APPENDIX

B

Exercise Answers

This appendix provides answers to each of the chapter exercises. There are many ways to accomplish tasks in Linux. What is provided here are suggestions

Some of the exercises require that you modify system files that could change the basic functioning of your system, or even make it unbootable. Therefore, we recommend that you do the exercises on a Linux system that you are free to modify and erase if something should go wrong.

Chapter 2: Creating the Perfect Linux Desktop

The following section details some ways these tasks can be completed on both the GNOME 2 and GNOME 3 desktops.

1. To get started, you need a Linux system in front of you to do the procedures in this book. An installed system is preferable so you don't lose your changes when you reboot. To start out, you can use a Fedora Live CD (or installed system), an Ubuntu installed system, or a Red Hat Enterprise Linux installed system. Here are your choices:
   - **Fedora Live CD (GNOME 3)**—Get a Fedora Live CD as described in Appendix A. Run it live, as described in the "Starting with the Fedora GNOME Desktop Live CD" section of Chapter 2, or install it and run it from hard disk as described in Chapter 9, "Installing Linux."
   - **Ubuntu (GNOME 3)**—Install Ubuntu and install the GNOME Shell software, as described in the beginning of Chapter 2.
   - **Red Hat Enterprise Linux (GNOME 2)**—Install Red Hat Enterprise Linux, as described in Chapter 9.
2. To launch the Firefox web browser and go to the GNOME home page (`http://gnome.org`), there are some easy steps to take. If your networking is not working, refer to Chapter 14, "Administering Networking," for help connecting to wired and wireless networks.
   - GNOME 3

     For GNOME 3, you can press the Windows key to get to the Overview screen. Then type **`Firefox`** to highlight just the Firefox Web Browser icon. Press Enter to launch it. Type **`http://gnome.org`** in the location box and press Enter.
   - GNOME 2

     For GNOME 2, select the Firefox icon from the top menu bar. Type **`http://gnome.org`** in the location box and press Enter.

3. To pick a background you like from the GNOME art site (`http://art.gnome.org/backgrounds`), download it to your Pictures folder, and select it as your current background on both GNOME 2 and GNOME 3 systems, do the following:
   - Type **`http://art.gnome.org/backgrounds`** in the Firefox location box and press Enter.
   - Find a background you like and click GO to display it.
   - Right-click the image and select Set as Desktop Background.
   - From the pop-up that appears, select the position and color of the background image.
   - Select the Set Desktop Background button. The image is used as your desktop background and the image is copied to the file `Firefox_wallpaper.png` in your home directory.
4. To start a Nautilus File Manager window and move it to the second workspace on your desktop, do the following:
   - For GNOME 3
     - Press the Windows key.
     - Grab the Files icon from the Dash (left side) and drag it onto an unused workspace on the right side. A new instance of Nautilus starts in that workspace.
   - For GNOME 2
     - Open the Home folder from the GNOME 2 desktop (double-click).
     - Right-click in the Nautilus title bar that appears and select either Move to Workspace Right or Move to Another Workspace (you can select which workspace you want from the list).
5. To find the image you downloaded to use as your desktop background and open it in any image viewer, first go to your Home folder.

   The image should appear in that folder when you open Nautilus. Simply double-click the `Firefox_wallpaper.png` icon to open the image in the default image viewer. If you have multiple image viewers on your system, right-click the icon and select the application you want to use to open it.
6. To move back and forth between the workspace with Firefox on it and the one with the Nautilus file manager is fairly straightforward.

   If you did the previous exercises properly, Nautilus and Firefox should be in different workspaces. Here's how you can move between those workspaces in GNOME 3 and GNOME 2:
   - GNOME 3

     Press the Windows key and double-click the workspace you want in the right column. As an alternative, you can go directly to the application you want by pressing Alt+Tab and pressing Tab again to highlight the application you want to open.

- GNOME 2

  Select the workspace you want with your mouse by clicking on the small representation of the workspace in the right side of the lower panel. If you happen to have Desktop Effects enabled (System ➢ Preferences Desktop Effects ➢ Compiz), try pressing Ctrl+Alt+right arrow (or left arrow) to spin to the next workspace.

7. To open a list of applications installed on your system and select an image viewer to open from that list using as few clicks or keystrokes as possible, do the following:

   - In GNOME 3

     Move the mouse to the upper-left corner of the screen to get to the Overview screen. Select Applications, select Graphics from the right column, and then select Image Viewer.

   - In GNOME 2

     Select Applications ➢ Graphics ➢ Image Viewer to open an image viewer window on the desktop.

8. To change the view of the windows on your current workspace to smaller views of those windows you can step through, do the following:

   - In GNOME 3

     With multiple windows open on multiple workspaces, press and hold the Alt+Tab keys. While continuing to hold the Alt key, press Tab until you highlight the application you want. Release the Alt key to select it. (Notice that applications that are not on the current workspace are to the right of a line dividing the icons.)

   - In GNOME 2

     With multiple windows open on multiple workspaces, press and hold the Ctrl+Alt+Tab keys. While continuing to hold the Ctrl+Alt keys, press Tab until you have highlighted the application you want. Release the Ctrl and Alt keys to select it.

9. To launch a music player from your desktop using only the keyboard, do the following:

   - In GNOME 3
     - Press the Windows key to go to the Overview screen.
     - Type **`Rhyth`** (until the icon appears and is highlighted) and press Enter. (In Ubuntu, if you don't have Rhythmbox installed, type **`Bansh`** to open the Banshee Media Player.)
   - In GNOME 2

     Press Alt+F2. From the Run Application box that appears, type **`rhythmbox`** and press Enter.

10. To take a picture of your desktop using only keystrokes, press the Print Screen key to take a screen shot of your entire desktop in both GNOME 3 and GNOME 2. Press Ctrl+Print Screen to take a screen shot of just the current window.

Chapter 3: Using the Shell

1. To switch virtual consoles and return to the desktop:
   - Hold Ctrl+Alt and press F2 (Ctrl+Alt+F2). A text-based console should appear.
   - Type your username (press Enter) and password (press Enter).
   - Type a few commands such as **`id`**, **`pwd`**, and **`ls`**.
   - Type **`exit`** to exit the shell and return to the login prompt.
   - Press Ctrl+Alt+F1 to return to the virtual console that holds your desktop. (On different Linux systems, the desktop may be on different virtual consoles. Ctrl+Alt+F7 is another common place to find it.)
2. For your Terminal window, make the font red and the background yellow.
   - From the GNOME desktop, select Applications ➢ System Tools ➢ Terminal to open a Terminal window.
   - From the Terminal window, select Edit ➢ Profiles.
   - With Default highlighted from the Profiles window, select Edit.
   - Select the Colors Tab and deselect the Use colors from system theme box.
   - Select the box next to Text Color, click the color red you want from the color wheel, and click OK.
   - Select the box next to Background Color, click the color yellow you want from the color wheel, and click OK.
   - Click Close on each window to go back to the Terminal window with the new colors.
   - Go back and reselect the Use colors from system theme box to go back to the default Terminal colors.
3. Find the `mount` command and `tracepath` man page.
   - Run `type mount` to see that the `mount` command's location is `/bin/mount`.
   - Run `locate tracepath` to see that the `tracepath` man page is at `/usr/share/man/man8/tracepath.8.gz`.
4. Run, recall, and change these commands as described:

```
$ cat /etc/passwd
$ ls $HOME
$ date
```

- Press the up arrow until you see the `cat /etc/passwd` command. If your cursor is not already at the end of the line, press Ctrl+E to get there. Backspace over the word `passwd`, type the word **`group`**, and press Enter.
- Type **`man ls`** and find the option to list by time (`-t`). Press the up arrow until you see the `ls $HOME` command. Use the left arrow key or Alt+B to position your cursor to the left of `$HOME`. Type **`-t`**, so the line appears as `ls -t $HOME`. Press Enter to run the command.
- Type **`man date`** to view the `date` man page. Use the up arrow to recall the `date` command and add the format indicator you found. A single `%D` format indicator will get the results you need:

```
$ date +%D
12/08/11
```

5. Use tab completion to type **`basename /usr/share/doc/`**. Type **`basen<Tab> /u<Tab>sh<Tab>do<Tab>`** to get basename `/usr/share/doc/`.
6. Pipe `/etc/services` to the `less` command:

```
$ cat /etc/services | less
```

7. Make output from the `date` command appear in this format: Today is Thursday, December 08, 2011.

```
$ echo "Today is $(date +'%A, %B %d, %Y')"
```

8. View variables to find your current hostname, username, shell, and home directories.

```
$ echo $HOSTNAME
$ echo $USERNAME
$ echo $SHELL
$ echo $HOME
```

9. Add a permanent `mypass` alias that displays the contents of the `/etc/passwd` file.
   - Type **`nano $HOME/.bashrc`**.
   - Move the cursor to an open line at the bottom of the page (press Enter to open a new line if needed).
   - On its own line, type **`alias m="cat /etc/passwd"`**.
   - Type Ctrl+O to save and Ctrl+X to exit the file.
   - Type **`source $HOME/.bashrc`**.
   - Type **`alias m`** to make sure the alias was set properly:

```
ias m='cat /etc/passwd'.
```

   - Type **`m`** (the `/etc/passwd` file displays on the screen).

10. To display the man page for the mount system call, use the `man -k` command to find man pages that include the word `mount` (using the ^ ensures that only commands beginning with the word `mount` are displayed). Then use the `mount` command with the correct section number (2) to get the proper `mount` man page:

```
$ man -k ^mount
mount                (2)  - mount file system
mount                (8)  - mount a filesystem
mountpoint           (1)  - see if a directory is a mountpoint
mountstats           (8)  - Displays NFS client per-mount statistics
$ man 2 mount
MOUNT(2)      Linux Programmer's Manual              MOUNT(2)
NAME
       mount - mount file system
SYNOPSIS
       #include <sys/mount.h>
.
.
.
```

Chapter 4: Moving Around the Filesystem

1. Create the projects directory, create nine empty files (`house1` to `house9`), and list just those files.

```
$ mkdir $HOME/projects/
$ touch $HOME/projects/house{1..9}
$ ls $HOME/projects/house{1..9}
```

2. Make the `$HOME/projects/houses/doors/` directory path and create some empty files in that path.

```
$ cd
$ mkdir projects/houses
$ touch /home/joe/houses/bungalow.txt
$ mkdir $HOME/projects/houses/doors/
$ touch $HOME/projects/houses/doors/bifold.txt
$ mkdir -p $HOME/projects/outdoors/vegetation/
$ touch projects/outdoors/vegetation/landscape.txt
```

3. Copy the files `house1` and `house5` to the `$HOME/projects/houses/` directory.

```
$ cp $HOME/projects/house[15] $HOME/projects/houses
```

4. Recursively copy the `/usr/share/doc/initscripts*` directory to the `$HOME/projects/` directory.

```
$ cp -ra /usr/share/doc/initscripts*/ ~/projects/
```

5. Recursively list the contents of the `$HOME/projects/` directory. Pipe the output to the `less` command so you can page through the output.

```
$ ls -lR $HOME/projects/ | less
```

6. Remove the files house6, house7, and house8 without being prompted.

```
$ rm -f $HOME/projects/house[678]
```

7. Move house3 and house4 to the $HOME/projects/houses/doors directory.

```
$ mv projects/house{3,4} projects/houses/doors/
```

8. Remove the $HOME/projects/houses/doors directory and its contents.

```
$ rm -rf projects/houses/doors/
```

9. Change the permissions on the $HOME/projects/house2 file so it can be read and written by the user who owns the file, only read by the group, and have no permission for others.

```
$ chmod 640 $HOME/projects/house2
```

10. Recursively change the permissions of the $HOME/projects/ directory so that nobody has write permission to any files or directory beneath that point in the file system.

```
$ chmod -R a-w $HOME/projects/
```


Chapter 5: Working with Text Files

1. Follow these steps to create the /tmp/services file, and then edit it so that "WorldWideWeb" appears as "World Wide Web".

```
$ cp /etc/services /tmp
$ vi /tmp/services
/WorldWideWeb<Enter>
cwWorld Wide Web<Esc>
```

The next two lines show the before and after.

```
http            80/tcp      www www-http    # WorldWideWeb HTTP
http            80/tcp      www www-http    # World Wide Web HTTP
```

