

IT 443 Network Security Administration (a new course)

Course Description

This course explores the application of policy and techniques to securing both public and private networks. The course is project-based and includes such topics as threat analysis and management, cryptography, firewalls, isolation, issues in securing wireless networks, and certificates.

Course Goals

The goal of this course is to prepare the student to be able to

- Understand the principal issues in network security.
- Define and implement a security policy.
- Evaluate the implementation of a security policy.
- Learn what one can do

This course builds on the basics of Linux systems administration covered in IT 341 Introduction to Systems Administration.

How the Course Serves Students

IT443 is a required course in the System Administration track of the new BS in Information Technology (IT) degree, offered jointly by the Department of Computer Science (CSM) and the MSIS Department (CM). The System Administration track is offered by the Computer Science Department. The track's purpose is to prepare the student for a career in computer systems administration and/or information technology in general.

Syllabus

- Physical structures, including hubs, routers, switches and servers.
- Cryptography basics
- DNS, ipAddressing management (static and DHCP), domains, WINS and troubleshooting NAT issues.
- Single sign-on management
- Wireless security
- Router security and ACL settings
- The internet and private networks
- Firewalls, DMZ, and honey pots
- Tools for monitoring event logs, and troubleshooting.
- VPNs and routed networks
- Virtual networks and portable media
- Certificates
- The effects of the operating system (Unix, Windows and Mac)

- Sniffers and what they can or cannot see.
- Intrusion detection
- Hacker attacks
- Computer forensics
- Privacy, intellectual property and theft

Projects

Much of the material in this course will be transmitted by way of hands-on projects, where students, working in small teams, set up small networks of computers running Linux.

- A threat analysis and management study and a security plan.
- Setting up SSH.
- Implementing single sign-on.
- Implementing a system to monitor logs for intrusions and threats to security.
- White-hat hacking.
- Installing, configuring and monitoring a network firewall.
- Setting up a DMZ.
- Setting up a virtual private network (VPN).
- Implementing certificates.
- Implementing web application authentication and security

Grading

Projects and Engineering Notebook	50%
Midterm Exam	20%
Final Exam	30%

Textbooks and Readings

There are very good textbooks that address both the policy issues of system administration, as well as the implementation details. Many are oriented towards specific systems such as Unix, Linux, Windows and (for people with taste) Macs. For this course, we will use the following:

(From IT341)

1. Thomas A. Limoncelli, Christine Hogan and Strata R. Chalup. *The Practice of System and Network Administration, 2nd Edition*. Addison Wesley, 2007. ISBN 978-0321492661. (This discusses the generic policy questions in system administration, and rarely talks about a particular operating system.)

2. Evi Nemeth, Garth Snyder, Scott Seebass and Trent R Hein. *Unix System Administration Handbook (Third Edition)*. Prentice Hall, 2001. ISBN 0-13-020601-6. (Unix specific.)
3. Matt Welsh and Matthias Daheimer. *Running Linux (5th edition)*. O'Reilly, 2005. (Linux specific.)

(New for this course)

4. Simpson Garfinkel with Gene Spafford. *Web Security, Privacy & Commerce*. O'Reilly & Associates, 2002.
5. Gert DeLaet and Gert Schauwers. *Network Security Fundamentals*. Cisco Press (September 8, 2004).
6. Matt Curtin. *Introduction to Network Security*. Kent Information Security, 1997. Also on the WWW at <http://www.interhack.net/pubs/network-security/>.

Additional readings will be assigned from the SAGE web site at <http://www.sage.org/>. SAGE is the System Administrators Guild, a special technical group of the USENIX Association. They maintain a fabulous web site (which Rick Martin pointed us to) with all sorts of resources including a series of monographs on core sysadmin subjects.

Accommodations

Section 504 of the Americans with Disabilities Act of 1990 offers guidelines for curriculum modifications and adaptations for students with documented disabilities. If applicable, students may obtain adaptation recommendations from the Ross Center for Disability Services, Campus Center 2nd Floor, 2100 Street, Room 2010, 617-287-7430. The student must present these recommendations and discuss them with each professor within a reasonable period, preferably by the end of Drop/Add period.

Academic Honesty

All students are expected to follow the [University's Code of Student Conduct](#). If you are caught cheating, we will follow the guidelines for punishment outlined in the code.

When you turn in work that you have discussed with someone, or which contains ideas that you found in a book, *you must indicate that fact*. We expect you to talk to each other and to read materials other than those assigned. We also expect to see in your work evidence that you have done so. Learning to acknowledge intellectual debts is part of learning. You should be reading, talking to each other, and telling the world that you have done so. When group work is called for the group solution should note whenever a part of the project was done by only a part of the group.

Some kinds of sharing, however, are unacceptable. You may not use the computer to copy someone's work and submit it as your own -- even if you acknowledge that theft! You may not have your friends do your work for you. Versions of some of the assignments in this course may have been given in previous years. You may not use answers to those assignments.