1. Semester and Year	: 2012 FALL
2. Course Number	: CS-227
3. Course Title	: Linux & System Software
4. Work Number	: LA-11
5. Work Name	: Lab 11
6. Work Version	: Version1
7. Long Date	: Sunday, 11, November, 2012
8. Author(s) Name(s)	: Jake Waffle

Task 7.2

This section is all about security restrictions for users. And this is important when having a public computer with unknown users, because then the user's damage can be limited.

Disk Quotas

Disk quotas are meant to limit the disk use for some specified users (Smith, pages 309, 311.) The kernel and various user-space utilities are required to support the disk quota system (Smith, 310.) To obtain the various utilities you must install the “quota” package. This package will contain utilities as well as configuration files and SysV startup scripts. Then the partitions of the disk that are needed to be limited for use will need to be specified in the /etc/fstab file. This can be done by adding the usrquota (for user quotas) and grpquota (for group quotas) keywords to the entries of partitions within the /etc/fstab file. Then after confirming that the SysV startup scripts are ran on boot up the systems can be activated by rebooting the computer.

Now to edit a quota for a particular user you just need to use edquota (Smith, 311.) This program opens Vi with a temporary configuration file and on exit the quota is created using the configuration file. And within the configuration file you can edit the soft and hard limits for the disk blocks and inodes that are in use. It seems like the units for the limits are bytes. From there on the book describes some quota commands that are commonly used with cron-jobs (Smith, pg 312.) But the quota commands however do not give off a response when called.

Setting CPU and Memory Limits

The description for PAM seems to do all of what the quota system can do and more. PAM allows limits on the amount of times a user can log onto the computer, the CPU's time consumption and the memory use (Smith, pg 312.) The Ubuntu version I have already has pam_limits on it, but its /etc/security/limits.conf file is completely blank (this file is used in configuring pam_limits.)

The limits.conf file takes in entries of the form “<domain> <type> <item> <value>” to specify how the limits are setup. Where the domain can be a user (@userName,) a group (@groupName) or a wild card that represents all of the users. The type specifies whether or not the limit is a hard or soft one. Hard limits cannot ever be exceeded and soft limits may temporarily be exceeded. Both limit types can also be specified with a hyphen “-”, but I'm not sure what that actually will do. The item field is where we actually specify what is going to be limited (because PAM can deal with a plethora of stuff.) And the value field denotes the actual limit that is to be done to the item specified. The actual uses of the PAM utility can be to limit the CPU time (cpu item) and the memory used for each of the data (data item,) stack (stack item) and RSS (rss item) memory.

To limit the number of logins for a user the maxlogins item can be used in the limits.conf file and there are many other items that the book doesn't go into. I found these items within the limits.conf file itself, as there is documentation for the available options for the entries. So to limit the logins for a group of users with no exceptions to five times, we could use the following entry:

```
@groupName hard maxlogins 5
```

References

-Roderick W. Smith. linux administrator StreetSmarts. Induanapolis, Indiana: Wiley Publishing, Inc, 2007