PSP0201

Week 5

Writeup

Group Name: CyberQuest

Members

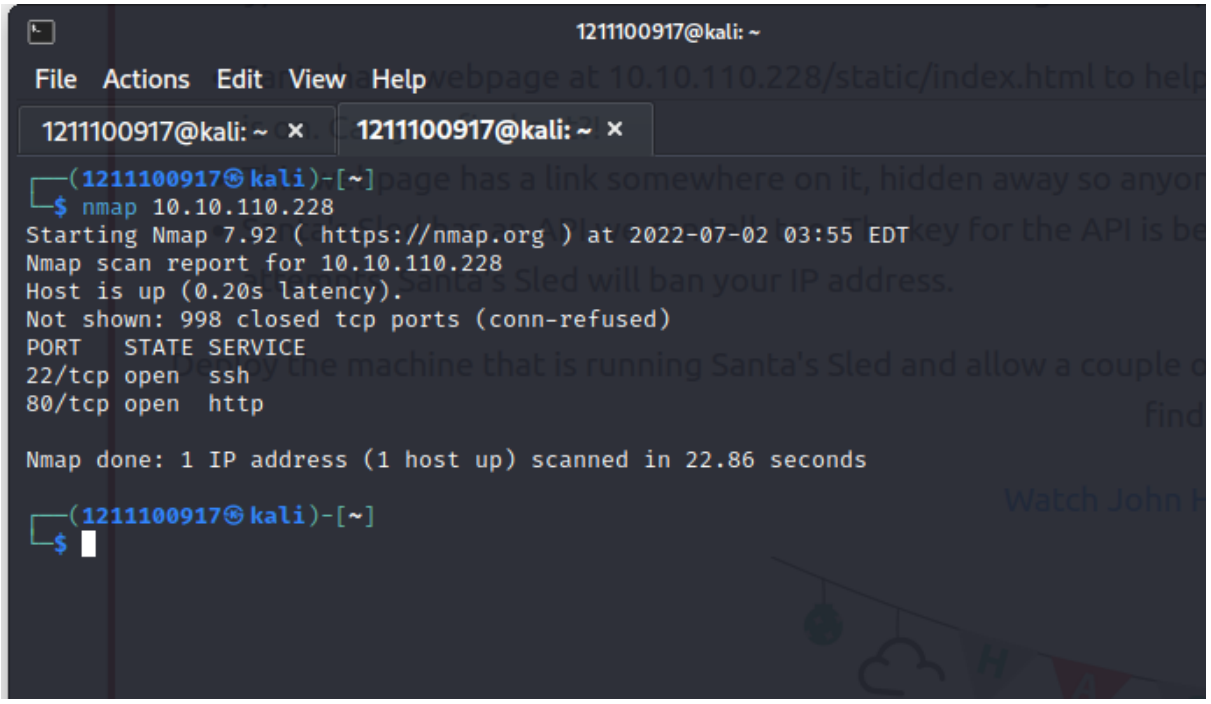
ID	Name	Role
1211102409	CHUA KAI ZHENG	Leader
1211102696	LEE JIA MENG	Member
1211100917	NATALIE TAN LI YI	Member

Day 16 : Scripting - Help! Where is Santa?

Tools : Sublime Text, Kali Linux, FireFox, Terminal

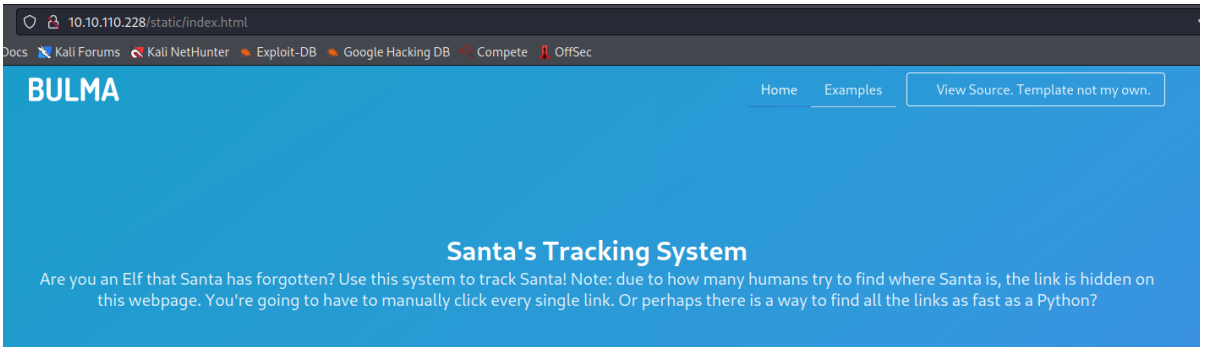
Question 1

Find port number for the web server using nmap



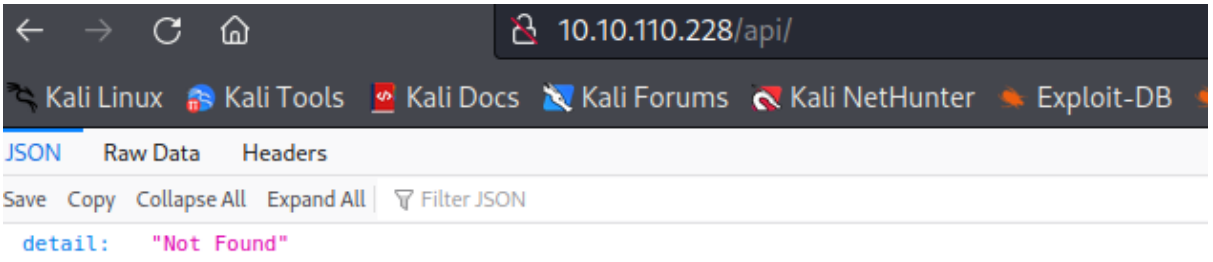
Question 2

Getting templates that are being used from website



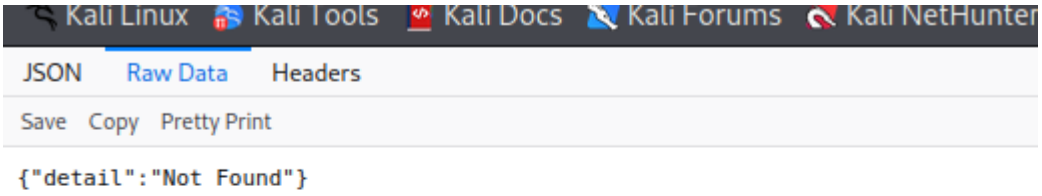
Question 3

Finding api of website using “/api”



