

# PSP0201

## Week 5

# Writeup

Group Name: Hacktocrats

Members

ID	Name	Role
1211103194	NUR FARAHIYA AIDA BINTI ABD RAZAK	Leader
1211103602	NUR ALIA AMELISA SYAZREEN BINTI MOHD SULEI	Member
1211103430	AINA SOFEA BINTI AMIER HAMZAH	Member
1211103237	NURUL AIN BINTI KAMARUDIN	Member

## Day 16: Help! Where Is Santa?

## Tools used: Terminal, Firefox

## Solution / walkthrough:

**Question 1:** nmap has been interred followed by our port number which lead us to know what was the port number for the web server

Deploy the machine that is running Santa's Sled and allow a couple of minutes for the target (10.10.151.54) 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?

80 Correct Answer

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

Answer format: /\*\*/Submit Hint

Where is Santa right now?

Answer format: \*\*\*\*\* \* \* \* \* , \* \* \* \* , \* \* \* \* \* 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.

To unblock yourself, simply terminate and re-deploy the target instance (10.10.151.54)

Answer format: \*\* Submit

Applications Places  Tue 12 Jul, 03:38 AttackBox IP:10.10.142.45

Santa's Tracker - | Woop woop! Your answer is correct.

Santa's Tracker x +

File Edit View Search Terminal Help

```
root@ip-10-10-142-45: ~
```

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-12 03:33 BST

Initiating ARP Ping Scan at 03:33

Scanning 10.10.151.54 [1 port]

Completed ARP Ping Scan at 03:33, 0.22s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 03:33

Completed Parallel DNS resolution of 1 host. at 03:33, 0.00s elapsed

Initiating SYN Stealth Scan at 03:33

Scanning ip-10-10-151-54.eu-west-1.compute.internal (10.10.151.54) [1000 ports]

- Discovered open port 22/tcp on 10.10.151.54
- Discovered open port 80/tcp on 10.10.151.54

Completed SYN Stealth Scan at 03:33, 1.25s elapsed (1000 total ports)

Nmap scan report for ip-10-10-151-54.eu-west-1.compute.internal (10.10.151.54)

Host is up (0.0024s latency).

Not shown: 998 closed ports

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

MAC Address: 02:B6:FC:B3:EE:1D (Unknown)

Read data files from: /usr/bin/../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds

Raw packets sent: 1002 (44.072KB) | Rcvd: 1002 (40.076KB)

```
root@ip-10-10-142-45: ~
```

**Category**

Lorem ipsum dolor sit amet  
Mastodon [https://mastodon.social](#)

1 You've started a streak. Keep it going for 6 days for a badge!

THM AttackBox

28°C Rain showers ENG 103822 12/7/2022

**Question 2:** this answer was obtained as we searched for our port number in firefox, it led us to the web browser. BULMA was clearly shown at the top left in the web browser.

The screenshot shows a Kali Linux desktop environment with a web browser window open. The browser title bar says "TryHackMe | 25 Days of... Santa's Tracker". The address bar shows "10.10.43.90:80" and "http://10.10.43.90/". The main content of the page is titled "Santa's Tracking System" and contains the following text:

Are you an Elf that Santa has forgotten? Use this system to track Santa! Note: due to how many humans try to find where Santa is, the link is hidden on this webpage. You're going to have to manually click every single link. Or perhaps there is a way to find all the links as fast as a Python?

Below this, there is a message box with the word "Important" in a red box:

All deliveries to Skidy for TryHackMe jumpers are to be stopped. That man has asked for 613 on the premise that they are the softest jumper in the world.  
Please, we need to share them out.

The browser interface includes a search bar with "Template not my own.", a sidebar with "BULMA" branding, and a status bar at the bottom showing network information (10.18.50.112) and battery level (87% 21:52).

**Question 3:** Then we proceed to firefox. We searched http followed by our port number and /api/. By pressing \*ctrl u\* we have obtained the directory for the API without using enumerations tools

The screenshot shows a web application interface. On the left, there is a sidebar with three task cards:

- Task 19** [Day 17] Reverse Engineering ReverseEngineering
- Task 20** [Day 18] Reverse Engineering The Bits of Christmas
- Task 21** [Day 19] Web Exploitation The Naughty or Nice List

The main area contains a form for entering a port number and an API key. The port number field has "80" entered, and the API key field has "/api/" entered. Below these fields are "Correct Answer" and "Hint" buttons. A "Submit" button is also present.

At the bottom of the main area, there is a message: "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." Below this, there is a note: "To unlock yourself, simply terminate and re-deploy the target instance (10.10.151.54)".

To the right of the form, a browser window is open showing the URL <http://10.10.151.54/>. The page content includes a list of categories and links, such as "Category 1" with links to "Lorem ipsum dolor sit amet", "Vestibulum errato isse", etc., and "Category 2" with links to "Aisia Caisis", "Murphy's law", "Flimsy Lavenrock", "Maven Mousie Lavender", etc.

**Question 4 & Question 5:** answer for question 4 and question 5 has been obtained by entering (our port number/api/\*the correct API key). It showed where Santa was.

The screenshot shows a web application interface with three questions:

- Q3:** Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key) \* 2 points  
Answer: /\*\*/  
/api/
- Q4:** Go the API endpoint. What is the Raw Data returned if no parameters are entered?  
Copy and paste from THM's website response. (See the Raw Data tab in Firefox.)  
Include the curly brackets.  
7:"q":"Winter Wonderland, Hyde Park, London."
- Q5:** Where is Santa right now? (Tick all correct answers.) \* 6 points  
 Colorado Springs  
 Pengu's Village  
 London  
 New York  
 Central Park  
 Santa's Castle  
 North Pole  
 Hyde Park

To the right of the questions, a Firefox browser window is open showing the URL <http://10.10.151.54/api/57>. The browser displays a JSON response: {"item": {"id": 57, "q": "Winter Wonderland, Hyde Park, London."}}

**Question 6:** this need to be done by using the try and error method, we have tried a few numbers till we obtained the right key which was 57

The screenshot shows a challenge interface on the left and a browser window on the right.

**Challenge Interface (Left):**

- Header: "Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)"
- Input field: "/api/"
- Buttons: "Correct Answer" and "Hint"
- Text area: "Answer format: \*\*\*\*\* \* \* \* \* \* , \* \* \* \* , \* \* \* \* \*"
- Submit button
- Text: "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."
- Text: "To unblock yourself, simply terminate and re-deploy the target instance (10.10.151.54)"
- Input field: "57"
- Buttons: "Correct Answer" and "Hint"
- List of tasks:
  - Task 19 [Day 17] Reverse Engineering ReverseELFneering
  - Task 20 [Day 18] Reverse Engineering The Bits of Christmas
  - Task 21 [Day 19] Web Exploitation The Naughty or Nice List
  - Task 22 [Day 20] Blue Teaming PowershELF to the rescue
  - Task 23 [Day 21] Blue Teaming Time for some ELForensics

**Browser Window (Right):**

- Title: Mozilla Firefox - Woop woop! Your answer is correct.
- URL: http://10.10.151.54
- Content: "Santa's Tracker" - TryHackMe | Learn Cy... - TryHackMe Support - Offline CyberChef - GitHub - swisskyrepo/...
- JSON Response:

```
item_id: 57
q: "Winter Wonderland, Hyde Park, London."
```

## **Thought process and methodology:**

First thing first, we use a map to scan the IP address and we get the port number of the IP Address. After that, we go to the web browser and search for "MACHINE\_IP:port" using our IP address and the port number that we got before. Then we view the page source of the website to find the directory for the API. From what we learn on day 15, we use python to obtain the correct API key. Finally we are able to know the information about Santa.

