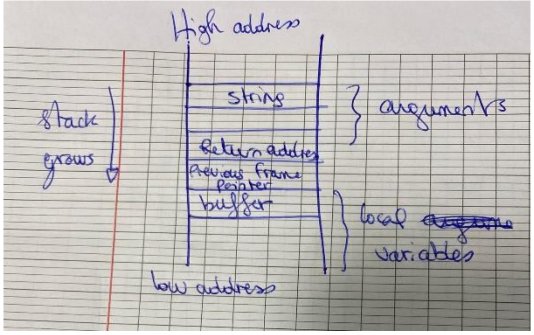
Assignment 6 – ECE 1155

Rayan Hassan – 4511021

Question 1

“i” is a global variable located in data segment. The pointer and the buffer are located in stack. The local variable “j” is also in stack. The static integer “y” is stored in BSS segment.

Question 2



Question 3

Buffer overflow is when we add data to a buffer surpassing the maximum limit it can hold.

In the previous code, strcopy doesn’t check the length of the inputs, so if it’s bigger than the capacity of the buffer, it will overflow.

Question 4

The consequences might be that an attacker crashes the program or gains control over it. Specifically, the attacker might change the address to point at a malicious code and executes it.

Question 5

NOP sled is a series of NOPs used to advance the program counter, which results in change of instruction execution of the CPU. They are used to “hide” the malicious code: we won’t be able to tell where the start of the malicious code is.

Question 6

Countermeasures to buffer overflow (mitigation) are ways to prevent it from happening or overcoming it. Non-executables are an example of that (NX). They work by preventing the processor from executing anything stored in the area marked as NX. Canary is another example used by stack-guard. Compiler adds a random value called canary below return address and saves it in another place, not the stack. Finally, ASLR (address space layout randomization) makes the start address of the stack random which makes it difficult to guess %ebp.

Question 7

a) The vulnerability here is that there is no information about the pointer *to so buffer overflow can occur.

b) we can simply write and if statement between the fread lines

if (len>size)

    # there is no more space, so no writing

    return 0

Question 8

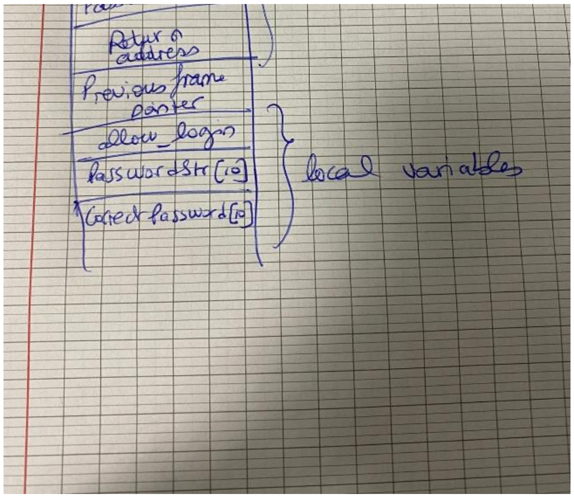
a) If “len” value is greater than the size of the array, we can have buffer overflow. Also “pos” should be positive because index starts from zero

b) we can write first if pos<0 {pos=0}

and also if (len>size-pos){//recalculate value of len to avoid buffer overflow}

Question 9

a)



b) Yes there is a vulnerability because of the function gets which doesn’t check for boundary. So for example an attacker can write a very long password which exceeds capacity, and overwrites all memory locations, specifically CorrecPassword. This will cause CorrectPassword = Password = NULL and therefore the signing in will be permitted.