Saint Leo University

COM 221
Fundamentals of Cybersecurity

Course Description:
The advent of global networks has provided communication capabilities for businesses and individuals unparalleled in the history of the world. Attacks on the system that deny service, destroy systems, and purloin information through the use of worms, viruses, and other criminal attacks make it imperative that information security be a significant part of any business plan and that individuals working in that or allied fields become knowledgeable in the principles of information security. This course provides an introduction to the field of information security that lays a necessary foundation for later courses.

Prerequisite:
COM 203

Textbooks*:*
Ciampa - Bundle: CompTIA Security+ Guide to Network Security Fundamentals, Loose-Leaf Version, 6th + MindTap Information Security, 1 term (6 months) Printed Access Card ISBN: 9781337685856

Learning Outcomes:

1. Describe and explain the key terms, essential concepts and origins of the field of information security;
2. Describe and explain the process involved in performing a security analysis including identifying, assessing and controlling risk;
3. Describe and explain the logical design of the accepted security models to the physical design and frameworks including business practices and standards, security policy, technologies employable, planning for information security;
4. Describe and explain the implementation of an information security system including outsourcing, change management, and personnel management;
5. **VALUES OUTCOME**: To achieve success in information security a high degree of **Integrity** and **Respect** for privacy is required. It is necessary for the security analyst to be discrete and not to exploit the discovered vulnerabilities of an organization. These core values are inherent to this course and frequently come up in discussions.

Evaluation:
A: Test (40%)
B: Labs (50%)
C: Participation (or Discussion)
(10%)

A. Test:
A minimum of four quizzes is recommended. It is recommended that one is given in the second module, fourth, sixth and eighth module.

Pre/Post Assessment: Provides students and instructors with a student's current base line (prior to taking the course) and post-course knowledge on the concepts reviewed in the course. **** Note- this (pre-assessment) should be evaluated at a lesser percentage value to ensure completion, yet provide fairness for those who are not yet familiar with the concepts outlined in the course.*

Student Requirements:

- **Pre-Assessment**: The students will be required to take the ***Pre-Assessment*** in M1 at the start of the course.
- **Post-Assessment**: The Post Assessment is a cumulative assessment that represents what students would be asked and seen if student takes the CompTia Security+ Exam. Therefore, this test will be assessed as the cumulative final for the course to quantify students' knowledge gain.

B. Labs:
Students will reinforce their knowledge with hands-on sessions included in the textbook. Each chapter will have lab. Students submit their findings in the lab for assessment.

C. Participation (or Discussion):
Students will engage in weekly discussions on topics related to topics on big data and data analytics. Students may be provided assigned reading, asked to research an assigned topic, or discuss assigned business cases. Each student will be required to post a discussion question and respond to two others posted by other students in the class.

Assessment of the Learning Outcomes:

Course Learning Outcome	Assessment Method
1	Lab, Test, Discussion
2	Lab, Test, Discussion
3	Lab, Test, Discussion
4	Lab, Test, Discussion

The following distribution will be used in assigning grades (decimal points will be rounded to the nearest whole number at semester's end)**:**

A	Exceptional	67% to 69%
A-	Superior	90% to 93%
B+	Excellent	87% to 89%
B	Very Good	84% to 86%
B-	Good	80% to 83%
C+	Above Average	77% to 79%
C	Average	74% to 76%
C-	Below Average	70% to 73%
D+	Marginal	67% to 69%
D	Poor	60% to 66%
F	Failure	Below 60%

Course Schedule:

Module 1 **Introduction to Security | Threats**

Objectives When you complete this module, you should be able to:

- Describe the challenges if securing information.
- Define information security and explain why it is important.
- Identify and list the types of attackers that are common today.
- Define malware.
- List different types of malware and identify the payloads.
- Describe the types of social engineering psychological and physical attacks.

Readings Chapters 1 and 2

Assignments

Items to be Completed:	**Due No Later Than:**
Post an introduction to the class	Thursday 11:59 PM EST/EDT
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 Labs and Labs	Sunday 11:59 PM EST/EDT
Complete MindTap Module 1 Activities	Sunday 11:59 PM EST/EDT

Module 2 **Network Security Device, Design, and Technology**

Objectives When you complete this module, you should be able to:

- List and explain the different types of server-side web application attacks.
- Define client-side attacks.
- Explain how overflow attacks work.
- List different types of networking-based attacks.
- List the steps for securing a host computer.
- Define application security.
- Explain how to secure data.

