PSP0201

Week 5

Writeup

Group Name: GGez

Group members:

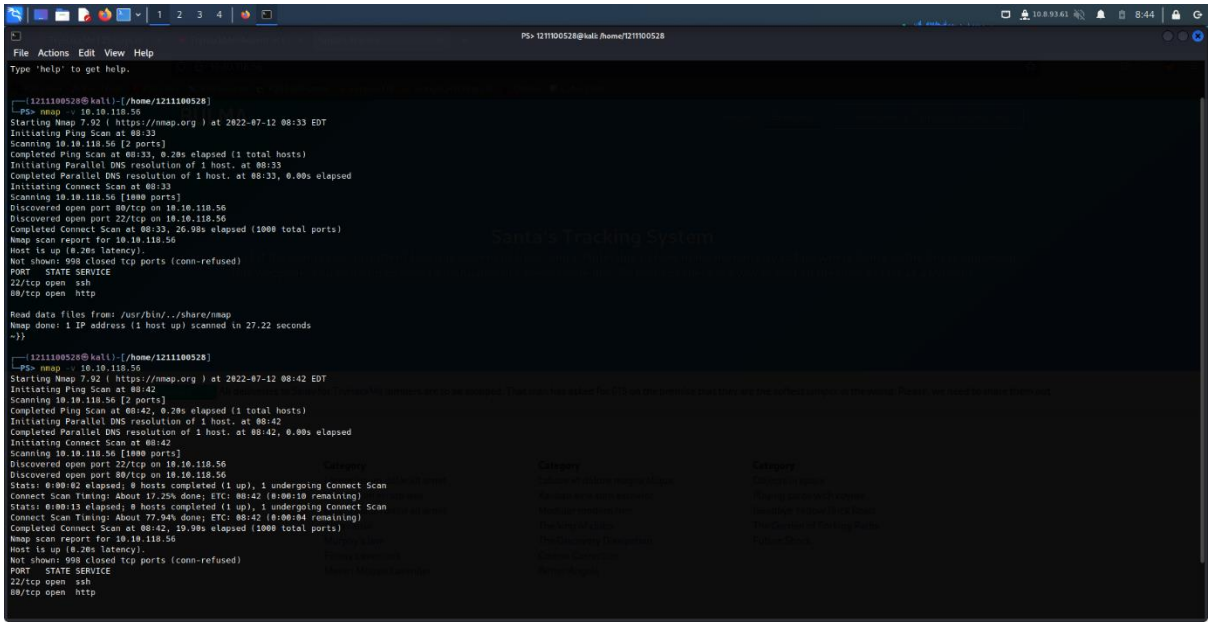
ID Number	Name	Role
1211101951	Muhammad Zaieff Danial Bin Mohd Suhaimi	Leader
1211100528	Muhammad Arief Fahmi Bin Syahril Anuar	Member
1211101120	Adam Uzair Bin Mohd Sori	Member
1211101643	Sivaharriharann A/L Ramanathan	Member

Day 16 : Scripting – Help! Where is Santa?

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

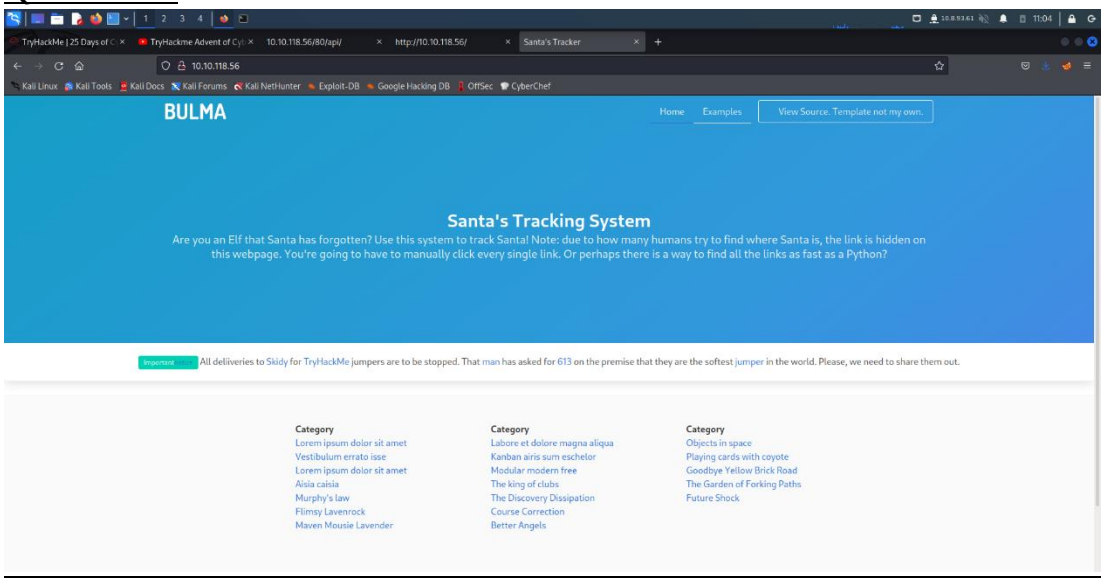
Solution/Walkthrough:

Question 1:



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:

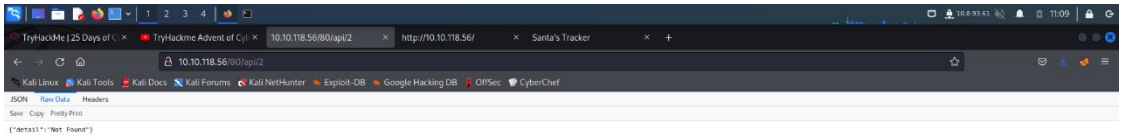


We can get the template name by visiting the url page .

Question 3:

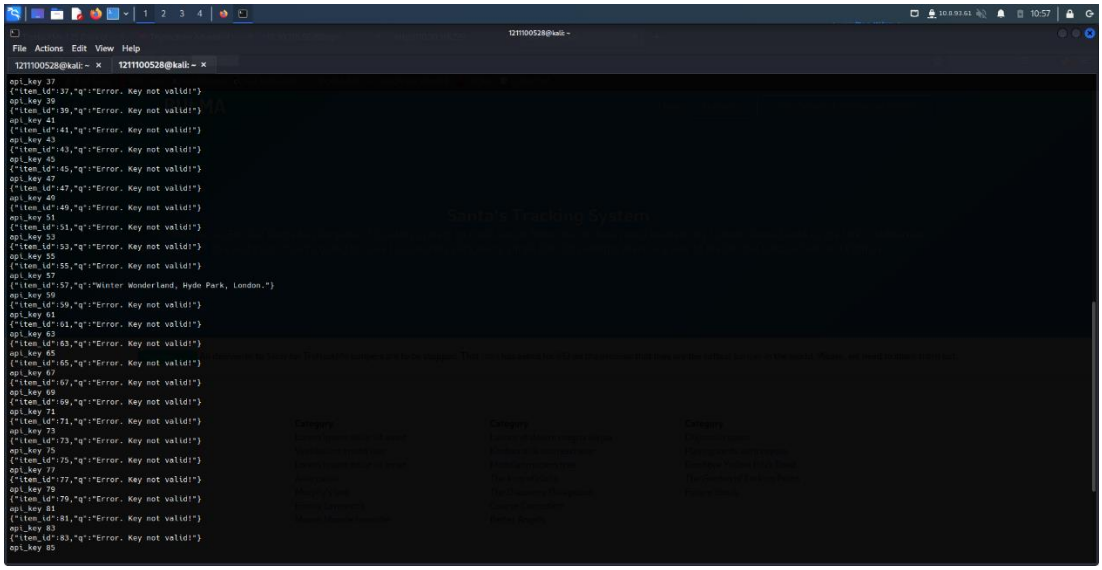
We can get the answer to this question by simply adding “/api/” to the url and port number for the web server.

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 infront of the address .

