PSP0201 Week 5 Writeup

Group Name: DHM

**Members:**

ID	Name
1211101844	TAN EASON
1211103145	AZRYL SHAMIN BIN AZRIZAL
1211103690	JERRELL SU MING JIE

Day 16: Scripting - Help! Where is Santa?
Tools used: Firefox, Python
Solution/walkthrough:
<u>Question 1</u>
After start the machine, type nmap -v and the IP address
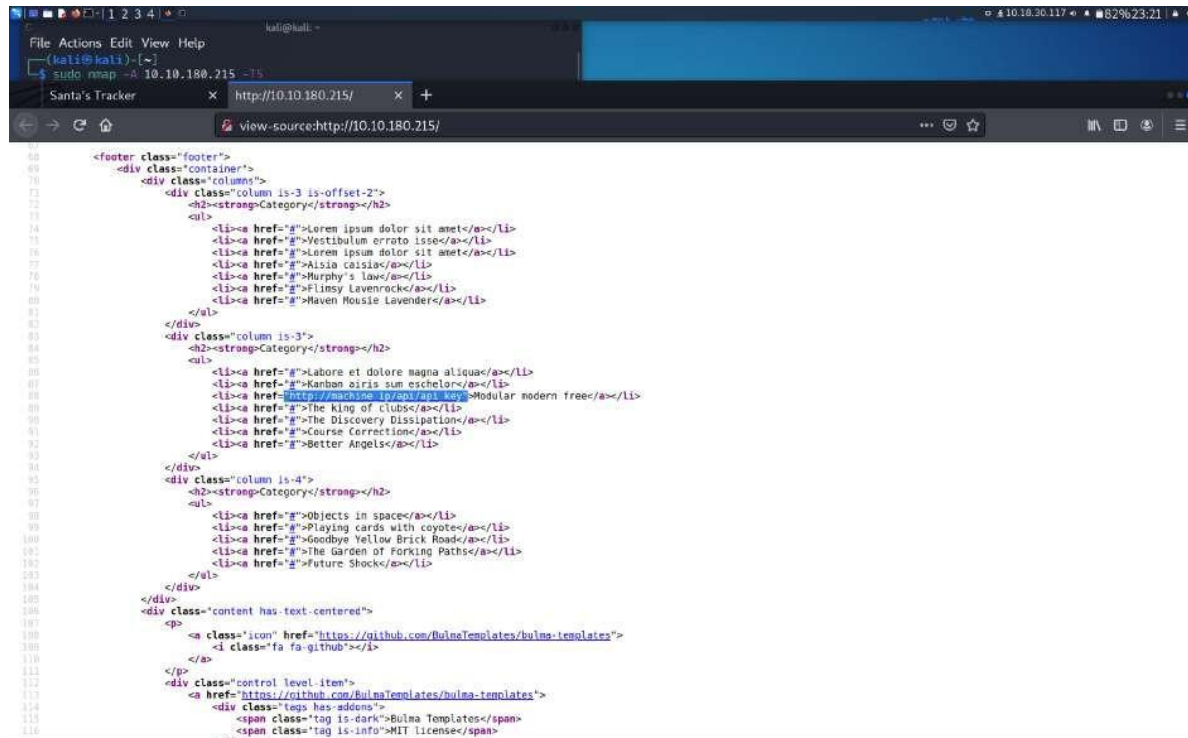

