Lecture 1

- This course is about two things: (1) being a sysadmin, and (2) linux.

- Goals:
    a. To let you know what it is like to be a system administration, and give some tips on how to be a good one.
    b. To teach you linux and how to use it as a sysadmin.
    c. To practice your technical communication skills.

- Disclaimer:
    o I'm new.
        ▪ I have not been a sysadmin. (I'm learning though.)
        ▪ I use Linux. But my two machines runs Windows.
            □ Don't expect me to be a guru.
    o This course is new.
        ▪ It's not clear the direction I'm taking it is the best one.
        ▪ Assignments and quizzes are not polished. They are prepared on a day-to-day basis.
        ▪ Syllabus will not be stable. I'll add more material as I learn new things.
    o Implications
        ▪ I need your feedback.
        ▪ If you don't like something, negotiate it with me.

- Administrivia
    o Four homework assignments (60%)
        i. An unattended Ubuntu installation disk --- 10%
        ii. Using-Linux-to-do-various-things hands-on --- 10%
        iii. A tutorial on how to use a linux program --- 10%
        iv. A survey of your organization's system --- 20%
    o Two quizzes
        ▪ 15% and 1.5 hour long each.
        ▪ In class.
    o Final exam
        ▪ 20% and 2 hour long.
    o Please sign up.
        ▪ Name.
        ▪ Email address.
    o Office hours
        ▪ Monday, Wednesday 10-12
        ▪ Or by appointment.
    o You can reach me via:
        ▪ pramook@gmail.com
        ▪ Cell phone: 08-5453-5857
        ▪ My trouble ticket system that I have yet to set up.
    o Detailed syllabus will be available next week. (And will be subjected to change without prior notice.)
    o Textbook
        ▪ Limoncelli, Hogan, and Chalup. *The Practice of System and Network Administration.*
        ▪ First edition is available in the department's library.
        ▪ Second edition is on its way here. Wait 2-3 weeks.

- What's a system administrator (sysadmin, SA)?
    o Someone who manage a system for someone else. In our case, a computer system.
    o What do sysadmins:
        ▪ They install and maintain:

- □ Workstations
- □ Servers
- □ Data centers
- □ Network
- □ Services
  - ◆ Email
  - ◆ Software depot
  - ◆ Printing
  - ◆ Data storage
  - ◆ Backups
  - ◆ Various web service
- ▪ They deal with:
  - □ Outages and disaster recovery
  - □ Questions and problems from customers
- ▪ They engineer:
  - □ How to organize a computer infrastructure.
  - □ How a site would grow.
  - □ How to move a computer infrastructure from one place to another
  - □ The security policy of a site
  - □ Performance tuning
- ▪ They educate:
  - □ Customers
  - □ Technical support staffs
- ○ In short, sysadmins:
  - ▪ Keep things running
  - ▪ Deal with changes (outages, merger and acquisitions, and moving)
- ○ Sysadmin do not develop new computer system or software.
- ○ Why do they matter?
  - ▪ Computer systems are pervasive nowadays. Companies and organizations become more dependent on computer systems. What if the wireless is down now?
  - ▪ People have high expectations. Customers and stockholders do not forgive. A single outage can make your company lose million dollars and bring the stock down.
  - ▪ Technology keeps changing. Someone has to figure out and manage how to update what your organization is using.

- You and your boss. (See Limoncelli Chapter 1)
  - ○ What Should SAs Expect from Their Managers?
    - ▪ Clearly communicated priorities
    - ▪ Enough budget to meet goals
    - ▪ Feedback that is timely and specific
    - ▪ Permission to speak freely in private in exchange for using decorum in public
  - ○ What Should SA Managers Expect from Their SAs?
    - ▪ To do their jobs
    - ▪ To treat customers well
    - ▪ To get things done on time, under budget
    - ▪ To learn from mistakes
    - ▪ To ask for help
    - ▪ To give pessimistic time estimates for requested projects
    - ▪ To set honest status of milestones as projects progress
    - ▪ To participate in budget planning
    - ▪ To have high ethical standards
    - ▪ To set at least one long vacation per year
    - ▪ To keep on top of technology changes
  - ○ What Should SA Managers Provide to Their Boss?
    - ▪ Access to monitoring and reports so that the boss can update himself or herself on status at will
    - ▪ Budget information in a timely manner
    - ▪ Pessimistic time estimates for requested projects

- - Honest status of milestones as projects progress
    - A reasonable amount of stability

