

CS 439/539 Applied Security Concepts Syllabus

Instructors: Dr. Paul W. Oman (McClure 409; 885-6899; oman@cs.uidaho.edu) and David Manz (JEB 1, 885-5562, davidmanz@vandals.uidaho.edu)

RADICL SysAd: Brandon Arp (McClure 437, 885-4956, brandonarp@vandals.uidaho.edu)

Class: TuTh 11:00-12:15 in JEB 21

Total Credits: 3 cr

URL: <http://www2.cs.uidaho.edu/~oman>

Current Catalog Description: CS J439/J539 Applied Security Concepts (3 cr). Hands-on approach to computer security with emphasis on developing practical knowledge of how cyber attacks work and how to defend against them. Detailed exploration of attacks such as buffer overruns, string attacks, worms, trojan horses, and denial-of-service attacks, and development of defenses against them. Additional work reqd for grad cr. Recommended preparation: Good knowledge of C, operating system concepts and Unix. **Prereq:** CS 336 or Permission

Textbook: None

References: Papers and presentations provided by the instructor.

Course Goals: The goal of this course is to give the students hands-on, applied knowledge of cyber-attacks, specifically, how they function and how they can be prevented. The course begins with an introduction to the class, followed by labs in which the students present varying malware threats (including viruses, worms, Denial of Service (DoS), man-in-the-middle, and buffer overruns and format string attacks and defenses). For each topic we discuss and demonstrate the defenses against those exploits. Each attack-defend scenario is covered in roughly 2 weeks duration, including student presentations.

Prerequisites by Topic:

- Fundamental concepts of operating systems
- Hands on knowledge of Unix

Major Topics Covered in the Course (tentative): (duration) (CC 2001 reference)

- Ethics (6 hours) (SP4, SP5, SP7)
- Basic networking concepts (3 hours) (NC2)
- Buffer Overrun attacks (3 hours) (NC3)
- Format String attacks (6 hours) (NC3)
- Introduction to DoS and DDoS attacks (6 hours) (NC3)
- Case studies (16 hours)
- Viruses and worms (3 hours) (NC3)

Laboratory projects (specify number of weeks on each): This is an applied laboratory class, so there are typically 8 to 10 laboratory assignments, and corresponding presentations, done in teams of three or four students. The presentation is a detailed discussion of a specific laboratory exercise, which takes an entire week of in-class and out-of-class activity. Every team is required to a presentation covering their laboratory exercises. After every presentation the class will evaluate and grade the presentation; and teammates will do peer evaluations.

Grades: Grades will be based on two exams, peer and group evaluations, and an instructor evaluation, broken down as follows.

| | |
|------------------------|------------|
| Midsemester exam | 100 points |
| Final exam | 200 points |
| Team evaluations | 100 points |
| Class evaluations | 100 points |
| Instructor evaluations | 100 points |

Letter grades will be assigned using a normal 90%, 80%, 70%, ... curve for A, B, C, ...

Tentative Project List and Schedule

| Week | Date | Topic | Responsibility |
|------|------------|--|---------------------------|
| 1 | Jan. 15 | First class; Welcome & RADICL Introduction | |
| 2 | Jan. 20 | Team assignments Begin task scheduling | Paul Oman David Manz |
| | Jan. 22 | VRAD Lab review | Corey Thuen & Brandon Arp |
| 3 | Jan. 27 | Scanners; Sniffers; Metasploit open lab | |
| | Jan. 29 | Scanners & Sniffers presentations | Indefactable, Edge |
| 4 | Feb. 3 | Metasploit presentation; Lab review; Worm & Virus selection | ?; All teams |
| | Feb. 5 | Worm & Virus open lab | All teams |
| 5 | Feb. 10 | Worms/Viruses presentations | TBD |
| | Feb. 12 | Finish Worms/Viruses presentations; DOS/DDOS selection | TBD; All teams |
| 6 | Feb. 17 | DOS/DDOS open lab | All teams |
| | Feb. 19 | DOS/DDOS presentations | TBD |
| 7 | Feb. 24 | Finish DOS/DDOS presentations; Web vulnerability & Password cracking selection | TBD; All teams |
| | Feb. 26 | Web vulnerability & Password cracking open lab | All teams |
| 8 | Mar. 3 | Passwd cracking presentations | TBD |
| | Mar. 5 | Web vulnerability presentation; Root kit & OS hardening selection | TBD; All teams |
| 9 | Mar. 10 | Midsemester Review | Paul Oman & David Manz |
| | Mar. 12 | Midsemester Exam | David Manz |
| 10 | Mar. 16-20 | Spring Break | |
| 11 | Mar. 24 | Root kit & OS hardening open lab | All teams |
| | Mar. 26 | Root kit & OS hardening open lab | All teams |
| 12 | Mar. 31 | Root kit & OS hardening presentations | TBD |
| | April 2 | Root kit & OS hardening presentations Buffer overflow and Format string selection | TBD; All teams |
| 13 | Apr. 7 | Buffer overflow and Format string open lab | All teams |
| | Apr. 9 | Buffer overflow and Format string open lab | All teams |
| 14 | Apr. 14 | Buffer overflow presentations | TBD |
| | Apr. 16 | Format string presentations | TBD |
| 15 | Apr. 21 | Capture the flag preparation | All teams |
| | Apr. 23 | Capture the flag operation | All teams |
| 16 | Apr. 28 | Red / Blue preparation | All teams |
| | Apr. 30 | Red / Blue practice | All teams |
| 17 | May 5 | Red / Blue Tournament | All teams |
| | May 7 | Semester & Final Review | Paul Oman & David Manz |
| 18 | May 11-15 | Finals week – Final is May 12, 12:30-2:30 | David Manz |