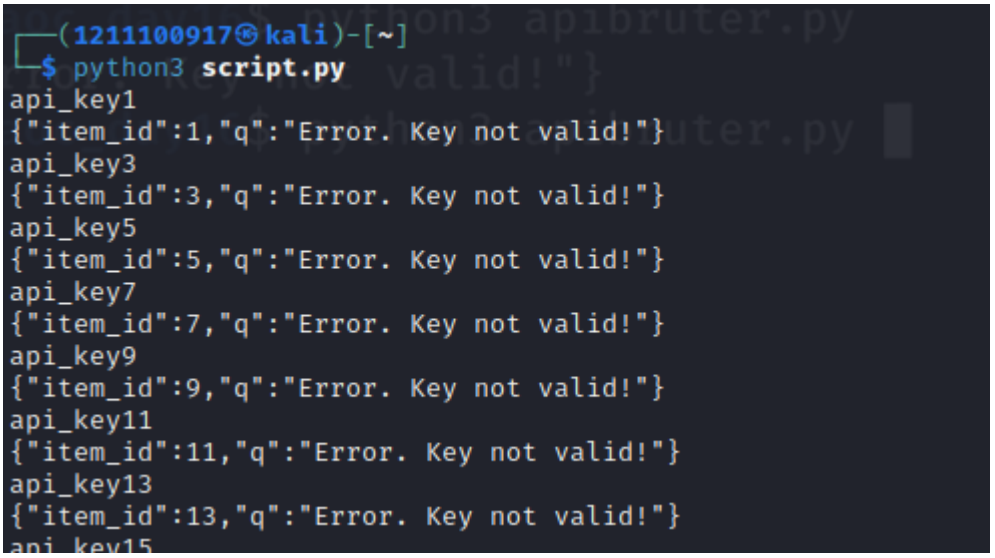
Question 4

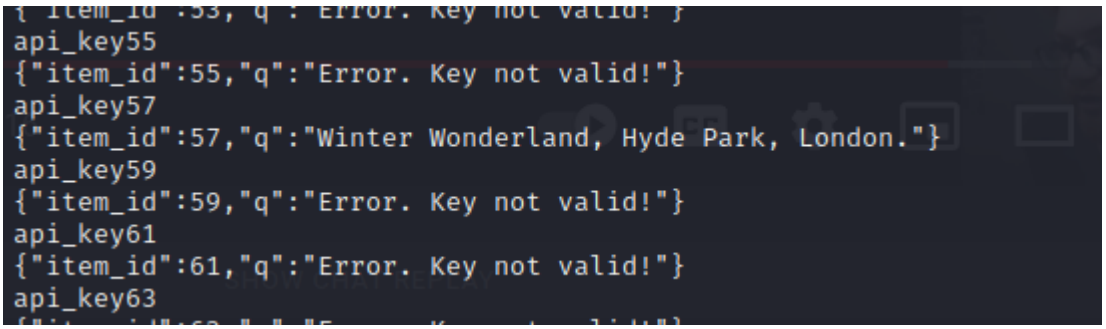
Find raw data returned if no parameters are entered



Question 5

Use sublime text to create ‘script.py’ to find Santa’s position





Thought Process/Methodology
We first copy the ip address and paste it at another tab. We then use nmap to find out the port number of the web server (80). The templates being used can be found at the left upper corner named as BULMA. Then, we try "/api/" behind the ip address to find out the directory for the API. We click at the Raw Data section to get answer for return when no parameters are entered Next, we download Sublime Text using the terminal and paste the example code from Day 15. Then, we edit some parts of the code to let it loop the api in order to find Santa's placing and API key, which we save it as 'script.py'. We then use 'script.py' to find Santa's location.

Day 17: Reverse Engineering: ReverseELFneering

Tools used: Kali, Firefox, Terminal

Question 1
Get the answer from THM table

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

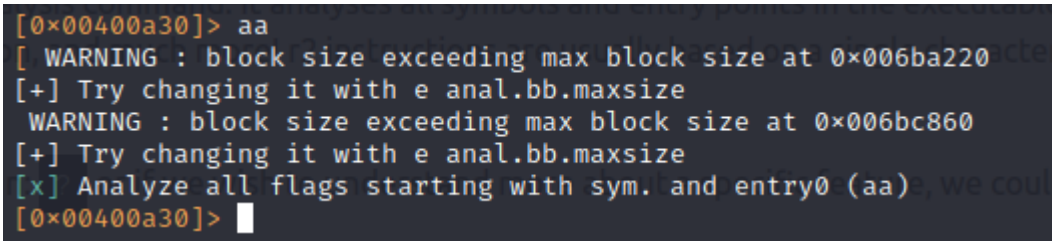
The core of assembly language involves using registers to do the following:

- 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

Question 2

Use aa



Question 3

Use db

Question 4

Use dc

```
[0×00400a30]> dc
hit breakpoint at: 400b55
[0×00400b55]>
```

Question 5

Use pdf@main to assembly code

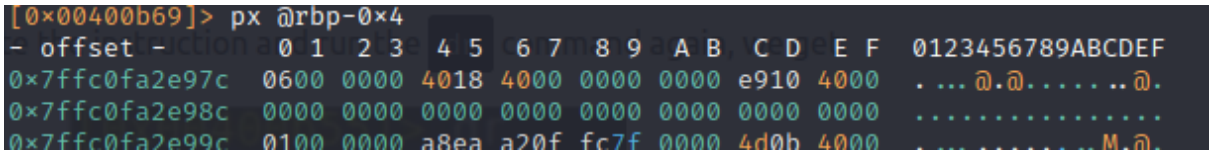
```
elfmceager@tbfc-day-17: ~
File  Actions  Edit  View  Help
1211102409@kali: ~ ×   elfmceager@tbfc-day-17: ~ ×
Do you want to quit? (Y/n)
Do you want to kill the process? (Y/n)
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1586 started...
= attach 1586 1586
bin.baddr 0×00400000
Using 0×400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[0×00400a30]> aa
[ WARNING : block size exceeding max block size at 0×006ba220
[+] Try changing it with e anal.bb.maxsize
 WARNING : block size exceeding max block size at 0×006bc860
[+] Try changing it with e anal.bb.maxsize
[x] Analyze all flags starting with sym. and entry0 (aa)
[0×00400a30]> pdf @main
            ;-- main:
/ (fcn) sym.main 35
|   sym.main ();
|           ; var int local_ch @ rbp-0×c
|           ; var int local_8h @ rbp-0×8
|           ; var int local_4h @ rbp-0×4
|              ; DATA XREF from 0×00400a4d (entry0)
|           0×00400b4d      55              push rbp
|           0×00400b4e      4889e5          mov rbp, rsp
|           0×00400b51      c745f4010000.   mov dword [local_ch], 1
|           0×00400b58      c745f8060000.   mov dword [local_8h], 6
|           0×00400b5f      8b45f4          mov eax, dword [local_ch]
|           0×00400b62      0faf45f8        imul eax, dword [local_8h]
|           0×00400b66      8945fc          mov dword [local_4h], eax
|           0×00400b69      b800000000      mov eax, 0
|           0×00400b6e      5d              pop rbp
\           0×00400b6f      c3              ret
[0×00400a30]>
```

