

Course Syllabus

[Jump to Today](#)

CMPS 4620 - Network and Computer Security Sections 1 and 2 - Fall 2023

Instructor and Contact Information

Instructor: Dr. Melissa Danforth (she/her)

Office Hours: MW 5:30-6:30pm (after class), TuTh 12:00-1:30pm (after meetings)

Office: Science III 319

Office Phone: (661) 654-3180

Email: mdanforth@csub.edu (<mailto:mdanforth@csub.edu>)

Website: <https://www.cs.csub.edu/~melissa/>  (<https://www.cs.csub.edu/~melissa/>)

Other: You can also direct message me on Slack or Discord to contact me. Links to my Discord server and the course Slack workspace are available in the [General Course Information module](https://csub.instructure.com/courses/26350/modules/194769) (<https://csub.instructure.com/courses/26350/modules/194769>)

Note: Please give at least 2 business days for replies to emails and direct messages

Class Information

Course meets MW 4:00-5:15pm (lecture) and Fr 4:00-6:30pm (lab) in Science III 240

Zoom link available by request for those who cannot attend in person. Email or direct message me for the link.

Attendance and General Class Structure

Attendance is optional in this course. The topics covered in lecture and the lab assignments will be listed on Canvas. Recordings of lectures and lab demos will also be provided after post-processing (give 2-3 business days for post-processing). It is your responsibility to watch the recording if you cannot attend class.

Class structure:

- Mondays and Wednesdays (lecture days): Lectures will be on textbook material and additional materials relevant to the week's topics. Slides and recordings will be posted to Canvas.
- Fridays (lab days): Attendance is optional, but strongly encouraged since the classroom computers will be pre-configured for the labs. If you opt to do the lab from home, you will be responsible for configuring your computer to run the lab software.

Please be mindful of the evolving risks with the pandemic and other illnesses. If you are feeling sick, please stay home and either request the Zoom link or watch the recordings later. Likewise, if I am feeling sick and need to cancel class or convert a class to a Zoom session, I will let everyone know by email, Canvas announcement, and Slack announcement.

Note: There is also the possibility of faculty union action that may cause some class meetings to be canceled. Notification of any such action will also be given by email, Canvas announcement, and Slack announcement.

Team/Group Assignments

Working in teams or groups is optional for lab assignments in this course. If you do opt to work in groups on the lab assignments, collaboration options include git, Slack, Discord, Zoom, MS Teams, and so on. If you opt for a face-to-face team or group meeting, you must adhere to all current campus COVID-19 policies and procedures regarding face-to-face meetings.

Important Caveat: If you want a team private channel on the course Slack workspace, you must contact me to create that channel. Any Slack private channels created directly by students will be considered a violation of the campus academic integrity policy (unauthorized collaboration).

Catalog Description

Fundamentals of network and computer security and information assurance. Topics covered include basic cryptography, authentication, access control, formal security policies, assurance and verification, trusted OS design, and network attacks. Methods to provide better security at both the system and network level will be presented, particularly with respects to risk analysis, cost-benefit analysis, and psychological acceptability. Ethics and legal issues related to security research will also be discussed.

Catalog Prerequisites: CMPS 2020 with a grade of C- or better and either CMPS 3620 or CMPS 3650

Prerequisites by Topic

Knowledge of programming languages in C/C++ family

Knowledge of TCP/IP networking and/or digital forensics

Units and Contact Time

4 semester units. 3 units lecture (150 minutes), 1 unit lab (150 minutes).

Class Expectations

As a 4000-level elective course, students are expected to engage in independent learning in this course through reading assignments, case studies, and a project. Critical thinking, independent evaluation, and troubleshooting are important traits for the cybersecurity profession.

Since the textbook is freely available online through multiple sources, lectures after the first week will assume that you have completed the reading assignments. While the lectures will cover some of the textbook concepts, particularly the more complicated concepts, the lectures will primarily focus on exploring examples, applications of the concepts, and scenarios to provide a deeper understanding of the concepts. Additional materials may also be brought in from other sources during the lectures to provide more breadth and/or depth on the concepts.

Most labs will require the use of virtual machines (VMs). The lab computers will have the VM pre-installed. If you want to create a VM at home, the department has a subscription service to VMware which provides students with a free one-year license to VMware software for Linux, Windows, and Mac. Contact the instructor for more info.

