COLLEGE OF THE DESERT

Course Code CIS-064

Course Outline of Record

1. Course Code: CIS-064
2. a. Long Course Title: Introduction to Cybersecurity: Ethical Hacking
   b. Short Course Title: ETHICAL HACKING
3. a. Catalog Course Description:
   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 will emphasize network attack methodologies with the emphasis on student use of network attack techniques and tools and appropriate defenses and countermeasures. Students will receive course content information through a variety of methods: lecture and demonstration of hacking tools will be used in addition to a virtual environment. Students will experience a hands-on practical approach to penetration testing measures and ethical hacking.
   b. Class Schedule Course Description:
   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 will emphasize network attack methodologies with the emphasis on student use of network attack techniques and tools and appropriate defenses and countermeasures. Students will receive course content information through a variety of methods: lecture and demonstration of hacking tools will be used in addition to a virtual environment. Students will experience a hands-on practical approach to penetration testing measures and ethical hacking.
   c. Semester Cycle (*if applicable*): *N/A*
   d. Name of Approved Program(s):
   - COMPUTER INFORMATION SYSTEMS AS Degree for Employment Preparation
   - COMPUTER INFORMATION SYSTEMS Certificate of Achievement
   - COMPUTER INFORMATION SYSTEMS* Certificate of Achievement
   - COMPUTER INFORMATION SYSTEMS AS DEGREE AS Degree for Employment Preparation
4. Total Units: 3.00 Total Semester Hrs: 54.00
   Lecture Units: 3 Semester Lecture Hrs: 54.00
   Lab Units: 0 Semester Lab Hrs: 0
   Class Size Maximum: 32 Allow Audit: No
   Repeatability 0x
   Justification 0
5. Prerequisite or Corequisite Courses or Advisories:
   Course with requisite(s) and/or advisory is required to complete Content Review Matrix (CCForm1-A)
   Prerequisite: CIS 060 with a minimum grade of C or equivalent
6. Textbooks, Required Reading or Software: *(List in APA or MLA format.)*
   a. Simpson, M. T., Backman, K. & Corley, J. (2016). *Hands-On Ethical Hacking and Network Defense* Cengage.
   College Level: Yes
   Flesch-Kincaid reading level: 12
   b. Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. & Williams, T. (2016). *Gray Hat Hacking: The Ethical Hackers Handbook* McGraw Hill.
   College Level: Yes
   Flesch-Kincaid reading level: 11
7. Entrance Skills: *Before entering the course students must be able:*

a.

Information Systems Security.

- CIS 060 - Describe the fundamental principles of information systems security.

b.

Malware and Social Engineering Attacks.

- CIS 060 - Define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.

c.

Application and Network Attacks.

- CIS 060 - Define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.
- CIS 060 - Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls.

d.

Vulnerability Assessment and Mitigating Attacks.

- CIS 060 - Determine appropriate strategies to assure confidentiality, integrity, and availability of information.
- CIS 060 - Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls.

e.

Host, Application, and Data Security.

- CIS 060 - Determine appropriate strategies to assure confidentiality, integrity, and availability of information.

f.

Network Security and its administration

- CIS 060 - Create and maintain a comprehensive security model.
- CIS 060 - Design and guide the development of an organization’s security policy.

g.

Wireless Network Security.

- CIS 060 - Determine appropriate strategies to assure confidentiality, integrity, and availability of information.
- CIS 060 - Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls.

h.

Access Control Fundamentals.

- CIS 060 - Evaluate the need for the careful design of a secure organizational information infrastructure.

i.

Authentication and Account Management.

- CIS 060 - Evaluate the need for the careful design of a secure organizational information infrastructure.
- CIS 060 - Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls.

j.

Risk Mitigation

- CIS 060 - Perform risk analysis and risk management.

8. Course Content and Scope:

Lecture:

A. Ethical Hacking Overview
- Getting Started
- Soft Skills
- Stay Legal

B. Transmission Control Protocol/Internet Protocol (TCP/IP) Concepts Review
- Application layer
- Transport layer
- Network layer
- Data link layer

C. Network and Computer Attacks
- Eavesdropping
- Data Modification
- IP Address Spoofing Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Compromised-Key Attack
- Sniffer Attack
- Application-Layer Attack

D. Footprinting and Social Engineering
- Information-gathering methodology
- Competitive intelligence
- Whois and American Registry for Internet Numbers (ARIN) lookup
- Types of Domain Name System (DNS) records
- Email tracking
- Web spiders
- Dumpster diving
- Reverse social engineering

E. Port Scanning

F. Enumeration
- Methods to retrieve usernames and info on groups, shares, and services of networked computers (using Nmap and Nessus).

G. Programming for Security Professionals

H. Embedded Operating Systems
- Operating systems for digital watches, MP3 players, traffic lights and hybrid vehicles.

I. Linux Operating System Vulnerabilities
- Stack Operations
- Buffer Overflows
- Exploit Development process

J. Hacking Web Servers

K. Hacking Wireless Networks

L. Cryptography
- Symmetric-key
- Public-key
- Cryptanalysis
- Primitives
- Cryptosystems

M. Protecting Networks with Security Devices
- Create a Wireless Security Policy
- Secure the Wireless Local Area Network (WLAN)
- Protect Your Wired Network from Wireless Threats
- Protect Your Company from Outside Threats
- Get Employees Involved

Lab: *(if the "Lab Hours" is greater than zero this is required)*

9. Course Student Learning Outcomes:

1.
Apply the same tools and methods a "hacker" uses to break into a computer or network.

2.
Compare different hands-on computer network defence strategies.

10. Course Objectives: *Upon completion of this course, students will be able to:*

a. Describe the tools and methods a "hacker" uses to break into a computer or network.
b. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.
c. Practice and use safe techniques on the World Wide Web.

