Common Course Outline
DCOM 212
Introduction to Intrusion Detection/Prevention Systems
3 Credits

Community College of Baltimore County

Description

DCOM 212 – Introduction to Intrusion Detection/Prevention Systems provides students with the foundational information and skills required to design, implement, and administer Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS). Students use IDS/IPS to capture and analyze network traffic and detect various attack signatures.

3 Credits

Prerequisite: DCOM 211

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/IPS for optimal performance;
5. utilize network diagrams; and
6. describe 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 procedures will be determined by the individual faculty member but will include the following:

Grading/exams

- A minimum of six laboratory projects
- A minimum of six quizzes
- A minimum of two exams

Written Assignments: Students are required to use appropriate academic resources.

Other Course Information

This course is a program requirement for the Information Systems Security degree.

Date Revised: 02/05/2019