410 exercise 3

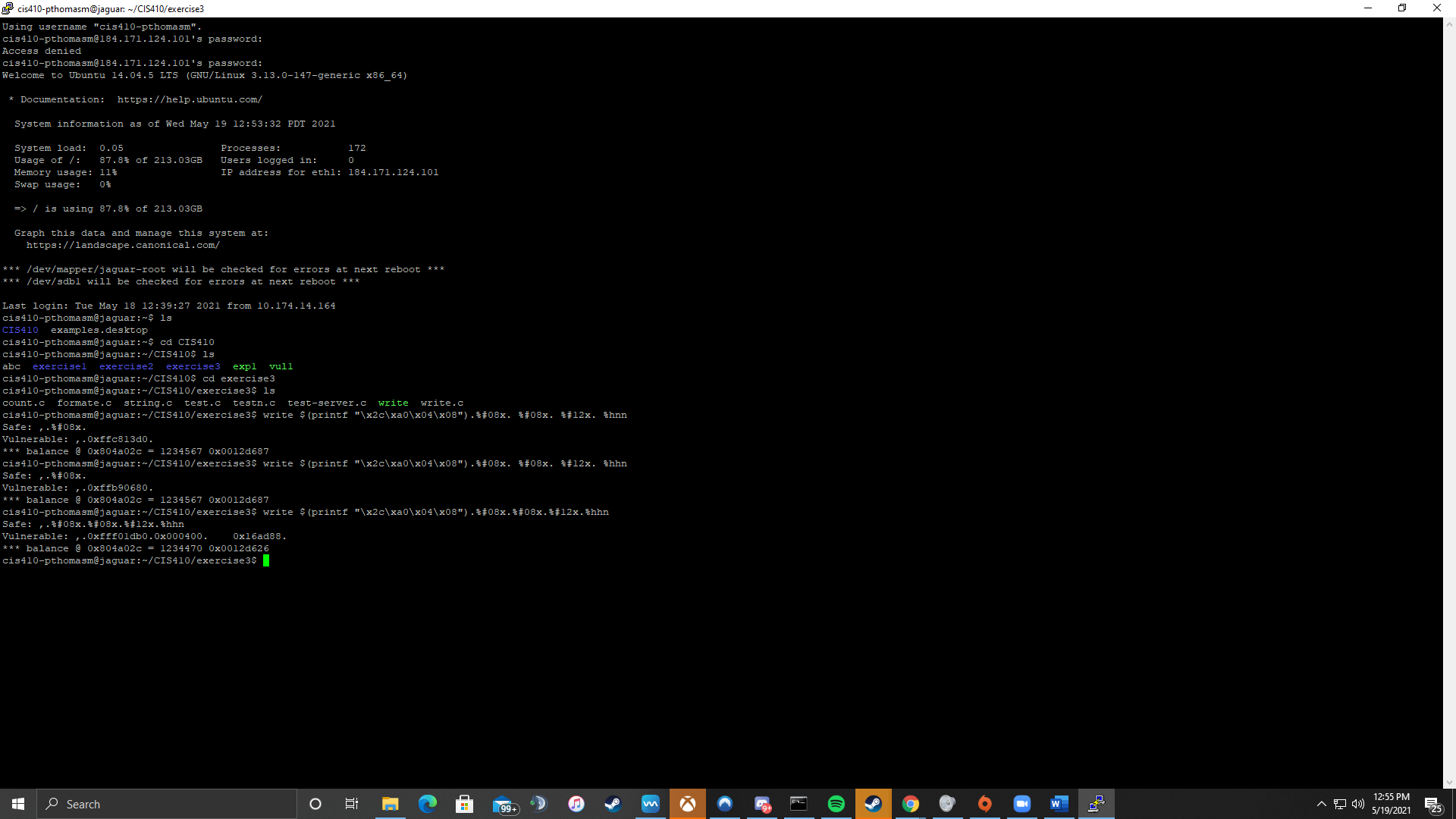
Patrick Thomasma

May 18th 2021

Format String attack:

In this exercise we are doing a format string attack in order to change the balance variable too 1234470

For this project on the command line I ran write $(printf “\x2c\xa0\x04\x08”).%#08x.%#08x.%#12x.%hhn the address for this starts at 0x804a02c which is an int and it ends at 0x0804a02f. Using %hhn will overwrite the last significant byte of the balance variable that is pointed by the format string in printf. Parameter will write in formatted bytes so (4 \* ‘.’ = 4) + (2 \* 08x = 16) + (12x = 12) + (3 \* “0x” = 6) = 38. Thus balance will be initialized to 0x0012d626 then changed to 0x0012d626 since 26 = hex 38.



Above is running the code in jaguar server to show that balance variable is 1234470