Activity File: Process Investigation

- In the last activity, we completed a basic audit of the system and found some malicious script files and a user that was not supposed to be on the system. Now we will investigate all the processes running on the system to check if there are any obvious processes that should not be running.

- Your senior administrator has asked that you record snapshots of processes, as well as review the processes in real time for anything suspicious.

- You must review the processes that are running on the system to make sure nothing is amiss. If it is, you will want to `kill` that process and add what you found to your report.

Instructions

Log into the lab environment with the following credentials:

- Username: `sysadmin`
- Password: `cybersecurity`

To get started with your activity, run the following command in your terminal:

- `sudo bash /home/instructor/Documents/setup_scripts/instructor/processes.sh </dev/null &>/dev/null`

After which, you'll be able to use your terminal like usual.

Please read the following instructions and complete the steps.

1. During the last activity, you found a script file in a strange location on the system. Review the contents of this script file to get an idea of what commands you might be searching for.

    - List all the running processes in real time.

    - Review the help menu for this command and get a few ideas of what you want to investigate.

    - Highlight the column that you are sorting by.

2. To get an idea of how the system is currently running, answer these questions:

    - How many tasks have been started on the host?

      270 total, 3 running

    - How many of these are sleeping?

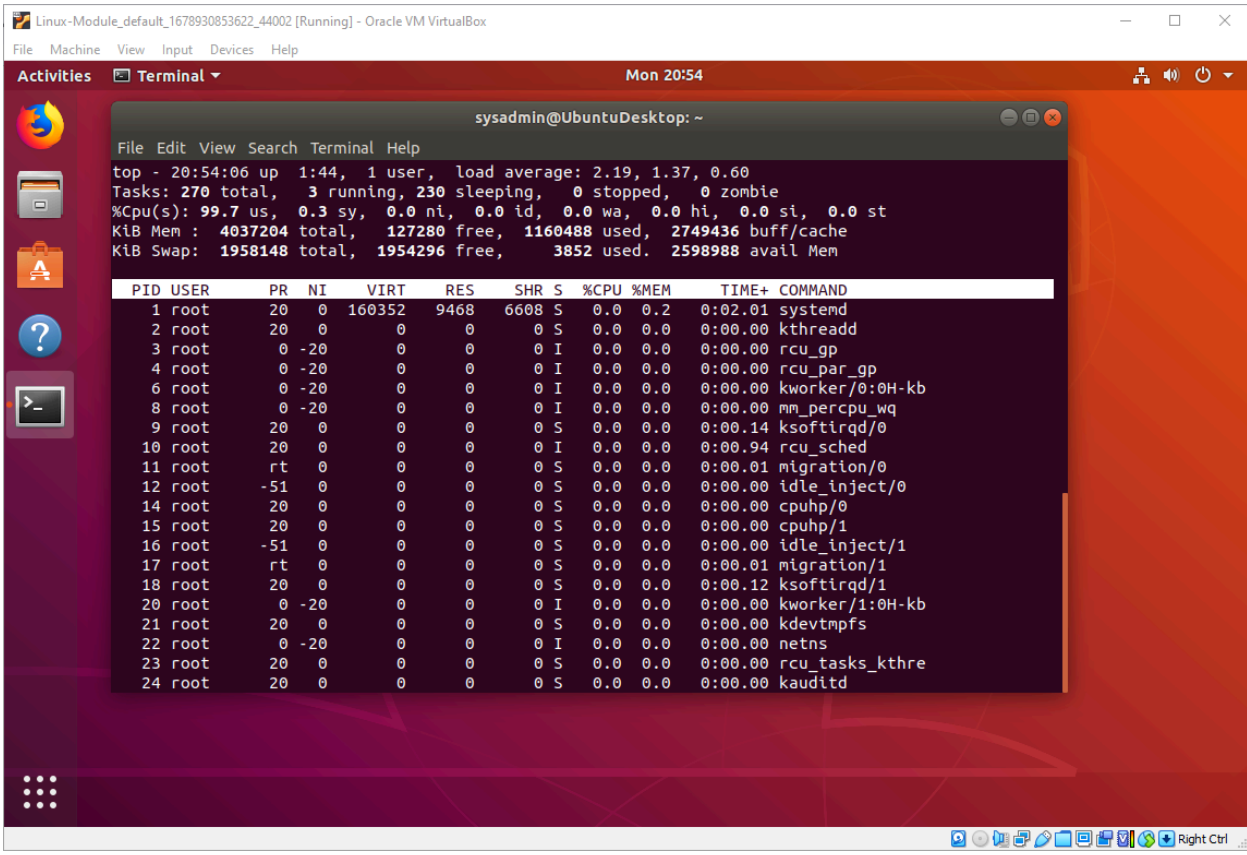
      229 sleeping

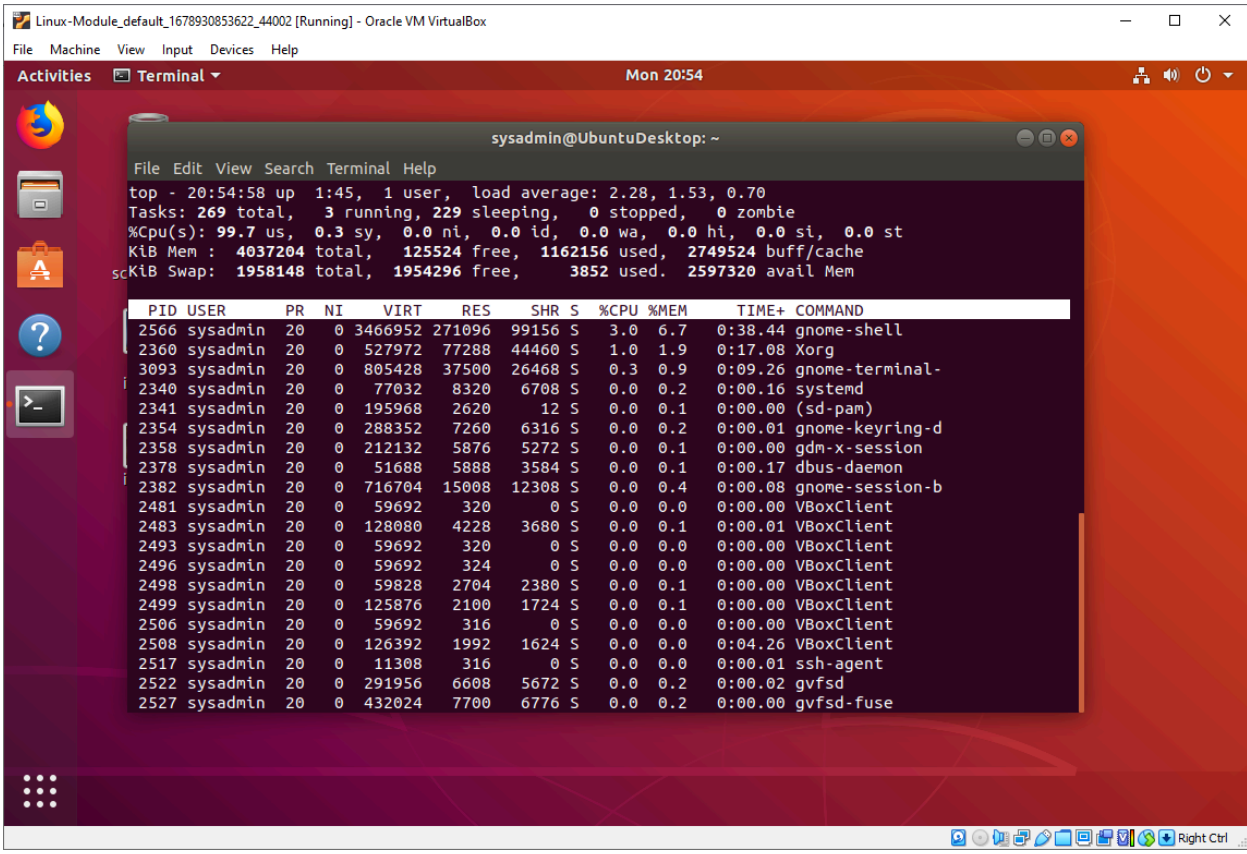
    - Which process uses the most memory?