And the port will be given
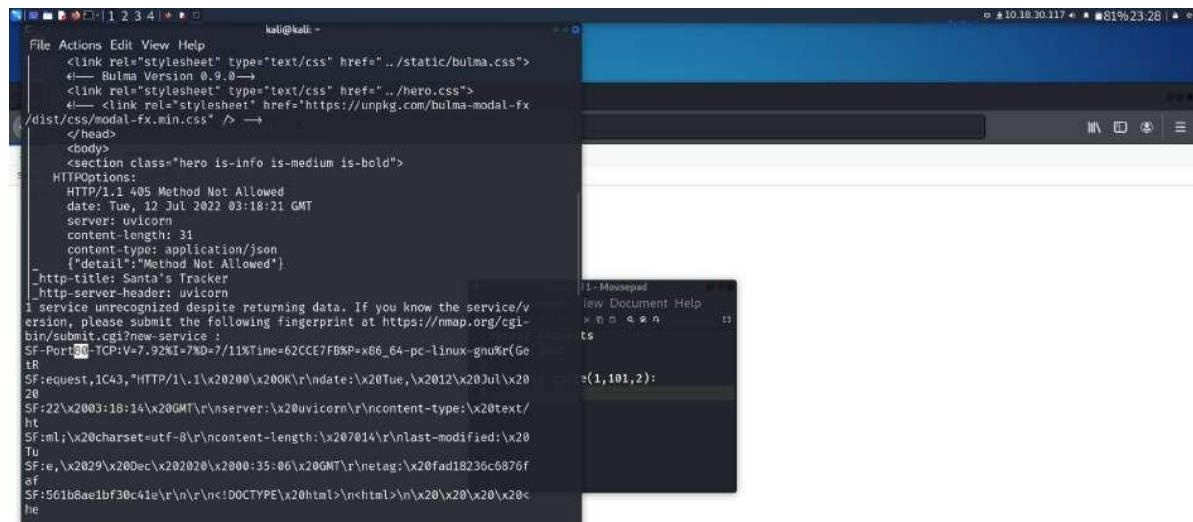
Question 2

In the firefox, enter the IP address and right click to view page resource
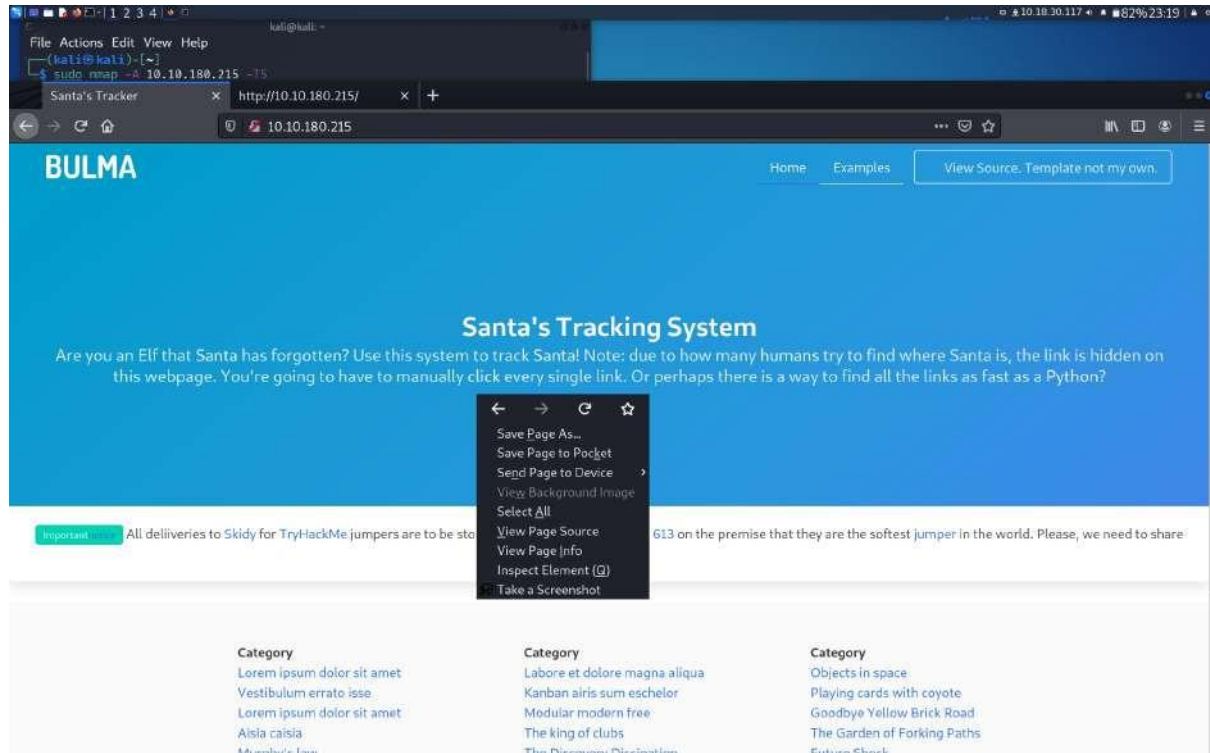
And you will see the API

Question 3

After that, create a new python with nano brute.py. Then, import requests
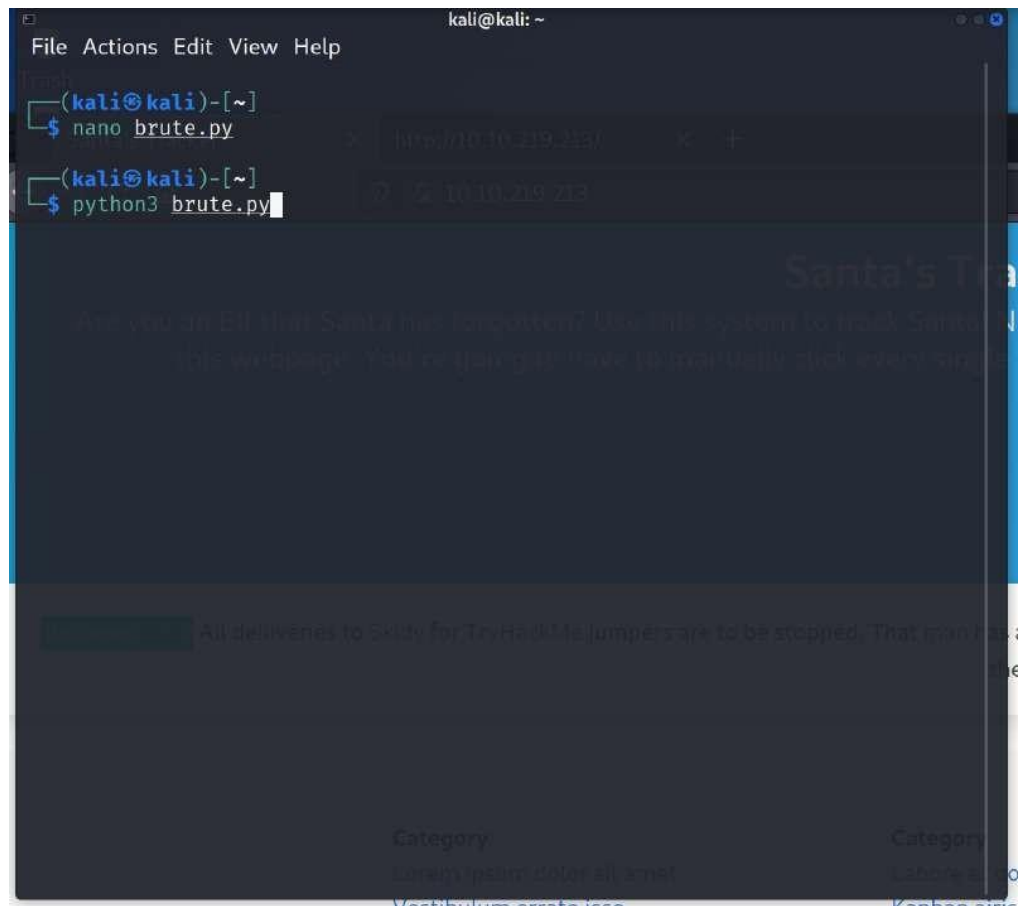
```
import requests

#       http://10.10.49.56:8000/api/4

#url = 'http://10.10.49.56:8000/api/'
#r = requests.get(url)

#print(r.text)

for i in range(1,100,2):
        r = requests.get(url+str(i))
        if 'Error' not in r.text:
                print(i)
                print(r.text)
```

```
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Linter  ^  Go To Line
```

Thus, use python3 and brute.py and show the result

```
                                    kali@kali: ~
File Actions Edit View Help

┌──(kali㊉kali)-[~]
└─$ nano brute.py

┌──(kali㊉kali)-[~]
└─$ python3 brute.py
```

Thus, we can know where is santa now

{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}

Question 4:

Finally, the correct API key will also be shown and it is an odd number as well.

57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}

Thought Process/Methodology:

This is a python scripting task so that we need to script a little bit to do it. Firstly, type nmap -v and the IP address after starting the machine. Then, find out the port, it will be given somewhere. Also, enter the IP address in the firefox and right click to view page resources as well. Later, we can type the IP address and :8000 to look for it. Also, we can try /api/… and api key to try it behind the port. After that, create a new python with nano brute.py. Then, import requests. There are multiple ways to use the command by the way. And then, I have created a new python which is brute.py. After finishing the command, use python3 and brute.py. After that, save it and modify it. Furthermore, type python3 and brute.py behind the python3. it will show you the result. Hence, we can know where Santa is now, which is winter wonderland, hyde park, london. With the command I type, I can directly know the API key as well,which is 57.

Day 17: Reverse Engineering - ReverseELFneering

Tools used: Command Prompt, elfmceager

Solution/walkthrough:

Question 1

First, login as *elfmceager@IPaddress* and key in the password given by THM which is *adventofcyber*.

After the file is analysed, open the file "*challenge 1*" and enter the main file and get the value of local_ch is 1.