Plan to spend an average of 8-12 hours outside of class each week on this course. More time may be required in some weeks.

Class Principles

The following principles will guide this course:

- *Communication*: I understand if something unexpected has come up that interferes with your course work. Please communicate with me as soon as possible though, so we can discuss extensions and other options for moving forward in the course. Similarly, should something come up unexpectedly in my life that affects a class meeting, I will let the course know by Canvas announcements, Slack announcements, and email. Please keep the lines of communication open.
- *Respect*: There are many situations in cybersecurity where differing, but equally valid, opinions may exist. Respect the rights of others to form different opinions and conclusions than your own.
- *Critical Thinking*: While there may be some rote assignments in this course, many assignments will require applying critical thinking and analysis skills. My grading approach for those "thinking questions" is more about seeing your thought process than seeking "perfect" answers. It is also okay to state what you don't understand in an assignment submission. That is all part of the learning process.
- *Compassion*: Remember that other people in the class (and me) are balancing many competing priorities beyond this course. Exercise compassion, kindness, and consideration when interacting with others.




Course Type

Selected elective for CS

Required Textbook

Security Engineering, 3rd edition. Ross Anderson. Wiley, 2020. ISBN: 978-1-119-64281-7.

Links related to the textbook:

- Author's website: <https://www.cl.cam.ac.uk/~rja14/book.html> 
(<https://www.cl.cam.ac.uk/~rja14/book.html>)
- Free e-book through CSU O'Reilly Safari Tech Books subscription:
<https://learning.oreilly.com/library/view/security-engineering-3rd/9781119642787/> 
(<https://learning.oreilly.com/library/view/security-engineering-3rd/9781119642787/>). (Note: First click the following link to activate the CSU subscription on their domain: <https://go.oreilly.com/california-state-university-bakersfield/> ) (<https://go.oreilly.com/california-state-university-bakersfield/>.)

Recommended Textbook and Other Supplemental Materials

Computer Security: Art and Science, 2nd edition. Matt Bishop. Addison-Wesley, 2019, ISBN-13: 978-0-321-71233-2. <http://nob.cs.ucdavis.edu/book/>  (<http://nob.cs.ucdavis.edu/book/>)

(Note: There is an abridged version of the book available that is titled "Introduction to Computer Security" by Matt Bishop)

Supporting articles and current events relating to the course will be posted on Canvas

Coordinator(s)

Melissa Danforth

Student Learning Outcomes

This course covers the following ACM/IEEE CS2013 (Computer Science) Body of Knowledge student learning outcomes:

- CS-HCI/Human Factors and Security
 - Explain the concepts of phishing and spear phishing, and how to recognize them.
 - Explain the concept of identity management and its importance.
 - Analyze a security policy and/or procedures to show where they consider, or fail to consider, human factors.
- CS-IAS/Foundational Concepts in Security
 - Describe the concepts of risk, threats, vulnerabilities and attack vectors (including the fact that there is no such thing as perfect security).
 - Explain the concepts of authentication, authorization, access control.
 - Explain the concept of trust and trustworthiness.
- CS-IAS/Principles of Secure Design
 - Describe the principle of least privilege and isolation as applied to system design.
 - Summarize the principle of fail-safe and deny-by-default.
 - Discuss the implications of relying on open design or the secrecy of design for security.
 - Discuss the benefits of having multiple layers of defenses.
 - For each stage in the lifecycle of a product, describe what security considerations should be evaluated.

- Describe the concept of mediation and the principle of complete mediation.
- Explain the concept of trusted computing including trusted computing base and attack surface and the principle of minimizing trusted computing base.
- Discuss the importance of usability in security mechanism design.
- CS-IAS/Threats and Attacks
 - Discuss the limitations of malware countermeasures (e.g., signature-based detection, behavioral detection).
 - Identify instances of social engineering attacks and Denial of Service attacks.
 - Discuss the concepts of covert channels and other data leakage procedures.
- CS-IAS/Network Security
 - Describe the different categories of network threats and attacks.
 - Describe the architecture for public and private key cryptography and how public key infrastructure (PKI) supports network security.
 - Identify the appropriate defense mechanism(s) and its limitations given a network threat.
- CS-IAS/Cryptography
 - Describe the purpose of cryptography and list ways it is used in data communications.
 - Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities.
 - Use cryptographic primitives and describe their basic properties.
 - Summarize security definitions related to attacks on cryptographic primitives, including attacker capabilities and goals.
- CS-SP/Professional Ethics
 - Explain the ethical responsibility of ensuring software correctness, reliability and safety.
 - Evaluate the professional codes of ethics from the ACM, the IEEE Computer Society, and other organizations. (Course Note: We will focus on cybersecurity professional organizations instead of ACM and IEEE)

