Hands-on Projects

These projects should be completed in the order given. The hands-on projects presented in this chapter should take a total of three hours to complete. The requirements for this lab include:

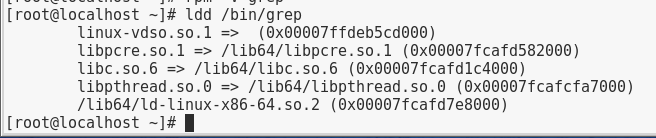
* A computer with Fedora Linux installed according to Hands-on Project 2-1 and Ubuntu Server Linux installed according to Hands-On Project 6-1.

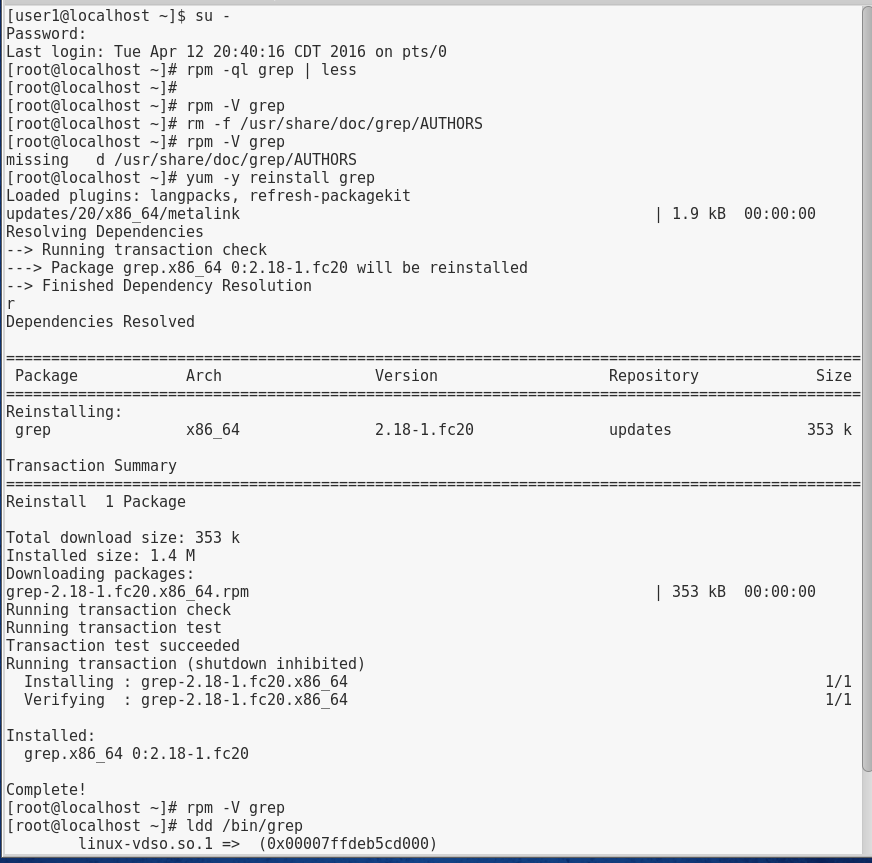
# Project 14-1

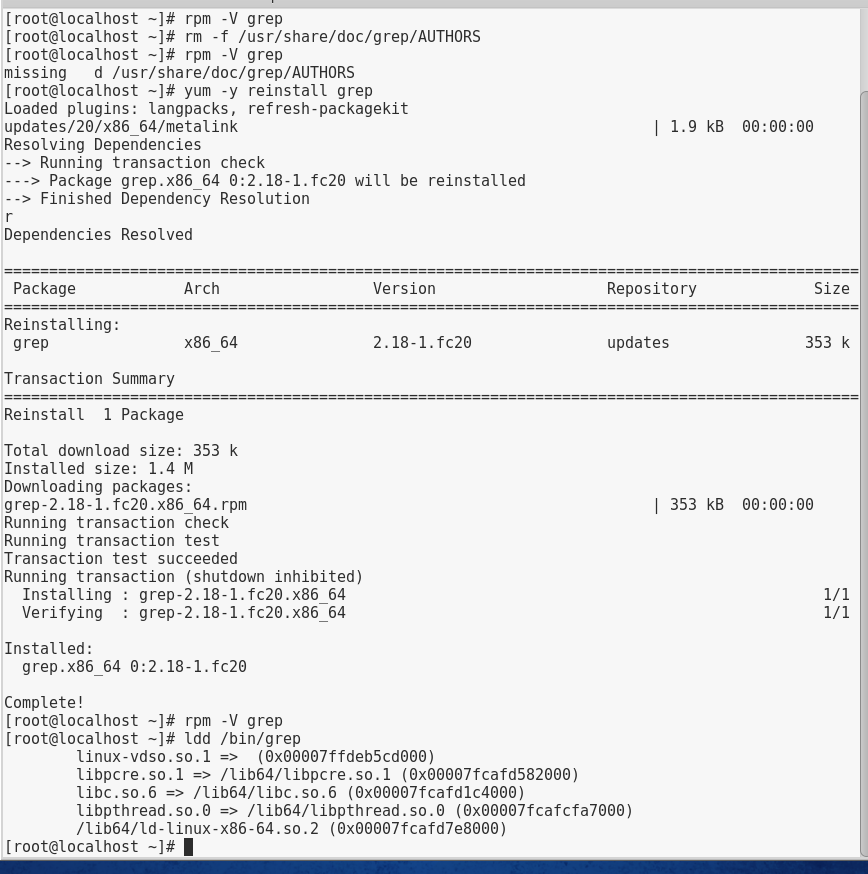
In this hands-on project, you detect modified package contents and observe shared libraries used by programs on your Fedora Linux virtual machine.

1. Boot your **Fedora** Linux virtual machine. Login to your chosen desktop environment as **user1** using password **LNXrocks!** and open up a terminal window.
2. At the terminal, become **root** by typing **su -** and press enter and provide **LNXrocks!** as the password.
3. At the command prompt, type **rpm -ql grep | less** and press Enter to view the file contents of the grep package on the system. When finished, press q to quit the less utility. Next, type **rpm -V grep** at the command prompt and press Enter to verify the existence of these files on the filesystem.
4. At the command prompt, type **rm -f /usr/share/doc/grep/AUTHORS** and press Enter to remove a file that belongs to the grep package. Next, type **rpm -V grep** at the command prompt and press Enter to verify the existence of all files in the grep package. Were any errors reported? **Missing d /usr/share/doc/grep/AUTHORS**
5. At the command prompt, type **yum -y reinstall grep** and press Enter to re-install the grep utility. Next, type **rpm -V grep** at the command prompt and press Enter to verify the deleted file was recovered.
6. Type **ldd /bin/grep** at the command prompt and press Enter to determine the shared libraries used by the grep command. Were any missing libraries reported in the output of the command? **Yes, see screenshot of libraries**
7. **Provide screenshot(s) of steps 3 through 5.**

