Adversarial Cyber Tradecraft

CIS 4930 Section 67MW

Class Periods: M Period 7 1:55-2:55 PM, W Period 7-8 1:55-3:50 PM

Location: M WEIM 1070, W WEIM 1084

Academic Term: Fall 2025

Instructor:

Cheryl Resch
Cheryl.resch@ufl.edu
Office Hours: M 12:30-1:30, F 2:30-3:30 Mala 4110

Supervised Teaching Student:

- Ben Ruddy, bruddy@ufl.edu

Course Description

The course introduces a theory of adversarial engagement and related game theoretical concepts.
It addresses the theory and practice through conflict principles associated with both offense and defense along the dimensions of deception, physical access, humanity, economy, planning, innovation, and time.
Students engage in weekly exercises putting these theories into practice in adversarial competitions.
Students will be able to identify and employ these concepts in both offensive and defensive cyber activities.

Course Pre-Requisites / Co-Requisites

COP3503C or COP3504C

Course Objectives

By the end of this course, students will be able to identify and explain the role of penetration testing in improving the security posture of an enterprise; properly scope the elements of a penetration test to satisfy the needs of an enterprise, and enumerate rules of engagement appropriate to such a test; identify and explain the role of penetration testing techniques and tools; employ penetration testing techniques and tools to exploit vulnerabilities in an enterprise's computer systems, services, and networks; and communicate the business risk of computer system, network, and service vulnerabilities and identify and explain methods of avoiding and/or mitigating security risk.

Materials and Supply Fees

N/A

Relation to Program Outcomes (ABET):

Outcome	*Coverage**
1. An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics	Medium
2. An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors	
3. An ability to communicate effectively with a range of audiences	Medium

4. An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts	Medium
5. An ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives	High
6. An ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions	High
7. An ability to acquire and apply new knowledge as needed, using appropriate learning strategies	High

Recommended Textbooks and Software

Title: Adversarial Tradecraft in Cybersecurity
Author: Dan Borges
Publication date and edition: 2021
ISBN: 978-1801076203

Recommended Textbooks and Software
Title: PTFM: Purple Team Field Manual
Author: Tim Bryant
Publication date and edition: 2020
ISBN: 979-8682974061

Title: Operator Handbook: Red Team + OSINT + Blue Team Reference
Author: Joshua Picolet
Publication date and edition: 2020
ISBN 979-8605493952

Recommended Materials – N/A

Required Computer

Recommended Computer Specifications: https://it.ufl.edu/get-help/student-computer-recommendations/

HWCOE Computer Requirements: https://www.eng.ufl.edu/students/advising/fall-semester-checklist/computer-requirements/

Course Schedule

Week	Topic	Activity
Week 1	Theory of Operation (Chap. 1)	Driving Linux
Week 2	Basic Networking and Command Line Control (Linux)	Basic Networking
Week 3	Basic Networking and Command Line Control (Windows)	Driving Windows
Week 4	Practical Networking from a Sys Admin Perspective	Network config and concepts
Week 5	Preparing for Battle (Chap. 2)	Network logging and event detection
Week 6	Invisible is Best (Chap. 3)	Process exploitation and C2 frameworks
Week 7	Blending In (Chap. 4)	LoLbins, DLLS, covert channels, detection

Week 8	Active Manipulation (Chap. 5)	Log clearing, rootkits, detection, Distracting and tricking attackers
Week 9	Real-time Conflict part 2 (Chap. 6)	Bash and PowerShell history, keylogging, other valuable techniques
Week 10	Real-time Conflict Part 2	Linux iptables, Windows firewall, services
Week 11	The Research Advantage	More log awareness and mining
Week 12	Clearing the Field (Chap. 7)	Attacker Containment
Week 13	Recent Competition Debriefs	Nov. Wargames
Week 14	How to Win at CCDC (multiple red/blue perspectives)	Nov. Wargames
Week 15	Review	Practical Red/Blue Examination

Important Dates

See the Canvas calendar.

Attendance Policy, Class Expectations, and Make-Up Policy

Attendance is strongly recommended but not mandatory. Due to the course format, students who miss many lectures will be at a significant disadvantage.

QUIZ/EXAM DATES/POLICIES: Quizzes and the final examination must be taken before the due date published on Canvas.

If an extension (late or make-up assignments) is required for a UF-approved reason or an otherwise legitimate reason (e.g., medical, travel, family, religious exemption, etc.), this will be accommodated.

Requirements for class attendance and make-up exams, assignments, and other work in this course are consistent with university policies. Click here to read the university attendance policies: https://catalog.ufl.edu/UGRD/academic-regulations/attendance-policies/

Evaluation of Grades

Assignment	**Percentage of Final Grade**
Quizzes	20%
Activity Reports	40%
Practical Examination	40%
	100%

Grading Policy

Percent	**Grade**	**Grade Points**
93.4 - 100	A	4.00
90.0 - 93.3	A-	3.67
86.7 - 89.9	B+	3.33
83.4 - 86.6	B	3.00
80.0 - 83.3	B-	2.67
76.7 - 79.9	C+	2.33
73.4 - 76.6	C	2.00

70.0 - 73.3	C-	1.67
66.7 - 69.9	D+	1.33
63.4 - 66.6	D	1.00
60.0 - 63.3	D-	0.67
0 - 59.9	E	0.00

More information on UF grading policy may be found at:
https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx

Academic Policies & Resources

To support consistent and accessible communication of university-wide student resources, instructors must include this link to academic policies and campus resources: https://go.ufl.edu/syllabuspolicies. Instructor-specific guidelines for courses must accommodate these policies.

Commitment to a Positive Learning Environment

The Herbert Wertheim College of Engineering values varied perspectives and lived experiences within our community and is committed to supporting the University's core values.

If you feel like your performance in class is being impacted, please contact your instructor or any of the following:

- Your academic advisor or Undergraduate Coordinator
- HWCOE Human Resources, 352-392-0904, student-support-hr@eng.ufl.edu
- Pam Dickrell, Associate Dean of Student Affairs, 352-392-2177, pld@ufl.edu