JOHN A. LOGAN COLLEGE
COURSE SYLLABUS

General Information

Course: CIS 208 – Security Awareness
IAI No: NA
Semester:
Section:
Time:
Room:
Credit Hours: 3
Lecture Hours: 2
Lab Hours: 2

Instructor Information

Name: Roger Jeter
Office: B75A
Virtual Office Hours:

Monday	
Tuesday	
Wednesday	
Thursday	
Friday	

Phone:
Email:

Course Textbook & Materials

Prowse. CompTIA Security+ SY0-501. 2nd Edition. Pearson, 2017
ISBN: 9780789759122

Prowse. CompTIA Security+ SY0-501 Pearson uCertify and Labs Student Access Card. 2nd Edition. Pearson, 2017.
ISBN: 9780789759139

Course Prerequisites

NA

Course Description

This course is designed to provide a security awareness overview and emphasize the importance of information systems as well as the home computer system will be covered. Issues will include personal, Internet, and organizational security. Types of security attacks will be discussed, prevention methods will be determined, and recovery plans will be developed. Policies and procedures that will assist in preventing an invasion of privacy will be covered.

Course Objectives

1. Understand the need for information security and concepts of the Information Assurance/Cyber Defense discipline.
2. Describe Cyber Defense tools, methods and components.
3. Describe legal, ethical, professional, and public relations implications of security and privacy issues.
4. Plan for and respond to intruders in an information system.
5. Identify the different types of attacks used by potential intruders.
6. Determine the steps to take if an information system has been attacked.
7. Identify the elements of a cryptographic system.
8. Describe the differences between symmetric and asymmetric algorithms
9. Describe which cryptographic protocols, tools and techniques are appropriate for different situations.
10. Describe how cryptography can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation.
11. Apply Cyber Defense methods to prepare a network or information system to prevent intrusion.
12. Understand the concepts behind the use of a firewall to prevent unauthorized access.
13. Determine the importance of an Intrusion Detection System.
14. Explain why anonymity may be one of the best forms of security.
15. Understand the importance of dependability, reliability and participation.
16. Describe how the fundamental concepts of cyber security can be one of the best forms of security.

College-Wide Student Learning Outcomes

The faculty and staff of John A. Logan College are committed to providing students with opportunities to develop learning abilities that will last a lifetime. Graduates will be prepared to succeed in their personal and professional lives because of achieved competence in the following student learning outcomes. In this course, students will be assessed in the following learning outcome:

	Communication: Students express thoughts, ideas, and feelings in both written and oral modes.
	Critical Thinking: Students apply a rational and methodical approach to problem solving based on use of appropriate evidence.
	Cultural and Global Awareness: Students demonstrate an understanding of the influence of culture and society.
	Information Literacy: Students locate, evaluate, retrieve, organize, create, and disseminate information.
	Quantitative Reasoning: Students use and understand numbers to interpret, evaluate, and express information in quantitative terms.

Topic Outline

Chapter 1: Introduction to Security
Chapter 2: Computer Systems Security Part 1
Chapter 3: Computer Systems Security Part 2
Chapter 4: OS Hardening and Virtualization
Chapter 5: Application Security
Chapter 6: Network Design Elements
Chapter 7: Networking Protocols and Threats
Chapter 8: Network Perimeter Security
Chapter 9: Securing Network Media and Devices
Chapter 10: Physical Security and Authentication Models
Chapter 11: Access Control Methods and Models
Chapter 12: Vulnerability and Risk Assessment
Chapter 13: Monitoring and Auditing
Chapter 14: Encryption and Hashing Concepts
Chapter 15: PKI and Encryption Protocols
Chapter 16: Redundancy and Disaster Recovery
Chapter 17: Social Engineering, User Education, and Facilities Security
Chapter 18: Policies and Procedures
Chapter 19: Taking the Real Exam

Course Schedule

Tentative Assignment Schedule

Week	Unit	Assignments
Week 1	Chapter1: Introduction to Security Chapter 2: Computer Systems Security Part 1	Chapter 1 Quiz, Chapter 1 Labs Chapter 2 Quiz, Chapter 2 Labs

