WIIT 7780 Lab 4: Exploring Processes and Process Data Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 1**

Sign into your Ubuntu Desktop with credentials provided by your Instructor

Exercise 1: Package Management with APT-CACHE

1. Open a Terminal window
2. At the prompt, type **ip -s link** and press Enter. This will pull up your network device status information.
3. Look through the network information presented, ignoring the information for the loopback (lo). You should see an information item named state. The state should be UP. If your system is not currently connected to the Internet, then do what is needed to get your network started with access to the Internet.
4. Once you ensure your network is up and running, on the tty2 terminal, type **apt-cache pkgnames** and press Enter. (Be patient! If it has been "a while" since you issued an apt-cache command, the package database will update before providing the apt-cache command's results and it can take some time.) Once the repository information is updated, you will see a LOT of packages fly by on the screen.
5. When the output from the preceding step has stopped, look at the first column, bottom of the apt-cache list, and record the package name you find there: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
6. Type in **apt-cache show *PackageName*** and press Enter. Don’t actually type *PackageName*, but instead use the name of the package you recorded in step #7. You should see about the same information on the software packages as you did above. However, this command shows information on a particular software package.

Exercise 1: Package Management with APT-CACHE (continued)

1. Find out if the emacs package is installed. emacs is another popular text editor with graphic capabilities. Type in **emacs** and press Enter. Note if the package is installed. If it is not, note options for use if installed.
2. Find out if the gedit package is installed. emacs is another popular text editor with graphic capabilities. Type in **gedit** and press Enter. Note if the package is installed. If it is not, note options for use if installed
3. Pick a package that is not currently installed (hopefully one of the editors from the preceding steps) and install the package by typing  
   **apt-get install Package** and pressing the Enter key. Don’t actually type *Package*, but instead type the name of the package you wish to install (for example, if you are installing the gedit package, you would type **apt-get install gedit**).
4. Type **y** and press Enter to answer any yes/no questions asked during the installation process. (If the package you have chosen to install has lots of dependencies, you will need to be patient. It may take a while to download and install all the dependency packages!) You will know it’s done when you get a shell prompt.
5. Check to see if the package is installed by typing **apt-cache show Package** and pressing Enter. Don’t actually type *Package*, but instead type the name of the package you just installed. Find the line that starts with Repo. You should see the words installed on that line, indicating that the package is installed.
6. Now, after all that hard work, you are going to remove the software package you just installed. Type **apt-get purge *Package*** and press Enter. Don’t actually type *Package*, but instead type the name of the package you installed a few steps ago. If you get a prompt similar to "Is this okay [y/N]:", type in **y** and press Enter. You will know the package has been removed when you get a message similar to "Complete!" and the prompt back.
7. Double-check that the software package has been uninstalled by typing  
   ***Package*** and pressing Enter. Don’t actually type *Package*, but instead type the name of the package you just uninstalled. Notice that it is listed as "Available." If you really wanted to, you could install it again! Remember, the packages themselves reside on a network repository server awaiting your whim to install them.
8. To see what repositories (repos) your system will search for packages, type in **apt-cache policy** and press Enter. Sometimes you need a package that is not on one of the standard repositories. This is a way to check and see what repositories you have configured.
9. Another way to see the repos your system will search for a package is to type **apt-cache policy |grep http |awk '{print $2 $3}' |sort -u**  and press Enter. Occasionally you will need to add a repository for a package that does not exist in the standard repositories
10. Type **exit** to exit out of the root user account.

Exercise 2: Package Management with dpkg

* 1. List the installed Ubuntu packages by typing

**sudo dpkg --get-selections | less** and pressing Enter. (There are TWO dashes ahead of get-selections. Don’t leave them out.) You will need to enter your password when prompted and press Enter. This will show you all the currently installed packages on this system. When you are done viewing the various packages, press **q** to quit the less pager.

* 1. Display information about the sudo package by typing   
     **sudo dpkg -p sudo** and pressing Enter. You will need to enter your password if prompted and press Enter.
  2. View all of the files associated with the sudo package by typing  
     **sudo dpkg -L sudo**  **| less** and pressing Enter. You will need to enter your password if prompted and press Enter. When you are done viewing the various files, press **q** to quit the less pager.
  3. Install the tint game package using apt-get by typing

**sudo apt-get install tint** and pressing Enter. You may need to enter your password if prompted and press Enter. Type **y** and press Enter for any yes/no prompts. You will know the installation is complete when you get the prompt back.

* 1. Display information about the tint game by typing **sudo dpkg -p tint** and pressing Enter. You may need to enter your password if prompted and press Enter.
  2. Determine the status of the tint game by typing in **sudo dpkg -s tint** and pressing Enter. You may need to enter your password if prompted and press Enter. Find the Status: line. It should say install or something similar.
  3. Start the tint game by typing **./usr/games/tint** and pressing Enter. Type in **1** and press Enter for the game level prompt, and then use the arrow keys to “arrange” the blocks as they descend.
  4. When you are done “testing out” the game, remove the tint game from your system by typing **sudo apt-get remove tint** and pressing Enter. You may need to enter your password if prompted and press Enter. Type **y** and press Enter for any yes/no prompts. You will know the removal is complete when you get the prompt back.
  5. Determine the status of the tint game by typing in **sudo dpkg -s tint** and pressing Enter. You may need to enter your password if prompted and press Enter. Find the Status: line. It should say deinstall or something similar.

