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

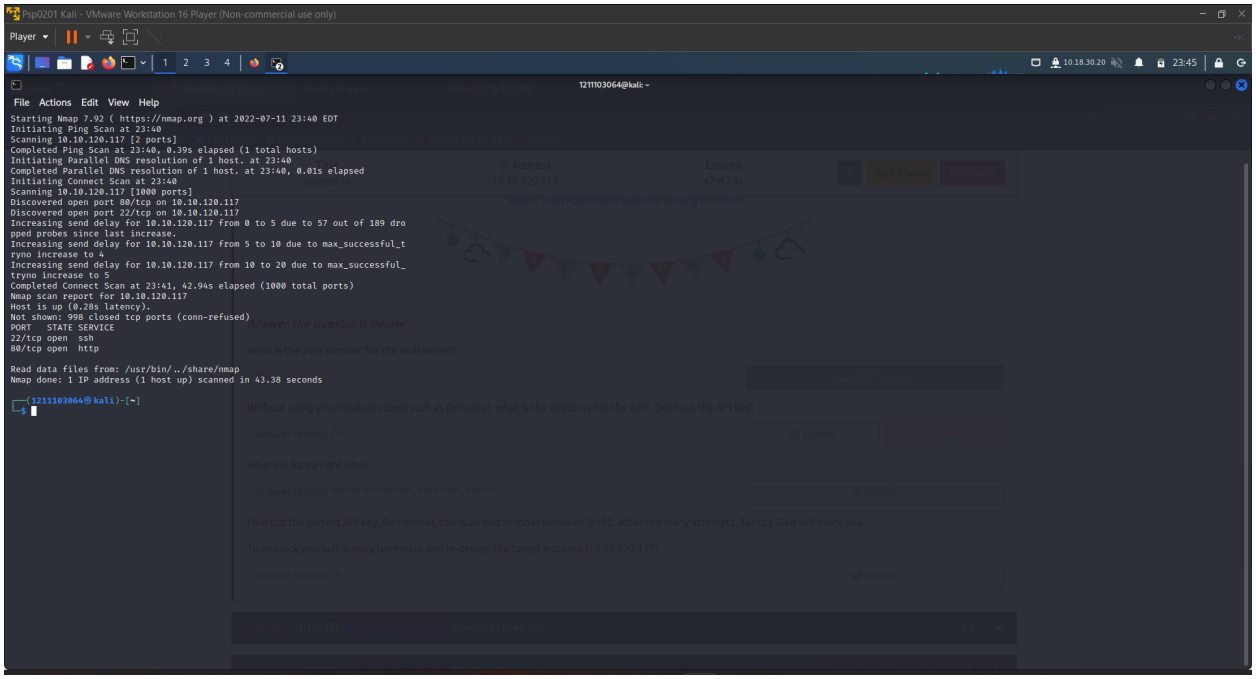
Day 16 : Help! Where is Santa?

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

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

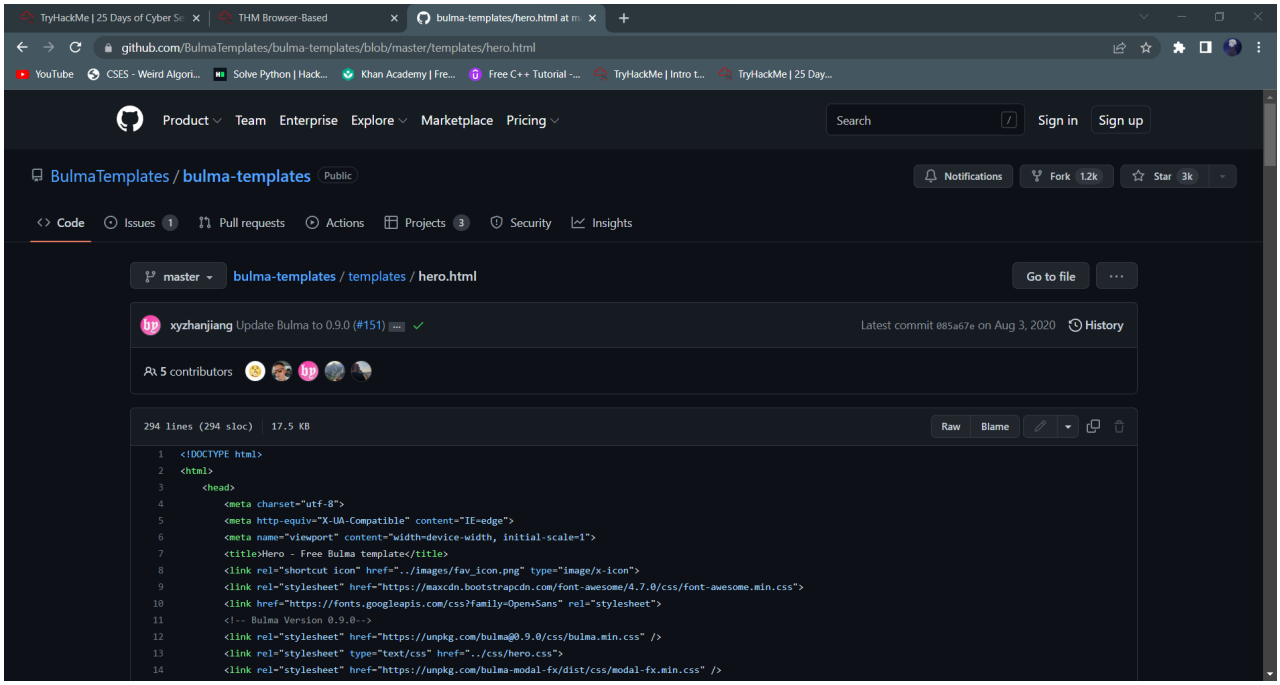
Answer : 80

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



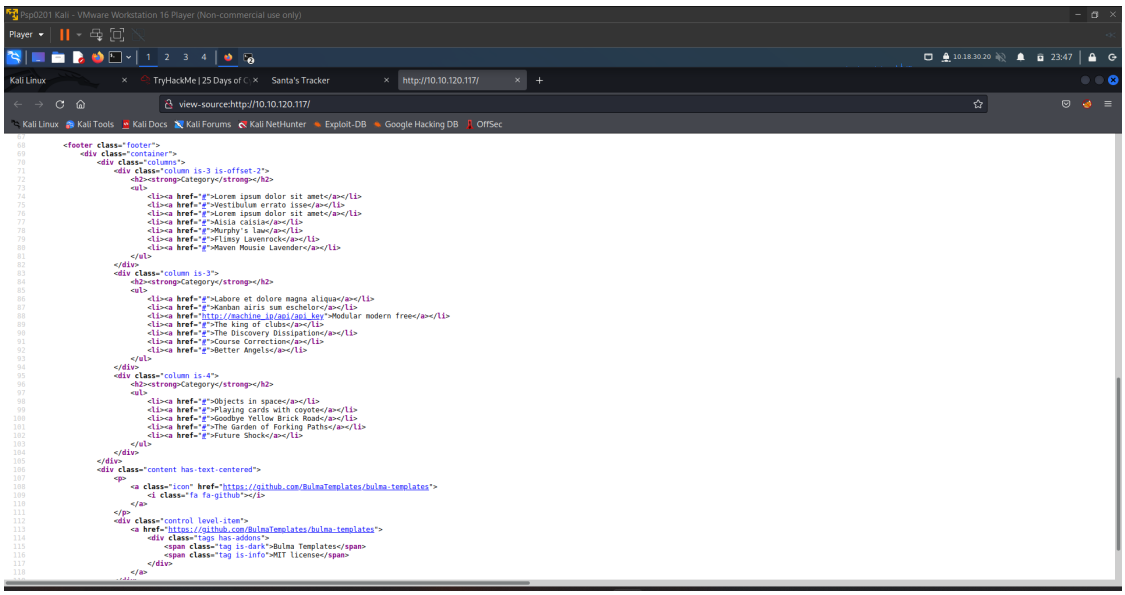
Question 2 : What templates are being used?

