



BAKER COLLEGE
STUDENT LEARNING OUTCOMES

ITS 2110 Introduction to Network Security
3 Semester Hours

Student Learning Outcomes and Enabling Objectives

- 1. Implement security configuration parameters on network devices**
 - a. Describe the concepts of confidentiality, integrity and availability (CIA)
 - b. Discuss the challenges of securing networks.
 - c. Differentiate appropriate network design elements and compounds
 - d. Apply secure network administration principles
 - e. Explain the security function and purpose of network devices and technologies
 - f. Employ wireless network in a secure manner
 - 2. Prescribe the best practices of compliance and operational security**
 - a. Differentiate among types of malware, and network attacks
 - b. Determine the appropriate mitigation and deterrent techniques
 - c. Analyze assessment tools and techniques to discover security threats and vulnerabilities
 - d. Investigate aspects of business continuity
 - e. Explain the impact and proper use of environmental controls
 - f. Defend the importance of security related awareness and training
 - 3. Incorporate controls for application, data and host security**
 - a. Identify methods of securing the host.
 - b. Classify types of application attacks
 - c. Carry out appropriate procedures to establish host security
 - d. Summarize mobile security concepts and technologies
 - e. Prescribe techniques to secure data and applications.
 - 4. Determine access and identity management strategies**
 - a. Describe the fundamental concepts and best practices related to authentication, authorization and access control
 - b. Implement appropriate security controls when performing account management
 - c. Apply appropriate cryptographic tools and products
 - d. Explain the core concepts of public key infrastructure
 - e. Examine PKI, certificate management and associated components
-

Big Ideas

- Network architecture and security
- Data and application security
- Threats and Vulnerabilities
- Access and Authentication

Essential Questions

1. How can organizations keep information in their network safe?
2. How does the security triad, relate to the administration of a network?
3. What are the prevalent threats to network security?
4. How can developers make applications more secure?
5. What is the role of cryptography in protecting data?
6. What is the importance of protecting mobile devices?
7. What is the significance of access control?
8. Why is it necessary for an organization to have a business continuity plan?
9. How does understanding risk and risk management relate to an information security plan?

This message was at the bottom of the previous SLO

These SLOs are not approved for experiential credit.

Effective: Fall 2017