Cosumnes River College
CISS 310
Network Security Fundamentals
An Online Course
Spring 2015

Instructor: Buddy Spisak **Office Hours**: Mon. 7:30-8:30 p.m. (Jan. 26 to May 18)

Office: BS-143
Voice Mail: (916) 286-3691 ext. 14162
Email: spisakj@crc.losrios.edu The turnaround time for responding to most emails is about one to two days. Be sure to include your name and the course number in each email so I can identify who you are and what the email is about.
Course Web page: https://d2l.losrios.edu/
Instructor Web page: http://crc.losrios.edu/spisakj/

Prerequisites: CISN 330
Advisory: None
Lecture: Online
Accepted for Credit: CSU
Class Credits: 3 units

Required Textbook:

Title:	*Security + Comp TIS*
Author:	Testout
Publishing Info:	Testout
E-Book ISBN13:	978-1-935-08040-4

Optional Materials: None at this time

Course Description:

Organizations today are linking their information systems across enterprise-wide networks and Virtual Private Networks, as well as increasing their exposure to the Internet. Each connection magnifies the vulnerability to unauthorized access. This course provides the fundamental knowledge needed to analyze risks to the system and implement a workable security policy that protects information assets from potential intrusion, damage or theft. Students will learn which countermeasures to deploy to thwart potential attacks. This course also prepares students for CompTIA's Security+ certification exam.

Student Learning Outcomes and Course Objectives:
- ANALYZE FUNDAMENTAL SECURITY CONCEPTS (SLO #01).
    - Describe the challenges of securing information.
    - Define information security and explain why it is important.
    - Identify the types of attackers that are common today.
    - List the basic steps of an attack.
    - Explain the different types of information security careers and how the Security+ certification can enhance a security career.

- ANALYZE SYSTEM THREATS AND THE RISKS ASSOCIATED WITH THEM (SLO #02).
    - Describe the different types of software-based attacks
    - List types of hardware attacks.
    - Define virtualization and explain how attackers are targeting virtual systems.
- ANALYZE WAYS TO HARDEN AN OPERATING SYSTEM (SLO #03).
    - Describe various software security applications.
    - Explain how to protect systems from communications-based attacks.
    - List ways to prevent attacks through a Web browser.
    - Explain how to harden operating systems.
- EXAMINE SOME OF THE MAJOR WEAKNESSES THAT ARE FOUND IN NETWORK SYSTEMS AND WAYS TO PREVENT THEM (SLO #04).
    - Explain the types of network vulnerabilities.
    - Define different methods of network attacks.
    - List the different types of network security devices and explain how they can be used.
    - Define network address translation and network access control.
    - Explain how to enhance security through network design.
- INVESTIGATE THE BASIC WIRELESS SECURITY PROTECTIONS AVAILABLE TO THEM (SLO #05).
    - Describe the basic IEEE 802 wireless security protections.
    - Define the vulnerabilities of open system authentication, WEP, and device authentication. Describe the WPA and WPA2 personal security models.
    - Explain how enterprises can implement wireless security.
- INVESTIGATE LOGICAL AND PHYSICAL ACCESS CONTROL METHODS (SLO #06).
    - Define access control and list the four access control models.
    - Describe logical access control methods.
    - Explain the different types of physical access control.
- EXAMINE AUTHENTICATION AND UNDERSTAND HOW IT FITS INTO ACCESS CONTROL (SLO #07).
    - Define authentication. Describe the different types of authentication credentials.
    - List and explain the authentication models.
    - Define authentication servers.
    - Describe the different extended authentication protocols.
- DEFINE RISK AND RISK MANAGEMENT (SLO #08).
    - Define risk and risk management.
    - Describe the components of risk management.
    - List and describe vulnerability scanning tools.
    - Define penetration testing.
    - Describe how usage audits can protect security.
    - List the methodologies used for monitoring to detect security-related anomalies.
- EXAMINE HOW TO PROTECT DATA USING THREE COMMON TYPES OF ENCRYPTION ALGORITHMS: HASHING, SYMMETRIC ENCRYPTION, AND ASYMMETRIC ENCRYPTION (SLO #09).
    - Define cryptography and hashing.
    - List the basic symmetric cryptographic algorithms.
    - Describe how asymmetric cryptography works.
    - List types of file and file system cryptography. Explain how whole disk encryption works.
    - Define digital certificates. List the various types of digital certificates and how they are used.
    - Describe the components of Public Key Infrastructure (PKI).
- FORMULATE REDUNDANCY PLANS AND SECURITY POLICIES (SLO #10).
    - Describe the components of redundancy planning.
    - List disaster recovery procedures.
    - Describe incident response procedures.
    - Define organizational security policy. List the types of security policies.
    - Describe how education and training can limit the impact of social engineering.