Answer : Bulma



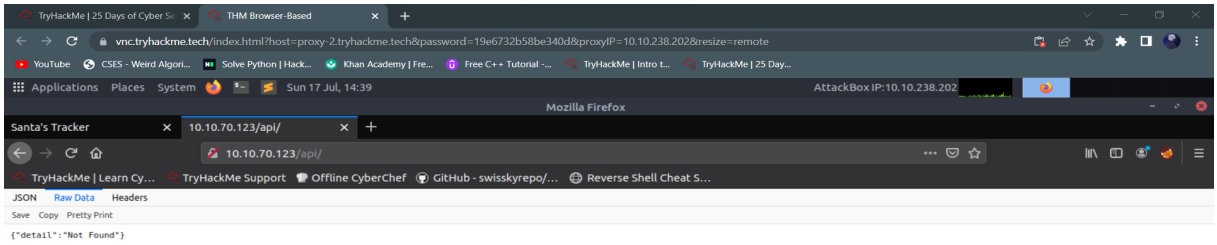
Question 3 : Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)

Answer : /api/



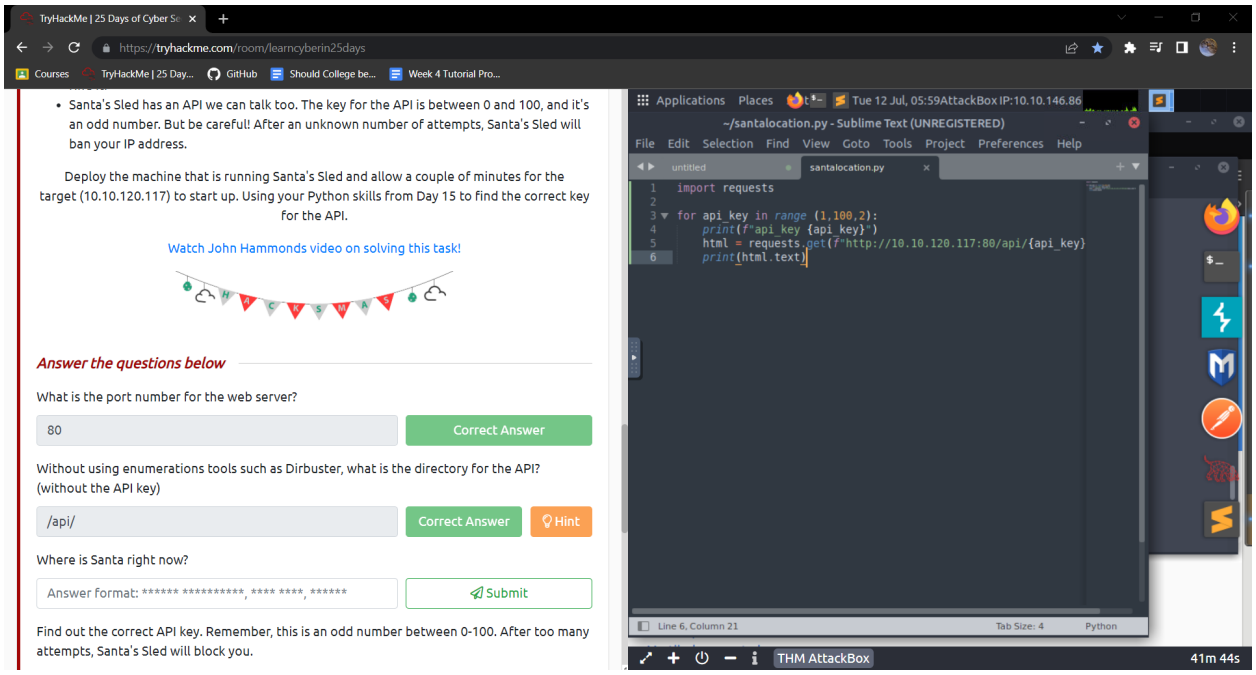
Question 4 : Go to the API endpoint. What is the Raw Data returned if no parameters are entered?

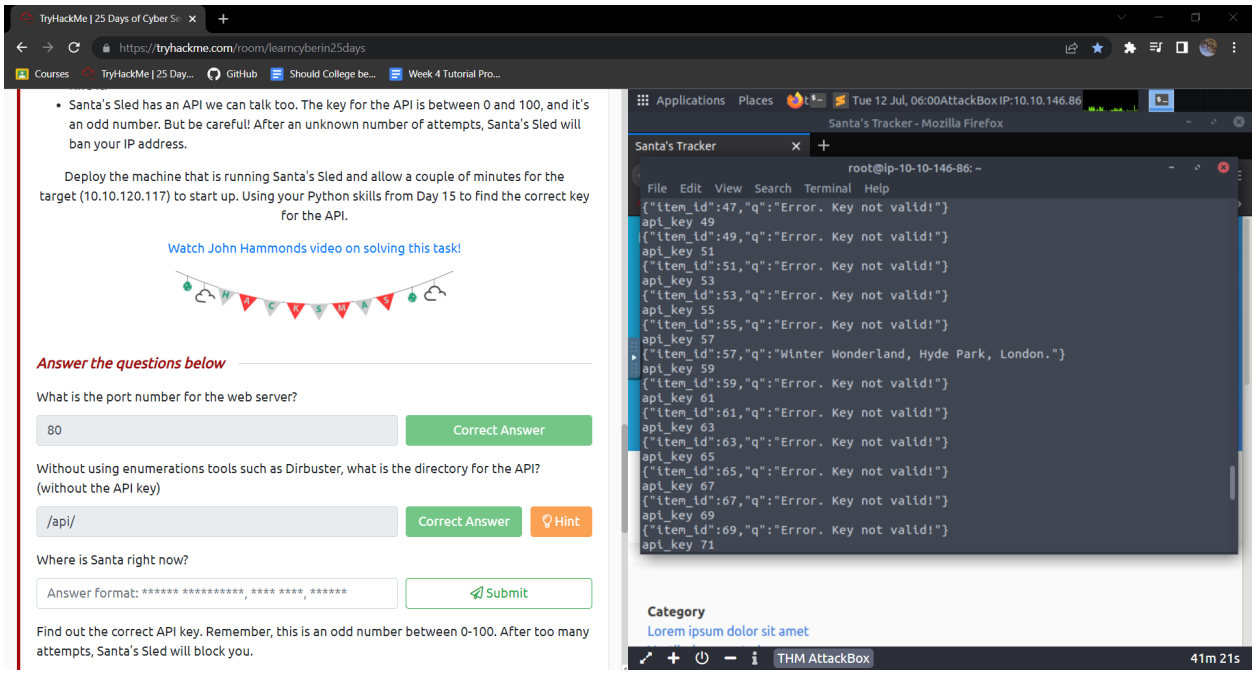
Answer : {"detail":"Not Found"}



Question 5 : Where is Santa right now?

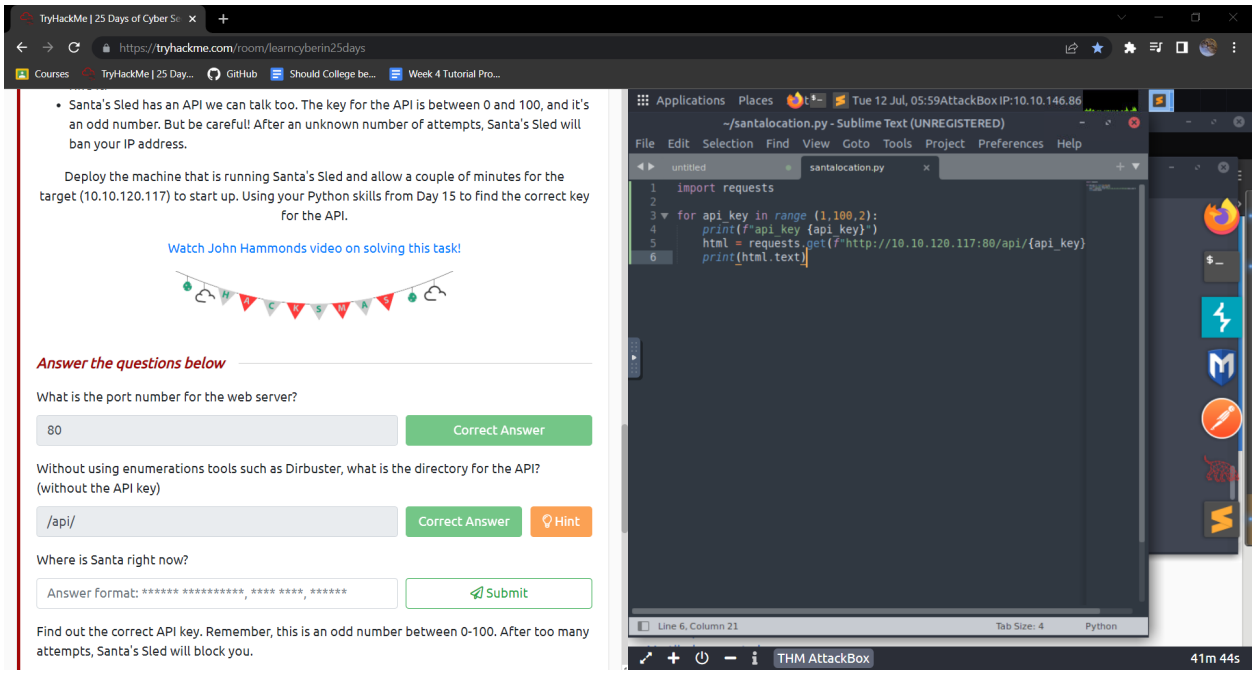
Answer : Winter Wonderland, Hyde Park, London

