**CS 345 Week 5 Homework**

Make sure you put your answers in numerical order! Answers are in yellow

1. Show how to start a job in the background and then bring it to the foreground. Also show how to send a job from the foreground to the background. (Run the commands and show the necessary output – no screenshots)

root@CS345:~# sleep 1000 &

[1] 724

root@CS345:~# jobs

[1]+ Running sleep 1000 &

root@CS345:~# fg %1

sleep 1000

root@CS345:~# sleep 1000

^Z

[1]+ Stopped sleep 1000

root@CS345:~# jobs

[1]+ Stopped sleep 1000

root@CS345:~#

1. Explain the difference between a block device and a character device. Show the output from ls -l that gives an example of each type of device (run the command(s) and show the necessary output – no screenshots). Comment on the advantages of one device type over the other. Provide examples of physical peripherals that are block devices and some that are character devices.

A block device handles data in large chunks, whereas character devices handles data one character at a time. Block devices examples are hard disk, flash drives, etc. Character devices are some printers, tape drives, serial ports. Block devices are helpful for hard digs where large data transfer is required, character devices are useful for small devices requiring small amount of data transfer.

root@CS345:~# ls -l /dev/sda

brw-rw---- 1 root disk 8, 0 Jun 13 21:18 /dev/sda

root@CS345:~# ls -l /dev/ttyS0

crw-rw---- 1 root dialout 4, 64 Jun 13 21:18 /dev/ttyS0

root@CS345:~#

1. Explain the difference between a symbolic link and a hard link.

Symbolic links can be made to both files and directories, while hard links can only be made between files. Symbolic links also can be made between different file systems, whereas hard links cannot. Hard links also share the inode number, and symbolic links do not.

1. Explain the purpose of the fsck utility. Comment on any special requirements needed to use the utility.

The purpose of the fsck utility is to check the integrity of a Unix/Linux filesystem. fsck stands for file system check. It is automatically run every time the OS is booted, and it checks all partitions indicated to be scanned for issues.

Fsck requires the filesystem to be unmounted. If the user plans to defrag the root partition, you need to boot from a media device besides the one you want to defrag in order to remain unmounted.

1. Explain the kill signals values of –1 (-SIGHUP), -9 (-SIGKILL) and –15 (SIGTERM). Why would we use one signal over the others?

SIGKILL uses the UNIX kernel to stop the process. SIGTERM is a generic signal used for program termination. This signal can be blocked, handled, or ignored. You should always try and use SIGTERM first because if the program is able to respond to SIGTERM it can shutdown orderly. SIGHUP can be used to tell a daemon to reread its configuration file. If you changed a configuration file and want a process to start over reading the modified file, you would use SIGHUP.

1. Start a process and show how to change its default nice level to +5 from the command line (Run the commands and show the necessary output – no screenshots). Comment on what +5 means.

root@CS345:~# sleep 1000

^C

root@CS345:~# ps -l

F S UID PID PPID C PRI NI ADDR SZ WCHAN TTY TIME CMD

4 S 0 607 587 0 80 0 - 2013 do\_wai pts/0 00:00:00 bash

0 T 0 725 607 0 80 0 - 1386 do\_sig pts/0 00:00:00 sleep

4 R 0 733 607 0 80 0 - 2213 - pts/0 00:00:00 ps

root@CS345:~# renice +5 725

725 (process ID) old priority 0, new priority 5

root@CS345:~# ps -l

F S UID PID PPID C PRI NI ADDR SZ WCHAN TTY TIME CMD

4 S 0 607 587 0 80 0 - 2013 do\_wai pts/0 00:00:00 bash

0 T 0 725 607 0 85 5 - 1386 do\_sig pts/0 00:00:00 sleep

4 R 0 735 607 0 80 0 - 2213 - pts/0 00:00:00 ps

+5 means that it will be “nicer” to other process allowing them to have higher CPU process than the sleep process (or the current process selected)

1. Now that you have seen everything that exists under the /proc directory, explain why this is mounted as a special filesystem. Comment on whether or not /proc physically exists on disk.

It is mounted to obtain information on the hardware of the system as well as processes.

/proc is a window into the kernel where we can obtain info about any process currently running and the hardware of the system. It is not physically existing, it is just a window to kernel data.

1. Perform a vmstat and comment on the procs and cpu output produced. (Run the command and show the necessary output – no screenshots)

root@CS345:/# vmstat

procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----

r b swpd free buff cache si so bi bo in cs us sy id wa st

1 0 0 741616 14892 166452 0 0 25 3 51 80 0 0 100 0 0

root@CS345:/#

r - number of processes waiting for run time -1

b - number of uninterruptible processes - 0

us: user time % (nonkernel) - 0

sy: system time % (kernel) - 0

id: idle time % - 100

wa: waiting for I/O time % - 0

st: stolen from VM (only on virtual machines) - 0

1. Explain the purpose of a quota and when you would implement them. Discuss both hard disk space quotas and process limits. What are the appropriate commands to implement them?