Methods of Measuring Student Learning Outcomes:

- Students will demonstrate knowledge of network and internet security applications and standards through class discussions and achievement on modules, quizzes, and final examination.
- Students will demonstrate competence in the coursework by participating in discussions during the semester.

Student Obligations:

- **Attendance**: Since this course is online, only attendance at the final exam is necessary. It's up to you to go to TestOut and do all of the required work. Please note that failure to complete 10% of the total course work by the third week of the class may result in your being dropped from the course.
- **Discussions**: I want everyone to take a pro-active approach to learning this material. This includes using the Discussions link to ask questions and also answer other students' questions. I will also post questions each week that you can answer to further your understanding of the material. I expect two postings each week unless otherwise noted.
- **Modules**: Students will responsible for completing 11 modules in TestOut. The modules will help reinforce what you are learning in each lesson. The due dates are located in the schedule portion of this handout.
- **Projects**: Students will be responsible for completing 11 case projects during the course of the semester. The due dates are located in the schedule portion of this handout.
- **Quizzes**: After each lesson you may be required to take a short quiz, which will test you on the material covered. It is open-book and open-notes. You can take the quiz multiple times to improve your score, but be aware that the questions will change each time and that your most recent score will be the one counted toward the module grade.
- **Practice Exams:** There are 9 practice exams broken down into server+ domains. Students will need an 80% pass rate in order to receive full credit for them. Students will have 2 weeks to complete these exams.
- **Final Exam**: The Final Exam will be matching, short-answer and essay in format. You can use both your notes and your book. You must submit the answers for the Final at the college on Saturday, May 16, from 11:30a.m. to 1:30 p.m. in the BS-153 classroom. It is necessary to show a picture ID for identity verification.
- **Late Work**: Unless noted, all assignments are due on Sunday by midnight each week. Late work will be accepted ONLY if you have contacted me prior to the due date either by email or voice mail. In general, late work is due the next week, and no late assignments may be turned in after one week from the original due date, regardless of the reason. For every day an assignment is late, you will lose 10% of its grade.
- **Due Dates**: Unless noted, all assignments will be completed in TestOut. If, for any reason, you cannot submit an assignment on time, please email me so that you are not penalized for being late. If you miss a quiz and you want to make up points, you can take advantage of the extra credit assignments posted in d2l. Everyone is welcome to work on the extra credit assignments. Typically, they are five to ten points each, depending on the difficulty of the assignment.
- **Plagiarism Policy**: It is inappropriate, and a violation of academic policy, to copy information from any source (including, but not limited to, textbooks, magazine articles, newspaper articles and internet articles) without giving proper credit to the author by using standard quotation procedures such as in-line quotes, footnotes, endnotes, etc. Quotes may not exceed 25% of the assignment's total length. You will receive no credit (0 points) for any assignment that copies any material from any other source without giving proper credit to the author(s). Repeat offenders of this policy are subject to academic discipline as outlined in the policies published by the college.
- **Cheating**: Students who cheat will receive a failing grade for the course. [See the Student Behavior and Academic Integrity page of the college website (https://www.crc.losrios.edu/catalog/geninfo/integrity).]