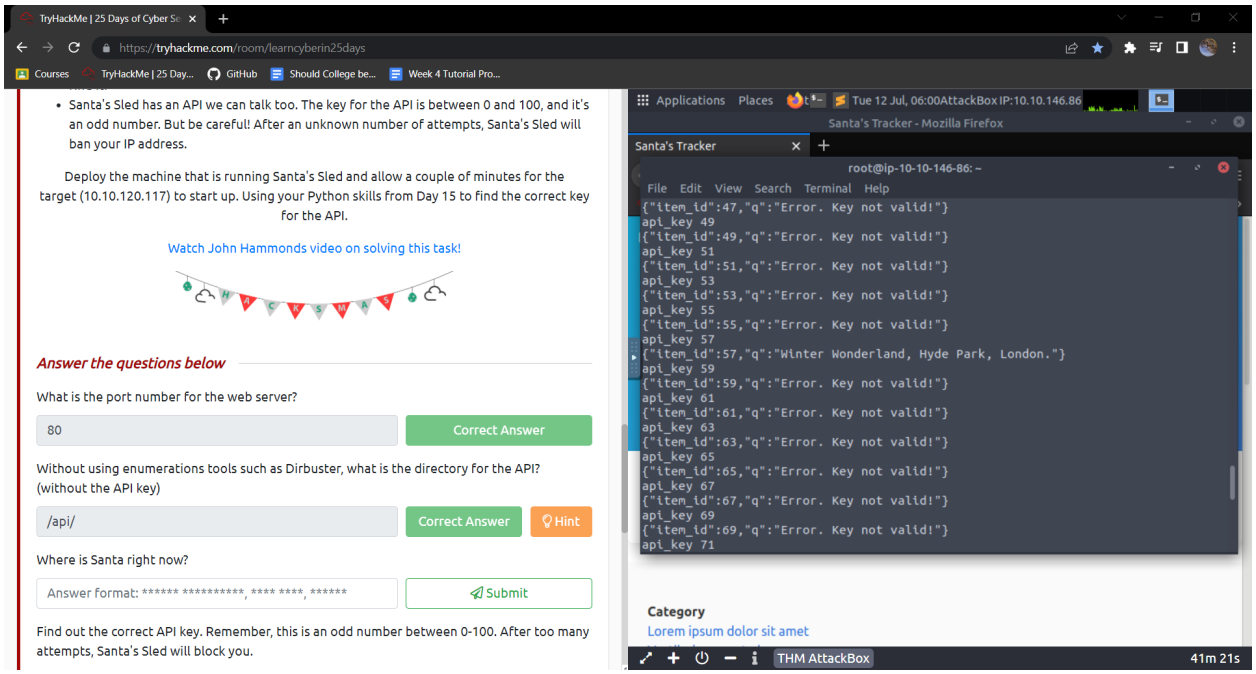




Question 6 : Find out the correct API key. Remember, this is an odd number between 0-100. After too many attempts, Santa's Sled will block you. To unblock yourself, simply terminate and re-deploy the target instance (MACHINE_IP)

Answer : 57





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.

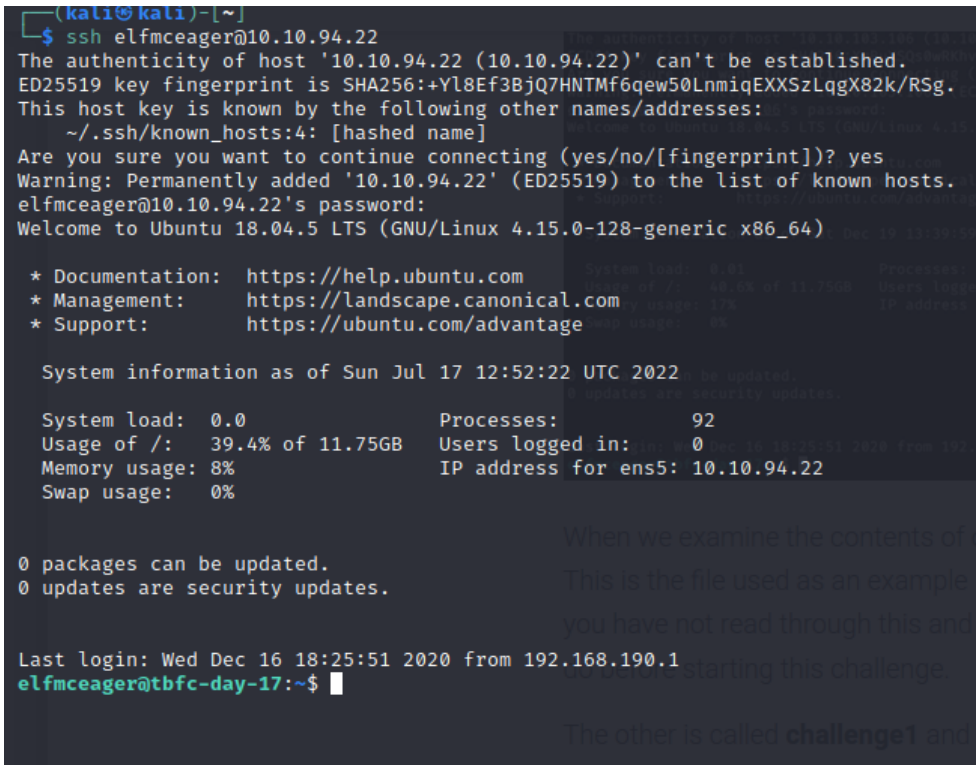
Question 4 : What is the command to execute the program until we hit a breakpoint?

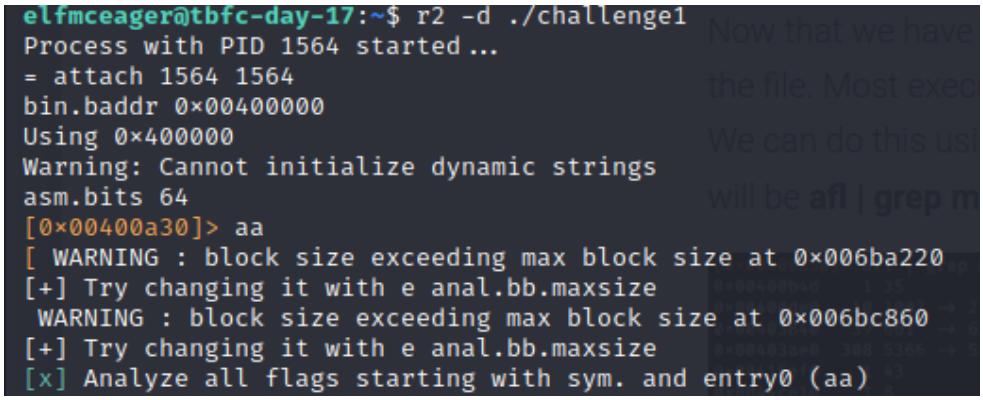
Answer :

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 :





```
[0×00400a30]> afl | grep main
0×00400b4d     1 35           sym.main
0×00400de0    10 1007 → 219   sym.__libc_start_main
0×00403840    39 661  → 629   sym._nl_find_domain
0×00403ae0   308 5366 → 5301  sym._nl_load_domain
0×00415ef0     1 43           sym._IO_switch_to_main_get_area
0×0044ce10     1 8            sym._dl_get_dl_main_map
0×00470430     1 49           sym._IO_switch_to_main_wget_area
0×0048f9f0     7 73   → 69    sym._nl_finddomain_subfreeres
0×0048fa40    16 247  → 237   sym._nl_unload_domain
```

```
[0×00400a30]> db 0×00400b5f
[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 b    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]> dc
hit breakpoint at: 400b5f
[0×00400b5f]> px @ rbp-0×c
- offset -       0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0×7ffd370a5464  0100 0000 0600 0000 0000 0000 4018 4000  ..... ........@.@.
0×7ffd370a5474  0000 0000 e910 4000 0000 0000 0000 0000  ......@.........
0×7ffd370a5484  0000 0000 0000 0000 0100 0000 9855 0a37  ......... ....U.7
0×7ffd370a5494  fd7f 0000 4d0b 4000 0000 0000 0000 0000  ....M.@.........
0×7ffd370a54a4  0000 0000 1700 0000 0100 0000 0000 0000  ..... ... ........
0×7ffd370a54b4  0000 0000 0000 0000 0200 0000 0000 0000  ................
0×7ffd370a54c4  0000 0000 0000 0000 0000 0000 0000 0000  ................
0×7ffd370a54d4  0000 0000 0000 0000 0000 0000 0004 4000  ..............@.
0×7ffd370a54e4  0000 0000 102e 6c0f 2915 abae e018 4000  ......l.).....@.
0×7ffd370a54f4  0000 0000 0000 0000 0000 0000 1890 6b00  ..............k.
0×7ffd370a5504  0000 0000 0000 0000 0000 0000 102e ec96  ................
0×7ffd370a5514  bd7b 5151 102e d81e 2915 abae 0000 0000  .{QQ....)... ....
```

