Homework 10

Jason Park

Park1036

4/15/2021

A x 40 + \x18\x0e\x40\x00

I first set a breakpoint in clientComm, and then checked for the address of str, which ended in 0x…dd90. I then printed out the stack, and I saw that the return value for the function was in 0x…ddb8. Since this is where we want to start overwriting, I took the absolute difference between 90 and b8 and got 40 As. Next, I disassembled secretFunction and found that the current address that would show $rbp on the stack is 0x00400e18. That's how I came up with my string: 40 As, and then (in little endian) the address 0x00400e18.

I modified the server code by adding a check if the string entered is longer than the buffer size. If it is, then the program exits and prints an error message. Alternatively, I could use strncpy, and pass in a third parameter that is the buffer size. If the copied string is too large, I believe strncpy would cut off the rest of the string. Both of these methods would be a defense against the buffer overflow attack.