

PSP0201

Week 5

Writeup

Group Name: GGez

Group members:

ID Number	Name	Role
1211101951	Muhammad Zaieff Danial Bin Mohd Suhaimi	Leader
1211100528	Muhammad Arief Fahmi Bin Syahril Anuar	Member
1211101120	Adam Uzair Bin Mohd Sori	Member
1211101643	Sivaharriharann A/L Ramanathan	Member

Day 16 : Scripting – Help! Where is Santa?

Tools used: Kali Linux , Firefox , Terminal , Nano , Python

Solution/Walkthrough:

Question 1:

```
PS> 121100528@kali: /home/121100528
File Actions Edit View Help
Type 'help' to get help.

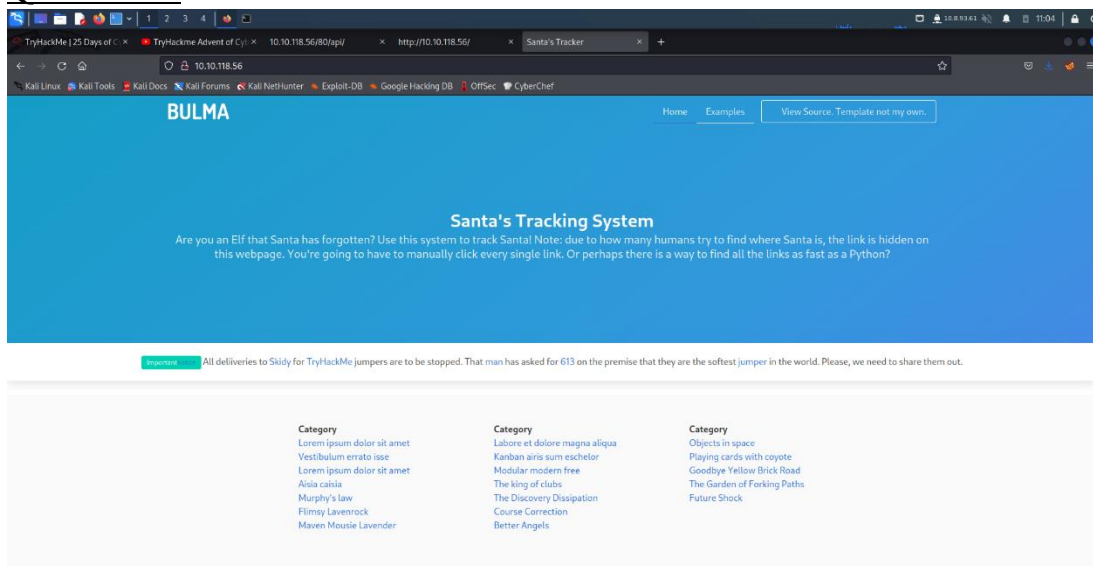
[121100528@kali:~/home/121100528]
PS> nmap -sS 10.10.118.56
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-12 08:33 EDT
Initiating Ping Scan at 08:33
Scanning 10.10.118.56 [2 ports]
Completed Ping Scan at 08:33, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:33
Completed Parallel DNS resolution of 1 host. at 08:33, 0.00s elapsed
Initiating Connect Scan at 08:33
Scanning 10.10.118.56 [1000 ports]
Discovered open port 80/tcp on 10.10.118.56
Discovered open port 22/tcp on 10.10.118.56
Completed Connect Scan at 08:33, 26.98s elapsed (1000 total ports)
Nmap scan report for 10.10.118.56
Host is up (0.26s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 27.22 seconds
->

[121100528@kali:~/home/121100528]
PS> nmap -sS 10.10.118.56
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-12 08:42 EDT
Initiating Ping Scan at 08:42
Scanning 10.10.118.56 [2 ports]
Completed Ping Scan at 08:42, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:42
Completed Parallel DNS resolution of 1 host. at 08:42, 0.00s elapsed
Initiating Connect Scan at 08:42
Scanning 10.10.118.56 [1000 ports]
Discovered open port 22/tcp on 10.10.118.56
Discovered open port 80/tcp on 10.10.118.56
Status: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 17.25% done; ETC: 08:42 (0:00:18 remaining)
Status: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 77.94% done; ETC: 08:42 (0:00:04 remaining)
Completed Connect Scan at 08:42, 19.98s elapsed (1000 total ports)
Nmap scan report for 10.10.118.56
Host is up (0.26s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

By using nmap while using the address that we get , we can get the port number that we require to open the API .

Question 2:

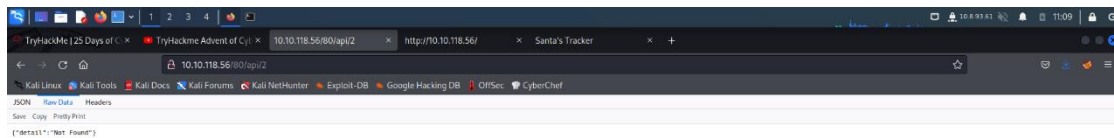


We can get the template name by visiting the url page .

Question 3:

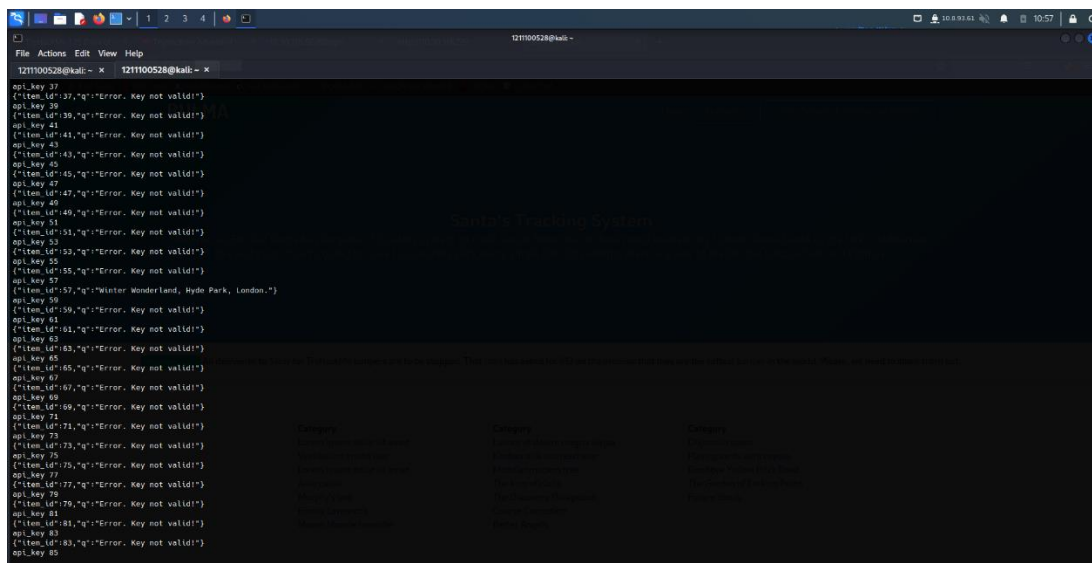
We can get the answer to this question by simply adding “/api/” to the url and port number for the web server.

Question 4:



To get to this page we have to type in the url code plus the port number and the api . After that just open the Raw Data tab in the page .

Question 5 & 6:



To get to the address we should use the brute.py method and also the nano app to then use python commands to get the location address and also the correct api key in front of the address .

Thought Process / Methodology :

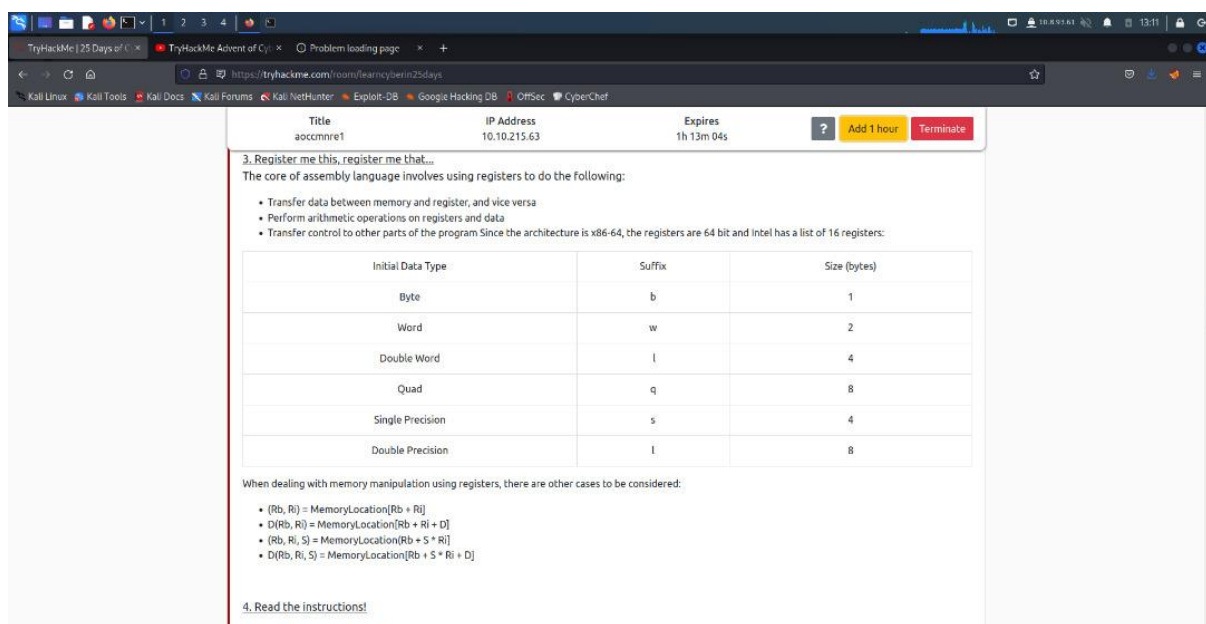
First of all we have to open the website by starting the machine to get to the IP address . Then , we need to get the port number by opening the terminal and use the nmap method . Then we can open the website by using IP address plus the port number to open the website . Next we can add “ /api/ ” at the url to open the api secret page to find a lot of information such as the Raw Data . Finally , to get the location address of santa and the api key , we need to use the brute technic and use the python language to as a command to get the things that we want .

Day 17 : Reverse Engineering – ReverseELFneering

Tools used: Kali Linux , Firefox , Terminal

Solution/Walkthrough:

Question 1:



The screenshot shows a web browser window with the URL <https://tryhackme.com/room/learnassembly25days>. The page title is "3. Register me this, register me that...". The content explains that the core of assembly language involves using registers and lists three types of operations: transferring data between memory and registers, performing arithmetic operations, and transferring control. It also mentions that the architecture is x86-64 and lists 16 registers. A table follows, detailing initial data types, their suffixes, and sizes in bytes.

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

Below the table, it states: "When dealing with memory manipulation using registers, there are other cases to be considered:" and lists four cases involving MemoryLocation and registers Rb, Ri, S, and D.

4. Read the instructions!

For question 1 we can find the answer in the tryhackme question itself .

Question 2:

```

File Actions Edit View Help
gdbfc-day17:~$ ./2 -d -f file1
Process with PID 1602 started...
= attach 1022 1022
bin.baddr: 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits: 64
[0x00400030]~> aa
WARNING: block size exceeding max block size at 0x00400270
[-] try changing it with e.asm.bb_maxsize
WARNING: block size exceeding max block size at 0x00400c00
[-] try changing it with e.asm.bb_maxsize
[-] Analyze all fregs starting with sym, and entry0 (aa)
[0x00400a20]~> afl
0x00400000 3 23 sym__init
0x00400020 1 6 fcn.00400420
0x00400030 1 6 fcn.00400430
0x00400040 1 6 fcn.00400430
0x00400050 1 6 fcn.00400430
0x00400060 1 6 fcn.00400450
0x00400070 1 6 fcn.00400450
0x00400080 1 6 fcn.00400450
0x00400090 1 6 fcn.00400450
0x004000a0 1 6 fcn.00400450
0x004000b0 1 6 fcn.00400450
0x004000c0 1 6 fcn.00400460
0x004000d0 1 1 sym.backtrace_and_maps.constprop.1
0x004000e0 1 00 sym.__malloc_usert_callbacks
0x004000f0 1 35 sym__grave_release_step.part.1
0x00400100 1 33 sym__uex
0x00400110 4 120658 -> 41 entry0_fini
0x00400120 90 2157 entry0_init
0x00400130 1 42 entry0
0x00400140 1 2 sym__dl_relocate_static_pic
0x00400150 3 35 sym__deregister_tls_callbacks
0x00400160 3 53 sym__register_tm_clones
0x00400170 5 50 -> 49 sym__do_global_ctors_aux
0x00400180 3 45 -> 48 entry0_init
0x00400190 1 60 sym__main
0x004001a0 31 613 -> 600 sym__get_common_indeces.constprop.1
0x004001b0 10 1807 -> 210 sym__libc_start_main
0x004001c0 25 305 -> 301 sym__libc_check_standard_fds
0x004001d0 15 501 -> 500 sym__libc_setup_tls
0x004001e0 7 140 sym__libc_csu_init
0x004001f0 5 65 -> 74 sym__libc_csu_fini
0x00400200 11 539 sym__user_i_fall_base
0x00400210 1 66 sym__abort_fat1
0x00400220 04 2127 -> 2244 sym__cleanup_text
0x00400230 10 510 -> 101 sym__transcsp
0x00400240 02 1908 -> 1123 sym__plural_eval
0x00400250 170 3064 -> 2001 sym__nl_init_msg

```

The command that we need to input to analyse the program in radare2 is the command **“aa”** .

Question 3:

```

121100528@kali: -
File Actions Edit View Help
121100528@kali: - x 121100528@kali: - x 121100528@kali: - x

0x77fe39a38184 0000 0000 1700 0000 0100 0000 0000 0000 .....
0x77fe39a38114 0000 0000 0000 0000 0200 0000 0000 0000 .....
0x77fe39a380c4 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a38034 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a38344 0000 0000 c6fa 0b71 6f98 d3fe 1919 4000 .....
0x77fe39a38314 0000 0000 0000 0000 0000 0000 1500 0000 .....
0x77fe39a38364 0000 0000 0000 0000 0000 0000 c6fa 20ca .....
0x77fe39a38374 a0eb 2f01 c6fa 7fee 6f98 d3fe 0000 0000 .....
0x77fe39a38384 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a38394 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a383a4 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a383b4 0000 0000 0000 0000 0000 0000 0000 0000 .....
[0x00400055]- ds
[0x00400055]- px @rbp-0xc
offset 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0x77fe39a382c4 0400 0000 0500 0000 0000 0000 0000 7010 4000 .....
0x77fe39a382d4 0000 0000 1910 4000 0000 0000 0000 0000 .....
0x77fe39a382e4 c000 0000 0000 0000 0100 0000 f803 a330 .....
0x77fe39a382f4 fe7f 0000 a0eb 4000 0000 0000 0000 0000 .....
0x77fe39a38304 0000 0000 1700 0000 0100 0000 0000 0000 .....
0x77fe39a38314 0000 0000 0000 0000 0200 0000 0000 0000 .....
0x77fe39a38324 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a38334 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a38344 0000 0000 c6fa 0b71 6f98 d3fe 1919 4000 .....
0x77fe39a38354 0000 0000 0000 0000 0000 0000 1500 0000 .....
0x77fe39a38364 0000 0000 0000 0000 0000 0000 c6fa 20ca .....
0x77fe39a38374 a0eb 2f01 c6fa 7fee 6f98 d3fe 0000 0000 .....
0x77fe39a38384 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a38394 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a383a4 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a383b4 0000 0000 0000 0000 0000 0000 0000 0000 .....
[0x00400055]- ds
[0x00400055]- px @rbp-0xb
offset 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0x77fe39a38200 0500 0000 0000 0000 7010 4000 0000 0000 .....
0x77fe39a38208 1910 4000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a38210 c000 0000 0000 0000 0100 0000 f803 a330 .....
0x77fe39a38218 1700 0000 0100 0000 0000 0000 0000 0000 .....
0x77fe39a38310 0000 0000 0200 0000 0000 0000 0000 0000 .....
0x77fe39a38220 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a38338 0000 0000 0000 0000 0000 0000 c6fa 20ca .....
0x77fe39a38340 c6fa 0b71 6f98 d3fe 1919 4000 0000 0000 .....
0x77fe39a38350 0000 0000 0000 0000 1500 0000 0000 0000 .....
0x77fe39a38360 0000 0000 0000 0000 c6fa 20ca a0eb 2f01 .....
0x77fe39a38370 c6fa 7fee 6f98 d3fe 0000 0000 0000 0000 .....
0x77fe39a38380 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a38390 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a383a0 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x77fe39a383b0 0000 0000 0000 0000 0000 0000 0000 0000 .....

```

The command to set a breakpoint in radare2 would be the command “**db**”.

Question 4:

```

File Actions Edit View Help
0x040f2a29 11 190      sys.free_mem_1
0x040f2a2e 7 73       -> 60      sys._nl_tindonatin_subtraeres
0x040f3330 26 247     -> 237     sys._nl_unload_dmain
0x040f3c38 4 57       sys.buffer_free
0x040f3c70 218 179    -> 3667    sys.free_derivation
0x040f3f30 23 266    -> 298     sys.free_modules_db
0x040f3f48 204 668    -> 4406    sys.free_mon
0x040f398e9 4 34      -> 31      sys.free_mem_2
0x040f39118 8 53      -> 74      sys.free_mem_3
0x040f39159 3 27      sys.do_release_all
0x040f39178 1 30      sys.free_mem_4
0x040f391e9 159 1971   -> 1987    sys._nl_local_subtraeres
0x040f3960a 14 718    -> 286     sys.free_mem_5
0x040f39648 9 92      sys.free_mem_6
0x040f396a8 17 210    -> 246     sys.free_slotinfo
0x040f39680 72 903    -> 939     sys.free_mem_7
0x040f39f59 237 4239  -> 4172    sys.arena_thread_freeres
0x040f3f608 1 0       sys.finit
0x040f3e219 1 1321    obj._d_init_static_its
0x040f3e868 1 1878    obj._d_wait_lookup_done
[0x040f3e20] pdf @main
C++ module
/ (local) symtab: 58
  symtab(1):
    l var int local_ch @ rbp-8xc
    l var int local_0h @ rbp-840
    l var int local_4h @ rbp-8x4
    0x040f39648 15m 0x040f39648 (init)
    0x040f39648 55      push rbp
    0x040f39648 4800c5    mov rbp, rbp
    0x040f39651 4803c18    sub rbp, 0x18
    0x040f39652 c745f40a00000000    mov dword [local_ch], 4
    0x040f39653 c745f00500000000    mov dword [local_0h], 5
    0x040f39663 8b05f4      mov edx, dword [local_ch]
    0x040f39664 8b45f8      mov esi, dword [local_0h]
    0x040f39669 0109      add esi, edx
    0x040f3966b 0945f8      mov dword [local_4h], esi
    0x040f3966c 8b45f8      mov esi, dword [local_0h]
    0x040f39671 8b05f8      mov esi, dword [local_0h]
    0x040f39674 8b45f4      mov esi, dword [local_ch]
    0x040f39677 89c5      mov esi, ecx
    0x040f39678 4803c00100000000    lea edi, dword str.the_value_of
    a.is_d.the_value_of.b.is_d.and.the_value_of.c.is_d (0x040f39678)
    value_of.b.is_d.the_value_of.c.is_d.and.the_value_of.d.is_d (0x040f39678)
    0x040f39683 b800000000    mov eax, 0
    0x040f39685 09f0e00000    call sym._printf
    0x040f39686 b800000000    mov esi, 0
    0x040f39687 c9      leave
    0x040f39688 c3      ret
[0x040f3960]

```

The command that we need to execute the program until we hit a breakpoint would be the command “**pdf @main**”.

Question 5:

The screenshot shows a Windows desktop with a taskbar at the top containing icons for a file explorer, a terminal, and a clock showing 13:54. The active window is a terminal titled "elfmccsger@tbfic-day-17: ~". The terminal output shows the execution of a challenge named "challenge1". The user runs a command to attach to a process with PID 1813. The terminal displays assembly code for a function named "main". The code includes comments in Chinese and assembly instructions. The assembly code is as follows:

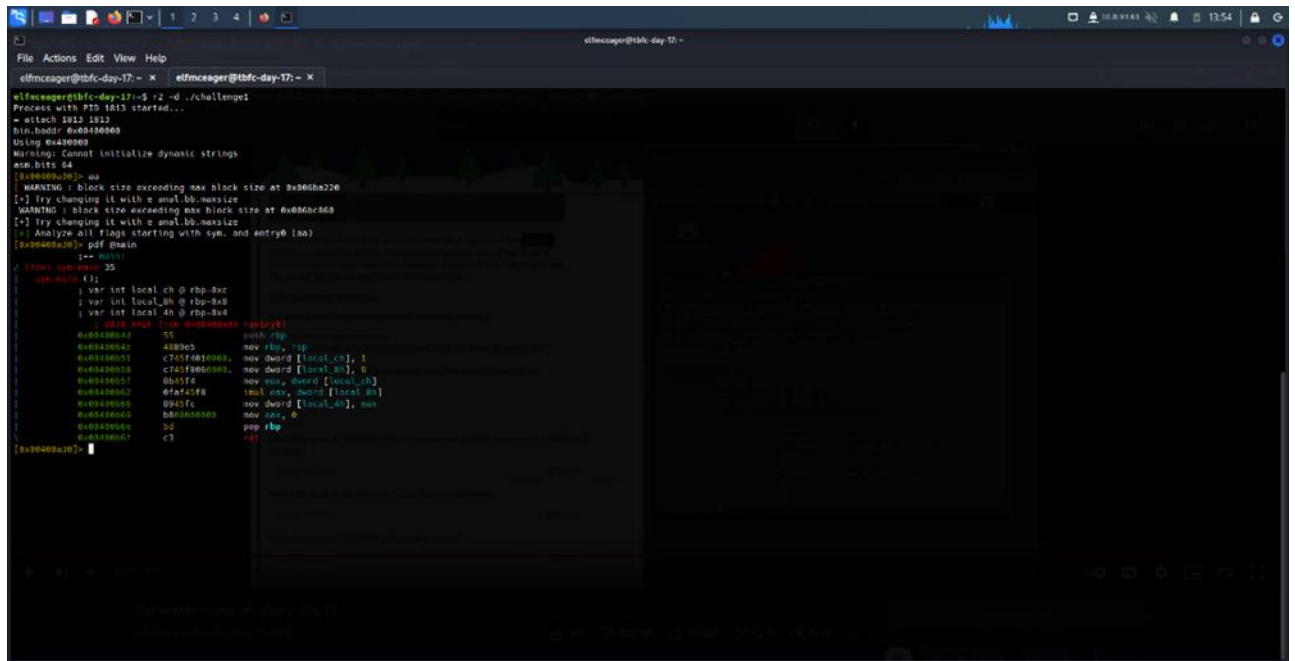
```

[0x00401000]-> 00
WARNING : block size exceeding max block size at 0x00401000
[+] Try changing it with e asm.bb.maxsize
WARNING : block size exceeding max block size at 0x00401000
[+] Try changing it with e asm.bb.maxsize
[*] Analyze all flags starting with sym. and entry0 [no]
[0x00401000]-> pdf main
-- main
/ P201 sym.main 35
asm.main (1);
{
    ; var int local_ch @ rbp-8xc
    ; var int local_0h @ rbp-8x8
    ; var int local_4h @ rbp-8x4
    mov dword [local_ch], 1
    push rbp
    mov rbp, esp
    mov dword [local_ch], 1
    mov dword [local_0h], 0
    mov max, dword [local_0h]
    incl eax, dword [local_0h]
    mov dword [local_0h], max
    mov eax, 0
    pop rbp
    mov dword [local_0h], 0
}
[0x00401000]->

```

The value of local_ch when its corresponding movl instruction is called “1” as in the numeral digit .

Question 6:

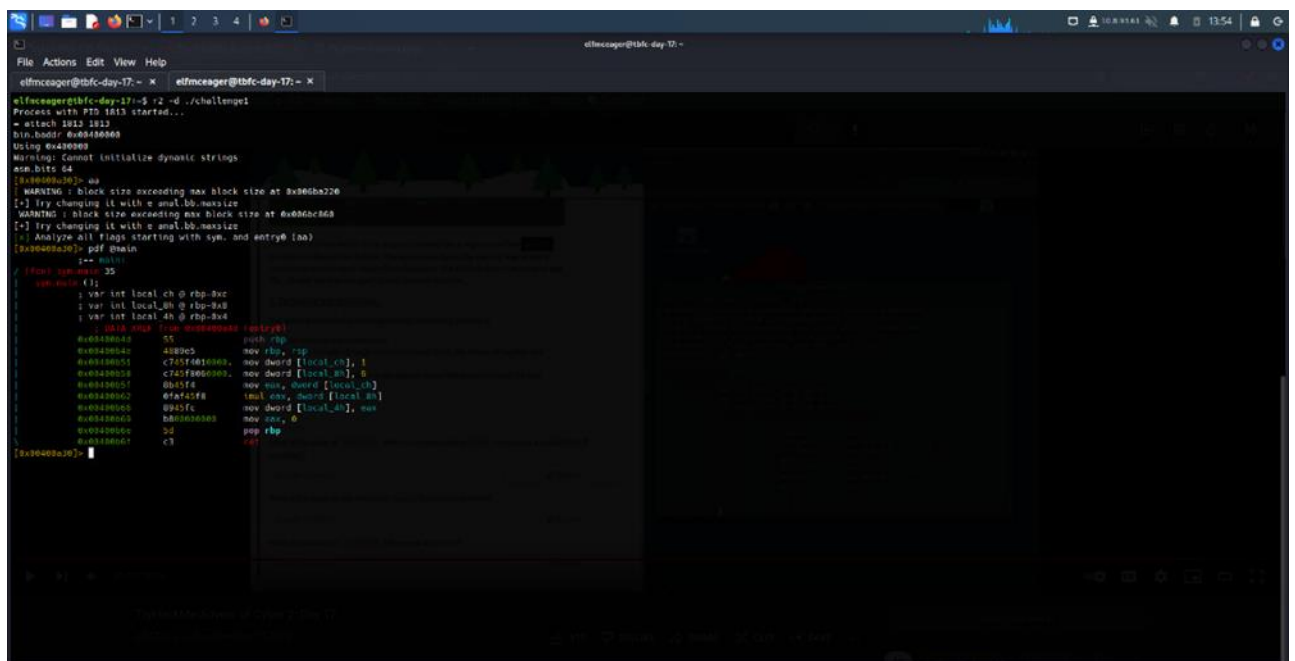


The screenshot shows a debugger window with the following assembly code and warnings:

```
File Actions Edit View Help
elfmceager@tbfc-day-17:~$ xelfmceager@tbfc-day-17:~$ x
elfmceager@tbfc-day-17:~$ x2 -d ./challenge1
Process with PID 1813 started...
- attach 1813 1813
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[0x00400000] aa
[WARNING] : block size exceeding max block size at 0x00400020
[?] try changing it with e asm.bb.maxsize
[WARNING] : block size exceeding max block size at 0x00400060
[?] try changing it with e asm.bb.maxsize
[?] Analyze all flags starting with sym. and entry@ (aa)
[0x00400000] pdf @main
[?] sym.main: 35
[0x00400000] {1}
[?] var int local_ch @ rbp-8xc
[?] var int local_ah @ rbp-8x8
[?] var int local_4h @ rbp-8x4
[?] 0x00400000: 55 push rbp
[?] 0x00400001: 4889c5 mov rbp, rbp
[?] 0x00400002: c745f8010000 mov dword [local_ch], 1
[?] 0x00400003: c745f8060000 mov dword [local_ah], 6
[?] 0x00400004: 8b45f8 mov eax, dword [local_ch]
[?] 0x00400005: 0045f8 imul eax, dword [local_ah]
[?] 0x00400006: 0045f8 mov dword [local_4h], eax
[?] 0x00400007: b800000000 mov ecx, 0
[?] 0x00400008: 5d pop rbp
[?] 0x00400009: c3 ret
```

The value of eax when the imull instruction is called “6” as in the numeral digit.

Question 7:



The screenshot shows a debugger window with the following assembly code and warnings:

```
File Actions Edit View Help
elfmceager@tbfc-day-17:~$ xelfmceager@tbfc-day-17:~$ x
elfmceager@tbfc-day-17:~$ x2 -d ./challenge1
Process with PID 1813 started...
- attach 1813 1813
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[0x00400000] aa
[WARNING] : block size exceeding max block size at 0x00400020
[?] try changing it with e asm.bb.maxsize
[WARNING] : block size exceeding max block size at 0x00400060
[?] try changing it with e asm.bb.maxsize
[?] Analyze all flags starting with sym. and entry@ (aa)
[0x00400000] pdf @main
[?] sym.main: 35
[0x00400000] {1}
[?] var int local_ch @ rbp-8xc
[?] var int local_ah @ rbp-8x8
[?] var int local_4h @ rbp-8x4
[?] 0x00400000: 55 push rbp
[?] 0x00400001: 4889c5 mov rbp, rbp
[?] 0x00400002: c745f8010000 mov dword [local_ch], 1
[?] 0x00400003: c745f8060000 mov dword [local_ah], 6
[?] 0x00400004: 8b45f8 mov eax, dword [local_ch]
[?] 0x00400005: 0045f8 imul eax, dword [local_ah]
[?] 0x00400006: 0045f8 mov dword [local_4h], eax
[?] 0x00400007: b800000000 mov ecx, 0
[?] 0x00400008: 5d pop rbp
[?] 0x00400009: c3 ret
```

The value of local_4h before eax is set to 0 would be the value “6” .

Thought Process / Methodology:

First of all, we have to connect the terminal to the web page that we need to access and that is by using the command “nmap” and “cat target.txt” to target the web page. Then, we just need to access the page by using the username and password that were given so that we can use **Radare2** to open the binary debugging mode. After that we can use the command “aa” to start analyse the r2 program. Once the analysis is complete we need to find on where to start analysing from like an entry point and that is by using the command “afl” . After we found out the main function, we can examine the assembly code by running the command “pdf @main”. Then we can set a breakpoint by using the command “db”. After we’ve set a breakpoint, we can run the program by using the command “dc” to execute the program until we hit the breakpoint. Then we need to view the contents of the variable and to do that we should use the command “rbp-0xc”. Finally, we just need to repeat the same process by using the command “ds” to execute and move on to the next binary values that we need.

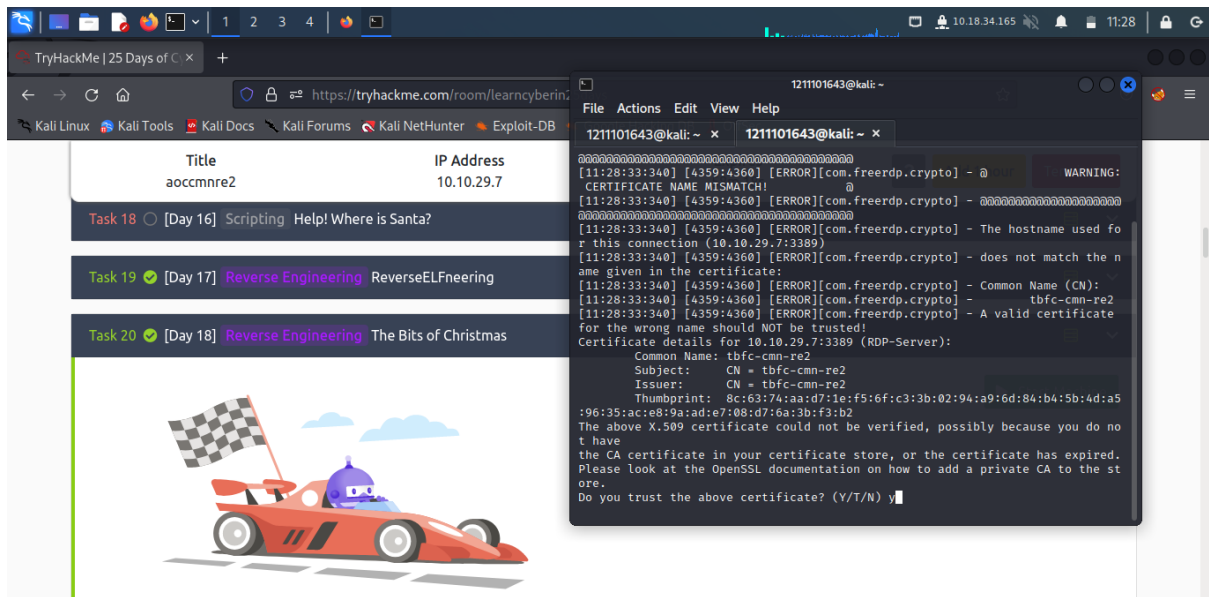
Day 18: Reverse Engineering - The Bits of Christmas

Tools used: Kali Linux, Firefox, Terminal

Solution/Walkthrough:

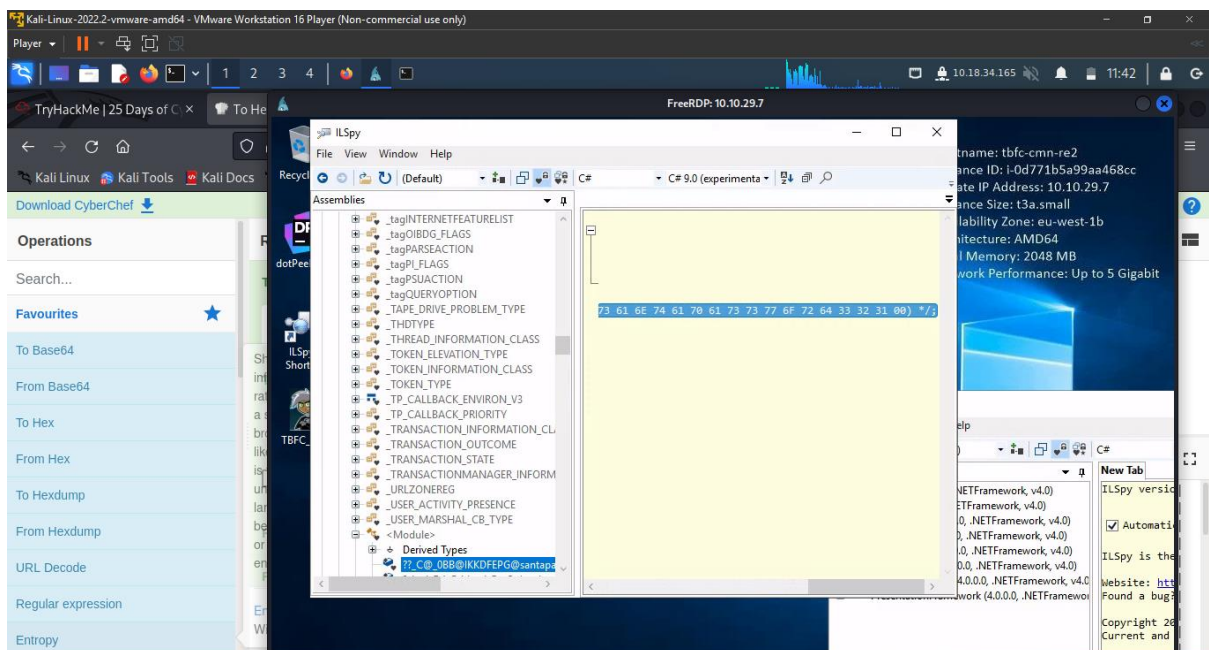
Question 1:

First of all, we install remmina open remmina using terminal



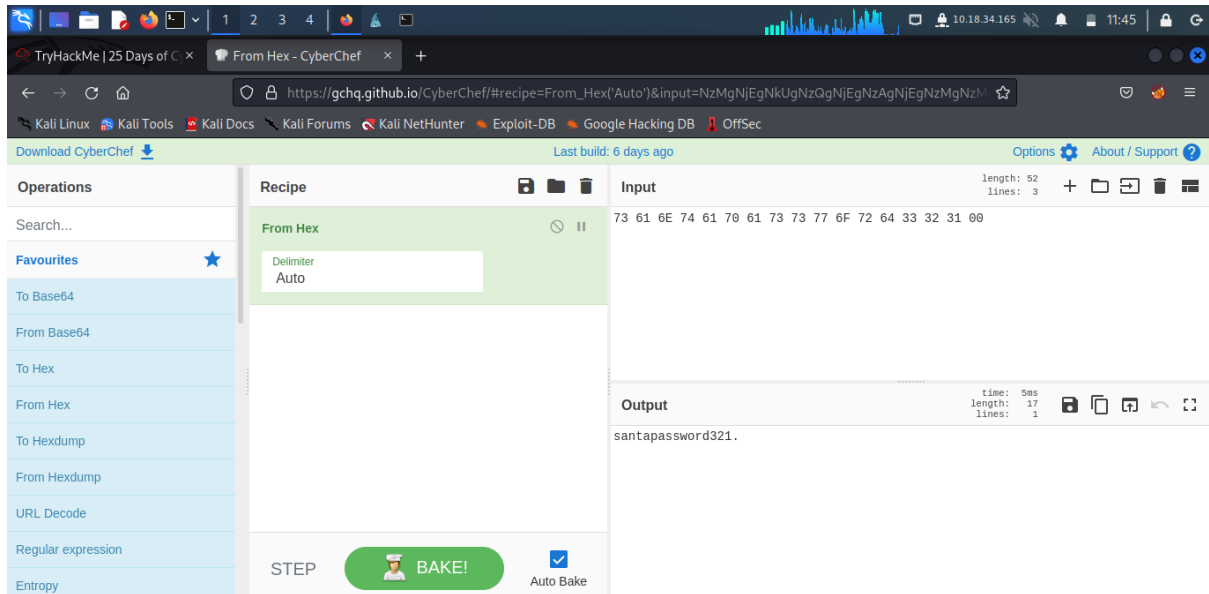
Question 2:

Then we log in into rdp server and we click the password is formatted in hexadecimal.



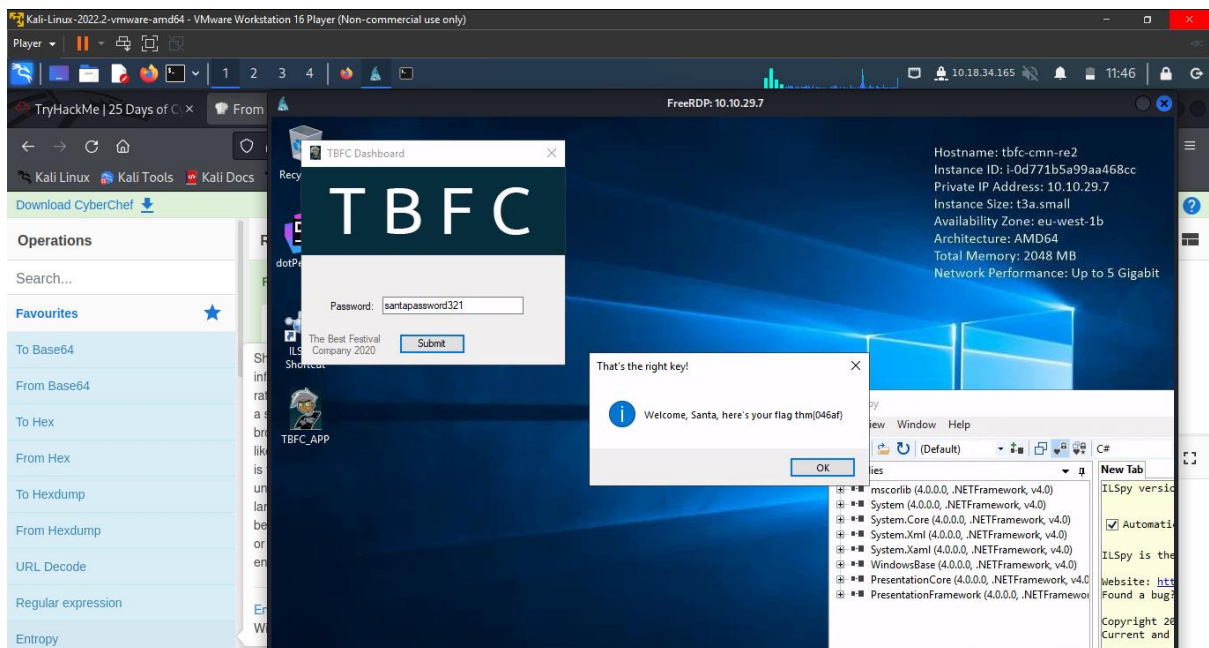
Question 3:

We get the password from the cyberchef.



Question 5:

Finally, we put the password in TBFC and get the right key.



Methodology:

Open terminal and open remmina to get the password of TBFC. Then, get into the RDP and get the password. The file that displayed to us after we click the password is formatted in hexadecimal. We can use an online tool such as Cyberchef to decode that and the results gives by Cyberchef is the same password on the previous file. After that, we put the password in the TVFC and get the thm to answer the tryhackme question.

Day 19: The Naughty or Nice List

Tools used: Firefox, Kali Linux

Question 1:

Type in the name provided into the search bar.

Name:

JJ is on the Naughty List.

Name:

Tib3rius is on the Nice List.

Name:

YP is on the Nice List.

Name:

Search

Kanes is on the Naughty List.

Name:

Search

Timothy is on the Naughty List.

Question 2:

Type in “/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F” to the url.



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

Not Found

The requested URL was not found on this server.



Question 3:

Type in “/?proxy=http%3A%2F%2Flist.hohoho%3A80” to the url.



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:

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



Question 4:

Type in `"/?proxy=http%3A%2F%2Flist.hohoho%3A22"` to the url.



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:

Recv failure: Connection reset by peer



Question 5:

Type in `"/?proxy=http%3A%2F%2Flocalhost"` to the url.



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:

Your search has been blocked by our security team.



Question 6 & 7:

Type in “?proxy=http%3A%2F%2Flist.hohoho.localtest.me” to the url.

Then, you will receive a message from Elf McSkidy that contains the password for santa. Insert the password to the admin login form.

List Administration

This page is currently under construction.

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

🌐 10.10.40.12

THM{EVERYONE_GETS_PRESENTS}

Thought Process / Methodology:

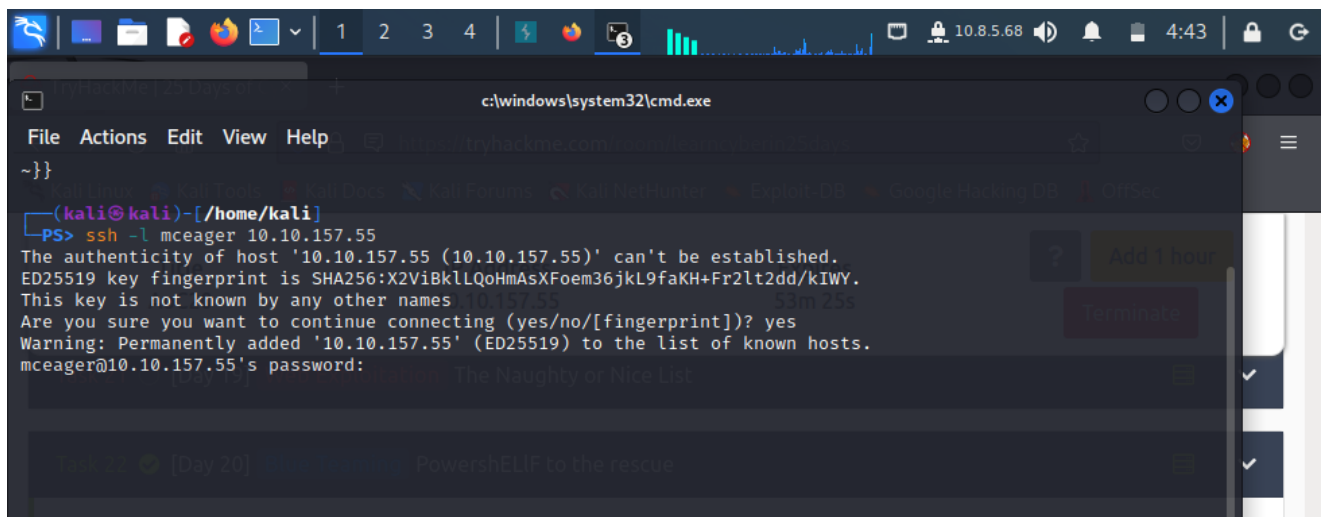
For day 19th we need to use Server-Side Request Forgery (SSRF) to complete this challenge. Basically by changing the url we can get different results based on what we thought such as hostnames, port number, etc. First, we need to get the ip address and put it in the url. Then, we can try to put names into the search bar to see if it had any responses. Then we can try changing the url by using localhost or a different port number to see the changes. To get Santa's password we need to change the portnames to a different one so that we can observe the changes. We will insert list.hohoho.localtest.me to see if it passes because it resolves every subdomain to 127.0.0.1. We can actually use any portnames but in this specific challenge, we will use localtest.me. Finally after inserting localtest.me ,we can finally get Santa's passwords and get the flag.

DAY 20: Powershell to the rescue

Tools used: Kali Linux, Terminal, Powershell

Solution/Walkthrough:

Question 1



You will use the SSH to connect to the remote machine. The command to run to connect to the remote machine is `ssh -l mceager MACHINE_IP`. Prompt the password 'r0ckStar!'


