**Su** /sbin/auditctl -w /directory -p rwxa

/sbin/ausearch -f /dir > file

Daemon constantly running in background.

Every night –

1. Change permissions of live site(Read+Write) + intranet(Read only) to read only (DONE)
2. Backup live site to separate directory (DONE)
3. On completion of live site backup begin transfer from intranet to live site
4. Only transfer files edited by users
5. On completion of transfer change permissions back – livesite(Read) + intranet(read + write) (DONE)

Always –

1. Watching intranet folder for edits made using auditd
2. Maintain list of file updates based on this info
3. Be able to communicate with Daemon to force backup (DONE)
4. Live always read.
5. Intranet unlocked

Extra add ons

1. Boot daemon (and auditctl?) on start up - /etc/init.d/skeleton
2. Singleton Pattern
3. Makefile
4. Error logging and reporting
5. Message Queue for completion of tasks

Ausearch run as sudo

Msg queue halts daemon

**Files:**

allowAccess.c – change to read+write

denyAccess.c – change to read

backup.c -copy livesite to backup location

transfer.c -call ausearch

-parse results for time->CURRENT\_DATE

-get edited filenames

-copy filenames from intranet to live

daemon.c - count to time == 0

-call allowAccess.c

-call backup.c

-call transfer.c

-call denyAccess.c

-msgQueue == “backup”

-call backup.c

**Questions for Jonathan:**

1. Can you call a different file from a Daemon? I know calling from a regular file is fine because you can use a header file, but aren’t all file descriptors closed in a Daemon?
2. Ausearch writes to a file. Do we then parse that file to know which files have been edited on our current day in order to know which files to transfer?
3. Is error logging and reporting the same details as what’s being recorded in our message queue (success/failure of tasks)?

4)Auditctl boot on startup with daemon? - chkconfig auditd on (Doesn’t work – Debian issue?)