

Course Syllabus

Fall 2026, CS 6265-001/OCY,

Information Security Lab: Reverse Engineering and Exploitation Labs

Professor: Dr. Taesoo Kim

Course Description

This course covers advanced techniques for writing exploits and patching vulnerabilities, taught through an intense, hands-on security laboratory. A significant part of this course involves solving [Capture-The-Flag \(CTF\)](#) and discussing strategies for solving such problems. This course covers a variety of topics including (but not limited to) reverse engineering, exploitation, binary analysis, and web.

Prerequisite

- Operating systems or equivalent (e.g., CS 3210 at GT).

Class Meetings

- Online course
- Online recitation in EST time
 - TBD

Course Goals

- Learn classes of security vulnerabilities
- Learn how to exploit security vulnerabilities
- Learn how to defend or mitigate security vulnerabilities

Grading Policy

100% of your grade is determined by the total number of points earned across all labs. No tests, quizzes, exams, or projects. If you don't turn in at least one flag for every lab, you will get an F. **The precise point cutoffs will be announced on Canvas and/or Ed Discussion**, but you can use the following **approximate** criteria as a guideline:

- A: Average 5+ challenges per lab*
- B: Average 4+ challenges per lab*
- C: Average 3+ challenges per lab*

- D: Average 3- challenges per lab*
- F: Zero flags submitted for at least one lab.

*This assumes that you also earned all available points from the tutorials (meaning you actually got more than N flags per lab on average).

The expected grade distribution is 40% A, 30-40% B, and 20-30% C and below. Details about points can be found at [General Rules](#).

Class Website

- Visit <https://tc.gts3.org/cs6265/2026> to find tutorials and reference materials.

Lab Due Dates

- All labs will be due at the times in the table at the end of this syllabus.
- These times are subject to change so please check back often.

Plagiarism Policy

- Plagiarism is considered a serious offense. You are not allowed to copy and paste or submit materials created or published by others, as if you created the materials. All materials submitted and posted must be your own.
- We also strictly follow the cheating policy (read [GT's Academic Misconduct Policy](#)).
- **Don't publish or post your work online (e.g., on GitHub). Any violation of these rules will result in a course grade of F.**

Student Honor Code

- All degree students should abide by the Georgia Tech Student Honor Code
- [Review the Georgia Tech Student Honor Code.](#)
- Any OMS Analytics degree student suspected of behavior in violation of the Georgia Tech Honor Code will be referred to Georgia Tech's Office of Student Integrity.

Communication

- Often, discussions with fellow learners are the sources of key pieces of learning.
- Online discussion is strongly encouraged, and it will help you a lot in solving lab problems. Please join Ed Discussion and post your questions, ideas and thoughts.

Netiquette

- Netiquette refers to etiquette that is used when communicating on the Internet. Review the Core Rules of Netiquette. When you are communicating via email, discussion forums

or synchronously (real-time), please use correct spelling, punctuation and grammar consistent with the academic environment and scholarship¹.

¹ Conner, P. (2006-2014). Ground Rules for Online Discussions, Retrieved 4/21/2014 from <http://teaching.colostate.edu/tips/tip.cfm?tipid=128>

Course Topics and Release Dates

- The table below contains a course topic outline and assignment due dates.

Weeks		Course Topics	Release Dates (Eastern Time)
Week 1	Introduction Lesson 1	Introduction Tools and x86	Aug 28, 2026 at 8:00 a.m.
	Lab 1	Bomb Lab1	Aug 28 at 8:00 a.m. - Sep 3, 2026 at 11:59 p.m.
Week 2	Lesson 2	Shellcode and x86_64	Sep 4, 2026 at 8:00 a.m.
	Lab 2	Bomb Lab2 / Shellcode	Sep 4 at 8:00 a.m. - Sep 10, 2026 at 11:59 p.m.
Week 3 & 4	Lesson 3	Stack Overflow	Sep 11, 2026 at 8: 00 a.m.
	Lab 3	Stack Overflow	Sep 11 at 8:00 a.m. - Sep 24, 2026 at 11: 59 p.m.
Week 5	Lesson 4	Bypassing Stack Protections	Sep 25, 2026 at 8:00 a.m.
	Lab 4	Bypassing Stack Protections	Sep 25 at 8:00 a.m. - Oct 1, 2026 at 11:59 p.m.
Week 6	Lesson 5	Bypassing DEP and ASLR	Oct 2, 2026 at 8:00 a.m.
	Lab 5	Bypassing DEP/ASLR	Oct 2 at 8:00 a.m. - Oct 8, 2026 at 11:59 p.m.
Week 7 & 8	Lesson 6	Return-oriented Programming	Oct 9, 2026 at 8:00 a.m.
	Lab 6	Return-oriented Programming	Oct 9 at 8:00 a.m. - Oct 22, 2026 at 11:59 p.m.

Week 9 & 10	Lesson 7	Remote Exploitation	Oct 23, 2026 at 8:00 a.m.
	Lab 7	Remote Attacks	Oct 23 at 8:00 a.m. - Nov 5, 2026 at 11:59 p.m.
Week 11	Lesson 8	Miscellaneous Topics	Nov 6, 2026 at 8:00 a.m.
	Lab 8	Miscellaneous Topics	Nov 6 at 8:00 a.m. - Nov 12, 2026 at 11:59 p.m.
Week 12 & 13 & 14	Lesson 9	Heap Exploitation	Nov 13, 2026 at 8:00 a.m.
	Lab 9	Exploiting Heap Bugs	Nov 13 at 8:00 a.m. - Dec 3, 2026 at 11:59 p.m.
Week 15	Lesson 10	Online CTF	Dec 4, 2026 at 3:30 p.m.
	Lab 10	NSA Codebreaker Challenge	Dec 4, 2026 at 11:59 p.m.
Final exam week	NO FINAL	NO FINAL	Dec 10 – Dec 17, 2026

Course Materials

- All content and course materials can be accessed online
- There is no required textbook for this course
- Optional materials:
 - Books & Manuals
 - [Phrack Magazine](#)
 - [The Shellcoder's Handbook: Discovering and Exploiting Security Holes](#)
 - [The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws](#)
 - [Intel Architecture Software Developer Manuals](#)

Staff/TA

- TBD
- Feel free to send us an email for support (6265-staff@cc.gatech.edu)

Technology/Software Requirements

- Internet connection (DSL, LAN, or cable connection desirable)
- Adobe Acrobat PDF reader (free download; see <https://get.adobe.com/reader/>)