

Date Adopted: January 2005

Date Reviewed: August 2009

Date Revised: August 2009

## **CIS 280      Network Security**

### **I. CIS 280 Network Security – 3 Semester Hours**

#### **II. Course Description**

This course provides a study of threats to network security and methods of securing a computer network from such threats. Topics included in this course are security risks, intrusion detection, and methods of securing authentication, network access, remote access, Web access, and wired and wireless network communications. Upon completion, students will be able to identify security risks and appropriate counter measures.

#### **III. Prerequisite**

CIS 277 and CIS 278

#### **IV. Textbook**

Textbook:      70-236: Microsoft Exchange Server 2007 Configuration Package with Virtual Lab  
                    70-236 Set

Publisher:      Wiley

Author:         Microsoft Office Academic Course

#### **V. Course Objectives**

1. Identify threats to network security and detect intrusion.
2. Identify methods of securing network authentication, network access, remote access, and Web access.
3. Identify methods of securing network communications.

#### **VI. Course Outline of Topics**

1. Identify threats to network security and detect intrusion.
  - a. Network security terms and concepts
  - b. Risks associated with authentication
    - i. Authentication protocols
    - ii. Certificates
    - iii. Usernames and Passwords
    - iv. Biometrics
  - c. Risks associated with services, protocols, and the network infrastructure
    - i. Services
    - ii. Protocols
    - iii. Network infrastructure
  - d. Network intrusion methods
    - i. DOS / DDOS (Denial of Service / Distributed Denial of Service)
    - ii. Back Door
    - iii. Spoofing
    - iv. Man in the Middle
    - v. Replay
    - vi. TCP/IP Hijacking
    - vii. Weak Keys
    - viii. Mathematical
    - ix. Social Engineering
    - x. Password Guessing
    - xi. Brute Force

- xii. Dictionary
    - xiii. Software Exploitation
  - e. Risks associated with malicious code
    - i. Viruses
    - ii. Trojan Horses
    - iii. Logic Bombs
    - iv. Worms
  - f. Auditing, logging, and system scanning
- 2. Identify methods of securing network authentication, network access, remote access, and Web access.
  - a. Securing authentication
  - b. Firewalls
  - c. Public Key Infrastructure (PKI)
    - i. Certificate authority
    - ii. Digital certificates
  - d. Remote access technologies
    - i. Virtual private networks (VPN)
    - ii. RADIUS (Remote Authentication Dial-In User Service)
    - iii. IPSEC (Internet Protocol Security)
    - iv. L2TP
    - v. PPTP
  - e. Internet security concepts and protocols
    - i. Secure Sockets Layer (SSL)
    - ii. Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS)
    - iii. Pretty Good Privacy (PGP)
    - iv. Secure Multipurpose Internet Mail Extension (S/MIME)
- 3. Identify methods of securing network communications.
  - a. Physical network infrastructure security
  - b. Establishing security policies
  - c. Data encryption
  - d. Securing wireless communication
  - e. File and folder level security
    - i. Sharing
    - ii. File system security
  - f. Hardening
    - i. Updates
      - 1. Hotfixes
      - 2. Service Packs
      - 3. Patches
      - 4. Firmware
    - ii. Securing servers
    - iii. Securing clients
  - g. System backup

## VII. Evaluation and Assessment

Evaluation and assessment will be determined by the instructor and specified on the instructor's class syllabus. Grades will be based upon following scale: A = 90 – 100%, B = 80 – 89%, C = 70 – 79%, D = 60 – 69%, and F = below 60%.

## VIII. Attendance

Students are expected to attend all classes for which they are registered. Students who are unable to attend class regularly, regardless of the reason or circumstance, should withdraw from that class before poor attendance interferes with the student's ability to achieve the objectives required in the course. Withdrawal from class can affect eligibility for federal financial aid.

### **IX. Statement on Discrimination/Harassment**

The College and the Alabama State Board of Education are committed to providing both employment and educational environments free of harassment or discrimination related to an individual's race, color, gender, religion, national origin, age, or disability. Such harassment is a violation of State Board of Education policy. Any practice or behavior that constitutes harassment or discrimination will not be tolerated.

### **X. Americans with Disabilities**

The Rehabilitation Act of 1973 (Section 504) and the Americans with Disabilities Act of 1990 state that qualified students with disabilities who meet the essential functions and academic requirements are entitled to reasonable accommodations. It is the student's responsibility to provide appropriate disability documentation to the College. The ADA Accommodations Office is in FSC 305 (205-856-7731).