

Name\_\_\_\_\_ /40 pts.

Name\_\_\_\_\_

## SE 4C03 Winter 2004

### Lab Exercise 4

Instructor: Kartik Krishnan S.

Revised: 16th March 2004

Assigned: 16-Mar-2004  
Demonstration due: 29-Mar-2004  
Lab report due: 5-Apr-2004

This lab deals with network security and firewall design. It consists of two independent parts: 4A on public key authentication with `ssh` and 4B on firewall design with the `iptables` service. Read the rules for completing and submitting parts 4A and 4B for this assignment carefully.

#### Part 4A

Do this part of the lab exercise by yourself.

Configure your account to use public key authentication with the Secure Shell network service.

1. Suppose your account name is  $a$ . Ask one of the other groups in the class to give you an account named  $a$  on their host. (Do not use the `intruder` account for this purpose). Let  $x$  denote your host and  $y$  denote the other host. \_\_\_\_\_/ 2 pts.
2. Use the command

`ssh-keygen - d`

to create a DSA public key pair for your account on  $x$ , and an `.ssh` directory. You will have to enter a passphrase which will be used to encrypt/decrypt your private key. Name the private and public key files `id_dsa` and `id_dsa_x.pub`, respectively. Do the same on host  $y$ . \_\_\_\_\_/ 3 pts.

3. On both  $x$  and  $y$ , create a file named `authorized_key2` in the `.ssh` directory. Make these two files readable and writable by the owner only, and then put in both of them the contents of `id_dsa_x.pub` and `id_dsa_y.pub`. \_\_\_\_\_/ 2 pts.
4. Test the set up by executing

```
ssh -v a_y
```

on host  $x$ , where  $a_y$  is one of the two IP addresses of host  $y$ . Authenticate yourself with your passphrase instead of your password. The `-v` option for *verbose* will show each step of the process of creating a secure shell communication channel from your host computer  $x$  to  $y$ . After the communication channel is established, try starting an X windows client like `xterm`. Repeat the process with `ssh -v a_x` on host  $y$ . Based on this, how do you think `ssh` with public-key authentication actually works?. \_\_\_\_\_/ 5 pts.

5. **Demonstrate individually your set up of secure shell with public key authentication to one of the TAs during their office hours (hosts 1-18 will give a demo to Zhihui and hosts 19-36 will give a demo to Hany). I expect all of you to complete your demonstrations by the 29th of March, 2004. You must include the results for part 4 in your final lab report.**

#### Part 4B

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` that enforces the IP network security policy below with input, output, and forwarding packet-filtering rules. Read the man page for `iptables`, 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
```

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-4`, put 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 the 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 address on a host in  $H$  is denied (in the `iptables` sense). \_\_\_\_\_/ 3 pts.
3. An outgoing TCP telnet packet with a destination address on a host in  $H$  is denied. \_\_\_\_\_/ 3 pts.
4. A forwarded TCP ssh packet with both a source 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.

Test your results with `Telnet`, `ssh`, and `traceroute` with and without the IP network security policy. \_\_\_\_\_/ 10 pts.

For your final lab report, hand in these two exercise sheets, your results for part 4A (point 4), a copy of your `iptables` shell script, and a copy of your results for part 4B.