CS 6265 Syllabus

Information Security Lab: Reverse Engineering and Exploitation Labs

3 Credit Hours

Instructor Information

Instructor: Dr. Taesoo Kim

Email: taesoo@gatech.edu

Office: S0925, CODA Building

General Course Information

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) challenges and discussing strategies for such problems. Topics include (but are not limited to) reverse engineering, exploitation, binary analysis, and web security.

Course Learning Outcomes

Upon successful completion of this course, students should be able to:

- Identify and classify common security vulnerabilities in software systems
- Exploit security vulnerabilities using techniques such as buffer overflows, return-oriented programming, and heap exploitation
- Apply defensive techniques to mitigate security vulnerabilities
- Analyze and reverse-engineer compiled binaries to understand program behavior

Pre- and Co-Requisites

Operating systems or equivalent (e.g., CS 3210 at Georgia Tech).

Required Course Materials

All content and course materials are accessible online. There is no required textbook for this course. Optional reference materials include:

- Phrack Magazine (http://www.phrack.com/)
- 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

Grading Policy

100% of the grade is determined by the total number of points earned across all labs. There are no tests, quizzes, exams, or projects. If a student does not submit at least one flag for every lab, the student will receive an F. The precise point cutoffs will be announced on Canvas and/or Ed Discussion. The following approximate criteria serve as a guideline:

- A: Average 7+ challenges per lab

- B: Average 6+ challenges per lab
- C: Average 5+ challenges per lab
- D: Average fewer than 5 challenges per lab
- F: Zero flags submitted for at least one lab

These thresholds assume that tutorial points have also been earned. The expected grade distribution is approximately 40% A, 30–40% B, and 20–30% C and below.

At Georgia Tech, final course grades are awarded on a scale of A–F with no +/– grades permitted.

Description of Graded Components

Labs (100%): Each lab consists of a set of CTF-style challenges with increasing difficulty. Students earn points by capturing flags (solving challenges) and submitting them to the course scoring server. Labs are released on a weekly or biweekly basis. Each lab has a fixed deadline; specific dates are announced each semester. In fall, TKCTF and NSA Codebreakers events are assigned as individual labs.

Tutorials: Tutorial challenges accompany each lesson and serve as guided practice. Points earned from tutorials count toward the overall grade.

Course Topics and Schedule

The table below provides a general course topic outline. Specific release dates and deadlines are announced each semester via Canvas.

Week(s)	Lesson	Course Topic	Lab
Week 1	Lesson 1	Introduction, Tools, and x86	Bomb Lab 1
Week 2	Lesson 2	Shellcode and x86_64	Bomb Lab 2 / Shellcode
Weeks 3–4	Lesson 3	Stack Overflow	Stack Overflow
Week 5	Lesson 4	Bypassing Stack Protections	Bypassing Stack Protections
Week 6	Lesson 5	Bypassing DEP and ASLR	Bypassing DEP/ASLR
Weeks 7–8	Lesson 6	Return-Oriented Programming	Return-Oriented Programming
Weeks 9–10	Lesson 7	Remote Exploitation	Remote Attacks
Week 11	Lesson 8	Miscellaneous Topics	Miscellaneous Topics
Weeks 12–13	Lesson 9	Heap Exploitation	Exploiting Heap Bugs
Week 14	Lesson 10	Online CTF	CTF Challenge
Final Exam Week	—	No Final Exam	—

Class Meetings

Lecture and recitation times and locations are announced each semester. The course website provides up-to-date scheduling information.

Class Website: https://tc.gts3.org/cs6265/

Course Policies

Attendance and Participation

Attendance is not graded; however, students are strongly encouraged to attend all lectures and recitations. Lecture and recitation sessions provide essential guidance for solving lab challenges. Students who miss class are responsible for obtaining any missed material on their own.

Academic Integrity

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. Review Georgia Tech's Honor Code (https://catalog.gatech.edu/policies/honor-code/) and the student Code of Conduct (https://catalog.gatech.edu/rules/18/).

Any student suspected of cheating or plagiarism on a quiz, exam, or assignment will be reported to the Office of Student Integrity, who will investigate the incident and identify the appropriate penalty for violations.

Plagiarism is considered a serious offense. Students may not copy, paste, or submit materials created or published by others as if they created the materials. All materials submitted must be the student's own work.

Students must not publish or post their work online (e.g., on GitHub). Any violation of these rules will result in a course grade of F.

Collaboration, Group Work, and Use of Generative AI

Online discussion is strongly encouraged and will help significantly in solving lab problems. Students should use Ed Discussion to post questions, ideas, and thoughts. However, directly sharing solutions, flags, or exploit code with other students is prohibited. The specific policy on the use of Generative AI tools will be announced each semester.

Extensions, Late Assignments, and Missed Exams

All labs have fixed deadlines announced each semester. Lab due dates are subject to change; students should check the course website and Canvas regularly. There are no exams in this course.

Technology and Software Requirements

- Internet connection (DSL, LAN, or cable connection desirable)
- Access to a x86 Linux environment (virtual machine or native installation)
- Additional tool and software requirements are documented on the course website.

Communication

Online discussion is strongly encouraged. Students should join Ed Discussion and use it as the primary channel for course-related questions. For private matters, students may email the course staff at the address provided each semester.

When communicating via email or discussion forums, students should use correct spelling, punctuation, and grammar consistent with the academic environment.

Accommodations for Students with Disabilities

If you are a student with learning needs that require special accommodation, contact the Office of Disability Services (http://disabilityservices.gatech.edu/, 404-894-2563) as soon as possible to make an appointment to discuss your special needs and to obtain an accommodations letter. Please also e-mail the instructor as soon as possible in order to set up a time to discuss your learning needs.

Student-Faculty Expectations Agreement

At Georgia Tech, we believe that it is important to strive for an atmosphere of mutual respect, acknowledgement, and responsibility between faculty members and the student body. The Student-Faculty Expectations (http://www.catalog.gatech.edu/rules/22/) articulate some basic expectations that students can have of the instructor and that the instructor has of students. In the end, simple respect for knowledge, hard work, and cordial interactions will help build the environment we seek. Students are encouraged to remain committed to the ideals of Georgia Tech while in this class.

Campus Resources for Students

Graduate Student Academic and Professional Success Resources

A list of resources for graduate students is available on the Office of Graduate and Postdoctoral Education website (https://gradpostdoc.gatech.edu/). Specific information for current graduate students (https://grad.gatech.edu/current-students) includes:

- Academic Resources such as the Communications Center, Language Institute, Library, and resources for conducting research
- Student Resources such as Campus Services, Health and Wellness, and Career Services
- Professional Development such as programming from the Career Center and other professional development resources and events

Student Well-Being

At Georgia Tech, we are concerned about your overall physical, social, and mental well-being. A comprehensive list of wellness-related resources has been compiled and maintained by the Office of the Vice President for Student Engagement and Well-being (https://students.gatech.edu/student-resource-guide).