

Course Syllabus

Fall 2021, 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 (EST time, TBD)
 - Monday 12-1PM (TA)
 - Tuesday 9-10PM (TA)
 - Thursday 5-6PM (TA)
 - Friday 10-11AM (TA)

Course Goals

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

Grading Policy

- 100% Lab.
- If you didn't turn in **a single (full) lab**, you will get an **F**.
 - In other words, you have to submit **AT LEAST one flag** per lab. Solving the tutorial counts, so if you solve all tutorials in all labs, you will not get an F.
- **No midterm or final exams.**

- 40%: A, 30-40%: B, 30-20%: C and below (in each group).
 - A: **Five** or more challenges per lab, **AND** all the tutorials
 - B: **Four** challenges per lab, **AND** all the tutorials
 - C: Up to **three** challenges per lab, **AND** all the tutorials
 - Three groups: undergraduate, masters and PhD students
- We provide a week of a grace period (50% points after due date)
- See [Game Rules](#) for detailed information.

Class website

- Visit <https://tc.gts3.org/cs6265/2021> to find tutorials and reference materials.

Homework and Quizzes 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.

Timing Policy

- The Modules follow a logical sequence
- Assignments should be completed by their due dates.
- You will have access to the course content for the scheduled duration of the course.

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 strictly follow the cheating policy (read GT's [Academic Misconduct Policy](#)).
- **Do not publish or post your work online (e.g., GitHub). Any violation of these rules would result in F in your grade.**

Student Honor Code

- All degree students should abide by the Georgia Tech Student Honor Code
- Review the Georgia Tech Student Honor Code: www.honor.gatech.edu.
- 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

- Please contact your instructor, teaching assistants, and fellow learners via the Piazza discussion forums.
- 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 [Piazza](#) 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 27, 2021 at 8:00 a.m.
	Lab 1	Bomb Lab1	Aug 27 at 8:00 a.m. - Sep 2, 2021 at 11:59 p.m.
Week 2	Lesson 2	Shellcode and x86_64	Sep 3, 2021 at 8:00 a.m.
	Lab 2	Bomb Lab2 / Shellcode	Sep 3 at 8:00 a.m. - Sep 9, 2021 at 11:59 p.m.
Week 3 & 4	Lesson 3	Stack Overflow	Sep 10, 2021 at 8: 00 a.m.
	Lab 3	Stack Overflow	Sep 10 at 8:00 a.m. - Sep 23, 2021 at 11: 59 p.m.
Week 5	Lesson 4	Bypassing Stack Protections	Sep 24, 2021 at 8:00 a.m.
	Lab 4	Bypassing Stack Protections	Sep 24 at 8:00 a.m. - Sep 30, 2021 at 11:59 p.m.
Week 6	Lesson 5	Bypassing DEP and ASLR	Oct 1, 2021 at 8:00 a.m.

	Lab 5	Bypassing DEP/ASLR	Oct 1 at 8:00 a.m. - Oct 7, 2021 at 11:59 p.m.
Week 7 & 8	Lesson 6	Return-oriented Programming	Oct 8, 2021 at 8:00 a.m.
	Lab 6	Return-oriented Programming	Oct 8 at 8:00 a.m. - Oct 21, 2021 at 11:59 p.m.
Week 9 & 10	Lesson 7	Remote Exploitation	Oct 22, 2021 at 8:00 a.m.
	Lab 7	Remote Attacks	Oct 22 at 8:00 a.m. - Nov 4, 2021 at 11:59 p.m.
Week 11	Lesson 8	Miscellaneous Topics	Nov 5, 2021 at 8:00 a.m.
	Lab 8	Miscellaneous Topics	Nov 5 at 8:00 a.m. - Nov 11, 2021 at 11:59 p.m.
Week 12 & 13	Lesson 9	Heap Exploitation	Nov 12, 2021 at 8:00 a.m.
	Lab 9	Exploiting Heap Bugs	Nov 12 at 8:00 a.m. - Nov 25, 2021 at 11:59 p.m.
Week 14	Lesson 10	Online In-class CTF	Dec 3, 2021 at 3:30 p.m.
	Lab 10	NSA Codebreaker Challenge	Dec 3, 2021 at 11:59 p.m.
Final exam week	NO FINAL	NO FINAL	Dec 9 – Dec 16, 2021

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

- Seulbae Kim, Mingyi Liu
- 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/>)