

Name	Laura Adam
------	------------

CTS-120-841-Lab Module 5

- In this lab you will enter different Linux commands and answer questions about the results.
- Include a screen print of **just the area of the screen with the desired result** (not the whole screen) in the table cell below the question, unless otherwise instructed.
 - *Reminder: Use the **Shift-Ctrl-Prtscr** shortcut & select just the area that you want.*
- The lab is worth a total of 10 points – some questions have multiple sections

Ungraded, but important

- Go through the **Cursor movement (table 8-1), text editing (table 8-2), cut and paste (table 8-2), completion, and Using History** commands at the beginning of Chapter 8.
- Try some/all of these.
- There **will** be quiz questions on them, plus lots of them will be used in future labs to make your Linux lives easier.

In order to complete these questions & many in the future you will need to change the password for the user **root**:

In the terminal type:

```
sudo passwd root
```

1. It will ask you to enter **your** student password to elevate your privileges
2. Type a new root password that you will remember & then type it again
3. If you use a simple password such as **Password**, it will tell you it is a **BAD PASSWORD**, BUT IT WILL LET YOU USE THAT PASSWORD

```
[student@localhost ~]$ sudo passwd root
```

```
[sudo] password for student:
```

```
Changing password for user root.
```

```
New password:
```

```
Retype new password:
```

```
passwd: all authentication tokens updated successfully.
```

```
[student@localhost ~]$ sudo passwd root
[sudo] password for student:
Changing password for user root.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
[student@localhost ~]$ █
```

1. Create a file mod5-file.txt What are the default permissions on the file		1 Pt
Owner- Owner Group- World -	rw- read and write rw- read and write r--read only	
Screenprint:	-rw-rw-r--. 1 student student 0 Feb 26 19:31 mod5-file.txt	

2. Change the permissions on the file mod5-file.txt to allow only the owner and group to read and write, give no privileges to world		1 Pt
Command:	chmod o-rw mod5-file.txt	
Screenprint:	[student@localhost ~]\$ chmod o-rw mod5-file.txt [student@localhost ~]\$ ls -l mod5-file.txt -rw-rw----. 1 student student 0 Feb 26 19:31 mod5-file.txt	

3. 3. Using symbolic representation add execute permission for the owner, group, and world to mod5-file.txt		1 Pt
Command:	chmod +x mod5-file.txt	
Screenprint:	[student@localhost ~]\$ chmod +x mod5-file.txt [student@localhost ~]\$ ls -l mod5-file.txt -rwxrwx--x. 1 student student 0 Feb 26 19:31 mod5-file.txt	

4. Using umask set the default permissions to be: User = rw- Group=r- - World=r- - Create a file umask-test and show me the resulting permissions		1 Pt
Command:	Umask 022 unmask.test	
Screenprint:	-rw-rw-r--. 1 student student 0 Mar 4 13:01 unmask-test	

5. Use the command: <code>tail -5 /etc/shadow</code> Show me the last 5 lines of the shadow file. Do it WITHOUT starting a shell as another user. Your normal user will not have the permissions to do this; you will have to change identities		1 Pt
Command:	<code>Sudo 'tail -5 /etc/shadow</code>	
Screenprint:	<pre>student@localhost ~]\$ sudo 'tail-5/etc/shadow > sudo 'tail-5/etc/shadow [sudo] password for student:</pre>	

6. Run <code>tail -5 /etc/shadow</code> as a single command by passing it to a shell for execution as another user (root).		1 Pt
Command:	<code>su -c 'tail -5 /etc/shadow'</code>	
Screenprint:	<pre>[student@localhost ~]\$ su -c tail-5/etc/shadow Password: su: Authentication failure</pre>	

7. Change the ownership of the file mod5-file.txt to: User=sshd Group= wheel		1 Pt
Command:	<code>chown student :wheel mod5-file.txt</code> <u>CHOWN SSHD:WHEEL MOD5_FILE.TXT DIDNT</u>	
Screenprint:	<code>-rw-rw-r--. 1 student wheel 0 Mar 4 13:01 mod5-file.txt</code>	

8. Show all your running processes regardless of what terminal (if any) they are controlled by. It will be a long list , just show me the last 5 or so.		1 Pt
Command:	<code>[student@localhost ~]\$ ps x</code>	
Screenprint:	<pre>2930 ? SI 0:00 /usr/libexec/gvfsd-metadata 2957 ? SI 0:05 /usr/libexec/gnome-terminal-server</pre>	

	2963 ? S 0:00 gnome-pty-helper 2964 pts/0 Ss 0:00 bash 51612 pts/0 R+ 0:00 ps x
--	---

9. Show me the top processes on the system. It will be a long list, just show me the header and the top 5.		1 Pt
Command:	[student@localhost ~]\$ ps x	
Screenprint:	<pre>[student@localhost ~]\$ ps x PID TTY STAT TIME COMMAND 1877 ? SI 0:00 /usr/bin/gnome-keyring-daemon --daemonize --login 1882 ? Ssl 0:00 /usr/libexec/gnome-session-binary --session gnome-classic 1891 ? S 0:00 dbus-launch --sh-syntax --exit-with-session 1892 ? Ssl 0:00 /usr/bin/dbus-daemon --fork --print-pid 5 --print-address 7 1961 ? SI 0:00 /usr/libexec/imsettings-daemon</pre>	

10. What is the process ID (PID) and command that is using the most memory? 11.		1 Pt
PID:	2119	
Top Command:	/usr/bin/gnome-shell	
Screenprint:	<pre>USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND student 2119 1.2 15.6 3010692 156660 ? SI 11:48 0:46 /usr/bin/gnome-shell</pre>	

My password keeps defaulting to the CENTOS Student password – Why? IS the new password only associated with the temporary virtual machine?

What am I missing from the examples in the book syntax wise? They don't run on my VM ? I use google to get more info on the command but still get errors (#4,5,6,7)