# Syllabus: CSCI 3330 Cybersecurity Fall 2025

Jeffrey Knockel

## 1 Course description

This course offers an introduction to cybersecurity principles with a focus on attacks targeting cryptography, network security, and web technologies. Students will actively engage in ethical hacking, learning not only how to identify and exploit vulnerabilities in systems but also how to design resilient systems capable of withstanding various attack methods. By the end of the course, students will gain a deep understanding of the core principles that unify different attack techniques and their respective defenses. Additionally, the course covers legal and ethical issues in cybersecurity, including how to engage in the responsible disclosure process.

## 2 Attendance, location, and time

Attendance is not taken but is expected and will be essential for succeeding in the class. Bring a laptop to every class for completing in-class exercises.

- Location: Searles Science Building 223
- Time: MW 1:15pm – 2:40pm
- Website: https://tildesites.bowdoin.edu/~j.knockel/csci3330f25/

## 3 Learning outcomes

Overall I would like you to habituate thinking like a hacker would. A hacker is constantly evaluating in their mind how a system is expected to work versus how it works in practice, looking for any kind of inconsistency between the two that they can exploit. I would like you to think this way not just when you are formally analyzing a system for vulnerabilities but in everyday scenarios when you are reading someone else's code or writing your own code, especially when that affects other users. In this course I will assess you on the following learning outcomes:

- To evaluate computer systems to identify vulnerabilities in multiple domains (e.g., Web, databases, networks, operating systems) and explain their root causes.

- To construct proof-of-concept exploits and corresponding fixes in controlled environments.
- To explain the high-level commonalities between vulnerabilities and transfer experience identifying vulnerabilities and executing exploits in familiar domains taught in the course to novel ones not explicitly taught.

# 4 Grading

- Assignments: 25%
- Final portfolio: 25%
- Midterm exam (Oct. 15): 20%
- Final exam (Dec. 20 1:30–4:30pm): 30%

All assignments and exams will be graded out of 100 points. Just like in your future career, it is important for you to turn in work on time. If you are sick or have other extenuating circumstances, let me know as soon as possible before the assignment deadline that you would like an extension. For *unexcused* late submissions that are $n > 0$ days late, $3^n$ points will be deducted from the grade before being applied toward the final course grade.

Assignments will be graded in two dimensions: (1) completion and (2) the traditional grading criteria which also includes correctness. Only (1) will be used to determine your grade in the class, whereas (2) will be informational only. This means that as long as you earnestly complete the assignment, you will receive full marks toward your grade in the class even if you made mistakes. My intention for this grading policy is that I want you to become comfortable making mistakes while you are learning, and I want your assignment to provide an accurate signal of your progression in the class. You should still strive to submit fully correct assignments, as this will be valuable practice for the exams, and in any case acing an assignment is *cool*.

Note that your final portfolio and the midterm and final exams will be graded using traditional means that include both completeness and correctness.

The final portfolio project will be a composition of your three favorite assignments which you are most proud of, which you will compose into an application for either a job or for graduate school. You will have an opportunity to make improvements to your assignments between their original submission and your final portfolio project in response to feedback. More information will be provided during the semester.

As an extra credit opportunity, I encourage you to find and report vulnerabilities in real-world software. Come talk to me first so that we can discuss whether what you are thinking about looking for is feasible to find and appropriate for extra credit. If you find a vulnerability, I will also help you to report the vulnerability in a responsible fashion. (In addition to receiving extra credit in this course, many but not all vendors pay out monetary bug bounties in response to disclosing vulnerabilities.)

## 5 AI Policy

In this class, you should not use generative AI technology (e.g., ChatGPT) outside what the assignment expressly allows.

The ultimate goal of this course is not to generate specific exploits or remediations but rather to learn to think differently and more critically about how complex computer systems work. Getting stuck on a difficult problem is normal, and when we finally solve it and have that breakthrough moment — that is when we have developed a new way of thinking that we can resource for the rest of our lives. Unfortunately, there is no shortcut to this process. By using generative AI tools or otherwise reappropriating solutions from other sources we deprive ourselves of becoming better thinkers. Of course, sometimes we get *too* stuck on a problem, and even if we aren't stuck, it is natural to still have questions. As your class instructor, I am available to help you think about a problem without depriving yourself of crucial opportunities to cultivate new ways of thinking critically.

## 6 Office hours and contact information

During my office hours, you may talk to me about anything directly related to the class, such as assignments, but also other topics adjacent to the class like internships, graduate school opportunities, etc.

1. Office location: Searles Science Building 219
2. Office hours: MW 3:00pm – 4:00pm, F 9:00am – 10:00am, or by appointment
3. Email: j.knockel – bowdoin.edu
4. Slack: you will receive instructions on joining during our first assignment.

I also invite you to provide anonymous feedback about this course here.

## 7 Tentative schedule

The following is a tentative schedule for the material covered in this course and is subject to change:

1. Sept. 3: Introduction
2. Sept. 8, 10: Ethical hacking, responsible disclosure, entropy, passwords
3. Sept. 15, 17: Database security, SQL injection
4. Sept. 22, 24: The World Wide Web, XSS, CSRF, command line injection
5. Sept. 29; Oct. 1: Network layers, the Internet, IP, TCP, port scanning

6. Oct. 6, 8: DNS, DNSSEC, firewall evasion
7. Oct. 15: Midterm exam
8. Oct. 20, 22: Symmetric cryptography, asymmetric cryptography
9. Oct. 27, 29: Diffie-Hellman, TLS
10. Nov. 3, 5: Cryptographic hash functions, digital signatures, hash collisions
11. Nov. 10, 12: Memory layout, ASLR, buffer overflows, ROP
12. Nov. 17, 19: Dynamic linking, format string vulnerabilities
13. Dec. 1, 3: Adversarial machine learning, adversarial A.I.
14. Dec. 8, 10: Race conditions, TOCTTOU vulnerabilities, conclusion
15. Final exam: Dec. 20 1:30–4:30pm

# 8 About me

In my research I fight to defend our safety and freedom online. I use novel techniques to uncover harmful software behavior. I reveal applications' secret censorship rules and hidden surveillance activity, and I expose how gaps in applications' security put the safety and privacy of our data in jeopardy. See my personal site for more information.