ALLEN COMMUNITY COLLEGE
COMMON COURSE OUTLINE
CIS 242 NETWORK SECURITY +

Allen COMMUNITY COLLEGE
www.allencc.edu

I. COURSE INFORMATION

A. Computer Science 242 Network Security +
B. 3 credit hours
C. Ciampa, Mark. *CompTIA Security+ Guide to Network Security Fundamentals.* 5th ed. MA: Cengage, 2016
D. Prerequisites: CIS 125 or 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.

III. LEARNING OUTCOMES

A. Implement security configuration parameters on network devices and other technologies
B. Given a scenario, use secure network administration principles
C. Explain network design elements and components
D. Given a scenario, implement common protocols and services
E. Given a scenario, troubleshoot security issues related to wireless networking
F. Explain the importance of risk related concepts
G. Summarize the security implications of integrating systems and data with third parties
H. Given a scenario, implement appropriate risk mitigation strategies
I. Given a scenario, implement basic forensic procedures
J. Summarize common incident response procedures
K. Explain the importance of security related awareness and training
L. Compare and contrast physical security and environmental controls
M. Summarize risk management best practices
N. Given a scenario, select the appropriate control to meet the goals of security
O. Explain types of malware
P. Summarize various types of attacks
Q. Summarize social engineering attacks and the associated effectiveness with each attack
R. Explain types of wireless attacks
S. Explain types of application attacks
T. Analyze a scenario and select the appropriate type of mitigation and deterrent techniques
U. Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities
V. Explain the proper use of penetration testing versus vulnerability scanning
W. Explain the importance of application security controls and techniques
X. Summarize mobile security concepts and technologies
Y. Given a scenario, select the appropriate solution to establish host security
Z. Implement the appropriate controls to ensure data security
AA. Compare and contrast alternative methods to mitigate security risks in static environments
BB. Compare and contrast the function and purpose of authentication services
CC. Given a scenario, select the appropriate authentication, authorization or access control
DD. Install and configure security controls when performing account management, based on best practices
EE. Given a scenario, utilize general cryptography concepts
FF. Given a scenario, use appropriate cryptographic methods
GG. Given a scenario, use appropriate PKI, certificate management and associated components

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