Adaptive Pedagogy Framework for Risk Management, Incident Response and Disaster Recovery Education

Hsiao-An Wang
Marquette University

ADAPTIVE PEDAGOGY FRAMEWORK FOR RISK MANAGEMENT, INCIDENT RESPONSE AND DISASTER RECOVERY EDUCATION

by

Hsiao-An Justin Wang

A Dissertation submitted to the Faculty of the Graduate School,
Marquette University,
in Partial Fulfillment of the Requirements for
the Degree of Doctor of Philosophy

Milwaukee, Wisconsin

June 2022

ABSTRACT

The field of Cybersecurity, both in cybersecurity education and cybersecurity workforce demands, has been growing steadily as the dangers of cyber-threats continue to rise. The gap between the supply and demand of the cybersecurity workforce has been widening throughout the past decade. In response to the increased demand, many government agencies have actively engaged in collaborative efforts with higher education institutions to produce more capable graduates to address the need. However, with the various educational utilities available to instructors, few utilities offer content related to risk management, incident response, and disaster recovery practices. Furthermore, many students lack the awareness to assess the risks of their behaviors on the internet. They are unaware of methods they can use to protect their personal information and proprietary data from potential cyber threats. In response to the ongoing issue, I propose to create an adaptive educational framework that would assist the instructors and enable them to easily demonstrate relevant risk management practices, incident response, and disaster recovery to their students using any pedagogical approach. I argue that students exposed to the framework content will demonstrate increased knowledge of risk management, incident response, and disaster recovery practices. The statistical results presented by the T-tests performed against the student knowledge assessment ratings show that except for three questions within the survey, the responses to the remaining fifteen questions offered by the students demonstrated an increase in knowledge at the 0.05 significance level. The expected contribution of this dissertation includes increased cybersecurity awareness among students and an increased understanding of risk management, incident response, and disaster recovery. In addition, I contribute to cybersecurity education research by offering materials to help students establish proper cyber hygiene and standardized operational protocol to respond to cyber incidents and recover potential losses. The framework proposed within this dissertation also offers instructors and educators the necessary resources to ensure efficient learning, offer standardized feedback, and provide students with the opportunity to increase cybersecurity awareness while enabling the instructors to instruct these topics using the pedagogy approach of their choice.

ACKNOWLEDGMENTS

During the first few years of my Ph.D. studies, some professors doubted my ability to conduct research, others questioned my motive for pursuing a Ph.D., and several individuals were pessimistic about my knowledge and anticipated my departure from the program. At times, I felt lost and frustrated because I had no idea what I was doing and what I should research. However, many people blessed me with guidance, encouragement, inspiration, friendship, support, and love. I am deeply grateful for everything my mentors, friends, and families have offered me throughout this journey. Their words of encouragement, support, helpful insights, and friendship enabled me to transform the negativity I experienced into the fuel and positive motivations to overcome the obstacles along this most challenging education journey and get to where I am today. I am specifically indebted to the individuals mentioned below:

Professor Debbie Perouli, my advisor and colleague at Marquette, has impacted me significantly positively. She was the first researcher that showed support for my passion in cybersecurity education. She has always been there to provide guidance and encouragement at times when I am troubled, lost, or deflated. I am incredibly grateful for her words of encouragement, kindness, and patience as I continuously maneuver through the Ph.D. journey without knowing what I want to do. I appreciate the freedom she gave me to work on problems or ideas that I found interesting, even when these ideas were random and sometimes a little crazy. Professor Perouli has been patient with my imperfections and randomly sparked "not so great" ideas throughout my journey in the newly created computer science program here at Marquette. Her knowledge, recommendations, and edits have improved the quality of our manuscripts, grant proposals, posters, and this dissertation. I am also grateful for the opportunities to collaborate on externally funded grants. We collaborated and worked coherently together as we hosted a week-long virtual Gen Cyber camp in the summer of 2021.

Due to her recommendations, I began to consult with Dr. Dennis Brylow, who eventually became my co-advisor. I frequently inquired him regarding the feasibility and gaps that exist in the realm of cybersecurity education and computer science education research. Dr.Brylow's feedback, support, passion, and deep commitment to the computer science education front inspired me deeply. He is someone I look up to as a role model and aspire to become in my tenure as an instructor within academia. Professor Brylow's expertise in Computer Science Education has been invaluable for our projects and attempts to incorporate additional cybersecurity content and materials into the existing K-12 CS education curriculum. I am also grateful for the career advice Dr. Brylow has offered as I search for potential openings to stay in the academic industry as an assistant professor. I am indebted to Dr.Brylow for his recommendations to secure the assistant professor of practice position here at Marquette during my last year of study. The teaching experiences that I have accumulated helped me tremendously in securing a job after graduation at Northeastern University's Boston campus.

Both of my advisor's expertise and experiences not only helped me to finalize my topic of interest quickly, but also inspired several of my ideas specifically related to

teaching. For example, the development of a portable cyber range on Raspberry Pi and the collaboration with EDURange to develop cybersecurity exercise scenarios. Both of those projects are scalable and reusable for instructors interested in incorporating cybersecurity education into their existing curriculum were both the byproduct of their inspirations.

I would like to thank Dr. Tom Kaczmarek and Dr. Lee Za Ong for their insightful comments and recommendations throughout the editing process of this dissertation. I am thankful for their suggestions, as they enabled me to improve the quality of this document. Dr. Ong provided insights on how education performance should be measured and analyzed. Dr. Kaczmarek challenged me on the accessibility of the resource and the scope of the risk management work, which were inspiring, and beneficial and helped me to realize the areas where I can make further improvements as I seek to continue the development of this educational resource. I thank Dr. Kaczmarek and Dr. Ong for their time, patience, effort, and timely responses throughout the manuscript editing procedure.

I also want to thank Dr. Terrance Ow, a mentor, a friend, and a colleague at the College of Business Administration. He entrusted me with the opportunity to instruct students over at the college of Business when I was still a clueless second-year Ph.D. student. His care, patience, and passion for students and teaching truly inspired me to be an instructor that can inspire and help others in any way possible. His work ethic was the perfect example that demonstrated the concept of leading by doing. The times collaborating and working with him over at the college of business have significantly impacted my ability to instruct students. In addition, he has affected and cultivated my work ethic when responding to student inquiries. More than anything else, he helped me understand how to teach and interact with students effectively while ensuring that the class content was intellectually challenging enough so that the students would reach out to ask the right questions and challenge themselves to strive for better. I thoroughly enjoyed my time working with him as a colleague, and now to this day still benefiting from the advice and recommendations he has offered me in my academic career ever since I first met him as a student. Words cannot describe my appreciation and gratitude for all the help he has offered me. I thank him so much for the opportunity to teach, learn and grow alongside him. I will treasure the memorable moments working as his colleague and learning from him as a friend and a student.

I appreciate the time, effort, and patience that the staff members at the Nice Challenge Project, specifically Alex Hillock and Rob Hancock. They spent hours after hours demonstrating their available content about the topics or subtopics of my research. Through them and the weekly curator meetings, I understood the NICE Challenge project better and made this adaptive pedagogy framework a reality. I still owe them a nice dinner and a toast to cheer for that.

I also want to express my gratitude towards our friends at Trend Micro, Michael Draeger and Sergio Avila. They shared their abundant knowledge regarding cybersecurity and cybersecurity education with no hesitation. They kindly offered me a

cybersecurity decision scenario game that I still use as an exciting injection module to educate students that I come across through my classes a little bit of cybersecurity. In addition, I also learned diverse ways to utilize the atomic-red framework, a framework used to duplicate and perform vulnerability testing from Sergio and Michael. This further increased my knowledge of offensive security.

I am grateful for my family, specifically my parents and my uncle in Taiwan. My dad provided me financial support while my uncle and my mom gave moral support and words of encouragement throughout this challenging journey. When I first decided to pursue a Ph.D. in Computer Science, they were shocked but also excited about the opportunity and encouraged me to try my best. Their words of encouragement and prayer played a significant role in cheering me up when I felt defeated and lost and thought I could no longer carry onward. While they may not necessarily be nearby when I needed them the most, I know they are all supportive of me becoming the first doctor in the family, and I miss them dearly. I also attribute my accomplishment to my grandma, who raised and cared for me when I was a rebellious little kid. Even though she may not be able to see my accomplishment and celebrate this moment with me, I will never forget her.

Finally, I would like to take this opportunity to thank all the undergraduate students, whom I have had the honor of instructing here at Marquette. Your honest opinions regarding the course offerings that I was held responsible for and me serving as your instructor and mentor helped me grow professionally as a professor and instructor and personally as an individual. I thoroughly enjoyed my time spent with them, whether within the classroom, virtually due to the Pandemic, or late into the night when responding to your panic emails. These are the memories that I will continue to cherish and bring forth with me as I start my new position at Northeastern University. Thank you all for your kind words, encouragement, and harsh comments. Those are the fuel that continues to push me forward, motivate me to learn, grow, and cultivate me to be the best I can ever be.

To conclude, I must admit that I would be lying if I said I have always believed in myself and would materialize the promise I declared to my mom 18 years ago. When I was thirteen, I swore to my mom that I would one day obtain three degrees and be the most knowledgeable person in the family. I still remember that was a promise I jokingly made after a poor quarter performance while I was in middle school. However, I appreciate the 13-year-old me because I would have given up my Ph.D. career a long time ago without that promise, I made to myself and my mom. I thank God for the perseverance, the grit, and the optimism that he has given me. The promise that I made was one of the most critical elements that held me together. It was that fearless little me and the promise that I made that got me through the roller-coaster ride of a Ph.D. tenure.

The past twelve years at Marquette have mostly been great. I will always cherish the experiences that I had at Marquette, whether it be staying up late responding to student emails, working in the laboratory until 7:30 AM, or sleeping on the couch of the library. Those are valuable memories that will be dear to my heart. Thanks to

all the wonderful people I have come across throughout my time at Marquette, even though you may no longer be in Milwaukee, or we may rarely be in contact, Cheers!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter1

INTRODUCTION

Cybersecurity is a field that has seen its workforce demand rising steadily throughout the past decade. The "National Cyber-ethics, Cyber-safety, Cybersecurity baseline study" of 2008 stated that Education on cyber-ethics, cyber-safety, and cybersecurity is inadequate. Many urge the federal government, in partnership with educators and industry, to conduct a national cybersecurity education and awareness campaign to increase public awareness of cybersecurity. Upon realizing weakness in the current state of cybersecurity, many parties, including the Internet Security Alliance, and federal agencies such as NSA, strongly encourage collaboration between academic and industrial laboratories to develop a strategy to expand and train cyber professionals to work within the federal government. In the wake of cybersecurity breaches and attacks on Fortune 500 companies and popular websites, cybersecurity-related roles within the industry have also been in high demand throughout the past decade.

Even though the demand for cybersecurity specialists continues to rise, there appears to be a supply shortage of cybersecurity professionals across the United States. According to Cyberseek, the collaborative initiative between the National Initiative for Cybersecurity Education (NICE), burning glass, and CompTIA, 72 percent of the states within the U.S have more than 1300 cybersecurity-related role openings as of the end of March 2019. In addition, according to the NICE workforce demand fact sheet, as of December of 2021, the global shortage of cybersecurity professionals is estimated to be 2.72 million. There are approximately 597,767 cybersecurity job openings available; on average, it takes six or more months to fill a single cybersecurity position; cybersecurity professionals require two years of training before they

become proficient [68]. However, we are not producing enough proficient graduates from the education programs to fill the gap.

For us as researchers, educators, and instructors to solve the supply shortage issue in cybersecurity professionals, we ought to take the initiative to create, develop and grow cybersecurity education programs and begin raising cybersecurity awareness among students by teaching cybersecurity topics. Sample topics such as proper hygiene, staying safe on the web, and essential operation of the internet would enable younger generations to protect themselves on the internet better. Incorporating cybersecurity education initiatives early in the education curriculum is especially important when most of them will be growing up with a smartphone. If not, an intelligent device with access to the internet where cybersecurity threats are present. When the education starts early, the likelihood of raising more students motivated to learn more about cybersecurity will be higher.

In addition, we believe cybersecurity education is a crucial discipline that may aid in addressing, if not reducing, the number of costly cybersecurity crises and help fill the void of demands for well-trained security professionals. As cybersecurity education efforts become more accustomed to the academic atmosphere, many higher education institutions have realized an urgent need to train students interested in cybersecurity. Besides being interested, students willing to devote time to research, study, and independent studies of secure programming, vulnerability analysis, risk assessment, system defense, and exploitation tactics are the key to satisfying the industry's security professional demands. As of now, many higher education institutions are offering cybersecurity-related disciplines as an official degree. According to ABET, there are 649 institutions with 3328 programs related to cybersecurity that ABET accredits. [1]

However, among the institutions that provide cybersecurity tracks, programs may

only sparsely offer topics courses emphasizing risk management, incident response, penetration testing, and disaster recovery. Institutions that combine cybersecurity into a traditional computer science curriculum may offer even fewer options. Even when offered, topics courses are often provided as optional elective courses rather than parts of the graduation requirements that students must meet. When these topic courses are offered as elective courses, only a few students interested in cybersecurity will enroll, resulting in smaller class sizes. A potential cause of this issue is that students lack awareness of risk management and do not see themselves becoming cybersecurity professionals. Instead of enrolling in those security-related courses, students often vow to select technical knowledge-based classes that help them to secure software engineering opportunities within the industry instead.

Moreover, the industry organizations usually classify any information related to incident response plans and disaster recovery plans as confidential material. Those plans are solely established, executed, and updated by the personnel working within the security teams only. Typical engineers will rarely be exposed to such knowledge and often fail to create, edit, and maintain their incident response and disaster recovery plans should they become victims of cyber-attacks. There is a void in the education sector on risk awareness, incident response, and appropriate knowledge on the best practices of forming an incident response and disaster recovery plan for personal use.

Although many current issues persist, we still have hope, as there are abundant non-commercial resources that, if used correctly and appropriately by the instructors, will offer the means to educate children and young adults correctly. These resources will provide students with the correct knowledge and help them be cyber-aware as they enter a constantly evolving digital world. In this dissertation, I achieved several objectives. I first introduced the practical educational pedagogical approaches.

By using the cognitive walkthrough method, I examined the freely available non-commercial cybersecurity education utilities. I also discussed a few beneficial ongoing projects. I conclude by proposing a new educational framework that is adaptive to any pedagogical approach and can be used to instruct students on risk management, incident response, and disaster recovery on the personal level.

