PSP0201

Week 5

Writeup

Group Name: hiSpec

Members

ID	Name	Role
1211101670	Nur Lycia Nisriena binti Razidy	Leader
1211101007	Aisyah binti Ahmad Kassim	Member
1211101073	Muhammad Adam bin Mazli Zakuan	Member
1211101619	Nik Syareena Aida binti Nik Ahmad Faizul	Member

Day 16 (Scripting): Where's Santa?

Tools used: Terminal, AttackBox, Nmap, nano, FireFox, Python3

Solution/walkthrough:

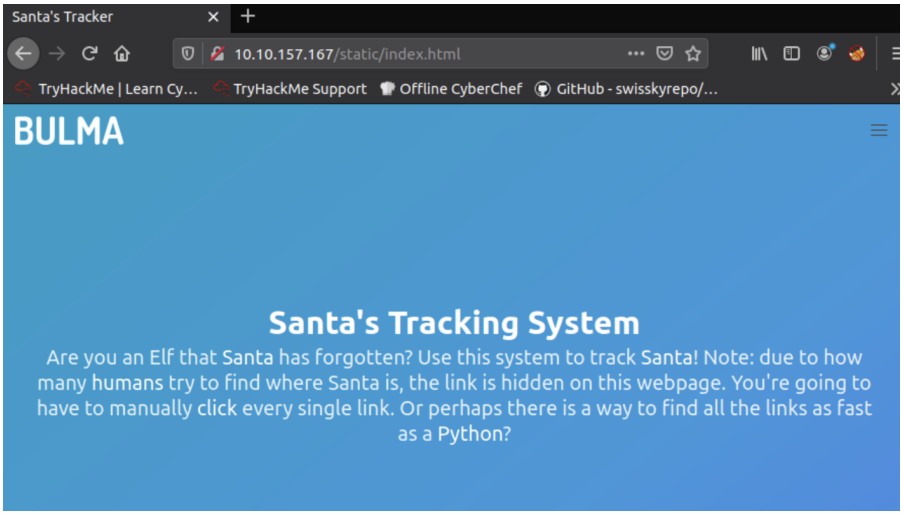
Question 1

Scan the machine IP address using nmap MACHINE_IP and we will see the web is running on port 80.

```
root@ip-10-10-13-118:~# nmap 10.10.49.145

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-08 09:40 BST
Nmap scan report for ip-10-10-49-145.eu-west-1.compute.internal (10.10.49.145)
Host is up (0.0014s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:9A:3D:A2:88:9B (Unknown)
```

Question 2

The template used is 'BULMA'



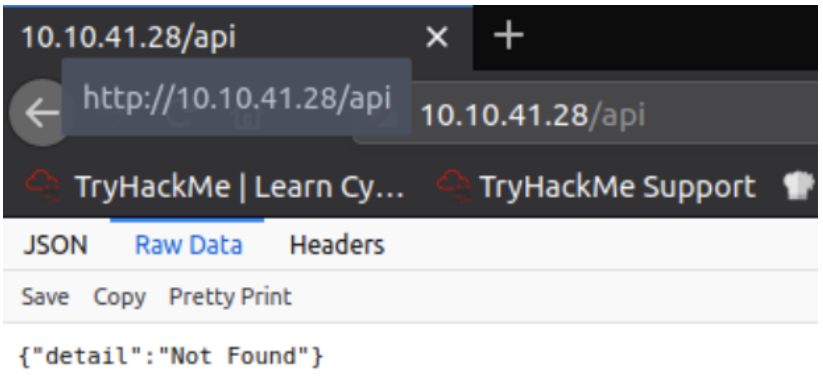
Question 3

Through the webpage given, view the page source and we will find the api directory.

```
<li><a href="#">Labore et dolore magna aliqua</a></li>
<li><a href="#">Kanban airis sum eschelor</a></li>
<li><a href="http://machine_ip/api/api_key">Modular modern free</a></li>
<li><a href="#">The king of clubs</a></li>
<li><a href="#">The Discovery Dissipation</a></li>
<li><a href="#">Course Correction</a></li>
<li><a href="#">Better Angels</a></li>
```

Question 4

Below is the raw data from the API endpoint without any parameter.



Question 5

From here, we could also see that the Santa is at Winter Wonderland, Hyde Park, London.

```
{"item_id":51,"q":"Error. Key not valid!"}
API Key:53
{"item_id":53,"q":"Error. Key not valid!"}
API Key:55
{"item_id":55,"q":"Error. Key not valid!"}
API Key:57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
API Key:59
{"item_id":59,"q":"Error. Key not valid!"}
API Key:61
{"item_id":61,"q":"Error. Key not valid!"}
```

Question 6

Create a python script using the command below.

```
root@ip-10-10-13-118:~# nano key.py
```

Follow the code below to obtain the correct api key.Then, save it.

```
  GNU nano 2.9.3                    key.py                          Modified

import requests

target_ip = '10.10.49.145' #machine_ip

for api_key in range(1,100,2):
        print(f'API Key:{api_key}')
        response = requests.get(f'http://{target_ip}/api/{api_key}')
        print(response.text)
```

Run the script.

```
root@ip-10-10-13-118:~# python3 key.py
API Key:1
{"item_id":1,"q":"Error. Key not valid!"}
API Key:3
{"item_id":3,"q":"Error. Key not valid!"}
API Key:5
{"item_id":5,"q":"Error. Key not valid!"}
API Key:7
```

Scroll down and we will see the correct api key (57).

```
{"item_id":51,"q":"Error. Key not valid!"}
API Key:53
{"item_id":53,"q":"Error. Key not valid!"}
API Key:55
{"item_id":55,"q":"Error. Key not valid!"}
API Key:57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
API Key:59
{"item_id":59,"q":"Error. Key not valid!"}
API Key:61
{"item_id":61,"q":"Error. Key not valid!"}
```

Thought process / methodology :

Firstly, we did a port scan to see which port the web is running on, (it is running on port 80).Secondly,from the web, we could see that the template used is 'BULMA'.To find the api directory, we will need to view the page source of the web.From there will see the directory is /api/. Next, we went to the API endpoint to see the raw data returned if no parameters were entered ({"detail":"Not Found"}).Lastly, to find the correct API key , we created a python script with the code given as above.Then , run the python script and we will find the API key (57) and Santa's location (Winter Wonderland, Hyde Park, London).

