PSP0201 Week 5 Writeup

Group Name:Suibian

Members:

ID	Name
1211101851	ANG ZHE JIE
1211103790	KOK YEW YAN
1211103039	OOI YI SIANG
1211104005	WONG CHUN RONG

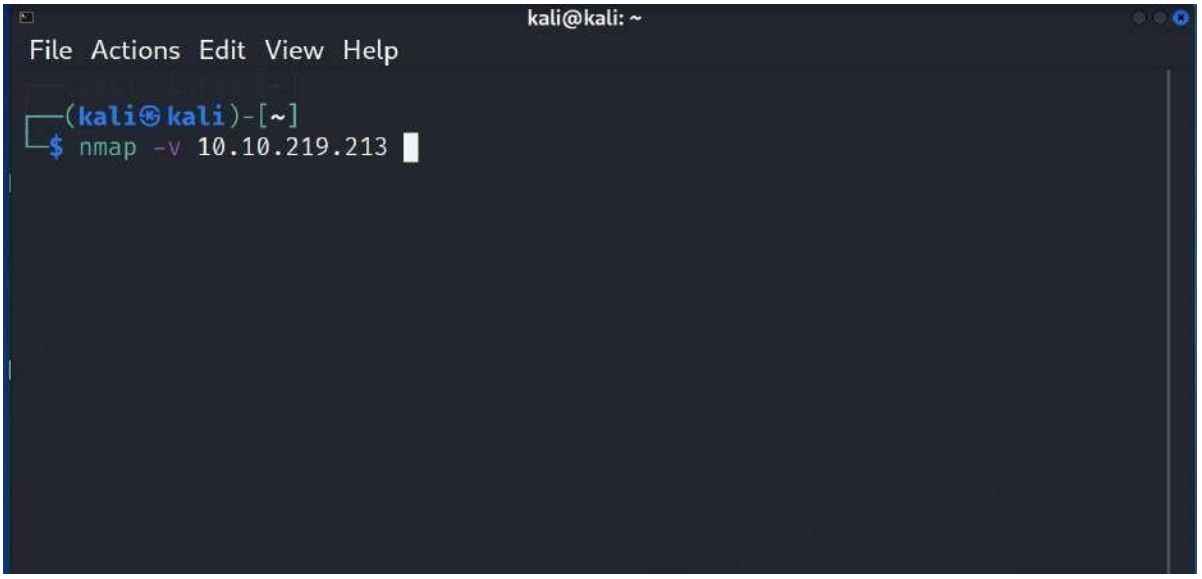
Day 16: Scripting - Help! Where is Santa?

Tools used: Firefox, Python

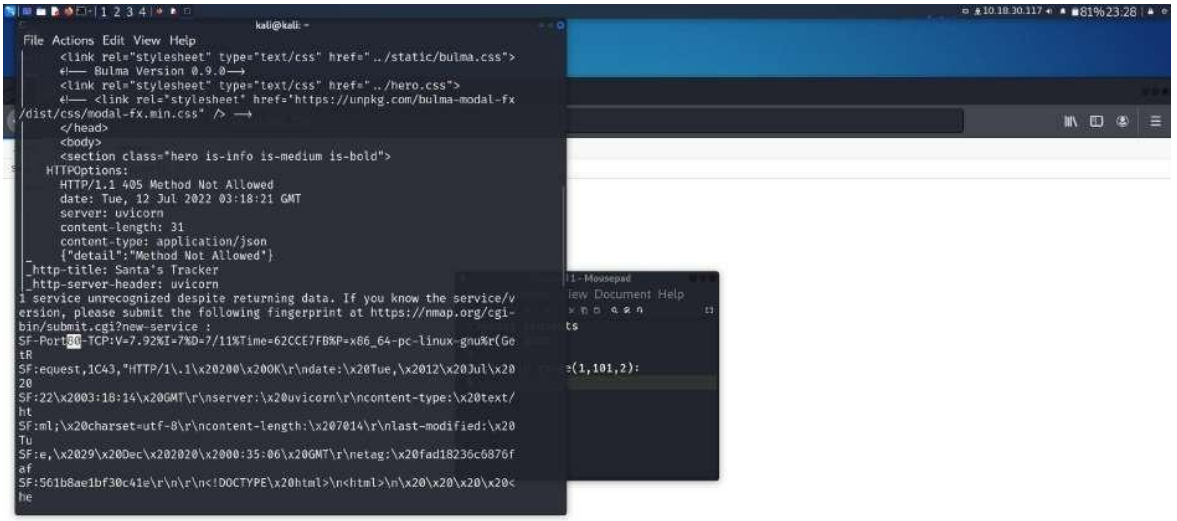
Solution/walkthrough:

Question 1:

After starting the machine, type nmap -v and key in IP address

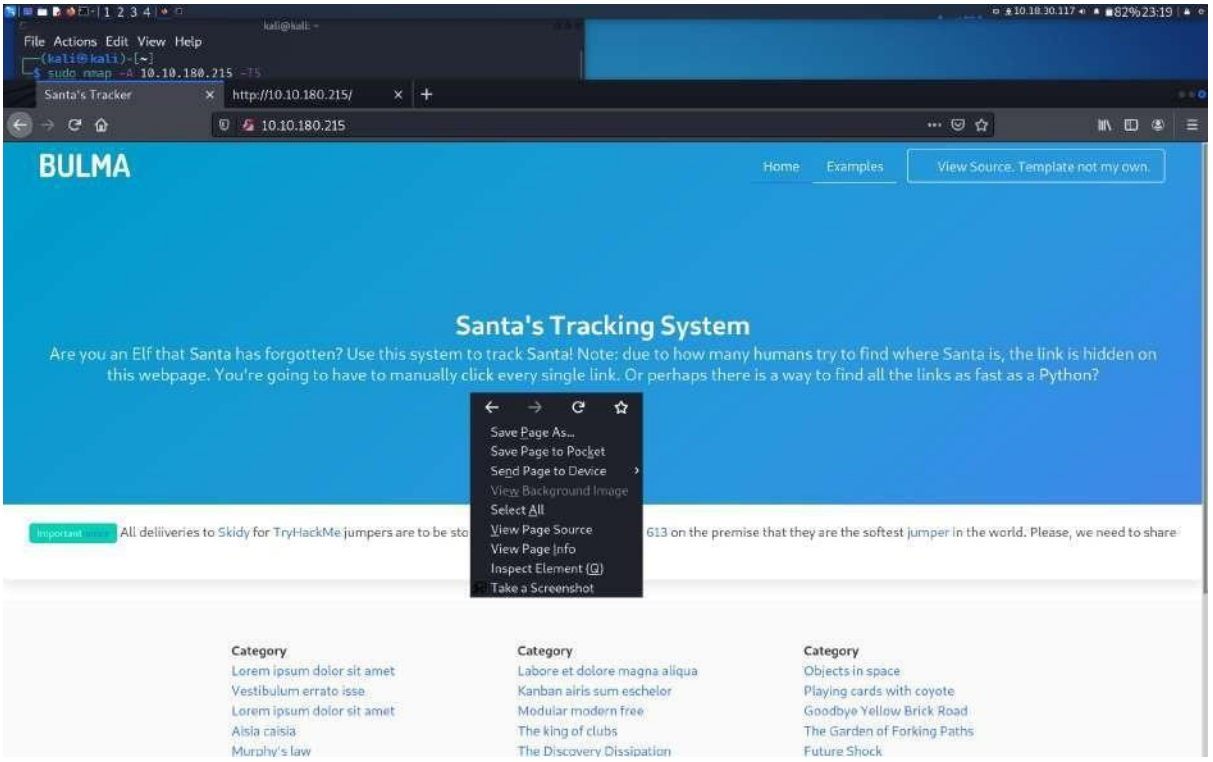


the port will be shown

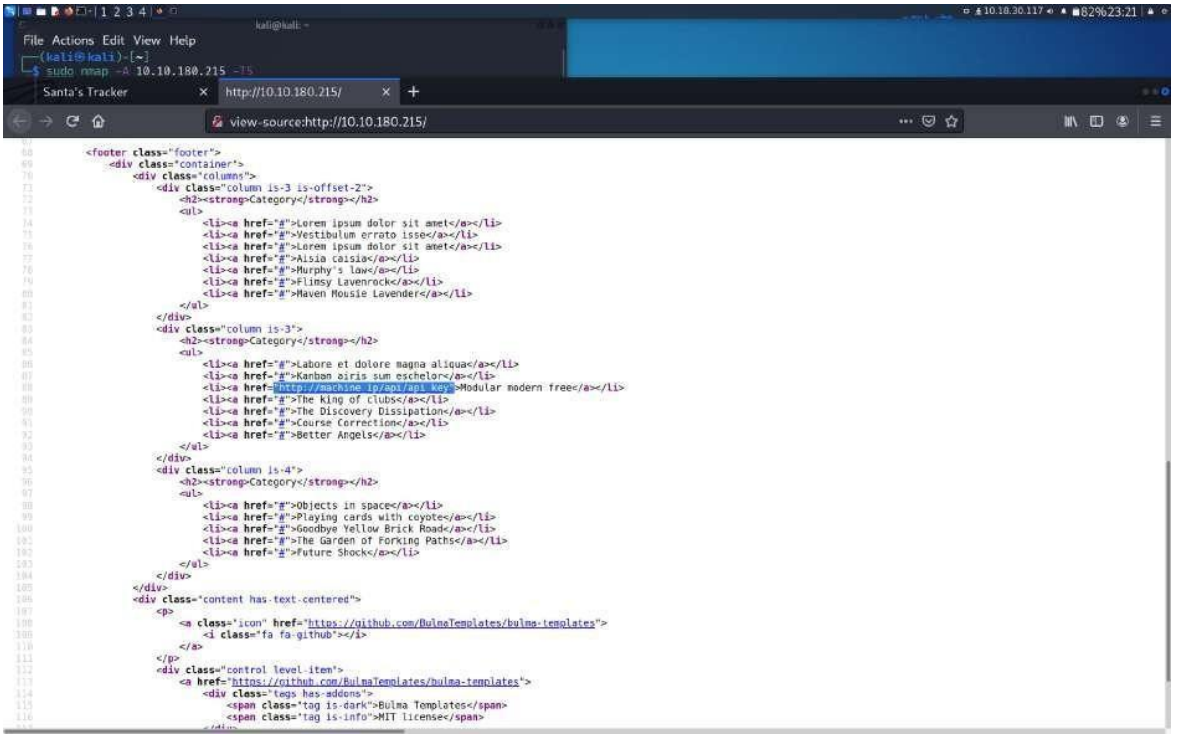


Question 2:

Open firefox, key in the IP address then right click to view the page resource

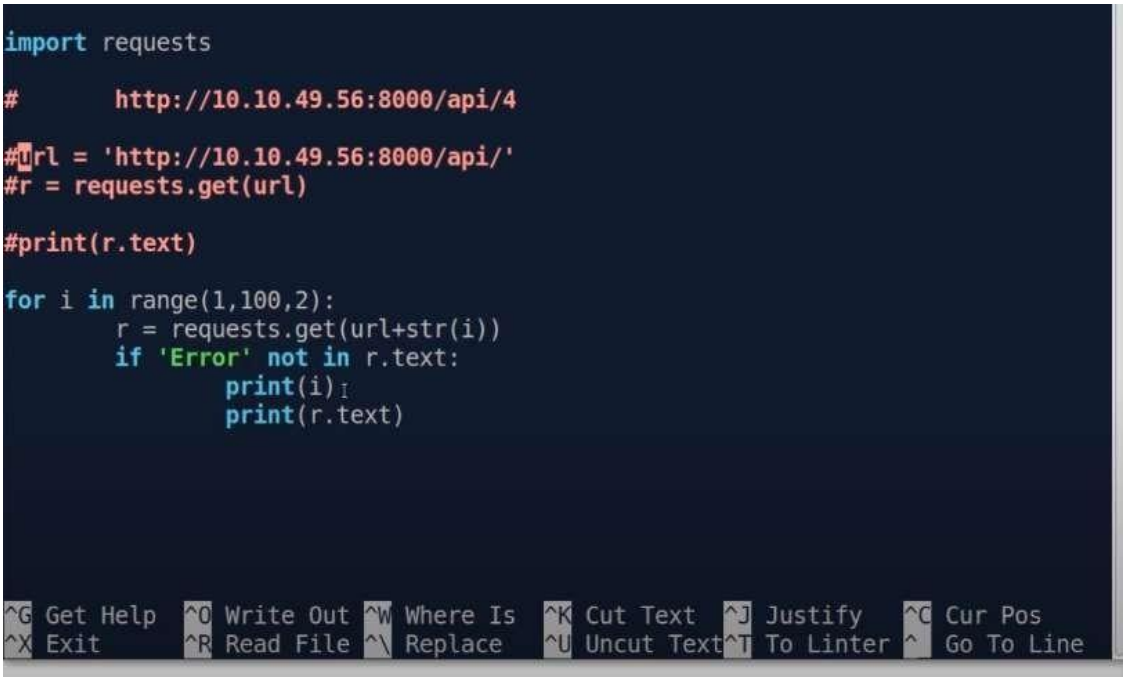


And API is shown

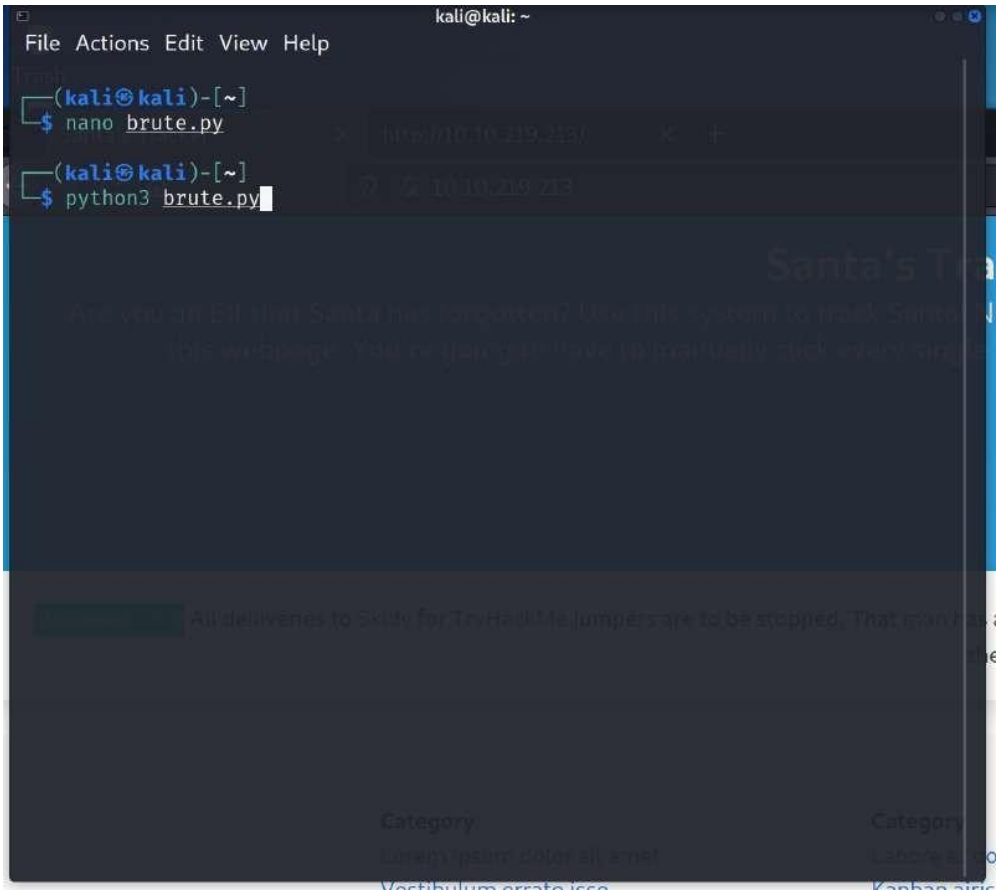


Question 3:

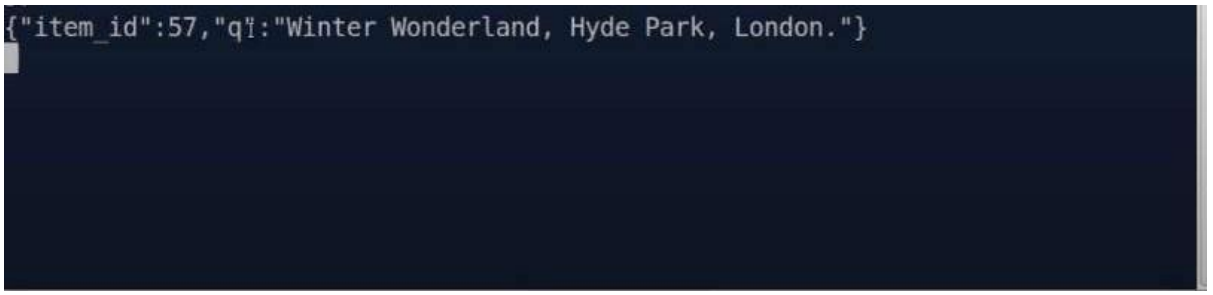
The next step, create a new python by using nano brute.py. After that, import requests



Then, use python3 and brute.py to show the result

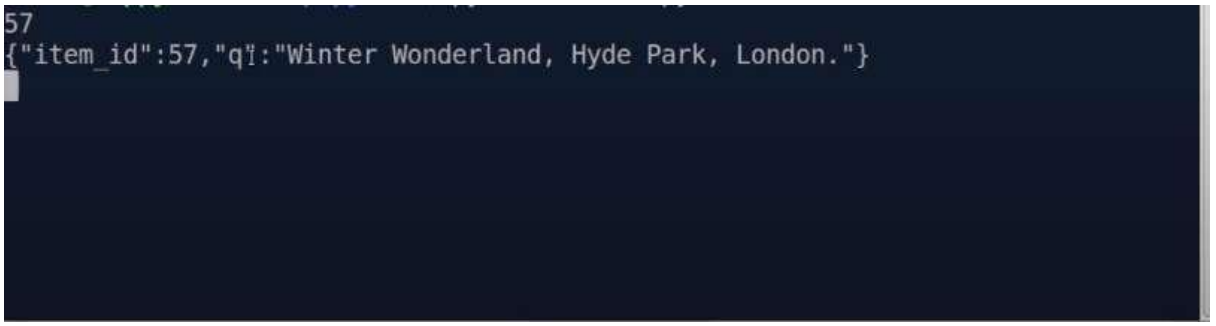


Next, Santa location is shown



Question 4:

Lastly, the right API key will be shown and it is an odd number.



Thought Process/Methodology:

First, after starting the machine, key in nmap -v and the IP address.Then, the port is shown.After that , open the firefox and key in the IP address then right click to view the page source. Use Ctrl+f and key in api to search it. The next step, create a new python by using nano brute.py.Next, import requests. And then, I have created a new python which is brute.py. After done command, use python3 and brute.py. Then save and modify it. Moreover, key in python3 and brute.py at the back of the python3.The result is shown.So, we know the location of Santa, which is winter wonderland, hyde park, London.

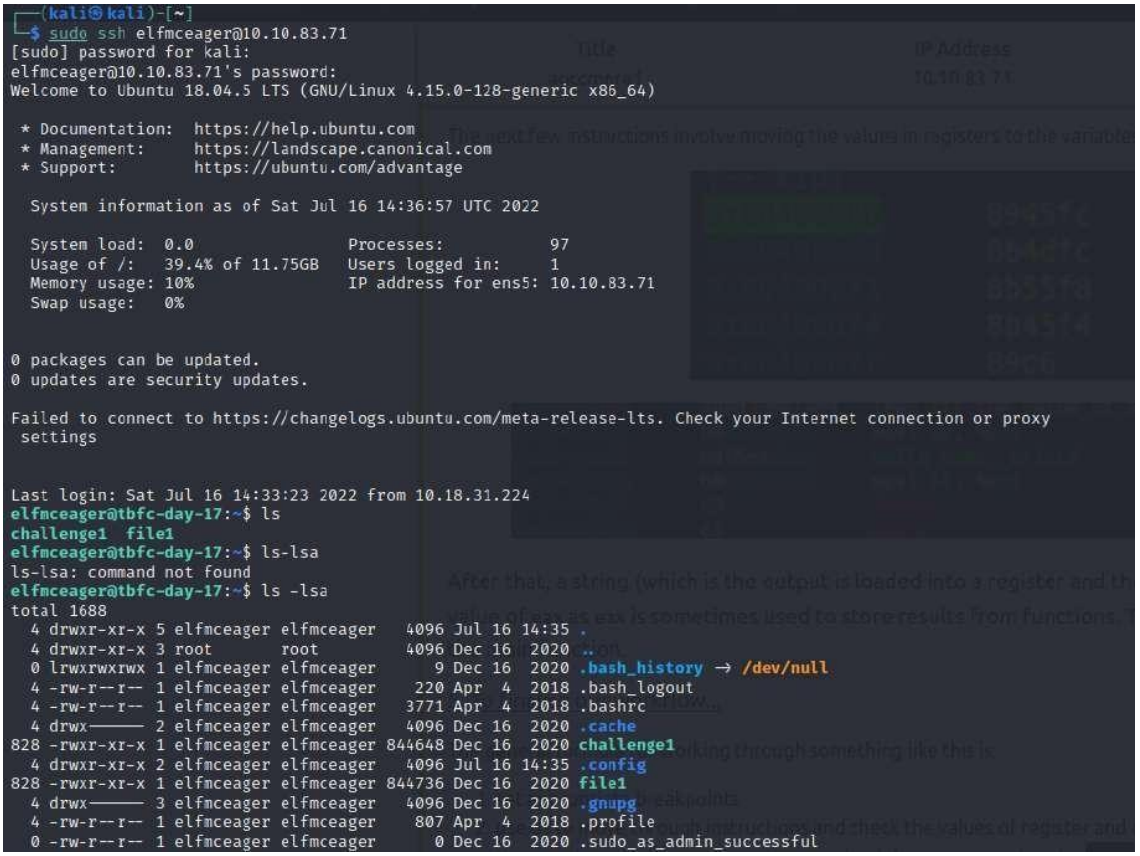
Day 17: Reverse Engineering - ReverseELFneering

