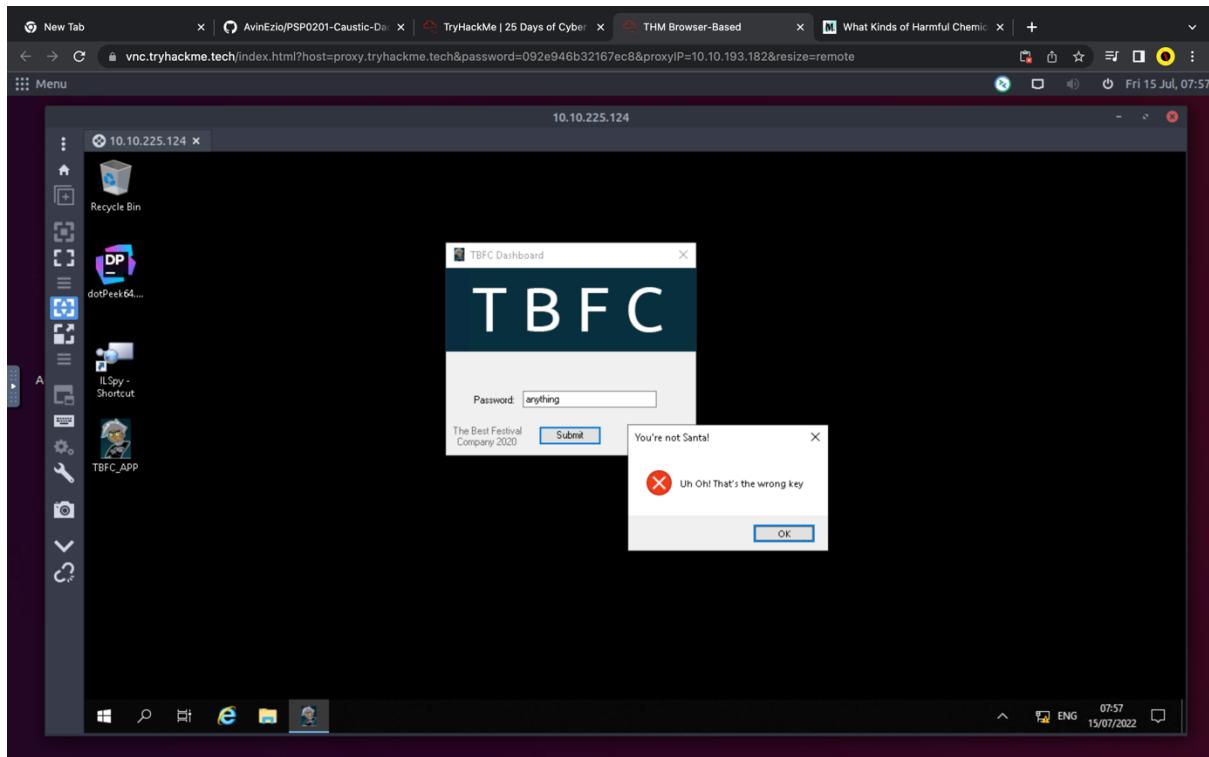
Tools used: Kali linux, Windows, Firefox, CyberChef

Question 1: What is the message that shows up if you enter the wrong password for TBFC_APP?

- Navigate to the apps tab and open Remmina.
- Enter the machine ip and enter.



- Enter the username and password which is given in the task description.
- Once logged in, open the TBFC app.
- Enter anything as the password to display the message.

