Applied Cybersecurity Community Clinic
Applied Cybersecurity Foundations Course
I 320 – Fall 2024 – 27460/64

Contact Info

Professor Francesca Lockhart
francesca.lockhart@austin.utexas.edu
Office: SRH 3.349
Office hours: Monday 12:00-2:00 PM, Wednesday 1:30-3:30 PM by appointment only

Class Meetings

Mondays and Wednesdays from 3:30-4:45 PM in GDC 1.406

Class Overview

The Applied Cybersecurity Community Clinic is a two-semester sequence that first equips students with the technical and business skills of an entry-level cybersecurity analyst (semester 1) and then partners them in (supervised) teams with a small business, public sector organization, or nonprofit to render pro bono cybersecurity services (semester 2). During the first semester, students will learn key cybersecurity defense concepts and skills, such as risk assessment, network configuration and security, access controls, responding to a cyberattack, business planning, and penetration testing. Students will also learn how to form an effective cybersecurity consulting team and communicate with organization leaders and employees about essential cybersecurity controls and functions. By the conclusion of this course, students will be prepared to work within their assigned teams to assess, design, and render a cybersecurity improvement project plan for their assigned clinic client organization next semester.

Learning Objectives

Students will:

- Learn how to assess, prioritize, and mitigate cyber risks to small organizations through readings, lectures, case studies, and simulated exercises on access and authorization controls, vulnerability management, secure configuration of networking assets, cyber incident response, and other tools and concepts commonly utilized to protect under-resourced organizations
- Understand how to project plan and communicate cybersecurity risks and solutions with organization and business leaders with no prior cybersecurity knowledge or experience
- Prepare to provide supervised hands-on cybersecurity services on a day-to-day basis to a small business, public sector organization, or nonprofit in Texas during the second semester clinic course

Grading and Assessment Methods

This course will use plus/minus grades.

Assignments submitted on Canvas (12 total) will cumulatively account for **55% of your grade**.

- The first ten assignments will be weighted equally and graded on a pass/fail basis based on completion to make up **25% of your overall grade**. Several of the first ten assignments have two assignment options (A or B) you may pick from based on your interests and goals for growth in the field.

- Assignments #11 and #12 are the final class project and will each count for **15% of your overall grade (30% total).** These assignments will be graded out of 100 according to the provided guidelines and rubric available on Canvas. These assignments will be due the night before and presented on the last class day, **December 9th.**

- Please note that assignments are listed below according to the dates they become available in Canvas. It is your responsibility to note the due date for each assignment and submit via Canvas on or prior to that date. Concerns about meeting the below deadlines will be considered, but only if they are communicated to the instructor **before** the assignment due date/time, not after.

There will be a midterm exam consisting of 60 multiple-choice questions to be completed on Canvas during a class session. The midterm exam will account for **30% of your grade**.

As stated in the Cybersecurity Clinic Student Code of Conduct, regular and punctual attendance is required for you to be a successful cyber clinic team member. Therefore, class attendance and participation will count for **15% of your grade**.

Assigned Materials
Please do the readings before the assigned class date and come to class prepared to be asked to discuss and apply them. As there were no formal prerequisites for this course, the readings will cover basic cybersecurity concepts and give you the theoretical background you need to be successful in the applied clinical component of semester two.

- Assigned textbook:
  - *CompTIA Security+ Study Guide Exam SY0-701* by Mike Chapple and David Seidl (Provided in eBook format at no cost to you, courtesy of the Strauss Center. See email sent to your preferred email address or course Canvas site for your personal link to download.

- Assigned online materials:
  - Google Cybersecurity Professional Certificate – Provided at no cost to you via Coursera, courtesy of Google.org. Access the certificate via the email sent to your preferred email address.
  - Tryhackme.com – Create a free account to complete assigned labs.

- Optional/recommended materials for continuing education:
  - Professor Messer's CompTIA SY0-701 Security+ Training Course Videos
  - *Foundations of Information Security* by Jason Andress
  - Should you seek to attain the CompTIA Security+ credential following completion of this course, please let me know so we can discuss other study and financial resources.

Accommodations
The university is committed to creating an accessible and inclusive learning environment consistent with university policy and federal and state law. Please let me know if you experience any barriers to learning so I can work with you to ensure you have equal opportunity to participate fully in this course. If you are a student with a disability, or think you may have a disability, and need accommodations please contact Disability & Access (D&A). Please refer to the D&A website for more information: http://diversity.utexas.edu/disability. If you are already registered with D&A, please deliver your Accommodation Letter to me as early as possible in the semester so we can discuss your approved accommodations and needs in this course.