Tools used: Command Prompt, elfmceager

Solution/walkthrough:

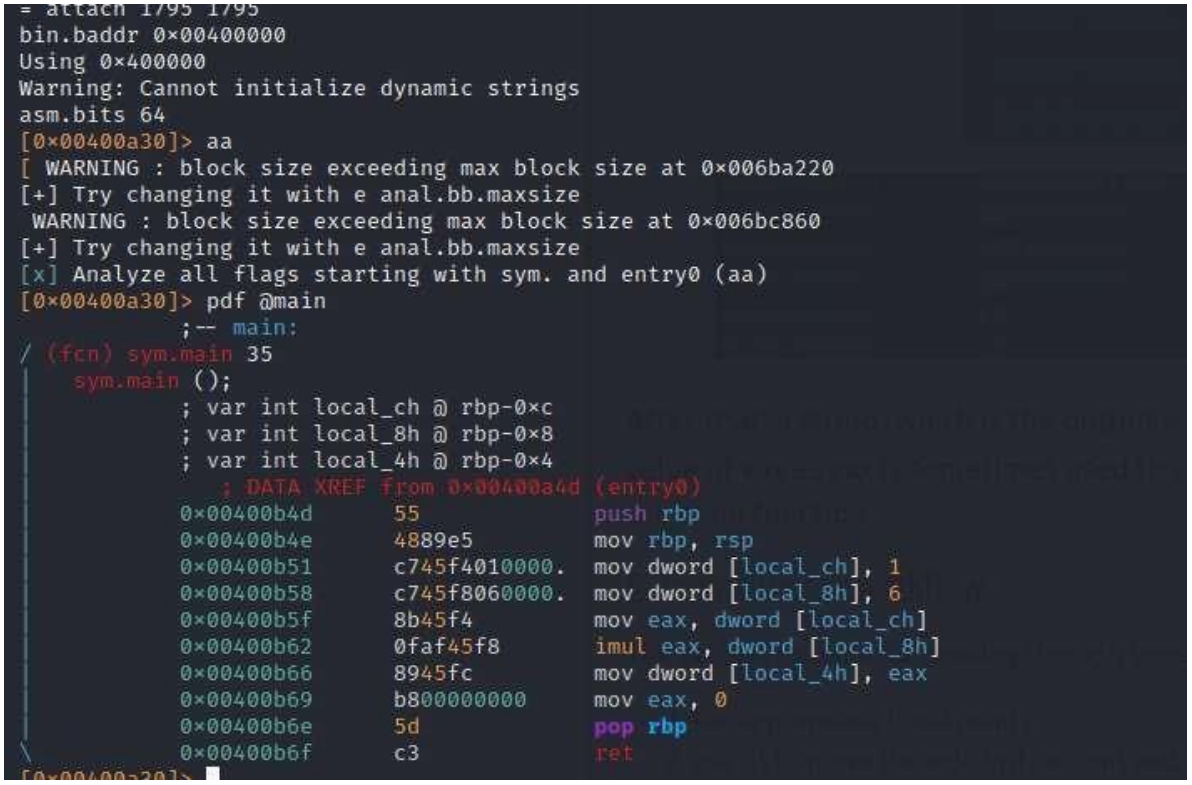
Question 1:

First, login by *elfmceager@IPaddress* and enter the password given by THM ---- *adventofcyber*.

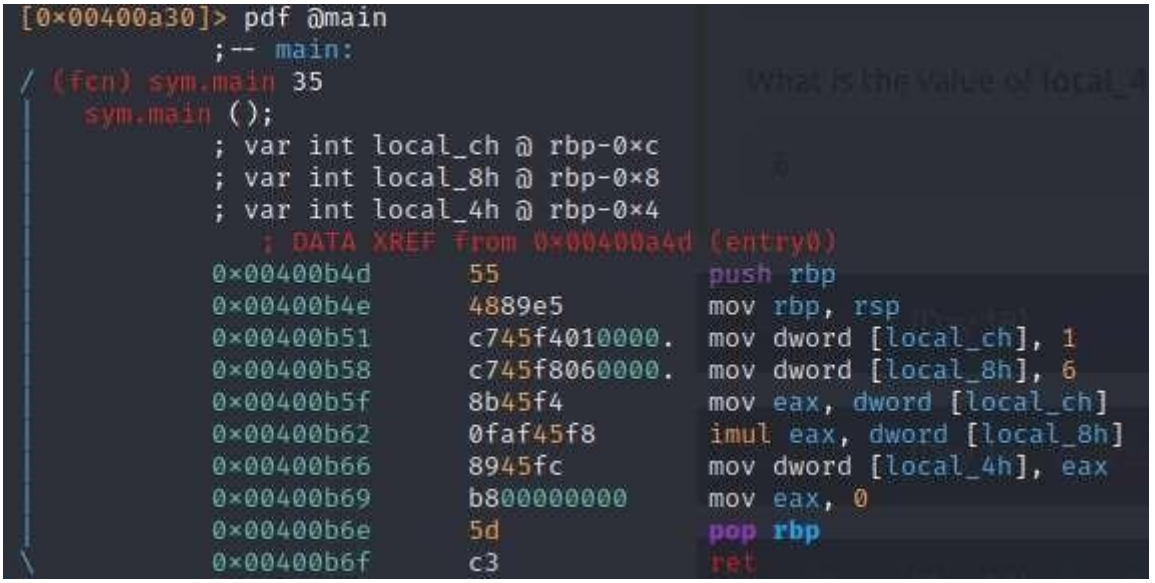


Question 2:

After analyzing the file, open the file which named"*challenge 1*" and enter the main file ,you will get the value of local_ch which is 1.



Discover the value of eax and local_4h which is both 6



Thought Process/Methodology:

The first step, login by using *elfmceager@IPaddress* and enter the password given by THM ---- *adventofcyber*. Then open the file "*challenge 1*" and enter the main page ,then we obtain the value of *local_ch* which is *1* and the value of eax is
Equal to *6* and the value of *local_4h* in front of eax is also 6.

Day 18: Reverse Engineering - The Bits of Christmas

Tools used: Remmina

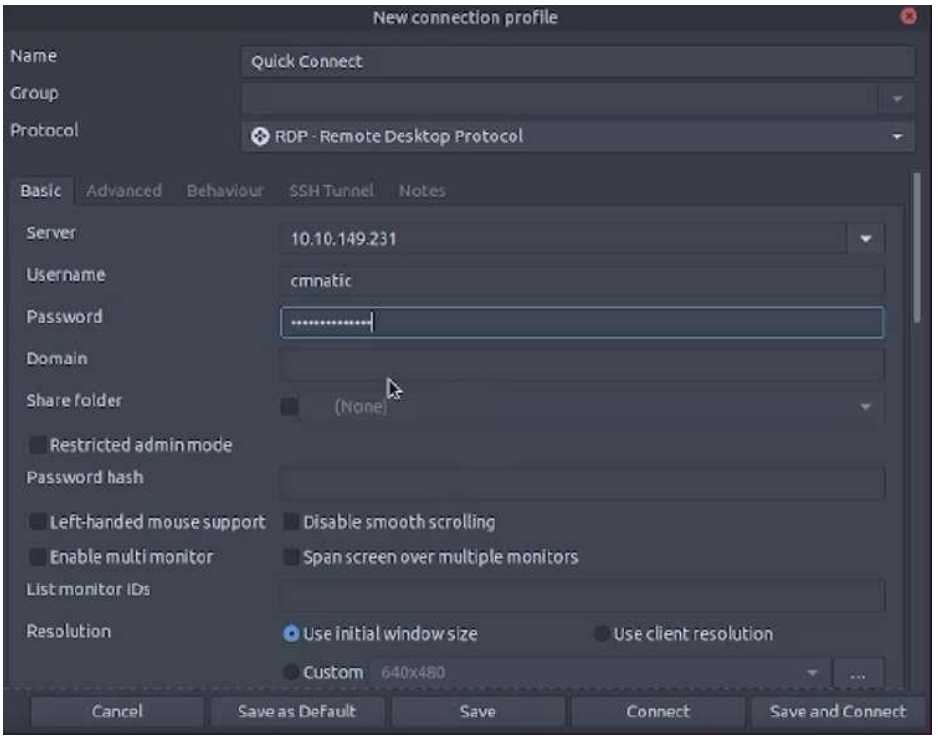
Solution/walkthrough:

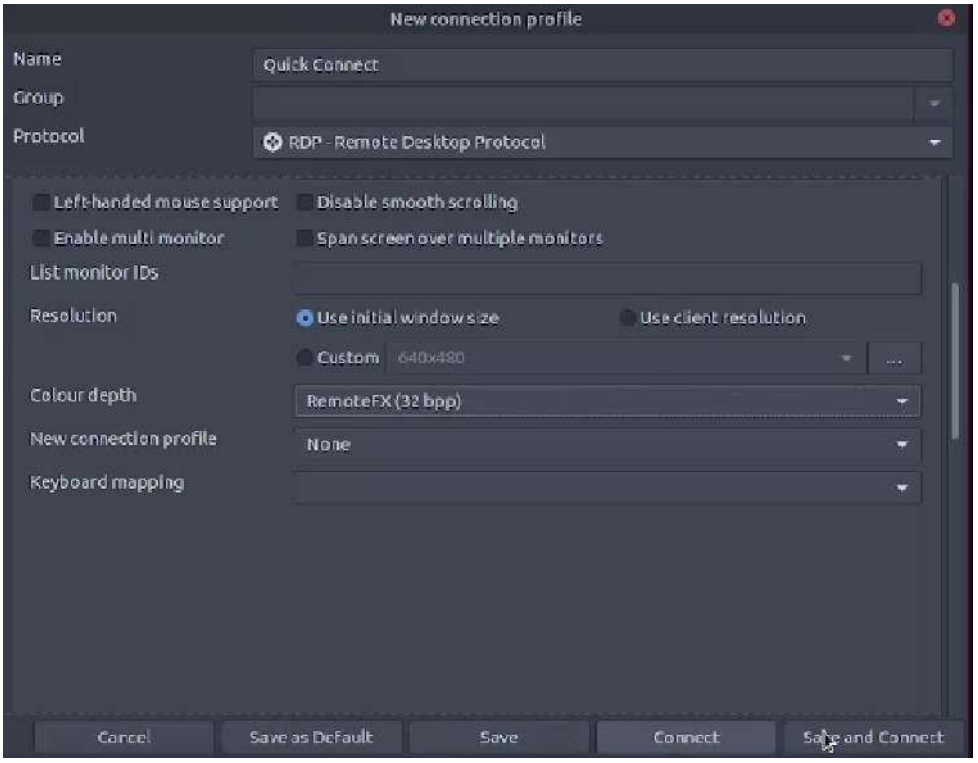
Question 1:

After installing Remmina, it required password to save the session, then press "*Cancel*".