Day 17: Reverse Engineering - ReverseELFneering
Tools Used: THM Attackbox, Terminal, Nmap, Radare2
Solution/Walkthrough:

Question 1
Based on THM notes, we can match the data type with the size in bytes.

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

Question 2
Based on THM notes, the command to analyze the program in radare2 is “aa”.

> This will open the binary in debugging mode. Once the binary is open, one of the first things to do is ask r2 to analyze the program, and this can be done by typing in: `aa`

Question 3
Based on THM notes, the command to set a breakpoint in radare2 is “db”.

> A **breakpoint** specifies where the program should stop executing. This is useful as it allows us to look at the state of the program at that particular point. So let's set a breakpoint using the command `db` in this case, it would be `db 0x00400b55` To ensure the breakpoint is set, we

Question 4
Based on THM notes, the command to execute the program until we hit a breakpoint is “dc”.

> Running `dc` will execute the program until we hit the breakpoint. Once we hit the breakpoint and print out the main function, the rip which is the current instruction shows where

Question 5, 6, 7

Deploy the attack box and using the terminal, type out the command “ssh elfmceager@10.10.237.67” and key in the password given, “adventofcyber”.

```
root@ip-10-10-46-89:~# ssh elfmceager@10.10.237.67
The authenticity of host '10.10.237.67 (10.10.237.67)' can't be established.
ECDSA key fingerprint is SHA256:XrBuXSQs0wRKhvVRdrSfE/0F5ccAZQiXAhMhzB1dV7U.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.237.67' (ECDSA) to the list of known hosts.
elfmceager@10.10.237.67's password:
```

Next, using radare2 to analyze the “challenge1” file, type out the command “r2 -d ./challenge1”. Then, type out “aa”.

```
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1642 started...
= attach 1642 1642
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[0x00400a30]> aa
```

After the command is finished analyzing, type out the command “pdf @main” to examine the assembly code at main. There we can see three variables that are used to answer Question 5, 6 and 7.

For Question 5, we can see that the value of local_ch is “1”. Next, for Question 6, the value of eax when the imull is called is received by multiplying 1 with 6 to get the value “6”. Lastly, for Question 7, the value of local_4h before eax is set to 0 is “6”.

```
[0x00400a30]> pdf @main
            ;-- main:
/ (fcn) sym.main 35
|   sym.main ();
|           ; var int local_ch @ rbp-0xc
|           ; var int local_8h @ rbp-0x8
|           ; var int local_4h @ rbp-0x4
|              ; DATA XREF from 0x00400a4d (entry0)
|           0x00400b4d      55              push rbp
|           0x00400b4e      4889e5          mov rbp, rsp
|           0x00400b51      c745f4010000.   mov dword [local_ch], 1
|           0x00400b58      c745f8060000.   mov dword [local_8h], 6
|           0x00400b5f      8b45f4          mov eax, dword [local_ch]
|           0x00400b62      0faf45f8        imul eax, dword [local_8h]
|           0x00400b66      8945fc          mov dword [local_4h], eax
|           0x00400b69      b800000000      mov eax, 0
|           0x00400b6e      5d              pop rbp
\           0x00400b6f      c3              ret
```

Thought Process/Methodology:

For Question 1, 2, 3 and 4, we refer to THM notes given to answer the question. Next for Question 5, 6 and 7, we first deploy THM Attackbox and use the information given to log on to our Instance. Then, we use the radare2 command by typing out “r2 -d ./challenge1” and then, “aa” to start analyzing the file. Then, to examine the assembly code at main, we type out the command “pdf @main” and received three variables that can be used to answer Question 5, 6 and 7. In the assembly code, line 3, we get the value of local_ch, which is “1”. Then, we get the value of eax where we multiply 1 with 6 by referring to line 6 in the assembly code. Lastly, the value of local_4h can be received by referring to line 7.

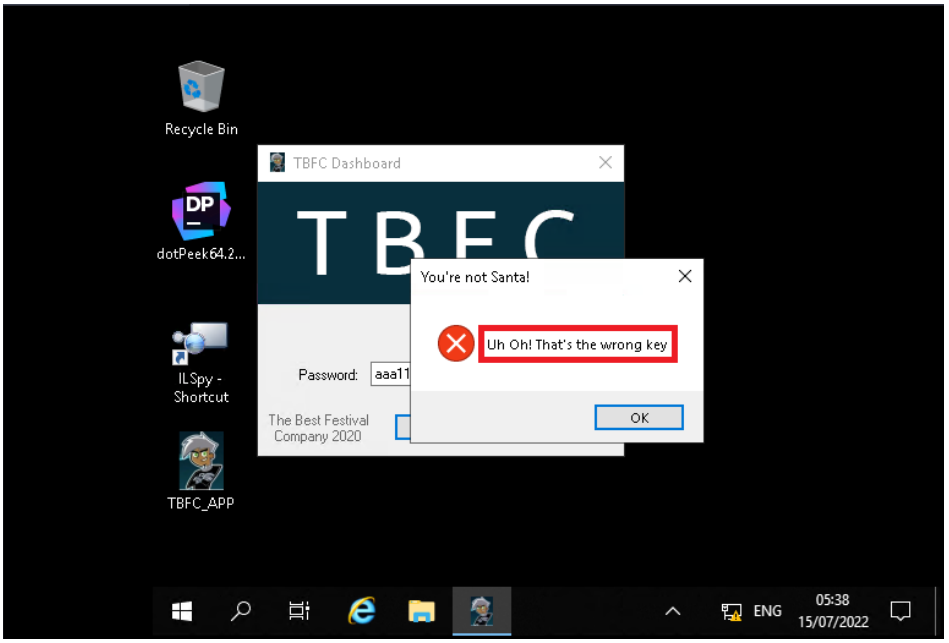
Day 18 (Reverse Engineering): The Bits of Christmas

Tools used: AttackBox, ILSpy, Remmina, CyberChef, TBFC

Solution/walkthrough:

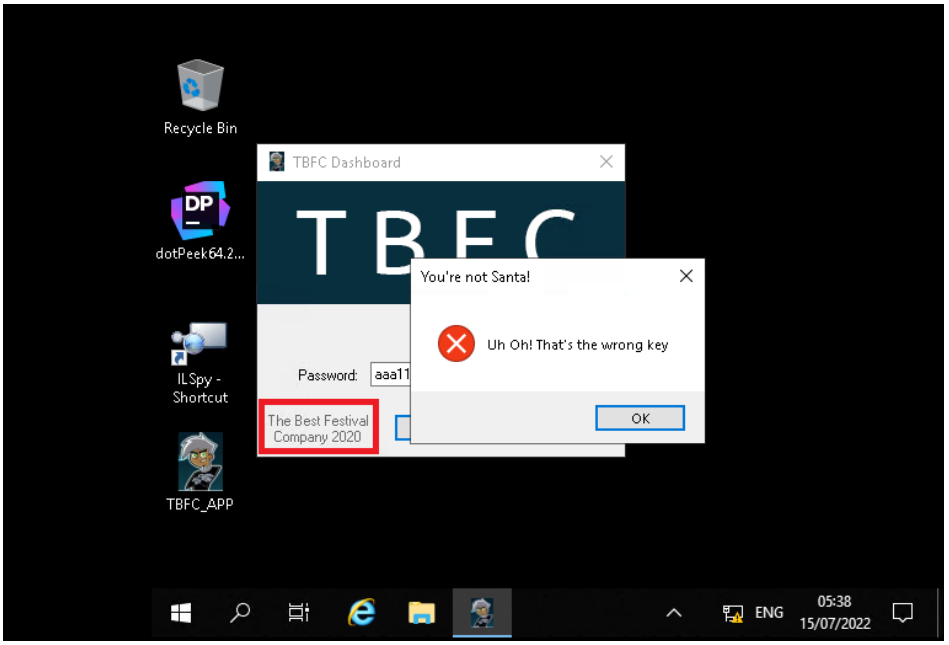
Question 1

Enter a random incorrect password. Then, we got **Uh Oh! That's the wrong key**



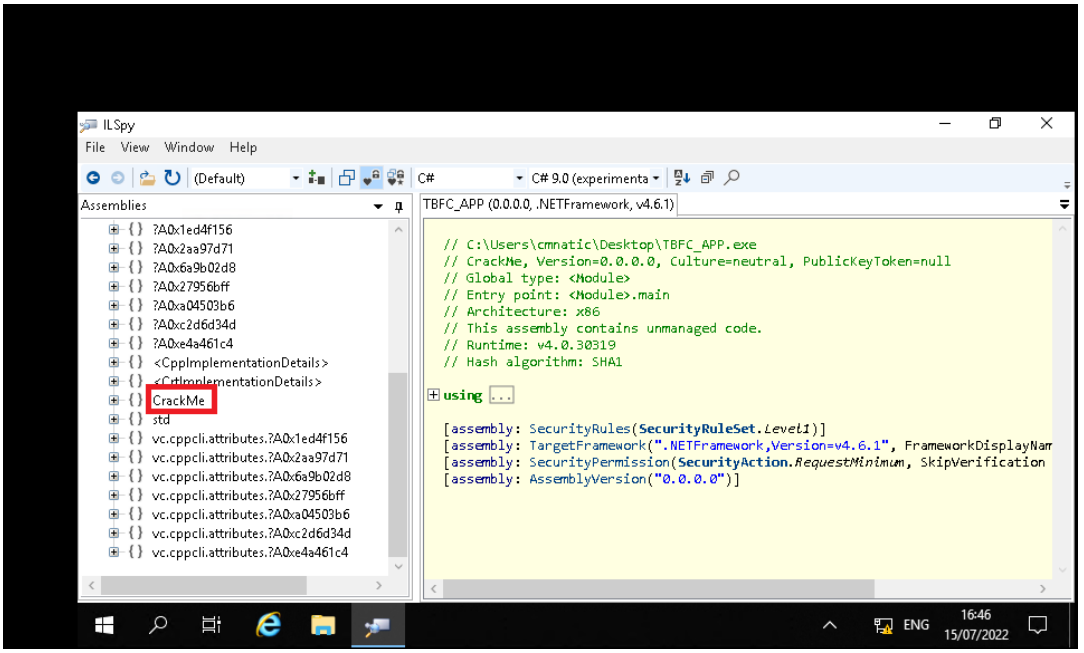
Question 2

From TBFC Dashboard, it shows that TBFC stand for The Best Festival Company 2020.



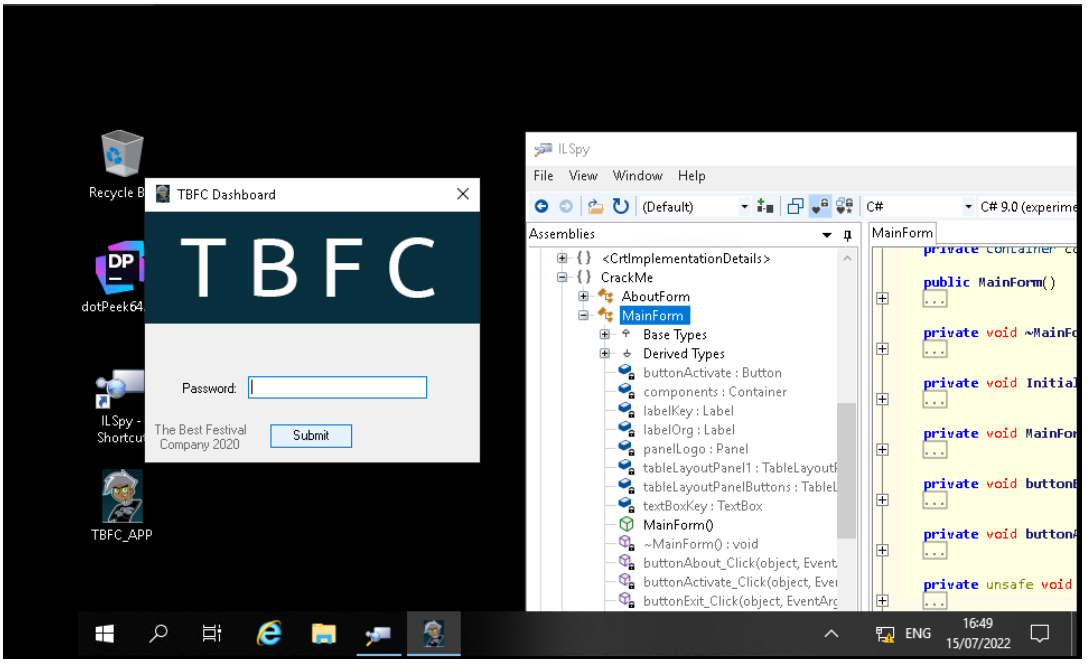
Question 3

The module that catches our attention is ‘CrackMe’.



