CYBR C230: NETWORK SECURITY (SECURITY+)

Item	Value
Curriculum Committee Approval Date	10/27/2023
Top Code	070800 - Computer Infrastructure and Support
Units	3 Total Units
Hours	68 Total Hours (Lecture Hours 54; Lab Hours 14)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Open Entry/Open Exit	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

This course introduces the concepts of enterprise security, network and application attacks, cybersecurity resilience, secure network designs, and incident response. The principles and structure of threats, attacks, and vulnerabilities are surveyed to provide a foundation for further study of cybersecurity. This course covers governance, risk, and compliance to examine the nature and roles of organizational security policies and risk management processes. Hands-on exercises help students develop skills to prepare for careers such as Security Administrator or Systems Administrator. Helps students gain knowledge in preparation for the CompTIA Security+ certification exam. ADVISORY: CYBR C101 and IT C128. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Define fundamental terminology and describe the theory associated with network security.
2. Given a scenario, use the appropriate tool to assess organizational security.
3. Given a scenario, apply mitigation techniques and/or configure controls to secure a network environment.

Course Objectives

- 1. Describe security assessment techniques to determine organizational security vulnerabilities.
- 2. Define secure application development, deployment, and automation concepts that improve organizational security posture.
- 3. Identify the different security solutions for hosts, applications, wireless networks, and cloud environments.
- 4. Develop basic policies, procedures, and processes for incident response.

Lecture Content

Threats, Attacks, and Vulnerabilities Social engineering techniques Determining the type of attack Application attacks Network attacks Threat actors, vectors, and intelligence sources Various types of vulnerabilities Security assessments techniques Penetration testing Architecture and Design Security concepts in an enterprise environment Virtualization and cloud computing concepts Secure application development, deployment, and automation concepts Authentication and authorization design concepts Cybersecurity resilience Embedded and specialized systems Physical security controls Cryptographic concepts Implementation Secure protocols Host and application security solutions Secure network designs Wireless security settings Secure mobile solutions Cybersecurity solutions to the cloud Identity and account management controls Authentication and authorization solutions Public key infrastructure Operations and Incident Response Assessment tools for organizational security Policies, processes, and procedures for incident response Data sources to support an investigation Secure an environment with mitigation techniques or controls Key aspects of digital forensics Governance, Risk, and Compliance Various types of controls Regulations, standards, or frameworks that impact organizational security posture Organizational security policies Risk management processes and concepts Privacy and sensitive data concepts Ethical concerns in security </ ol>

Lab Content

Classify how applications, devices, and protocols relate to the OSI model Identify common TCP and UDP default ports Use appropriate software tools to troubleshoot connectivity issues Conduct network monitoring to identify performance and connectivity issues Install and configure a basic firewall Use appropriate software tools to troubleshoot connectivity

Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)
- Lab (04)
- DE Live Online Lab (04S)
- DE Online Lab (04X)

Instructional Techniques

This course will utilize a combination of lecture, remote virtual machine lab assignments, classroom discussion with student interactions, problem-solving techniques, quizzes, exams, and troubleshooting assignments to achieve the goals and objectives of this course. All instructional methods are consistent across all modalities.

Reading Assignments

Read textbook and research the secure configuration and management of common network devices. Read materials about how to properly maintain security documentation. Read materials and textbook to learn about computer security best practices.

Writing Assignments

Complete documentation of the purpose of default ports. Explain the security concerns associated with various types of vulnerabilities. Identify appropriate security policies and best practices for network security.

Out-of-class Assignments

Complete hands-on lab assignments to setup and configure a secure network. Complete hands-on lab assignments to install and configure a basic firewall. Research based on a given scenario to find a solution using the troubleshooting methodology.

Demonstration of Critical Thinking

Students will write lab reports based on the instructions provided in the remote lab environment to demonstrate the application of critical thinking for enterprise security solutions.

Required Writing, Problem Solving, Skills Demonstration

Configure various network security software tools. Use remote lab environment to demonstrate mitigation techniques to secure a computer network environment.

Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelor's degree and two years of professional experience, or any associate degree and six years of professional experience. Computer service technology: Any bachelor's degree and two years of professional experience, or any associate degree and six years of professional experience.

Textbooks Resources

1. Required Ciampa, M. Security+ Guide to Network Security Fundamentals, 7th ed. Cengage Learning, 2021

Other Resources

1. Coastline Library 2. IT white papers are available at no charge to all IT students through the Microsoft IT Academy website. 3. OER Materials