

## SEC 220 Defense-In-Depth

Credit Hours	Lecture Hours	Lab Hours	Prerequisite or Corequisite
3	2	2	SEC 160 and SEC 210

### CATALOG DESCRIPTION

This course introduces students to the concepts of defense in-depth, a security industry best practice. Topics include firewalls, backup systems, redundant systems, disaster recovery, and incident handling. Upon completion, students should be able to plan effective information security defenses, backup systems, and disaster recovery procedures.

### REQUIRED RESOURCES

#### Textbook(s)

Guide to Network Defense and Countermeasures by Greg Holden, Course Technology

#### Materials

#### Technology

none

### LEARNING OBJECTIVES

- 1 Develop skills needed to prevent system attacks.
- 2 Develop skills to identify specific attack types and reasons why the attack is possible, and how to stop or avoid these attacks.
- 3 Develop skills to control packet flow into and out of a network
- 4 Be able to implement a layered defense approach
- 5 Be able to utilize learnt skills both Linux and Windows systems in conjunction to provide security to a network or device
- 6 Be able to effectively monitor a potential system and respond to threats.
- 7 Setup and maintain a replicated production server.

### COURSE DELIVERY METHODS

If this course is taught as an online, hybrid, or web enhanced course; the course will require access to the PCC Blackboard learning system via the Internet. Students are expected to login to the Blackboard course **AT LEAST 3 times per week**. Students are also expected to use the PCC Campus Cruiser web mail system to correspond with the instructor and **check email at least once every 24 hours Monday – Friday**.

### COURSE SPECIFIC INFORMATION

**Complete syllabus** with due dates, attendance policies, and other information is provided by the instructor for the course.

*Last Updated July, 2007*