Applied Cybersecurity Community Clinic
Course 1: Applied Cybersecurity Foundations
I 320 - Fall 2023

Contact Info
Francesca Lockhart
francesca.lockhart@austin.utexas.edu
Office: JON 6.264 (Spring 2023) – subject to change

Class Meetings
Monday, Wednesday, Friday from 1-2 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 or nonprofit to render pro bono cybersecurity services (semester 2). 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, penetration testing. Students will also understand how to form an effective cybersecurity team and communicate with organization and business leaders and employees about cybersecurity controls and functions.

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
- Understand how to communicate risks and mitigations 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 or nonprofit in the Austin, Texas area during the second semester clinic course

Course Sequence, Readings, and Assignments

Week 1: Introduction and Overview of Cyber Threats
A. Syllabus review and course expectations / policies
B. Review typical cybersecurity organization structures
C. Review key cyber threat actors and the threat to small businesses / nonprofits

Week 2: How to Conduct a Current State Inventory and Analysis
A. Review cybersecurity basic terms and lexicon
B. Examine the steps and tools to inventory devices and applications within an organization
C. Learn to implement automatic updates and device/data encryption as you inventory

Week 3: Account and Device Security - Passwords
A. Review what makes a strong password and password manager
B. Understand types of cryptography and encryption standards
C. Examine relevant steps and tools to strengthen authentication protocols and deprovisioning processes at a small business
D. Learn to implement 2FA, minimum password length, and password manager across an organization

**Week 4: Prevent Phishing and Malware, Mitigate Known Vulnerabilities**
A. Examine relevant steps and tools to defend against ransomware, viruses, phishing attempts, and other malware and find holes in current security configuration
B. Learn to configure antivirus software, DNS filtering, ad blockers, within an organization
C. Scan for known vulnerabilities, system configuration gaps and ensure patches or mitigation steps complete
D. Implement automatic system backups

**Week 5: Network / Cloud Security and Access Management**
A. Review access control types and when/how to implement authorization controls for an organization’s data
B. Learn to centrally manage security on existing cloud services (email services, data storage, productivity software, and/or website hosting services),
C. Implement DMARC
D. Learn how to ensure HTTPS and other secure ports and protocols are used by default after conducting network analysis

**Week 6: Firewalls**
A. Review host-based and network-based firewalls and placement
B. Understand NAT and PAT devices and placement on network
C. Conceptualize packet filtration / stateful packet inspection

**Week 7: Intrusion Detection and Prevention Systems and SIEMs**
A. Review differences between IDSs, IPSs, and SIEMs and explore free providers
B. Define security logging and log storage best practices
C. Practice log analysis

**Week 8: Midterm Exam (Canvas); Receive Service Semester Team Assignments**

**Week 9: Cyber Attack Types**
A. Review common cyber attack vectors and attack types
B. Map attacks onto defenses and mitigations covered in Weeks 1-7 of the course

**Week 10: Linux Operating System**
A. Review basic commands in Linux and uses of Kali Linux for cybersecurity operations
B. Use Linux commands to review and manage authorization
C. Use Linux commands to review logs

**Week 11: Penetration Testing**
A. Learn how to use the Metasploit CLI and the Armitage GUI to conduct basic penetration testing

**Week 12: Python for Security**
A. Use Python to automate security tasks, including using pre-built and new functions
B. Practice opening, reading, and parsing files

**Week 13: Incident Response and Continuity Planning**
A. Learn incident analysis tools and techniques for eradication and recovery
B. Differentiate between incident response plans, business continuity plans, and disaster recovery plans and who is responsible for creating and implementing each within an organization
Week 14: Implementing a Cybersecurity Improvement Project Plan

A. Review the security baseline of a fictional small business and synthesize a cybersecurity improvement project plan
B. Use CISA and CIS checklists to describe sequential steps you and your team will take and tools you will use to implement your cybersecurity solution
C. Recall and review key cybersecurity resources for their future organization partners, including reporting resources and requirements for applicable businesses
D. Review free / miscellaneous cyber tools they may use in their service semester