**NewYorkUniversityTandonSchoolofEngineering**
ComputerScience
CourseOutlineCS-GY9223-IntrotoOffensiveSecurity
**Spring2021**
**ProfessorMikhailSosonkin**

To contact professor: on the class slack

Office hours:

## Course Prerequisites:

None

This course aims to teach Offensive Security in the context of Capture the Flag (CTF) competitions. We will cover common flaws in websites, techniques and methods to reverse x86 assembly, exploitation strategies for binaries, and basic cryptographic flaws.

## Course Objectives:

Upon completion of this course, students should be able to

- Recognize web-based vulnerabilities and develop relevant attacks
- Assess the logic of source-less code via binary reverse engineering and solve programming challenges based on the functionality of the binary
- Employ memory corruption tactics and strategies to exploit binaries
- 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 events

## Course Structure

Throughout the course, we will be running 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. Additionally, you will be required to compete in at least one CTFTime-ranked CTF, and provide a writeup about at least one non-trivial problem that your team worked on. We encourage you to form teams with classmates and submit a group writeup. Please send an email to the teachers with your team name and writeup within one week of competing, no later than 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 teaching assistants and/or professor. They will begin with discussing 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. There will be slides distributed at the start of the class.

The midterm and final will have the same structure as other weeks, but will be more complex and cumulative. For instance, the midterm will encompass all previous sections, include more challenges and more points, as well as more time to complete. In past classes, this means that there are 4 challenges for a total of 1000 points (600 points required for passing), and 2 weeks to accomplish.

The final will be similar: 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 (replace a 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 to use the extra credit and just accomplish each as it comes).

## Grade Calculation

Weekly grading will be based on the number of points you score in the CTF each week. If you score at least 300 CTF points in the week, you will receive credit for that week's homework. 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 we recommend that you solve as many of them as you can.

The final grade will be calculated as follows:

- Homework will be worth 90% of your final grade.
- 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.

## Course requirements

Additionally, since I am remote, I will provide office hours support in the form of zoom, or Slack interactivity. Since the majority of our discussions require technical back and forth, I've found that Slack is the most effective method of communication. We can schedule as many discussions as you need, just please be cognizant of my timing and provide me as much lead time as possible.

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

We will provide a VM with many other common tools. Instructions for setting up the VM can be found at https://class.osiris.cyber.nyu.edu/vm.

While CTF is largely a team sport, 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.

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.

**Part I: Introduction to CTF**

1 - 29JAN Introduction

- What is CTF
- Syllabus overview
- Environment/Tooling Setup
- First simple warmup challenges (basic programming warmups) assigned

**Part II: Web-Based Vulnerabilities (WEBVULN)**

2 - 05FEB Intro to Web-Based Vulnerabilities

- SQL Injection
- XML Entity Injection
- XSS
  - Previous week CTF challenges due ; next week assigned

3 - 12FEB Additional Web-Based Vulnerabilities

- Command Injection
- File Inclusion
- Serialization
  - Previous week CTF challenges due ; next week assigned

**Part III: Reverse Engineering (RE)**

4 - 19FEB Intro to Reverse Engineering

- Basics of assembly
- x86 semantics
- Techniques / Strategies
- Debugging
  - Previous week CTF challenges due ; next week assigned

5 - 26FEB Further Reverse Engineering

- Structs
- Symbolic Execution
  - Previous week CTF challenges due ; next week assigned

**Part IV: Exploitation (RCE)**

6 - 04MAR Intro to Exploitation

- Control Flow
- Stack Overflow
  - Previous week CTF challenges due ; next week assigned

7 - 11MAR Further Exploitation

- Structs
- Symbolic Execution
  - Previous week CTF challenges due ; midterm assigned 4

18MAR No Classes - Spring Break (16-22MAR)

8 - 25MAR Defeating Exploit Mitigations

- Binary layout
- Mitigations and bypasses
- Return-Oriented Programming
- Midterm due ; next week assigned

9 - 01APR Introduction to Heap Exploitation

- Heap basics
  - Previous week CTF challenges due ; next week assigned

10 - 08APR Further Heap Exploitation

- More complex heap primitives and exploitation
  - Previous week CTF challenges due ; next week assigned

**Part IV: Cryptography (CRYPTO)**

11 - 15APR Introduction to Cryptanalysis

- Frequency analysis
- XOR
  - Previous week CTF challenges due ; next week assigned

12 - 22APR Further Cryptanalysis

- Block ciphers
- Common RSA attacks/mistakes
- Padding oracle attacks
- Hash-length extension

- Previous week CTF challenges due ; next week assigned

13 - 29APR Special Topic

- TBD based on class voting
- Final exam assigned

14 - 06MAY Final Exam Topic Discussion

- CTF Participation and Write-up Deadline
- asd

**13MAY Final Assignment Due**

**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

Deanna Rayment, deanna.rayment@nyu.edu, is the Coordinator of Student Advocacy, Compliance and Student Affairs and handles excused absences. She is located in 5 MTC, LC240C and can assist you should it become necessary. **NYU School of Engineering Academic Calendar – complete list here.** The last day of the final exam period is _____. Final exam dates for undergraduate courses will not be determined until later in the semester. Final exams for graduate courses will be held on the last day of class during the week of _____. If you have two final exams at the same time, report the conflict to your professors as soon as possible. Do not make any travel plans until the exam schedule is finalized.

Also, please pay attention to notable dates such as Add/Drop, Withdrawal, etc. For confirmation of dates or further information, please contact Susana: sgarcia@nyu.edu