****

****

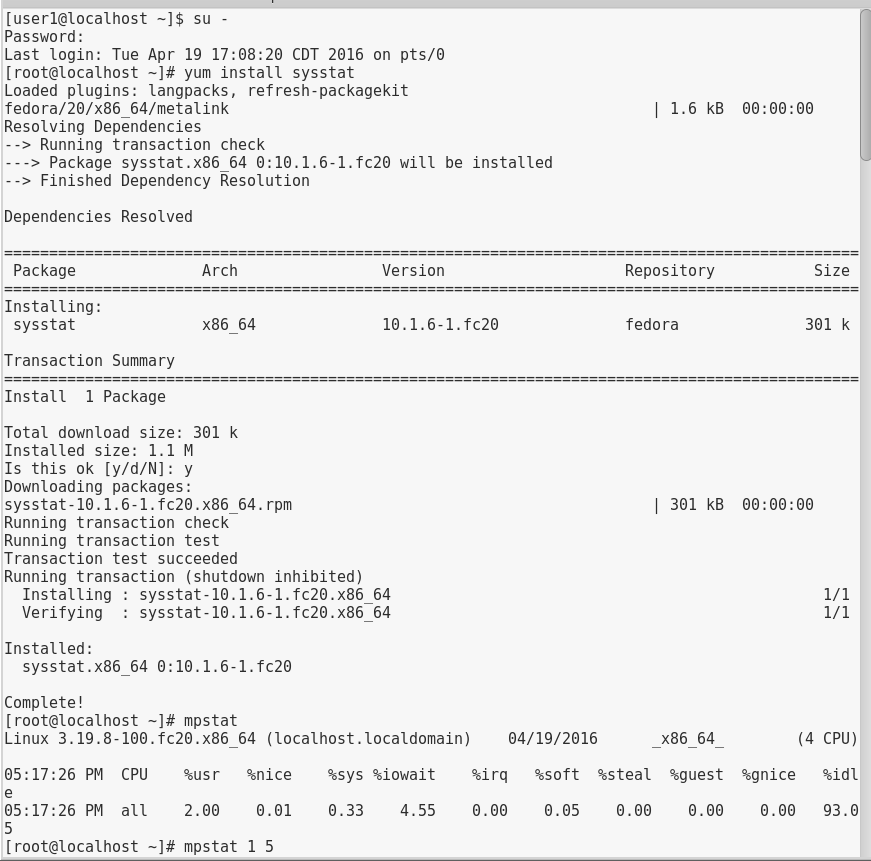
****

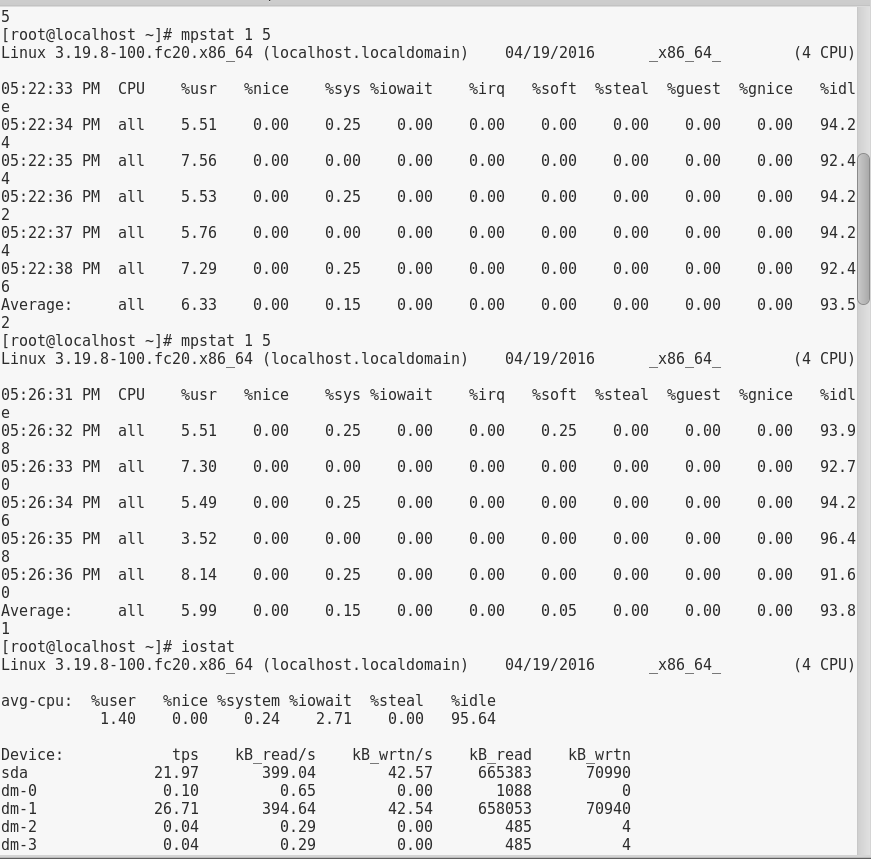
****

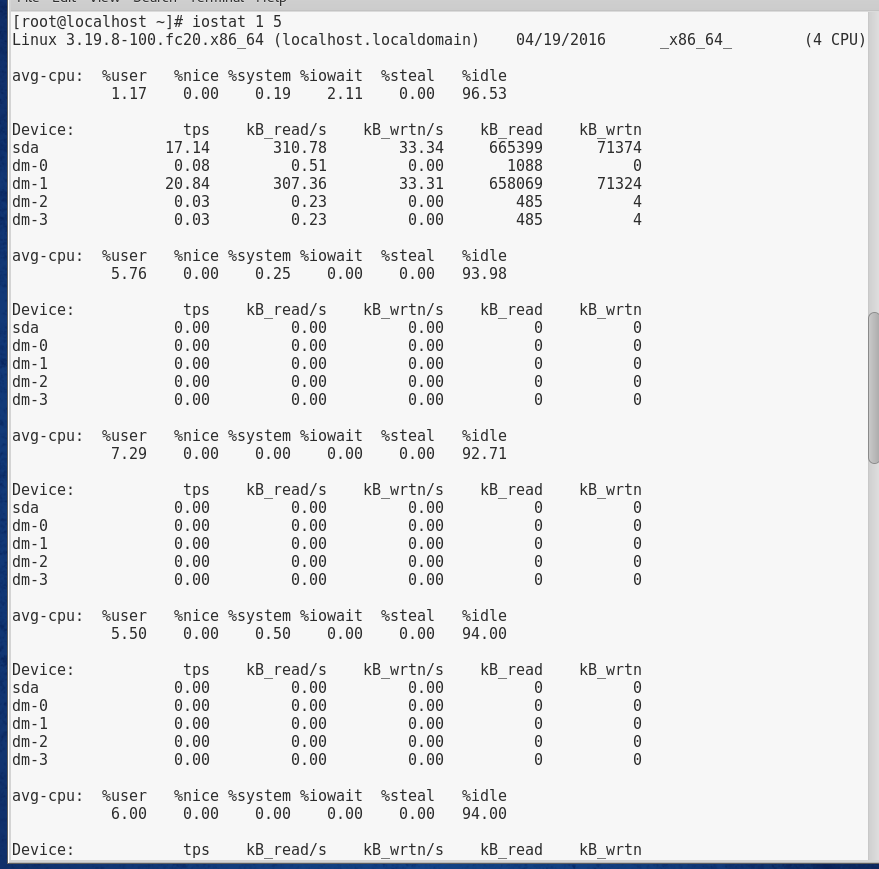
# Project 14-2

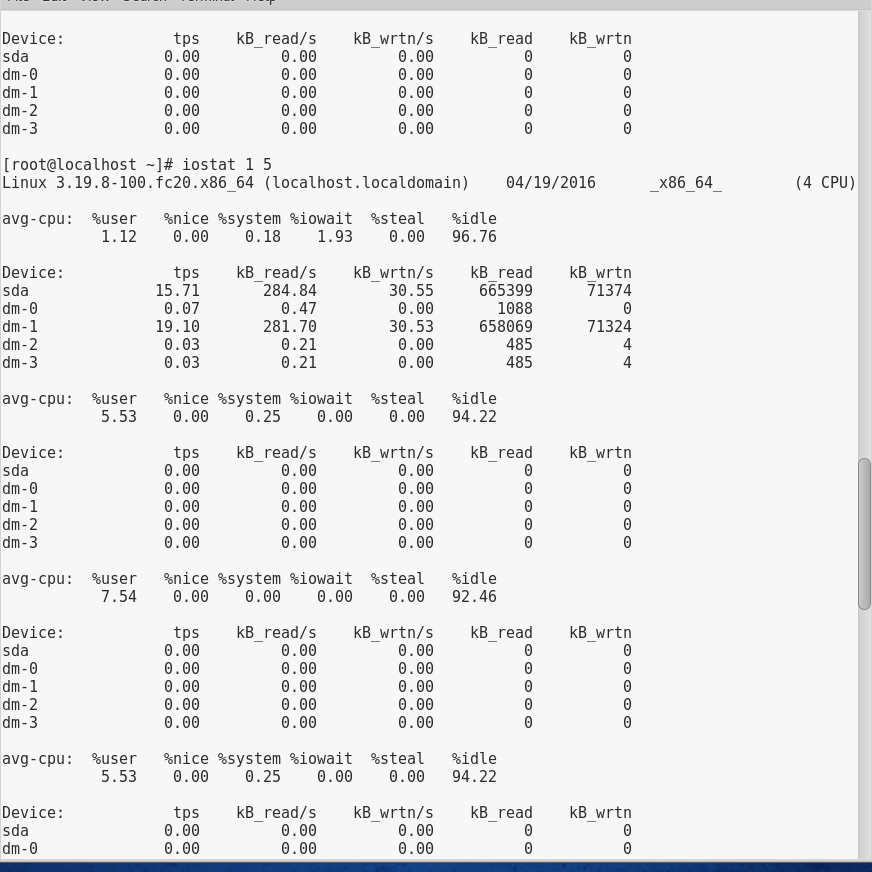
In this hands-on project, you install the sysstat package on your Fedora Linux virtual machine and monitor system performance using the command-line utilities included within the package.

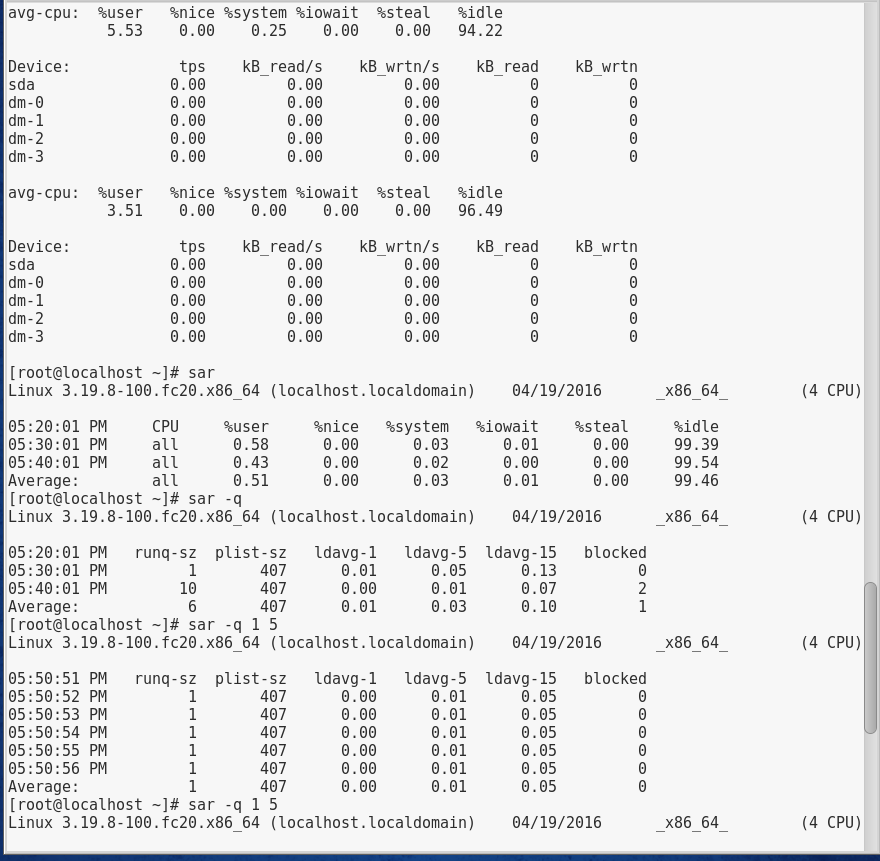
1. Boot your **Fedora** Linux virtual machine. Login to your chosen desktop environment as **user1** using password **LNXrocks!** and open up a terminal window.
2. At the terminal, become **root** by typing **su -** and press enter and provide **LNXrocks!** as the password.
3. At the command prompt, type **yum install sysstat** and press Enter. Press y when prompted to complete the installation of the sysstat package.
4. At the command prompt, type **mpstat** and press Enter to view average CPU statistics for your system since the last boot time. What is the value for %usr? **2.00** Is this higher, lower, or the same as %system? **Higher.** What is the value for %idle? **93.05** What should this value be over? **It should be over 0.**
5. At the command prompt, type **mpstat 1 5** and press Enter to view five CPU statistic measurements, one per second. How do these values compare to the ones seen in the previous step? **They fluctuate depending on what you’re doing.**
6. Open several applications of your choice from the applications menu.
7. Switch back to your terminal and type **mpstat 1 5** at the command prompt and press Enter to view five CPU statistic measurements, one per second. How do these values compare to the ones seen in Step 4? **The %usr went up and the %idle went down.**
8. Close all programs you just opened.
9. Switch back to your terminal and type **iostat** at the command prompt and press Enter to view average device I/O statistics since the last boot time. What devices are displayed? **Sda, dm-0, dm-1, dm-2, dm-3** How many blocks were read and written to your hard disk since the last boot time, on average? **Read: 665383 and Write: 70990**
10. At the command prompt, type **iostat 1 5** and press Enter to view five I/O statistic measurements, one per second. How do these values compare to the ones seen in the previous step? **The first of the 5 lists blocks, while the last four don’t list any blocks.**
11. Open several applications of your choice from the applications menu.
