Active Learning for Introductory Cybersecurity

Jeffrey J. Yackley
Division of Computer Science
University of Michigan-Flint
Flint, Michigan, USA
jyackley@umich.edu

***Abstract*—This innovative practice full paper describes the author's efforts to create an introductory course for cybersecurity using a flipped classroom model with active learning. The University of Michigan-Flint recently opened a new, four-year, undergraduate cybersecurity program. As part of this new program, the author was tasked with developing the first course of the program without requiring any pre-requisite knowledge to facilitate first- and second-year students to enter the program regardless of their academic background. Further, a requirement was added to all of the author's institution's undergraduate computing majors to require this course as part of their programs. This course is designed to introduce students to the field of cybersecurity and the foundational principles of security and networking needed for future courses. The author describes their iterative experience in designing this face-to-face course moving from more traditional lecture practices to using the flipped classroom model and active learning techniques. The use of the flipped classroom model, active learning, and collaborative learning were spurred by several motivations. The first motivation was that students have a strong preference for less lectures and more hands-on practical and collaborative experiences as indicated in the first asynchronous offering of the course before the face-to-face version was designed. The second motivation was the expressed desire to start developing students' soft skills to help them be able to pursue internships and co-operative education opportunities in alignment with the College of Innovation & Technology's new polytechnic focus. Students were surveyed to measure their thoughts on the course design and their engagement with the material of the course. The course is assessed using these surveys in addition to the instructor evaluation surveys and student assessment data from the in-person offerings of the course in Winter 2023, Fall 2023, and Winter 2024. The initial assessment data indicates greater student achievement and satisfaction with the active learning version of the course most recently offered in Fall 2023 and Winter 2024 in comparison to the more traditional approach used in Winter 2023.**

***Index Terms*—Cybersecurity, Active Learning, Flipped Classroom, Collaborative Learning**

I. Introduction

Currently, there exists a significant cybersecurity skills gap with both a deficit of cybersecurity graduates for available jobs and with graduates being poorly prepared for cybersecurity roles in industry [1]–[3]. It has long been acknowledge that one difficulty is the high pre-requisite knowledge (e.g., programming languages, operating systems, computer networking, etc.) for cybersecurity courses leading to them being treated as upper-level courses offered near the end of a traditional computer science student's program [4]. This led to the development of standards for cybersecurity curriculum which encouraged teaching the necessary pre-requisite knowledge alongside the cybersecurity content to facilitate first- and second-year students to enter the program regardless of their academic background [5].

In Fall 2022, the College of Innovation & Technology (CIT) at the University of Michigan-Flint (UM-Flint) started a new four-year cybersecurity undergraduate program [6]. This program was designed to meet the United States of America's Cybersecurity and Infrastructure Security Agency (CISA) National Initiative for Cybersecurity Education (NICE) framework [7]. A similar published curriculum can be seem from Palo Alto Networks [8]. The author was assigned to create the first course in the new program, Cybersecurity 101 (CYB 101): Security Fundamentals I. This course is the first in a two-course introductory sequence and is required for all computing majors (Computer Science, Cybersecurity, Computer Information Systems, Data Science, Information Technology & Informatics, and Software Engineering) in CIT. However, when designing the new course the author found limited information on available tools, environments, and activities that were updated to work with the new collegiate curriculum guidelines and easy enough to learn for students with no prior background knowledge. Additionally, the need for an accessible lab environment that would be available for students using their own computers without complicated set-up and extensive support was a major obstacle.

The iterative course design process began in the early fall for the first offering of CYB 101 which would run during the second-half of the Fall Semester 2022. This course was piloted in an asynchronous, online-only, accelerated program at UM-Flint whose student population would be significantly different than for the standard version of the course. These students would be pursing a bachelor's of interdisciplinary studies and were not interested in detailed technical content as non-computing majors. The first version of the in-person CYB 101 course designed for all computing majors ran during the Winter 2023 Semester. Due to the heavy revisions from the asynchronous version of the course, the author decided to start with a traditional, lecture-based course using the SEED lab modules [9]. Student comments and experiences would later result in the author revising the course using the flipped classroom model [10] to allow for the introduction of collaborative learning activities during class time and the switch to a newer, more content-rich and diverse, online cybersecurity lab environment called TryHackMe (THM) [11].

This active learning version of the course was first run during the Fall 2023 Semester. After a minor revision and due to the popularity of the new cybersecurity program, it ran again during the Winter 2024 Semester.

The background and related work is discussed further in Section II. Then, the author's approach to designing an introductory undergraduate course in cybersecurity for first- and second-year computing majors is described in Section III. The evaluation of the course through student surveys, course evaluations, and student performance data is shown in Section IV. Lastly, the author concludes with a discussion of the limitations of the work and proposes future work in Section V.

II. Background & Related Work

Traditional course design at the collegiate level often relies upon the lecture model where an instructor explains a topic to students with or without visual aides. Yet, students frequently struggle with this model and fail to truly master the covered material [12]. Freeman et al. [13] have found through a meta-analysis that active learning increases student performance in science, engineering, and mathematics over the use of traditional lecturing.

Active learning is defined by Prince [14] "as any instructional method that engages students in the learning process". Prince [14] further explains some of the common forms of active learning such as: collaborative learning where "students work in small groups toward a common goal" with "emphasis on student interactions", cooperative learning where "students pursue common goals while being assessed individually", and problem-based learning which is where "relevant problems are introduced [...] and used to provide context and motivation for the learning that follows". Ultimately, Prince [14] determines that the core of active learning is to introduce activities into lecture and promote student engagement.

