CSE 265: System and Network Administration

MW 9:10-10:00am Packard 258
F 9:10-11:00am Packard 112

http://www.cse.lehigh.edu/~brian/course/sysadmin/
Find syllabus, lecture notes, readings, etc.

Instructor: Prof. Brian D. Davison
               davison@cse.lehigh.edu
               http://www.cse.lehigh.edu/~brian/

LEHIGH UNIVERSITY

Computer Science and Engineering
Computer Science and Engineering
Computer Science and Engineering
Computer Science and Engineering
CSE
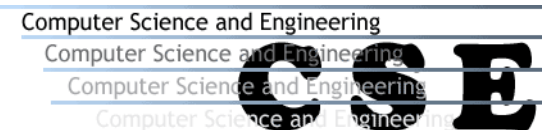
# Who is this course for?

- Students interested in learning
  - The roles and responsibilities of a computer systems and network administrator
  - How to configure & manage their own linux systems
  - How to diagnose and debug problems
  - How some of the major system services operate
  - Why they need to be nice to the sysadmin
- UNIX/Linux familiarity and programming experience required (CSE17)

What will the course cover?

- Understand the role & responsibilities of a system administrator
- Configure the Linux operating system
- Describe the system boot process
- Setup and manage user accounts and groups
- Manage the resources and security of a computer running Linux
- Make effective use of Unix utilities and scripting languages (bash, Perl)
- Configure and manage simple network services on a Linux system
- Develop an appreciation of the documentation available as part of an installed Unix/Linux system

What will it not cover?

- Networking in depth
  - Take CSE342 or CSE404 instead
- Network security in depth
  - Take CSE343 instead
- Windows administration
- Many hardware issues
- All the details needed for certification
  - Lots of certification courses available
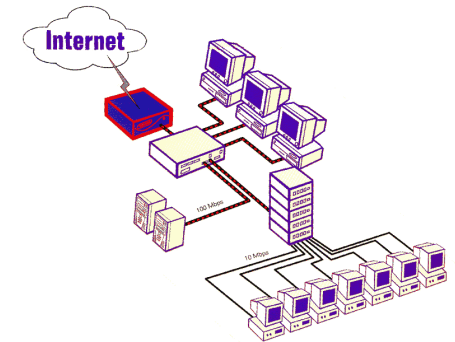
What will it not cover?

- Networking in depth
  - Take CSE342 or CSE404 instead
- Network security in depth
  - Take CSE343 instead
- Windows administration
- Many hardware issues
- All the details needed for certification
  - Lots of certification courses available

What does a sysadmin do?

CSE 265: System and Network Administration
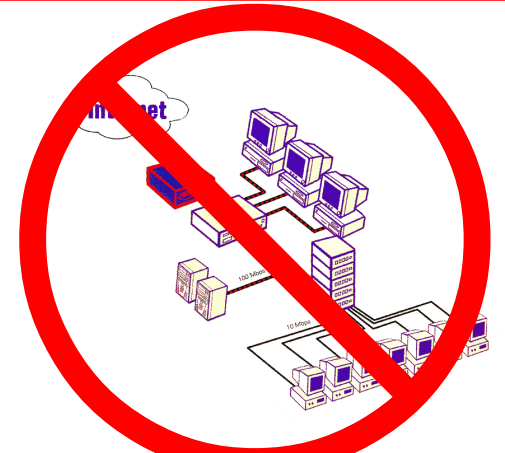
What does a sysadmin do?

- User account management
- Hardware management
- Perform filesystem backups, restores
- Install and configure new software and services
- Keep systems and services operating
    - Monitor system and network
    - Troubleshoot problems
- Maintain documentation
- Audit security
- Help users, performance tuning, and more!

User Account Management

- User Ids
- Mail
- Home directories (quotas, drive capacities)
- Default startup files (paths)
- Permissions, group memberships, accounting and restrictions
- Communicating policies and procedures
- Disabling / removing user accounts

Hardware Management

- Capacity planning

- Inventory

- Hardware evaluation and purchase

- Adding and removing hardware

  - Configuration

  - Cabling, wiring, DIP switches, etc.

