Department of Computer Science
Computer Networks
Due: Monday 26th Sept (23.59)

Your name:
TA Name:
Time Taken:
Estimated Time: 20 hours

This is group assignment, you may (and should) work in teams of 2 students.

This assignment should be completed using C++ 11. The tar archive that you submit should contain all source files in a single directory, accompanied by a Makefile and README. The Makefile should take care of compiling the code. The README should explain how to compile and run the code. Try not to include any hidden files (.git, .DS_Store, .vscode) files in your submission and include your group name in the submission file name. Zip files renamed as tar files will result in an automatic 0.

This assignment requires that you use your laptop (or other computer) to create a port scanning/knocking program that interacts with a server on 130.208.242.120.

Optional: Please include a rough estimate of how long it took you do the assignment so that we can calibrate the work being assigned for the course. (The estimated time is provided purely as a guideline.)

Question:	1	2	3	4	5	Total
Points:	40	30	20	10	10	110
Score:						

Speak easy to the port, and perhaps it will let you in.

In this assignment you will be introduced to the delights of packet crafting, bit twiddling and UDP subterfuge.

Somewhere on 130.208.242.120, a server is listening to some ports in the range 4000-4100. Find the ports, send them the right packets, and use the secret knock to gain access to the secret information!

During the first week the ports are less likely to drop packets.

1 ..... *40 points*

Write a UDP port scanner, that takes in as arguments the IP address of the machine, and a range of ports to scan between. The scanner should be run with the command:

./scanner <IP address> <low port> <high port>

Use it to scan between ports 4000-4100 on 130.208.242.120 and print out the open ports that you find in this range.

Do not rely on the ports always being the same. Also, note that UDP is an unreliable protocol. Some packets may be dropped randomly.

2 ..... *30 points*

The ports you discovered in part 1 are puzzle ports, safeguarding information about two additional ports which are not showing up on your scan. Your task is to write ***a separate program*** to solve the puzzle ports, in order to reveal the two hidden ports and the secret phrase. Each port will send you instructions on how to reveal its secret port if you send it a UDP message.

The program should be run with the command:

./puzzlesolver <IP address>
or
./puzzlesolver <IP address> <port1> <port2> <port3> <port4>

The program should interact with the ports discovered in part 1 by sending them a UDP message following the instructions provided by the puzzle port.

Remember that the ports might change over time. So, do not hard-code the ports in your program, but allow for the ports to be discovered by your program or be provided as command line arguments.

3 ..... *20 points*

After identifying one of the ports as oracle port and finding the two hidden ports, you can send a comma-separated message containing the hidden ports to the oracle, and the oracle will reply with a message telling you the order and number of knocks to use on the hidden ports. For the final part of this assignment, you should extend your program from part 2 with functionality to knock on the hidden ports in the correct order, and finally print out the message from the final hidden port.

You may either fully automate this step after finishing the previous step, or you can execute the port-knocking functionality with the following command line (last parameter being NOT a number)

./puzzlesolver <IP address> <oracleport> <hiddenport1> <hiddenport2> <secretphrase>

Each knock must contain the secret phrase from part 2 as a message.

4 ..... *10 points*

Points will be awarded for code quality, commenting and submission as follows:

(a) (3 points) Code compiles using the supplied Makefile

(b) (2 points) Code follows command line invocations described above.

(c) (5 points) Code is well commented, and modular

5 ..... *10 points*

For 10 bonus points. After completing the port-knocking, you were sent a secret message, follow the instructions in the secret message for 10 bonus points.