SOUTHEAST COMMUNITY COLLEGE
CONSTRUCTION MANUFACTURING AND TECHNOLOGY DIVISION
Computer Information Technology Program
Revision Date: August 26, 2019

I. CATALOG DESCRIPTION

Course Number:	INFO2691
Course Title:	Enterprise Security Capstone
Prerequisite(s):	INFO2581, INFO2586
Corequisite(s):	INFO2596
Catalog Description:	This is project-based course using cybersecurity techniques and best practices to secure and defend computing systems and network infrastructures. Security is approached from both a red team and blue team aspect.
Credit Hours:	3.0
Class Hours:	45
Lab Hours:	0
Total Contact Hours:	45

II. COURSE OBJECTIVES: *Course will:*

A. Verify knowledge of various InfoSec techniques learned in previous CIT courses.
B. Evaluate students' ability to secure system and network infrastructures using current industry and governmental security frameworks.
C. Measure ability to perform a network vulnerability analysis to practice and refine attach methodologies with attacker tools and techniques.
D. Assess decision-making skills when presented with a variety of scenarios and students' ability to implement InfoSec solutions in a real-world environment.

III. STUDENT LEARNING OUTCOMES AND GENERAL EDUCATION LEARNING OUTCOMES:

A. Student Learning Outcomes: *Student will be able to:*
  1. Design, plan and implement a secure enterprise network
  2. Create written documentation of a security design, attack methodology, tools and techniques used to secure an enterprise network.
  3. Demonstrate the ability to conduct a vulnerability analysis and penetration tests on an enterprise network.
  4. Evaluate methods and processes to gain unauthorized access into protected networks.
  5. Formulate responses and design modifications to ongoing simulated attacks.
B. General Education Learning Outcomes (GELOs)
  1. GELO 3: Critical Thinking & Problem Solving
  Outcome 2: Synthesize information to arrive at reasoned solutions to problems.

IV. CONTENT/TOPICAL OUTLINE

A. Identification and cataloging of IT System Components; Workstations, Servers, Network Storage Systems, Mobile Devices, Routers, Switches, VPNs, and Security Devices
B. Network Mapping and Vulnerability Scanning: Document network components and their potential exposure to attack to Minimizing Exposure (Attack Surface and Vectors)
C. Network Security Techniques and Components, including Access controls, OS/Application Updates and Patching, Network Hardening, Applications of Cryptography, Honeypots, and Security Devices.

D. Identification and Defense against Attacks: Password Attacks, Backdoors/Trojans/viruses, Sniffing/spoofing, session hijacking, DoS/DDoS, and insider attacks

E. Defense in Depth (DiD) approach using Separation, Isolation, Obfuscation, Encapsulation, and Least Privilege to implement IDS/IPS, Firewalls, VPNs, DMZs, and Proxy Servers to achieve the desired level of security

F. Network Monitoring and Traffic Analysis

G. Application of Computer and Digital Forensics techniques to understand, document, and defend against future attacks

V. INSTRUCTIONAL MATERIALS

A. Required Text(s): None

B. Ancillary Resources: Enterprise Security Capstone Supplemental Materials and project files

C. Computer and Internet access

VI. METHODS OF PRESENTATION/INSTRUCTION

A. Methods of presentation typically include a combination of the following:

1. Technology enhanced lectures and classroom discussions

2. In class hands-on assignments

3. Interactive group activities

VII. METHODS OF EVALUATION

A. Methods of evaluations, although determined by the individual instructor, traditionally includes a combination of the following:

1. Attendance and/or participation activities

2. Homework and hands-on assignments

3. Research projects

VIII. SPECIFIC COURSE REQUIREMENTS

A. This course will not qualify as a prerequisite if the student receives a final grade below a C 70%).