12. Switch back to your terminal and type **iostat 1 5** at the command prompt, and press Enter to view five I/O statistic measurements, one per second. How do these values compare to the ones seen in Step 10? Were there any significant changes? **All of the blocks that were listed in step 10 are lower here.**
13. Close all programs you just opened.
14. Switch back to your terminal and type **sar** at the command prompt, and press Enter. What statistics are displayed by default? What times were the statistics taken? **CPU, %usr, %nice, %system, %iowait, %steal, and %idle are displayed. The statistics were taken at 5:20, 5:30, and 5:40.**
15. At the command prompt, type **sar -q** and press Enter to view queue statistics. What times were the statistics taken? **5:20, 5:30, and 5:40** How does this compare to the output from the previous step? **They both were taken at the same time, but it lists runq-sz, plist-siz, ldavg-1, ldavg-5, and blocked.** What is the queue size? **407** What is the average load for the last minute? What is the average load for the last five minutes? **0.01 for the last minute and 0.03 for the last five minutes.**
16. At the command prompt, type **sar –q 1 5** and press Enter to view five queue statistics, one per second. How do these values compare to those taken in the previous step? **This one lists five statistics per second and the average load went down compared to the previous.**
17. Open several applications of your choice from the applications menu.
18. Switch back to your terminal and type **sar -q 1 5** at the command prompt, and press Enter to view five queue statistic measurements, one per second. How do these values compare to the ones seen in Step 16? **There is no change between the two steps.**
19. Close all programs you just opened.
20. Switch back to your terminal and type **sar -W** at the command prompt, and press Enter. How many pages were swapped to and from the swap partition today, on average? **0.00**
21. At the command prompt, type **sar –W 1 5** and press Enter to view five swap statistics, one per second. How do these values compare to those taken in the previous step? **The statistics stay the same.**
22. Open several applications of your choice from the applications menu.
23. Switch back to your terminal and type **sar -W 1 5** at the command prompt, and press Enter to view five swap statistic measurements, one per second. How do these values compare to the ones seen in Step 21? **The statistics still don’t change.**
24. **Provide screenshot(s) of steps 3 through 23.**

