Advance Cyber Security Serial No 09

Assignment 6

shreyyash

2020

April

Contents

1. Assignment 6: Linux Process Monitoring Using ps 3
   1. Introduction……………..…………………………. 3
   2. Answer 1..………….…….…………………………. 3
      1. Print Process Tree…………………………… 3
      2. View PID, PPID etc for a process…………………… 4
      3. Custom Output……………………………………….. 4
      4. Execution Time………………………………………. 5
      5. Top CPU and Memory Usage Process……………… 5
      6. PID Unresponsive process……………………………. 6
      7. Repetitive output for Process Monitoring……………. 7

List of figures

1.2.1 Figure 1: Process tree for keybase….………..…………..………… 3

1.2.2 Figure 2: View PID, PPID etc for a Process ……………………… 4

1.2.3 Figure 3: Custom Output view of a Process….………………. …… 4

1.2.4 Figure 4: Execution time of a Command………….…….....………. 5

1.2.5 Figure 5: Top running processes by Memory ………..…………… 5

1.2.5 Figure 6: Top running processes by CPU ………………………… 6

1.2.6 Figure 7: Searching for unresponsive processes…………………… 6

1.2.7 Figure 8: Watch command to check memory use..………………… 7

1.2.7 Figure 9: Output of the Watch command …………….…………… 7

CHAPTER 6

Assignment 6: Linux Process Monitoring Using *ps*

(Process Status)

* 1. Introduction

Ps command displays information about a selection of the active processes. This command gives three modes of using switches

UNIX options - Must be preceded by a dash

BSD options - Must not be used with dash

GNU long option - preceded by two dashes

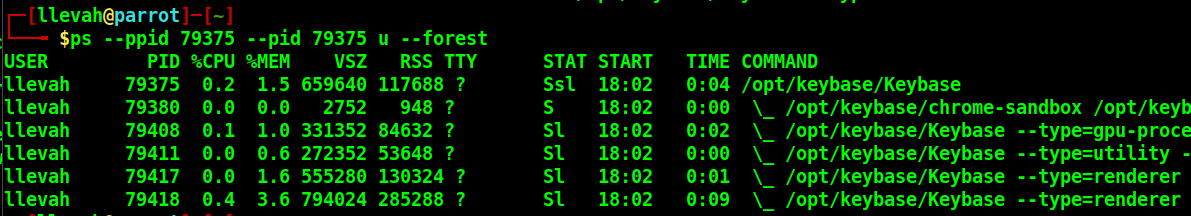
* 1. Answer 1

1.2.1 Print process tree

We have used the process keybase having pid 79375 and have printed keybase process and all process having parent pid (ppid) as 79395 and displayed them in process tree format.

Command and Usage

**ps --ppid 79375 --pid 79375 u --forest**



*Figure 1: Process tree for keybase*

Usage

**ps** - Process Status

**--ppid** - Parent process id

**--pid** - Process id

**u** - Display user oriented format

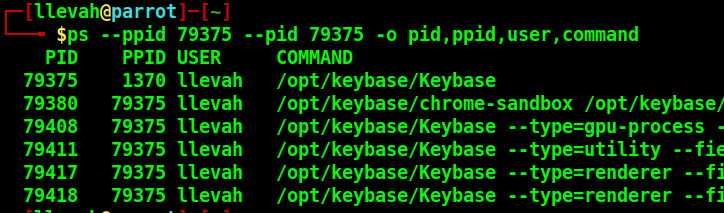
**--forest** - ASCII art process tree

1.2.2 View PID, PPID, Command and User Name of a process

We have used the same keybase process to display the required fields.

Command and Usage

**ps --ppid 79375 --ppid 79375 –o pid,ppid,user,command**



*Figure 2: View PID, PPID, Command and User Name of a Process*

Usage (less those covered previously)

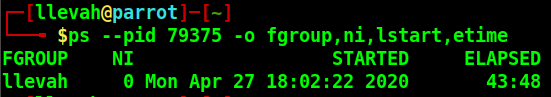
**-o -** User defined format, offers a way to specify individual output columns

1.2.3 Custom Output

Custom output showing file system group, nice value, start time and elapsed time for the keybase process.