Question 2:

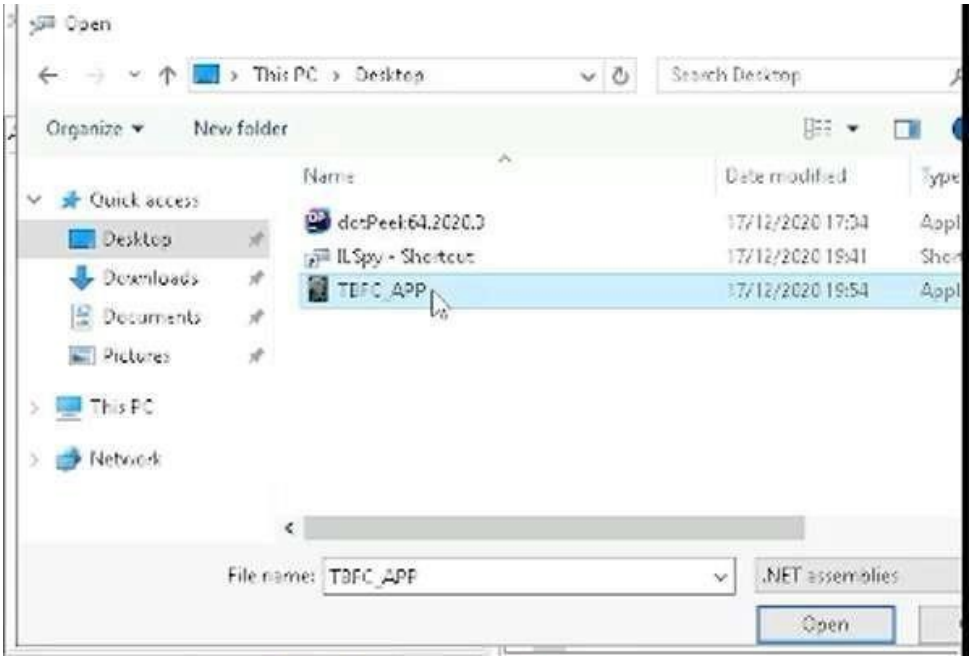
Enter the IP Address, using username "*cmnatic*" and password "*Adventofcyber!*" given by THM. Change the colour depth to "RemoteFX (32 bpp)" and "*save and connect".*

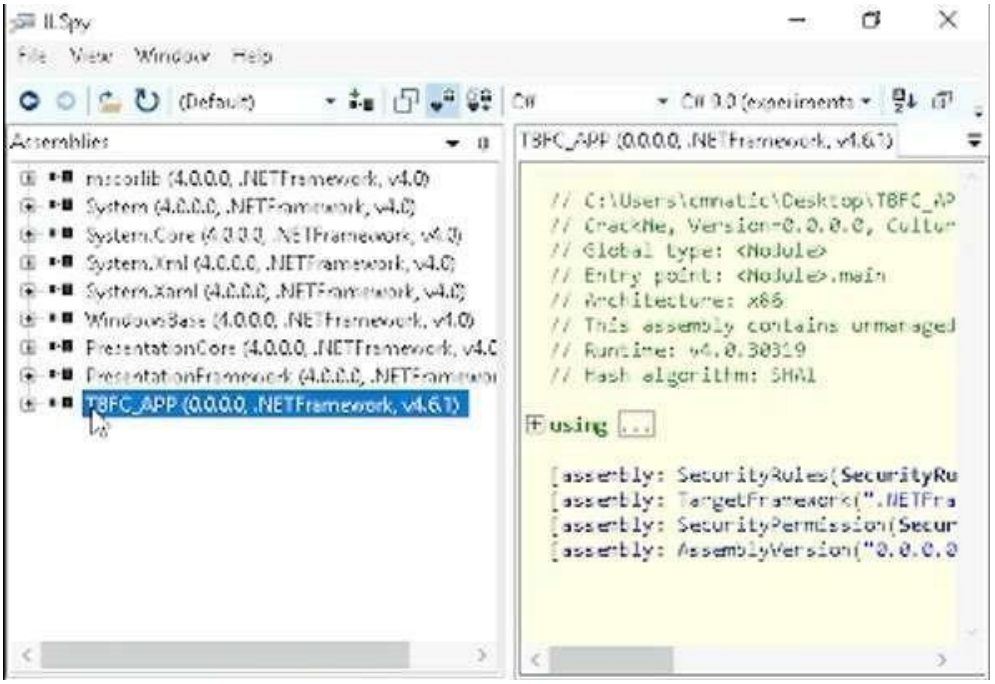




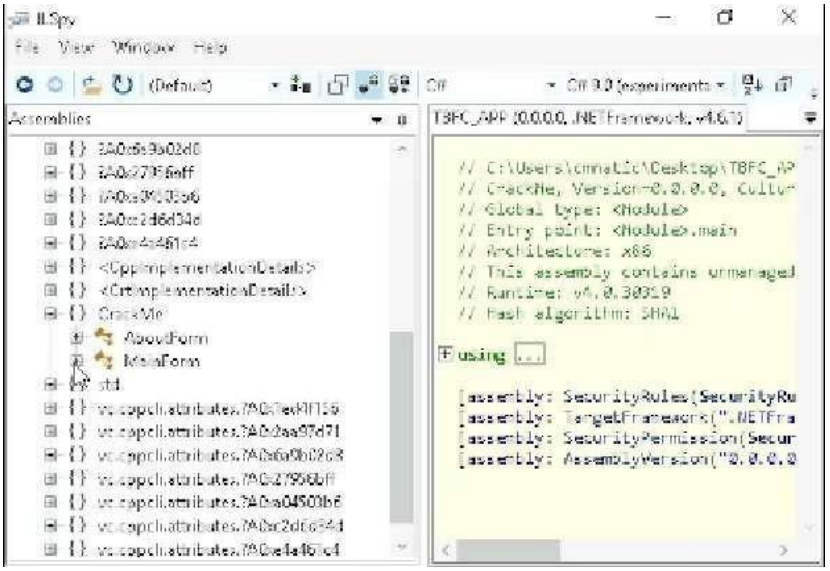
Question 3:

Open “TBFC_APP” in ILSpy and decompile the code.



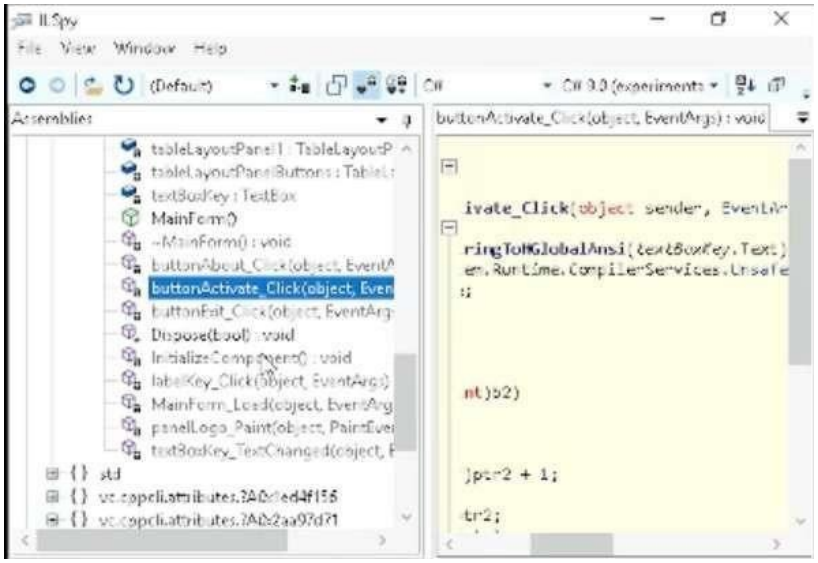


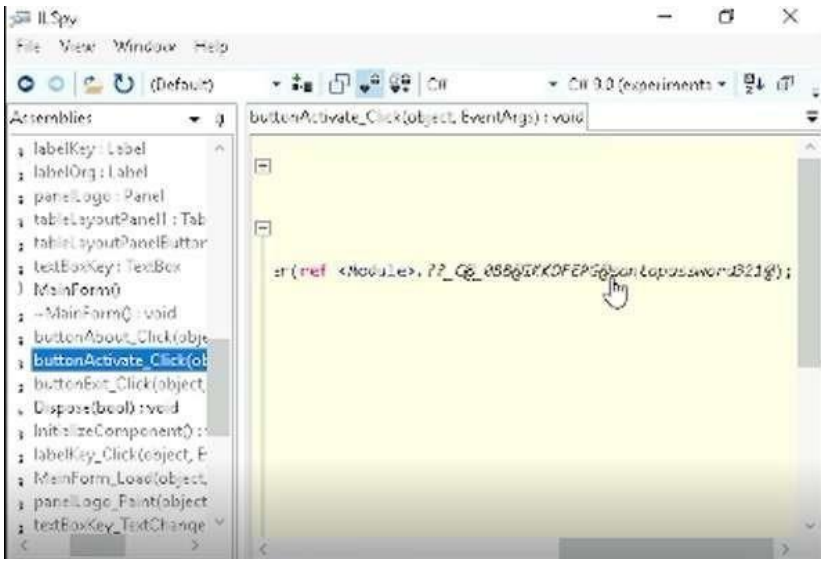
Expand TBFC_APP resources, next expand the “CrackMe” button and look for MainForm.