Question 6

Set the breakpoint at the 0x00400b62 and execute it. Find the value with px @rbp-0x8.

Question 7

Set the breakpoint at the 0x00400b69 and execute it. Find the value with px @rbp-0x4.



Thought Process/Methodology

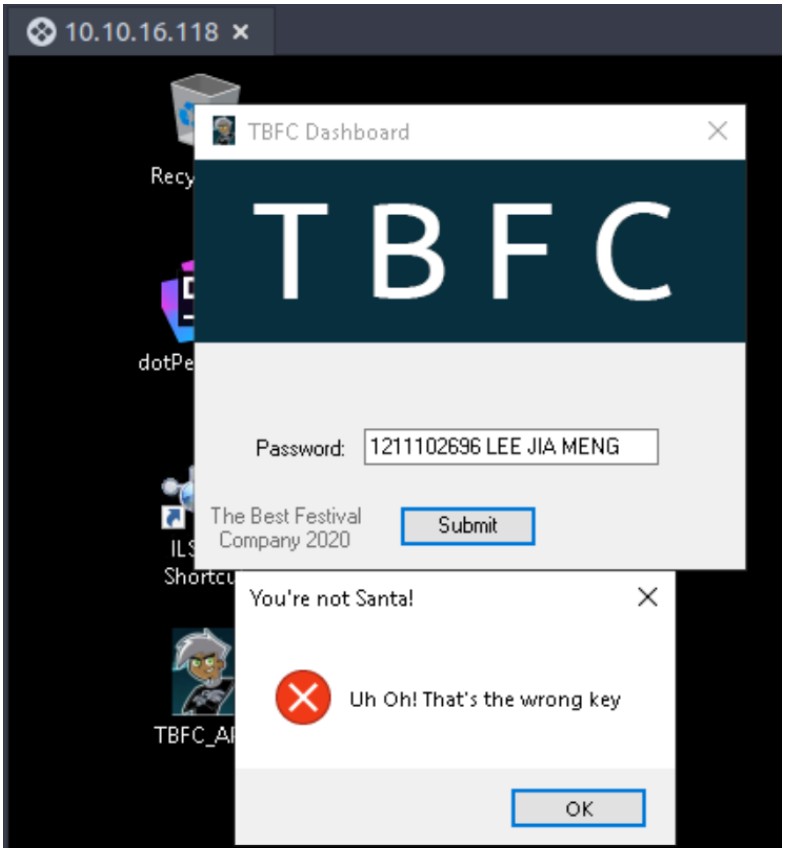
First log in using ssh username(elfmceager)@MACHINE_IP with the password(adventofcyber) that is provided in THM.Run through Radare 2 in debugging mode with the command r2 -d ./challenge1 .Ask r2 to analyze the program with ‘aa’.Use ‘afl’ to find the list of the functions. After that, we assembly code at main by running the command pdf @main.We can find the answer for Q5 by looking at the output. Then, we set the breakpoint at the imul eax to find the value with px @rbp-0x8.Last, we exit and re-enter debugging mode. This time we set the breakpoint at 0x00400b69 and execute it to find the value of local_4h before eax set to 0 with px @rbp-0x4.

Day 18: [Reverse Engineering] The Bits of Christmas

Tools used: THM AttackBox, Remmina, CyberChef.

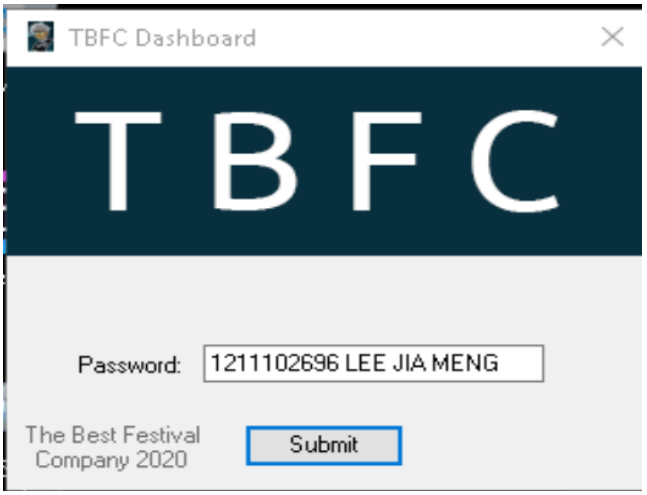
Question 1

Open up TBFC_app after getting into Remmina and entering anything into the password box.