- Device driver installation

- System configuration and settings

- User notification and documentation

Data Backups

- Perhaps most important aspect!

- Disk and backup media capacity planning

- Performance, network and system impact

- Disaster recovery

  - Onsite/Offsite

  - Periodic testing

  - Multiple copies

- User communication

 - Schedules, restore guarantees and procedures, loss tolerance
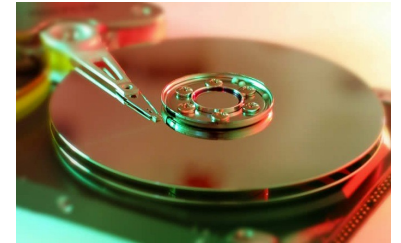
Software Installation/Maintenance

- Evaluation of software

- Downloading and building (compiling and tweaking)

- Installation

- Maintenance of multiple versions

- Security

- Patches and updates

- User notification, documentation
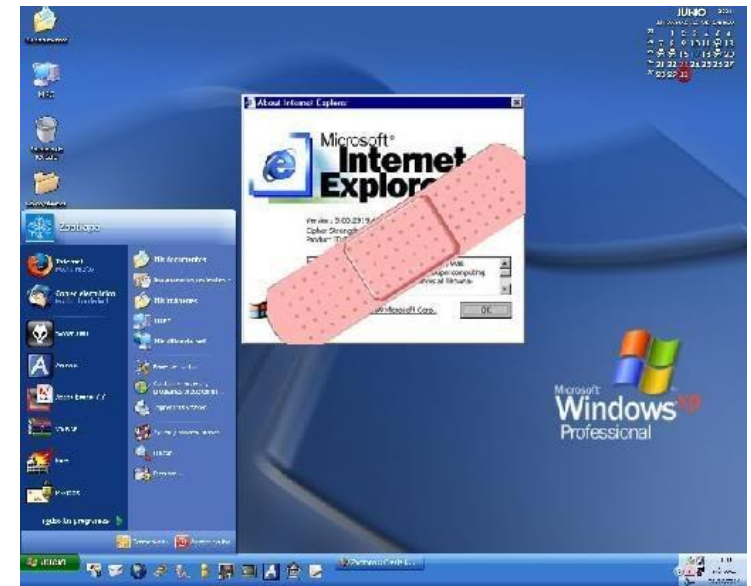
System Monitoring

- Hardware and services functioning and operational
- Capacity
  - Disk, RAM, CPU, network
- Security
  - Passwords
  - Break-ins
- System logs
  - Examination
  - Periodic rotation and truncation
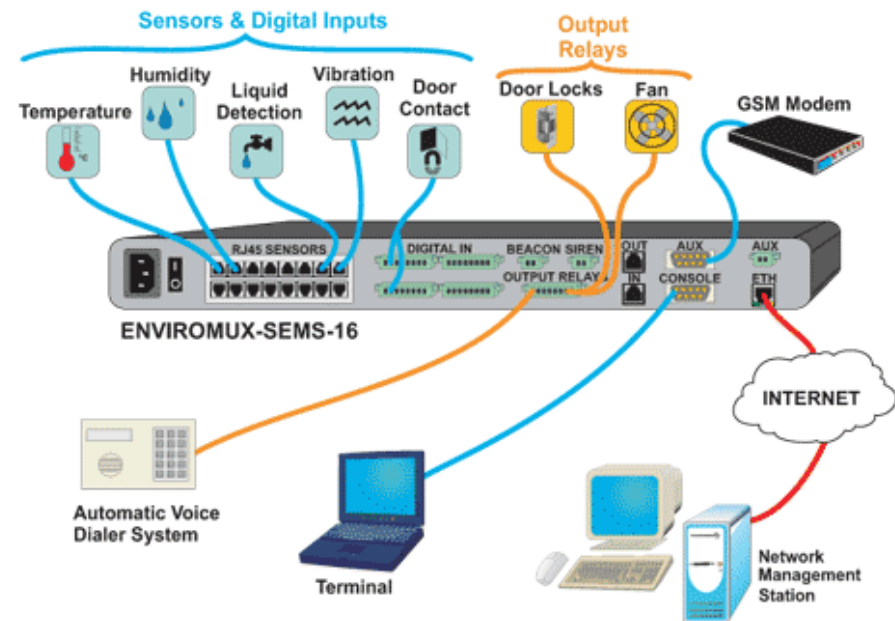
Troubleshooting