2. One way to move the paragraph in your /tmp/services file is to search for the first line of the paragraph, delete five lines (5dd), go to the end of the file (G), and put in the text (p):

```
$ vi /tmp/services
/Note that it is<Enter>
5dd
G
p
```

3. To use ex mode to search for every occurrence of the term tcp (case sensitive) in your /tmp/services file and change it to WHATEVER, you can type the following:

```
$ vi /tmp/services
:g/tcp/s//WHATEVER/g<Enter>
```

4. To search the /etc directory for every file named passwd and redirect errors from your search to /dev/null, you can type the following:

```
$ find /etc -name passwd 2> /dev/null
```

5. Create a directory in your home directory called `TEST`. Create files in that directory named `one`, `two`, and `three` that have full read/write/execute permissions on for everyone (user, group, and other). Construct a `find` command that would find those files and any other files that have write permission open to "others" from your home directory and below.

```
$ mkdir $HOME/TEST
$ touch $HOME/TEST/{one,two,three}
$ chmod 777 $HOME/TEST/{one,two,three}
$ find $HOME -perm -002 -type f -ls
148120  0 -rwxrwxrwx   1 chris chris 0 Jan  1 08:56 /home/chris/TEST/two
148918  0 -rwxrwxrwx   1 chris chris 0 Jan  1 08:56 home/chris/TEST/three
147306  0 -rwxrwxrwx   1 chris chris 0 Jan  1 08:56 /home/chris/TEST/one
```

6. Find files under the `/usr/share/doc` directory that have not been modified in more than 300 days.

```
$ find /usr/share/doc -mtime +300
```

7. Create a `/tmp/FILES` directory. Find all files under the `/usr/share` directory that are more than 5MB and less than 10MB and copy them to the `/tmp/FILES` directory.

```
$ mkdir /tmp/FILES
$ find /usr/share -size +5M -size -10M -exec cp {} /tmp/FILES \;
$ du -sh /tmp/FILES/*
7.0M   /tmp/FILES/cangjie5.db
5.4M   /tmp/FILES/cangjie-big.db
8.3M   /tmp/FILES/icon-theme.cache
```

8. Find every file in the `/tmp/FILES` directory and make a backup copy of each file in the same directory. Use each file's existing name and just append `.mybackup` to create each backup file.

```
$ find /tmp/FILES/ -type f -exec cp {} {}.mybackup \;
```

9. Install the `kernel-doc` package in Fedora or Red Hat Enterprise Linux. Using `grep`, search inside the files contained in the `/usr/share/doc/kernel-doc*` directory for the term `e1000` (case insensitive) and list the names of the files that contain that term.

```
# yum install kernel-doc
$ cd /usr/share/doc/kernel-doc*
$ grep -rli e1000 .
./Documentation/powerpc/booting-without-of.txt
/usr/share/doc/kernel-doc-2.6.32/Documentation/networking/e100.txt
```

10. Search for the `e1000` term again in the same location, but this time list every line that contains the term and highlight the term in color.

```
$ cd /usr/share/doc/kernel-doc-*
$ grep -ri --color e1000 .
```

Chapter 6: Managing Running Processes

1. To list all processes running on your system with a full set of columns, while piping the output to less, type the following:

```
$ ps -ef | less
```

2. To list all processes running on the system and sort those processes by the name of the user running each process, type the following:

```
$ ps -ef --sort=user | less
```

3. To list all processes running on the system with the column names process ID, user name, group name, nice value, virtual memory size, resident memory size, and command, type the following:

```
$ ps -eo 'pid,user,group,nice,vsz,rss,comm' | less
  PID USER     GROUP      NI    VSZ   RSS COMMAND
    1 root     root        0  19324  1236 init
    2 root     root        0      0     0 kthreadd
    3 root     root        -      0     0 migration/0
    4 root     root        0      0     0 ksoftirqd/0
```

4. To run the `top` command and then go back and forth between sorting by CPU usage and memory consumption, type the following:

```
$ top
P
M
P
M
```

5. To start the `gedit` process from your desktop and use the System Monitor window to kill that process, do the following:

```
$ gedit &
```

   Next, select Applications ➢ System Tools ➢ System Monitor. Find the `gedit` process on the Processes tab (you can sort alphabetically to make it easier by clicking on the Process Name heading). Right-click the `gedit` command and then select either End Process or Kill Process, and the `gedit` window on your screen should disappear.

6. To run the `gedit` process and use the `kill` command to send a signal to pause (stop) that process, type the following:

```
$ gedit &
[1] 21532

$ kill -SIGSTOP 21578
```

7. To use the `killall` command to tell the `gedit` command (paused in the previous exercise) to continue working, do the following:

```
$ killall -SIGCONT gedit
```

Make sure the text you typed after `gedit` was paused now appears in the window.

8. To install the `xeyes` command, run it about 20 times in the background, and run `killall` to kill all 20 `xeyes` processes at once, type the following:

```
# yum install xorg-x11-apps
$ xeyes &
$ xeyes &
...
$ killall xeyes &
```

Remember, you need to be the root user to install the package. After that, remember to repeat the `xeyes` command 20 times. Spread the windows around on your screen and move the mouse for fun to watch the eyes move. All the `xeyes` windows should disappear at once when you type **`killall xeyes`**.

9. As a regular user, run the `gedit` command so that it starts with a nice value of 5.

```
# nice -n 5 gedit &
[1] 21578
```

10. To use the `renice` command to change the nice value of the `gedit` command you just started to `7`, type the following:

```
# renice -n 7 21578
21578: old priority 0, new priority 7
```

Use any command you like to verify that the current nice value for the `gedit` command is now set to 7. For example, you could type this:

```
# ps -eo 'pid,user,nice,comm' | grep gedit
21578 chris     7 gedit
```

Chapter 7: Writing Simple Shell Scripts

1. Here's an example of how to create a script in your `$HOME/bin` directory called `myownscript`. When the script runs, it should output information that looks as follows:

```
Today is Sat Dec 10 15:45:04 EST 2011.
You are in /home/joe and your host is abc.example.com.
```

The following steps show one way to create the script named `myownscript`:

- If it doesn't already exist, create a bin directory:

```
$ mkdir $HOME/bin
```

- Using any text editor, create a script called `$HOME/bin/myownscript` that contains the following:

```
#!/bin/bash
# myownscript
# List some information about your current system
```

```
echo "Today is $(date)."
echo "You are in $(pwd) and your host is $(hostname)."
```

- Make the script executable:

```
$ chmod 755 $HOME/bin/myownscript
```

2. To create a script that reads in three positional parameters from the command line, assigns those parameters to variables named ONE, TWO, and THREE, respectively, and then outputs that information in the specified format, do the following:

   Replace X with the number of parameters and Y with all parameters entered. Then replace A with the contents of variable ONE, B with variable TWO, and C with variable THREE.

   - Here is an example of what that script could contain:

```
#!/bin/bash
# myposition
ONE=$1
TWO=$2
THREE=$3
echo "There are $# parameters that include: $@"
echo "The first is $ONE, the second is $TWO, the third is $THREE."
```

   - To make the script executable, type this:

```
$ chmod 755 $HOME/bin/myposition
```

   - To test it, run it with some command-line arguments, as in the following:

```
$ myposition Where Is My Hat Buddy?
There are 5 parameters that include: Where Is My Hat Buddy?
The first is Where, the second is Is, the third is My.
```

3. To create the script described, do the following:

   - Make the script executable:

```
$ chmod 755 $HOME/bin/myposition
```

   - Here's what the script mytown might look like:

```
#!/bin/bash
# myhome
read -p "What street did you grow up on? " mystreet
read -p "What town did you grow up in? " mytown
echo "The street I grew up on was $mystreet and the town was $mytown."
```

   - Run the script to check that it works. The following example shows what input and output for the script could look like:

```
$ myhome
What street did you grow up on? Harrison
What town did you grow up in? Princeton
The street I grew up on was Harrison and the town was Princeton.
```

4. To create the required script, do the following: Using any text editor, create a script called $HOME/bin/myos and make the script executable:

```
$ chmod 755 $HOME/bin/myos
```

   - The script could contain the following:

```
#!/bin/bash
# myos
read -p "What is your favorite operating system, Mac, Windows or Linux? "
opsys
if [ $opsys = Mac ] ; then
  echo "Mac is nice, but not tough enough for me."
elif [ $opsys = Windows ] ; then
  echo "I used Windows once. What is that blue screen for?"
elif [ $opsys = Linux ] ; then
  echo "Great Choice!"
else
  echo "Is $opsys an operating system?"
fi
```

5. To create a script named `$HOME/bin/animals` that runs through the words moose, cow, goose, and sow through a for loop and have each of those words appended to the end of the line,"I have a . . . ," do the following:

   - Make the script executable:

```
$ chmod 755 $HOME/bin/animals
```

   - The script could contain the following:

```
#!/bin/bash
# animals
for ANIMALS in moose cow goose sow ; do
  echo "I have a $ANIMALS"
done
```

   - When you run the script, the output should look as follows:

```
$ animals
I have a moose
I have a cow
I have a goose
I have a sow
```

Chapter 8: Learning System Administration

1. You can open the Date & Time window from a GNOME desktop in RHEL or Fedora by doing one of the following:

   - Open a Terminal window, and then type **`system-config-date`**. If you do that as a regular user, you are prompted for the root password.

- From a GNOME 2.X desktop, select System Administration Date & Time.
- From a GNOME 3 desktop, select Activities ➢ Applications ➢ System-Config-Date.

When the Date & Time window opens, select the Time Zone tab to check your time zone.

2. To run a `ps` command to sort all processes running on your system by username, type the following:

```
$ ps -ef --sort=user | less
chris    3774  3202  0 21:08 pts/0    00:00:00 less

dbus      1869     1  0 20:42 ?        00:00:00 dbus-daemon --system

gdm       2616     1  0 20:44 ?        00:00:00 /usr/bin/dbus-launch
68        2010     1  0 20:43 ?        00:00:00 hald

lp        1971  1970  0 20:43 ?        00:00:00 cups-polld example
root         1     0  0 20:40 ?        00:00:01 /sbin/init
```

I trimmed the output above to show a few different users. Here's an alternative where you just show the user and command:

```
$ ps -eo 'user,args' --sort=user | less
```

3. To find all files under the `/var/spool` directory that are owned by users other than root and do a long listing of them, type the following (I recommend becoming root to find files that might be closed off to other users):

```
$ su -
Password: *********
# find /var/spool -not -user root -ls | less
```

4. To become root user and create an empty or plaintext file named `/mnt/test.txt`, type the following:

```
$ su -
Password: *********
# touch /mnt/test.txt
# ls -l /mnt/test.txt
-rw-r--r--. 1 root root 0 Jan  9 21:51 /mnt/test.txt
```

5. To become root and edit the `/etc/sudoers` file to allow your regular user account (for example, bill) to have full root privilege via the `sudo` command, do the following:

```
$ su -
Password: *********
# visudo
o
bill     ALL=(ALL)      ALL
Esc ZZ
```

Because `visudo` opens the `/etc/sudoers` file in vi, the example types `o` to open a line, and then types in the line to allow bill to have full root privilege. Once the line is typed, press ESC to return to command mode and type **`ZZ`** to write and quit.

6. To use the `sudo` command to create a file called `/mnt/test2.txt` and verify that the file is there and owned by the root user, type the following:

```
[bill]$ sudo touch /mnt/test2.txt
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.
[sudo] password for bill:
*********
[bill]$ ls -l /mnt/text2.txt
-rw-r--r--. 1 root root 0 Jan  9 23:37 /mnt/text2.txt
```

7. To watch messages as they come into the `/var/log/messages` file as you plug in a USB drive (which will mount it automatically), and then unmount the device and remove it, do the following:

   - Become the root user and watch messages as they come into `/var/log/messages` by doing the following:

```
$ su -
Password: *********
# tail -f /var/log/messages
Jan  9 23:44:14 chris kernel: usb 1-1.1: new high speed USB device
     using ehci_hcd and address 6
Jan  9 23:44:15 chris kernel: usb 1-1.1: New USB device found,
     idVendor=090c, idProduct=1000
...
Jan  9 23:44:15 chris kernel: Initializing USB Mass Storage driver...
Jan  9 23:44:15 chris kernel: scsi6: SCSI emulation for USB Mass Storage
devices
...
Jan  9 23:44:21 chris kernel: sd 6:0:0:0: [sdb] 8343552 512-byte logical
blocks:
   (4.27 GB/3.97 GiB)
Jan  9 23:44:21 chris kernel: sd 6:0:0:0: [sdb] Write Protect is off
Jan  9 23:44:21 chris kernel: sd 6:0:0:0: [sdb] Assuming drive cache:
  write through
Jan  9 23:44:21 chris kernel: sd 6:0:0:0: [sdb] Assuming drive cache:
  write through
Jan  9 23:44:21 chris kernel: sdb: sdb1
```

   - Unmount the device by right-clicking on the device's icon on the desktop and selecting Safely Remove Drive, or as root type `umount /media/?????`, where *`?????`* is replaced by the name created when the device was mounted.
   - Remove the device, but continue to watch the messages file. Then press Ctrl+C to quit tailing the file.

