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 4.

The Red Hat exams are unique based on their reliance on labs and hands-on demonstrations. Be aware, although Labs 5, 6, and 7 cover different topics, they are designed to be run consecutively.

Lab 1

In this lab you'll explore the role of the SUID bit.

1. Remove SUID permissions on the /usr/bin/passwd executable file with the **chmod u-s /usr/bin/passwd** command.
2. Try to run the **passwd** command as a regular user. What happens? Did your password change? Try again. What worked when prompted for the current password?
3. Return to the root user account and restore SUID permissions on the /usr/bin/passwd file.
4. Try to run the **passwd** command again as a regular user. Change your password. What happens this time?

Lab 2

In this lab, you'll create a script, set up file permissions on that script, and then configure ACLs for that script to be executed by a regular user.

1. In a text editor, open file script1 in the /usr/local/bin directory.
2. Enter the following lines in that file:

```
#!/bin/bash
/bin/ls > filelist
```

3. Save the file.
4. Try to execute that script as the root administrative user. What happens?

5. Set up execute permissions for the user owner of the script1 file with the **chmod u+x /usr/local/bin/script1** command. Can you now execute the script as the root administrative user?
6. Change the permissions on the script1 file created in Lab 1 with the **chmod 700 /usr/local/bin/script1** command.
7. Log in as a regular user. Try to execute that script. What happens?
8. By default, ACL support is already enabled on XFS filesystems. Configure read and execute ACLs for one regular user on the script1 file. Verify with the **getfacl** command.
9. Repeat Step 7, logging in as the regular user given ACL privileges to the script1 script. What happens?
10. If you want to restore the original configuration, delete the script1 file from the /usr/local/bin directory.

Lab 3

In this lab, you'll set ACLs for a regular user on the root administrative user's home directory, /root. Start with setting ACLs for the directory and then review the results from the regular user's account. What files can be read from the /root directory? What else do you have to do to set up ACLs on a specific file in the /root directory?

Just make sure to disable ACLs on the /root directory when the lab is complete.

Lab 4

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/selinux/config 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 5

In this lab, you'll set up one regular user in the SELinux guest_u category. Remember that the relevant commands start with **semanage login**. Given the options with the __default__ user, there are multiple ways to meet the requirements of this lab.

Before making any changes, record the current status of SELinux users; one method is with the following command, which records the output in the selinuxusers.txt file:

```
# semanage login -l > selinuxusers.txt
```

Your work will continue in Lab 6.

Lab 6

Now with the regular user in the guest_u category, see what you can do. Try the following actions:

1. Try logging in to the GUI. What happens?
2. Log in to a regular console. Try to ssh to another machine. What happens?
3. Back in the console, try the **su -** command and type the root password. What happens?
4. Try some of the **system-config-*** commands. What happens?

Lab 7

In this lab, you'll deactivate the guest_exec_content SELinux boolean. Do so with a command that ensures that the change survives a reboot. Once complete, log out as the configured guest user and then log back in. Copy a binary, such as **/bin/ls**, into the user's home directory and run the program:

```
$ cp /bin/ls ~
$ ~/ls
```

What happens? Try running a program from the /tmp directory.

When the process is complete, log in to the GUI as an unconfined user and review the SELinux users in the GUI SELinux Administration tool. (For this purpose, it's acceptable to log in to the GUI with the root administrative account.) Use the User Mapping section as well as the

tools available to restore the original configuration as documented in the selinuxusers file. Don't forget to deactivate the guest_exec_content boolean.

Lab 8

In this lab, you'll create a new /ftp directory with SELinux contexts appropriate for that directory. It should be based on the contexts in the /var/ftp/pub directory. Use the knowledge that you gained in this chapter to complete this lab. When you are done, restore the original contexts on the /ftp directory. How do the SELinux contexts differ? From what file did the restored contexts come? Are the restored contexts the same as when the /ftp directory was created?

Lab 9

At this point, you should have some data available in an audit.log file in the /var/log/audit directory. If so, try to read the log file. If not, make sure SELinux is set in enforcing mode (or at least in permissive mode). Make sure the audit service is working with the **systemctl status auditd** command.

Apply the **sealert -a** command to that file; you may want to redirect that output to a text file for easier perusal. Can you identify problems in the file? What users have been listed in that file? Can you identify users and groups by their UID and GID numbers? For more information on UIDs and GIDs, see Chapter 8. Are there any proposed solutions?