```
c:\windows\system32\cmd.exe - powershell

File Actions Edit View Help
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\Documents> cd..
PS C:\Users\mceager> Get-ChildItem

Directory: C:\Users\mceager

Mode                LastWriteTime         Length Name
----                -
d-r-----       12/7/2020 10:29 AM             Contacts
d-r-----       12/7/2020 11:26 AM             Documents
d-r-----       12/7/2020 10:29 AM             Favorites
d-r-----       12/7/2020 10:29 AM             Links
d-r-----       12/7/2020 10:29 AM             Music
d-r-----       12/7/2020 10:29 AM             Pictures
d-r-----       12/7/2020 10:29 AM             Saved Games
d-r-----       12/7/2020 10:29 AM             Searches
d-r-----       12/7/2020 10:29 AM             Videos

PS C:\Users\mceager> Set-Location Documents
PS C:\Users\mceager\Documents> Get-ChildItem -File -Hidden

Directory: C:\Users\mceager\Documents

Mode                LastWriteTime         Length Name
----                -
-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
```

Launch powershell and navigate to the documents folder. To list the contents of the current directory we are in, we can use the Get-ChildItem cmdlet. Next, use the -Hidden cmdlet to get only hidden items, and you are able to see the text file.

```
c:\windows\system32\cmd.exe - powershell

File Actions Edit View Help
At line:1 char:16
+ cat elfone.txt -Hidden
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Get-Content], ParameterBindingException
+ FullyQualifiedErrorId : NamedParameterNotFound,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> cd..
```

Enter cat text.file to reveal what does the Elf 1 want?

Question 2

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

Directory: C:\Users\mceager\Desktop

Mode                LastWriteTime         Length Name
----                -
d--h--             12/7/2020  11:26 AM              elf2wo
-a-hs-             12/7/2020  10:29 AM      282 desktop.ini

PS C:\Users\mceager\Desktop> ls -Hidden -Directory

Directory: C:\Users\mceager\Desktop

Mode                LastWriteTime         Length Name
----                -
d--h--             12/7/2020  11:26 AM              elf2wo

PS C:\Users\mceager\Desktop> cd .\elf2wo\
PS C:\Users\mceager\Desktop\elf2wo> Get-ChildItem

Directory: C:\Users\mceager\Desktop\elf2wo

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>
```

Reset the file directory location to desktop location. Repeat the question 1 process. Find the hidden file that contains what the Elf 2 wants. Enter cat text.file to reveal what does Elf 2 want?

Question 3

```
PS C:\Users\mceager\Desktop\elf2wo> cd
PS C:\Users\mceager\Desktop\elf2wo> cd C:/Windows/
PS C:\Windows> ls
```

Directory: C:\Windows

Mode	LastWriteTime	Length	Name
d-----	9/15/2018 12:19 AM		ADFS
d-----	9/15/2018 12:19 AM		appcompat
d-----	9/6/2019 5:31 PM		apppatch
d-----	12/7/2020 10:50 AM		AppReadiness
d-r-----	9/15/2018 2:11 AM		assembly
d-----	9/15/2018 12:19 AM		bcastdvr
d-----	9/15/2018 12:19 AM		Boot
d-----	9/15/2018 12:19 AM		Branding
d-----	12/7/2020 11:16 AM		CbsTemp
d-----	9/15/2018 12:19 AM		Containers
d-----	9/15/2018 12:19 AM		Cursors
d-----	11/23/2020 1:43 PM		debug
d-----	9/15/2018 12:19 AM		diagnostics
d-----	9/15/2018 2:08 AM		DigitalLocker
d--s----	9/15/2018 12:19 AM		Downloaded Program Files
d-----	9/15/2018 12:19 AM		drivers
d-----	9/15/2018 2:08 AM		en-US
d-r-s----	9/6/2019 5:31 PM		Fonts
d-----	9/15/2018 12:19 AM		Globalization
d-----	9/15/2018 2:08 AM		Help
d-----	9/15/2018 12:19 AM		IdentityCRL
d-----	9/15/2018 2:08 AM		IME
d-r-----	11/23/2020 1:42 PM		ImmersiveControlPanel
d-----	1/21/2021 7:05 AM		INF
d-----	9/15/2018 12:19 AM		InputMethod
d-----	9/15/2018 12:19 AM		L2Schemas
d-----	9/15/2018 12:19 AM		LiveKernelReports
d-----	12/3/2020 1:02 PM		Logs
d-r-s----	9/15/2018 12:19 AM		media
d-r-----	7/13/2022 1:51 AM		Microsoft.NET
d-----	9/15/2018 12:19 AM		Migration
d-----	9/15/2018 12:19 AM		ModemLogs
d-----	9/15/2018 2:09 AM		OCR
d-r-----	9/15/2018 12:19 AM		Offline Web Pages
d-----	11/23/2020 1:42 PM		Panther
d-----	9/15/2018 12:19 AM		Performance
d-----	9/15/2018 12:19 AM		PLA
d-----	9/6/2019 5:31 PM		PolicyDefinitions

Reset the file directory. Enter the windows file and type ls for the file list.

