COURSE DESCRIPTION:

Prerequisites: SEC 160
Corequisites: None

This course introduces students to the concepts of defense-in-depth, a security industry best practice. Topics include firewalls, backup systems, redundant systems, disaster recovery, and incident handling. Upon completion, students should be able to plan effective information security defenses, backup systems, and disaster recovery procedures. This course is restricted to the Information Systems Security, the Information Systems Security/Operating Systems, and the Information Systems Security/Security Hardware curriculums. Course Hours Per Week: Class, 2. Lab, 2. Semester Hours Credit, 3.

LEARNING OUTCOMES:

Upon completion of this course, students will be able to:

a. Explain and implement network defense fundamentals
b. Design security policies with inclusion of risk analysis
c. Implement security policies on Windows platform
d. Design, apply, and search network traffic signatures
e. Design and create virtual private networks (VPN)
f. Explain and implement intrusion detection systems
g. Outline and plan security incident response
h. Choose, design, and implement firewalls using appropriate topology
i. Strengthen and manage firewalls

OUTLINE OF INSTRUCTION:

I. Network Defense Fundamentals
   a. TCP/IP networking review
   b. Network security threats overview
   c. Goals of network security
   d. Using defense technologies in layers

II. Risk Analysis
   a. Fundamental concepts of risk analysis
   b. Approaches and process of risk analysis
   c. Deciding how to minimize risk
III. Security Policy Implementation
   a. Security policy best practices
   b. Seven steps for a security policy and their components
   c. Ongoing risk analysis

IV. Network Traffic Signatures
   a. Signature analysis
   b. Detecting traffic signatures
   c. Identifying suspicious events
   d. Common Vulnerability and Exposures (CVE) standards

V. Virtual Private Network Concepts and Implementation
   a. VPN concepts and purpose
   b. Encapsulation protocols
   c. Encryption protocols
   d. Authentication protocols
   e. Advantages / disadvantages
   f. Design a VPN
   g. Configure a VPN
   h. Firewall configuration for VPN traffic
   i. Auditing VPN and firewall rules

VI. Intrusion Detection Concepts
   a. Components of IDS
   b. Seven steps of implementation and monitoring
   c. Host- and network-based IDS
   d. Implementing and evaluating IDS

VII. Incident Response to Intrusion
   a. Developing and modifying filter rules
   b. Security Incident Response Team (SIRT)
   c. Six step response to incidents
   d. False positive, false negative, true negative, true positive
   e. Handling legitimate security alerts

VIII. Choosing and Designing Firewalls and Topologies
   a. Overview of packet filtering firewalls
   b. Stateful versus stateless firewalls
   c. Software versus hardware firewalls
   d. Creating rule bases that implement policies
   e. Appropriate firewall configurations
   f. Network perimeter security
   g. Bastion hosts, proxy servers
   h. Network Address Translation (NAT)
   i. User authentication
IX. Strengthen and Manage Firewalls
   a. Editing rule bases
   b. Managing logs
   c. Improving performance
   d. Implementation of multiple firewalls

X. Ongoing Defense
   a. Security event management
   b. Security auditing
   c. Managing an IDS
   d. Adding security layers
   e. Keeping pace with network growth
   f. Maintain your knowledge base

REQUIRED TEXTBOOK AND MATERIALS:

Text to be assigned by the instructor each semester

STATEMENT FOR STUDENTS WITH DISABILITIES:

Students who require academic accommodations due to any physical, psychological, or learning disability are encouraged to request assistance from a disability services counselor within the first two weeks of class. Likewise, students who potentially require emergency medical attention due to any chronic health condition are encouraged to disclose this information to a disability services counselor within the first two weeks of class. Counselors can be contacted by calling 919-536-7207, ext. 1413 or by visiting the Student Development Office in the Phail Wynn Jr. Student Services Center, room 1209.