8. To see what USB devices are connected to your computer, type the following:

```
$ lsusb
```

9. To load the `bttv` module, list the modules that were loaded, and unload it, type the following:

```
# modprobe -a bttv
# lsmod | grep bttv
bttv                   124516  0
v4l2_common             10572  1 bttv
videobuf_dma_sg          9814  1 bttv
videobuf_core           20076  2 bttv,videobuf_dma_sg
btcx_risc                4416  1 bttv
rc_core                 19686  7 ir_lirc_codec,ir_sony_decoder,
     ir_jvc_decoder,ir_rc6_decoder
tveeprom                14042  1 bttv
videodev                76244  3 bttv,v4l2_common,uvcvideo
i2c_algo_bit             5728  2 bttv,i915
i2c_core                31274  9 bttv,v4l2_common,tveeprom,videodev,
     i2c_i801,i915,drm_kms_helper
```

   Notice that other modules (`v4l2_common`, `videodev`, and others) were loaded when you loaded `bttv` with `modprobe -a`.

10. Type the following to remove the `bttv` module along with any other modules that were loaded with it. Notice that they were all gone after running `modprobe -r`.

```
# modprobe -r bttv
# lsmod | grep bttv
```

Chapter 9: Installing Linux

1. To install a Fedora system from a Fedora live CD, follow the instructions in the "Installing Fedora from a Live CD" section. In general, those steps include:
   - Booting the Live CD.
   - Launching the Install to Hard Drive icon on the desktop.
   - Adding information as prompted about your keyboard, storage, hostname, timezone, root password, and other items needed to initially configure your system.
   - Rebooting your computer, removing the Live CD, so the newly installed system boots from hard disk.
2. To update the packages, after the Fedora Live CD installation is complete, do the following:
   - Reboot the computer and fill in the first boot questions as prompted.
   - Using a wired or wireless connection, make sure you have a connection to the Internet. Refer to Chapter 14, "Administering Networking," if you have trouble getting your networking connection to work properly. Open a shell as the root user and type **`yum update`**.

- When prompted, type **y** to accept the list of packages displayed. The system begins downloading and installing the packages.

3. To run the RHEL installation in text mode, do the following:
   - Boot the RHEL DVD.
   - When you see the boot loader begin to count down, press a key to interrupt the boot process.
   - With the title of the RHEL system you want to boot highlighted, press **e**. Move the cursor right to the end of the kernel line and type the literal option **text** at the end of that line. Press Enter and then **b** to boot.
   - Try out the rest of the installation in text mode.
4. To set the disk partitioning as described in Question 4 for a Red Hat Enterprise Linux DVD installation, do the following:

NOTE

This procedure will ultimately delete all content on your hard disk. If you want to just use this exercise to practice partitioning, you can reboot your computer before clicking Next at the very end of this procedure without harming your hard disk. Once you go forward and partition your disk, assume that all data has been deleted.

- On a computer you can erase with at least 11GB of disk space, insert a RHEL installation DVD, reboot, and begin stepping through the installation screens.
- When you get to the screen that asks which type of installation you would like, select Create Custom Layout and click Next.
- From the Disk partitioning screen, select the device to use for the installation (probably `sda` if you have a single hard disk that you can completely erase).
- To create a 400MB /boot partition, select the Free line, and select Create. From the Create Storage pop-up select Standard Partition, and click Create. From the Add Partition pop-up, fill in **/boot** as the Mount Point, **ext4** as the file system, and **400** as the size, then click OK.
- To create a 10GB LVM partition, select the Free line, and click Create. From the Create Storage pop-up, select LVM Physical Volume, and click Create. In the Add Partition pop-up, type **10000** as the size, select Fixed size, and click OK.
- To create a volume group named `tracker` from the LVM physical volume you just created, click Create. From the Create Storage pop-up, select LVM Volume Group, and click Create. In the Make LVM Volume Group pop-up, type **tracker** as the Volume Group Name. Make sure there is a check mark next to the LVM device you just created in the Physical Volumes to Use box, and click OK.
- To create a 3GB / partition from the `tracker` volume group, select the LVM `tracker` volume group you just created under LVM Volume Groups,

and select Edit. From the Edit LVM Volume Group pop-up, select Add. In the Make Logical Volume pop-up, type **/** as the Mount Point, type **3000** as the Size, and select OK. Select OK to return to the main screen.

- To create a 2GB /var partition from the tracker volume group, select the LVM tracker volume group you just created under LVM Volume Groups, and select Edit. From the Edit LVM Volume Group pop-up, select Add. In the Make Logical Volume pop-up, type **/var** as the Mount Point, type **2000** as the Size, and select OK. Select OK to return to the main screen.
- To create a 3GB /home partition from the tracker volume group, select the LVM tracker volume group you just created under LVM Volume Groups, and select Edit. From the Edit LVM Volume Group pop-up, select Add. In the Make Logical Volume pop-up, type **/home** as the Mount Point, type **3000** as the Size, and select OK. Select OK to return to the main screen.

At this point, you should see tracker under LVM Volume Groups and three partitions (/, /var, and /home) listed under the tracker group. Under Hard Drives, you should see your disk name (probably sda) with /boot partition and tracker physical volume listed under that. Now you have the choice to continue with the installation by clicking Next or, if you don't want to complete the installation, you can simply reboot your computer and remove the disk without having done any harm to your currently installed system.

Chapter 10: Getting and Managing Software

1. To search the YUM repository for the package that provides the mogrify command, type the following:

   ```
   # yum provides mogrify
   ```

2. To display information about the package that provides the mogrify command and determine what that package's home page (URL) is, type the following:

   ```
   # yum info ImageMagick
   ```

   You will see that the URL to the home page for ImageMagick is http://www.imagemagick.org.

3. To install the package containing the mogrify command, type the following:

   ```
   # yum install ImageMagick
   ```

4. To list all the documentation files contained in the package that provides the mogrify command, type the following:

   ```
   # rpm -qd ImageMagick
   ...
   /usr/share/doc/ImageMagick-6.7.0.10/README.txt
   ...
   /usr/share/man/man1/identify.1.gz
   ```

```
/usr/share/man/man1/import.1.gz
/usr/share/man/man1/mogrify.1.gz
```

5. To look through the changelog of the package that provides the `mogrify` command, type the following:

```
# rpm -q --changelog ImageMagick | less
```

6. To delete the `mogrify` command from your system and verify its package against the RPM database to see that the command is indeed missing, type the following:

```
# type mogrify
mogrify is /usr/bin/mogrify
# rm /usr/bin/mogrify
rm remove regular file '/usr/bin/mogrify'?
# rpm -V ImageMagick
missing   /usr/bin/mogrify
```

7. To reinstall the package that provides the `mogrify` command and make sure the entire package is intact again, type the following:

```
# yum reinstall ImageMagick
# rpm -V ImageMagick
```

8. To download the package that provides the `mogrify` command to your current directory, type the following:

```
# yumdownloader ImageMagick
ImageMagick-6.7.0.10-4.fc16.i686.rpm
```

9. To display general information about the package you just downloaded by querying the package's RPM file in the current directory, type the following:

```
# rpm -qip ImageMagick-6.7.0.10-4.fc16.i686.rpm
Name        : ImageMagick
Version     : 6.7.0.10
Release     : 4.fc16
Architecture: i686
...
```

10. To remove the package containing the `mogrify` command from your system, type the following:

```
# yum remove ImageMagick
```

Chapter 11: Managing User Accounts

For questions that involve adding and removing user accounts, you can use either the User Manager window or command-line tools such as `useradd` and `usermod`. The point is to make sure that you get the correct results shown in the answers that follow, not necessarily do it exactly the same way I did. There are multiple ways you can achieve the same results. The answers here show how to complete the exercises from the command line. (Become root user when you see a # prompt.)

1. To add a local user account to your Linux system that has a username of jbaxter and a full name of John Baxter, that uses `/bin/sh` as its default shell, and that is the next available UID (yours may differ from the one shown here), type the following. You can use the `grep` command to check the new user account. Then set the password for jbaxter to: **My1N1te0ut!**

```
# useradd -c "John Baxter" -s /bin/sh jbaxter
# grep jbaxter /etc/passwd
jbaxter:x:1001:1001:John Baxter:/home/jbaxter:/bin/sh
# passwd jbaxter
Changing password for user jbaxter
New password: My1N1te0ut!
Retype new password: My1N1te0ut!
passwd: all authentication tokens updated successfully
```

2. To create a group account named testing that uses group ID 315, type the following:

```
# groupadd -g 315 testing
# grep testing /etc/group
testing:x:315:
```

3. To add jbaxter to the testing group and the bin group, type the following:

```
# usermod -aG testing,bin jbaxter
# grep jbaxter /etc/group
bin:x:1:bin,daemon,jbaxter
jbaxter:x:1001:
testing:x:315:jbaxter
```

4. To become jbaxter and temporarily have the testing group be jbaxter's default group, run `touch /home/jbaxter/file.txt` — so the testing group is assigned as the file's group — and do the following:

```
$ su - jbaxter
Password: My1N1te0ut!
-sh-4.2$ newgrp testing
sh-4.2$ touch /home/jbaxter/file.txt
sh-4.2$ ls -l /home/baxter/file.txt
-rw-rw-r--. 1 jbaxter testing 0 Jan 25 06:42 /home/jbaxter/file.txt
sh-4.2$ exit ; exit
```

5. Note what user ID has been assigned to jbaxter and then delete the user account without deleting the home directory assigned to jbaxter.

```
$ userdel jbaxter
```

6. Use the following command to find any files in the `/home` directory (and any subdirectories) that are assigned to the user ID that recently belonged to the user named jbaxter (when I did it, the UID/GID were both 1001; yours may differ). Notice that the username jbaxter is no longer assigned on the system, so any files that user created are listed as belonging to UID 1001 and GID 1001, except for a couple of files that were assigned to the testing group, because of the `newgrp` command run earlier:

```
# find /home -uid 1001 -ls
262184  4 drwx------ 4 1001  1001  4096 Jan 25 08:00 /home/jbaxter
262193  4 -rw-r--r-- 1 1001  1001   176 Jan 27  2011 /home/jbaxter
/.bash_profile
262196  4 -rw------- 1 13602 testing 93 Jan 25 08:00 /home/jbaxter
/.bash_history
262194  0 -rw-rw-r-- 1 13602 testing  0 Jan 25 07:59 /home/jbaxter/file.txt
...
```

7. Run these commands to copy the `/etc/services` file to the `/etc/skel/` directory; then add a new user to the system named mjones, with a full name of Mary Jones and a home directory of `/home/maryjones`. List her home directory to make sure the services file is there.

```
# cp /etc/services /etc/skel/
# useradd -d /home/maryjones -c "Mary Jones" mjones
# ls -l /home/maryjones
total 628
-rw-r--r--. 1 mjones mjones 640999 Jan 25 06:27 services
```