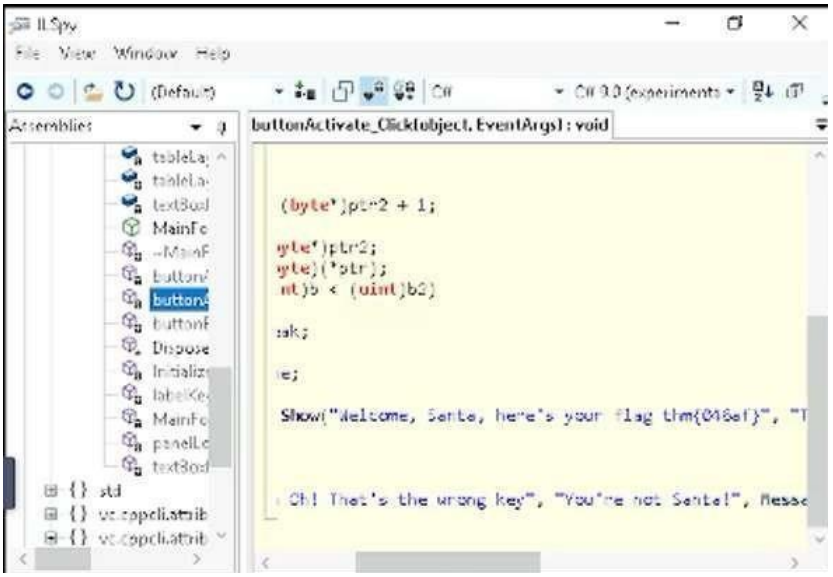


Question 4:

Find “*buttonActivate_Click (object,EventArgs)*” to look for santa password that is “*santapassword321*” and flag is obtained.


ILSpy
File View Window Help
(Default)
C#
C# 9.0 (experiments)
Assemblies
buttonActivate_Click(object, EventArgs) : void
tableLayoutPanel1 : TableLayoutP
tableLayoutPanelButtons : TableL
textBoxKey : TextBox
MainForm()
~MainForm() : void
buttonAbout_Click(object, EventA
buttonActivate_Click(object, Even
buttonExit_Click(object, EventArg
Dispose(bool) : void
InitializeComponent() : void
labelKey_Click(object, EventArgs)
MainForm_Load(object, EventArg
panelLogo_Paint(object, PaintEve
textBoxKey_TextChanged(object, E
{} std
{} vc.cppcli.attributes.?A0x1ed4f156
{} vc.cppcli.attributes.?A0x2aa97d71
ivate_Click(object sender, EventA
ringToHGlobalAnsi(textBoxKey.Text)
em.Runtime.CompilerServices.Unsafe
;
nt)b2)
]ptr2 + 1;
tr2;


ILSpy
File View Window Help
(Default)
C#
C# 9.0 (experiments)
Assemblies
buttonActivate_Click(object, EventArgs) : void
labelKey : Label
labelOrg : Label
panelLogo : Panel
tableLayoutPanel1 : Tab
tableLayoutPanelButtor
textBoxKey : TextBox
MainForm()
~MainForm() : void
buttonAbout_Click(obje
buttonActivate_Click(ob
buttonExit_Click(object,
Dispose(bool) : void
InitializeComponent() :
labelKey_Click(object, E
MainForm_Load(object,
panelLogo_Paint(object
textBoxKey_TextChange
er(ref <Module>.??_C@_0BB@GKKOFEPG@yourpassword321@);



Thought Process/Methodology:

Install the Remmina.Open the Remmina, the password is required so that you can save the session and then press the "*Cancel*". Fill in the IP Address, username "*cmnatic*" and password "*Adventofcyber!*" given by TryHackMe. Next, change the colour depth to "*RemoteFX (32 bpp)*" and *Save and Connect.* It will bring us to a homepage, and used the *ILSpy .* Then open *TBFC_APP* to decompile the code. After that,expand *TBFC_APP* resources, and expand the *CrackMe* button and look for *MainForm*.The last step, search for *buttonActivate_Click* to look for santa password ---- "*santapassword321*" and and the flag is obtained----"*thm{046af}*".

Day 19: Web Exploitation - The Naughty or Nice List

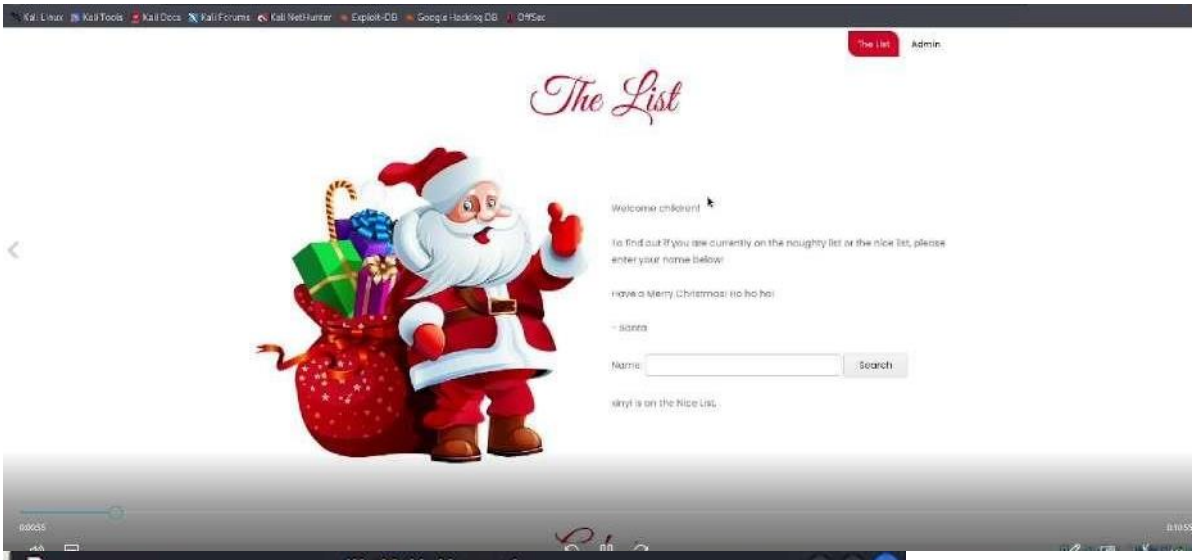
Tools used: Firefox

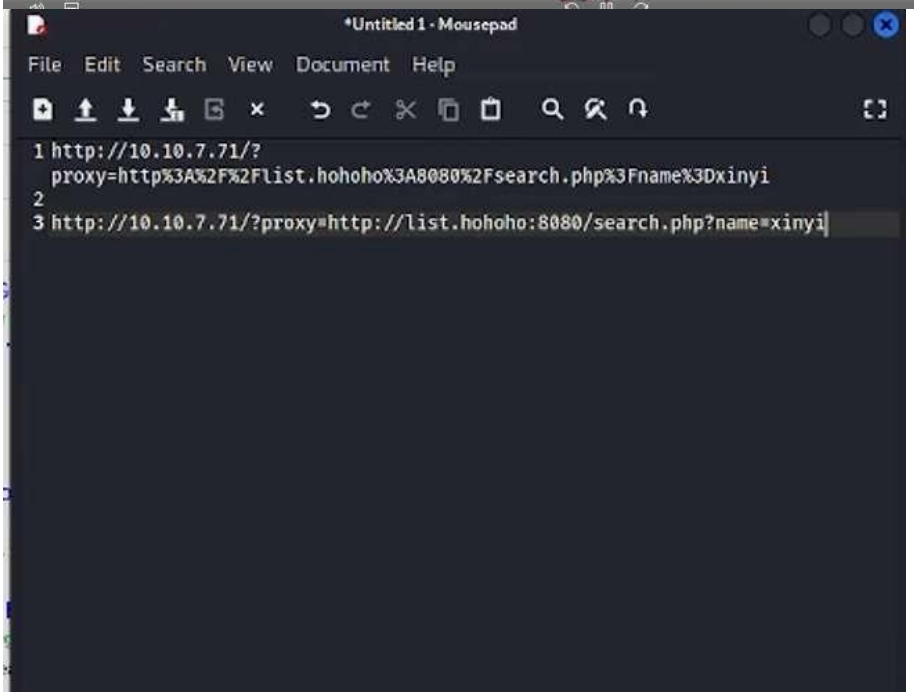
Solution/walkthrough:

Question 1:

Enter the IP machine address given by THM. Key in name in the blank and the url “http://10.10.7.71/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3dxinyi” is shown.

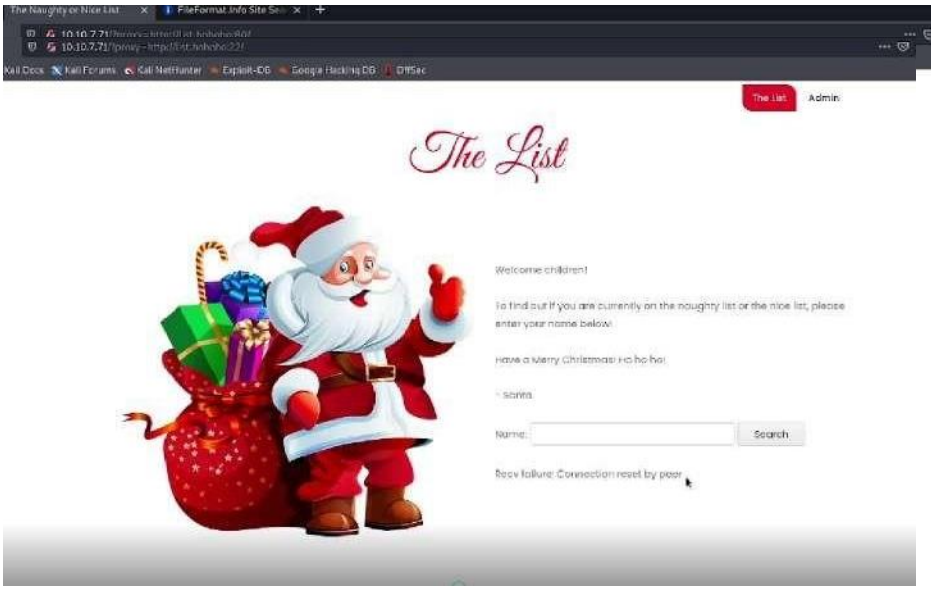
Look for the value of the parameter by using url decoder, then “http://10.10.7.71/?proxy=http://list.hohoho:8080/search.php?name=xinyi” is obtain

