

CS 82.56 Course Outline as of Fall 2016**CATALOG INFORMATION**

Dept and Nbr: CS 82.56 Title: COMPUTER NETWORK SECURITY

Full Title: Computer Network Security

Last Reviewed: 2/22/2016

Units		Course Hours per Week		Nbr of Weeks	Course Hours Total	
Maximum	4.00	Lecture Scheduled	4.00	17.5	Lecture Scheduled	70.00
Minimum	4.00	Lab Scheduled	0	6	Lab Scheduled	0
		Contact DHR	0		Contact DHR	0
		Contact Total	4.00		Contact Total	70.00
		Non-contact DHR	0		Non-contact DHR	0

Total Out of Class Hours: 140.00

Total Student Learning Hours: 210.00

Title 5 Category: AA Degree Applicable

Grading: Grade or P/NP

Repeatability: 00 - Two Repeats if Grade was D, F, NC, or NP

Also Listed As:

Formerly: CIS 56.22

Catalog Description:

An in-depth exploration of the essentials of computer network security. Students will analyze security objectives and the role of policy deployment while they practice defending against network attacks. Students will learn about attacks and malware, E-mail, web components, software development, disaster recovery, risk, change and privilege management, forensics and legal issues. Scenario-based curriculum describing a start-up company in which the students are employed with specific roles, will also be incorporated in the class. Tasks and product deliverables, for the start-up company, which are based on industry standards, augment assignments and exams. Coverage of both CompTIA's Security+ certification exam and the (ISC)2 SSCP certification, is integral to this course. Students should have a familiarity with network operating systems.

Prerequisites/Corequisites:**Recommended Preparation:**

Course Completion of CS 82.21A AND Eligibility for ENGL 100 or ESL 100

Limits on Enrollment:

Schedule of Classes Information:

Description: An in-depth exploration of the essentials of computer network security. Students will analyze security objectives and the role of policy deployment while they practice defending against network attacks. Students will learn about attacks and malware, E-mail, web components, software development, disaster recovery, risk, change and privilege management, forensics and legal issues. Scenario-based curriculum describing a start-up company in which the students are employed with specific roles, will also be incorporated in the class. Tasks and product deliverables, for the start-up company, which are based on industry standards, augment assignments and exams. Coverage of both CompTIA's Security+ certification exam and the (ISC)2 SSCP certification, is integral to this course. Students should have a familiarity with network operating systems. (Grade or P/NP)

Prerequisites/Corequisites:

Recommended: Course Completion of CS 82.21A AND Eligibility for ENGL 100 or ESL 100

Limits on Enrollment:

Transfer Credit: CSU;

Repeatability: Two Repeats if Grade was D, F, NC, or NP

ARTICULATION, MAJOR, and CERTIFICATION INFORMATION:

AS Degree:	Area	Effective:	Inactive:
CSU GE:	Transfer Area	Effective:	Inactive:
IGETC:	Transfer Area	Effective:	Inactive:
CSU Transfer:	Transferable	Effective: Spring 2007	Inactive: Fall 2022
UC Transfer:		Effective:	Inactive:

CID:

Certificate/Major Applicable:

Not Certificate/Major Applicable

Approval and Dates

Version:	04	Course Created/Approved:	10/23/2006
Version Created:	4/13/2015	Course Last Modified:	12/1/2021
Submitter:	Michael McKeever	Course last full review:	2/22/2016
Version Status:	Approved (Changed Course)	Prereq Created/Approved:	2/22/2016
Version Status Date:	2/22/2016	Semester Last Taught:	Spring 2021
Version Term Effective:	Fall 2016	Term Inactive:	Fall 2022

COURSE CONTENT

Student Learning Outcomes:

At the conclusion of this course, the student should be able to:

1. Define and explain attacks and malware, E-mail, web components, software development, disaster recovery, risk, change and privilege management, forensics and legal issues.
2. Analyze security objectives and the role of policy deployment and practice defending against network attacks.
3. Pass a mock certification exam for Computing Technology Industry Association (CompTIA)

Objectives:

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

1. Differentiate various types of computer and network attacks.
2. Evaluate various e-mail security practices.
3. Compare the component protocols used for website development and contrast internet applications and their associated security issues.
4. Summarize the methods of incorporating security into the software development process.
5. Evaluate disaster recovery and business continuity best practices.
6. Study risk management and diagram an approach to effectively manage risk.
7. Differentiate the essential elements of change management.
8. Evaluate methods of managing access.
9. Examine the steps in investigating a computer crime or policy violation.
10. Relate the role of ethics in computer security and survey the laws that enforce ethical behavior.