8. Run the following command to find all files under the `/home` directory that belong to mjones. If you did the exercises in order, notice that after you deleted the user with the highest user ID and group ID, those numbers were assigned to mjones. As a result, any files left on the system by jbaxter now belong to mjones. (For this reason, you should remove or change ownership of files left behind when you delete a user.)

```
# find /home -user mjones -ls
262184 4 drwx------ 4 mjones mjones 4096 Jan 25 08:00 /home/jbaxter
262193 4 -rw-r--r-- 1 mjones mjones 176 Jan 27 2011 /home/jbaxter
/.bash_profile
262189 4 -rw-r--r-- 1 mjones mjones 18 Jan 27 2011 /home/jbaxter/.bash_logout
262194 0 -rw-rw-r-- 1 mjones testing 0 Jan 25 07:59 /home/jbaxter/file.txt
262188 4 -rw-r--r-- 1 mjones mjones 124 Jan 27 2011 /home/jbaxter/.bashrc
262197 4 drwx------ 4 mjones  mjones 4096 Jan 25 08:27 /home/maryjones
262207 4 -rw-r--r-- 1 mjones mjones 176 Jan 27 2011 /home/maryjones
/.bash_profile
262202 4 -rw-r--r-- 1 mjones mjones 18 Jan 27 2011 /home/maryjones
/.bash_logout
262206 628 -rw-r--r-- 1 mjones mjones 640999 Jan 25 08:27 /home/maryjones/
services
262201 4 -rw-r--r-- 1 mjones mjones 124 Jan 27 2011 /home/maryjones/.bashrc
```

9. As the user mjones, you can use the following to create a file called `/tmp/maryfile.txt` and use ACLs to assign the bin user read/write permission and the lp group read/write permission to that file.

```
[mjones]$ touch /tmp/maryfile.txt
[mjones]$ setfacl -m u:bin:rw /tmp/maryfile.txt
[mjones]$ setfacl -m g:lp:rw /tmp/maryfile.txt
```

```
[mjones]$ getfacl /tmp/maryfile.txt
# file: tmp/maryfile.txt
# owner: mjones
# group: mjones
user::rw-
user:bin:rw-
group::rw-
group:lp:rw-
mask::rw-
other::r—
```

10. Run this set of commands (as `mjones`) to create a directory named `/tmp/mydir` and use ACLs to assign default permissions to it so that the `adm` user has read/write/execute permission to that directory and any files or directories created in it. Test that it worked by creating the `/tmp/mydir/testing/` directory and `/tmp/mydir/newfile.txt`.

```
[mary]$ mkdir /tmp/mydir
[mary]$ setfacl -m d:u:adm:rwx /tmp/mydir
[mjones]$ getfacl /tmp/mydir
# file: tmp/mydir
# owner: mjones
# group: mjones
user::rwx
group::rwx
other::r-x
default:user::rwx
default:user:adm:rwx
default:group::rwx
default:mask::rwx
default:other::r-x
[mjones]$ mkdir /tmp/mydir/testing
[mjones]$ touch /tmp/mydir/newfile.txt
[mjones]$ getfacl /tmp/mydir/testing/
# file: tmp/mydir/testing/
# owner: mjones
# group: mjones
user::rwx
user:adm:rwx
group::rwx
mask::rwx
other::r-x
default:user::rwx
default:user:adm:rwx
default:group::rwx
default:mask::rwx
default:other::r-x
[mjones]$ getfacl /tmp/mydir/newfile.txt
# file: tmp/mydir/newfile.txt
```

```
# owner: mjones
# group: mjones
user::rw-
user:adm:rwx     #effective:rw-
group::rwx       #effective:rw-
mask::rw-
other::r--
```

Notice that the `adm` user effectively has only `rw-` permission. To remedy that, you need to expand the permissions of the mask. One way to do that is with the `chmod` command, as follows:

```
[mjones]$ chmod 775 /tmp/mydir/newfile.txt
[mjones]$ getfacl /tmp/mydir/newfile.txt
# file: tmp/mydir/newfile.txt
# owner: mjones
# group: mjones
user::rwx
user:adm:rwx
group::rwx
mask::rwx
other::r-x
```

Chapter 12: Managing Disks and Filesystems

1. To determine the device name of a USB flash drive that you want to insert into your computer, type the following and insert the USB flash drive.

```
# tail -f /var/log/messages
kernel: [sdb] 15667200 512-byte logical blocks:
     (8.02 GB/7.47 GiB)
Feb 11 21:55:59 cnegus kernel: sd 7:0:0:0:
     [sdb] Write Protect is off
Feb 11 21:55:59 cnegus kernel: [sdb] Assuming
     drive cache: write through
Feb 11 21:55:59 cnegus kernel: [sdb] Assuming
     drive cache: write through
```

2. To list partitions on the USB flash drive, type the following:

```
# fdisk -c -u -l /dev/sdb
```

3. To delete partitions on the USB flash drive, assuming device `/dev/sdb`, do the following:

```
# fdisk -cu /dev/sdb
Command (m for help): d
Partition number (1-6): 6
Command (m for help): d
Partition number (1-5): 5
Command (m for help): d
Partition number (1-5): 4
```

```
Command (m for help): d
Partition number (1-4): 3
Command (m for help): d
Partition number (1-4): 2
Command (m for help): d
Selected partition 1
Command (m for help): w
# partprobe /dev/sdb
```

4. To add a 100MB Linux partition, 200MB swap partition, and 500MB LVM partition to the USB flash drive, type the following:

```
# fdisk -cu /dev/sdb

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First sector (2048-15667199, default 2048): <ENTER>
Last sector, +sectors or +size{K,M,G} (default 15667199): +100M
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 2
First sector (616448-8342527, default 616448): <ENTER>
Last sector, +sectors or +size{K,M,G} (default 15667199): +200M
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 3
First sector (616448-15667199, default 616448): <ENTER>
Using default value 616448
Last sector, +sectors or +size{K,M,G} (default 15667199): +500M
Command (m for help): t
Partition number (1-4): 2
Hex code (type L to list codes): 82
Changed system type of partition 2 to 82 (Linux swap / Solaris)
Command (m for help): t
Partition number (1-4): 3
Hex code (type L to list codes): 8e
Changed system type of partition 3 to 8e (Linux LVM)
Command (m for help): w
# partprobe /dev/sdb
# grep sdb /proc/partitions
   8       16    7833600 sdb
```

```
8       17     102400 sdb1
8       18     204800 sdb2
8       19     512000 sdb3
```

5. To put an `ext3` filesystem on the Linux partition, type the following:

   ```
   # mkfs -t ext3 /dev/sdb1
   ```

6. To create a mount point called `/mnt/mypart` and mount the Linux partition on it temporarily, do the following:

   ```
   # mkdir /mnt/mypart
   # mount -t ext3 /dev/sdb1 /mnt/mypart
   ```

7. To enable the swap partition and turn it on so that there is additional swap space immediately available, type the following:

   ```
   # mkswap /dev/sdb2
   # swapon /dev/sdb2
   ```

8. To create a volume group called `abc` from the LVM partition, create a 200MB logical volume from that group called `data`, create a VFAT filesystem on it, temporarily mount the logical volume on a new directory named `/mnt/test`, and then check that it was successfully mounted, type the following:

   ```
   # pvcreate /dev/sdb3
   # vgcreate abc /dev/sdb3
   # lvcreate -n data -L 200M abc
   # mkfs -t vfat /dev/mapper/abc-data
   # mkdir /mnt/test
   # mount /dev/mapper/abc-data /mnt/test
   ```

9. To grow the logical volume from 200MB to 300MB, type the following:

   ```
   # lvextend -L +100M /dev/mapper/abc-data
   # resize2fs -p /dev/mapper/abc-data
   ```

10. To safely remove the USB flash drive from the computer, do the following:

    ```
    # umount /dev/sdb1
    # swapoff /dev/sdb2
    # umount /mnt/test
    # lvremove /dev/mapper/abc-data
    # vgremove abc
    # pvremove /dev/sdb3
    ```

    You can now safely remove the USB flash drive from the computer.

Chapter 13: Understanding Server Administration

1. To log in to any account on another computer using the `ssh` command, type the following, and then enter the password when prompted:

   ```
   $ ssh joe@localhost
   joe@localhost's password:
   ```

```
********
[joe]$
```

2. To display the contents of a remote `/etc/system-release` file and have its contents displayed on the local system using remote execution with the `ssh` command, do the following:

```
$ ssh joe@localhost "cat /etc/system-release"
Fedora release 16 (Verne)
```

3. To use X11 forwarding to display a gedit window on your local system, then save a file on the remote home directory, do the following:

```
$ ssh -X joe@localhost "gedit newfile"
joe@localhost's password:
********
$ ssh joe@localhost "cat newfile"
joe@localhost's password:
********
This is text from the file I saved in joe's remote home directory
```

4. To recursively copy all the files from the `/usr/share/selinux` directory on a remote system to the `/tmp` directory on your local system in such a way that all the modification times on the files are updated to the time on the local system when they are copied, do the following:

```
$ scp -r joe@localhost:/usr/share/selinux /tmp
joe@localhost's password:
********
irc.pp.bz2                              100% 9673     9.5KB/s   00:00
dcc.pp.bz2                              100%   15KB  15.2KB/s   00:01
$ ls -l /tmp/selinux | head
total 20
drwxr-xr-x. 3 root root  4096 Apr 18 05:52 devel
drwxr-xr-x. 2 root root  4096 Apr 18 05:52 packages
drwxr-xr-x. 2 root root 12288 Apr 18 05:52 targeted
```

5. To recursively copy all the files from the `/usr/share/logwatch` directory on a remote system to the `/tmp` directory on your local system in such a way that all the modification times on the files from the remote system are maintained on the local system, try this:

```
$ rsync -av joe@localhost:/usr/share/logwatch /tmp
joe@localhost's password:
********
receiving incremental file list
logwatch/
logwatch/default.conf/
logwatch/default.conf/logwatch.conf
$ ls -l /tmp/logwatch | head
total 16
drwxr-xr-x. 5 root root 4096 Apr 19  2011 default.conf
```

```
drwxr-xr-x. 4 root root 4096 Feb 28  2011 dist.conf
drwxr-xr-x. 2 root root 4096 Apr 19  2011 lib
```

6. To create a public/private key pair to use for SSH communications (no passphrase on the key), copy the public key file to a remote user's account with `ssh-copy-id`, and use key-based authentication to log in to that user account without having to enter a password, use the following code:

```
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/joe/.ssh/id_rsa): <ENTER>
/home/joe/.ssh/id_rsa already exists.
Enter passphrase (empty for no passphrase):  <ENTER>
Enter same passphrase again:  <ENTER>
Your identification has been saved in /home/joe/.ssh/id_rsa.
Your public key has been saved in /home/joe/.ssh/id_rsa.pub.
The key fingerprint is:
58:ab:c1:95:b6:10:7a:aa:7c:c5:ab:bd:f3:4f:89:1e joe@cnegus.csb
The key's randomart image is:
$ ssh-copy-id -i ~/.ssh/id_rsa.pub joe@localhost
joe@localhost's password: ********
Now try logging into the machine, with "ssh 'joe@localhost'",
and check in:
.ssh/authorized_keys
to make sure we haven't added extra keys that you weren't expecting.
$ ssh joe@localhost
$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyN2Psp5/LRUC9E8BDCx53yPUa0qoOPd
v6H4sF3vmn04V6E7D1iXpzwPzdo4rpvmR1ZiinHR2xGAEr2uZag7feKgLnww2KPcQ6S
iR7lzrOhQjV+SGb/a1dxrIeZqKMq1Tk07G4EvboIrq//9J47vI4l7iNu0xRmjI3TTxa
DdCTbpG6J3uSJm1BKzdUtwb413x35W2bRgMI75aIdeBsDgQBBiOdu+zuTMrXJj2viCA
XeJ7gIwRvBaMQdOSvSdlkX353tmIjmJheWdgCccM/1jKdoELpaevg9anCe/yUP3so31
tTo4I+qTfzAQD5+66oqW0LgMkWVvfZI7dUz3WUPmcMw== chris@abc.example.com
```

7. To create an entry in `/etc/rsyslog.conf` that stores all authentication messages at the info level and higher into a file named `/var/log/myauth`, do the following. Watch from one terminal as the data comes in.

```
# vim /etc/rsyslog.conf
authpriv.info                                 /var/log/myauth
# service rsyslog restart
     or
# systemctl restart rsyslog.service
<Terminal 1>                                  <Terminal 2>
# tail -f /var/log/myauth                     $ ssh joe@localhost
Apr 18 06:19:34 abc unix_chkpwd[30631]        joe@localhost's password:
Apr 18 06:19:34 abc sshd[30631]               Permission denied,try again
 :pam_unix(sshd:auth):
 authentication failure;logname= uid=501
 euid=501 tty=ssh ruser= rhost=localhost
 user=joe
```

```
Apr 18 06:19:34 abc sshd[30631]:
 Failed password for joe from
 127.0.0.1 port 5564 ssh2
```

8. To determine the largest directory structures under `/usr/share`, sort them from largest to smallest, and list the top 10 of those directories in terms of size using the `du` command, type the following:

```
$ du -s /usr/share/* | sort -rn | head
458320  /usr/share/locale
129400  /usr/share/doc
124116  /usr/share/icons
80524   /usr/share/gnome
...
```

9. To show the space that is used and available from all the filesystems currently attached to the local system, but exclude any `tmpfs` or `devtmpfs` filesystems by using the `df` command, type the following:

```
$ df -h -x tmpfs -x devtmpfs
Filesystem      Size  Used Avail Use% Mounted on
/deev/sda4       20G  4.2G 16G    22% /
```

10. To find any files in the `/usr` directory that are more than 10MB in size, do the following:

```
$ find /usr -size +10M
/usr/lib/jvm/java-1.6.0-openjdk-1.6.0.0/jre/lib/rt.jar
/usr/lib/jvm/java-1.7.0-openjdk-1.7.0.3/jre/lib/rt.jar
/usr/lib/llvm/libLLVM-2.9.so
/usr/lib/flash-plugin/libflashplayer.so
```

Chapter 14: Administering Networking

1. To use the desktop to check that NetworkManager has successfully started your network interface (wired or wireless), do the following:

   Left-click the NetworkManager icon in your top panel. Any active wired or wireless network connections should be highlighted in bold.

