

Common Course Outline
DCOM 214
Operating Systems Security
4 Semester Hours

The Community College of Baltimore County

Description

DCOM 214 – 4 Credits – Operating Systems Security provides students with the hands-on skills needed to protect networks from the inside-out by focusing on Linux and Windows system hardening. The class is designed to help students prepare for professional careers in the information and communication technology (ICT) field and the Security Certified Network Professional (SCNP) certification exam.

Prerequisite: CINS 142 or consent of the program coordinator

Overall Course Objectives

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

1. describe the core concepts of cryptography, especially as they relate to information security;
2. utilize information security tools to harden systems;
3. harden Red Hat Enterprise Linux (RHEL) systems;
4. harden Windows Server 2003 systems;
5. perform a risk analysis on a simulated network;
6. create a security policy for a fictitious company;
7. analyze traffic using Wireshark, and
8. demonstrate ethical behavior appropriate to security-related technologies.

Major Topics

- I. Cryptography and data security
- II. Ethical hacking tools and techniques
- III. Hardening Linux and Windows systems
- IV. Security on the Internet and the WWW
- V. Risk analysis
- VI. Information security policies and procedures
- VII. Traffic analysis

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