USCSchool Name

INF526 Secure System Administration

Units: 4 units (2 units lecture, 2 units lab)
Meets two times per week, 2 hours per lecture
(one lecture per week needs to be in a computer lab setting)

Location: Physical address and/or course-related URLs, etc.

Instructor: Clifford Neuman
Office: Physical or virtual address
Office Hours: (General guideline: 1 weekly office hour for each 4 unit class taught. Office hours are not to be calculated in "contact hours.")

Contact Info: bcn@isi.edu, 310-448-8736.

Teaching Assistant:
Office: Physical or virtual address
Office Hours:
Contact Info: Email, phone number (office, cell), Skype, etc.

IT Help: Group to contact for technological services, if applicable.
Hours of Service:
Contact Info: Email, phone number (office, cell), Skype, etc.

Course Description

The system security administrator is the focal point for planning security in the installation and the "front line" when defending systems from cyber attack. Typically systems come with security features turned off to facilitate initial operation and must be tailored to the security needs of the organization. The only thing between a new system and a cyber attacker is the knowledge of the system administrator. The system administrator not only assures that user IDs and an initial password are set robustly, but also configures firewalls, intrusion detection systems, etc. and facilitates the development and enforcement of effective security policy for the organization.

The system security administrator plays an integral role in the system security design, testing, certification, accreditation, and operation of complex cyber systems, as well as operationally defending the system against real-time attacks.

The course provides students with hands on experience in the field of security administration. The student will learn how a security professional fulfills various Information Assurance requirements using the Linux operating system (the same principles apply to other operating systems). Students will be presented throughout the semester with a series of hypothetical systems representative of typical services and organizational models. Working in groups, students will design their information architecture for the systems in such organizations, paying careful attention to the required and prohibited information flows. Students will individually submit their plans for the placement of data and defense technologies.

Lecture topics include an examination of server, workstation and network vulnerabilities; procedures and tools for security assessment; development of security policies, procedures and standards; firewalls, logging and audit tools, hardening scripts as well as other tools and techniques used to implement secure computing environments.

This course is intended for graduate students with the following qualification: typically coming out of computer science, mathematics, computer engineering, informatics, and/or Information security undergraduate program. Also, it is highly recommended that students have successfully completed coursework involving policy and network security.

Students in this class will learn primarily from hands on activities, augmented by lecture and weekly assigned readings. There will be a mid-term and final exam, and four case study group hands on exercises.

Lab Description

In teams, students will deploy systems to manage access to data according to their plans and deploy defensive technologies. The teams will participate in a capture the flag competition where they seek to defend their systems, while compromising the security of the systems deployed by other teams. This process will be repeated four times during the semester, each focused on a different scenarios representing different classes of systems.

Learning Objectives

This course is designed to transfer both knowledge and applicable skills in utilizing technology, methods and policy to solve information security challenges. In doing so, many of the objectives will require a “hands-on” approach to learning. After completing this course, students will be able to:

1. Analyze the needs of an organization and create an appropriate security policy and

concomitant documentation
2. Develop security requirements
3. Evaluate exposure to risk in a computing environment
4. Determine tools and techniques necessary to meet requirements
5. Lead efforts to implement the necessary steps to meet security requirements
6. Demonstrate the ability to recognize characteristics of various computer attacks to include:
    a. Malicious code
    b. Network attacks
7. Develop responses to computer attacks
8. Demonstrate the ability to interpret log files
9. To demonstrate fluency in the use of the following security tools:
    a. Firewall
    b. Intrusion detection system
        i. Host-based
        ii. Network-based
    c. Logfile watcher
10. Create a firewall based upon a security policy.
11. Use tools to conduct a vulnerability analysis of a live network
    a. Nmap
    b. Nessus
    c. Others as necessary
12. Interpret the results of the vulnerability analysis, including defining recommendations for the network owner

Methods of Teaching:

This course is highly applied and therefore the primary teaching methods are interactive lectures and demonstrations. In addition, hands on exercises are used to reinforce what the student has learned. The exercises are meant to mimic what a student would find in real-world organizations.

Students are expected to perform directed self learning outside of class which encompasses, among other things, a considerable amount of literature review.

Prerequisite(s): CSci530
Co-Requisite (s): none
Concurrent Enrollment: none
Recommended Preparation: none.

Required Readings and Supplementary Materials

All books, papers or reports will be available to students in one of three ways: 1) in the USC bookstore; 2) online through Desire 2 Lean and the web

Required Course Book:

(ANON) Anonymous. (2002). Maximum Linux Security: A Hackers Guide to Protecting Your Linux Server and Workstation. SAMS Publishing.

Other Books (Recommended unless otherwise noted in course schedule):

(HLK) Hacking Linux Exposed, by Hatch, Lee and Kurtz, Osborne Press (COE)

Cole, E. (2002). Hacker's Beware. SANS Institute.