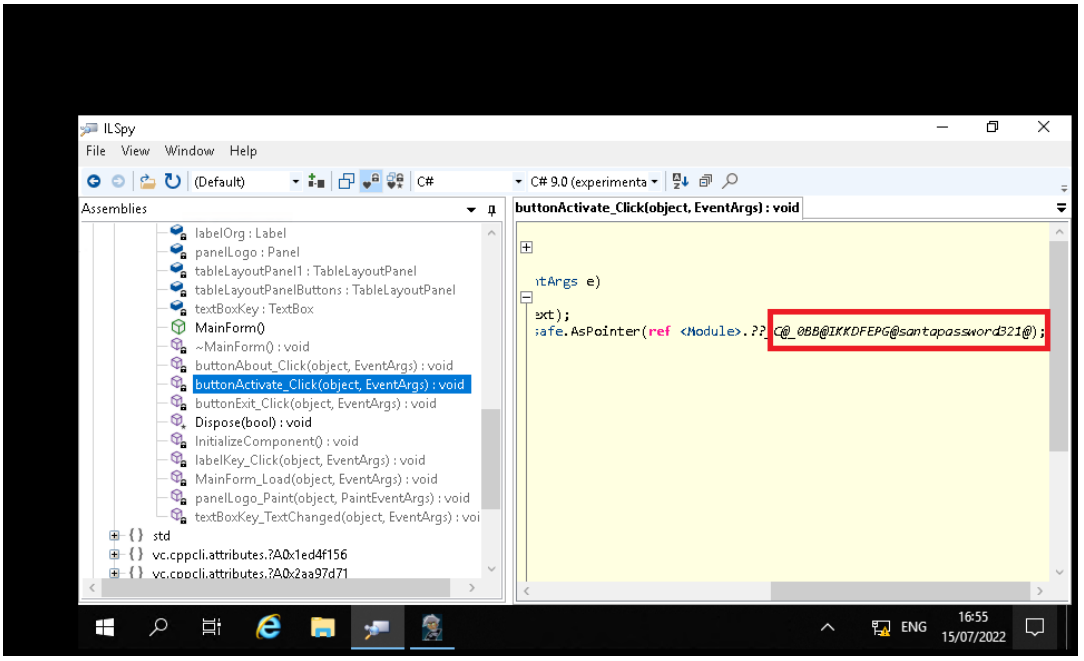
Question 4

Mainform is the form that has the information we are looking for, since it contains code for login system of TBFC app.



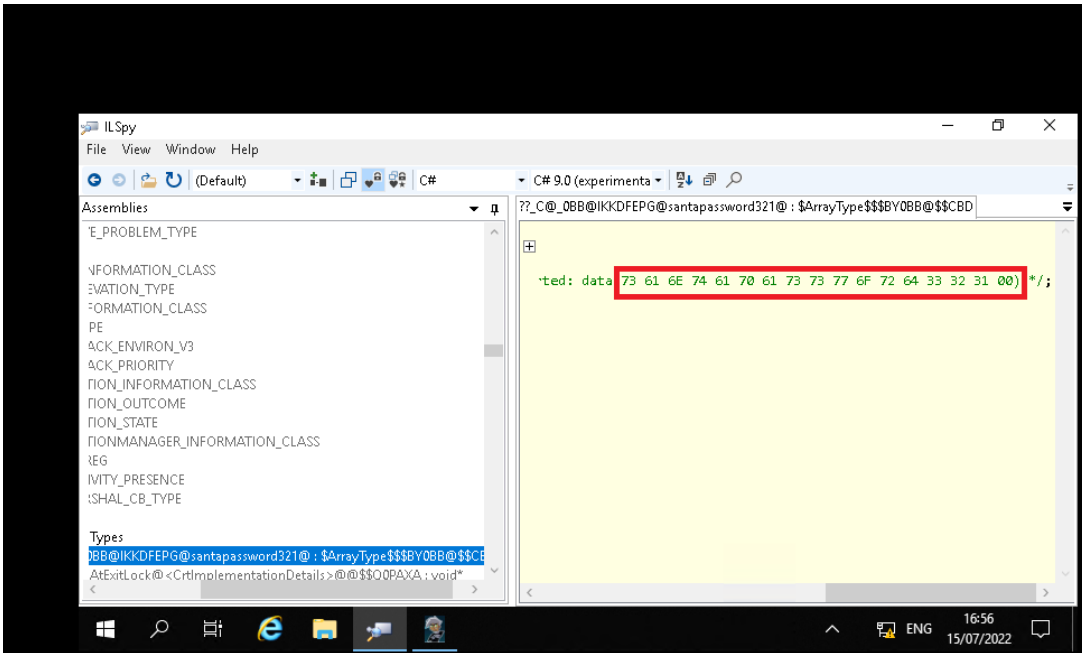
Question 5

The information that we need is in ‘buttonActivate_Click’ method. Click the code in the redbox