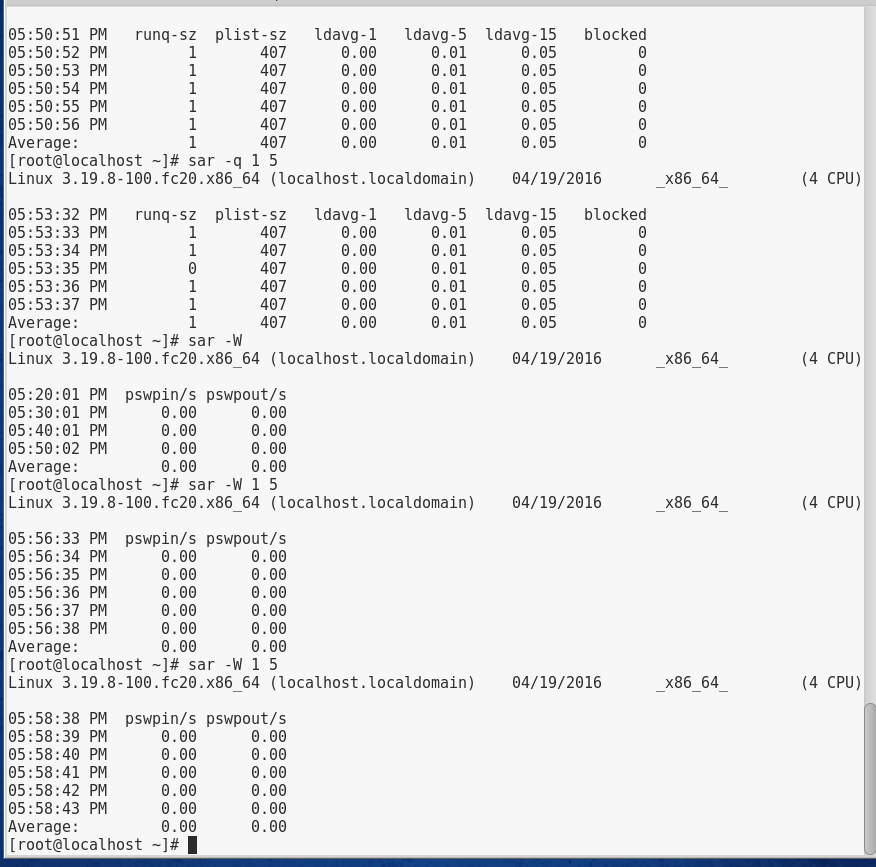
****

****

****

****

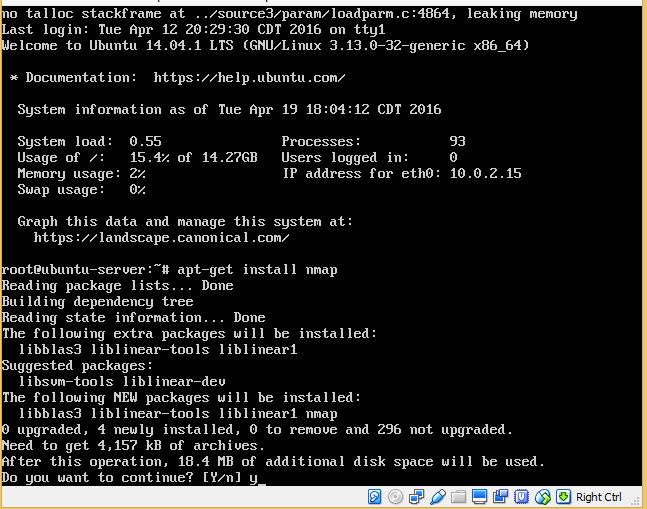
****

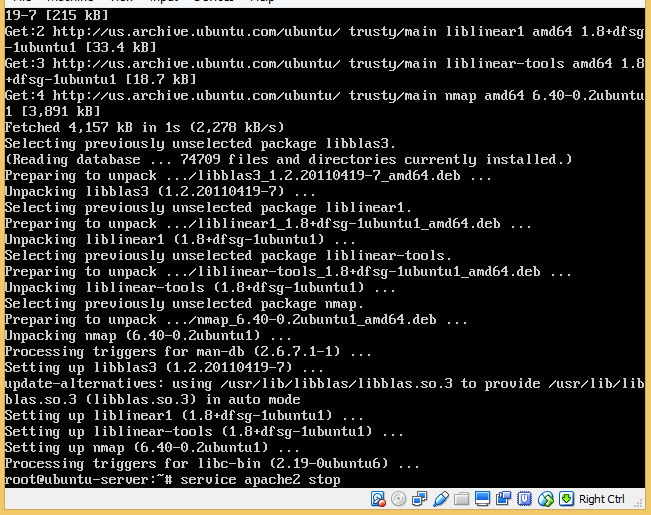
****

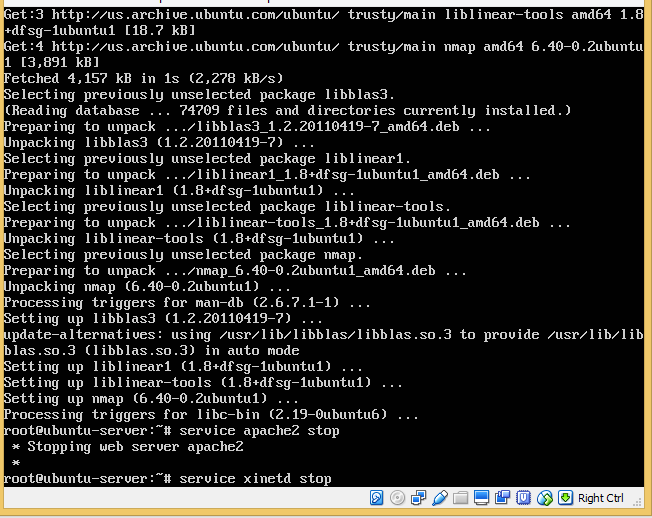
# Project 14-3

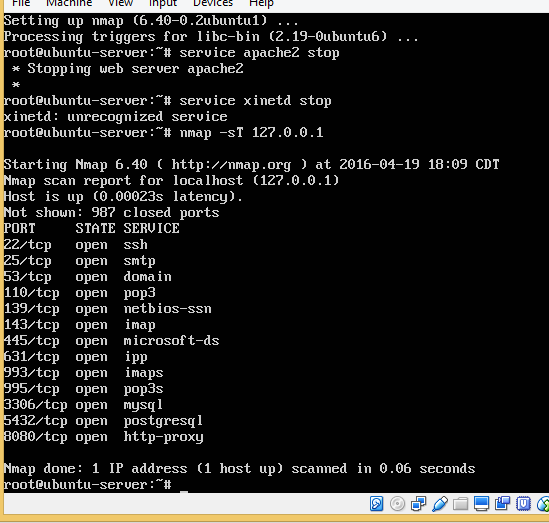
In this hands-on project, you examine the services running on your Ubuntu Server Linux virtual machine using the nmap utility and /etc/services file.

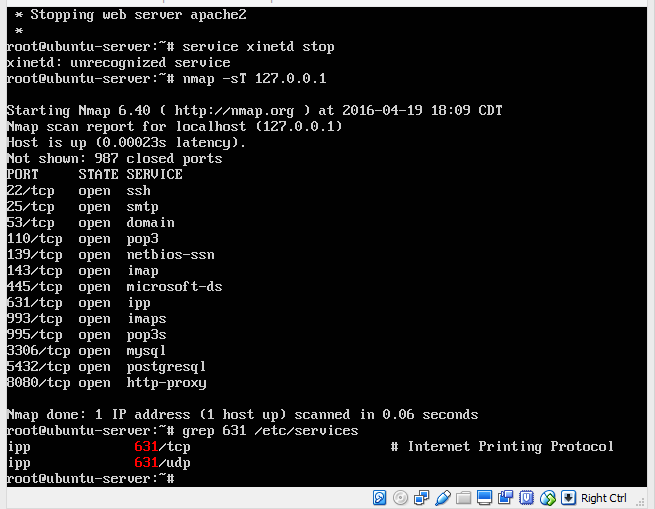
1. Boot your **Ubuntu** Linux virtual machine. Login to your chosen desktop environment as **root** using password **LNXrocks!** and open up a terminal window.
2. At the command prompt, type **apt-get install nmap** and press Enter. Press y and press Enter when prompted to complete the installation of the nmap utility.
3. At the command prompt, type **service apache2 stop** and press Enter.
4. At the command prompt, type **service xinetd stop** and press Enter.
