Name________________________________ _____/20 pts.

Name________________________________

CS 3CN3 and SE 4C03 Winter 2009

Lab Exercise 5

Instructor: William M. Farmer

Revised: 29 March 2009

Assigned:	29 March 2009
Lab report due for SE 4C03:	31 March 2009
Lab report due for CS 3CN3:	4 April 2009

Do this lab exercise with your group.

The `iptables` software enables one to administer the IP packet filtering facility in the Linux kernel. Working with your partner, write a shell script of `iptables` commands that enforces the IP network security policy below with input, output, and forwarding packet-filtering rules. You will need to carefully read the man page for `iptables` or an `iptables` tutorial on the web.

Go to the setup menu, turn on iptables, and reset your computer. Start your script off by flushing the rules of the three built-in firewall chains:

```
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
```

After running the script, use the commands

```
iptables -L INPUT
iptables -L OUTPUT
iptables -L FORWARD
```

to list the packet filtering rules that have been installed in the Linux kernel. Name the script `packet-filter-ex-5`, put it in `/etc`, set its group to `group`, and make sure that it is accessible, readable, and executable by its group.

_____/2 pts.

IP Network Security Policy

1. Unless otherwise stated by this policy, all inputted, outputted, and forwarded packets are accepted. _____/3 pts.
2. An inputted or forwarded packet with a source address in the loopback subnet is dropped. _____/3 pts.
3. A forwarded or outputted ICMP packet is dropped. _____/3 pts.
4. An inputted TCP telnet packet that is initiating a TCP connection is dropped.
   _____/3 pts.
5. A forwarded TCP telnet packet with a destination address on an SPN directly connected to your host is dropped. _____/3 pts.
6. A forwarded UDP packet with source port 1000 is dropped.
   _____/3 pts.

For your group's lab report, hand in this sheet, a copy of your `packet-filter-ex-5` shell script, and a paper copy of each group member's log book (if it is more convenient, you may hand this in at the beginning of the next lecture). If your log book is missing or incomplete, 4 points will be deducted from your mark. *You and your other group members must hand the lab report in together before the end of the lab session. If you do not attend the lab session or leave the lab before handing in the lab report, you will receive a mark of 0 for the lab exercise.*