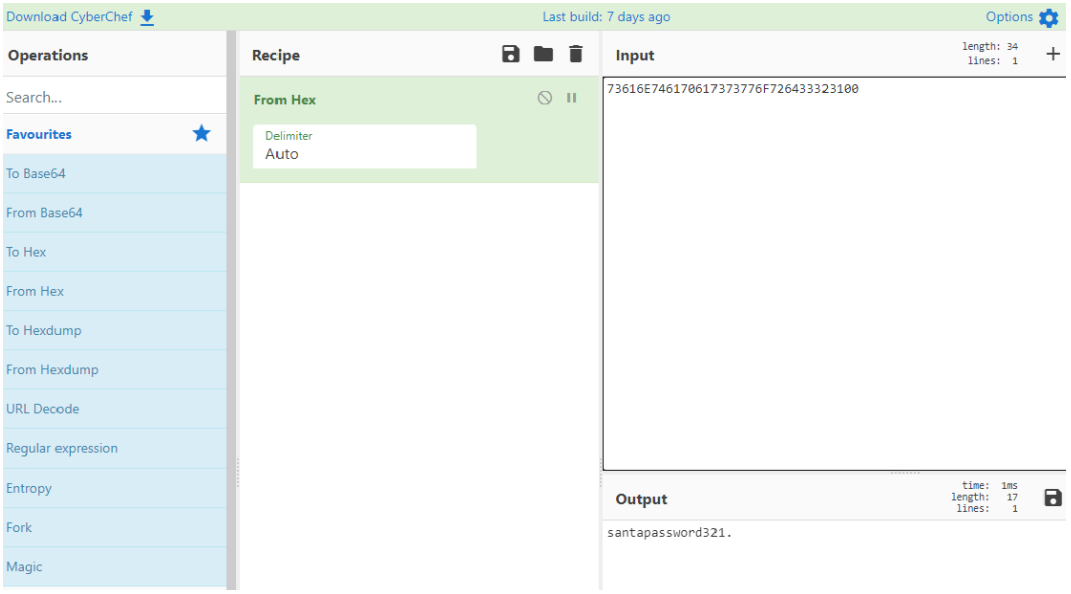


Question 6

Use CyberChef to decode hexadecimal code

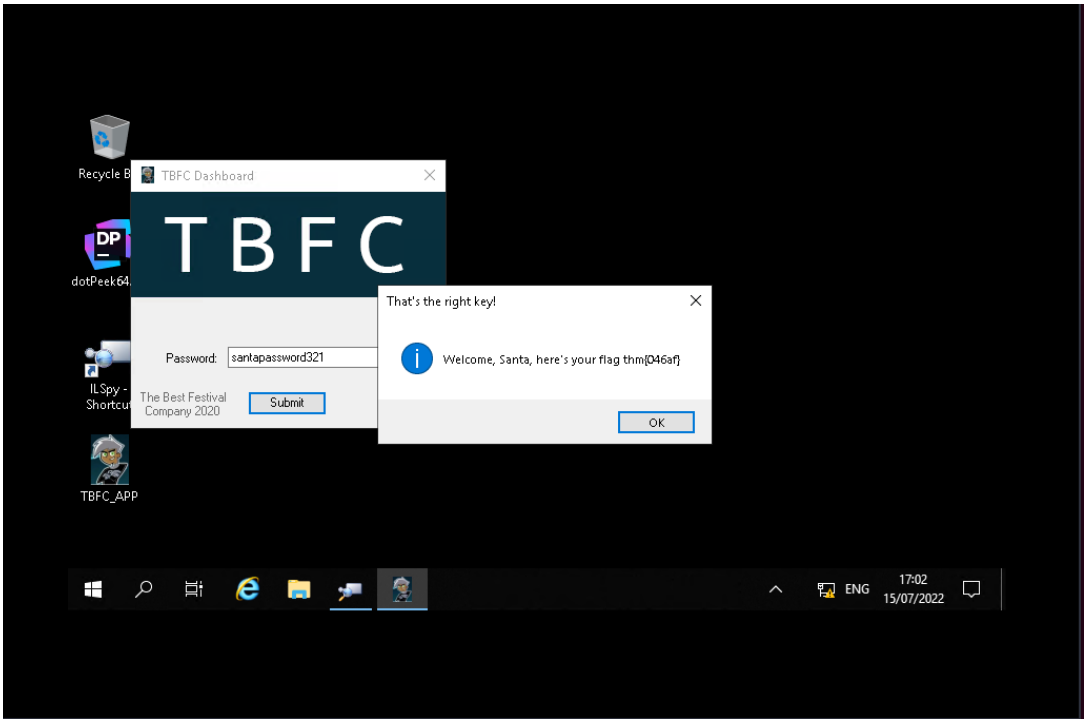


We will obtain the password from the decode. That the password is santapassword321.



Question 7

Enter the santa's password that we got and obtain flag thm{046af}.



Thought process / methodology :
Firstly, open the “Remmina” software. After logging in, the Remmina will run virtual Microsoft Windows. Run the “TBFC_APP” and enter a random word for the password thus the error message will appear. The meaning of “TBFC” can also be found at the bottom left of the TBFC Dashboard. Next, decompile the “TBFC_APP” by using ILSpy. Inside the assemblies of the ILSpy, there are many objects that make up the app and among them, “Crack Me” seems eye-catching. There are two modules inside which are “AboutForm” and “MainForm”. Since the button “Submit” will process the password, we need to search for objects related to button. “buttonActivate_Click” module stores the code of the process if we enter the correct password or wrong password. We can click the code as in the red box shown and we will be directed to the module that contains hexadecimal number. Decode the hexadecimal number using CyberChef thus we will obtain santa's password. Enter the password in the “TBFC_APP” and the flag will appear !

Day 19 (Web Exploitation): The Naughty or Nice List

Tools used: AttackBox, Mozilla Firefox

Solution/walkthrough:

Question 1

Enter a name from the name list (Tib3rius, Kanes, Ian Chai, YP, Timothy, JJ) in the name box to see who is in naughty/nice list.

The List

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

Tib3rius is on the Nice List.