The remainder of this dissertation work will be organized as follows: Chapter 1, the introduction offers a brief background of the cybersecurity profession, the current situation with the continuously widening gap between the supply and demand of cybersecurity professionals and discusses several potential solutions that could address this concerning gap.

Chapter 2 discusses an exploratory approach to evaluate existing non-commercial cybersecurity education utilities that are readily available for instructors to use. Within this chapter, I carefully evaluated twenty-two educational utilities using the cognitive walkthrough approach from a student's perspective. I then offer my opinion on the pre-requisites students should meet to maximize their learning and each tool's potential advantages and disadvantages to help instructors evaluate whether the utility would fit their needs.

Chapter 3 discusses the feasibility and investigation of the local Computer Science Education programs within the state of Wisconsin. I offer potential ways to enable us to begin cybersecurity education earlier by offering training to the teachers like how we train the local teachers on computer science concepts. Besides training the teachers, we can host summer camps across Wisconsin to increase awareness of cybersecurity and incorporate simple but important cybersecurity topics into the existing computer science education curriculum that many middle and high schools across Wisconsin have adapted.

Chapter 4 describes my work with the authors of EDURange to create a frame-

work of the authoring process that enables instructors to easily develop cybersecurity exercises within the EDURange utility. This process explicitly discusses how instructors can deploy docker containers to host cybersecurity exercises for their students to have their own independent instances of a sandbox to work on security-related activities freely and safely.

Chapter 5 describes my future project work associated with deploying intentionally vulnerable cybersecurity containers using Raspberry Pis. Specifically, I dedicate this chapter to describe my collaborative effort with a team of graduated computer science seniors and a non-profit organization named Wisconsin Cyber Threat Response Alliance (WICTRA). We collaborated to deploy two of the very well-known intentionally vulnerable boxes (Mr. Robot and BWapp) prototypes for students to engage in an attempt to obtain the administrative privileges of an independent Raspberry Pi. I intend to continue this work as this work is a potentially scalable project that can be used to offer students hands-on experiences performing offensive security tactics and facilitate active learning.

Chapters 6 focuses on introducing the proposed framework components in detail. It is also within this chapter that I present my effort with the trial framework implementation in a regular course offering across two semesters. The materials within the framework were introduced to a mix of undergraduate computer science students enrolled in different courses to ensure data diversity.

Chapter 7 reports the collected and valid results from the trial implementation. This chapter also explains how I processed the data collected through the student knowledge assessment and how I used the T-test to demonstrate that the derived outcome of this trial implementation offers supportive evidence to validate my thesis statement.

Chapter 8 offers my insight on factors that may have contributed to the varying

student performances. For example, several factors such as content delivery modality, student maturity, course offering time and observed student behavior may each contribute to the different performances demonstrated on the knowledge assessment surveys.

Lastly, in the concluding chapter of the work, I conclude this work with critical findings of the framework implementation trial, reinforce the criticality of the developed educational resources, and offer a few insights towards the future direction of my research activities and related work.

Overall, I intend to use this resource to increase cybersecurity risk awareness through the introduction and creation of the material. Specifically, I aim to help my students, K-12 teachers, and other individuals interested in cybersecurity understand that cybersecurity risk exists. I seek to help students understand that it is not a matter of whether they will become the victim of a cybersecurity attack but a matter of when and that security is a continuous process that should be continuously optimized to ensure maximum protection on personal information. I also aim to constantly develop, optimize, and make the components of this framework a beneficial addition to the cybersecurity education research community.

Chapter2
AN EXPLORATORY APPROACH TO EVALUATE NON-COMMERCIAL TOOLS FOR CYBERSECURITY EDUCATION

This chapter describes a work-in-process paper that played a crucially significant role in helping me identify the existing gap within the available educational resources, either open-source or offered non-commercially. In this chapter, we enumerate pedagogical cybersecurity education approaches, explore the prerequisites of twenty non-commercial tools, and identify the content gaps within non-commercial education utilities. Through a comparison of topic coverage, we provide recommendations on cohesively combinations of utilities and pedagogy that would increase learning efficiency when used together and incorporating into new or existing cybersecurity curricula for K-12, undergraduate, or graduate students. Finally, we identify areas of growth for future cybersecurity education projects.

2.1 Utility Analysis through the Cognitive Walkthrough Approach

To better explore the user usability of the non-commercial educational utilities, we decided to use the cognitive walkthrough approach, developed by Wharton et al. [89] to inspect each utility. Specifically, the investigation will emphasize the ease of learning of each non-commercial and list a few potential advantages and drawbacks for consideration. The cognitive walkthrough approach is a form of evaluation where an expert (or group of experts) steps through the design and interfaces to evaluate the design's usability. The emphasis of the walkthrough will focus on the ease of learning characteristics from the perspective of a typical user in the target audience group. The evaluators will ask several critical questions [89]. In our scenario, the evaluator will ask three questions: Will the user know their expectations of them?

Will the user know how to achieve the expectations? Will the user see progress as they navigate the presented problems? We chose to use the cognitive walkthrough for several reasons. First, it will help other instructors to understand the usability of each presented educational utility. The walkthrough allowed us to evaluate the tool from the perspective of a regular user that will interact with the utility. The goal of our evaluation was to present our findings of potential advantages and drawbacks the users may find for the instructors.

2.2 Existing Pedagogical Approaches

In response to the demand that calls for undergraduate students of all disciplines to be exposed to cybersecurity and increase their awareness of risks from security breaches [71], collegiate institutions have taken the initiative to establish security education programs that align with various existing pedagogical approaches. In this section, we list several widely adopted and known pedagogical practices by institutions, instructors, and the corresponding suiting target audience to help raise student awareness related to computer security issues.

The *traditional approach* is often text-based and lecture-oriented single courses where students learn the foundations of security concepts in breadth but not necessarily in-depth. The conventional lectures usually consist of conceptual content and limited practical experiences [59]. The traditional approach is considered the most straightforward approach that novice instructors may leverage to educate students. However, explicitly using the conventional approach to lecture students is not recommended since other researchers have shown that a pedagogy approach such as active learning produces better material absorption and development of critical thinking [61]. Therefore, given that instructors can easily integrate the traditional pedagogical approach with other approaches to create a vivid learning atmosphere. We strongly encourage instructors to combine lecturing with different activity-based

approaches. Alternatively, incorporating other interactive learning utilities such as concept maps, DETER Labs, and security injection modules to keep the students motivated and engaged would facilitate student learning.

Compared to traditional lecturing, *active learning* is more engaging and motivating for students and produces better absorption of material and development of critical thinking [61]. Active learning typically provides an environment for the students to have the freedom to fail and try additional experiments when learning an unfamiliar concept. Learning occurs when the users explore different scenario choices presented and understand the potential impact the "wrong choices" may have [81]. We recommend that novice and experienced instructors adapt to the active learning approach. The active learning approach will work cohesively with an interactive laboratory or challenge-based utility. The tasks within these utilities are often open-ended, and students can solve the tasks in many ways. This feature will provide students with sufficient motivation to spend extended time engaging with learning resources which not only deepen their knowledge but also give them the opportunity to solve problems using novel approaches or methodologies.

Experiential learning consists of a four-stage cycle of learning and four distinct learning styles. It is an approach best suited for institutions that design their cybersecurity laboratory in an open-ended fashion. Learning occurs primarily when the students engage in experiments, reflect on the experiments, and gather conclusions from the experiments [33, 56, 58]. We recommend instructors with some experience consider the use of the experiential approach. Even though experiential learning may require the instructor to spend additional preparatory time to create a baseline experiment, the instructor's role transitions into a facilitator once the students begin their experiments. This pedagogical approach helps teach students how to use experimental results, adjust accordingly and continue to test the feasibility and usability

of their design. Experiential learning can work brilliantly with sand-boxed utilities such as Labtainer, EDURange and SEED Lab Project.

In *peer education* settings, the instructor becomes a facilitator who asks students leading questions. Students must respond to the leading question based on assigned readings and their knowledge, then engage in discussions to exchange ideas with their peers and further increase their understanding of the topic [15]. Being a successful facilitator that can answer questions on the fly requires experience. Therefore, we recommend experienced instructors use the peer education approach along with utilities such as HackTheBox, PicoCTF, Nice Challenge, and TryHackMe, allowing students to collaborate in small groups and share their knowledge.

The essence of *injection-based learning* is that security content should be added into existing computer science curricula. Course material injections, security track offerings and threaded cybersecurity educational modules all accomplish the same goal of injecting security content into existing curricula [18, 59, 78]. Injection based learning is an approach that can be used by instructors of all levels. This approach can work coherently with utilities such as SEED Lab Project, Labtainers, TryHackMe and DETER Labs that offer laboratory exercises with instructions to enhance learning efficiency.

Challenge-based or *competitive learning* is the methodology that utilizes a combination of a competitive atmosphere and challenging problems to invoke student learning. A typical example of this learning approach would be the capture the flag (CTF) activities, where students are required to solve problems to obtain a "flag" and redeem it for points. Research has shown that CTFs can be valuable components of undergraduate cybersecurity courses and that students displayed higher motivation, more self-directed learning, and the ability to push the boundaries of their knowledge when engaging in CTF activities [69, 92]. Utilities such as Nice Challenge, PicoCTF,

EDURange, and HackThisBox can complement challenge-based learning approaches very well. However, considering that the challenges and content these utilities present may be complex, students engaging with these utilities may need additional guidance from the instructors to avoid frustration. We only recommend this approach to experienced and veteran instructors who are experts in cybersecurity and computer science.

2.3 Non-Commercial Educational Tools

In this section, we examined twenty-two non-commercial educational tools commonly used for cybersecurity education through the cognitive walkthrough method with emphasis on usability, ease of access, and ease of learning characteristics from the perspective of a typical user in the target audience group. We also explore and present potential advantages and disadvantages for each utility and recommend prerequisites for incorporation into educational curricula. We derive our survey results from our institution's local experience using the tools; We also base the derived prerequisite, advantages, and disadvantages on the user experiences. We recognize and appreciate the arduous work and efforts of the authors dedicated to each utility. If the limitations include any issues identified by the authors, we will cite their work and contribution.

2.3.1 PicoCTF

PicoCTF is the international "capture the flag" competition hosted by the Carnegie Mellon College of Engineering's Information Networking Institute. The competition typically takes place in mid-September. This challenge has been viral among middle and high school users throughout the North American regions every year since its initial release. While the target audience focuses on middle and high school students, college students and beyond can acquire valuable security knowledge by engaging in the challenges. PicoCTF offers challenges across six primary domains, including

general computing skills (e.g., command line tools), cryptography, web exploitation, forensics, binary exploitation, and reverse engineering [69, 92].

2.3.1.1 Cognitive Walkthrough

The challenges and problems offered within the PicoCTF platform can be viewed directly on the challenge portal while downloading the file for closer examination is an option. The portal is easy to navigate. Participants can use mini-game tokens to redeem hints for challenges. The scoreboard tracks individual participating teams' progress, but the only data monitored for each problem is the number of groups successfully solved this problem.

2.3.1.2 Prerequisites

Based on our participation in the annual competition during the last three years, we encourage instructors who intend to incorporate PicoCTF as part of their cybersecurity course to ensure the students understand the command shell and methods to inspect webpages using a modern browser. While programming experience is not required, familiarity with coding basics will be helpful for students who are engaging in binary exploitation and reverse engineering activities.

2.3.1.3 Strengths

The platform offers a Piazza [73] classroom, where participants can freely exchange ideas, ask for hints, and report potential issues with specific challenge problems or the shell server. The challenge contents are available year-round after the competition period, and for each topic category, several on-ramp exercises are available for students new to cybersecurity. In addition, the Pico platform presents its challenges in two formats: a dashboard and a Unity game [80]. The game contains mini-exercises that generate tokens for students to purchase in-game hints, a storyline, and a mini-game world that presents challenges in different rooms.

2.3.1.4 Potential Drawbacks

Although the developers at Carnegie Mellon did not list programming experience as a prerequisite, many challenges require students to use programs in various languages to solve problems. We encourage the instructors to dedicate additional time to help motivate students to learn about the content exposed within the platform. Lastly, attempting to solve challenging problems can be time-consuming and frustrating, especially for students who may not have any background in cybersecurity.

2.3.2 SEED Lab Project

The SEED Labs is a virtual machine-based cybersecurity sandbox using the Linux operating system and developed by Dr. Wenliang Du of Syracuse University. The project categorizes its twenty-eight exercises into three groups: vulnerability and attack labs, design and implementation labs, and exploration labs [37].

2.3.2.1 Cognitive Walkthrough

SEED Labs requires students to download a premade virtual machine image for deployment. Students may occasionally encounter issues during the image deployment, but instructors can mitigate most problems quickly. Each related project provides the user with a lab manual describing expected learning objectives and tasks. Correctly identifying the methods to achieve laboratory objectives may be difficult for some labs as the wording of the manual can be confusing without guidance. Students will not always realize that they are making progress as they navigate a lab exercise since SEED Labs does not offer built-in evaluation tools. The instructor must complete grading based on the student's submission.

2.3.2.2 Prerequisites

Instructors who intend to use SEED Labs should ensure the students have experience working with a C-Compiler within Linux and programming experience in C/C++ and bash. Depending on the exercises instructors select, JavaScript and

HTML experience may also be required.

2.3.2.3 Strengths

The utility is a standalone sandbox environment that allows students to engage in active learning while attempting to solve open-ended problems within a Linux environment. The education utility also gets distributed with user manuals and installation instructions which is beneficial for first-time users. The exercise content is versatile and covers many security principles such as cryptography, attacks like Meltdown and Spectre, and access control [37].

2.3.2.4 Potential Drawbacks

The exercise description manuals sometimes contain ambiguous wording that might mislead students if they were to engage in the exercises independently. However, instructors have access to the manuals and can update them for their classes. Some exercises require multiple instances of the SEED Labs image running simultaneously, which could be resource-intensive for students with limited memory and storage space on their devices.

2.3.3 Labtainers

Labtainers is a cybersecurity exercise container developed by the Center for Cybersecurity and Cyber Operations of the Naval Postgraduate School. The Naval Post Graduate School created the Labtainers as an expansion toolset of the SEED Labs. The toolkit supplies a single Docker [35] virtual machine image for educators and students to freely engage with cybersecurity-related tools while working within a sandbox-safe environment [48, 84].

