Instructor: Dr. Eric Swedin
Office: DV137L (at Davis campus)
Office phone: 395-3553
E-mail: eswedin@weber.edu
Web site: http://www.swedin.org/
Office Hours: 3:00-5:30 Tuesday and Thursday
Other office hours are available by appointment.


**Class Description:**
In a computer-literate age, sophisticated criminals use computers in their illegal and destructive activities. This course discusses cyber crime and teaches students how to: recognize the patterns of an impending attack; detect attacks; set up a secure environment; and use tools to investigate cyber crime. Prerequisites: CJ 3130 and IS&T Core. Co-requisite: IS&T 3620.

Class participation and discussion are expected. While some lecture might be presented, for the most part, the class will focus on the discussion of the assigned topics and reading.

**Grading Policies:**
Grades will be determined on the following basis:

- Class Participation: 10%
- Class Presentations (2): 20%
- Class Project: 30%
- Mid-term Exam: 20%
- Final Exam: 20%

Grades:
- A: 90 - 100%
- B: 80 - 89%
- C: 70 - 79%
- D: 60 - 69%
- E: 0 - 59%

**Students with Disabilities:**
Any student requiring accommodations or services due to a disability must contact Services for Students with Disabilities (SSD) in Room 181 of the Student Service Center on the main campus. SSD can also arrange to provide materials (including this syllabus) in alternative formats if necessary.
Exam and Assignment Policy:
Exams can be taken early, with arranged permission. Questions on all the exams will come from text readings, class lectures, and lab assignments.

Cheating Policy:
Cheating and deceit are not accepted in the Goddard School of Business and Economics. *Cheating on an exam or assignment, or turning in someone else's work as your own, will result in an E for the class.* You may work together on your assignments, but you must turn in your own work. If you quote from a book, article, or web site, you must properly quote and cite your work. **Avoid even the appearance of cheating or plagiarism.**

Class Presentations:
Each student make two presentations in class on a bug/virus/worm or security problem. They will also write a two-page report on each presentation. These presentations should be specific rather than general, such as on a particular trojan horse rather than the concept of trojan horses. Each presentation should take about ten minutes. Students may not make more than one presentation a day, and cannot turn in presentations that they have not presented to the class.

Some useful sites to find known security problems/bugs/viruses/worms:
http://www.cert.org/ - CERT Coordination Center
http://www.vmyths.com/ - Vmyths.com - Truth About Virus Myths/Hoaxes
http://www.nipc.gov/ - National Infrastructure Protection Center (FBI)
http://hackingtruths.box.sk/ - Hacking Truths
http://www.wildlist.org/ - The WildList Organization International

Students in the past have made presentations on: instant messaging security, hacking the Playstation 2 and other console gaming systems, encryption algorithms, IP spoofing, telephone phrasing, viruses, Trojan horses, hacking satellite TV systems, TCP/IP sniffers, war dialing, war driving, wireless security, and so on. These are all still valid topics for your own presentations.

Class Project:
The class will be divided into two person teams. Each team will work in the lab to develop a demonstration of a security product or security problem. They will take an hour to demonstrate their project to the rest of the class. Each member of the team will also turn a 4-page describing their project (team members may not help each other on their reports). There will be a collective grade for the presentation and individual grades for the written reports. Each team member will fill out evaluation forms at the end of the semester on themselves and their fellow team members. These evaluations will affect
shared grades. If a team member is not participating fully (a free rider), please bring it to my attention as soon as possible, rather than waiting until the end of the semester.

**Content of each team’s project must receive prior approval by the instructor.** This is done by each team handing in a one-page description of their project.

<table>
<thead>
<tr>
<th>Date</th>
<th>Wednesday</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 14</td>
<td>Introduction to class. <em>Why Security?</em></td>
</tr>
<tr>
<td>January 21</td>
<td><em>Encryption.</em> McClure 1; Kruse 4.</td>
</tr>
<tr>
<td>February 4</td>
<td><em>Types of attacks.</em> In-class content. Students 1 and 2 presentations.</td>
</tr>
<tr>
<td>February 11</td>
<td><em>Hacking Microsoft and UNIX.</em> McClure 4-7. Students 3 and 4 presentations.</td>
</tr>
<tr>
<td>February 18</td>
<td><em>Hacking Networks.</em> McClure 8-12. Students 5 and 6 presentations.</td>
</tr>
<tr>
<td>March 3</td>
<td><strong>Midterm Exam</strong>; Students 9 and 10 presentations.</td>
</tr>
<tr>
<td>March 10</td>
<td><em>Introduction to Forensics.</em> Kruse 2-3, Appendix G. Students 1 and 2 presentsations.</td>
</tr>
<tr>
<td>March 17</td>
<td>SPRING BREAK</td>
</tr>
<tr>
<td>March 24</td>
<td><em>Data Hiding.</em> Kruse 5-6. Students 3 and 4 presentations.</td>
</tr>
<tr>
<td>March 31</td>
<td><em>Analyzing Microsoft Hacks.</em> Kruse 7-8, Appendix D. Students 5 and 6 presentations.</td>
</tr>
<tr>
<td>April 7</td>
<td><em>Analyzing UNIX Hacks.</em> Kruse 9-11, Appendixes C, E, F. Students 7 and 8 presentations.</td>
</tr>
<tr>
<td>April 14</td>
<td><em>Forensic Wrap-up and Handling Incidents.</em> Kruse 12-13, Appendixes A, B. Students 9 and 10 presentations; Group #1 presentation.</td>
</tr>
<tr>
<td>April 21</td>
<td>Group #2 and Group #3 presentations.</td>
</tr>
<tr>
<td>April 28</td>
<td>Group #4 and Group #5 presentations.</td>
</tr>
<tr>
<td>May 5</td>
<td><strong>Final Exam</strong> (same time and same room as the regular class)</td>
</tr>
</tbody>
</table>