(G&S 1996)Garfinkel, S., & Spafford, E. (1996). Practical UNIX & Internet Security. O-Reilly.

(G&S 2001) Garfinkel, S., & Spafford, E. (2001). Web Security, Privacy, & Commerce. O'Reilly.

(GAGNE) Gagne, M. (2001). Linux System Administration. Prentice-Hall. (ZIG)

Ziegler, M. (2002). Linux Firewalls. New Riders.

(ZWE) Zwicky, E.D. (2001). Building Internet Firewalls. O'Reilly.

(OPP) Opplinger, R. (2001). Internet and Intranet Security. Artech House.

(N&N)Northcutt, S., & Novak, J. (2001). Network Intrusion Detection: An Analysts Handbook. New Riders.

(P&M)Prosise, K, & Mandia, K. (2002). Incident Response: Investigating Computer Crime.

(S&S) Saltzer & Schroeder

(S&S) Schulz, E.E., & Shumway, R. (2002). Incident Response: A Strategic Guide to Handling System and Network Security Breaches. New Riders.

(SKK) Seglem, K. K. (2002). Introduction to Digital Evidence Reconstruction using UNIX Systems. In E. Casey (Ed.), Handbook of Computer Crime Investigation.
Academic Press.

Other Readings (Recommended unless otherwise noted in course schedule):

SANS. (2002). The intrusion detection FAQ.
http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm

U.S. Department of Justice. (July, 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Computer Crime and Intellectual Property Section. Criminal Division, United States Department of Justice.

Venema, W. (Dec., 2000). File recovery techniques: Files wanted, dead or alive. Dr. Dobb's Journal.

(VEN) Venema, W. (Nov., 2000). Strangers in the night: Finding the purpose of an unknown program. Dr. Dobb's Journal.

(GCS) General Computer Security: www.packetstorm.com

(SSP) *A System Security Policy for You* - GIAC
*www.GIAC.org/paper/gsec/734/**system-security-policy**/101613*

Description and Assessment of Assignments

The following are representative of the assignments in this class. The specific assignments will change from semester to semester.

Assignment #1:

- Scope: Threat Analysis and Security planning
- Objective: Understand threat as it relates to assets in an organization and with regards to information security challenges, and understand initial protection and mitigation strategies. Demonstrate Security planning for system to be deployed in Programming Assignment 4
- Tasks: Using security requirements and system scenario provided by the instructor, develop a security plan including asset-threat analysis, protection measures, incident detection methods, system security tests for system that will be implemented in programming Assignment 4.

Assignment #2:

- Scope: Residual Risk Analysis
- Objective: To gain understanding the principles of residual risk with regards to current information protection challenges and secure systems administration, management and strategy
- Tasks: Complete systems risk analysis exercise; complete residual risk analysis and report findings

Assignment #3:

- Scope: Security Policy Interoperability
- Objective: Understand the security implications of interconnection of systems with separate dissimilar security policy implementations originating from similar security requirements.
- Tasks: Develop a vulnerability analysis of the interconnection of two systems with different security policy implementations specified by the instructor.

Assignment #4:

- Scope: Residual Risk Analysis of System Studied in CTF Exercise
- Objective: Understanding practical applications of residual risk analysis; introduction to some forensic principles in information security
- Tasks: Perform analysis of CTF exercise via outline provided by instructor; conduct residual risk analysis on all systems involved in the exercise; report findings

Assignment #5:

- Scope: Interconnection of dissimilar implementations

- Objective: Analyze security issues associated with interconnection of enclaves using dissimilar operating systems
- - Tasks: Scenario: Management mandates a connection between the corporation's Linux and Windows machine for purpose of file sharing - Write a paper (5 to 10 pages) on how to go about this and analyze resulting security issues with respect to file security permissions implemented in Windows and in Linux.

Grading Breakdown

Assignment	Points	% of Grade
Capture the Flag Exercies (student writeup)		20
Capture the Flag Exercies (team performanc		20
Mid-Term Exam		20
Final Exam		20
Homework		20
TOTAL	0	100

Additional Policies

Students with Disabilities

Any student requesting academic accommodations based on a disability is required to register with Disability Services and Programs (DSP) each semester. A letter of verification for approved accommodations can be obtained from DSP. Please be sure the letter is delivered to me as early in the semester as possible. Your letter must be specific as to the nature of any accommodations granted. DSP is located in STU 301 and is open 8:30 am to 5:30 pm, Monday through Friday. The telephone number for DSP is (213) 740-0776.

Emergency Preparedness/Course Continuity in a Crisis

In case of a declared emergency if travel to campus is not feasible, USC executive leadership will announce an electronic way for instructors to teach students in their residence halls or homes using a combination of Blackboard, teleconferencing, and other technologies.

Return of Course Assignments

Returned paperwork, unclaimed by a student, will be discarded after a year and hence, will not be available should a grade appeal be pursued following receipt of his/her grade.