2.3.3.1 Cognitive Walkthrough

Labtainers is like SEED Labs offering a single virtual machine image for deployment. Laboratory contents and corresponding manuals are accessible from the resource repository upon request. Students should be able to follow the laboratory

guidance and complete the tasks without additional assistance from the instructor. In addition, students may use the grade lab feature to track their progress.

2.3.3.2 Prerequisites

Experience deploying Docker images onto host machines and familiarity with command shell is required. Students can only fetch exercises through the command line interface within the Docker image. Rudimentary knowledge of programming languages such as Python and C/C++ will help students be successful [84].

2.3.3.3 Strengths

The instructions and wording of the exercises are concise, and the portable Docker image enables students to work remotely and access learning materials at any time. The activities are session-based with randomized seeds. The individualized Docker container will record student actions once the session has been configured and initiated. Student submissions contain artifacts that deter students from engaging in academic dishonesty practices [84]. Instructors can add their exercises to the toolset.

2.3.3.4 Potential Drawbacks

The prerequisites the students must fulfill are higher than other utilities for this tool to offer a meaningful learning experience. Labtainers focus on computer science students who wish to learn more about security; it may not be feasible for non-majors unfamiliar with programming to use this resource. Instructors may need to dedicate additional preparatory hours to familiarize themselves with this resource due to the complexity of the components [84].

2.3.4 CyberCIEGE

CyberCIEGE was also developed by the Naval Post Graduate School and initially released in 2005. It has gone through many subsequent phases of optimization and improvement. It is a resource management and network security simulation that is packaged and distributed as a stand-alone game to enhance computer security by

demonstrating abstract functions of security mechanisms [53, 81, 83].

2.3.4.1 Cognitive Walkthrough

The gamification offered by the CyberCIEGE engine enables students to engage in challenging scenarios and complete tasks. Through the presented scenario, the students will know the tasks at hand. However, solutions can be open-ended, and students can solve challenges through various methods. Students can track progress by observing the reaction of the characters and the objectives. The interface may seem complex, but the utility offers students opportunities to explore additional ways to address the presented issues without penalty.

2.3.4.2 Prerequisites

Unlike other educational utilities, CyberCIEGE has no prerequisites that the students need to meet. An evaluation instance of the simulation engine restricts users to twenty-minute sessions. The instructors can submit a request to the Naval Post Graduate School for permission to use the full version of the scenario engine.

2.3.4.3 Strengths

The simulation engine does a beautiful job at delivering security concepts and best practices through scenario presentation and storytelling. An objective checklist is provided to the students to motivate and encourage them to complete all challenges within a given scenario. Interaction with simulation characters and elements gives students hints. Special effects may be displayed when the student makes the wrong choice. The simulation engine introduces the concept of security clearance to students, something that many utilities tend to leave out but is common, especially in the public sector. This engine also enables the instructors to create customized scenarios.

2.3.4.4 Potential Drawbacks

The utility components are unique and have a learning curve that the students will have to overcome over time. The automated event trigger due to time passage

may cause the scenario to end abruptly without informing the user that they have failed to achieve the objectives (the message that hints at user failure will repeatedly appear, but the scenario will not necessarily terminate). Further, some event triggers may behave strangely without much explanation, leading to unexpected outcomes and requiring the user to restart the scenario. Lastly, some component placements within the simulation engine are incredibly close together, making it difficult for users to identify the correct options needed to achieve the scenario objectives.

2.3.5 NICE Challenge Projects

The NICE Challenge is a cybersecurity challenge range that offers real-world scenarios with topics on network mapping, configuration troubleshooting, penetration testing, password cracking, incident response, asset management, and malware mitigation for students. Within the challenge range, students will learn the problems cybersecurity professionals of various roles may have to troubleshoot or resolve daily. Academia instructors and professors can request access to the NICE cybersecurity challenge range, and students may only receive access through their educator. Although the challenge range is reservation based with an upper-bound limitation of four hundred concurrent students, the challenge project designed the problem scenarios in an open-ended format. The challenge format enables students to engage in active learning practices, as there is often more than one way to resolve the issue. The challenge platform also allows students to create a professional grade report detailing the tools and methodology used to solve the problem. That is the only way to submit their response and work [65].

2.3.5.1 Cognitive Walkthrough

The NICE Challenge project is accessible through the challenge portal, and instructors will not need to do any additional deployment work. The cloud-based platform will deploy all required virtual machines when students deploy their challenges

of interest. The preparatory meeting of the challenges will offer hints regarding the challenge objective to the students. The pre-defined challenge objectives will also be displayed on a panel next to the virtual machines so that the students will know the goals of each corresponding challenge. Although hints and deployment diagrams are available, the student may not necessarily know how to achieve the tasks without instructor facilitation and additional tips on keywords. The platform tracks student progress based on the defined objectives such that if the students make any progress, the objective's status will change, and the students would know that they are progressing towards completing the challenge.

2.3.5.2 Prerequisites

Familiarity with the various operating system is not required but preferred. The operating systems vary from Linux to all suites of Microsoft Windows. Familiarity with command line interface preferred. Previous knowledge of real-world challenge scenarios is preferred.

2.3.5.3 Strengths

The NICE Challenge offers the curator(instructor) an easy-to-navigate web portal that enables instructors to make reservations and preview available challenges filtered by difficulty, estimated duration, work roles, and challenge types. Curators may also select multiple challenge scenarios in a single reservation for the students to attempt. Curators may monitor the learning progress of individual students through their submission attempts and the class's overall performance through the report statistic feature. The curator may also provide the student's feedback for each submission. The challenge is installation free as the student can access the virtual machines directly through their browser. Students also receive the opportunity to learn how to create a detailed documentation report that describes their approach, methodology, and tools used for each of the challenges they attempted. In addition, the platform

offers a monthly deep dive learning session for instructors to attend. Throughout the meeting, instructors may ask questions regarding specific scenarios and receive assistance on selected scenarios. Curators can also schedule private appointments more frequently than the monthly curator meeting. During these private meetings, a staff member will assist the instructor through selected scenarios so that the instructors can be better equipped with specific hints and details to look for as they facilitate the learning process of their students.

2.3.5.4 Potential Drawbacks

Although the challenges that the NICE Challenge offers are realistic and easy to access, it can be difficult for instructors and students who may not have much experience in cybersecurity problem-solving. The hints and challenge check only provide a minimal explanation. To further increase learning efficiency, instructors may have to explore the laboratory contents and create customized lab notes or guides before assigning the task to the students. This utility is more favorable and adaptable to instructors with abundant experience teaching cybersecurity.

2.3.6 EDURange

EDURange is a cyber range that offers topic-oriented challenge scenarios. The utility supports one-click deployment of target machines, the ability to create additional scenarios, and real-time response validation. Dr. Weiss from Ever Green State college and Dr. Mache from Lewis and Clark College created and published the initial release of EDURange. The two professors and a team of students, led by Jack Cook, are actively developing the refactored version. Instructors at Evergreen and Lewis and Clark college have adapted the range within classrooms with outstanding success in facilitating student learning. The range currently offers ten exercises that cover topics such as network security, system security, software security, binary exploit, and reverse engineering [51].

2.3.6.1 Cognitive Walkthrough

The EDURange will need to be cloned and deployed from a GitHub repository. Detailed and step-by-step instructions for deployment are available from the author. The current deployment process is optimal and smooth; users will only need to execute the install script to deploy the components [32] automatically. We recommend that users deploy EDURange on a fresh Ubuntu OS through a virtual machine. The range deployment is now automatic and follows a single, strict workflow. In the deployed scenarios within EDURange, the users will need to provide answers to question prompts, which will entail the scenario-related objectives. The laboratory guides will provide relevant information to help learners understand how to achieve the corresponding goals. When answers are delivered into the answer fields of the questions provided as a regular user and click submit, the range will validate the solutions provided, and the evaluation result will be displayed underneath the question to demonstrate progress.

2.3.6.2 Prerequisites

Many exercise scenarios offered by EDURange are command line based, while most commands needed can easily be found through a quick search engine query. We still recommend students to have a basic idea of command line before attempting to solve challenges offered by the scenarios. For instructors, the prerequisite would be basic computer network knowledge, port forwarding, and command line commands. If the instructors intend to create customized exercise scenarios, then the knowledge of Docker images will be required.

2.3.6.3 Strengths

The EDURange does not require students to install anything on their own devices. If the instructors correctly configure the servers, they will have access to all the scenarios offered by the EDURange. For cloud deployment, the deployment requirement

is limited, and the current version of EDURange has an installation script that students can use to complete the installation with one click. All student-submitted data is collected automatically and evaluated by the instructors.

2.3.6.4 Potential Drawbacks

The EDURange offers minimal error handling and feedback. When users deviate from the single, strict deployment workflow, the users will encounter many errors not explained by the deployment guide. However, this should no longer be an issue since the installation and deployment are now automatic. Most scenarios are command line based and may not necessarily offer as much flexibility in exercise types. Currently, the number of exercises is limited compared to the other educational utilities available for instructor adaptation.

2.3.7 Security Injections

Security Injections are strategically placed security modules for existing undergraduate computer science classes. The authors of security injections also offer training workshops that help instructors to adapt and deploy security injections modules into existing classes [54]. Security injection modules offer learning materials that cover web security, network security, binary exploit, software security, and general skills. Security Injections also offer many of its modules in multiple programming languages. Students will be required to examine given code snippets and provide answers to multiple choice questions. Once answers are submitted, the learning modules will provide immediate feedback. [78, 79]

2.3.7.1 Cognitive Walkthrough

Security Injection modules are available through the official website by using a standard browser. No deployment is necessary. The objective of each module is clear, and students should compile and execute the code snippet to determine the answers. Students should know how to achieve their goals and see progress through

the instant response validation displayed on the web page.

2.3.7.2 Prerequisites

The prerequisite may differ depending on how the instructors deploy the security modules into the classrooms. Students will need basic knowledge of the selected programming language (C++/Java/Python), a basic understanding of the integrated development environment, and basic knowledge of the compiler.

2.3.7.3 Strengths

Instructors can deploy the modules into classrooms without additional software deployment. The topics are covered in multiple programming languages, offering support for introductory programming languages based on different languages. The Security Injections modules cover many topics and provide a step-by-step learning process. Students must complete the module sections with the correct responses before students can move on to the next section. Each module also offers brief background information to help students understand the importance of the concept.

2.3.7.4 Potential Drawbacks

The instructor will need to facilitate the learning process and ensure the students are not just blindly trying out the answer options of the multiple-choice questions without examining the provided code snippet.

2.3.8 Security Knitting Kit

The Security Knitting Kit is an NSF-funded project at Tennessee Tech University. It is a series of educational modules that aims to help instructors to teach security principles in the computer science curricula. The educational module series includes software engineering security, database management systems security, network security, and system security. We were unable to access the educational module series. Therefore, we could not conduct a cognitive walkthrough or analyze the Security Knitting Kit's materials. [77]

2.3.9 Kypo Cyber Range Platform

Kypo Cyber Range Platform is an open source, cloud-based cybersecurity range developed by faculty and staff at Masaryk University. Kypo offers a full-fledged operating system and network devices using standardized components to offer cybersecurity challenges and built-in learner analysis. The engine of the environment is based on OpenStack, a cloud platform that provides architecture, identity services, and a dashboard for data analytic functions [86]. The installation of OpenStack and deployment of Kypo are significantly more complicated than many of the educational utilities we surveyed. This utility is only recommended to instructors who have experience working with OpenStack, considering that the deployment process is complicated despite documentation and installation guides being available. If deployment and installation assistance is needed, the development team also offers full-function deployment assistance for a cost.

2.3.10 SANS CyberStart

CyberStart is a web-based challenge learning educational utility developed and maintained by SANS Institute. It offers interactive and fun scenarios to learn about distinct aspects of cybersecurity. The challenges cover diverse topics, including software security, binary exploits, reverse engineering, cryptography, and system security. The game offers twenty-nine levels of challenges across the three bases. [11]

2.3.10.1 Cognitive Walkthrough

Users and students can access the content of the utility through its online portals, and deployment effort is minimal. Still, as the users and students advance onto higher levels, they may need virtual machines. The utility offers briefing reports for each independent challenge that briefly describes the challenge's objective. Students may find additional information regarding the challenge within the challenge itself to help participants complete objectives to conquer the obstacles. When progress is made

towards completion, the utility will notify the user by providing flags that enable the participant to complete the challenge and move on to the next level.

2.3.10.2 Prerequisites

No technical prerequisites need to be met to deploy or use this utility. The target group is high school students, while instructors and others can request access to the content or purchase an independent license.

2.3.10.3 Strengths

The utility provides a field manual that answers most questions and a briefing report, and notes presented within the challenge help to clear the objective of each challenge. The platform also offers a personal progress tracking and badge system to encourage students to engage in more problem-solving activities. The breadth of topics is comprehensive and exciting. Solutions and hints are available should the participant find themselves stuck.

2.3.10.4 Potential Drawbacks

The potential drawback of this utility is that it may not necessarily be suitable to be used for collegiate participants. Some of the challenge contents are relatively easy, potentially decreasing student motivation from advancing onward.

2.3.11 Nova Labs

Nova Labs is a collaboration effort between Nova and cybersecurity experts from Whitehat Security, Gigaom Research, Sans Institute, Oxford internet institute Deter Cyber Security Project, and the Center for Identity at UT Austin. The lab's objective is to offer a cybersecurity game that covers password complexity and social engineering topics, explicitly identifying phishing emails and introductory programming through block codes. The NOVA cybersecurity lab offers twenty-seven challenges across three levels and a storyline that helps to keep the participants interested and engaged. [22]

2.3.11.1 Cognitive Walkthrough

The laboratory and its corresponding exercises are accessible and available through a modern web browser. No additional deployment or installation is needed. The utility offers clear objectives and hints that help users understand the challenge at hand to achieve their objective. The progress of challenge completion is also tracked for users so that challenges are available for the users to retry challenges that they may not have gotten correct on their first attempt.

2.3.11.2 Prerequisites

No prerequisites need to be satisfied before instructors can use the education utility to teach students about basic cybersecurity practices with password complexity and identifying phishing emails.

2.3.11.3 Strengths

The challenges offered are exciting, and solutions to the challenge are available upon the submission of the initial attempt. The participant may also use hints to help themselves solve the challenges. The storyline helps to provide the student context on a typical cybersecurity scenario and provides the instructor the opportunity to educate their students regarding best practices.

