ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSC 2204 Security +

Date: August 28, 2018

Credit Hours: 3

Prerequisite(s): CSN 1225

Delivery Method:		
	☒ **Lecture**	**2 Contact Hours (1 contact = 1 credit hour)**
	☐ **Seminar**	**0 Contact Hours (1 contact = 1 credit hour)**
	☒ **Lab**	**2 Contact Hours (2-3 contact = 1 credit hour)**
	☐ **Clinical**	**0 Contact Hours (3 contact = 1 credit hour)**
	☒ **Online**	
	☒ **Blended**	

Offered: ☒ **Fall** ☐ **Spring** ☐ **Summer**

IAI Equivalent –***Only for Transfer Courses***-go to *http://www.itransfer.org*:

CATALOG DESCRIPTION:
This course focuses on CompTIA's Security+ Certification exam. Currently the SY0-501 exam consists of six domains: Threats, Attacks and Vulnerabilities; Technologies and Tools; Architecture and Design; Identity and Access Management; Risk Management; and Cryptography and PKI. This course is designed to provide you with the foundational knowledge necessary to prepare you to sit for the Security+ certification exam.

GENERAL EDUCATION GOALS ADDRESSED

[See last page for Course Competency/Assessment Methods Matrix.]

Upon completion of the course, the student will be able:

[Choose up to three goals that will be formally assessed in this course.]

☐ To apply analytical and problem solving skills to personal, social, and professional issues and situations.
☒ To communicate successfully, both orally and in writing, to a variety of audiences.
☐ To construct a critical awareness of and appreciate diversity.
☐ To understand and use technology effectively and to understand its impact on the individual and society.
☐ To develop interpersonal capacity.
☐ To recognize what it means to act ethically and responsibly as an individual and as a member of society.
☐ To recognize what it means to develop and maintain a healthy lifestyle in terms of mind, body, and spirit.
☒ To connect learning to life.

EXPECTED LEARNING OUTCOMES AND RELATED COMPETENCIES:

[Outcomes related to course specific goals. See last page for more information.]

Upon completion of the course, the student will be able to:

1. Understand the different types of threats, attacks and vulnerabilities
   1.a. Discuss the different forms of malware
   1.b. Understand the different types of attacks
   1.c. Understand the benefits of vulnerability scanning

2. Describe the various technologies and tools used with Security
   2.a. Discuss the basic security components
   2.b. Use Command Line and Software Security tools
   2.c. Analyze Security output

3. Explain the frameworks used in Security Architecture and Design.
   3.a. Explain Defense in Depth
   3.b. Describe Secure Network Topologies
   3.c. Understand Cloud Technologies and virtualization
   3.d. Understand redundancy, fault tolerance and high availability

4. Understand Identity and Access Management
   4.a. Discuss Access Control and Access Management
   4.b. Understand Account Management

5. Identify the components in a Risk Management Plan
   5.a. Assess Security Policies
   5.b. Perform a Business Impact Analysis
   5.c. Understand the Risk Management Process

6. Explain Cryptography and PKI
   6.a. Explain the difference between weak and Strong Cryptography
   6.b. Understand Algorithms
   6.c. Understand Wireless Security Protocols
   6.d. Understand the components and concepts of PKI Infrastructures

MAPPING LEARNING OUTCOMES TO GENERAL EDUCATION GOALS

[For each of the goals selected above, indicate which outcomes align with the goal.]

Goals	Outcomes
First Goal	
To communicate successfully, both orally and in writing, to a variety of audiences	2. Describe the various technologies and tools used with Security. 2.a. Discuss the basic security components 2.b. Use Command Line and Software Security tools. 2.c. Analyze Security output. 5. Identify the components in a Risk Management Plan. 5.a. Assess Security Policies 5.b. Perform a Business Impact Analysis 5.c. Understand the Risk Management Process
Second Goal	
To connect learning to life	1. Understand the different types of threats, attacks and vulnerabilities. 1.a. Discuss the different forms of malware. 1.b. Understand the different types of attacks. 1.c. Understand the benefits of vulnerability scanning. 3. Explain the frameworks used in Security Architecture and Design. 3.a. Explain Defense in Depth. 3.b. Describe Secure Network Topologies. 3.c. Understand Cloud Technologies and virtualization. 3.d. Understand redundancy, fault tolerance and high availability. 4. Understand Identity and Access Management 4.a. Discuss Access Control and Access Management. 4.b. Understand Account Management.

