Saint Leo University
Graduate Business Studies

COM520
Systems Security Management

Course Description:
Securing the systems that run our computers is the key to ensuring that our essential information remains safe and available. This course provides a foundation in systems security principles, disaster recovery principles and planning, and the importance of incident response planning and execution to minimize downtime. A computer system with appropriate software will be required.

Prerequisite:
COM 510

Textbooks:

Student Note: Students ordering from our online bookstore will access the materials from the links in the course. There is nothing to receive from the bookstore once the order has been placed. This class has direct digital access within the course.

Created From the National lab package:

Solomon. *Security Strategies in Windows Platform & Apps* (Print book package with lab access) (3rd ed.). Jones & Bartlett Learning. ISBN: 9781284266375

Learning Outcomes:
- Describe and explain the terminology involved in the management of systems security.
- Describe and explain the software threats to systems security and the methods required for maintaining security.
- Explain and demonstrate policies, programs, and procedures for prevention of unauthorized internal access.
- Describe and explain systems security management policies and procedures for dealing with wireless, Web, remote access, VPN, and email security.
- Describe and explain systems and security through disaster planning, monitoring, and auditing.
- VALUES OUTCOME: Students will demonstrate an understanding of the Saint Leo University core value Personal Development, including the criticality of Ethical Behavior, in using computers in an organizational environment.

Core Value:
Personal Development: Saint Leo University stresses the development of every person's mind, spirit, and body for a balanced life. All members of the Saint Leo University community must demonstrate their commitment to personal development to help strengthen the character of our community.

Evaluation:

Quizzes	20%
Assignments	60%
Discussions	20%

Grading Scale:

Grade	**Score (%)**
A	95-100

A-	90-94
B+	86-89
B	83-85
B-	80-82
C	75-79
F	Below 75

Assignments: Each module will have written and/or laboratory assignments that need to be completed and uploaded by the end of the module. Note that the lab can only be accessed through some browsers such as IE, but not via some others such as Chrome.

Quizzes: There are four quizzes in the course, one for every two modules, and will consist of multiple-choice questions. They are designed to ensure that you have read and understood the material in the text for the chapters covered in the quiz.

Discussion/Participation: Each module will include a discussion assignment (Module 1 will also include an additional “Introduction” topic). For each discussion topic, you are required to post an initial response to the question, as well as substantial responses to at least two classmates. Your original discussion postings are supposed to be based on research. Simply repeating the text is neither adequate nor appropriate. Since you are doing research in the discussion questions, you are required to provide a citation of where you got the material. The purpose of this is for you to provide up-to-date material from the Internet or other appropriate sources (NOT Wikipedia) to help your classmates. Similarly, simply saying what a wonderful job your classmate did on his or her posting is not adequate. You are expected to provide constructive comments adding to the discussion.

Course Schedule:

Module 1 **Security Features in Microsoft Windows**

Objectives **At the conclusion of this module, you will be able to:**

- Discuss the tenets of information security: A-I-C Triad.
- List the main objectives and describe the limitations of liability in the Microsoft EULA.
- Categorize Windows threats and vulnerabilities.
- Describe the basic Windows OS architecture.
- Discuss access controls and authentication.
- Explain security tokens, rights, and permissions.
- Identify and discuss the purposes and features of users, groups, and directory services.
- Summarize the fundamentals of Microsoft Windows security monitoring and maintenance.

Assignments

Items to be Completed:	**Due No Later Than:**
Post an introduction to the class	Thursday 11:59 PM EST/EDT
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Written Assignment 1	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 1	Sunday 11:59 PM EST/EDT

Module 2 **Encryption, Authentication, and Account-based Security**

Objectives **At the conclusion of this module, you will be able to:**

- Differentiate between identification, authentication, and authorization.
- Illustrate the use of Windows ACLs.
- Identify forms of identification in Microsoft Windows.
- Examine auditing and tracking Microsoft Windows access.
- Outline best practices for managing Microsoft Windows and application vulnerabilities.
- Identify encryption methods supported by Microsoft Windows.
- Explain setup and enabling of file, folder, and volume level encryption.
- Outline encrypted Microsoft Windows protocols.
- Describe PKI and security certificates.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	

Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Written Assignment 2	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 2	Sunday 11:59 PM EST/EDT
Complete Quiz 1	Sunday 11:59 PM EST/EDT

Module 3 **Protecting Microsoft Windows Systems**

Objectives **At the conclusion of this module, you will be able to:**

- Classify and explain the effects and working of malicious code.
- Identify strategies for maintaining a malware-free environment.
- Outline best practices for malware prevention.
- Explain Group Policy and Group Policy Objects (GPO).
- Recognize the relationship between Group Policy and security policy.
- Illustrate how to make Group Policy conform to security policy.
- Describe GPOs in the Windows registry and Active Directory.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Written Assignment 3	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 3	Sunday 11:59 PM EST/EDT

Module 4 **Microsoft Windows Auditing and Backup/Recovery Tools**

Objectives **At the conclusion of this module, you will be able to:**

- Describe the need for profiling the security of a Windows system.
- Explain how to use common Windows security profiling tools.
- Explain the process of auditing Windows security.
- Describe how to use Windows security audit tools.
- Describe Microsoft Windows Operating System and application backup and recovery techniques.
- Compare different options for creating backups.
- Incorporate backups and restore operations into a business continuity plan.
- Use virtual images to create backups.

Assignments

Items to be Completed:	Due No Later Than:
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Written Assignment 4	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 4	Sunday 11:59 PM EST/EDT
Complete Quiz 2	Sunday 11:59 PM EST/EDT

Module 5 **Securing Microsoft Windows Networks**

Objectives **At the conclusion of this module, you will be able to:**

- Describe goals for securing Microsoft Windows networks.
- Secure Microsoft Windows networking services.
- Secure Microsoft Windows wireless networks.
- Secure Microsoft Windows workstations and servers.
- Describe Microsoft Windows OS security administration.
- Maintain the A-I-C Triad in the Microsoft Windows OS.
- Ensure due diligence and regulatory compliance.
- Explain the need for security policies, standards, procedures, and guidelines.

Assignments

Items to be Completed:	Due No Later Than:
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Written Assignment 5	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 5	Sunday 11:59 PM EST/EDT

Module 6 **Securing the Microsoft Windows Operating System and Applications**

Objectives **At the conclusion of this module, you will be able to:**

- Describe the Windows Operating System hardening process.
- Harden all aspects of Windows computers and network environments.
- Provide security training and awareness.
- Describe the principles of Microsoft application security.
- Secure Microsoft client applications.
- Secure Microsoft server applications.
- Apply lessons learned from application security case studies.

Assignments

Items to be Completed:	Due No Later Than:
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Written Assignment 6	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 6	Sunday 11:59 PM EST/EDT
Complete Quiz 3	Sunday 11:59 PM EST/EDT

Module 7 **Microsoft Windows Incident Handling and Management**

Objectives **At the conclusion of this module, you will be able to:**

- Describe Microsoft Windows OS security incidents.
- Use available tools to handle and manage security incidents.
- Investigate incidents, including acquiring and managing evidence.

Assignments

Items to be Completed:	Due No Later Than:
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Written Assignment 7	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 7	Sunday 11:59 PM EST/EDT

Module 8 **Security Life Cycle and Microsoft Windows Best Practices**

Objectives **At the conclusion of this module, you will be able to:**

- Describe system life-cycle phases.
- Manage the existing Microsoft Operating System and application software security.
- Implement, evaluate, and test Microsoft Operating System and application software.
- Describe how to manage the process of secure software development.
- Describe basic rules of Microsoft Windows Operating System and application security.
- Use best practices for securing Microsoft Windows Operating System and application software.

- Explain trends in Microsoft Windows Operating System and application software security management.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Written Assignment 8	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 8	Sunday 11:59 PM EST/EDT
Complete Quiz 4	Sunday 11:59 PM EST/EDT