2.3.11.4 Potential Drawbacks

The potential drawback of this utility is the limited number of exercises and topic coverage. This utility only offers twenty-seven activities, nine on code block programming, nine on phishing emails, and nine on password complexity. This utility may only provide limited benefits to their students for instructors that intend to offer more topics within their classes.

2.3.12 OWASP Juice Shop Vulnerable Web Application

OWASP Juice Shop is a free, open-sourced, intentionally vulnerable application created for training, concept demonstration, and learning purposes. The shop was

developed by Björn Kimminich and is actively being maintained and updated by a group of volunteers. It is also a good utility for instructors interested in adopting challenge-based learning pedagogy. The Juice Shop encompasses vulnerabilities from the OWASP top ten, and many security flaws found in real-world web applications [55]. The Juice Shop contains challenges associated with many topics of interest, including cryptography, system security, general skills, software security, and best practices. The Juice Shop can be deployed as an independent range for students to engage in on their host machine or through cloud application platforms such as Heroku or Google Cloud Console. In addition, instructors can use it to demonstrate specific security concepts in class settings or host a standard capture the flag competition after the shop has been customized. The project offers an official project guide on all existing challenges and support for customization. It is a beginner-friendly utility that instructors can use to educate students interested in web application security and other security topics related to the OWASP top ten vulnerabilities.

2.3.12.1 Cognitive Walkthrough

OWASP Juice Shop allows its users to hack vulnerable web applications safely and freely. Deployment instructions are provided in detail for users to choose their deployment options freely. Challenge solutions for the off-the-shelf Juice Shop version are available, which could help instructors to facilitate learning and training. The users will require instructor facilitation to identify their objectives until they resolve the challenge of "finding the scoreboard." Without prior exposure to challenge-based learning activities, students may struggle to achieve exercise objectives after they are identified. While a solution manual is available for use, we recommended that the instructor carefully utilize it to offer hints to its students as a supplemental resource to facilitate the learning experience. As challenges are solved through student interaction with the web application, a hint ribbon will appear on the page if students solve an

existing challenge successfully to indicate progress has been made to encourage users to attempt other challenges.

2.3.12.2 Prerequisites

There are no formal prerequisites, but experience in inspecting web applications through a web browser is recommended. Some challenges may require the users to use programming language-specific syntax or commands, but students can find these commands and syntax easily through a quick search query on Google.

2.3.12.3 Strengths

The Juice Shop is self-contained, offers self-healing, supports performance statistics monitoring and CTF features, and can be customized to create variant instances for unique learning experiences. It can be deployed and installed quickly and offers a safe environment for students to test their skills and familiarity with different tools. It also provides step-by-step tutorials in the application and step-by-step solutions in the e-book for instructors to refer to answer student questions that may arise as they engage with the utility.

2.3.12.4 Potential Drawbacks

Although Juice Shop is beginner friendly, the students may find it challenging to identify their objectives without guidance from their instructors. Since a step-by-step solution is available, it is more difficult to prevent users from cheating when solving the challenges offered by the Juice Shop. Instructors can customize the challenge to prevent cheating attempts from the students. The Juice Shop provides a simple cheat detection mechanism based on the time difference between current and previous attempts.

2.3.13 Trend Micro Cybersecurity Scenario Game Engine

Trend Micro Cybersecurity Scenario Game Engine offers two scenarios where the end user will be functioning as a key security executive of an organization who will be

required to make executive decisions regarding security configurations, security policy enforcement and decisions related to noncompliance of policy and or incidents that an organization may face. The scenario focuses critically on the decision making when the security executive face ransomware threats and targeted attack threats. [14]

2.3.13.1 Cognitive Walkthrough

The Trend Micro Scenario Game suite is easy to use, easy to access and is available to anyone interested in interacting with the game and offers users the opportunity to get a brief overview of the decisions in which cybersecurity executives must make. The learning takes place through the facilitation of the game and explanation of options by the instructor. Students will be able to expand their cybersecurity related knowledge when the instructor explains the concepts behind each of the available choices. Although the game itself does not track progress but based on the choices in which the user selects, the ending of the game will differ.

2.3.13.2 Prerequisites

There is no prerequisite for this utility, students can freely engage with the game until they identify the correct path in which leads to successful conclusion of the game. Though, having a knowledgeable instructor to facilitate through the game will make the learning experience more interactive and interesting.

2.3.13.3 Strengths

The utility provides the instructors the opportunity to engage and interact the students in an interesting way, it also offers key words such as open-source software, intrusion detection, deep security that incentivize students to conduct research of the keyword and learn more about cybersecurity.

2.3.13.4 Potential Drawbacks

When students engage in this utility without the instructor's assistance to elaborate on each of the potential options, the learning that takes place may be minimal

as it transforms the educational utility into a mere cybersecurity narrative.

2.3.14 Hack The Box

Hack The Box is a web-based learning ground that offers the users to register accounts for free and engage with various carefully crafted vulnerable virtual machine servers for users to learn about distinct aspects of cybersecurity including offensive security, cyber defense, blue team practices, OWASP top 10 vulnerabilities, privilege escalation amongst other topics through capture the flag mechanisms. The site offers a personalized profile, various learning paths where students can freely connect to and engage the machines, each of the machines offers information such as difficulty level, user rating, the operating system needed, released date, the number of users that have completed the challenge and some boxes may also offer a walkthrough guide to help users get started into learning about cyber. Additional features such as organized topic-centric learning paths are also available for uses who purchase VIP subscriptions. [23]

2.3.14.1 Cognitive Walkthrough

The utilities, virtual machines and challenges can be easily accessed through the browser, users will be able to ping and communicate with the machines once the VPN connection is active. The challenges offered at this site are designated for users to test their skills and abilities, so while there may be challenges that are rated easy or beginner friendly, there may exist a learning curve for students who are new to capture the flag based active learning. The objective of each of the challenge boxes may not necessarily be clearly presented and accessible, but through the exploration of the machine, hints regarding the flag and tasks can often be located within the machines.

2.3.14.2 Prerequisites

Users are required to download the OpenVPN client to communicate with the virtual machines that the site offers. Other than that, the only prerequisite will be an account registration.

2.3.14.3 Strengths

The utility offers a wide variety of hands on, gamified and self-paced challenges for users to engage in, the content and servers are accessible through web browser without requiring any configuration on the user's end. The learning environment offered by this utility is realistic in that there may not necessarily be a graphical user interface and that every communication or tasks must be done through a command prompt.

2.3.14.4 Potential Drawbacks

While the learning environment is realistic, for users new to cybersecurity, this utility may be slightly confusing to the users. There will be a learning curve for users who has never engaged in other learning utilities that requires the users to communicate through via command prompt only. Some content is only exclusive to individuals who purchase VIP subscriptions.

2.3.15 Try Hack Me

Try Hack Me is a web-based utility that offers step by step instruction and videos for end users to learn about the various aspects of cybersecurity. Each module contains tasks that the user must complete through the submission of correct answers that are either introduced in the module or mentioned in the instructional videos. This utility is very beginner friendly as the tasks are presented clearly and is a utility that we recommend using along with Hack The Box. [85]

2.3.15.1 Cognitive Walkthrough

The utility is easy to access, easy to use, each of the modules covers a different subtopic within cybersecurity which is perfect for someone who may be interested in transitioning into a cybersecurity related role. The users will know the tasks they need to finish to complete the learning module, progress will be actively tracked by the system, and the users should know that they are making progress towards learning more about specific concepts as they engage in learning from the various modules organized by content topics.

2.3.15.2 Prerequisites

There is no technical prerequisite for this learning utility, users will have to register for accounts to begin using the utility though.

2.3.15.3 Strengths

Learning modules and learning paths are clearly labeled, each of the learning module consists of sub modules that help the users learn more about concepts, fundamental basics, and the various utilities. The utility is accessible and user friendly, the interface is very self-explanatory and offers small tasks for users to engage in as they learn more about different security topics.

2.3.15.4 Potential Drawbacks

The learning offered by this utility are more guided, which may not necessarily be a desirable choice for learning for individuals who wish to freely explore vulnerable machines in hands-on approach.

2.4 Non-Commercial Educational Technique and Resources

This section discusses the non-commercial educational technique and resources that are not stand-alone utilities that students or instructors can directly use.

2.4.1 CyberWar Laboratory

CyberWar Labs are the "go-to" option when designing computer security curricula because they offer students the opportunity to learn about penetration testing and defensive tactics, gain exposure to digital forensics and understand the concept of offensive mindset [44]. Institutions must ensure that the CyberWar Labs provide its user's easy accessibility, including the ability to simulate realistic scenarios, simulate computing devices for lab exercises, observe host activities and network traffic while staying isolated from the production campus network. In addition, the adopters should also evaluate how the lab will share limited resources between student users and whether it is feasible for the students to configure systems remotely. In general, these are desirable characteristics for many information security labs [64, 70]. CyberWar Labs can be instantiated physically, with dedicated hardware and networking, or virtually, using virtual machine images and virtual networks. Several institutions offer duplicate templates for CyberWar Labs images, including the University of New Mexico, Carnegie Mellon, and University of Alaska - Fairbanks [64].

2.4.1.1 Cognitive Walkthrough

CyberWar laboratory's contents and exercises vary significantly from institution to institution. Still, most CyberWar laboratories will offer their students a specific objective (e.g., defending a particular server from intruders through hardening or conducting digital forensics to identify threat sources). Depending on the instructor, the students may work in teams and learn through peer education or experiential learning. Hints may be available to students who are unfamiliar with achieving the objective, and they may also seek help from their peers through active discussions. In a typical red team and blue team exercise carried out through a CyberWar laboratory, student progress towards the objective is likely not tracked actively.

2.4.1.2 Prerequisites

For institutions that wish to have a physical laboratory based on specifications from Carnegie Mellon, requirements include a rack of servers with ample CPU and memory capacity, a library of disk images, and a database of lab configurations. A web application and Java-based client that grants students necessary access to the deployed environment is recommended. Each of the students will also receive step-by-step instruction manuals for all exercises. The utilities and core system requirements remain identical to ensure virtual labs yield a similar learning experience. The University of New Mexico incorporated a virtual lab to complement their existing physical lab, allowing students to connect to the laboratory environment remotely and share the workload of the physical labs [64]. Knowledge and skill prerequisites vary based on the specific laboratory requirement and configuration. A student consent form signed by the department chair and student is required to ensure the students will not misuse the resources within the CyberWar Lab or deploy the experience they gain to conduct offensive security against the campus network and other individuals [44, 64, 70].

2.4.1.3 Strengths of Virtual Lab

The virtual CyberWar laboratory provides excellent flexibility regarding laboratory configuration, such as system IP address, support for central logging, rapid prototyping of computer network configurations, and a more consistent learning experience for all students [66, 74]. The virtual lab also offers more accessible access to resources, less administrative overhead, and live support for complex exercises [24]. It is an ideal utility candidate for instructors who wish to deliver security content through experiential and active learning methodologies. The students will be granted access to various tools and could potentially use different combinations of tools within the lab to craft their offensive plan.

2.4.1.4 Potential Drawbacks of Virtual Lab

Training requirements to equip the instructor and students to navigate the resources available within the virtual laboratory can be substantial. Limited technical support, significant demand for underlying server resources, and its corresponding management workload may be overwhelming. Maintaining such infrastructure requires a sustained effort from engaged faculty or staff [24].

2.4.1.5 Strengths of Physical Lab

The physical CyberWar laboratory offers students the means to be more knowledgeable about how to secure systems, detect vulnerabilities and manage software patches. Physical access to computer systems enables the students to closely monitor and examine the effectiveness of their offensive security tactics in real-time. Furthermore, having a physical laboratory also allows the instructors to determine how the course content can be delivered and set limitations on what the students are allowed to do with the computing resources made available to them. The physical laboratory also supports learning pedagogies such as active learning and peer education as the environment can be easily configured to support such instruction styles [60].

2.4.1.6 Potential Drawback of Physical Lab

Transforming the physical laboratory into a heterogeneous and realistic environment requires time and effort. Adequate training of adopters will be required to respond to unexpected events such as resource corruption or potential outages during lab time. Students working in teams may need to be restricted to launch one well-orchestrated attack at a time to avoid resource exhaustion [60].

2.4.2 Concept Mapping

Concept mapping is a well-known pedagogical tool used by instructors of various disciplines to help students develop a deep understanding and to organize their knowledge appropriately. Studies have shown that “concept maps are effective for student

to clarify their knowledge structures" [16]. Concept maps as a teaching technique enable the students to organize the concept of interest into a graphical hierarchy structure that presents how the subtopics can correlate to the abstract topic placed at the top as the starting node [16]. Concept maps are ideal for measuring student learning growth, as they reiterate ideas using their own words; any inaccuracies or incorrect links identified can alert the instructor to what the student does not understand [16]. Concept maps are good candidates for instructors who wish to use peer education. Through the idea exchange process, students with different concept maps may be able to complete and optimize their concept maps.

In the following, we focus on two related works. One presents concept maps as a tool for cybersecurity education and evaluates an automated analysis method. The other (Cmap analysis) is a tool developed to help instructors assess concept maps in an automated fashion.

2.4.2.1 Cognitive Walkthrough

Concept mapping is an instructor-led activity where students are provided instructions on crafting a concept map based on their current knowledge. With minimal guidance and facilitation, the students are not expected to have issues preparing a concept map emphasizing the topic of interest. Student progress in the concept map generation may not be actively monitored or recorded, but the instructor may aid and offer additional guidance if necessary.

2.4.2.2 Prerequisites

There are no content prerequisites required for students to use concept maps.

2.4.2.3 Strengths of Cmap Analysis

Canas et al. [26] note flexibility as an advantage of the Cmap analysis tool since it allows instructors to select digital concept maps created in two different formats freely. In addition, it enables instructors to add additional evaluation measures without hav-

ing to make massive modifications to the assessment configuration. In addition, the tool considers additional aspects when evaluating the quality of the concept map [26], such as the root child count and the average words per concept.

2.4.2.4 Potential drawbacks of Cmap Analysis

The instructor must have existing survey results regarding the concept maps' size, quality, and structure that meet their expectations. Otherwise, additional work in terms of survey collection will be needed to ensure the instructors can evaluate the concept maps holistically [26].