Course Sequence, Readings, and Assignments
Subject to change at instructor's discretion. Updates will be announced in class and new versions of the syllabus will be located on the course Canvas site.

Week 1

Monday, August 26: Syllabus Review and Clinic Policies

- **Assignment 1 (due Sunday, September 1 by 11:59pm CST)**: Turn in signed code of conduct via Canvas Assignment #1 AND complete Student Pre-Engagement Questionnaire via Canvas Quizzes.

Wednesday, August 28: Foundational Cyber Policies and Agencies

- Readings (Also available to read on Canvas):
  - PPD 41
  - EO 14028 Fact Sheet
  - National Cyber Strategy Overview
  - Fact Sheet: 2024 Report on the Cybersecurity Posture of the United States

Week 2

Monday, September 2: Labor Day – No Class

Wednesday, September 4: Cyber Attacks, Threat Actors, and Methods: The Threat to Target-Rich, Resource-Poor Organizations

- Readings:
  - Textbook chapter 2: "Exploring Cybersecurity Threats" section
  - Small Business Cybersecurity Statistics for 2024
  - Statescoop Article – "Local Governments Don't Have Enough Cyber Funding, Survey Finds"
  - "PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders" (Canvas)
  - Optional: "Cyber Advisory: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to US Critical Infrastructure" (Canvas)

- **Assignment 2A (due Sunday, September 8 by 11:59pm CST)**: Pick one of the following three articles (Dallas Cyber Attack, North Texas Municipal Water Authority Cyber Attack, UT Health East Texas Cyber Attack – also available to read on Canvas) and identify the following items for your selected case study. Submit paragraphs describing the following via Canvas Assignment #2, and note that you may need to do some additional research:
  - Attack type
  - Attack vector (or your best guess, if unknown)
  - Recommended mitigation to prevent this attack in the future

- **Assignment 2B (due Sunday, September 8 by 11:59pm CST)**: Pick one of the following three articles (Dallas Cyber Attack, North Texas Municipal Water Authority Cyber Attack, UT Health East Texas Cyber Attack – also available to read on Canvas) and identify the following items for your selected case study. Prepare to verbally brief a summary of the case study and the following items for 1-2 minutes during class on Monday, September 9. Submit which article you chose via Canvas Assignment #2 to help Professor Lockhart prepare the briefing order.
  - Attack type
  - Attack vector (or your best guess, if unknown)
  - Recommended mitigation to prevent this attack in the future

Week 3

Monday, September 9: Inventory Assets and Assess Risks

- **National Security Career Fair Today: 9am-3pm in the Etter-Harbin Alumni Center!**

- Readings:
  - Textbook chapter 17: "Analyzing Risk," "Managing Risk," and "Risk Tracking" sections
  - Global Cyber Alliance (GCA) Small Business Toolkit - Step 1

- **Assignment 3 (due Sunday, September 15 by 11:59pm CST):** Complete Module 1 of the "Assets, Threats, and Vulnerabilities" course from the Google Cybersecurity Professional Certificate; submit screenshot(s) showing completion via Canvas Assignment #3.

Wednesday, September 11: Manage Authentication and Authorization

- Readings:
  - Textbook chapter 4
  - Textbook chapter 8: "Authentication methods" section through end

- **Assignment 4A (due Sunday, September 22 by 11:59pm CST):** Complete the "Encryption Methods" and "Authentication, authorization, and accounting" sections within Module 2 of the "Assets, Threats, and Vulnerabilities" course from the Google Cybersecurity Professional Certificate; submit screenshots showing completion via Canvas Assignment #4.

- **Assignment 4B (due Sunday, September 22 by 11:59pm CST):** Use the 2FA Directory to implement 2FA on five of your personal accounts that did not previously have it enabled. Submit the names of the five websites/platforms and what type of 2FA you enabled on each via Canvas Assignment #4.