Find the value of eax which is resulted as 6 and the value of local_4h which is also 6.

Thought Process/Methodology:

First, login as *elfmceager@IPaddress* and key in the password given by THM which is *adventofcyber*. Then we open the file "*challenge 1*" and get into the main page in the "*main page*" we can get the value of *local_ch* when its corresponding movl instruction is called is *1* and the value of eax when the imul instruction is called *1 x 6* = *6* and the value of *local_4h* before eax is set to 0 is *6* also.

Day 18: Reverse Engineering - The Bits of Christmas
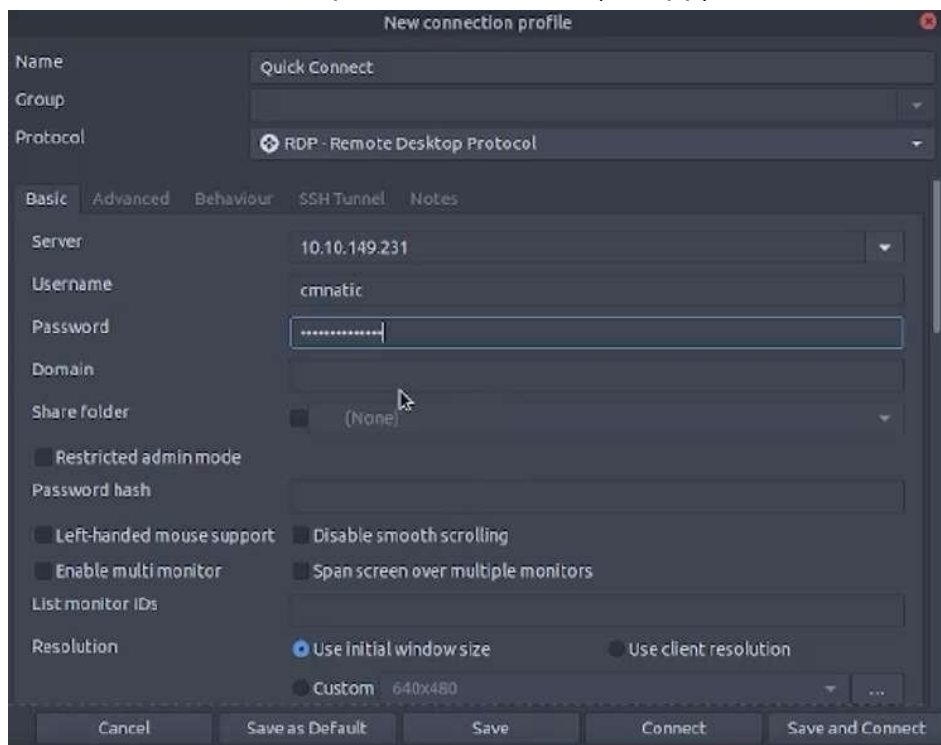
Tools used: Remmina

Solution/walkthrough:

<u>Question 1</u>

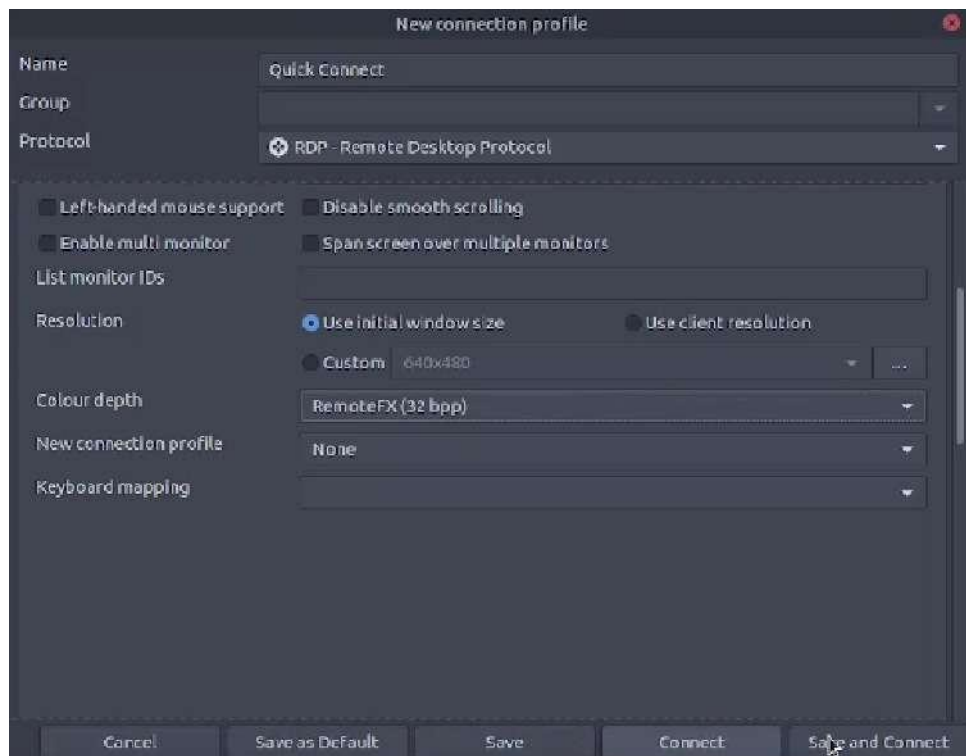After installing Remmina, Remmina will ask for a password to save the session, we can press "*Cancel*".