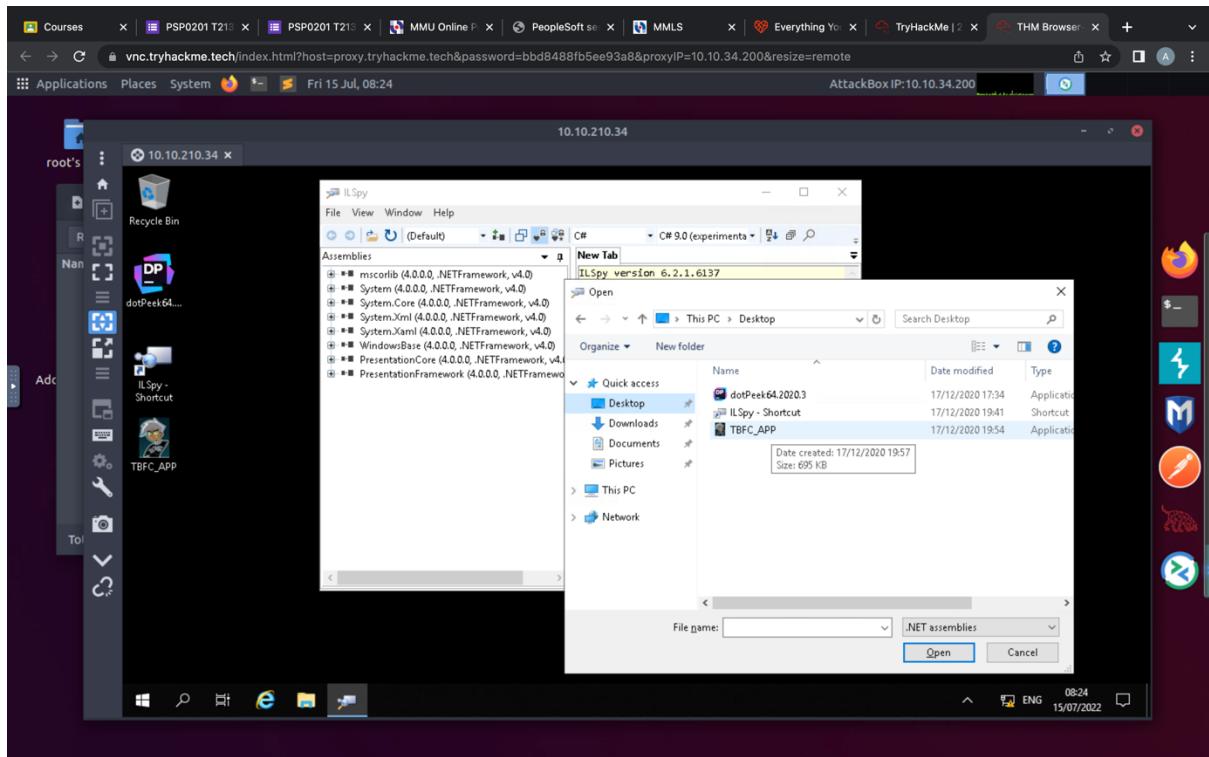


Question 2: What does TBFC stand for?

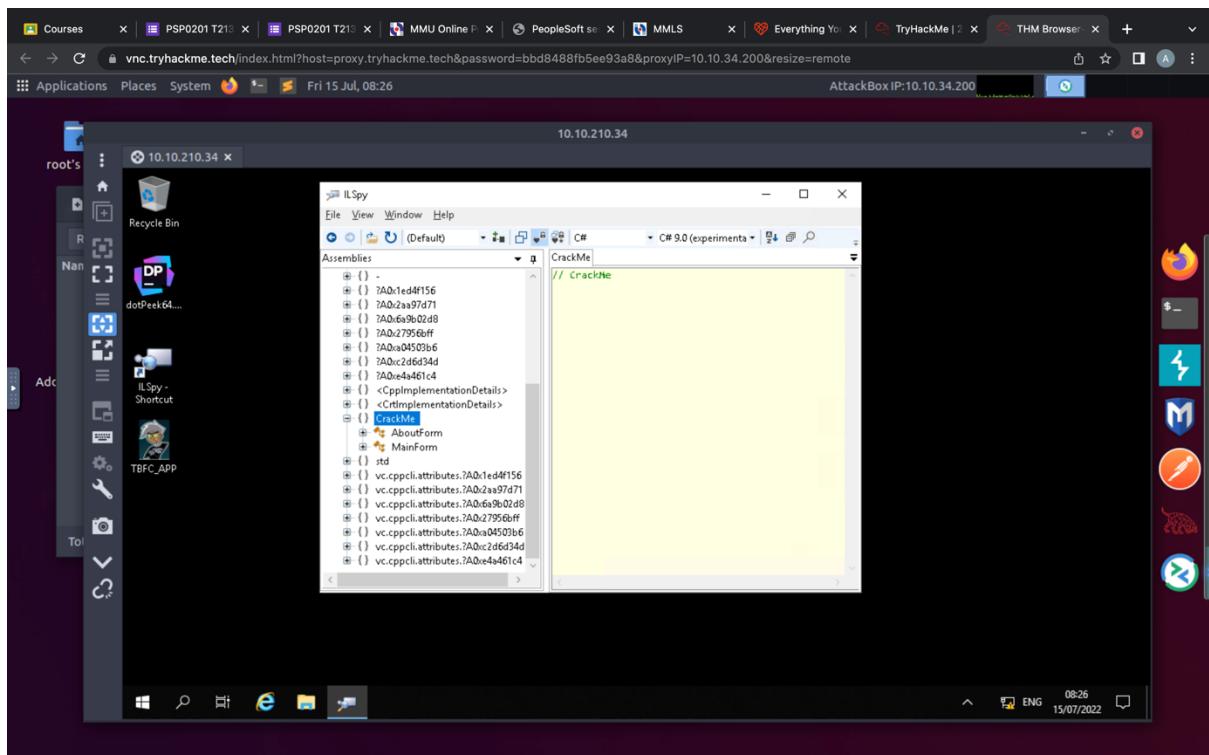
- The full name of the app can be found at the bottom left of the app window.