- Two non-technical issues I want to talk about.
  - Documentation
  - Ethics

- Documentation
  - What?
    - Keep record of where things are.
    - Explain how to do things
    - Make useful information available
  - I know it's hard. I don't like documentation either, but it can help you a lot.
  - Why document?
    - Let your team improve your team's skills.
    - Prevent you from being trapped in your position.
    - Make your job easier, really.
    - Free up mental space. Your brain has better used than remembering mindless stuffs.
  - Common types of documetations
    - HOWTOs
      - Environment specific.
      - Oriented to achieving some goals.
      - Solve particular problem rather than teach a concept.
    - Frequently Asked Questions
      - A list of questions that get asked over and over again with answers.
      - Convenient place, but hard to navigate.
      - Evolving over time.
      - Mine your trouble ticket system to create one.
    - Reference Lists
      - Not accessed very often
      - Serve a specific purpose.
      - Examples
        - Vendors and their contact info.
        - Serial numbers of hardware.
        - License keys and number of users of a particular software.
        - Compatibility list.
        - Employee directory.
        - Local restaurants.
        - Whom to contact under which situations.
    - Procedures
      - Useful when your organization is under ISO or other standards.
      - Useful also when dealing with law enforcements.
    - Checklists
      - Documentation such that each line or paragraph contains only one step.
      - Why?
        - Reduce mistakes
        - Improve accountability.
      - Examples
        - Task to be done for each new hire.
        - Task to be done for employee termination.
        - Installation tasks.
        - How to archive data:
          - Off-site storage.
          - When data is required by law enforcement.
        - How to secure an OS before deploying.
  - Principle: Being selfish. Use it to make your job easier.
    - Questions you are asked over and over.
    - Tasks that you don't like to do.

- □ You can use the list of these tasks as job description for a new hire.
  - ▪ Things that only you can do.
  - ▪ Mistakes you have to fix, but could have been prevent if you have a cheklist.
- ○ Criteria for things to document.
  - ▪ (1) Complicated and (2) unpleasant
  - ▪ Applies to both the process itself and its consequences.
  - ▪ Examples
    - □ Setting up a new employee's computer and account.
    - □ Process that has lots of steps, and their orders matter.
- ○ Template:
  - ▪ Title
  - ▪ Metadata
    - □ Author
    - □ Contact information
    - □ Revision date
    - □ History
  - ▪ What
    - □ A sentence or two describing the content.
  - ▪ How
    - □ The steps to accomplish the goal.
    - □ You may also add a why for a step that seems complicated.
- ○ Documentation QA
  - ▪ Check for:
    - □ Typos
    - □ Skipped steps
  - ▪ Have some person follow the instructions you wrote. Observe him. If he gets stuck, you know where to fix.
  - ▪ Create a "quick guide" of the process once you know your documentation works.
- ○ Gathering materials
  - ▪ Saving screenshots
    - □ It's a cross-check for correctness. Other people can compare their screens with your screenshots.
  - ▪ Capturing command lines
    - □ Unix "script" command
      - ◆ Logs everything a terminal output.
      - ◆ Output can have weird characters.
    - □ Unix "history" command
      - ◆ Only the last commands you typed.
    - □ Cut and paste works just find too.
  - ▪ Emails
    - □ Not as easily sharable.
    - □ You may have to combine several messages into a coherent documentation.
    - □ Sort your email by conversation or threads to make life easier.
      - ◆ Gmail can do that for you.
  - ▪ Ticket system
    - □ Some ticket system has "knowledge base" features.
    - □ You can also customize your ticket system so that you can tag items as "knowledge base."
    - □ Or create a ticket "this item needs to be put in the documetation repository."
- ○ Document repositories
  - ▪ A directory in a shared server.
    - □ Items are text files.
    - □ Should maintain an intuitive subdirectory structures.
    - □ Adding source control can be a boon.
      - ◆ Subversion is great.
  - ▪ Wiki
    - □ Web-based publishing and collaboration tool that everyone (who is allowed to edit) can edit.

- □ Low "barrier to entry"
- □ Low maintenance cost and effort. Documentation just miraculously get updated and evolve.
- □ Can create placeholders for topics and fill them in as you go.
- □ http://www.wikimatrix.org to compare popular wiki.
- □ I and the theory lab use MediaWiki. Other people like DokuWiki.
- Your documentation repository should have a search facility.
  - □ For just directory in a shared server, ls and grep should be enough.
  - □ Should use wiki that has built-in search facility. (MediaWiki is great for this.)
- ○ Getting people to use your documentation system.
  - Have more than one way to access it.
    - □ RSS Feed
    - □ People may subscribe to "updates" mailing list.
    - □ Frequently updated "Recent Changes" sections.
  - If someone handles documentation management:
    - □ Make sure he knows that he's an "enabler" rather than a "gatekeeper."
    - □ Only move. Don't delete.
    - □ Don't worry about structure on the outset.
    - □ Refactor the repository as it go.
  - Develop a "culture of respect."
    - □ Don't feel that you need to be approved before posting documentation.
    - □ Don't hesitate to edit other people's work if you think the edit should be done.
    - □ Middle ground: Have a comment page that anyone can edit, and promote the content their to the real page after discussion.
    - □ Different organizations have different cultures. Find yours.
- ○ External Links
  - The IntraWeb is your friend.
    - □ Tutorials
    - □ Blog posts
    - □ Wikipedia
  - Make sure you use **anonymizing redirection service**.
    - □ You can unknowingly reveal your company secrets!
    - □ Privacy!

