Information Technology Security (ITSY 1342)

Credit: 3 semester credit hours (2 hours lecture, 4 hours lab)

Prerequisite/Co-requisite: None

Course Description

Instruction in security for network hardware, software, and data, including physical security: backup procedures: relevant tools: encryption: and protection from viruses.

Required Textbook and Materials

1. *Security+ Guide to Network Security Fundamentals, Fourth Edition,* Mark Ciampa, Course Technology, Cengage Learning, 2009.
    a. ISBN number is 978-1-1116-4012-5
2. Computer Networking and Troubleshooting Technology students are required to have one portable external Hard Drive with a capacity of 500GB or larger to be used for the duration of the time to complete their respective degree.

Course Objectives

Upon completion of this course, the student will be able to:

1. Employ the physical security of network infrastructure components using National Institute of Standards and Technology (NIST) Guidelines and other best practices.
2. Develop backup procedures to provide for data security.
3. Use network operating system features to implement network security.
4. Identify computer and network threats and vulnerabilities and methods to prevent their effects.
5. Use tools to enhance network security.
6. Use encryption techniques to protect network data.

Course Outline

A. Introduction to security
    1. Challenges of Securing Information
    2. What is Information security?
    3. Who are the Attackers?
    4. Attacks and Defenses
    5. Surveying Information Security careers and the Security+ Certification

B. System Threats and Risks
    1. Software-Based Attacks
    2. Hardware-Based Attacks
    3. Attacks on Virtual Systems

C. Protecting Systems
    1. Hardening the Operating System
    2. Preventing Attacks that Target the Web browser
    3. Hardening Web Servers
    4. Protecting Systems from Communications-Based Attacks
    5. Applying Software Security Applications

D. Network Vulnerabilities and Attacks
    1. Network Vulnerabilities
    2. Categories of Attacks

Approved 12/2013

3. Methods of network Attacks

E. Network Defenses
   1. Crafting a Secure network
   2. Applying Network Security Devices
   3. Host and network Intrusion Prevention Systems (HIPS/NIPS)
   4. Protocol Analyzers
   5. Internet Content Filters
   6. Integrated Network Security Hardware

F. Wireless Network Security
   1. IEEE 802.11 Wireless Security Protections
   2. Vulnerabilities of IEEE 802.11 Security
   3. Personal Wireless security
   4. Enterprise Wireless Security

G. Access Control Fundamentals
   1. What is Access Control?
   2. Logical Access Control methods
   3. Physical Access Control

H. Authentication
   1. Definition of Authentication
   2. Authentication Credentials
   3. Extended Authentication Protocols (EAP)
   4. Remote Authentication and Security

I. Performing Vulnerability Assessments
   1. Risk Management, Assessment, and Mitigation
   2. Identifying Vulnerabilities

J. Conducting Security Audits
   1. Privilege Auditing
   2. Usage Auditing
   3. Monitoring Methodologies and Tools

K. Basic Cryptography
   1. Defining Cryptography
   2. Cryptographic Algorithms
   3. Using Cryptography on Files and Disk

L. Applying Cryptography
   1. Digital Certificates
   2. Public Key Infrastructure (PKI)
   3. Key Management
   4. Cryptographic Transport Protocols

M. Business Continuity
   1. Environmental Controls
   2. Redundancy Planning
   3. Disaster Recovery Procedures
   4. Incident Response Procedures

N. Security Policies and Training
   1. Organizational Security Policies
   2. Types of Security Policies
   3. Education and Training

Grade Scale

90 – 100	A
80 – 89	B
70 – 79	C
60 – 69	D
0 – 59	F

Course Evaluation

Final grades will be calculated according to the following criteria:

1. Labs	20%
2. Study Guides	20%
3. Chapter Tests	30%
4. Final Exam	30%

Course Requirements

1. Demonstration of proficiency through hands-on labs as assigned.
2. Completion of Study Guides and work sheets as assigned.

Course Policies

1. No food, drinks, or use of tobacco products in class.
2. Beepers, telephones, headphones, and any other electronic devices must be turned off while in class.
3. Do not bring children to class.
4. No late assignments will be accepted.
5. Certification. If a student passes the certification test that is associated with this class, you will receive an "A" on the final exam and credit for 25% of your labs. If you have missed a previous test, you must still take the final exam to substitute for that grade.
6. Attendance Policy. Three absences are allowed. If a student is tardy to class or departs early three (3) times, it will be equal to one (1) absence. Each absence beyond three absences will result in a 2 point deduction from your final grade.
7. If you wish to drop a course, the student is responsible for initiating and completing the drop process. If you stop coming to class and fail to drop the course, you will earn an 'F' in the course.
8. Labs. Due dates will be announced by the instructor.
9. Tools. Return all tools and/or software to their designated place.
10. A grade of 'C' or better must be earned in this course for credit toward degree requirement.
11. Additional class policies as defined by the individual course instructor.

Disabilities Statement

The Americans with Disabilities Act of 1992 and Section 504 of the Rehabilitation Act of 1973 are federal anti-discrimination statutes that provide comprehensive civil rights for persons with disabilities. Among other things, these statutes require that all students with documented disabilities be guaranteed a learning environment that provides for reasonable accommodations for their disabilities. If you believe you have a disability requiring an accommodation, please contact the Special Populations Coordinator at (409) 880-1737 or visit the office in Student Services, Cecil Beeson Building.

Course Schedule

Week of	Topic	Reference
Week 1	Syllabus and policies Course Introduction	

Week of	Topic	Reference
Week 2	Chapter 1: Introduction to Security	pp. 1-38
Week 3	Chapter 2: System Threats and Risks	pp. 38–78
Week 4	Chapter 3: Protecting Systems	pp. 79-118
Week 5	Chapter 4: Network Vulnerabilities and Attacks	pp. 119-152
Week 6	Chapter 5: Network Defenses	pp. 153-188
Week 7	Chapter 6: Wireless network Security	pp. 189-224
Week 8	Chapter 7: Access Control Fundamentals	pp. 225-264
Week 9	Chapter 8: Authentication	pp. 265-300
Week 10	Chapter 9: Performing Vulnerability Assessments	pp. 301-330
Week 11	Chapter 10: Conducting Security Audits	pp. 331-364
Week 12	Chapter 11: Basic Cryptography	pp. 365-398
Week 13	Chapter 12: Applying Cryptography	pp. 399-438
Week 14	Chapter 13: Business Continuity	pp. 439-476
Week 15	Chapter 14: Security Policies and Training	pp. 477-508
Week 16	Lab Completion Final Exam	

Contact Information:

Program Director: Lauri Arnold
Program Director
Computer Networking and Troubleshooting Technology

Office: Office 103C, TA-4

Telephone: (409) 839-2050

E-mail: lauri.arnold@lit.edu

Additional Course Policies

Additional policies may be determined by individual course instructors. These policies will be indicated in the syllabus that is issued at the start of the course.