Applied Cybersecurity Community Clinic
Applied Cybersecurity Foundations Course
I 320 - Fall 2023

Contact Info
Professor Francesca Lockhart
francesca.lockhart@austin.utexas.edu
Office: SRH 3.349
Office hours: Monday 11 AM-12:30 PM, Wednesday 2:15-4 PM by appointment only

Class Meetings
Monday, Wednesday, Friday from 1-1:50 PM in MEZ 1.202

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 local business, municipal government, nonprofit to render pro bono cybersecurity services (semester 2). During the first semester, students will learn key cybersecurity defense concepts and skills, such as vulnerability assessment, network configuration and security, access controls, authorization techniques, responding to a cyberattack, business planning, and penetration testing. Students will also learn how to form an effective cybersecurity operations team and communicate with organization and business 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 client organization next semester.

Learning Objectives
Students will:

- Learn how to assess, prioritize, and mitigate cyber risks to small organizations through case studies and simulated exercises on access and authorization controls, vulnerability scanning, network configuration and monitoring, penetration testing, and cyber incident response, amongst other topics
- Understand how to 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 the greater Austin, Texas area during the second semester clinic course

Grading and Assessment Methods
This course will use plus/minus grades.

There will be a midterm exam consisting of 75 multiple-choice questions to be completed on Canvas. The midterm exam will account for 30% of your grade. There will be no final exam.

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 20% of your grade. For participation: what matters is quality, not quantity. **Please refrain** from using your phones during class, and keep computer use to **only** notetaking and referencing the textbook/course materials. I will ask you to put your computer away if I suspect you are not paying attention.

Assignments submitted on Canvas (13 total) will cumulatively account for 50% of your grade, with each assignment weighted an equal amount. These will be graded on a pass/fail basis based on completion, except for Assignments #12 and 13. These two assignments will be graded out of 100 according to the provided guidelines and rubrics (see Canvas).

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.

Assigned Materials
It is imperative that you do the readings before the assigned class date and come to class prepared 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+ SY0-601 Exam Cram – 6th Edition by Martin Weiss (Provided in eBook format at no cost to you, courtesy of the Strauss Center. See 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. More instructions on enrollment to follow)
  - Tryhackme.com – Create a free account to complete assigned labs later in the semester

- Important materials to continually reference during and after the course:
  - Glossary of Essential Terms and Components (located at the end of your textbook)
  - CISA Cybersecurity Performance Goals Checklist
  - Global Cyber Alliance (GCA) Small Business Toolkit
  - CIS Blueprint for Ransomware Defense Tools and Resources

- Optional/recommended books for continued education:
  - CompTIA Security+ Study Guide: Exam SY0-601 8th Edition by Mike Chapple
  - 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 exam 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 21: Syllabus Review and Course Policies

- Readings:
  - Clinic Student Code of Conduct (Canvas) – Copy provided in class

Wednesday, August 23: Foundational Policies and Documents

- Readings:
  - PPD 41
  - EO 14028 Fact Sheet
  - National Cyber Strategy Overview
  - NIST Cybersecurity Framework Overview
  - CISA Cybersecurity Performance Goals

Friday, August 25: The Cyber Threat to Small Businesses and Nonprofits (Guest Speakers)

- Readings:
  - Exam Cram Part I Chapters 1 and 2
  - Dallas Cyber Attack
  - Solar Winds
  - Norton Health

- **Assignment 1 (due Thursday, August 31 by 11:59pm CST)**: Pick one of the above (Dallas, Solar Winds, or Norton) and identify the following for your selected case study. Respond via Canvas Assignment #1, and note that you may need to do some additional research:
  - Attack type:
  - Attack vector (or your best guess, if unknown):
  - Recommended (or only) mitigation:

Week 2

Monday, August 28: Cyber Attacks, Threat Actors, and Methods (Guest Speaker)

- Readings:
  - Exam Cram Part I Chapter 3, Chapter 5, and Part IV Chapter 27 (Beginning through page 511)

Wednesday, August 30: Inventory Devices and Applications

- Readings:
  - Week 1 of the "Assets, Threats, and Vulnerabilities" course from the Google Cybersecurity Professional Certificate
  - Global Cyber Alliance (GCA) Small Business Toolkit - Step 1

- **Assignment 2 (due Thursday, September 7 by 11:59pm CST):** Utilize Fing and exploration of your personal devices to complete your own Hardware and Software Asset Tracking spreadsheet (also available for download on Canvas). Ensure you are running the latest possible version of your OS and all installed applications. Submit your completed spreadsheet (Hardware and Software tabs only – leave off Sensitive!) via Canvas Assignment #2.

Friday, September 1: Automatic Updates and Encryption (Guest Speaker)

- Readings:
  - Exam Cram Part II Chapter 16
  - GCA Toolkit - Step 2
  - What Should I Know About Encryption?

