Cosumnes River College
ITIS 160 / CISS 310
Network Security Fundamentals
An Online Course
Fall 2022 8w2

Instructor: Buddy Spisak **Online Office Hours**: Mondays/Wednesdays 1:30 to 3:00 p.m.
Tuesdays/Thursdays 1:30 to 2:30 p.m.
Office: SOC 115
Phone: (916) 691-7062
E-mail: spisakj@crc.losrios.edu The turnaround time for responding to most e-mails is about one to two days. Be sure to include your name and the course number in each e-mail so I can identify who you are and what the e-mail is about.
Course Web page: https://lrccd.instructure.com
Instructor Web page: http://crc.losrios.edu/spisakj/

Prerequisites: None
Advisories: CISN 300 and CISN 304
Lecture/Lab: Fully online (14620) Tuesday 6 to 8 p.m.

Accepted for Credit: CSU
Class Credits: 3 units

Required Textbook: No textbook is required for this course.

Labs: Some labs are done through NDG Netlab+ at https://netlabve6.coastline.edu.

Supplies: Ear buds or a headset would be beneficial when listening to videos and a camera for Zoom conferencing.

A flash drive is recommended (at least 16GB, but 32GB is preferred) to store your work for the class**.**

Course Description:

This course is an introduction to the fundamental principles and topics of Information Technology security and Risk Management at the organizational level. It also addresses hardware, software, processes, communications, applications, and policies and procedures with respect to cyber-security. In addition, this course prepares students for the CompTIA Security+ certification exam. C-ID ITIS 160

Student Learning Outcomes and Course Objectives:

- ANALYZE FUNDAMENTAL SECURITY CONCEPTS (SLO #01).
  - Describe the fundamental principles of information systems security.
  - Define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.
  - Evaluate the need for the careful design of a secure organizational information infrastructure.
  - Explain the need for a comprehensive security model and its implications for the security manager or Chief Security Officer (CSO).

    - Explain the different types of information security careers and how the Security+ certification can enhance a security career.
- DESCRIBE POTENTIAL SYSTEM ATTACKS AND THE ACTORS THAT MIGHT PERFORM 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 basic cryptography, its implementation considerations, and key management.
- DEFINE RISK AND RISK MANAGEMENT (SLO #08).
    - Perform risk analysis and risk management.
    - Describe the components of risk management.
    - Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls.
    - 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 files 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. Describe appropriate measures to be taken should a system compromise occur.

Methods of Measuring Student Learning Outcomes:

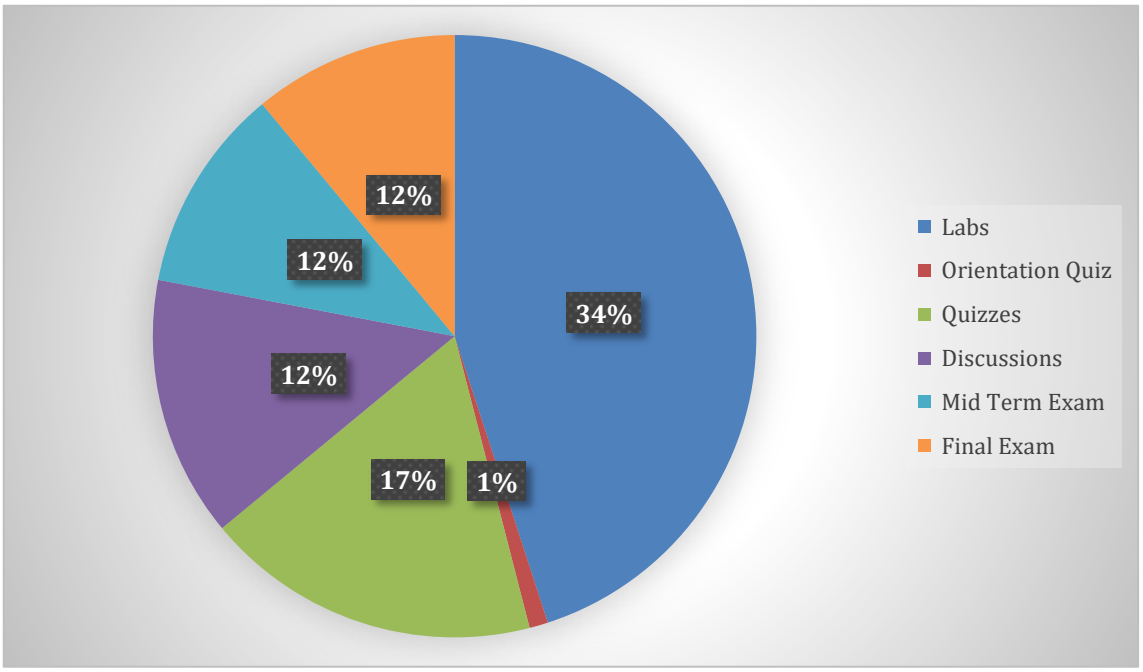
- You will demonstrate knowledge of course concepts through class discussions and achievement on quizzes and a final examination.
- You will demonstrate competence in the coursework by completing lab work and participating in discussions during the semester.