5. At the command prompt, type **nmap -sT 127.0.0.1** and press Enter. What ports are listed that you recognize?**Port 53, 8080** Are there any unknown ports? **Yes.** Where could you find information regarding the unknown ports? **You can look up the port listings online.** What is the service associated with port 631/tcp? **Printer sharing**
6. At the command prompt, type **grep 631 /etc/services** and press Enter. What is the full name for the service running on port 631? **Ipp 631/tcp and ipp 631/udp. Nothing else is listed.**
7. At the command prompt, type **service apache2 start** and press Enter.
8. At the command prompt, type **service xinetd start** and press Enter.
9. At the command prompt, type **nmap -sT 127.0.0.1** and press Enter. What additional ports were opened by the Apache Web server and Extended Internet Super Daemon? **http**
10. **Provide screenshot(s) of steps 2 through 9.**

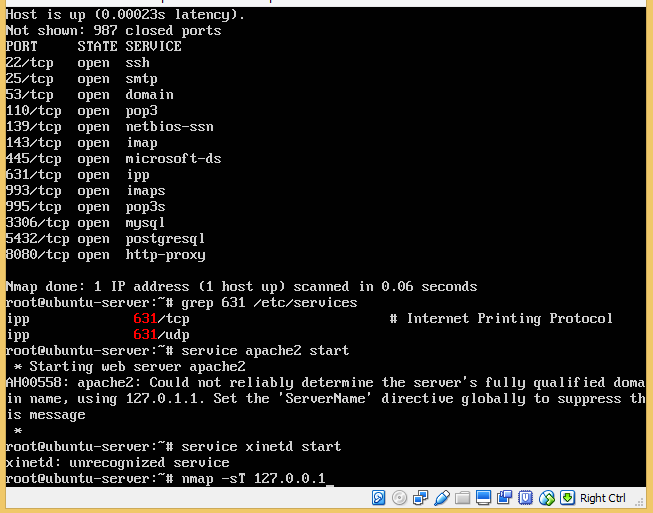
****

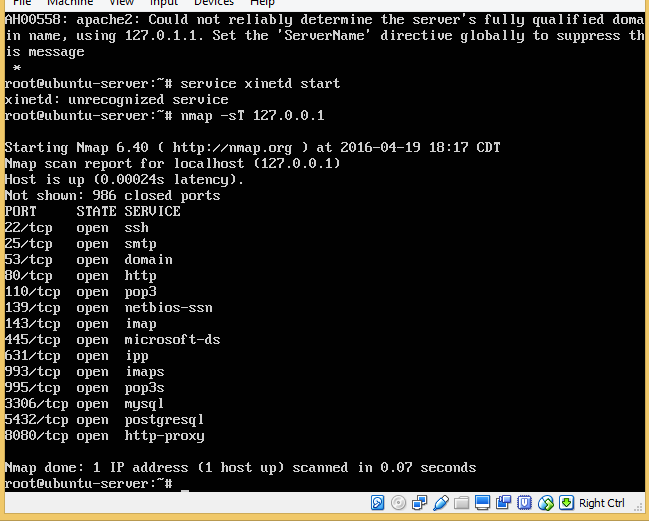
****

****

****

****

****

****

# Project 14-4

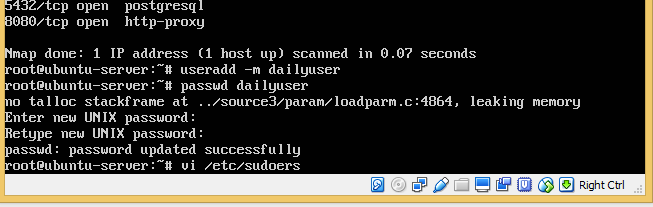
In this hands-on project, you configure and use the sudo utility to gain root access on your Ubuntu Server Linux virtual machine.