ABET Outcome Coverage

The course maps to the following student learning outcomes for Computer Science (CAC/ABET):

- 1. An ability to analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
- 3. An ability to communicate effectively in a variety of professional contexts.
- 4. An ability to recognize professional responsibilities and make informed judgements in computing practice based on legal and ethical principles.

Lecture Topics and Rough Schedule

Week	Chapter(s)	Topics
1	Outside Materials	Ethics of security research, Responsible disclosure, Legal foundations

2	Chapter 5	Basics of cryptography, Historic ciphers, Block ciphers
3	Chapter 5	Block chaining, DES and AES, Hash functions
4	Chapter 5	Public key encryption, Uses of cryptography
5	Chapter 4	Identity, Authentication, Secure authentication
6	Chapters 3 and 6	Passwords, Access control
7	Chapters 9 and 10, and Outside Materials	Mandatory access control, Bell-LaPadula model, Biba model, Lattice model
8	Chapters 10 and 12	Conflict of interest model, Clark-Wilson model
9	Chapter 27	Secure design, Trusted operating systems
10	Chapter 28 and Outside Materials	Saltzer-Schroeder principles, Evaluation of OSes, Formal vs informal evaluation
11	Chapter 28	Evaluation history and current methods: Red Book, Green Book, British Criteria, Common Criteria
12	Chapter 21	Network attacks, Types of malware
13	Chapter 21	Vulnerability classification, Prevention and mitigation
14	Chapters 21 and 2	Intrusion detection and prevention systems, Social engineering, Advanced persistent threats
15	None	Project presentations

Specific reading assignments for each week will be posted to Canvas.

Civility During Discussions

Over the course of the term, there will be classroom discussions on contentious issues in cybersecurity, such as discussing various approaches to disclosing vulnerabilities. Opinions will differ, sometimes drastically, during these discussions, hence why they are matters of debate within the cybersecurity field. Students are expected to be civil to, and respectful of, one another during these discussions.

Course Academic Integrity Policy

Lab assignments may be optionally completed in groups. For a group lab assignment, one person in the group can turn in one submission for the entire group, but make sure everyone's name is on the submission so all members of the group receive credit for the assignment.

All other assignments are individual assignments. That means you may discuss the assignments with one another, but each student must turn in their own work in their own words. It is also okay to reference external sources in your submission, but you must appropriately paraphrase that source by expressing the information you researched in your own words.

For example, you cannot copy-and-paste from a website (including generative AI responses) or copy another student's submission, but you can refer to that website and summarize what you've learned, or summarize your discussion with the other student. I even encourage you to add questions you still have, and, if I have time during grading, I'll try to customize my grading comments to answer those questions.

In summary, no direct copying from any source (other students, external sources, textbook, etc.) is allowed. Instances of direct copying that are detected may be referred to the Dean of Students as an academic integrity violation.

Additionally, any Slack private channels created directly by students will be considered a violation of the academic integrity policy (unauthorized collaboration) and may be referred to the Dean of Students.


Campus Academic Integrity Policy

Certain forms of conduct violate the university's policy of academic integrity and the student conduct code. Academic dishonesty (cheating) is a broad category of actions that use fraud and deception to improve a grade or obtain course credit. Academic dishonesty is not limited to exams alone but arises whenever students attempt to gain an unearned academic advantage. Plagiarism is claiming the published or unpublished work of someone else as your own. This includes handing in someone else's work; turning in copied or purchased compositions; using paragraphs, sentences, phrases, words, or ideas, including paraphrasing, written by another writer; or using data and/or statistics compiled by someone else as your own without giving appropriate credit to the original writer. Plagiarism also includes using your work submitted in another class without permission of your current instructor.

