Ethan Sorrell
CS-591 Assignment 2

I found that the provided accuse.c program was vulnerable to a buffer overflow attack. My input assumed that the program was compiled for a 32-bit linux system with ASLR disabled and flags to disable stack protectors and allows execution of code in the stack. The program could be exploited by providing input that would write past the provided 256 byte buffer for victim in order to manipulate the stack. Because of the way that the stack is structured, after writing a few bytes past the buffer we reach the return address for main. I found that this address was like a double pointer, and that I had to write an address containing the address that I wanted to begin execution at. This address of execution was within victim, which we had provided the input for. I filled the beginning of victim with NOP instructions to give myself a wider range of addresses to hit. I then had shellcode that would print the desired output. I then wrote a filler character that getchar would overwrite with '\0'. This exploit could be patched by replacing the get_line function with a call to fgets.