- Problem discovery, diagnosis, and resolution
  - Root cause analysis
  - Often quite difficult!
- Often requires
  - Broad and thorough system knowledge
  - Outside experts
  - Luck
- Expediency
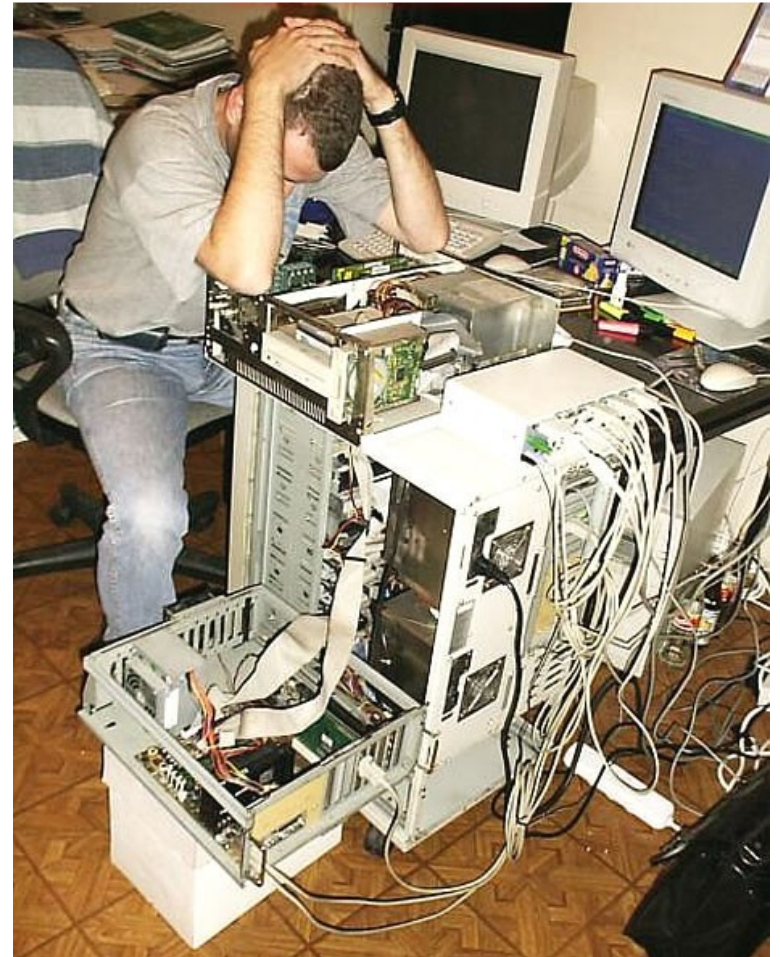
Local Documentation

- Administrative policies and procedures

  - Backup media locations

  - Hardware

    - Location

    - Description, configuration, connections

  - Software

    - Install media (or download location)

    - Installation, build, and configuration details

   - Patches installed

- Acceptable use policies

Security Concerns

- ## System logging and audit facilities
  - Evaluation and implementation
  - Monitoring and analysis
  - Traps, auditing and monitoring programs

- ## Unexpected or unauthorized use detection

- ## Monitoring of security advisories
 - Security holes and weaknesses
  - Live exploits