When a faculty member discovers a violation of the university's policy of academic integrity, the faculty member will meet with the student(s) involved and is required to notify the Dean of Students Office and detail the alleged violation, including the name(s) of the student(s) suspected, the class in which the alleged violation occurred, the circumstances of the alleged violation, and the evidence (including witnesses) supporting the allegation. The faculty member will also formally notify the student(s) suspected of violating the university's policy of academic integrity, the department chair for the course involved in the incident, and the appropriate school dean. The Dean of Students or designee will investigate; confer with the faculty member, student(s), and any witnesses identified; and review all evidence submitted by the faculty member and student(s) to impose an administrative sanction, beyond the academic penalty already placed by the faculty member. Students who perform dishonestly in this course may earn zero credit on the assignment/exam or a failing grade in the course, depending on the level of severity of the offense.


Students are expected to uphold the standards of academic integrity. Cheating in any form will not be tolerated and will result in a formal report to the University Dean of Students. You are always expected to follow the student conduct code and uphold the CSUB Guiding Principles while learning on this campus.



Academic Accommodations


To request academic accommodations, please contact the Office of Services for Students with Disabilities (SSD) and either email me or bring me an accommodations letter from the SSD Office. Policies from the SSD Office relating to accommodations, such as scheduling policies for using their testing center, must also be followed. For more information about the services and policies of the SSD Office, contact their staff by email and/or visit their website at <https://www.csub.edu/ssd/> 
[\(https://www.csub.edu/ssd/\)](https://www.csub.edu/ssd/)


Basic Needs Assistance

If you are experiencing challenges related to basic needs, such as food insecurity, housing insecurity, or other challenges, there are resources available to you.

The campus Food Pantry, located next to the Student Union, is open and available to all students, staff, and faculty. Please visit the Food Pantry website for hours and information at <https://www.csub.edu/basicneeds/food-pantry>  [\(https://www.csub.edu/basicneeds/food-pantry\)](https://www.csub.edu/basicneeds/food-pantry)


Information about food distributions, CalFresh, and other food resources can be found at <https://www.csub.edu/basicneeds/food-security>  [. \(https://www.csub.edu/basicneeds/food-security\)](https://www.csub.edu/basicneeds/food-security). Information about food assistance at the Antelope Valley campus is at <https://www.csub.edu/basicneeds/resources-students-csub-av-campus> 
[\(https://www.csub.edu/basicneeds/resources-students-csub-av-campus\)](https://www.csub.edu/basicneeds/resources-students-csub-av-campus)


The campus also has emergency housing available for full-time students on a first-come, first-served basis. For housing concerns, please contact Jason Watkins, Assistant Director for Basic Needs. You can find more information about housing assistance and contact information at <https://www.csub.edu/basicneeds/housing-stability>  [\(https://www.csub.edu/basicneeds/housing-stability\)](https://www.csub.edu/basicneeds/housing-stability)

More information on basic needs assistance is on the Basic Needs website: <https://www.csub.edu/basicneeds>  [\(https://www.csub.edu/basicneeds\)](https://www.csub.edu/basicneeds)

Health and Well-Being


This continues to be a trying time mentally, physically, and with work / life balance issues. If you need additional time for assignments due to your current situation, please contact me to discuss the options available to you. Similarly, should something come up unexpectedly in my life that affects a class meeting, I will let everyone know through email / Slack / Canvas.


The CSUB Counseling Center has both regular-hours and after-hours counseling services available. Call 654-3366 to connect with their services. After their normal operating hours, you can press 2 at any time to connect to the after-hours service. More information is at <https://www.csub.edu/counselingcenter/>  [\(https://www.csub.edu/counselingcenter/\)](https://www.csub.edu/counselingcenter/)


CSUB's Student Health Services is available for basic health care needs, at little to no cost for CSUB students. You can find more information about their services at <https://www.csub.edu/healthcenter/> 
 (<https://www.csub.edu/healthcenter/>)

Current information about CSUB's COVID-19 plans, policies, and resources can be found at <https://www.csub.edu/covid-19>  (<https://www.csub.edu/covid-19>)

Technology Assistance and Software

If you need help with technology, such as a loaner laptop and/or hotspot, ITS has programs to provide technology assistance to students. Go to the following ITS webpage to learn more about their programs: <https://its.csub.edu/step>  (<https://its.csub.edu/step>)

