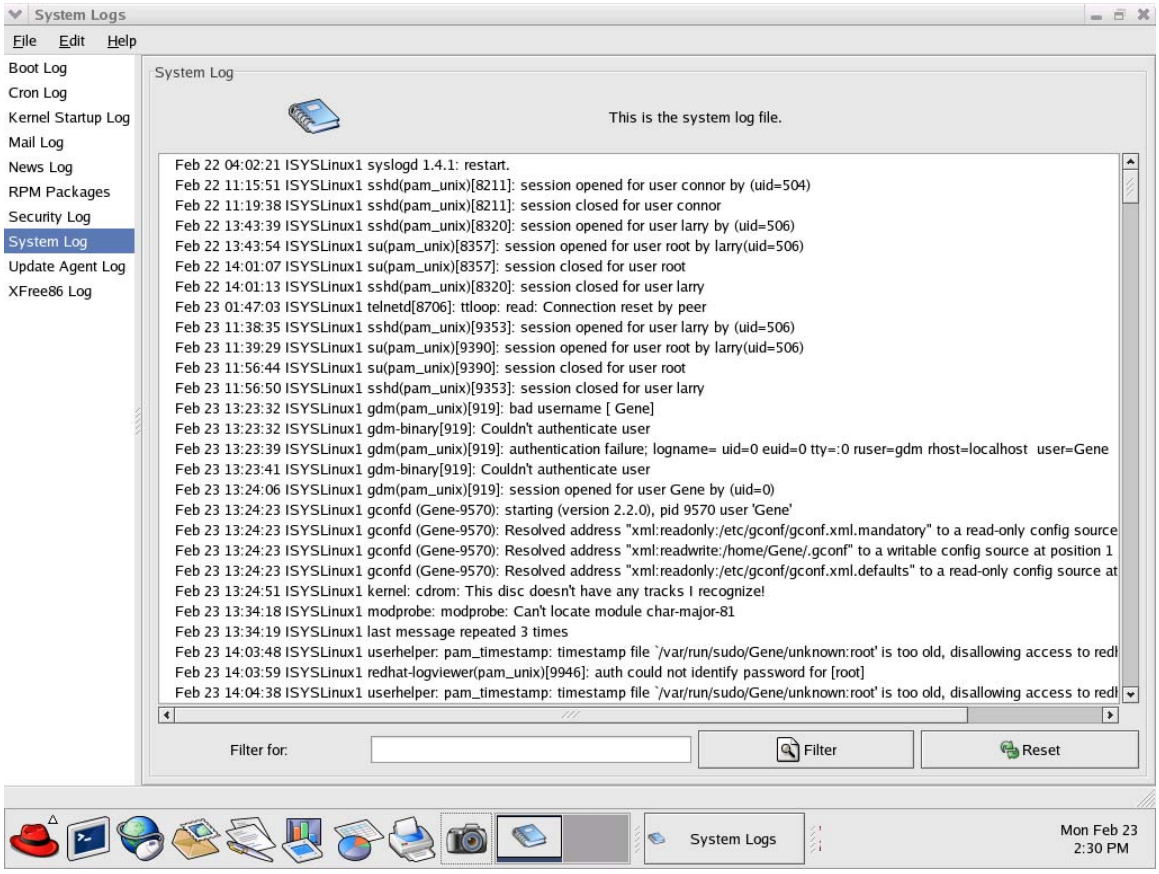
4.4.1

Linux Log File Administration

(Red Hat Linux 9)



Laboratory Overview

Objective

Students will learn how to administer Linux log files, enabling them to identify and troubleshoot problems on a Linux system or network.

Information for Laboratory

A. Students will use standard tools distributed with Linux.
B. Students will examine log files on their student PC.
C. Students will observe the effect of successful and unsuccessful login attempts on the Linux log files.
D. Students will learn techniques for archiving and clearing the Linux log files.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Estimated Completion Time

45 Minutes

Linux Log File Administration

Since administrators cannot observe all events that take place on a Linux system over time, most daemons record error and informational messages to **log files**. These are text files typically stored in the **/var/log** directory, or a subdirectory within it. For example, the **/var/log/samba** directory contains the log files created by the samba file-sharing daemons.

Administrators must routinely examine the log files to uncover and debug configuration problems, but also to look for possible instances of inappropriate use or breaches in security.

The following are some of the most common log files, all of which are stored in the **var/log** directory:

- secure (network access through sshd and xinetd daemons)
- wtmp (login session history)
- rpmpkgs (software packages installed)
- xferlog (FTP)
- Xfree86 (X Windows)
- messages ("initialization and after" daemon startup messages)
- maillog (sendmail daemon messages)

Note that all these log files may not be present on any particular Linux workstation, depending on actual use. For example, if no FTP activity has been performed, the xferlog file will not be present.

