Course Syllabus

Course Information

Course Prefix, Number, Section: cs4459.001
Course Title: Cybersecurity Attacks and Defenses Laboratory (CANDL)
Term: Spring 2025
Meetings: Face-to-Face

Professor Contact Information

Instructor: Kangkook Jee
Office Phone: 972-883-3853
Office Location: ECSS 3.226
Email Address: <firstname>‘dot’<lastname> ‘at’ utdallas ‘dot’ edu
Office Hours: Fri 14:00 ~ 16:00 (Weekly)
Course Website: https://cs4459.syssec.org
Class room: ECSS 2.311

Course Modality and Expectations

Instructional Mode	Traditional/Face-to-Face
Course Platform	The course will be taught face-to-face. Instructor and students meet according to the schedule. Limited availability due to classroom spacing.
Expectations	After completing the course, students are expected to learn (1) execution model for software programs (2) primary attack vectors to exploit insecure software programs, (3) various measures to protect software programs.
Asynchronous Learning Guidelines	By default, students are mandated to attend class synchronously. Students *should* consult to the instruction *in advance* and get excuses, in case they cannot attend the class on time for any reasons.

Course Pre-requisites, Co-requisites, and/or Other Restrictions

Students are required to satisfy the following prerequisites:

- Computer Architecture (cs2340) or equivalent
- Data Structures and Introduction to Algorithmic Analysis (cs3345) or equivalent
- C Programming in a UNIX Environment (cs3377) or equivalent

The following courses are not required but recommended:

- Operating System Concepts (cs4348)

Optionally, the course assignment would require students with the following programming skills:

- Fluency in C/C++ and Python
- Basic understanding on how program runs at low-level machine instructions-level (e.g., IA32, AMD64)

Course Description

This course aims to teach a wide spectrum of offensive and defensive techniques for computer systems. In particular, the course will cover introductory (e.g., stack overflow, shellcode) to intermediary level (e.g., heap exploits) binary reversing and pwning techniques, which include vulnerability analysis, exploit development, patching vulnerabilities, bug hunting, etc. The course comprises of eight units of hands-on labs with Capture-The-Flag (CTF) style challenges.

The course will be hands-on heavy. The lecture will only take 50% or less portion, and the hands-on labs will cover the remaining half. The course will required students to work on a series of in-class and out-of-class CTF style challenges.

This course will evaluate student performance using the format of CTF challenges for not only learning techniques required to solve the challenge but also enjoying the fun of taking over the systems and countering attacks.

Student Learning Objectives/Outcomes

The course is primarily intended for senior-level undergraduate and graduate students interested in obtaining skill sets required to thwart cyberattacks in the wild.

Throughout lab exercises, students will become confident in competing in Capture-the-Flag (CTF) challenges, exploiting sophisticated software vulnerability, chasing real-world bug bounties, and contributing to open-source projects by disclosing vulnerability and reporting their patches.

Required Textbooks and Materials

The course does not require any textbook.

Suggested Course Materials

Students will find more resources / materials will be posted on the course website.

Assignments & Academic Calendar

Please refer to schedule section from the course website for more details.

Weeks	Date	Topic (Tentative)	Assignments
1	1/21/25	Intro & Preliminary reverse engineering	Unit1
2	1/28/25	Buffer overflow	Unit2
3	2/4/25	Buffer overflow/frame-pointer attack	
4	2/11/25	Shellcoding #1	Unit3-part1
5	2/18/25	Shellcoding #2	Unit3-part2
6	2/25/25	System security defenses	
7	3/4/25	Stack canary; DEP/NX; ASLR	Unit4
8	3/11/25	Return-Oriented-Programming (ROP)	Unit5
9	3/18/25	Spring break	
10	3/25/25	Arbitrary Read (AR), Arbitrary Write (AW), Format String Vulnerability (FSV)	Unit6
11	4/1/25	Advanced topics I	Unit 7
12	4/8/25	Advanced topis II	
13	4/15/25	Heap overflow	Unit 8
14	4/22/25	Advanced system security defenses	
15	4/29/25	Class wrap-up and inclass CTF	Inclass CTF

Grading Policy

- 80% Lab challenge, 20% from class participation and external CTF activities.
- If you miss any entire single lab, you will get an F (so please submit at least one flag per each lab).
- No midterm or final exams.

Grading Scale: Based on 4 assignments anc extra scores

Scaled Score (%)	Letter Equivalent
90.1 - 100	A- and above
80.1 - 90	B- and above
70.1 - 70	C- and above
60.1 - 70	D- and abov e
Less than 60	F

Class Attendance

The University's attendance policy requirement is that individual faculty set their course attendance requirements. Regular and punctual class attendance is expected regardless of modality. Students who fail to attend class regularly are inviting scholastic difficulty. In some courses, instructors may have special attendance requirements; these should be made known to students during the first week of classes. These attendance requirements will not be used as part of grading (see Class Participation below for grading information).

In-person participation records may be used to assist the University or local public health authorities in performing COVID-19 occurrence monitoring. Please note – in-person attendance requires consistently adhering to University requirements, including wearing a face covering and other public safety requirements related to COVID-19, as presented in this syllabus. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Class Participation

Regular class participation is expected regardless of course modality. Students who fail to participate in class regularly are inviting scholastic difficulty. A portion of the grade for this course is directly tied to your participation in this class. It also includes engaging in group or other activities during class that solicit your feedback on homework assignments, readings, or materials covered in the lectures (and/or labs). Class participation is documented by faculty. Successful participation is defined as consistently adhering to University requirements, as presented in this syllabus. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Class Recordings

The instructor may record meetings of this course. Any recordings will be available to all students registered for this class as they are intended to supplement the classroom experience.

Students are expected to follow appropriate University policies and maintain the security of passwords used to access recorded lectures. Unless the Office of Student AccessAbility has approved the student to record the instruction, students are expressly prohibited from recording any part of this course. Recordings may not be published, reproduced, or shared with those not in the class, or uploaded to other online environments except to implement an approved Office of Student AccessAbility accommodation. If the instructor or a UTD school/department/office plans any other uses for the recordings, consent of the students identifiable in the recordings is required prior to such use unless an

exception is allowed by law. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Class Materials

The instructor may provide class materials that will be made available to all students registered for this class as they are intended to supplement the classroom experience. These materials may be downloaded during the course, however, these materials are for registered students' use only. Classroom materials may not be reproduced or shared with those not in class, or uploaded to other online environments except to implement an approved Office of Student AccessAbility accommodation. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Off-campus Instruction and Course Activities
(Below is a description of any travel and/or risk-related activity associated with this course.)

Comet Creed
This creed was voted on by the UT Dallas student body in 2014. It is a standard that Comets choose to live by and encourage others to do the same:

"As a Comet, I pledge honesty, integrity, and service in all that I do."

Academic Support Resources

The information contained in the following link lists the University's academic support resources for all students.

Please see http://go.utdallas.edu/academic-support-resources.

UT Dallas Syllabus Policies and Procedures

The information contained in the following link constitutes the University's policies and procedures segment of the course syllabus.

Please go to http://go.utdallas.edu/syllabus-policies for these policies.

The descriptions and timelines contained in this syllabus are subject to change at the discretion of the Professor.