Cosumnes River College
CISS 356

Introduction to Information Assurance

(Formerly Ethical Hacking)
A Hybrid-Online Course
Summer 2019

Instructor: Buddy Spisak **Online Office Hours:** Mon. 6:00-8:00 p.m. (Jun. 10 to Aug. 2)

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://canvas.losrios.edu
Instructor Web page: http://crc.losrios.edu/spisakj/

Prerequisites: CISS 310 with a grade of "C" or better
Lecture: Online (11750)
Lab: W 6:00 to 9:20 p.m.
Accepted for Credit: CSU
Class Credits: 3 units

Title:	*Hacker Techniques, Tools, and Incident Handling, 3rd ed.*
Author:	Sean-Philip Oriyano
Publishing Info:	Jones and Bartlett Learning, 2020
ISBN10:	1284172600
ISBN13:	9781284172607
E-book ISBN:	9781284172614
Optional Materials:	a flash drive (32gb or larger) to store your work for the class

Course Description:

This course introduces the network security specialist to the various methodologies for attacking a network. Students will be introduced to the concepts, principles, and techniques, supplemented by hands-on exercises, for attacking and disabling a network within the context of properly securing a network.

The course will emphasize network attack methodologies with the emphasis on student use of network attack techniques and tools and appropriate defenses and countermeasures.

Students will receive course content information through a variety of methods: lecture and demonstration of hacking tools will be used in addition to a virtual environment. Students will experience a hands-on practical approach to penetration testing measures and ethical hacking. C-ID ITIS 164

Student Learning Outcomes and Course Objectives:

As a result of completing this course, you will be able to:

SLO #01: UNDERSTAND ETHICAL HACKING CONCEPTS, INCLUDING THE TERM "ETHICAL HACKER", AS WELL AS PENETRATION AND SECURITY TESTING CONCEPTS AND THE DIFFERENCES BETWEEN THEM

- Describe the role of an ethical hacker. Differentiate between what you can or cannot do legally as an ethical hacker.
- Describe how the fundamental concepts of cyber defense can be used to provide system security.
- List the fundamental concepts of the Information Assurance discipline.

SLO #02: DESCRIBE MAJOR CONCEPTS AND ASPECTS OF THE TCP/IP PROTOCOL SUITE, INCLUDING EACH OF THE FOUR LAYERS OF THE PROTOCOL STACK: APPLICATION, TRANSPORT, INTERNET, AND NETWORK

- Describe the TCP/IP protocol stack and be able to review the addressing schemes and how they relate to TCP/IP protocol and security
- Explain the basic concepts of IP addressing.
- Explain the binary, octal, and hexadecimal numbering systems.

SLO #03: CATEGORIZE THE DIFFERENT TYPES OF MALICIOUS SOFTWARE AND THEIR EFFECT ON A SOFTWARE OR HARDWARE

- Critique the physical security attacks and their vulnerabilities.
- Describe the different types of malicious software.
- Classify the different methods of protecting against malware attacks.
- Examine the architecture of a typical, complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed.

SLO #04: EVALUATE THE VARIOUS TOOLS USED FOR PORT SCANNING

- Research the different types of port scans currently being used; the tools available to most hackers; their purpose, and function.
- Reason what ping sweeps are used for.
- Uncover how shell scripting is used to automate security tasks.

SLO #05: ANALYZE SEVERAL NETWORK SECURITY DEVICES THAT SECURITY PROFESSIONALS AND NETWORK ADMINISTRATORS CAN USE TO BETTER PROTECT THEIR NETWORKS

- Describe symmetric and asymmetric encryption algorithms. Describe possible attacks on cryptosystems.
- Critique the advantages and disadvantages of different Intrusion Detection (IDS) technology currently available.
- Critique the advantages and disadvantages of different software firewall technology currently available.
- Investigate honeypots, their purpose and usefulness in a network security plan.

SLO #06: ABILITY TO CREATE SIMPLE SCRIPTS/PROGRAMS TO AUTOMATE AND PERFORM SIMPLE OPERATIONS.

- Demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks).
- Write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL).
- Write simple linear and looping scripts.

Methods of Measuring Student Learning Outcomes:

