CSIT 4355 - ENTERPRISE SECURITY

CREDIT HOURS: 3
PREREQUISITES: CSCI 3321 or CSCI 3331 or CSIT 3355.
GRADE REMINDER: Must have a grade of C or better in each prerequisite course.

CATALOG DESCRIPTION

Practical approaches to ensuring the security of information systems. May not be used to satisfy computer science requirements for a major or minor in computer science or computer information systems.

PURPOSE OF COURSE

The purpose of this course is to provide the student with an understanding of tools and techniques employed to assure security in information systems. Legal, ethical, professional, and technical issues will be addressed. Current topics will be explored.

EDUCATIONAL OBJECTIVES

Upon successful completion of the course, students should be able to:

1. Demonstrate an understanding of the computer security field through identification of need, social issues, risk assessment and planning.
2. Demonstrate an understanding of the threats and controls for operating system and network security and to study specific system vulnerabilities.
3. Identify techniques of disaster planning and recovery.
4. Identify the tools and techniques of digital forensics.
5. Describe current topics in the computer security field.

COURSE CALENDAR

This course meets for a minimum of 37.5 lecture contact hours during the semester, including the final exam. Students have significant weekly reading assignments. Students are expected to complete 8-9 homework assignments, and 2-3 periodic exams in addition to the final exam. Students are expected to prepare for any class assignments or quizzes over the material covered in class or in the reading material. Successful completion of these activities requires at a minimum six additional hours of outside of classroom work each week.

CONTENT

Introduction and Scope .................................................................3
   Legal, Ethical, Professional Issues
   Risk Management and Planning
   Personnel, Physical, and Maintenance Security Issues

Security Assessment .................................................................................10
   Attack Vectors
   Vulnerability Assessment and Audit
Disaster Planning

Security Implementation Policy

Intrusion Prevention, Detection, and Recovery

Authentication

Firewalls

Architecture

Components

Bastion Hosts

Cryptography

Virtual Private Networks

Current Topics

Exams (plus final)

TOTAL 45

REFERENCES


Smith, Elementary Information Security, Jones and Bartlett, 2016
