SEC 210
INTRUSION DETECTION

COURSE DESCRIPTION:

Prerequisites: None
Corequisites: None

This course introduces the student to intrusion detection methods in use today. Topics include the types of intrusion detection products, traffic analysis, and planning and placement of intrusion detection solutions. Upon completion, students should be able to plan and implement intrusion detection solution for networks and host-based systems.
Course Hours Per Week: Class, 2. Lab, 2. Semester Hours Credit, 3.

LEARNING OUTCOMES:

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

a. Explain network traffic fundamentals
b. Define components and types of intrusion detection
c. Compare intrusion detection vs. intrusion prevention systems (IDS & IPS)
d. Explain and implement network and host intrusion detection systems
e. Design and apply network traffic signatures
f. Define and discuss effective of honeypots and honeynets
g. Integrate IDS/IPS devices into network and firewall design
h. Analyze logging data to locate intrusion patterns
i. Classify and respond to network intrusion incidents
j. Develop and document appropriate response to intrusion

OUTLINE OF INSTRUCTION:

I. Networking review
   a. TCP/IP fundamentals
   b. Transport layer protocols and ports
   c. Segmentation and reassembly
   d. IP and ICMP
   e. Network exploits and targets
   f. Traffic capture and analysis
   g. Port scanning

II. Intrusion Detection Concepts
   a. Components of IDS
   b. Steps of implementation and monitoring
   c. Host- and network-based IDS
   d. Implementing and evaluating IDS
   e. Intrusion detection versus intrusion prevention

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

IV. Snort Implementation
   a. Architecture overview
   b. Windows capturing and filtering
   c. Linux capturing and filtering
   d. Rules format and creation
   e. Log analysis and correlation

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

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.