Computer Science Department
cs.salemstate.edu

CSC 235 Computer Security Basics **3 cr.**

Instructor: TBA **Office:** location **Phone:** (978) 542-extension
email: TBA@salemstate.edu **Office Hours:** days and times

Section	Time	Room	Final Exam
nn	days and times	location	date and time
Lnn	days and times	location	

Catalog description:

This course presents a unified view of information security that examines the closely related areas of software security, system security, and network security using a common set of underlying security principles. The resulting synthesis of knowledge will enable students to understand the challenges faced by contemporary designers of secure information technology infrastructure. Each of these three security areas is examined in sufficient detail for students to understand the complexity of modern threats and the corresponding sophistication of the software and hardware that is designed to counter these threats.

Prerequisites: CSC 101 or CSC 105 or CSC 200A, and CSC 110 or CSC 201J.

Goals:

Upon completion of the course, a student should be able to do the following:

CG01: identify basic issues, problems, and solutions in computer, software, and network security;
CG02: describe algorithms, tools, and methods used in implementing secure computer systems and networks;
CG03: use a variety of software tools employed in securing computer system and networks;
CG04: analyze software tools and organizational methods used by IT departments to ensure the security of their networks;
CG05: describe methods and mechanisms used in security assessment and security testing.

Course Objectives:

Upon successful completion of the course, a student will have demonstrated the ability to:

CO01: apply correct technical terminology when describing the main issues and solutions in security concerns at the computer, software, and network levels;
CO02: identify the ways in which software security fails, explain methods and technologies that can help in the development of secure software, and apply these techniques in practice;
CO03: apply assessment techniques to common operating systems and network configurations and develop security trouble shooting skills;
CO04: demonstrate ability to analyze a system configuration and propose ways to improve security at both the technical and administrative levels;
CO05: exercise a generic set of security tools used for penetration testing and security hardening and interpret the results.

Course Objective / Assessment Mechanism matrix

Program Objective (condensed form)	**CO01**	**CO02**	**CO03**	**CO04**	**CO05**
PO-A: apply knowledge of computing and math	✓	✓	✓	✓	✓
PO-B: analyze a problem and define its computing requirements		✓			✓
PO-C: design, implement and evaluate applications				✓	✓
PO-D: function effectively in teams to accomplish a common goal					

Program Objective (condensed form)	CO01	CO02	CO03	CO04	CO05
PO-E: professional, ethical, and social responsibilities					
PO-F: communicate effectively with a range of audiences		✓			
PO-G: local and global impact of computing on people and society					
PO-H: need for continuing professional development				✓	✓
PO-I: use current techniques, skills, and tools	✓	✓	✓	✓	✓
PO-J: apply theory and principles to model and design systems				✓	✓
PO-K: apply design and development principles in constructing software					
note - full statements of the **P**rogram **O**utcomes (objectives) for the Computer Science Major can be found in the document *Computer Science Major Program Educational Objectives and Program Outcomes* on the Assessment page of the Computer Science Major (cs.salemstate.edu)					

Course topics:

- Review of necessary material
  - Computer architecture (hardware and software) AR1(1), AR2(1), AR4(1)
  - Structure of Operating System OS1(1), OS2(1), OS4(1), OS6(1)
  - Overview of programming concepts AL1(1), AL2(1), PL1(1), PL2(1)
  - Overview of Networking NC1(1), NC2(2), NC6 (1)
- An Introduction to Information Security
  - Defining the key issues in information security NC3(1)
  - Assigning responsibility for providing Information Security
  - Attackers and their attacks (technical tools and methods as well as social engineering)
  - Standards in security systems and security models
  - Fundamentals of cryptography (private and public key algorithms) AL9 (2)
  - Core concepts in computer security OS7(1), NC3(2), AL4 (1)
  - Secure Operating Systems OS7 (1)
  - Authentication and identification schemes OS7 (1)
  - Resource protection schemes OS6(1), OS7(1),OS8(1)
- Introduction to Secure Software
  SE5(1),SE2(1),SE3(1),SE6(1),SE8(1)
  - Concepts and principles in secure programming
  - Processes and technical controls necessary to develop secure software.
- Networking Security NC3 (1)
  - Vulnerabilities of computer networks
  - Architecture of IP protocol-level security solution (IPsec)
  - Analysis of threats and discussion of security products
- Secure IT infrastructures
  - Designing secure computer systems and networks OS7(1), NC3(1)
  - Software security products such as firewalls, network address translators, Kerberos, secure remote login, single sign-on, biometrics etc. IM1(1), IM11(1)
  - Administration of security policies in IT NC6(1)
  - Building a secure IT infrastructure SP2(1),SP5(1),SP6(1)
  - Security issues in mobile computing NC9(1)
  - Web security NC4(1), NC5(1)
  - Evaluating and testing computer and network security
  - Basic concepts in computer forensics SP8(1)

Organization of the course

The course consists of lectures, labs, homework assignments, quizzes, and two exams – a midterm and a final. Lectures are accompanied by live demonstration of security products and solutions. Weekly labs consist of hands-on exercises that include examination of security software and usage of different security tools. Homework assignments, given weekly, consist of doing

research on different aspects of computer and network security. Individual and group projects include analyzing and solving security-related tasks.