- Ethics (จรรยาบรรณ)
  - ○ A principle of conduct that govern a group of people.
    - As a sysadmin, what you should do, what you should not do, and what should you strive for.
    - Not morals (คุณธรรม) = what is right and what is wrong.
  - ○ Why?
    - Sysadmins are normally superusers.
    - You have access to confidential information.
    - With great power comes great responsibility.
  - ○ Professional code of conduct.
    - SAGE and LOPSA has a great guideline, and I quote.
  - ○ Informed Consent
    - Medical ethics version
      - □ Educate patient first.
        - ◆ All treatment options.
        - ◆ Benefits, drawbacks, and probability of success of each.
        - ◆ In the way, that the person is competent to understand.
      - □ Patient decides by himself which option, if one at all, to take.
      - □ No coercion.
    - Sysadmin version
      - □ People should understand the rules.
      - □ What is going to be done should be clearly written in the Service Level Agreement (SLA).
        - ◆ What hours are the maintenance going to take place?

- ◆ How sysadmin will operate in various circumstances.
  - □ Tell people what you are going to do, and what will happen to them.
- ○ Customer Usage Guidelines
  - ▪ Basically, what you can use your organization's computers for.
  - ▪ How to report harassment communications, and how the report is going to be processed.
  - ▪ Different organizations have different philosophy.
    - □ Academic institution wants to maintain freedom and privacy.
    - □ Financial companies need to keep secret and preserve resource.
    - □ Government organizations needs to be accountable.
- ○ Privileges-Access Code of Conduct
  - ▪ Use only for work-related issues.
  - ▪ Mistakes can happen. So we should be minimize its damage. So, backup as you go.
  - ▪ There should be written procedure on what to do if privileged users gains information that should not be made public.
    - □ If you accidentally see someone's email?
      - ◆ And found that he's doing something illegal with the network?
      - ◆ And found that there's going to be a business deal with company X?
  - ▪ Specify consequences of making mistakes
    - □ If it's honest, there should be no penalty.
    - □ But mistakes should be report as soon as possible to minimize damage.
  - ▪ Privileged users should sign a statement that they acknowledge and will abide by the code of conduct.
  - ▪ Track who has privileged access. Remove the access when the person leave the company.
- ○ Working with Law Enforcement
  - ▪ Need clear policy.
    - □ What to do if you get contacted.
    - □ What to do to contact them.
  - ▪ You MUST identify the person claiming to be from law enforcement. Don't say that you're a sysadmin before doing so.
    - □ Ask for the person's contact information, and call back later.
    - □ Forward the contact to your boss or the legal department.
    - □ This is done to prevent social engineering.
  - ▪ Be careful on what you say on the phone.
  - ▪ Always shred documents that contain sensitive information.
  - ▪ Don't take situations into your own hands.
  - ▪ Follow requests of corporate security.
- ○ Setting expectations
  - ▪ Inform your customers how secure their emails or other means of communication are.
  - ▪ Constantly remind them that their communications are subjected to monitoring.
    - □ Every time they log in.
    - □ In company's internal publications.
  - ▪ Have employees sign a documents that say they understand the conditions.
  - ▪ Why?
    - □ If users don't understand, they'll do risky things.
      - ◆ Talking about business deals via email.
    - □ If users don't understand, they'll assume the worst.
      - ◆ Oh, the sysadmins will read everyone's email.
- ○ What to do when you are asked to do something illegal/unethical?
  - ▪ Log, log, and log.
    - □ What was the request.
    - □ When was the request given to you.
    - □ What did you do to complete the request.
    - □ Why was it requested.
  - ▪ Process
    - □ Verify the request.

- ◆ Repeat the request, and ask that you understand it correctly.
- ◆ Ask that the request be written or emailed.
  - ◆ **Someone who is unwilling to write the request down is not willing to take responsibility for it.**
- ▫ If the request is against the law or policy,
  - ◆ State that, politely.
  - ◆ Reject the request explicitly.
- ▫ If he/she persists, go to a higher authority.
- ▪ You may decide to comply, but that doesn't bode you well.
  - ▫ You'll be an accomplice.
  - ▫ The other party will use that fact to coerce you do his bidding in the future.