Readings Chapters 5 and 6

Assignments

Items to be Completed:	**Due No Later Than:**
Post an introduction to the class	Thursday 11:59 PM EST/EDT
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 Labs	Sunday 11:59 PM EST/EDT
Complete MindTap Module 2 Activities	Sunday 11:59 PM EST/EDT

Module 3 **Cryptography**

Objectives

When you complete this module, you should be able to:

- Describe the challenges of securing information.
- Define cryptography
- Describe hash, symmetric, and asymmetric cryptographic algorithms.
- List the various ways in which cryptography is used.
- Define digital certificates.
- Describe the components of Public Key Infrastructure (PKI).
- List the tasks associated with key management.
- Describe the different transport encryption protocols.

Readings

Chapters 3 and 4

Assignments

Items to be Completed:	**Due No Later Than:**
Post an introduction to the class	Thursday 11:59 PM EST/EDT
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 Labs	Sunday 11:59 PM EST/EDT
Complete MindTap Module 3 Activities	Sunday 11:59 PM EST/EDT

Module 4 **Network Security Fundamentals**

Objectives When you complete this module, you should be able to:

- List the different types of network security devices and how they can be utilized.
- Explain how network technologies
- Describe secure network design elements.
- List and describe the functions of common network protocols.
- Explain how network administration principles can be applied.
- Define different network applications and how they can be secured.

Readings Chapters 7 and 8

Assignments

Items to be Completed:	**Due No Later Than:**
Post an introduction to the class	Thursday 11:59 PM EST/EDT
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 Labs	Sunday 11:59 PM EST/EDT
Complete MindTap Module 4 Activities	Sunday 11:59 PM EST/EDT

Module 5 **Device Security**

Objectives When you complete this module, you should be able to:

- List the steps for securing a client device
- Define application security
- Explain how physical security can be used for protection
- List ways to secure a mobile device
- Describe different types of embedded systems and IoT devices and how to secure them

Readings Chapters 9 and 10

Assignments

Items to be Completed:	**Due No Later Than:**
Post an introduction to the class	Thursday 11:59 PM EST/EDT
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 Labs	Sunday 11:59 PM EST/EDT
Complete MindTap Module 5 Activities	Sunday 11:59 PM EST/EDT

Module 6 **Access Control Fundamentals | Authentication and Account Management**

Objectives When you complete this module, you should be able to:

- Define access control and list the four access control models.
- Describe how to implement access control.
- Explain the different types of authentication services.
- Describe the different types of authentication credentials.
- Explain what single sign-on can do.
- List the account management procedures for securing passwords.

Readings Chapters 11 and 12

Assignments

Items to be Completed:	**Due No Later Than:**
Post an introduction to the class	Thursday 11:59 PM EST/EDT
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 Labs	Sunday 11:59 PM EST/EDT
Complete MindTap Module 6 Activities	Sunday 11:59 PM EST/EDT

Module 7 **Vulnerability Assessment**

Objectives When you complete this module, you should be able to:

- Define vulnerability assessment and explain why it is important.
- Explain the differences between vulnerability scanning and penetration testing.
- Describe the security implications of integration with third parties.
- List techniques for mitigating and deterring attacks.

Readings Chapter 13

Assignments

Items to be Completed:	**Due No Later Than:**
Post an introduction to the class	Thursday 11:59 PM EST/EDT
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 Labs	Sunday 11:59 PM EST/EDT
Complete MindTap Module 7 Activities	Sunday 11:59 PM EST/EDT

Module 8 **Business Continuity & Risk Management**

Objectives When you complete this module, you should be able to:

- Define business continuity.
- List the features of a disaster recovery plan.
- Explain different environmental controls.
- Describe forensics and incident response produces.
- Explain how to control risk.
- List the ways in which security policies can reduce risk.
- Describe how awareness and training can provide increased security.

Readings Chapters 14 and 15

Assignments

Items to be Completed:	**Due No Later Than:**
Post an introduction to the class	Thursday 11:59 PM EST/EDT
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 Labs	Sunday 11:59 PM EST/EDT
Complete MindTap Module 8 Activities	Sunday 11:59 PM EST/EDT