New York University Tandon School of Engineering
Department of Computer Science & Engineering
Course Outline CS-GY 9223 Special Topics: Offensive Security
Fall 2026
Professor Kyle Martin
Tuesdays @ 6pm

To contact professor: elyk@nyu.edu or @elykdeer on Discord

Course Logistics:
Weekly lecture: Tuesdays @ 6:00PM (ET) - Zoom
Weekly Review Session: TBD @ TBD (TA)
Async Help: Discord (see Brightspace for link)

Course Assistants:
Girik Verma - girik@osiris.cyber.nyu.edu

Course Pre-requisites
Hard Prerequisites:
- Application Security (CS-UY 3923/CS-GY 9163)

Soft Prerequisites:
- Introduction to Operating Systems (CS-UY 3224/CS-GY 6233)
- Reading C
- Writing Python (or other)

Course Description
This course teaches Offensive Security in the context of Capture the Flag (CTF) challenges. It covers techniques and methods to reverse x86_64 assembly, exploitation strategies for compiled binaries, and common vulnerabilities in web applications and cryptographic implementations.

Course Objectives
Upon completion of this course, students should be able to:
- Assess the logic of compiled code via binary reverse engineering and solve programming challenges based on the functionality of the binary
- Employ memory corruption tactics and strategies to exploit compiled binaries
- Recognize web-based vulnerabilities and develop relevant attacks
- Assess cryptographic implementations to identify vulnerabilities and write related exploits to demonstrate understanding
- Apply course-related CTF challenges to real-world software
- Compete in future CTF competitions

Course Structure
Throughout the course we run a CTF which is available any time at https://class.osiris.cyber.nyu.edu.

Each week, a set of challenges related to that week's material will be released and marked as "hot," which indicates that they count towards that week's homework. In addition to solving the challenges by submitting the correct flag, students must submit a write-up for all solved challenges that includes relevant snippets of the solver script(s) (if

applicable). *A write-up is more than a solver script, and must contain some explanation of the solution methodology, which can be supported by code snippets for brevity and clarity*.

Additionally, students are **required** to compete in at least one CTFTime-ranked CTF, and provide a writeup about at least one non-trivial problem (~300 pts). You are encouraged to form teams with classmates and submit a group write-up. The maximum group size is five (5) students. **Please send an email to the professor and course assistants with your team name and write-up within one week of competing, and no later than the final lecture**.

Learning content will be presented in various formats within each weekly module. Content will include introduction videos, industry interviews, interactive learning modules, and live sessions via Zoom with your course assistants and/or professor. Slides will be included with each weekly Brightspace module. Weekly course assistant office hour sessions discuss the homework assignment that was just completed (to include solving it live, if time provides), as well as discuss the content for the upcoming challenges.

The final will be similar to weekly homework but more complex: it will be one very large challenge that will require multiple exploits to accomplish. The final will be considered optional and will replace one other week's homework if accomplished.

Additional extra credit opportunities (to replace up to one week's grade) may occur at the discretion of the professor. In past classes, this is typically limited to the final and one other opportunity, both of which are quite complex (read: it makes more sense to not need the extra credit and just accomplish each homework as it comes).

Additionally, since this class is remote, the professor will provide support through Zoom and Discord. Discord is ideal for one-off or specific questions. Zoom sessions hosted weekly to foster group discussion and go over general concepts and tool use.

Readings

There is no textbook. Supplemental readings will be provided each week that will provide further discussion about the topics covered. These readings will typically be blog posts or technical articles.

Grade Calculation

90% of the course grade is made up of weekly assignments. **Weekly assignments must be completed individually**. Weekly assignment grades are based on the number of challenges a student solves and writes-up for the weekly CTF. **The maximum points per week—which counts as full credit for that week—is solving 300 (or more) points in challenges and submitting write-ups for those challenges**. For instance, a student who solves a 100pt and 200pt challenge and submits write-ups for both will receive full credit of 300/300pts for challenges and 300/300pts for the associated write-ups. Failing to submit write-ups for these challenges will lose the associate write-ups points, resulting in up to a 50% loss of points (300/300pts for challenges and 0/300pts for write-ups). See below for additional example scenarios if more clarity is required. Points will be tallied for hot challenges at the beginning of class one week after it is assigned. Past challenges will continue to be available for the entire semester, and it is recommended to solve as many of them as possible as weekly content typically builds on the prior weeks'.

