Chan Ng Cashin

ECE404

HW10

A screenshot of a computer

Description automatically generated

Here is the string that caused a buffer overflow. I found this by setting a breakpoint at the end of clientComm and then continuing past that address until I found where multiple A’s were being printed. Once that was found I determined through further investigation that 40 leading A’s were needed before the address of the start of secret function was inputted. After inputting these A’s followed by the start address of secretFunction the string caused a buffer overflow.

A computer code with text

Description automatically generated

This was the few lines of code I added to server.c that prevented the buffer overflow. This way the sender buffer size address that the client sends will never exceed the data size of the server and a buffer overflow won’t occur.

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

Here are some email logs from my mail spam mail account.