CSE 3140: Cybersecurity Lab

Spring 2023
January 17, 2023

Instructor
Amir Herzberg (Storrs), amir.herzberg@uconn.edu. Office hours: in office (ITE 217), during any of the lab sessions, except if in the lab; students may coordinate by email, or just come in.

TAs
Ali Arastehfard, ali.arastehfard@uconn.edu
Ronald Maule, ronald.maule@uconn.edu
Connor Rickermann, connor.rickermann@uconn.edu
Mason Tumminelli, mason.tumminelli@uconn.edu
Ezequiel Valencia, ezequiel.valencia@uconn.edu
Karan Patel karan.2.patel@uconn.edu
Hunter Krasnickik hunter.krasnicki@uconn.edu

Office and open-lab hours
The instructor would be available in his office when there is any section of the course, except if he is in the lab itself; you can walk in or coordinate.

TAs will provide office open-lab hours in the lab on Tuesday from 3:30 to 6pm, as well as on Monday 4-5:30pm and Wednesday 3:20-5:30pm.

Communication

We use HuskyCT to post resources and announcements, handle assignments and grades.

We use **Piazza** for non-personal questions, discussions, announcements and more. Sign up for our Piazza at: https://piazza.com/uconn/spring2023/cse3140. We encourage you to actively communicate through illustrative questions or sharing valuable materials. Your engagement and collaboration with others is part of our learning goals for this course. Do not directly solve project questions in the discussion board or any shared communication channel. Clarification and pointers are great, direct solutions are not.

For personal questions and issues, contact the instructor using email or in office hours. However, if you have significant personal issues, including health problems, that may require/justify special accommodations, do not disclose this to the instructor. Instead, contact the **Dean of Students (DoS) office**, which would provide discreet evaluation of your conditions, and offer advice and recommendations to you and to the lecturer. There is no need to discuss your personal or medical problems with the lecturer or the TAs.

Course description, goals and process
This course is designed with two main goals. The first is to introduce basic concepts and techniques of cybersecurity, which are essential to every CSE graduate. The second is as a hand-on lab to teach you applied programming tools and techniques, and in particular, to train you to work in (small) teams – which are also critical elements for every CSE graduate.

The learning is hand-on. You will perform Labs 0-6 as described in the schedule. Lab 0 (introductory) is only one week, other labs are two weeks. The lecturer will introduce each lab. You will perform the labs in ITE 138, following lab guides which we provide in HuskyCT. Most labs can also be done completely remotely, using VPN connection to the lab, from any computer connected to the Internet; however, attendance is mandatory.

Pairs. You will usually work in pairs, preassigned by us, mostly randomly. Requests to avoid an undesired partner should be filled, *in advance*, in a form we provide; we cannot commit to respecting these, but usually, these requests will be honored. We also allow you to ask for higher probability for doing the lab again with a partner you liked; both partners must ask for such requests to have impact. **If you have problems working with your partner**, e.g., does not do anything or (worse!) is abusive, contact TA/Lecturer *immediately*. You may have to complete the lab on your own, but it's much better than trying to work with a bad partner. We will try to identify students that do not cooperate well and they may lose points from their course grade (see below).

Our TAs will guide and assist you at your scheduled lab section, and on the TA office hours (see above). We also encourage cooperation between groups, in lab and outside of it, as long as it is not noisy or otherwise disruptive to other students, and as long as it is ethical (answering technical questions such as `how do I…' is Ok, providing code or solutions is not). Helping, and asking for help, are important skills – and would make learning more productive and much more fun.

Attendance is mandatory. In person participation in your section is mandatory and missing sections will penalize our grade. However, we will not penalize students missing only one or two meetings. You also do not have to attend sessions of the last lab if you inform us, *in advance*, that you 'drop' that lab. If you miss a class, please let the instructor, TA and lab partner know as soon as possible.

If you miss more than two meetings, or require other accommodation, due to special personal situation or medical condition, contact the DoS as discussed under `Communication' above.

Class meetings and schedule
Sections will meet in the Altschuler lab, ITE 138. Planned schedule (for Monday and Wednesday sections):

Lab topic	Monday (1,2,6)	Wednesday (3,4,5)
Introduction, including Acknowledgment of Expectations (sign and submit), Ethics and Legal. Lab 0: SSH, VPN, and Linux basics	Jan. 23	Jan. 18
Lab 1: Passwords and Hashing	Jan 30	Jan 25
	Feb 6	Feb 1
Lab 2: Malware: Virus, Worm and USB transmitted malware (using Rubber-Duckie)	Feb 13	Feb 8
	Feb 20	Feb 15
Lab 3: Ransomware and Crypto	Feb 27	Feb 22
	March 6	March 1
Lab 4: Web technologies (JS, PhP) and Phishing	March 20	March 8

		March 27	March 22
Lab 5: Wireless network security		April 3	March 29
		April 10	April 5
Lab 6: Web security		April 17	April 12
		April 24	April 19
Makeup		April 26	

Required Texts & Learning Materials

We will provide instructions for each lab, including references to supporting materials. We will not follow any textbook.