User Assistance

- Time intensive!
- Techniques
  - Help desks
  - Trouble-ticket systems
- Software availability and usage
- Software configuration settings
- Hardware usage, maintenance, and troubleshooting
- Writing FAQs
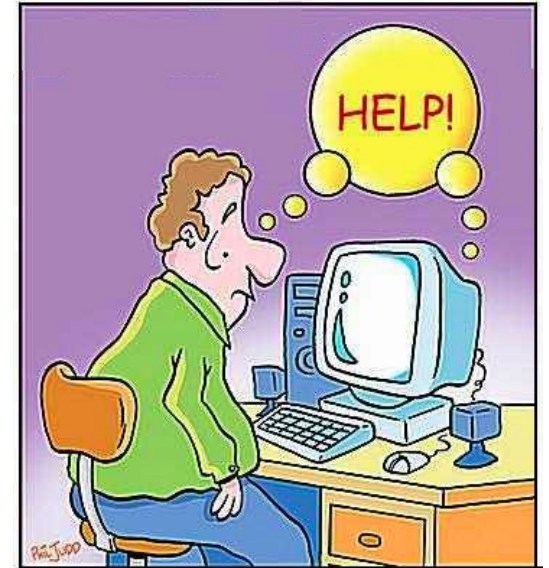
Administration Challenges

- Need
  - Broad knowledge of hardware and software
  - To balance conflicting requirements
    - Short-term vs. long-term needs
    - End-user vs. organizational requirements
    - Service provider vs. police model
  - To work well and efficiently under pressure
  - 24x7 availability
  - Flexibility, tolerance, and patience
  - Good communication skills
- People think of sysadmins only when things don't work!
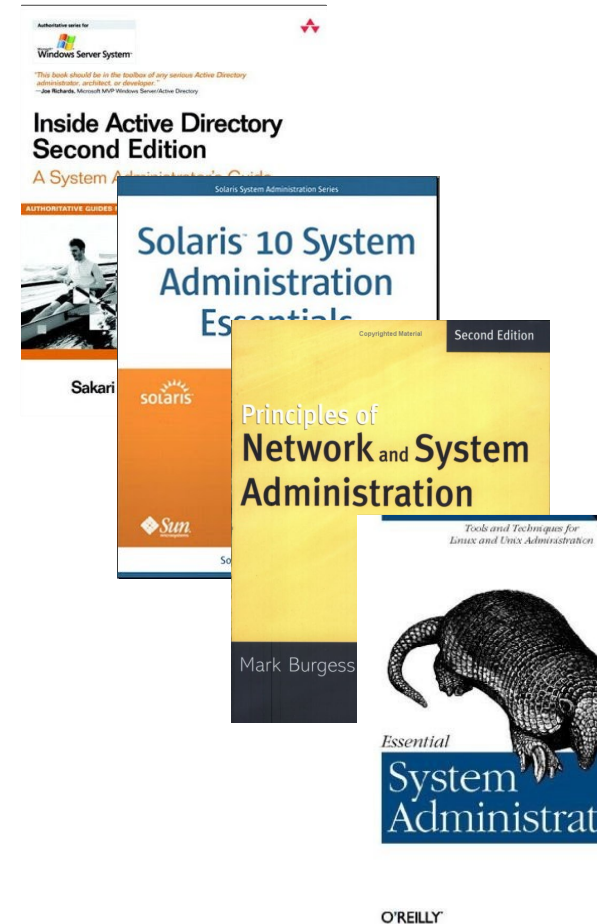
Which OS to learn to admin?

I'm a Mac   I'm UNIX   I'm Vista

Why (Red Hat/CentOS) Linux?

- Need to use some OS to make ideas concrete

- Really only two choices:
  - Windows (I'm not qualified)
  - UNIX (and UNIX-like OSes such as Linux)

- Both are useful and common in the real world

- Linux is popular, free, and usable on personal machines, but also handles large-scale services

- Red Hat/CentOS is relatively polished, popular
  - I've been using it since ~1996
  - There are, of course, many alternatives

What is Linux?
much is courtesy of www.kernel.org

- Linux is a clone of the operating system Unix, written by a loosely-knit team of hackers across the Net. It aims towards POSIX and Single UNIX Specification compliance.