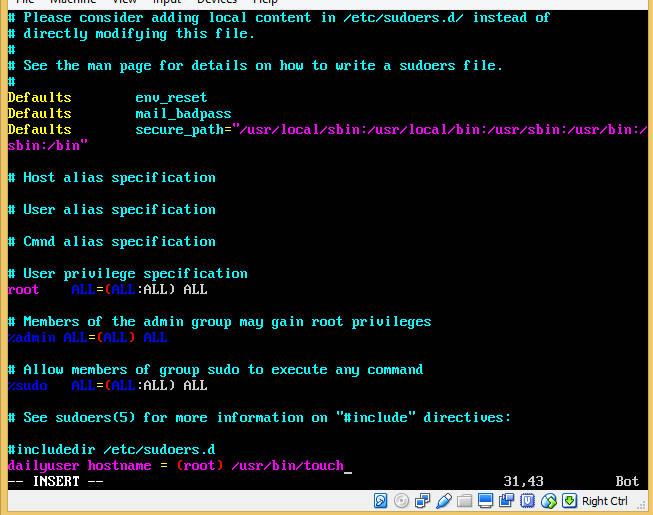
1. Boot your **Ubuntu** Linux virtual machine. Login to your chosen desktop environment as **root** using password **LNXrocks!** and open up a terminal window.
2. At the command prompt, type **useradd -m dailyuser** and press Enter.
3. At the command prompt, type **passwd dailyuser** and press Enter. Supply the password **LNXrocks!** when prompted both times.
4. Run the command **vi /etc/sudoers**. Add the following line to the end of the file (*where hostname is the hostname of your Ubuntu Server Linux virtual machine*):

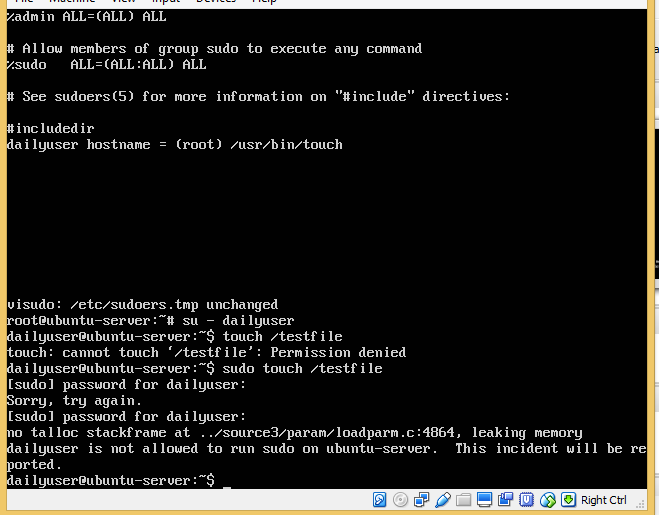
dailyuser *hostname* = (root) /usr/bin/touch

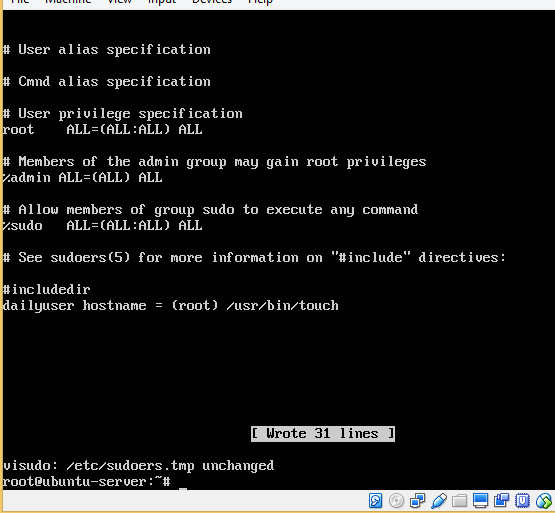
When finished, save your changes (you must use :w!) and quit the vi editor.

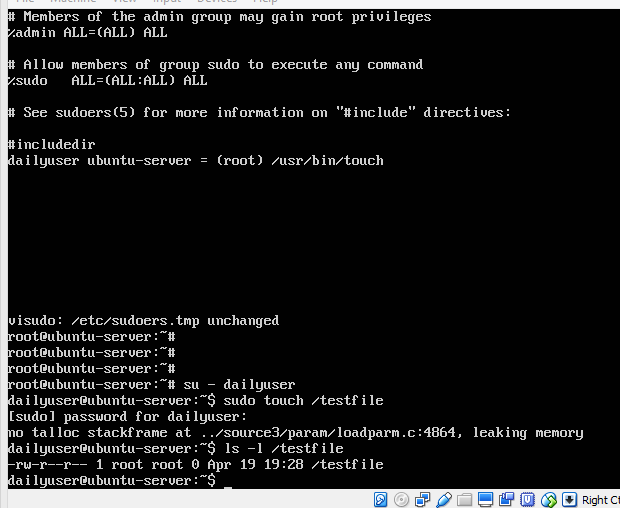
1. At the command prompt, type **su - dailyuser** and press Enter.
2. At the command prompt, type **touch /testfile** and press Enter. Were you able to create a file under the / directory? **No**
3. At the command prompt, type **sudo touch /testfile** and press Enter, then enter the password **LNXrocks!** when prompted. Were you able to create a file under the / directory? **Yes**
4. At the command prompt, type **ls -l /testfile** and press Enter. Who is the owner and group owner for this file? Why? **Root, because in the sudo you gave it the credentials for root.**
5. Type exit and press Enter to end your dailyuser session.
6. **Provide screenshot(s) of steps 2 through 9.**