Command and Usage

**ps --pid 79375 –o fgroup,ni,lstart,etime**



*Figure 3: Custom Output view of a Process*

Usage (less those covered previously)

**fgroup** - Filesystem access group id(privileges avail), textual group id(if avail), else decimal representation

**ni** - Nice value (user defined process priority), ranges from

-20(highest) to +19(lowest). Default value = 0.

**lstart** - Time the command started

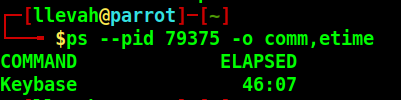
**etime** - Elapsed time since processed started in hh:mm:ss format

1.2.4 Execution Time

The execution time of keybase process was checked.

Command and Usage

**ps --pid 79375 –o comm,etime**



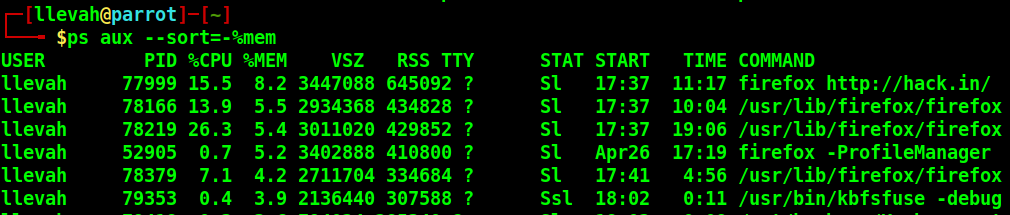
*Figure 4: Execution time of a Command*

1.2.5 Top CPU and Memory usage processes

The highest Memory and CPU usages of the linux system were checked.

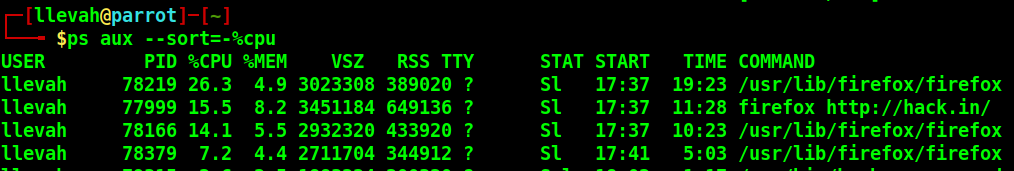
Command and Usage

**ps aux –-sort=-%mem**



*Figure 5: Top running processes by Memory*

**ps aux –sort=-%cpu**



*Figure 6: Top running processes by CPU*

Usage

**a** -Display processes of all users

**u** - User oriented format

**x** - Include processes started at boot and in background

**--sort=** - Sort as per following argument

**-%mem** - (-/+) (descending/ascending), memory sorting

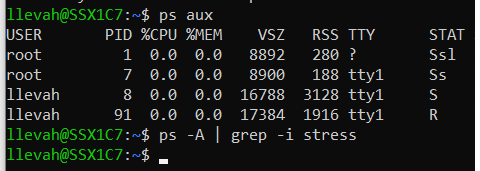
**-%cpu -** (-/+) (descending/ascending), CPU usage sorting

1.2.6 PID Unresponsive process

All running commands were checked for an unresponsive process, however none were found.

Command and Usage

**ps –A | grep –i stress**



*Figure 7: Searching for unresponsive processes*

1.2.7 Repetitive output for Process Monitoring

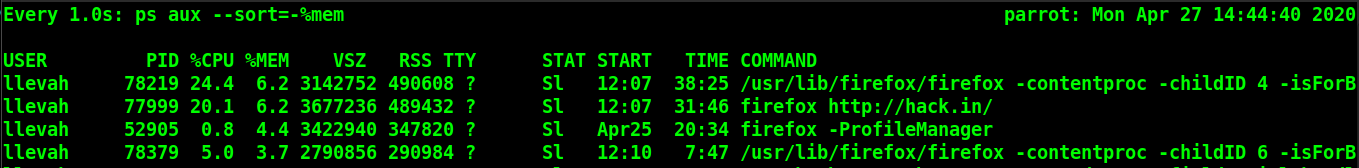
Process monitoring can be carried out with the help of watch command. This command gives the output repeatedly at a default value of 2s(can be user defined also).

Command and Usage

**watch –n 1 ps aux –sort=-%mem**



*Figure 8: Watch command to check memory use*



*Figure 9: Output of the Watch command*

Usage

Watch - Execute a program periodically, showing full screen output

-n - Time in which the command is to be repeated