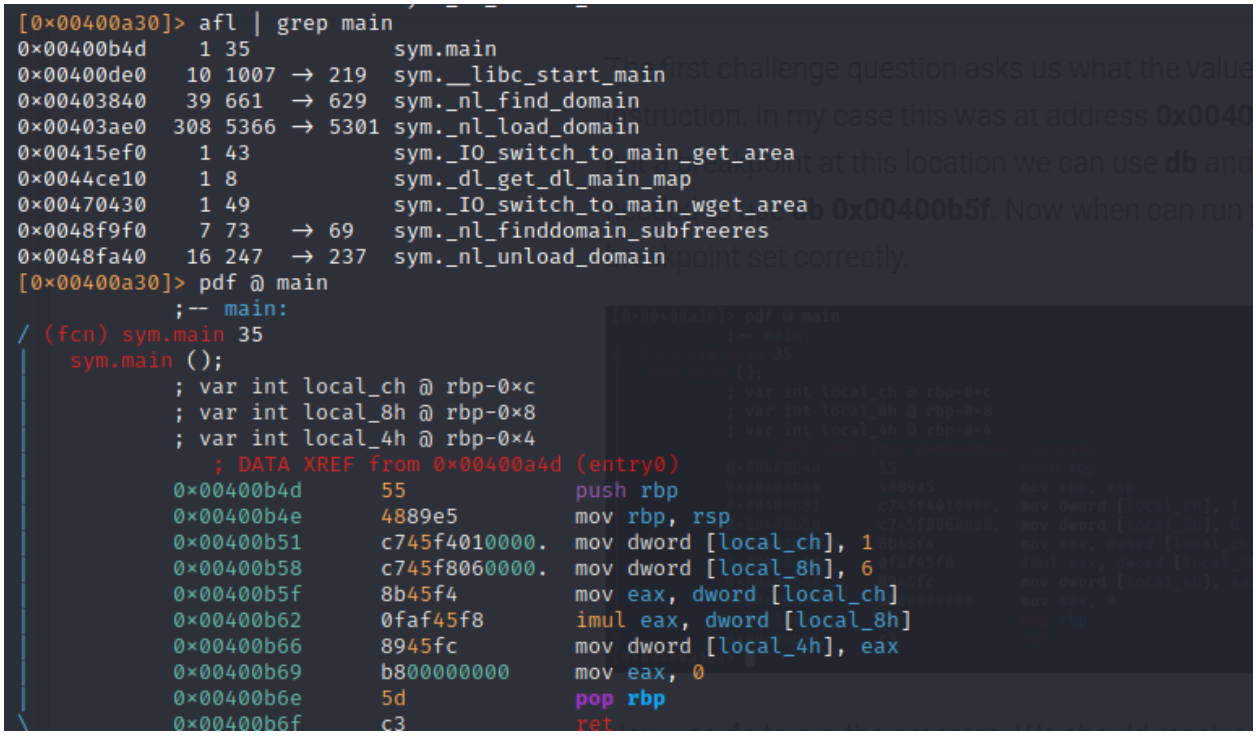
Question 6 : What is the value of eax when the imull instruction is called?

Answer :

```
[0×00400b5f]> ds
[0×00400b5f]> dr
rax = 0×00000006
rbx = 0×00400400
rcx = 0×0044b9a0
rdx = 0×7ffd370a55a8
r8 = 0×01000000
r9 = 0×006bb8e0
r10 = 0×00000015
r11 = 0×00000000
r12 = 0×004018e0
r13 = 0×00000000
r14 = 0×006b9018
r15 = 0×00000000
rsi = 0×7ffd370a5598
rdi = 0×00000001
rsp = 0×7ffd370a5470
rbp = 0×7ffd370a5470
rip = 0×00400b66
```

Question 7 : What is the value of local_4h before eax is set to 0?

Answer :



```
[0×00400a30]> afl | grep main
0×00400b4d    1 35           sym.main
0×00400de0   10 1007 → 219   sym.__libc_start_main
0×00403840   39 661  → 629   sym._nl_find_domain
0×00403ae0  308 5366 → 5301  sym._nl_load_domain
0×00415ef0    1 43           sym._IO_switch_to_main_get_area
0×0044ce10    1 8            sym._dl_get_dl_main_map
0×00470430    1 49           sym._IO_switch_to_main_wget_area
0×0048f9f0    7 73   → 69    sym._nl_finddomain_subfreeres
0×0048fa40   16 247  → 237   sym._nl_unload_domain
[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]> db 0×00400b69
[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 b    b800000000     mov eax, 0
|           0×00400b6e      5d             pop rbp
\           0×00400b6f      c3             ret
[0×00400a30]> dc
hit breakpoint at: 400b69
[0×00400b69]> px @ rbp-0×4
- offset -       0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0×7ffc4983de5c  0600 0000 4018 4000 0000 0000 e910 4000  ....@.@.......@.
0×7ffc4983de6c  0000 0000 0000 0000 0000 0000 0000 0000  ................
0×7ffc4983de7c  0100 0000 88df 8349 fc7f 0000 4d0b 4000  .......I....M.@.
0×7ffc4983de8c  0000 0000 0000 0000 0000 0000 1700 0000  ................
0×7ffc4983de9c  0100 0000 0000 0000 0000 0000 0000 0000  ................
0×7ffc4983deac  0200 0000 0000 0000 0000 0000 0000 0000  ................
0×7ffc4983debc  0000 0000 0000 0000 0000 0000 0000 0000  ................
0×7ffc4983decc  0000 0000 0004 4000 0000 0000 f286 0656  ......@........V
0×7ffc4983dedc  1b7c 70e3 e018 4000 0000 0000 0000 0000  .|p...@.........
```

Thought Process / Methodology :

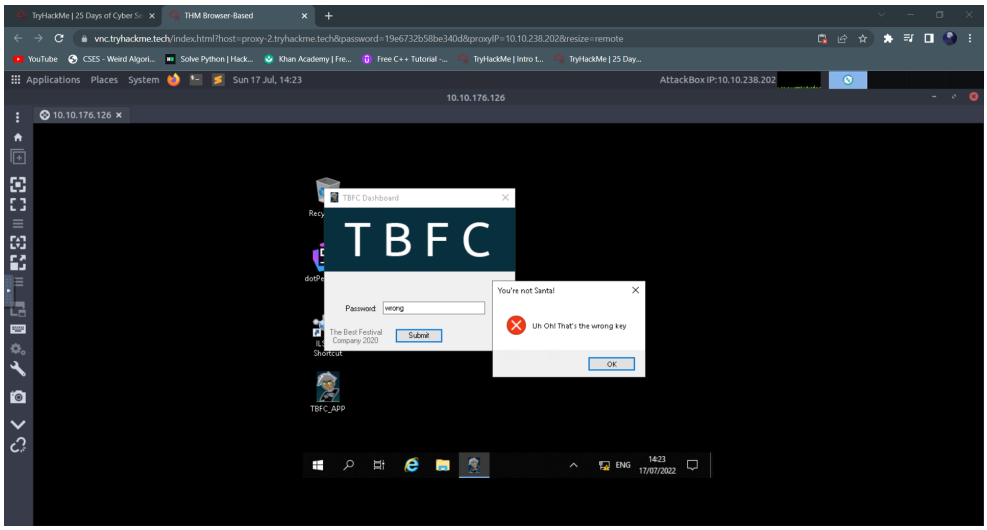
In the terminal , run ssh mceager@[machine_IP] then enter the password. Use aa to analyze. Then pick db to breakpoint . pdf@main to check the breakpoint then dc to execute. Px

Day 18 : The Bits Of Christmas

Tool Used : Kali Linux, Firefox, Attackbox, Remmina, ILSpy, TBFC_app, CyberChef

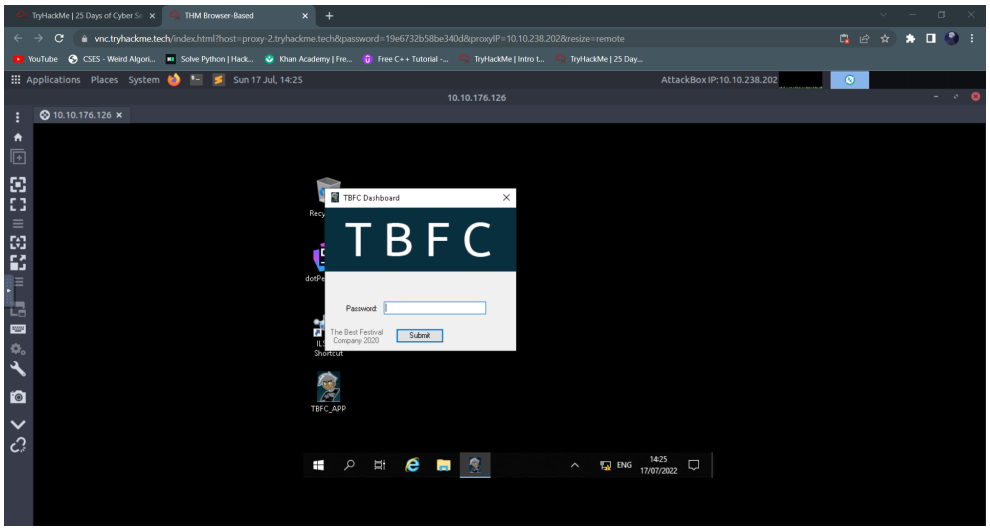
Question 1 : What is the message that shows up if you enter the wrong password for TBFC_APP?

