CS 406/591 – Linux System Administration – Summer 2015
MWF 1:20–3:10 p.m., Faner 2525

See the course web page for more complete information: http://www.cs.siu.edu/~cs406

Professor: Dr. Norman Carver, Faner 3121, phone 453-6048, email: carver@cs.siu.edu. Office hours: MWF 3:15–4:15 p.m. (or by appointment).


Workload CS 406: labs (30% total), two exams (35% each).
Workload CS 591: labs (25% total), two exams (25% each), and project (25%).

Course Objectives:
- To prepare students to be able to install and maintain networked Linux systems.
- To gain some familiarity with the security issues that face networked systems.
- To prepare students to assess, secure, and monitor networked Linux systems.
- To prepare students to pursue a basic Linux certification.

This course will provide an introduction to the administration of Linux systems, with emphasis on security for networked systems. Topics to be covered include: installation and configuration of Linux distributions, typical maintenance activities, security issues faced by networked systems, and testing and securing networked Linux machines. This is a first course in Linux system administration, focusing on networked desktop machines. It covers the topics required for basic Linux certifications such as CompTIA’s Linux+ cert. Administration of server machines and large-scale, mixed OS networks will be touched on only briefly.

It is critical that students gain hands-on practice working on, configuring, and installing Linux systems as part of this class. Luckily, the availability of free virtual machine software has made this much easier for students to achieve with their own personal machines. In addition, students in the course will have access to CS Dept. lab machines running Linux as well as machines on which to practice installing and configuring networked Linux systems.

Since CS 306 is a prerequisite for this course, Linux basics will be reviewed only briefly at the start of this course. Graduate students without equivalent Linux background will need to spend some additional time getting up to speed.

Many of the lectures will be available as online videos, for review or if class is missed. However, some lectures may be available only as slides/readings, or not at all. It is important that you read material that is assigned in the textbook as well.

Those registered for the course as CS 591 will be required to do additional work in the form of an (individual) project. Projects will require that students investigate, install, and configure a key Linux software system such as a server (e.g., mail server, web server, etc.). CS 591 students will give a presentation in class to teach others about this software and will also demonstrate their working software installation to the instructor/TA.
Course Outline:

1. Linux Basics
   - OS basics: filesystem, users, groups, permissions, processes
   - CLI: key commands, Bash shell
   - GUI: X11, KDE, Gnome

2. Linux Distribution Selection, Installation, and Configuration
   - Preparation: network settings, hardware, disk partitioning, backups
   - Boot loaders and booting multiple OSs
   - Installation: settings, software, services
   - Configuration: distribution tools, initial settings, network, printers, graphics
   - Basic security: services, permissions, tcpwrappers, etc.
   - Secure remote access: SSH

3. Bash Shell Programming
   - variables, parameters, I/O
   - metacharacters, shell expansions
   - control constructs (if, for, while, etc.)
   - associated tools (SED, AWK, etc.)

4. System Maintenance
   - Software installation: compiling from source vs. packages
   - Software updating/patching
   - System monitoring and log files
   - Backups
   - Kernel configuration and compilation

5. Overview of Computer Security Issues
   - Software bugs (buffer overflows, format string bugs)
   - Privilege escalation
   - Passwords, users/groups, and permissions
   - Networking basics
   - Footprinting, scanning, OS detection, and enumeration
   - Network attacks and services
   - Denial-of-service attacks

6. System Security Measures
   - Security scanners
   - Firewalls
   - Port scanning
   - Scan detectors
   - Log file assessment
   - Intrusion detection systems
   - Server configuration/hardening

7. Encryption
   - Encryption basics
   - Tools: SSH, SSL, GPG/PGP

8. Servers and services (mainly via projects)
   - remote access (e.g., SSH, FTP, Telnet)
   - file/print sharing (e.g., NFS, Samba, CUPS)
   - mail and web (e.g., Sendmail, Apache, Tomcat )
   - authentication (e.g., NIS, LDAP)
   - DNS (Bind)
   - database (mysql, PostgreSQL)