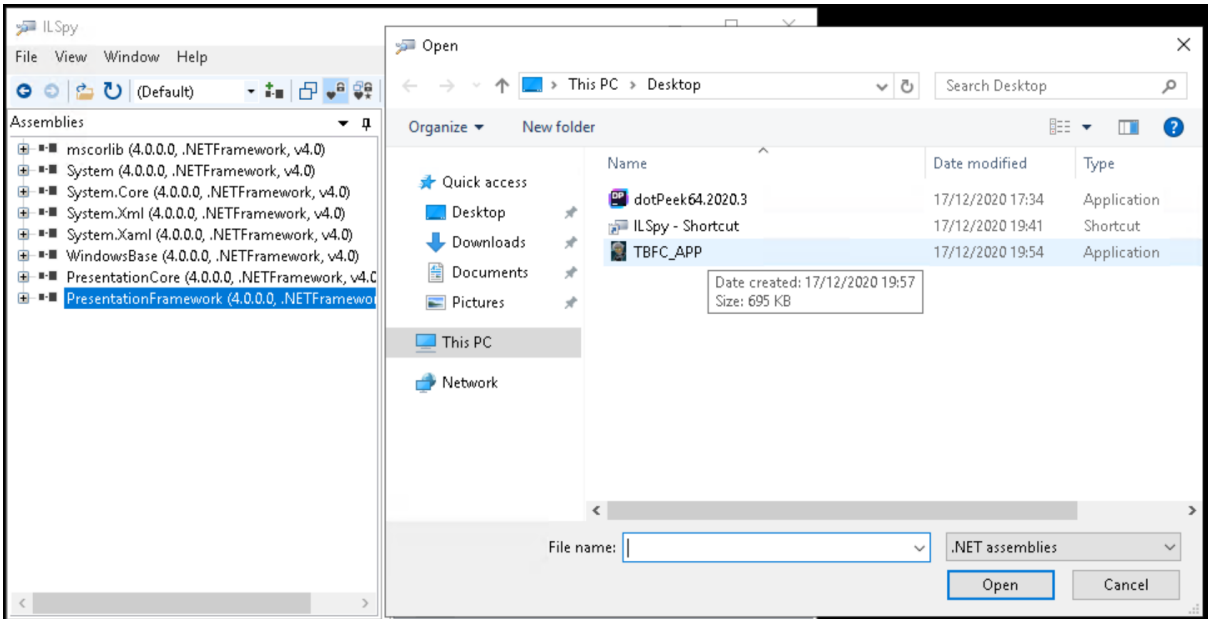
Question 2

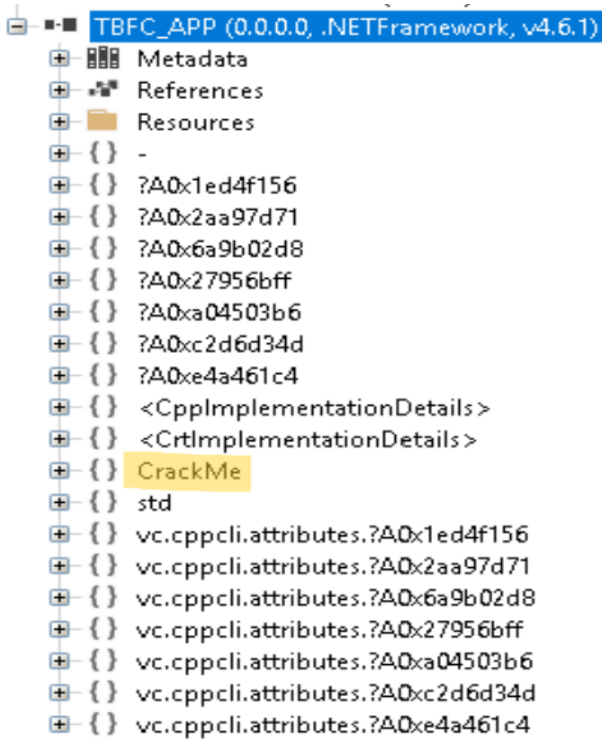
TBFC stands for



Question 3

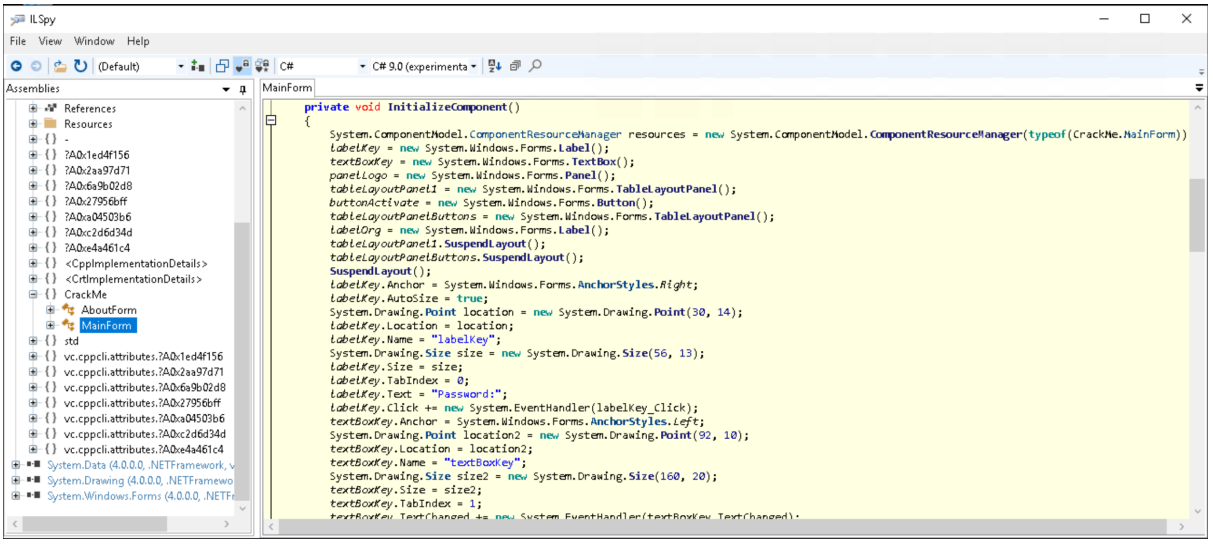
Module that catches my attention is



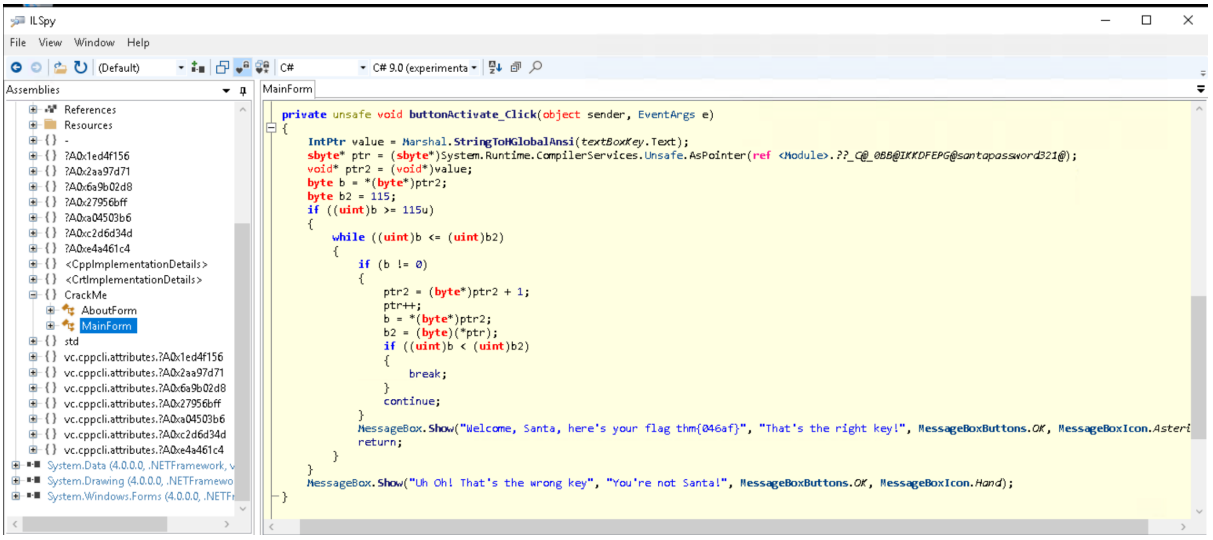


Question 4

