PSP0201 Week 5 Writeup

GROUP NAME:GLHF

ID	NAME	ROLE
1211103400	Rohit	Leader
1211103299	Shuuban Subramaniam	Member

Day 16 - Help! Where is Santa?
Tools Used: Linux

Question 1

```
Discovered open port 80/tcp on 10.10.209.96
```

Question 2

Question 3

```
'http://machine_ip/api/api_key">
```

Question 4

```
'Error. Key not valid!"}
```

Question 5

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

Thoughts:
We accessed the machine, used nmap to find the port number and looked through the page source to get the api and then we used python loop to get the correct api key and we managed to track down santa.

Day 17: ReverseELFneering
Tools Used: Linux

Question 1

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

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`

Note, when using the `aa` command in radare2, this may take between 5-10 minutes depending on your system.

Question 3

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 run the `pdf @main` command again and

Question 4

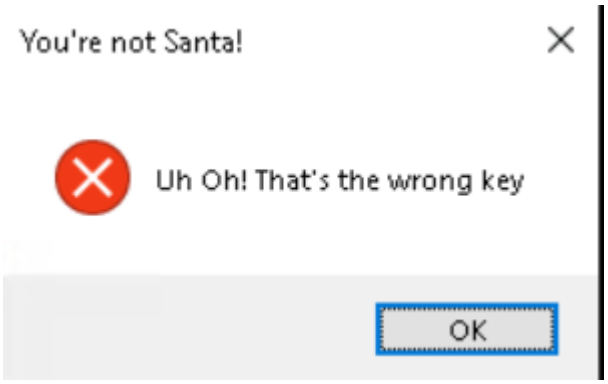
Running `dc` will execute the program until we hit the breakpoint.