      5217 and 5218

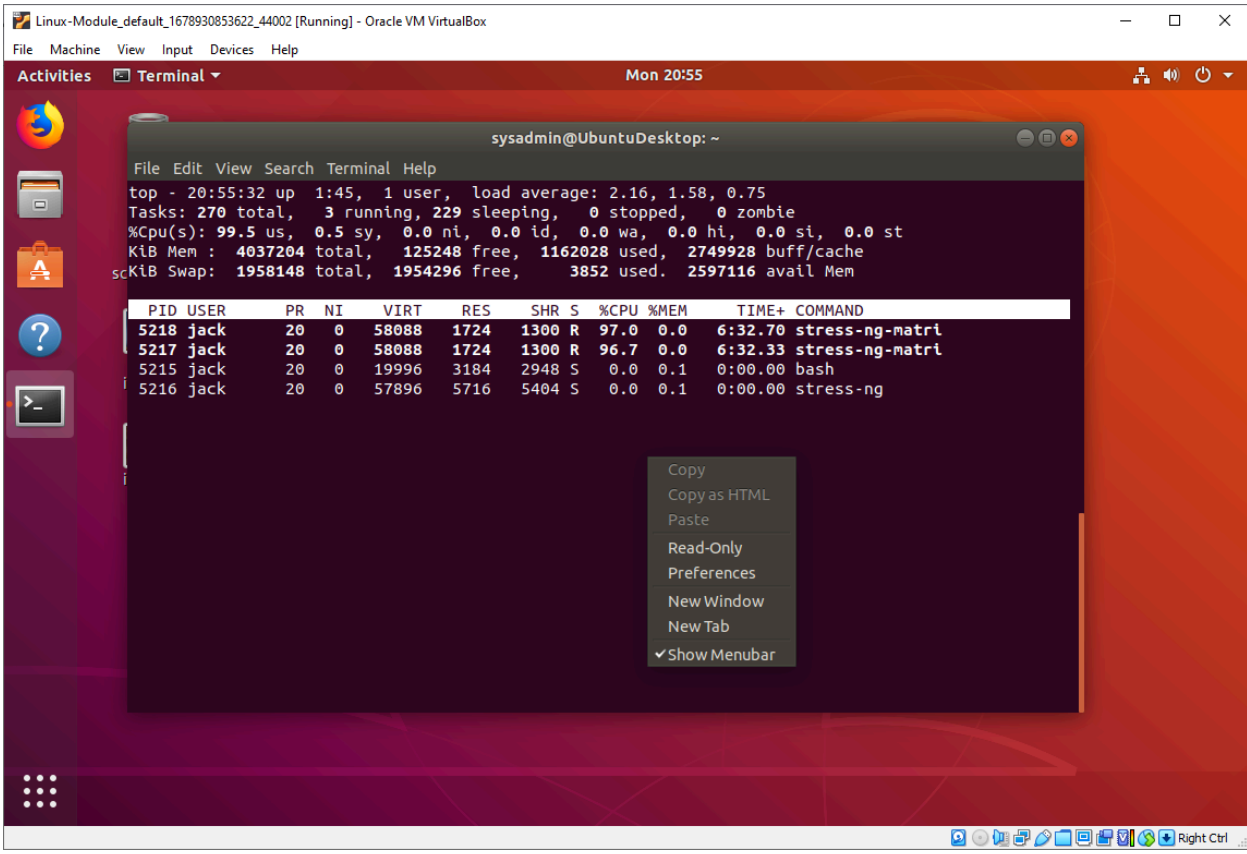
3. Search all running processes for a specific user.

    - Review all the processes started by the `root` or `sysadmin` user.





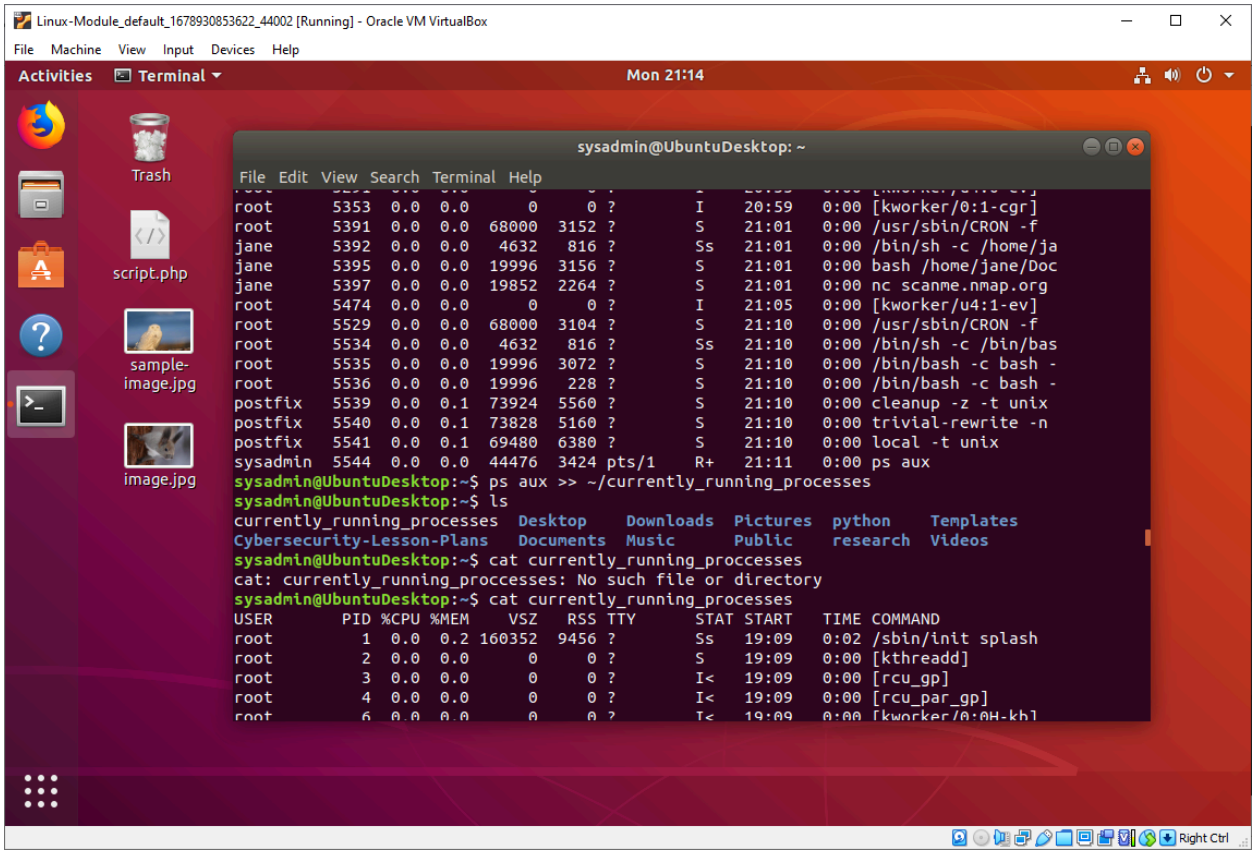
- Sort by other users on the system that may be of interest