## Day 17 : Reverse Engineering - ReverseELFneering

Tools used: Terminal, Google Chrome

### Solution / Walkthrough:

#### Question 1 :

Refer TryHackMe web page on topic 3(Register me this, register me that...) to match data type in registers with their respective size in bytes

The screenshot shows a web browser window with the URL [tryhackme.com/room/learnyberin25days](https://tryhackme.com/room/learnyberin25days). The page content is as follows:

3. Register me this, register me that...

The core of assembly language involves using registers to do the following:

- Transfer data between memory and register, and vice versa
- Perform arithmetic operations on registers and data
- Transfer control to other parts of the program Since the architecture is x86-64, the registers are 64 bit and Intel has a list of 16 registers:

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

When dealing with memory manipulation using registers, there are other cases to be considered:

- (Rb, Ri) = MemoryLocation[Rb + Ri]
- D(Rb, Ri) = MemoryLocation[Rb + Ri + D]
- (Rb, Ri, S) = MemoryLocation(Rb + S \* Ri)
- D(Rb, Ri, S) = MemoryLocation[Rb + S \* Ri + D]

4. Read the instructions!

#### Question 2:

Browse through TryHackMe website to find command to analyse the program in radare2 which is: aa

tryhackme.com/room/learncyberin25days

Username: elfmceager  
Password: adventofcyber

Let's proceed to run through how Radare2 works exactly. Although you shouldn't do this if the program is unknown, it is safe for us to execute to see what should be happening like so:

```
ashu@ashu-Inspiron-5379 ~/D/t/c/christmas-re> ./file1
the value of a is 4, the value of b is 5 and the value of c is 9
```

The above program shows that there are 3 variables(a, b, c) where c is the sum of a and b.

Time to see what's happening under the hood! Run the command r2 -d ./file1

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

Note, when using the aa command in radare2, this may take between 5-10 minutes depending on your system.

Which is the most common analysis command. It analyses all symbols and entry points in the executable. The analysis, in this case, involves extracting function names, flow control information, and much more! r2 instructions are usually based on a single character, so it is easy to get more information about the commands.

i.e. For general help, we can run: ? or if we wish to understand more about a specific feature, we could provide a?

**3. Computer says...Done?!**

Once the analysis is complete, you would want to know where to start analysing from - most programs have an entry point defined as main. To find a list of the functions run: afl

```
[0x00400a30]> afl | grep main
```

### Question 3:

Browse further through TryHackMe webpage to find command to set a breakpoint in radare2 which is: db

tryhackme.com/room/learncyberin25days

```
0x0040003c    c74518050000 . movl $5, local_bh
0x00400063    8b55f4    movl local_ch, %edx
0x00400066    8b45f8    movl local_8h, %eax
0x00400069    01d0    addl %edx, %eax
0x0040006b    8945fc    movl %eax, local_4h
0x0040006e    8b4dfc    movl local_4h, %ecx
0x00400071    8b55f8    movl local_8h, %edx
0x00400074    8b45f4    movl local_ch, %eax
0x00400077    89c6    movl %eax, %esi
0x00400079    488d3d881409. leaq str.the_value_of_a_i
0x00400080    h80000000    movl $0, %eax
```

The line starting with sym.main indicates we're looking at the main function. The next 3 lines are used to represent the variables stored in the function. The second column indicates that they are integers(int), the 3rd column specifies the name that r2 uses to reference them and the 4th column shows the actual memory location.

The first 3 instructions are used to allocate space on that stack (ensures that there's enough room for variables to be allocated and more). We'll start looking at the program from the 4th instruction (movl \$.4). We want to analyse the program while it runs and the best way to do this is by using breakpoints.

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 0x00400055. 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.

```
0x00400a30> pdf @main
::: main:
(fen) sym.main 68
sym.main (int argc, char **argv, char **envp);
; var int local_ch @ rbp-0xc
; var int local_8h @ rbp-0x8
; var int local_4h @ rbp-0x4
; DATA XREF from entry0 (0x400a4d)
0x0040004d    55      pushq %rbp
0x0040004e    4889e5    movq %rsp, %rbp
```

### Question 4:

Scroll down to 4.Read the instructions! section in TryHackMe webpage to find commands to execute the program until we hit a breakpoint. The command is dc

tryhackme.com/room/learnyberin25days

Github Telegram WhatsApp MMLS Canvas Student Sci-Hub Z-Library CaMSys Rumah Terbuka IU ... TryHackMe | Dashb... code/dirty.c at master

```
sym.main (int argc, char **argv, char **envp);
; var int local_ch @ rbp-0xc
; var int local_8h @ rbp-0x8
; var int local_4h @ rbp-0x4
; DATA XREF from entry0 (0x4000a4d)
0x00400b4d    55          pushq %rbp
0x00400b4e    4889e5      movq %rsp, %rbp
0x00400b51    4883ec10    subq $0x10, %rsp
; size=16
```

Running `ds` 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 transferring the value 4 into the `local_ch` variable. To view the contents of the `local_ch` variable, we use the following instruction `px @memory-address`. In this case, the corresponding memory address for `local_ch` will be `rbp-0xc` (from the first few lines of `@pdf main`) This instruction prints the values of memory in hex.

```
[0x00400b55]> px @ rbp-0xc
- offset - 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0x7ffc914f7bc4 0000 0000 1890 6b00 0000 0000 7018 4000 .....k....p.0.
0x7ffc914f7bd4 0000 0000 1911 4000 0000 0000 0000 0000 .....@...
0x7ffc914f7be4 0000 0000 0000 0000 0000 0100 0000 f87c 4f91 .....|0...
0x7ffc914f7bf4 fc7f 0000 4dbb 4000 0000 0000 0000 0000 .....M.0...
0x7ffc914f7cb4 0000 0000 0600 0000 8e00 0000 8000 0000 .....0...
0x7ffc914f7c14 0a00 0000 0000 0000 0000 0000 0000 0000 .....0...
0x7ffc914f7c24 0000 0000 0000 0000 0000 0000 0000 0000 .....0...
0x7ffc914f7c34 0000 0000 0000 0000 0000 0000 0000 0004 4000 .....R..A93...0...
0x7ffc914f7c44 0000 0000 52db fe41 3933 915f 1019 4000 .....R...A93...0...
0x7ffc914f7c54 0000 0000 0000 0000 0000 0000 1890 6b00 .....0...
0x7ffc914f7c64 0000 0000 0000 0000 0000 0000 52db de86 .....R...
0x7ffc914f7c74 2711 68a0 52db 8a50 3933 915f 0000 0000 'h.R..P93...
0x7ffc914f7c84 0000 0000 0000 0000 0000 0000 0000 0000 .....0...
0x7ffc914f7c94 0000 0000 0000 0000 0000 0000 0000 0000 .....0...
```

## Question 5:

If we run `ds` command, it will execute `mov` instruction that will move value 1 into `local_ch` variable

Sharing this tab to meet.google.com Stop sharing View tab: meet.google.com

- set appropriate breakpoints
- use `ds` to move through instructions and check the values of register and memory
- if you make a mistake, you can always reload the program using the `oad` command

You may find this [radare2 cheatsheet](#) useful in your adventures...

