# Wicked Quick Unix Forensics

**Type of Systems**: Unix (Ubuntu, CentOS, FreeBSD)
**Complete Goal:** A quick scan for glaring security issues that you can do when you log on to a box for the first time or periodically throughout the competition. This should take less than 5 minutes.
**Steps**: Get a notebook to keep notes on your findings as you go through the investigation; being able to reference what you found in the past will be very helpful. Be sure to record the time of any findings, and spread the word to your section leader or team captain of any significant malicious activity.

Note that most Unix systems use UTC time, which is 5 hours ahead of EST.

1. Who has been on the system?
    a. Who has an active shell/console session?
        i. `> w`
    b. Who has recently logged in?
        i. `> last`
    c. Check auth logs
        i. (Ubuntu) > sudo tail /var/log/auth.log -n 50 | less
        ii.
2. What has recently been done on the system?
    a. Look at history files, ".bash_history", ".mysql_history", and similar. If there is interesting activity, save a copy of these files somewhere else.
    b. Check the status of packages
        i. (Ubuntu) > apt install debsums && debsums_init  && debsums -ca
        ii. (CentOS) > rpm -Va
        iii. (FreeBSD) > pkg check -a
        iv. See Linux Forensics bits for more
        v. > ls -lt /etc
3. What services are running on the system?
    a. Check listening ports
        i. (Linux) `> sudo ss -tulpn`
        ii. (FreeBSD) `> sockstat -l46`
    b. Check active daemons
        i. (Linux) `> systemctl`
        ii. (FreeBSD) `> service -e`

   c. Check crontab
      i. (Linux) `> systemctl list-timers --all`
      ii. `> crontab -u <user> -l`
      iii. Check `/etc` for crontab config files
4. What processes and connections exist on the system?
   a. Check outgoing connections
      i. (Ubuntu) `> apt install lsof && lsof -nPi`
   b. Take a brief look at all processes
5. Who has access to the system?
   a. Check out the users
      i. `> less /etc/passwd`
   b. Check out ssh authorized_keys. Each user has one at ~/.ssh/authorized_keys. Don't forget to check root!
   c. Do checks for any other services that allow for remote access, like VNC

**Appendix:**

- More on mode and permissions: http://man.openbsd.org/ls#The_Long_Format
- Using chmod commands: https://en.wikipedia.org/wiki/Chmod#Octal_modes
- More intrusion detection: https://marksforensicblog.wordpress.com/2011/11/29/intrusion-discovery-cheat-sheet-linux/