Topics and Scope:

I. Computer Attacks

- A. Denial-of-Service Attacks
- B. Backdoors and Trapdoors
- C. Other Attacks such as Malware

II. E-mail

- A. Security of E-mail Transmissions
- B. Malicious Code
- C. Hoax E-mails
- D. Unsolicited Commercial E-mail (Spam)
- E. Mail Encryption

III. Web Components

- A. Current Web Components and Concerns
- B. Protocols
- C. Code-Based Vulnerabilities

IV. Software Development

- A. The Software Engineering Process
- B. Good Practices

V. Disaster Recovery, Business Continuity, and Organizational Policies

- A. Disaster Recovery
 1. Disaster Recovery Plans/Process
 2. Backups
- B. Policies and Procedures
 1. Security Policies
 2. Privacy
 3. Service Level Agreements

VI. Risk Management

- A. An Overview of Risk Management
- B. Business Risks
- C. Risk Management Models
 1. General Risk Management Model
 2. Software Engineering Institute Model
- D. Qualitatively Assessing Risk

- VII. Change Management
 - A. Why Change Management?
 - B. The Key Concept: Segregation of Duties
 - C. Elements of Change Management
- VIII. Privilege Management
 - A. User, Group, and Role Management
 - B. Single Sign-On
 - C. Centralized vs. Decentralized Management
 - D. Auditing (Privilege, Usage, and Escalation)
 - E. Handling Access Control
 - 1. Mandatory Access Control (MAC)
 - 2. Discretionary Access Control (DAC)
 - 3. Role-Based Access Control (RBAC)
- IX. Computer Forensics
 - A. Evidence
 - 1. Standards for Evidence
 - 2. Types of Evidence
 - 3. Three Rules Regarding Evidence
 - B. Collecting Evidence
 - C. Chain of Custody
 - D. Free Space vs. Slack Space
 - E. Message Digest and Hash
 - F. Analysis
- X. Security and Law
 - A. Import/Export Encryption Restrictions
 - B. Digital Signature Laws
 - C. Digital Rights Management
 - D. Privacy Laws
 - 1. United States Laws
 - 2. European Laws
 - E. Computer Trespass
 - F. Ethics

Assignment:

1. Online research of current security appliances and best practices
2. Read topical weekly online newsletters and security reports
3. Read approximately 50 pages per week from textbook
4. Write a sample company security policy
5. 2-4 objective examinations and quizzes
6. 6-10 skill demonstration assignments

Methods of Evaluation/Basis of Grade:

Writing: Assessment tools that demonstrate writing skills and/or require students to select, organize and explain ideas in writing.

Compose a sample company security policy
--

Writing 10 - 30%

Problem Solving: Assessment tools, other than exams, that demonstrate competence in computational or non-computational problem solving skills.

Research and delineate best current computer and network security appliances and practices

Problem solving
10 - 30%

Skill Demonstrations: All skill-based and physical demonstrations used for assessment purposes including skill performance exams.

6-10 skill demonstration assignments

Skill Demonstrations
20 - 30%

Exams: All forms of formal testing, other than skill performance exams.

2-4 objective examinations and quizzes

Exams
20 - 30%

Other: Includes any assessment tools that do not logically fit into the above categories.

Attendance and participation

Other Category
10 - 20%

Representative Textbooks and Materials:

Principles of Computer Security (4th). Conklin, Wm Arthur. McGraw-Hill Osborne Media: 2015

OTHER REQUIRED ELEMENTS

STUDENT PREPARATION

Matric Assessment Required:	E	Requires English Assessment
Prerequisites-generate description:	NP	No Prerequisite
Advisories-generate description:	U	User-Generated Text
Prereq-provisional:	N	NO
Prereq/coreq-registration check:	N	No Prerequisite Rules Exist
Requires instructor signature:	N	Instructor's Signature Not Required

BASIC INFORMATION, HOURS/UNITS & REPEATABILITY

Method of instruction:	02	Lecture
	71	Internet-Based, Simultaneous Interaction
	72	Internet-Based, Delayed Interaction
Area department:	CS	Computer Studies
Division:	72	Arts & Humanities
Special topic course:	N	Not a Special Topic Course
Program status:	2	Not Certificate/Major Applicable
Repeatability:	00	Two Repeats if Grade was D, F, NC, or NP
Repeat group id:		

SCHEDULING

Audit allowed:	N	Not Auditable
Open entry/exit:	N	Not Open Entry/Open Exit
Credit by exam:	N	Credit by examination not allowed
Budget code: Program:	0000	Unrestricted
Budget code: Activity:	0701	Computer & Information Science

OTHER CODES

Discipline:	Computer Information Systems OR Computer Science	
Basic skills:	N	Not a Basic Skills Course
Level below transfer:	Y	Not Applicable
CVU/CVC status:	Y	Distance Ed, Not CVU/CVC Developed
Distance Ed Approved:	N	None
Emergency Distance Ed Approved:	Y	Fully Online Partially Online Online with flexible in-person activities
Credit for Prior Learning:	N	Agency Exam
	N	CBE
	N	Industry Credentials
	N	Portfolio
Non-credit category:	Y	Not Applicable, Credit Course
Classification:	Y	Career-Technical Education
SAM classification:	C	Clearly Occupational
TOP code:	0708.00	Computer Infrastructure and Support
Work-based learning:	N	Does Not Include Work-Based Learning
DSPS course:	N	Not a DSPS Course

In-service:

N

Not an in-Service Course