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: 3:30-5:30 Wednesday and Thursday at Davis office.
Other office hours are available by appointment.


**Class Description:**
This course covers the basic principles and concepts in information security and information assurance. It examines the technical, operational, and organizational issues of securing information systems. Topics include operating system issues, viruses, security awareness at the executive, technical and user levels, physical security, personnel security issues, policies, procedures, and the need for an enterprise security organization. Case studies and exercises in the computer lab will be used to provide examples of the need for organizations to develop security procedures and policies. Prerequisites: IS&T 3620 and IS&T 4600.

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 (3) 30%
- Class Project 40%
- 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 will 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. *These presentations may not duplicate material used in a previous 4600 course or even material that was presented by another student.*

Some useful sites to find known security problems/bugs/viruses/worms:
- [http://www.cert.org/](http://www.cert.org/) - CERT Coordination Center
- [http://hackingtruths.box.sk/](http://hackingtruths.box.sk/) - Hacking Truths

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 phreaking, 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 or three person teams. Each team will have a chance to be a Blue team and a Red team.

Blue teams are the defenders and will set up a network with three machines (a Linux, Win 2000/XP, and Win9x machine). They will set up two web servers, two ftp servers, and at least three other applications or services. The Blue team must also create an e-mail server and must have ports open for e-mail, web, and ftp. The Blue team will place three files on each machine:
- The file <hack1.txt> will be located in C:\ and or root set to global read.
- The file <hack2.txt> will be located in C:\Windows or /usr/local/bin/ and set with permissions partially restricted.
- The file <hack3.txt> will be located in C:\ and or root set with no permissions.
The following web site is useful in learning to secure a machine:

Red teams are the attackers and will set up a network of machines of their choice. The Red Team will have three hours to break into the Blue team systems and retrieve the nine files.

Rules of Engagement:
- IP addresses will be assigned by the instructor and known to both teams.
- There will be NO social engineering.
- You may not try to exploit other teams before the Red/Blue day.
- You may not have physical access to machines of the other team.
- Other rules may be announced by the instructor during the course of the semester.

The first pair of Red/Blue days will have firewall software enabled and no physical access to the machines of the Blue team. The second pair of Red/Blue days will have firewall software disabled and physical access will be granted to the Blue team machines.

Each member of the team will also turn a 6-page describing their project (team members may not help each other on their 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.
<table>
<thead>
<tr>
<th>Date</th>
<th>Thursday</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2</td>
<td>Introduction to class. <em>Introduction to UNIX.</em></td>
</tr>
<tr>
<td>September 9</td>
<td><em>More UNIX.</em> Read all of Ray; McCarthy chapters 1-2.</td>
</tr>
<tr>
<td>September 16</td>
<td><em>More UNIX.</em> Read McCarthy chapters 3-4. Students 1-3 presentations.</td>
</tr>
<tr>
<td>September 23</td>
<td>Lab only (instructor will not be present).</td>
</tr>
<tr>
<td>September 30</td>
<td>Read McCarthy chapters 4-6. Students 4-10 presentations.</td>
</tr>
<tr>
<td>October 7</td>
<td>Read McCarthy chapters 7-9. Students 1-5 presentations.</td>
</tr>
<tr>
<td>October 14</td>
<td>Red/Blue day.</td>
</tr>
<tr>
<td>October 21</td>
<td>Read McCarthy chapters 10-12. Students 6-10 presentations.</td>
</tr>
<tr>
<td>October 28</td>
<td>Red/Blue day.</td>
</tr>
<tr>
<td>November 4</td>
<td>Students 1-5 presentations.</td>
</tr>
<tr>
<td>November 11</td>
<td>Red/Blue day.</td>
</tr>
<tr>
<td>November 18</td>
<td>Students 6-10 presentations.</td>
</tr>
<tr>
<td>November 25</td>
<td>Thanksgiving.</td>
</tr>
<tr>
<td>December 2</td>
<td>Red/Blue day.</td>
</tr>
<tr>
<td>December 9</td>
<td>Red/Blue day.</td>
</tr>
<tr>
<td>December 16</td>
<td><strong>Final Exam</strong> (same time and same room as the regular class)**</td>
</tr>
</tbody>
</table>