Name:

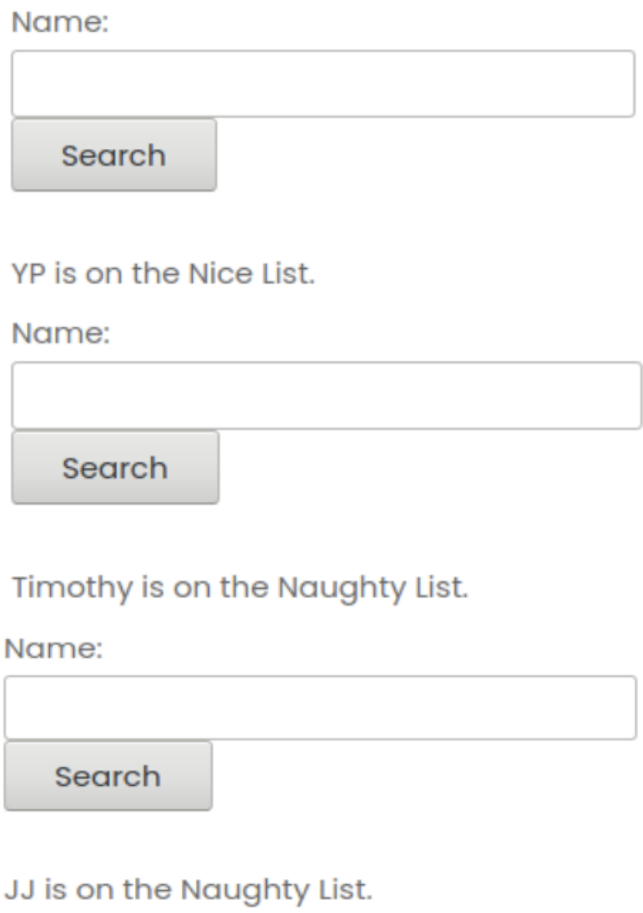
Search

Kanes is on the Naughty List.

Name:

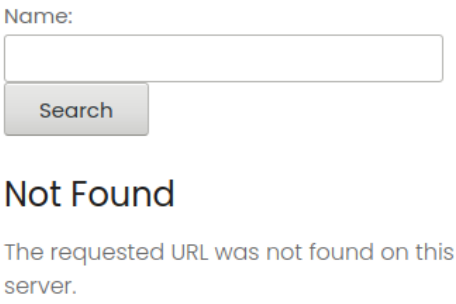
Search

Ian Chai is on the Nice List.



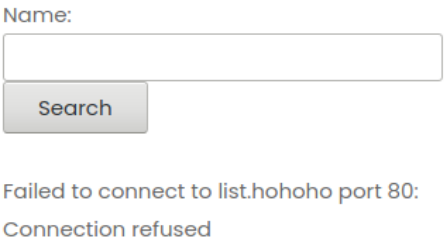
Question 2

Visit the root of the website (`http://10.10.254.47/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F`). The message below pops up.



Question 3

With the same URL, change the port to 80. (`http://10.10.254.47/?proxy=http%3A%2F%2Flist.hohoho%3A80`). The message says “Failed to connect to list.hohoho port 80: Connection refused”

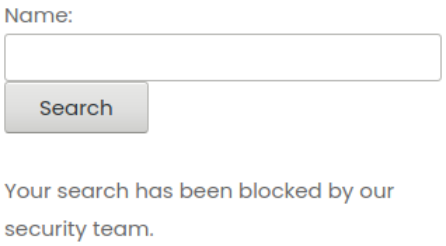


Question 4

Change to port 22. (`http://10.10.254.47/?proxy=http%3A%2F%2Flist.hohoho%3A22`) . The message now changes to "Recv failure: Connection reset by peer"

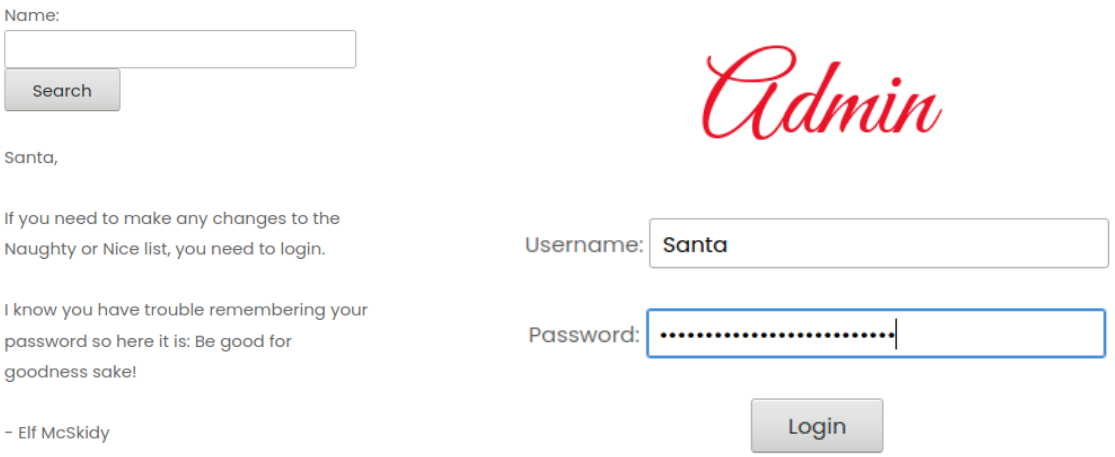
Question 5

Change the domain to localhost. (`http://10.10.254.47/?proxy=http%3A%2F%2Flocalhost`) .The web then says that “Your search has been blocked by oour security team”.



