P3. Port and IP Address Scanner

Design

Part 1: Live IP Address scanner

This part of the program is responsible for finding the IP addresses of hosts that are in the network described by the network mask provided. This is done by first calculating the lowest IP address possible for a host on the network, and the range of IP addresses that the netmask provides. From here, it is trivial to find the greatest IP address on the network. Once this information is obtained, the program then proceeds to send an ICMP ECHO message to all IP addresses starting from the lowest to the greatest. The program then immediately tries to receive an ICMP ECHO REPLY message from the host that it sent the message to. It sets a timeout of 1 second before receiving the message so that it does not waste time waiting for messages from hosts that are possibly unreachable.

Part 2: Port Scanner

This part of the program is responsible for finding out all the open ports on the system. This is done by starting a loop on the port number, and iterating through the entire range of port numbers (0 – 65535). In every iteration, the program makes a TCP socket and tries to connect to the port number in that iteration. In case the connect returns -1, we acknowledge that the connection did not pass through and the program continues to the next iteration. In case the connect call returns a valid fd, we report the port to be open.

Files Included

scan.c, Makefile

How to run

compile by running `make`
for port scan only, `./scan`
for port scan and ip scan, `./scan <netmask>`

Limitations

The port scan works only on TCP ports

Ashwin Kiran Godbole
Samarth Krishna Murthy