Subject:	CIS
Course Number:	123
Descriptive Title:	Advanced Ethical Hacking
Division:	Business
Department:	Computer Information Systems
Course Disciplines:	Computer Information Systems
Catalog Description:	This advanced course in ethical hacking expands on penetration testing techniques and tools with an emphasis on real-world scenarios, advanced exploitation, persistence mechanisms, red team operations, and exploit development. Students will simulate adversarial attacks in a lab environment and evaluate the effectiveness of defense mechanisms. Legal and ethical responsibilities are emphasized throughout.
Prerequisite:	CIS 122 with a minimum grade of C
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:	TBD
Transfer UC:	Yes
Effective Date:	
General Education ECC:	
Term:	
Other:	
CSU GE:	
Term:	
Other:	
IGETC:	
Term:	
Other:	

CalGETC:	
Term:	
Other:	
Student Learning Outcomes:	**SLO #1:** Simulate advanced cyberattacks and evaluate the success of red team operations. **SLO #2:** Identify and implement post-exploitation techniques including privilege escalation and maintaining access. **SLO #3:** Assess and document the effectiveness of security controls against advanced threats. **SLO #4:** Demonstrate the ethical and legal boundaries of advanced penetration testing engagements.
Course Objectives:	1. Perform advanced reconnaissance using open-source intelligence (OSINT) tools. 2. Develop and execute custom payloads and exploits. 3. Execute lateral movement, privilege escalation, and persistence techniques. 4. Simulate a red team vs. blue team engagement. 5. Analyze and interpret post-engagement reports and suggest remediations. 6. Apply principles of exploit development and buffer overflow attacks.
Major Topics:	I. Advanced Reconnaissance Techniques (6 hours, lecture) A. OSINT automation B. DNS enumeration, subdomain takeover C. Social media mining II. Exploit Development (6 hours, lecture) A. Stack and heap overflows B. Return Oriented Programming (ROP) C. Exploit frameworks (Immunity Debugger, pwntools) III. Advanced Password Attacks (5 hours, lecture) A. Hashcat rules and masks B. Password spraying C. Cracking Windows password hashes IV. Privilege Escalation Techniques (5 hours, lecture) A. Linux enumeration scripts B. Windows UAC bypass C. Kernel exploit usage V. Persistence and Evasion (4 hours, lecture) A. Scheduled tasks and services B. DLL injection C. Antivirus evasion and obfuscation VI. Red Team Operations (6 hours, lecture) A. Attack planning and chain of command B. C2 frameworks (Cobalt Strike, Mythic) C. Reporting and debrief VII. Post-Engagement Analysis (4 hours, lecture) A. Report writing B. Remediation recommendations C. Lessons learned VIII. **Laboratory Topics (54 hours, lab):** A. Custom Reconnaissance Scripts (6 hours) B. Exploit Development and Testing (6 hours)

	C. Hashcat and Password Cracking Exercises (6 hours) D. Linux and Windows Privilege Escalation Labs (6 hours) E. Malware and Persistence Mechanism Labs (6 hours) F. C2 Communications and Evasion Labs (6 hours) G. Red Team Simulated Engagements (6 hours) H. Final Red Team Project and Reporting (6 hours) I. Defensive Analysis and Remediation Plan (6 hours)
Total Lecture Hours:	36
Total Laboratory Hours:	54
Total Hours:	90
A.1. Primary Methods of Evaluation (Part 1 - CCN courses only):	
Primary Method of Evaluation:	2) Problem solving demonstrations (computational or non-computational)
Typical Assignment Using Primary Method of Evaluation:	Plan and execute an end-to-end red team attack scenario using advanced hacking tools and tactics. Deliverables include a one-page written report documenting every phase, tools used, and post-engagement recommendations.
Critical Thinking Assignment 1:	Analyze a real-world cyberattack reported in the news. Write a 2- to 3-page report identifying the tactics used, how they could be replicated in a lab environment, and how organizations could defend against such threats.
Critical Thinking Assignment 2:	Research a Command and Control (C2) framework. Test it in a sandbox environment and write a proposal detailing its features, capabilities, and use in red team operations. The report must address ethical considerations and legal use cases.
Other Evaluation Methods:	Laboratory Reports, Objective Exam, Presentation, Quizzes
If Other:	
Instructional Methods:	Demonstration, Discussion, Group Activities, Guest Speakers, Lab, Lecture, Multimedia presentations, Role play/simulation
If other:	
Work Outside of Class:	Problem solving activity, Required reading, Skill practice, Written work (such as essay/composition/report/analysis/research)
If Other:	
Up-To-Date Representative Texts:	Wil Allsopp. Advanced Penetration Testing: Hacking the World's Most Secure Networks, 2nd ed., Wiley, 2020.
Alternative Texts:	Georgia Weidman. Penetration Testing: A Hands-On Introduction to Hacking, No Starch Press, 2014. (Discipline Standard)
Required Supplementary Readings:	
Other Required Materials:	USB 3.0 flash drive, Virtual Machine access, Kali Linux
Requisite	Prerequisite

Category	sequential
Requisite course:	CIS 122
Requisite and Matching skill(s): Bold the requisite skill. List the corresponding course objective under each skill(s).	**Students must demonstrate ethical hacking skills such as port scanning, reconnaissance, and post-exploitation** CIS 122 - Understand the entire penetration testing process including planning, reconnaissance, scanning exploitation, post-exploitation, and result reporting
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:	10/1/2025
Original Board Approval Date:	01/21/2026
Effective Term:	FA 2026