Thought Process / Methodology :

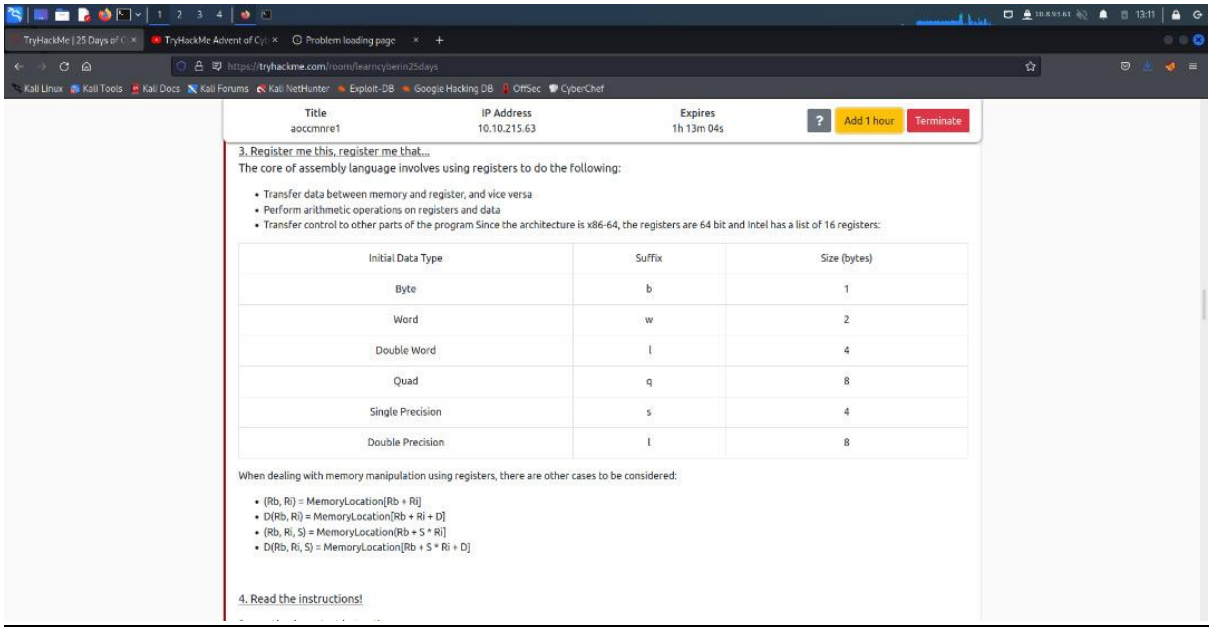
First of all we have to open the website by starting the machine to get to the IP address . Then , we need to get the port number by opening the terminal and use the nmap method . Then we can open the website by using IP address plus the port number to open the website . Next we can add “ /api/ ” at the url to open the api sercret 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 .

<u>Day 17 : Reverse Engineering – ReverseELFneering</u>

Tools used: Kali Linux , Firefox , Terminal

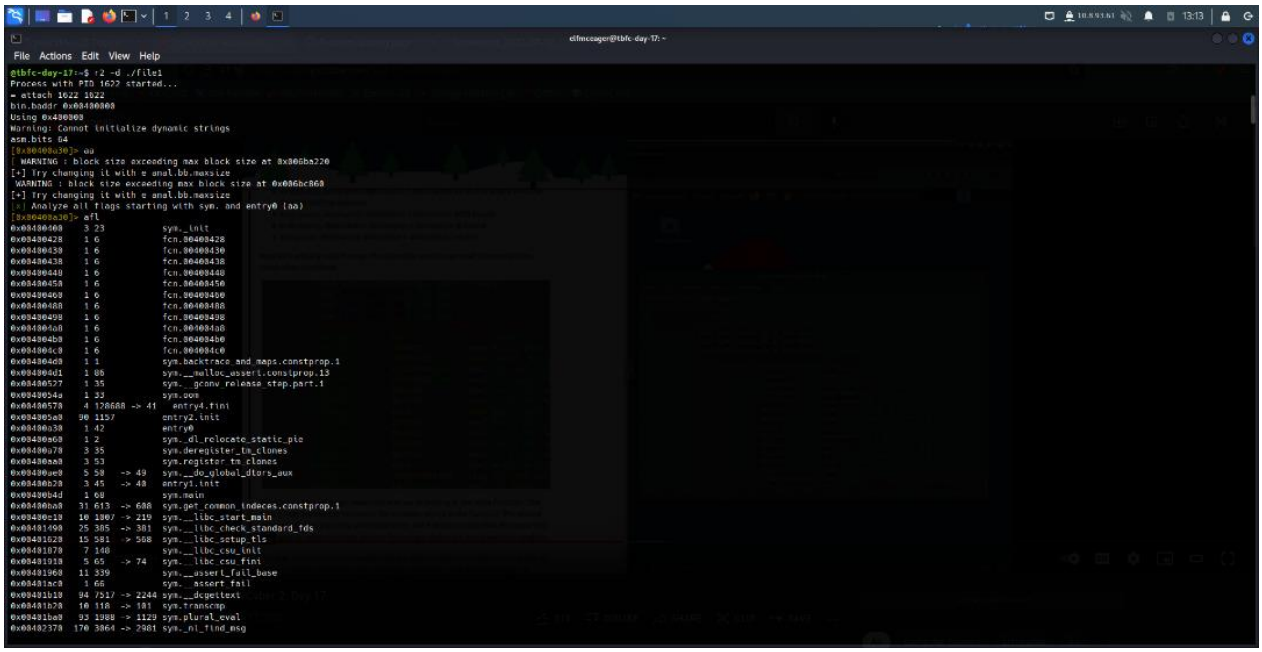
Solution/Walkthrough:

<u>Question 1:</u>



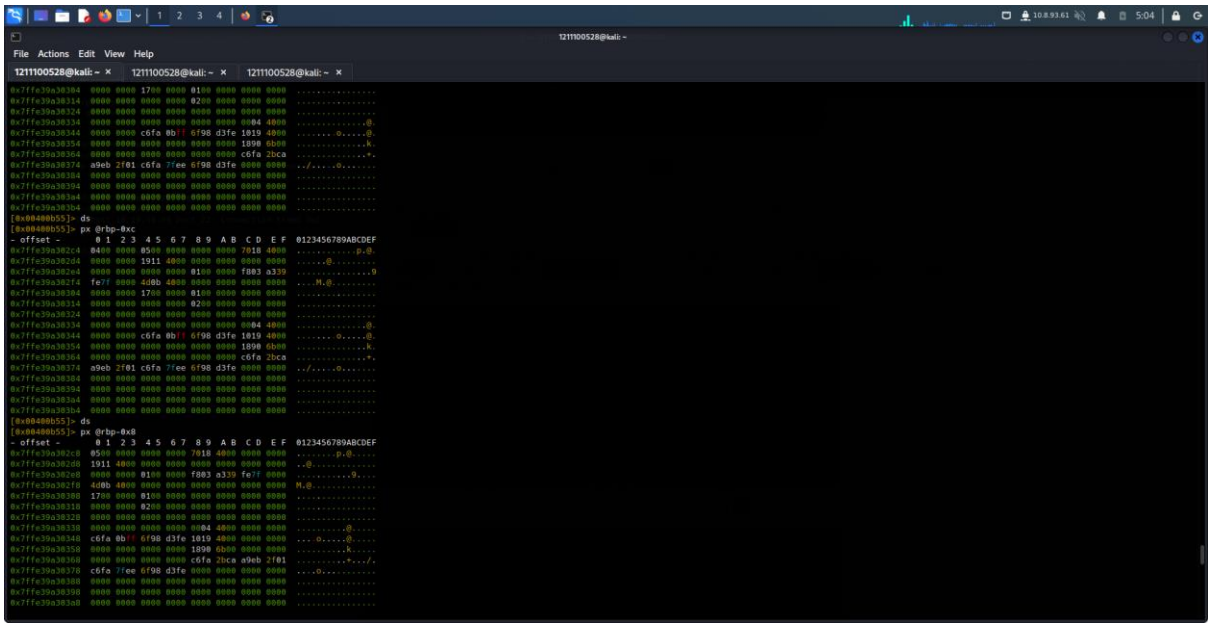
For question 1 we can find the answer in the tryhackme question itself .