The form that contain the information are looking for is

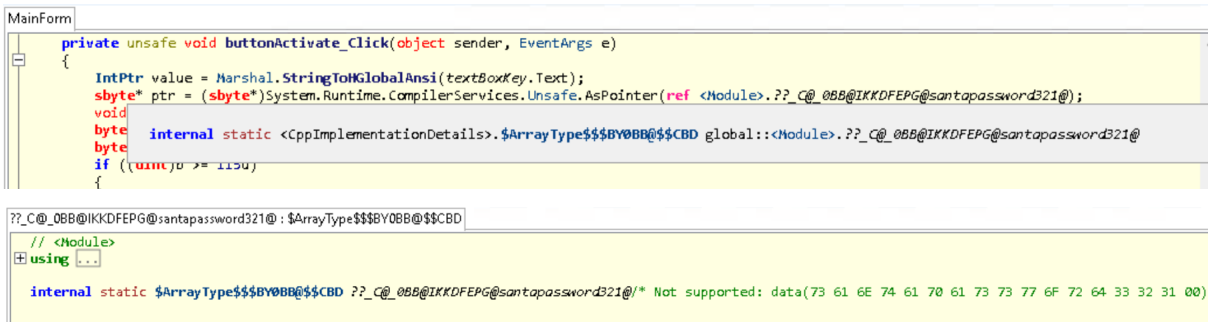


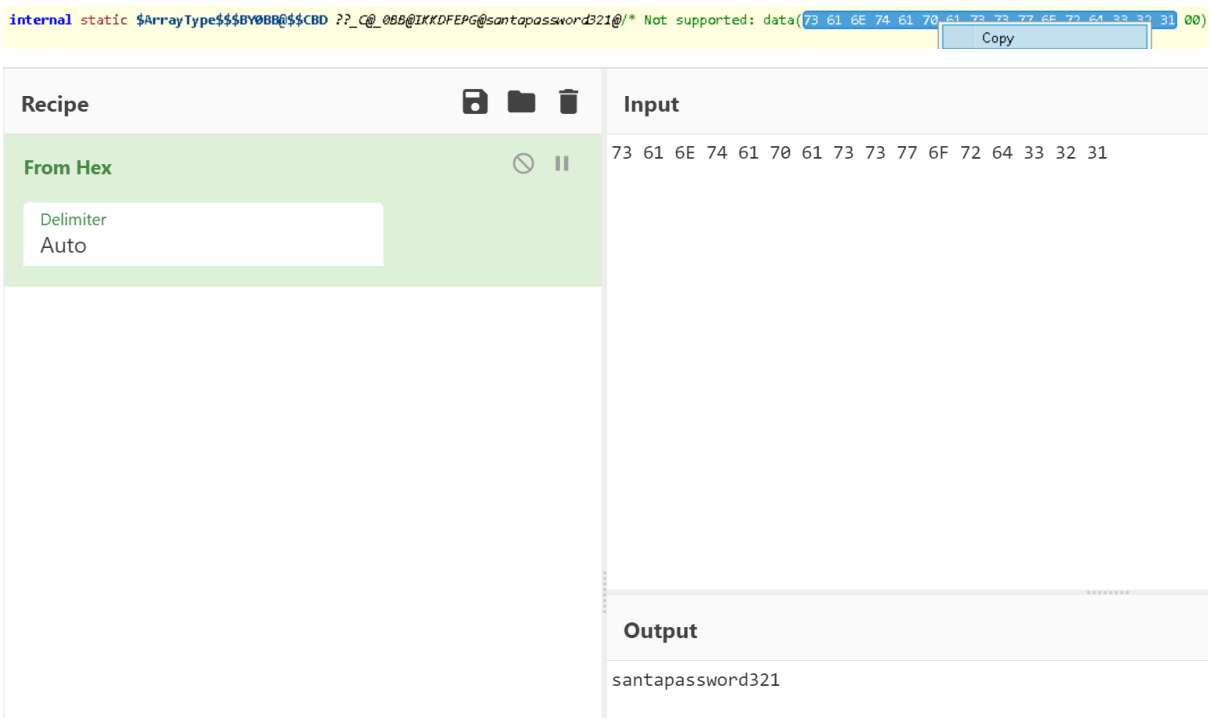
Question 5



Question 6

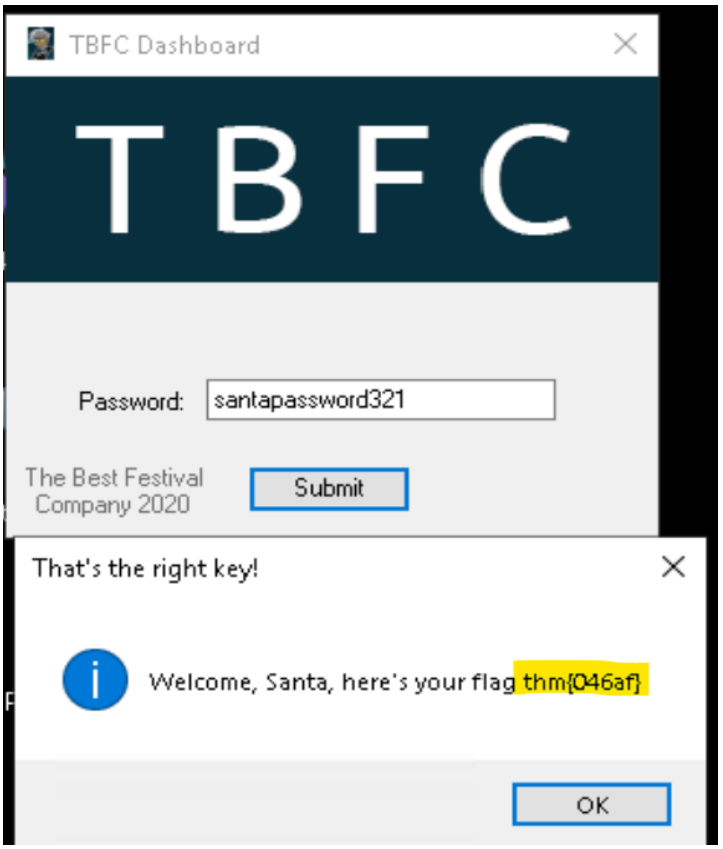
Expand the buttonActivate_Click and look through for password.