Question 5

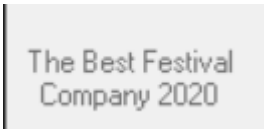
```
mov dword [local_ch], 1
```

DAY 18: The Bits Of Christmas
Tools Used: AttackBox

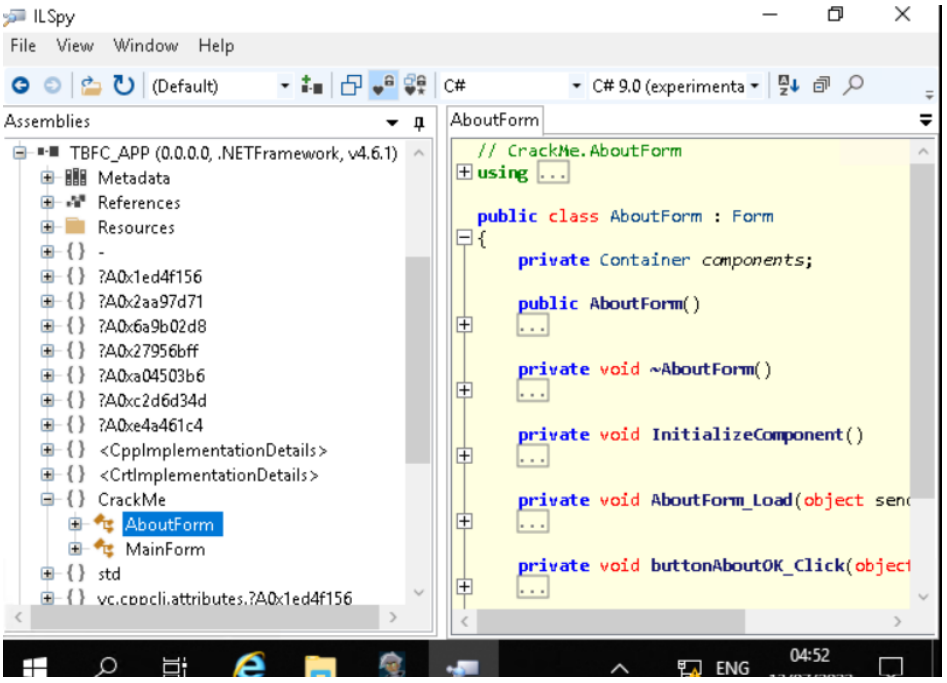
Question 1



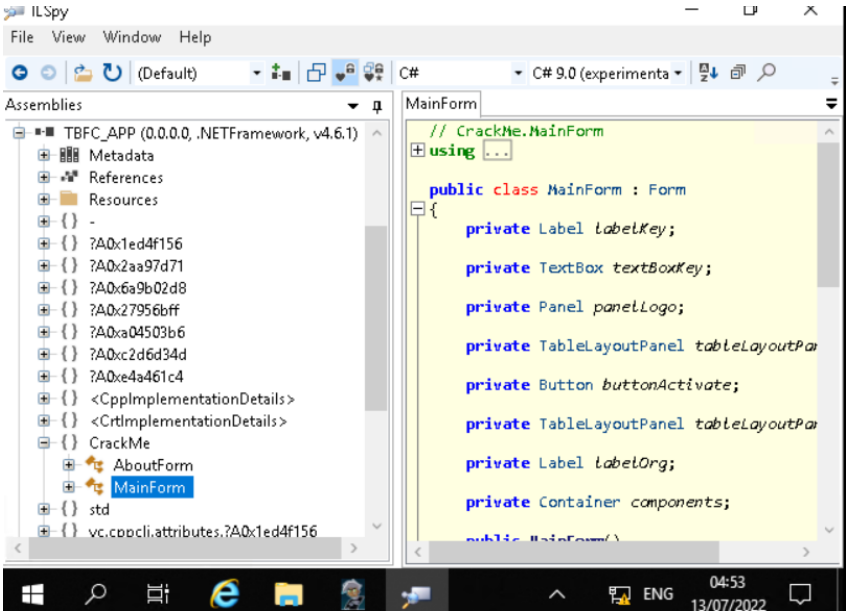
Question 2



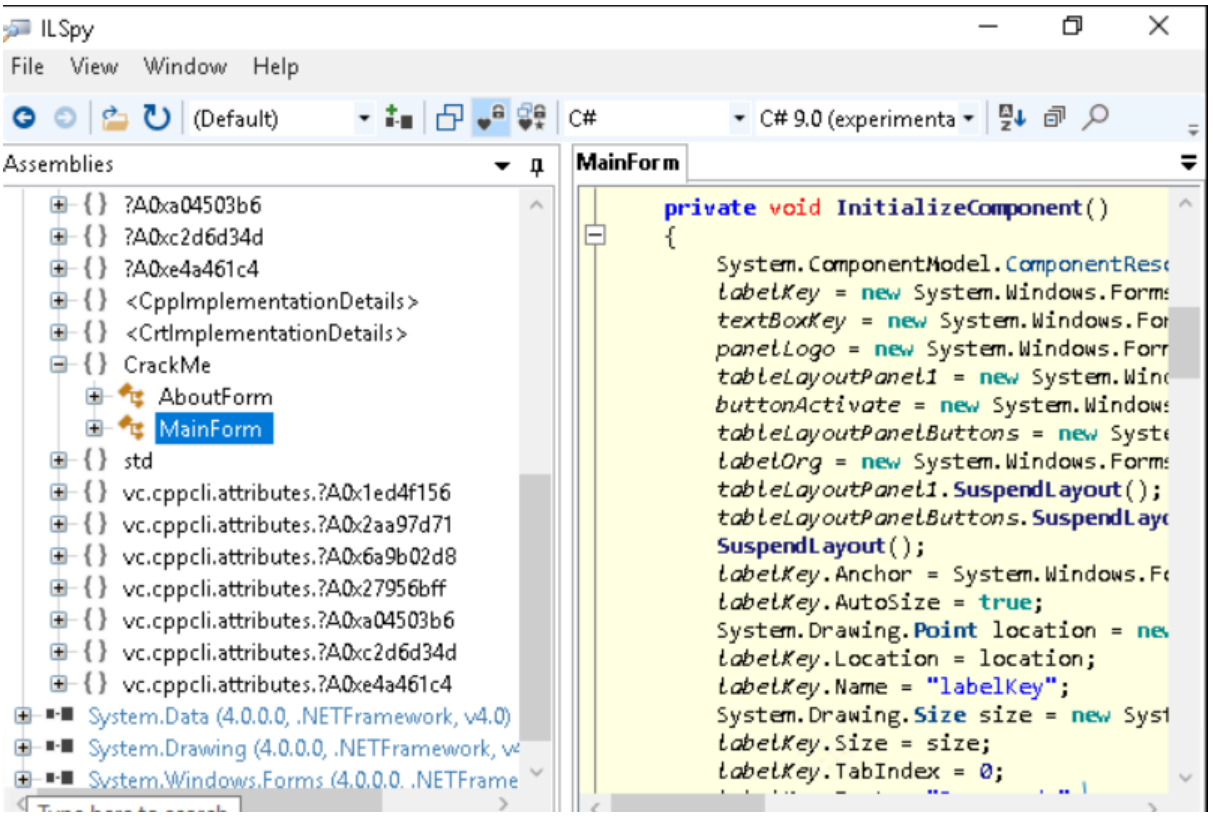
Question 3



Question 4



Question 5



Question 6

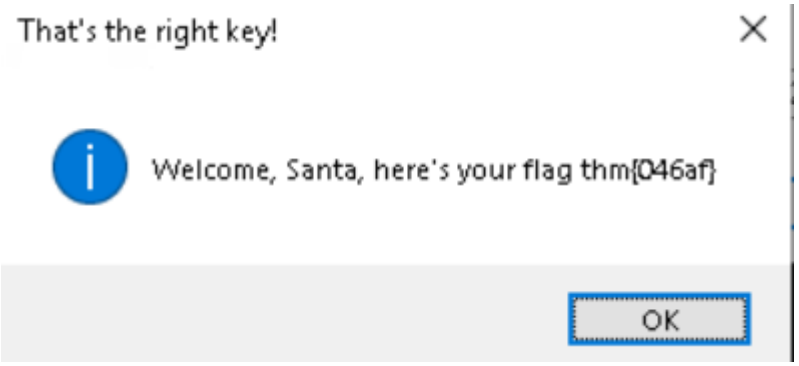
```
73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31
```

Output

time: 2ms
length: 16
lines: 1

```
santapassword321
```

Question 7



Thoughts: We Accessed Remmina and entered the ip given and entered to the virtual machine and clicked the tbfc app and we used the ILspy app and opened the tbfc app with the ilsply and managed to get the value, then we converted the value to word and got the password.

Day 19: The Naghty Or Nice List
Tools: Linux

Question 1

YP is on the Nice List.

JJ is on the Naughty List.

Tib3rius is on the Nice List.

Timothy is on the Naughty List.

