HPC INTRUSION DETECTION & COUNTER MEASURES
HPC 2007

Class Hours: 3.0  Credit Hours: 4.0
Laboratory Hours: 3.0  Date Revised: spring 03

NOTE: This course is not designed for transfer credit.

Catalog Course Description:

This course is a practical, comprehensive solution to designing, deploying, and maintaining network defenses for the HPC clusters. It discusses perimeter components, such as firewalls, VPNs, routers, and intrusion detection systems, and it explains how to integrate them into a unified whole to meet real-world business requirements.

Entry Level Standards:

College level reading and math skills; keyboarding skills of at least 20 wpm; familiarity with HPC architecture and related internetworking issues; problem solving and analytical skills also important.

Prerequisites:

HPC 1010 (NETW 2530) or consent of instructor

Textbook(s) and Other Reference Materials Basic to the Course:


I. Week/Unit/Topic Basis:

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Perimeter and Security Fundamentals</td>
</tr>
<tr>
<td>2</td>
<td>Packet Filtering and Stateful Firewalls</td>
</tr>
<tr>
<td>3</td>
<td>Proxy Firewalls</td>
</tr>
<tr>
<td>4</td>
<td>Security Policy</td>
</tr>
<tr>
<td>5</td>
<td>Extending the Perimeter</td>
</tr>
<tr>
<td>6</td>
<td>The Role of a Router</td>
</tr>
<tr>
<td>7</td>
<td>Network Intrusion Detection</td>
</tr>
<tr>
<td>8</td>
<td>Virtual Private Networks</td>
</tr>
</tbody>
</table>
II. Course Objectives*

A. Develop a working understanding of the terminology and hardware devices associated with HPC intrusion detection. I, II, IV

B. Demonstrate basic fundamentals of HPC packet filtering security concepts. I, III

C. Demonstrate applied principles of installing, configuring, and managing perimeter security devices. I, II, III

D. Exhibit a knowledge of security threats and HPC VPN security systems. I, II, IV

E. Exhibit a knowledge of HPC log analysis security software. I, II, IV, V

F. Develop an understanding of the technologies to combat HPC troubleshooting security threats. II, IV, V

*Roman numerals after course objectives reference goals of the HPC program.

III. Instructional Processes*

Students will:

1. Use router security configuration utilities to perform practical tasks for secure High Performance Computing. Active Learning Strategy, Problem Solving and Decision Making Outcome, Technological Literacy Outcome, Information Literacy Outcome

2. Solve problems in perimeter computer security within HPC. Problem Solving and Decision Making Outcome, Information Literacy Outcome

3. Use professionally accepted methods and materials in completion of cluster defense components. Technological Literacy Outcome, Personal Development Outcome

4. Use the Internet as a medium for obtaining documentation and instruction. Information Literacy Outcome, Communication Outcome, Technological Literacy Outcome

5. Use the Computer-Based Training for obtaining instruction. Communication Outcome, Information Literacy Outcome, Transitional Strategy

6. Prepare, review, and study documents for distribution to all class members via E-mail. Personal Development Outcome, Communication Outcome, Problem Solving and Decision
Making Outcome, Technological Literacy Outcome, Information Literacy Outcome

7. Practice elements of the work ethic such as punctuality, professionalism, dependability, cooperation, and contribution. Personal Development Outcome

*Strategies and outcomes listed after instructional processes reference Pellissippi State’s goals for strengthening general education knowledge and skills, connecting coursework to experiences beyond the classroom, and encouraging students to take active and responsible roles in the educational process.

IV. Expectations for Student Performance*:

Upon successful completion of this course, the student should be able to:

1. Use terminology associated with intrusion detection fields as related to HPC architecture. A,B,C,D,E,F
2. Use perimeter security hardware, DOS. A,B,C,D,E
3. Log-on/boot-up, operate, communicate, and use HPC security lab system. A,B,D,E
4. Use internal and external security countermeasures. D
5. Prove proficiency in the creation of security models for host defense of the HPC cluster. B, D
6. Load and run software products and facilities available on the system. A,B,C,D,E,F
7. Transfer data files from one HPC cluster to another using VPN integration. C
8. Produce documentation of methods used to secure HPC clusters. B,C,D,E
9. Illustrate an understanding of host hardening, separating resources, and perimeter design. A, C, F

*Letters after performance expectations reference the course objectives listed above.

V. Evaluation:

A. Testing Procedures:

Twelve chapter exams each worth 100 points will be given. Pretests and post quizzes may be given. A group project will be required. Teamwork will count as 100 points.

B. Laboratory Expectations:

Hands-on learning activities done individually and in teams will also serve as the basis for course evaluation.

C. Field Work:

N/A

D. Other Evaluation Methods:

Other assessment activities worth 100 points each will consist of special projects, research papers, team activities, essays, short answer documents, or other work assigned.
E. Grading Scale:

90 - 100 % A  
80 - 89 %  B  
70 - 79 %  C  
60 - 69 %  D  
< 60 %  F

VI. Policies:

A. Attendance Policy:

Pellissippi State Technical Community College expects students to attend all scheduled required instructional activities. As a minimum, students in all courses MUST BE PRESENT for at least 75 percent of their scheduled class and laboratory meetings in order to receive credit for the course (Pellissippi State Catalog).