- **CRC Honor Code:** Academic integrity requires honesty, fairness, respect and responsibility. [See the Cosumnes River College Honor Code posted on the college website (https://www.crc.losrios.edu/facstaff/resourceguide/faculty/student-behavior-academic-integrity/honorcode.)]
- **Email**: Every student will be required to have an email account. If you do not have an email account, the college provides free email accounts for all current students. To activate your account, go to https://apps.losrios.edu/login.html and follow the directions provided.
- **Email etiquette**: I will not tolerate rude and demeaning comments or emails to anyone in this class. Please keep your comments and emails topic-related. If I determine that a comment or email to anyone else in the class is rude or demeaning, I will warn you once. If your behavior continues to be unacceptable, I will refer you to the administration of the college for disciplinary action.
- **Personal belongings**: No food or drinks are allowed in the classroom on the day of the final exam. All cell phones, beepers, pagers, etc. should be turned off or set to vibrate.
- **Disabilities:** If you have a documented disability and wish to discuss academic accommodations, please contact me or contact the Office of Disabled Student Programs and Services at 691-7275 as soon as possible.
- **Campus Police**: You can call 691-7777 to request a safety escort.
- **Desire 2 Learn (d2l):** This class utilizes a product called "Desire 2 Learn." It is highly recommended that you check the website frequently for scheduling updates and homework assignments.
- **Online Course Responsibilities:** This course requires significant self-motivation. You must not get behind. Projects and weekly assignments can take up to 9 hours to finish. Please don't try to finish them in one day. Not all activities are created equal. Some may take a bit longer than others. You would normally spend 3 hours per week in class for this course, a total of 54 hours. Allow yourself at least 9 hours per week to complete the activities online, including the time spent writing for the postings to the discussions page. You should plan additional time to read the class material and study for the quizzes. Some people believe that an online format provides a much easier way to study this subject than an on-campus framework because they love to read and avoid the parking problems. Others feel very intimidated at first. Be patient as you work your way through the activities.

Grading:

Course Topic		Points	Total	Approximate % the of Grade
Orientation Quiz (1)		10	10	1
Discussions (11)		10	110	8
Practice exams (9)		30	270	19
Modules (11)		60	660	46
Case Projects (11)		15	165	12
Final Exam (1)		200	200	14

Point System: There are 1415 total assigned points.

Grade Ranges: A=1274-1415, B=1132-1273, C=991-1131, D=849-990, F=0-848

Schedule: It is tentative and can change during the course of the term. All changes will be located under the "News" section in d2l for the course.

Week:	Module:	Proposed Schedule:	Assignment Due:	Due Date (By Midnight):
Weeks 1-2	One	Orientation and Introductions	Orientation Discussion	Sun., Feb. 1
		View the Student Start-up Guide	Orientation Quiz	
		Do Mod. 1: Security Overview	Complete Mod. 1	
		Using the Simulator	Discussion #1	
			Case Project #1	
Week 3	Two	Do Mod. 2: Access Control	Complete Mod. 2	Sun., Feb. 8
		Identity Management	Discussion #2	
			Case Project #2	
Week 4	Three	Do Mod. 3: Cryptography	Complete Mod. 3	Sun., Feb. 15
			Discussion #3	
			Case Project #3	
Week 5	Four	Do Mod. 4: Policies	Complete Mod. 4	Sun., Feb. 22
		Procedures	Discussion #4	
		Awareness	Case Project #4	
Week 6	Five	Do Mod. 5: Physical Security	Complete Mod. 5	Sun., Mar. 1
			Discussion #5	
			Case Project #5	
Week 7	Six	Do Mod. 6: Perimeter Defenses	Complete Mod. 6	Sun., Mar. 8
			Discussion #6	
			Case Project #6	
Week 8	Seven	Do Mod. 7: Network Defenses	Complete Mod. 7	Sun., Mar. 15
			Discussion #7	
			Case Project #7	
Week 9	Eight	Do Mod. 8: Host Defenses	Complete Mod. 8	Sun., Mar. 22
			Discussion #8	
			Case Project #8	
Week 10	Nine	Do Mod. 9: Application Defenses	Complete Mod. 9	Sun., Mar. 29
			Discussion #9	
			Case Project #9	
		Spring Recess, Mar. 30 through Apr. 5		
Week 11	Ten	Do Mod. 10: Data Defenses	Complete Mod. 10	Sun., Apr. 12
			Discussion #10	
			Case Project #10	
Week 12	Eleven	Do Mod. 11: Assessments	Complete Mod. 11	Sun., Apr. 19
		Audits	Discussion #11	
			Case Project #11	
Week 13		Do Practice Exams for Domains 1-3		Sun., Apr. 26
Week 14		Do Practice Exams for Domains 4-6		Sun., May 3
Week 15		Do Practice Exams for Domains 7-9		Sun., May 10
		Final Exam (identity verification required) Sat., May 16, 11:30-1:30 pm, in BS-153		All work needs to be turned in.