Answer : Uh Oh! That's the wrong key



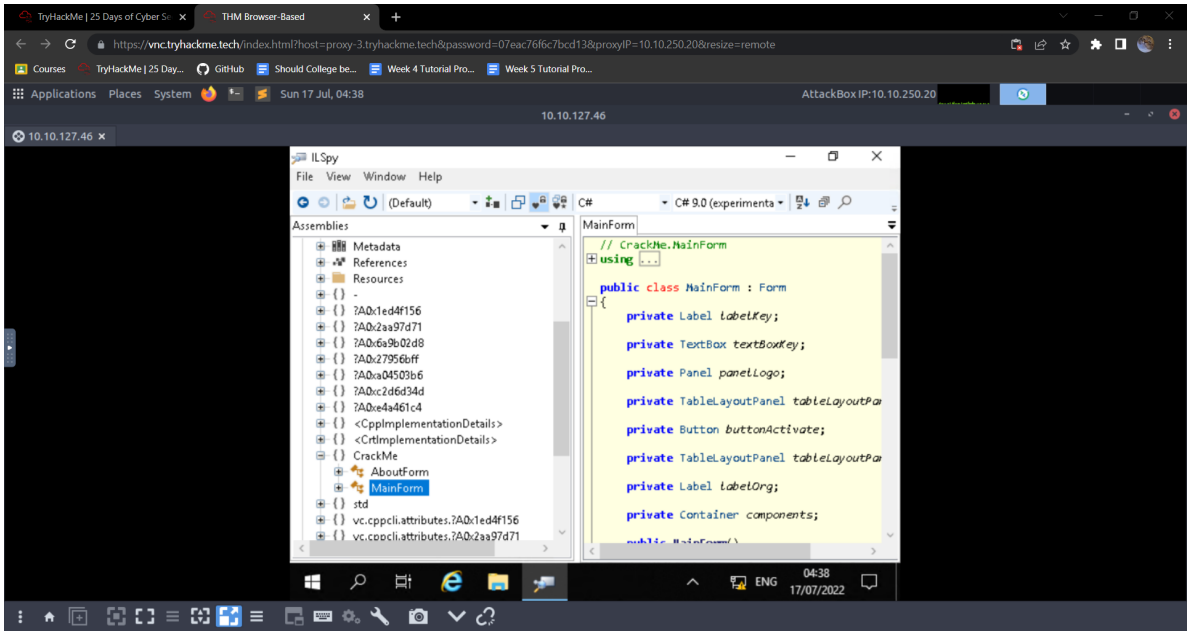
Question 2 : What does TBFC stand for?

Answer : The Best Festival Company



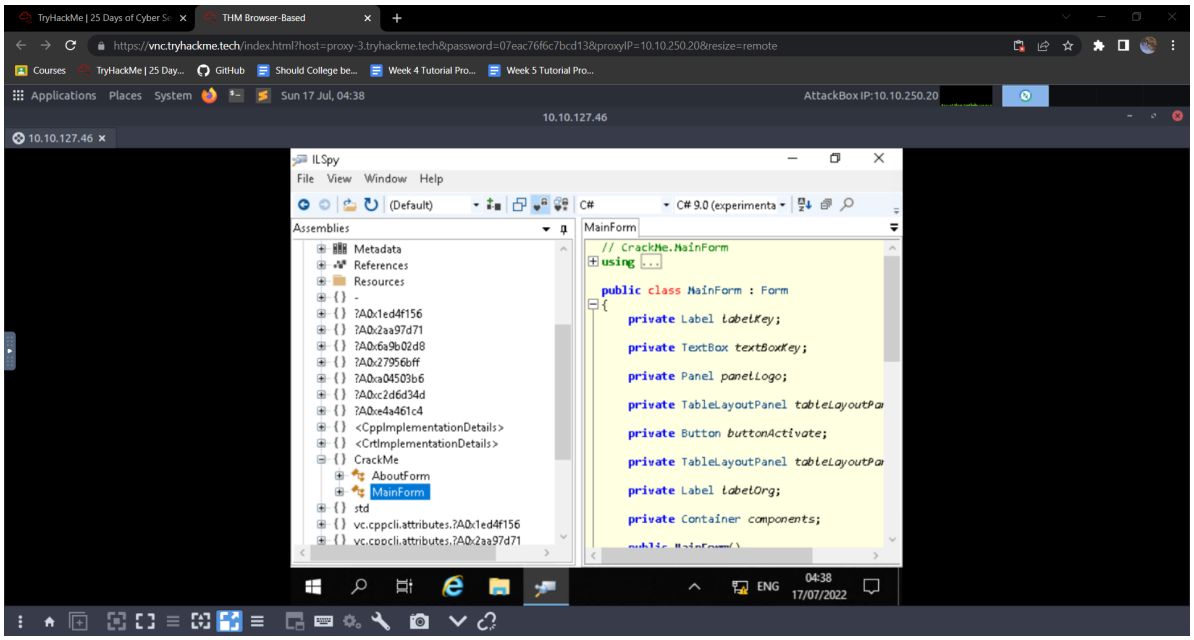
Question 3 : Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?

Answer : CrackMe



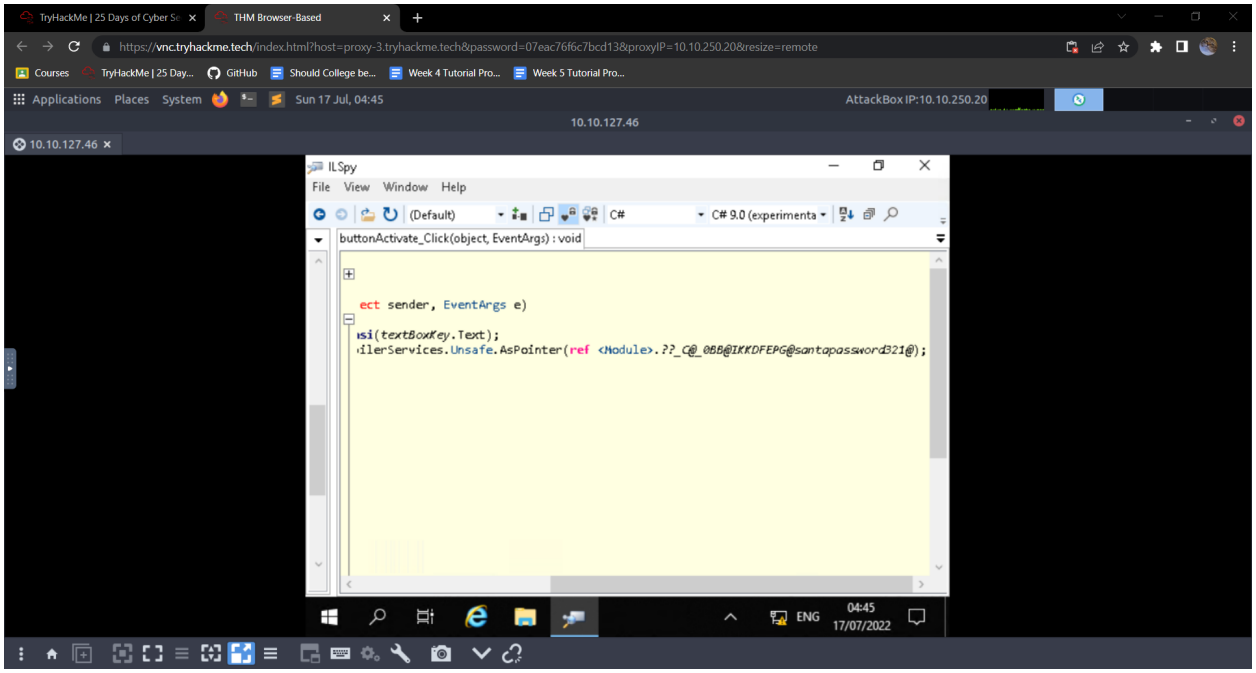
Question 4 : Within the module, there are two forms. Which contains the information we are looking for?