6. Challenge

Use your new-found knowledge of Radare2 to analyse the "challenge1" file in the Instance [10.10.198.63](http://10.10.198.63) that is attached to this task to answer the questions below.

Answer the questions below

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

Correct Answer

What is the value of `eax` when the `imull` instruction is called?

Correct Answer

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

Correct Answer

elfmceager@bfc-day-17:~

```
File Edit View Search Terminal Help
0x00400a4d 48c7c74d0b40. mov rdi, sym.main ; 0x40004d
d 0x00400a54 67e880030000 call sym._libc_start_main ; int __libc_start_main(void *main, int argc, char **argv, void (*init)(void), void (*fini)(void), void *stack_end)
[0x00400a30]> pdf @main
;--- main:
;--- main:
(tcn) 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_4h], 1
0x00400b58 c745f8060000. mov dword [local_8h], 6
0x00400b5f 8b45f4        mov eax, dword [local_ch]
0x00400b62 0faf45f8      imul eax, dword [local_ch]
0x00400b66 8945fc        mov dword [local_4h], eax
0x00400b69 b800000000    mov eax, 0
0x00400b6e 5d             pop rbp
0x00400b6f c3             ret
```

Task 20 [Day 18] Reverse Engineering The Bits of Christmas

THM AttackBox 14m 04s

## Question 6:

When imull instruction is called, the value inside eax will be multiplied by the value inside dword[local\_8h]. At first, value 1 inside dword[local\_ch] was moved into eax. After that, the value 1 is multiplied by the value inside dword[local\_8h] which is 6. Therefore, the product value is 6

The screenshot shows a web browser with multiple tabs open. The main tab displays a challenge page for "tryhackme.com/room/learnycberin25days". The challenge involves reverse engineering a program. The terminal window on the right shows assembly code from the file `sym.main`:

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

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

```
0x00400a4d 49c7c74d0b40. mov rdi, sym.main ; 0x400b4
```

```
0x00400a54 67e886030000 call sym._libc_start_main ; int __l
```

```
IBC_start_main(func_main, int argc, char ***ubp_av, func init, func finit, func rt
```

```
ld_fini, void *stack_end)
```

```
[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)
```

```
0x00400a4d 55 push rbp
```

```
0x00400a4e 4889e5 mov rbp, rsp
```

```
0x00400a51 c745f4010000. mov dword [local_ch], 1
```

```
0x00400a58 c745f8060000. mov dword [local_8h], 6
```

```
0x00400a5f 8b45f4 mov eax, dword [local_ch]
```

```
0x00400a62 0faf45f8 imul eax, dword [local_8h]
```

```
0x00400a66 8945fc mov dword [local_4h], eax
```

```
0x00400a69 b800000000 mov eax, 0
```

```
0x00400a6e 5d pop rbp
```

```
0x00400a6f c3 ret
```

The terminal window title is "Applications Places Terminal Tue 12 Jul, 05:28 AttackBox IP:10.10.80.213". The status bar at the bottom right says "13m 32s".

## Question 7:

The value 6 inside the eax variable was transferred into dword[local\_4h]. Thus, the final value for local\_4h before eax is set to 0 is 6.

The screenshot shows a web browser with multiple tabs open. The main tab displays a challenge page for "tryhackme.com/room/learnycberin25days". The challenge involves reverse engineering a program. The terminal window on the right shows assembly code from the file `sym.main`:

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

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

```
0x00400a4d 49c7c74d0b40. mov rdi, sym.main ; 0x400b4
```

```
0x00400a54 67e886030000 call sym._libc_start_main ; int __l
```

```
IBC_start_main(func_main, int argc, char ***ubp_av, func init, func finit, func rt
```

```
ld_fini, void *stack_end)
```

```
[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)
```

```
0x00400a4d 55 push rbp
```

```
0x00400a4e 4889e5 mov rbp, rsp
```

```
0x00400a51 c745f4010000. mov dword [local_ch], 1
```

```
0x00400a58 c745f8060000. mov dword [local_8h], 6
```

```
0x00400a5f 8b45f4 mov eax, dword [local_ch]
```

```
0x00400a62 0faf45f8 imul eax, dword [local_8h]
```

```
0x00400a66 8945fc mov dword [local_4h], eax
```

```
0x00400a69 b800000000 mov eax, 0
```

```
0x00400a6e 5d pop rbp
```

```
0x00400a6f c3 ret
```

The terminal window title is "Applications Places Terminal Tue 12 Jul, 05:28 AttackBox IP:10.10.80.213". The status bar at the bottom right says "13m 04s".

Thought process and methodology:

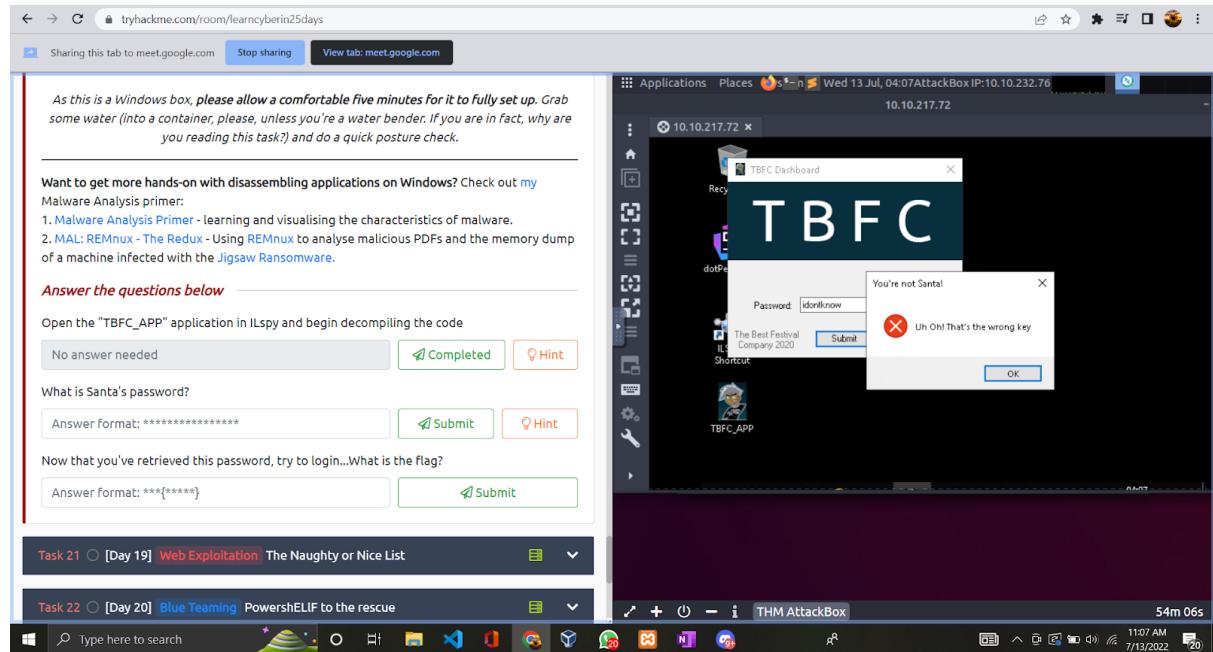
We need to SSH the target ip address given prior running the binary in debugging mode using radare2. After that, we ask radare2 to analyse the program using aa command and open a list of functions using afl command. Next, we need to find the main function in the list and examine the assembly code inside the main function using command pdf @main. Before executing the instructions, a breakpoint was set to allow us to look at the state of the program at a particular point. Run dc command to execute the program until breakpoint, and px @memory-address command to view the contents in the variables. Run ds command to execute the current instruction that we are at and go to the next one. In Day 17 task, ds command allows us to move a value into the variable stated. We can also run the dr command to view the register variable and check if the values are correct.