- Optional: Exam Cram Part III Chapter 25; "Encryption methods" section within Week 2 of the "Assets, Threats, and Vulnerabilities" course from the Google Cybersecurity Professional Certificate

Week 3

Monday, September 4: Labor Day Holiday – No Class

Wednesday, September 6: Passwords / Authentication (Guest Speaker)

- Readings:
  - Exam Cram Part II Chapter 12
  - GCA Toolkit - Step 3
  - CISA Checklist – Sections 1 (Account Security) and 3.4

Friday, September 8: Passwords / Authorization

- Readings:
  - Exam Cram Part III Chapters 23 and 24 (stop at "Authentication Protocols" section on page 457)
  - "Authentication, authorization, and accounting" section within Week 2 of the "Assets, Threats, and Vulnerabilities" course from the Google Cybersecurity Professional Certificate
  - Preventing Unauthorized Access Table (Canvas)

- **Assignment 3 (due Thursday, September 14 by 11:59pm CST):** Use the 2FA Directory to implement 2FA on three of your personal accounts that did not previously have it enabled. Submit the names of the three websites/platforms and what type of 2FA you enabled on each via Canvas Assignment #3.

Week 4

Monday, September 11: Vulnerability Management

- Readings:
  - Exam Cram Part I Chapters 6 and 7 (stop at "Threat Assessment" section on page 103)
  - CISA Checklist – Section 5 (Vulnerability Management)
  - Flaws in the system" and "Find the flaws" sections within Week 3 of the "Assets, Threats, and Vulnerabilities" course from the Google Cybersecurity Professional Certificate

Wednesday, September 13: Malware

- Optional: National Security Career Fair today, 9am-3:30pm at the Alumni Center
- Readings:
  - Exam Cram Part III Chapter 18
  - GCA Toolkit Steps 4 and 5
  - Likely Malware Indicators Table (Canvas)
  - Steps to Remove Malware Using Anti-Malware Software (Canvas)

- **Assignment 4 (due Thursday, September 21 by 11:59pm CST):** Install antivirus software and an ad blocker on your computer (reminder: the Blueprint for Ransomware Defense Tools and Resources has a robust list of free/open source tools for most basic cybersecurity purposes). Via Canvas Assignment #4:
  - Submit which software tools you selected for these purposes (including if completed prior to this course) and explain why you picked those.
  - Name and define 2 types of DNS attacks prevented by DNS filtering.

- Optional: While you're at it, install a DNS security tool.

Friday, September 15: Free Day – No Class

- **Assignment 5 (due Thursday, September 28 by 11:59pm CST):** Complete Weeks 1 and 2 of the "Connect and Protect: Networks and Network Security" course from the Google Cybersecurity Professional Certificate; submit screenshot(s) showing completion via Canvas Assignment #5.

Week 5

Monday, September 18: Network Security

- Readings:
  - Exam Cram Part I Chapter 4, Part II Chapters 17 and 19
  - (ISC)² - Ports and Protocols Chart (Canvas)

Wednesday, September 20: Wireless, Mobile, and Email Security (VIP Class Visitor)

- Readings:
  - Exam Cram Part III Chapters 20 and 21
  - GCA Toolkit Step 6
  - DMARC, SPF, and DKIM explainer

Friday, September 22: Cloud Security

- Readings:
  - Exam Cram Part II Chapter 10
  - "Cloud Hardening" section within Week 4 of "Connect and Protect: Networks and Network Security" course from the Google Cybersecurity Professional Certificate

Week 6

Monday, September 25: More Cloud Security (Guest Speaker) / Catch Up on Security

- Readings:
  - Exam Cram Part III Chapter 22

- **Assignment 6 (due Thursday, October 5 by 11:59pm CST):** Complete Weeks 2 and 4 of the "Sound the Alarm: Detection and Response" course from the Google Cybersecurity Professional Certificate; submit screenshot(s) showing completion via Canvas Assignment #6.

Wednesday, September 27: Firewalls, IDSs/IPSs

- Readings:
  - Exam Cram Part IV Chapter 29 (page 544 to end)
  - "Network Hardening" section within Week 4 of "Connect and Protect: Networks and Network Security" course from the Google Cybersecurity Professional Certificate
  - "Overview of Detection Tools" reading within Week 1 of "Sound the Alarm: Detection and Response" course from the Google Cybersecurity Professional Certificate

Friday, September 29: SIEM and SOAR

- Readings:
  - Exam Cram Part I Chapter 7 ("Threat Assessment" section beginning on page 103 to end)
  - All of Week 3 and "SIEM technology to identify threats, risks, and vulnerabilities" section within Week 4 of the "Play It Safe: Manage Security Risks" course from the Google Cybersecurity Professional Certificate

Week 7

Monday, October 2: Special Laws and Regulations (Guest Speaker)

- Readings:
  - Exam Cram Part V Chapter 32

Wednesday, October 4: Midterm Review Session / Catch Up

- **Midterm (due Thursday, October 12 by 11:59pm CST):** 75 question multiple choice completed through Canvas—open note and book. Please take it on your own; no collaboration with other students.

Friday, October 6: Receive Team and Client Assignments (Guest Speakers)

Week 8

Monday, October 9: Meet Your Industry Expert Mentors (Guest Speakers)

Wednesday, October 11: Midterm Exam – No Class *(Subject to change to accommodate guest speaker schedules)*

- Optional: CyberForce Virtual Collegiate Career Fair today, 1-4pm online

Friday, October 13: Linux, Packet Sniffers, and Other Tools

- Readings:
  - Exam Cram Part IV Chapter 26

- **Assignment 7 (due Thursday, October 19 by 11:59pm CST):** Complete Weeks 2 and 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 #7.