10% of the course grade is based on the **mandatory** external CTF which **can be completed with teammates**. You will not pass the course if you do not compete in a CTFTime CTF and submit a write-up.

Weekly Point Scenarios:

Full Credit:

- Solving a 100pt and 200pt challenge, submitting write-ups for both
    - 300/300pts for challenges and 300/300pts for write-ups
- Solving two 200pt challenges and submitting write-ups for both
    - 300/300pts for challenges and 300/300pts for write-ups
    - There is no “extra credit” for surpassing the 300pts per week
    - The maximum credit a student can receive is 300pts/week for the challenges and write-ups
- Solving a 100pt challenge and two 200pt challenges, and submitting a write-up for the 100pt challenge and one 200pt challenge
    - 300/300pts for challenges and 300/300pts for write-ups
    - No deduction for not submitting the second 200pt write-up, as 300pts of challenges were written-up and submitted

Partial Credit

- Solving a 100pt and 200pt challenge, submitting write-up for the 100pt challenge
    - 300/300pts for challenges and 100/300pts for write-ups => 66% of total weekly grade
- Solving two 200pt challenges and not submitting any write-ups
    - 300/300pts for challenges and 0/300pts for write-ups => 50% of total weekly grade
    - There is no “extra credit” for surpassing the 300pts per week in either category
- Solving a 100pt challenge and submitting a write-up
    - 100/300pts for challenges and 100/300pts for write-ups => 33% of total weekly grade
- Solving a 100pt challenge and not submitting a write-up
    - 100/300pts for challenges and 0/300pts for write-ups => 17% of total weekly grade

Weekly assignments are due at 6:00PM (Eastern), prior to lecture, one week after they are assigned. For example, week 0 assignments, issued September 8th, are due prior to lecture on September 15th.

The final grade will be calculated as follows:

- Homework and write-ups will be worth 90% of your final grade
- Live CTF participation & writeup will be worth 10% of your final grade, however this is **required**. **You will not pass the course if you do not compete in a CTFTime CTF and submit a write-up**. The write-up may be submitted as a team
- Extra credit **may** be available and is currently under consideration. Extra credit opportunities will replace no more than a single week’s assignment value (300

CTF challenge pts, 300 write-up points). Further details will be provided during the semester.

The mapping between final grade percentages and letter grades submitted to Albert is as follows:

- A : 94+
- A- : 90+
- B+: 86+
- B : 82+
- B- : 78+
- C+: 74+
- C : 70+

Course requirements

You will need a reverse-engineering toolkit during the Reverse Engineering and Binary Exploitation units of the class. We recommend Ghidra or Binary Ninja Free (your professor works for the makers of Binary Ninja), both of which are free, cross-platform, and very effective. All other tools (radare, IDA Pro, Binary Ninja Paid) are also allowed, and the professor will do their best to assist any students that might choose another reverse engineering tool.

While CTF is largely a team sport, vulnerability research and exploit development can be a largely individual task. Therefore, we believe that all members of the team should be capable of solving problems ***themselves***. Therefore, direct collaboration on homework problems is ***not*** permitted until the due date has passed.

