Assessed Exercise 2

Deadline: Friday 31 October, 4pm

The Task

Write an extension to the linux firewall which makes it possible to specify which programs are allowed use which outgoing port.

More precisely, you should write a user space program and a kernel module.

- The kernel module processes the packets and maintains the firewall rules, and displays the firewall rules via `printk` in `/var/log/kern.log`.

- When the kernel module is unloaded, the firewall extensions should be deleted.

- The user space program has commands firstly for triggering the listing of the firewall rules in `/var/log/kern.log`, and secondly for setting the firewall rules. A new set of firewall rules overrides the old set. You should use a suitable file in the `proc`-directory for communication between the user program and the kernel.

- A firewall rule consists of a port number and a filename of a program separated by a space, meaning that the corresponding program is allowed to make outgoing connections on this port. If there is no rule for a given port, any program should be allowed to make outgoing connections on this port.

- To make marking easier, there should be two ways of calling the user space program. The first one is

  <program> L

  where `<program>` is the program name. This way of calling the client program causes the firewall rules to be displayed in `/var/log/kern.log`.

  The second way of calling the program is

  <program> W <filename>

  where `<program>` is as above, and `<filename>` is the name of the file containing the firewall rules. This file contains one firewall rule per line. The client program should check (via the `stat`-system call) whether the filename in the firewall rule denotes an existing executable file.

- You need to ensure that you handle concurrency in the kernel correctly. In particular, any number of outgoing connections may be started at any time, hence several instances of the procedures handling the packets may be executed at the same time.

Marking Scheme

Please use the canvas for submitting your code. Please submit only the source files you have written yourself. We will compile and run your code on the virtual machine and mark it accordingly. Please in particular note that we will use the compiler option introduced in the lecture and deduct 6 marks immediately if there is any compiler error or warning.

We will award marks as follows:

- 5 marks for correctly extending the firewall.

- 5 marks for correct handling the list of firewall rules.

- 5 marks for correct handling the concurrency.

- 5 marks for the correct functioning of the user space program.