

Justin Landolina

UID: 01214163

Assignment 14 System Admin

CYSE270_33410 LINUX SYSTEM FOR CYBERSECURITY

Task A

```
root@jland018: ~  
File Actions Edit View Help  
[root@jland018]~# ps  
  PID TTY          TIME CMD  
 2037 pts/1    00:00:00 zsh  
 2573 pts/1    00:00:00 ps  
[root@jland018]~# ps a  
  PID TTY          STAT       TIME COMMAND  
  595 tty1      Ss+        0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux  
  597 tty7      Ssl+       0:21 /usr/lib/xorg/Xorg :0 -seat seat0 -auth /var/run/lightdm/root/:0 -nolisten tcp vt7 -novtswi  
 1973 pts/0      Ss+        0:00 /usr/bin/zsh  
 2037 pts/1      Ss         0:00 /usr/bin/zsh  
 3212 pts/1      R+         0:00 ps a  
[root@jland018]~# ps -f  
UID          PID    PPID  C STIME TTY          TIME CMD  
root         2037    1965  0 15:11 pts/1    00:00:00 /usr/bin/zsh  
root         3300    2037  0 15:17 pts/1    00:00:00 ps -f
```

In this screenshot I list the processes running in the current shell and list all the processes running on the system.

```
root@jland018: ~  
File Actions Edit View Help  
top - 15:19:58 up 12 min,  1 user,  load average: 0.01, 0.25, 0.34  
Tasks: 166 total,  1 running, 165 sleeping,  0 stopped,  0 zombie  
%Cpu(s):  0.4 us,  0.2 sy,  0.0 ni, 99.4 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st  
MiB Mem : 7943.2 total, 6932.8 free,  543.7 used,  466.7 buff/cache  
MiB Swap:  976.0 total,  976.0 free,  0.0 used,  7164.8 avail Mem  


| PID  | USER   | PR | NI  | VIRT   | RES    | SHR   | S | %CPU | %MEM | TIME+   | COMMAND                     |
|------|--------|----|-----|--------|--------|-------|---|------|------|---------|-----------------------------|
| 597  | root   | 20 | 0   | 366872 | 117508 | 48964 | S | 1.0  | 1.4  | 0:23.55 | Xorg                        |
| 560  | root   | 20 | 0   | 294084 | 3244   | 2728  | S | 0.3  | 0.0  | 0:00.26 | VBoxService                 |
| 902  | justin | 20 | 0   | 215312 | 32400  | 17236 | S | 0.3  | 0.4  | 0:03.62 | panel-13-cpugra             |
| 1965 | root   | 20 | 0   | 406708 | 78968  | 63884 | S | 0.3  | 1.0  | 0:02.52 | x-terminal-emul             |
| 1    | root   | 20 | 0   | 164428 | 10824  | 8016  | S | 0.0  | 0.1  | 0:02.12 | systemd                     |
| 2    | root   | 20 | 0   | 0      | 0      | 0     | S | 0.0  | 0.0  | 0:00.01 | kthreadd                    |
| 3    | root   | 0  | -20 | 0      | 0      | 0     | I | 0.0  | 0.0  | 0:00.00 | rcu_gp                      |
| 4    | root   | 0  | -20 | 0      | 0      | 0     | I | 0.0  | 0.0  | 0:00.00 | rcu_par_gp                  |
| 5    | root   | 20 | 0   | 0      | 0      | 0     | I | 0.0  | 0.0  | 0:00.00 | kworker/0:0-events          |
| 6    | root   | 0  | -20 | 0      | 0      | 0     | I | 0.0  | 0.0  | 0:00.00 | kworker/0:0H-events_highpri |
| 7    | root   | 20 | 0   | 0      | 0      | 0     | I | 0.0  | 0.0  | 0:01.56 | kworker/u8:0-flush-8:0      |
| 8    | root   | 0  | -20 | 0      | 0      | 0     | I | 0.0  | 0.0  | 0:00.00 | mm_percpu_wq                |
| 9    | root   | 20 | 0   | 0      | 0      | 0     | S | 0.0  | 0.0  | 0:00.00 | rcu_tasks_rude_             |
| 10   | root   | 20 | 0   | 0      | 0      | 0     | S | 0.0  | 0.0  | 0:00.00 | rcu_tasks_trace             |
| 11   | root   | 20 | 0   | 0      | 0      | 0     | S | 0.0  | 0.0  | 0:00.00 | ksoftirqd/0                 |
| 12   | root   | 20 | 0   | 0      | 0      | 0     | I | 0.0  | 0.0  | 0:00.70 | rcu_sched                   |
| 13   | root   | rt | 0   | 0      | 0      | 0     | S | 0.0  | 0.0  | 0:00.02 | migration/0                 |
| 15   | root   | 20 | 0   | 0      | 0      | 0     | S | 0.0  | 0.0  | 0:00.00 | cpuhp/0                     |
| 16   | root   | 20 | 0   | 0      | 0      | 0     | S | 0.0  | 0.0  | 0:00.00 | cpuhp/1                     |
| 17   | root   | rt | 0   | 0      | 0      | 0     | S | 0.0  | 0.0  | 0:00.43 | migration/1                 |
| 18   | root   | 20 | 0   | 0      | 0      | 0     | S | 0.0  | 0.0  | 0:00.05 | ksoftirqd/1                 |
| 20   | root   | 0  | -20 | 0      | 0      | 0     | I | 0.0  | 0.0  | 0:00.00 | kworker/1:0H-events_highpri |
| 21   | root   | 20 | 0   | 0      | 0      | 0     | S | 0.0  | 0.0  | 0:00.00 | cpuhp/2                     |
| 22   | root   | rt | 0   | 0      | 0      | 0     | S | 0.0  | 0.0  | 0:00.42 | migration/2                 |
| 23   | root   | 20 | 0   | 0      | 0      | 0     | S | 0.0  | 0.0  | 0:00.00 | ksoftirqd/2                 |
| 25   | root   | 0  | -20 | 0      | 0      | 0     | I | 0.0  | 0.0  | 0:00.00 | kworker/2:0H-kblockd        |