Question 2:



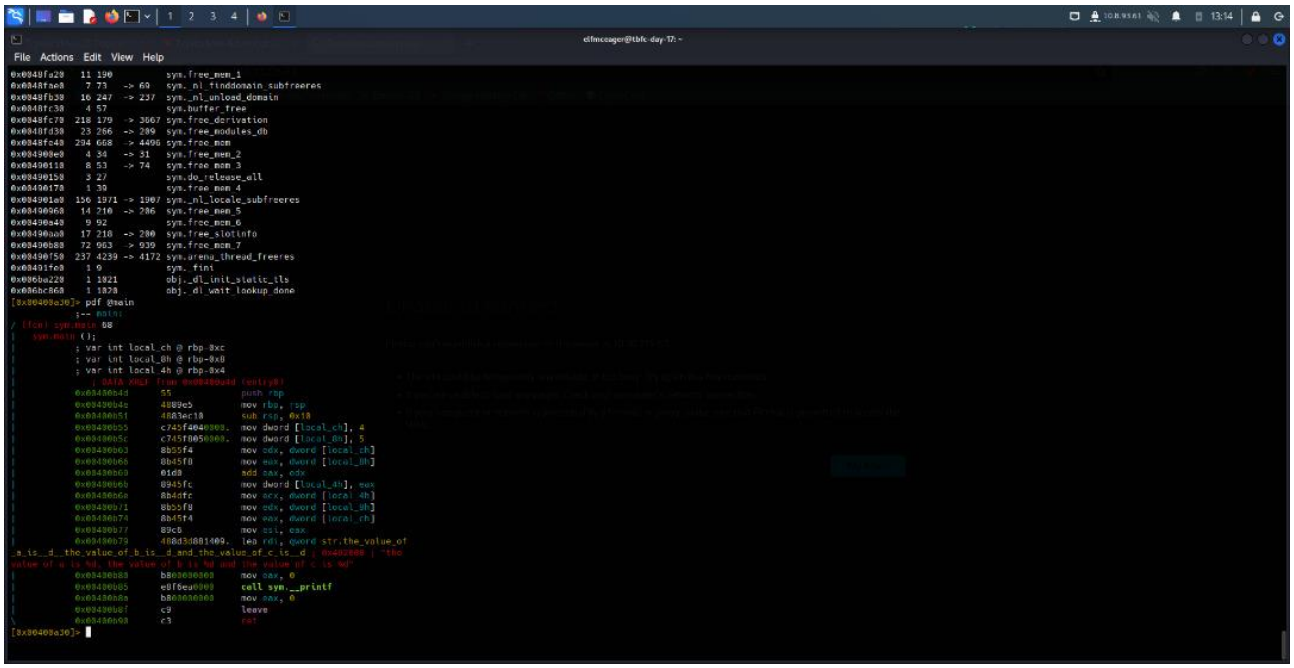
The command that we need to input to analyse the program in radare2 is the command **“aa” .**

Question 3:



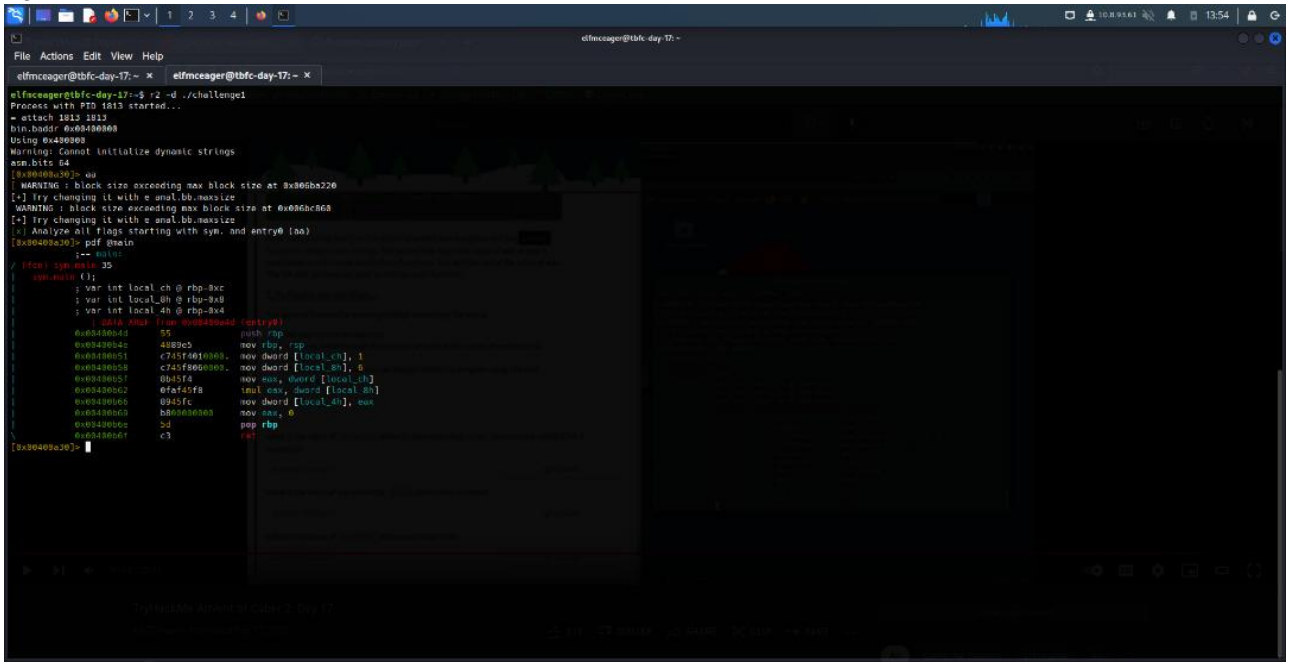
The command to set a breakpoint in radare2 would be the command **“db” .**

Question 4:



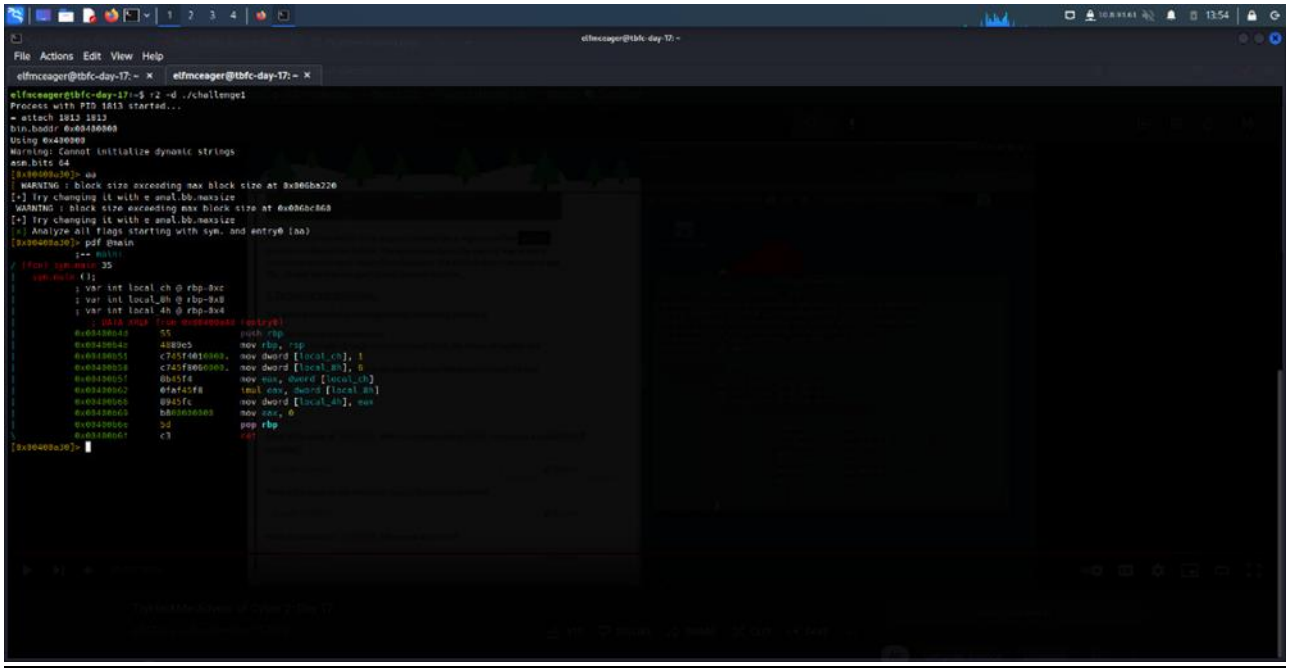
The command that we need to execute the program until we hit a breakpoint would be the command **“pdf @main” .**

