

Course Outline

1. Document Information

Degree Program	Computer Science
Course Number	CS 406
Course Title	Basic Linux System Administration
Semester Hours	3
Course Coordinator	Norman Carver
Revision Term	Spring 2020
Latest Revision	Fall 2020

2. Catalog Description

This course will be 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, and security measures for networked systems. Students will have access to lab machines for hands on practice.

3. Textbooks

- Nemeth, E., Snyder, G., Hein, T.R., & Whaley, B. (2018). Unix and Linux System Administration Handbook. Addison-Wesley, 5th Edition. ISBN: 9780134277554.

4. References

5. Course Learning Outcomes

- To learn to install and maintain networked Linux systems.
- To learn the security issues that face networked systems.
- To learn how to assess, secure, and monitor networked Linux systems.
- To gain some familiarity with common network server software packages

6. Assessment of the Contribution to Student Outcomes

Outcome	1	2	3	4	5	6
Assessed		X				X

7. Prerequisites by Topic

CS 306 with a grade of C or better or graduate standing.

8. Major Topics Covered in the Course

- Linux Basics
 - GUI: X11, KDE, Gnome, etc.
 - CLI: shells, key commands
 - OS basics: root, UIDs, GIDs, file system, processes, signals {4 classes}
- Linux distribution selection, installation, and configuration
 - Preparation: network settings, hardware, disk partitioning, backups boot loaders and booting multiple OS
 - Installation: settings, software, services
 - Configuration: distribution tools, initial settings, network
 - Basic security: services, permissions, tcp wrappers, etc {9 classes}
- System maintenance
 - Software installation: compiling from source vs. packages
 - Software updating/patching, system monitoring and log files, backup's kernel compilation. {4 classes}
- Overview of computer security issues: software bugs (buffer overflows, format string bugs), privilege escalation, passwords, users/groups, and permission, networking basics, foot printing, scanning, OS detection, and enumeration, network attacks and services, denial of service attack {6 classes}
- System security measures: security scanners, firewalls, port scanning, scan detectors, log file assessment, intrusion detection systems, server configuration/hardening {9 classes}
- Encryption 2: encryption basics Tools: SSH, SSL, GPG/PG {2 classes}
- Servers and service: remote access (e.g., SSH, FTP, Telnet), file/print sharing (e.g., NFS, Samba, CUPS), mail and web (e.g., Send mail, Apache, Tomcat), authentication (e.g., NIS, LDAP), DNS (Bind), database (mySQL) {10 classes}