Question 7

Use the password that was obtained using CyberChef to login.



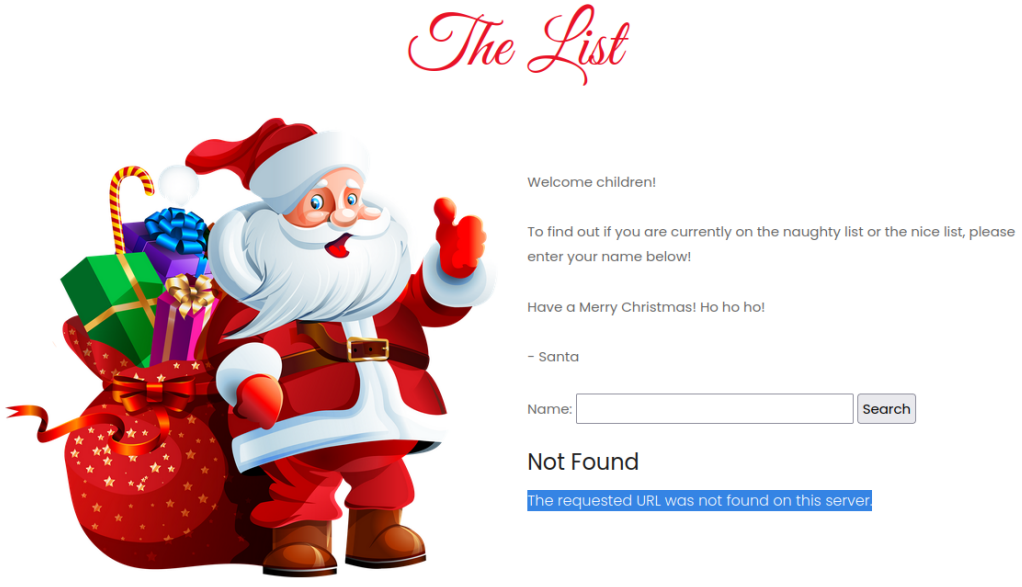
Thought Process/Methodology
Start the AttackBox and open up Remmina. Connect to it using the MACHINE_IP, username , and password provided in THM. Open the TBFC_app and randomly type in the password to obtain the message. From the TBFC dashboard, it shows that it stands for The Best Festival Company. Moving forward, close the TBFC_app and open up ILSPY. Now, open up TBFC_app in ILSPY and look through the TBFC_app by expanding it. The module that catches my eyes is the ‘CrackMe’ module that was standing out. From then on, expand the ‘CrackMe’ module to explore the two forms under it. The form that will give us information is the MainForm as it lets the user interact with. Look through the method within the MainForm for Santa's password. By expanding the buttonActivate_Click method, a string that seems to be a clue to Santa’s password would appear. Double click on it and ILSPY will take us to a dedicated page of it. In the new page, there is a set of data that seems to be Santa’s password, copy the data and convert the hexadecimal by using CyberChef. Santa’s password will be obtained and used to login to the TBFC_app. Lastly, we will obtain the flag when we key in the correct password.