	6. Explain Cryptography and PKI 6.a. Explain the difference between weak and Strong Cryptography. 6.b. Understand Algorithms. 6.c. Understand Wireless Security Protocols. 6.d. Understand the components and concepts of PKI Infrastructures.

COURSE TOPICS AND CONTENT REQUIREMENTS:

Security+ Certification Six Domains

- Threats, Attacks, and Vulnerabilities
- Technologies and Tools
- Architecture and Design
- Identity and Access Management
- Risk management
- Cryptography and PKI

INSTRUCTIONAL METHODS:

- Lecture
- Lab
- TestOut or equivalent simulation software

INSTRUCTIONAL MATERIALS:

CompTIA SY0-501
https://www.professormesser.com/security-plus/sy0-501/sy0-501-training-course/

STUDENT REQUIREMENTS AND METHODS OF EVALUATION:

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

OTHER REFERENCES

NIST publications for additional guides

Course Competency/Assessment Methods Matrix

(Dept/# Course Name)	Assessment Options																																
For each competency/outcome place an "X" below the method of assessment to be used.	**Assessment of Student Learning**	Article Review	Case Studies	Group Projects	Lab Work	Oral Presentations	Pre-Post Tests	Quizzes	Written Exams	Artifact Self Reflection of Growth	Capstone Projects	Comprehensive Written Exit Exam	Course Embedded Questions	Multi-Media Projects	Observation	Writing Samples	Portfolio Evaluation	Real World Projects	Reflective Journals	Applied Application (skills) Test	Oral Exit Interviews	Accreditation Reviews/Reports	Advisory Council Feedback	Employer Surveys	Graduate Surveys	Internship/Practicum /Site Supervisor Evaluation	Licensing Exam	In Class Feedback	Simulation	Interview	Written Report	Assignment
Assessment Measures – Are direct or indirect as indicated. List competencies/outcomes below.	**Direct/ Indirect**	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	I	I	I	I	D	D							
1. Understand the different types of threats, attacks and vulnerabilities.					X			X	X				X					X														X
1.a. Discuss the different forms of malware.		X			X			X	X				X					X														X
1.b. Understand the different types of attacks.		X			X			X	X				X					X														X
1.c. Understand the benefits of vulnerability scanning.					X			X	X				X					X														X
2. Describe the various technologies and tools used with Security.					X			X	X				X																			X
2.a. Discuss the basic security components.					X			X	X				X																			X

2.b. Use Command Line and Software Security tools.					X			X	X				X																	X
2.c. Analyze Security output.					X			X	X				X																	X
3. Explain the frameworks used in Security Architecture and Design.					X			X	X				X																	X
3.a. Explain Defense in Depth.					X			X	X				X				x													X
3.b. Describe Secure Network Topologies.					X			X	X				X																	X
3.c. Understand Cloud Technologies and virtualization.					X			X	X				X				X													X
3.d. Understand redundancy, fault tolerance and high availability.					X			X	X				X				X													X
4. Understand Identity and Access Management					X			X	X				X																	X
4.a. Discuss Access Control and Access Management					X			X	X				X				X													X
4.b. Understand Account Management.					X			X	X				X																	X
5. Identify the components in a Risk Management Plan.					X			X	X				X																	X
5.a. Assess Security Policies.					X			X	X				X				X													X
5.b. Perform a Business Impact Analysis.					X			X	X				X				X													X
5.c. Understand the Risk Management Process.					X			X	X				X																	X
6. Explain Cryptography and PKI.					X			X	X				X																	X
6.a. Explain the difference between weak and Strong Cryptography.					X			X	X				X																	X
6.b. Understand Algorithms.					X			X	X				X																	X

6.c. Understand Wireless Security Protocols.					X			X	X				X																	X
6.d. Understand the components and concepts of PKI Infrastructures.					X			X	X				X																	X