Week 4

Monday, September 16: Identify and Patch Vulnerabilities

- Readings:
  - "Flaws in the System" section and "Approaches to vulnerability scanning" reading within Module 3 of the "Assets, Threats, and Vulnerabilities" course from the Google Cybersecurity Professional Certificate
  - Textbook chapter 5: "Vulnerability Management" and "Vulnerability Life Cycle" sections

Wednesday, September 18: Automatic Updates and Encryption

- Readings:
  - Textbook chapter 7: "Goals of Cryptography" section through "Cryptographic Attacks" section

Week 5

Monday, September 23: Endpoint and Mobile Security

- Readings:
  - Textbook chapter 3
  - Textbook chapter 11: "Endpoint Security Tools" subsection within "Protecting Endpoints"
  - Textbook chapter 13: "Managing Secure Mobile Devices" section

- **Assignment 5A (due Sunday, September 29 by 11:59pm CST):** Play the Financial Times' Ransomware Negotiation simulation and submit a screenshot showing completion via Canvas Assignment #5.

- **Assignment 5B (due Sunday, September 29 by 11:59pm CST):** Install/enable antivirus software and an ad blocker on your computer (hint: use Step 4 of the GCA Toolkit). Via Canvas Assignment

#5, submit which software tools you selected for these purposes (including if completed prior to this course) and explain why you picked those.

Wednesday, September 25: Network and Wireless Security

- Readings:
    - Textbook chapter 12: beginning through "Virtual Private Networks and Remote Access" section; "Secure Protocols" section
    - Textbook chapter 13: "Building Secure Wireless Networks" section
- **Assignment 6 (due Thursday, October 3 by 11:59pm CST):** Complete Modules 1, 2, and 3 of the "Connect and Protect: Networks and Network Security" course from the Google Cybersecurity Professional Certificate; submit screenshot(s) showing completion via Canvas Assignment #6.

Week 6

Monday, September 30: Network Security Devices; Email Security

- Readings:
    - Textbook chapter 12: "Network Appliances and Security Tools" section through "Network Security, Services, and Management" section
    - "Network Hardening" section within Module 4 of "Connect and Protect: Networks and Network Security" course from the Google Cybersecurity Professional Certificate
    - DMARC, SPF, and DKIM explainer
- **Assignment 7 (due Tuesday, October 8 by 11:59pm CST):** From the Google Cybersecurity Professional Certificate:
    - Complete Module 3 of the "Play It Safe: Manage Security Risks" course
    - Complete Module 2 and Module 4 of the "Sound the Alarm: Detection and Response" course
    - Submit screenshot(s) showing completion via Canvas Assignment #7.

Wednesday, October 2: Cloud Models and Security

- Readings:
    - Textbook Chapter 10

Week 7

Monday, October 7: AI in Cybersecurity

- Readings:
    - "Envisioning Cyber Futures with AI" from Aspen Digital
    - Textbook chapter 6: "Automation and Orchestration" section
    - Optional: "Secure, Empower, Advance: How AI Can Reverse the Defender's Dilemma" from Google

Wednesday, October 9: Midterm Review Session

Week 8

Monday, October 14: Midterm Exam: 60 question multiple choice completed through Canvas in class; open note and book.

- Receive midterm participation grade preview – this is not factored into your final grade, but is simply intended to show you where I assess your grade at should you continue at your current participation and attendance levels.

Wednesday, October 16: Data Privacy; Governance, Risk, and Compliance

- Readings:
  - "Information privacy: Regulations and compliance" section within Module 2 of the "Assets, Threats, and Vulnerabilities" course from the Google Cybersecurity Professional Certificate
  - Textbook chapter 16, "Complying with Laws and Regulations" section
  - UT Austin Internal Cyber Clinic Data Guidance (Canvas)

<u>Week 9</u>

Monday, October 21: Organizational Security Policies and Plans

- Readings:
  - "Best practices for effective documentation" section within Module 3 of "Sound the Alarm: Detection and Response" course from the Google Cybersecurity Professional Certificate
  - Textbook chapter 16: "Understanding Policy Documents", "Personnel Management", and "Third-Party Risk Management" sections

- **Assignment 8 (due Sunday, October 27 by 11:59pm CST):** Utilize the provided "Assignment 8 – Nonprofit Profile" to fill out the "Assignment 8 – Sample Information Security Policy Template" for the fictional nonprofit. Note that in addition to filling in the highlighted portions of the template correctly, you may add or remove sections from the template. Submit the completed information security policy for the nonprofit via Canvas Assignment #8.