Add any additional policies that students should be aware of: late assignments, missed classes, attendance expectations, use of technology in the classroom, etc.

Course Schedule: A Weekly Breakdown

Provide a detailed course calendar that provides a thorough list of deliverables—readings, assignments, examinations, etc., broken down on at least a weekly basis. The format may vary, but the content must include:

- **Subject matter (topic) or activity**
- **Required preparatory reading, or other assignments (i.e., viewing videos) for each class session, including page numbers.**
- **Assignments or deliverables.**

IMPORTANT:
In addition to in-class contact hours, all courses must also meet a minimum standard for out-of-class time, which accounts for time students spend on homework, readings, writing, and other academic activities. **For each unit of in-class contact time, the university expects two hours of out of class student work per week over a semester.**

(Please refer to the *Contact Hours Reference,* located at usc.edu/curriculum/resources.)

	Topics/Daily Activities	**Readings and Homework**	**Deliverable/ Due Dates**
Week 1 Dates	Introduction to class, Schedule, Overview, Motivation, historical perspective on security administration	CS,GCS, Anon:1,2,3, Puppy Linux Tutorial	**Introduction to first CTF exercise scenario.** **Assignment 1**
Week 2 Dates	Policy driven administration, principles of protection	SSP, S&S 1-13, ANON:4	Take home quiz, assignment 2, Wireshark, work on CTF1
Week 3 Dates	Metasploit and automated exploit tools	ANON:5	wrap up preparation for CTF.
Week 4 Dates	Generation of security requirements, operational environments, System High and Multi Level Systems	**ANON:6,7**	**CTF competition for first Scenario Install and Deploy Systems in team and defend system.**
Week 5 Dates	Composition of systems, adversarial security plan	**ANON:8 VEM**	**Assignment 3, Introduction to second CTF exercise scenario**
Week 6 Dates	Adversarial Emulation / Red Teaming, Windows Security Administration	**ANON:9**	**Wrap up preparation for CTF2**
Week 7 Dates	Linux Security Administration Review for mid-term	**ANON 10,11,12**	**CTF competition for second Scenario**
Week 8 Dates	Mid-term exam	**ANON 13**	**Mid-term exam, Introduction for third CTF scenarios**
Week 9 Dates	Pre and Post TPM Security administration	**ANON 14**	**Assignment 4, Wrap up preparation for CTF3**
Week 10 Dates	Integrating Hardware Based Security Mechanisms, Policy/Operational conflicts	**ANON 15,16**	**CTF competition for third Scenario**
Week 11 Dates	System Acquisition, Certification and Accreditation	**ANON 17**	**Introduction to 4th CTF scenario**

Week 12 Dates	Intrusion Detection, Firewalls, Encryption, Audit, SIEM	**ANON 18,19**	**Assignment 5, Preparation for 4th CTF**
Week 13 Dates	Disinfecting and decommissioning Systems	**ANON 20,21**	**More preparation for 4th CTF**
Week 14 Dates	Operational Validation of Hardware and Software	**Review of Semester Readings**	**4th CTF exercise**
Week 15 Dates	Forensics, Review for final		**Debrief report on CTF exercises due.**
FINAL Date			Date: For the date and time of the final for this class, consult the USC *Schedule of Classes* at www.usc.edu/soc.

Statement on Academic Conduct and Support Systems

Academic Conduct

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in *SCampus* in Section 11, *Behavior Violating University Standards* https://scampus.usc.edu/1100-behavior-violating-university-standards-and-appropriate-sanctions. Other forms of academic dishonesty are equally unacceptable. See additional information in *SCampus* and university policies on scientific misconduct, http://policy.usc.edu/scientific-misconduct.

Discrimination, sexual assault, and harassment are not tolerated by the university. You are encouraged to report any incidents to the *Office of Equity and Diversity* http://equity.usc.edu or to the *Department of Public Safety* http://adminopsnet.usc.edu/department/department-public-safety. This is important for the safety of the whole USC community. Another member of the university community – such as a friend, classmate, advisor, or faculty member – can help initiate the report, or can initiate the report on behalf of another person. *The Center for Women and Men* http://www.usc.edu/student-affairs/cwm/ provides 24/7 confidential support, and the sexual assault resource center webpage http://sarc.usc.edu describes reporting options and other resources.

Support Systems

A number of USC's schools provide support for students who need help with scholarly writing. Check with your advisor or program staff to find out more. Students whose primary language is not English should check with the *American Language Institute* http://dornsife.usc.edu/ali, which sponsors courses and workshops specifically for international graduate students. *The Office of Disability Services and Programs* http://sait.usc.edu/academicsupport/centerprograms/dsp/home_index.html provides certification for students with disabilities and helps arrange the relevant accommodations. If an officially declared emergency makes travel to campus infeasible, *USC Emergency Information* *http://emergency.usc.edu* will provide safety and other updates, including ways in which instruction will be continued by means of blackboard, teleconferencing, and other technology.