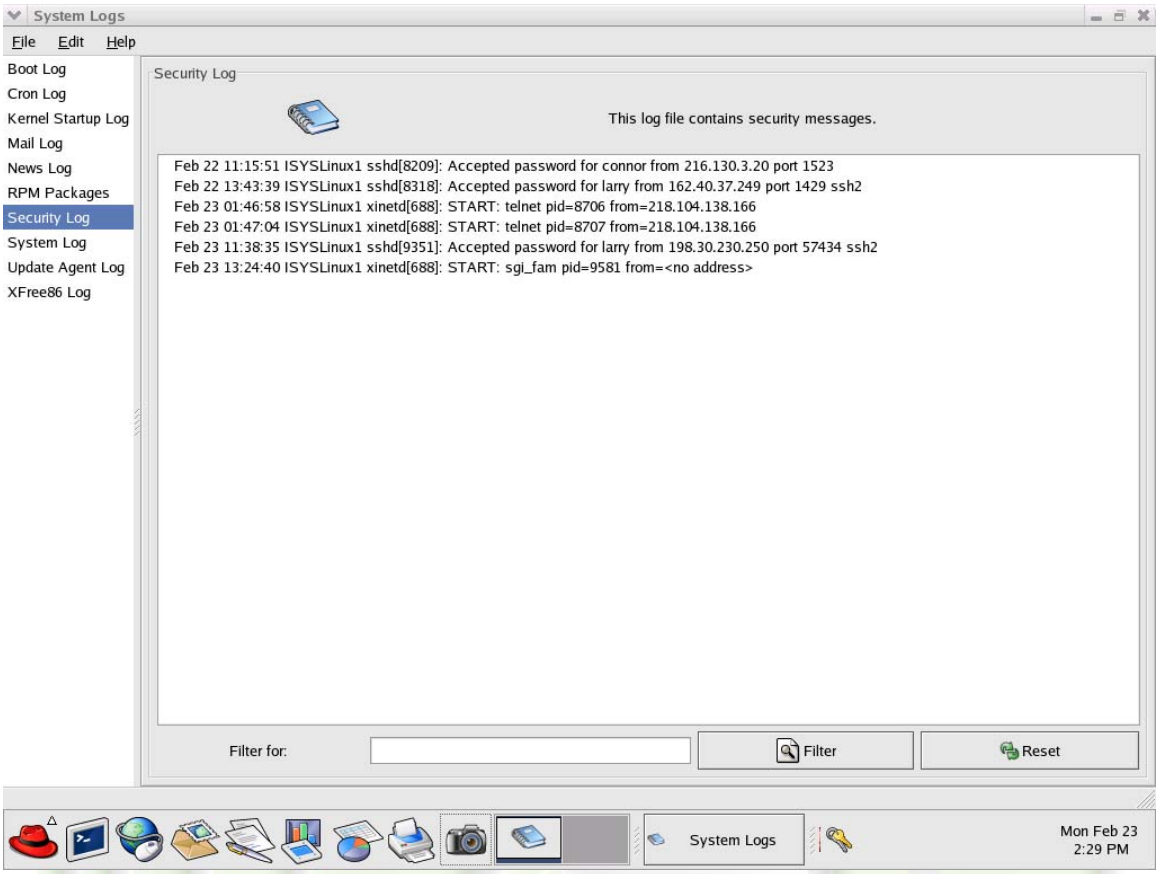
Viewing and Managing Linux Log Files

Step 1:

BOOT your student PC under Linux and login, preferably as root.
From the Gnome menu, **select**:

- **System Tools**
- **System Logs**
- **< enter the root password if prompted >**

The following Log Selection screen (or one similar to it) will be displayed:



Explore the contexts of each system log displayed on the left by selecting it, and scrolling through the contents.

Step 2:

The log files can also be accessed via a command window using UNIX commands. From the Gnome menu select,

- **System Tools**
- **Terminal**

A command window should appear with a prompt similar to

```
user@machine user]$
```

where the `user@machine` represents the username and localhost name. The last designation of `user` within the prompt is for the current directory.

The following UNIX commands operable within the Linux command window may be useful:

pwd	print working directory
ls	lists your files
ls -l	lists your files and displays their sizes
rm	deletes a file
rmdir	deletes an empty directory
mkdir	creates a directory
cd *name*	changes directory to one called name
cd ~ or cd	moves to your home directory
cd /	changes to the root directory
*	the wild card symbol
mv oldfile newfile	moves/renames oldfile to newfile

DOS commands are largely based on the older structure of UNIX commands. One major difference in syntax is the use of the forward slash (/) in writing directory paths in UNIX, versus the backslash for DOS.

