1 SSH Tricks

There are some interesting things you can do with ssh, other than just getting a remote shell. These include a ssh gateway to access hosts behind a firewall, accessing cvs from behind a firewall, and administering embedded router systems securely.

2 SSH gateway

The SSH gateway works by forcing a ssh to another host as a particular username, based on the ssh key. The assumption is that there is a gateway box between the internal hosts and the internet, that has ssh running on it. Create a user on the gateway box, in this example user gw. Then edit the users authorized_keys file and add a line similar to the following:

```
command="ssh -t username@internal.host" \
   ssh-dss AAAAB3N .... 95nxu8Zjg username@host
```

To use the gateway, you then use something like:

```
$ ssh gw@firewall.example.com
```

This should, assuming you have the correct ssh key in the authorized keys file and the correct permissions, ask you to log into internal.host as the specified username.

3 CVS gateway

The CVS gateway is similar to the ssh gateway in that it forces an action based on the ssh key. However, there is also the requirement for ssh agent to be running and for agent forwarding to be enabled.

Create a user for this gateway, called cvs, then add the following to the authorized_keys file.

```
command="ssh -t bmarshal@hopper /usr/bin/cvs server" \
   ssh-dss ANzaalk94tl2 .. lkanbLKDljq8Zjg username@host
```

First start by running the following commands:

```
$ ssh-agent bash
$ ssh-add
```

This will start ssh-agent and add in the users keys. Then run the following:

```
$ export CVS_RSH=ssh
$ cvs -d :ext:cvs@firewall.example.com:/path/to/cvs/repo co module
```

This will allow you to check out the module stored in the repository at /path/to/cvs/repo.

4 Embedded Router Administration

There are many embedded routers available now that provide both telnet and web based administration. As telnet and http are not encrypted protocols and the routers do not usually have enough grunt to run encryption easily the administration interfaces are not suitable for being made available over the internet, yet it is useful to do so.

There is a way of administrating these boxes securely, but there is a bit of setup required. First, if the router is providing network translation for the LAN behind it, set the router to port forward 22 to an internal host, and make sure you can connect to it.

In this example we will assume that the router is 192.168.1.1, and the internal box is 192.168.1.2. To setup a port forward to allow administration via http, run the following:

```
$ ssh -L 8080:192.168.1.1:80 username@router
```

You can then connect to http://localhost:8080/ to talk to the remote router's web interface securely. To do the same for telnet, replace port 80 with 23.

5 Conclusion

These simple tricks using ssh have proved themselves very useful, and are in use almost every day. As you have seen, there is nothing complicated about their setup, and they can provide a very useful service to you.