The flipped classroom model [10] is used to enable active learning in the classroom by moving the process of content delivery outside the classroom thereby freeing class time for activities that provide hands-on, experiential learning to reinforce the material and provide opportunities for students to analyze and synthesize lessons [15]. Roehl et al. [16] suggest that the flipped classroom models leads to greater teacher to student mentoring and peer-to-peer collaboration driving student engagement in a course.

Mouheb et al. [5] survey various approaches to curriculum design for cybersecurity which include active learning techniques. Redman et al. [17] discuss a general introductory cybersecurity course using newly designed lab exercises on virtual machines for all university undergraduates. However, Redman et al.'s [17] generalized course does not address the technical skill gap or needs of cybersecurity, IT, and computer science specialists. Similarly, Arora [18] teaches cybersecurity to non-computing major students using the Hydra Minerva environment for incident management simulations. Greenlaw et al. [19] introduce a set of three lab exercises designed for all first-year undergraduates at the U.S. Naval Academy using virtual machines. Moore and Cappos [20] use magic tricks with playing cards to simulate and describe several cybersecurity attacks at the introductory-level. Conklin [21] uses a cyber defense competition to provide active learning in a capstone course for information security. Srivatanakul and Annansingh [22] use think-pair-share, buzz group, and roleplay activities in the design for an undergraduate software and web security course. Buriachok and Sokolov [23] implement active learning through lab exercises and research projects in a number of different master's level graduate courses in Ukraine.

Ultimately, while there have been many different proposed lab environments and techniques there has not been a course design description that is able to be 1) offered specifically for computer science, IT, and cybersecurity students at the introductory-level with technical rigor, 2) uses a virtual lab environment with minimal set-up and maintenance to work on modern systems accessible at any time by students to practice hands-on skills, and 3) also offers a variety of activities to keep students interested, help them practice soft skills, and most importantly engaged in applying, analyzing, and evaluating the course material according to Bloom's taxonomy of learning [24].

III. Course Structure

Cybersecurity 101: Security Fundamentals I is an introductory cybersecurity course with the purpose to introduce students to the fundamentals of cybersecurity, computer networking, and the Linux operating system. The course is offered as a four-credit in-person course which meets twice a week for one hour and forty minutes each session. It is organized by week and topic as shown in Table I. This version of the course was designed as a required course for all students enrolling in the author's institution's new undergraduate program in Cybersecurity as well as a required course for students in all of our other four-year computing programs (Computer Science, Computer Information Systems, Data Science, Information Technology & Informatics, and Software Engineering).

This course uses a flipped classroom model [10] where students are required to watch a lecture video and optionally read the course textbook [25] on the topic of the day before coming to class. In class, the students complete a hands-on activity related to the material they watched in the video and work through the THM Lab Modules [11]. These activities take many forms such as Linux command practice exercises, case studies, roleplays, boardgames, and more with each activity being designed to reinforce important topics with hands-on, collaborative learning. Students work with each other in small groups (2-4 members depending on the activity). Short quizzes are given every 2-3 weeks in the course to attempt to encourage students to keep up with the course material and check their understanding of material in the course. The class prior to each quiz students are given a Kahoot [26] review to help them prepare. For the midterm of the course, students are given a list of infamous malware, malicious software, such as worms (e.g., Morris Worm [27]), viruses (e.g., Creeper [28]),

trojans (e.g., Zeus [29]), ransomware (e.g., WannaCry [30]), and more. Students form teams of two and work together to write a report covering the malware which they present to the class around the middle point of the term. Students are expected to write peer evaluations for their classmates and complete a short self assessment reflection. There is also a final cumulative exam on all material covered in the course. Additionally, at some point in the semester an industry guest speaker related to IT and Cybersecurity is invited to present to the class about their work and company. Students must write a reflection on the guest speaker as a short report.

Students are graded based on their completion of the in-class activities (10%), THM labs (20%), 4 quizzes (20%), midterm project (20%), guest speaker report (5%), and final exam (25%).

A. Course Evolution

The asynchronous, online version of the course was the first version of CYB 101. However, it was designed for non-computing majors and was required to follow a pure, asynchronous, online format. This resulted in the development of video lectures based largely on the content from the selected course texts [4], [31]. In this version of the course, students complete modules in the Canvas learning management system (LMS) [32]. Each topic has a lecture video and associated homework. There are no activities to complete as the requirements for this accelerated, online program preclude student group work and synchronous meetings. Students work at their own pace, but are able to reach out to the instructor for help as needed. The selected SEED lab environment [9] was chosen to challenge students and focus on specific vulnerabilities tied to the lecture content. The SEED labs are easily accessible online with detailed instructions. However, they require students to be bootstrapped on various programming languages if they do not have this background already and they are computing resource intensive. Further, they require a lot of instructor support for configuration of the virtual machine environment which has to either be hosted by the instructor on a local server or be run on a virtual machine on each individual student's computer. This resulted in problems when the required virtual machine software did not support recent updates to MacOS and Windows 11 resulting in many issues with student machines particularly in an asynchronous environment. Due to the near complete overhaul in the course due to feedback from students, instructor experiences, and strict course format requirements the design for the in-person version of the course uses little from the asynchronous version. The course is so significantly different that it will not be used as a comparison in the evaluation performed in section IV.

