

# COURSE OUTLINE

**CMSY-163**

**Introduction to Firewalls and Network Security**

**3 Credit Hours**

## **HOWARD COMMUNITY COLLEGE**

### **Description**

This course is designed to give students experience with firewall hardware and software. Different firewall systems will be illustrated, and students will be given the opportunity to install and configure them. The course is designed with a network administrator in mind. An extensive background in network administration, or a computer professional with an MCSE or equivalent would have adequate background knowledge for waiver. Prerequisites: CMSY-162. (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/CMSY163.html](http://www.howardcc.edu/academics/academic_divisions/business_and_computers/instructional/network/CMSY163.html)

### **Overall Course Objectives**

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

- 1) Describe the characteristics of TCP and UDP packets
- 2) Describe ingress and egress filtering and when to use each
- 3) Describe what a packet filter is, and how it functions
- 4) Describe what a proxy is, and how it functions
- 5) Describe what stateful inspection is, and how it functions
- 6) Compare and contrast packet filters, proxies, and stateful inspection
- 7) Identify the differences between normal and attacking traffic on a firewall
- 8) Setup and configure a firewall for proper outgoing and incoming policies
- 9) Determine the limitations of firewall technology, and define when other security measures need to be in place

### **Major Topics**

- I. TCP/IP Protocol
  - a. Identify TCP/IP protocols such as IPSec, TCP, & UDP
  - b. Determine applications via port numbers
  - c. Identify attacks as opposed to valid traffic
- II. Packet Filtering
  - a. Define access control lists
  - b. Create and implement access control lists
- III. Proxy Firewalls
  - a. Define a proxy
  - b. Show how proxies function in relation to packets
  - c. Create and implement a proxy firewall system
- IV. Stateful Inspection
  - a. Define stateful inspection
  - b. Show how stateful inspection speeds up packet analysis

- V. Personal Firewalls
  - a. Show how a personal firewall functions differently from a border firewall
  - b. Implement a personal firewall on local systems and configure properly
- VI. Logging and Auditing
  - a. Implement logging features of firewalls to get information regarding traffic
  - b. Show various attacks on firewalls systems and identify
  - c. Show blocked access of valid traffic, and determine how to identify allowed traffic
- VII. Firewall Limitations
  - a. Define the limitations of firewall technology
  - b. Show where other security measures such as anti-virus and IDS need to be implemented

### **Course Requirements**

**Grading/Exams/Projects** This course will feature more extensive hand-on labs and configuration of network systems. Students will be exposed various firewall systems and expected to be able to set them up properly. Grading will be based upon a combination of exams and labs. The labs will be hands-on system configuration with the students having to properly configure and implement a firewall system.