The CEE/CS Department has academic software subscriptions available to students enrolled in CMPS and ECE courses. This currently includes Microsoft, VMware, and Mathematica. Go to the following page for more information: <https://www.cs.csub.edu/downloads.php> 
 (<https://www.cs.csub.edu/downloads.php>)

CSUB ITS also many software products available to students through the Virtual Computer Lab (VCL). You will need to use your myCSUB credentials to access VCL. To see the full list of software and to access VCL, go to <https://its.csub.edu/VCL>  (<https://its.csub.edu/VCL>)

Grading

Academic Integrity Quizzes	5%
Reading Assignments	10%
Lab Assignments	25%
Checkpoint Assignments	20%
Project and Project Milestones	20%
Final Exam	20%

Grades are posted on Canvas. It is your responsibility to check Canvas for grades and any comments on assignments. If you believe you submitted your assignment on time but Canvas is not showing it, contact me.

Late Policy

Canvas is configured to record a 0 grade if an assignment is not received by the due date. That 0 will remain on late submissions until I grade the submission.

End-of-term deadline: All assignments except for the final exam must be submitted to Canvas by December 13th at 11:59pm to give me sufficient time to grade before grades are due on December 20th.

Late policies for specific assignment categories are:

- Academic Integrity Quizzes: No due date, but they must be completed by the above end-of-term deadline.
- Reading Assignments: Assignments may be submitted late, but questions from late submissions will not be incorporated into lectures. Assignments will be assessed a 10% late penalty for each week they are late, with a grace period of 3 days. For example, if you turn the assignment in 2 days late, there will be no penalty. But if you turn the assignment in 4 days late, there will be a 10% late penalty.
- Labs and Checkpoint Assignments: Assignments may be submitted late through the above end-of-term deadline. Assignments turned in more than 2 weeks late will be assessed a 10% late penalty for every week they are late. For example, if you turn an assignment 1 week after the deadline, there will be no late penalty. If you turn an assignment in 4 weeks after the deadline, there will be a 20% late penalty. If you turn the assignment in 6 weeks after the deadline, there will be a 40% late penalty.
- Project and Milestones: Since you will need to present your project during the last week of class to everyone, contact me if you miss a deadline for the milestones.
- Final Exam: Contact me if you are unable to take the final exam during its scheduled time.

If your reason for being late with an assignment falls under the university excused absence policy (e.g., illness, campus event, etc.), contact me to discuss an extension to the submission deadline.

Canvas Submission Guidelines

Submissions must be in a standardized document format (e.g., ODT, DOC, DOCX, PDF, PNG, JPEG, etc.). Avoid RTF format, as it has caused issues in the past. Also, make sure to check your file after it has uploaded to be sure there were no upload errors.

If you have drawn something out by hand, take a picture or use a scanner to incorporate the image into your submission. Please keep the file sizes reasonable, but also make sure the image is legible.

If you submit multiple files, please name them in a fashion that indicates what they contain and what order I should read them in, e.g. q2_drawing.jpg, part1.pdf, part2.docx, and so on.

If you have any difficulties submitting to Canvas, contact me or ITS for help. Emailed submissions are not guaranteed to be accepted since my email volume is so high and the spam detection software can silently drop emails.

Academic Integrity Quizzes

The campus academic integrity module is required for this course. There is no deadline for completing the modules and quizzes, but I recommend you complete them at the start of the semester, as the resources will be useful for your project.

Reading Assignments

As an elective course, you are expected to spend the time before class on the reading assignments. For each reading assignment, you will need to turn in your thoughts and questions from the assignment.

Questions that many students have about the reading assignment will be incorporated into that week's lecture, so this is your best avenue for letting me know what you'd like to be covered during lecture.

Reading assignments are graded on an effort basis, which means you will receive full points if you submit something that shows honest effort by the assignment deadline. Reading assignments are due on Sundays at 11:59pm to give me sufficient time to incorporate common questions into the lecture materials for the week.

The lowest reading assignment grade will be dropped from the overall grade calculation.

Lab Assignments

Lab assignments reinforce concepts from lecture and give you an opportunity to practice hands-on skills. The lab reports are due at 11:59pm on the Thursday following the lab. Partial credit will be given for incomplete lab reports.

