Homework – 6

- I downloaded Docker toolbox for windows 10.
- After running the .exe file, Docker Quickstart Terminal was installed.
- Then as per the instructions provided in the assignment, I built the IST 543 dockerfile and gave it privilege.

```
MINGW64:/c/Users/sp226/Desktop/problem_set_6

docker is configured to use the default machine with IP 192.168.99.100
For help getting started, check out the docs at https://docs.docker.com


Start interactive shell

sp226@Batman MINGW64 /c/Program Files/Docker Toolbox
$ cd ..

sp226@Batman MINGW64 /c/Program Files
$ ls
'Common Files'/       Java/                  'Rivet Networks'/              'Windows Portable Devices'/
Dell/                 McAfee/                'Uninstall Information'/       'Windows Security'/
desktop.ini           McAfee.com/            'Windows Defender'/            'Windows Sidebar'/
'Docker Toolbox'/     'Microsoft Office'/    'Windows Mail'/                WindowsApps/
Git/                  'Microsoft Office 15'/ 'Windows Media Player'/        WindowsPowerShell/
Goodix/               ModifiableWindowsApps/ 'Windows Multimedia Platform'/
Intel/                Oracle/                'Windows NT'/
```

```
MINGW64:/c/Users/sp226/Desktop/problem_set_6
Links/                 Searches/
'Local Settings'@      SendTo@
MicrosoftEdgeBackups/  'Start Menu'@
Music/                 Templates@
'My Documents'@        Videos/
NetHood@               'VirtualBox VMs'/
NTUSER.DAT

sp226@Batman MINGW64 ~
$ cd Desktop

sp226@Batman MINGW64 ~/Desktop
$ ls
'~$pics of interest.docx'  desktop.ini  Doc/  ghidra_9.1.2_PUBLIC/  problem_set_6/  problem_set_6.tar

sp226@Batman MINGW64 ~/Desktop
$ cd problem_set_6

sp226@Batman MINGW64 ~/Desktop/problem_set_6
$ ls
build/  Dockerfile  problem_set_6.txt  pseudocode/

sp226@Batman MINGW64 ~/Desktop/problem_set_6
$ docker buid . -t ist543:problem_set_6
unknown shorthand flag: 't' in -t
See 'docker --help'.

Usage:  docker [OPTIONS] COMMAND

A self-sufficient runtime for containers
```