Quotas are convenient ways for sysadmins to limit the amount of space users are allowed to use up. You would implement them whenever you need restrictions for the data/space, or if you want to create limits. Hard disk space quotas are limits when if an account hits this limit, any data that is attempted to be written will be denied. Process limits are limiting the user’s core file size, maximum CPU time, data segment size, and number of files allowed to be opened and more.

ulimit -Hu 5000

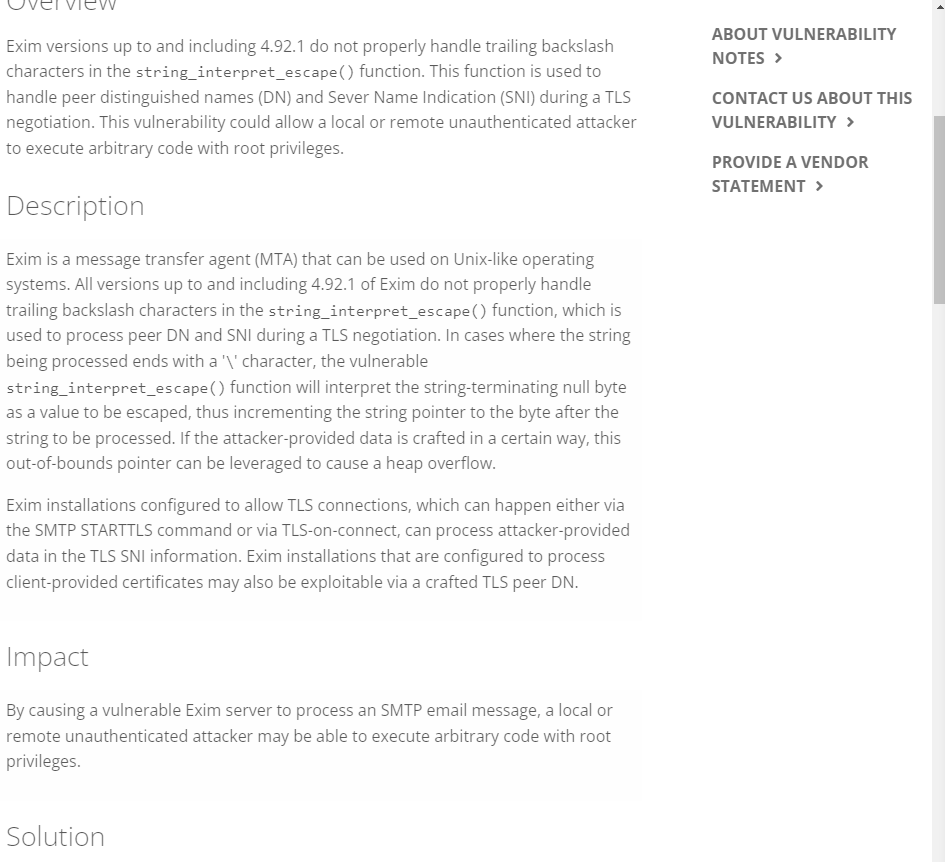
apt install quota, quotacheck -ugm /, edquota -u reguser

1. Show how to configure the syslogd messages such that all messages of exact info are directed to the file /var/log/info-log.

In order to configure syslogd messages the user must edit the syslog.conf file. The user can specify where they want messages of exact info to go in here.

1. Part of a good disaster planning strategy is to read up on security bulletins. Visit CERT (Computer Emergency Response Team at Carnegie Mellon University) on the Internet and print out one page related to a UNIX system vulnerability.

<https://www.kb.cert.org/vuls/id/672565>



1. Attempt to locate a UNIX script which attempts to gain root access. Print this script out. **Be careful:** you might end up at a hacker/cracker site where there are viruses/spyware and possibly pornography. If you object to seeing this stuff, just note that on your answer and don’t go looking. I will warn you however, that if you are a sysadmin, you will undoubtedly end up on those types of sites trying to learn about the newest risks so that you can safeguard your system.

I do not want to see that type of stuff.

1. Explain the difference between the UNIX/old school klogd daemon and the syslogd daemon. This is an important distinction since modern distros now use a single daemon…

Klogd watches for messages coming from the kernel and writes them to message files, syslogd watches for syslog messages coming from any other program and will write that message into whatever file has been specified in the syslog.conf file. These messages can be generated from any program calling the standard syslog library function. Both of these write messages into files.

1. List 3 items that you believe are imperative in a disaster recovery plan for any organization.

I think that the three most important things in a disaster recovery plan are identifying sensitive data, identifying roles, and disaster recovery procedures. Identifying sensitive data is important because it could contain personal information, credit card data, and much more which is leaked would lead to huge problems. Having disaster recovery procedures like documented procedures with clear steps, simple language, and how to ensure a successful recovery. Identifying roles is important because you can assign people to lead/manage certain situations and aid the recovery process.

1. Show some examples of getting hardware related information from what’s available in the /proc directory. I am interested in seeing things like information on the CPU, interrupts, ports and so forth… Explain to me what we’re looking at in the files that you display… (Run the commands and show the necessary output – no screenshots)

rroot@CS345:/# cat /proc/cpuinfo

-shows what type of processor your system is running including number of CPU’s present

processor : 0

vendor\_id : AuthenticAMD

cpu family : 23

model : 113

model name : AMD Ryzen 7 3700X 8-Core Processor

stepping : 0

microcode : 0x6000626

cpu MHz : 3593.250

cache size : 512 KB

physical id : 0

siblings : 1

core id : 0

cpu cores : 1

apicid : 0

root@CS345:/# cat /proc/interrupts

-Provides details of interrupts generated in the system.

CPU0

0: 29 IO-APIC 2-edge timer

1: 29 IO-APIC 1-edge i8042

8: 0 IO-APIC 8-edge rtc0

9: 0 IO-APIC 9-fasteoi acpi

.

.

.

NPI: 0 Nested posted-interrupt event

PIW: 0 Posted-interrupt wakeup event

root@CS345:/# cat /proc/ioports

-Provides list of currently registered port regions used for input or output communications with a device

0000-0cf7 : PCI Bus 0000:00

0000-001f : dma1

0020-0021 : pic1

0040-0043 : timer0

0050-0053 : timer1

.

.

.

d258-d25b : ahci

d260-d26f : 0000:00:0d.0

d260-d26f : ahci