Question 5:



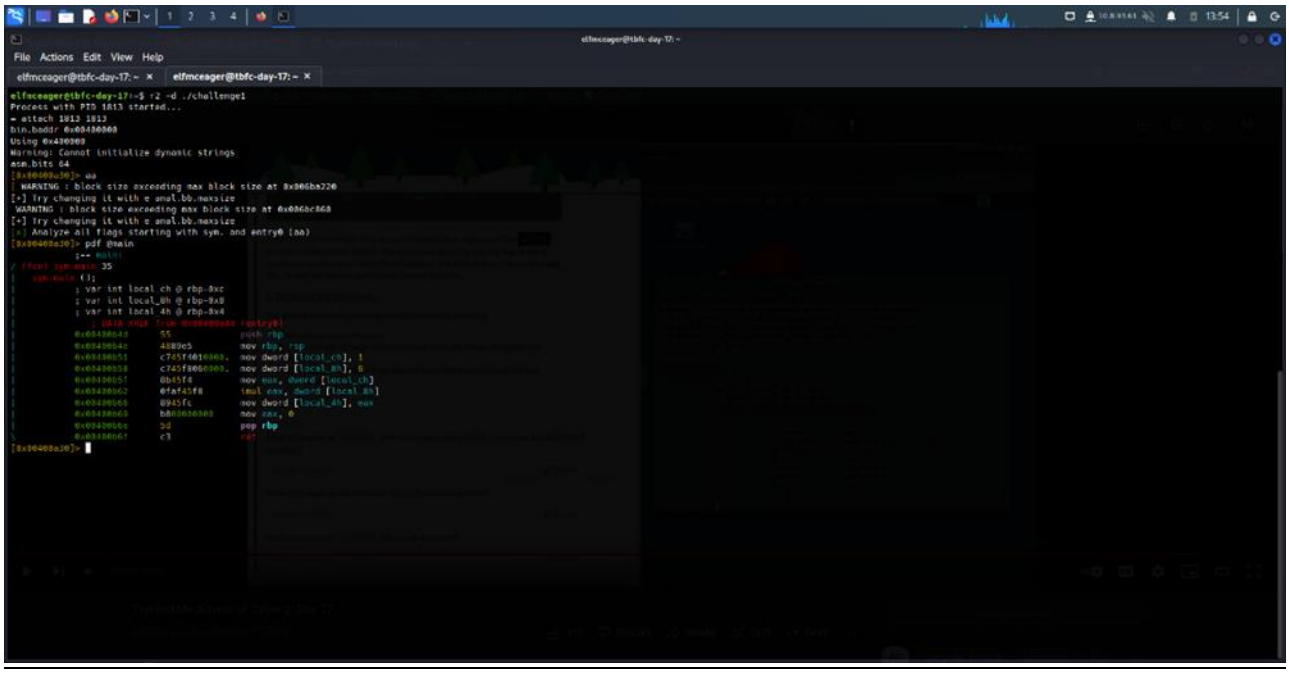
The value of local_ch when its corresponding movl instruction is called **“1”** as in the numeral digit .

Question 6:



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

Question 7:



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.

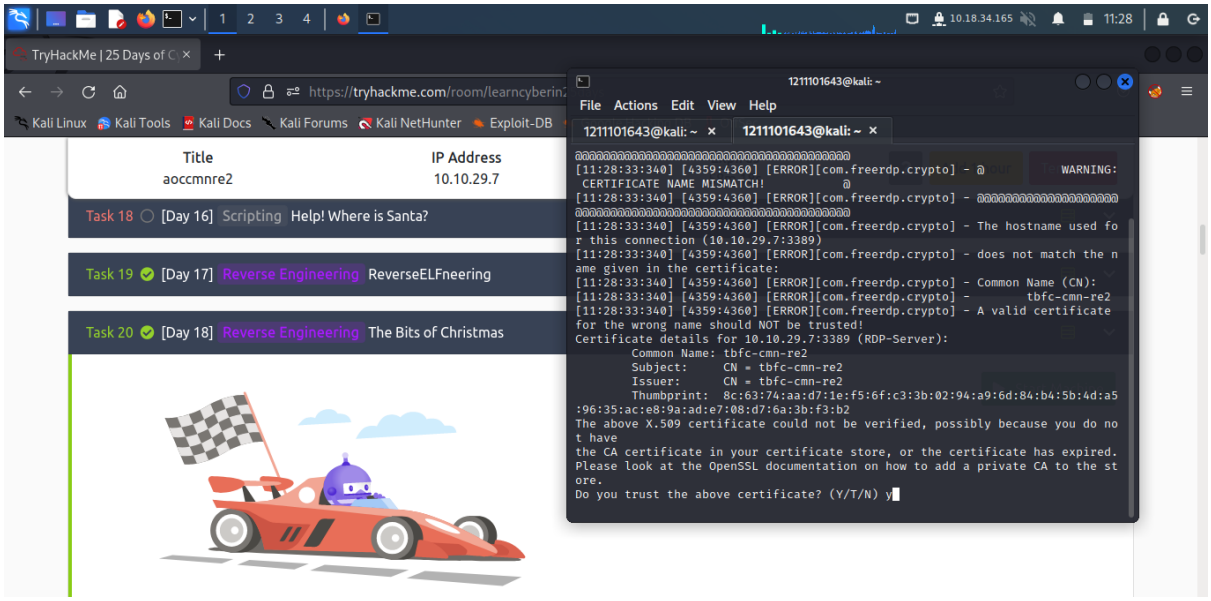
Day 18: Reverse Engineering - The Bits of Christmas

Tools used: Kali Linux, Firefox, Terminal

Solution/Walkthrough:

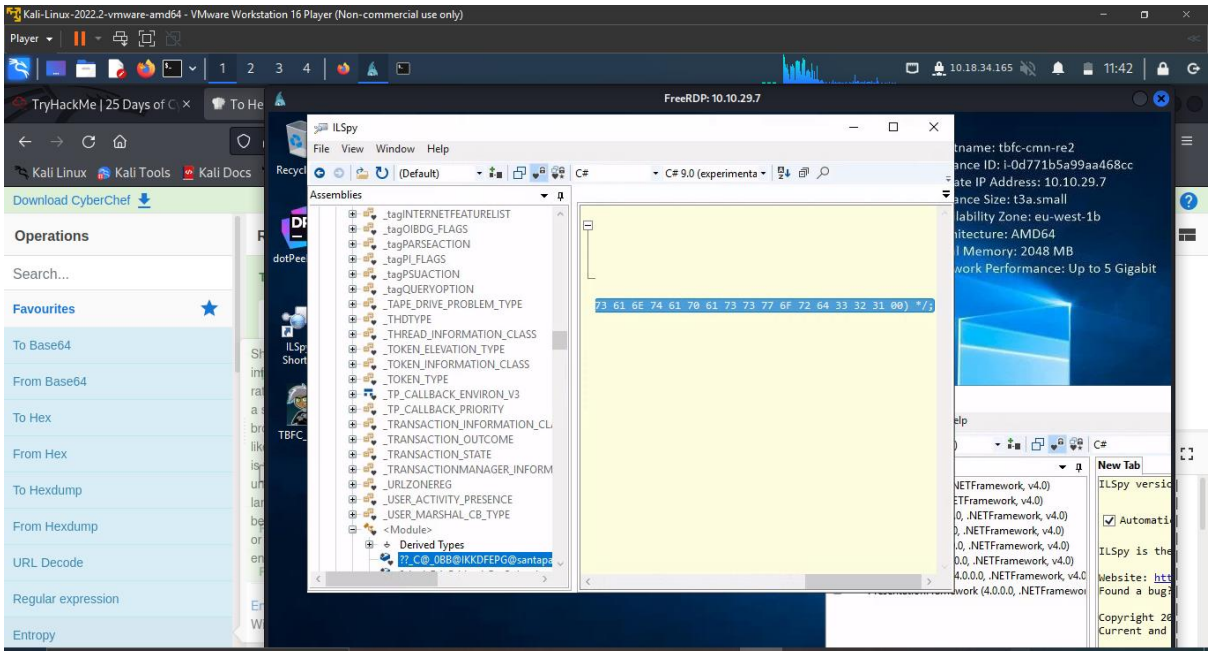
Question 1:

First of all, we install remmina open remmina using terminal



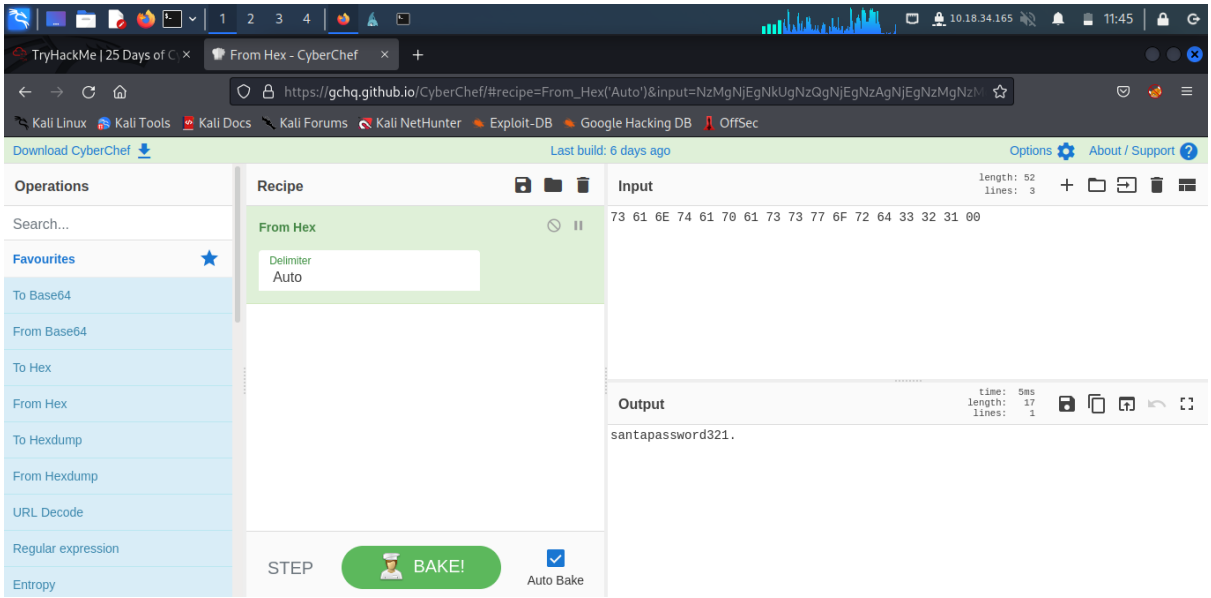
Question 2:

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



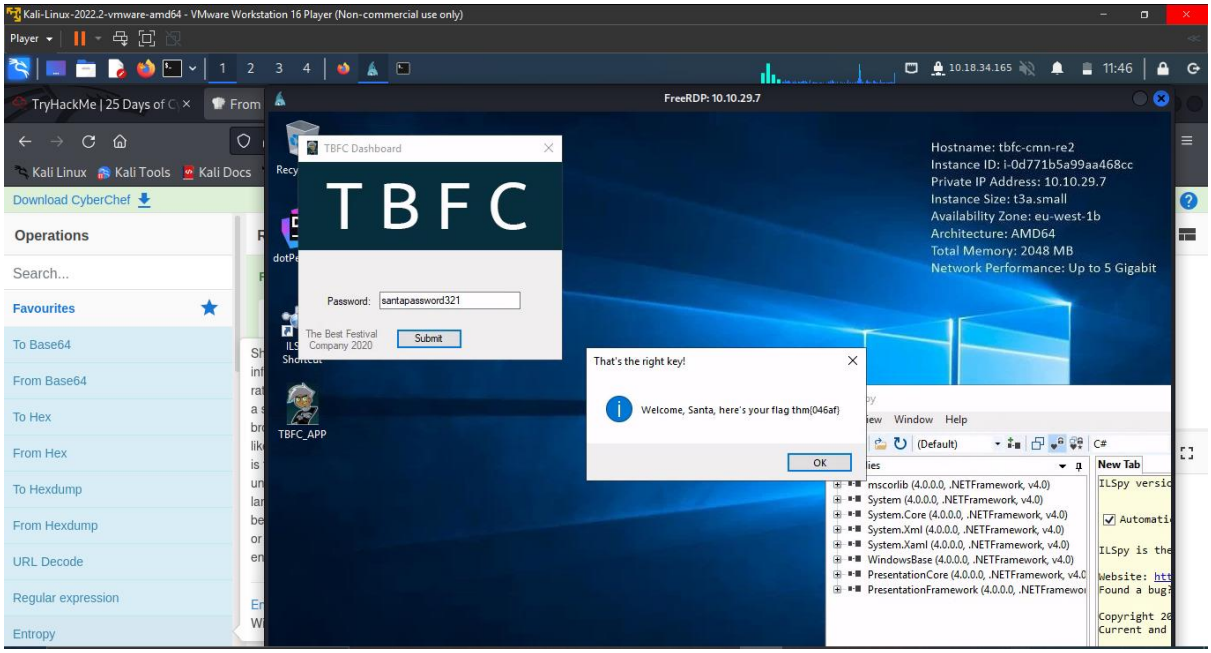
Question 3:

We get the password from the cyberchef.



Question 5:

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



Methodology:

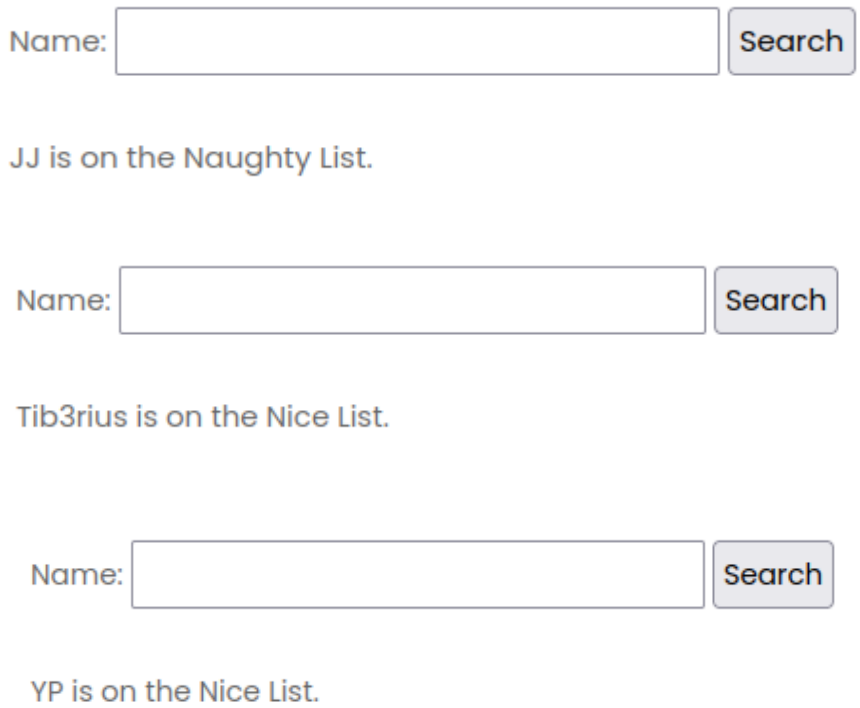
Open terminal and open remmina to get the password of TBFC. Then, get into the RDP and get the password. The file that displayed to us after we click the password is formatted in hexadecimal. We can use an online tool such as Cyberchef to decode that and the results gives by Cyberchef is the same password 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: Search

