Welcome to
Computer Security!

CSC 482/582 (Fall 2021)

Meets on Thursdays 6:15-9:00pm in GH 250

Dr. James Walden

waldenj@nku.edu

(859) 572-5571

http://faculty.cs.nku.edu/~waldenj

Table of Contents

1 Summary

Computer security is an exciting and rapidly growing discipline that touches on all of our lives. We see news about data breaches and ransomware attacks weekly. This class will teach you why such events occur and how we can make security incidents less common in the future. We'll learn about common mistakes developers make and how to write secure software that eliminates or mitigates the vulnerabilities arising from those mistakes.

Computer security has grown into a much larger subject than one can learn in a single course. This class focuses on three areas of security: software security, network security, and applied cryptography. Our approach to security is hands-on, so we will learn about these topics by writing code to implement both attacks and defenses. There will be lab activities in most class meetings.

1.1 Prerequisites

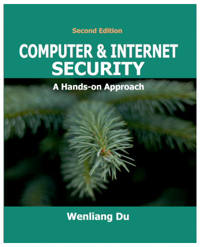
CSC 362. Students should be able to write simple C programs. Familiarity with simple binary and hexadecimal arithmetic is important, as is knowing the basics of the TCP/IP network model. The ability to program in python and use the Linux command line is helpful but not necessary to know before the course. These topics can be learned during the course of the semester.

1.2 Student Learning Outcomes

After successfully completing this course, you should be able to

1. Describe common security vulnerabilities and the risks they impose.
2. Explain how attacks exploit common vulnerabilities.
3. Explain how appropriate security controls can mitigate attacks.
4. Detect vulnerabilities in source code, then apply secure coding techniques to remove or mitigate them.
5. Describe common cryptographic techniques and apply them to mitigate risks.

1.3 Required Textbooks



Computer and Internet Security: A Hands-on Approach, Second Edition by Wenliang Du. ISBN:978-1733003926. 2019.

You **must** have the textbook before the second class meeting. The textbook contains essential readings that will not be covered in lecture. There is no electronic version of the textbook, so be sure to order the book early enough to receive it before the second week of classes.

2 What Can I Expect to Happen During Class?

In order to learn, you will need to be actively engaged with the course content. The schedule on the class Canvas page provides a summary of what you need to be doing for each class meeting. Before each class meeting, complete the readings listed in the Readings column of the class schedule for that meeting. Material in the readings will not be covered by lectures in class meetings. If there is a quiz listed in the Quiz column for that class meeting, be sure to complete the quiz *by 11:59pm on the night before the class meeting*. Quizzes will cover the readings and material from previous class meetings.

Some readings will be from the textbook, which are listed as `Du, chapter N`, where `N` is the number of the chapter to read before class. Other readings will be given as hyperlinks to an article or book chapter on the web. Some of the hyperlinked readings have the word `(reference)` after the link. Reference readings provide additional information, which can be useful if you need a refresher on topics like TCP/IP networking or SQL queries. Quizzes do not cover material in the reference readings.

Class meetings will be divided into multiple segments, including mini-lectures, small group activities, discussions, and lab activities. Small group activities will typically involve writing, but some will require the use of software. We will begin working on labs during class times, but most labs will require time outside of class to complete. Lab reports will always be written individually outside of class, but it can be useful to be recording your results in a Google or Office 365 document during class.

3 Technology Used in This Class

Each student will have their own virtual lab environment, consisting of three virtual machines (VMs), labeled Seed, Attacker, and Server. Early labs will use only one VM, while later labs will use two or three VMs. Each VM has the same configuration based on Ubuntu Linux 16.04, with specific changes made so that course labs will work on them. The virtual lab environment is accessed through the NKU College of Informatics vSphere system.

vSphere is available through a web interface at `https://coivcenter.hh.nku.edu`. NKU's vSphere system can only be accessed while using NKU's Virtual Private Network (VPN). If you have already installed and configured the NKU VPN, you can use your current installation. If you have not installed NKU's VPN yet, go to `https://vpn.nku.edu` to download and install the VPN software.

4 Available Help and Support

I am available to help you with the class via e-mail, discussion forums, office hours, and scheduled appointments (in person or via Zoom). I will respond to questions within one business day, unless an emergency arises. Please see the Communication Policy below for how to best get answers to your questions.

Cybersecurity content resources specific to this course can be found via the Resources page on the class web site, while cybersecurity resources for the university and local area can be found on the web site for NKU's http://cis.nku.edu/.

NKU's tutoring program and writing center are both available online at `https://inside.nku.edu/plus/tutoring/online.html`. Help and resources for NKU's learning management system are available from `https://inside.nku.edu/cite/technologyresources/Canvas_student.html`. The student technology guide, including support for student services, can be found at `https://inside.nku.edu/it/student-tech-guide.html`.

