Department of Computer Science
Computer Networks
Due: Sunday 15th Sept (23.59)

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

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

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.

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	Total
Points:	100	10	110
Score:			

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

1 . . . . *100 points*

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 lurks, listening to some ports, that are in the range 4000-4100. Find the ports, send them the right packets, and use the secret knock to get the oracle to give you its secrets.

All code used to complete the assignment should be submitted, with a README file explaining how to compile and run your program(s).

(a) (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.

(b) (40 points) Each port you discovered in **a)** is safeguarding information about a hidden port which is not showing up on your scan. Your task is to modify your port scanning program to solve the three puzzle ports, in order to reveal the three hidden ports. 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 a) by sending them a UDP message, and use their replies to discover 2 hidden ports, one secret phrase, and determine which port is the oracle.

(c) (20 points) When the oracle receives the correct sequences of ports, it will return a message telling you the order and no. of knocks to use. For the final part of this assignment, you should modify your program 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 b).

(d) (points) Points will be awarded for code quality, commenting and submission as follows:

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

2 . . . . *10 points*

For 1 bonus mark. Complete the assignment you were sent in the ICMP packets that the oracle sent to you.