# Chapter 8 Lab Questions

During the RHCSA exam, 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 8.

## Lab 1

In this lab, you’ll review the process for disabling and re-enabling SELinux on a system. Review the current status of SELinux with the **sestatus** command. You can disable SELinux through the /etc/sysconfig/selinux file or through the SELinux Administration tool. Do so and reboot the system. Try the **sestatus** command again. Re-enable SELinux and reboot the system. What happens? Does the process take long? How many times does the system reboot? What would happen if you had to wait for the relabel and the reboot process during a Red Hat exam?

## Lab 2

In this lab, you’ll set up an Apache web server that you will use for the subsequent lab exercises. Although the configuration of a web server is not part of the RHCSA exam objectives, you may be required to troubleshoot issues related with firewall configuration or SELinux.

1. Log in as root into server1.example.com and confirm that firewalld is running.
2. Install the httpd RPM package.
3. Start the httpd service and ensure that it is enabled to start at boot. If the installation was successful, you should be able to browse the default test web page at http://localhost.
4. Check the current default firewall zone. Set the zone to dmz.
5. Add the http service to the default firewall zone.
6. From tester1.example.com, open Firefox and point the browser to the IP address of server1.example.com (i.e., http://172.16.0.100, or substitute accordingly the IP address of your server1 machine). If successful, you should see the default test page of the web server
7. Reboot server1.example.com to ensure that your configuration survives a reboot.

## Lab 3

This lab follows from the web server that you have configured in Lab 2. You will run the web server on a different port.

1. Open the /etc/httpd/conf/httpd.conf file and change the **Listen 80** directive to **Listen 81**.
2. Restart the httpd service.
3. On server1.example.com, open Firefox and point the browser to http://localhost:81. What happens?
4. On tester1.example.com, open Firefox and point the browser to http://172.16.0.100:81 (substitute with the IP address of server1). What happens?
5. Add TCP port 81 to the http service on the firewall and repeat steps 4. What do you see.
6. Finally, reboot server1.example.com, to ensure that your configuration survives a reboot.

## Lab 4

This lab is almost identical to Lab 3, but with an additional caveat.

1. Open the /etc/httpd/conf/httpd.conf file and change the **Listen** directive to **Listen 82**.
2. Restart the httpd service. What is the problem here? Check the logs and fix it.
3. Add TCP port 82 to the http service on the firewall and repeat restart the service.
4. On tester1.example.com, open Firefox and point the browser to http://172.16.0.100:82 (substitute with the IP address of server1). What do you see?
5. Reboot server1.example.com to ensure that your configuration survives a reboot.

## Lab 5

In this lab, you will continue the configuration of the web server by setting a nondefault location to serve web pages.

1. Open the /etc/httpd/conf/httpd.conf file and change the **Listen** directive to **Listen 80**.
2. Restart the httpd service.
3. Create a new default web page:

# echo "Hello world!" > /var/www/html/index.html

1. On tester1.example.com, open Firefox and point the browser to http://172.16.0.100 (substitute with the IP address of server1). What do you see?
2. Create the directory /html.
3. Open the /etc/httpd/conf/httpd.conf file and change the **DocumentRoot "/var/www/html"** directive to **DocumentRoot "/html"**. Next, add the following lines:

<Directory "/html">
 Require all granted
 Option Indexes
</Directory>

1. Create a new test web page:

# echo "A new test page" > /html/index.html

1. Restart the httpd service.
2. On tester1.example.com, open Firefox and point the browser to http://172.16.0.100 (substitute with the IP address of server1). What do you see? Check the logs and fix the problem.

## Lab 6

Your task is to perform the following operations on tester1.example.com and server1.example.com:

1. Create a new user named bob on tester1.example.com.
2. Generate an SSH key pair for bob without using a passphrase.
3. Create a new user named alice on server1.example.com. Set the passwords for both bob and alice to “changeme”.
4. Enable bob to SSH into server1.example.com as alice without using a password.
5. Confirm that bob is able to SSH into server1.example.com as alice without being prompted for a password.