- Like any modern fully-fledged Unix, Linux includes true multitasking, virtual memory, shared libraries, demand loading, shared copy-on-write executables, proper memory management, and TCP/IP networking.

- Linux really refers to the kernel – most of the commands that you are familiar with are really separate programs, not specific to Linux, and often are part of the Free Software Foundation's GNU project.

- Linux was first developed for 32-bit x86-based PCs (386 or higher). These days it also runs on dozens of other processors.

Brief history of UNIX

- Originated as a research project in 1969 at AT&T Bell Labs
    - Made available to universities (free) in 1976
- Berkeley UNIX started in 1977 when UCB licensed code from AT&T.
- Berkeley Software Distribution started in 1977 with 1BSD, and ended in 1993 with 4.4BSD
- Licensing costs from AT&T increased, so Berkeley attempted to remove AT&T code, but ran out of funds before completion.
- Final release of AT&T-free code called 4.4BSD-Lite.
    - Most current BSD distributions (FreeBSD, NetBSD, OpenBSD) are derived from 4.4BSD-Lite.
- Most commercial versions of UNIX (Solaris, HP-UX) are derived from the AT&T code

Brief history of Linux

- Created as a personal project (and still controlled) by Linus Torvalds, a Finnish graduate student, in 1991

- Conceived as an offshoot of Minix (a model OS)
  - Not derived from AT&T or BSD UNIX

- Red Hat (one of many Linux vendors) founded in 1993

- Kernel v1.0 released 1994

- Most recent (Jan 2012) kernel release is 3.2.1

Where to get answers

- Linux/UNIX documentation can be found in many places

  - Manual pages (man pages, using man command)

  - Texinfo documents (read with info command)