## Day 18 - [Reverse Engineering] The Bits of Christmas

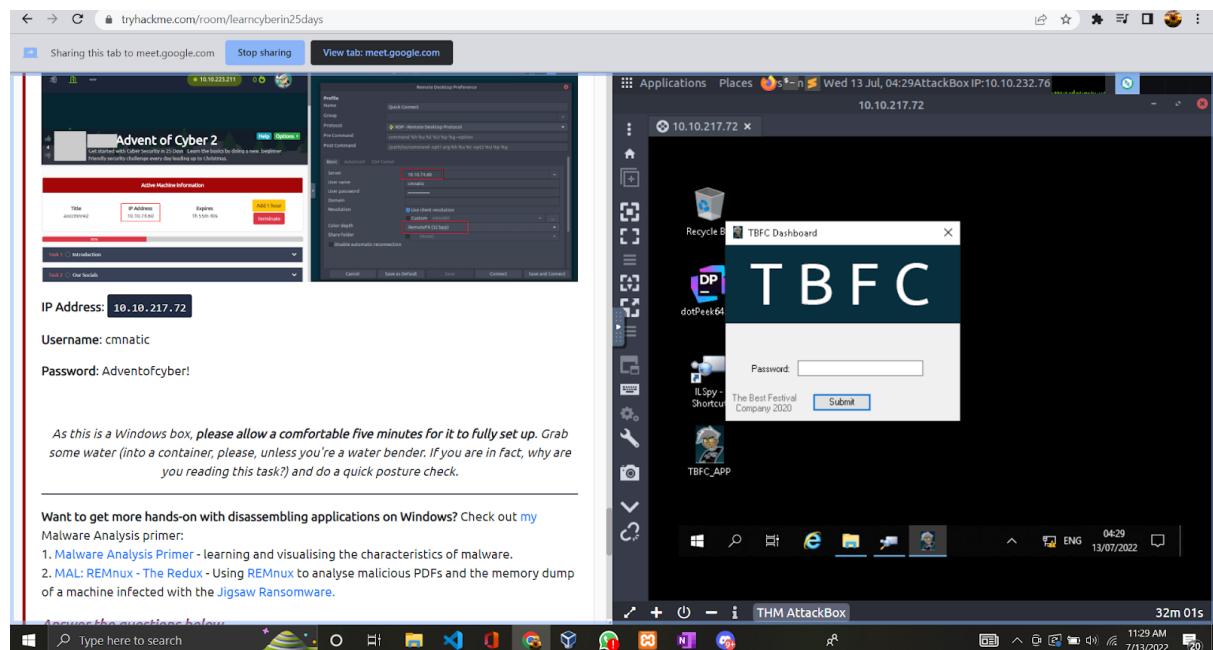
**Tools used:** Remmina, TBFC\_APP, ILSPY Window.