Question 3: Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?

- Open the ILSpy using the shortcut in the desktop page.
- Navigate to the file tab at the top, and open the TBFC app



- Find for the Crack Me module.

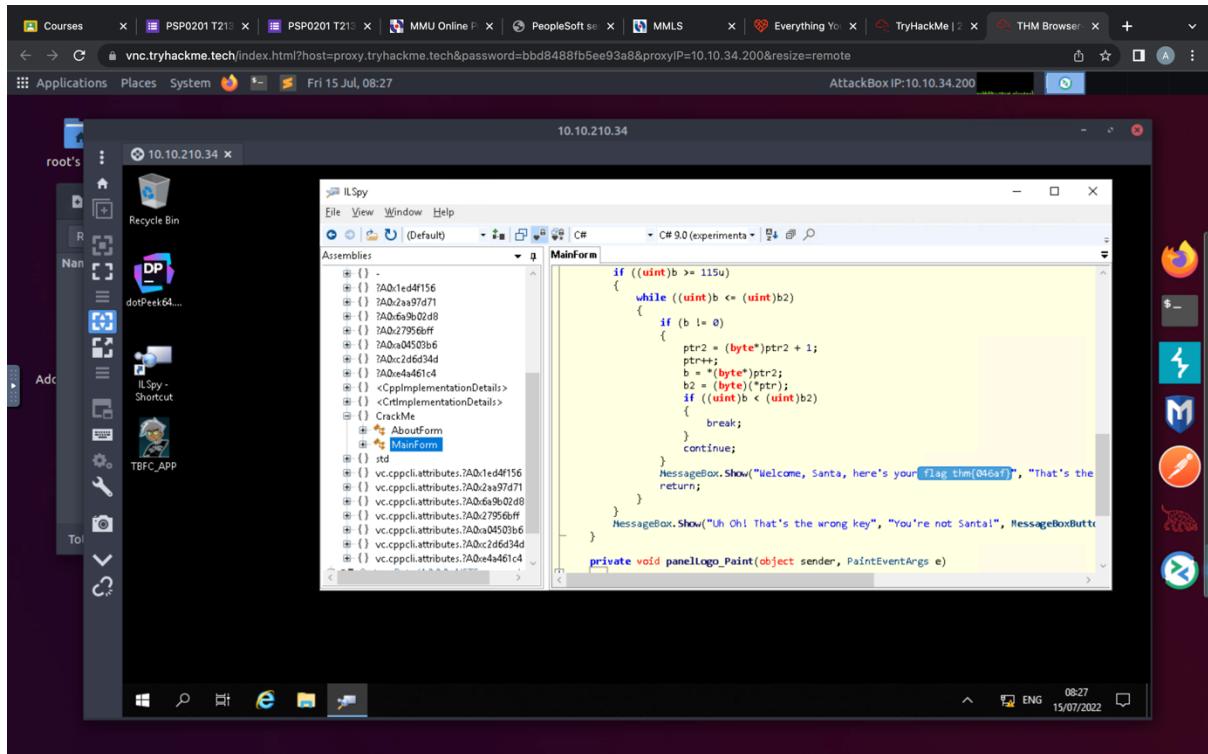


Question 4: Within the module, there are two forms. Which contains the information we are looking for?

