CSI -Reverse + Exploit Development Project:

In the attached zip file, you'll find a C program compiled on the protostar machine, it's recommended to "solve the project" on the protostar machine as it was tested there, however it should be also solvable on the Linux environment we've been using as long as ASLR is turned off.

1. Reverse the program – Write the logic of the program in python. (Use net3 and heap3 as reference, feel free to compile the following codes: https://www.binarytides.com/socket-programming-c-linux-tutorial/ for more socket references) (40%)
2. Connect to the program:
    a. Figure out what input does the program expect for a "legal" login (30%)
    b. Use heap overflow to achieve "Illegal" successful login (20%)
    c. Use heap overflow to gain execution on the system (\xcc\x90) (10%)
    d. Use heap overflow to gain a shell on the system. (Bonus (10%)
3. Create a report that includes all of the process you've gone through.