4. **Hint**: In the previous exercise, you found a home folder for a user who should not be on this system. Is that user running processes?

Bonus

4. Next, take a static "snapshot" of all currently running processes, and save it to a file in your home directory with the name `currently_running_processes`.
    - Use the flag to list all processes that have a TTY terminal.
    - In the short list of output, do you notice any processes that seem suspicious?
5. Identify the ID of any suspicious process. Stop that process with the `kill` command.
6. `Kill` all processes launched by the user who started the command you just stopped.
    - Use Google and the man pages to identify a command and flag that will let you stop all processes owned by a specific user.


Linux-Module_default_1678930853622_44002 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mon 21:14
Trash
script.php
sample-image.jpg
image.jpg
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
root 5353 0.0 0.0 0 0 ? I 20:59 0:00 [kworker/0:1-cgr]
root 5391 0.0 0.0 68000 3152 ? S 21:01 0:00 /usr/sbin/CRON -f
jane 5392 0.0 0.0 4632 816 ? Ss 21:01 0:00 /bin/sh -c /home/ja
jane 5395 0.0 0.0 19996 3156 ? S 21:01 0:00 bash /home/jane/Doc
jane 5397 0.0 0.0 19852 2264 ? S 21:01 0:00 nc scanme.nmap.org
root 5474 0.0 0.0 0 0 ? I 21:05 0:00 [kworker/u4:1-ev]
root 5529 0.0 0.0 68000 3104 ? S 21:10 0:00 /usr/sbin/CRON -f
root 5534 0.0 0.0 4632 816 ? Ss 21:10 0:00 /bin/sh -c /bin/bas
root 5535 0.0 0.0 19996 3072 ? S 21:10 0:00 /bin/bash -c bash -
root 5536 0.0 0.0 19996 228 ? S 21:10 0:00 /bin/bash -c bash -
postfix 5539 0.0 0.1 73924 5560 ? S 21:10 0:00 cleanup -z -t unix
postfix 5540 0.0 0.1 73828 5160 ? S 21:10 0:00 trivial-rewrite -n
postfix 5541 0.0 0.1 69480 6380 ? S 21:10 0:00 local -t unix
sysadmin 5544 0.0 0.0 44476 3424 pts/1 R+ 21:11 0:00 ps aux
sysadmin@UbuntuDesktop:~$ ps aux >> ~/currently_running_processes
sysadmin@UbuntuDesktop:~$ ls
currently_running_processes Desktop Downloads Pictures python Templates
Cybersecurity-Lesson-Plans Documents Music Public research Videos
sysadmin@UbuntuDesktop:~$ cat currently_running_proccesses
cat: currently_running_proccesses: No such file or directory
sysadmin@UbuntuDesktop:~$ cat currently_running_processes
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.2 160352 9456 ? Ss 19:09 0:02 /sbin/init splash
root 2 0.0 0.0 0 0 ? S 19:09 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? I< 19:09 0:00 [rcu_gp]
root 4 0.0 0.0 0 0 ? I< 19:09 0:00 [rcu_par_gp]
Right Ctrl