CS 82.57 Course Outline as of Fall 2022

CATALOG INFORMATION

Dept and Nbr: CS 82.57 Title: CYBEROPS
Full Title: Cybersecurity Operations
Last Reviewed: 2/22/2021

Units		Course Hours per Week		Nbr of Weeks	Course Hours Total	
Maximum	3.00	Lecture Scheduled	3.00	17.5	Lecture Scheduled	52.50
Minimum	3.00	Lab Scheduled	0	8	Lab Scheduled	0
		Contact DHR	0		Contact DHR	0
		Contact Total	3.00		Contact Total	52.50
		Non-contact DHR	0		Non-contact DHR	0

Total Out of Class Hours: 105.00 Total Student Learning Hours: 157.50

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:	

Catalog Description:
This course equips students with the knowledge and skills needed by today's organizations that are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. The student could be part of a team of people in Security Operations Centers (SOC) keeping a vigilant eye on security systems, protecting their organizations by detecting and responding to cybersecurity threats or a Systems/Network Administrator desirous of better securing their organization. Cisco Certified Network Associate (CCNA) Cyber Ops prepares candidates to begin a career working with associate-level cybersecurity analysts within security operations centers.

Prerequisites/Corequisites:

Recommended Preparation:
Eligibility for ENGL 100 or ESL 100 or appropriate placement based on AB705 mandates; and Completion of CS 81.21 and CS 81.81A and CS 82.22A and CS 82.58

Limits on Enrollment:

Schedule of Classes Information:

Description: This course equips students with the knowledge and skills needed by today's organizations that are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. The student could be part of a team of people in Security Operations Centers (SOC) keeping a vigilant eye on security systems, protecting their organizations by detecting and responding to cybersecurity threats or a Systems/Network Administrator desirous of better securing their organization. Cisco Certified Network Associate (CCNA) Cyber Ops prepares candidates to begin a career working with associate-level cybersecurity analysts within security operations centers. (Grade or P/NP)
Prerequisites/Corequisites:
Recommended: Eligibility for ENGL 100 or ESL 100 or appropriate placement based on AB705 mandates; and Completion of CS 81.21 and CS 81.81A and CS 82.22A and CS 82.58
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:	Fall 2021	Inactive:	
UC Transfer:		Effective:		Inactive:	

CID:

Certificate/Major Applicable:
Both Certificate and Major Applicable

COURSE CONTENT

Student Learning Outcomes:
At the conclusion of this course, the student should be able to:
1. Classify the various types of network attacks
2. Analyze network intrusion data to identify compromised hosts and vulnerabilities
3. Apply incident response models to manage network security incidents

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

1. Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
2. Explain the role of the Cybersecurity Operations Analyst in the enterprise.
3. Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
4. Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.
5. Explain the features and characteristics of the Linux Operating System.
6. Analyze the operation of network protocols and services.

7. Explain the operation of the network infrastructure.
8. Classify the various types of network attacks.
9. Use network monitoring tools to identify attacks against network protocols and services.
10. Use various methods to prevent malicious access to computer networks, hosts, and data.
11. Explain the impacts of cryptography on network security monitoring.
12. Explain how to investigate endpoint vulnerabilities and attacks.
13. Evaluate network security alerts.
14. Analyze network intrusion data to identify compromised hosts and vulnerabilities.
15. Apply incident response models to manage network security incidents.

Topics and Scope:

I. Cybersecurity and the Security Operations Center
   A. The danger
   B. Fighters in the war against cybercrime
II. Windows Operating System
   A. Windows overview
   B. Windows administration
III. Linux Operating System
   A. Using Linux
   B. Linux administration
   C. Linux clients
IV. Network Protocols and Services
   A. Network protocols enable network operations
   B. Ethernet and Internet Protocol (IP)
   C. Connectivity verification
   D. Address resolution protocol
   E. The transport layer and network services
   F. Network services enable network functionality
V. Network Infrastructure
   A. Network communication devices
   B. Network security infrastructure
   C. Network representations and topologies
VI. Principles of Network Security
   A. Attackers and their tools
   C. Common threats and attacks
VII. Network Attacks: A Deeper Look
   A. Observing network operation
   B. Attacking the foundation
   C. Attacking what we do
VIII. Protecting the Network
   A. Understanding defense
   B. Access control
   C. Threat intelligence
IX. Cryptography and the Public Key Infrastructure
   A. Cryptographic tools
   B. Public key infrastructure supports network security
   C. Endpoint security and analysis
   D. Endpoint protection
   E. Endpoint vulnerability assessment
X. Security Monitoring
   A. Technologies and protocols

B. Log files
XI. Intrusion Data Analysis
A. Evaluating alerts
B. Working with network security data
C. Digital Forensics
XII. Incident Response and Handling
A. Incident response models
B. Computer Security Incident Response Team (CSIRT)

Assignment:

Reading assignments include:
1. Online research of security devices and deployment practices
2. Approximately 50 pages weekly from the textbook

Homework problems include:
1. Weekly online discussion thread participation
2. Hands-on exercises and class performances to demonstrate proficiency with topics
3. Online quizzes
4. Creation of network, operating system and security design diagrams and layouts

Other assignments include:
1. Quizzes (9 - 11) and skill demonstration exam
2. Classroom scenario-based exercises

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.

Weekly written online discussions	Writing 5 - 10%

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

Homework problems, Creation of network, operating system and security design diagrams and layouts	Problem solving 15 - 30%

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

Skill demonstration exam	Skill Demonstrations 20 - 30%

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

Quizzes and skill demonstration exam	Exams 20 - 30%

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

Attendance and participation in scenario-based exercises	Other Category 5 - 20%

Representative Textbooks and Materials:
CCNA Cybersecurity Operations Companion Guide. Cisco Networking Academy. Cisco Press. 2018
CCNA Cybersecurity Operations Course Booklet. Cisco Networking Academy. Cisco Press. 2018