Answer : MainForm



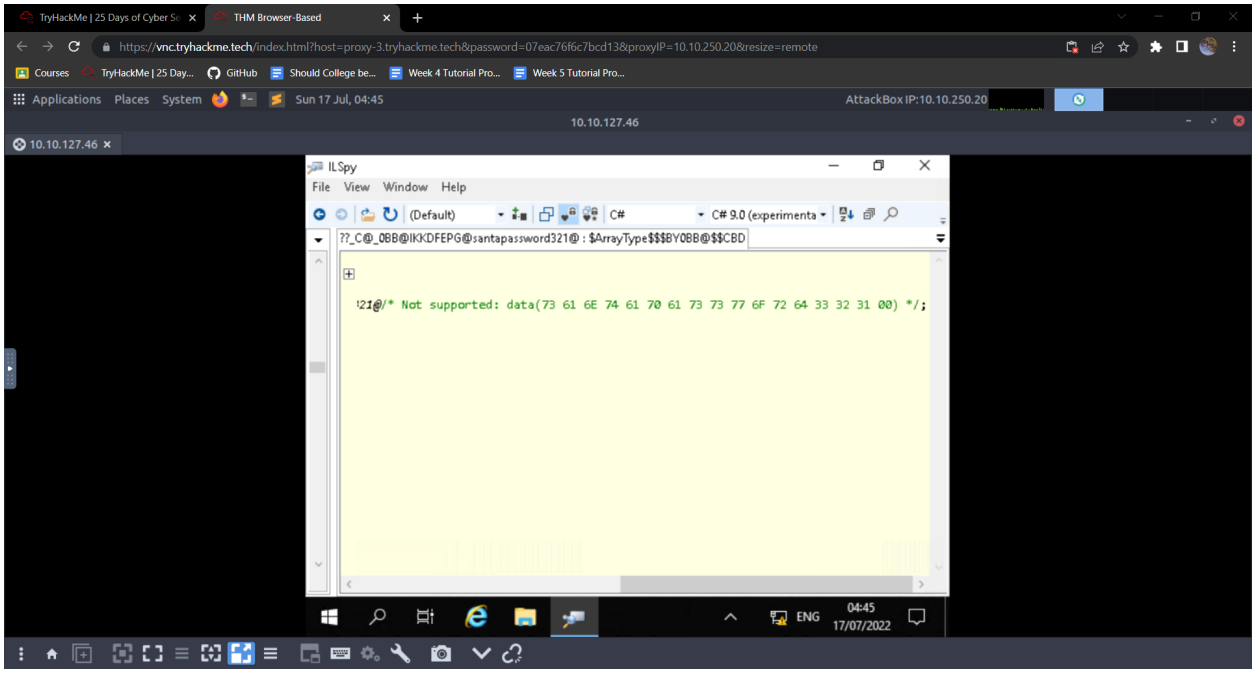
Question 5 : Which method within the form from Q4 will contain the information we are seeking?

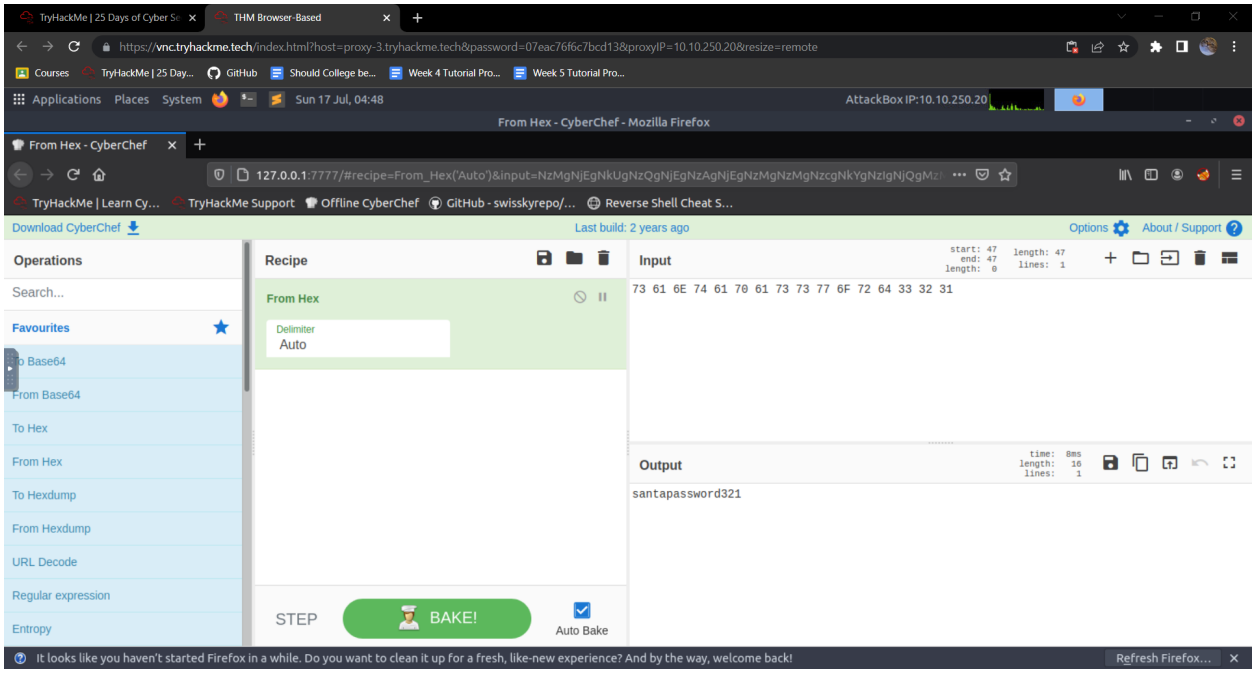
Answer : buttonActivate_Click



Question 6 : What is Santa's password?

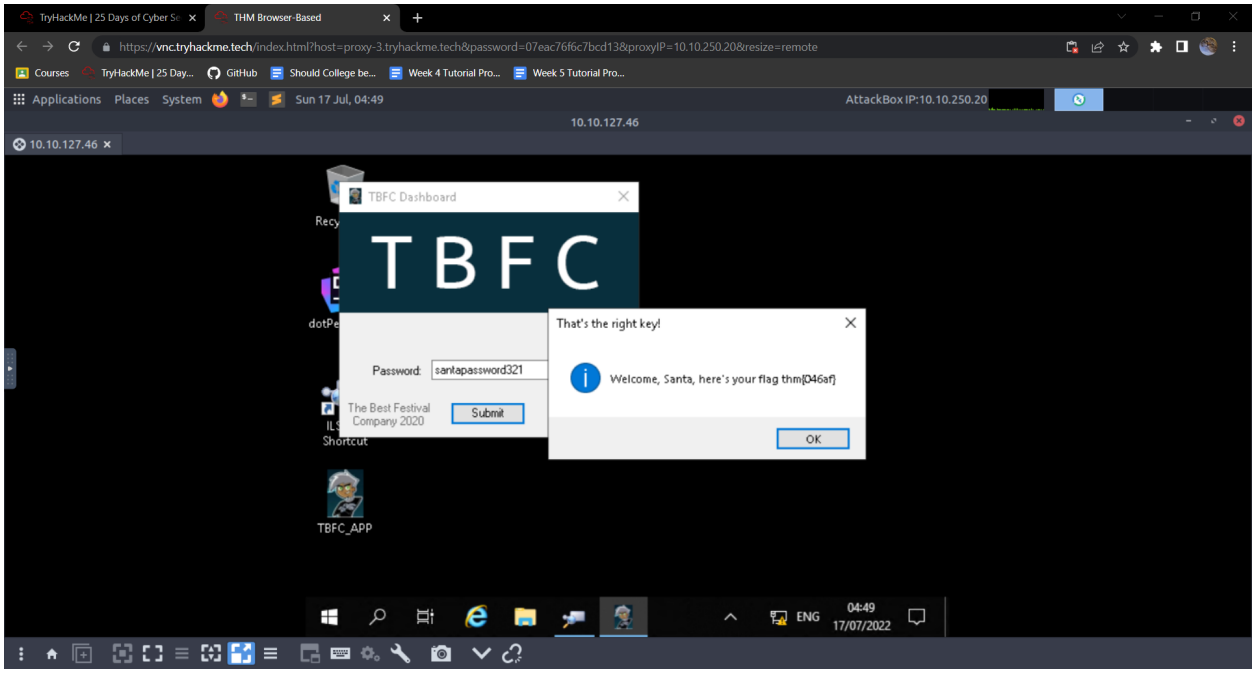
Answer : santapassword321





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

Answer : thm{046af}



Thought Process / Methodology :