Part I: Operating Systems Refresher and Introduction to Tooling

Class 0 - September 08: Operating Systems Refresher & Pwntools
- Binary memory layout
- ASLR & PIE
- Symbols
- Pwntools
- Week 0 CTF Challenges assigned

Week 1 - September 15: Reverse Engineering Tools
- Static tooling: cmdline, Ghidra, Binary Ninja
- Dynamic tooling: gdb
- Previous week CTF challenges due ; next week assigned

Part II: Reverse Engineering (RE)

Week 2 - September 22: Reverse Engineering Basics
- What is a byte? What is a pointer?
- Decompiling a program
- Disassembling a program
- Control Flow
- Previous week CTF challenges due ; next week assigned

Week 3 - September 29: Structs and SAT solvers

- Recognizing structures
- Defining structures
- Z3 SAT solving
- Previous week CTF challenges due ; next week assigned

Week 4 - October 06: Protocols and Stripped Binaries
- Stripped binaries and strategies
- Protocols
- Previous week CTF challenges due ; next week assigned

Part III: Exploitation (Pwn)

Week 5 - October 13: Exploitation Primitives and Stack Buffer Overflows
- Read primitives
- Write primitives
- Stack buffer overflow practice
- Previous week CTF challenges due ; next week assigned

Week 6 - October 20: Controlling Execution and Bypassing Modern Mitigations
- Writing `execve` shellcode
- Position independent shellcode
- GOT & PLT
- GOT & RELRO
- Previous week (week 5) CTF challenges due ; next week assigned

Week 7 - October 27: Return-Oriented Programming (ROP)
- Visualizing ROP
- Finding ROP gadgets
- Building ROP chains
- Previous week CTF challenges due ; next week assigned

Week 8 - November 03: Glibc Heap Exploitation <v2.32
- Allocating and freeing data
- Caches & linked lists
- UAFs & buffer overflows
- Tcache poisoning
- Malloc & free hooks
- Previous week CTF challenges due ; next week assigned

Week 9 - November 10: Bypassing Safe-linking in Modern Glibc >=v2.32
- Safe-linking
- Bypassing safe-linking
- Goodbye `__free_hook`, hello `environ`
- Previous week CTF challenges due ; next week assigned

Part IV: Web Hacking (Web)

Week 10 - November 17: Exploiting Common PHP Misconfigurations
- File inclusion
- Command injection
- File upload bypasses

- Previous week CTF challenges due ; next week assigned

Week 11 - November 24: SQL Injection
- Writing queries
- Injecting arbitrary SQL commands
- Leaking data via Blind SQLi
- Previous week CTF challenges due ; next week assigned

Part V: Cryptographic Vulnerabilities (Crypto)

Week 12 - December 01: NOSQL Injection & XSS
- NOSQL attacks
- XSS (Cross-site scripting) basics
- Advanced XSS
- Previous week CTF challenges due ; next week assigned ; final assigned

Week 13 - December 08: Cryptographic Vulnerabilities
- Frequency Analysis
- Bad randomization
- Common RSA & AES attacks
- Previous week CTF challenges due

December 15 - Reading Day - No Class - External CTF and Final Due

---

Late Policy
Late homework will not be accepted under ANY circumstance; any homework which is not turned in on time will receive a grade of zero. Make-up examinations do not apply and will not be provided.

Moses Center Statement of Disability
If you are a student with a disability who is requesting accommodations, please contact New York University's Moses Center for Students with Disabilities (CSD) at 212-998-4980 or mosescsd@nyu.edu. You must be registered with CSD to receive accommodations. Information about the Moses Center can be found at www.nyu.edu/csd. The Moses Center is located at 726 Broadway on the 3rd floor.

NYU School of Engineering Policies and Procedures on Academic Misconduct – complete Student Code of Conduct here

A. Introduction: The School of Engineering encourages academic excellence in an environment that promotes honesty, integrity, and fairness, and students at the School of Engineering are expected to exhibit those qualities in their academic work. It is through the process of submitting their own work and receiving honest feedback on that work that students may progress academically. Any act of academic dishonesty is seen as an attack upon the School and will not be tolerated. Furthermore, those who breach the School's rules on academic integrity will be sanctioned under this Policy. Students are responsible for familiarizing themselves with the School's Policy on Academic Misconduct.