5 Course Topics

We will cover the following topics this semester. A detailed schedule of topics and what needs to be done for each class meeting with due dates can be found on the class web site.

1. Introduction and terminology
2. Cybersecurity fundamentals
3. Threats, attacks, and vulnerabilities
4. Access control
5. Privileged programs
6. Environment variables
7. Shellshock
8. Buffer overflows
9. Format strings
10. Integer security
11. Race conditions
12. Authentication
13. Cross-Site Request Forgery (CSRF)
14. Election security
15. Cross-Site Scripting (XSS)
16. SQL Injection
17. Packet sniffing and spoofing
18. TCP attacks
19. Firewalls
20. DNS Attacks
21. Virtual Private Network (VPN)
22. Security protocols
23. Secret-key cryptography
24. Hash functions
25. Public key cryptography
26. Public key infrastructure (PKI)
27. Transport layer security (TLS)
28. Bitcoin and blockchain

6 Grading

Your grade in this course will be based on the following classes of assessments, each of which counts for the specified percentage of your semester grade.

Labs (42%) Students will begin working on labs in the class session on which they appear in the schedule. Students are responsible for completion of any parts of the lab not completed during class on their own. In-class lab work will be completed in pairs, while out of class work can be completed individually or with your partner. Each student must individually write and submit their own lab report, which is due about a week after the class period in which students began working on the lab. There are 14 labs in total. Lab descriptions and due dates can be found on the Canvas assignments page.

Quizzes (13%) Online quizzes will be due by the end of the day on Wednesdays, starting in the second week of class. These quizzes are designed to assess both your understanding of previous classes and your preparation for the next class period, so you will need to complete the readings for the next class meeting before taking a quiz. Quizzes are designed using learning principles of spaced repetition and interleaving, in order to ensure that you retain the material long term and are well prepared for exams. This means that quizzes are comprehensive. You're welcome to use your book and notes when taking quizzes. There are 14 quizzes in total, and your lowest quiz score will be dropped when computing your grade.

Midterm Exam (20%) The midterm examination will be open book and completed outside of class. It will cover all material up until the date of the exam. While quiz questions are given in a multiple choice or multiple answer format, exam questions will typically be in an essay format.

Final Exam (25%) A comprehensive examination covering all of the material in the course given. The final exam will be an open book exam in the same format as the midterm exam. It will be given during the last class meeting and will be due during finals week.

Graduate students taking this class as CSC 582 will be responsible for posting cybersecurity news articles with a one paragraph description of how the article ties into class content. The instructor will create a weekly thread for such articles. CSC 582 students will be responsible for posting a total of 14 articles, due on the same dates as the quizzes. These articles and their tie-in descriptions will receive a binary grade of zero or one, which is used as a multiplier for the quiz grade that is due on the same date. This means that graduate students must post an article with a tie-in description to the class forum by the quiz due date to receive credit for a quiz.

Your letter grade will be based on your percentage score from the sum of the assessment areas above as shown in the table below.

Undergraduate Students			
Grade	**Percent**	**Grade**	**Percent**
A	93-100	C+	77-80
A-	90-93	C	73-77
B+	87-90	C-	70-73
B	83-87	D+	67-70
B-	80-83	D	60-67
		F	0-60

Graduate Students			
Grade	**Percent**	**Grade**	**Percent**
A	93-100	C+	77-80
A-	90-93	C	73-77
B+	87-90	F	0-73
B	83-87		
B-	80-83		

Midterm grades will be provided to all students in 100 - 400 level courses, except in cases where the Department Chair and Dean have waived midterm grade reporting for pedagogical reasons. Midterm grades are only an estimate of performance as of the middle of the semester and are not an absolute predictor of final performance. Mid-term grades will be posted in myNKU by the deadline established in the Academic Calendar.

7 Participation Policy

You are expected to be an active participant in class discussions and other in-class activities. To do this, you must prepare by completing the readings and other learning activities specified on the class schedule before coming to class. Class activities have been designed to help prepared students achieve the class learning outcomes. Missing class, not actively participating, and not being prepared will negatively affect your ability to learn course content.

8 Communication Policy

I'm here to help you learn, and I have a few communication guidelines to make the course run as smoothly as possible. Questions about course content or technology should be asked in the General Questions & Answers forum, so that other students can provide and benefit from posted answers. Personal matters should be discussed with me through e-mail.

When asking questions on a discussion forum or by e-mail, be sure to include:

- A subject that provides a summary of your question. Include the class number at the beginning of the subject for e-mail messages.
- A detailed description of the problem. Specify precisely on which assignment, virtual machine, user account, and software the problem occurred and provide a detailed list of steps needed to reproduce the problem. Include the full text of any error messages.
- The message should close with your full name.

