Cosumnes River College
CISS 342
Implementing Linux Operating System Security
A Hybrid-Online Course
Spring 2018
(Full Term)

Instructor: Buddy Spisak **Office Hours**: Wed. 7:00-8:00 p.m. (Jan. 17 to May 16)
Office: BSS-143
Voice Mail: (916) 286-3691, ext. 14162
Email: spisakj@crc.losrios.edu The turn-around time for responding to most emails is approximately 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
Lab: Wednesday 6:00 to 6:50 p.m. (20189)
Accepted for Credit: CSU
Class Credits: 3 units

Required Textbooks:

Title: *Security Strategies in Linux Platforms and Applications* (2nd ed.)
Authors: Michael Jang and Ric Messier
Publishing Info: Jones and Bartlett Learning, 2017
Textbook ISBN: 978-1-284-09065-9
E-book ISBN: 978-1-284-11028-9

Optional Materials: a 32GB flash drive to store your work for the class

Course Description:

Developers and other IT professionals for their flexibility and openness prize the UNIX family of operating systems. Vulnerabilities in standard configurations, however, can make UNIX systems susceptible to security threats. For the many organizations that depend upon UNIX systems, protection against intrusion is an absolute requirement.

This course provides the knowledge and skills you need to establish security for the Linux platform. It will present in-depth explanations of operating system security features as well as systematic configuration guides for proper operating system configuration.

In addition, this course will cover the knowledge and skills students will need to maintain the integrity, authenticity, availability, and privacy of data.

Student Learning Outcomes and Course Objectives:
Because of completing this course, you will be able to:

EXPLAIN WHAT OPERATING SYSTEM AND NETWORK SECURITY MEANS (SLO #01).
- Discuss why security is necessary.
- Explain the cost factors related to security.
- Describe the types of attacks on operating systems and networks.
- Discuss system hardening, including features in operating systems and networks that enable hardening.

EXPLAIN HOW VIRUSES, WORMS, AND TROJAN HORSES SPREAD (SLO #02).
- Discuss typical forms of malicious software and understand how they work.
- Use techniques to protect operating systems from malicious software and to recover from an attack.

EXPLAIN ENCRYPTION AND AUTHENTICATION METHODS AND HOW THEY ARE USED (SLO #03).
- Discuss attacks on encryption and authentication methods.
- Explain and configure IP Security.

CREATE ACCOUNT NAMING AND SECURITY STRATEGIES (SLO #04).
- Discuss how to develop account naming and security policies.
- Explain and configure user accounts.
- Discuss and configure account policies and logon security techniques.
- Discuss and implement global access privileges.
- Use group policies and security templates.

IMPLEMENT DIRECTORY, FOLDER, AND FILE SECURITY (SLO #05).
- Configure shared resource security, using share permissions in Linux or UNIX.
- Use groups to implement security.
- Troubleshoot security.

CONFIGURE THE FIREWALL CAPABILITIES IN OPERATING SYSTEMS (SLO #06).
- Understand how TCP, UDP, and IP work and understand the security vulnerabilities of these protocols.
- Explain the use of IP addressing on a network and how it is used for security.
- Explain border and firewall security.

EXPLAIN PHYSICAL SECURITY METHODS FOR WORKSTATIONS, SERVERS, AND NETWORK DEVICES (SLO #07).
- Implement a network topology for security.
- Explain network communications media in relation to security.

CONFIGURE SECURITY FOR WIRELESS INTERFACES IN WORKSTATION OPERATING SYSTEMS (SLO #08).
- Explain wireless networking and why it is used.
- Describe IEEE 802.11 radio wave networking.
- Explain Bluetooth networking.
- Describe attacks on wireless networks.
- Discuss wireless security measures.

EXPLAIN HOW E-MAIL CAN BE SECURED THROUGH CERTIFICATES AND ENCRYPTION (SLO #09).
- Discuss general techniques for securing e-mail.
- Configure security in popular e-mail tools.

