Course Title:
INF-273 Intrusion Detection and Prevention

Credits/Hours:
2 lecture, 2 lab, 3 credits

Prerequisite:
INF-160 OR INF-170 OR permission of Department Chair
Recommended corequisite: INF-267 (To be successful in this course, students should adhere to the recommendation.)

Course Description:
INF-273 Intrusion Detection and Prevention introduces the tools, methods and resources to help identify, assess and report unauthorized or unapproved network activity. Students will learn to analyze packets to find special patterns in network traffic, to monitor network traffic and to take action based on prescribed rules when an intrusion occurs. Students will configure Intrusion Prevention Systems / Intrusion Detection Systems, analyze results and prevent network intrusions. 2 lecture, 2 lab, 3 credits

Textbooks and Supplies:
See course outline

<table>
<thead>
<tr>
<th>Student Learning Objectives</th>
<th>Assessment Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Recognize unauthorized activity on the network</td>
<td>Written Exam</td>
</tr>
<tr>
<td></td>
<td>Lab Exam</td>
</tr>
<tr>
<td>2. Configure IDS/IPS to protect the network</td>
<td>Written Exam</td>
</tr>
<tr>
<td></td>
<td>Lab Exam</td>
</tr>
<tr>
<td>3. Use tools to detect network anomalies</td>
<td>Written Exam</td>
</tr>
<tr>
<td></td>
<td>Lab Exam</td>
</tr>
<tr>
<td>4. Respond to incidents of unauthorized intrusion</td>
<td>Written Exam</td>
</tr>
<tr>
<td></td>
<td>Lab Exam</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>College Competencies:</th>
<th>Student Learning Objective:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Technological and Information Fluency</td>
<td>1 – 4</td>
</tr>
<tr>
<td>2. Critical Thinking</td>
<td>1</td>
</tr>
<tr>
<td>3. Applied Knowledge</td>
<td>4</td>
</tr>
</tbody>
</table>

Course Content:
See course outline
Assessment:
An average of 60% from combined assessment measures is required to demonstrate proficiency in course material.

5 Exams 100%

Quizzes:
There may be several quizzes, each worth 10 points, given at the beginning pre-selected classes. The quiz material will be based upon the prior lectures and labs, homework, and/or the reading assignments. A quiz cannot be made up if missed. A student entering class late, after a quiz has begun, will not be entitled to extra time to complete the quiz. Students entering class after a quiz is completed will not be permitted to take the quiz and a zero grade will be assigned.

Testing:
Students are required to take examinations on the day and time they are scheduled. If special circumstances require a test schedule adjustment, this must be worked out in advance with the instructor. If a student misses an exam (except for prearranged circumstances with the instructor) a zero grade will be assigned.

The instructor can be reached by telephone (see course outline for appropriate phone number), e-mail, or a written note can be left in the Divisional Office (during the day) A-306C or in the Evening Office L-113. If there are extreme circumstances (documentation may be required) that prevent a student from taking a test or an exam according to the published schedule, the student should use one of the above options to contact the instructor before the next class. An arrangement for a special testing schedule is solely at the discretion of the instructor. A student who waits for the next class session to speak with the instructor will not be accommodated with a special test schedule.

It is the student’s responsibility to finish an examination correctly and completely. Therefore, when computer Scantron forms are used as answer sheets, the student must use a Number 2 lead pencil and erase all stray marks completely. The burden of proper erasure is at test taking time. Once the examinations are returned to the students, there will be no grade adjustments made due to inappropriate completion of the response form.

The use of electronic devices during exams is prohibited. Any student using an electronic device during an exam (unless directed to do so by the instructor) will receive a 0 for the exam.

Projects, Assignments, Laboratory Work:
Assignments are hands-on productions that show the instructor that the student understands concepts presented in class and in the readings and can competently use specified software to apply specific concepts.

It is anticipated that students will spend at least 4 hours per week perfecting their skills and completing their assignments. Some assignments are required for grading. They must be submitted on the assignment due date, and cannot be handed in late. Acceptance of late assignments is solely at the discretion of the instructor.

Some assignments are instructional and need not be submitted. However lab assignments that are correct and complete and submitted on-time will help students prepare for graded assignments, quizzes, and exams.

Homework:
In addition to any homework assignment given during class, it is a **standing assignment** that the student read each chapter of the book prior to its discussion. Following the class discussion, the student should reread the material and work with the exercises throughout the text. It is anticipated that students will spend at least 4-hours per week reading the text and working with the exercises and supplemental resources.

**Policies:**

- **Lateness** – The roll will be taken at the beginning of class. If the student is not in attendance at that time, he/she will be carried in the roll book as being absent unless the instructor is notified immediately after class. Attendance sheets cannot be adjusted at following class meetings.