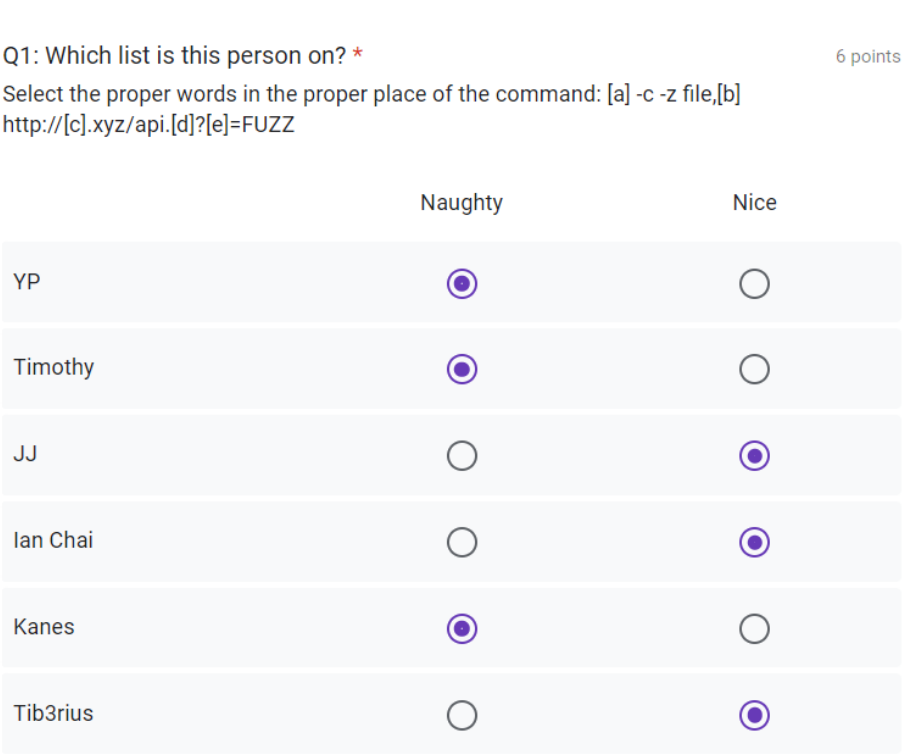
Firstly, we used Remmina to connect to the instance. We put the MACHINE_IP, username which is **cmnatic** and password which is **Adventofcyber!**. After log in into the Remote Desktop Protocol (RDP). We open the **TBFC_APP** and we put the incorrect password to see the message that shows up if you enter 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 :



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"?

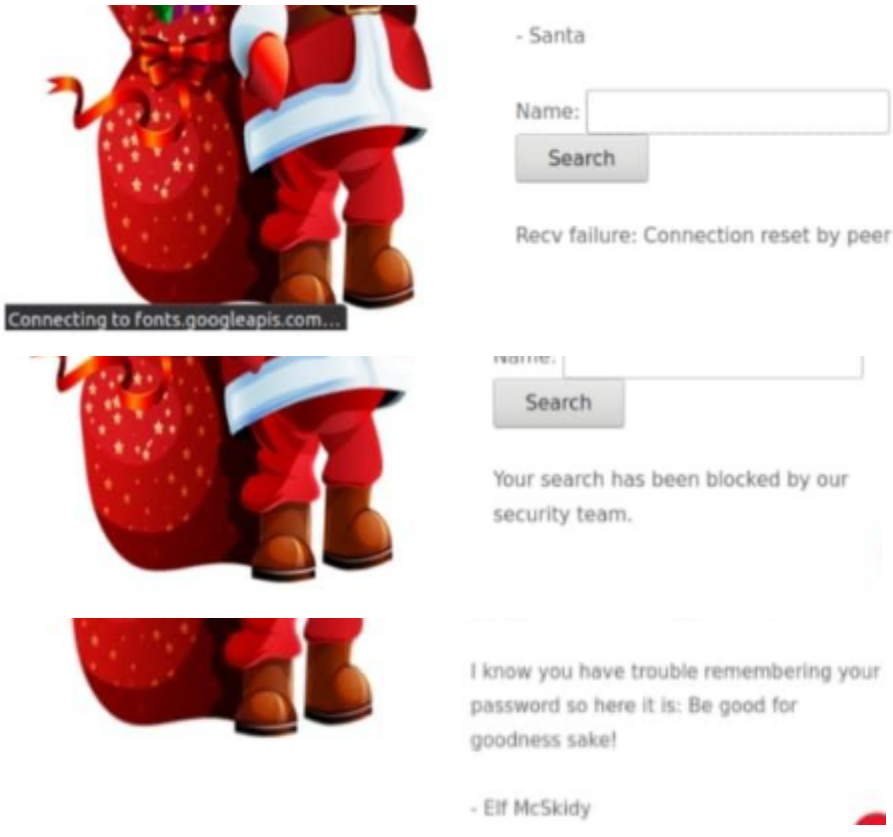
Answer : Failed to connect to list.hohoho port 80: Connection refused

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

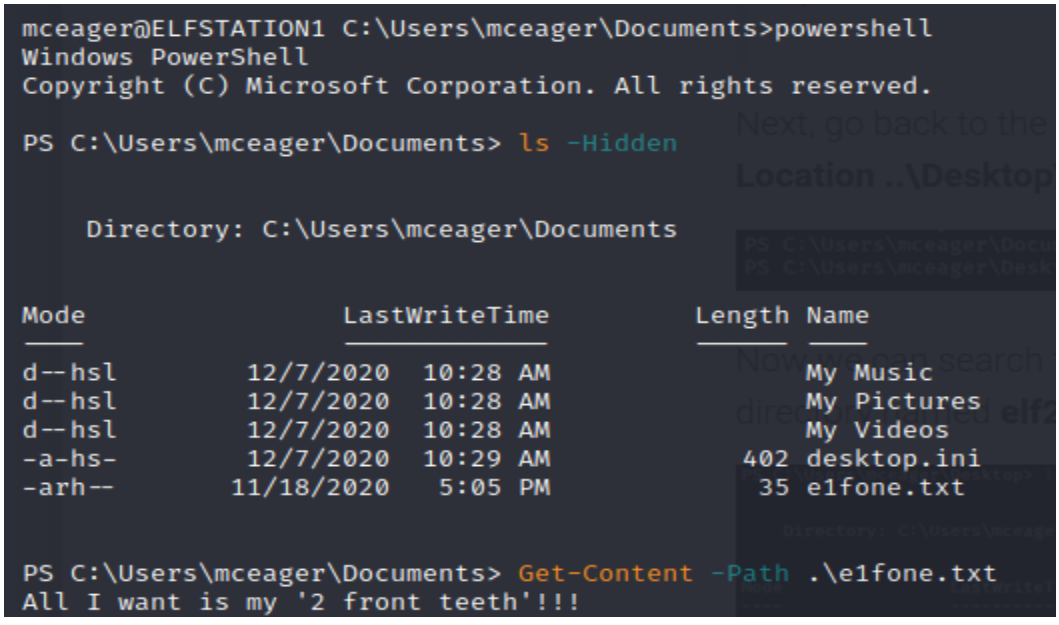
Question 1 : Check the ssh manual. What does the parameter -l do?

