**Project Report**

We decided that we wanted to implement our own custom firewall for our project. We did this for a couple of reasons, one, it is something we can put on our resumes, two, we wanted to learn more about how a firewall works and the different ways you can configure it. Our firewall does two things, block all traffic or specific traffic and unblock all or specific traffic.

Description: We are going to write a simple firewall that will filter the incoming and outcoming traffic based on the rules specified by user.

Firewall will be managed from the user space using binary called "minifw".

Following commands can be executed to operate the firewall:

"minifw run" will run the firewall

"minifw exit" will exit the firewall

"minifw addrule" add new rule

"minifw rmrule" removes the rule

"minifw lsrules" prints all the rules from the file

Rule structure will be as following

<action> <in/out> <protocol> <src\_ip> <src\_netmask> <src\_port> <dest\_ip> <dest\_netmask> <dest\_port>

For example:

BLOCK INOUT ALL NULL NULL NULL NULL NULL NULL will block all the incoming and outcoming traffic (both tcp and udp)

BLOCK IN TCP 137.132.165.27 255.255.255.255 NULL NULL NULL NULL will block incoming tcp traffic from given ip address with given netmask

minifw run

This command will plug in module fwmod inside the kernel. The module has functions required to process network packets. Upon the load, the module will read all the rules from local file. "/proc/firewallfile" file will consist of rules, separated by a new line.

The user will be able to add and remove rules from /proc/firewallfile file. If firewall currently runs, the new rule that is put inside the /proc/firewallfile file will be immidiatly applied (placed inside the linked list of policies that is stored inside the kernel).

Info about module:

sudo insmod fwmod.ko loads the module to the kernel

sudo rmmod fwmod removes the module from the kernel

dmesg /var/log/messages display the log of all the modules

dmesg | tail -20 display last 20 lines of the log file

Example of commands:

0 1 2 3 4 5 6 7 8 9 10

minifw ADDRULE BLOCK INOUT ALL NULL NULL NULL NULL NULL NULL

0 1 2 3 4 5 6 7 8 9 10

minifw ADDRULE BLOCK IN TCP 137.132.165.27 255.255.255.255 NULL NULL NULL NULL