Applied Cybersecurity Community Clinic
Applied Cybersecurity Foundations Course
I 320 – Spring 2024 – 27435

Contact Info
Professor Francesca Lockhart
francesca.lockhart@austin.utexas.edu
Office: SRH 3.349
Office hours: Monday 12 PM-1:30 PM, Wednesday 3:15-4:45 PM by appointment only

Class Meetings
Monday, Wednesday, Friday from 2-2:50 PM in RLP 0.104

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.

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. Assignments #11 and 12 (the final class project) will each count for 15% of your overall grade (30% total) and be graded out of 100 according to the provided guidelines and rubrics (see Canvas).

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 **15% 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.

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 clinic instructor **before** the assignment due date/time, not after.

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. Access the certificate using this link (and create a Coursera account, should you not already have one): https://coursera.org/programs/the-university-of-te-google-learning-program-a10ys
  - Tryhackme.com – Create a free account to complete assigned labs

- 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

Wednesday, January 17: Syllabus Review and Course Policies

- Readings:
  - Clinic Student Code of Conduct (Canvas) — Signed copy due via Canvas by **11:59pm Sunday, January 21st**

Friday, January 19: Cyber Attacks, Threat Actors, and Methods (Guest Speaker)

- Readings:
  - Exam Cram Part I Chapter 1, Chapter 5, and Part IV Chapter 27 (beginning through page 511)

Week 2

Monday, January 22: The Cyber Threat to Small Organizations (Guest Speaker)

- Readings:
  - Exam Cram Part I Chapters 2 and 3
  - Statescoop Article

- **Assignment 1 (due Sunday, January 28 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 three items for your selected case study. Submit 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:

Wednesday, January 24: Foundational Cyber Policies and Agencies

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

Friday, January 26: Careers in National Security (Guest Speakers)

Week 3

Monday, January 29: Inventory Devices and Applications

- Readings:
  - Exam Cram Part V Chapter 34 (stop at "Single Loss Expectancy" section on page 605)
  - Module 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 Sunday, February 4 by 11:59pm CST):** 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.

- Hint: Utilize Fing or another free network scanning tool if you are *not* on the UT or another enterprise network (in other words, use only on your private home network, if you have one. Uninstall after use to prevent being blocked from the utexas and other enterprise networks).

Wednesday, January 31: Encryption (Guest Speaker)

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

Friday, February 2: Automatic and Secure Updates; Public Key Infrastructure

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

Week 4

Monday, February 5: Passwords / Authentication

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

- **Assignment 3 (due Sunday, February 11 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.

Wednesday, February 7: Passwords / Authorization

- Readings:
  - Exam Cram Part III Chapter 23
  - "Authentication, authorization, and accounting" section within Module 2 of the "Assets, Threats, and Vulnerabilities" course from the Google Cybersecurity Professional Certificate
  - Optional: Exam Cram Part III Chapter 24 (stop at "Authentication Protocols" section on page 457)

Friday, February 9: 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 Module 3 of the "Assets, Threats, and Vulnerabilities" course from the Google Cybersecurity Professional Certificate

Week 5

Monday, February 12: Malware (Guest Speaker)

- Readings:
  - Exam Cram Part III Chapter 18
  - GCA Toolkit Steps 4 and 5

- **Assignment 4 (due Sunday, February 18 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.

Wednesday, February 14: Network Security

- Readings:
    - Exam Cram Part II Chapters 17 and 19 (stop at "Security Devices and Boundaries" section on page 347)
    - Optional: Exam Cram Part I Chapter 4

- **Assignment 5 (due Thursday, February 22 by 11:59pm CST):** Complete Modules 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.

Friday, February 16: Wireless, Mobile, and Email Security

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

Week 6

Monday, February 19: Cloud Threat Intelligence (Guest Speaker)

- Readings:
    - Exam Cram Part II Chapter 10 (start with "Cloud Models" section on page 155 through end) and Part III Chapter 22 (start with "Third-Party Cloud Security Solutions) on page 428 to end)
    - "Cloud Hardening" section within Module 4 of "Connect and Protect: Networks and Network Security" course from the Google Cybersecurity Professional Certificate

Wednesday, February 21: Firewalls, IDSs/IPSs

- Readings:
    - Exam Cram Part II Chapter 19 (page 347 to end)
    - "Network Hardening" section within Module 4 of "Connect and Protect: Networks and Network Security" course from the Google Cybersecurity Professional Certificate
    - "Overview of Detection Tools" reading within Module 1 of "Sound the Alarm: Detection and Response" course from the Google Cybersecurity Professional Certificate

- **Assignment 6 (due Thursday, February 29 by 11:59pm CST):** Complete Module 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.

