Another useful command in your auditing toolkit is the lastlog command. The lastlog utility pulls data from the /var/log/lastlog file. You can determine when a particular  
user last logged into the system by adding the -u username option as shown here:  
$ **lastlog -u Christine**  
Username Port From Latest  
Christine tty3 Wed Nov 12 10:20:36 -0500 2015  
$  
Be aware that if a particular user is logged into the system multiple times, lastlog will  
not display multiple login entries. It only shows the *last* time a user logged into the system.

It is helpful to view every account’s /var/log/lastlog entry. You can use this as an  
auditing tool to determine if accounts that should not be logged into have been accessed.  
Here is a snipped example of this audit tool’s display:  
$ **lastlog**  
Username Port From Latest  
root tty3 Wed Nov 12 09:32:51 -0500 2015  
[...]  
**sshd \*\*Never logged in\*\***  
tcpdump \*\*Never logged in\*\*  
Christine tty3 Wed Nov 12 10:20:36 -0500 2015  
sally \*\*Never logged in\*\*  
Rich tty4 Tue Nov 11 12:36:01 -0500 2015  
Timothy tty3 Tue Nov 11 12:33:08 -0500 2015  
[...]  
$  
As you can see from the preceding example, the sshd account has never been logged  
into, and that is a good thing! All of the auditing tools covered in this section can help you  
keep an eye on your system to discover any potential security breaches. However, while  
seeing what happened in the past is helpful, it’s even better to put limits in place to prevent  
bad things from happening in the future.