# Managing Processes

Note

All labs rely on previous courseware and lab information.

## Scenario

After a week of working with Mrs. Y, you can already understand why she was hired. She is extremely goal oriented, works much better with building the team, and it seems as though she has a much more security focused mind set. She provided you with a set of overall goals that she wants you to complete for the week. With her security mindset, she wants to ensure that you are setting up the Linux machine to monitor certain processes.

## Objectives

In this lab, you will:

* Create and update Mrs. Y’s username, password, and validate proper permissions on appropriate folders
* Create a new log file for process listings
* Establish a repetitive task that runs your previous auditing commands once a day

## Exercise 1: Create User Account

As Mrs. Y approaches your desk, you prepare your morning update for her. It is Monday and you can already tell that she is in need of something. As soon as she gets to your desk, she stops you and says that she still doesn’t have an account and is unable to access the computer systems. Did this task somehow slip by without you realizing it? Either way, she has expressed that this will reflect on your performance evaluation. Reprioritize everything to get this done as soon as possible.

Helpful Hint

You may have to use **sudo** to complete this exercise if you are not root.

### TODO

1. Create account for Mrs. Y based on the following information.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| First Name | Last Name | userid | Job Role | Starting password |
| Y | Mandalou | ymandalou | IT Management | SuperSecret12@@ |

### Steps

1. Validate that you are in the home folder of your current user by typing **pwd** and pressing ENTER.

**cd /home**

1. Create a user account for the new IT Manager by typing

**sudo useradd ymandalou -p SuperSecret12@@**

and pressing ENTER.

1. Validate your work by typing

**sudo getent passwd | grep ymandalou** and pressing ENTER.

[labsuser@centos ~]$ sudo getent passwd | grep ymandalou

ymandalou:x:1022:1028::/home/ymandalou:/bin/bash

## Exercise 2: Create List of Processes

Now that the stress of the negative start to the week is over, you can finally chip away at that task list that was provided to you. In order to find potential problems, you have been instructed to create a log file from the **ps** command. That log file should be added to the **SharedFolders** in the company structure.

Helpful Hint

You may have to use **sudo** to complete this exercise if you are not root.

### TODO

1. Create a log file named **processes.csv** from **ps -aux** and omit any processes that contain root user or contain “[“or “]” in the COMMAND section.

### Steps

1. Validate that you are in the **/home/labsuser/companyA** folder by typing **pwd** and pressing ENTER.

**cd /home/labsuser/companyA**

1. View all processes running on the machine and filter out the word root by typing **sudo ps -aux | grep -v root | sudo tee** **SharedFolders/processes.csv**

and pressing ENTER.

1. Validate your work by typing

**cat** **SharedFolders/processes.csv**

and pressing ENTER.

[labsuser@centos companyA]$ sudo ps -aux | grep -v root | sudo tee SharedFolders/processes.csv

USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND

labsuser 99 0.0 0.0 150508 4244 ? S 01:03 0:00 sshd: labsuser@pts/0

labsuser 100 0.0 0.0 15264 3608 pts/0 Ss 01:03 0:00 -bash

## Exercise 3: Use History to Create a Cron Job

It’s the end of a long week; you haven’t had a long break in a while and you are ready for the weekend. The final task before you can get going is to create some sort of repetitive tasking that will run on specified intervals. You remember a few weeks ago you created a company audit csv file that was saved in the **.CEO** folder. Unfortunately, you no longer have access to the original file, but you do have some bash history.

Helpful Hint

You may have to use sudo to complete this exercise if you are not root.

### TODO

1. Search your bash history to find the command that outputs to the **CEO** folder or the **SharedFolders** for the company audit file.
2. Use the command that you found to create a daily **cron** job that saves a **filteredAudit.csv** file in the shared folder. Ensure that the data is stripped of all filenames and replaced with “#####” i.e. “#####.csv”.

### Steps

1. Validate that you are in **/home/labsuser/companyA**. Typing **pwd** and press ENTER.

**cd /home/labsuser/companyA**

1. Search through your history to look for the command used to create the **CompanyAudit.csv** by typing

**history | grep CompanyAudit** and pressing ENTER. Note that the command you should expect to find is **ls -la $(find .)**.

1. Using the command found in step 2, create a cron job that creates the audit file with **#####** to cover all csv files. Type

**sudo crontab -e**

and press ENTER to enter the default text editor.

1. Type

**SHELL=/bin/bash** on to the first line, followed by **PATH=/usr/bin:/bin:/usr/local/bin**

on the second line, and

**MAILTO=root** on the third.

1. For the last line, type **0 \* \* \* \* ls -la $(find .) | sed -e 's/.\*\.csv/#####.csv/g' >** **/home/YOURUSERNAME/companyA/SharedFolders/filteredAudit.csv** and use your text editor save method to save and exit.
2. Validate your work by typing **sudo crontab -l** and pressing ENTER. Inspect the crontab to ensure it matches the text exactly.

[labsuser@centos companyA]$ sudo crontab -l

SHELL=/bin/bash

PATH=/usr/bin:/bin:/usr/local/bin

MAILTO=root

0 \* \* \* \* ls -la $(find .) | sed -e 's/.\*\.csv/#####.csv/g' > /home/labsuser/companyA/SharedFolders/filteredAudit.csv

## STOP

You have successfully completed this lab.