The in-person version of the course was originally designed as a more traditional, lecture-based course where the instructor would present the material to the class for the majority of the class time and activities would be given as homework assignments to be completed outside of the assigned class time. The class was offered with this design during the Winter 2023 Semester (W23-TL for traditional lectures). Based on feedback received from students as well as their performance in the course, the instructor reworked the course based on similar computer science courses that had experienced success transitioning from a lecture-based format to a flipped-classroom format with active learning occurring through in-class activities [33]–[35]. The first class where the newly designed activities were used was during the Fall Semester 2023 (F23-FC for flipped classroom). The activities were further refined based on feedback received and used in the most recent offering of the course during the Winter 2024 Semester (W24-FC).

B. In-class Activities

The in-class activities are largely based on or draw inspiration from exercises in the course textbooks [25] and [36]. They generally start with a short presentation by the instructor in order to motivate the activity, provide a quick review of necessary background knowledge, and explain the instructions for an activity. This preliminary presentation generally takes between 15-20 minutes. The rest of the class time is then given over to students completing the activity and reporting back out their experiences or findings to the entire class which is followed by class discussion and reflection. Remaining class time (if any) is used to facilitate in-class pair-work on the THM labs which is motivated by the pair programming concept [37] from software development practices. Activities were designed and refined using the ADDIE model [38]. A complete list of activities can be found in Table I and a description of the activities can be found in the online appendix supplement [39].

One example of an activity that was widely popular with students was the Transmission Control Protocol (TCP) Board Game activity during Week 8. This activity, is used to review how one of the key Transport Layer protocols, TCP [40], functions by requiring students to set-up a connection, and reliably transmit a set number of packets before closing their connection to win the game. Students use a player sheet, Fig. 1, to track their connection and data packet transmission as well as acknowledgement (ACK) packets while running in to common network problems such as network congestion, corrupted packets, and buffer overflow chance cards that result in them losing progress towards their goal of fully transmitting their data. Students therefore review TCP from the establishment of a connection with the three-way handshake, to properly assigning sequence and ACK packet numbers, to handling errors, and finally how to formally close the connection. To play the game, players roll a six-sided die (D6) in order to travel on the playing board, Fig. 2. The color of the square determines if the player gets to transmit or receive a packet (blue squares), an error occurs through a chance card (yellow squares), or if nothing but the current time-to-live counter for their current packet in transmission is incremented (white squares) which also happens on blue and yellow squares.

Another activity that draws a lot of interest and favorable comments from students earlier in the class is the Am I Compromised activity. In this activity, students have previously been introduced to personal security topics

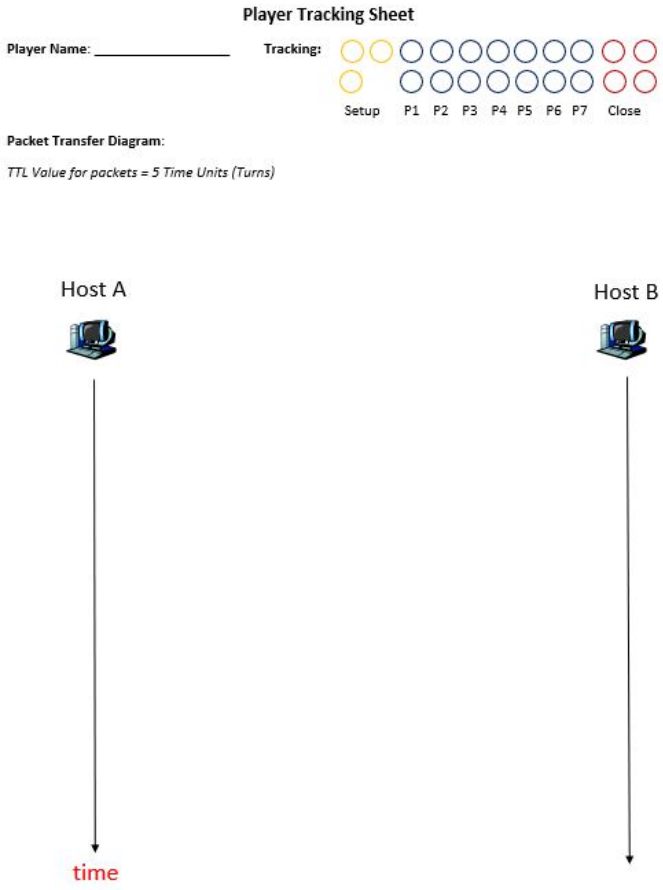

Fig. 1. TCP Game - Player Card.

