# Week 5 Notes

## Review

- The HW was a preview of the first phase of the final project
- You should know what a daemon and a web server are

## Logs, logs, and more logs...

- Understanding what is in logs helps realize what is up with the operating system: is somebody trying to compromise my server, is a driver crashing my computer, etc
- Can edit file **/etc/syslogd.conf** where logs should go
- **/var/adm/messages**: a catchall file for lots of messages from the Unix kernel and other logging applications like syslogd. Also sometimes used to store miscellaneous log files, including those created by syslog for messages not written to **/usr/adm/messages** or the console.
- **var/adm/lastlog**: stores information about a logged on user. File is in binary and is used by **last**
- **/var/adm/sulog**: records all attempts by users to execute su.
- Unix makes backup files, numbering them sequentially higher
- Files labeled o.logname usually indicate an overflow log. If a log file overflows, all auditing put there stops.
- **/var/adm/utmpx** - keeps information on who is currenly logged in. File used by **who** command.
- **/var/adm/wtmpx** - keeps information on who logs in/out and of when the machine reboots
- More information on HTTP Logs can be found here:
  http://httpd.apache.org/docs/1.3/logs.html

## Log Rotation

- When running a server, even one at home, the size of logs would become very large. Since the standard is keeping the most recent one without any additional numbers at the end, all of the logs need to be rotated down when the current ones becomes too large or the time is set to rotate it.

- **syslogd** daemon accomplishes this

### Cron Jobs

- It is an automated process which operates at preset intervals. For example, clearing out your accumulated spam at the end of the week. You can also use a daemon to do this, but it would be harder to write and would have to constantly run and take up your system's resrouces.
- Accomplished through **crontab** command, which uses **crond** daemon which constantly runs and check if its time to execute your process
- **crontab -l** lists your current crons
- **crontab -e** edits the file containing your crons
- **contab -r** deletes all of your cron jobs