

**COURSE OUTLINE**  
**CMSY-164**  
**Introduction to Intrusion Detection Systems**  
**3 Credit Hours**

**HOWARD COMMUNITY COLLEGE**

**Description**

From this introduction to intrusion detection systems, students will develop a solid foundation for understanding IDS and how they function. This course will give students a background in the technology of detecting network attacks. It will introduce all the concepts and procedures used for IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems). Students will have hands-on experience with implementing and configuring software and hardware based IDS in a network infrastructure. This course is designed with a network administrator in mind. A fairly extensive background in network administration, or a computer professional with an MCSE or equivalent would have adequate background knowledge for waiver. Prerequisites: CMSY-162 or CMSY-163 (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/CMSY164.html](http://www.howardcc.edu/academics/academic_divisions/business_and_computers/instructional/network/CMSY164.html)

**Overall Course Objectives**

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

1. Define what an IDS is and how it functions.
2. Determine where IDS should be placed in a network.
3. Employ a packet sniffer and identify the critical parts of a TCP/IP packet.
4. Identify attack signatures and relate them to specific attacks.
5. Identify false-positives and false-negatives, and have the ability to determine what causes them.
6. Define and identify the different types of IDS including:
  - Host based IDS
  - Network based IDS
  - Hybrid IDS.
7. Build and implement an open-source IDS system.

**Major Topics**

- I. IDS systems
  - a. Describe host and network based IDS, and hybrid systems
  - b. Introduce different IDS systems and how they function
  - c. Compare host vs. network based IDS, and when to deploy them
- II. TCP/IP
  - a. Introduce packet sniffing
  - b. Describe a TCP/IP packet, and isolate the critical parts of a packet
  - c. Show how IDS systems function similar to a packet sniffer
- III. Security technology
  - a. Show where different technologies fit within a secure network
  - b. Determine where an IDS system should be within the structure
- IV. Attacks
  - a. Describe the type of attacks that may occur on critical systems
  - b. Show how attacks may breach other network security devices
- V. Attack signatures

- a. Introduce attack signatures, and how they are structured to determine an attack
  - b. Compare an attack signature to packets captured via a sniffer
  - c. Describe and write custom attack signatures to capture specific traffic
- VI. False Positives / False Negatives
- a. Define the terms for IDS understanding
  - b. Show how to limit the level of false positives and negatives
  - c. Learn how to determine if a packet indicates a false positive, or a true attack
- VII. Alerting & Attack Response
- a. Learn how an IDS alerts when attacked
  - b. Determine how to structure alerts so that an admin is not overwhelmed
  - c. Discuss the differences between alerting and logging
  - d. Show incident procedures, and what should be done when an attack is occurring or has occurred.
- VIII. Passive IDS / Active IDS
- a. Compare a IDS system that interacts with security policy, and one that does not
  - b. Show why it is often recommended that IDS work as a passive device
  - c. Show upcoming technology that will allow for more active devices
- IX. IDS Implementation
- a. Install, configure, and manage an IDS system
  - b. Simulate attacks on the system, eval data to determine correct actions, and respond accordingly
  - c. Adjust the system for functionality on different parts of the network

### **Course Requirements**

Grading/exams/projects: Grading procedures will be determined by the individual faculty member but will include the following:

This course is more advanced than an introductory course. It will have much more extensive hands-on labs and configuration of network systems. During the course, the students will be exposed to IDS and be expected to be able to set it 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 working IDS.