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.
```

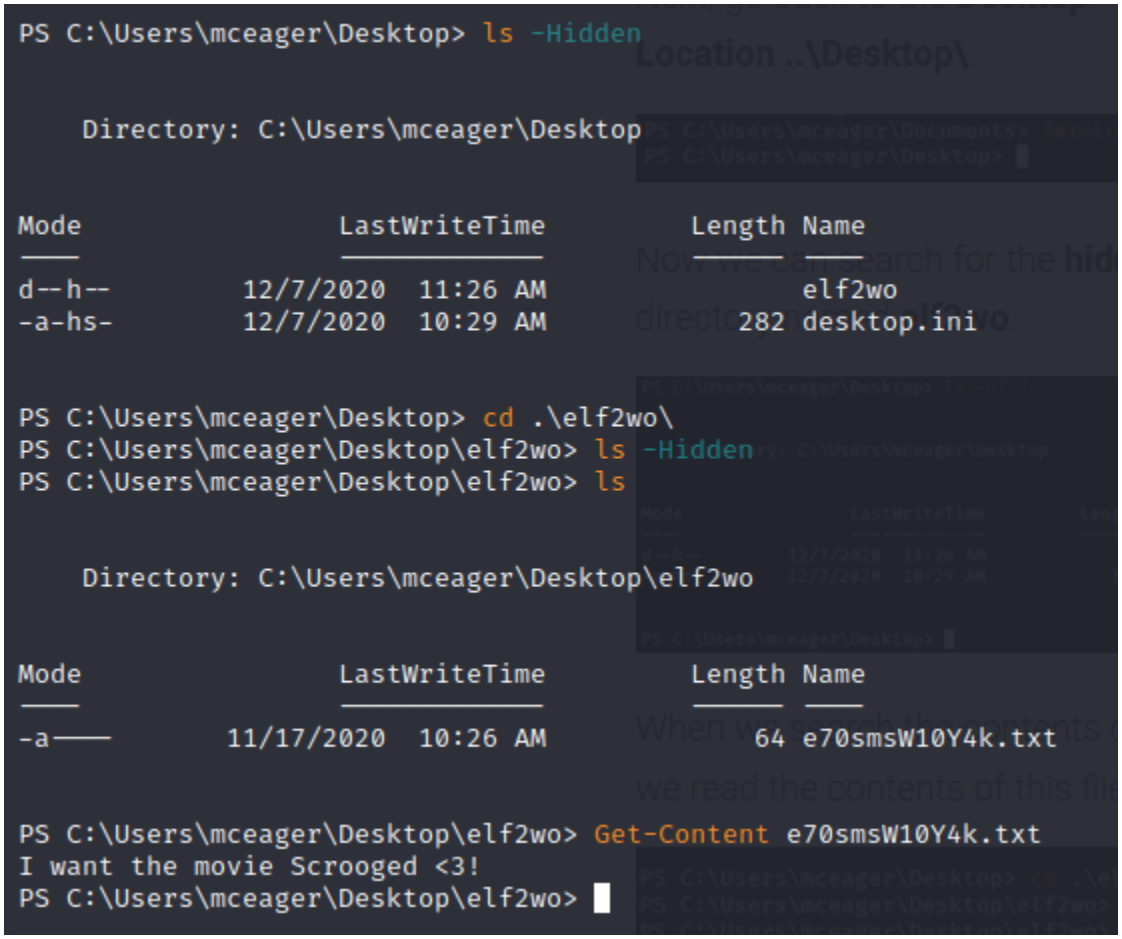
Question 2 : Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

Answer : 2 front teeth



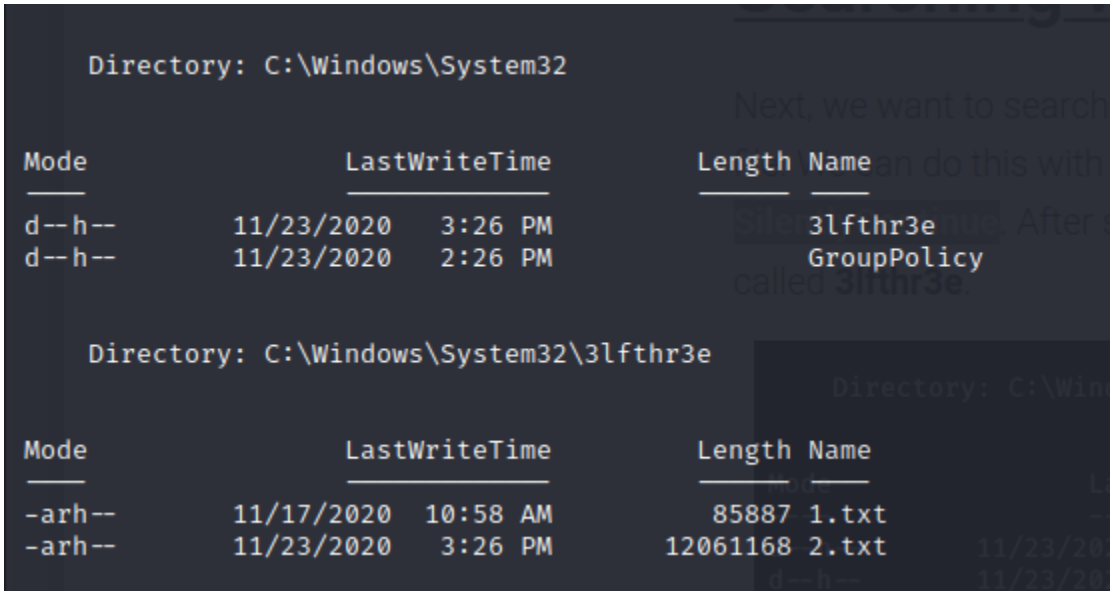
Question 3 : Search on the desktop for a hidden folder that contains the file for Elf 2. Read the contents of this file. What is the name of that movie that Elf 2 wants?

Answer : Scrooged



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

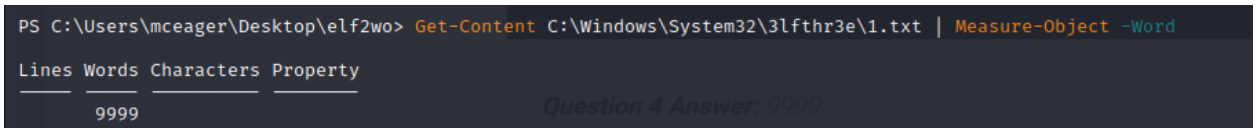
Answer : 3lfthr3e



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

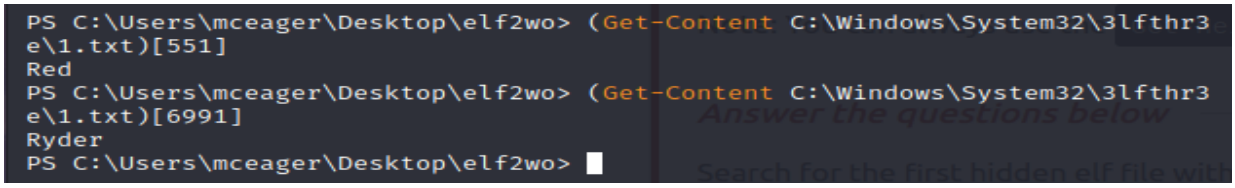
Question 5 : How many words does the first file contain?

Answer : 9999



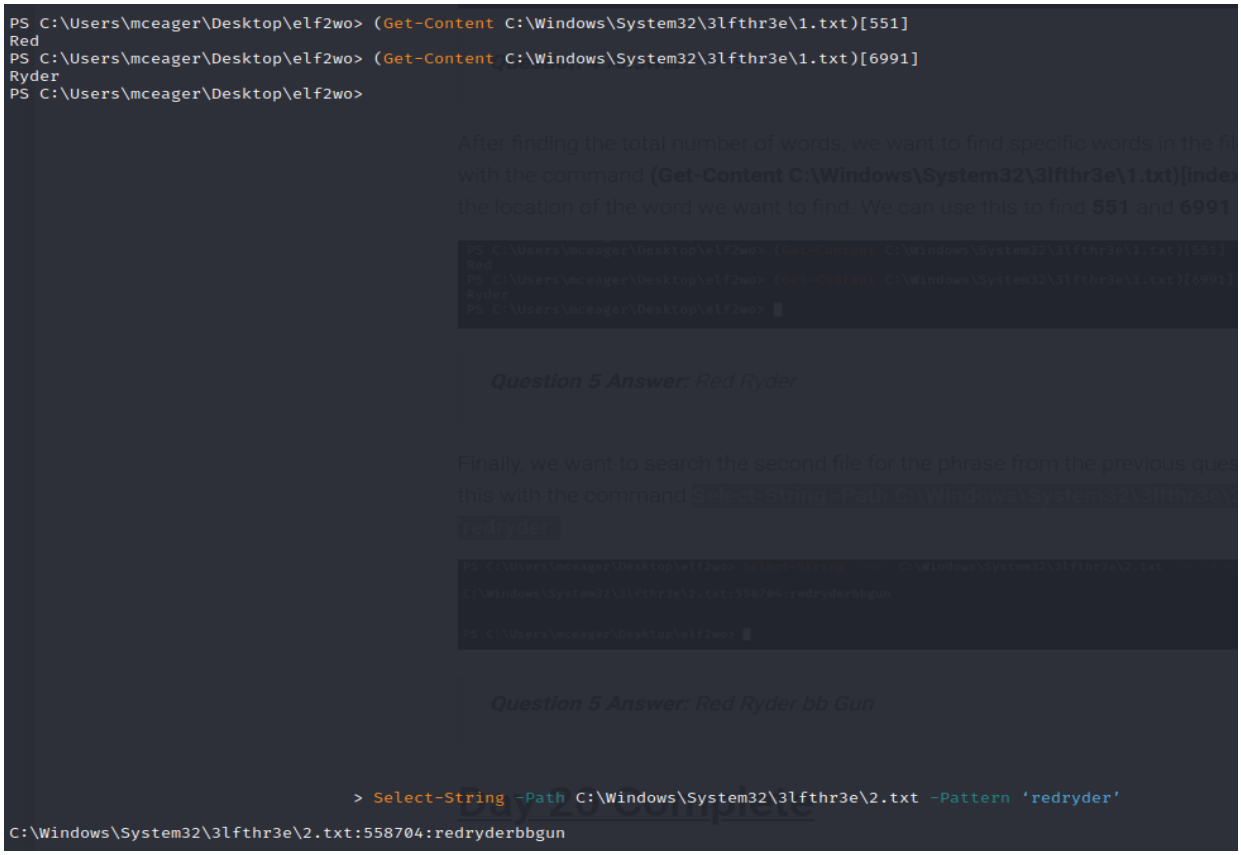
Question 6 : What 2 words are at index 551 and 6991 in the first file?

Answer : Red Ryder



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



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.