Cosumnes River College
CISS 341
Implementing Windows Operating System Security
A Hybrid-Online Course
Fall 2016

Instructor: Buddy Spisak

Office Hours: Mon. 6:00-7:00 p.m. (Aug. 29th to Dec. 12th)
Office Location: SOC-109

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://d2l.losrios.edu/
Instructor Web page: http://crc.losrios.edu/spisakj

Prerequisites: CISS 310
Advisory: CISC 308
Lecture: Online (20072)
Lab: Wednesday 7:00 to 9:35 p.m. (19494)
Accepted for Credit: CSU
Class Credits: 3 units

Required Textbooks:

Title:	*Security Strategies in Windows Platforms and Applications* (2nd edition)
Authors:	Michael Solomon
Publishing Info:	Jones and Bartlett Learning, 2014
ISBN13:	978-1-284-15843-4 (textbook bundle with lab)
ISBN13:	978-1-284-23973-7 (ebook bundle with lab)

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

Course Description:

As organizations increasingly come to rely on Windows-based networks, it is essential that system administrators have a complete understanding of the security models integral to Windows Server and Workstation. This course will provide in depth explanations of operating system security features as well as step-by-step configuration guides for proper operating system configuration. It also provides the knowledge and skills students will need to know in order to maintain the integrity, authenticity, availability, and privacy of data.

Student Learning Outcomes and Course Objectives:

As a result 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 Windows.
- 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 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 the Desire 2 Learn discussions during the semester.

Student Obligations:

- **Attendance**: Since this course is hybrid, it is important to attend the first day of class on campus for the orientation on Wednesday, Aug. 24, and the on-campus final exam on Wednesday, Dec. 14. 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 Desire 2 Learn (d2l) under the "Dropbox" link. If, for any reason, you cannot access d2l 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 d2l 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 d2l. Instead, I will visually confirm your work and assign your points in class.
- **Desire 2 Learn 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.
- **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 d2l.
- **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 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 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.
- **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. Most of the homework assignments and quizzes will be done on d2l.
- **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 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 54 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 (10)		50	500	47
Orientation Quiz (1)		10	10	0
Quizzes (14)		15	210	20
Discussions (14)		10	140	13
Final Exam (1)		200	200	20

Point System:

There are 1060 total assigned points.

Grade Ranges:

A= 954-1060, B= 848-953, C= 742-847, D=636-741, F=0-635

Schedule: It is tentative and can change during the course of the term. All changes will be located under the "News" section in Desire 2 Learn for the course.

	Day:		Lecture/Lab Schedule:	Assignment Due:	Due Date (By Midnight):
Week 1	Wed.	8/24	Orientation and Introductions	View the Online Orientation	Sun., 8/28
			Chapter 1: Microsoft Windows and the Threat Landscape	Orientation Disc. Orientation Quiz	
Week 2	Wed.	8/31	Chapter 2: Security in the Microsoft Windows Operating System	(Chapter 1) Disc. #1 Quiz #1	Sun., 9/4
			Lab #1: Implementing Access Controls with Windows Active Directory		
Week 3	Wed.	9/7	Chapter 3: Managing and Maintaining Microsoft Windows Security	(Chapter 2) Disc. #2 Quiz #2	Sun., 9/11
			Lab #2: Using Access Control Lists to Modify File System Permissions on Windows Systems	Lab Review #1	
Week 4	Wed.	9/14	Chapter 4: Microsoft Windows Encryption Tools and Technologies	(Chapter 3) Disc. #3 Quiz #3	Sun., 9/18
			Lab #3: Configuring BitLocker and Windows Encryption	Lab Review #2	
Week 5	Wed.	9/21	Chapter 5: Protecting Microsoft Windows Against Malware	(Chapter 4) Disc. #4 Quiz #4	Sun., 9/25
			Lab #4: Identifying and Removing Malware from Windows Systems	Lab Review #3	
Week 6	Wed.	9/28	Chapter 6: Group Policy Control in Microsoft Windows	(Chapter 5) Disc. #5 Quiz #5	Sun., 10/2
				Lab Review #4	
Week 7	Wed.	10/5	Chapter 7: Microsoft Windows Security Profile and Audit Tools	(Chapter 6) Disc. #6 Quiz #6	Sun., 10/9
			Lab #5: Managing Group Policy Objects Within the Microsoft Windows Environment		
Week 8	Wed.	10/12	Chapter 8: Microsoft Windows Backup and Recovery Tools	(Chapter 7) Disc. #7 Quiz #7	Sun., 10/16
			Lab #6: Creating a Scheduled Backup and Replicating System Folders	Lab Review #5	

Note: Schedule continued onto next page.

	Day:		Lecture/Lab Schedule:	Assignment Due:	Due Date (By Midnight):
Week 9	Wed.	10/19	Chapter 9: Microsoft Windows Network Security	(Chapter 8) Disc. #8 Quiz #8	Sun., 10/23
				Lab Review #6	
Week 10	Wed.	10/26	Chapter 10: Microsoft Windows Security Administration	(Chapter 9) Disc. #9 Quiz #9	Sun., 10/30
Week 11	Wed.	11/2	Chapter 11: Hardening the Microsoft Windows Operating System	(Chapter 10) Disc. #10 Quiz #10	Sun., 11/6
			Lab #7: Securing Servers with the Security Configuration Wizard and Windows Firewall		
Week 12	Wed.	11/9	Chapter 12: Microsoft Application Security	(Chapter 11) Disc. #11 Quiz #11	Sun., 11/13
			Lab #8: Securing Internet Client and Server Applications on Windows Systems	Lab Review #7	
Week 13	Wed.	11/16	Chapter 13: Microsoft Windows Incident Handling and Management	(Chapter 12) Disc. #12 Quiz #12	Sun., 11/20
			Lab #9: Protecting Digital Evidence, Documentation, and the Chain of Custody	Lab Review #8	
Week 14	Wed.	11/23	Chapter 14: Microsoft Windows and the Security Life Cycle	(Chapter 13) Disc. #13 Quiz #13	Sun., 11/27
				Lab Review #9	
Week 15	Wed.	11/30	Chapter 15: Best Practices for Microsoft Windows and Application Security	(Chapter 14) Disc. #14 Quiz #14	Sun., 12/4
			Lab #10: Hardening Windows Server Security Using Microsoft Baseline Security Analyzer		
			Final Review		
Week 16	Wed.	12/14	Final Exam (8 to 10 p.m.)		Sun., 12/11
				Lab Review #10	All work needs to be turned in.