Course Syllabus

Spring 2024, CS 6265-O01/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) (Check Canvas)

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**.
- Expected distribution: 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.

Class website

- Visit https://tc.gts3.org/cs6265/2024-spring/ 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- **Do not publish or post your work online (e.g., GitHub).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 Ed 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 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 scholarship[1].

  [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**	Jan 12, 2024 at 8:00 a.m.
	Lab 1	**Bomb Lab1**	Jan 12 at 8:00 a.m. - Jan 18, 2024 at 11:59 p.m.
Week 2	Lesson 2	**Shellcode and x86_64**	Jan 19, 2024 at 8:00 a.m.
	Lab 2	**Bomb Lab2 / Shellcode**	Jan 19 at 8:00 a.m. - Jan 25, 2024 at 11:59 p.m.
Week 3 & 4	Lesson 3	**Stack Overflow**	Jan 26, 2024 at 8: 00 a.m.
	Lab 3	**Stack Overflow**	Jan 26 at 8:00 a.m. - Feb 8, 2024 at 11: 59 p.m.
Week 5	Lesson 4	**Bypassing Stack Protections**	Feb 9, 2024 at 8:00 a.m.
	Lab 4	**Bypassing Stack Protections**	Feb 9 at 8:00 a.m. - Feb 15, 2024 at 11:59 p.m.
Week 6	Lesson 5	**Bypassing DEP and ASLR**	Feb 16, 2024 at 8:00 a.m.
	Lab 5	**Bypassing DEP/ASLR**	Feb 16 at 8:00 a.m. - Feb 22, 2024 at 11:59 p.m.
Week 7 & 8	Lesson 6	**Return-oriented Programming**	Feb 23, 2024 at 8:00 a.m.

	Lab 6	**Return-oriented Programming**	Feb 23 at 8:00 a.m. - Mar 7, 2024 at 11:59 p.m.
Week 9 & 10 & 11	Lesson 7	**Remote Exploitation**	Mar 8, 2024 at 8:00 a.m.
	Lab 7	**Remote Attacks**	Mar 8 at 8:00 a.m. - Mar 28, 2024 at 11:59 p.m.
Spring break			Mar 18 – Mar 22, 2024
Week 12	Lesson 8	**Miscellaneous Topics**	Mar 29, 2024 at 8:00 a.m.
	Lab 8	**Miscellaneous Topics**	Mar 29 at 8:00 a.m. - Apr 4, 2024 at 11:59 p.m.
Week 13 & 14	Lesson 9	**Heap Exploitation**	Apr 5, 2024 at 8:00 a.m.
	Lab 9	**Exploiting Heap Bugs**	Apr 5 at 8:00 a.m. - Apr 18, 2024 at 11:59 p.m.
Week 15	Lesson 10	**Automatic Bug Finding**	Apr 19, 2024 at 8:00 a.m.
	Lab 10	**No Lab**	Apr 19 at 3:00 p.m. - Apr 20, 2024 at 2:59 p.m.
Final exam week	NO FINAL	NO FINAL	Apr 25 – May 2, 2024

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

- Gyejin Lee & Xiang Cheng
- 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/)