

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 grounding in the design, implementation, and administration of Intrusion Detection/Prevention Systems (IDSes/IPSes), as well as practical, hands-on experience working with these systems. In addition, students analyze various attack signatures and the network traffic these systems collect.

Prerequisite: DCOM 252 or consent of the program coordinator

Overall Course Objectives

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

1. differentiate between host-based and network-based IDS/IPS solutions;
2. design, install, and configure a network-based IDS in a working network;
3. dissect and analyze various types of normal and unusual traffic;
4. tune the IDS for optimal performance;
5. utilize network diagrams; and
6. demonstrate ethical behavior appropriate to security-related technologies.

Major Topics

- I. Introduction to Network Security Monitoring (NSM)
- II. Network- and host-based IDS/IPS solutions
- III. Dissecting packets using Wireshark
- IV. Examining normal and unusual protocol traffic
- V. Working with filters/rules for network monitoring
- VI. Analyzing and deconstructing various attack signatures
- VII. Security-related ethics

Course Requirements

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

Minimum of six 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

This course is a program requirement for the Network Technology Security degree.
This course is taught in a computerized environment.

Date Revised: 05/17/09