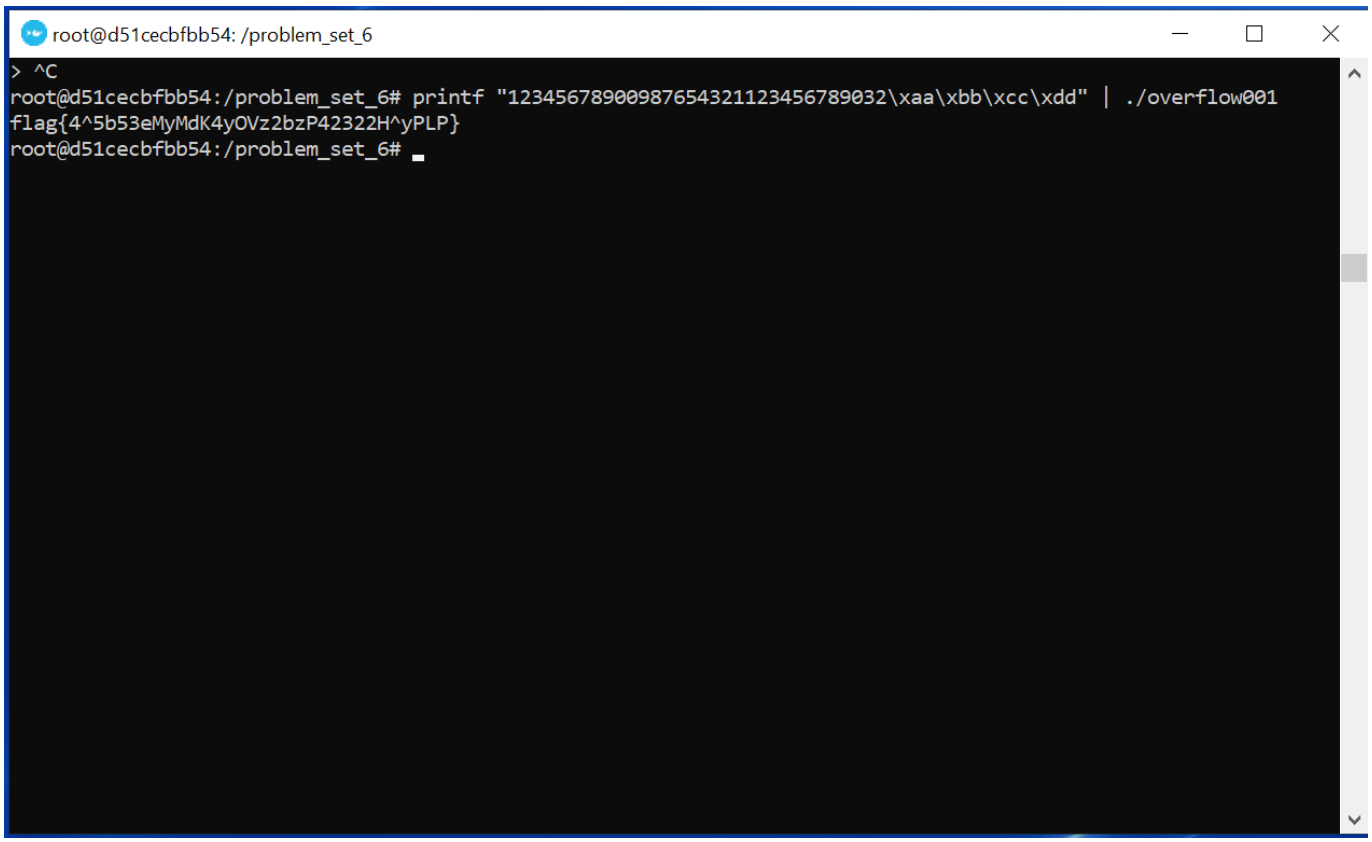
Overflow000

1. Run the code
2. According to the code, an array of 32 places is initialized in the memory stack.
3. Now in order to overwrite the value of key, we need to input 32 random values and the 33rd value will be the key.
4. To catch the flag, the value of key should be 1
5. Thus entering the 33rd place vale as 1, we retrieve the flag.

```
root@d51cecbfbb54: /problem_set_6
8
9
0
1
2
3
4
5
6
7
8
9
0
0
9
8
7
6
5
4
3
2
1
1
2
1
flag{216^742Ryv30RHLRJx6JOT6SR235HLO2}
root@d51cecbfbb54:/problem_set_6#
```