Kanes is on the Naughty List.

Ian Chai is on the Naughty List.

Question 2

Not Found

The requested URL was not found on this server.

Question 3

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

Question 4

Recv failure: Connection reset by peer

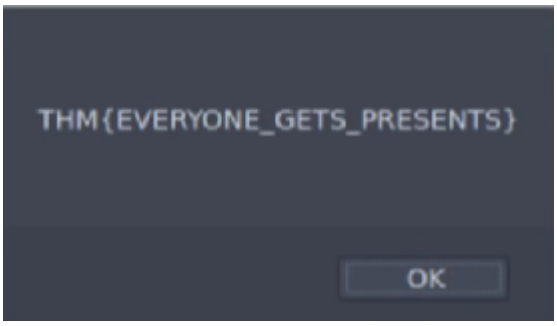
Question 5

Your search has been blocked by our security team.

Question 6

Be good for goodness sake!

Question 7



Thoughts :
We accessed the machine and tried all the links given and we changed the hostname to list.hohoho.localtest.me and got the password and deleted the naughty list.

Day 20: PowershELIF to the rescue
Tools Used: Attackbox

Question 2:

```
All I want is my '2 front teeth'!!!
```

Question 3:

```
I want the movie Scrooged <3!
```

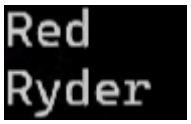
Question 4

```
3lfthr3e
```

Question 5

```
Words
-----
 9999
```

Question 6



Question 7

Thoughts: We accessed the machine and used powershell to access the documents and to get the answers.