Next, enter System32 command and type ls for the file list.

```
PS C:\Windows> cd System32
PS C:\Windows\System32> ls
```

Directory: C:\Windows\System32

Mode	LastWriteTime	Length	Name
d-----	9/15/2018 2:08 AM		0409
d-----	9/15/2018 12:19 AM		AdvancedInstallers
d-----	9/15/2018 12:19 AM		am-et
d-----	9/15/2018 12:19 AM		AppLocker
d-----	9/6/2019 5:31 PM		appraiser
d-----s-	9/15/2018 2:10 AM		AppV
d-----	9/15/2018 2:08 AM		ar-SA
d-----	9/15/2018 12:19 AM		BestPractices
d-----	9/15/2018 2:08 AM		bg-BG
d-----	9/6/2019 5:31 PM		Boot
d-----	9/15/2018 12:19 AM		Bthprops
d-----	9/15/2018 12:19 AM		CatRoot
d-----	12/7/2020 2:44 PM		catroot2
d-----	9/15/2018 12:19 AM		CodeIntegrity
d-----	9/15/2018 2:08 AM		com
d-----	1/21/2021 7:18 AM		config
d-----s-	9/15/2018 12:19 AM		Configuration
d-----	9/15/2018 2:08 AM		cs-CZ
d-----	9/15/2018 2:08 AM		da-DK
d-----	9/15/2018 12:19 AM		DDFs
d-----	9/15/2018 2:08 AM		de-DE
d-----s-	9/6/2019 5:31 PM		DiagSvc
d-----	9/6/2019 5:31 PM		Dism
d-----	9/14/2018 11:09 PM		downlevel
d-----	11/26/2020 11:30 AM		drivers
d-----	9/15/2018 12:19 AM		DriverState
d-----	11/26/2020 11:24 AM		DriverStore
d-----	11/23/2020 1:45 PM		DRVSTORE
d-----s-	9/15/2018 2:08 AM		dsc
d-----	9/15/2018 2:08 AM		el-GR
d-----	9/6/2019 5:31 PM		en
d-----	9/15/2018 2:08 AM		en-GB
d-----	9/6/2019 5:31 PM		en-US
d-----	9/15/2018 2:08 AM		es-ES
d-----	9/15/2018 2:08 AM		es-MX
d-----	9/15/2018 2:08 AM		et-EE
d-----s-	9/15/2018 2:08 AM		F12


```
PS C:\Windows\System32> Get-ChildItem -Filter "*3*" -Recurse

Directory: C:\Windows\System32

Mode                LastWriteTime         Length Name
----                -
-a-----          9/15/2018 12:12 AM       659720 advapi32.dll
-a-----          9/15/2018 12:13 AM        2560 advapi32res.dll
-a-----          9/15/2018 12:12 AM       79872 avicap32.dll
-a-----          9/15/2018 12:12 AM      115712 avifil32.dll
-a-----          9/15/2018 12:12 AM      293344 cfmgr32.dll
-a-----          9/15/2018 12:12 AM       73728 clfs32.dll
-a-----          9/15/2018 12:12 AM       37888 cmc32.dll
-a-----          9/15/2018 12:12 AM      556032 cmd32.dll
-a-----          9/15/2018 12:12 AM       51712 cmd32.exe
-a-----          9/15/2018 12:12 AM       43008 cmmon32.exe
-a-----          9/15/2018 12:12 AM       29696 cmpbk32.dll
-a-----          9/15/2018 12:12 AM      674304 comctl32.dll
-a-----          9/6/2019  5:29 PM     1171968 comdlg32.dll
-a-----          9/15/2018 12:12 AM     1933200 crypt32.dll
-a-----          9/15/2018 12:12 AM        66082 C_037.NLS
-a-----          9/15/2018 12:12 AM     177698 C_10003.NLS
-a-----          9/15/2018 12:12 AM        66082 C_1143.NLS
-a-----          9/15/2018 12:12 AM        66082 C_1253.NLS
-a-----          9/15/2018 12:12 AM     189986 C_1361.NLS
-a-----          9/15/2018 12:12 AM     185378 C_20003.NLS
-a-----          9/15/2018 12:12 AM        66082 C_20273.NLS
-a-----          9/15/2018 12:12 AM        66082 C_20423.NLS
-a-----          9/15/2018 12:12 AM        66082 C_20833.NLS
-a-----          9/15/2018 12:12 AM        66082 C_20838.NLS
-a-----          9/15/2018 12:12 AM     180770 C_20932.NLS
-a-----          9/15/2018 12:12 AM     173602 C_20936.NLS
-a-----          9/15/2018 12:12 AM        66082 C_28593.NLS
-a-----          9/15/2018 12:12 AM        66082 c_28603.nls
-a-----          9/15/2018 12:12 AM       66594 C_437.NLS
-a-----          9/15/2018 12:12 AM       66594 C_737.NLS
-a-----          9/15/2018 12:12 AM       66594 C_863.NLS
-a-----          9/15/2018 12:12 AM      162850 C_932.NLS
-a-----          9/15/2018 12:12 AM     196642 C_936.NLS
-a-----          9/15/2018 12:12 AM     227840 C_G18030.DLL
-a-----          9/15/2018 12:12 AM     1219584 d3d10.dll
-a-----          9/15/2018 12:12 AM       36352 d3d10core.dll
-a-----          9/15/2018 12:12 AM     386456 d3d10level9.dll
-a-----          9/6/2019  5:28 PM     7556392 d3d10warp.dll
-a-----          9/15/2018 12:12 AM       179712 d3d10_1.dll
-a-----          9/15/2018 12:12 AM       37376 d3d10_1core.dll
```

Next, enter filter to reveal the file directory list

```
c:\windows\system32\cmd.exe - powershell

File Actions Edit View Help
-a----- 8/10/2020 8:50 AM 181184 vm3dddevapi64.dll
-a----- 8/10/2020 8:50 AM 30820288 vm3dgl64.dll
-a----- 8/10/2020 8:50 AM 178792 vm3dglhelper64.dll
-a----- 8/10/2020 8:50 AM 569960 vm3dservice.exe
-a----- 8/10/2020 8:50 AM 575944 vm3dum64-debug.dll
-a----- 8/10/2020 8:50 AM 548296 vm3dum64-stats.dll
-a----- 8/10/2020 8:50 AM 488048 vm3dum64.dll
-a----- 8/10/2020 8:50 AM 555976 vm3dum64_10-debug.dll
-a----- 8/10/2020 8:50 AM 526792 vm3dum64_10-stats.dll
-a----- 8/10/2020 8:50 AM 429168 vm3dum64_10.dll
-a----- 8/10/2020 8:50 AM 181864 vm3dum64_loader.dll
-a----- 9/6/2019 5:28 PM 646656 w32time.dll
-a----- 9/6/2019 5:28 PM 248832 w32tm.exe
-a----- 9/15/2018 12:12 AM 35328 w32topl.dll
-a----- 9/6/2019 5:29 PM 71696 win32appinventorycsp.dll
-a----- 9/15/2018 12:13 AM 697856 win32calc.exe
-a----- 9/6/2019 5:29 PM 193536 Win32CompatibilityAppraiserCSP.dll
-a----- 9/6/2019 5:29 PM 543744 win32k.sys
-a----- 9/6/2019 5:28 PM 2421248 win32kbase.sys
-a----- 9/6/2019 5:29 PM 3634688 win32kfull.sys
-a----- 9/15/2018 12:12 AM 17920 win32kns.sys
-a----- 9/15/2018 12:13 AM 847872 win32spl.dll
-a----- 9/15/2018 12:12 AM 125704 win32u.dll
-a----- 9/15/2018 12:12 AM 27648 Win32_DeviceGuard.dll
-a----- 9/15/2018 12:12 AM 2276864 Windows.Graphics.Printing.3D.dll
-a----- 9/15/2018 12:12 AM 606720 Windows.UI.Xaml.Resources.rs3.dll
-a----- 9/15/2018 12:12 AM 792992 winsqlite3.dll
-a----- 9/6/2019 5:28 PM 366592 Wldap32.dll
-a----- 9/15/2018 12:12 AM 17408 wowreg32.exe
-a----- 9/15/2018 12:12 AM 434952 ws2_32.dll
-a----- 9/15/2018 12:12 AM 66560 wsnmp32.dll
-a----- 9/15/2018 12:12 AM 18944 wsock32.dll
-a----- 9/15/2018 12:12 AM 64792 wtsapi32.dll
-a----- 9/15/2018 12:12 AM 143360 xwtpw32.dll

PS C:\Windows\System32> Get-ChildItem -Hidden -Directory -Filter "*3*"

Directory: C:\Windows\System32

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

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

Therefore, enter the same command with the hidden files and it shows the hidden file name that the Elf3 wanted.

Question 4

```
PS C:\Windows\System32> cd 3lfthr3e
PS C:\Windows\System32\3lfthr3e> ls
PS C:\Windows\System32\3lfthr3e> dir
PS C:\Windows\System32\3lfthr3e> Get-ChildItem
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 1.txt | Measure-Object

Count           : 9999
Average          :
Sum              :
Maximum         : 11/17/2020  10:58 AM           85887 1.txt
Minimum         : 11/23/2020   3:26 PM        12061168 2.txt
Property        :

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

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

Enter the command directory for the hidden file that shown in question 3 before.
Enter Get-Content text with measure object to get on how many words in the first file.