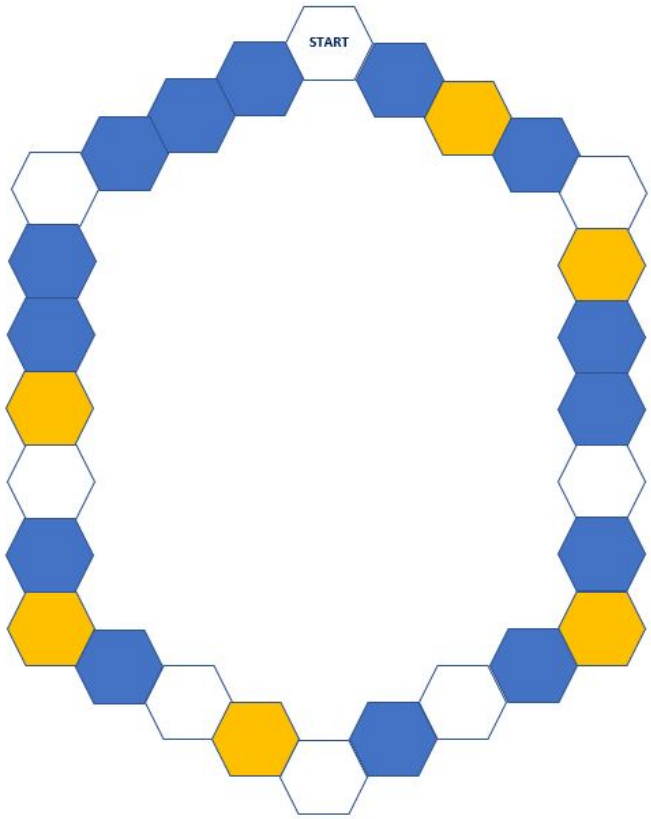

Fig. 2. TCP Game - Game Board.

such as password security, social engineering attacks, and how to create a defensive security posture and are now asked to analyze their own vulnerabilities. Students visit https://haveibeenpwned.com/ [41] and enter one or more of their email addresses with the recommendation to use at least their official university email address. Students are often surprised by the number of data breeches they could be affected by because they gave their personal information out to a game application on a social media site. Students are encouraged to discuss how they are similar and different to their group members before they report out their findings to the class. The class then examines the commonalities between groups to discover larger patterns with the guidance of the instructor to hit home the vulnerabilities and strategies malicious users use to accomplish their attacks.

C. TryHackMe Labs

Several different labs and lab environments were considered for use in the course. The top three were the SEED Labs [9], [31], U.S. Cyber Range [42], and TryHackMe (THM) [11]. It was important that the labs be accessible by students which generated the first challenge since sandbox environments are essential when exploring cybersecurity topics both to protect the students and university systems from accidental malware infection and accidental or malicious exploitation of resources. However, many students can not afford top of the line computers capable of devoting 8-16+ GB of RAM to sandbox virtual machines on top of the RAM required for running their actual operating system. Further, there are know installation problems between Apple and PC computers and conflicts with both newer and older versions of the required VM for the SEED labs. Additionally, lack of IT support for non-university vendor VM solutions meant that the instructor would need to be solely responsible for setting up and configuring any kind of server for the students to connect to which further limited lab environment selection. The SEED Labs would have resulted in too much of a burden on both students and instructor to support without a dedicated team of support staff as discussed in Section III-A. TryHackMe [11] offered a web-based solution, that didn't require any advanced hardware requirements, and still allowed students to gain hands-on practical experience with popular cybersecurity and networking tools and techniques. The U.S. Cyber Range [42] seemed to offer the same potential benefits of THM, but also some of the drawbacks of the SEED labs requiring custom configuration of virtual environments. THM was ready out of the box for instructors to select modules and assign them to students without any configuration.

While THM offers a free-tier of access, it was determined that this would be insufficient for a class as the free-tier

only allows students to have one hour of access per day to their attack box which is a virtual machine that is hosted on THM's servers. Therefore, student lab fees for the course were used to provide VIP-tier access that allows students unlimited access to their attack box as well as access to any module, or learning room, on their site. THM offers a wide selection of rooms, some of which were pre-grouped in to learning pathways such as Red Teaming or Pre-Security that makes module selection for a course quick and easy. Additionally, instructors can be given access to a management dashboard where they can assign specific rooms for completion by the students in their course and can track their students' progress towards completion. As a student completes the tasks in a room, they earn points which are marked completed in the student's module if they are correct. This auto-grading feature was a nice addition to the other features allowing students to learn and progress without need to wait for an instructor to check the answers. A current weakness is that while one can see a student's progress it is still not possible to determine where a student is stuck or struggling unless the student reaches out first and clarifies these points. Additionally, there is not current support for connection to learning management systems which means instructors need to perform additional work to get the scores from THM and then manually input them in to their students' LMS. This was a point of frustration for students as they want to see they get credit as soon as they complete the assigned THM module.

The chosen THM modules in this course were selected based on the course topics from the syllabus as seen in Table I. After some trial and error, around five to six modules seems to be the best number of module assigned per week for the course based on the credit hours of the course and students' other responsibilities in the course such as class time, watching lecture videos, reading, project work, and reviewing for quizzes. Additionally, several modules were chosen to challenge students given that the instructor would be in-class to assist and guide students through particularly challenging sections in the John the Ripper, Phising Analysis, Wireshark, and Nmap lab rooms.

IV. Evaluation

In order to assess the changes to the course, the author devised three research questions:

- RQ1: *(Student Performance)* Did introduction of in-class activities affect student performance in the course?
- RQ2: *(Student Perception)* How do students perceive their engagement in the course?
- RQ3: *(Student Preference)* Which approach (traditional lecture vs. active learning) do students prefer?

A. RQ1: Student Performance

For the first research question, the author compared the number of late and missing assignments as well as the average overall grade for students as collected by the Canvas LMS in each of the three offerings of the course (W23-TL, F23-FC, and W24-FC) as seen in Table II.

