CS 82.71 Course Outline as of Fall 2022

CATALOG INFORMATION

Dept and Nbr: CS 82.71 Title: ETHICAL HACKING
Full Title: Ethical Hacking and Systems Defense
Last Reviewed: 5/10/2021

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 combines an ethical hacking methodology with the hands-on application of security tools to better help students secure their systems. Students are introduced to common countermeasures that effectively reduce and/or mitigate attacks. Learn how hackers penetrate computers and networks, and how to protect Windows and Linux systems. Legal restrictions and ethical guidelines will be taught and enforced. The course will help students prepare for the EC-Council "Certified Ethical Hacker" certification exams.

Prerequisites/Corequisites:
Course Completion of CS 81.21 and CS 82.58 (or CS 82.55)

Recommended Preparation:
Eligibility for ENGL 100 or ESL 100

Limits on Enrollment:

Schedule of Classes Information:
Description: This course combines an ethical hacking methodology with the hands-on application of security tools to better help students secure their systems. Students are introduced to common countermeasures that effectively reduce and/or mitigate attacks. Learn how hackers

penetrate computers and networks, and how to protect Windows and Linux systems. Legal restrictions and ethical guidelines will be taught and enforced. The course will help students prepare for the EC-Council "Certified Ethical Hacker" certification exams. (Grade or P/NP)
Prerequisites/Corequisites: Course Completion of CS 81.21 and CS 82.58 (or CS 82.55)
Recommended: 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:	Fall 2022	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. Demonstrate the ability to attack and defend a network
2. Investigate how to attack a computer system
3. Perform penetration testing

Objectives:
At the conclusion of this course, the student should be able to:
1. Utilize various information security tools given different target systems in different environments.
2. Discuss how the tools interrelate with each other in an overall penetration testing process.
3. Implement countermeasures for various types of attacks.
4. Apply a common ethical hacking methodology to carry out a penetration test.
5. Analyze how penetration testing and ethical hacking fit into a comprehensive enterprise information security program.
6. Demonstrate ethical behavior appropriate to security-related technologies.

Topics and Scope:

I. Ethical Hacking Overview
II. Transmission Control Protocol/Internet Protocol (TCP/IP) Concepts Review
III. Network and Computer Attacks
IV. Footprinting and Social Engineering
V. Port Scanning

VI. Enumeration
VII. Programming for Security Professionals
VIII. Embedded Operating Systems
IX. Linux Operating System Vulnerabilities
X. Penetration Testing
A. Hacking Web Servers
B. Hacking Wireless Networks
XI. Cryptography
XII. Protecting Networks with Security Devices

Assignment:

Reading assignments include:
1. Online research of hacking tools and techniques
2. Approximately 50 pages weekly from the textbook

Homework problems include:
1. Weekly written online discussion thread participation
2. Hands-on exercises to demonstrate proficiency with topics
3. Online quizzes (5 - 12)
4. Assignments for hacking various system environments

Other assignments include:
1. Skill demonstration examinations
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, assignments for hacking various system environments	Problem solving 15 - 30%

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

Class performances of hacking techniques and skill demonstration examinations	Skill Demonstrations 20 - 30%

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

Quizzes and skill demonstration examinations	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:
CEH Certified Ethical Hacker Bundle. 4th ed. Walker, Matt. McGraw-Hill Education. 2019

Ethical Hacking and Systems Defense: National CyberWatch Center Edition. Oriyano, Sean-Philip. Jones & Bartlett Learning. 2016 (classic)

Hands-On Ethical Hacking and Network Defense. 3rd ed. Simpson, Michael T. and Antill, Nicholas. Cengage Press. 2017 (classic)