   If it has not connected to the network, select from the list of wired or wireless networks available, and then enter the username and password, if prompted, to start an active connection.

2. To run a command to check the active network interfaces available on your computer, type:

```
$ ifconfig
```

   or

```
$ ip addr show
```

3. Try to contact `google.com` from the command line in a way that ensures that DNS is working properly:

```
$ ping google.com
Ctrl-C
```

4. To run a command to check the routes being used to communicate outside of your local network, type:

```
$ route
```

5. To trace the route being taken to connect to `google.com`, use the `traceroute` command:

```
$ traceroute google.com
```

6. To turn off and disable NetworkManager and start the network service, do the following:

   From an RHEL 6 system, type:

```
# service NetworkManager stop
# service network restart
# chkconfig NetworkManager off
# chkconfig network on
```

   For newer Fedora systems, type:

```
# systemctl stop NetworkManager.service
# systemctl disable NetworkManager.service
# service network restart
# chkconfig network on
```

7. To create a host entry that allows you to communicate with your local host system using the name myownhost, do the following:

   Edit the `/etc/hosts` file (`vi /etc/hosts`) and add `myownhost` to the end of the localhost entry so it appears as follows (then ping `myownhost` to see if it worked):

```
127.0.0.1               localhost.localdomain localhost myownhost
# ping myownhost
Ctrl+C
```

8. To add the public Google DNS server (IP address 8.8.8.8) as the last in your list of DNS servers, take the following action:

   Make a copy of your `resolv.conf` file before proceeding (then copy it back after the procedure is done):

```
# cp /etc/resolv.conf $HOME
```

   If you are using the NetworkManager service, left-click the NetworkManager icon and select Network Settings. Select the IPv4 Settings. Then select the Method box and choose Automatic (DHCP) addresses only and fill in 8.8.8.8 in

the DNS servers box (along with any other DNS servers you need). If that doesn't work, try one of the DNS servers listed in the `resolv.conf` file you just copied to your home directory.

Or, if you are using the network service, edit the `/etc/resolv.conf` file directly, so the file includes at least the following line:

```
nameserver 8.8.8.8
```

In either case, use the `dig` command to check that the DNS server was able to resolve an address:

```
# dig google.com
...
google.com.      91941    IN      NS      ns3.google.com.
;; Query time: 0 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Apr 30 13:57:44 2012
;; MSG SIZE  rcvd: 276
```

9. To create a custom route that directs traffic destined for the 192.168.99.0/255.255.255.0 network to some IP address on your local network, such as 192.168.0.5 (first ensuring that the 10.0.99 network is not being used at your location), do the following:

   Determine the name of your network interface. For RHEL, your first network interface is probably `eth0`. In that case, as root run the following commands:

   ```
   # cd /etc/sysconfig/network-scripts
   # vi route-eth0
   ```

   Add the following lines to that file:

   ```
   ADDRESS0=192.168.99.0
   NETMASK0=255.255.255.0
   GATEWAY0=192.168.0.5
   ```

   Restart networking and run `route` to see that the route is active:

   ```
   # service network restart
   # route
   Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
   default         192.168.0.1     0.0.0.0         UG    0      0        0 eth0
   192.168.0.0     *               255.255.255.0   U     1      0        0 eth0
   192.168.99.0    192.168.0.5     255.255.255.0   UG    0      0        0 eth0
   ```

10. To check to see if your system has been configured to allow IPv4 packets to be routed between network interfaces on your system, type the following:

    ```
    # cat /proc/sys/net/ipv4/ip_forward
    0
    ```

    A `0` shows that IPv4 packet forwarding is disabled; a `1` shows it is enabled.

Chapter 15: Starting and Stopping Services

1. To determine which `init` daemon your server is currently using, consider the following:

   - You have the `Upstart init` daemon if:

   Your Linux server runs one of the following distributions: RHEL version 6, Fedora versions 9 through 14, Ubuntu versions 6–10 or greater, or openSUSE versions 11.3 or greater. And the `strings` command shows `Upstart init` in use as demonstrated in the example below:

```
$ strings /sbin/init | grep -i upstart
upstart-devel@lists.ubuntu.com
UPSTART_CONFDIR
UPSTART_NO_SESSIONS
...
```

   - You have the `systemd` daemon if:

   Your Linux server runs Fedora version 15 or greater. And the `strings` command shows `systemd` in use as demonstrated in the example below:

```
# strings /sbin/init | grep -i systemd
systemd.unit=
systemd.log_target=
systemd.log_level=
...
```

   - Most likely, you have the `SysVinit` or `BSD init` daemon if your `init` daemon is not the `Upstart init` daemon or `systemd`. But double check at `http://wikipedia.org/wiki/Init`.

2. To determine what `init` daemon `sshd` is using on your Linux server, be aware that the `init` daemon that `sshd` uses is not solely dependent upon which `init` daemon the server is currently using. Several services may not yet be ported over to new `init` daemons. Therefore, try out both the newer `init` daemon and the classic `SysVinit` commands.

   - For the `Upstart init` daemon, a positive result, shown here, means the `sshd` has been converted to `Upstart`:

```
# initctl status ssh
ssh start/running, process 2390
```

   - For `systemd`, a positive result, shown here, means the `sshd` has been converted to `systemd`:

```
# systemctl status sshd.service
sshd.service - OpenSSH server daemon
  Loaded: loaded (/lib/systemd/system/sshd.service; enabled)
  Active: active (running) since Mon, 30 Apr 2015 12:35:20...
```

- If you don't see positive results for the preceding tests, try the following command for the SysVinit `init` daemon. A positive result here, along with negative results for the preceding tests, means `sshd` is still using the SysVinit daemon.

```
# service ssh status
sshd (pid 2390) is running...
```

3. To determine your server's previous and current `runlevel`, use the `runlevel` command. It still works on all `init` daemons:

```
$ runlevel
N 3
```

4. To change the default `runlevel` or `target unit` on your Linux server, you can do one of the following (depending upon your server's `init` daemon):
   - For the SysVinit daemon, edit the file `/etc/inittab` and change the # in the line `id:#:initdefault:` to either `2`, `3`, `4`, or `5`.
   - For the `Upstart init` daemon, edit the file `/etc/inittab` and change the # in the line `id:#:initdefault:` to either `2`, `3`, `4`, or `5`.
   - For `systemd`, change the `default.target` symbolic link to the desired `runlevel#.target`, where # is either `2`, `3`, `4`, or `5`. The following shows you how to change the symbolic link for the `target unit` to `runlevel3.target`.

```
# ln -sf /lib/systemd/system/runlevel3.target
 /etc/systemd/system/default.target
/lib/systemd/system/runlevel3.target
```

5. To list out services running (or active) on your server, you will need to use different commands, depending upon the `init` daemon you are using.
   - For the SysVinit daemon, use the `service` command as shown in the example that follows::

```
# service --status-all | grep running... | sort
anacron (pid 2162) is running...
atd (pid 2172) is running...
...
```

   - For the `Upstart init` daemon, use the `initctl` command. However, also be sure to use the `service` command, because not all services may have been ported to `Upstart`:

```
# initctl list | grep start/running
tty (/dev/tty3) start/running, process 1163
...
# service --status-all | grep running
abrtd (pid  1118) is running...
...
```

- For systemd, use the systemctl command, as follows:

```
# systemctl list-unit-files --type=service | grep -v disabled
UNIT FILE                                   STATE
abrt-ccpp.service                           enabled
abrt-oops.service                           enabled
...
```

6. To list out the running (or active) services on your Linux server, use the appropriate command(s) determined in Answer 5 for the init daemon your server is using.
7. For each init daemon, the following command(s) will show a particular service's current status:
   - For the SysVinit daemon, the service *service_name* status command is used.
   - For the Upstart init daemon, the initctl status *service_name* command is used.
   - For systemd, the systemctl status *service_name* command is used.
8. To show the status of the cups daemon on your Linux server, use the following:
   - For the SysVinit daemon:

```
# service cups status
cupsd (pid 8236) is running...
```

   - For the Upstart init daemon:

```
# initctl status cups
cups start/running, process 2390
```

     Remember that if a service has not yet been ported to Upstart, you will need to use the service command instead of initctl.

   - For systemd:

```
# systemctl status cups.service
cups.service - CUPS Printing Service
    Loaded: loaded (/lib/systemd/system/cups.service; enabled)
    Active: active (running) since Tue, 01 May 2015 04:43:5...
  Main PID: 17003 (cupsd)
    CGroup: name=systemd:/system/cups.service
            17003 /usr/sbin/cupsd -f
```

9. To attempt to restart the cups daemon on your Linux server, use the following:
   - For the SysVinit daemon:

```
# service cups restart
Stopping cups:          [  OK  ]
Starting cups:          [  OK  ]
```

   - For the Upstart init daemon:

```
# initctl restart cups
cups start/running, process 2490
```

Remember that if a service has not yet been ported to `Upstart`, you will need to use the `service` command instead of `initctl`.

- For `systemd`:

```
# systemctl restart cups.service
```

10. To attempt to reload the `cups` daemon on your Linux server, use the following:
    - For the `SysVinit` daemon:

```
# service cups reload
Reloading cups:            [  OK  ]
```

    - For the `Upstart init` daemon:

```
# initctl reload cups
```

      Remember that if a service has not yet been ported to `Upstart`, you will need to use the `service` command instead of `initctl`.

    - For `systemd`, this is a trick question. You cannot reload the `cups` daemon on a `systemd` Linux server!

```
# systemctl reload cups.service
Failed to issue method call: Job type reload is
 not applicable for unit cups.service.
```


Chapter 16: Configuring a Print Server

For questions that involve working with printers, you can use either graphical or command-line tools in most cases. The point is to make sure that you get the correct results, shown in the answers that follow. The answers here include a mix of graphical and command-line ways of solving the exercises. (Become root user when you see a # prompt.)

1. To use the printer configuration window to add a new printer called `myprinter` to your system (generic PostScript printer, connected to a port), do the following from Fedora 16:
   a. From the GNOME 3 desktop, select Applications ➢ Other ➢ Printing.
   b. Select the Add button (type the root password, if prompted).
   c. Select a Serial, LPT, or other port as the device and click Forward.
   d. For the driver, choose Generic and click Forward; then choose PostScript Printer and click Forward.
   e. Click Forward to skip any installable options.
   f. For the printer name, call it `myprinter`, give it any Description and Location you like, and click Apply.
   g. Click No, to not print a test page. The printer should appear in the Printer Configuration window.