  - HOWTOs – focused descriptions of a topic

  - Distribution-specific documentation

  - Your favorite Web search engine

    - Will typically find online versions of the above

Where to get answers
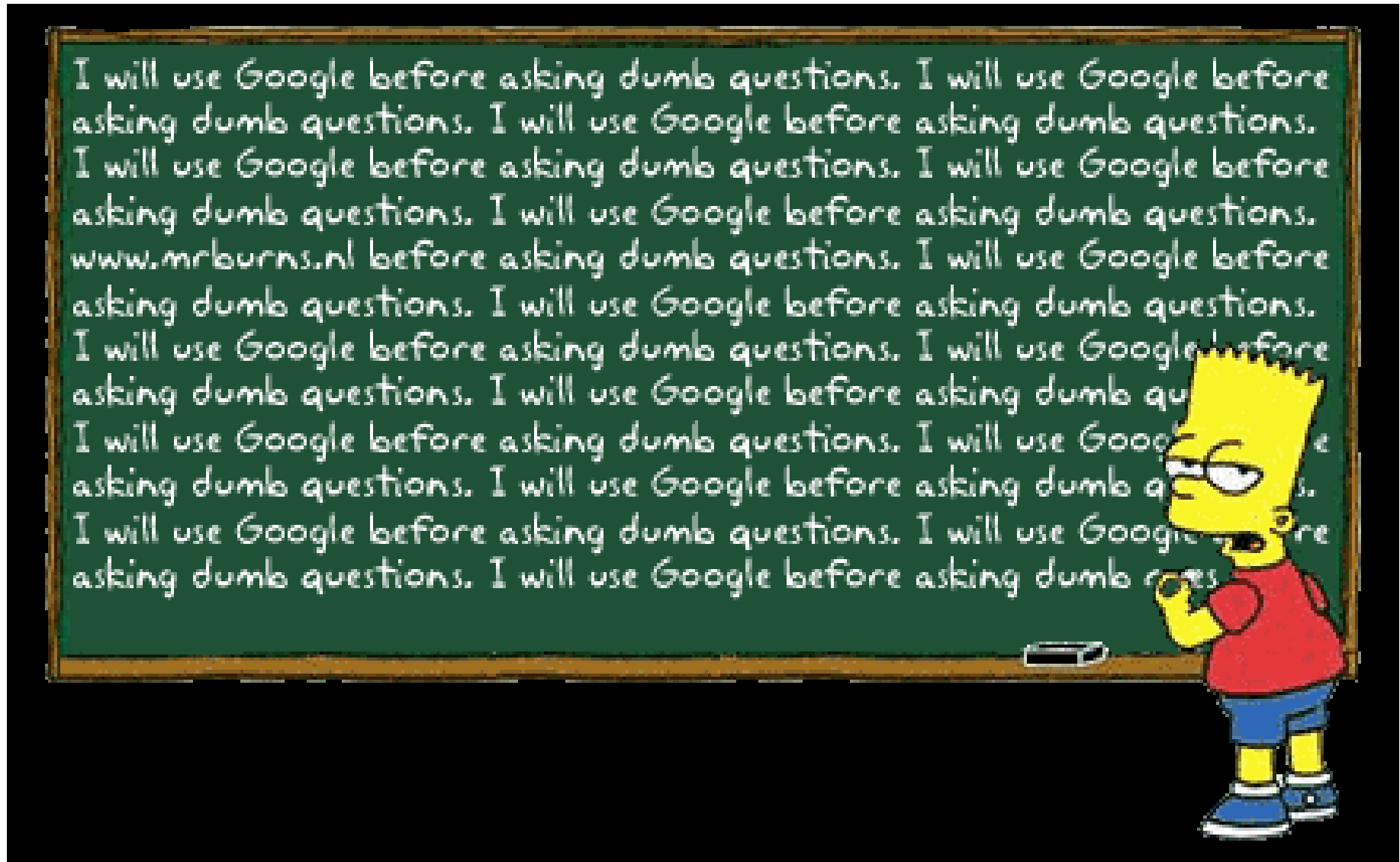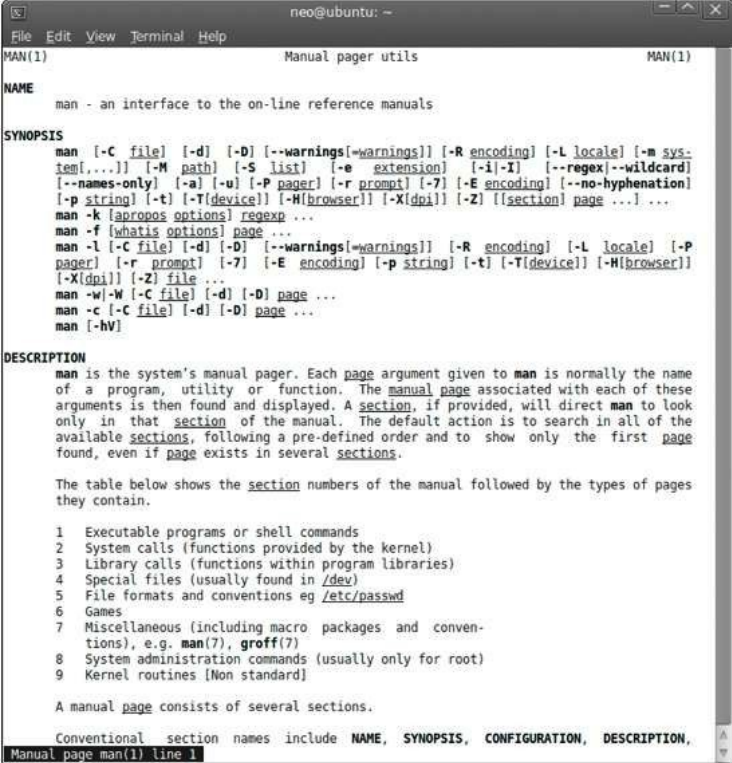
man pages