<u>Question 2</u>

Fill in the IP Address, username "*cmnatic*" and password "*Adventofcyber!*" given by THM. Set the colour depth to "RemoteFX (32 bpp)" then "*save and connect*".
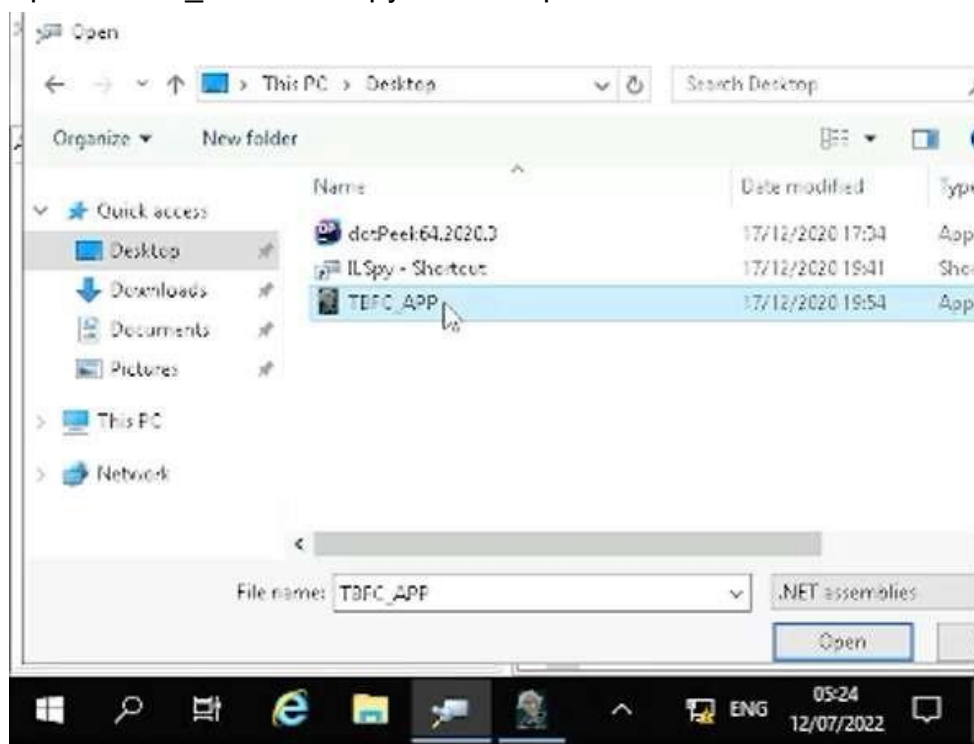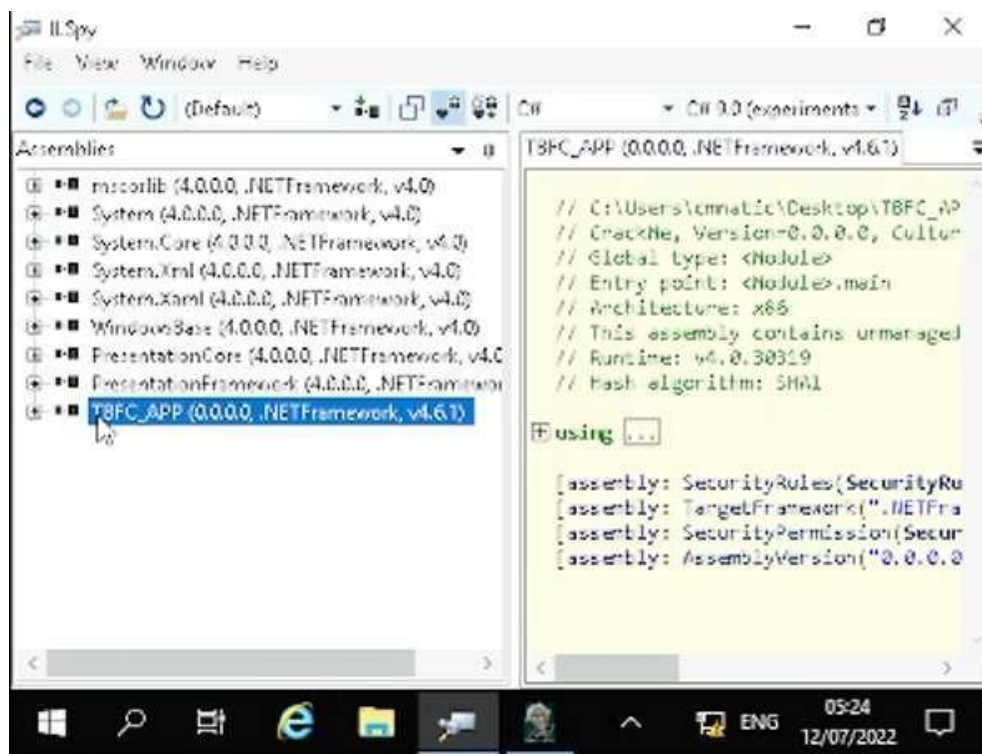