Grading, assignments and exams

There will be seven labs throughout the semester. While you work in pairs, each student should submit separately; however, you are allowed to write the lab report together (just submit it separately). You submit your work as per the instructions of each lab: for all labs you will need to write and submit a report in HuskyCT, but for most labs, there will also be submission requirements in the lab, by saving files in your VM and/or by uploading solutions in the lab's web server. The lab web-server may provide you with immediate feedback on your answers and automatically grade some questions.

Please always maintain backup copies.

Your numeric grade g will be computed as: $g = a + b + \sum_{i=0}^{6} l_i - min\{l_i\}_{i=1}^{6}$, where:

- $a \leq 6$ is your attendance grade. Missing more than two lab sessions will result in losing all or some of these points. One exception is the last lab which you may skip if you don't need its grade, by informing the lecturer by email *before* the lab begins.
- $b < 8$ are your bonus points. For most students these will be four. You may lose all or some of these points if the lecturer decides that you did not collaborate properly with your lab partners or other students; and you may gain additional points if the lecturer decides that you made special contributions, mainly, by helping other students in class or in our course forums (in Piazza).
- l_i is your grade for the corresponding lab. For lab 0, your grade is between 0 and 6. For the other labs, your grade is between 0 and 17, but we exclude the lowest grade among labs 1 to 6. This includes the possibility that you miss a lab entirely (e.g., due to sickness).

Mapping numeric grade to letter grade:

94-100	90-93	86-89	82-85	78-81	74-77	70-73	66-69	62-65	58-61	0-57
A	A-	B+	B	B-	C+	C	C-	D+	D	F

Grading guidelines:
- Each student is allowed five (5) penalty-free late submission days (for the entire term). You will need to declare how many of these you apply when submitting each lab.
- Each additional late day (after these five penalty-free days), will cause reduction of 10% from the grade of that lab.
- If a student submits after lab was already graded, or after answers were collected the VMs or HuskyCT, their submission would not be graded (as if they didn't submit).

- Up to 20 points may be deducted for submission problems, including badly written/formatted submissions, submissions where answers were only in Husky or only in submission webserver, missing details on report (including names, Net-IDs, section, IP of VM), etc.

Collaboration

We encourage you to discuss related material with your classmates. The lab projects in this class are pair based. You will be assigned a lab mate for each lab. Part of the goal of this assignment is to get you to work with someone who thinks and does things differently than you. Naturally, you are free to communicate freely with your lab mate. Using public resources such as Wikipedia and other websites for information and background is permitted. Students should not seek solutions either through searching or asking a question on any forums. ***You may collaborate with individuals from other groups in problem sets, but your solutions must be written up only by individuals from your group.*** For questions posted on huskyCT assignments (if any), you must write up your solutions independently.
Students may ask technical questions to each other. An example of a permitted question is requesting help in setting up a required program or asking suggestions on helpful resources. Bad questions include asking for code or a technique to solve the project. If you come across some resources that you think will benefit the class, posting it or letting the instructors know will be highly appreciated.

Academic Honesty

The collaboration policy described above is designed to allow students the resources to succeed while ensuring they learn and master the material. If you are unsure if something is acceptable according to the collaboration policy, ask the lecturer by email, in lab or in office hours!
Violations of this policy will be considered violations of the academic integrity policy and will be reported to the Academic Integrity Hearing Board. Consequences may include (but are not limited to) failure of the class. Example violations include jointly solving a project with another team, copying or plagiarizing solutions from other sources, and hacking into another team's resources to gain any advantage.

Ethics

Due to the sensitive nature of the labs, before you start, we need you to sign an *acknowledgment of expectation*, to avoid any misuse of UConn's resources. All work is conducted, in person and/or remotely, in UConn's "***CyberSecurity lab***" environment, which is a separated network that cannot reach the Internet or be accessed directly from the general UConn network. You will need to download a ***VPN client*** and enable two factor authentication to be able to login remotely. We will guide you through the steps during the first week of the semester. This course provides hands-on training in a controlled environment so that students can gain the necessary skills and knowledge. You have explicit permission to conduct the attacks described in this environment only. Security holes and vulnerabilities that are created in this course should only be used in an ethical manner and only in this provided and controlled virtual environment. Usually, these actions would be illegal if conducted on another computer. Acting lawfully and ethically is forbidden and would be your responsibility. Unauthorized access to data, computers, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences. Carefully read the *Computer Fraud and Abuse Act (CFAA)*, a federal statute that broadly criminalizes computer intrusion. This is one of several laws that govern "hacking." Understand what this law prohibits. The general guidance is this: do not use computer systems without authorization or beyond what has been authorized. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail time. Our policy is that you must respect the privacy and property rights of others at all times, or else you will fail the course and possibly face other penalties. If you are ever unsure of what is allowed legally or ethically, please contact your instructor prior to any experimentation.
The first week of the class includes *ethical and legal training*. Completing the training and signing (submitting in HuskyCT) the *acknowledgment of expectation* are required to access the lab.