2.4.2.5 Strengths of Topological Scoring

Topological scoring is a method to automate the concept map assessment and evaluation process. It reduces the evaluation workload of the instructor significantly as concepts map submissions can be very open-ended and challenging to evaluate, which makes providing actionable feedback and proper evaluation time-consuming and difficult for instructors [34].

2.4.2.6 Potential drawbacks of Topological Scoring

The assessment results yielded by the topological scoring approach were inconsistent compared to the results generated through manual grading. Suggesting that topological scoring may only be applicable when evaluating concept map submissions on select topics. This finding was apparent in the original work, where the authors compared concept map evaluation results using topological scoring and a manual grading rubric. While automatic assessment of concept maps is attractive and can be valuable, the accuracy and ability to automatically evaluate concept maps of all security topics of interest is still questionable [34].

2.4.3 Virtual Machine Introspection

Virtual machine (VM) introspection is more of a technique than a stand-alone utility. Introspection is realized through extraction and reconstruction of the guest OS

state in the host. Introspection empowers the monitoring system to control, isolate, interpose, inspect, secure, and manage a VM from the outside [27]. Cybersecurity professionals have widely used introspection in other areas of cybersecurity, such as vulnerability analysis and digital forensics.

2.4.3.1 Prerequisites

Students should have prior experience using kernel payloads and understand how memory could be modified through the read and write operations within a given system. Previous experience with kernel payloads would help the student understand better why the system behaves in a certain manner [19].

2.4.3.2 Strengths

Introspection-based exercises allow the students to engage in attacks based on malicious low-level kernel modules and observe the results in detail. Students will be able to modify the memory of the VM through the read directly and write operations from outside of the VM and observe the effects their operations may have on memory [19].

2.4.3.3 Potential Drawbacks

Instructors may need to attend training sessions led by security professionals or other means to understand how introspection functions fully. Additional research may be required for the students to harness the power and benefits VM introspection offers [19].

2.4.4 Test-bed Environment

A test-bed environment is a cloud-based platform that offers researchers and students the means to conduct research over the cloud using shared resources maintained by a third party. The advantage of a test-bed is that researchers can request resources that they do not physically own from the test-bed platform and do not need to worry about maintenance. The potential downside of relying on a test-bed environment is

that server resources may not always be available upon request when needed since resources are shared amongst the user body.

DETER Lab is one of the more recognized test-bed platforms that offer cybersecurity researchers the means to engage in research, development, discovery, experimentation, and testing of innovative cybersecurity technology. USC/ISI and UC Berkeley host it. It currently consists of more than four hundred computing nodes and a set of tools used for cybersecurity experimentation. DETER Lab will load a low-level disk copy of an operating system image onto a free node and install files based on experiment configuration to produce a live network of real machines that users can access remotely [61].

2.4.4.1 Cognitive Walkthrough

DETER Lab provides the underlying platform on which educators can build their assignments. Currently, there are several assignments from different institutions and instructors. Many built-in and pre-existing assignments do a decent job of specifying the work or task objective students must achieve. Depending on the assignment specifications offered by the instructor, the students should know how to achieve the expected objectives without excess assistance from the instructor. Since DETER Lab provides a wide range of assignments created by other instructors who also leverage the platform, we cannot claim that all assignments offer clear guidance to help students achieve the assigned objective. Lastly, the DETER Lab platform and the corresponding assignments created by the instructors do not have any built-in feature to track student progress while engaging with a specific project available on the platform.

2.4.4.2 Prerequisites

The instructors must register and submit a project application to DETER Lab through a short form to receive access to the computing nodes. The form also specifies

the total number of nodes needed for the experiments.

2.4.4.3 Strengths

For each DETER Lab project experiment, the user will gain exclusive, privileged access to a set of computing nodes through a secure shell (SSH). Computing nodes will run the OS and application at the user's discretion. DETER Lab provides a controlled environment that allows users to test security threats and defenses. Instructors can assign pre-made exercises to students as homework assignments, and the platform also offers instructors the flexibility of creating customized exercises [61].

2.4.4.4 Potential Drawbacks

Instructors need to get familiar with the test-bed configuration environment, estimate the computing resources required by the students and reserve them in advance (one week). Students must learn the necessary steps to load their experiments and resume them if needed. A student that does not start an assignment in time may not be able to complete it if computing resources are not available at a particular time within the test-bed.

2.4.5 Tele-Lab

Tele-Lab is a web-based tutoring system developed by the students and staff at the University of Trier in Germany. The tool offers resources that instructors can use to educate students on fundamental information technology (IT) security concepts and practical virtual laboratory exercises for students to reinforce their learning experience. The operation of Tele-Lab depends on a standalone computer-based tutoring system named E-learning platform IT security (LPF); a tool also developed at Trier. LPF must be deployed onto the VM systems to grant students assigned to the specific system the privilege to interact with the VM through LPF [45]. Since this tool is only offered in German, we could not evaluate it firsthand. Therefore, most of the information presented below is derived from the author's published work.

2.4.5.1 Prerequisites

Familiarity with Linux based operating system will be desired, as the students will primarily be working within the Linux-based VM to accomplish learning tasks. The tool is in German.

2.4.5.2 Strengths

Ease of access, as the utility, makes remote learning possible. It offers an all-in-one package containing educational lecturing on security principles, web-based tools, hands-on exercises, and a student progress tracker [45].

2.4.5.3 Potential Drawbacks

Misuse of access to the VM could lead to corruption in the system. While there is a fail-safe mechanism (assign new virtual machines to students), restoration of the corrupted partition depends on a backup of the partition or a pre-built CD-ROM, potentially interrupting the learning experience should the tool be used in a classroom setting with supervision [45].

2.4.6 TeachCyber

TeachCyber is not a standard utility but an aggregated collection of resources that the instructors may freely explore and adopt. TeachCyber categorizes the utilities based on their properties (CS education, offense, defense, and interdisciplinary). For each utility, it also listed a brief description for each corresponding utility that includes the content in the utility offer and the programming language that may be used when interacting with the tool. In addition to offering a hyperlink to security utilities and course modules, TeachCyber also provides a list of educational videos, tools, and news articles related to cybersecurity incidents and vulnerabilities [12].

2.4.6.1 Prerequisites

There are no content prerequisites for students and instructors to browse and use this resource collection.

2.4.6.2 Strengths

This web page offers a list of hyperlinks that redirects to a wide variety of non-commercial educational tools and educational materials such as training videos and an encyclopedia for offensive security tools. It is also adequately categorized and easy to navigate for instructors who may be looking for a specific type of educational utility.

2.4.6.3 Potential Drawbacks

Considering that this website is a collection of educational resources, materials, and established courses on diverse topics, no drawback can be linked to this web page itself.

2.4.7 K12 CyberTalk

K12 CyberTalk is a podcast by Dr. Dan Manson from California State Polytechnic University. The podcast series aims to increase cybersecurity awareness, empower K-12 students to pursue a career in cybersecurity, and provide students the opportunity to learn and explore cybersecurity. Topics include network security, security competitions, security introduction, and cryptography. The website also hosts periodic talk shows introducing cybersecurity to K-12 students.

2.4.7.1 Wisconsin Cyber Threat Response Alliance

The Wisconsin Cyber Threat Response Alliance is a local non-profit organization that functions as cyber information sharing hub. Members of the public, private sector, and federal agencies collaborate to leverage cross-sector resources to analyze and respond to Wisconsin's cyber threats effectively. This organization offers training content through the mobile cyber warfare ranges built with various exercise ranges for users to learn about the red team, blue team concepts, forensics, malware analysis, and other cybersecurity topics. The organization openly collaborates with higher education institutions to organize training workshops, offers students the opportunity

to learn about cybersecurity through engagement in research projects, and offers training events for students in Wisconsin who may be interested in learning about cyber security. []

2.4.8 MITRE ATT&CK Framework

MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The knowledge base is a foundation for developing specific threat models and methodologies in the private sector, government, and cybersecurity product and service community [17].

2.4.8.1 Cognitive Walkthrough

This utility, unlike other educational resources, is not exercise-driven. It is a collection of the knowledge base of the tactics actively used by threat actors causing cybersecurity problems in the real world against organizations. Therefore, the cognitive walkthrough approach does not apply to the MITRE ATT&CK framework. However, if necessary, the instructors can use the MITRE ATT&CK framework to create assignments requiring students to gather threat intelligence information and identify the tactics and techniques that a specific threat actor group uses. In that usage scenario, the student should know the objective, whether they are making progress or not (e.g., are they creating a corresponding heat map to highlight the tactics of the threat actor). However, the utility does not track progress in real-time.

2.4.8.2 Prerequisites

There is no technical prerequisite for this learning resource. Users can freely browse the knowledge base to obtain information regarding attack tactics and techniques used by threat actors. The matrix enables users to filter by attack technique, threat actor groups, the industry of interest, and other variables.

2.4.8.3 Strengths

This learning resource offers a comprehensive collection of attack mechanisms and techniques active threat actor groups use. The framework provides a solution for cybersecurity analysts to consider incorporating those techniques to prevent them. This resource is excellent for students interested in research regarding offensive security mechanisms. The students may be able to make use of the atomic red scripting library to gain a deeper understanding of specific techniques used by threat actors.

2.4.8.4 Potential Drawbacks

The atomic red scripting library has a steep learning curve for users who are new to the utility. Instructors who are unfamiliar with the framework may not necessarily fully utilize the benefits which the framework offers. To further use this resource to facilitate learning, the instructors must craft custom exercises for students, which could take significant prep time.

2.5 Discussion

This section offers a detailed explanation of categorizations that we have made when comparing the non-commercialized cybersecurity education utilities. We also provide definitions for the utility usage difficulty, content coverage, and instructor levels based on experiences to help readers better understand the graphs demonstrating the differences in content in each of the utilities we examined offers.

2.5.1 Utility Usage Difficulty and Content Coverage Definition

In this paper, we recognize that students and instructors may have a wide range of knowledge and understanding of cybersecurity-related concepts. For each of the pedagogy and utilities described in this paper, we will briefly mention the target audience groups (K-12 students, instructors, non-major students, and Computer science students with or without emphasis on cybersecurity) that may find the utility or pedagogy more useful. In addition, a definition for the difficulty of utilities and

Table 2.1: Utility Name Map

Tool/Name	Abbreviated Term
Labtainers	LT
CyberCiege	CC
PicoCTF	PC
DETER Labs	DL
VMI	VMI
Concept Maps	CM
CyberWar Labs	CWL
Tele-Lab	TL
SEED Labs Project	SP
NICE Challenge	NC
Security Injection	SI
Teach Cyber	TC
Security Knitting Kit	SKK
EDU Range	ER
K12CyberTalk	KCT
Kypo Cyber Range	KCR
SANS CyberStart	SCT
NOVA Labs	NL
OWASP Juice Shop	OJ
Trend Micro	TM
HackTheBox	HT
TryHackMe	THM

their corresponding content coverage will also be defined here. These definitions will be used in the comparison tables that are incorporated within the paper.

2.5.2 Instructor Level Definition

In this section, we classify instructors based on experience and subject of instruction. The instructors classified as novice level instructors are individuals with 0-3 years of teaching experience on the subject matter that are familiar with 3-4 topics. Whereas experienced corresponds to 4-7 years and 5-7 topics, veteran level instructors correspond to 8 years of teaching experience and familiarity with more than seven topics.

Tool/Methods	Traditional	Active	Experiential	Peer	Injection	Challenge-Based
LT		↘	↘		↘	↘
CC		↘	↘	↘	↘	
PC		↘		↘	↘	↘
DL	↘	↘			↘	
VMI	↘		↘		↘	
CM	↘			↘	↘	
CWL	↘	↘	↘	↘	↘	↘
TL	↘		↘		↘	
SP	↘	↘	↘	↘	↘	↘
NC		↘	↘			↘
TC	↘	↘	↘	↘	↘	↘
SI	↘	↘	↘		↘	
TC						
SKK						
ER		↘	↘	↘	↘	
KCT	↘					
KCR		↘	↘		↘	↘
SCT	↘	↘	↘	↘	↘	↘
NL	↘	↘	↘	↘	↘	
OJ		↘	↘		↘	↘
TM	↘			↘	↘	
HT		↘	↘		↘	↘
THM		↘	↘		↘	↘

Table 2.2: Utility Correspondence to Pedagogical Strategies

Table 2.3: Difficulty Mapping

Utility Difficulty	Numeric Value
Easy	1
Moderately Difficult	2
Complex	3
Challenging	4
Highly Challenging	5

Table 2.4: Coverage Mapping

Utility Content Coverage	Acronym
Not Applicable	N/A
Minimal Coverage	M
Sufficient Coverage	S
Abundant Coverage	A

2.5.3 Utility Difficulty Definition

We classify the difficulty level of the utilities into five categories: easy, moderately difficult, complex, challenging, and highly challenging. Easy is designated to utilities offering students simple and easy-to-understand content. Moderately Difficult is assigned to utilities offering cybersecurity content that may have minimal knowledge prerequisites. The complex difficulty is designated to utilities that provide cybersecurity content with prerequisites that students must meet; these types of utilities typically offer more suitable content to instructors and students with cybersecurity knowledge. The challenging difficulty is designated to utilities that offer more fitting for instructors specializing in cybersecurity education with several years of experience and students with some knowledge of cybersecurity, including web security, network security, network management, threat analysis, and network analysis, among others. Extremely challenging is a difficulty level designated to utilities offering cybersecurity content in a virtualized real-world scenario with little hints or guidance. These types of utility primarily target seasoned cybersecurity instructors with an abundant amount of experience and students with advanced cybersecurity knowledge across the various breadth of topics.

2.5.4 Challenge Content Coverage Classification

For content coverage, we also attempt to classify the content level coverage of each utility corresponding to a list of topics in cybersecurity. They include software security, system security, network security, reverse engineering, binary exploit, cryp-

Table 2.5: Utility Instructor Correspondence

Tool/Instructor Level	Novice Instructor	Experienced Instructor	Veteran Instructor
Labtainers	2	1	1
CyberCiege	1	1	1
PicoCTF	3	2	1
DETER Lab	3	2	1
VMI	4	3	2
Concept Maps	2	1	1
CyberWar Labs	3	2	1
Tele-Lab	2	1	1
SEED Lab Project	3	2	1
NICE Challenge	5	4	3
Security Injection	3	2	1
Teach Cyber	1	1	1
Security Knitting Kit			
EDU Range	3	2	1
K12CyberTalk	1	1	1
Kypo Cyber Range	5	4	4
SANS CyberStart	1	1	1
NOVA Labs	1	1	1
OWASP Juice Shop	4	3	2
Trend Micro	2	1	1
HackTheBox	5	4	4
TryHackMe	5	4	3

tography, incident response, and disaster recovery. The coverage levels are classified as follows: Not applicable(N/A), the content provided by the utility offers no coverage of the concept, minimal coverage(M), where the content offered provides less than three module or laboratory exercises corresponding to the concept, sufficient coverage(S), where the utility provides content that grants the student foundation knowledge of specific concepts, and ample coverage(A), where the content provided by the utility demonstrates high emphasis of concepts.