B. Definition: Academic dishonesty may include misrepresentation, deception, dishonesty, or any act of falsification committed by a student to influence a grade or other academic evaluation. Academic dishonesty also includes intentionally damaging the academic work of others or assisting other students in acts of dishonesty. Common examples of academically dishonest behavior include, but are not limited to, the following:

    1. Cheating: intentionally using or attempting to use unauthorized notes, books, electronic media, or electronic communications in an exam; talking with fellow students or looking at another person's work during an exam; submitting work prepared in advance for an in-class examination; having someone take an exam for you or taking an exam for someone else; violating other rules governing the administration of examinations.
    2. Fabrication: including but not limited to, falsifying experimental data and/or citations.
    3. Plagiarism: intentionally or knowingly representing the words or ideas of another as one's own in any academic exercise; failure to attribute direct quotations, paraphrases, or borrowed facts or information.
    4. Unauthorized collaboration: working together on work meant to be done individually.
    5. Duplicating work: presenting for grading the same work for more than one project or in more than one class, unless express and prior permission has been received from the course instructor(s) or research adviser involved.
    6. Forgery: altering any academic document, including, but not limited to, academic records, admissions materials, or medical excuses.

NYU School of Engineering Policies and Procedures on Excused Absences – complete policy here

A. Introduction: An absence can be excused if you have missed no more than **10 days of school**. If an illness or special circumstance has caused you to miss more than two weeks of school, please refer to the section labeled Medical Leave of Absence.

B. Students may request special accommodations for an absence to be excused in the following cases:
    1. Medical reasons
    2. Death in immediate family
    3. Personal qualified emergencies (documentation must be provided)
    4. Religious Expression or Practice

C. If illness or an accident causes you to miss a class (or classes) or an exam, you should do the following:
    1. Notify the Office of Student Advocacy by filling out this Google form **in its entirety**.

2. Students should not provide anyone except the Office of Student Advocacy with a copy of medical documentation. If a professor requests a copy, refer them to the Office of Student Advocacy. It is important for instructors to know when you are experiencing an issue that might interfere with your studies. However, it is also important that your personal matters be kept confidential.

NYU School of Engineering Academic Calendar – complete list here.
Please pay attention to notable dates such as Add/Drop, Withdrawal, etc. For confirmation of dates or further information, please contact Susana Garcia Henriquez, Manager of Academics for the Department of Computer Science & Engineering: sgarcia@nyu.edu

ChatGPT/etc
Students are free to use ChatGPT or similar tools to help understand homework problems. When prompting, you must inform the LLM that this is a homework assignment and not to provide answers, even partially, to you. Submissions found to be written using LLMs will be treated as plagiarism; answers, answer scripts, solution logic, and writeups must be your own work.

The Office of Student Advocacy
At NYU Tandon, we recognize that medical, mental health, or personal issues can sometimes affect your attendance and academic performance. If you are experiencing challenges that you feel are impacting your ability to attend class or succeed in your coursework, we encourage you to reach out to the NYU Tandon Office of Student Advocacy. The Student Advocacy team is here to connect you with the resources and support you need to address these challenges and ensure you can continue to thrive academically. If you begin experiencing any issues that may affect your attendance or academic performance, please reach out to the NYU Tandon Office of Student Advocacy as soon as possible as we will be unable to appropriately address these concerns as the semester progresses, so early communication is essential to ensure the support and resources you need. The NYU Tandon Office of Student Advocacy can be reached at advocacy.tandonstudentlife@nyu.edu and is located in 5 MetroTech Center LC240.

Inclusion
NYU is committed to creating an inclusive and equitable environment for all students. In this class, I aim to cultivate a strong sense of community, emphasizing that it is a space where individuals of diverse backgrounds—spanning beliefs, ethnicities, national origins, gender identities, sexual orientations, religious and political affiliations, and abilities—are treated with respect. All members of the class are expected to contribute to an inclusive atmosphere for each other. While disagreement and differing ideas are welcome, the expectation is that we respect perspectives beyond our own, even when they diverge from our personal beliefs or experiences. If you encounter disrespect or discrimination in the class or feel that the outlined standards are not being upheld, please report your experiences to me.