****

****

****

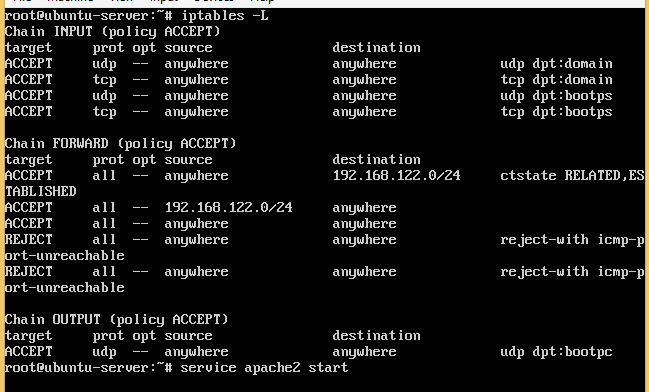
****

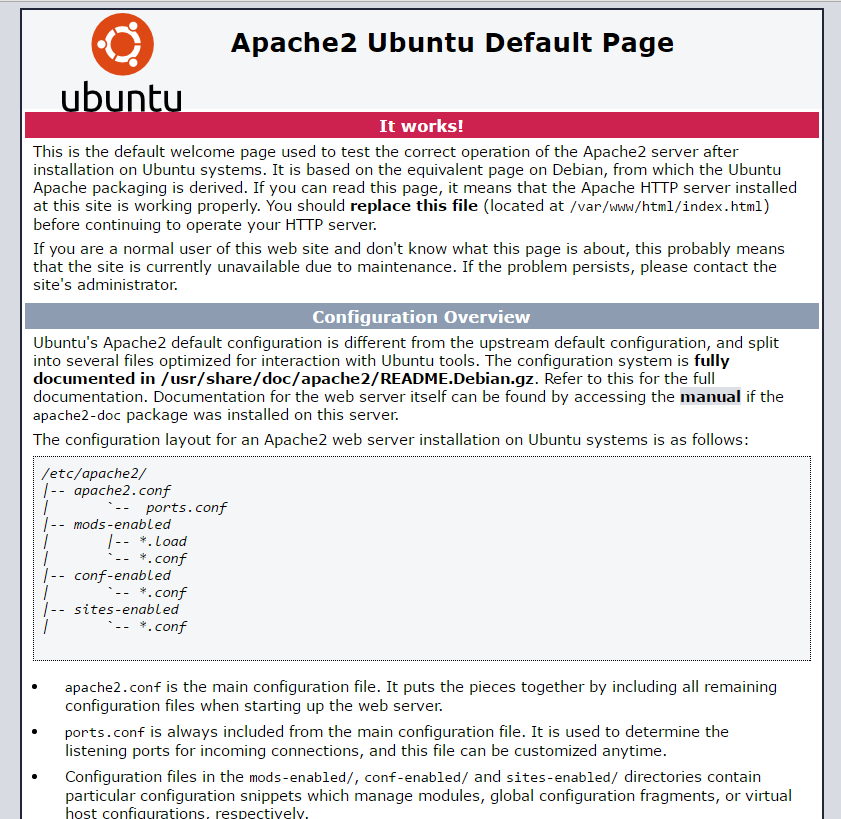
****

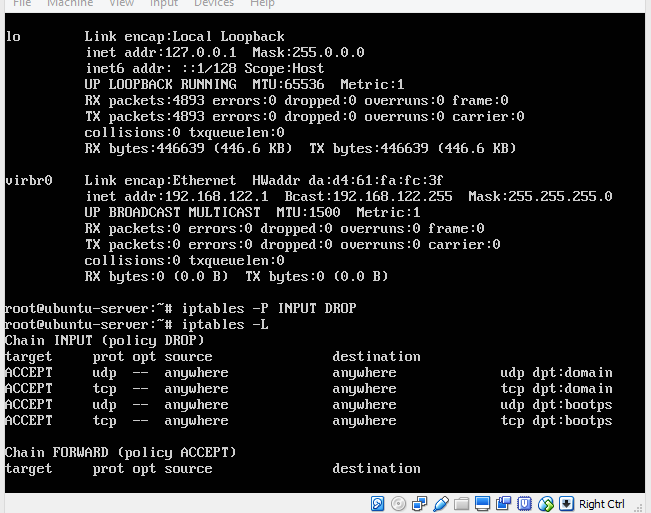
# Project 14-5

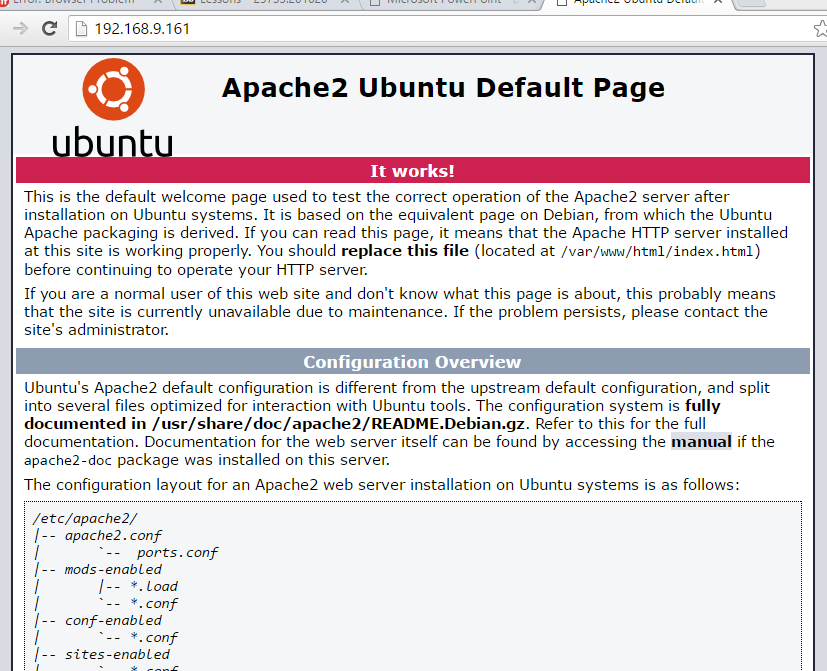
In this hands-on project, you configure and test the netfilter firewall on your Ubuntu Server Linux virtual machine.

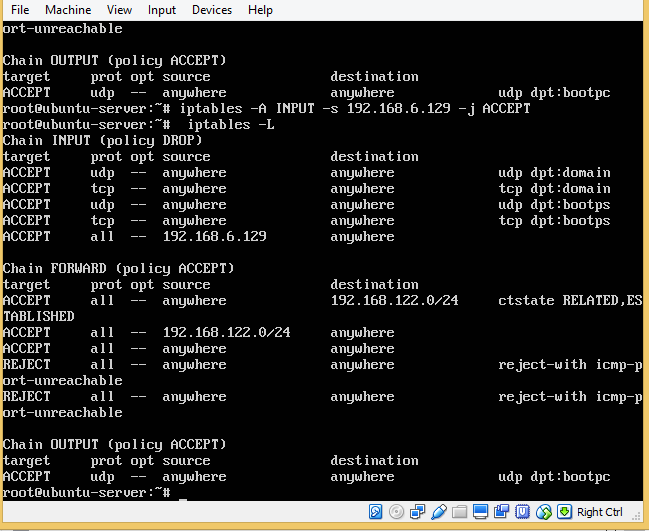
1. Boot your **Ubuntu** Linux virtual machine. Login to your chosen desktop environment as **root** using password **LNXrocks!** and open up a terminal window.
2. At the command prompt, type **iptables -L** and press Enter. What is the default action for the three chains? **All three Accept**
3. At the command prompt, type **service apache2 start** and press Enter to ensure that the Apache Web server is running.
4. Open a Web browser on your Windows host and enter the IP address of your Ubuntu Server Linux virtual machine in the location dialog box. Is your Web page displayed? **Yes**
5. On your Ubuntu Server Linux virtual machine, type **iptables -P INPUT DROP** at the command prompt and press Enter. What does this command do? **It drops incoming packets.**
6. At the command prompt, type **iptables -L** and press Enter. What is the default action for the three chains? **Drop, accept, accept**
7. Switch back to the Web browser on your Windows host and click the reload button. Does your page reload successfully? **No**
8. On your Ubuntu Server Linux virtual machine, type **iptables -A INPUT -s IP -j ACCEPT** at the command prompt (where IP is the IP address of your Windows host) and press Enter. What does this command do? **It adds it to the tables.**
9. At the command prompt, type **iptables -L** and press Enter. Do you see your rule underneath the INPUT chain? **Yes**
10. Switch back to the Web browser on your Windows host and click the reload button. Does your page reload successfully? **Yes**
11. On your Ubuntu Server Linux virtual machine, type **iptables -F** at the command prompt and press Enter. Next, type **iptables -P INPUT ACCEPT** at the command prompt and press Enter. What do these commands do? **–F removes any rules from chains and –P specifies the default policy.** At the command prompt, type **iptables -L** and press Enter to verify that the default policies for all three chains have been restored (additional stateful rules will be re-added over time as traffic passes to your Ubuntu Server Linux virtual machine).
12. **Provide screenshot(s) of steps 2 through 11.**

