# Cybersecurity

**Activity 3.1.3 Analyzing Processes**

Copy and paste screenshots and/or answer questions from the activity.

#4 Record at least two variations of ps that you can use “to see every process on the system using standard syntax.”

* Ps -e
* Ps -ef

#12

c. Answer the following questions using *your* output, rather than the image above.

1. What is the PID of your -bash?
   1. 3110
2. What is the PPID (the parent process ID) of the process that spawned (launched) your -bash process?
   1. 3109
3. What is the command that spawned your -bash process?
   1. -bash

#14 Notice the other users on the system. Other than you, alpha, what other users have processes running on the system?

Root, daemon, www-data, 101, statd, mysql, 103, 06

#18 Screenshot of the process

Text

Description automatically generated

#20 Why do you think a malicious user would run background processes as different users?

To disguise said malicious process and so it doesn’t disturb and programs lifecycle.

Text

Description automatically generated

#22 Screenshot of the output

A picture containing text

Description automatically generated

#29 Screenshot of the output

Graphical user interface, text, application

Description automatically generated

#30 In alpha’s shell, find and record the PID of beta’s bogus\_sw command.

3462

#31 Record bogus\_sw’s PPID—its parent process, which should be bash. Find the PPID in beta’s process tree and note the name of that parent process.

3265, -bash

#34 In Linux, which user type has the most priviledge?

root

What command do you use to switch to this user type?

Su - root

What does the command stand for?

Switch user

#36 Screenshot the results

Text

Description automatically generated

#37 Screenshot the results

Text

Description automatically generated with medium confidence

#38 What is the purpose of the kill command?

Graphical user interface, text

Description automatically generated

Some processes will not respond to the kill command. What type of processes and why won’t they respond.

VERY IMPORTANT INTERNAL PROCESSES

Conclusion:

#1 Consider a scenario where you are a security analyst for a Linux-based system. You see a user called gamma running a process called exploreallfiles that is not authorized on the system.

1. Describe the actions you should take to secure the system.

Look for any sussy processes in the terminal and kill them

1. If gamma is an employee of your company, what might you say to them?

Fire the shit out of them