- To find the Santa's password and the flag, we have to search in the MainForm.

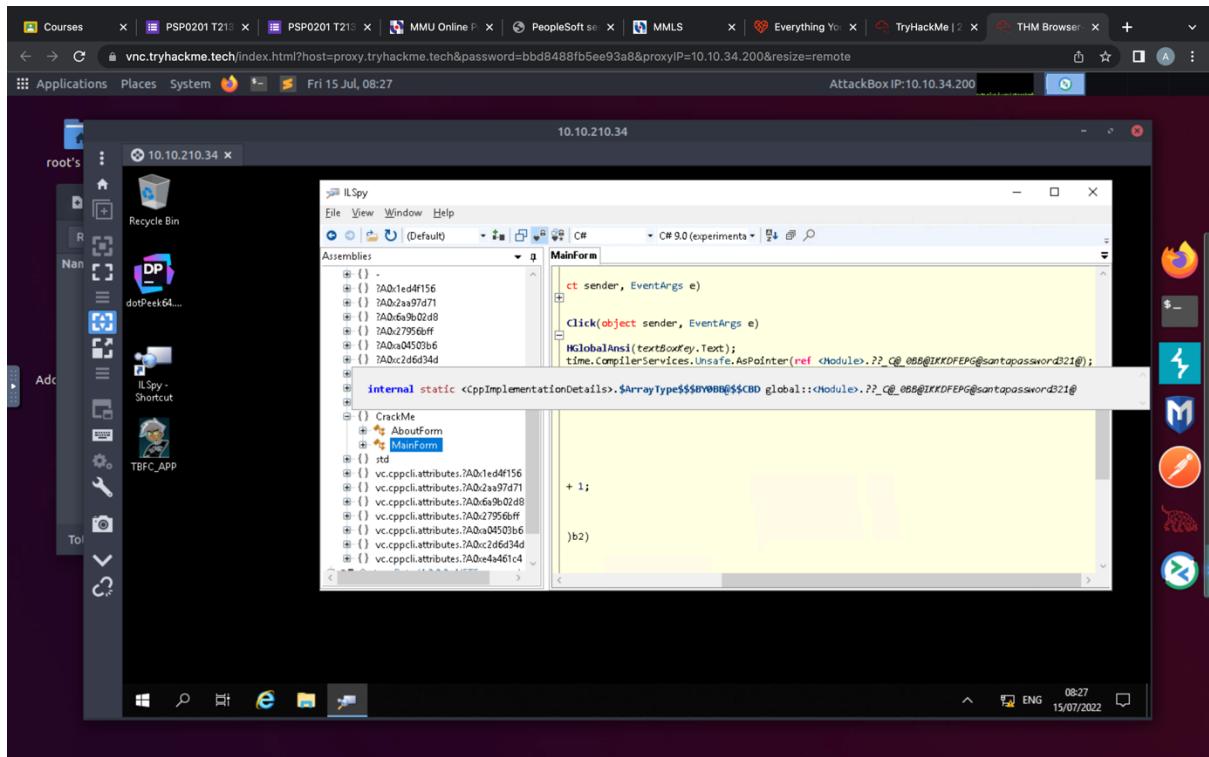
Question 5: Which method within the form from Q4 will contain the information we are seeking?

- Scroll through the MainForm and search for the activate button to find Santa's password and the flag.



Question 6: What is Santa's password?

- In the MainForm, find for the password module and double click on it.



