Scott Christensen

11/10/16

C.S. 465

Lab #8: Buffer Overflow

Part 1:

Key:

*Sophomore’s function arguments*

Junior’s function arguments

**Senior’s function arguments**

*Sophomore’s local variables*

Junior’s local variables (The buffer for the string “cougars” is not easily apparent, so I marked where sections of it reside)

**Senior’s local variables**

Freshman’s return address

*Sophomore’s return address*

Junior’s return address

Freshman’s saved frame pointer (ebp)

*Sophomore’s saved frame pointer*

Junior’s saved frame pointer

At seniors:

0xffffd608:    0x0804825c    0xf7e26474    0x0804820c    **0x00007530**

0xffffd618:    0xffffd648    0x080484bf    **0x000007dc**    **0x00000002**

0xffffd628:    0xffffd734    0xffffd66e    0x6f63d6f0    0x72616775

0xffffd638:    0x00000073    0x8e7e1600    0xffffd6a8    0xf7ffda94

0xffffd648:    *0xffffd678*    *0x080484f0*    0x000007dc    0xffffd66e

0xffffd658:    0x00000001    0xf7ffd938    0x00000000    0x00000000

0xffffd668:    0x00000000    *0x00080000*    0x00000003    0x00000009

0xffffd678:    0xffffd6c8    0x08048551    *0x00000025*    *0x000007dc*

Part 2: Here are my results after doing Section C. I rewrote the code to make to function return to the line when it grants us access.

