COMP8505 Assignment 3
User Manual

Deric Mccadden

Dimitry Rakhlei

Summary

This program can be executed in two modes. The first is called backdoor and is specified via the flag “-b” in the command line. The second mode is controller which is specified with a “-c” flag in the command line. When the program is run in the controller mode it will send messages from the terminal to a backdoor on the other end and read the responses. The backdoor uses libpcap to capture messages sent to it with raw sockets. It parses the messages and executes the payload. When it is time to send back a response, it encrypts the data and sends it to the controller.

Controller

The controller is specified with the “-c” flag and takes two more arguments. It needs the IP of the machine which has a the backdoor and a port to listen on. Once the arguments are specified the program allows the user to begin sending commands to the other machine.

Example

sudo ./NotABackdoor -c 192.168.0.25 8505

Backdoor

The backdoor only takes the “-b” flag and a port as an argument. It uses the port to filter for the correct packets which it will later authenticate using the header. After executing the backdoor it will run passively and listen for all incoming messages from the controller.

Example

sudo ./NotABackdoor -b 8505