```

Top command running

```
root@jland018: ~
File Actions Edit View Help
Help for Interactive Commands - procps-ng 3.3.17
Window 1:Def: Cumulative mode Off. System: Delay 3.0 secs; Secure mode Off.

Z,B,E,e Global: 'Z' colors; 'B' bold; 'E'/'e' summary/task memory scale
l,t,m,I Toggle: 'l' load avg; 't' task/cpu; 'm' memory; 'I' Irix mode
0,1,2,3,4 Toggle: '0' zeros; '1/2/3' cpu/numa views; '4' cpus two abreast
f,F,X Fields: 'f'/'F' add/remove/order/sort; 'X' increase fixed-width

L,&,<,> . Locate: 'L'/'&' find/again; Move sort column: '<'/'>' left/right
R,H,J,C . Toggle: 'R' Sort; 'H' Threads; 'J' Num justify; 'C' Coordinates
c,i,S,j . Toggle: 'c' Cmd name/line; 'i' Idle; 'S' Time; 'j' Str justify
x,y . Toggle highlights: 'x' sort field; 'y' running tasks
z,b . Toggle: 'z' color/mono; 'b' bold/reverse (only if 'x' or 'y')
u,U,o,O . Filter by: 'u'/'U' effective/any user; 'o'/'O' other criteria
n,#,^O . Set: 'n'/'#' max tasks displayed; Show: Ctrl+'O' other filter(s)
V,v . Toggle: 'V' forest view; 'v' hide/show forest view children

k,r Manipulate tasks: 'k' kill; 'r' renice
d or s Set update interval
W,Y,! Write config file 'W'; Inspect other output 'Y'; Combine Cpus '!'
q Quit
( commands shown with '.' require a visible task display window )
Press 'h' or '?' for help with Windows,
Type 'q' or <Esc> to continue
```

Top help command

```
justin@justin-VirtualBox: ~
gnome-calculator &
[1] 3301
justin@justin-VirtualBox:~$ jobs
[1]+  Done                  gnome-calculator
justin@justin-VirtualBox:~$ sudo killall gnome-calculator
[sudo] password for justin:
gnome-calculator: no process found
justin@justin-VirtualBox:~$ jobs
justin@justin-VirtualBox:~$ ps
  PID TTY          TIME CMD
 3295 pts/0        00:00:00 bash
 3397 pts/0        00:00:00 ps
justin@justin-VirtualBox:~$
```

Had to switch back to Ubuntu here, was having trouble with locked directories in Kali. Ran the calculator in the background before killing the process. I then use the ps command to see the running processes in the current shell.

Task B

```
justin@justin-VirtualBox:~$ sudo dpkg -i ./skypeforlinux-64.deb
Selecting previously unselected package skypeforlinux.
(Reading database ... 220137 files and directories currently installed.)
Preparing to unpack ./skypeforlinux-64.deb ...
Unpacking skypeforlinux (8.83.0.408) ...
```

Installing skype using dpkg

```
justin@justin-VirtualBox: /etc/apt
justin@justin-VirtualBox:~$ cd /etc/apt/
justin@justin-VirtualBox:/etc/apt$ ls
apt.conf.d  preferences.d  sources.list.d
auth.conf.d sources.list   trusted.gpg.d
justin@justin-VirtualBox:/etc/apt$ cp sources.list sources.list.bk
cp: cannot create regular file 'sources.list.bk': Permission denied
justin@justin-VirtualBox:/etc/apt$ sudo cp sources.list sources.list.bk
[sudo] password for justin:
justin@justin-VirtualBox:/etc/apt$
```

Making a backup copy of sources.list

```
justin@justin-VirtualBox: /etc/apt
justin@justin-VirtualBox:~$ cd /etc/apt/
justin@justin-VirtualBox:/etc/apt$ ls
apt.conf.d  preferences.d  sources.list.d
auth.conf.d sources.list   trusted.gpg.d
justin@justin-VirtualBox:/etc/apt$ cp sources.list sources.list.bk
cp: cannot create regular file 'sources.list.bk': Permission denied
justin@justin-VirtualBox:/etc/apt$ sudo cp sources.list sources.list.bk
[sudo] password for justin:
justin@justin-VirtualBox:/etc/apt$ vi sources.list
justin@justin-VirtualBox:/etc/apt$ vi sources.list.bk
justin@justin-VirtualBox:/etc/apt$ vi sources.list
justin@justin-VirtualBox:/etc/apt$ sudo vi sources.list
justin@justin-VirtualBox:/etc/apt$ sudo cp sources.list sources.list.bk
justin@justin-VirtualBox:/etc/apt$ sudo vi sources.list
justin@justin-VirtualBox:/etc/apt$ sudo vi sources.list
justin@justin-VirtualBox:/etc/apt$ sudo apt-get install joe
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.
justin@justin-VirtualBox:/etc/apt$
```

Deleting all the data in the sources.list file and tried to install joe with no success

```
justin@justin-VirtualBox:~$ cd /etc/apt/
justin@justin-VirtualBox:/etc/apt$ sudo cp sources.list.bk sources.list
justin@justin-VirtualBox:/etc/apt$ sudo apt-get install joe
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.
justin@justin-VirtualBox:/etc/apt$ sudo dpkg --configure -a
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
justin@justin-VirtualBox:/etc/apt$ sudo apt-get install joe
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

In this screenshot I copied back over the backup for sources and ran the apt get install joe command again.