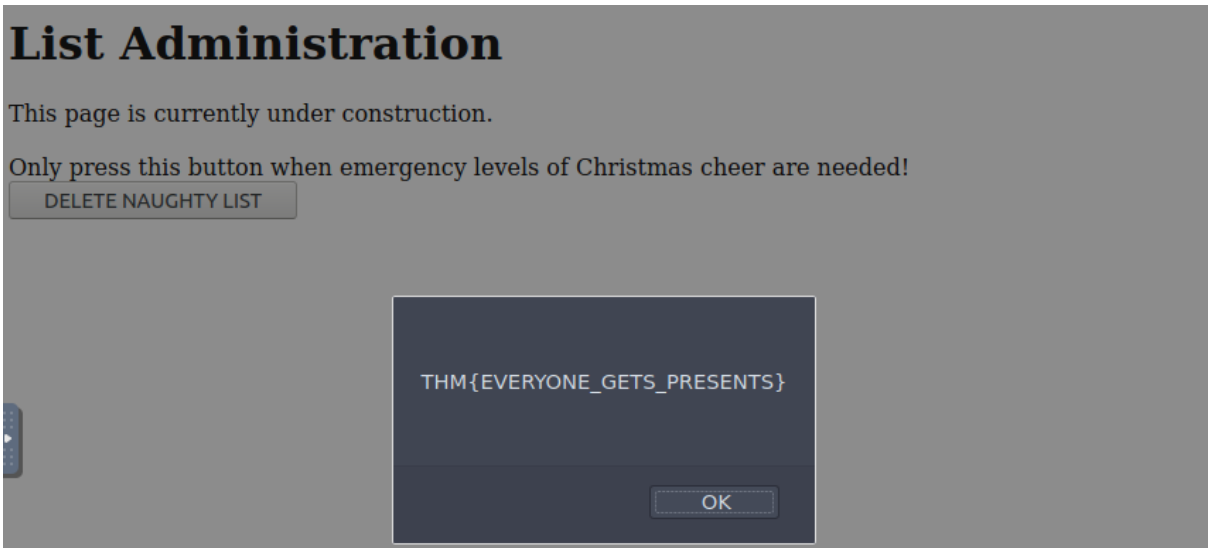
Question 6

Since the hostname should starts with "list.hohoho", and will block any hostnames that don't. Hence, set the hostname in the URL to "list.hohoho.localtest.me", and use “http://10.10.249.22/?proxy=http%3A%2F%2Flist.hohoho.localtest.me”. Then, we received the message left by Elf McSkidy that santa's password is “Be good for goodness sake!” and it is successful login with that password.



Question 7

Delete the naughty list and we will get the flag as below.



Thought process / methodology :

Open the URL <http://10.10.64.117/> since the target IP address is 10.10.64.117. Inside the webpage, try to enter any name such as "Tib3rius" to see whether the name belongs to the "Nice List" or the "Naughty List". Once we entered the name, URL will change to <http://10.10.64.117/**?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DTib3rius**>. We can try to visit the root of the website which is <http://10.10.64.117/**?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F**> but we will get "The requested URL was not found on this server." message instead. Next, try to change the port number to 80 <http://10.10.64.117/?proxy=http%3A%2F%2Flist.hohoho%3A**80**> and 22 <http://10.10.64.117/?proxy=http%3A%2F%2Flist.hohoho%3A**22**>. The results are "Failed to connect to list.hohoho port 80: Connection refused" and "Recv failure: Connection reset by peer" respectively. This time replace "list.hohoho" with "localhost" <http://10.10.64.117/**?proxy=http%3A%2F%2Flocalhost**> we will get "Your search has been blocked by our security team." Lastly, edit the URL to <http://10.10.64.117/**?proxy=http%3A%2F%2Flist.hohoho.localtest.me**> and now it works! The password is obtained and log in as Santa thus we will get the flag.

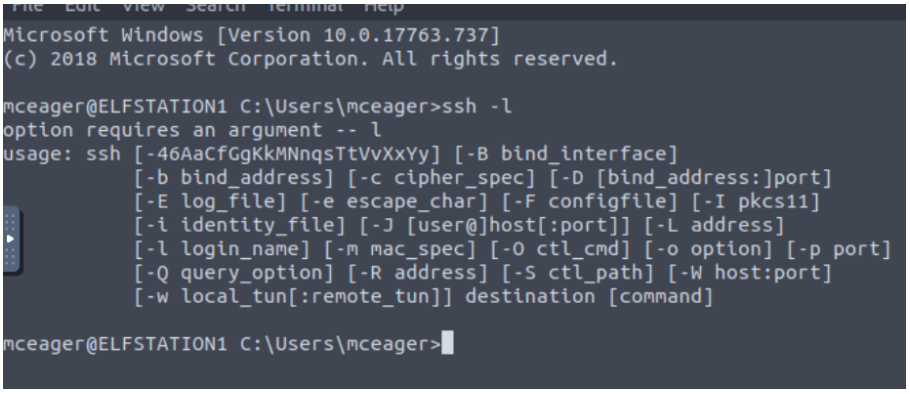
Day 20 (Blue Teaming): PowershELIF to the rescue?

Tools used: attackbox, terminal, PowerShell, SSH

Solution/walkthrough:

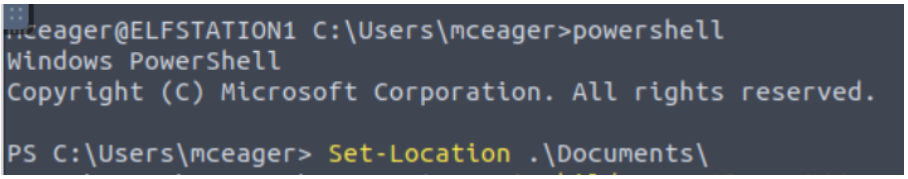
Question 1

After checking the ssh manual, parameter -l is for login_name.

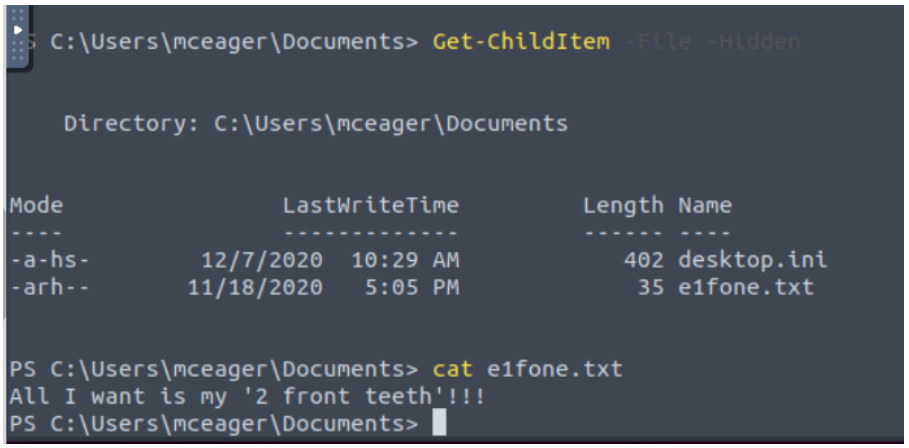


Question 2

Launch PowerShell and navigate to the Documents folder by using command Set-Location



Use the Get-ChildItem cmdlet to list the contents of the current directory and command -File -Hidden to get a list of files including the hidden one. Then, use the command cat to see the contents of e1fone.txt. The content is " All I want is my '2 front teeth'!!!".