Exercise 3: Viewing Processes and System Information

1. Open a Terminal window.
2. Type **ps** and press Enter. You should see four columns of displayed information, similar to the following:  
   PID TTY TIME CMD  
   2056 tty2 00:00:00 bash  
   2110 tty2 00:00:00 ps  
   The ps command allows you to see your current processes. The first column, PID, stands for Process ID number. Each process is assigned a Process ID number. The second column, TTY, shows what terminal the process is running on. The fourth column, CMD, shows the name of the program running.
3. Using the information you obtained in the preceding step, list two programs you are running:  
   1) \_\_\_\_\_\_\_\_\_\_\_  
     
   2) \_\_\_\_\_\_\_\_\_\_\_
4. Type in **ps -l** and press Enter. The option is a lowercase L and not a one.  
   The -l option gives you a long listing of processes.  
   You should see 14 columns of displayed information, similar to the following:
5. F S UID PID PPID C PRI NI ADDR SZ WCHAN TTY TIME CMD  
   0 S 500 2056 2054 0 80 0 1131 wait tty2 00:00:00 bash  
   0 R 500 2110 2056 0 80 0 - 1177 - tty2 00:00:00 ps
6. In the information you obtained in the preceding step, notice that your bash process is in a sleeping (S) process state (S column), while your ps process is in a running (R) process state. This is due to the fact that the ps command takes a picture of the system at one particular moment in time…the time that the ps command is running.
7. To see every process on a system, you need to add a couple of additional options to the ps command. Type **ps -elf** and press Enter. You should see a lot of process information go flying by on your screen!

Exercise 3: Viewing Processes and System Information (continued)

9. Pipe the process information into the less pages to allow a more leisurely view of the processes. Type **ps -elf | less** and press Enter. Page through the listing of the various processes. If you see a ? in the listing anywhere, that is a terminal listing for a daemon process. A daemon is a process on a Linux system that performs a particular service, such as printing. These processes do not run on a terminal, and therefore a ? is put in the terminal column for results from the ps command.

10. Press **q** when you are done reviewing the process listing to quit the less command.

11. Another ps command to try is called a BSD-style, because it uses no dashes in its options. Type **ps aux**  and press Enter. Slightly different information is displayed, but it is just as useful as the information you saw in the previous steps. There are lots of ways to display process information using the ps command. (Type **man ps** and press Enter to see more ways and methods, if you so desire.)

12. You can view an interactive display of process information by typing **top** and pressing Enter. Take a look around this busy screen. See if you can find:  
1) Process State totals  
2) How many users are on the system  
3) Memory usage  
One of the primary purposes of the top utility is to view what processes are using the most cpu time. However, there is a lot of additional information here! By the way, using top, you can also kill processes, change process priorities, etc. There are several commands that you can enter. See the man pages on top for more information.

13. Press **q** to quit the top utility. You should get your prompt back.

14. To see the amount of memory being used on the Linux system, type **free** and press Enter.

15. Take a look at the amount of time the system has been up by typing **uptime** and pressing Enter. Notice that you are also shown a load average here.

Exercise 4: Locating Log Files and Using dmesg

1. If you have not already done so, connect to your hosted desktop machine and login.
2. Open a Terminal window.
3. Type **unalias ls** and press Enter. This will make it easier to see the various files in the next step.

Type **ls -F /var/log** and press Enter. Check off the following log files or log file directories you find in this directory:  
  
\_\_\_\_\_ auth.log \_\_\_\_\_ gdm/   
  
\_\_\_\_\_ boot.log \_\_\_\_ messages   
  
\_\_\_\_\_ cups/ \_\_\_\_ secure   
  
\_\_\_\_\_ dmesg \_\_\_\_ syslog  
  
System log files are stored in the /var/log directory. Notice that the directory also contains several subdirectories (denoted by the / symbol at the end of their names) where various daemons, such as cups, store their log files.

1. Take a look at the syslog file by typing **tail /var/log/syslog** and pressing Enter. The syslog file contains various messages from various processes, including daemons.
2. Try another log file (warning: this won’t work!) by typing **tail /var/log/secure** and pressing Enter. Did you get a “No such file” error message? You should! This file is not available on Ubuntu. Instead the /var/log/auth.log takes its place.
3. Take a look at the auth.log file by typing **sudo** **tail /var/log/auth.log** and pressing Enter. Can you also view the file now? This log file contains security-related messages.
4. Take a look at the kernel ring buffer’s log file. (Be aware that this file may NOT be on your system. It depends upon the system’s configuration.) Type **tail /var/log/dmesg** and press Enter. This file contains messages concerning the kernel ring buffer…but only during system boot time! (See the next step for more details).
5. To see the latest kernel ring buffer information, you need to use a utility. Type in **dmesg** and press Enter. This utility allows you to see the latest and greatest kernel ring buffer messages. (But it’s nice to have the /var/log/dmesg file for a record of boot information. This is especially true if your system has been running for a while!)