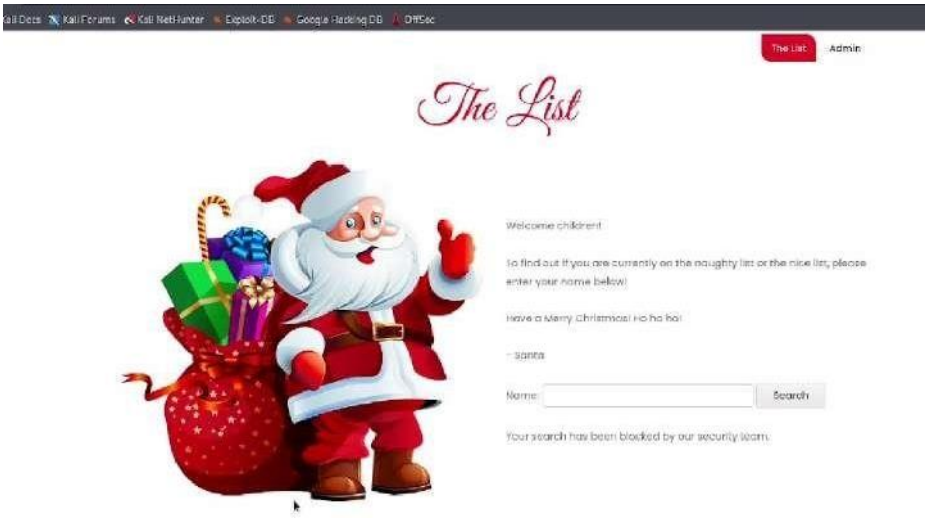


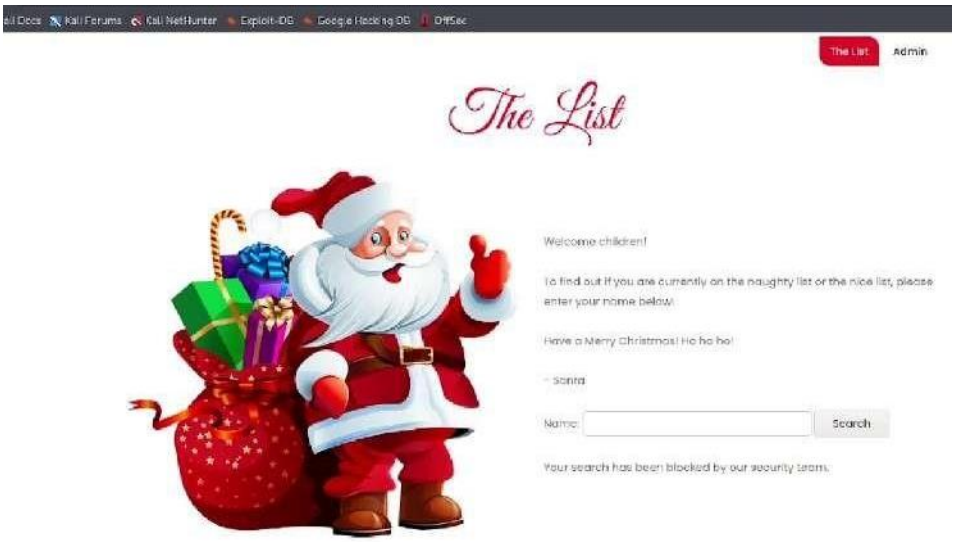


Question 2:

To fetch the root and find URLs of the "list.hohoho" site, try few port number and hostname For example: 8080 to 80, change port 8080 to 22, hostname to “localhost” and “127.0.0.1”. But the URLs did not obtained

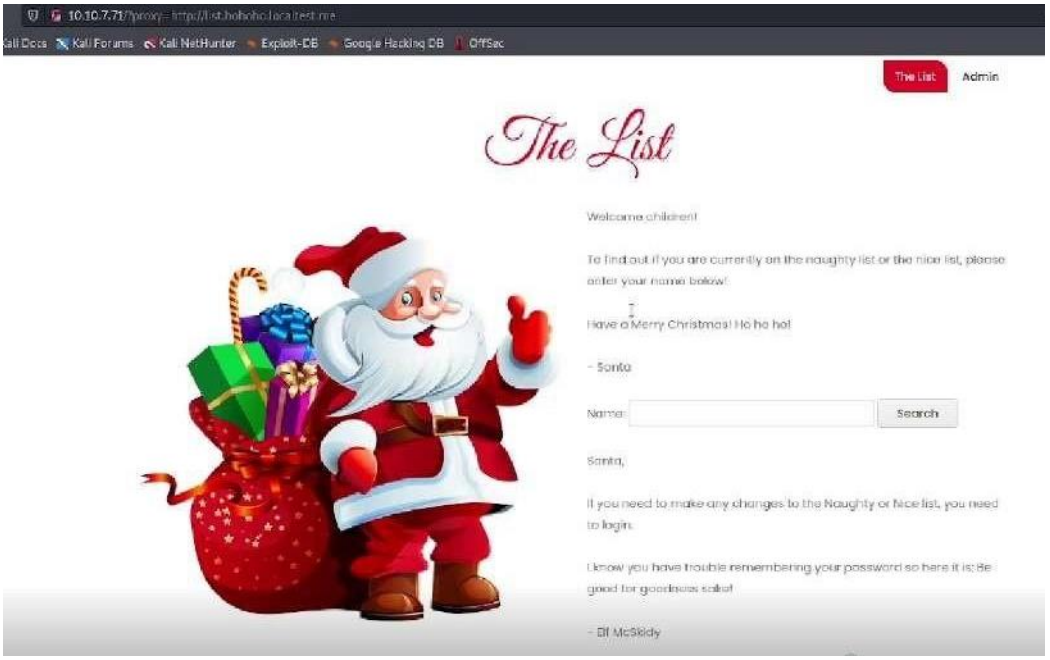






Question 3

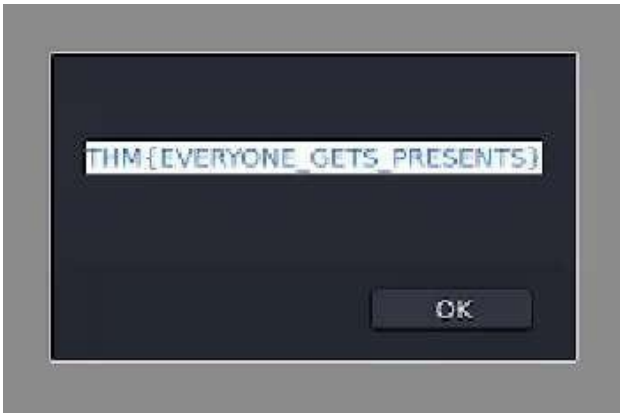
Moreover, change the hostname in URL to "list.hohoho.localtest.me", and the correct URLs is obtained. We know that Santa's password ---- " Be good for goodness sake!"



Key in the username and password and it leads us to an admin form.

Question 4:

Delete the naughty list to look for the flag ----“THM{EVERYONE_GETS_PRESENTS}”



Thought Process/Methodology:

First step, enter the IP address given by TryHackMe. Enter a name and search. Next use URL decoder with the value of proxy parameter *http://10.10.7.71/?proxy=http://list.hohoho:8080/search.php?name=xinyi* is obtained . Next, try to fetch the root, and try few port number and hostname ,for example: *8080* to *80*, change port *8080* to *22*, and hostname to "*localhost"* and "*127.0.0.1*".But the URLs did not obtained.Hence,change to "*http://10.10.7.71/?proxy=http://list.hohoho.localtest.me*", and correct URLs is obtained. We know that Santa's password is "*Be good for goodness sake!*" After that key in username and password and it leads us to admin form.Final step, *delete the naughty list* and the flag is obtained----- "*THM{EVERYONE_GETS_PRESENTS}*"

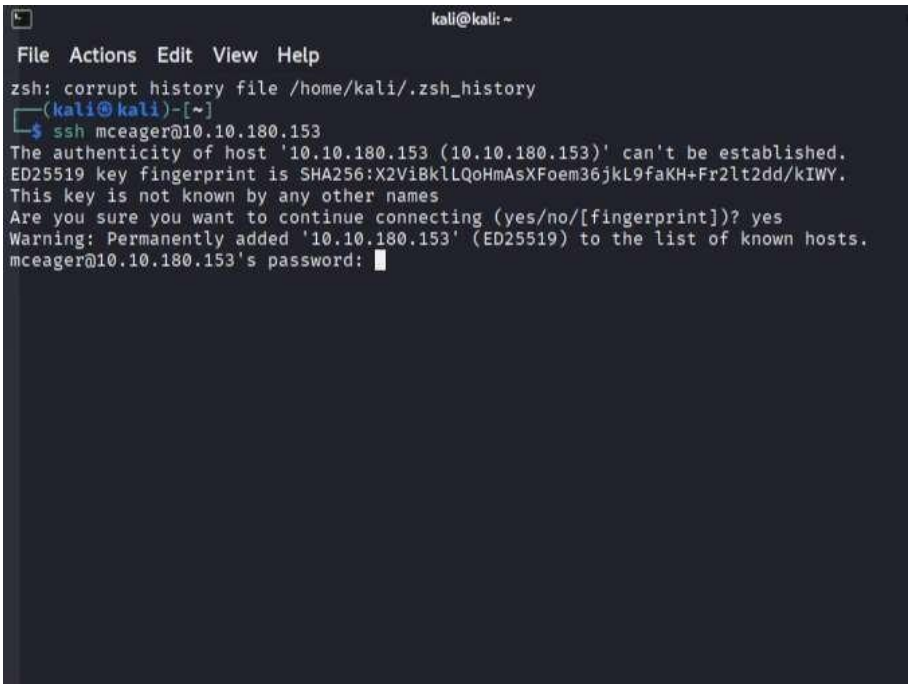
Day 20: Blue Teaming - PowershELlF to the rescue

Tools used: Terminal

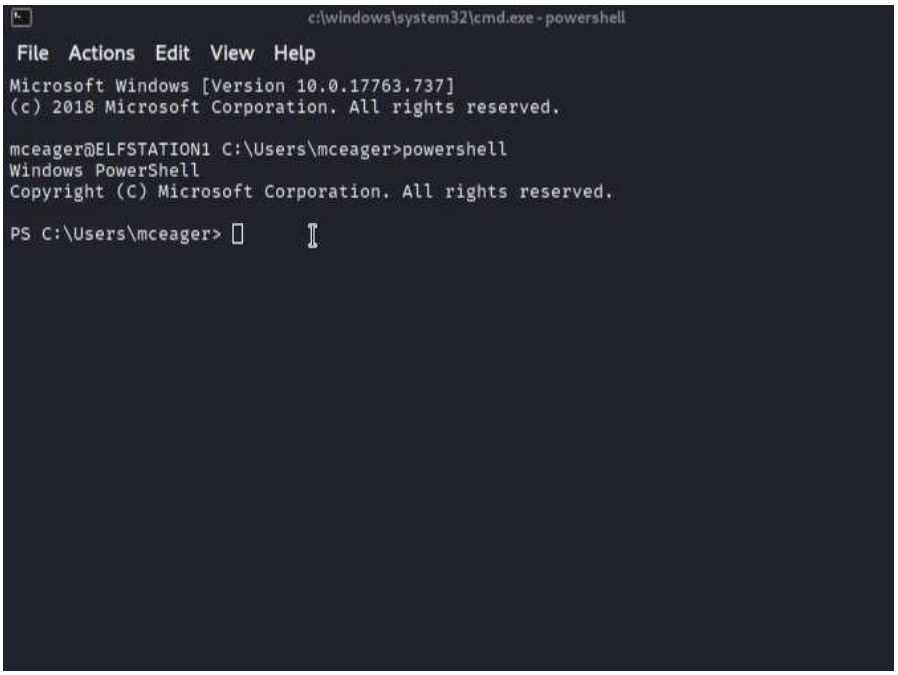
Solution/walkthrough:

Question 1:

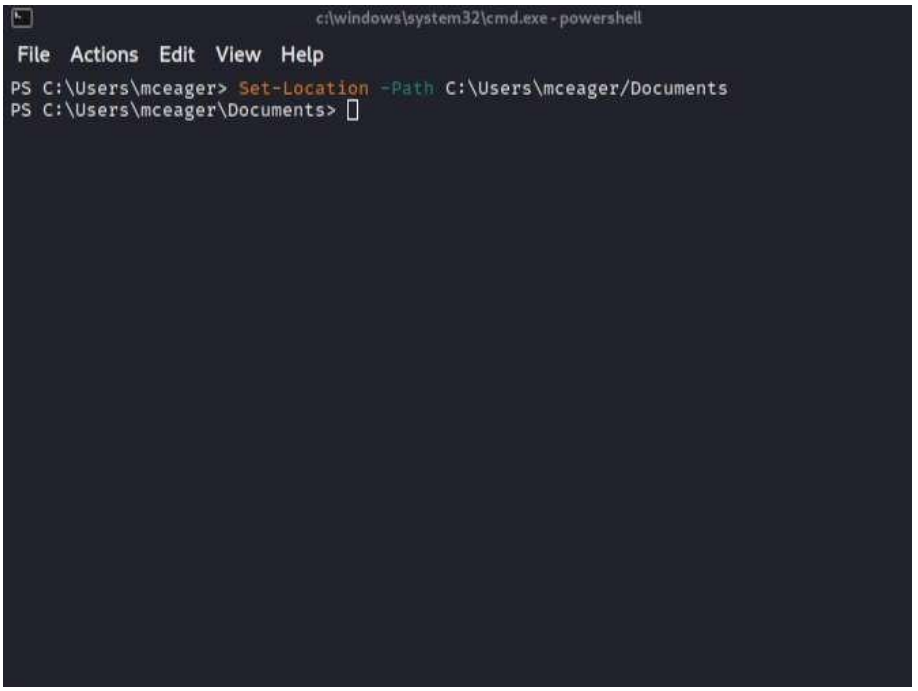
After connecting to machine IP, login to the Windows machine using SSH command: *ssh mceager@10.10.180.153 and the password is :r0ckStar!*



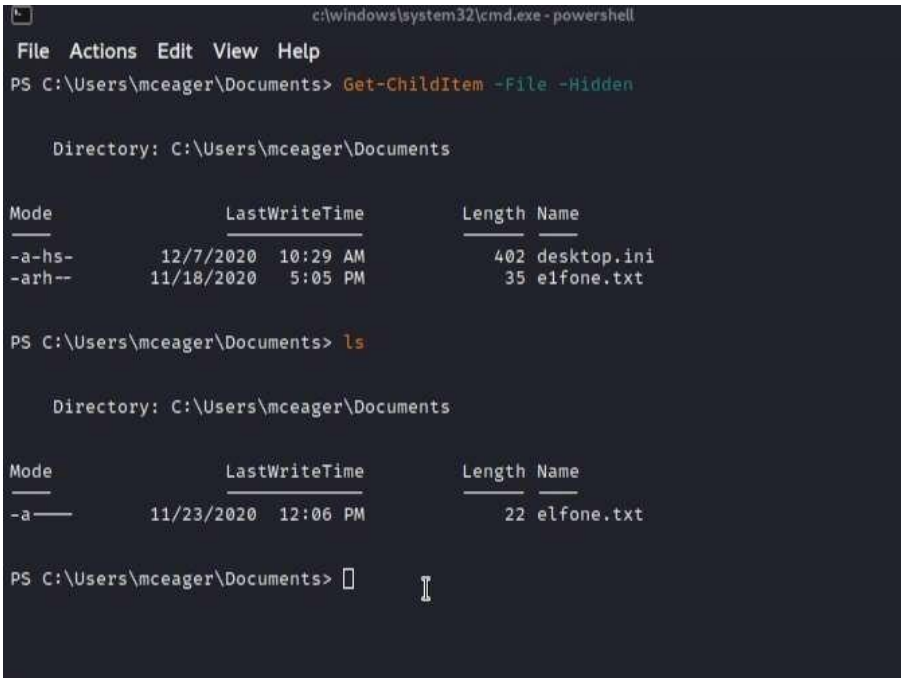
Enter *powershell*



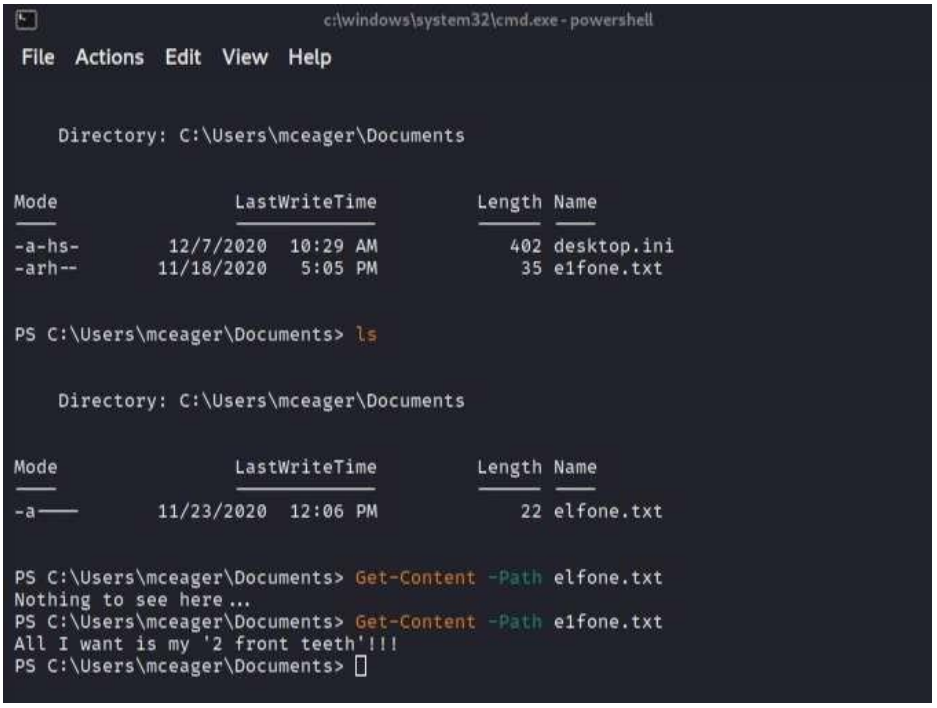
Change file location to *Documents*



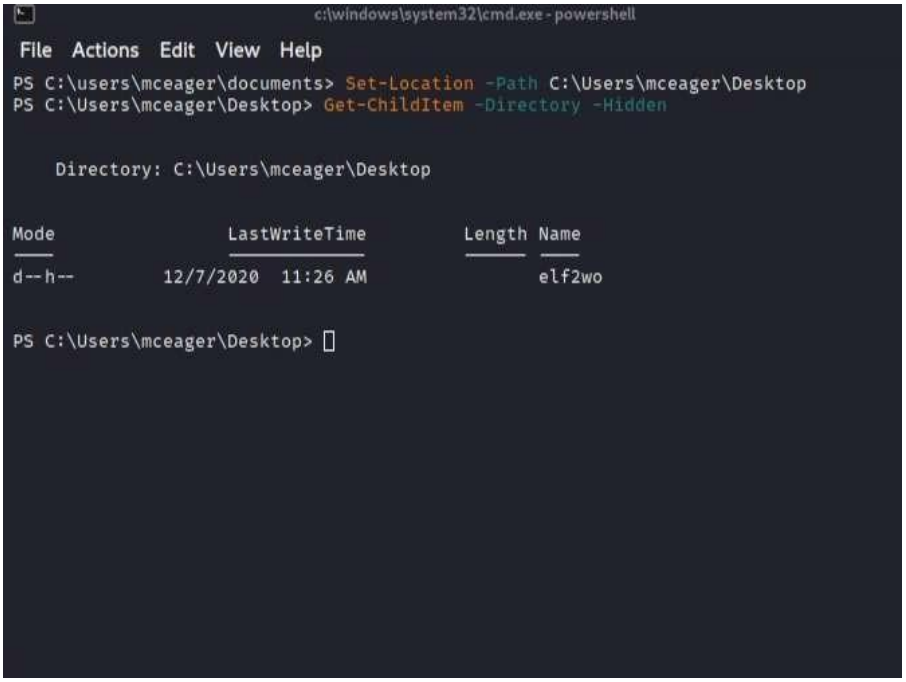
Find the hidden file by key in the command:
Get-ChildItem -File -Hidden



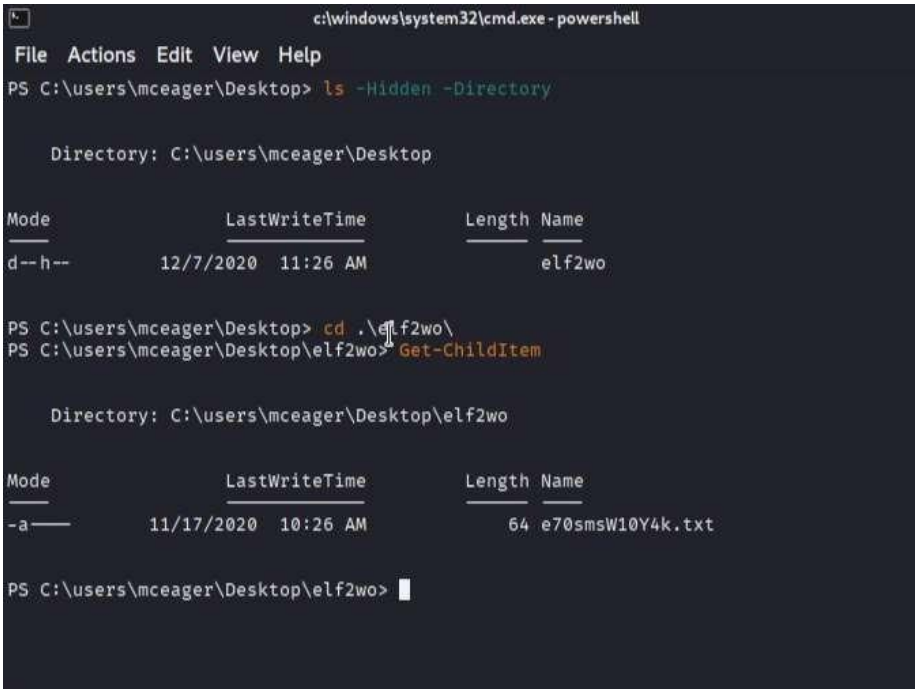
View the hidden file by key in this command:
Get-Content -Path e1fone.txt



