## COURSE OVERVIEW

**CS GY 6573 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 be to get you to have the knowledge so students may think and work like a successful ethical penetration tester.

https://brightspace.nyu.edu/d2l/home/25997

## LEARNING OBJECTIVES

By the end of this course students should be able to:
- Think and work like an ethical penetration tester, implementing a repeatable and mature methodology that is tailored for each assessment.
- With a given target, successfully identify vulnerabilities, score their risk, and explain mitigations.
- Responsibly disclose findings in a professional report that can be used to recreate the exploit, explain the impact to the target, and prioritize each finding.
- Enumerate target hosts, domains, exposures, and attack surface.
- Identify flaws and vulnerabilities in applications, websites, networks, systems, protocols, and configurations using both manual techniques and assistive tools.
- Reverse engineer compiled applications to discover exploitable weaknesses.
- Write new exploits to test various types of vulnerabilities on clients, against servers, and to escalate privileges.

## REQUIREMENTS

**Knowledge:** 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, using a command shell, and programming.

**Technical:** You will be required to run virtual machines on your computer using VirtualBox, but you are free to use other tools. 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 minimum amount of ram required for good virtualization (2GB host + 2GB Kali + either 2GB Windows VM or 1GB * 2 Linux VMs), but 12 GB is the recommended amount of RAM.  You will need about 50GB free space for storing the VM images.

## COURSE STRUCTURE

The course will be delivered entirely online and each week you will be responsible for listening to a lecture and completing a lab. All course work will be posted and completed on NYU's Brightspace website. External resources may be posted and shared but the Brightspace page is the primary tool which the class will use.

## LEARNING TIME RUBRIC

| Learning Time Element | Weekly Time on Task | Notes |
|---|---|---|
| Lecture (Active Module) | 2-3 hours | Video and interactive text format. Expect quizzes throughout the module. |
| Discussions | 0.5 hours | Students discuss the instructor's questions for each lesson. |
| Reading & Research | 2.5 hour | Students complete recommended readings (online journal articles and tutorials) and work on their related research presentation. |
| Online Labs | 2-3 hours | Students independently work on Online cybersecurity labs. Students will submit a screenshot of their completion. |
| Peer Review | 2.0 hours | Students participate in peer review sessions with other students' work, reviewing and providing feedback. |

All learning time will be asynchronous. Asynchronous is defined as any non-real time student learning, such as recorded lecture, podcast, interactive module, articles, websites, etc. This also includes any student-to-student or faculty-to-student communication that may happen with an asynchronous tool, such as discussion board, chatroom, e-mail, text, etc.

## COURSE COMMUNICATION

NYU Classes will be the primary location for the course homepage, lessons, labs, announcements, day-to-day communication, questions, discussion, and webinars.

Class website: https://brightspace.nyu.edu/d2l/home/25997

**Weekly virtual office hours**

Once a week on an evening to be determined, we will have a 1 to 2 hour webinar/office hour session with the professor. This is an opportunity to hear more details, discuss, and ask questions about the course material, labs, or any other topic. These are not structured, and attendance is optional but encouraged especially if you have questions about lectures.

**COURSE MATERIAL**

Reading and course material will be provided each week. Is it expected that you complete all readings, lessons, and labs. You will not need to purchase any books or materials for this course.

You can access NYU's central library here: http://library.nyu.edu/

**COURSE OUTLINE**

We will follow the NYU calendar and schedule the course as if it were on a Thursday.

https://www.nyu.edu/registrar/calendars/university-academic-calendar.html

https://calendar.google.com/calendar/embed?src=nyu.edu_5peqldm6fpaj6hj2ko75jhpak8%40group.calendar.google.com

| Unit | Date | Title | Assignments | Test Plan / Report |
|---|---|---|---|---|
| 1 | 1/28 | Intro & Pen Test Methodologies | | |
| 2 | 2/4 | Pen Test Process and Reporting | | Plan Introduction |
| 3 | 2/11 | Recon and Enumeration for Pen Testers | #1 released | Plan Scope |
| --- | 2/18 | *Prez Day, NYU Thurs is a Mon* | | |
| 4 | 2/25 | Scanning and Vulnerability Enumeration | **#1 due** | Plan Methodology |
| 5 | 3/4 | *Exploitation 1 - Foundations* | | Plan Deliverables |
| 6 | 3/11 | Exploitation 2 – App Debug and Reversing | | Peer Feedback |
| 7 | 3/18 | *Exploitation 3 – Exploit Development* | | |
| 8 | 3/25 | Web App Testing | #2 released | **Submit Plan (Midterm)** |
| 9 | 4/1 | *Web App Vulns and Exploits 1* | | |
| --- | 4/8 | Final Project Release / Review week | **#2 due** | Release Final - Report |
| 10 | 4/15 | *Web App Vulns and Exploits 2* | | |
| 11 | 4/22 | Post Exploitation - Owning, Pivoting, Priv Esc | #3 released | |
| 12 | 4/29 | Exploitation – Passwords and Authentication | | |
| --- | 5/6 | *Continue work on Final* | **#3 due** | |
| --- | 5/13 | Finals Week. Submit Final Project on May 13 | | **Pen Test Report (Final)** |

**GRADING**

- Assignments 30%
- Midterm 15%
- Final 15%
- Labs 20%
- Quizzes 20%

**Quizzes**

There will be quizzes to complete after most units. Details will be released and available on the class website.

**Labs**

Each lesson will have a hands-on lab to complete. The labs will be opportunities to get some practice implementing the methodologies and using some tools to exercise the techniques we will cover. All labs are mandatory, and you are expected to complete them. Some labs will have an additional component to submit after the lab as proof of completion.

**Assignments**

There will be assignments given through the semester to test your course knowledge and skills. Completion of these assignments will require knowledge and skills practiced in the labs too.

**Midterm and Final**

For the midterm, you will be creating a Penetration Test Plan. We will work on it in several phases with each phase including peer review and feedback. These phases will be opportunities for improvement before the final Test Plan is submitted.

For the final, you will perform a penetration test and write a report on your findings. That will be due the week of finals. More detail will be released during the semester.

**Cheating**

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. Please do not cheat. This includes plagiarism and not citing your sources.**

**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 2nd floor.

**Turnitin**

Students will submit assignments to Turnitin, an originality detection service.

Please read the TurnItIn Terms of Use:
https://help.turnitin.com/Privacy_and_Security/Privacy_and_Security.htm