Question 5

```
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[551]
Red
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[551,6991]
Red
Ryder
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[6991]
Ryder
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Select-Object -Index
Select-Object : Missing an argument for parameter 'Index'. Specify a parameter of type 'System.Int32[]' and
try again.
At line:1 char:35
+ Get-Content 1.txt | Select-Object -Index
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Select-Object], ParameterBindingException
+ FullyQualifiedErrorId : MissingArgument,Microsoft.PowerShell.Commands.SelectObjectCommand

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

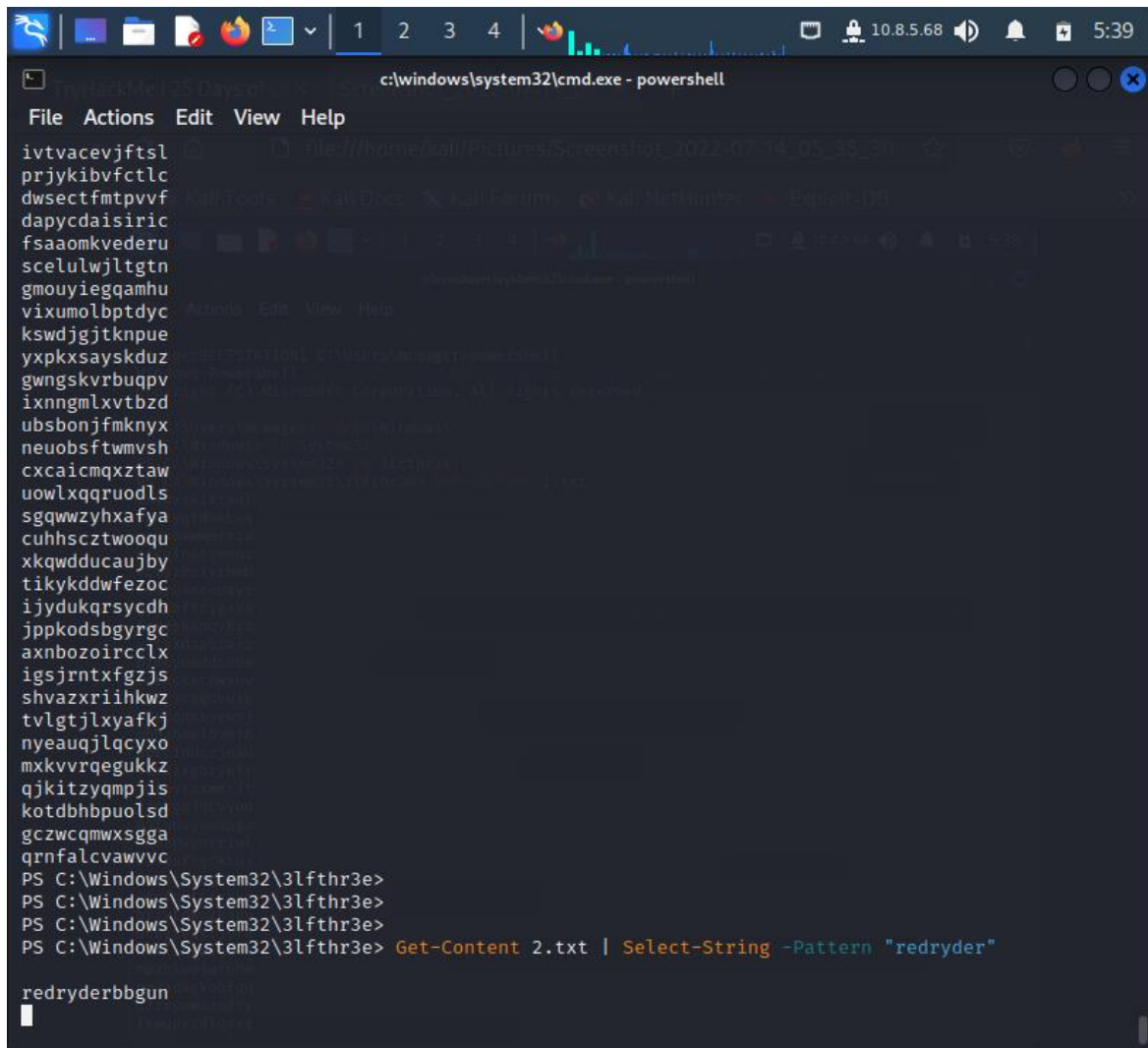
Enter the 2 words at index 551 and 6991 in the first file which going to reveal the 2 words from the index

Question 6

```
PS C:\Windows\System32> cd 3lfthr3e
PS C:\Windows\System32\3lfthr3e> Get-Content 2.txt
```

l hvvxskzktmdl
y wuxyqfdhkkvq
v cdsamwwmrszs
c jcglnatjmeqz
v ctyzhsiyrhmb
e dsruxmeenayr
g ykwbfttrigxbs
f gdzskxpqvks
y atvxdapbralz
p zmcyomddoddw
o dthcexcpwxuv
x jfgscpgdvuic
v trtoqxsviewsj
o hhahswldvmtb
p prciduczjeku
f zmkixgbryeff
l dlwvrxxwmtjt
f jmegbjqcvyoo
h jludoyumupgz
h hurgwghrriwl
z bvdafxgckkoj
i ndacgmqgenvg
u fqfxttfgkxt
b rivotdwozkjgv
d ceyteqmtjefa
o ooklingwiounn
m pzhlwojwfuhm

Reset command directory with the hidden folder and list Get-Content 2nd text



```
c:\windows\system32\cmd.exe - powershell
File Actions Edit View Help
ivtvacevjftsl
prjykibvfctlc
dwsectfmpvfv
dapycdaisiric
fsaaomkvederu
scelulwjltgtn
gmouyieggamhu
vixumolbptdyc
kswdjgjtgnpue
yxpkxsayskdus
gwngskvrbuqpv
ixnngmlxvtbzd
ubsbonjfmknyx
neuobsftwmvsh
cxcaicmqxtaw
uowlxqqrudls
sgqwwzyhxafya
cuhhscztwoogu
xkqwdducaujby
tikiykdwwfezoc
ijydukqrsycdh
jppkodsbgrygc
axnbozoircclx
igsjrntxfgzjs
shvazxriihkwz
tvltjlxayafkj
nyeauqjlqcyxo
mxkvvrqegukkz
qjkitzyqmpjis
kotdbbpuolsd
gczwcqmwxsnga
qrnfalcvawvvc
PS C:\Windows\System32\3lfthr3e>
PS C:\Windows\System32\3lfthr3e>
PS C:\Windows\System32\3lfthr3e>
PS C:\Windows\System32\3lfthr3e> Get-Content 2.txt | Select-String -Pattern "redryder"
redryderbbgun
```

Therefore, search in the list by use select-string pattern “redryder”

Methodology

First of all, use powershell to reveal most of the file within the documents include the hidden files. According to this task, the subject file which is Elf is what we needed to find the content that is hidden. By using the command directory list, we can identify the location and certain contents that inside the file. Therefore, different type of hidden folder name which accessible through different type of command directory. The last 2 words are from index 551 and 6991 are shown in the first and the second file which wis wanted from the last Elf. At the end, we be able to complete all the file directory and any content that being hidden inside the hidden file by using powershell under the command prompt and windows system 32.