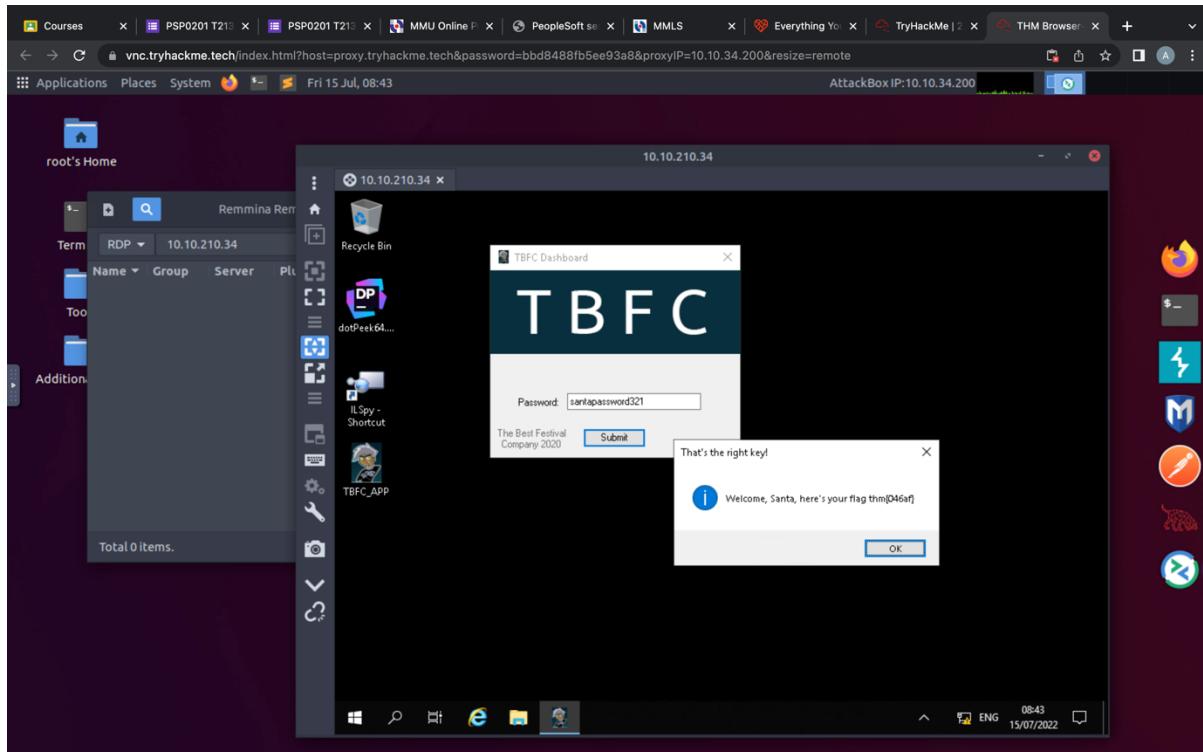
- Once redirected to Derived Types, copy the hexadecimal value displayed.
- Open Firefox and search for CyberChef.
- Paste the hex value in the input section and set the Recipe as From Hex.

The screenshot shows the CyberChef interface with the following details:

- Operations:** Favourites (To Base64, From Base64, To Hex, From Hex, To Hexdump, From Hexdump, URL Decode, Regular expression, Entropy, Fork, Magic).
- Recipe:** From Hex (Delimiter: Auto).
- Input:** 73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31 00
- Output:** santapassword321.
- Buttons:** STEP, BAKE!, Auto Bake.

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

- Copy the output value from CyberChef.
- Open the TBFC app and paste the password.
- The flag will be displayed once you have successfully logged in.



Thought process / Methodology

We first opened the Remmina app and type out the machine ip. Then we entered the username and password that was given in the task description. Once we launched the Windows. Then, we opened the TBFC app and entered anything as the password. After that we opened the ILSpy shortcut on the desktop page. We opened the TBFC app in the ILSpy and searched the CrackMe module for Santa's password and the flag. Once we found the hex value of Santa's password we opened CyberChef on Firefox to convert it into a string. We then opened the TBFC app again to use the correct password, we were greeted with a message and also the flag.

Day 19: Web Exploitation- The Naughty Or Nice List

Tools Used: Try Hack Me Attack Box, Firefox

Solutions/ Walkthrough:

Question 1

Searching on the names given to state on which list their names are on.