In Table II, students in the flipped classroom versions of the course using active learning activities had higher overall grades (84.5% and 87.1%) than students in the traditional lecture version of the course (71.1%). Student t-tests revealed that there was a significant difference at the 95% confidence level between the FC versions of the course and the traditional lecture versions: F23-FC vs. W23-TL (p-value = 0.0022) and W24-FC vs. W23-TL (p-value = 0.0010). We also observed from Table II, that the average number of late (0.2 and 0.0 vs. 0.9) and missing assignments (3.0 and 1.6 vs. 3.6) was lower for the flipped classroom versions of the course than the traditional lecture version. The difference between courses was statistically significant at the 95% confidence level for the number of late assignments for F23-FC vs. W23-TL (p-value = 0.0148) and W24-FC vs. W23-TL (p-value = 0.0184), and the number of missing assignments for W24-FC vs. W23-TL (p-value = 0.0202). However, the difference between F23-FC vs. W23-TL (p-value = 0.5804) for the average number of missing assignments per student was not statistically different at the 95% confidence level.

Overall students performed better in the FC versions of the course than the in the traditional lecture version of the course. The author attributes this difference in performance to the switch to using class time for activities giving students more time and support with the material rather than only a lecture.

B. RQ2: Student Perception

Students were surveyed in the final weeks of the semester in F23 and W24 in order to gather the students' perceptions on their own levels of engagement in the course as it related to the in-class activities and THM labs. Unfortunately, students were not surveyed in W23 so it is not possible to compare student perceptions between the traditional lecture and flipped classroom with these surveys. The need to change was motivated by student comments from W23-TL. The data from the surveys for F23-FC and W24-FC is presented in Table III. Students were asked to complete an online form to gather their responses to the seven questions with students indicating their agreement with the survey statement on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree). The count for the number of responses is shown in each column with the rounded percent of responses shown in parenthesis next to the count for each course (F23-FC and W24-TC). The author performed a statistical analysis of the responses using the Mann-Whitney U Test. There is no statistical difference at the 95% confidence level between the responses.

From Table III, we can see that the majority of students in each course were in agreement that the course let them apply what they learned (66% and 79%), that the course is an example of active learning (81% and 88%), and that they were actively engaged in their learning (81% and 79%). Students also agreed that they were able to apply the course material to the real world (69% and 75%). Students also disagreed in the W24-FC version that the in-class activities would be as useful if they completed them on their own as

TABLE I
WEEKLY TOPICS, ACTIVITIES, AND LAB MODULES FOR CYB 101

Week	Topic	Activities & Assignments	THM Lab Modules
1	Course Introduction Cybersecurity Fundamentals	Icebreaker Exploring Data Breaches Evaluating Info Sources	Tutorial Intro to Offensive Security Intro to Defensive Security Careers in Cyber Security Awareness Security Operations
2	Linux Fundamentals	Linux Command Demo Linux Command Practice Review 1	Principles of Security Linux Fundamentals 1 Linux Fundamentals 2 Linux Fundamentals 3
3	Personal Security	Am I Compromised Quiz 1	Common Attacks Identity & Access Mgmt. Password Attacks Hashing - Crypto 101 Encryption - Crypto 101 John the Ripper
4	Computer Security	Ransomware Case Study Ransomware Resources Review 2	History of Malware Intro to Malware Analysis Cyber Scotland 2021 Phishing Analysis Phishing Emails in Action
5	Network Fundamentals Internet Basics	Quiz 2 Investigating OSI Model	What is Networking? Intro to LAN OSI Model Packets & Frames Extending Your Network
6	Malware Presentations	Malware Report Malware Presentation Malware Peer Review Malware Self Assessment	DNS in Detail HTTP in Detail How Websites Work Putting It All Together
7	Application Layer	HTTP Roleplay DNS Roleplay	Introductory Networking Wireshark 101 Wireshark: The Basics Wireshark: Packet Ops. Wireshark: Traffic Anlys.
8	Transport Layer	TCP Board Game Review 3	Passive Reconnaissance Active Reconnaissance Nmap Live Host Discovery Nmap Basic Port Scans Nmap Adv. Port Scans
9	Network Layer	Quiz 3 Forwarding Tables	Nmap Post Port Scans Protocols & Servers Protocols & Servers 2 Net Sec. Challenge
10	Link Layer Physical Layer	MAC Protocols	Jr. Security Analyst Intro Pyramid of Pain Cyber Kill Chain Unified Kill Chain Diamond Model MITRE
11	Internet Security	Web Browser Security XSS Game Review 4	Web Application Security Governance & Regulation Threat Modelling Risk Management Security Engineer Intro
12	Privacy	Quiz 4 Privacy Case Study THM Lab & Activity Survey	
13	Guest Speaker Course Review	Final Exam Review Guest Speaker Report	
14	Final Exam	Final Exam	

TABLE II
CANVAS DATA FOR EACH OFFERING OF CYB 101

	W23-TL (N=29)	F23-FC (N=35)	W24-FC (N=24)
Average Overall Course Grade	71.1%	84.5%	87.1%
Average Number of Late Assignments Per Student	0.9	0.2	0.0
Average Number of Missing Assignments Per Student	3.6	3.0	1.6

opposed to collaboratively in-groups (54% disagreement vs. 21% agreement with 23% neutral). Students in the F23-FC version were more split on the benefits of completing the activities on their own (34% disagreement vs. 47% agreement with 19% neutral). Similarly students in the W24-FC course agreed (58% vs. 12% disagreement with 29% neutral) that they preferred the in-class activities to lecture only content. Again students were more split in F23-FC (41% agreement vs. 28% disagreement with 31% neutral). The author takes this as a positive indication of the improvement of the activities to foster collaborative learning between students. Lastly, students in both courses were in large agreement that the course made them excited about cybersecurity (79% and 88%) which is an encouraging sign for an introductory course and potential student retention.