Student Obligations:

- **Attendance**: Since this course is online, it is important to participate frequently in the class.
- **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 e-mail 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 submitted in Canvas. If, for any reason, you cannot access Canvas or are unable to submit the assignment on time, please e-mail it to me instead so that you are not penalized for being late. Quizzes and discussion items cannot be taken past their due dates. If you miss a quiz and you want to make up points, you can take advantage of the extra credit assignments posted in Canvas. 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.
- **Labs**: There will be seven labs credited for homework for the class. The due dates are in the **SCHEDULE** portion of this handout. We will spend a lot of time working on lab activities. Each lab has a set of review questions that you will need to answer in Canvas to receive points for that assignment.
- **Discussions**: I want everyone to take a pro-active approach to learning this material. This includes using the discussion feature in Canvas to ask questions and 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.
- **Language Matters:** Part of communicating effectively with one another involves communicating correctly with one another. This is not an English class; however, I will be looking at and commenting on the basic accuracy of your written English, such as sentence boundaries, spelling, and other basic grammar issues. While you will not fail the class because of your English, you may lose some points for frequent and repeated errors. Keep in mind that your use of English can influence your readers positively—or negatively.
- **Mid-Term Exam and Final Exam**: These exams will be administered through Canvas.
- **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://crc.losrios.edu/about-us/our-values/student-rights-and-responsibilities/student-standards-of-conduct.)
- **CRC Honor Code:** Academic integrity requires honesty, fairness, respect, and responsibility. [See the Cosumnes River College Honor Code posted on the college website (https://crc.losrios.edu/about-us/our-values/student-rights-and-responsibilities/student-honor-code)].

- **E-mail:** 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://sso.losrios.edu then choose the option for *Expired/Forgotten Password* and then *Initial Password and Security Questions Setup*. Now, follow the directions provided.
- **E-mail etiquette:** I will not tolerate rude and demeaning comments or e-mails to anyone in this class. Please keep your comments and e-mails topic related. If I determine that a comment or e-mail 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:** All cell phones, beepers, pagers, etc. should be turned off or set to vibrate during any of the online lectures/labs.
- **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 916-691-7275 as soon as possible.
- **Canvas:** This class utilizes a product called "Canvas." It is highly recommended that you check the website frequently for scheduling updates and homework assignments. Most of the homework assignments and quizzes will be done on Canvas.
- **Online Course Responsibilities:** This course requires significant self-motivation. You must not get behind. Labs 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: total of 162 hours. Allow yourself at least 9 hours per week to complete the activities online, including the time spent writing the class discussion postings. You should plan additional time to read the textbook and study for the quizzes. Some people believe that an on-line 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.
- **Online Access via Zoom:** This class utilizes a product called "Zoom". It is highly recommended that you are in a quiet room without distractions, have stable internet access, and use a video camera with a quality microphone so that you are seen and heard by everyone.

Grading:



Course Topic		Points	Total	Approximate % the of Grade
Orientation Quiz (1)		10	10	1
Discussions (6)		20	120	14
Quizzes (5)		30	150	18
Labs (20)		20	400	45
Mid Term (1)		100	100	11
Final Exam (1)		100	100	11

Point System: There are 880 total assigned points.

Grade Ranges: A=792-880, B=704-791, C=616-703, D=528-615, F=0-527

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

	Day:		Lecture/Lab Schedule:	Assignment Due:	Due Date (By Midnight):
Week 1	Tues.	10/18	Orientation and Introductions	View the Online Orientation	Sun., Oct. 23
			Introduction to Cybersecurity	Orientation Disc.	
			Lab #1	Orientation Quiz	
Week 2	Tues.	10/25	Threats, Attacks and Vulnerabilities	Disc. #1	Sun., Oct. 30
			Lab #2	Lab Review #1	
				Quiz #1	
Week 3	Tues.	11/1	Technologies and Tools	Disc. #2	Sun., Nov. 6
			Labs #3 through 5	Lab Review #2	
				Quiz #2	
			Finishing up the first half of the course	Disc. #3	Sun., Nov. 13
Week 4	Tues.	11/8	Architecture and Design	Lab Review #3-5	
			Mid Term Exam	Quiz #3	
			Labs #6 through 8		
Week 5	Tues.	11/15	Identity and Access Management	Disc. #4	Sun., Nov. 20
			Labs #9 through 12	Lab Review #6-8	
				Mid Term Exam	
Week 6	Tues.	11/22	Risk Management	Disc. #5	Sun., Nov. 27
			Labs #13 through 16	Lab Review #9-12	
				Quiz #4	
Week 7	Tues.	11/29	Cryptography and PKI	Disc. #6	Sun., Dec. 4
			Final Review	Lab Review #13-16	
			Labs #17 through 20	Quiz #5	
			Finishing up the second half of the course		
Week 8	Tues.	12/6	Security and Me	Lab Review #17-20	Fri., Dec. 9
			Final Exam		
			What is next after this class? meeting	Final Exam	All work needs to be turned in Fri., Dec. 9