Name________________________________ _____/20 pts.

Name________________________________

Name________________________________

SE 4C03 Winter 2003

Lab Exercise 5

Instructor: William M. Farmer

Revised: 23 March 2003

Assigned: 23 March 2003
Lab report due: 08 April 2003

The `iptables` software enables one to administer the IP packet filtering facility in the Linux kernel. Working with your partner(s), write a shell script of `iptables` commands that enforces the IP network security policy below with input, output, and forwarding packet-filtering rules. Read the man page for `iptables`, the the online document

```
/usr/share/doc/ipchains-1.3.10/HOWTO.txt,
```

and the Web document

```
http://www.redhat.com/docs/manuals/linux/RHL-7.2-Manual/
ref-guide/ch-iptables.html.
```

(Note: `iptables` is an extension of `ipchains`.)

Start your script off by flushing the rules of the three 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 `instructor`, and make it readable and executable by its group.
_____/2 pts.

IP Network Security Policy

Let H be the set of 12 hosts in same row as your host, and let H' be the other 24 hosts that are in different rows than your host.

1. Unless otherwise stated by this policy, all incoming, outgoing, and forwarded packets are accepted (in the `iptables` sense). _____/3 pts.
2. An incoming TCP telnet packet with a source or destination address on a host in H is denied (in the `iptables` sense). _____/3 pts.
3. An outgoing TCP telnet packet with a source or destination address on a host in H is denied. _____/3 pts.
4. A forwarded TCP ssh packet with both a source address on a host in H' and a destination address on a host in H' is rejected (in the `iptables` sense). _____/3 pts.
5. An incoming UDP packet with a source address on a host in H' is rejected. _____/3 pts.
6. An outgoing UDP packet with a destination address on a host in H' is rejected. _____/3 pts.

For your lab report, hand in these two exercise sheets, a copy of your `iptables` shell script, and a copy of your log book.