**ITCS 461 Computer & Communication Security Date : ­­­\_\_\_\_19/02/2023\_\_\_\_\_\_**

**ID: 6388014 Name: Waris Damkham Section :** \_\_\_\_\_\_\_2\_\_\_ **\_\_\_\_\_\_**

Save this answer sheet as “ **Lab5-63xxxxx.docx**” (Removing all figures will help reduce the file size).

Submit this file to the lab folder in e-learning website according to your session.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Lab 5 : Buffer Overflow**

Follow 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 decimal 1432778632 , in hex 55667788
   5. address of “name”: 0022FDF0
   6. address of “secret\_function”: 00401505
2. What is the name you enter? Waris
3. Is the length of the name program printed out is the correct length? Y (Y/N)
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:**

1. How long is the input string that starts to change value of variable “b”? 200
2. Capture the screen when “b” starts to change.

Text

Description automatically generated

1. How long is the input string that starts to change value of variable “a”? 204
2. Capture the screen when “a” starts to change.

Text

Description automatically generated

1. What is your input string (or your python command) that can change variable “a”

to 0xDEADC0DE? python -c "print('A'\*204 + '\xDE\xC0\xAD\xDE')"|Lab5.exe

1. Finally, capture the screen to show that you have bypass the value checking.

Text

Description automatically generated

**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.)

1. What is starting address of variable “name” 0022FDF0
2. How long of your input string that starts to make the program crashes? 220
3. Append your current input string with the address of “secret\_function” to overwrite the “return address” value. (hint: backwards, in hex)

python -c "print('C'\*220 + '\x05\x15\x40\x00')"|Lab5.exe

1. Capture the screen when you manage to execute the “secret\_function”.

Text

Description automatically generated

1. 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!