C. RQ3: Student Preference

Students at UM-Flint are asked to complete course evaluations for the instructor and the course at the end of each semester. The questions are standardized at the university level. Students are asked their agreement with statements and rate their agreement on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree). The data from the course evaluations is presented in Table IV. The count for the number of responses is shown in each column with the rounded percent of responses shown in parenthesis next to the count for each course (W23-TL, F23-FC, and W24-TC). The author performed a statistical analysis of the responses using the Mann-Whitney U Test comparing the traditional lecture version of the course to the flipped classroom versions of the course: W23-TL vs. F23-FC and W23-TL vs. W24-FC. There is one statistical difference at the 95% confidence level (p-value = 0.02227) for W23-TL vs. W24-FC for the statement indicating a student's interest in the subject has increased. All other statements for both comparisons showed no statistical difference at the 95% confidence level.

From Table IV, although not statistically different we can see students generally responded with more agreement in the flipped classroom versions of the course to the statements than the students in the traditional lecture version of the course. Overall students consider CYB 101 an excellent course (63% W23-TL, 92% F23-FC, and 93% W24-FC) which advanced their understanding of the subject (88% W23-TL, 100% F23-FC, and 100% W24-FC). Further, they agreed that their interest in cybersecurity had increased (63% W23-TL, 92% F23-FC, and 100% W24-FC). Students felt the course was well organized (76% W23-TL, 92% F23-FC, and 92% W24-FC). Students found the hands-on learning was valuable for their future (88% F23-TL, 79% W23-FC, and 93% W24-FC). The guest speaker was also seen as a valuable component of the course (100% W23-TL, 88% F23-FC, and 94% W24-FC). Lastly, students reported that the course helped them to improve their ability to work in teams (63% F23-TL, 80% W23-FC, and 93% W24-FC). Ultimately, it is an encouraging sign that students found value in the course regardless of version, but seem to be finding some increased value from the flipped classroom offering particularly as it improved semester to semester.

V. CONCLUSION & FUTURE WORK

Students have responded very positively to the changes in course design with the flipped classroom model. Particularly encouraging is that student success metrics have improved dramatically as seen in Table II. Students are missing far fewer assignments, turning in fewer assignments late, and the course average grade has improved up to 1 and 2/3 of a letter grade. It is demonstrated how students were able to get hands-on practice through a new, online lab environment that solved the problem of providing technical rigor with enough options to cover the course content as well as being easily accessible by students without complicated installation or setup for each lab. Further, student satisfaction and enthusiasm for active learning in cybersecurity at the introductory-level is shown, helping them to begin to acquire hands-on and soft skills from the moment they enter UM-Flint's computing programs.

The limitations of this study are that the author only attempted to design a course for in-person students and that the flipped classroom model and activities may not be appropriate for online synchronous or asynchronous course offerings. Additionally, this course was designed with maximum student course enrollment between 25-40 students and may also face challenges in being scaled up for larger course sizes. Further, the assessment was limited by student completion of the course evaluations and small population sizes potentially limiting the generalizability of the findings. Lastly, it was not possible to evaluate every possible software tool or environment for use in the course and the considered selection was therefore limited to the largest and most current lab environments available that met the criteria discussed in Section II and III.

The author's plan is to continue refining the collaborative learning activities for future course offerings. One such improvement is the ability to offer the TCP game digitally to facilitate playing the game without the need for pen, paper, and physical playing pieces. The author also hopes to explore the use of a large language model (LLM) learning assistant to offer real-time tutoring. Additionally, the author plans to investigate how to offer this course in a fully-online capacity for non-computing majors while maintaining the active learning components. Lastly, the author hopes to follow the students throughout their time at UM-Flint and investigate the success of the program's first cohort.

TABLE III
STUDENT PERCEPTIONS OF CYB 101 COURSE[a]

Survey Statement	SD	D	N	A	SA	Course
1. Course assignments let me apply what I learned	0 0	2(6%) 3(13%)	9(28%) 2(8%)	12(38%) 12(50%)	9(28%) 7(29%)	F23-FC W24-FC
2. Course is an example of active learning	0 0	1(3%) 0	2(6%) 3(13%)	14(44%) 9(38%)	15(47%) 12(50%)	F23-FC W24-FC
3. I was actively engaged in my learning	0 0	2(6%) 1(4%)	4(13%) 4(17%)	9(28%) 11(46%)	17(53%) 8(33%)	F23-FC W24-FC
4. I applied course material to real world situations	0 0	1(3%) 2(8%)	9(28%) 4(17%)	17(53%) 13(54%)	5(16%) 5(21%)	F23-FC W24-FC
5. Completing course assignments would be just as beneficial on my own as with a group	1(3%) 1(4%)	10(31%) 12(50%)	6(19%) 6(23%)	10(31%) 3(13%)	5(16%) 2(8%)	F23-FC W24-FC
6. I prefer use of activities and discussion to lecture only content	3(9%) 1(4%)	6(19%) 2(8%)	10(31%) 7(29%)	9(28%) 7(29%)	4(13%) 7(29%)	F23-FC W24-FC
7. Course made me excited about cybersecurity	0 0	2(6%) 2(8%)	5(16%) 1(4%)	12(38%) 11(46%)	13(41%) 10(42%)	F23-FC W24-FC

