

COURSE OUTLINE

CMSY-162

Introduction to Network Security Systems

3 Credit Hours

HOWARD COMMUNITY COLLEGE

Description

This course is designed to introduce students to the fundamentals of network security in preparation for advanced courses. It will give students a solid foundation for understanding different security technologies and how they function. They will also be able to design a basic network with the proper network security structures in place. This course is designed as an entry-level, Information Assurance class, but it is highly recommended that students have a background in computer and network administration. After taking this course, students should be prepared to take the CompTIA Security+ exam. A good understanding of the Windows and Linux operating system, and TCP/IP protocol, or an extensive background in network administration is highly recommended. (3 hours lecture, 1 hour lab)

For a more detailed course description, objectives, and outline please visit our website at the following link:

http://www.howardcc.edu/academics/academic_divisions/business_and_computers/instructional/network/CMSY162.html

Overall Course Objectives

Upon completion of this course, the student will be able to:

- 1) Identify and illustrate the three concepts in protecting data:
 - Data Confidentiality
 - Data Availability
 - Data Integrity
- 2) Describe the seven layers of the OSI model for network protocols
- 3) Demonstrate the ability to subnet networks
- 4) Identify which layer of the OSI model TCP/IP protocols fall into
- 5) Determine where network security technologies fit within a network including:
 - Access Control Lists
 - Firewalls
 - VPN's
 - Intrusion Detection Systems
 - Authentication Systems (PKI, Biometrics)
 - Encryption
- 6) Design a basic network diagram with security structures properly in place.

Major Topics

- I. TCP/IP Protocol
 - a. IP Numbering and sub-netting
 - b. TCP and UDP identification
 - c. Parts of an IP packet

- II. Network Policy
 - a. User Acceptance Agreement
 - b. Security Policies defined
 - c. Auditing / Logging
 - d. Password policies
 - e. Content Filtering
- III. Firewalls
 - a. History of firewalls
 - b. ACL's and how they function
 - c. Proxy vs. Packet filter firewalls
 - d. Stateful Inspection defined
 - e. Personal Firewalls
- IV. Encryption
 - a. Types of encryption
 - b. Define when you should use encryption, and why
- V. IDS
 - a. Define IDS
 - b. Show what an IDS does, and how it does it
 - c. Define where in a network you should place IDS
- VI. VPN's
 - a. Describe VPN's and how they function
 - b. Show the benefits and limitations of VPN technology
- VII. Authentication Systems
 - a. Password systems
 - b. Biometrics
 - c. Token Based
- VIII. Disaster Recovery & Backup Systems
 - a. System Backups
 - b. Hot/Warm Sites

Course Requirements

Grading/Exams/Projects: Students will be introduced to tools and methodology that will help with later courses and should have a computer available. Grading will be based on exams and at least two projects, designed to test the ability of the student to structure a network with the correct network security technologies in place.