Week 2	Chapter 3: Computer Systems Security Part 2 Chapter 4: OS Hardening and Virtualization	Chapter 3 Quiz, Chapter 3 Labs Chapter 4 Quiz, Chapter 4 Labs
Week	**Unit**	**Assignments**
Week 3	Chapter 5: Application Security Chapter 6: Network Design Elements	Chapter 5 Quiz, Chapter 5 Labs Chapter 6 Quiz, Chapter 6 Labs
Week 4	Chapter 7: Networking Protocols and Threats	Chapter 7 Quiz, Chapter 7 Labs
Week 5	Chapter 8: Network Perimeter Security	Chapter 8 Quiz, Chapter 8 Labs
Week 6	Chapter 9: Securing Network Media and Devices	Chapter 9 Quiz, Chapter 9 Labs
Week 7	Chapter 10: Physical Security and Authentication Models	Chapter 10 Quiz, Chapter 10 Labs
Week 8	Chapter 11: Access Control Methods and Models	Chapter 11 Quiz, Chapter 11 Labs
Week 9	Chapter 12: Vulnerability and Risk Assessment	Chapter 12 Quiz, Chapter 12 Labs
Week 10	Chapter 13: Monitoring and Auditing	Chapter 13 Quiz, Chapter 13 Labs
Week 11	Chapter 14: Encryption and Hashing Concepts	Chapter 14 Quiz, Chapter 14 Labs
Week 12	Chapter 15: PKI and Encryption Protocols	Chapter 15 Quiz, Chapter 15 Labs
Week 13	Chapter 16: Redundancy and Disaster Recovery Chapter 17: Social Engineering, User Education, and Facilities Security	Chapter 16 Quiz, Chapter 16 Labs Chapter 17 Quiz
Week 14	Chapter 18: Policies and Procedures Chapter 19: Taking the Real Exam	Chapter 18 Quiz
Week 15	Exam	Exam
Week 16	Finals	

Method of Presentation

Lecture/Demonstration
Discussion
Research
Simulations

Method of Evaluation

Course Information Quiz: There will be one quiz **in D2L** covering the information contained in the course syllabus and course information document. That quiz will be worth 20 points.

Quizzes: There will be 18 quizzes **in D2L,** one per textbook chapter. Each will be worth 10 points.

Labs: There will be 15 chapters with labs **in Ucertify**. Screen shots or print screen captures of completed labs must be submitted to the appropriate D2L Dropbox. Each chapter of labs will be worth 20 points.

Exam: There will be one exam **in D2L** worth 100 points.

1 Course Information Quiz @ 20 points	**20**
18 chapter quizzes @ 10 points each	**180**
15 Ucertify Dropbox labs @ 20 points each	**300**
1 Exam @ 100 points	**100**
Total	**600**

Grading Scale:

A: 90% - 100%
B: 80% – 89%
C: 70% - 79%
D: 60% – 69%
F: 0% – 59%

Specific Course Requirements

Student Responsibilities: The student is required to read and study the textbook materials. Students are responsible for all discussion, assignments, and announcements made in class and posted on the course Web site. ***Note:*** *All inquiries/questions should be directed to the instructor via e-mail. A response time of 24 hours Mon. – Fri. by noon and 48 hour response time Fri. noon – Sun. will be observed by both the instructor and students.*

Academic Dishonesty: Academic dishonesty will not be tolerated. If it is found that a student has been dishonest regarding academics, a zero will be given for said exercise, assignment, project, or test. In addition, academic dishonesty may result in expulsion, suspension, probation, or reprimand by the vice-president for administration. Please refer to Article IV, p. 34 of the John A Logan College's *Students Rights and Responsibilities: A Code of Conduct* publication.

Recording of lectures: You may not tape record any part of the lectures without the written permission from the instructor.

Class Conduct: Students are to behave in a respectful manner while in the classroom. Respect should be given to the classroom instructor, classmates, and classroom activities. Students should not engage in activities that will distract from the learning environment. Therefore, the following conduct must be followed:

- Students are to give the instructor/presenter their full attention during presentations.
- Students should not be working on anything other than class material during class time.
- Students should not be surfing the Internet, checking e-mail, instant messaging, playing games, etc., during class time.
- Personal electronic device activity such as: cell phones, lap tops, PDA's, iPods, etc., are not permitted in the classroom without prior permission.
- Software should not be disabled on classroom computers.
- **Cell Phones if your cell phone goes off in class you will be asked to leave and receive an absence for the day.**

If, during lab time, all assigned class work has been completed and submitted for grading, the students may engage in other school related activities while in the computer lab. However, under **NO** circumstances should a student be doing anything other than what the instructor is presenting during lectures.

If students engage in activities contrary to the above, the following procedures will be adhered to:

- First Offense – students will be warned and counted absent for the day.
- Second Offense – students will be asked to leave the classroom with no questions asked and will lose all attendance points for the class.
- Third Offense – students will be asked to leave the classroom and will not be allowed back until they have met with the department chair. Students could at this time, be subject to expulsion from the class.

Additional College Information and Resources

Please see the JALC Syllabus Attachment