[a]F23-FC N = 32/35, W24-FC N = 24/24

TABLE IV
CYB 101 SELECTED COURSE ASSESSMENT QUESTIONS[a]

Assessment Statement	SD	D	N	A	SA	Course
1. Overall, this was an excellent course	0 1(4%) 0	2(25%) 0 1(7%)	1(13%) 1(4%) 0	2(25%) 9(38%) 6(40%)	3(38%) 13(54%) 8(53%)	W23-TL F23-FC W24-FC
2. This course advanced my understanding of the subject	0 0 0	0 0 0	1(13%) 0 0	5(63%) 10(42%) 7(47%)	2(25%) 14(58%) 8(53%)	W23-TL F23-FC W24-FC
3. My interest in subject has increased due to this course	0 1(4%) 0	2(25%) 1(4%) 0	1(13%) 0 0	3(38%) 9(38%) 5(33%)	2(25%) 13(54%) 10(67%)	W23-TL F23-FC W24-FC
4. The course as a whole was well organized[b]	1(13%) 0 0	1(13%) 1(4%) 0	0 1(4%) 1(7%)	3(38%) 7(29%) 3(21%)	3(38%) 15(63%) 10(71%)	W23-TL F23-FC W24-FC
5. Hands-on learning in course is valuable for my future studies and work[b]	0 0 0	0 2(8%) 0	1(13%) 2(8%) 1(7%)	5(63%) 7(29%) 5(36%)	2(25%) 12(50%) 8(57%)	W23-TL F23-FC W24-FC
6. Guest speakers added a valuable component to course	0 0 0	0 1(4%) 1(7%)	0 2(8%) 0	4(50%) 9(38%) 4(27%)	4(50%) 12(50%) 10(67%)	W23-TL F23-FC W24-FC
7. Course helped me improve ability to work in teams	0 0 0	0 1(4%) 0	3(38%) 3(13%) 1(7%)	3(38%) 9(38%) 8(53%)	2(25%) 10(42%) 6(40%)	W23-TL F23-FC W24-FC

[a]W23-TL N = 8/29, F23-FC N = 24/35, W24-FC N = 15/24; [b]W24-FC N = 14/24

REFERENCES

[1] ISC2, "ISC2 Cybersecurity Worforce Study: Looking Deeper into the Workforce Gap," 2023. [Online]. Available: https://www.isc2.org/Insights/2023/11/ISC2-Cybersecurity-Workforce-Study-Looking-Deeper-into-the-Workforce-Gap

[2] Secuirty Magazine Staff, "71% of Orginizations are Impacted by Cybersecurity Skills Shortage," 2023. [Online]. Available: https://www.securitymagazine.com/articles/99865-71-of-organizations-are-impacted-by-cybersecurity-skills-shortage

[3] S. N. John, E. Noma-Osaghae, F. Oajide, and K. Okokpujie, *Cybersecurity Education: The Skills Gap, Hurdle!* Springer, 2020, pp. 361–376.

[4] M. T. Goodrich and R. Tamassia, *Introduction to Computer Security*, 1st ed. Addison Wesley, 2011.

[5] D. Mouheb, S. Abbas, and M. Merabti, *Cybersecurity Curriculum Design: A Survey*. Springer, 2009, pp. 93–107.

[6] The Regents of the University of Michigan, "University of Michigan-Flint Bachelor's Degree in Cybersecurity," 2024. [Online]. Available: https://www.umflint.edu/cit/cybersecurity/

[7] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel, and G. Witte, "Workforce framework for cybersecurity (nice framework)," National Institute of Standards and Technology, Tech. Rep., 2022. [Online]. Available: https://niccs.cisa.gov/cybersecurity-career-resources/additional-resources

[8] Palo Alto Networks Inc., "Palo Alto Networks Cybersecurity Academy," 2022. [Online]. Available: https://www.paloaltonetworks.com/resources/datasheets/cybersecurity-academy-curriculum

[9] W. Du and R. Wang, "Seed: A suite of instructional labratories for computer security education," *ACM Journal on Educational Resources in Computing*, vol. 8, no. 1, p. 24, 2008.

[10] J. Bishop and M. A. Verleger, "The flipped classroom: A survey of the research," in *Proceedings of the 2013 American Society for Engineering Eduction Annual Conference & Exposition*. Atlanta, Georgia: ASEE, 2013, pp. 1–18.

[11] THM-LTD, "Tryhackme," 2024. [Online]. Available: https://tryhackme.com/

[12] J. K. Knight and W. B. Wood, "Teaching more by lecturing less," *Cell Biology Education*, vol. 4, no. 4, pp. 261–343, 2017.

[13] S. Freeman, S. L. Eddy, M. McDonough, M. K. Smith, N. Okoroafor, H. Jordt, and M. P. Wenderoth, "Active learning increases student performance in science, engineering, and mathematics," *Proceedings of the National Academy of Sciences*, vol. 111, no. 23, pp. 8410–8415, 2014.

