

Common Course Outline
DCOM 212
Introduction to Intrusion Detection/Prevention Systems
4 Semester Hours

The Community College of Baltimore County

Description

DCOM 212 – 4 Credits – Introduction to Intrusion Detection/Prevention Systems provides students with a thorough introduction to both software- and hardware-based IDSes and IPSes. This class combines the theoretical concepts and hands-on skills needed to design, implement, and administer both IDSes and IPSes.

4 credits; 4 lecture hours per week

Prerequisite: DCOM 211 or consent of the program coordinator

Overall Course Objectives

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

1. identify and classify different IDSes and IPSes;
2. define the pros and cons for host- and network-based IDSes and IPSes;
3. design an IDS/IPS in a working network;
4. install and configure working software- and hardware-based network IDSes;
5. install and configure working software- and hardware-based network IPSes;
6. dissect Transmission Control Protocol (TCP)/Internet Protocol (IP) suite packets;
7. identify false positives and false negatives;
8. utilize network diagrams; and
9. demonstrate appropriate and ethical behavior and good work habits.

Major Topics

- I. Network-based IDS/IPS solutions
- II. TCP, IP, and ICMP concepts
- III. Examining embedded protocol header fields
- IV. Introduction to TCPdump and packet dissection using TCPdump
- V. Fragmentation
- VI. Stimulus and response
- VII. Domain Name System (DNS)
- VIII. Introduction to filters and signatures
- IX. Architectural issues
- X. Interoperability and correlation

- XI. Organizational issues
- XII. Automated and manual response
- XIII. Business case for IDS/IPS
- XIV. Future directions

Course Requirements

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

Minimum of five laboratory projects

Minimum of three exams

Writing: The individual faculty member will determine specific writing assignments, such as an Acceptable Usage Policy.

Other Course Information

Individual faculty members may include additional course objectives, major topics, and other course requirements to the minimum expectations stated in the Common Course Outline.