Assignment 2

SID：12012919

Name: 廖铭骞

题目1 KFC crazy Thursday

题目描述：input something in shell to get the flag

分析

We can follow the steps

步骤

1. input 4 in the shell
2. input -1 as quantity
3. when the shell occurs, input `ls` to list all the file
4. then use `cat` to watch the `flag.txt` file
5. get the flag

Flag

```
flag{88f5cdf3-d7ce-46b4-9994-dd9a50855311}
```

题目2 Buffer overflow in heap

题目描述：A heap of the heap.

分析

We can follow the steps

步骤

1. Get the port and use `nc 10.20.55.12 port` to connect to server
2. use objdump to get the GOT's position
3. write GOT of the function `cout` and redirect to the function named "call_me"
4. send info '2' or '4' to push the server call the `cout`, then trap in `call_me`.
5. Use `ls` to list all the files, and use `cat` to catch the flag

Flag

flag{fd971856-08e0-425b-acdc-50c01ae7102d}

flag{fd971856-08e0-425b-acdc-50c01ae7102d}