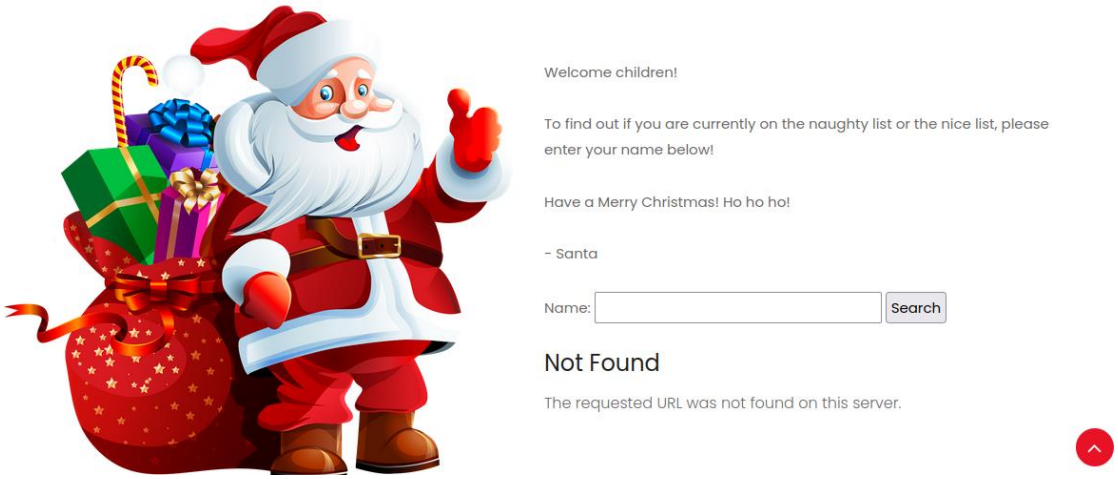
Kanes is on the Naughty List.

Name: Search

Timothy is on the Naughty List.

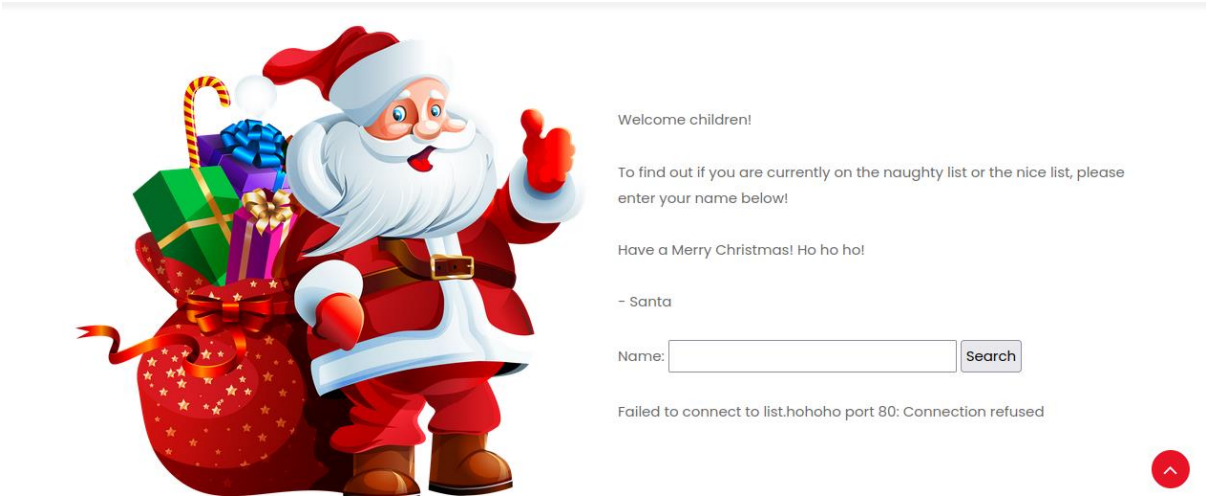
Question 2:

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



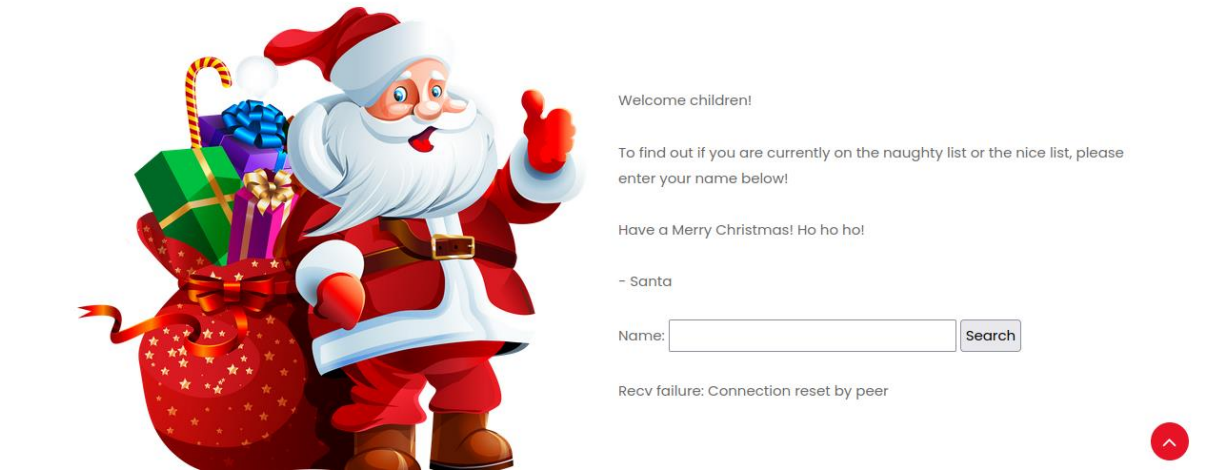
Question 3:

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



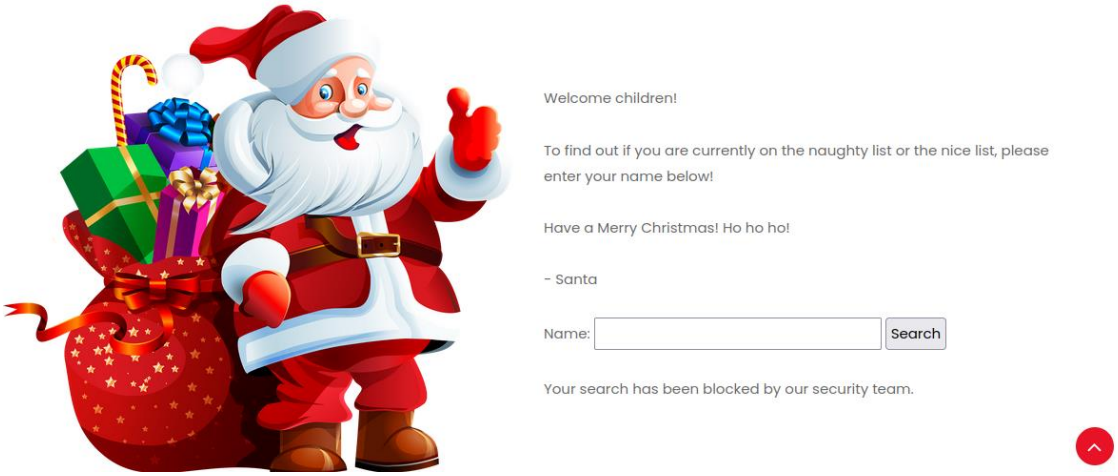
Question 4:

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



Question 5:

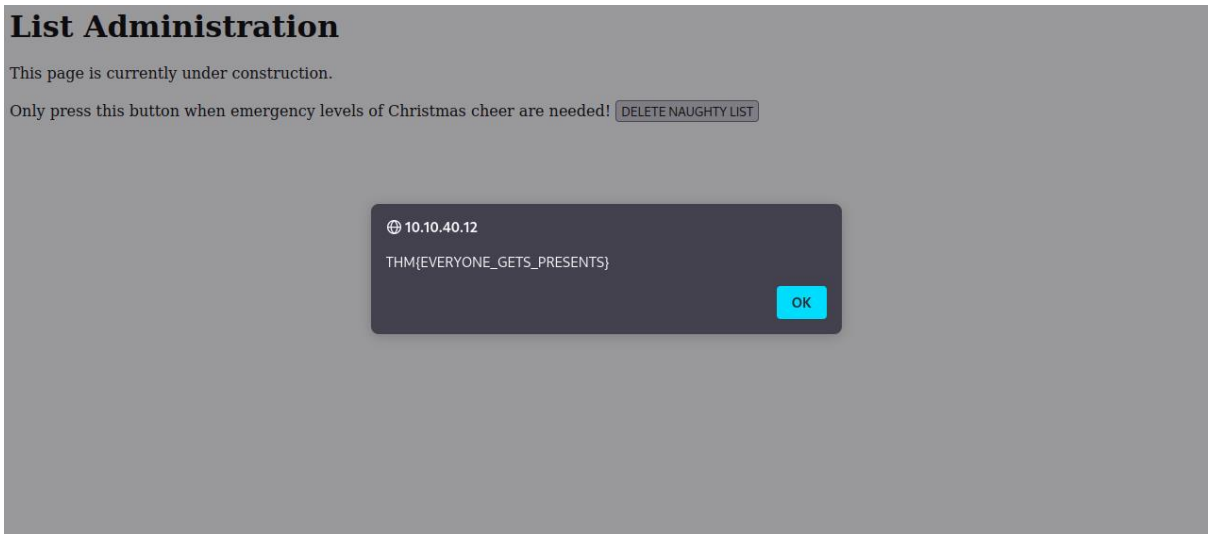
Type in “/?proxy=http%3A%2F%2Flocalhost” to the url.



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.



Thought Process / Methodology:

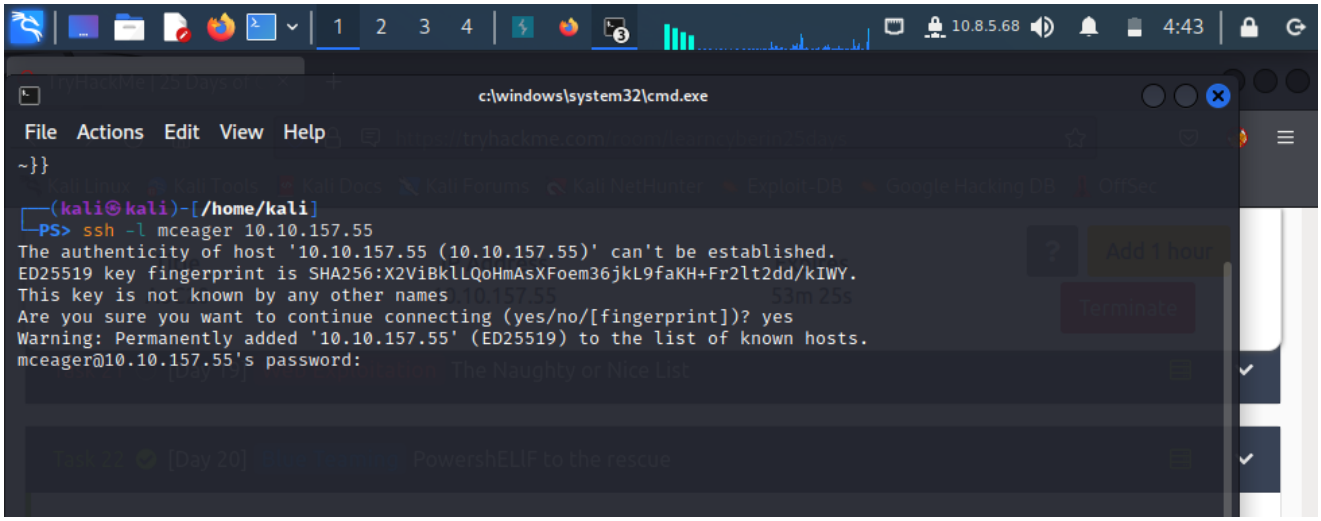
For day 19th we need to use Server-Side Request Forgery (SSRF) to complete this challenge. Basically by changing the url we can get different results based on what we thought such as hostnames, port number, etc. First, we need to get the ip address and put it in the url. Then, we can try to put names 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: PowershELIF 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 e1fone.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 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 e1fone.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?

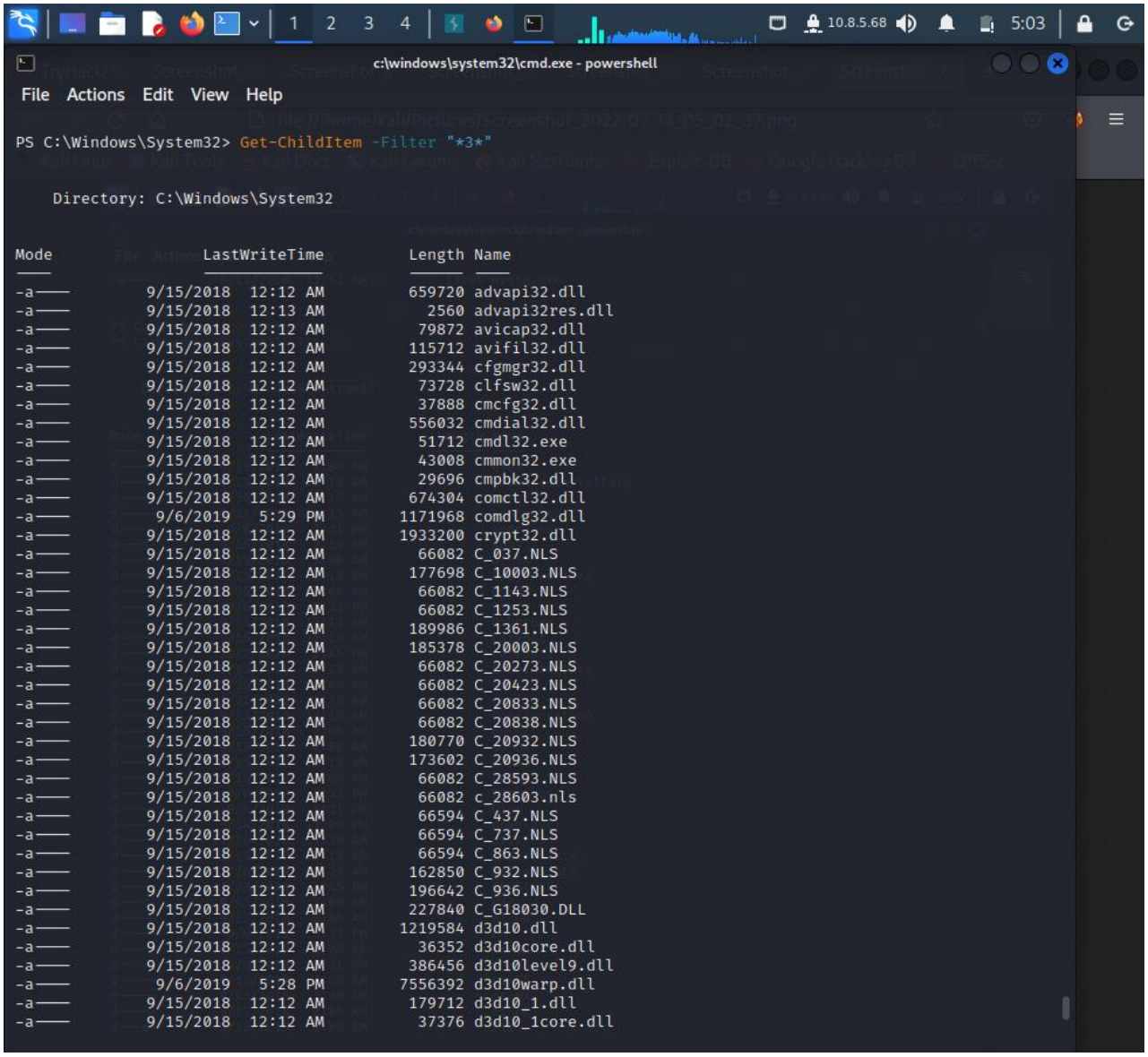
Question 3

```
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                DiagSvcs
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
```