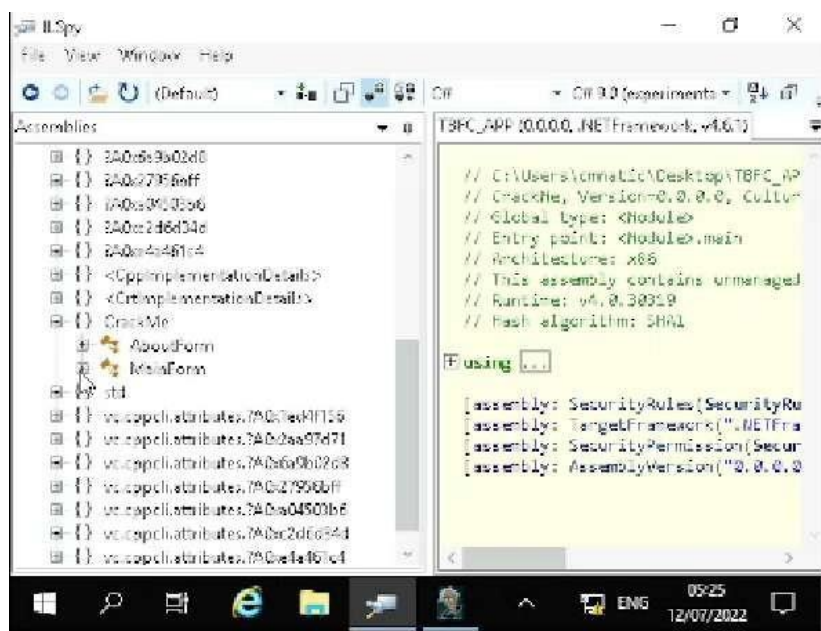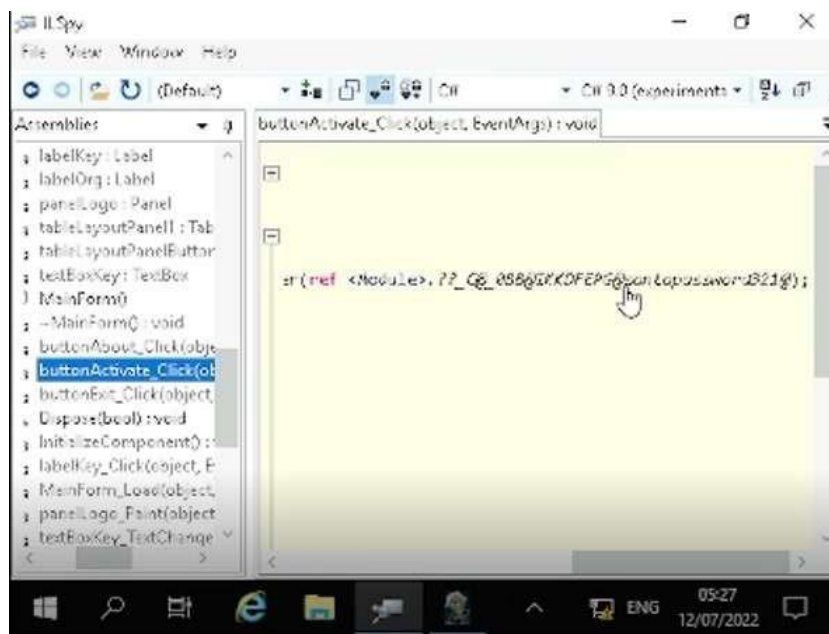
Question 3
Open "TBFC_APP" in ILSpy to decompile the code.
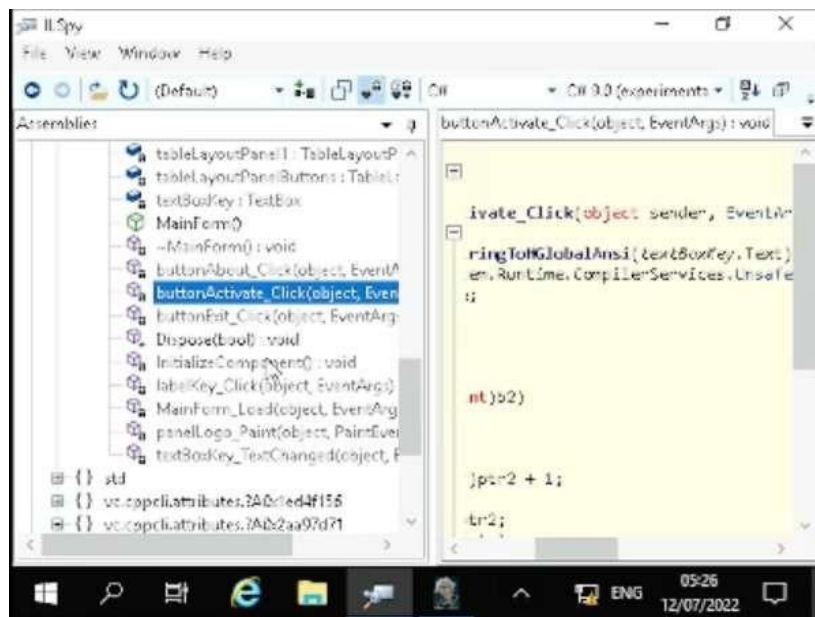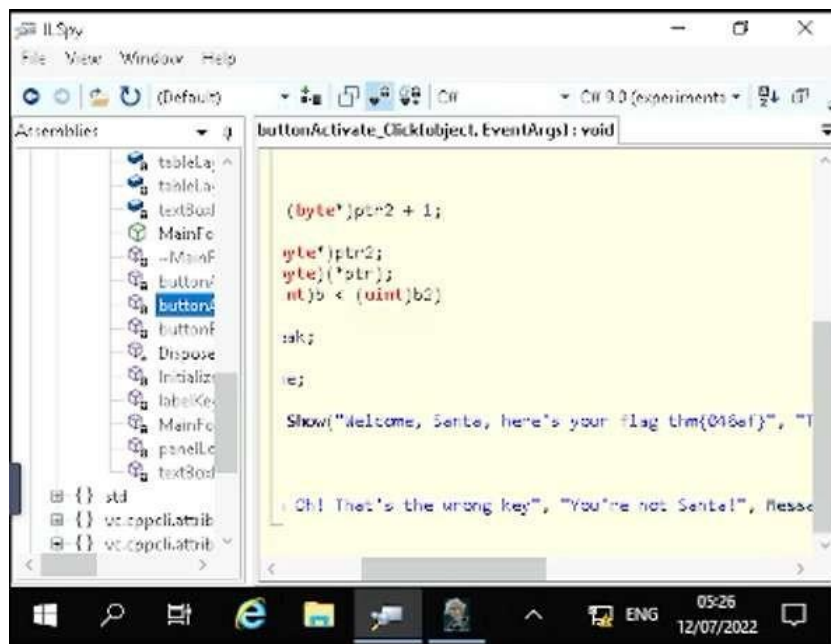
Expand TBFC_APP resources, then expand the "CrackMe" button and find MainForm.

