Course Acronym:	CIS
Course Number:	122
Descriptive Title:	Ethical Hacking
Division:	Business
Department:	Computer Information Systems
Course Disciplines:	Computer Information Systems
Catalog Description:	This course introduces the principles and techniques associated with the cybersecurity practice known as penetration testing or ethical hacking. Topics covered will include planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting. Students will learn how system vulnerabilities are exploited and security problems can be avoided.
Prerequisite:	Computer Information Systems 13 with a minimum grade of C or equivalent experience
Co-requisite:	
Recommended Preparation:	
Enrollment Limitation:	
Hours Lecture (per week):	2
Hours Laboratory (per week):	3
Outside Study Hours:	4
Total Course Hours:	90
Course Units:	3
Grading Method:	Letter grade only
Credit Status:	Credit, degree applicable
Transfer CSU:	Yes
Effective Date:	06/19/2017
Transfer UC:	No
Effective Date:	
General Education: ECC	
Term:	
Other:	
CSU GE:	
Term:	
Other:	

IGETC:	
Term:	
Other:	
Student Learning Outcomes:	**SLO #1** Identify and analyze the steps an ethical hacker would take in order to compromise a target system. **SLO #2** Identify the tools and techniques used to carry out a penetration testing. **SLO #3** Assess potential vulnerabilities in a network security system within executable programs or within network protocols. **SLO #4** Understand the basic techniques for gaining unauthorized access into a network and computer system using both technical and non-technical means.
Course Objectives:	1. Understand the entire penetration testing process including planning, reconnaissance, scanning exploitation, post-exploitation, and result reporting 2. Conduct penetration testing on various infrastructure components. 3. Know the credentials of an ethical hacker, and what an ethical hacker can and cannot do legally. 4. Perform port scans to locate potential entry points to servers and networks.
Major Topics:	**I. The Ethics of Hacking and Cracking (3 hours, lecture)** A. The impact of ethical hacking B. Ethics and issues of information technology 1. State and federal laws C. Planning 1. Protect ethical hackers and clients with a written contract. **II. Cryptography (5 hours, lecture)** A. Cryptography basics B. Password cracking tools 1. John the ripper 2. Hydra C. Cryptography attacks 1. Brute force 2. Man-in-the-middle **III. Reconnaissance (5 hours, lecture)** A. Legalities 1. Contracts B. Social engineering

C. SQL injection
D. Footprinting and reconnaissance

IV. Armitage Software (3 hours, lecture)

A. System hacking
B. Penetration testing

V. Scanners and Sniffers (5 hours, lecture)

A. Network scanners
    1. Nmap (Software)
B. Packet sniffers
        1. SmartSniff (Software)
C. Metasploit exploitation

1. Network scanning
2. Numeration
3. Wireshark

VI. Hacking Wireless Networks (3 hours, lecture)

A. Components of wireless network
        1. Wireless router
B. The 802.11 Standard

VII. Types of Attacks (4 hours, lecture)

A. Hacking web servers
B. Nitko
C. Hacking web applications
        1. Understanding security in web applications
D. Buffer overflows
        1. Stack based overflow
        2. Heap based overflow

VIII. Post Exploitation (5 hours, lecture)

A. Evading intrusion detection system
B. Evading firewalls
C. Honeypots
D. Anti-Virus
        1. Trojans
        2. Backdoors

