Department of Computer Science
Computer Networks
Due: Sunday 20th Sept (23.59)

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

This is pair assignment, you may work either on your own or with a partner of your choice.

This assignment should be completed using C++ 11, the hand-in format is up to you as long as the program compiles with the make command from the source folder.

For those who like to dabble in the dark arts, the latex version is also available. Please use tar to bundle your source code and program submission. Zip files renamed as tar files will result in an automatic 0. Please include your group name in the submission file name. Do **NOT** include any hidden files (.git, .DS_Store .vscode) files in your submission. All code used to complete the assignment should be submitted, with a README file explaining how to compile and run your program(s).

This assignment requires that you use your laptop to create a port scanning/knocking program that interacts with a server on skel.ru.is.

Marks are awarded for question difficulty. While there is typically a relationship between difficulty and length of answer, it may not be a strong one. Always justify your answer if necessary, especially with somewhat open ended design questions.

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:	30	30	20	10	10	100
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 skel.ru.is, 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 ..... *30 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 skel.ru.is and print out the open ports that you find in this range.

Do not rely on the ports always being the same.

2 ..... *30 points*

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

3 ..... *20 points*

When the oracle receives a comma-separated message containing the hidden ports it will reply with a message telling you the order and no. of knocks to use. For the final part of this assignment, you should modify your program from **(2)** to knock on the hidden ports in the correct order, and print out the message from the final hidden port.

Each knock must contain the message "knock", except for the last knock, which should contain the secret phrase from part 2.

4 ..... *10 points*

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

(a) (points) i. (3 points) Code compiles using the supplied Makefile
ii. (2 points) Code follows command line invocation described above.
iii. (5 points) Code is well commented, and modular

5 ..... *10 points*

For 1 bonus mark. After completing the port-knocking, you were sent a secret message, follow the instructions in the secret message for 1 bonus mark.