Ubuntu 12.04 Checklist

* Check shadow hash storage security
  + /etc/pam.d/common-password
  + /etc/login.defs
* Change passwords
  + sudo passwd username
* Configure ssh daemon
  + sudo vi /etc/ssh/sshd\_config
  + change the line “PubkeyAuthentication yes” to “PubkeyAuthentication no”
    - gets rid of ssh public key authentication
  + change the line “PermitRootLogin yes” to “PermitRootLogin no”
  + set up the script to run on client login - see the other sheet “setting a batch script … when they log in via ssh”
* Check auth.log - try and see if someone has logged in already
  + lastlog
  + /var/log/auth.log
* Check logged on users, and kill anyone that isn’t you
  + run “who” : it will show you either the tty or pts/# of all people that are logged on
  + determine the PID of the remote shell: either “ps -fu <username>” or ps -aux | grep “<pts or tty value>”
  + Now that you know the PID, run “sudo kill -HUP <PID>”
* Once you get inotify tools, set up monitoring on:
  + /etc/passwd
  + /etc/ssh/sshd\_config
  + /etc/sudoers
  + /etc/network/interfaces
* Firewall
  + See UFW document
* Check startup programs/cron jobs
  + bootchart - audit of boot programs in all locations
  + /etc/init upstart config’s
  + /var/spool/cron/crontabs
  + /etc/xdg/autostart/
* Start working on AppArmor
* Backup /etc to another directory
  + cp -a /etc <backup\_location>