

Syllabus for CMIT320 (Networking Security)

Course Materials

Wettern, Joern; Grasdahl, Martin. ALS Security+ Certification Textbook with 2 CDs and Laboratory Manual. Microsoft Press. ISBN: 0470067667.

Course Description

Prerequisite: CMIT 265 with grade of C or better or CompTIA Network+ certification. This course is designed to familiarize students with the fundamentals and implementation of computer network security. Course material relates to topics covered on the vendor-neutral CompTIA Security+ Certification examination. The Security+ Certification is recognized world wide as the standard of competency for entry-level network security professionals. Topics include authentication, remote access, Web security, intrusion detection, basic cryptography, physical security, and disaster recovery. Opportunities for hands-on exercises will be provided during class.

Course Goals/Objectives

After completing this course, you should be able to:

- articulate security threats and vulnerabilities to an organization
- explain how information is secured and resolve ethical dilemmas when securing information
- explain how cryptography is used to secure information and assess the strength of an encryption method for an organization secure information in an organization by using authentication and access control
- secure transmission of data and analyze the security of remote access for an organization
- identify network perimeter threats and monitor perimeter security for a network
- identify types of security policies used to manage operational security and use these policies to ensure compliance from users
- preserve business continuity by implementing a secure disaster recovery strategy
- identify, respond to, and participate in the investigation of security incidents
- write a technical research paper utilizing a variety of relevant sources

Course Introduction

This course is designed to familiarize students with the fundamentals and implementation of network security. The course material is based on the CompTIA Security+ Certification Exam, which is a vendor-neutral certification. This exam is the basis for worldwide standards of competency for entry-level network security professionals.

Grading Criteria

Section removed.

Academic Policies and Procedures

Section removed.

Project Descriptions

Technical Research Paper Topic:

Pick a topic relating to computer or network security. If you have any questions regarding the topic, I am available.

Students are encouraged to discuss with and get the instructor's approval of their topic before proceeding.

Technical Research Paper Guidelines:

- Use the American Psychological Association (APA) or Modern Language Association (MLA) style guide for the paper. General guidance information on either style can be found by linking to <http://www.umuc.edu/library/apa.html>.
- In addition to proper citation of sources, a well-written paper has an introduction, a body or main part, and a conclusion or concluding remarks. The body of the paper needs to be 5 (five) to 9 (nine) typed double-spaced pages. The font should be Times New Roman at 12-point font size.
- Utilizing at least five varied and relevant sources, research and write a technical paper relevant to network security. All sources must be properly cited and must be credible. At least two sources must be Internet sources (for help in evaluating the credibility of web sources, go to www.umuc.edu/library/guides/evaluate.shtml). At least one source must be from a scholarly journal (for help in identifying scholarly works, go to www.umuc.edu/library/guides/identify.shtml). Once you have completed a good draft, it is strongly advised that you submit it to UMUC's Effective Writing Center (EWC). In order to allow sufficient time for their review, you need to submit the draft to EWC two weeks prior to the paper's due date.

Note: Failure to follow these guidelines will result in substantial reduction of points. 5 points will be deducted for late submissions.

Course Schedule

Week	Module/Week Date	Readings/Assignments	Due Date
1	9/04/07	Introduction Ch. 1 - Addressing Security Threats and Vulnerabilities	
2	9/11/07	Ch. 2 – Creating Security Baselines	
3	9/18/07	Ch. 3 - Using Access Control and Authentication Quiz – 1	9/18/07
4	9/25/07	Ch. 4 – Using Encryption	
5	10/02/07	Ch. 5 – Using Public Key Infrastructure	
6	10/09/07	Ch. 6 – Securing Network Infrastructure Quiz – 2	10/9/07
7	10/16/07	Ch. 7 – Securing Communications	
8	10/23/07	Mid-term Exam (Chapters 1 – 7)	
9	10/30/07	Ch. 8 – Securing Network Applications Quiz – 3	10/30/07
10	11/06/07	Ch. 9 – Securing Instant Messaging	
11	11/13/07	Ch. 10 – Securing Network Perimeter	
12	11/20/07	Ch. 11 – Maintaining Operational Security Quiz – 4	11/20/07
13	11/27/07	Ch. 12 – Maintaining Organizational Security	
14	12/04/07	Ch. 13 – Detecting and Responding to Incidents Quiz – 5	12/4/07
15	12/11/07	Final Exam/Research Paper Due	12/11/07