CS 3910 – System Administration and Security
Syllabus

Course Description
This course covers the installation and configuration of mainstream operating systems, important network services, disaster recovery procedures, and techniques for ensuring the security of the system.

Course Objective
Students will learn and apply basic concepts and methodologies of System Administration and Security by building from the ground up a miniature corporate network. They will be responsible for installing backend servers that users would normally require for day to day operations. They will also be responsible for validating, from a user's perspective that their network is functional. Lastly, they will implement security measures into the network and do a risk assessment as to how effective their security measures are and their fellow students. Students will use Microsoft Windows Server 2008 for the Active Directories servers, and Microsoft Windows XP and/or 7 for the clients. Also, Ubuntu 10.10 and/or CentOS 5.6 will be used for the networking part of the class. All server and client computers are Virtual Machines working on a VMware environment.

Windows Portion:

I. Security Basics
- Principles of Information Security

II. Securing the Server Itself
- Authentication: Proof of identity
- Authorization: Limiting System Access and Controlling Using Behavior
- Restricting Access to Software; Restricting Software Access to Resources
- Controlling Access to Data
- EFS Basics

III. Maintenance and Recovery
- Maintenance Strategies and Administrative Practices
- Basics of Data Backup and Restore

IV. Monitoring and Audit
- Auditing
- Monitoring and Assessment

Laboratory Exercises:

Part 1. Server Installation and Configuration
- Introducing Windows Server 2008
- Installing Windows Server 2008
- Configuring Windows Server 2008 Basic Settings
- Configuring Server roles and services
- Managing hard drives and volumes

Part 2. Network Users, Resources, and Special Server Roles

Understanding and configuring Active Directory Domain services
Creating Active Directory groups, Organizational Units, and Sites
Adding client computers and member servers to the domain
Deploying group policy and network access
Working with network shares and the distributed file system

Linux Portion:

I. Introduction to Linux Systems

Booting and Shutting Down processes
Rootly Powers
Controlling Processes
The File System
Adding New Users
Periodic Processes

II. Understanding Configuration Management

Software and Configuration Management

III. Understanding Linux Networking

TCP/IP Networking

IV. Introduction to Networking Technologies (DHCP, DNS, NFS/iSCSI, SMTP, SNMP, LAMP)

Routing
Network Hardware
DNS
The Network File System
Network Management and Debugging

V. Introduction to Firewall/IDS/SSH

Key Certificates, etc.
Understanding Exposure Risk

VI. Securing Linux

Security

VII. Log Auditing and Vulnerability Assessment

Syslog and Log Files

VIII. Windows and Linux Coexisting

Cooperating with Windows

Laboratory Exercises:

Part 1. Linux OS installation

Ubuntu 10.10 installation
CentOS 5.6 installation

Part 2. DMZ setup and SSH server

Demilitarized Zone (DMZ) Setup
SSH Server Installation
Router Setup

Part 3. Key Certificates, IP Tables

Public Key Installation
Securing the network with IP Tables
Groogle incident

Part 4. DNS

DNS Master and Slave servers
Updating Microsoft DNS server

Textbooks:

Windows Portion:
Windows Server 2003 Security. A Technical Reference. Roberta Bragg. Addisson-Wesley

Linux Portion:
Linux Administration Handbook. Second Edition. Evi Nemeth, Garth Snyder, Trent R. Hein. Prentice Hall

References to be used during the course:

National Security Agency:
http://www.nsa.gov/
NIST, Computer Security Division, Computer Security Resource Center:
http://csrc.nist.gov/
Common Criteria for Information Technology Security Evaluation:
http://www.commoncriteriaportal.org/
U.S. Department of Homeland Security:
http://www.dhs.gov/
ITU (International Telecommunication Union:
http://www.itu.int/
Internet Society (ISOC):
http://www.isoc.org/
The Internet Engineering Task Force (IETF):
http://www.ietf.org/
Internet Architecture Board (IAB):
http://www.iab.org/
International Organization for Standardization (ISO):
http://www.iso.org
IEEE Computer Society:
http://www.computer.org
Association for Computing Machinery (ACM):
http://www.acm.org/
USENIX: The Advanced Computing Systems Association:
http://www.usenix.org/