Backdoor User Guide

The following instructions guide shows you how to use the client that will enter a password and a shell command, as well as the server receiving the command and sending the results back to the client using an XOR encryption scheme.

To compile (both client and server):

1. cd backdoor/src
2. make clean
3. make

To run client:

1. cd backdoor/exe
2. ./client -a [Server host] [-p port]
   - 2.1. -a - Server host to send commands to
   - 2.2. -p - Destination port to send commands to
     (if not specified, default is port 8080)
3. Enter password on prompt
4. Enter a shell command (ex. ls -l)
5. To quit client, hit Ctrl-C

To run server:

1. cd backdoor/exe
2. ./server [-d daemon mode] [-p port]
   - 2.1. -d - Daemon mode (run process in the background)
     (default is running server in foreground with messages displayed)
   - 2.2. -p - Destination port to capture packets from
     (if not specified, default is port 8080)
3. To stop server with daemon mode disabled, simply hit Ctrl-C
4. To stop server with daemon mode enabled:
   - 4.1. Run “ps -aux” on another terminal (server side)
   - 4.2. Look for pid (process ID) of the masked process (/sbin/rgnd -f -d)
   - 4.3. Run “kill <pid>” to stop the server from running in the background.