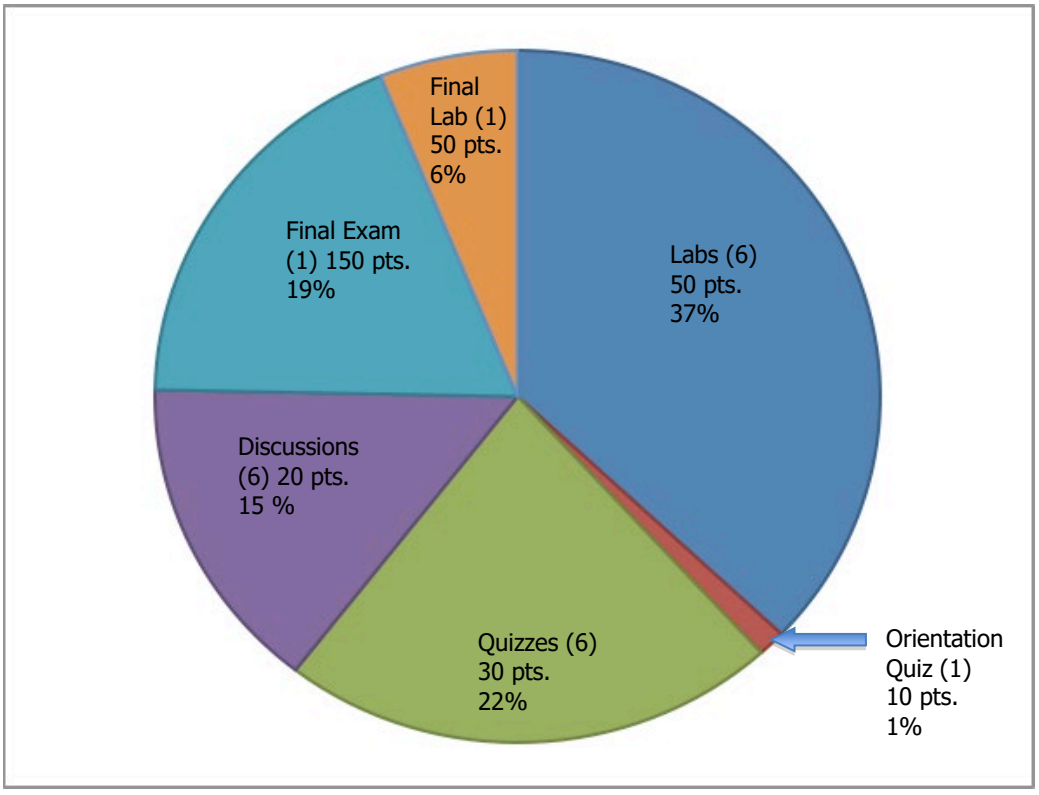
- You will demonstrate knowledge of network and Internet security applications and standards through class discussions and achievement on quizzes and final examination.
- You will demonstrate competence in the coursework by completing lab work and participating in discussions during the semester.

Student Obligations:

- **Attendance**: There will be weekly lab time on campus, and it is up to you to complete the lab assignments during the lab time or at home. Please note that failure to complete 10% of the total course work by the second week of the class may result in your being dropped from the course. Attendance for the on-campus final exam is required. Photo identification is required at the time of the exam to verify your identity.
- **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 submitted in Canvas. If, for any reason, you cannot access Canvas or are unable to submit the assignment on time, please email it to me instead so that you are not penalized for being late. Quizzes cannot be taken, nor can discussion items be completed after 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 six labs credited for homework for the class. The labs will consist of a combination of end-of-chapter review questions, case studies, and activities. The due dates are in the **SCHEDULE** portion of this handout. We will spend a good deal of time working on lab activities. Each lab has a set of review questions that you will need to answer in Canvas in order to receive points for that assignment. If you do the lab work at the college during the regularly scheduled lab time, you will not have to submit your results in Canvas. Instead, I will visually confirm your work and assign your points in class.
- **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.
- **Final Exam**: The final exam will consist of two parts. One part of the exam will be a hands-on practical demonstration of assigned tasks, and the other part will be an exam taken in 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://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 (http://www.crc.losrios.edu/files/resourceguide/CRC-HonorCodeForm.pdf).]
- **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 **http://www.losrios.edu/lrc/lrc_email.php** 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. 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 after class or contact the Office of Disabled Student Programs and Services at 691-7275 as soon as possible.
- **Campus Police**: You can call 558-2221 to request a safety escort.
- **Canvas Learning Management System:** 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 in Canvas.
- **Online Course Responsibilities:** This course requires significant self-motivation. You must not get behind. Labs and weekly assignments can take up to eight 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 4 hours per week in class and 16 hours out of class for this course, a total of 162 hours. Allow yourself at least 12 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 textbook and study for the quizzes. Some people believe that an online framework 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:



Point System: There are 810 total assigned points.

Grade Ranges: A= 729-810, B= 648-728, C= 567-647, D= 486-566, F=0-485

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	Wed.	6/12	Orientation and Introductions	Orientation Discussion Orientation Quiz	Sun., Jun. 16
			Ch 1, Hacking: The Next Generation	View the Online Orientation	
			Ch 2, TCP/IP Review		
			Lab #1		
Week 2	Wed.	6/19	Ch 3, Cryptographic Concepts	Discussion #1 Quiz#1	Sun., Jun. 23
			Ch 4, Physical Security	Lab Review #1	
			Lab #2		
Week 3	Wed.	6/26	Ch 5, Footprinting Tools and Techniques	Discussion #2 Quiz#2	Sun., Jun. 30
			Ch 6, Port Scanning	Lab Review #2	
			Lab #3		
Week 4	Wed.	7/03	Ch 7, Enumeration and Computer System Hacking	Discussion #3 Quiz#3	Sun., Jul. 7
			Ch 8, Wireless Vulnerabilities	Lab Review #3	
			Lab #4		
Week 5	Wed.	7/10	Ch 9, Web and Database Attacks	Discussion #4 Quiz#4	Sun., Jul. 14
			Ch 10, Malware	Lab Review #4	
			Lab #5		
Week 6	Wed.	7/17	Ch 11, Sniffers, Sessions Hijacking, and Denial of Service Attacks	Discussion #5 Quiz#5	Sun., Jul. 21
			Ch 12, Linux and Penetration Testing	Lab Review #5	
			Lab #6		
Week 7	Wed.	7/24	Ch 13, Social Engineering	Discussion #6 Quiz#6	Sun., Jul. 28
			Ch 14, Incident Response and Defensive Technologies		
			Ch 15, Defensive Technologies		
			Final Review	Lab Review #6	
Week 8	Wed.	7/31	Final Exam		Fri., Aug. 2 All work needs to be turned in (11:59pm, Aug. 2).