CS 6573

Syllabus

Welcome to CS6573 - Penetration Testing and Vulnerability Analysis! We have a wonderful and challenging semester planned for you. Below are the details for the upcoming semester - if you have any questions please don’t hesitate to contact me.

This syllabus is **subject to change!**

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 to get you to have the knowledge so students may think and work like a successful ethical penetration tester.

Course Format

The course will be delivered entirely online and each week you will be responsible for listening to a lecture and completing a lab. The lectures and labs will be posted the Sunday night before the following week of class. Lectures will be hosted on NYU’s newclasses site, recitations and office hour periods will be hosted on Slack/Google Hangouts.

Once a week on an evening to be determined by popular vote (Mon, Tues, Wed, or Thurs night), we will have a 2-hour recitation/office hour session. This is an opportunity to discuss and ask questions about the course material, labs, or any other topic. These are not structured, and attendance is optional.

We will use Slack as our main chatroom and discussion place. It’s mobile friendly and has many useful features for teaching, collaborating, having private conversations, and sharing resources. Slack sign up instructions will be posted in the first lecture. Google Hangouts is integrated into Slack and that is what we will use for office hours / recitations. During office hours, or by appointment, I will also be available by Skype or by phone if you have trouble with Hangouts.

Starting in mid-October, 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.

A note for online courses:

An online course has different expectations than an in-person course. This course allows you the flexibility of working at your own schedule, but requires your proactive commitment every week. The course load would be the same as an in-person class and you can easily be overwhelmed if you do not keep up every week. Students need to be significantly more proactive by asking questions and letting me know if there are any areas of confusion. I will be available every week for emails and once a week for the live online interactive sessions. While these are optional, is highly encouraged that you participate if there is any confusion or concern. Please do not wait until last minute.

It is not surprising that an online course does not provide the same kind of experience as an in-person course. Online can be less captivating, less of a unique individualized experience, and can be outright frustrating at times. I will be doing all I can do keep this class as satisfying as in-person course while catering to the needs and flexibility requirements students expect from an online course. If there is concern or feedback for the course at any point, please let me know. **My goal is to create the best environment for you to learn and do well.**

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, 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 VirtualBox but other hypervisors may work, however, you may run into difficulties with networking and deploying images.

Textbook and Course Materials

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 required to register for National Cyber League (NCL), which will count as course materials.

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. NCL registration will start on August 27 and the events will take place between October 19 and November 18. We will discuss this more during the semester. For more info: https://www.nationalcyberleague.org/fall-season

Grading

Assignments	3x15%
Final	30%
Participation	25%

There will be 3 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.

The final will be a project instead of a final exam. The project will be a complete professional Penetration and Vulnerability Analysis report on a special target. Your final grade will be scored evenly by technical accomplishments and findings, and by report quality and completeness. It will be released at the end of November and due at the start of finals, allowing you about 3 weeks to complete it.

Participation

Participation will count for 25% of the grade. This may seem high, but only 5% is for participation on our class site and 20% is participation in the NCL events in April.

The class site participation of 5% will be graded by activity on Slack. Just participate in conversations at least weekly.

The last 20% will be for your participation in NCL this Spring. There are 4 things I will be looking for, each 5%.

1. Complete the NCL Spring Gymnasium Training Labs, Oct 8 – Dec 15
2. Participate in the Pre-season CTF event (placement), Oct 19-27
3. Participate in the Regular Season CTF Event (individual), Nov 2-4
4. Participate in the Post-season CTF Event (teams of 2-5 people), Nov 16-18

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.

If you cannot participate in one of the NCL events due to a conflict, please let me know ahead of time so I can provide an alternative assignment. If you fail to participate without previously telling me, you will receive zero marks.

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. **Teamwork on these is and will be treated like 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 don't cheat. I have caught people every semester cheating on assignments, the final project, or with NCL.**

Schedule

Week	Date	Lesson	Title	Lab
1	10-Sep	1	Intro & Pen Test Methodologies	Lab 1 - Setting up virtualbox
2	17-Sep	2	Target Recon	Lab 2 - Recon (recon-ng, google hacking)
3	24-Sep	3	Scanning and Service Enumeration	Lab 3 - Scanning (netcat, nmap)
4	1-Oct	4	Vulnerabilities and Exploitation	Lab 4 - Exploitation (Metasploit)
5	8-Oct		Fall Recess, no new lecture	
6	15-Oct	5	Stack Buffer Overflows	Lab 5 - Buffer Overflow in Linux NCL Preseason 19-Oct
7	22-Oct	6	Exploitation - Web Applications	Lab 6 - Web Application Vulnerabilities and Attacks
8	29-Oct		Recap / Lab / NCL	NCL Regular Season 2-Nov
9	5-Nov	7	Post Exploitation - Owning, Pivoting, Privilege, Issues	Lab 7 - Post Exploitation (Windows Command Line, Powershell, bash scripting, data exfiltration)
10	12-Nov		Recap / Lab / NCL	NCL Post-Season Apr 27-29
11	19-Nov	8	Post Exploitation - Password Attacks	Lab 8 - Getting Hashes (manually with Windows, Unix, mimikatz)
12	26-Nov		Putting it together (Final Project)	Final Project - Penetration Test and Report
13	3-Dec		Final Project, continued	
14	10-Dec		Final Project, continued	
15	17-Dec		Project, due Monday, December 17, at midnight	

Instructor

Name: Professor Pete Klabe
Email: pete.klabe@nyu.edu
URL: https://engineering.nyu.edu/faculty/pete-klabe
LinkedIn: https://www.linkedin.com/in/pete-klabe-cissp

Professor Pete Klabe is a Cybersecurity Analyst and Risk Assessment Lead working with the US Air Force. As the cyber penetration team lead, he has helped engineers identify weaknesses in their systems and create more secure products to be used by the US military. He also provides software assurance and code analysis to developers to reduce software vulnerabilities in tactical applications. Pete is also an amateur radio operator (WA2YDS) and a member of the Association of Old Crows.

Students with Disabilities

If you are 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 http://www.nyu.edu/students/communities-and-groups/students-with-disabilities.

html. The Moses Center is located at 726 Broadway on the 2nd and 3rd floors.