ALLEN COMMUNITY COLLEGE
COMMON COURSE OUTLINE
CIS 242 NETWORK SECURITY +

www.allencc.edu

I. COURSE INFORMATION

A. Computer Science 242 Network Security +
B. 3 credit hours
C. Online Textbook
D. Prerequisites: CIS 241 or instructor approval

II. COURSE DESCRIPTION

This course is designed to provide hands-on skills in the area of network security, compliance and operation security, threats, and vulnerabilities in accordance with the Comp-TIA Security+ certification objectives. This course prepares students for the SYO-701 CompTIA Security+ certification exam.

III. LEARNING OUTCOMES

A. Explain general security concepts
   a. Compare and contrast various types of security controls
   b. Summarize fundamental security concepts
   c. Explain the importance of change management processes and the impact of security
   d. Explain the importance of using appropriate cryptographic solutions
B. Recognize common threats, Vulnerabilities, and Mitigations
   a. Compare and contrast common threat actors and motivations
   b. Explain common threat vectors and attack surfaces
   c. Explain various types of vulnerabilities
   d. Given a scenario, analyze indicators of malicious activity
   e. Explain the purpose of mitigation techniques used to secure the enterprise
C. Compare different security architectures
   a. Compare and contrast security implications of different architecture models
   b. Given a scenario, apply security principles to secure enterprise infrastructure
   c. Compare and contrast concepts and strategies to protect data
   d. Explain the importance of resilience and recovery in security architecture
D. Implement security operation techniques
   a. Given a scenario, apply common security techniques to computing resources
   b. Explain the security implications of proper hardware software, and data asset management
   c. Explain various activities associated with vulnerability management
   d. Explain security alerting and monitoring concepts and tools
   e. Given a scenario, modify enterprise capabilities to enhance security
   f. Given a scenario, implement and maintain identity and access management
   g. Explain the importance of automation and orchestration related to secure operations
   h. Explain appropriate incident response activities
   i. Given a scenario, use data sources to support an investigation
E. Explain security program management and oversight
   a. Summarize elements of effective security governance
   b. Explain elements of the risk management process
   c. Explain the processes associated with third-party risk assessment and management
   d. Summarize elements of effective security compliance
   e. Explain types and purposes of audits and assessments
   f. Given a scenario, implement security awareness practices

IV. MAJOR CONTENT AREAS

A. Network security
B. Compliance and operational security
C. Threats and vulnerabilities

D. Application, data and host security
E. Cryptography

V. ASSIGNMENTS

A. Reading assignments
B. Programming exercises
C. Simulation exercises
D. Discussions
E. Chapter examinations

VI. EVALUATION METHODS

A. Chapter quizzes
B. Assignments
C. Simulations
D. Final exam