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 vm3ddevapi64.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  :
Minimum  :
Property :


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

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


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

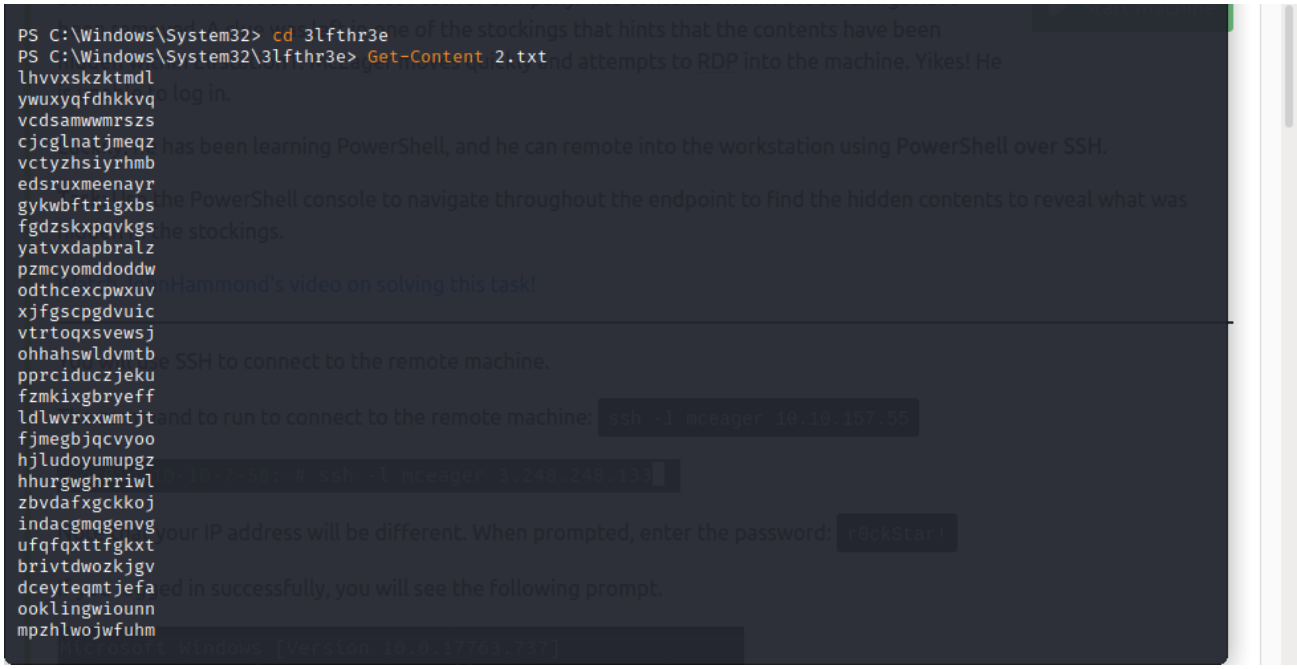
Enter the command directory for the hidden file that shown in question 3 before. Enter Get-Content text with measure object to get on how many words in the first file.

Question 5

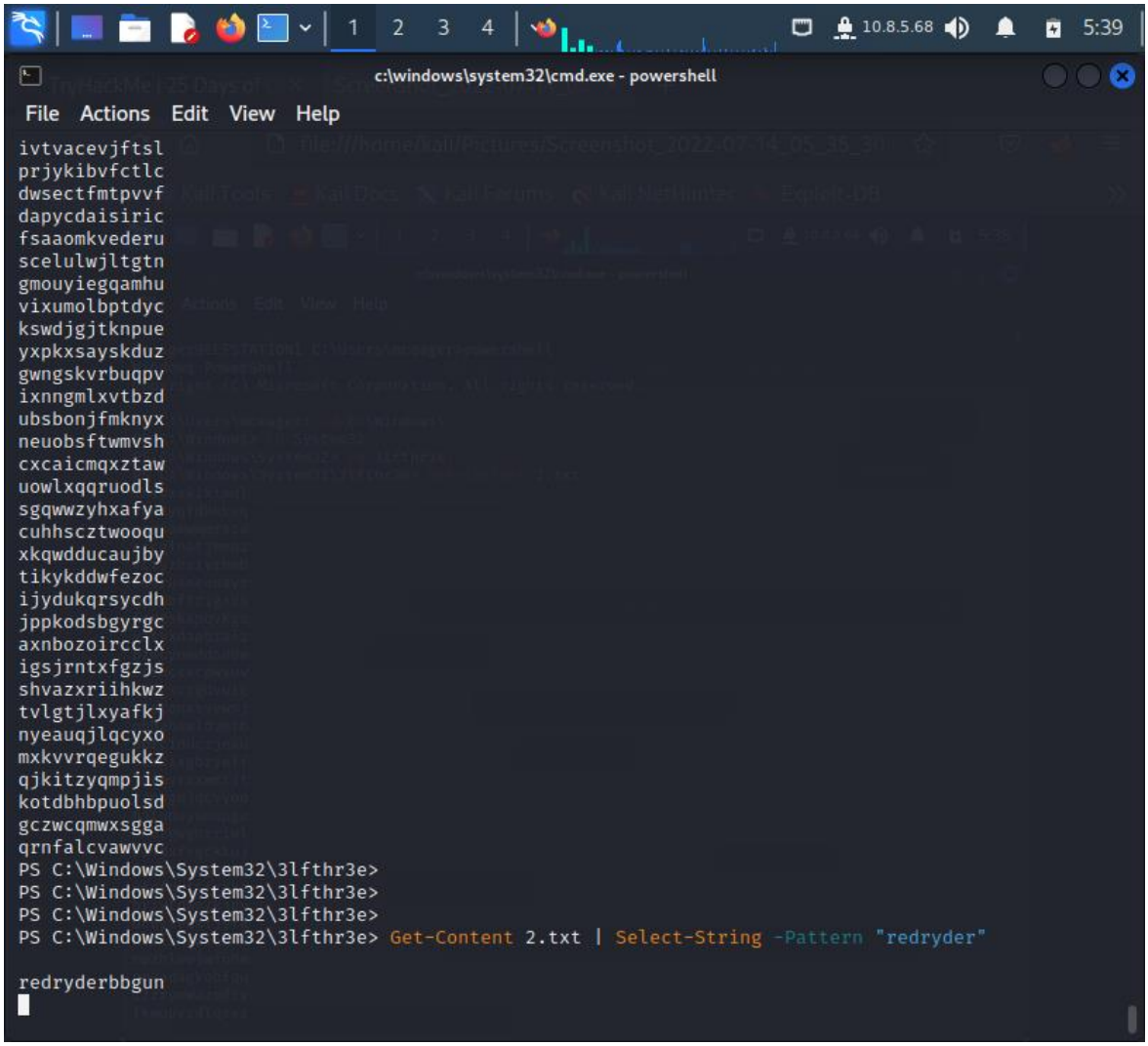
```
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[551]
Red
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[551,6991]
Red
Ryder
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[6991]
Ryder
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Select-Object -Index
Select-Object : Missing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



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



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.