Day 19: Web Exploitation: The Naughty or Nice List
Tools: Kali Linux

Question 1
Finding which list are the person on

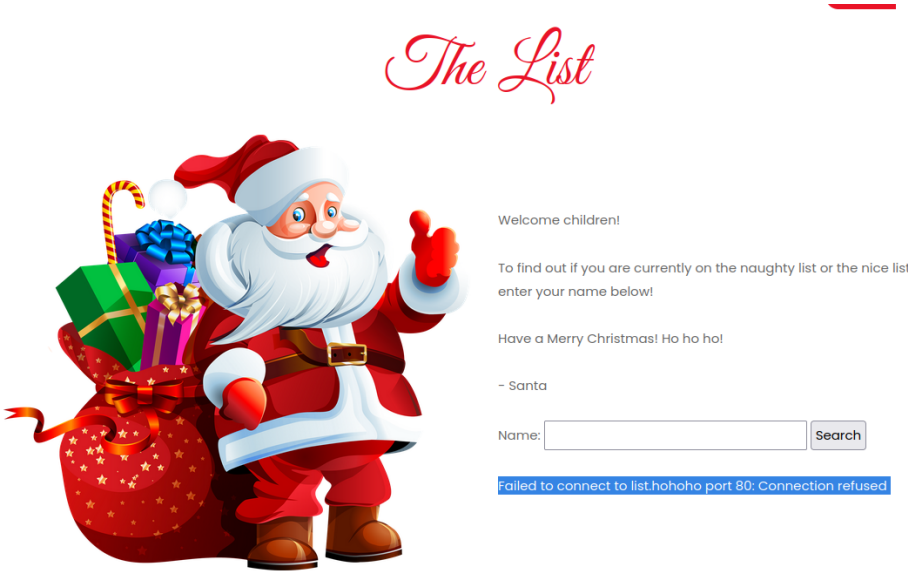
Question 2

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



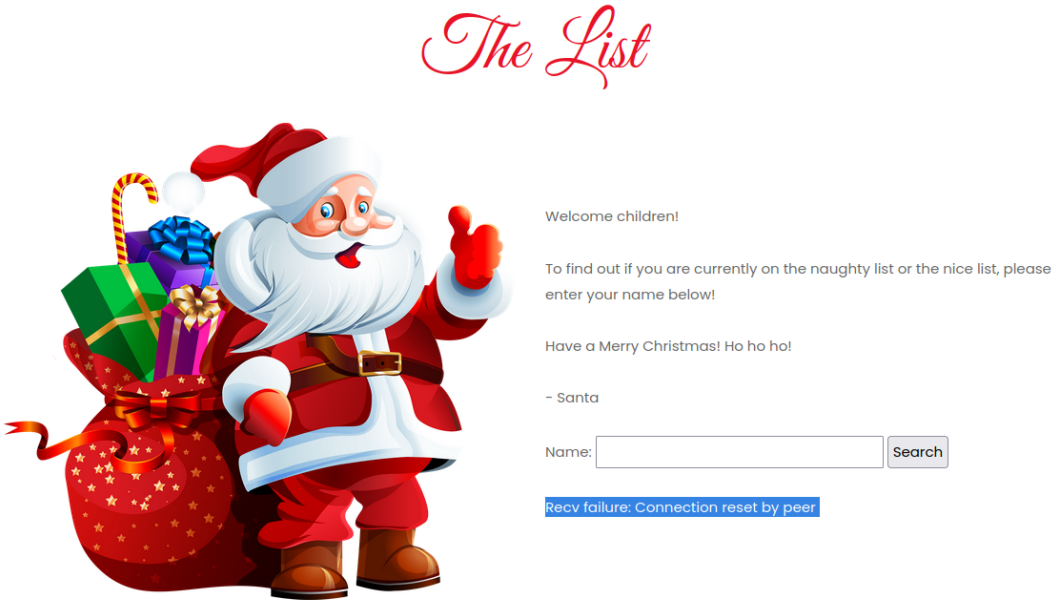
Question 3

Finding what is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"



Question 4

Finding what is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"

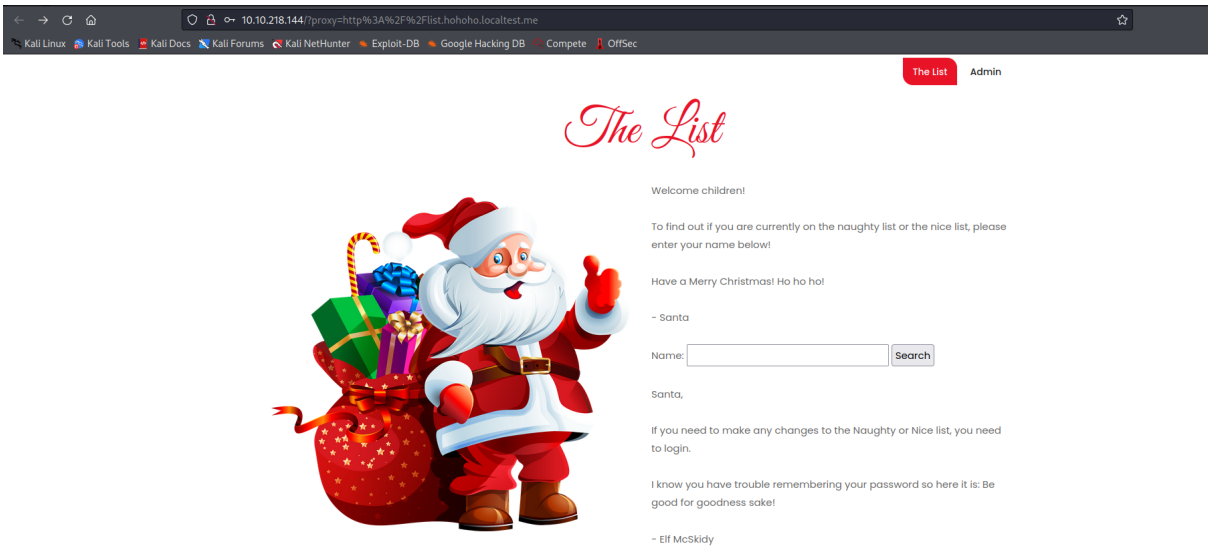


Question 5

Finding what is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"

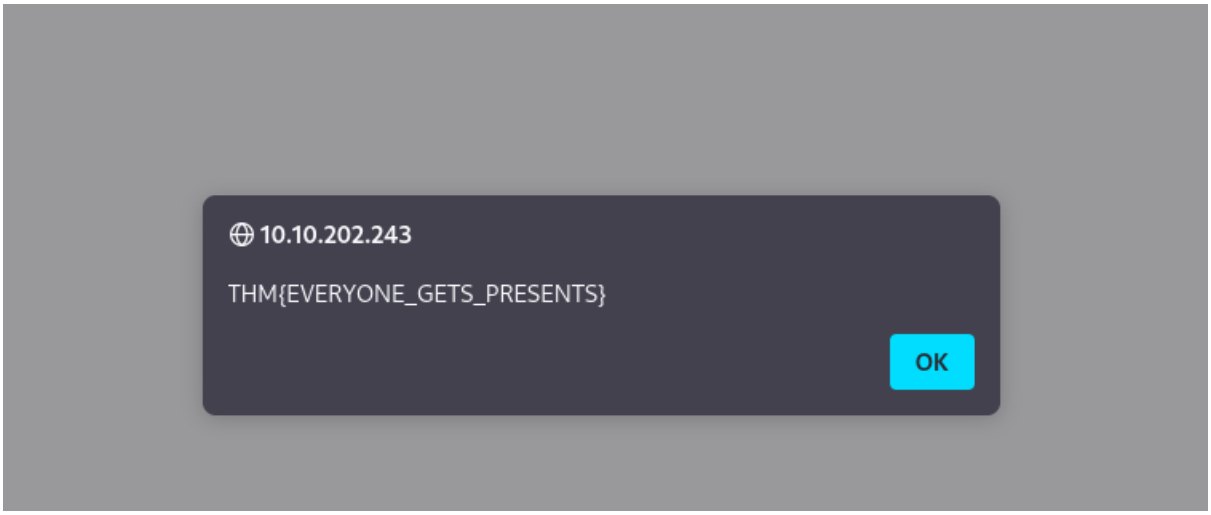
Question 6

Finding Santa's password



Question 7

Getting the challenge flag



Thought Process/ Methodology
Paste the IP address to a new page, then start by searching the names from the google form to see which list are they in. Then, paste all the links from google form (for Q2- Q5) in order to find what does the page display. Next, we add "list.hohoho.localtest.me" to the end of link to get the password for the admin. After getting the password, we log in using Santa as username and the password we got. Then we delete the name list to get the flag.