### Solution/walkthrough:

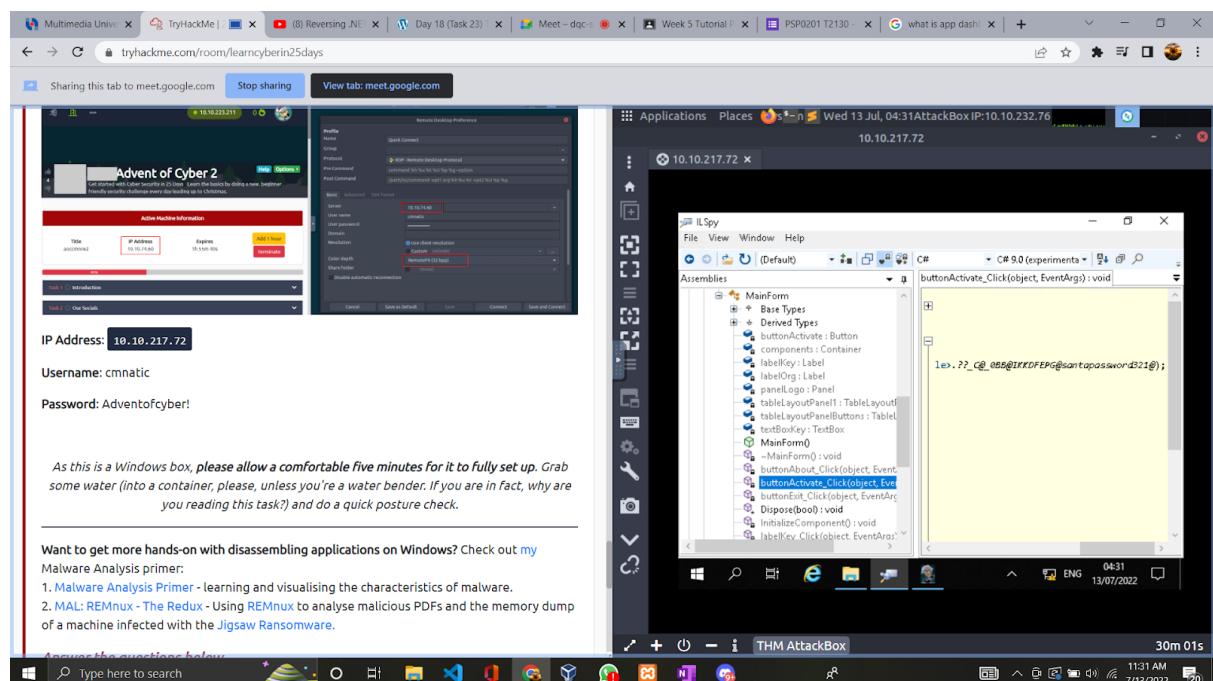
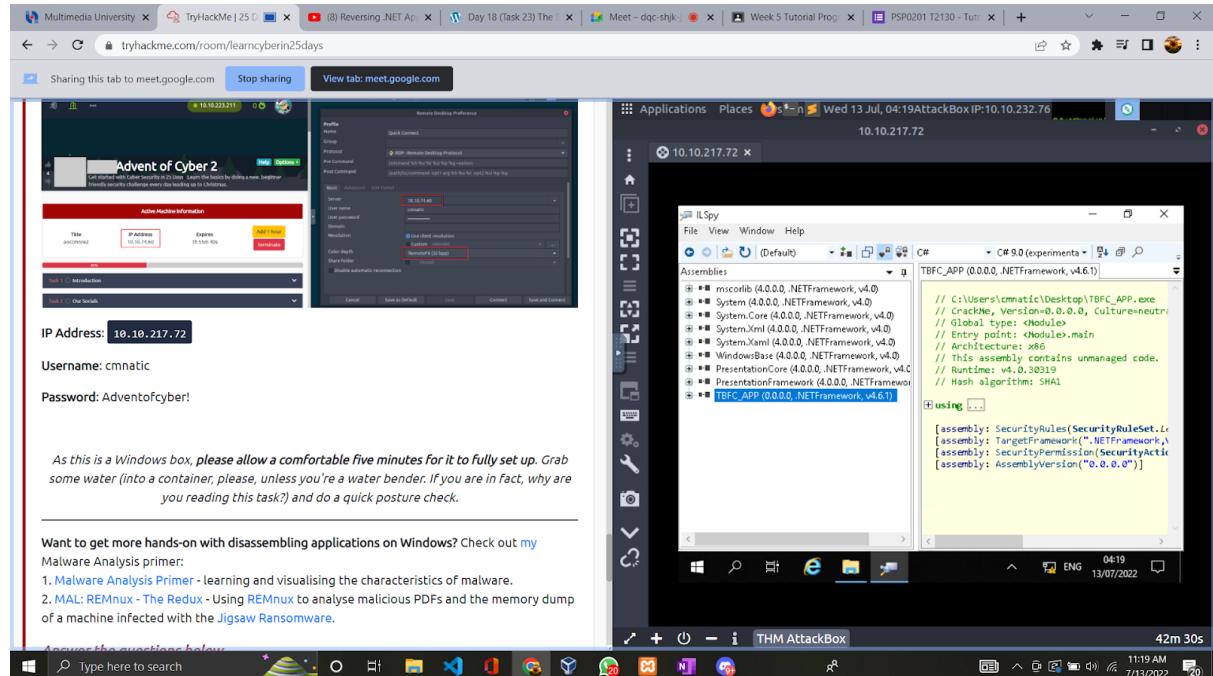
Question 1: open remmina, then enter IP address, hit enter, and accept certificate. Enter the username of cmnatic and the password of Adventofcyber! After logging in, open the TBFC\_APP and enter any keys for the password.



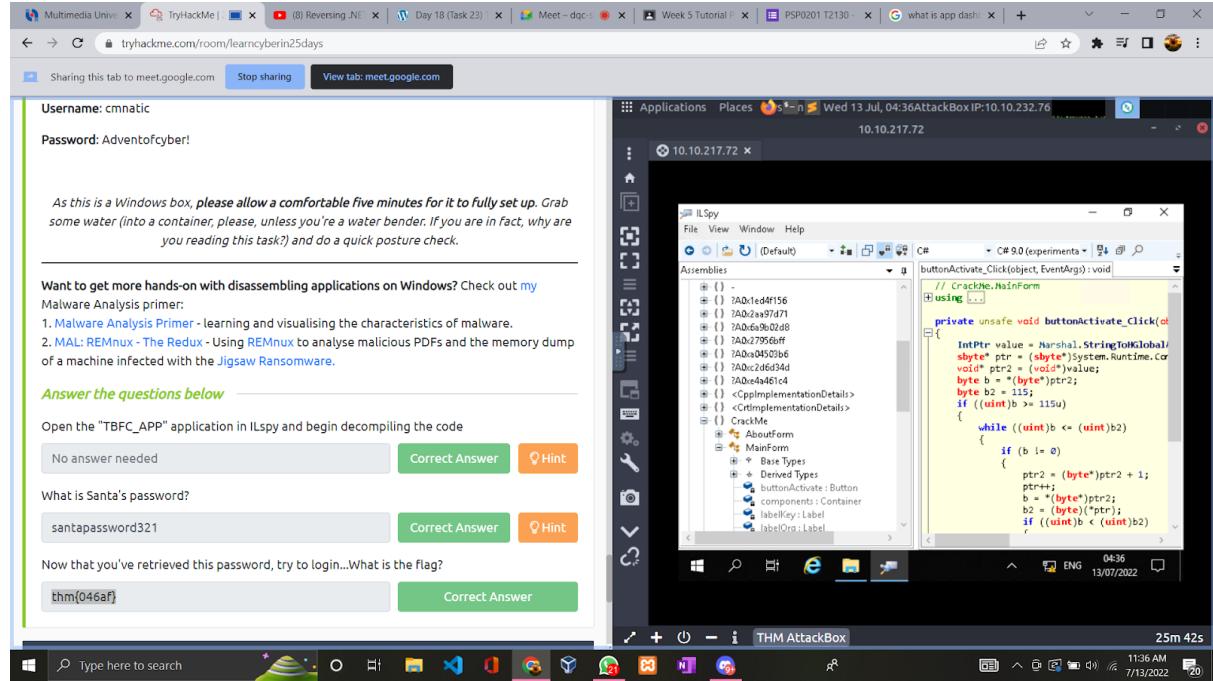
Question 2: when open the TBFC, the dashboard App itself will show the words TBFC stand for.



