IST 4600 **Information Security I** Fall 2009

Instructor: Dr. Eric Swedin
Office: DV137L (at Davis campus)
Office phone: 395-3553
E-mail: eswedin@weber.edu or eswedin@gmail.com
Web site: http://www.swedin.org/

Office Hours: 2:00-3:30 on Tuesday and 2:00-5:30 on Thursday. Other office hours are available by appointment.

Texts: Ed Skoudis, *Malware: Fighting Malicious Code* (Prentice Hall, 2004).
Ed Skoudis and Tom Liston, *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses* (Second edition, Prentice Hall, 2006).

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: 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 readings.

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

Quizzes	35%
Class Presentation	20%
Projects (3)	45%

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

Quizzes:
There will a quiz every day at the beginning of class. Each quiz will be based on the readings that you were given for that day. You may miss three quizzes; if you take extra quizzes, they will count as extra credit.

Campus Closure:
In the event of an extended campus closure, please look at your Weber State email in order for instructions on how we will continue the class via email and the Blackboard online course system.

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. SSD can also arrange to provide materials (including this syllabus) in alternative formats if necessary.

Cell Phones, Texting, and Laptops:
Put your cell phones on vibrate. Try to avoid leaving class to take a call, but an occasional emergency is understandable. There will be NO texting in this class. Laptops or other personal digital tools may be used to take notes, look up material relevant to class discussions, or for class projects. No other uses of laptops will be tolerated.

Cheating Policy:
Cheating and deceit are not accepted in the Goddard School of Business and Economics. *Cheating on a quiz 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, even in an informational handout for your fellow students. **Avoid even the appearance of cheating or plagiarism.**

Class Presentations:
Each student will make a presentation in class. The presentation will be accompanied with a one-page class handout, with enough copies for everyone in class. This 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 twenty minutes. You may not make a presentation on a topic already covered by another student (publically claim a topic if you want to preserve it for yourself).

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 techniques, hacking an iPhone, how a new example of malware works in detail, hacking satellite TV systems, new war driving techniques, wireless security, DCMA, BitTorrent issues, and so on. These are all still valid topics for your own presentations.

Individual Projects:
Each student will do these three projects. Each project will have to be demonstrated to the instructor and you will have to submit a three-page report describing what you did (i.e., what products you used, why you used those products, what problems you encountered, what security problem was solved by this project, and what security problem(s) that particular product solves). Note that most of these projects require you to use two systems.

1) Create a secured machine by doing the following:
   - Set up a firewall and demonstrate how the firewall works by using a port scanner. Be able to explain how firewalls and port scanners work. A useful site to look at is: http://www.firewallguide.com/software.htm. I also want you to demonstrate a packet sniffer to me, showing me the network traffic between the two machines, and explaining how the sniffer works and what the contents of the sniffer log mean.
   - Set up anti-virus software on your PC and try to infect the PC with a virus or other malware.

2) Using malware:
   - Set up a trojan horse product on your PC and demonstrate remote control features. Examples include Sub7 and BackOrifice.

3) Using physical access:
   - Successfully penetrate a Windows or Linux machine to which you have physical access and that is password protected. Success means that you can get access to any files on the hard drive without cracking a password.

You will often be downloading trial versions of software and the trial period will run out. Sometimes running CyberScrub (http://www.cyberscrub.com/) can let you do reinstall trial software again.

Schedule:

Date	Wednesday
August 27	Introduction to class. *Why Security?*
September 3	*Counter Hack Reloaded*, chapters 1-2.
September 10	*Counter Hack Reloaded*, chapter 3.
September 17	*Counter Hack Reloaded*, chapter 4.
September 24	*Counter Hack Reloaded*, chapter 5.
October 1	*Counter Hack Reloaded*, chapter 6.
October 8	Lab time. Instructor will not in class.
October 15	*Counter Hack Reloaded*, chapter 7. Students 1 & 2 presentation.
October 22	*Counter Hack Reloaded*, chapters 8 & 9. Students 3 & 4 presentation.
October 29	*Counter Hack Reloaded*, chapter 10. Students 5 & 6 presentation.
November 5	*Counter Hack Reloaded*, chapter 11. Students 7 & 8 presentation.
November 12	*Counter Hack Reloaded*, chapters 12 & 13. Students 9 & 10 presentation.
November 19	*Malware,* chapters 1 & 2. Students 11 & 12 presentation.
November 26	Thanksgiving.
December 3	*Malware,* chapter 3. Students 13 & 14 presentation.
December 10	**No Final Exam**