The image contains four separate screenshots of a web interface. Each screenshot shows a search bar with the placeholder '- Santa' and a 'Search' button. Below the search bar, a message indicates whether the name is on the Naughty or Nice list.

- Screenshot 1:** Name: Search. Message: Kanes is on the Naughty List.
- Screenshot 2:** Name: Search. Message: YP is on the Nice List.
- Screenshot 3:** Name: Search. Message: JJ is on the Naughty List.
- Screenshot 4:** Name: Search. Message: Tib3rius is on the Nice List.

Below these four screenshots is a large redacted area.

Question 2

Replacing the actual URL with the given URL to see what is displayed on the page.

A screenshot of a web browser window titled 'The Naughty or Nice List'. The address bar shows the URL '10.10.44.47/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F'. The page content includes a cartoon illustration of Santa's boots and a message: 'Not Found' followed by 'The requested URL was not found on this server'. At the bottom of the page, the word 'Admin' is prominently displayed in red.

Question 3

Obtaining the message displayed on the page when we replaced the URLD with the given.

The Naughty or Nice List

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

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

Admin

Question 4

Obtaining What is displayed on the page when the URL is replaced with the given.

The Naughty or Nice List - Mozilla Firefox

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

The List Admin

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!

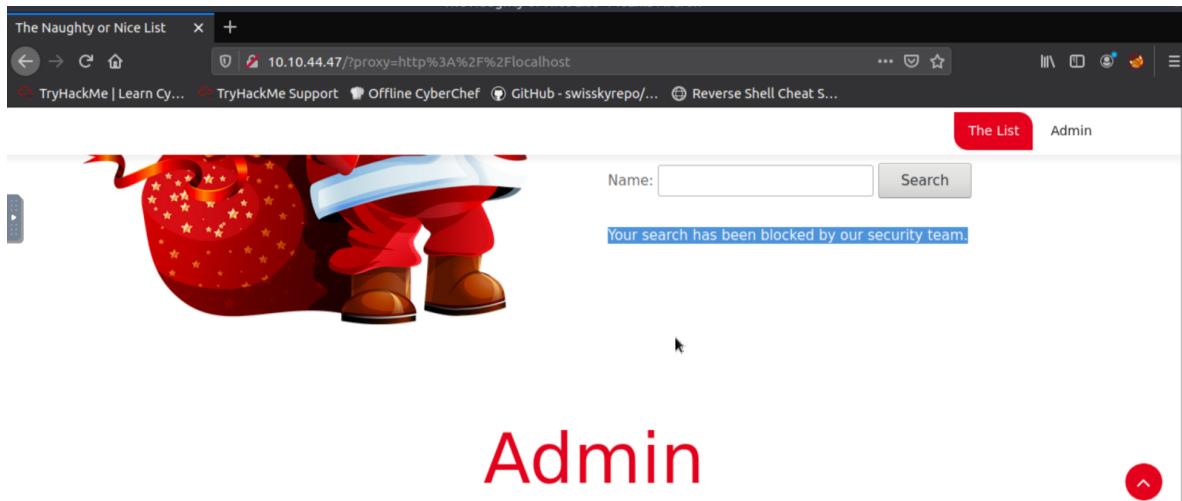
- Santa

Name: Search

Recv failure: Connection reset by peer

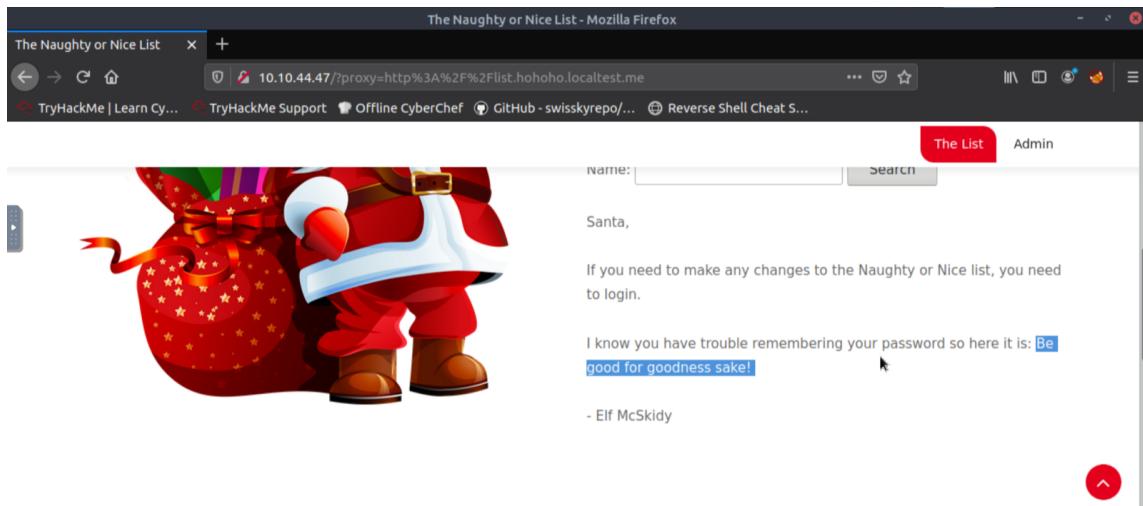
Question 5

Pasting the given URL to obtain what is displayed on the page.



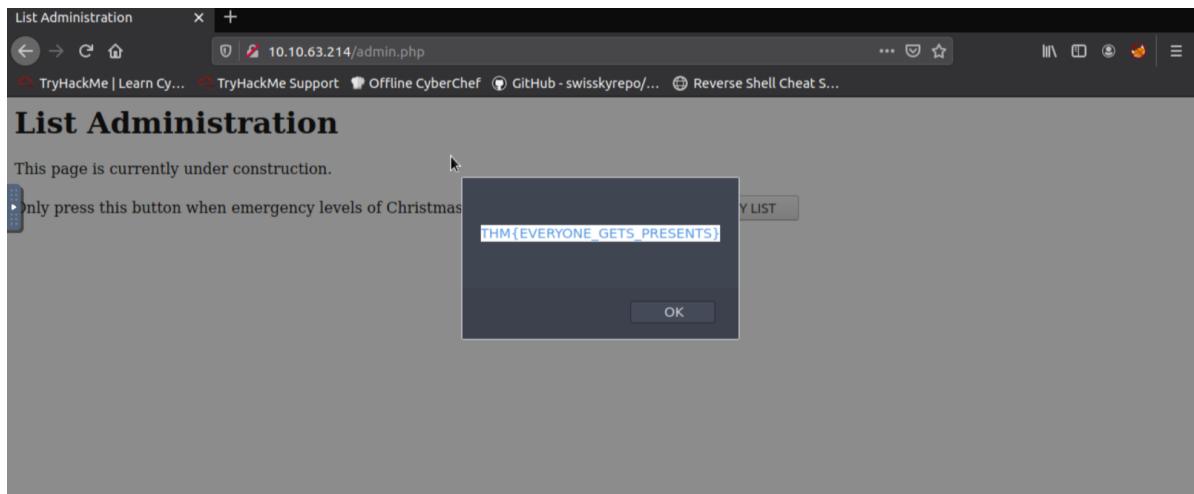
Question 6

Obtaining Santa's password by modifying the URL, by adding ".localhost.me"



Question 7

Obtaining the challenge flag by signing into the admin account and deleting the naughty list.



Thought Process/Methodology:

Starting off, we open Firefox and typed in the given IP address, we then proceeded to search on the given names on the naughty or nice list to check if their names were on the naughty or nice list. Moving on, we then replaced 4 different URL one at a time, with the existing one to acquire what is displayed on the page. Once we are done, we then moved on by modifying the URL by adding ".localtest.me" to it, to obtain Santa's password. Finally, we log into the Amin's account and deleted the naughty list to get the challenge flag.

Day 20 [Blue Teaming] Powershell to the rescue

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

In the terminal, type out ssh to display all the functions of each parameter.

New Tab x AvinElzio/PSP0201-Caustic-De x | What Kinds of Harmful Chem... x TryHackMe | 25 Days of Cyber... x New Tab x +

tryhackme.com/room/leancyberin25days

been hidden within ElfStation1. McEager moves quickly and attempts to RDP into the machine. Yikes! He is unable to log in.