Question 4

Look for "*buttonActivate_Click (object,EventArgs)*" to find santa password which is "*santapassword321*" and capture the flag.

Thought Process/Methodology:

In this task in order to capture the flag, we need to use Remmina. When we open Remmina, it will ask for a password to save the session but it is safe to "*Cancel*" it. Afterwards, Remmina will lead us to a *New Connection Profile,* we need to fill in the IP Address, username "*cmnatic*" and password "*Adventofcyber!*" given by TryHackMe. Then, set the colour depth to "*RemoteFX (32 bpp)*" and only can *Save and Connect.* It will lead us to a homepage, and we used the *ILSpy* App instead of *dotPeek64.* Then we open *TBFC_APP* from *File* in *ILSpy* to decompile the code. We expand *TBFC_APP* resources, then expand the *CrackMe* button and find *MainForm.* Lastly we look for *buttonActivate_Click (object,EventArgs)* in order to find santa password which is "*santapassword321*" and capture the flag "*thm{046af}*".
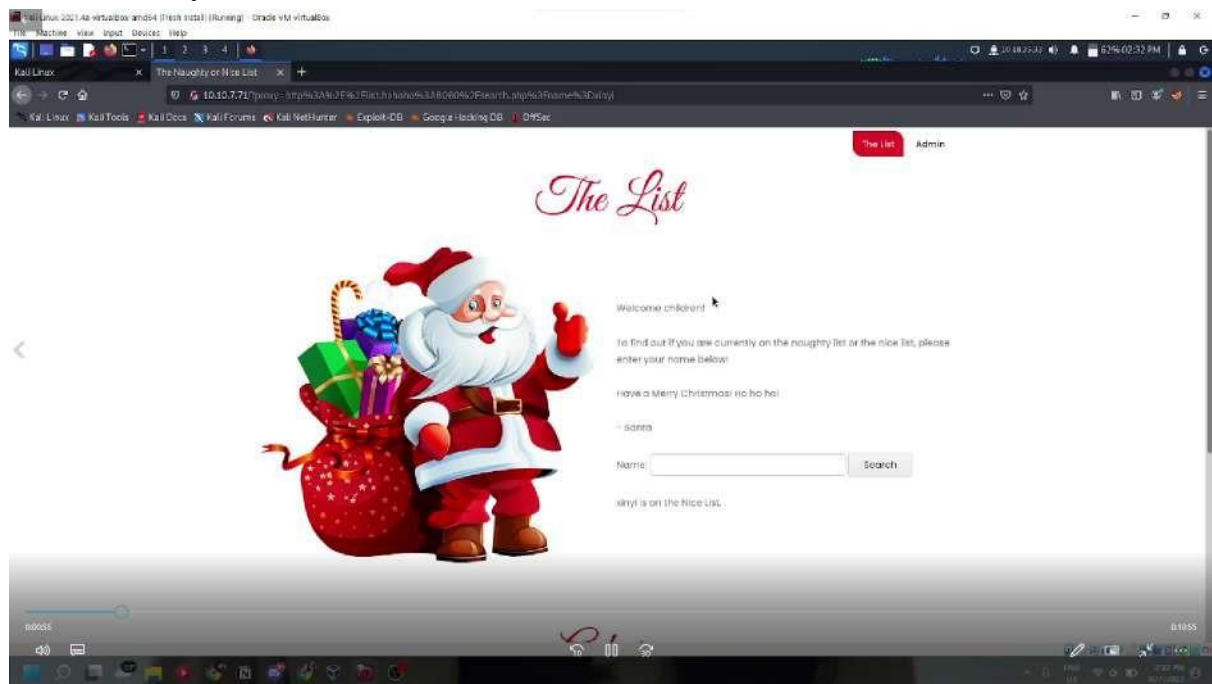
Day 19: Web Exploitation - The Naughty or Nice List
Tools used: Firefox
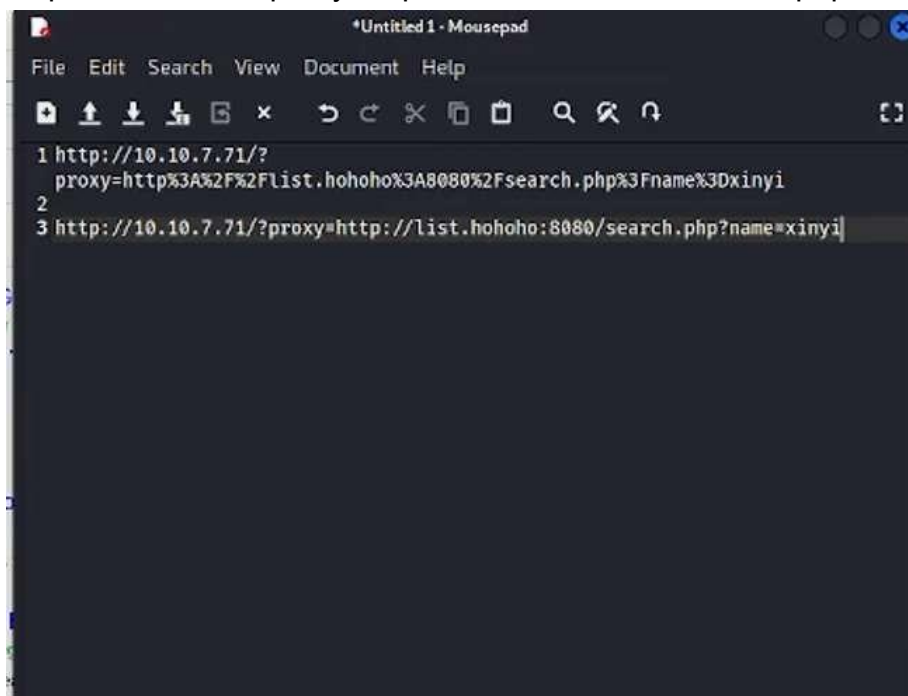**Solution/walkthrough**:
Question 1
Connect to the web app by using the IP machine address given by THM. Enter a name in the form and the url will become
"http://10.10.7.71/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3F name%3dxinyi"

We use the url decoder to find the value of the parameter, we get
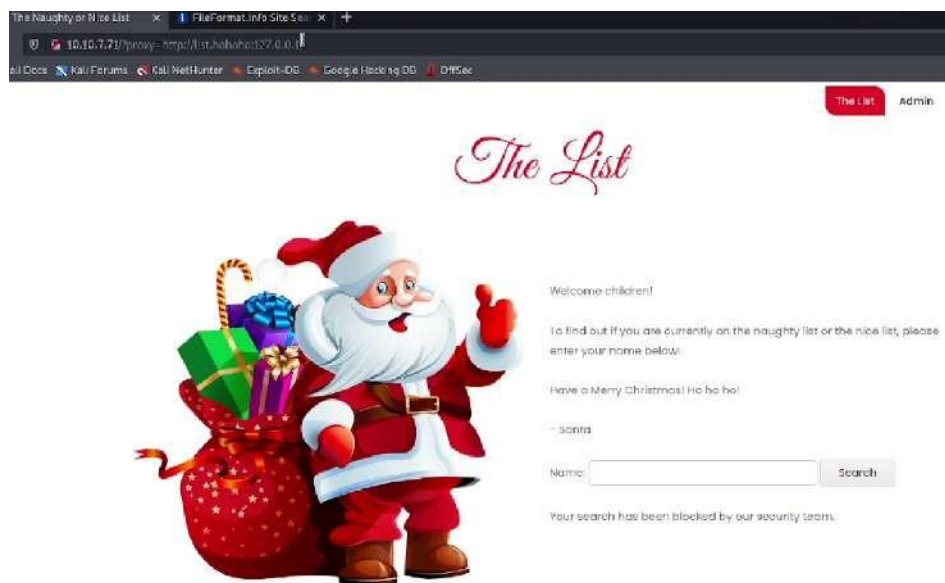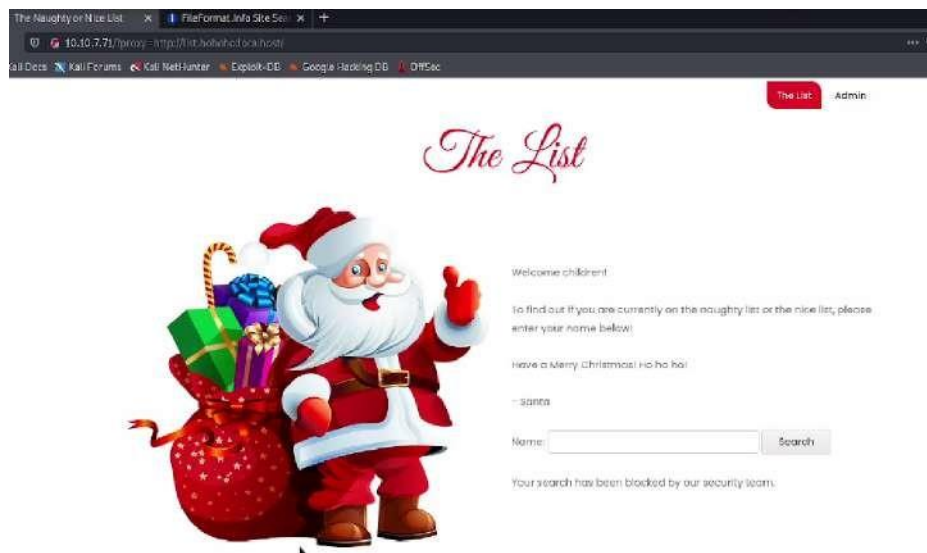"http://10.10.7.71/?proxy=http://list.hohoho:8080/search.php?name=xinyi"

