Common Course Outline
DCOM 261
Network Defense and Countermeasures
4 Semester Hours

The Community College of Baltimore County

Description

Network Defense and Countermeasures focuses on one of the most important and urgent concepts in computing – intrusion detection. Intrusion detection encompasses virtually all aspects of network security: performing risk analyses, writing security policies, assessing damage, responding to an intrusion(s), anticipating future attacks, and prosecuting intruders.

Network Defense and Countermeasures is intended for students and professionals who need hands-on introductory experience installing firewalls and intrusion detection systems. The course requires familiarity with the Internet and basic networking concepts such as TCP/IP, gateways, routers, and Ethernet. This course is taught in a combination lecture and hands-on format.

4 credits; 4 lecture hours; 0 laboratory hours required.

Prerequisite: DCOM 258 or consent of Program Director

Overall Course Objectives

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

1. articulate the reasons for developing a network security program;
2. design a network defense structure;
3. work with network security tools used to block intruder threats, such as packet filters, anti-virus software, log files and software to analyze them, and Intrusion Detection Systems (IDS);
4. perform a comprehensive risk analysis and risk assessment in regard to computer resources and security;
5. develop a security policy;
6. evaluate, design, configure, and manage a firewall;
7. establish a Virtual Private Network (VPN);
8. evaluate some of the most popular IDS packages available;
9. examine different types of intrusion detection signatures;
10. capture and analyze packets;
11. demonstrate the administration and ongoing support required for securing networks;
12. utilize network diagrams;
13. demonstrate appropriate and ethical behavior and good work habits; and
14. gain a working vocabulary of technical terms used by network security professionals.

Major Topics

-Introduction to class

I. Foundations of network security;
II. Designing a networking defense;
III. Risk analysis;
IV. Security policy design;
V. Choosing, designing, and configuring firewalls;
VI. Strengthening and managing firewalls;
VII. Virtual Private Networks (VPNs);
VIII. Intrusion detection; and
IX. Ongoing management.

Course Requirements

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

1. Minimum of 10 hands-on projects
2. Minimum of 3 tests (including comprehensive final exam)

Other Course Information

This course is taught in a computerized environment.
This course is the second course in a four-course sequence.

The Community College of Baltimore County is committed to providing a high-quality learning experience that results in knowledge, attitudes, and skills necessary to function successfully as a transfer student, in a career and as a citizen. To accomplish this goal, we maintain high academic standards and expect students to accept responsibility for their individual growth by attending classes, completing all homework and other assignments, participating in class activities and preparing for tests.

We take seriously our responsibility to maintain high-quality programs and will periodically ask you to participate in assessment activities to determine whether our students are attaining the knowledge, attitudes, and skills appropriate to various courses and programs. The assessment activities may take many forms such as surveys, standardized or faculty-developed tests, discussion groups or portfolio evaluations. We ask that you take these activities seriously so that we can obtain valid data to use for the continuous improvements of CCBC's courses and programs.

Date Revised: 01/21/04