You may work on labs in groups of up to 3 students. If you work in a group, only one student needs to submit the lab report, but make sure to put everyone's names on the submission. Only the students whose names are on the submission will get credit for the lab. If you are in a group but are not the one submitting the report to Canvas, you may add a comment to the Canvas assignment indicating who did submit the report for your group.

Submit your work to Canvas and I will grade it during my next grading session. Do NOT email your submission as the campus spam system sometimes silently blocks emails with attachments.

The lowest lab assignment grade will be dropped from the overall grade calculation.

Checkpoint Assignments

Checkpoint assignments will be a mix of theoretical questions and reinforcement of hands-on skills learned in labs. Assignments and due dates will be posted on the course website. Partial credit will be given for incomplete submissions.

Assignments must be turned in via Canvas. Do NOT email your submission as the campus spam system sometimes silently blocks emails with attachments.

Assignments may be discussed with others in the class, but every student must turn in their own assignments in their own words. Copying from other students, the Internet (including generative AI), previous solutions, the textbook, etc. are all considered violations of the Academic Integrity Policy.

Project and Project Milestones

All students will select a topic in security and conduct a survey project on that topic for this course. A list of potential topics will be posted to Canvas, but students are also welcome to propose ideas that are not on the list.

Each project will require the submission of a brief project proposal (1-2 paragraphs) describing the topic for the project. Topics will be approved by the instructor, or sent back for revision, to ensure that no one topic gets selected too many times by people in the class. The proposal will be part of the Project grade.

Topics will be approved on a first-come, first-served basis, based on the submission/last-edit time for the proposal on Canvas. You may include a "backup" second topic description in your proposal, in case too many students who submitted proposals before you had already selected your first topic.

There will also be project milestones throughout the term to see what sort of progress has been made on the project. These milestones include written assignments and a check-in meeting scheduled during one lab day and outside of the normal class meeting times. The milestones will be part of the Project grade.

At the end of the term, everyone will give a brief (~10 minutes) presentation about their project. The lecture and lab time slots in the last week of class will be used for presentations. A choice poll will be set up for everyone to choose a presentation time slot. Students will also be required to upload their slides to Canvas after their presentation. The presentation will count for a majority of the Project grade.

The oral communication rubric used to assess the presentation will be posted on Canvas.

Final Exam

The final exam time slot for this course is Monday December 18th from 5:00-7:30pm. Note that this is later than the normal class meeting time. A study guide will be posted to Canvas towards the end of the semester.

If you have more than two final exams scheduled on Monday December 18th or another university excused absence that would prevent you from taking the final exam that day, contact me at least ONE WEEK before the final exam to schedule an alternative window.


Prepared By



Melissa Danforth on 24 August 2023










Approval of Course Outline













Approved by CEE/CS Department in Spring 2014
Effective Fall 2016

Course Summary:

Date	Details	Due
Mon Sep 4, 2023	 Reading Assignment 1 (for lecture in Week 2) https://csub.instructure.com/courses/26350/assignments/467273	due by 11:59pm

Date	Details	Due
Thu Sep 7, 2023	 Lab 1: Linux in a Nutshell (https://csub.instructure.com/courses/26350/assignments/472957)	due by 11:59pm
Sun Sep 10, 2023	 Project Topic Selection (https://csub.instructure.com/courses/26350/assignments/467275)	due by 11:59pm
Sun Sep 10, 2023	 Reading Assignment 2 (for lecture in Week 3) (https://csub.instructure.com/courses/26350/assignments/467274)	due by 11:59pm
Thu Sep 14, 2023	 Lab 2: Networking Command Line Tools (https://csub.instructure.com/courses/26350/assignments/475055)	due by 11:59pm
Sun Sep 17, 2023	 Reading Assignment 3 (for lecture in Week 4) (https://csub.instructure.com/courses/26350/assignments/475472)	due by 11:59pm
Thu Sep 21, 2023	 Lab 3: Investigating MD5 Hash Collisions (https://csub.instructure.com/courses/26350/assignments/476617)	due by 11:59pm
Sun Sep 24, 2023	 Checkpoint Assignment 1 (https://csub.instructure.com/courses/26350/assignments/475607)	due by 11:59pm
Sun Sep 24, 2023	 Reading Assignment 4 (for lecture in Week 5) (https://csub.instructure.com/courses/26350/assignments/477321)	due by 11:59pm
Thu Sep 28, 2023	 Lab 4: Introduction to Password Cracking (https://csub.instructure.com/courses/26350/assignments/477669)	due by 11:59pm
Sun Oct 1, 2023	 Reading Assignment 5 (for lecture in Week 6) (https://csub.instructure.com/courses/26350/assignments/477323)	due by 11:59pm
Thu Oct 5, 2023	 Lab 5: Password Cracking - Week 1 (https://csub.instructure.com/courses/26350/assignments/479209)	due by 11:59pm
Thu Oct 12, 2023	 Lab 6: Password Cracking - Week 2	due by 11:59pm