Friday, February 23: SIEM Tools and SOAR

- Readings:
    - Exam Cram Part IV Chapter 29 (page 544 to end); Part I Chapter 7 ("Threat Assessment" section beginning on page 103 to end)

- All of Module 3 and "SIEM technology to identify threats, risks, and vulnerabilities" section within Module 4 of the "Play It Safe: Manage Security Risks" course from the Google Cybersecurity Professional Certificate

Week 7
Monday, February 26: Midterm Review Session

- **Midterm (due Thursday, March 7 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.
- 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, February 28: Data Privacy (Guest Speaker)
- Readings:
  - "Information privacy: Regulations and compliance" section within Module 2 of the "Assets, Threats, and Vulnerabilities" course from the Google Cybersecurity Professional Certificate
  - UT Austin Internal Cyber Clinic Data Guidance (Canvas)
  - Optional: Exam Cram Part V Chapter 35

Friday, March 1: Governance, Risk, and Compliance (Guest Speaker)
- Readings:
  - Exam Cram Part V Chapter 32

Week 8
Monday, March 4: Meet Industry Expert Mentors (Class Visitors)
- Receive Team Assignments via Canvas
- **Class held in SRH today – Location TBA**

Wednesday, March 6: Midterm Exam – No Class

Friday, March 8: Using and Securing Linux
- Readings:
  - Module 1 of the "Tools of the Trade: Linux and SQL" course
  - "Securing Linux" section within Module 4 of the "Connect and Protect: Networks and Network Security" course from the Google Cybersecurity Professional Certificate
  - Optional: Exam Cram Part IV Chapter 26

- **Assignment 7 (due Thursday, March 21 by 11:59pm CST):** Complete Modules 2 and 3 of the "Tools of the Trade: Linux and SQL" course and Module 2 of the "Sound the Alarm: Detection and Response" course from the Google Cybersecurity Professional Certificate; submit screenshot(s) showing completion via Canvas Assignment #7.

Week 9
March 11-15: Spring Break – No Class

Week 10
Monday, March 18: Python Uses in Cybersecurity

- **Assignment 8 (due Tuesday, March 26 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 #8.

Wednesday, March 20: Review of Cyber Attack Frameworks and Indicators; Penetration Testing Intro (Guest Speaker)

- Readings:
  - Exam Cram Part I Chapter 8

- **Assignment 9 (due Sunday, March 31 by 11:59pm CST):** From the Google Cybersecurity Professional Certificate:
  - Complete Module 3 of the "Connect and Protect: Networks and Network Security" course
  - Complete the "Attacker Mindset" section within Module 3 and the "Social Engineering," "Malware," and "Web-based exploits" sections within Module 4 of the "Assets, Threats, and Vulnerabilities" course
  - Submit screenshot(s) showing completion via Canvas Assignment #9.

Friday, March 22: Pentesting as a Career (Guest Speaker)

- **Assignment 10 (due Sunday, April 7 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 #10.

Week 11

Monday, March 25: Organizational Security Policies, Business Plans

- Readings:
  - Exam Cram Part V Chapter 33
  - "Create and Use Documentation" section within Module 3 of "Sound the Alarm: Detection and Response" course from the Google Cybersecurity Professional Certificate

Wednesday, March 27: Incident Response (Guest Speaker)

- Readings:
  - Exam Cram Part IV Chapter 27 (Page 511 to end)
  - Remainder of Module 1 of "Sound the Alarm: Detection and Response" course from the Google Cybersecurity Professional Certificate

Friday, March 29: Incident Forensics and Recovery (Guest Speaker)

- Readings:
  - Exam Cram Part IV Chapter 29 (beginning through page 543)
  - "Response and Recovery" and "Post-incident actions" sections within Module 3 of "Sound the Alarm: Detection and Response" course from the Google Cybersecurity Professional Certificate
  - Optional: Exam Cram Part IV Chapter 28

Week 12

Monday, April 1: Categorizing Controls

- Readings:
  - Exam Cram Part V Chapter 31

Wednesday, April 3: How to Communicate with Organizational Leaders (Guest Speaker)

- Readings:
  - Why Your Audience Should Care—and Act
  - How To Teach Adults
  - Recommending Security Tools

Friday, April 5: Creating a Cybersecurity Project Plan (Class to be held on Zoom – Link on Canvas)

- Readings:
  - BBB's Business Profile (Canvas)
  - BBB Project Plan and Presentation Rubric (Canvas)

- **Assignment 11 (due Tuesday, April 23 by 11:59pm CST):** With your group, create a PowerPoint identifying at least 5 critical and high cybersecurity risks and proposed controls/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. Only one team member needs to submit on behalf of your team via Canvas Assignment #11.

- **Assignment 12 (due Sunday, April 28 by 11:59pm CST):** Finish your group's project plan spreadsheet and written report for improving the cybersecurity of Ballot's Bowwow Box. Only one team member needs to submit both files on behalf of your team via Canvas Assignment #12.

Week 13
Monday, April 8: No class – Enjoy the eclipse!

Wednesday, April 10: Ballot's Bowwow Box: Asset Inventory, Risk Matrix

Friday, April 12: Ballot's Bowwow Box: Control for Critical Risks

Week 14
Monday, April 15: Ballot's Bowwow Box: Control for High Risks

Wednesday, April 17: Ballot's Bowwow Box: Control for Moderate Risks

Friday, April 19: Ballot's Bowwow Box: Business Planning and Reporting

Week 15
Monday, April 22: BBB Presentation Work Day

Wednesday, April 24: BBB Presentations (Class Visitors: Industry Experts)

- **Class held in SRH today – Location TBA**

Friday, April 26: BBB Presentations (Class Visitors: Industry Experts)

- **Class held in SRH today – Location TBA**

Week 16
Monday, April 29: Resource and Policies Review; Fall Course Expectations