Question 2

To fetch the root and try to find valid URLs for the "list.hohoho" site, we tried different port number and hostname such as changing port 8080 to 80, changing 8080 to 22 (which is the default SSH port), changing hostname from "list.hohoho" to "localhost" and "127.0.0.1". Yet it still can't be accessed.
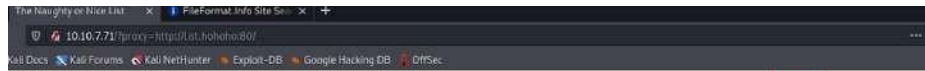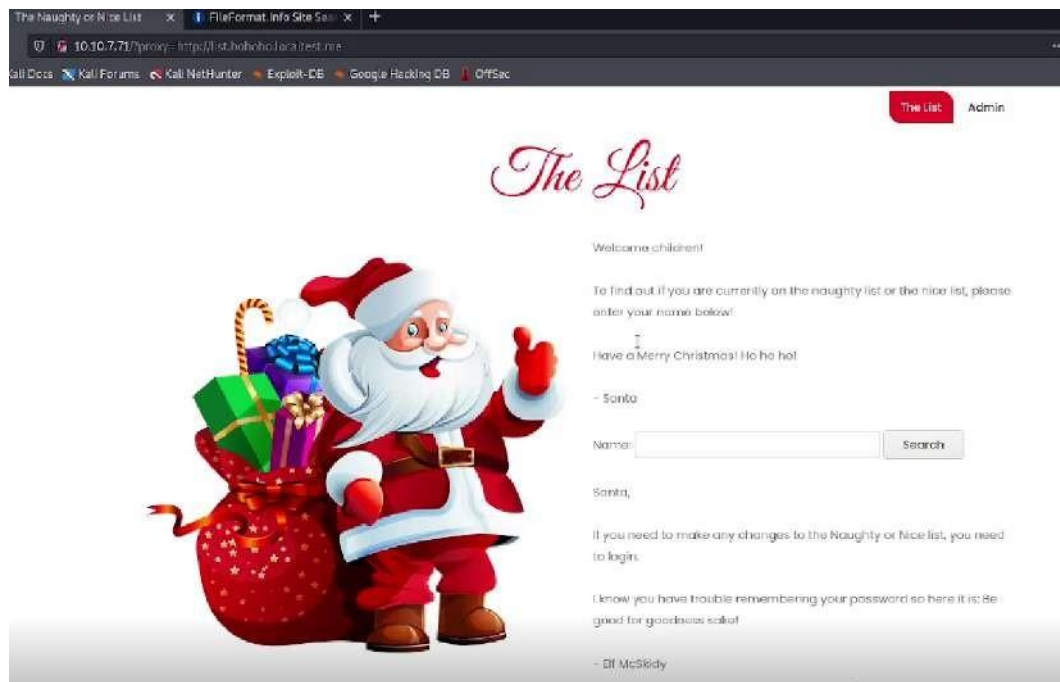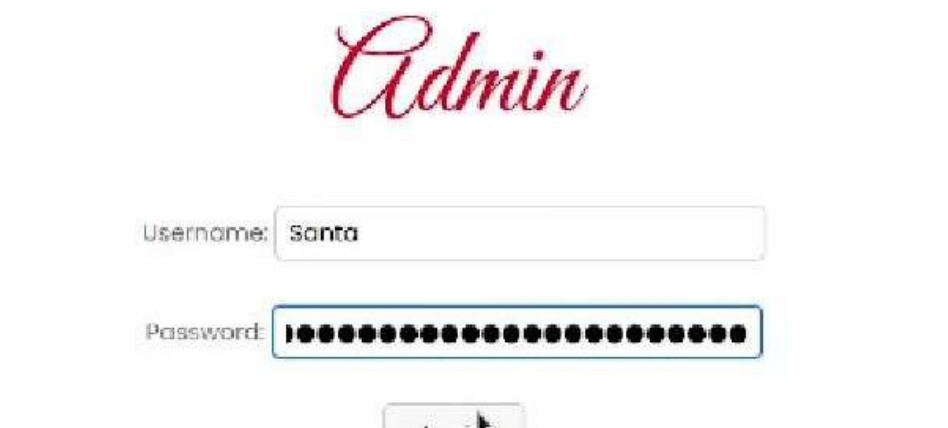
Question 3

Therefore, we set the hostname in the URL to "list.hohoho.localtest.me", and it succeeded. We found Santa's password which is " Be good for goodness sake!"
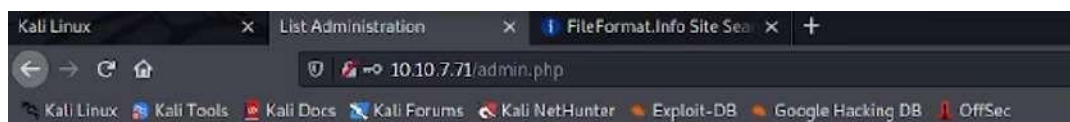
Then we input the username and password we found into the admin form.

Question 4

Delete the naughty list to find the challenge flag which is
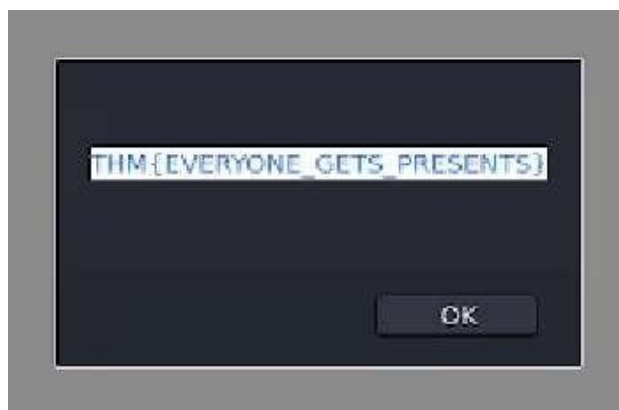"THM{EVERYONE_GETS_PRESENTS}"

Thought Process/Methodology:

To capture the flag, we only require Firefox. Firstly, we connect to the web app by using the IP machine address given by TryHackMe. Fill up the form with a name and press the "*Search*" button. When the website is loaded, it informs us that the name is on the Nice List. Then we use a URL decoder on the value of the proxy parameter and we get *http://10.10.7.71/?proxy=http://list.hohoho:8080/search.php?name=xinyi* . Since "*list.hohoho*" is not a valid hostname on the Internet**,** we need to try to fetch the root, and we tried different port number and hostname such as changing port *8080* to *80*, changing *8080* to *22* (which is the default SSH port), changing hostnamefrom "*list.hohoho*" to "*localhost"* and "*127.0.0.1*". Yet it still can't be accessed. But we found out the hostname can easily be bypassed. The one we will be using is "*localtest.me*", which resolves every subdomain to *127.0.0.1*. Therefore, we set the URL to "*http://10.10.7.71/?proxy=http://list.hohoho.localtest.me*", and it succeeded. Itappears a message from Elf McSkidy which contains Santa's password which is "*Be good for goodness sake!*" Then we entered the username and password we found into the admin form. Lastly, we *delete the naughty list* to find the challenge flag whichis "*THM{EVERYONE_GETS_PRESENTS}*"

Day 20: Blue Teaming - PowershELIF to the rescue
Tools used: Terminal
Solution/walkthrough:
Question 1
After connected to machine IP, login to the Windows machine using SSH command:
ssh mceager@10.10.180.153
pass: *r0ckStar!*

```
                          kali@kali:~
File  Actions  Edit  View  Help
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ ssh mceager@10.10.180.153
The authenticity of host '10.10.180.153 (10.10.180.153)' can't be established.
ED25519 key fingerprint is SHA256:X2ViBklLQoHmAsXFoem36jkL9faKH+Fr2lt2dd/kIWY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.180.153' (ED25519) to the list of known hosts.
mceager@10.10.180.153's password: █
```

Enter *powershell*

```
                 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> []        I
```

Change file location to *Documents*

Search for the hidden file using the following command:
Get-ChildItem -File -Hidden

View the hidden file using the following command:
Get-Content -Path e1fone.txt

Question 2

Change the file location to *Desktop* and search for the hidden directory using the
following command:
Get-ChildItem -Directory -Hidden

Change the file location to the hidden directory and list the files inside it using *Get-ChildItem* command

View the file.txt using *Get-Content*

Question 3

Change the file location to *C:\Windows\system32* and filter the hidden directory with number *3* by using the command:

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

Change the file location to the hidden directory and list the files inside it.

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

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

File  Actions  Edit  View  Help
PS C:\Windows\system32\3lfthr3e> Get-Content 1.txt | Measure-Object


Count    : 9999
Average  :
Sum      :
Maximum  :
Minimum  :
Property :


PS C:\Windows\system32\3lfthr3e> 
```

Question 5
Convert the *551* and *6991* by using the following 2 commands:
(Get-Content 1.txt)[551]
(Get-Content 1.txt)[6991]

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

File  Actions  Edit  View  Help
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)[551]
Red
PS C:\Windows\system32\3lfthr3e> (Get-Content 1.txt)[6991]
Ryder
PS C:\Windows\system32\3lfthr3e> 
```
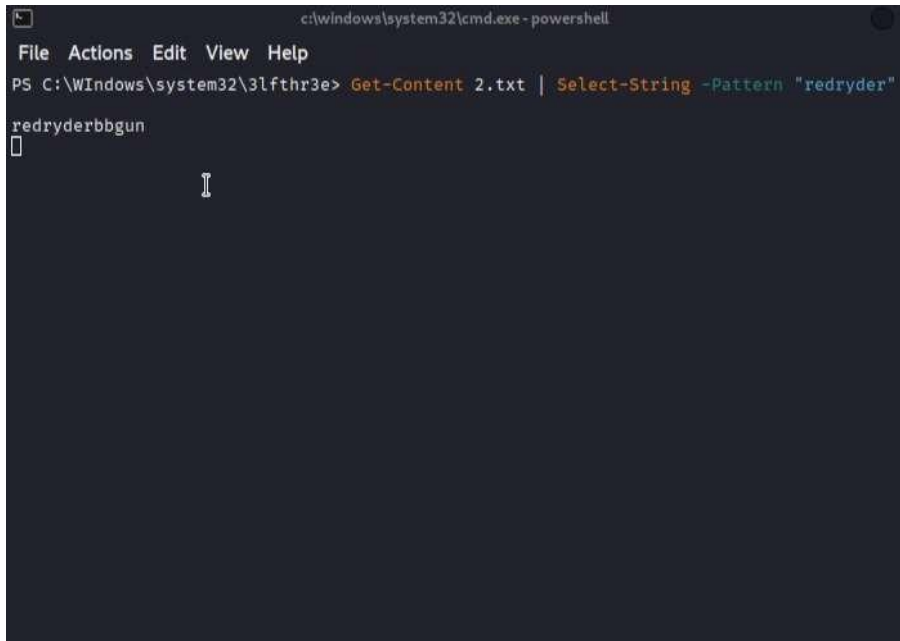
<u>Question 6</u>
Search the *2.txt* by using the following command:
Get-Content 2.txt | Select-String -Pattern "redryder"

Thought Process/Methodology:
After connecting and login to the Windows remote machine by using *ssh mceager@10.10.180.153* with the password(*r0ckStar!*), we are required to activate powershell mode by entering *powershell*. For the first question, we change the file location to Documents by using *Set-Location -Path C:\Users\mceager\Documents* or *cd Documents*. In *Documents*, search for the hidden file by the command *Get-ChildItem -Hidden -File* which the output is *e1fone.txt* and if we use the listing command *ls*, the output will be *elfone.txt* which is different. After we find the hidden file, we need to view the file using the command *Get-Content e1fone.txt* which the output is '*2 front teeth*'. For the second question, we must change the file location to *Desktop* first before we search the hidden directory which is *elf2wo* using the command *Get-ChildItem -Hidden -Directory*. Now change the file location to *elf2wo*, we will find the *e70smsW10Y4k.txt* by the command *Get-ChildItem* and then open the *.txt file* by command *Get-Content e70smsW10Y4k.txt* which the output is '*Scrooged*'. For the third question, we need to change the file location to *C:\Windows\system32* and filter the hidden directory with number *3* by the command *Get-ChildItem -Hidden -Directory -Filter "*3*"*. After that, we will see the directory named *3lfthr3e*. For the fourth question, we need to open the *3lfthr3e* directory to find the *1.txt* inside it and find the count by the command *Get-Content 1.txt | Measure-Object* which the outcome is *9999*. For the fifth question, we need to convert the 551 and 6991 inside 1.txt by the commands *(Get-Content 1.txt)[551]* and *(Get-Content 1.txt)[6991]*. Then, we combine the 2 outputs which result in 'Red Ryder'. For the sixth question, we search inside 2.txt by the command *Get-Content 2.txt | Select-String -Pattern "redryder"* and the output is *redryderbbgun.*