I will answer forum questions within one business day unless a student has already provided a correct answers. I will respond to e-mail messages within one business day except in the event of an emergency.

Students should check the class web site and NKU e-mail accounts for university-wide and class-specific announcements 24 hours before each class period.

9 Late Work/Missed Exam Policy

All students are expected to complete learning tasks on schedule. It is important to stay on track with your assignments. This is an important skill in the workplace and will help you feel less stressed. Being able to meet deadlines and juggle many tasks are important career and life skills. Thus, you will need to complete all exams, labs, and assignments according to the class schedule. However, I recognize that personal circumstances may at times make it difficult or impossible to complete a learning task on schedule. If you have a personal situation that prevents you from completing a task on time, you will need to discuss this with me prior to the due date if possible, or as soon as it becomes possible, so that we can develop a plan. Extensions are at my discretion. If an extension is provided, it is important to know that the format or content of an assignment or exam may be modified.

10 Registrar Withdrawal Information

Students sometimes need to withdraw from a course for personal or academic reasons. If you do encounter difficulties with the course, please contact me prior to withdrawing. NKU's Fall 2021 Academic Calendar includes deadlines for withdrawing for a course.

11 Academic Integrity Policy

Academic integrity benefits everyone in our community. It not only helps you reach the real goal of this class–learning–but also allows for the university and degree program to be perceived positively by others, including your future colleagues and employers. When students are dishonest, they lose out on valuable learning that will help them perform well in their career. Academic dishonesty is any attempt by a student to gain academic advantage through dishonest means or to help another student in gaining an unfair advantage. Academic integrity is important whether the work is graded or ungraded, group or individual, written or oral.

The Student Honor Code is a commitment by students of Northern Kentucky University, through their matriculation or continued enrollment at the University, to adhere to the highest degree of ethical integrity in academic conduct. It is a commitment individually and collectively that the students of Northern Kentucky University will not lie, cheat, or plagiarize to gain an academic advantage over fellow students or avoid academic requirements.

Students, faculty, staff, and administrators at NKU strive to achieve the highest standards of scholarship and integrity. Any violation of the Student or Graduate Student Honor Codes is a potentially serious offense because it threatens the quality of scholarship and undermines the integrity of the community. All NKU faculty members are asked to report incidents of academic misconduct to the office of Student Conduct Rights and Advocacy. While academic in scope, a violation of the NKU Honor Code may be considered a violation of the NKU Code of Student Rights and Responsibilities and will follow the adjudication processes described therein.

Through the NKU Honor Code, students who are responsible for academic dishonesty may receive sanctions, including, but not limited to, a final grade of F, or removal from the course in which the violation occurs. Repeated violations of the NKU Honor Code, or when suspension or expulsion from NKU may be a possible outcome of the violation, the incident will be referred to the office of Student Conduct, Rights and Advocacy.

12 Credit Hour Policy

In accordance with federal policy, NKU defines a credit hour as the amount of work represented in the achievement of student learning outcomes (verified by evidence of student achievement) that reasonably approximates one hour (50 minutes) of classroom instruction and a minimum of two hours of out-of-class student work. For every course credit hour, a typical student should expect to spend at least three hours per week of concentrated attention on course-related work including, but not limited to, class meeting time, reading, reviewing, organizing notes, studying and completing assignments. At least an equivalent amount of time is expected for other academic activities such as online courses, laboratory work, internships, practica, studio work and other academic work leading to the award of credit hours.

Estimates of the time required for a typical student to complete course expectations are:

In-Class (2 day x 75 min x 15 weeks)	37.5 hours
Class readings and quizzes (150 min x 15 weeks)	37.5 hours
Labs (5 hours x 14 labs)	70 hours
TOTAL	145 hours

13 NKU Policies

13.1 Accomodations Due to Disability

The University is committed to making reasonable efforts to assist individuals with disabilities in their efforts to avail themselves of services and programs offered by the University. To this end, Northern Kentucky University will provide reasonable accommodations for persons with documented qualifying disabilities. If you have a disability and feel you need accommodations in this course, you must present me a letter from the Office for Student Accessibility (OSA, SU 303) indicating the existence of a disability and the suggested accommodations. More information on OSA can be found at https://inside.nku.edu/osa.html.

13.2 Changes in the Syllabus

The syllabus is a projection of what the instructor anticipates for the course. The instructor has the right to modify the syllabus in order to adjust to changing circumstances.

13.3 Other Information

For information on university-wide policies governing students, please see the University Common Syllabus on your course Canvas site.