Question 3

Set-Location .\Desktop\ . Use Get-ChidItem -Directory -Hidden to get list of directories including the hidden one from the desktop.

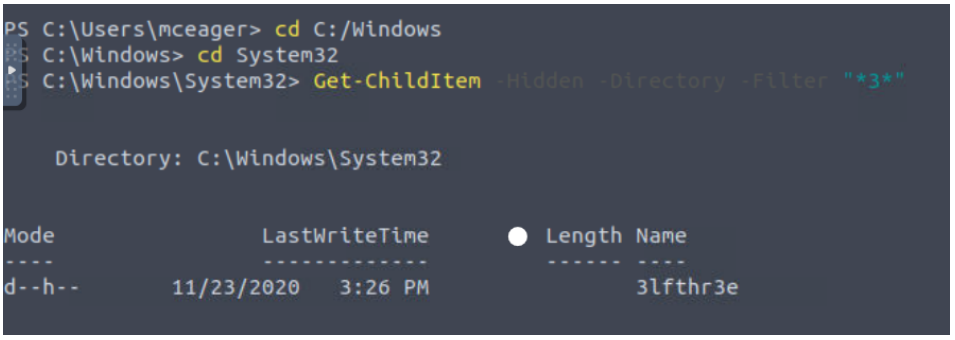
```
PS C:\Users\mceager\Desktop> cd..
PS C:\Users\mceager> Set-Location .\Desktop\
PS C:\Users\mceager\Desktop> Get-ChildItem -Directory -Hidden


    Directory: C:\Users\mceager\Desktop


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


PS C:\Users\mceager\Desktop>
```

Navigate to the .\elf2wo\ directory then use Get-ChildItem to see the file name. Use command Get-content e70smsW10Y4k.txt to read the content. So, the name of that movie that Elf 2 wants is Scrooged.

```
    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> Get-content e70smsW10Y4k.txt
I want the movie Scrooged <3!
PS C:\Users\mceager\Desktop\elf2wo>
```

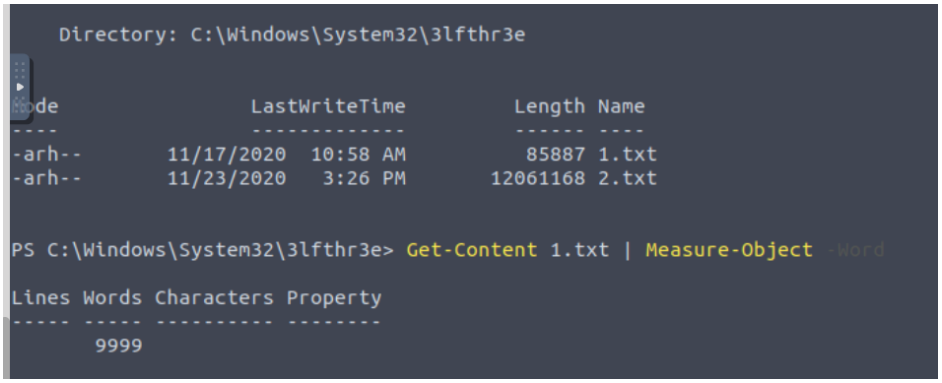
Question 4

Navigate to the Windows directory by using the command cd C:/Windows then to System32. Then, use Get-ChildItem -Hidden -Directory -Filter “*3*” to get a hidden folder that contains files for Elf 3. We used -Filter “*3*” to get the only list of directory that has 3.



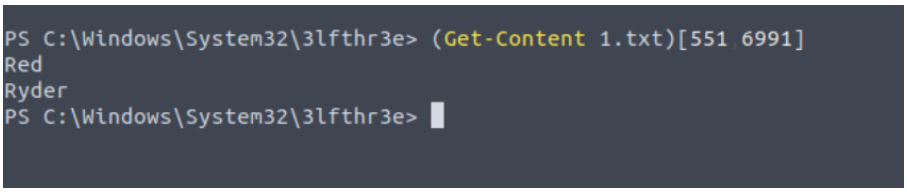
Question 5

After we get a list of file names from 3lfthr3e directory, run the command Get-Content 1.txt | Measure-Object -Word to measure how many words the first file contains. 1.txt file contains 9999 words.



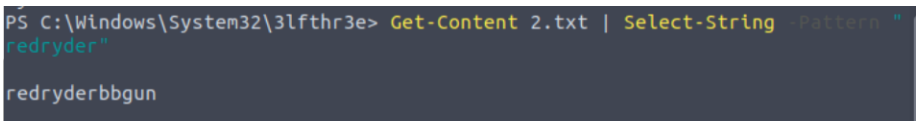
Question 6

Run command (Get-Content 1.txt)[551,6991] to get the contents from those 2 indexes from 1.txt file. The words that we get are Red and Ryder.



Question 7

Run command Get-Content 2.txt | Select-String -Pattern “redryder” to get content that has redryder from 2.txt file.



Thought process / methodology :

Firstly, we run command ssh -l mceager MACHINE IP to connect to the remote machine. After, we logged in successfully, launch powershell and navigate to the Documents folder. Use the Get-ChildItem -File -Hidden cmdlet to get a list of files including the hidden one. Next, change to desktop directory and get list of directories including the hidden one from desktop by using Get-ChidItem -Directory -Hidden . Then, navigate to the directory that we got so that we can get the file name. Use command Get-content e70smsW10Y4k.txt to read the content. Next, navigate to the Windows and System32 directories. Then, use Get-ChildItem -Hidden -Directory -Filter “*3*” to get the hidden list of directory that has 3 only. After that, run the command Get-Content 1.txt | Measure-Object -Word to measure how many words the first file contains. Then, we can run command (Get-Content 1.txt)[551,6991] to get the words from those index in 1.txt file. Lastly, we can also run command Get-Content 2.txt | Select-String -Pattern “redryder” to get only content that has ‘redryder’ word from 2.txt file.