The information contained on this page is designed to give students a representative example of material covered in the course. Any information related to course assignments, dates, or course materials is illustrative only.

NYU | TANDON SCHOOL OF ENGINEERING

Course Syllabus

Computer Science and Engineering

Penetration Testing and Vulnerability Analysis

Course Information

Course Prerequisites

CS-GY 6823 Network Security is the formal prerequisite for this class. Additionally, CS-GY 9163 Application Security should be considered an informal co-requisite. Beyond those two courses, students should have a thorough knowledge of networking protocols, Windows and Linux security controls, and scripting/programming. Technical: You will be required to run virtual machines on your computer. We will be virtualizing up to 3 Linux VMs or 1 Linux and 1 Windows VM at the same time. 6GB of ram is the minimal amount of ram required for good virtualization (2GB host, 2GB Kali, 2GB Windows VM), but I recommend at least 12GB. You will be required to use a hypervisor application, like VirtualBox or VMWare player, whichever you prefer.

Course Description

CS6573 is an advanced course introducing students to penetration testing and vulnerability analysis. It will cover in-depth methodologies, techniques, and tools to identify vulnerabilities, exploit, and assess security risk to networks, operating systems, and applications. The course goals will get you to have the knowledge, think, and work, like an ethical penetration tester.

Course Objectives

By the end of this course students should be able to:

- Describe a management view of cybersecurity
- Enumerate and illustrate the general principles of risk analysis
- Explain the fundamentals of business continuity management and how it can help address security incidents
- Analyse security components within organisational contest: identity and access management, data protection, security operations, etc.
- Create a plan for the third party risk assessments
- Apply this course knowledge to develop the system security strategy in practical cases

Course Structure

Online Format course, each week of the course will be aligned to modules.

Breakdown:

- Labs: 40%
- Quizzes: 30%
- Participation(NCL): 10%
- Term Project: 20%

Weekly Structure

Week	Title	Assignments
1	● Intro & Pen Test Methodologies ○ Testing methodologies (Black Box/White Box/Fuzz) ○ Engagement practices	● Lab Preparation Virtualbox Configuration ● Reading: Sample PenTest Report
2	● Passive Information Gathering ○ Open source information gathering	● Term Research Project
3	● Active Information Gathering ○ NMAP ○ Port Scanning ○ Enumeration	● Lab – Information Gathering
4	● Vulnerability Management ○ Vulnerability discovery ○ Vulnerability mitigation	● Quiz 1 ● Term Project Topic selection

5	● Exploitation ○ Metasploit ○ Buffer overflow ○ Fuzzing	● Lab – Network Exploitation
6	● Advanced binary exploitation ○ Reverse engineering ○ Static code analysis ○ Binary Analysis (no source code provided) ○ OllyDbg	● Quiz 2

Learning Time Rubric

Learning Time Element	Asynchronous* / Synchronous**	Time on Task for Students (weekly)	Notes
Reading Assignments / Recorded Lecture	Asynchronous	2.5 hours	Video format. Expect quizzes throughout the module or weekly chapter readings

Weekly Discussion Board	Asynchronous	1.5 hours	Students are expected to post initial response to weekly topic questions. See Interaction Policy.
Assessment (Labs and Programming assignments)	Asynchronous	2 hours	Students submit their assignments by [the end of the week]
Reading Assignment	Asynchronous	2 hours	Reading assigned textbook chapters and journal articles.
Live webinars	Synchronous	2 hours	Group discussion in class, live, overly weekly chapter

Readings

CS6573 covers many past and modern topics that are difficult to capture in just one book. Because of this, there is no one textbook designated for this class. However, you will be encouraged to register for National Cyber League (NCL), which will count as course materials.

Additionally, reference websites will be provided throughout the course to serve as recommended reading.

Assignments and Exams

Late Assignments

Due to the nature of this course, late assignments will not be accepted except in cases of documented personal illness/emergency, unforeseen and unavoidable professional/personal obligations (subject to the instructor’s discretion), or bereavement.

Time frame	Points reduced
Due Date - 7 Days past due date	25%
7- 14 Days past due date	50%
14+ Days	100%

National Cyber League

Registering for NCL costs a total of $35, cheaper than most books. What you get is access to their training labs and 3 capture the flag events. We will discuss this more during the semester. For more info: https://www.nationalcyberleague.org/fall-season

Starting in , we will participate in 3 Capture the Flag style events organized by the National Cyber League (NCL). While the course material is aimed at helping you learn technical and communication skills, the NCL events are fun hands-on games that will allow you to practice some of the topics we learn and also teach you some new things as well. More exposure and practice will help you become more proficient in your career.

- Complete the NCL Spring Gymnasium Training Labs - 25%
- Participate in the Pre-season CTF event (placement) - 25%
- Participate in the Regular Season CTF Event (individual) - 25%
- Participate in the Post-season CTF Event (teams of 2-5 people) - 25%

Performance in NCL will not be graded but it is highly encouraged that you work hard and do your best. These are easy points! Exceptional performance or rankings from the Regular and Post-season may be rewarded with bonus points at the end of the

semester. Each season will be equal to 25% of the participation grade. Complete all 4 seasons for the entire 100% of the participation grade. Working on this contributes to your participation grade.

Teamwork and Cheating

Teamwork is encouraged for the lectures, labs, and on the NCL Gymnasium and Post-Season CTF only. Teamwork is strictly prohibited for all assignments, the final, and the NCL pre-season and regular season.
While I say teamwork is sometimes encouraged, be mindful that cheating is not tolerated. Academic dishonesty is treated very seriously, if you have not already familiarized yourself with the policy, please do. It can be found at http://engineering.nyu.edu/academics/code-of-conduct/ . A single

offense may warrant an F for the course and may result in expulsion from NYU.

University Policies

Moses Center Statement of Disability

Academic accommodations are available for students with disabilities. Please contact the Moses Center for Students with Disabilities (212-998-4980 or mosescsd@nyu.edu) for further information. Students who are requesting academic accommodations are advised to reach out to the Moses Center as early as possible in the semester for assistance.

NYU Tandon School of Engineering Policies and Procedures on Academic Misconduct[1]

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:

    a. 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

[1] Excerpted from the Tandon School of Engineering Student Code of Conduct

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.

b. Fabrication: including but not limited to, falsifying experimental data and/or citations.

c. 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.

d. Unauthorized collaboration: working together on work that was meant to be done individually.

e. 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.

f. Forgery: altering any academic document, including, but not limited to, academic records, admissions materials, or medical excuses.