Assignments: Homework assignments, given weekly, consist of doing research on different aspects of computer and network security. Individual and group projects include analyzing and solving security-related tasks.

.

Labs: Weekly labs consist of hands-on exercises that include examination of security software and usage of different security tools.. Each lab consists of a set of actions and that cover material learned during the week. All labs will be conducted within an environment specifically created for this course

Quizzes, Tests and Examinations: There will be four quizzes (each covering one of the major topics), a midterm, and a cumulative final. Quizzes and exams will include multiple choice and problem solving tasks.

Grading: Final grades will be determined on the basis of the following approximate weights:

- Laboratory exercises 20%
- Homework assignments 15%
- Quizzes 25%
- Midterm exam 20%
- Final exam 20%

Course Objective / Assessment Mechanism matrix

	Lab assignment	Homework assignment	Quizzes	Midterm exam	Final Exam
CO1	✓	✓		✓	✓
CO2			✓	✓	✓
CO3	✓	✓	✓	✓	✓
CO4		✓		✓	✓
CO5	✓		✓	✓	✓

Bibliography:

Allsopp, Will; Kevin Mitnik. **Unauthorized access: Physical Penetration Testing for IT Security Teams.** Wiley, 2009.

Basin, Shweta. **Web Security Basics (Networking).** Muska & Lipman/Premier-Trade, 2002.

Ciampa, Mark. **Security+ Guide to Network Security Fundamentals.** Course Technology, 2008.

Frankel, Sheila. **Demystifying the Ipsec Puzzle** . Artech House Publishers, 2001.

Gollmann, Dieter. **Computer Security.** Wiley, 2006.

Harris, Shon. **Gray Hat Hacking.** McGraw-Hill Osborne Media, 2007.

McGraw, Gary. **Building Secure Software: How to Avoid Security Problems the Right Way**. Addison-Wesley Professional Computing Series, 2001.

Mel, H.X.; Baker, Doris. **Cryptography Decrypted**. Addison-Wesley Professional, 2000.

Whitman, Michael *et al.* **Guide to Firewalls and Network Security. Second Edition.** Course Technology, 2009.

Viega, John; Messier, Matt. **Secure Programming Cookbook for C and C++: Recipes for Cryptography, Authentication, Input Validation & More.** O'Reilly Media, 2003.

Tools and Web resources:

Utility for network exploration: http://nmap.org/

Network security lectures: http://www.cis.ufl.edu/~nemo/security/

Backtrack remote penetration toolset: www.remote-exploit.org

An illustrated guide to IPsec: http://www.unixwiz.net/techtips/iguide-ipsec.html

---

Academic Integrity Statement:

"Salem State University assumes that all students come to the University with serious educational intent and expects them to be mature, responsible individuals who will exhibit high standards of honesty and personal conduct in their academic life. All

forms of academic dishonesty are considered to be serious offences against the University community. The University will apply sanctions when student conduct interferes with the University primary responsibility of ensuring its educational objectives." Consult the University catalog for further details on Academic Integrity Regulations and, in particular, the University definition of academic dishonesty.

The Academic Integrity Policy and Regulations can be found in the University Catalog and on the University website (http://catalog.salemstate.edu/content.php?catoid=13&navoid=1295#Academic_Integrity). The formal regulations are extensive and detailed - familiarize yourself with them if you have not previously done so. A concise summary of and direct quote from the regulations: "Materials (written or otherwise) submitted to fulfill academic requirements must represent a student's own efforts". *Submission of other's work as one's own without proper attribution is in direct violation of the University's Policy* and will be dealt with according to the University's formal Procedures. *Copying without attribution is considered cheating in an academic environment - simply put,* ***do not do it!***

University-Declared Critical Emergency Statement:

In the event of a university-declared emergency, Salem State University reserves the right to alter this course plan. Students should refer to www.salemstate.edu for further information and updates. The course attendance policy stays in effect until there is a university-declared critical emergency.

In the event of an emergency, please refer to the alternative educational plans for this course, which will be distributed via standing class communication protocols. Students should review the plans and act accordingly. Any required material that may be necessary will have been previously distributed to students electronically or will be made available as needed via email and/or Internet access.

Equal Access Statement:

"Salem State University is committed to providing equal access to the educational experience for all students in compliance with Section 504 of The Rehabilitation Act and The Americans with Disabilities Act and to providing all reasonable academic accommodations, aids and adjustments. **Any student who has a documented disability requiring an accommodation, aid or adjustment should speak with the instructor immediately.** Students with Disabilities who have not previously done so should provide documentation to and schedule an appointment with the Office for Students with Disabilities and obtain appropriate services."

Note: This syllabus represents the intended structure of the course for the semester. If changes are necessary, students will be notified in writing and via email.