2. To use the `lpc` command to see the status of all your printers, type the following:

```
# lpc status
myprinter:
  queuing is enabled
  printing is enabled
  no entries
  daemon present
```

3. To use the `lpr` command to print the `/etc/hosts` file, type the following:

```
$ lpr /etc/hosts -P myprinter
```

4. To check the print queue for that printer, type the following:

```
# lpq -P myprinter
myprinter is not ready
Rank    Owner   Job     File(s)             Total Size
1st     root    655     hosts               1024 bytes
```

5. To remove the print job from the queue (cancel it), type the following.

```
# lprm -P myprinter
```

6. To use the printing window to set the basic server setting that publishes your printers so other systems on your local network can print to your printers, do the following:
   a. From the GNOME desktop, select System ➢ Administration ➢ Printing.
   b. Select Server ➢ Settings.
   c. Click to turn on the check box next to "Publish shared printers connected to this session" and click OK.
7. To allow remote administration of your system from a web browser, follow these steps:
   a. From the GNOME desktop, select System ➢ Administration ➢ Printing.
   b. Select Server ➢ Settings.
   c. Click to turn on the check box next to Allow remote administration, and click OK.
8. To demonstrate that you can do remote administration of your system from a web browser on another system, do the following:
   a. In the location box from a browser window from another computer on your network, type **http://*hostname*:631**.
   b. Replace ***hostname*** with the name or IP address of the system running your print service. The CUPS home page should appear from that system.

9. To use the `netstat` command to see which addresses the `cupsd` daemon is listening on, type the following:

```
# netstat -tupln | grep 631
tcp    0    0 0.0.0.0:631      0.0.0.0:*       LISTEN    6492/cupsd
```

10. To delete the `myprinter` printer entry from your system, do the following:
    a. From the Printer configuration window, right-click the myprinter icon and select Delete.
    b. When prompted, select Delete again.

Chapter 17: Configuring a Web Server

1. To install all of the packages associated with the Web Server group on a Fedora system, do the following:

```
# yum groupinstall "Web Server"
```

2. To create a file called `index.html` in the directory assigned to `DocumentRoot` in the main Apache configuration file (with the words My Own Web Server inside), do the following:
   - Determine the location of `DocumentRoot`:

```
# grep ^DocumentRoot /etc/httpd/conf/httpd.conf
DocumentRoot "/var/www/html"
```

   - Echo the words "My Own Web Server" into the `index.html` file located in DocumentRoot:

```
# echo "My Own Web Server" > /var/www/html/index.html
```

3. To start the Apache web server and set it to start up automatically at boot time, then check that it is available from a web browser on your local host, do the following (you should see the words "My Own Web Server" displayed if it is working properly):

   The `httpd` service is started and enabled differently in Fedora and RHEL. In Fedora, type the following:

```
# systemctl start httpd.service
# systemctl enable httpd.service
```

   In RHEL 6 or earlier, type:

```
# service httpd start
# chkconfig httpd on
```

4. To use the `netstat` command to see which ports the `httpd` server is listening on, type the following:

```
# netstat -tupln | grep httpd
tcp      0   0 :::80      :::*    LISTEN   2496/httpd
tcp      0   0 :::443     :::*    LISTEN   2496/httpd
```

5. Try to connect to your Apache web server from a web browser that is outside of the local system. If it fails, correct any problems you encounter by investigating the firewall, SELinux, and other security features.

   If you don't have DNS set up yet, use the IP address of the server to view your Apache server from a remote web browser, such as `http://192.168.0.1`. If you are not able to connect, retry connecting to the server from your browser after performing each of the following steps on the system running the Apache server:

```
# iptables -F
# setenforce 0
# chmod 644 /var/www/html/index.html
```

   The `iptables -F` command flushes the firewall rules. If connecting to the web server succeeds after that, you need to add new firewall rules to open `tcp` ports 80 and 443 on the server. Adding a rule before the last `DROP` or `REJECT` rule that does the following should do the trick.

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
```

   The `setenforce 0` command puts your firewall in permissive mode. If connecting to the web server succeeds after that, you need to correct SELinux file context and/or Boolean issues (probably file context in this case). The following should work:

```
# chcon --reference=/var/www/html /var/www/html/index.html
```

   If the `chmod` command works, it means that the apache user and group did not have read permission to the file. You should be able to leave the new permissions as they are.

6. To use the `openssl` or similar command to create your own private RSA key and self-signed SSL certificate, do the following:

```
# yum install openssl
# cd /etc/pki/tls/private
# openssl genrsa -out server.key 1024
# chmod 600 server.key
# cd /etc/pki/tls/certs
# openssl req -new -x509 -nodes -sha1 -days 365 \
   -key /etc/pki/tls/private/server.key \
   -out server.crt
Country Name (2 letter code) [AU]: US
State or Province Name (full name) [Some-State]: NJ
Locality Name (eg, city) []: Princeton
Organization Name (eg, company) [Internet Widgits Pty
```

```
Ltd]:TEST USE ONLY
Organizational Unit Name (eg, section) []:TEST USE ONLY
Common Name (eg, YOUR name) []:secure.example.org
Email Address []:dom@example.org
```

You should now have a `/etc/pki/tls/private/server.key` key file and a `/etc/pki/tls/certs/server.crt` certificate file.

7. To configure your Apache web server to use your key and self-signed certificate to serve secure (HTTPS) content, do the following:

   Edit the `/etc/httpd/conf.d/ssl.conf` file to change the key and certificate locations to use the ones you just created:

   ```
   SSLCertificateFile /etc/pki/tls/certs/server.crt
   SSLCertificateKeyFile /etc/pki/tls/private/server.key
   ```

8. To use a web browser to create an HTTPS connection to your web server and view the contents of the certificate you created, do the following:

   From the system running the Apache server, type **`https://localhost`** in the browser's location box. You should see a message that reads, "This Connection is Untrusted." To complete the connection, do the following:

   - Click I Understand the Risks.
   - Click Add Exception.
   - Click Get Certificate.
   - Click Confirm Security Exception.

9. To create a file named `/etc/httpd/conf.d/example.org.conf`, which turns on name-based virtual hosting and creates a virtual host that 1) listens on port 80 on all interfaces, 2) has a server administrator of `joe@example.org`, 3) has a server name of `joe.example.org`, 4) has a `DocumentRoot` of `/var/www/html/joe.example.org`, and 5) has a `DirectoryIndex` that includes at least `index.html`, and create an `index.html` file in `DocumentRoot` that contains the words "Welcome to the House of Joe" inside, do the following:

   Create an `example.org.conf` file that looks like the following:

   ```
   NameVirtualHost *:80
   <VirtualHost *:80>
       ServerAdmin     joe@example.org
       ServerName      joe.example.org
       ServerAlias     web.example.org
       DocumentRoot    /var/www/html/joe.example.org/
   DirectoryIndex  index.html
   </VirtualHost>
   ```

   This is how you could create the text to go into the `index.html` file:

   ```
   # echo "Welcome to the House of Joe" > /var/www/html/joe.example.org/index
   .html
   ```

10. To add the text **joe.example.org** to the end of the localhost entry in your /etc/hosts file on the machine that is running the web server, and check it by typing **http://joe.example.org** into the location box of your web browser to see "Welcome to the House of Joe" when the page is displayed, do the following:

    - Reload the httpd.conf file modified in the previous exercise:

    ```
    # apachectl graceful
    ```

    - Edit the /etc/hosts file with any text editor so the local host line appears as follows:

    ```
    127.0.0.1       localhost.localdomain localhost joe.example.org
    ```

    - From a browser on the local system where httpd is running, you should be able to type http://joe.example.org into the location box to access the Apache web server using name-based authentication.

Chapter 18: Configuring an FTP Server

CAUTION

Don't do the tasks described here on a working, public FTP server, because these tasks will interfere with its operations. (You could, however, use these tasks to set up a new FTP server.)

1. To determine which package provides the Very Secure FTP Daemon service, type the following as root:

    ```
    # yum search "Very Secure FTP"
    ...
    ================== N/S Matched: Very Secure FTP ==================
    vsftpd.i686 : Very Secure Ftp Daemon
    ```

    The search found the vsftpd package.

2. To install the Very Secure FTP Daemon package on your system and search for the configuration files in that package, type the following:

    ```
    # yum install vsftpd
    # rpm -qc vsftpd | less
    ```

3. To start the Very Secure FTP Daemon service and set it to start when the system boots, type the following on a Fedora system:

    ```
    # systemctl start vsftpd.service
    # systemctl enable vsftpd.service
    ```

    On a Red Hat Enterprise Linux system, type the following:

    ```
    # service vsftpd start
    # chkconfig vsftpd on
    ```

4. On the system running your FTP server, type the following to create a file named `test` in the anonymous FTP directory that contains the words "Welcome to your vsftpd server":

   ```
   # echo "Welcome to your vsftpd server" > /var/ftp/test
   ```

5. To open the `test` file from the anonymous FTP home directory, using a web browser on the system running your FTP server, do the following:

   Start the Firefox web browser, type the following in the location box, and press Enter:

   ```
   ftp://localhost/test
   ```

   The text "Welcome to your Very Secure FTP Daemon server" should appear in the Firefox window.

6. To access the `test` file in the anonymous FTP home directory, do the following. (If you cannot access the file, check that your firewall [`iptables`], SELinux, and TCP wrappers are configured to allow access to that file, as described here.)

   a. Type the following into the location box of a browser on a system on your network that can reach the FTP server (replace *`host`* with your system's fully qualified hostname or IP address):

      ```
      ftp://host/test
      ```

      If you cannot see the welcome message in your browser window, check what may be preventing access. To temporarily turn off your firewall (flush your `iptables` rules), type the following command as the root user from a shell on your FTP server system and then try to access the site again:

      ```
      # iptables -F
      ```

   b. To temporarily disable SELinux, type the following, and then try to access the site again:

      ```
      # setenforce 0
      ```

   c. To temporarily disable TCP wrappers, add the following to the beginning of the `/etc/hosts.allow` file (be sure to remove this line again when the test is done):

      ```
      ALL: ALL
      ```

   Once you have determined what is causing the file on your FTP server to be unavailable, go back to the "Securing Your FTP Server" section and go through the steps to determine what might be blocking access to your file. Likely possibilities include:

   - For `iptables`, make sure there is a rule opening TCP port 21 on the server.
   - For SELinux, make sure the file context is set to `public_content_t`.
   - For TCP wrappers, make sure that there is a `vsftpd: ALL` or similar line in the `/etc/hosts.allow` file. An entry such as this should only be needed if

there is a line in the /etc/hosts.deny file that denies access to services that are not explicitly allowed.

7. To configure your Very Secure FTP Daemon server to allow file uploads by anonymous users to a directory named in, do the following as root on your FTP server:

   a. Create the in directory as follows:

```
# mkdir /var/ftp/in
# chown ftp:ftp /var/ftp/in
# chmod 770 /var/ftp/in
```

   b. Inside the /etc/vsftpd/vsftpd.conf file, make sure that the following variables are set:

```
anonymous_enable=YES
write_enable=YES
anon_upload_enable=YES
```

   c. Configure your iptables firewall to allow new requests on TCP port 21 by adding the following rule at some point before a final DROP or REJECT rule in your /etc/sysconfig/iptables file:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
```

   d. Configure your iptables firewall to do connection tracking by loading the appropriate module to the /etc/sysconfig/iptables-config file:

```
IPTABLES_MODULES="nf_conntrack_ftp"
```

   e. For SELinux to allow uploading to the directory, first set file contexts properly:

```
# semanage fcontext -a -t public_content_rw_t "/var/ftp/in(/.*)?"
# restorecon -F -R -v /var/ftp/in
```

   f. Next, set the SELinux Boolean to allow uploading:

```
# setsebool -P allow_ftpd_anon_write on
```

   g. Restart the vsftpd service (service vsftpd restart or systemctl restart vsftpd.service).

8. To install the lftp FTP client (if you don't have a second Linux system, install lftp on the same host running the FTP server) and try to upload the /etc/hosts file to the incoming directory on the server, run the following commands as the root user:

```
# yum install lftp
# lftp localhost
lftp localhost:/> cd in
lftp localhost:/in> put /etc/hosts
89 bytes transferred
lftp localhost:/in>
quit
```

You won't be able to see that you copied the `hosts` file to the incoming directory. However, type the following from a shell on the host running the FTP server to make sure the `hosts` file is there:

```
# ls /var/ftp/in
Hosts
```

If you cannot upload the file, troubleshoot the problem as described in Exercise 7, recheck your `vsftpd.conf` settings, and review the ownership and permissions on the `/var/ftp/in` directory.

