Labs

During the Red Hat exams, the tasks will be presented electronically. Therefore, this book presents most of the labs electronically as well. For more information, see the "Lab Questions" section toward the end of Chapter 11. Most of the labs for this chapter are straightforward and require very few commands or changes to one or two configuration files.

Lab 1

The intent of this lab is to demonstrate some of the capabilities of the files in the /etc/sysconfig directory. It's an opportunity for you to experiment, to see how such files can be used to modify how a service is started.

In this lab you'll work with the /etc/sysconfig file associated with the Apache web server, httpd. As with any other configuration file, you should back it up before making any changes. If you haven't yet installed the Apache web server, follow the related instructions in the body of Chapter 1.

1. Back up the current version of /etc/sysconfig/httpd.
2. Make sure the Apache web server is running; you can restart it with the **systemctl restart httpd** command. Review currently running Apache processes with the **ps aux | grep httpd** command. How many Apache processes are currently running?
3. Open the /etc/sysconfig/httpd file and add the following directive:

```
OPTIONS="-l"
```

4. Review the httpd man page. What do you think this option will do?
5. Restart the Apache web server. What happens?
6. Are there any Apache processes currently running?
7. Restore the original version of the /etc/sysconfig/httpd file.
8. Be brave. Assuming you've saved the backup of the /etc/sysconfig/httpd configuration file, try using another option, based on Steps 4 through 8.

Lab 2

In this lab you'll set up public/private key–based authentication between two RHEL 7 systems. Any two systems will work for this purpose. Just be prepared to use the same two systems in Labs 3, 4, and 5. In preparation for this lab, make sure that each system has a regular user named hawaii. Use the following passphrase:

```
I love Linux!
```

Lab 3

Repeat Lab 2, but with two differences: set up ECDSA key pair, and set up a user named tonga on the client, configured to connect to user hawaii's account on the server.

Lab 4

In this lab you'll set up user-level security on an SSH server. Use the same systems configured for Labs 2 and 3. Limit access to the user hawaii set up in Lab 2, and then try to access a different account on the SSH server. Try access again to the root administrative account on the SSH server.

Lab 5

In this lab you'll set up the SSH server configured in earlier labs on TCP port 8122. Once this is complete, reload the service. Try connecting locally. Set up the systems so that you can also connect from a remote system. As an optional task, repeat the same exercise using port 8022. What happens?

Lab 6

In this lab you'll configure the /virtual/web directory with the same SELinux file context as the /var/www directory. In addition, configure the /virtual/web/cgi-bin directory with the same SELinux file context as the /var/www/cgi-bin directory.