[14] M. Prince, "Does active learning work? a review of the research," *Journal of Engineering Education*, vol. 93, no. 3, pp. 223–231, 2004.

[15] I. del Arco, P. Mercade-Mele, A. Ramos-Pla, and O. Flores-Alarcia, "Bibliometric analysis of the flipped classroom pedagogical model: Trends and strategic lines of study," in *Education and Innovatibe Perspectives in Higher Education*. Frontiers Media SA, 2024, pp. 91–104.

[16] A. Roehl, S. L. Reddy, and J. S. Gayla, "The flipped classroom: An opportunity to engage millennial students through active learning strategies," *Journal of Family and Consumer Sciences*, vol. 105, no. 2, pp. 44–49, 2013.

[17] S. M. Redman, K. J. Yaxley, and K. F. Joiner, "Improving general undergraduate cyber security education: A responsibility for all universities?" *Creative Education*, vol. 11, no. 12, p. 18, 2020.

[18] B. Arora, "Teaching cyber security to non-tech students," *Politics*, vol. 2019, no. 2, pp. 252–265, 2019.

[19] R. Greenlaw, A. Phillips, J. Schultz, D. Stahl, and S. Standard, "Network reconnaissance, attack, and defense laboratories for an introductory cyber-security course," in *Proceedings of the 51st ACM Southeast Conference*. Association for Computing Machinery, 2013.

[20] P. Moore and J. Cappos, "Cybersecurity shuffle: Using card magic to teach introductory cybersecurity topics," *Joural of Computing Sciences in Colleges*, vol. 12, no. 1, pp. 52–61, 2022.

[21] A. Conklin, "Cyber defense competitions and information security education: An active learning solution for a capstone course," in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, vol. 9, 2006, pp. 1–6.

[22] T. Srivaranakul and F. Annansingh, "Incorporating active learning activities to the design and development of an undergraduate software and web security course," *Journal of Computers in Education*, vol. 9, pp. 25–50, 2022.

[23] V. Buriachok and V. Sokolov, "Implementation of active learning in the master's program on cybersecurity," in *Advances in Computer Science for Engineering and Education II*. Springer, 2020, pp. 610–624.

[24] D. R. Krathwohl, "A revision of bloom's taxonomy: An overview," *Theory into Practice*, vol. 41, no. 4, pp. 212–218, 2002.

[25] M. Ciampa, *Security Awareness: Applying Practical Cybersecurity in Your World*, 6th ed. Cengage, 2023.

[26] M. Versvik, J. Brand, and J. Brooker, "Kahoot!" 2024. [Online]. Available: https://kahoot.com/

[27] T. Eisenberg, D. Gries, J. Hartmanis, D. Holcomb, M. S. Lynn, and T. Santoro, "The cornell commission: on morris and the worm," *Commun. ACM*, vol. 32, no. 6, p. 706–709, June 1989.

[28] T. M. Chen and J.-M. Robert, "The evolution of viruses and worms," in *Statistical methods in computer security*. CRC press, 2004, pp. 289–310.

[29] K. P. Grammatikakis, I. Koufos, N. Kolokotronis, C. Vassilakis, and S. Shiaeles, "Understanding and mitigating banking trojans: From zeus to emotet," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2021, pp. 121–128.

[30] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "Wannacry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms," *Journal of Telecommunications and Information Technology*, no. 1, pp. 113–124, 2019.

[31] W. Du, *Computer Security: A Hands-on Approach*, 1st ed. CreateSpace, 2017.

[32] Instructure, "Canvas," 2024. [Online]. Available: https://www.instructure.com/canvas

[33] J. J. Yackley, B. R. Maxim, and A. Decker, "Active learning and gamification in game design courses," in *Proceedings of the 2018 Meaningful Play Conference*. Carnegie Mellon University ETC Press, 2019, pp. 1–14.

[34] S. Acharya and W. W. Schilling, "Effective active learning approaches to teaching software verification," in *Proceedings of the 2012 American Society for Engineering Education Annual Conference & Exposition*. San Antonio, TX, 2012, pp. 1–19.

[35] B. R. Maxim, T. Limbaugh, and J. J. Yackley, "Socially distant active learning and student engagement in software engineering courses," in *Proceedings of the 2022 American Society for Engineering Education Annual Conference & Exposition*. Minneapolis, MN, 2022, pp. 1–22.

[36] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 8th ed. Pearson, 2020.

[37] B. Hanks, S. Fitzgerald, R. McCauley, L. Murphy, and C. Zander, "Pair programming in education: A literature review," *Computer Science Education*, vol. 21, no. 2, pp. 135–173, 2011.

[38] R. M. Branch, *Instructional Design: The ADDIE Approach*, 1st ed. Springer, 2009.

[39] J. J. Yackley, "Active learning for introductory cybersecurity online supplement," 2024. [Online]. Available: https://sites.google.com/umich.edu/activelearningforcybersecurity

[40] W. M. Eddy, "Transmission control protocol (tcp)," Internet Engineering Task Force (IETF), RFC 9293, 2022. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9293

[41] T. Hunt, C. Hunt, and S. J. Sigurdarson, "';–have i been pwned?'," 2024. [Online]. Available: https://haveibeenpwned.com/

[42] U.S. Cyber Range of Virginia Tech, "U.S. Cyber Range," 2023. [Online]. Available: https://www.uscyberrange.org/