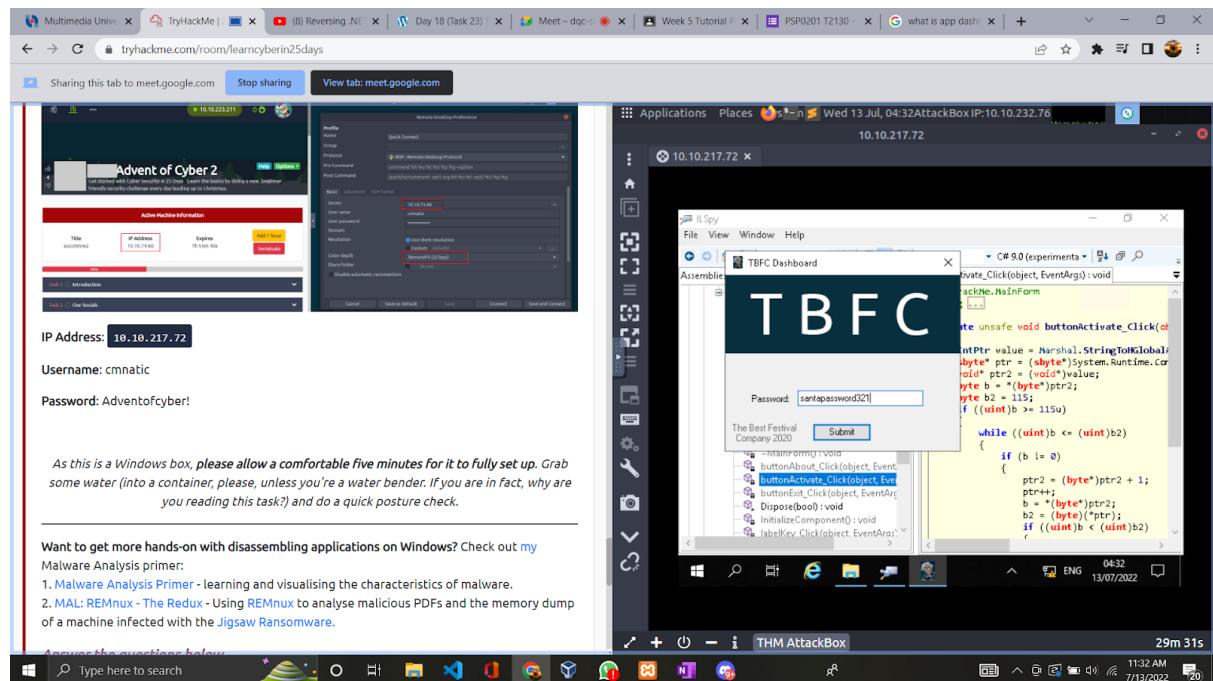
Question 3: Open the ILSpy – Shortcut and then drag the TBFC\_APP into the ILSPY Window. The Crackme file, has the password for the TBFC\_APP



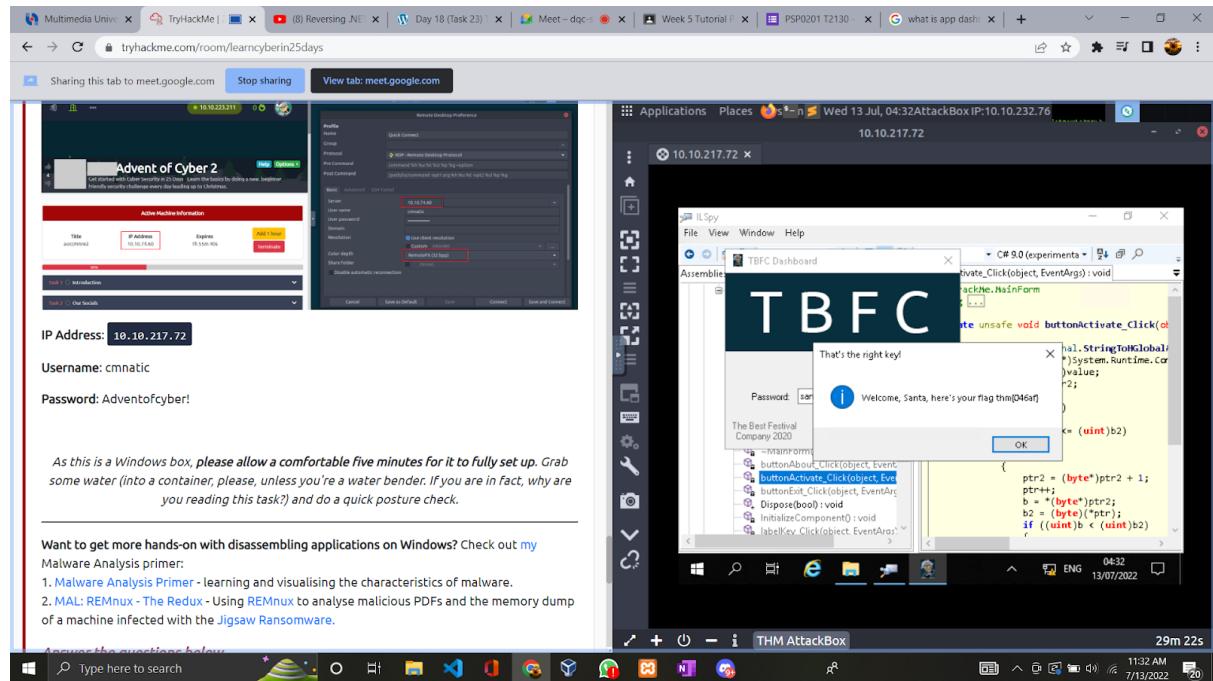
Question 4 and question 5: We can see it appears in MainForm.buttonActivate\_Click. That makes sense because when we click the submit button the error message appears. Double click on the MainForm and look at the code.



Question 6: There's a reference to santapassword321, maybe that's the password!



Question 7: After submitting the password, the flag is shown.



### Thought Process/Methodology:

The TBFC APP code will be decompiled using ILspy. Finding the password will allow us to access the programme. The flag will be sent to us once we log in. We can use the ILspy and try to find the hidden password in the specific files. Thus, we have to find the files and seek the hidden password in those codes.

## DAY 19 : Web Exploitation- The Naughty or Nice List.

Tools used: Firefox

### Solution/Walkthrough:

#### Question 1:

Type the IP address for this task on FireFox. We will be directed to a web page that can be used to look for the naughty and nice kids name. Refer to the google form and enter every name stated in it into the search box.

Sharing this tab to meet.google.com Stop sharing View tab: meet.google.com

tryhackme.com/room/learncyberin25days

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

YP is on the Nice List.

Admin

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!

THM AttackBox

13/7/2022 11:56 AM 48m 41s

## Question 2:

We modify the current URL by fetching the root of the same site. This will return the below message to us. This indicates that we succeeded in requesting the latest URL.

The screenshot shows a Windows desktop environment. At the top, there's a taskbar with various icons. In the center, a Firefox browser window is open. The address bar shows 'tryhackme.com/room/learn cyberin25days'. Below the address bar, there are sharing options: 'Sharing this tab to meet.google.com' with 'Stop sharing' and 'View tab meet.google.com'. The main content area of the browser shows two separate pages side-by-side. The left page is a text-based guide about SSRF and port enumeration. The right page is a 'The Naughty or Nice List' page from TryHackMe. It has a search bar at the top with 'Name:' and 'Search' buttons. Below it, the text 'Not Found' is displayed with the message 'The requested URL was not found on this server.' Further down, there's a red 'Admin' section containing 'Username:' and 'Password:' fields, along with a large red circular button. At the bottom of the browser window, a notification says '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! Refresh Firefox...'. The status bar at the bottom of the screen shows the date and time as 'Wed 13 Jul, 05:21' and '13/7/2022'.

## Question 3:

We try to change the port number of the URL from 8080 to 80. The below message will pop up stating that port 80 is not open for list.hohoho.

This screenshot is similar to the previous one, showing a Windows desktop with a Firefox browser window. The address bar shows 'tryhackme.com/room/learn cyberin25days'. The browser content area displays the same text-based guide on SSRF and port enumeration on the left, and the 'The Naughty or Nice List' page on the right. The right page includes a 'Name:' search field, a 'Not Found' message, an 'Admin' section with 'Username:' and 'Password:' fields, and a 'Failed to connect to list.hohoho port 80: Connection refused' message at the bottom. The status bar at the bottom of the screen shows the date and time as 'Wed 13 Jul, 05:20' and '13/7/2022'.