- The student must adhere to all college polices. Due to the nature of this course, it is recommended that the student review the policy titled “Acceptable Information Technology Use at Bergen Community College”.

- The use of portable electronic devices such as pagers and cell phones is not permitted while class is in session. Please be sure to silence electronic devices before entering class.

- The use of audio CD or tape players, radios, and college computers to play music during class is prohibited.

- Students are expected to demonstrate listening, reading, note taking, and writing skills. The student will need to take notes during class discussions and understand and follow verbal and written directions. All assignments and correspondence with the instructor (including e-mail) must be well written in full sentence format. Proper paragraph format must be used for all postings to the student bulletin board (if applicable).

- The subject line of all e-mail correspondence to the instructor must contain the course number and section and student's name. Any e-mail received without this information will not be opened.

- Plagiarism in any form will be treated as a failure to complete an assignment. All work submitted should reflect individual effort by the student.

- In borderline cases that arise in almost every class each semester a student’s attendance, class participation, attitude, and observed effort will be considered in helping to determine the student’s final grade.

If the instructor does not appear after 20 minutes following the scheduled time, students should generate an attendance list. One volunteer member need deliver the list, containing the course title, date, and instructor’s name, to the Evening Office L-113 or to the Divisional Office (during the day) A-306C.

Additional policy and assessment information may be distributed by individual instructors.
# Intrusion Detection and Prevention

**Course Title:** INF-2xx  
**Instructor:**  
**Faculty Web-Site:**  
**E-mail:**  
**Telephone:**  
**Office:**  
**Office Hours:**

**Course Title:** Intrusion Detection and Prevention  
**Course Syllabus at** [http://www.bergen.edu/departments/business/inf/syllabi](http://www.bergen.edu/departments/business/inf/syllabi)  
**Course Web Site:** [http://dl.bergen.edu](http://dl.bergen.edu)

**Textbooks and Supplies:**  

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic*</th>
<th>Assignments*</th>
</tr>
</thead>
</table>
| 1    | Chap 1 Intrusion Detection  
Intrusion detection, Intrusion Prevention  
Analysis, Rule based detection, Profile based detection, Stealth  
Probes  
Heuristics |  |
| 2    | Chap 2 IP Protocol Suite  
OSI reference model – seven layers  
IP, TCP, UDP, ICMP, ARP, DNS |  |
| 3    | Chap 3 Unauthorized Activity  
ARP abuses, IP abuses, TCP abuses, UDP abuses  
**Exam 1** |  |
| 4    | Chap 4 Unauthorized Activity  
Memory buffer overflow  
Format string overflow  
Encrypted communication |  |
| 5    | Chap 5 TCP/IP Dump  
TCPSplice, TCPFlow, TCPJoin  
Command line options, expressions, bulk capture |  |
<table>
<thead>
<tr>
<th>Week</th>
<th>Topic*</th>
<th>Assignments*</th>
</tr>
</thead>
</table>
| 6    | Chap 6 IDS and IPS Architecture  
      | Tiered architecture  
      | Sensors, agents  
      | **Exam 2** |  |
| 7    | Chap 7 IDS and IPS Internals  
      | Packet capture, filtering, packet decoding  
      | Storage, fragment reassembly, stream reassembly  
      | Stateful inspection |  |
| 8    | Chap 8 Internet Security Systems Real Secure  
      | Configuring Real Secure  
      | Creating and Implementing Event Filters  
      | Reporting  
      | Signatures |  |
| 9    | Chap 9 Cisco Secure IDS  
      | Collecting requirements  
      | Defense  
      | Event viewer  
      | Network IDS  
      | Assigning packet capture to signatures  
      | **Exam 3** |  |
| 10   | Chap 10 SNORT  
      | SNORT Modes, sniffer  
      | Packet capture, detection  
      | File order  
      | Filters, Alerts |  |
| 11   | Chap 11 NFR Detection  
      | NER Sentivist Sensor  
      | Signatures  
      | Alerts and forensics |  |
| 12   | Chap 12 Data Correlation  
      | Data correlation definitions  
      | Data fusion, alert fusion  
      | Using statistical correlation  
      | Correlation coefficient  
      | Statistical inference  
<pre><code>  | **Lab Exam** |  |
</code></pre>
<p>| 13   | Chap 13 Incident Response |  |</p>
<table>
<thead>
<tr>
<th>Week</th>
<th>Topic*</th>
<th>Assignments*</th>
</tr>
</thead>
</table>
|      | Response types  
Response process  
Risk analysis  
Response methodology  
UDS and IPS incident response phases | | |
| 14   | Chap 14 Policies and Procedures  
IDS/IPS policy  
Standard, Baselines and procedures | | |
| 15   | **Final Exam** | | |

*Topics, quizzes, exams, and assignments may be modified due to time constraints*