EXPLAIN HOW TO USE DISASTER RECOVERY TECHNIQUES TO SECURE OPERATING SYSTEMS, PREVENT DATA LOSS, AND REDUCE DOWNTIME (SLO #10).
- Deploy UPS systems.
- Create hardware redundancy and apply fault-tolerance.
- Deploy RAID.
- Back up data and operating system files.
- Understand the relationship between baselining and hardening.
- Explain intrusion-detection methods.
- Use audit trails and logs.
- Monitor logged-on users.
- Monitor a network.

Methods of Measuring Student Learning Outcomes:

- You will demonstrate an understanding of how to make data secure through class discussions and achievement on quizzes and final examination will assess configuring Simple Network Service and File Sharing Services.
- You will demonstrate competence in the coursework by completing lab work and participating in the Canvas discussions during the semester.

Student Obligations:

- **Attendance**: This course is online; however, attending the on-campus orientation on January 17, 2018 and taking the on-campus final exam on May 9, 2018 are required. 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.
- **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 and the discussion items cannot be taken past their due dates.
- **Labs**: There will be six labs credited for homework for the class. The due dates are located 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 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.
- **Canvas Discussions**: I want everyone to take a pro-active approach to learning this material. This includes using the Discussions link 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.
- **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) for additional information.
- **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://sso.losrios.edu/idp/profile/SAML2/Redirect/SSO?execution=e2s1, 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 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:** 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 8 hours to finish. Please do not 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 2 hour per week in class for this course: total of 162 hours. Allow yourself at least 8 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 material and study for the quizzes. Some people believe this is 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
Labs (6)		50	300	37
Orientation Quiz (1)		10	10	1
Quizzes (6)		30	180	22
Discussions (6)		20	120	15
Final Exam (1)		200	200	25

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 course of 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):
Weeks 1-2	Wed.	(1/17)	Orientation and Introductions	View the Online Orientation	Sun., 1/28
			Orientation Discussion	Orientation Quiz	
			Chapter 1: Security Threats to Linux Chapter 2: Basic Components of Linux Security Chapter 3: Starting Off-Getting Up and Running		
			Lab #1		
Weeks 3-4	Wed.	(1/31)	Chapter 4: User Privileges and Permissions Chapter 5: Filesystems, Volumes, and Encryption	(Chapters 1-3) Disc. #1 Quiz #1	Sun., 2/11
			Lab #2	Lab Review #1	
Weeks 5-6	Wed.	(2/14)	Chapter 6: Securing Services	(Chapters 4-5) Disc. #2 Quiz #2	Sun., 2/25
			Lab #3	Lab Review #2	
Weeks 7-8	Wed.	(2/28)	Chapter 7: Networks, Firewalls, and More Chapter 8: Networked Filesystems and Remote Access	(Chapter 6) Disc. #3 Quiz #3 Lab Review #3	Sun., 3/11
			Lab #4		
Weeks 9-10	Wed.	(3/14)	Chapter 9: Networked Application Security Chapter 10: Kernel Security Risk Mitigation	(Chapters 7-8) Disc. #4 Quiz # 4	Sun., 3/25
			Lab #5	Lab Review #4	
			Spring Recess Mar. 26 – Apr. 1 **No class meeting Mar. 28**		
Weeks 11-12	Wed.	(4/4)	Chapter 11: Managing Security Alerts and Updates	(Chapters 9-10) Disc. #5 Quiz #5	Sun., 4/15
			Lab #6	Lab Review #5	
Weeks 13-14	Wed.	(4/18)	Chapter 12: Building and Maintaining a Security Baseline Chapter 13: Testing and Reporting	(Chapter 11) Disc. #6 Quiz #6	Sun., 4/29
				Lab Review #6	
Weeks 15-16	Wed.	(5/2)	Chapter 14: Detecting and Responding to Security Breaches Chapter 15: Best Practices and Emerging Technologies		Wed., 5/9
Final	Wed.	(5/9)	Final Exam from 6:00-6:50pm, BSS-153		All work due today