IX. Physical Attacks (3 hours, lecture)

A. Lock picking
B. Master keys
C. Keyloggers

X. Password cracking (6 hours, lab)

A. Rainbow tables
B. John the ripper (Software)
C. Hydra (Software)
D. Cryptography Attacks
    1. Brute force

XI. Social Engineering (6 hours, lab)

A. Social engineering attacks
B. SQL injection
C. Footprinting and reconnaissance

XII. Armitage (Software) to attack the network (6 hours, lab)

A. System hacking
B. Penetration testing

XIII. Active and Passive Techniques to Enumerate Network Hosts (6 hours, lab)

A. Network scans
B. Packet sniffers

XIV. Metasploit exploitation (6 hours, lab)

A. Network scanning
B. Numeration
C. Wireshark

XV. Hacking Wireless Networks (6 hours, lab)

A. Components of a wireless network
B. The 802.11 Standard

XVI. Hacking Web Applications (6 hours, lab)

A. Hacking webservers
B. Hacking web application
C. Buffer overflows

XVII. Post Exploitation (9 hours, lab)

A. Evading intrusion detection system
B. Evading firewalls
C. Honeypots
D. Anti-Virus
    1. Trojans
    2. Backdoors

XVIII. Physical Attacks (3 hours, lab)

	A. Lock picking B. Master keys C. Keyloggers
Total Lecture Hours:	36
Total Laboratory Hours:	54
Total Hours:	90
Primary Method of Evaluation:	Problem solving demonstrations (computational or non-computational)
Typical Assignment Using Primary Method of Evaluation:	Jeffrey, a 10th-grade student, loves reading any book. One day, he found a book titled Basics of Hacking. Having always wondered how hacking works, he immediately started reading. After reading the book, Jeffrey was eager to put some of his new knowledge into practice. Jeffrey launched the tools from a CD that was offered with the book and discovered plenty of loopholes in the school's network. Is anything wrong with Jeffrey's actions? Are his actions justified? Write a one- to two-page report.
Critical Thinking Assignment 1:	Research a security testing software tool that you practiced using from the textbook. Determine whether the tool would be beneficial in testing the security of a corporate network. Use the vendor's website to collect necessary information about the tool to be able to explain its purpose and benefit. Include 3rd party endorsements and case studies about the tool. Integrate the information from your own experience with the tool into your proposal. Produce a two- to three-page report.
Critical Thinking Assignment 2:	You will need to present information that proves a chosen security tool will be beneficial to the security of a corporate information system. To accomplish this, you will need to research the product, and if possible, test the product in a virtual lab environment. If the tool is part of your Lab exercise, it is recommended that you practice using and testing the tool beyond the scope of the lab exercise. Based on your research and analysis, you will include this information in your proposal in a way that the executive staff can understand and allow them to make an informed decision to approve purchase of the product. Produce a two- to three-page report.
Other Evaluation Methods:	Objective Exams, Quizzes, Other, Written Reports, Lab exercises
Instructional Methods:	Demonstration, Lecture, Multimedia presentations
If other:	
Work Outside of Class:	Study, Required reading, Problem solving activities, Written work
If Other:	
Up-To-Date Representative Texts:	Michael T.Simpson, Nicholas Antill. Hands-On Ethical Hacking and Network Defense. 4th ed. Course Technology, 2023.
Alternative Texts:	
Required Supplementary Readings:	
Other Required Materials:	USB 3.0 flash drive 2 GB or larger
Requisite:	Prerequisite

Category:	Sequential
Requisite course(s): List both prerequisites and corequisites in this box.	CIS 13
Requisite and Matching skill(s):Bold the requisite skill. List the corresponding course objective under each skill(s).	Demonstrate an understanding of general security concepts and how computer networks operate.
Requisite Skill:	
Requisite Skill and Matching Skill(s): Bold the requisite skill(s). If applicable	
Requisite course:	
Requisite and Matching skill(s):Bold the requisite skill. List the corresponding course objective under each skill(s).	
Requisite Skill:	
Requisite Skill and Matching skill(s): Bold the requisite skill. List the corresponding course objective under each skill(s). If applicable	
Enrollment Limitations and Category:	
Enrollment Limitations Impact:	
Course Created by:	Richard Perkins
Date:	05/01/2017
Original Board Approval Date:	06/19/2017
Last Reviewed and/or Revised by:	Richard Perkins
Date:	10/09/2023
Last Board Approval Date:	12/18/2023
Effective Term:	FALL 2024