- Usually my first resource
- Provide OS installation-specific information
- Man pages document (almost) every command, driver, file format, and library routine
- "man -k topic" will list all man pages that use topic
- Parameters are not the same for every UNIX, e.g.:
  - Linux: man 4 tty
  - Solaris: man -s4 tty
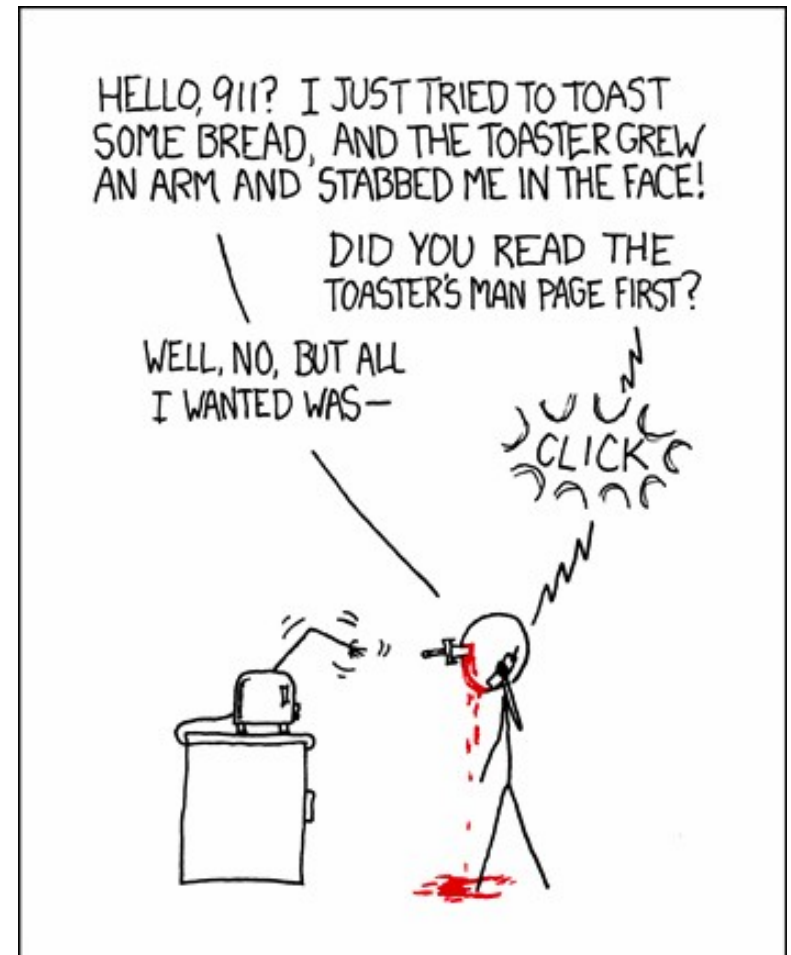
man page organization

- Man pages are divided into sections (somewhat Linux specific)
  - 1: User-level commands and applications
  - 2: System calls and kernel error codes
  - 3: Library calls
  - 4: Device drivers
  - 5: Standard file formats
  - 6: Games and demonstrations
  - 7: Miscellaneous files and documents
  - 8: System administration commands
  - 9: Obscure kernel specs and interfaces
- Some sections are subdivided
  - 3M contains pages for math library
  - Section "n" often contains subcommands (such as bash built-in cmds)
- Sections 6 and 9 are typically empty

Where do we go from here?

- In this course, I'll assign homework projects that require root access on a RHEL/CentOS 5 system.

- In our first lab, you will be provided with a hard drive that can be used in the Sandbox lab (PL112) with the OS, and root privileges so that you will administer it.

- In addition, you can (and should) use

  - the department Suns for most things
  - A CentOS 5 system (on the CSE network) called edgar.cse.lehigh.edu to explore a minimal working system

- See course web page for syllabus and schedule for topics and readings.