9. Using any FTP client you choose, visit the `/pub/linux/docs/man-pages` directory on the `ftp://kernel.org` site and list the contents of that directory. Here's how to do that with the `lftp` client:

```
# lftp ftp://kernel.org/pub/linux/docs/man-pages
cd ok, cwd=/pub/linux/docs/man-pages
lftp kernel.org:/pub/linux/docs/man-pages> ls
drwxrwsr-x 2 536  536   24576 May 10 20:29 Archive
-rw-rw-r-- 1 536  536 1135808 Feb 09 23:23 man-pages-3.34.tar.bz2
-rw-rw-r-- 1 536  536 1674738 Feb 09 23:23 man-pages-3.34.tar.gz
-rw-rw-r-- 1 536  536     543 Feb 09 23:23 man-pages-3.34.tar.sign
...
```

10. Using any FTP client you choose, download the `man-pages-3.41.tar.gz` file from the `kernel.org` directory you just visited to the `/tmp` directory on your local system.

```
# lftp ftp://kernel.org/pub/linux/docs/man-pages
cd ok, cwd=/pub/linux/docs/man-pages
lftp kernel.org:man-pages> get man-pages-3.41.tar.gz
1739208 bytes transferred in 4 seconds (481.0K/s)
lftp kernel.org:man-pages> quit
```

Chapter 19: Configuring a Windows File Sharing (Samba) Server

1. To install the `samba`, `samba-client`, and `samba-doc` packages, type the following as root from a shell on the local system:

```
# yum install samba samba-client samba-doc
```

2. To start and enable the `smb` and `nmb` services, type the following as root from a shell on the local system:

```
# systemctl enable smb.service
# systemctl start smb.service
# systemctl enable nmb.service
# systemctl start nmb.service
```

or

```
# chkconfig smb on
# service smb start
# chkconfig nmb on
# service nmb start
```

3. To set the Samba server's workgroup to `TESTGROUP`, the `netbios name` to `MYTEST`, and the server string to `Samba Test System`, as root user in a text editor, open the `/etc/samba/smb.conf` file and change three lines so they appear as follows:

```
workgroup = TESTGROUP
netbios name = MYTEST
server string = Samba Test System
```

4. To add a Linux user named `phil` to your system and add a Linux password and Samba password for `phil`, type the following as root user from a shell (be sure to remember the passwords you set):

```
# useradd phil
# passwd phil
New password: *******
Retype new password: *******
# smbpasswd -a phil
New SMB password: *******
Retype new SMB password: *******
Added user phil.
```

5. To set the `[homes]` section so that home directories are browseable (`yes`) and writable (`yes`), and that `phil` is the only valid user, open the `/etc/samba/smb.conf` file as root and change the `[homes]` section so it appears as follows:

```
[homes]

        comment = Home Directories
        browseable = yes
        writable = yes
        valid users = phil
```

6. To set SELinux Booleans that are necessary to make it so `phil` can access his home directory via a Samba client, type the following as root from a shell:

```
# setsebool -P samba_enable_home_dirs on
```

7. From the local system, use the `smbclient` command to list that the homes share is available.

```
# smbclient -L localhost
Enter root's password:
<ENTER>
Anonymous login successful
Domain=[DATAGROUP] OS=[Unix] Server=Samba 3.6.5-85.fc16
```

```
    Sharename       Type      Comment
    ---------       ----      -------
    homes           Disk      Home Directories
...
```

8. To connect to the `homes` share from a Nautilus (file manager) window on the Samba server's local system for the user `phil` in a way that allows you to drag and drop files to that folder, do the following:
   a. Open the Nautilus window (select the files icon).
   b. Under the Network heading in the left pane, select Browse Network.
   c. Open the Samba server (MYTEST icon).
   d. Open the `homes` share.
   e. When prompted, type **`phil`** as the username and enter phil's password.
   f. Open another Nautilus window and drop a file to phil's homes folder.

9. To open up the firewall so anyone who has access to the server can access the Samba service (`smbd` and `nmbd` daemons), change the `/etc/sysconfig/iptables` file so the firewall appears like the following (the rules you add being those in bold):

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-I INPUT -m state --state NEW -m udp -p udp --dport 137 -j ACCEPT
-I INPUT -m state --state NEW -m udp -p udp --dport 138 -j ACCEPT
-I INPUT -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT
-I INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

   Then type the following for the firewall rules to be reloaded:

```
# service iptables restart
```

10. To open the `homes` share again as the user `phil` from another system on your network (Windows or Linux), and make sure you can drag and drop files to it, do the following:

    This step is really just repeating the Nautilus example described previously or accessing a Windows Explorer window and opening the share (by selecting Network, then the Samba server). The trick is to make sure the service has been made available through the Linux server security features.

If you cannot access the Samba share, try disabling your firewall and then disabling SELinux. If the share is accessible when you turn off either of those services, go back and debug the problems with the service that is not working:

```
# setenforce 0
# service iptables stop
```

When you have fixed the problem, set SELinux back to Enforcing mode and restart `iptables`:

```
# setenforce 1
# service iptables start
```

Chapter 20: Configuring an NFS File Server

1. To install the packages needed to configure the NFS service on the Linux system you choose, type the following as root user at a shell (Fedora or RHEL):

   ```
   # yum install nfs-utils
   ```

2. To list the documentation files that come in the package that provides the NFS server software, type the following:

   ```
   # rpm -qd nfs-utils
   /usr/share/doc/nfs-utils-1.2.5/ChangeLog
   ...
   /usr/share/man/man5/exports.5.gz
   /usr/share/man/man5/nfs.5.gz
   /usr/share/man/man5/nfsmount.conf.5.gz
   /usr/share/man/man7/nfsd.7.gz
   /usr/share/man/man8/blkmapd.8.gz
   /usr/share/man/man8/exportfs.8.gz
   ...
   ```

3. To determine the name of the NFS service, start it, and enable it, type the following as root user on the NFS server:

   ```
   # systemctl start nfs-server.service
   # systemctl enable nfs-server.service
   ```

4. To check the status of the NFS service you just started on the NFS server, type the following as root user:

   ```
   # systemctl status nfs-server.service
   ```

5. To share a directory `/var/mystuff` from your NFS server as available to everyone, read-only, and with the root user on the client having root access to the share, first create the mount directory as follows:

   ```
   # mkdir /var/mystuff
   ```

   Then create an entry in the `/etc/exports` file that is similar to the following:

   ```
   /var/mystuff    *(ro,no_root_squash,insecure)
   ```

To make the share available, type the following:

```
# exportfs -v -a
exporting *:/var/mystuff
```

6. To make sure the share you created is accessible to all hosts, first check that `rpcbind` is not blocked by TCP wrappers by adding the following entry to the beginning of the `/etc/hosts.allow` file:

   ```
   rpcbind: ALL
   ```

   To open the ports needed to allow clients to reach NFS through the `iptables` firewall, you need to open at least TCP and UDP ports 111 (`rpcbind`), 20048 (`mountd`), and 2049 (`nfs`) by adding the following rules to the `/etc/sysconfig/iptables` file and starting the `iptables` service:

   ```
   -A INPUT -m state --state NEW -m tcp -p tcp --dport 111 -j ACCEPT
   -A INPUT -m state --state NEW -m udp -p udp --dport 111 -j ACCEPT
   -A INPUT -m state --state NEW -m tcp -p tcp --dport 2049 -j ACCEPT
   -A INPUT -m state --state NEW -m udp -p udp --dport 2049 -j ACCEPT
   -A INPUT -m state --state NEW -m tcp -p tcp --dport 20048 -j ACCEPT
   -A INPUT -m state --state NEW -m udp -p udp --dport 20048 -j ACCEPT
   ```

   SELinux should be able to share NFS filesystems while in Enforcing mode without any changes to file contexts or Booleans. To make sure the share you created can be shared read-only, run the following command as root user on the NFS server:

   ```
   # setsebool -P nfs_export_all_ro on
   ```

7. To view the shares available from the NFS server, assuming the NFS server is named `nfsserver`, type the following from the NFS client:

   ```
   # showmount -e nfsserver
   Export list for nfsserver:
   /var/mystuff  *
   ```

8. To create a directory called `/var/remote` and temporarily mount the `/var/mystuff` directory from the NFS server (named `nfsserver` in this example) on that mount point, type the following as root user from the NFS client:

   ```
   # mkdir /var/remote
   # mount -t nfs nfsserver:/var/mystuff /var/remote
   ```

9. To add an entry so that the same mount is done automatically when you reboot, first unmount `/var/remote` as follows:

   ```
   # umount /var/remote
   ```

   Then add an entry like the following to the `/etc/fstab` on the client system:

   ```
   /var/remote   nfsserver:/var/mystuff  nfs bg,ro 0 0
   ```

   To test that the share is configured properly, type the following on the NFS client as the root user:

   ```
   # mount -a
   ```

```
# mount | grep /var/remote
nfsserver:/var/mystuff on /var/remote type nfs4
 (ro,relatime,vers=4,rsize=524288...
```

10. To copy some files to the /var/mystuff directory, type the following on the NFS server:

    ```
    # cp /etc/hosts /etc/services /var/mystuff
    ```

    From the NFS client, to make sure you can see the files just added to that directory and to make sure you can't write files to that directory from the client, type the following:

    ```
    # ls /var/remote
    hosts    services
    # touch /var/remote/file1
    touch: cannot touch `/var/remote/file1': Read-only file system
    ```

Chapter 21: Troubleshooting Linux

1. To go into Setup mode from the BIOS screen on your computer, do the following:
   - Reboot your computer.
   - Within a few seconds, you should see the BIOS screen, with an indication of which function key to press to go into Setup mode. (On my Dell workstation, it's the F2 function key.)
   - The blue BIOS screen should appear. (If the system starts booting Linux, you didn't press the function key fast enough.)
2. From the BIOS setup screen, do the following to determine if your computer is 32-bit or 64-bit, if it includes virtualization support, and if your network interface card is capable of PXE booting.

   Your experience may be a bit different from mine, depending on your computer and Linux system. The BIOS setup screen is different for different computers. In general, however, you can use arrow keys and tab keys to move between different columns, and press Enter to select an entry.
   - On my Dell workstation, under the System heading, I highlight Processor Info to see that mine is a 64-bit Technology computer. Look in the Processor Info, or similar, section on your computer to see the type of processor you have.
   - On my Dell workstation, under the Onboard Devices heading, I highlight Integrated NIC and press Enter. The Integrated NIC screen that appears to the right lets me choose to enable or disable the NIC (On or Off) or enable with PXE or RPL (if I intend to boot the computer over the network).

3. To interrupt the boot process to get to the GRUB boot loader, do the following:
   - Reboot the computer.
   - Just after the BIOS screen disappears, when you see the countdown to booting the Linux system, press any key (perhaps the spacebar).
   - The GRUB boot loader menu should appear, ready to allow you to select which operating system kernel to boot.
4. To boot up your computer to runlevel 1 so that you can do some system maintenance, get to the GRUB boot screen (as described in the previous exercise), and then do the following:
   - Use the arrow keys to highlight the operating system and kernel you want to boot.
   - Type **e** to see the entries needed to boot the operating system.
   - Move your cursor to the line that included the kernel. (It should include the word `vmlinuz` somewhere on the line.)
   - Move the cursor to the end of that line, add a space, and then type the number **1**.
   - Follow the instructions to boot the new entry. You will probably either press `Ctrl+X` or press Enter; then when you see the next screen, type **b**.

     If it worked, your system should bypass the login prompt and boot up directly to a root user shell, where you can do administrative tasks without providing a password.
5. To start up Red Hat Enterprise Linux (through RHEL 6.*x*) so that you can confirm each service as it is started, do the following:
   - Follow the previous two exercises, but instead of putting a `1` at the end of a kernel line, put the word `confirm`.
   - When the boot process gets to the point where it is starting runlevel services, you are prompted to confirm (Y) or deny (N) each service, or continue (C) to simply start all the rest of the services.

     Note, this option is not available with the latest Fedora and Ubuntu releases.
6. To look at the messages that were produced in the kernel ring buffer (which shows the activity of the kernel as it booted up), type the following from the shell after the system finishes booting:

   ```
   # dmesg | less
   ```
7. To run a trial `yum update` from Fedora or RHEL, and exclude any kernel package that is available, type the following (when prompted, type **N** to not actually go through with the update, if updates are available):

   ```
   # yum update --exclude='kernel*'
   ```

8. To check to see what processes are listening for incoming connections on your system, type the following:

```
# netstat -tupln | less
```

9. To check to see what ports are open on your external network interface, do the following:

   If possible, run the `nmap` command from another Linux system on your network, replacing `yourhost` with the hostname or IP address of your system:

```
# nmap yourhost
```

10. To clear your system's page cache and watch the effect it has on your memory usage, do the following:
    - Select Terminal from an application menu on your desktop (it is located on different menus for different systems).
    - Run the `top` command (to watch processes currently running on your system), and then type a capital **`M`** to sort processes by those consuming the most memory.
    - From the Terminal window, select File and Open Terminal to open a second Terminal window.
    - From the second Terminal window, become root user (`su -`).
    - While watching the `Mem` line (used column) in the first Terminal window, type the following from the second Terminal window:

```
# echo 3 > /proc/sys/vm/drop_caches
```

    - The used `RES` memory should go down significantly on the `Mem` line. The numbers in the `RES` column for each process should go down as well.