11. Methods of Instruction: *(Integration: Elements should validate parallel course outline elements)*

a. Activity
b. Collaborative/Team
c. Demonstration, Repetition/Practice
d. Discussion
e. Distance Education
f. Individualized Study
g. Lecture
h. Observation
i. Participation
j. Technology-based instruction

12. Assignments: *(List samples of specific activities/assignments students are expected to complete both in and outside of class.)*

In Class Hours: 54.00
Outside Class Hours: 108.00

a. In-class Assignments

- Passive and active reconnaissance
- Linux/OSX exploits
- Vulnerability assessment reports
- Windows exploits
- Social Engineering and Advanced Persistent Threats (APT)
- Evasive Maneuvers and Post Exploitation
- Utilize Google Hacking Database (GHDB) and Other Google Hacking tools
- Present an overview of network scanning and the most commonly used tools
- Use of simulation software to develop networks which students can hack into. All these activities can be performed virtually.

b. Out-of-class Assignments

- Hands-on projects (hardening computer and server security)
- Problem solving assignment such as hackthissite.org - realistic missions.
- Students will be assigned case based assignments involving reading, computer manuals, and general textbook reading that cover network communications and possible exploits.
- Various assignments for this course involve the hacking of dummy networks. These activities will be performed by students on an individual basis outside of class time.
- Case studies will be assigned requiring outside research and readings like the following. Setup Man-in-the-Middle type of attacks on your personal home network.

13. Methods of Evaluating Student Progress: *The student will demonstrate proficiency by:*
    - Written homework
    - Self-paced testing
    - Laboratory projects
    - Computational/problem solving evaluations
    - Presentations/student demonstration observations
    - Group activity participation/observation
    - True/false/multiple choice examinations
    - Student participation/contribution
    - Other

14. Methods of Evaluating: Additional Assessment Information:

15. Need/Purpose/Rationale -- *All courses must meet one or more CCC missions.*

PO - Career and Technical Education

Fulfill the requirements for an entry- level position in their field.

Apply critical thinking skills to execute daily duties in their area of employment.

Apply critical thinking skills to research, evaluate, analyze, and synthesize information.

Display the skills and aptitude necessary to pass certification exams in their field.

IO - Personal and Professional Development

Demonstrate an understanding of ethical issues to make sound judgments and decisions.

IO - Scientific Inquiry

Collect and analyze data. Skills of data collection include an understanding of the notion of hypothesis testing and specific methods of inquiry such as experimentation and systematic observation.

IO - Critical Thinking and Communication

Apply principles of logic to problem solve and reason with a fair and open mind.

IO - Global Citizenship - Scientific & Technological Literacy

Synthesize, interpret, and infer, utilizing information, data, and experience to solve problems, innovate, and explore solutions.

IO - Global Citizenship - Ethical Behavior

Apply ethical reasoning to contemporary issues and moral dilemmas.

16. Comparable Transfer Course

University System	Campus	Course Number	Course Title	Catalog Year

17. Special Materials and/or Equipment Required of Students:

18. Materials Fees: □ Required Material?

Material or Item	Cost Per Unit	Total Cost

19. Provide Reasons for the Substantial Modifications or New Course:

This course serves as a preparation for the Certified Ethical Hacker or CEH

20. a. Cross-Listed Course *(Enter Course Code)*: *N/A*
    b. Replacement Course *(Enter original Course Code)*: *N/A*

21. Grading Method *(choose one)*: Letter Grade Only

22. MIS Course Data Elements

a. Course Control Number [CB00]: CCC000579568
b. T.O.P. Code [CB03]: 70100.00 - Information Technology, G
c. Credit Status [CB04]: D - Credit - Degree Applicable
d. Course Transfer Status [CB05]: B = Transfer CSU
e. Basic Skills Status [CB08]: 2N = Not basic skills course
f. Vocational Status [CB09]: Clearly Occupational
g. Course Classification [CB11]: Y - Credit Course
h. Special Class Status [CB13]: N - Not Special
i. Course CAN Code [CB14]: *N/A*
j. Course Prior to College Level [CB21]: Y = Not Applicable
k. Course Noncredit Category [CB22]: Y - Not Applicable
l. Funding Agency Category [CB23]: Y = Not Applicable
m. Program Status [CB24]: 1 = Program Applicable

Name of Approved Program *(if program-applicable)*: COMPUTER INFORMATION SYSTEMS,COMPUTER INFORMATION SYSTEMS

Attach listings of Degree and/or Certificate Programs showing this course as a required or a restricted elective.)

23. Enrollment - Estimate Enrollment
First Year: 12
Third Year: 32

24. Resources - Faculty - Discipline and Other Qualifications:
a. Sufficient Faculty Resources: Yes
b. If No, list number of FTE needed to offer this course: *N/A*

25. Additional Equipment and/or Supplies Needed and Source of Funding.
N/A

26. Additional Construction or Modification of Existing Classroom Space Needed. *(Explain:)*
N/A

27. FOR NEW OR SUBSTANTIALLY MODIFIED COURSES
Library and/or Learning Resources Present in the Collection are Sufficient to Meet the Need of the Students Enrolled in the Course: Yes

28. Originator Felix Jose Marhuenda-Donate Origination Date 10/06/16