Wednesday, October 23: Recognizing Cyber Threats

- Readings:
  - Textbook chapter 12: "Network Attacks" section
  - Textbook chapter 14: "Incident Response" section

<u>Week 10</u>

Monday, October 28: Cyber Threat Intelligence and Pentesting

- Readings:
  - Textbook chapter 2, "Threat Data and Intelligence" section
  - Textbook chapter 5, "Penetration Testing" section
  - "Attacker Mindset" section within Module 3 of the "Assets, Threats, and Vulnerabilities" course from the Google Cybersecurity Professional Certificate
  - "Securing Linux" section within Module 4 of the "Connect and Protect: Networks and Network Security" course from the Google Cybersecurity Professional Certificate

- **Assignment 9A (due Sunday, November 3 by 11:59pm CST):** Complete Module 2 and Module 3 of the "Tools of the Trade: Linux and SQL" course from the Google Cybersecurity Professional Certificate; submit screenshot(s) showing completion via Canvas Assignment #9.

- **Assignment 9B (due Sunday, November 3 by 11:59pm CST):** Complete Pentesting Fundamentals, Basic Pentesting, and Metasploit: Introduction modules through TryHackMe; submit screenshot(s) showing completion of all three labs via Canvas Assignment #9.

Wednesday, October 30: Incident Response and Recovery

- Readings:
  - Textbook chapter 14: "Incident Response Data and Tools" section through end

- **Assignment 10 (due Sunday, November 10 by 11:59pm CST):** Within the Google Cybersecurity Professional Certificate:
  - Complete "The incident response lifecycle" and "Incident response operations" sections within Module 1 of "Sound the Alarm: Detection and Response" course;
  - Complete "Response and recovery" and "Post-incident actions" sections within Module 3 of "Sound the Alarm: Detection and Response" course;
  - Submit screenshot(s) showing completion via Canvas Assignment #10.

Week 11

Monday, November 4: Selecting and Categorizing Controls

- Readings:
  - Textbook chapter 1: "Implementing Security Controls" section
  - Recommending Security Tools
  - Trusted CI Framework 16 Musts One Pager (Canvas)

Wednesday, November 6: Creating a Cybersecurity Project Plan

- **Receive team assignments in class and via Canvas**
- Readings:
  - BBB Business Profile (Canvas)
  - BBB Project Plan and Presentation Rubric (Canvas)

- **Assignment 11 (due Sunday, December 8 by 11:59pm CST):** Within your group, any 4 students should work together to create a 10-minute presentation identifying at least 5 risks and proposed controls to mitigate these risks for Ballot's Bowwow Box. Prepare to present in class on Monday, December 9th, followed by 5 minutes Q&A. Only one team member needs to submit the presentation on behalf of your group via Canvas Assignment #11.
  - Include at a minimum the sections outlined in the presentation template provided on Canvas, including but not limited to:
    - Executive summary
    - Risk matrix
    - Suggested controls to address risks, including estimated cost
    - Who within your group is assigned to implement each control
    - Who within the company will need to assist with install/configuration/long-term management of each control
    - Timeline/schedule for implementation

- **Assignment 12 (due Sunday, December 8 by 11:59pm CST):** Within your group, the remaining (other 4) students not developing the presentation for Assignment #11 should create a written report summarizing your group's project plan for improving the cybersecurity of Ballot's Bowwow Box. Only one team member needs to submit on behalf of your group via Canvas Assignment #12.
  - Include at a minimum the sections outlined in the report template provided on Canvas, including but not limited to:
    - Executive summary
    - Asset inventory
    - Risk assessment methodology and results (including a risk matrix)
    - Suggested controls to address risks, including control type, goal, and estimated cost

- Who within your group is assigned to implement each control
- Who within the company will need to assist with install/configuration/long-term management of each control
- Timeline/schedule for implementation

- Refer to the BBB Project Plan and Presentation Rubric provided on Canvas for grading. Groups will be graded holistically based on the scores assigned to both the presentation and the written report.

Week 12
Monday, November 11: Ballot's Bowwow Box: How to Fact-Find and Communicate with Organizational Leaders

- Readings:
  - Why Your Audience Should Care—and Act
  - How To Teach Adults
  - Textbook chapter 16: "Security Awareness and Training" section

Wednesday, November 13: Ballot's Bowwow Box: Asset Inventory, Risk Assessment

Week 13
Monday, November 18: Ballot's Bowwow Box: Research Controls for Risks

Wednesday, November 20: Ballot's Bowwow Box: Suggest Controls for Risks

Week 14
Fall Break – No Classes

Week 15
Monday, December 2: Ballot's Bowwow Box: Task Assignments and Timeline

Wednesday, December 4: Ballot's Bowwow Box: Presentation and Report Work Day

Week 16
Monday, December 9: Final Project Presentations; Spring Course Expectations and Resource Review (Guests: Industry Expert Mentors)