Chapter 22: Understanding Basic Linux Security

1. To create a list from a log file of which services were started on your system at system initialization time:
   a. At the command line, type **`cat /var/log/boot.log`**.
   b. View the log file to find the daemons started.
2. To list the permissions on your system's password file and determine if they are appropriate, you can type **`ls -l /etc/shadow`** at the command line. (If no shadow file exits, then you need to run `pwconv`.)

   The following are the appropriate settings:

```
# ls -l /etc/shadow
-r--------. 1 root root 1049 Feb  2 09:45 /etc/shadow
```

3. To determine your account's password aging and if it will expire using a single command, type **`chage -l`** ***`user_name`*** or **`cat /etc/shadow | grep`** ***`user_name`***.

4. To start auditing writes to the `/etc/shadow` with the `auditd` daemon, type the following at the command line:

   ```
   # auditctl -w /etc/shadow -p w
   ```

   To check your audit settings, type in **`auditctl -l`** at the command line.

5. To create a report from the `auditd` daemon on the `/etc/shadow` file, type **`ausearch -f /etc/shadow`** at the command line. To turn off the auditing on that file, type **`auditctl -W /etc/shadow -p w`** at the command line.

6. To verify an installed software package on your system against the package's metadata for Fedora or RHEL, type **`rpm -V`** ***`package_name`*** at the command line.

   For Ubuntu, type **`debsums`** *`package_name`* at the command line.

7. If you suspect you have had a malicious attack on your system today and important binary files have been modified, you can find these modified files by typing the following at the command line: **`find`** ***`directory`*** **`-mtime -1`** for the directories,
   `/bin`, **`/sbin`**, **`/usr/bin`**, and **`/usr/sbin`**.

8. To install and run `chkrootkit` to see if the malicious attack from the exercise above installed a rootkit, choose your distribution and do the following:

   a. To install on a Fedora or RHEL distribution, type **`yum install chkrootkit`** at the command line.

   b. To install on a Ubuntu or debian-based distribution, type **`sudo apt-get install chkrootkit`** at the command line.

   c. To run the check, type **`chkrootkit`** at the command line and review the results.

9. To find files with the SetUID permission set, type **`find / -perm -4000`** at the command line.

10. To find files with the SetGID permission set, type **`find / -perm -2000`** at the command line.

Chapter 23: Understanding Advanced Linux Security

1. To encrypt a file using the `gpg` utility and a symmetric key, type **`gpg -c`** ***`filename`*** at the command line. The `gpg` utility will ask for a passphrase to protect the symmetric key.

2. To generate a key ring using the `gpg` utility, type **`gpg --gen-key`** at the command line. You will have to provide the following information:

   a. What kind of asymmetric key you want:

      - RSA and RSA (default)
      - DSA and Elgamal

- DSA (sign only)
- RSA (sign only)

b. What key size (in number of bits) you want.

c. How many days, weeks, months, years the key should be valid. You can also request that the key be valid permanently.

d. Your real name, e-mail address, and a comment to create the User ID for the public key.

e. A passphrase for the private key.

3. To list out the key ring you generated, type **`gpg --list-keys`** at the command line.

4. To encrypt a file and add your digital signature using the `gpg` utility, do the following:

   a. You must have first generated a key ring (Exercise 2).

   b. Once you have generated the key ring, type **`gpg --output`** ***`Encrypted&SignedFile`*** **`--sign`** ***`FiletoEncrypt&Sign`*** at the command line.

5. To use the appropriate message digest utility to ensure the downloaded file is not corrupted, you need to do the following. (Remember that a message digest is also called a checksum.)

   a. Review the download website for the MD5 or SHA-1 file or number.

      - If it is a checksum number, you need to go on to the next step.
      - If it is a checksum file, you will need to download that file, too, and then use the `cat` command to display the checksum file's contents to your screen.

   b. If it is a MD5, then type **`md5sum`** ***`FirstDownloadedFile`*** at the command line and compare the numbers to the MD5 checksum file or number on the website.

   c. If it is an SHA-1 hash, then type **`sha1sum`** ***`FirstDownloadedFile`*** at the command line and compare the numbers to the SHA-1 checksum file or number on the website.

6. To determine if the `su` command on your Linux system is PAM-aware, type **`ldd`** ***`suDirectory/su`*** **`|`** **`grep pam`** at the command line. *`suDirectory`* is the location of the `su` command you found with the `where su` command. If the `su` command on your Linux system is PAM-aware, you will see a PAM library name listed when you issue the `ldd` command.

7. To determine if the `su` command has a PAM configuration file, type **`ls /etc/pam.d/su`** at the command line. If there is a PAM configuration file, the file listing will display. If it does exist, then type **`cat /etc/pam.d/su`** at the command line to display its contents. The PAM contexts it uses will be any of the following: `auth`, `account`, `password`, `session`.

8. To list out the various PAM modules on your Fedora or RHEL system, type **`ls /lib/security/pam*.so`** at the command line. To list out the various PAM modules on your Ubuntu Linux system, type **`sudo find / -name pam*.so`** at the command line.
9. To find the PAM "other" configuration file on your system, type **`ls /etc/pam.d/other`** at the command line. An "other" configuration file that enforces Implicit Deny should look similar to the following code:

```
$ cat /etc/pam.d/other
#%PAM-1.0
auth     required       pam_deny.so
account  required       pam_deny.so
password required       pam_deny.so
session  required       pam_deny.so
```

10. To find the PAM limits configuration file, type **`ls /etc/security/limits.conf`** at the command line. Display the file's contents by typing **`cat /etc/security/limits.conf`**. Settings in this file to prevent a fork bomb will look like the following:

```
@staff       hard    nproc           50
@staff       hard    maxlogins        1
```


Chapter 24: Enhancing Linux Security with SELinux

1. To set your system into the permissive Operating Mode for SELinux, type **`setenforce permissive`** at the command line. It would also be acceptable to type **`setenforce 0`** at the command line.
2. To set your system into the enforcing Operating mode for SELinux without changing the SELinux primary configuration file, use caution. It is best not to run this command on your system for an exercise until you are ready for the SELinux to be enforced. Use the following command: **`setenforce enforcing`** at the command line. It would also be acceptable to type **`setenforce 1`** at the command line.
3. To find and view the current SELinux Policy type, go to the main SELinux configuration file, `/etc/selinux/config`. To view it, type **`cat /etc/selinux/config`** at the command line.
4. To list a file's security context and identify the different security context attributes, type **`ls -Z`** ***`filename`*** at the command line.
   - The file's user context will end with a `u`.
   - The file's role will end with an `r`.
   - The file's type will end with a `t`.
   - The file's sensitivity level starts with an `s` and ends with a number. It may be listed in a range of numbers, such as `s0-s3`.
   - The file's category level starts with a `c` and ends with a number. It may be listed in a range of numbers, such as `c0-c102`.

5. The command that would change a file's `type` attribute is **`chcon -t newtype_t filename`**. (Caution: Do not issue the command on your system unless you want to change the file's type.)
6. To list a current process's security context and identify the different security context attributes, type **`ps -Z pid`** at the command line.
   - The process's user context will end with a `u`.
   - The process's role will end with an `r`.
   - The process's type or domain will end with a `t`.
   - The process's sensitivity level starts with an `s` and ends with a number. It may be listed in a range of numbers, such as `s0.s3`.
   - The process's category level starts with a `c` and ends with a number. It may be listed in a range of numbers, such as `c0.c102`.
7. The command that would restore a file's SELinux default file context is **`restorecon -R filename`**. (Caution: Don't run this command on your system unless you know its effects.)
8. To get a listing of the current Booleans used on your system, type **`getsebool -a`** at the command line. You could use either of the following commands to modify one of the Booleans: **`setsebool Boolean_name off`** or **`setsebool Boolean_name on`** or **`togglebool Boolean_name.`**
9. The command that would list out all the SELinux policy modules on your system, along with their version numbers, is **`semodule -l.`**

   Note: If you wrote `ls *.pp` as your answer that is okay, but this command doesn't give you the version numbers of the policy modules. Only `semodule -l` will give the version numbers.
10. To create an AVC denial message and then review the log(s) for the message, do the following:
    a. As a non-administrator user type **`chcon -u fake_u filename`** at the command line.
    b. If you have only the `auditd` daemon running on your system, type the following at the command line:

       ```
       aureport | grep AVC
       ausearch -m avc
       ```

    c. If you have only the rsyslogd daemon running on your system, type in at the command line:

       ```
       grep "SELinux is preventing" /var/log/messages
       ```

    d. If you have the `rsyslogd` daemon and the `setroubleshootd` daemon running on your system, type in at the command line:

```
grep "SELinux is preventing" /var/log/messages
sealert -l AVC_denial_message_id_number
```

Chapter 25: Securing Linux on a Network

1. To install the Network Mapper (aka `nmap`) utility on your local Linux system:
   a. On Fedora or RHEL, type **`yum install nmap`** at the command line.
   b. On Ubuntu, `nmap` may come pre-installed. If not, type **`sudo apt-get install nmap`** at the command line.

2. To run a TCP Connect scan on your local loopback address, type **`nmap -sT 127.0.0.1`** at the command line. The ports you have running on your Linux server will vary. However, they may look similar to the following:

```
# nmap -sT 127.0.0.1
...
PORT    STATE SERVICE
25/tcp  open  smtp
631/tcp open  ipp
```

3. To run a UDP Connect scan on your Linux system from a remote system:
   a. Determine your Linux server's IP address by typing **`ifconfig`** at the command line. The output will look similar to the following and your system's IP address follows "`inet addr:`" in the `ifconfig` command's output.

```
# ifconfig
...
p2p1  Link encap:Ethernet  HWaddr 08:00:27:E5:89:5A
      inet addr:10.140.67.23
```

   b. From a remote Linux system, type the command **`nmap -sU`** ***`IP address`*** at the command line, using the *`IP address`* you obtained from above.

4. To check and see if the `ssh` daemon on your Linux system uses TCP Wrapper support, type **`ldd /usr/sbin/sshd | grep libwrap`** at the command line. The output will look similar to the following if it does use TCP Wrapper support. If it does not, there will be no output.

```
$ ldd /usr/sbin/sshd | grep libwrap
libwrap.so.0 => /lib/libwrap.so.0 (0x0012f000)
```

5. To allow access to the `ssh` tools on your Linux system from a designated remote system and deny all other access using TCP Wrappers, you will need to modify both the `/etc/hosts.allow` file and the `/etc/hosts.deny` file. The modifications will look similar to the following:

```
# cat /etc/hosts.allow
...
sshd: 10.140.67.32
#
# cat /etc/hosts.deny
#...
ALL: ALL
```

6. To determine your Linux system's current `netfilter/iptables` firewall policies and rules, type **`iptables -L`** at the command line.
7. To flush your Linux system's current firewall rules, type **`iptables -F`** at the command line. To restore the firewall's rules on a Fedora or RHEL system, type **`iptables-restore < /etc/sysconfig/iptables`**.
8. This is a trick question! You cannot set a Linux system's firewall policy to reject. You can set it to drop, but not reject. To set your Linux system's firewall filter table for the input chain to a policy of `DROP`, type **`iptables -P INPUT DROP`** at the command line.
9. To change your Linux system firewall's filter table policy back to `accept` for the input chain, type **`iptables -P INPUT ACCEPT`** at the command line.
   To add a rule to drop all network packets from the IP address, 10.140.67.23, type **`iptables -A INPUT -s 10.140.67.23 -j DROP`** at the command line.
10. To remove the rule you added above, without flushing or restoring your Linux system firewall's rules, type **`iptables -D INPUT 1`** at the command line. This is assuming that the rule you added above is rule 1. If not, change the `1` to the appropriate rule number in your `iptables` command.