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. *TestOut Security Pro* by www.TestOut.com, 2016.
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

1. Introduction
   a. Security Overview
   b. Using the Simulator
2. Access Control and Identity Management
   a. Access Control Models
   b. Authentication
   c. Authorization
   d. Access Control Best Practices
   e. Active Directory Overview
   f. Windows Domain Users and Groups
   g. Linux Users
   h. Linux Groups
   i. Linux User Security
   j. Group Policy Overview

   k. Hardening Authentication 1
   l. Hardening Authentication 2
   m. Remote Access
   n. Network Authentication
   o. Identity Management

3. Cryptography
   a. Cryptography
   b. Hashing
   c. Symmetric Encryption
   d. Asymmetric Encryption
   e. Public Key Infrastructure (PKI)
   f. Cryptography Implementations
4. Policies, Procedures, and Awareness
   a. Security Policies
   b. Manageable Network Plan
   c. Business Continuity
   d. Risk Management
   e. Incident Response
   f. Social Engineering
   g. Certification and Accreditation
   h. Development
   i. Employee Management
   j. Third-Party Integration
5. Physical Security
   a. Physical Security
   b. Hardware Security
   c. Environmental Controls
   d. Mobile Devices
   e. Mobile Device Security Enforcement
   f. Telephony
6. Perimeter Defenses
   a. Network Layer Protocol Review
   b. Transport Layer Protocol Review
   c. Perimeter Attacks 1
   d. Perimeter Attacks 2
   e. Security Appliances
   f. Demilitarized Zones (DMZ)
   g. Firewalls
   h. Network Address Translation (NAT)
   i. Virtual Private Networks (VPN)

   j. Web Threat Protection
   k. Network Access Control (NAC)
   l. Wireless Overview
   m. Wireless Attacks
   n. Wireless Defenses

7. Network Defenses
   a. Network Devices
   b. Network Device Vulnerabilities
   c. Switch Attacks
   d. Router Security
   e. Switch Security
   f. Intrusion Detection and Prevention
   g. SAN Security

8. Host Defenses
   a. Malware
   b. Password Attacks
   c. Windows System Hardening
   d. Hardening Enforcement
   e. File Server Security
   f. Linux Host Security
   g. Static Environment Security

9. Application Defenses
   a. Web Application Attacks
   b. Internet Browsers
   c. E-Mail
   d. Network Applications
   e. Virtualization
   f. Application Development

10. Data Defenses
   a. Redundancy
   b. Backup and Restore
   c. File Encryption
   d. Secure Protocols
   e. Cloud Computing

11. Assessments and Audits
   a. Vulnerability Assessment
   b. Penetration Testing
   c. Protocol Analyzers
   d. Log Management
   e. Audits

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:

Labs	25%
Practice Questions	10%
Module Tests	35%
Final Exam	30%

Course Requirements

1. Demonstrate proficiency through hands-on labs as assigned.
2. Completion of Study Guides as assigned.

Course Policies

1. No food, drinks, or use of tobacco products in class.
2. Electronic devices not being used for the class, such as phones and headphones, must be turned off while in class.
3. Do not bring children to class.
4. 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.
5. 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.
6. 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.
7. Tools: Return all tools and/or software to their designated place.
8. A grade of ‘C’ or better must be earned in this course for credit toward degree requirement.
9. Additional course policies, as defined by the individual course instructor, will be outlined in the course addendum and provided by the 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.

Technical Requirements (for courses using Blackboard)

The latest technical requirements, including hardware, compatible browsers, operating systems, software, Java, etc. can be found online at:

https://help.blackboard.com/en-us/Learn/9.1_2014_04/Student/015_Browser_Support/015_Browser_Support_Policy

A functional broadband internet connection, such as DSL, cable, or WiFi is necessary to maximize the use of the online technology and resources.

Student Code of Conduct Statement

It is the responsibility of all registered Lamar Institute of Technology students to access, read, understand and abide by all published policies, regulations, and procedures listed in the LIT Catalog and Student Handbook. The LIT Catalog and Student Handbook may be accessed at www.lit.edu or obtained in print upon request at the Student Services Office. Please note that the online version of the LIT Catalog and Student Handbook supersedes all other versions of the same document.

Certification Requirement

CNTT majors are required to earn certification in one of the following areas prior to graduation.

- A+ Certification
- Cisco Certified Entry Network Technician (CCENT)
- Cisco Certified Network Associate (CCNA)
- Microsoft Certified Solutions Associate (MCSA)

This course covers the material to prepare for CompTIA's Security+ certification, exam number SY0-401. Students are responsible for scheduling and paying for the certification through the LIT Testing Center. More information about the certification can be found online at https://certification.comptia.org/certifications/a.

Course Schedule

Week of	Topic	Reference
Week 1	Hybrid	www.testout.com
Week 2	Syllabus and policies Course Introduction Module 1:Introduction	

Week of	Topic	Reference
Week 3	Module 2: Access Control and Identity Management	
Week 4	Module 2: Access Control and Identity Management	
Week 5	Module 2: Access Control and Identity Management	
Week 6	Module 3:Cryptography	
Week 7	Module 4: Policies, Procedures, and Awareness	
Week 8	Module 4: Policies, Procedures, and Awareness	
Week 9	Module 5: Physical Security	
Week 10	Module 6: Perimeter Defenses	
Week 11	Module 6: Perimeter Defenses	
Week 12	Module 7: Network Defenses	
Week 13	Module 8: Host Defenses	
Week 14	Module 9: Application Defenses	
Week 15	Module 10: Data Defenses	
Week 16	Module 11: Assessments and Audits	

Contact Information:

Program Director:	Lauri Arnold-Calder Program Director Computer Networking and Troubleshooting Technology
Office:	Office 103C, TA-4
Telephone:	(409) 839-2050
E-mail:	ldarnold@lit.edu