2.5.5 Utility Coverage and Evaluation

This section discusses our experiences evaluating commercial training utilities and non-commercial educational tools that focus on cybersecurity. We also aim to identify gaps in content, topics covered, and target audience within non-commercial educa-

tional utilities that may help fellow researchers identify a project of interest. Furthermore, we relate the explored utilities to existing pedagogy that would yield the most benefit in student learning.

2.5.6 Utility and Pedagogy Correspondence

In Table 2.8, we note the suitability of each non-commercial utility to the corresponding pedagogical strategies described in Section 2.2. We determined each utility's suitability for a given pedagogical approach based on three primary criteria: local institutional experiences, the nature of the utility's content, the potential we envisioned the utility might have with specific pedagogical approaches, and conclusions drawn from the original reference publications.

2.5.7 Utility Topic Coverage

Table 2.6 notes the security concepts each of the utilities covers through exercises, project work, and other forms of assignment such as scenario challenges. We categorize the activities into various commonly known cybersecurity topic categories. Other researchers can find a detailed list of activities and exercises on the official sites of each of the utilities. From the content illustrated in the table, it is apparent that most non-commercial educational utilities do not offer coverage of topics such as security clearance, reverse engineering, incident response scenarios, and disaster recovery.

2.5.8 Utility Usage Difficulty

This work categorized the overall difficulty levels of utility usage into five categories. When assessing the difficulty of utility usage, many factors are taken into consideration. These factors may include but are not limited to instructor knowledge requirement, prerequisite, ease of deployment, ease of use, topics of coverage, availability of user manual, lab manual, or solutions. Precisely, ease of deployment, ease of use, and availability of guiding manuals weigh slightly more than other factors. The difficulty levels assigned to the utility may also differ based on the instructor's

experience and the utility coverage of topics.

2.5.9 Utility recommendation to instructors

Instructors should choose educational utilities based on the topic of interest, the usage difficulty level, and the coverage of topics as it corresponds to the instructor's experience level and the pedagogical approach the instructor chooses to adopt. As a result, we do not make specific recommendations for utilities. Instead, we provide a comparison table for instructors to cross-reference the number of tools available for adaptation based on the pedagogical approaches and the tool topic coverage in alignment with the identified topic of interest within cybersecurity education.

2.5.10 Utility Properties

The educational utilities we surveyed, examined, and conducted cognitive walk-throughs against are further categorized into two groups: virtual machine, sand-boxed based utilities, and web-based utilities. While web-based resources may provide easier access to the students and instructors, most practical exercise-oriented utilities require some form of deployment (usually the deployment of pre-built virtual machine images, but in some cases, deployment could also involve the deployment and installation of numerous services and virtualized servers)

2.5.11 Pedagogy recommendation to instructors

Based on examining and categorizing the educational utilities, we recommend instructors adopt active and experiential learning pedagogy. These two pedagogical approaches can be associated with many practical and hands-on exercises through various utilities. If traditional lecturing is preferred, educational module injection and challenge-based learning activities should be considered to ensure student engagement while keeping the class livelier and more enjoyable.

Table 2.9 notes whether the utilities are offered as a standalone virtual machine image, sandbox, docker image, an independent executable file or offered as a platform

versus webpage-based utilities in which the user must have internet access to engage in the exercises.

2.5.12 Commercial versus Non-Commercial Educational Resources

This report focuses on non-commercial educational resources. We chose this focus because educators often find it infeasible to purchase the commercial tools and the complexity of the commercial tools. In many cases the target market for commercial tools is cybersecurity professionals with technical knowledge of cyber risks and common computing infrastructure. The complexity of the commercial offerings is perplexing to the less knowledgeable and inexperienced student. Consequently, it is challenging for instructors to motivate students to engage in the commercially available tools and exercises except in the case of courses that go deep into the technical details.

2.5.12.1 Training Resources

Many professional organizations and vendors such as EC-Council [38], InfoSec Institute [7], ISC2 [50] and SANS Institute [46] offer training and examination for certification purposes. The InfoSec Institute, EC-Council, ISC2, and SANS Institute offer online, on-demand cybersecurity courses. InfoSec Institute provides utilities such as phishing simulation and offers various certification learning paths, cyber ranges, knowledge assessments, boot camps, and practice exams through the InfoSec skills platform. The SANS Institute and EC-Council offer courses on specific topics such as "red team" (offensive security exercises), penetration testing, and many others. At the same time, ISC2 offers short format courses and exercise-driven courses. In addition to commercial solutions and offerings, these sites also offer free webinars that focus on recent cyber incidents and additional resources, such as security cheat sheets, which describe tactics cybersecurity administrators can use to strengthen system security [7, 38, 46, 50].

2.5.12.2 Professional Certification Resources

SANS Institute, EC-Council, ISC2, and ISACA, among others, offer training courses for professional certification and examination. These courses are provided in two formats: on-demand learning and instructor-led training. Topics of a professional certification include penetration testing, ethical hacking, digital forensics, and cloud security [38, 46, 49, 50].

2.6 Concluding Remarks

This chapter of the work discusses the non-commercial utilities available for instructor adoption. I know this may not necessarily be all the public utilities. Still, this set of utilities should cover most of the utilities that instructors frequently use in higher education institutions. The objective of this explorative analysis was to help inexperienced instructors decide on the utility that fits their needs while ensuring they do not necessarily need to spend the time to investigate the feasibility of each utility before making a choice. I am also aware that the opinions regarding the suitability of resources and pedagogical approach are subjective, and others may not necessarily agree with my classification. Nonetheless, this work should benefit instructors seeking to incorporate cybersecurity into the existing computer science curriculum to increase student awareness of cybersecurity risks.

Topics/Utility	LT	CC	PC	SP	CWL	CM	DL	NC	TC	SI	ER	KCT	SCT	NL	OJ	TM	HT	THM	VMI
General Skills	S	S	S	M	S		S	M		M	A		S		S	S	S	S	S
Software Security	A		M	A	S		S	M		A	M				S		M	S	S
Network Security	A	S	M	S	S		S	A		M	M		M		S		M	A	A
Web Security	S	M	A	M	S					M	M				S		A	M	S
System Security	A	S		M	S	S	S	S		M	M		M		S	M		A	A
Cryptography	A	S	S	S	S	S	S						M		S				
Mobile				M															
Industrial Control	S			M		S													
Binary Exploit			S		S		S											M	M
Reverse Engineering			S		M													M	M
Security Clearance	M	M																	
Incident Response					M			A			M								
Disaster Recovery																			

Table 2.6: Utility Topic Coverage

Tool/Methods	Easy	Moderately Difficult	Difficult	Challenging	Extremely Challenging
Labtainers	✓	✓	✓		
CyberCiege	✓	✓	✓		
PicoCTF	✓	✓	✓	✓	
DETER Labs		✓	✓		
VMI		✓	✓		
Concept Maps	✓				
CyberWar Labs	✓	✓	✓	✓	✓
Tele-Lab	✓				
SEED Lab Project	✓	✓	✓	✓	✓
NICE Challenge			✓	✓	✓
Security Injection	✓	✓			
TeachCyber	✓				
Security Knitting Kit					
EDU Range	✓	✓			
K12CyberTalk	✓				
Kypo Cyber Range				✓	✓
SANS CyberStart	✓	✓	✓		
NOVA Labs	✓				
OWASP JuiceShop	✓	✓	✓	✓	
TrendMicro	✓	✓			
HackTheBox	✓	✓	✓	✓	✓
TryHackMe	✓	✓	✓	✓	

Table 2.7: Utility Usage Difficulty

Table 2.8: Utility Correspondence to Pedagogical Strategies

Tool/Methods	Traditional	Active	Experiential	Peer	Injection	Challenge-Based
Novice Instructor	✓	✓			✓	
Experienced Instructor	✓	✓	✓		✓	✓
Veteran Instructor	✓	✓	✓	✓	✓	✓

Table 2.9: Utility Properties

Name/Utility Nature	VM or Executable	Web-Based
Labtainers	✓	
CyberCiege	✓	
PicoCTF		✓
DETER Labs	✓	
VMI	✓	
Concept Maps		
CyberWar Lab	✓	✓
Tele-Lab	✓	
SEED Project	✓	✓
NICE Challenge	✓	✓
Security Injection		✓
TeachCyber		✓
Security Knitting Kit		
EDU Range	✓	
K12CyberTalk		✓
Kypo Cyber Range	✓	
SANS CyberStart		✓
NOVA Labs		✓
OWASP JuiceShop	✓	
Trend Micro		✓
HackTheBox	✓	✓
TryHackMe	✓	✓

Chapter3
IMPLEMENTING CYBER SECURITY INTO THE WISCONSIN K-12 CLASSROOM

This work was pertaining to my initial exploration of the K-12 Computer Science education curriculum to see if there were any cybersecurity content being offered. As per the description offered in the background, there was a widening gap between the supply and demand of cybersecurity professionals. So, my initial thought was exploring the computer science education program for K-12 to see if it would be possible for us to incorporate more cybersecurity related topics into it. This approach would make the younger generation more cyber-aware and potentially spark their interest to further investigate cybersecurity as a potential career path.

3.1 Introduction

Cybersecurity is a young field that has received public attention and become highly valued by organization executives in recent years. In the wake of cybersecurity breaches and attacks on Fortune 500 companies and popular websites, cybersecurity related roles have had high demand throughout the past decade. Even though the demand for cybersecurity specialists continues to rise, there appears to be a supply shortage of cybersecurity professionals across the United States. For example, the state of Wisconsin thrives in the manufacturing, food processing, health, and utility industries. Based on the Verizon Data Breach Report [25], these industries suffered from 653 cyber incidents nationwide in the fiscal year of 2017 alone (utilities: 22, manufacturing: 389, healthcare: 242).

Cyberseek is a collaborative initiative between the National Initiative for Cybersecurity Education (NICE), Burning Glass Technologies and CompTIA. The interactive

website provides detailed and actionable data on the cybersecurity job market across the United States. According to the website "heatmap", 72% of the states within the U.S. have more than 1300 cybersecurity related role openings as of the end of March 2019.

The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) are involved in the development of cybersecurity related standards [39]. NICE, a division of NIST, has published the NICE Cybersecurity Workforce Framework (NCWF). They have also taken the initiative to host educational camps on cybersecurity across many states in hopes of raising cybersecurity awareness and promote cybersecurity as a promising career path. The National Science Foundation (NSF) CyberCorps is a program offering scholarships for service to students studying in preselected university programs. In addition, the Department of Homeland Security (DHS) jointly with NSA have established designations for two-year colleges and four-year universities as National Centers of Academic Excellence (CAE). If such an institution satisfies rigorous requirements, it can earn the CAE designation with a focus on Education, Security, Research or Cyber Operations.

As of 2019, when this work was initially published, only five institutions that offer cybersecurity programs are accredited by the Accreditation Board for Engineering and Technology (ABET): the U.S Naval Academy, U.S. Air Force Academy, Towson University, Southeast Missouri State University, and University of Central Missouri. The Joint Task Force on Cybersecurity Education, which is a collaboration among the Association for Computing Machinery (ACM), the IEEE Computer Society (IEEE CS), the Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8), launched the 2017 Cybersecurity Curricular Guideline that attempts to define the field of cyberse-

curity and list the requirements for a major in this field. However, currently higher education institutions often categorize cybersecurity as a concentrated discipline under computer science or information technology and offer elective topics courses to their students.

Despite the efforts undertaken at a national level, most of the initiatives have not yet affected the primary and secondary school (grades "K-12") environment. In this paper, we explore the challenges that are preventing local government agencies from raising cybersecurity awareness and we provide potential solutions to address the identified issues. In addition, we discuss current practices and efforts that are sponsored by the government to spark students' interest in cybersecurity practices and exercises in hopes of addressing the global issues of defending the cyberspace and closing out the skill gap that is ever-increasing throughout the past decade. We finally encourage and identify opportunities for all residents to get educated on privacy and security.

3.2 Current Challenges

Multiple factors have contributed to the formation of the workforce gap that we have observed during the last decade. In this section, we list contributing factors: limited security curricula content in K-12 classrooms, lack of effective training methods for teachers, lack of programs or other initiatives that promote cybersecurity principles in the state of Wisconsin, and lack of cyber risk awareness among residents. We also discuss the consequences of each of these factors.

3.2.1 Limited Security Curricula Content and Educator Skills

The Wisconsin Standards for Computer Science were approved by the state Department of Public Instruction in June of 2017 [91]. The development committee explicitly included cybersecurity related topics throughout the K-12 grades. However, the current adoption rate of this framework is low in the state of Wisconsin.

As a "local control" state, it falls to each of the 446 individual public-school districts to act on academic standards approved by the state. As a new academic standards area, many school districts have struggled to understand this unfamiliar content, or to find qualified teachers that can teach Computer Science.

Recent pushes by the PUMP-CS Project [75] have used funding from the National Science Foundation and national non-profit Code.org to drive up the number of well-prepared K-12 computer science teachers. This includes professional development for Computer Science Fundamentals (CSF) [30] for K-5 students, Project GUTS [47] and Computer Science Discoveries (CSD) [29] for middle grades and Exploring Computer Science (ECS) [42] and Computer Science Principles (CSP) [31] for high school students. Despite rapid strides that have more than doubled the number of CS teachers in the state in the past five years, more than 80% of public schools still lack any identified computer science teachers or coursework.

Where computer science curriculum is present, there are frequently elements of cybersecurity also in evidence. For example, in the CSF curricula [30], one of the courses designed for first graders enables the students to learn about their digital footprints and how to stay safe when visiting websites. Students who are in third grade learn what information is appropriate to share online and what should stay confidential in the digital citizenship course. The CSP course [31], which is designed for high school students, contains lesson plans oriented around the concept of encryption to provide the students the opportunity to explore practical measures to encrypt sensitive information.

