Name_____ _____/20 pts.

Name_____

Name_____

SE 4C03 Winter 2002

Lab Exercise 5

Instructor: William M. Farmer

Revised: 31 March 2002

Assigned: 21 March 2001
Lab report due: 10 April 2001

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` and the online document

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

(`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 `iptables-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 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. _____/3 pts.

2. Forwarded TCP ssh packets are rejected (in the `iptables` sense). _____/3 pts.

3. Incoming UDP packets with source addresses on a host in H are rejected. _____/3 pts.

4. Outgoing UDP packets with destination addresses on a host in H are rejected. _____/3 pts.

5. Incoming TCP http packets requesting a connection are denied (in the `iptables` sense). _____/3 pts.

6. Incoming packets with a source address in the loopback subnet are denied. _____/3 pts.

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