## Question 4:

Try changing the port number again by using SSH port,22. It shows that port 22 is open for list.hohoho but since SSH and HTTP are both different protocols, there's nothing we can do about it.

The screenshot shows a browser window with a guide on the left and a Firefox window on the right. The guide discusses changing ports and SSRF. The Firefox window shows a 'The Naughty or Nice List' page with a message about being on the naughty list and a search field. A tooltip at the bottom right of the Firefox window says '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! Refresh Firefox...'. The taskbar at the bottom shows various icons and the date/time: 12:23 PM 13/7/2022.

## Question 5:

Another thing that we can do is by replacing list.hohoho hostname to localhost. In return, the security team will block our search as they allow hostname "list.hohoho" only.

The screenshot shows a browser window with a guide on the left and a Firefox window on the right. The guide discusses bypassing a hostname check by using a local subdomain. The Firefox window shows a 'The Naughty or Nice List' page with a search field and a message about being blocked. A tooltip at the bottom right of the Firefox window says '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! Refresh Firefox...'. The taskbar at the bottom shows various icons and the date/time: 12m 02s.

## Question 6:

Since we now know that we need to use only list.hohoho hostname, we can create our own domain for example in this task, we use localtest.me to resolve to 127.0.0.1. Add the domain to the hostname and search the current URL. We now found a running web server and we can see Santa's password left by ElfMcSkidy.

The screenshot shows a Windows desktop environment. On the left, a browser window displays a challenge page from tryhackme.com. The page contains instructions about DNS subdomains and how to bypass a check for a local service. It also lists two tasks: Task 22 and Task 23. Task 22 is completed, while Task 23 is pending. On the right, another browser window titled "The Naughty or Nice List" is open, showing a message from Santa. Below it, a smaller window titled "THM AttackBox" is visible, displaying a message about Firefox being restarted. The taskbar at the bottom shows various pinned icons and the system clock indicating 7:42 AM on 17/7/2022.

tryhackme.com/room/learn cyber in 25 days

start with "list.hohoho", we can take advantage of DNS subdomains and create our own domain "list.hohoho.evilsite.com" which resolves to 127.0.0.1. In fact, we don't even need to buy a domain or configure the DNS, because multiple domains already exist that let us do this. The one we will be using is localtest.me, which resolves every subdomain to 127.0.0.1.

We can therefore set the hostname in the URL to "list.hohoho.localtest.me", bypass the check, and access local services: <http://10.10.76.240/?proxy=http%3A%2F%2Flist.hohoho.localtest.me>

Success! It appears that there is a web server running locally, and it has a message from Elf McSkidy that contains some sensitive information we can use!

8. Click the "Admin" link at the top or scroll down to the login. Guess the username and use the password you found to login as Santa.

9. Delete the naughty list to find the challenge flag!

**Answer the questions below**

What is Santa's password?

Be good for goodness sake! Correct Answer

What is the challenge flag?

THM{EVERYONE\_GETS\_PRESENTS} Correct Answer

Task 22 [Day 20] Blue Teaming Powershell to the rescue

Task 23 [Day 21] Blue Teaming Time for some ELForensics

The Naughty or Nice List - Mozilla Firefox

Sun 17 Jul, 00:42 AttackBox IP:10.10.138.108

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

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub swisskyrepo/...

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 log in.

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

- Elf McSkidy

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!

Refresh Firefox... 43m 12s

26°C Mostly clear

Windows Start Menu

7:42 AM 17/7/2022

## Question 7:

Login to the admin page using the password we got and username Santa. Click delete the naughty list and now we found the flag!

Success! It appears that there is a web server running locally, and it has a message from Elf McSkidy that contains some sensitive information we can use!

8. Click the "Admin" link at the top or scroll down to the login. Guess the username and use the password you found to login as Santa.

9. Delete the naughty list to find the challenge flag!

**Answer the questions below**

What is Santa's password?

Be good for goodness sake! Correct Answer

What is the challenge flag?

Answer format: \*\*\*{\*\*\*\*\*} Submit

Task 22 [Day 20] Blue Teaming PowersELIF to the rescue

Task 23 [Day 21] Blue Teaming Time for some ELForensics

Task 24 [Day 22] Blue Teaming Elf McEager becomes CyberElf

Task 25 [Day 23] Blue Teaming The Grinch strikes again!

Task 26 [Day 24] Final Challenge The Trial Before Christmas

**List Administration**

This page is currently under construction.

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

DELETE NAUGHTY LIST

THM{EVERYONE\_GETS\_PRESENTS}

OK

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! Refresh Firefox... 46m 38s

26°C Mostly clear

7:39 AM 17/7/2022

## Thought process/Methodology:

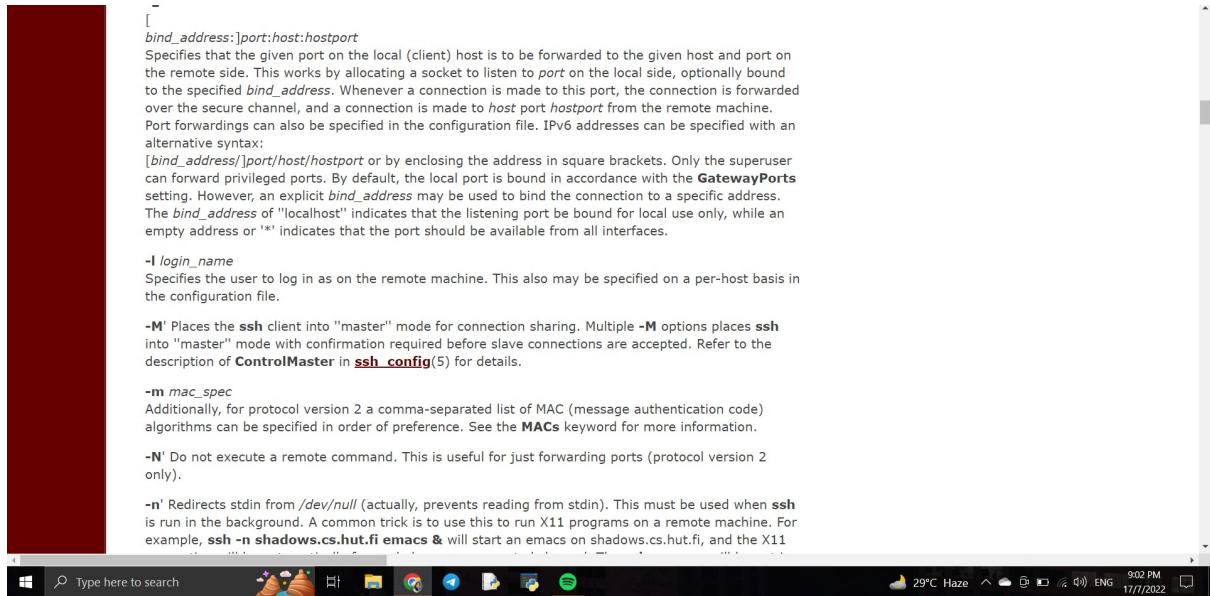
In this task, we use Server-Side Request Forgery to force web applications to request resources that would benefit us. Since we want to exploit the web page that contains a list of the nice and naughty kids, we have to figure out the things we can modify to the original URL so that we can access the admin page later on. It could be modifying the port number, domain and whatsoever. Finally, after trying out many changes, we will get the latest modified URL that we can use to see the password to the admin page and login to delete the naughty list. After deleting the list, the flag will be shown.

