<https://os.cybbh.io/public/os/latest/010_linux_process_validity/linproc_fg.html>

linux commands

top

htop

ps

ps -elf | head

ps -p 2

cd /proc

ls -shilat

ps -aux | head

ps --ppid 2 -lf | head

ps --ppid 2 -Nlf | head

ps --ppid 1 -lf | head

ps -elf --forest | tail

4.1 Process Ownership

grep UID /etc/login.defs

ls -l /usr/bin/passwd

5.2 Linux signals

kill -l

6 Foreground and Background process

6.3

Daemons-intentionally orphaned process in order to have a background process.

* All daemons are Orphans, but all orphans are not Daemons

systemctl status ssh.service

ps --ppid 1 -lf

6.4 Job Control

jobs’ - Display List of Jobs running in the background

‘fg’ or ‘bg’ - Push / Pull jobs to / from the foreground / background

‘kill %<job number>’ - Terminate the process by job number

‘[ctrl -z]’ or ‘kill -19’ - stop / suspend the job

‘kill -9 <PID>’ or ‘pkill -9 <process name>’

Stop Process = SIGSTOP(19) (pause signal, let’s you continue later, does not kill process)

End Process = SIGTERM(15) (termination signal, the right way, the application can intercept this signal and initiate shutdown tasks such as temp file cleanup)

Kill Process = SIGKILL(9) (kill signal, extreme, only use if SIGTERM doesn’t work, won’t initiate shutdown tasks)

6.5 Cron Jobs

etc/cron.d

* d is for daemon

‘crontab -u [user] file’ - sets users crontab file to the contents of listed file

‘crontab -l -u [user]’ - Displays user’s crontab contents

‘crontab -r -u [user]’ - Removes user’s crontab contents

‘crontab -e -u [user]’ - edits user’s crontab contents

system cron jobs:

/etc /crontab

user cron jobs:

/var/spool/cron/crontabs/

lsof -u garviel

lsof -p 2

ls -shilat /proc

ps -elf | grep sshd

↳gives links

How many child processes did SysV Init daemon spawn?

**ps --ppid 1 -lf | wc -l**

**23**

Linux Processes 3

10

Identify all of the arguments given to the ntpd daemon (service) using ps.

**ps aux | grep ntpd**

Linux Processes 4

10

What is the parent process to Bombadil’s Bash process?

**htop > F5 to see tree**

Linux Processes 5

Identify the file mapped to the fourth file descriptor (handle) of the cron process.

HINT: There might be multiple cron processes, but only one with the answer.

**sudo lsof | grep cron**

Linux Processes 6

Identify the permissions that cron has on the file identified in Processes 5.

HINT: Read the man page for lsof to understand permissions.

**sudo lsof -c cron > grep #PID**

**r,w**

Linux Processes 9

Locate the strange open port on the SysV system.

Identify the command line executable and its arguments

**htop > persistence process > pid 11713 >**

Linux Processes 9

Locate the strange open port on the SysV system.

Identify the command line executable and its arguments.

Flag format: /executable/path -arguments

**netstat -ano**

when talking about persistence look at:

/etc/inittab to start creating processes in groups called Run Levels.

cat /etc/inittab

**ANSWER: /bin/netcat -lp 9999**

Identify the file that contains udp connection information. Identify the process using port 123.

For the flag, enter:

Process name

File descriptor number for the udp socket

Its permissions as shown in lsof

Flag format: name,#,permission

**cat /proc/net/udp**

**sudo -l**

**man lsof**

**sudo lsof -p 12353**

**sudo lsof -p12353**

**sudo lsof | grep 12353**