COURSE DESCRIPTION:

Prerequisites: None
Corequisites: None

This course provides an overview of security administration and fundamentals of designing security architectures. Topics include networking technologies, TCP/IP concepts, protocols, network traffic analysis, monitoring, and security best practices. Upon completion, students should be able to identify normal network traffic using network analysis tools and design basic security defenses. Course material will focus on securing Operating Systems. Course material will focus on securing Operating Systems. Course Hours Per Week: Class, 2. Lab, 2. Semester Hours Credit, 3.

LEARNING OUTCOMES:

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

1. Participate effectively in class. This objective ensures that a student gets as much as possible from the class. Independent work, Group assignments, active question and answer participation, and performing assigned reading are all part of this objective.
2. Demonstrate methods for keeping networks and their computers secure. This objective is central to showing understanding of the facilities for securing networks, including protection against viruses, worms, malware, and OS and application exploits. Network topology, host- and network-based firewalls, patches, authentication and encryption, and policy enforcement are all methods that can use used to demonstrate comprehension. Benefits of virtual machines will also be integrated.
3. Implement secure access through authentication and encryption. This objective shows special interest in remote access to resources, and the difference between public network and private ones. Cryptographic protocols will be discussed, as well as PKI certificate usage, password / token policy enforcement, VPN and VLANs, and IPsec.
4. Implement security policies. Policies will have been developed in a previous course, but they can sometimes be theoretical. This objective is designed with a focus on implementation – what policies can be enforced with respect to access methods, available resources, time and date restrictions, data management, and data classification or level of access.
5. Provide common application security. Specific issues with common applications (especially network-based applications) are dealt with in this objective. DNS, SMTP, HTTP, Instant Messaging, and other user- and system-accessible protocols with their implementation or protocol design weaknesses will be addressed and evaluated.
6. Ensure continuing security. This objective makes the assumption that any created network system, even if well designed, can never be assumed to be secure. Detection of active attacks through network traffic analysis, system and application log monitoring, and
auditing procedures are the approaches used for this objective. Also implied in this objective is that waiting for something to break is a bad idea – tracking the warning signs of a problem or attack is just as important.

7. Ensure continuity. Disaster planning and recovery issues will be dealt with via this objective. Redundancy (for systems and data), fault tolerance, power and environmental conditioning, backups, recovery strategies, and clustering will be available options for demonstrating facility with this topic.

8. Troubleshoot security vulnerabilities. This objective is a comprehensive look at synthesizing information and methods from the entire course. Specifically, this course lays the groundwork for penetration testing, by having students look for and identify weaknesses in configurations for operating systems, applications, firewalls, network devices, policies, and procedures in a given environment.

OUTLINE OF INSTRUCTION:

I. Securing Network and Computers
   a. Types of attacks – malware, DoS, spoofing, OS and application exploits
   b. Securing the network
   c. Securing the operating system

II. Authentication and Encryption
   a. Encryption methods
   b. Authentication methods
   c. VLANs and VPNs
   d. Certificates and PKI

III. Implementing Security Policies – implementation in Windows and Linux
   a. User and group account access policies
   b. Creating and naming user, group, and computer accounts
   c. Strong and effective password policies and templates

IV. Shared Resource Security – implementation in Windows and Linux
   a. File system rights
   b. Resource sharing
   c. Group security management
   d. Network Access Control

V. Firewall and Border Security – implementation in Windows and Linux
   a. TCP/IP protocols
   b. Packet filtering and firewalls
   c. NAT configuration

VI. Physical Network security
   a. Securing workstations and servers
   b. Securing media and topologies
   c. Structured design and VLANs
VII. Wireless Security
   a. Attacks on wireless physical and datalink layers
   b. Wireless security measures
   c. Configuration of wireless interfaces

VIII. Network application security
   a. SSL – Email, Web
   b. Authenticated connections for file transfer
   c. DNS, DHCP
   d. Remote access and VPN

IX. Email Security
   a. Email basics
   b. Message encryption with PGP/GPG and S/MIME

X. Monitoring, Auditing, and Network Analysis
   a. Intrusion Detection
   b. Audit Trails and Log Files
   c. Network Traffic Capture and Analysis

XI. Disaster Planning and Recovery
   a. UPS and AC – power and environmental conditioning
   b. RAID
   c. Hardware redundancy and clusters
   d. Data availability and backup

XII. Monitoring and Auditing
   a. Intrusion detection – active, passive, host, and network
   b. Creating audit trails and logging
   c. Monitoring active users
   d. Network monitoring and scanning

REQUIRED TEXTBOOKS AND MATERIALS:

Assigned by Instructor

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.