While some cybersecurity concepts such as the CIA triad (Confidentiality, Integrity, Availability) can be more easily understood, techniques such as address resolution protocol (ARP) poisoning, domain name service (DNS) spoofing, social engineering, and malware analysis are more technical and best understood through

practice and demonstrations. K-12 schools do not typically have the resources and expertise required to educate students through live demonstrations.

More than 2,000 Wisconsin school teachers have participated in some level of computer science professional development with Marquette University in the past five years. However, organized efforts to raise awareness and train teachers on cybersecurity are sporadic. There are several websites and tutorials that provide security training such as Pluralsight, Cybrary or even industry expert hosted YouTube channels such as Loi Liang Yang, John Hammond, Network Chuck, and David Bombal. However, those tutorials are often not well organized or are subscription-based [2, 13, 20, 43, 67]. Teachers should be supported to dedicate time and effort into cybersecurity training. In addition, considering that Cybersecurity is a new discipline, and that it consists a wide range of topics, the shortage of professionals interested in hosting a cybersecurity training workshop to train and equip teachers is an additional challenge.

3.2.2 Lack of Awareness from Non-Technical Residents

Technological advancements are progressing with speeds that are too rapid for most consumers to be able to follow. Internet connectivity is increasing, and many aspects of our lives now involve cyber infrastructure: from grocery shopping to managing the brightness of light bulbs and the temperature of thermostats at home. The habitual reliance of people on online connectivity has increased our vulnerability to cybersecurity risk since more consumers have not had the time to educate themselves on the risks of new technologies. Not many realize that a connected device can become a relay sending unwanted traffic to a specific destination or be at the receiving end of unwanted traffic that could paralyze an Internet of Things (IoT) device. This lack of awareness impacts the propagation of knowledge into the younger generations, since older adults are not able to advise and train their children.

3.2.3 Limited Collaborative Efforts

Several organizations in the private sector have allocated resources to train their employees on cybersecurity. For instance, in response to the breaches that took place in 2014, JPMorgan Chase indicated that they intend to spend 250 million on digital security annually [76]. In the state of Wisconsin, Northwestern Mutual (NM) has openly expressed interest in promoting security and information risk management. NM has been actively cultivating local talent through the STEM outreach program. In December of 2017, they invited local high school students to participate in a risk management and security topic-based capture the flag game for students to demonstrate their capabilities to function in teams and solve security related challenges in a competitive environment under limited time [57]. Nevertheless, the overall collaboration across Wisconsin is still considerably limited.

3.3 Current Efforts and Resources

While there exist several challenges that are preventing the cybersecurity workforce from growing systematically and consistently in Wisconsin, government agencies and other organizations do offer some resources that enable the students to get exposed to cybersecurity concepts and principles at an early age. We discuss those resources that are available to school districts across the state of Wisconsin.

3.3.1 AFA CyberPatriot

CyberPatriot is the National Youth Cyber Education (NYCE) program created by the Air Force Association (AFA) to inspire K-12 students towards careers in cybersecurity or other science, technology, engineering, mathematics majors that are critical to the nation's future. The CyberPatriot program primarily targets middle and high school students and presents to them a ten-unit curriculum aimed to educate the students on concepts such as cyber ethics, online safety, computer security and file protection. The students are also eligible to participate in team competitions

that test the students' ability to identify Windows and Linux system vulnerabilities and fix them. In addition, they are also presented with tasks related to virtual networking. The difficulty of the challenges presented in the competitions increases as the participants advance further into the competition [4]. In the 2019 school year, Fifty-two teams of various skill levels represent Wisconsin, and in 2021, Marquette University collaborated with the ROTC-Air Force to offer training to three additional teams that were interested in participating in the CyberPatriot program.

3.3.2 GenCyber Summer Camps

GenCyber is a summer camp program sponsored by both the National Science Foundation (NSF) and the National Security Agency (NSA). The term GenCyber stands for "Inspiring the Next Generation of Cyber Stars" and the program provides a summer cybersecurity camp experience for students and teachers at the K-12 level. The goal of the program is to increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation. This is one of the government's proposed solutions in addressing the shortage in skilled cybersecurity professionals. This summer camp is open to all students and teachers at no cost. Wisconsin was one of the last handful of states to participate in GenCyber. The first camp was hosted in the summer of 2017 by the University of Wisconsin Green Bay. In the summer of 2018, two additional GenCyber camps were hosted at Marquette University and the Waukesha Country Technical College (WCTC). The University of Wisconsin Green Bay hosted a GenCyber camp in 2020 and Marquette University also successfully hosted a virtual GenCyber camp in 2021 [6].

3.3.3 Private Sector Training

The Infosec Institute, which is headquartered in Madison, Wisconsin, was founded in 1998 by information security instructors that built a business offering top tier quality training experience to their students [7]. Although the service is not free, this

resource provides the means to individuals wishing to receive professional security training from instructor led courses and assistance on the preparation of their professional certification examinations through online test banks and exercises. There are also other Wisconsin based companies offering cybersecurity training to another organization's employees (e.g. Barracuda PhishLine).

3.3.4 Nationwide Resources

The OWASP Foundation is a non-for-profit organization dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. The foundation provides tools, documents and chapters that are free to anyone interested in improving application security. OWASP also maintains an open-source web application challenge-based learning (CBL) tool named OWASP Juice-Shop [10] that was built intentionally vulnerable to the top ten most common vulnerabilities within web applications as identified by OWASP.

CyberStart is a suite of challenges, tools and games designed by the Sans Institute to introduce young people to the field of cyber security. The Department of Administration in Wisconsin collaborated with SANS Institute on identifying students who may be interested in cybersecurity. This is done by inviting students to participate in the shortened version of the CyberStart challenges and solving problems in the topics of open-source intelligence, cryptography, web application exploits, forensics, binary attacks, and Linux related challenges [11] [3].

The Open Cyber Challenge Platform (OCCP) is a free, configurable open-source virtualization platform for cybersecurity educators. It is designed to provide a controlled scenario in cybersecurity areas including network defense, penetration testing, incident response, malware analysis, digital forensics, and secure programming [9].

TeachCyber [12] is a website that provides free lesson plans and hands on practice materials on foundational computer science and cybersecurity skill curricula organized

by grade levels based off the national K-12 Computer Science Framework in response to the rising need for security. Similarly, C5 Colleges (Catalyzing Computing and Cybersecurity in Community Colleges) focuses on raising awareness for students that attend community colleges. This NSF funded project provides free modules that are in alignment with the ACM Computer Science Curricular guidelines. Topics include applied cryptography, secure scripting, cyber threats and countermeasures, cybersecurity principles and responsible software development. Clark Center is a more recent open-source library funded by the NSA to advance the state of cybersecurity. The contents on this library feature cybersecurity and data science curricular modules that are freely available. Instructors can also upload content and course manuals for other teachers to use. Contents on this library are typically reviewed by either the C5 or the National Cybersecurity Curriculum Program [5].

Slightly more advanced are the following three hands-on resources. The SEED Labs [36], designed and developed by Dr. Wenliang Du at Syracuse University under an NSF grant, contain a variety of guided exercises on numerous cybersecurity topics. The Naval Postgraduate School has developed Labtainers, more than 40 exercises and tools to build more. It has also developed CyberCIEGE, which is an educational video game. [82].

Lastly, the National Initiative of Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST), is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. NICE has been hosting the NICE National K-12 Cybersecurity Education Conferences, an effort initiated in 2015.

3.4 Potential Solutions

Based on resources that are currently freely available, we have identified components, which are crucial to the success of establishing a sustainable and consistent

pipeline that will enable students to get exposed to the field of cybersecurity. With the idea that both the citizens and the government each have their due diligence to ensure the success of the proposed solution, we propose solutions that correspond to the cybersecurity challenges faced in Wisconsin in particular.

3.4.1 Incorporate CS Standards into the Existing K-12 Curricula

K-12 schools in Wisconsin need to adopt rapidly with the already established computer science standards. For example, in the framework under the NI.1 standard, ("Students will understand the importance of security when using technology") [91], learning priority NI.1.A states that students in the K-2 grade band are instructed on how to use secure practices, such as passwords, to protect confidential information. Students between the grades 3-8 are supposed to be instructed on the development of strong passwords and analyze the risks associated with the usage of weak passwords. Moreover, under learning priority NI.2.A, students begin their exploration of how packets are sent and travel through the network, which is one of the key points that will help them understand how malicious users implement network-based attacks. Additional cybersecurity concepts such as the CIA triad, exploration of security policies, encryption practices and brief discussions on ethics associated with hacking are all included within the computer science standards for students throughout the K-12 grade bands to explore and learn.

It is critical for the state to further promote the benefits of the computer science standards as well as to encourage and equip school districts to adopt specific curricula that meet the standards. The information could help students to understand risks within cyberspace, and to learn more about security related knowledge progressively over the entire K-12 sequence.

Apart from making children aware of the cybersecurity risks and helping them to understand procedures to protect themselves and their personal identifiable data,

this exposure will also enable them to pursue a career in that field. In addition to the contents covered within the computer science standard, motivated teachers can incorporate additional concepts such as counter measures against trojan viruses, phishing, and ransomware to help the students understand how to properly prevent themselves from becoming the victims of such threats.

3.4.2 Focused Professional Development

State-promulgated academic standards are a foundational piece required to promote broad acceptance of computer science content, and cybersecurity concepts. Wisconsin is only the ninth state to adopt model computer science academic standards for K-12, and the last version includes enhanced cybersecurity content beyond what was recommended by the computer science teachers association (CSTA) K-12 standards. However, in the absence of effective professional development for teachers, standard documents alone are unlikely to directly impact students in the K-12 classroom. Teachers in practice function as the first line of defense if information security contents are to be integrated into the curriculum. Adequate access to content training and support tools will help prepare them to respond to any potential issues or questions that the students may be having. While in many content areas, it is supposed that a little exposure is better than none. Cybersecurity is one domain in which poorly developed training or poorly executed curriculum could cause more harm than good.

We understand that most teachers have ample issues to deal with already; Therefore, we propose that an educational curriculum to be created to provide the teachers access to carefully vetted training materials. Marquette plans to host quarterly workshops to inform, update and educate participants on new security knowledge and concepts. More importantly, our workshops will allocate time for teachers to incorporate the newly adopted content into their existing curricula for conveying this complex

information to their students. Prior experience in a similar context has shown that this shared lesson planning and content assimilation time is an essential factor in effective classroom transfer [21]. Furthermore, our team has deep experience launching other computer science curricula in scores of school districts across the state.

3.4.3 Cybersecurity Exercise Test-Bed

In response to the ideas mentioned in the previous subsection, we further propose the development and construction of a cybersecurity exercise test-bed. With this, it will allow the teachers to better conduct live demonstrations for the students without having to worry about the configuration and set up of both the hardware and software components. The tasks and exercises within the cybersecurity exercises test-bed will adhere to the performance indicators as described in the computer science standards. Terms and instructions will also be designed around their grade band to ensure they are age appropriate and will not pose challenges for the students to understand the task at hand. Each exercise topic will include instruction for teachers and a step-by-step user operation manual for the students as they operate and obtain hands-on experiences with these topics.

The benefits of this proposed solution include: all operations are conducted in a sandbox contained environment where students will not be able to extract files from the test bed environment (their handcrafted Trojan files for instance); the software packages needed for exercises will be pre-installed, which helps to prevent them from installing powerful tools onto their own computer and utilizing those tools to cause harm to their peers that may not be aware of their newly obtained skills. Not only will it provide the teachers the instructions they need to guide the students through the exercises, but it will also provide teachers and students with both offensive security and defensive security experiences to ensure that they are aware of countermeasures that can be utilized when they suspect that they are under attack.

3.4.4 Cyber Sessions for Older Adults

Cybersecurity and cyber risks may be unfamiliar terms for many older adults. Although their Internet presence may be limited to basic email exchanges and web browsing, older adults are prone to cyberattacks due to the lack of relevant knowledge. To help raise cybersecurity awareness around all population groups, we propose the development of information sessions or bootcamps that target various age groups to spread cybersecurity knowledge. It is important for educators to recognize that information sessions need to vary in both content and pedagogy based on the audience's age and cybersecurity knowledge. The development of organized training efforts specifically targeting the older adults are of high significance as it helps prevent cyber criminals from abusing the personal identifiable data that they may have obtained from these individuals through email phishing attacks and click-baits.

3.4.5 Workshops for Students

Efforts such as classes, bootcamps, summer camps and competitions are fairly limited in Wisconsin, but efforts such as GenCyber are gradually providing the students who may be interested in security to have the opportunity to learn. We propose that the number of summer camps that focus on security topics should gradually increase. One way to accomplish that is by having teachers host summer camps based on the concepts included in the computer science standards.

The additional hours teachers spend will not only enable the teachers to become more familiar with the contents, but also help to broaden the coverage on cybersecurity awareness across the state. As a result, such effort will certainly lead to great improvements in terms of increasing cybersecurity awareness for the youth and their households.

3.4.6 Professionally Certified Training Bootcamps

Another solution that could help address the security expert shortage that we currently face is to collaborate with local corporations. Corporations need security experts to help secure their commercialized products. This collaborative effort between the organizations and the community would enable the local corporations and organizations to identify talent through the offering of professional instructor led training in the form of a bootcamp. At the conclusion of the bootcamp, the organization may provide the fitting participants with attractive initiatives such as part-time or full-time career opportunities, training plan vouchers or reimbursement of the participant's first attempt on a professional certification exam. The establishment of this collaborative effort will help encourage the local students and security hobbyists within the community to consider turning cybersecurity into a career and thus indirectly addressing the security expert shortage issue for both the sponsoring corporation and the state of Wisconsin.

3.4.7 Build Your Own Lab Environment for Experiments

In the current digital dominant world, much information and demonstration videos can be found online, although the information may not be well structured. We propose providing workshop consultations to help individuals interested in learning more about security to build their own isolated virtualized environment for experimentation of various toolkits. While creating a virtualized environment is not too challenging, knowing what to install and learning how to use some of the security toolkits that are available may not necessarily be easy. As a result, we propose the establishment of a security workshop that focuses on helping interested individuals. Not only will it build their own experimental security laboratory with various operating systems installed, but also provide them with lists of resources that would enable them to learn more about the proper toolkits they need, such as Nmap for port scanning, Armitage

or Metasploit for system exploitation and John The Ripper or Hydra for password brute-force cracking. Individuals would now be able to experiment with security tool by having a laboratory of their own and a recommended list of tools to use. This will enable them to launch an attack against other systems that are located on an isolated virtual network within the laboratory to gain more exposure and experience through these hands-on exercises at home.

