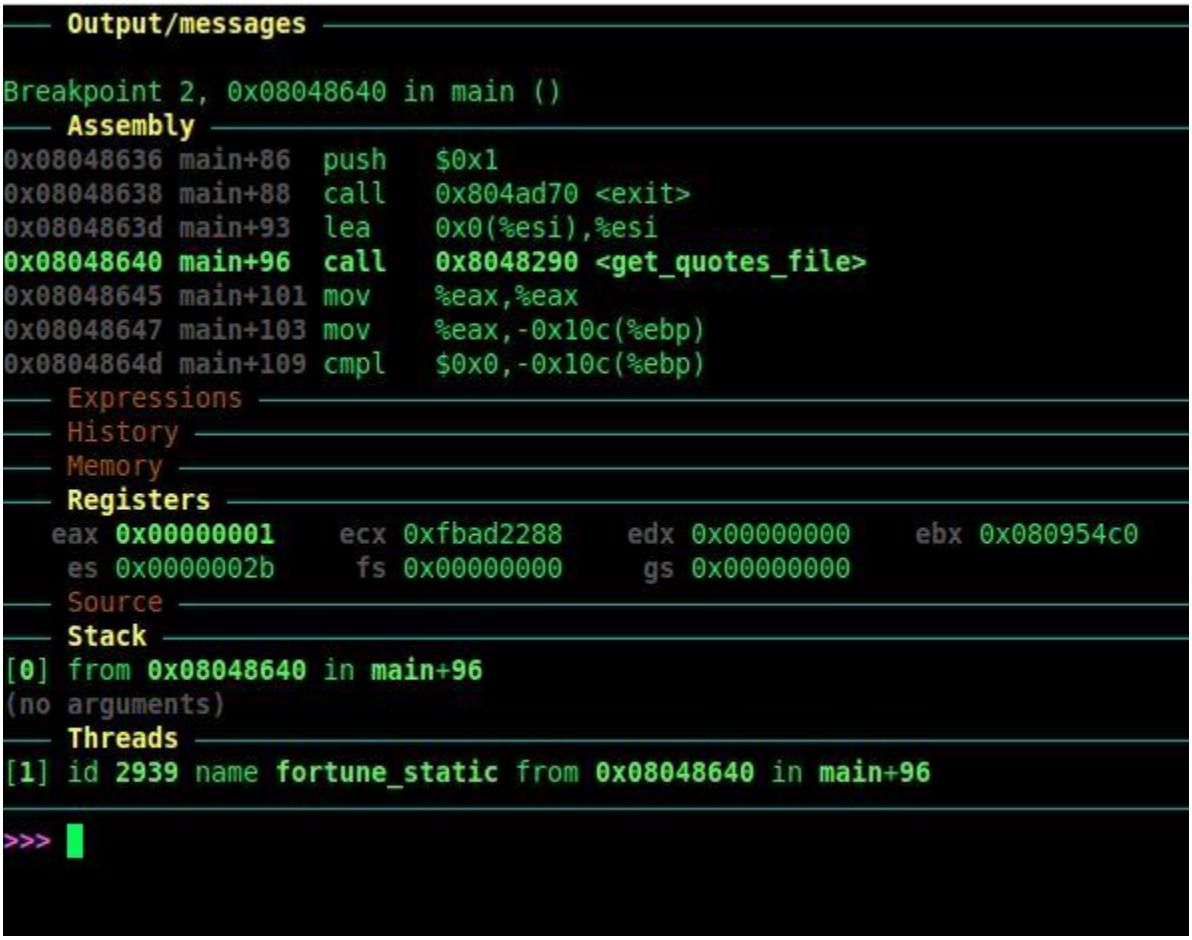
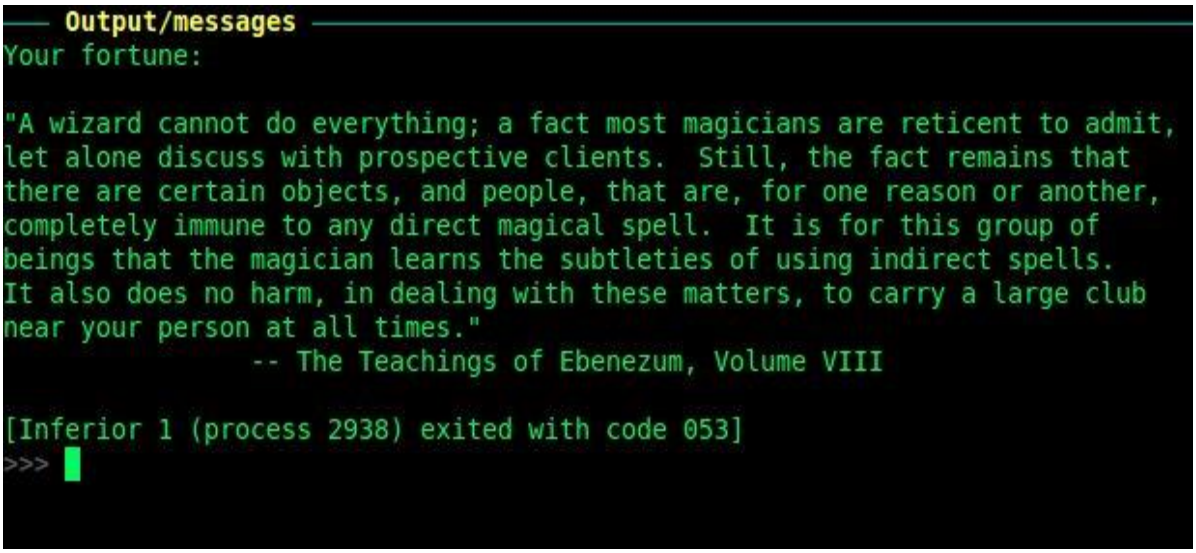
Anthony Constantino
Project 10

Password Cracking

1) First to hack the program I found where the program was going and placed a break point in the check_cdkey function. From there I followed the program until I found a point where it jumped to line 0x08048640 if there was condition met. So, I set a break point at that memory address and ran the program again. This time when I was in the check_cdkey function I forced a return of 1 and noticed that I hit the break point at that memory address which then proceeded to return a fortune.





2) To get the program to bypass the cdkey mechanism I broke the program down into assembly and found the portion where the function was located. The function would jump to two different lines returning 1 or 0. I modified the return 0 to also return 1. This made it so that it would always return 1 and hit that line of code at 0x08048640 and print a fortune.

3) Following the program to where I got the fortune previously it called the get_quotes_file function. Following the program into that function I noticed it called another function called print_fortune. Going into this function the first step was a pointer to the location of the fortunes. Setting breakpoint there and calling print on that memory location revealed the remaining fortunes.