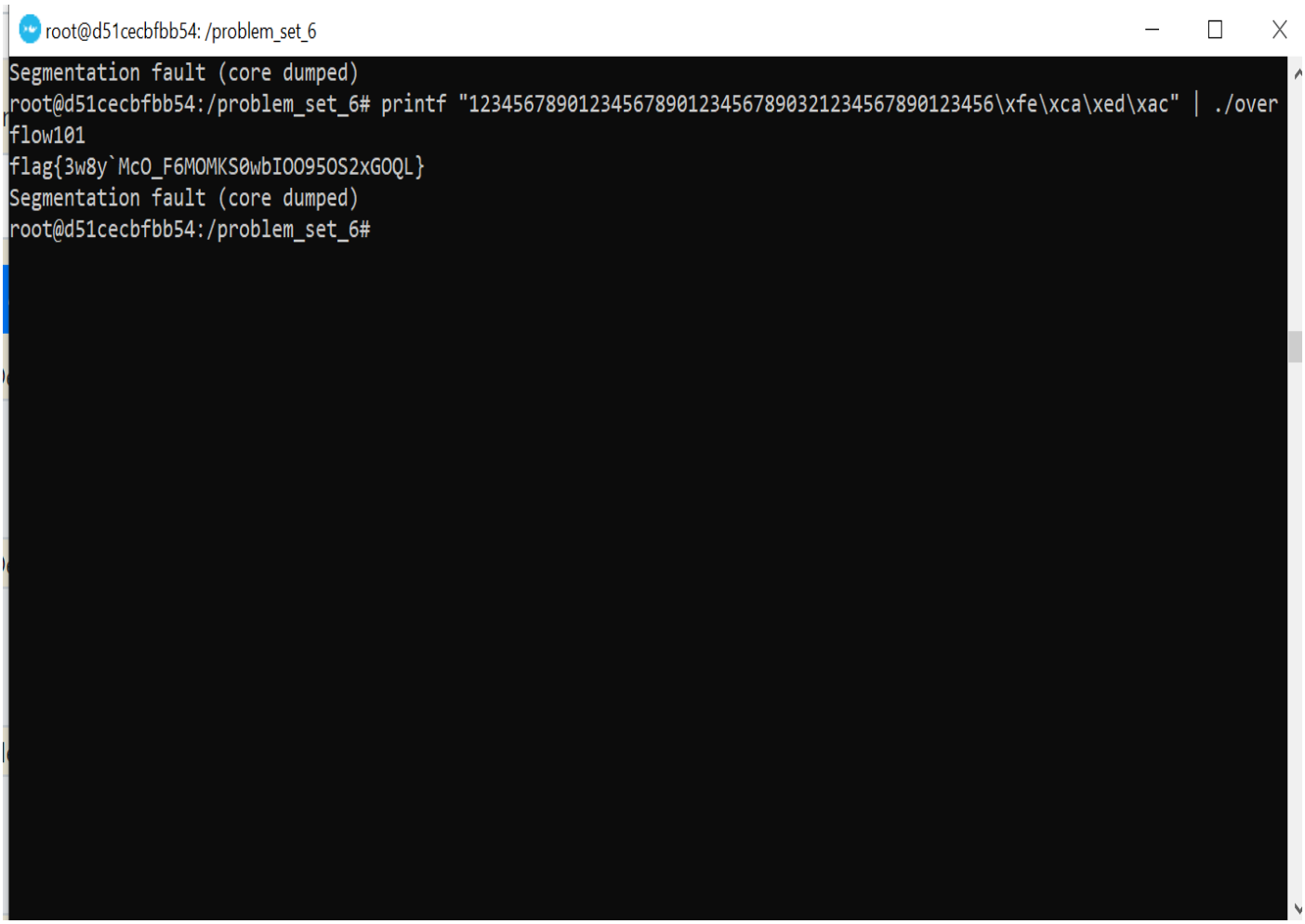
Overflow001

1. In the code, there is a character string array with 32 places.
2. The function is to read until the 36th place in the stack memory.
3. So the value of key is given in hexadecimal, and from the code it is realized that the four places from 33rd to 36th is the key.
4. Which means in the stack, in order to catch the flag we need to enter the value of key like this: aa, bb, cc, dd.
5. Thus after entering 32 random values, we overwrite the key and catch the flag.



Overflow002

1. From the code, we can see that in a stack, there is an array with 32 bytes, then a single byte short x, a single byte character y and then a single byte character key.
2. Since the order of inouts after array is not defined, we are going to assume that the key can be in either of the three places namely, 33rd, 34th or 35th.
3. Thus, we enter random values until 32 places.
4. At the 33rd place, we need to enter value of key thrice and convert it to decimal, so that in all the three places, we can overwrite the key.
5. So, since array accepts value in int, and there are 8 bits in it. Converted 000010 000010 000010 into decimal and got 657930.
6. If we enter this value, we get the flag.



Overflow101

1. There is a character string array of 32 values to be stored.
2. The key is of int type so 2 bytes or 16 bits memory in the stack.
3. After putting in 32 random values in the stack, to reach the key, we need to put in 16 bits more of garbage value to overwrite key.
4. Thus after 32+16 entries, we can enter key value in reverse order in pairs.
5. Thus we catch the flag.