IS&T 4600 **Computer Forensics** Spring 2005

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: 4:00-5:30 Tuesday, Wednesday, and Thursday at Davis office. Other office hours are available by appointment.

Texts: Stuart McClure, Joel Scambray, and George Kurtz, *Hacking Exposed: Network Security Secrets & Solutions* (Fourth edition, 2003).
Warren G. Kruse II and Jay G. Heiser, *Computer Forensics: Incident Response Essentials* (2002).

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 readings.

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

Quizzes	20%
Class Presentations (2)	20%
Individual Projects (3)	30%
Midterm Exam	10%
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.

Assignments are due the day shown in the schedule. You may turn them via e-mail or by hand. Late assignments are docked ten percent each week that they are overdue.

Quizzes:
There will be six quizzes, on random days. Each quiz will be based on the readings that you were given for that day. Only five quizzes will be counted, so that the lowest quiz score may be dropped.

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. Each presentation will be accompanied with a one-page class handout, with enough copies for everyone in class. Presentations must be two on the following three categories:

- a worm, virus, or dangerous bug
- a security tool (PGP, grc.com, SecureID, etc)
- on something interesting (DCMA, BitTorrent, hacking an X-box, Pringles can wireless receiver, RFIDs, steganography, etc)

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.SecurityFocus.com/ - SecurityFocus (including Bugtraq)
http://www.vmyths.com/ - Vmyths.com - Truth About Virus Myths/Hoaxes
http://www.nipc.gov/ - National Infrastructure Protection Center (FBI)
http://www.sans.org/ - SANS Institute
http://www.w3.org/Security/Faq/www-security-faq.html - World Wide Web Security FAQ
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 phreaking, viruses, Trojan horses, hacking satellite TV systems, TCP/IP sniffers, war dialing, war driving, wireless security, PGP, DCMA, BitTorrent, and so on. These are all still valid topics for your own presentations.

These presentations will be graded on the following criteria:

- 20% Is it new material that was not covered in class;
- 40% Quality of oral presentation;
- 40% Quality of class handout (I will take away 5% for the first grammar and spelling mistake, and then 1% for each subsequent grammar and spelling mistake).

Individual Projects:
Each student will do three individual projects out of the possible six projects below. Each project will have to be demonstrated to the instructor and you will have to submit a two-page report describing what you did (i.e., what products you used, why you used those products, what problems you encountered). Note that most of these projects require you to use two systems.

1) 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

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

3) Set up anti-virus software on your PC and try to infect the PC with a virus or other malware.

4) Set up a sniffer and show how it tracks network traffic and be able to explain to the instructor the sniffer log.

5) Successfully hack a Windows XP or Linux machine to which you have physical access. Hacking means that you can get access to any files on the hard drive.

6) Set up an intrusion detection system (IDS) and show it catching a suspicious event, such as a denial of service attack.

Schedule:

Date	Wednesday
January 12	Introduction to class. *Why Security?*
January 19	*How to Hack and General Issues in Security*. McClure 1-3.
January 26	*Encryption and Firewalls*. Kruse 4; McClure 11.
February 2	*Hacking Microsoft*. McClure 4, 5.
February 9	*Hacking UNIX*. McClure 7. Students 1-2 presentations.
February 16	*Network Hacking I*. McClure 8, 9. Students 3-4 presentations.
February 23	*Network Hacking II.* McClure 10, 12. Students 5-6 presentations.
March 2	*Software Hacking I*. McClure 13, 14. Students 7-8 presentations.
March 9	*Software Hacking II*. McClure 15, 16. Students 9-10 presentations.
March 16	SPRING BREAK
March 23	**Midterm Exam**
March 30	*Introduction to Forensics.* Kruse 1-3, Appendix G. Students 1-2 presentations.
April 6	*Data Hiding*. Kruse 5, 6. Students 3-4 presentations.
April 13	*Analyzing Microsoft Hacks*. Kruse 7, 8, Appendix D. Students 5-6 presentations.
April 20	*Analyzing UNIX Hacks*. Kruse 9-11, Appendixes C, E, F. Students 7-8 presentations.
April 27	*Forensic Wrap-up and Handling Incidents*. Kruse 12, 13, Appendixes A, B. Students 9-10 presentations.
May 4	**Final Exam** (same time and same room as the regular class)