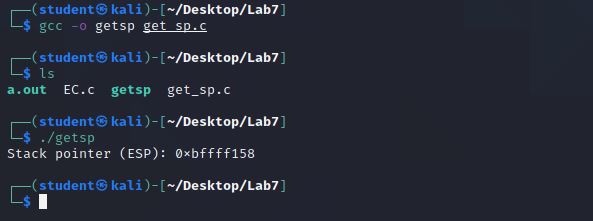
Xuan(James) Zhai

CS3339 Lab

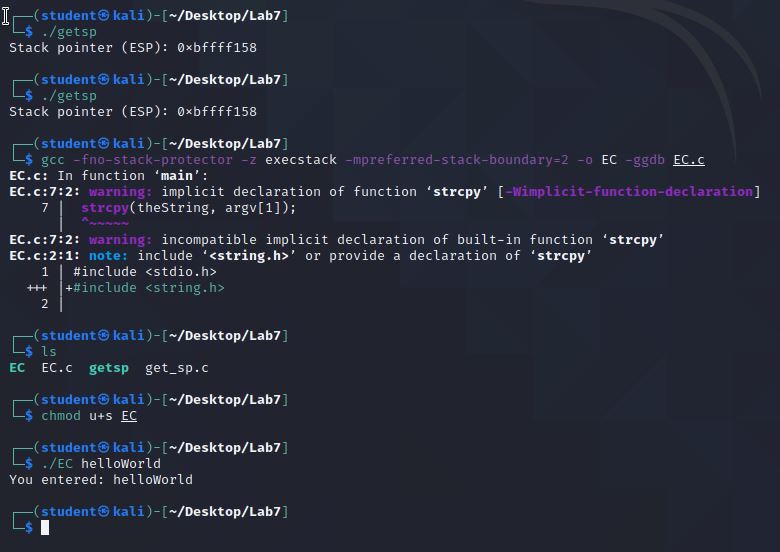
April 16th, 2021

CS 3339 - Lab 7 - Lab Report

1: Get stack pointer

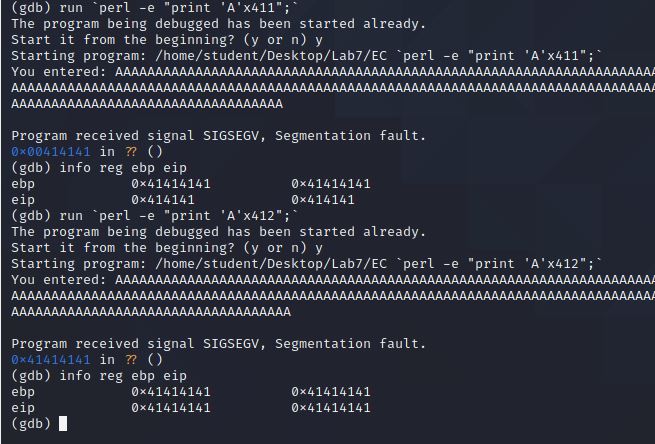


2: Check EC & get\_sp



3: Find the number of overwrite.





4: Open the terminal



5: What are some malicious ways this attack could be used?

Since the Buffer Overflow may overwrite other parts of the program or even things at the outside of the program, an attacker could overwrite parts of the program they shouldn’t have access to and even get program to execute their own code.

6: How could you protect against this type of attack?

The attack should be prevented at the beginning. For example, the development should use a memory safe language with kernel memory protection. Also, if the program requires a user to enter an input, the program needs to have some error-check mechanism to prevent input get out of bound.