Date	Details	Due
	https://csub.instructure.com/courses/26350/assignments/480700	
Sun Oct 15, 2023	 Reading Assignment 6 (for lecture in Week 8) https://csub.instructure.com/courses/26350/assignments/481342	due by 11:59pm
Thu Oct 19, 2023	 Lab 7: Password Cracking - Catch-up Week https://csub.instructure.com/courses/26350/assignments/481347	due by 11:59pm
Sun Oct 22, 2023	 Reading Assignment 7 (for lecture in Week 9) https://csub.instructure.com/courses/26350/assignments/481929	due by 11:59pm
Thu Oct 26, 2023	 Lab 8: Network Packet Capture with tcpdump https://csub.instructure.com/courses/26350/assignments/482664	due by 11:59pm
Wed Nov 1, 2023	 Reading Assignment 8 (for lecture in Week 10) https://csub.instructure.com/courses/26350/assignments/484294	due by 11:59pm
Thu Nov 2, 2023	 Lab 9: Investigating a Network Packet Capture File https://csub.instructure.com/courses/26350/assignments/484244	due by 11:59pm
Sun Nov 5, 2023	 Checkpoint Assignment 2 https://csub.instructure.com/courses/26350/assignments/482721	due by 11:59pm
Sun Nov 5, 2023	 Reading Assignment 9 (for lecture in Week 11) https://csub.instructure.com/courses/26350/assignments/484295	due by 11:59pm
Thu Nov 9, 2023	 Lab 10: Investigating Common Criteria in Windows, Apple, and Linux OSes https://csub.instructure.com/courses/26350/assignments/484304	due by 11:59pm
Sun Nov 12, 2023	 Reading Assignment 10 (for lecture in Weeks 12 and 13) https://csub.instructure.com/courses/26350/assignments/484303	due by 11:59pm
Sun Nov 19, 2023	 Project Research	due by 11:59pm

Date	Details	Due
	(https://csub.instructure.com/courses/26350/assignments/484312)	
Sun Nov 26, 2023	 Reading Assignment 11 (for lecture in Week 14) (https://csub.instructure.com/courses/26350/assignments/488705)	due by 11:59pm
Mon Nov 27, 2023	 Lab 11: Investigating Intrusion Detection Systems with Snort (https://csub.instructure.com/courses/26350/assignments/484310)	due by 11:59pm
Fri Dec 1, 2023	 Project Presentation Outline (https://csub.instructure.com/courses/26350/assignments/484313)	due by 11:59pm
Mon Dec 4, 2023	 Checkpoint Assignment 3 (https://csub.instructure.com/courses/26350/assignments/484600)	due by 11:59pm
Thu Dec 7, 2023	 Lab 12: Vulnerability Scanning with GVM (https://csub.instructure.com/courses/26350/assignments/484311)	due by 11:59pm
Mon Dec 11, 2023	 Checkpoint Assignment 4 (https://csub.instructure.com/courses/26350/assignments/484601)	due by 11:59pm
	 Project Presentation (https://csub.instructure.com/courses/26350/assignments/484314)	due by 11:59pm
	 Quiz: Academic Integrity (https://csub.instructure.com/courses/26350/assignments/459335)	due by 11:59pm
Wed Dec 13, 2023	 Quiz: Cheating (https://csub.instructure.com/courses/26350/assignments/459336)	due by 11:59pm
	 Quiz: Ethical Writing (https://csub.instructure.com/courses/26350/assignments/459337)	due by 11:59pm
	 Quiz: Plagiarism (https://csub.instructure.com/courses/26350/assignments/459338)	due by 11:59pm
Mon Dec 18, 2023	 Final Exam (https://csub.instructure.com/courses/26350/assignments/491980)	due by 11:59pm