## DAY 20 : Blue Teaming - Powershell to the rescue

Tools used: kali, powershell

### Solution/Walkthrough:

**Question 1:** as we checked the ssh manual, the -l parameter function has been shown



**Question 2:** the machine has been deployed and then we successfully open the powershell. The cd command has been used to go to the document folder. Then, the Get-ChildItem command has been used in order to see the hidden treasure in the folder.

```
PowerShell 7.1.3
Copyright (c) Microsoft Corporation. IP Address
https://aka.ms/powershell ABC20 10.10.53.118
Type 'help' to get help.

[Search on the desktop for a hidden folder that contains the file for Elf 2. Re]
[—(1211103282㉿kali)-[/home/1211103282]
PS> ssh -l mceager 10.10.53.118
The authenticity of host '10.10.53.118 (10.10.53.118)' can't be established.
ED25519 key fingerprint is SHA256:X2ViBkllQoHmAsXFoem36jkL9faKH+Fr2lt2dd/kIYW.
This host key is known by the following other names/addresses:
 ~/ssh/known_hosts:5: [hashed name]
 ~/ssh/known_hosts:8: [hashed name]
 ~/ssh/known_hosts:9: [hashed name]
 ~/ssh/known_hosts:11: [hashed name]First file containin
 ~/ssh/known_hosts:12: [hashed name]
 ~/ssh/known_hosts:13: [hashed name]
 ~/ssh/known_hosts:14: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.53.118' (ED25519) to the list of known hosts.
mceager@10.10.53.118's password: [REDACTED]
```

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

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

PS C:\Users\mceager> [REDACTED]

```
PS C:\Users\mceager> cd Documents
PS C:\Users\mceager\Documents> Get-ChildItem -Hidden
[Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder? (This command]
[Directory: C:\Users\mceager\Documents
[...]
Mode LastWriteTime Length Name
d--hsl 12/7/2020 10:28 AM My Music
d--hsl 12/7/2020 10:28 AM My Pictures
d--hsl 12/7/2020 10:28 AM My Videos
-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
cat : Cannot find path 'C:\Users\mceager\Documents\elfone' because it does not exist.
At line:1 char:1 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 w
+ cat elfone
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Users\mceager\Documents\elfone:String) [Get-Content], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand
```

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

**Question 3:** the command cd has been used to change the location to the desktop. After that, the Get-Children has been used with the -Hidden parameter to find the hidden folder. A folder named elf2wo has been found using the cd command again, we were in the elf2wo folder. Again, by using the Get-Children command, a file named e70smsW10Y4k.txt has been seen. We opened it using cat command and a file named that elf 2 wants has been seen

```
PS C:\Users\mceager\Documents> cd..
PS C:\Users\mceager> cd Desktop
PS C:\Users\mceager\Desktop> Get-ChildItem -Hidden
    Scrooged
Directory: C:\Users\mceager\Desktop
Search the Windows directory for a hidden folder that contains the file.

Mode          LastWriteTime      Length Name
--           <--->           <--->   <---> 
d--h--       12/7/2020 11:26 AM        0   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 -Hidden
PS C:\Users\mceager\Desktop\elf2wo> Get-ChildItem
This is only half the answer. Search in the 2nd file for the phrase "I want the movie Scrooged <3!".
Directory: C:\Users\mceager\Desktop\elf2wo
Search in the 2nd file for the phrase "I want the movie Scrooged <3!".

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>
```

**Question 4:** Then, the directory has been changed to Windows by using the cd command and system32 has been entered by using cd command again. After that, Get-Children command with -Hidden, -Filter “\*3\*” parameter to find the hidden folder named 3lfthr3e

```
PS C:\Users\mceager\Desktop\elf2wo> cd :\Windows\
cd : Cannot find path 'C:\Users\mceager\Desktop\elf2wo\:\Windows\' because it does not exist.
At line:1 char:1
+ cd :\Windows\
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Users\mceage...f2wo\:\Windows\:String) [Set-Location], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\Users\mceager\Desktop\elf2wo> cd C:\windows\<the first file>
PS C:\Windows> cd System32
PS C:\Windows\System32> Get-ChildItem -Hidden -Directory -Filter "*3*"

Directory: C:\Windows\System32<answer. Search in the 2nd file for the phrase from the previous question to get the full answer. What does Bill want? (use <submitting his answer)>

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

**Question 5:** Then, we used the cd command to go to the 3lfthr3e folder and used the Get-Children command with -Hidden parameter to see the files in the folder. After that, we used Get-Content command to see the contents of the first file and pipe the result by using Measure-Object with -Word parameter to see how many word does the first file contain

```
PS C:\Windows\System32> cd 3lfthr3e
PS C:\Windows\System32\3lfthr3e> Get-ChildItem -Hidden
How many words does the first file contain?

Directory: C:\Windows\System32\3lfthr3e

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

This is only half the answer. Search in the 2nd file for the phrase from the previous question to get the full answer.
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Measure-Object -Word

Lines Words Characters Property
----- ----- ----- -----
9999
```

**Question 6:** by using the Get-Contact parameter in a bracket to open the first file and using the square brackets to put in the index in order to see the exact position in this file

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

**Question 7:** last but not least, we used the Get-Content command in order to open the second file and pipe the result using Select-String with -Pattern "redryder" parameter to find what elf 3 wants.

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

### Thoughts Process / Methodology:

First, we launch a terminal and enter our IP address to connect to the host. To start it, we navigate to PowerShell. We go to the Documents directory.

Following that, we enter the directory to view all contents. One of the files listed there is called "e1fone.txt." We use the cat command to read the file and display the results. Next, we use the "Get-ChildItem -Directory -Hidden -ErrorAction SilentlyContinue" command to search 'elf2wo. Enter the "elf2wo" directory and list the directories there. It has a file named "e70smsW10Y4k.txt." To display the output, we use the cat command. Next, we go to Windows and run the "Get-ChildItem -Directory -Hidden -ErrorAction SilentlyContinue -Filter 3" command, which lists "3lfthr3e". We enter the directory "3lfthr3e" and list the file there. It contains two files. Using the 'Measure-Object -Word' command, which displayed the words in the first file. Then we use the '(Get-Content.1.txt)[551]' and '(Get-Content.1.txt)[6991]' commands to see the words. Next, we use the 'Select-String -Pattern redryder' command to display the output.