Try using the pwd command at the prompt.

```
user@machine user]$pwd
user
user@machine user]$
```

The notion of “print” working directory is anachronistic to the days of teleprinters. The command, like all others, simply displays to the default output device, which is now the monitor. If a printer is configured on the local host, the output of the command can be redirected to the printer by the following:

```
[user@machine user]$pwd > prn
[user@machine user]$
```

Help is available for any UNIX/Linux command through the manual or man pages.

```
[user@machine user]$man pwd
```

To paginate longer man pages, the output can be piped into “less”.

```
[user@machine user]$man ls|less
```

Piping the output into “less” allows the user to scroll down with the use of the space bar, and use page up/down keys. Exit “less” by striking the Q key.

To see the list of log files, change to the log file directory and list them.

```
[user@machine user]$cd /var/log
[user@machine log]$ls
```

A simple list of the files and directories in the log directory should be displayed. Use the –l switch to view file details, and note the leading “d” for directories. To see the contents of a file, use the cat or concatenate command.

```
[user@machine log]$cat secure|less
```

Note that if an error occurs here, you may attempt to enter superuser mode and try again.

```
[user@machine log]$su -
```

Otherwise, you need to logout and login as root or another administrator. Note too that the contents of the secure file match that of the Security Log viewed from the GUI System Logs application in step 1.

Step 3:

Use the cat command as in step 2 to view other files in the log directory, and compare the file contents with the information shown by the System Logs application used in step 2.

Complete the following table that associates System Logs application entries with respective log directory files:

System Log	Log File
Boot Log	_____
Cron Log	_____
Kernal Startup	_____
Mail Log	maillog
News Log	_____
RPM Packages	rpmpkgs
Security Log	secure
System Log	_____
Update Agent Log	_____
XFree86 Log	XFree86.x.y.log

Note once again that the list of entries in the System Logs application and therefore the list of log files may defer on your local machine depending on the history of services and applications utilized.

Step 4:

See how the log files change when a failed login occurs. Attempt to telnet into your local host using the command window.

```
[user@machine log]$telnet 127.0.0.1
```

Supply any text for username and password. You may wish to repeat this two or three times so that system logs are easier to discern. Now view the output of the Systems Logs application used in step 1. Where is the failed login attempt recorded?

Step 5:

View the contents of the /etc/syslog.conf file of your local machine.

```
[user@machine log]$cd /etc
[user@machine etc]$cat syslog.conf|less
```

Study how this configuration file controls logging.

Step 7:

Although the log files contain important system information, they can grow to be quite large over time. It is important to periodically backup and clear the contents of the log files.

Note that "clearing" does not mean "removing" the log file from the file system. If you remove a log file (rather than just clearing it) the permissions and ownership will be removed, as well.

Before clearing the log files, it is a good idea to archive them and store them in a safe place. It is common practice to store a printed copy of the archived logs in yet another safe place that would not likely be affected by a disastrous event that could destroy the electronic archive.

Return the current directory to /var/log and enter the superuser mode if you have not already done so.

```
[user@machine etc]$cd /etc/log
[user@machine log]$su -
```

If you have a printer configured, the following command will print the contents of the secure file:

```
[user@machine log]$lpr –P name /var/log/secure
```

Where "name" is the name of the printer. Archive the secure file using the copy command.

```
[user@machine log]$cp secure secure.oldxyz
```

Since archiving should be done periodically, you can use the naming convention for keeping track of logs, perhaps by imbedding the date.

You might also archive after files grow to a certain size. To see the size of the secure file, issue the following:

```
[user@machine log]$ls –l /var/log/secure
```

Issue the following command to clear the secure log (using the **>** redirection symbol):

```
[user@machine log]$>/var/log/secure
```

The redirection command has been used to redirect the contents of nothing into the secure file. Verify that the file is cleared using the cat command, and ls -l. Note the difference in the secure log file size before and after clearing.

The above procedure would need to be completed on each log file. This can be automated by placing the series of commands into a shell program similar to a DOS batch file.

Analysis

1) What security risks are present by UNIX/Linux using plain text files for logging?
2) What steps or actions should be included in an operations procedure for log file administration?
3) How often should log files be reviewed?
4) List six types of network services faults or security breaches that will likely be documented by log files.

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

1) If a Linux server is available, log into it and view its log files as you have done on the local machine.

2) Research application software that can assist you with Linux log file administration by searching the Internet.

How do the application software packages compare in terms of features, price, licensing, and other considerations? Identify some “other considerations” besides features, price, and licensing restrictions and include them as criteria in your research report. Be sure to include commercial, shareware, and freeware products in your research. Must you research each product individually? Or are there sources that can be trusted to do impartial evaluations of competitive products? Identify three of these sites that specialize in cyber security product reviews. How do you know that the product reviews published by these sites are not influenced by advertising revenue from product manufacturers and developers?

3) Is there hardware on the market to perform the same functions as the application software used in this lab exercise? Under what circumstances would a hardware solution be preferable to a software solution? And vice versa?

Appendix:

This lab was developed using the OS utilities within Red Hat Linux 9, which can be obtained from:

http://www.redhat.com

-or-

http://www.download.com

The OS environment for this lab was Red Hat Linux 9 (Service Pack 1).

CSSIA