Luckily, he has been learning PowerShell, and he can remote into the workstation using PowerShell over SSH.

Task: Use the PowerShell console to navigate throughout the endpoint to find the hidden contents to reveal what was hidden in the stockings.

[Watch JohnHammond's video on solving this task!](#)

You will use SSH to connect to the remote machine.

The command to run to connect to the remote machine: `ssh -l mceager MACHINE_IP`

```
root@ip-10-10-7-58:~# ssh -l mceager 3.248.248.138
```

Note that your IP address will be different. When prompted, enter the password: `r0ckStar!`

If you logged in successfully, you will see the following prompt.

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

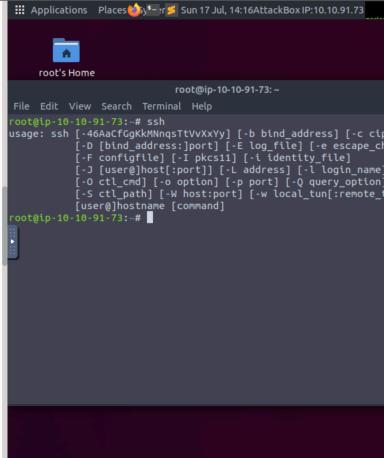
mceager@ELFSTATION1 ~
```

Before we begin, launch PowerShell and navigate to the Documents folder.

```
mceager@ELFSTATION1 ~
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\mceager>
PS C:\Users\mceager> Set-Location .\Documents
PS C:\Users\mceager\Documents>
```

Note: The virtual machine may take up to 3 minutes to load.



Question 2 : Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

After finding out the e1fone.txt file as the hidden file go ahead and cat the elfone.txt file and it will reveal the answer as shown below.

```
-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> ls

Directory: C:\Users\mceager\Documents

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

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

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?

After finding the hidden elf2 file go ahead and find the e70smsW10y4k.txt. Find the contents of this file and cat the e70smsW10y4k.txt and it will show the answer.

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

Question 4 : Search the Windows directory for a hidden folder that contains files for Elf 3.
What is the name of the hidden folder? (This command will take a while)

```
PS C:\Windows\System32> Get-ChildItem -Hidden -Directory -Filt  
  
Directory: C:\Windows\System32  
  
Mode          LastWriteTime      Length Name  
----          -----          ----  
d--h--       11/23/2020 3:26 PM           3lfthr3e  
  
PS C:\Windows\System32>
```

Use hidden directory to find the elf 3 file.

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

After finding the 1.txt file go ahead and get content and it should load up a bunch of words on your screen and after this you can measure object and it should come up to 9999 words.

```
Count    : 9999  
Average  :  
Sum      :  
Maximum  :  
Minimum  :  
Property :  
  
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Measure-Object  
  
Lines Words Characters Property  
----- ----- ----- -----  
      9999  
  
PS C:\Windows\System32\3lfthr3e>
```

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

Use get content 1.txt and get 551 which will show red and then find the word 6991 and it will show ryder thus making the answer red ryder.

```
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Select-
  551
Red
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Select-
  551, 6991
Red
Ryder
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Select
  991
Red
Ryder
PS C:\Windows\System32\3lfthr3e>
```

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)?

Use get content 2.txt and and select string redryder and it should show you the answer

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

```
PS C:\Windows\System32\3lfthr3e>
```

Thought Process and Methodology

To finish day 20 I first started with typing out ssh to display all the functions of each parameter. I then, found out the e1fone.txt file as the hidden file go ahead and cat the elfone.txt file and it will reveal the answer as shown. I continued by, finding the hidden elf2 file go ahead and find the e70smsW10y4k.txt. Find the contents of this file and cat the e70smsW10y4k.txt and it will show the answer. After that I used hidden directory to find the elf 3 file. After finding the 1.txt file go ahead and get content and it should load up a bunch of words on your screen and after this you can measure object and it should come up to 9999 words. Use get content 1.txt and get 551 which will show red and then find the word 6991 and it will show ryder thus making the answer red ryder. And finally, Use get content 2.txt and select string redryder and it should show you the answer