Week 9

Monday, October 16: More Linux; Review of Cyber Attack Indicators

- Readings:
  - "Securing Linux" section within Week 4 of the "Connect and Protect: Networks and Network Security" course from the Google Cybersecurity Professional Certificate

- **Assignment 8 (due Sunday, October 22 by 11:59pm CST):** From the Google Cybersecurity Professional Certificate:
  - Complete Week 3 of the "Connect and Protect: Networks and Network Security" course
  - Complete the "Attacker Mindset" section within Week 3 and the "Social Engineering," "Malware," and "Web-based exploits" sections within Week 4 of the "Assets, Threats, and Vulnerabilities" course
  - Submit screenshot(s) showing completion via Canvas Assignment #8.

Wednesday, October 18: Penetration Testing

- Readings:
  - Exam Cram Part I Chapter 8

- **Assignment 9 (due Sunday, October 29 by 11:59pm CST):** Complete Pentesting Fundamentals and Metasploit: Introduction modules through TryHackMe; submit screenshot(s) showing completion of both labs via Canvas Assignment #9.

Friday, October 20: Pentesting as a Career (Guest Speaker)

- **Assignment 10 (due Sunday, November 5 by 11:59pm CST):** Complete Linux PrivEsc and Basic Pentesting modules through TryHackMe; submit screenshot(s) showing completion of both labs via Canvas Assignment #10.

Week 10
Monday, October 23: Python for Security

- **Assignment 11 (due Sunday, November 12 by 11:59pm CST):** Complete the "Automate Cybersecurity Tasks with Python" course from the Google Cybersecurity Professional Certificate; submit screenshot(s) showing completion via Canvas Assignment #11.

Wednesday, October 25: Free Day – No Class

Friday, October 27: Types of Controls (Virtual Class via Zoom – Link available on Canvas)
- Readings:
  - Exam Cram Part V Chapter 31

Week 11
Monday, October 30: Organizational Security Policies, Business Plans
- Readings:
  - Exam Cram Part V Chapters 33 and 34
  - "Create and Use Documentation" section within Week 3 of "Sound the Alarm: Detection and Response" course from the Google Cybersecurity Professional Certificate

Wednesday, November 1: Sensitive Data, Labeling, and Privacy Policies (Guest Speaker)
- Readings:
  - Exam Cram Part II Chapter 9; Part V Chapter 35

Friday, November 3: Incident Response (Guest Speakers)
- Readings:
  - Exam Cram Part IV Chapter 27 (Page 511 to end)
  - Remainder of Week 1 of "Sound the Alarm: Detection and Response" course from the Google Cybersecurity Professional Certificate
  - Blueprint for Ransomware Defense Tools and Resources – Respond and Recover Sections

Week 12
Monday, November 6: Incident Investigation and Mitigation (Guest Speakers)
- Readings:
  - Exam Cram Part IV Chapter 28 and Chapter 29 (beginning through page 543)
  - "Response and Recovery" and "Post-incident actions" sections within Week 3 of "Sound the Alarm: Detection and Response" course from the Google Cybersecurity Professional Certificate

Wednesday, November 8: How to Communicate with Business Leaders (Guest Speaker)

- Readings:
  - Why Your Audience Should Care—and Act
  - Recommending Security Tools
  - Minimum Viable Teaching

Friday, November 10: Creating a Cybersecurity Project Plan

Week 13

Monday, November 13: Ballot's Bowwow Box: Key Risks and Basic Mitigations

- Readings: BBB's Business Profile (Canvas)

- **Assignment 12 (due Tuesday, November 28 by 11:59pm CST):** With your group, create a PowerPoint identifying at least 5 moderate and high cybersecurity risks and proposed mitigations for Ballot's Bowwow Box. Quantify the amount of time and cost you estimate for each mitigation, as well as who within your group will be assigned to complete it and who within the company will need to assist with install/configuration/long-term management of the risk. Submit the final copy via Canvas Assignment #13 and prepare to brief to the class and guests. Every group member should submit the same file(s).
  - Note: It will help immensely if you work on this concurrently with the BBB cybersecurity project plan to be completed for Assignment #13.

Wednesday, November 15: Ballot's Bowwow Box: Intermediate Mitigations

Friday, November 17: Ballot's Bowwow Box: Advanced Mitigations and Business Planning

- **Assignment 13 (due Sunday, December 3 by 11:59pm CST):** Finish your group's cybersecurity project plan spreadsheet for Ballot's Bowwow Box and submit the final copy via Canvas Assignment #14. Every group member should submit the same file(s).

Week 14

November 20-25: Fall Break – No Class

Week 15

Monday, November 27: Work Day

Wednesday, November 29: BBB Presentations (Class Visitors)

Friday, December 1: BBB Presentations (Class Visitors)

Week 16

Monday, December 4: Resource and Policies Review; Spring Course Expectations