Course ID: CIMS 150
Cat ID: 450172.00
State ID: CCC000608653

| | | |
|---|---|---|
| College: | A | Saddleback College |
| Division/School: | BS | Business Science |
| Department: | CIM | Computer Information Management |
| Program: | CIMNAD | Network Administrator |
| Subject: | CIMNAD | Network Administrator |

# O F F I C I A L  C O U R S E  O U T L I N E

## HISTORY AND STATUS

Course Status: A Active (Fully Approved)
Course Originator: Steve Korper

| | |
|---|---|
| Board of Trustees | 08/26/19 |
| State Approval | 02/23/09 |
| Curriculum Committee Approval | 07/24/19 |
| Division Approval | 07/24/19 |
| Tech Review Approval | 07/24/19 |

Technical Change Date: 02/25/13

Technical Change Comment:

taxonomy fr ecommerce-------3/5/01-taxonomy; 2/25/13-frmly CIM 294, rpt removed per Title 5; 10/21/19 chngd cb00 fr 513356 to 608653

Comments:

moe, assign

## BRIEF DESCRIPTION

Short Title: INTRO CYBERSECURITY
Full Title: INTRODUCTION TO CYBERSECURITY: ETHICAL HACKING

BRIEF DESCRIPTION

Catalog Description:

Prepares students for passing the EC-Council's Certified Ethical Hacker (CEH), a DOD cybersecurity certificate.
This course introduces the network security specialist to the various methodologies for attacking a network. Students will be introduced to the concepts, principles, and techniques, supplemented by hands-on exercises, for attacking and disabling a network within the context of properly securing a network. The course emphasizes network attack methodologies with the emphasis on student use of network attack techniques and tools and appropriate defenses and countermeasures. Students experience a hands-on practical approach to penetration testing measures and ethical hacking. (Formerly CIMS 250).

Prerequisite:

None

Enrollment Limitation:

None

Corequisite:

None

Recommended Preparation:

None

## COURSE FUNCTIONS

| | | |
|---|---|---|
| Course Prior to: | Y | Not Applicable |
| Course Classification: | Y | Credit Course |
| SC/IVC GE Code: | NA - Not Applicable | |
| CSU GE Code: | NA | Not Applicable |
| IGETC GE Code: | NA - Not Applicable | |
| UC Transferable Course: | N | No UC credit |
| Comparable SC/IVC: | | |
| Comparable CSU: | CSU<br>CSU San Bernardino<br>IST 215 - Cybersecurity | |
| Comparable UC: | | |
| Comparable CCC Baccalaureate: | | |
| TOP Code: | 0708.10 | Network Administrator |
| SAM Code: | C | Clearly Occupational |
| CAN Number: | | |
| CID Number: | | |

## COURSE OPTIONS

| | | |
|---|---|---|
| Grading Option: | GR | Letter Grade or Pass/No Pass |
| Open Entry: | N | No |
| Fixed, Optional or Variable Units: | F | Fixed Units |
| Repeatability Status: | N | No |
| Repeatability Model: | | |
| Repeatability Limit: | 0 | |
| Cross-Listed Courses: | NONE | |
| Cross-Listed Parent: | No | |

COURSE VALUES

| | | | |
|---|---|---|---|
| Method of Instruction: | L-L | Lecture/Lab Combination | |
| Maximum Enrollment: | 45 | Maximum WSCH: | 225 |
| Average Enrollment: | 22 | Average WSCH: | 110 |

| | Lecture | Lab | Learn Ctr | Total |
|---|---|---|---|---|
| WFCH | 2.00 | 3.00 | 0.00 | 5.00 |
| TFCH | 33.20 | 49.80 | 0.00 | 83.00 |
| TSCH | 33.20 | 49.80 | 0.00 | 83.00 |
| LHE | 2.00 | 2.50 | 0.00 | 4.50 |
| FTEF | 13.33 | 16.67 | 0.00 | 30.00 |
| UNITS | 2.00 | 1.00 | 0.00 | 3.00 |

Schedule Description:

Prepares students for passing the EC-Council's Certified Ethical Hacker (CEH) a DOD cybersecurity certificate. This course introduces the network security specialist to the various methodologies for attacking a network.(Formerly CIMS 250).

COURSE CONTENT
(Topics Covered)

**Lecture Topics:**

I. Ethical Hacking Overview
II. 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. Hacking Web Servers
XI. Hacking Wireless Networks
XII. Cryptography
XIII. Protecting Networks with Security Devices
XIV. Application of technical strategies, tools and techniques to secure data and information for a customer or client
XV. Adherence to a high standard of ethical behavior
XVI. Use of research in both established venues and innovative applications to expand the body of knowledge in information assurance
XVII. Application of principles of critical thinking to creatively and systematically solve the problems and meet the challenges of the ever-changing environments of cybersecurity
XVIII. Mastery of the skills necessary to move into leadership roles in companies, agencies, divisions, or departments

**Lab/Learning Center Content:**

I. Setup a computer and LAN to defend against various types of security attacks.
II. Implement safe World Wide Web techniques.
III. Detect various tools and methods hacker use to break a computer network.
IV. Practice exams and labs on passing EC-Council's CEH exam.

COURSE CONTENT
(Learning Objectives)

Students participating in this class will:

1. Describe the tools and methods a "hacker" uses to break into a computer or network.
2. Implement a defense for a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques
3. Describe and use various safe techniques on the World Wide Web.

COURSE CONTENT
(Student Learning Outcomes)

Students completing this course satisfactorily will be able to:

1. Define and identify the various terms and vocabulary related to cybersecurity.
2. Identify the background to and elements of pentration testing and ethical hacking.
3. Students will be able to detect various hacker break ins.

COURSE CONTENT
(Methods of Evaluation)

Evaluation of the student will be based upon the following items:

1. Writing Assignments
   term or other paper(s)
   written assignments
   other (specify)
   a. Evaluate student’s ability to write reports that require the student to demonstrate the knowledge of cybersecurity.

2. Problem Solving Demonstrations
   exams
   quizzes
   other (specify)
   a. Evaluation will include discussion or problem-solving assignments.

3. Skill Demonstrations
   performance (exam)
   other (specify)
   a. Evaluate students's ability to comprehend content using examinations.

4. Examinations
   multiple choice, true/false
   other (specify)
   a. Exams evaluating student’s ability to apply concepts related to course content.

5. Other
   other (specify)
      a. Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments.

COURSE CONTENT
(In and Out-of-Class Assignments)

1. Typical Reading Assignments:
   College-level text

2. Typical Writing Assignments:
   Explain the role of cybersecurity specialist in an organization

3. Typical Oral Assignments:
   Class discussions on cybersecurity and specifically ethical hacking.

COURSE CONTENT
(Other Requirements)

Textbooks / Supplies:
ROGER A. GRIMES, Hacking the Hacker: Learn From the Experts Who Take Down Hackers, 1st Edition Ed. Wiley. 2017
Simpson, M. T., Backman, K. & Corley, J, Hands-On Ethical Hacking and Network Defense, 1st Edition Ed. Cengage Learning. 2016
Regalado, D., Harper, A., Harris, S., Ness, J., Eagle, C.,, Gray Hat Hacking: The Ethical Hacker's Handbook, 5th Edition Ed. McGraw-Hill Education. 2018
EC-Council, Certified Ethical Hacker (CEH) Version 10 eBook w/ iLabs (Volume 1: Ethical Hacking Concepts and Methodology), 1st Ed. EC-Council Academia. 2018

Material Fees: $ 0.00 Transaction Code:

VALIDATION
(Corequisite, Limitation on Enrollment,
Prerequisite and Recommended Preparation)