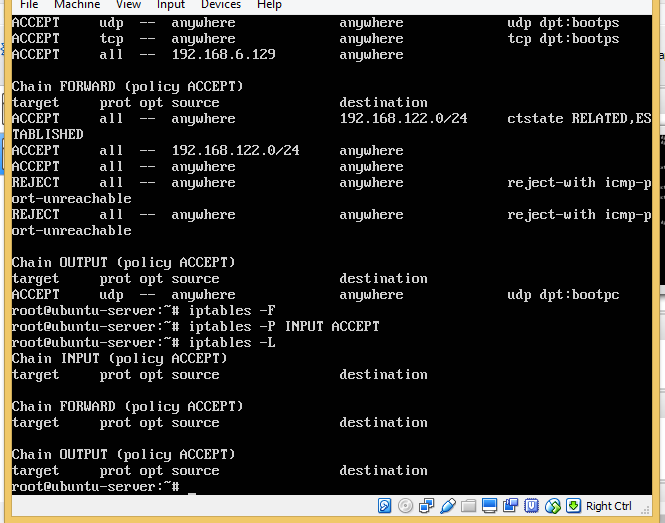
****

****

****

****

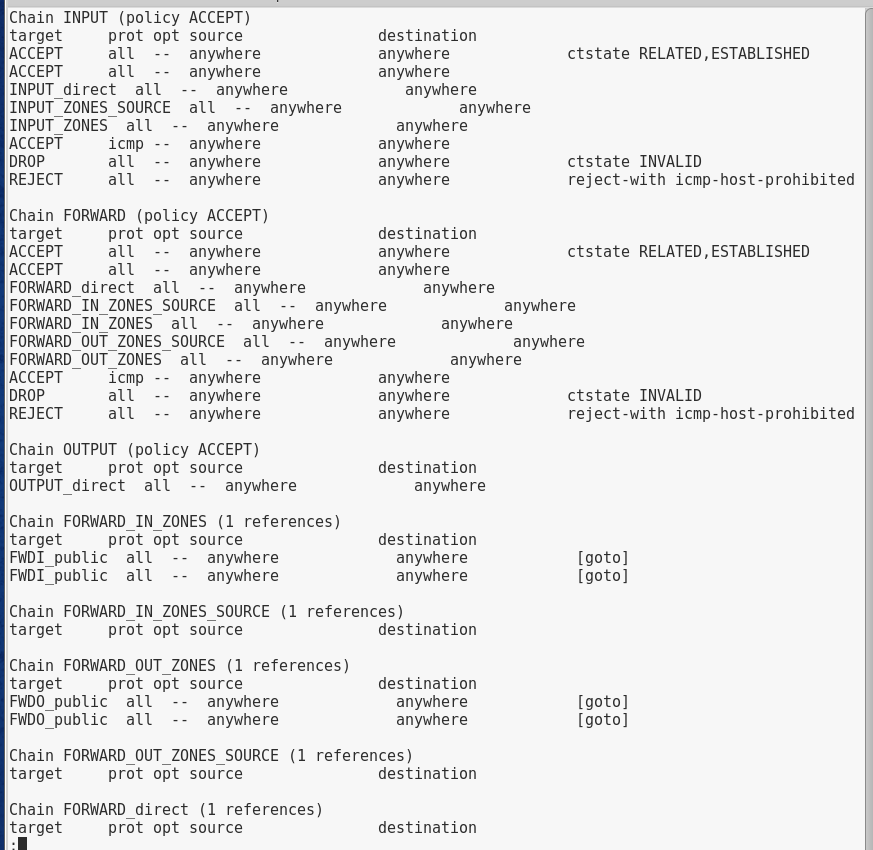
****

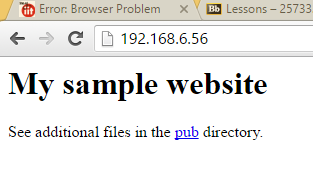
****

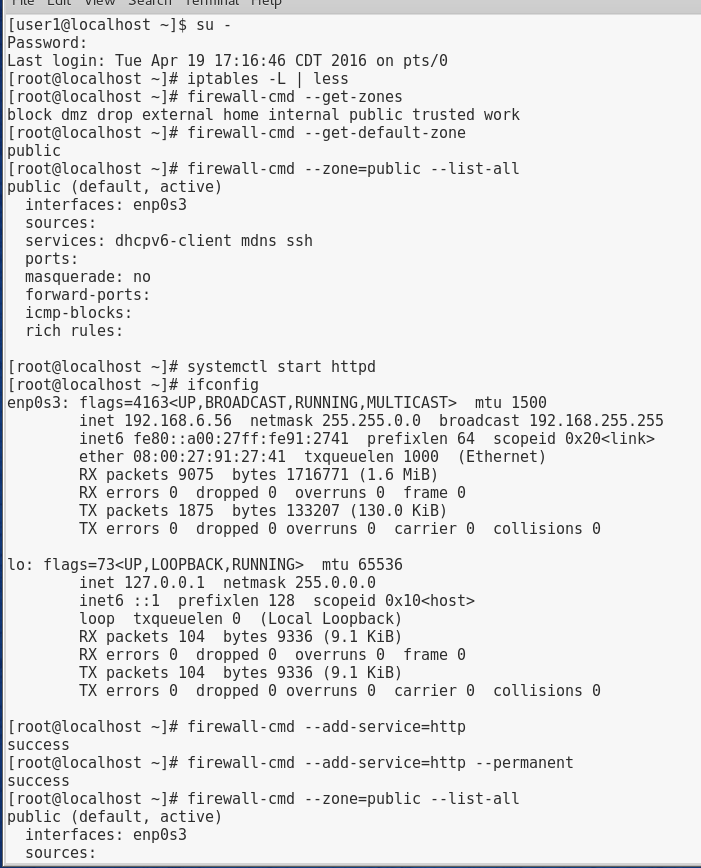
# Project 14-6

In this hands-on project, you configure firewalld and test the results on your Fedora Linux virtual machine.

1. Boot your **Fedora** Linux virtual machine. Login to your chosen desktop environment as **user1** using password **LNXrocks!** and open up a terminal window.
2. At the terminal, become **root** by typing **su -** and press enter and provide **LNXrocks!** as the password.
3. At the command prompt, type **iptables -L | less** and press Enter. Can you tell that firewalld is configured to set netfilter rules on your system? **Yes.**  Press q when finished to quit the less utility.
4. At the command prompt, type **firewall-cmd --get-zones** and press Enter to view the network zones on your system.
5. At the command prompt, type **firewall-cmd --get-default-zone** and press Enter. What is the default zone on your system? **public**
6. At the command prompt, type **firewall-cmd --zone=public -–list-all** and press Enter. What services are allowed in your firewall? Is the Apache Web server listed? Why not? **Dhcpv6-client mdns ssh, and no.**
7. At the command prompt, type **systemctl start httpd** and press Enter to ensure that the Apache Web server is started.
8. Open a Web browser on your Windows host and enter the IP address of your Fedora Linux virtual machine in the location dialog box. Is your Web page displayed? **No**
9. On your Fedora Linux virtual machine, type **firewall-cmd --add-service=http** at the command prompt and press Enter to allow the http service in your firewall. Next, type **firewall-cmd --add-service=http --permanent** and press Enter to ensure that the http service is allowed in the firewall after the next boot.
10. At the command prompt, type **firewall-cmd --zone=public -–list-all** and press Enter. Is http listed? **Yes**
11. Switch back to the Web browser on your Windows host and click the reload button. Did your page reload successfully? **Yes**
12. **Provide screenshot(s) of steps 3 through 11.**

****

****

****

****