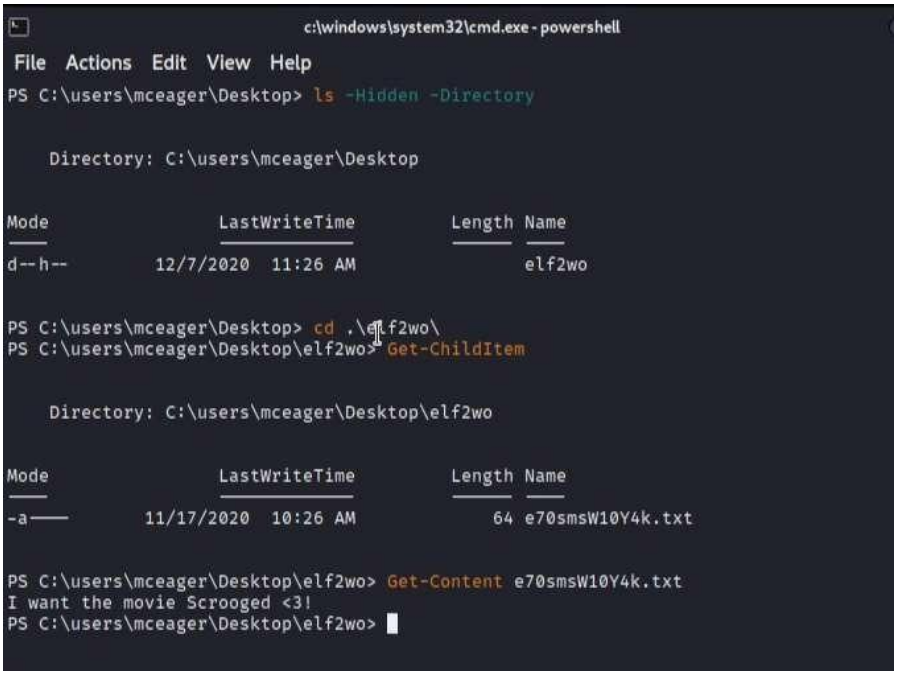
Question 2:
Relocate the file to *Desktop* and look for the hidden directory by key in the command:
Get-ChildItem -Directory -Hidden



Relocate the file to the hidden directory and place the files inside by key in *Get-ChildItem* command



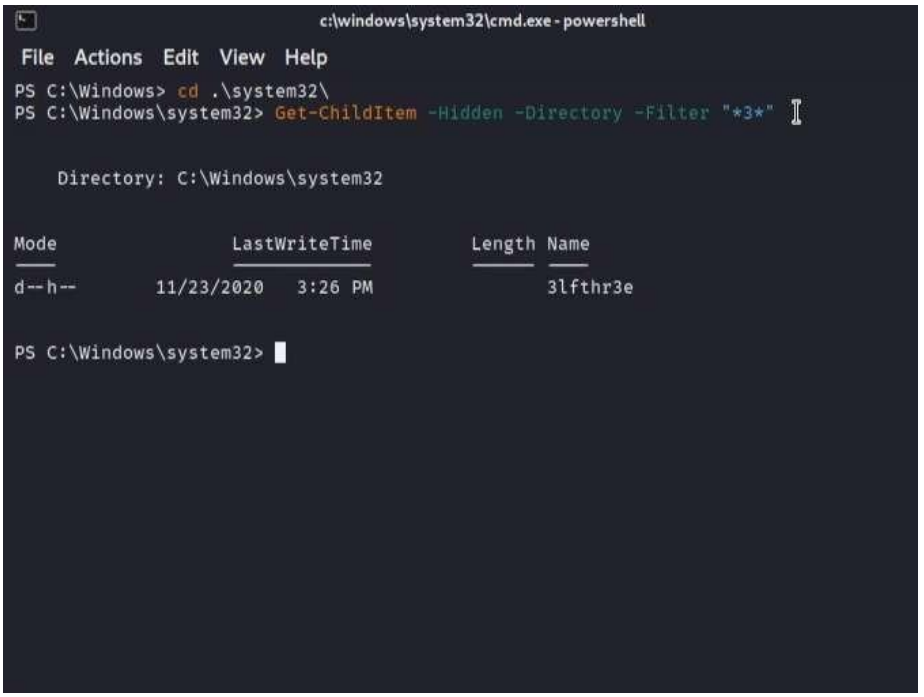
View the file.txt using *Get-Content*



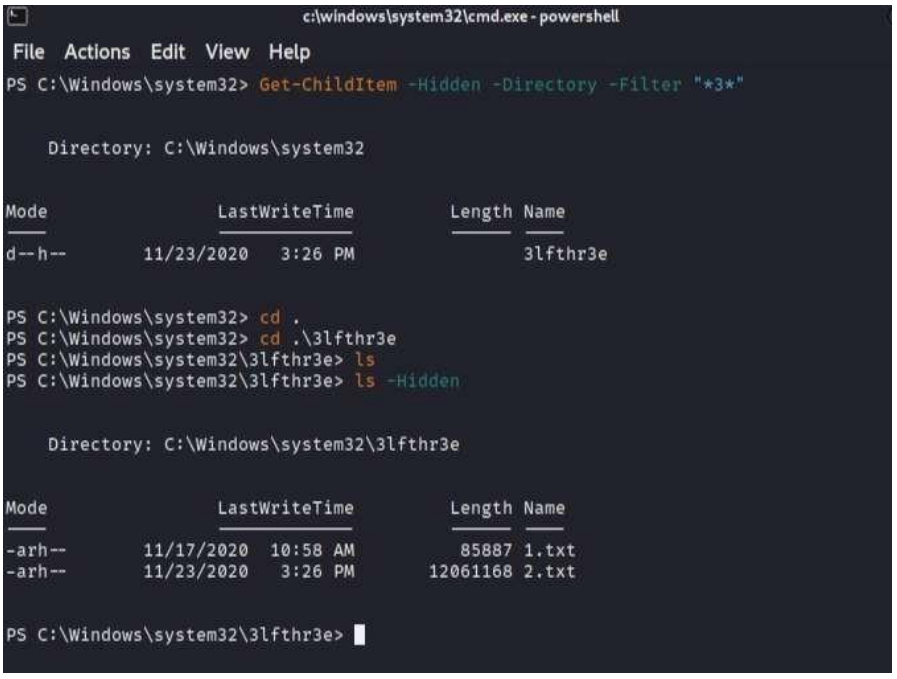
Question 3:

Relocate the file to *C:\Windows\system32* and filter the hidden directory with number *3* by key in this command:

*Get-ChildItem -Hidden -Directory -Filter "*3*"*

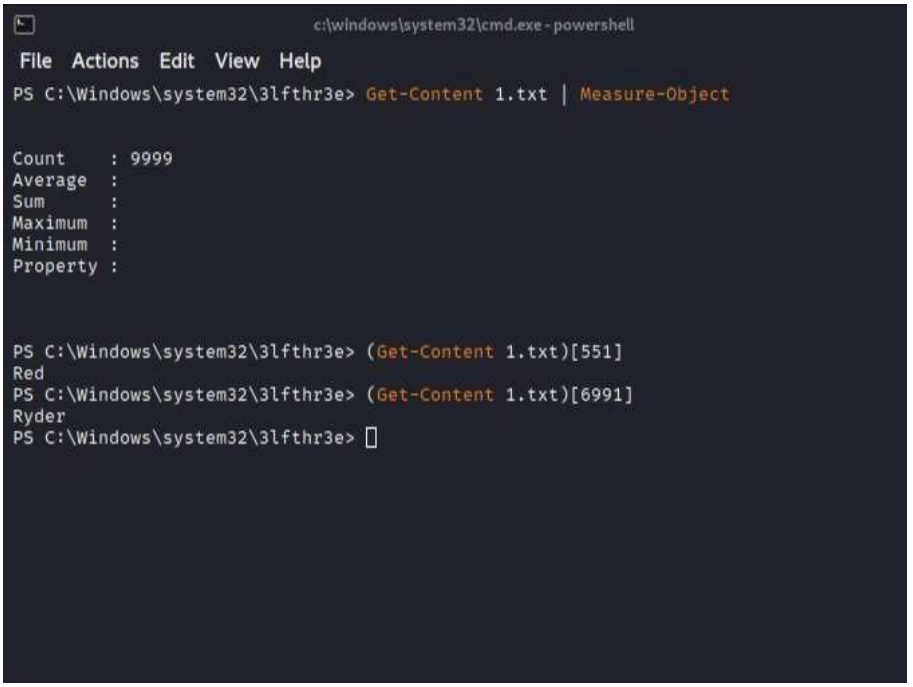


Relocate file location to the hidden directory and place the files in it.



Question 4:
Get the amount of words by key in command:
Get-Content 1.txt | Measure-Object

Question 5:
Convert the *551* and *6991* by entering these commands:
(Get-Content 1.txt)[551]
(Get-Content 1.txt)[6991]



Question 6:
Find the *2.txt* by key in command:
Get-Content 2.txt | Select-String -Pattern "redryder"

Thought Process/Methodology:
After connecting ,login to the Windows machine by using *ssh mceager@10.10.180.153* and the password:*r0ckStar!*,then key in *powershell*. Firstly, change the file location to Documents by key in *Set-Location -Path C:\Users\mceager\Documents* . In *Documents*, look for the hidden file by key in command *Get-ChildItem -Hidden -File* and *e1fone.txt is shown* and if we use the listing command *ls*, the output will be *elfone.txt* which is different. After hidden file ois found, view the file by key in the command *Get-Content e1fone.txt* and '*2 front teeth*' is shown. Secondly,relocate the file location to *Desktop* by key in command *Get-ChildItem -Hidden -Directory*. Next relocate the file to *elf2wo*, *e70smsW10Y4k.txt is found* by key in command *Get-ChildItem* and then open the *.txt fil*e by key in *Get-Content e70smsW10Y4k.txt* and'*Scrooged*' is shown. Thirdly, relocate file location to *C:\Windows\system32* and filter the hidden directory with number *3* by key in command *Get-ChildItem -Hidden -Directory -Filter "*3*"*. Then, *3lfthr3e* directory is shown.Fourthly, open the *3lfthr3e* directory to look for the *1.txt* inside it and search for the count by key in command *Get-Content 1.txt | Measure-Object* which the outcome ----*9999*.Next, convert the 551 and 6991 in 1.txt by key in commands *(Get-Content 1.txt)[551]* and *(Get-Content 1.txt)[6991]*. Then, merge the 2 outputs and 'Red Ryder' is obtained. Lastly, search in 2.txt by key in command *Get-Content 2.txt | Select-String -Pattern "redryder"* and *redryderbbgun* is shown.