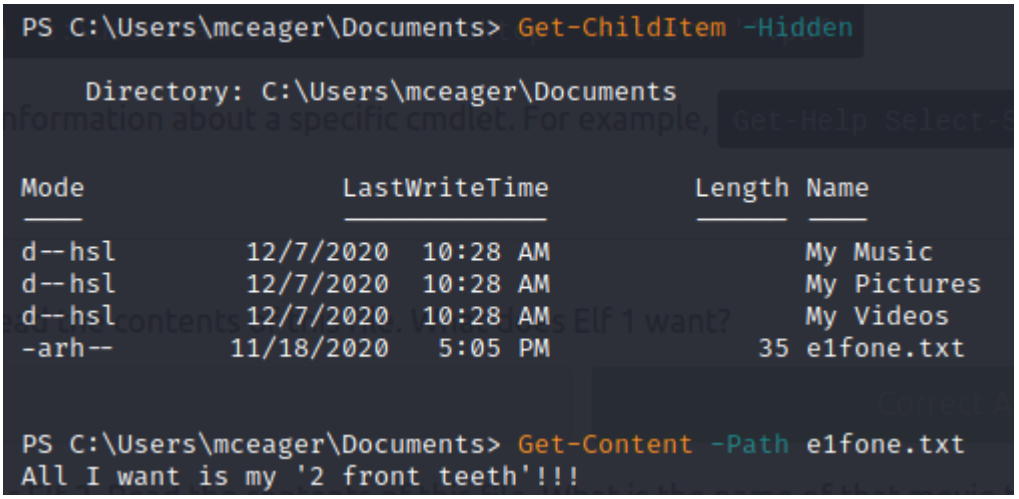
Day20:Blue Teaming: PowershELIF to the rescue
Tools used: Kali, Firefox, Terminal, PowerShell

Question 1
Use ssh -h to check the parameter

```
┌──(1211102409㉿kali)-[~]
└─$ ssh -h
unknown option -- h
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command [argument ...]]
```

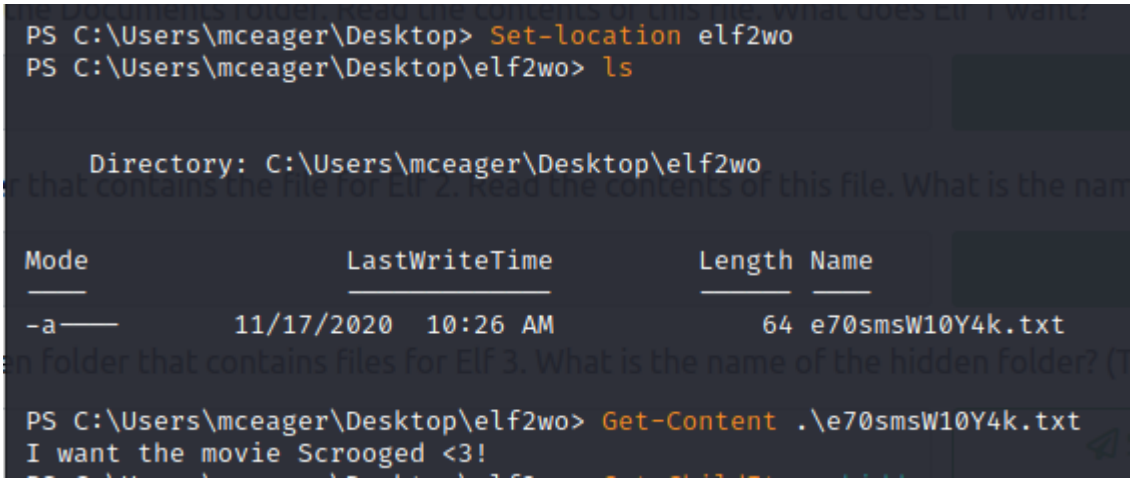
Question 2

Finding the hidden file with Get-ChildItem -Hidden. Get the content using Get-Content -Path e1fone.txt



Question 3

Find the hidden file in C:\Users\mceager\Dekstop\elf2wo and read the content with ‘Get-Content -Path e70smsW10Y4k.txt’



Question 4

Go to the Windows directory using ‘cd C:\Windows\’.Use ‘Get-ChildItem -Directory -Hidden -Recurse -Filter '*3*' -ErrorAction SilentlyContinue’ to find the hidden folder that contains files for Elf 3

```
PS C:\Windows> Get-ChildItem -Directory -Hidden -Recurse -Filter '*3*' -ErrorAction SilentlyContinue

    Directory: C:\Windows\System32

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

Question 5

```
PS C:\Windows\System32\3lfthr3e> Get-ChildItem -hidden


    Directory: C:\Windows\System32\3lfthr3e


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

PS C:\Windows\System32\3lfthr3e> Get-Content -Path 1.txt | Measure-object -Word

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

Use ‘Get-Content -Path 1.txt | Measure-object -Word ‘ to get the number for the words.

Question 6

Find the 2 words using ‘(Get-Content -Path 1.txt)[551/6991]’

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

Question 7

Search using ‘Select-String -Path ‘C:\Windows\System32\3lfthr3e\2.txt' -Pattern ‘redryder’ ’

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

2.txt:558704:redryderbbgun
```

Thought Process/Methodology

First, we log in using ‘ssh -l mceager MACHINE_IP’ with the password ‘r0ckStar!’. After that, we launch the PowerShell and navigate to the Documents folder with ‘Set-Location .\Documents\’. ‘Get-ChildItem -Hidden’ had been used to find the hidden elf file and ‘Get-Content -path e1fone.txt’ to read the content of e1fone.txt. Then, we got back to \mceager by using ‘cd ..’ and navigating to the Desktop file with ‘Set-Location .\Desktop\’. The e70smsW10Y4k.txt has been found and read in the same way as the e1fone.txt.To find the name of the hidden folder for Elf 3, we need to go back to the Windows directory using ‘cd C:\Windows\’ and find the file with ‘Get-ChildItem -Directory -Hidden -Recurse -Filter '*3*' -ErrorAction SilentlyContinue’.Next, we use ‘Get-ChildItem -hidden’ to get the hidden file in the folder and use ‘Get-Content -Path 1.txt | Measure-object -Word’ to get the number of words contained in the first file. We also find the two words at index 551 and 6991 with ‘(Get-Content -Path 1.txt)[551/6991]’.Lastly, we use ‘Select-String -Path ‘C:\Windows\System32\3lfthr3e\2.txt' -Pattern ‘redryder' ’ to search the phrase “redryder” in the 2nd file.