Project #1: TCP Port Scanner

In this project you will be writing a simple TCP port scanner. A port scanner is a program that tries to find active ports on a target server. This is accomplished by sending client requests to a range of server port addresses. This probing can determine which services are available on a host and more granular information such as the target's operating system through TCP/IP fingerprinting.

For simplicity, we will assume the host follows RFC 793 (TCP) and that services are running on their default port addresses (e.g. HTTP on 80).

Your goal is to develop a program that will scan a port range on a specific set of target hosts and will return the open ports. In addition, if a protocol's default port lies within the port range, list the name of the protocol.

Use the format:
"./program hostname [-p 15:25]"

Bonus. As an extra challenge (for extra credit), attempt to identify the operating system of the target host using it's TCP replies. For example, the TLL and window size combinations may be used to fingerprint an OS.

Operating System (OS)	IP Initial TTL	TCP window size
Linux (kernel 2.4 and 2.6)	64	5840
Google's customized Linux	64	5720
FreeBSD	64	65535
Windows XP	128	65535
Windows 7, Vista and Server 2008	128	8192
Cisco Router (IOS 12.4)	255	4128

You may use any language you choose to develop the program, but if it's anything besides python or C++, please let me know beforehand so I can approve it.

Deliverables:

The code and instructions on how to build/run the code. If its python and you follow the format shown above, only the code is needed. If you use c++ and use the described format, just include the code and a makefile.

Programs will be tested against a set of live hosts on the university network at the beginning of lecture.