3.4.8 Expand Challenge Based Learning Environments

Challenge-based learning is a learning methodology that is specifically applicable to learning security principles. In this competitive learning method, participants attempt to solve as many challenges of various topics as they can within a time frame. Those challenges include cryptography, reverse engineering, web exploitation, forensics, binary exploitation, and general computing skills. Research studies [28] have shown that the CBL environment encourages students to collaborate and operate cohesively together as a team, understand security concepts through hands on practice, and help students identify their knowledge gaps through the participation of timed capture the flag competitions. In addition, research work also demonstrates that most participants feel more confident handling security issues and or instructing others on security topics after they have gone through a cycle of challenge-based learning [28]. Therefore, for individuals who may be interested in becoming security experts, challenge-based learning is an appropriate starting point. There are many "capture the flag" (challenged-based learning) events that takes place year-round for participants of all age groups nationwide. If the development of a challenge-based learning platform is too difficult, engaging in the CTFs that are freely available online is also a viable alternative for individuals who wish to learn more about cybersecurity. For the above reasons, we recommended the department of administration in the state of the Wisconsin to develop a systematic challenge-based learning platform that

enables students of all age groups interested in learning more about cybersecurity to participate in the program. This will ensure satisfactory coverage in the effort to raise cyber-security awareness across the state and help students who may be interested in a career in cybersecurity receive proper training and experience before they graduate from high school or college.

3.5 Concluding Remarks

This chapter has described some of the challenges that Wisconsin has been facing that prevent the cybersecurity workforce from successfully expanding. By identifying the challenges and potential resources that are available, we identify the need to create a cyber security curriculum that is all age appropriate for students and teachers in Wisconsin. We propose the creation of a tool that enables the students to learn more about cybersecurity through the challenge-based learning methodology. Since the teachers within the K-12 school systems are critical in the success of a more cyber aware population here in Wisconsin, they need to be enabled to provide students with enough knowledge and skills so that students can establish proper cybersecurity practices. Finally, we outline ways though which older adults can be encouraged to get educated on matters of privacy and security.

Chapter4
AN AUTHORING PROCESS TO CONSTRUCT DOCKER CONTAINERS TO HELP INSTRUCTORS DEVELOP CYBERSECURITY EXERCISES

In attempt to create more cybersecurity related exercises, I collaborated with the faculty and project members of EDURange and worked on developing cybersecurity exercises using their pre-built docker architecture. This work describes how we developed an authoring process to help instructors create cybersecurity exercises.

4.1 Introduction

The development of new security exercises is a cornerstone to cybersecurity education. Several platforms for teaching cybersecurity through hands on exercises have been developed in the last 15 years. Many of them have more than a dozen exercises. Yet, they are not truly scalable from the perspective of developing a community unless they facilitate the ability of knowledgeable users to modify existing exercises or contribute new ones. There are only a couple of frameworks that are designed to make this easy. In this paper, we examine the creation of two quite different exercises to observe the current state of the art in tools that help instructors to create their own exercises in the domain of cybersecurity, which has some specific requirements. Some of the specific requirements are: 1) exercises may rely on installing specific versions of software, including ones with vulnerabilities, 2) software environments need to be complete, i.e. more than just the vulnerable applications, and 3) exercises should run on a variety of platforms, e.g. cloud and desktop.

Even when a platform provides a mechanism for creating exercises, there still is going to be a learning curve. We have tried to make that learning curve as gentle

as possible in our platform. Our platform uses two powerful tools Docker containers and Terraform. These are commonly used in IT for creating and configuring flexible computing environments. The use of Docker containers is becoming more popular than the use of virtual machines (VMs), especially when multiple virtual computing environments would be needed. Similarly, Terraform is becoming popular because it works with multiple cloud frameworks to configure hardware and software and interacts well with Docker. We have constructed a layer on top of both of those, to minimize the prerequisite knowledge that instructors would need to create or modify exercises. A prerequisite that instructors would need is some familiarity with the Linux command line interface. However, we believe that this is less of an issue for most cybersecurity instructors. Thus, we have not developed a graphical interface for creating exercises, although that would certainly be possible.

The two exercises that we developed were Ransomware and Web Fu. The learning goal of Ransomware is to teach some of the basics of cryptography in a context that would be truly clear and motivating to students. It also promotes the security mindset because it illustrates a failure mode. One thinks of cryptography as protecting secret information, but in this context, it is about abusing it to prevent the owner from accessing data. Web Fu teaches the basics of SQL injection.

This exercise was developed as a gentle introduction to the topic and as a proof of concept. While there are many CTF challenges that are based on SQL injection, we wanted an exercise for an introductory Web security course that would use a Web interface rather than the command line. In our experience, students sometimes struggle because of their limited understanding of SQL databases. While there are many tutorials on SQL, they focus on how to use the language rather than how to abuse it. We also wanted students to be aware of code injection and to recognize code as data. One of the goals for the developers of our platform was to demonstrate that

it could accommodate a wider range of exercises, not just ones limited to using the command line interface

4.2 Related Work

The other academic frameworks that we consider are Labtainers, EDURange, DETER Lab, SecKnitKit, Security Injections, NICE-challenge, NCL, and KYPO. Out of these academic frameworks, the two that have addressed the issue of user-generated scenarios most clearly are Labtainers [48]and EDURange [51, 87, 88]. Labtainers has a collection of base Docker images that can be combined in a variety of ways to produce new exercises using Docker-Compose. This has some pros and cons. One advantage is that they have implemented a GUI that is aware of the base containers and allows the user to select them and compose them. The disadvantage is that if the user wants to go beyond the existing types of exercise, then they need to be familiar with Docker-Compose syntax, craft a unique Docker file, and define networking rules from scratch. Labtainers can be used anywhere that has Docker installed, which could be a laptop or a Cloud environment.

EDURange takes a hybrid approach to this problem by providing templates for instructors to modify while also allowing the use of custom container images. As a result, instructors can either provide their own pre-configured images, or extend the base SSH server with a list of their own bash scripts. One disadvantage is that there is no GUI, so exercise designers need to be familiar with basic Docker commands. Nevertheless, they do not need to know Docker Compose and instead can use JSON to combine Docker commands. EDURange can be used anywhere that has Docker installed, which could be a laptop or a Cloud environment.

DETER Lab [62] also allows instructors to design their own exercises. It uses a combination of bash scripts and NS scripts. The NS scripts are not a commonly used format. There is not much documentation on the procedure for creating new

exercises. Plus, there are also hardware limitations. It runs on a specific platform and during times of heavy use, hardware nodes may not be available. NICE Challenge has on the order of one hundred exercises and has a staff of developers. The advantage for the instructor is that there is no expense and need little effort to use the exercises. The disadvantage is that it is not possible for instructors to modify or contribute exercises, to host exercises on their own hardware resources. The latter could limit scaling because the hardware resources are not easily expanded.

Security Injections [54], SecKnitKit [77], and SEED [36] are also valuable. While an instructor cannot contribute or modify exercises, they are scalable in terms of the number of instances of a course. Security Injections does not require provisioning of VMs or containers, so it is easier to use than the other systems. SecKnitKit does use VMs that can be run locally on the instructor's hardware. SEED has one large VM that the students run and an associated textbook. KYPO [86] is a remarkably interesting system in terms of the exercises provided and it is open-source. However, it is not easy for instructors to add exercises or to run it on their own hardware. There are several free non-academic frameworks such as Portswigger and overthewire.org. Instructors cannot modify or extend them, and they are harder to integrate into a course, in terms of assessment and prerequisite material. The tools that make our platform extensible, portable, and scalable for instructors are Docker and Terraform. Section 3 steps through the process one would go through in our platform to create a new exercise. Then, in sections 4 and 5, we discuss the requirements for those exercises.

4.3 Recipe for creating new cybersecurity exercises

Developing good hands-on exercises and homework assignments can be a difficult and time-intensive task. One standard method is backward design [90]. The author of an exercise would start with specifying the learning goals and develop a high-level

description. They would translate the goals into concrete objectives and create a plan for assessing them. In the case of hands-on exercises, the objectives and assessment are often realized as tasks and criteria for determining that those tasks have been completed satisfactorily.

Once the tasks have been described, they need to be implemented by creating the hardware and software environment. In our platform, we use a collection of containers running on Ubuntu. The author would need to describe each one in detail. They would specify the software and services they provide. They specify accounts for students and services and create files/artifacts that the students need to retrieve. The author needs to configure the network, e.g. assigning IP addresses and ports. All of this should be done using scripts, so that it is easy to modify the exercise and create new containers. Another approach that we have seen is to start with an existing virtual environment, where the instructor wants students to learn to work in that environment.

In this approach, the instructor must then create the goals and learning objectives, usually based on introspection to understand why that environment is important and what the essential goals and objectives are. Then, the author could generate tasks that would demonstrate those objectives in that environment. An example of such an environment is Metasploit on Kali Linux. A VM is easy to create, and student accounts can be created. A target with some vulnerabilities exists as the Metaspoitable VM. Both can be converted to containers and networked together. Both approaches are reasonable. In practice, we often see a hybrid. The part that our platform can help with in both is to make it easy to configure the virtual environment.

4.4 Developing an SQL-Injection Exercise (WebFu) using the LAMP stack

The goal of this exercise was to teach SQL-Injection in a hands-on fashion. This led to defining objectives, such as dumping tables from a database and bypassing a basic Web Application Firewall (WAF). These needed to be translated into an implementation in a concrete environment. For WebFu, the author chose the MySQL database system, and created the database schema and then the queries. The next section describes the experience of applying the tools in our platform.

4.4.1 Applying the Tools

Applying the tools are complex, but EDURange does offer a step-by-step guide to help instructors apply the tools. Prior experiences are not needed, though it would certainly speed up deployment. First, the author copied Terraform templates from another scenario and changed the container names to match the new scenario name. The author also copied the YAML file containing the assessment questions for the students and the Markdown file containing the scenario's student guide. Of course, the text in these needed to be changed for the new scenario, but that was not difficult. Next, the author pulled the existing our platform base image from DockerHub, which is based on a minimal Ubuntu installation. The author then set up a LAMP stack by extending the image with a) a MySQL database server; b) an Apache web server; and c) a PHP installation. These elements formed the infrastructure of the web application.

After populating the database tables with data (made up of public data sets and the hidden artifacts or flags), the author pushed this modified image to our platform DockerHub repository and edited a line in the Terraform template to invoke it. Lastly, the author wrote a bash script for starting the MySQL and Apache services at scenario launch time and added it to the description's JSON file. The development

of this infrastructure took about a month. However, this set up can now be reused to create a wide range of scenarios for practicing web security auditing skills. Potential labs include a website vulnerable to Cross-site Request Forgery (CSRF), Server-side Request Forgery (SSRF), Cross-site scripting (XSS), Local File Inclusion (LFI), and many other techniques. With the current infrastructure-as-code, the only task left to the author is writing or copying the vulnerable application(s).

On the scenario's development, it must be said that gaining familiarity with the Docker workflow was challenging at first. This was where most of the time was spent, as the author had a background in Linux system administration, but not in container-related technologies such as Docker. Every time the Docker image was changed, a commit needed to be made for the new container which resulted in a new image. Then, this image had to be tagged and pushed to the DockerHub repository. Finally, the instance of our platform had to pull from the remote repository to update its changes. Once these steps are quickly learned and are like Git's workflow, and the method of container deployment results in an agile and effective process. When trying to deploy this exercise in the classroom, the author ran into an unexpected problem. The exercise was being run on a cloud environment, but students needed to connect through the school's network through HTTP.

Students were experiencing problems connecting, and it turned out that an internal firewall was blocking malicious traffic (i.e., the SQL injection strings) over plain-text HTTP. The solution was to use HTTPS, but we wanted to avoid requiring an instructor to create a certificate for HTTPS. Using Terraform's bind property for SSL/TLS support and redirecting ports (from the container to the host) were the most significant changes. The former allowed us to easily add HTTPS support for the web application. The Let's Encrypt directory with the certificate and the private key on the host VM was made available to the guest container through a bind mount.

This removed the need for creating and maintaining additional SSL certificates. More importantly the entire process occurs at the scenario's creation time, thus not having the certificates stored in the repository's image, ensuring confidentiality. Lastly, the port redirection implemented with the Terraform API spared us from having to write and maintain iptables rules. This was particularly helpful due to how easy it was to add redirection rules in the Terraform file.

4.4.2 Script and Files

This exercise required a working database. The tables were created using scripts. How and where to run the scripts was specified in a JSON file. The author found it is easy to use an existing file for another exercise as a template, but ideally this would be produced by a user interface that would prompt the user for the information and produce the JSON file. The files for an exercise are organized into three categories. The JSON file defines a list of the containers to be provisioned for this scenario, as well as three categories of files that are used by Terraform to create the container: user files, system files, and global files. For each type of file, Terraform will take different actions to copy or execute them to prepare the scenario environment. Terraform copies a list of "User Files" into each students' home directory, "System Files" are executed once at scenario launch time for system configuration, and "Global Files" are added to the "/bin" folder so they can be run as bash commands.

4.4.3 Using Docker and Terraform in WebFu

Terraform is a scripting platform most used by system administrators and Cloud engineers to create and configure (provision) virtual machines (VMs) on all the major Cloud infrastructures, such as AWS, Azure, and Google Cloud. In the case where networks of VMs are needed, Terraform can be used with a VM orchestration configuration file which is like the Docker yml-based language for defining networks of containers. One of the common uses of Terraform is to modify the state of a VM run-

ning on a Cloud by applying rules while the VM is running. This takes the place of the administrator logging in to all VMs in the network and running update commands. However, this is not how we are using it.

Instead, we focus on rapidly setting up containers and configuring them. Our approach was to create a base Docker image and write configuration files to customize the image for each specific exercise. One could imagine using Docker scripts to do this, but there are potential problems with synchronization. For example, when configuring a network, some steps need to be done before others. Instead, our platform uses Terraform scripts to create containers and network them together. In this case, the network must be configured before the containers can use it, otherwise there will be errors. Docker scripts do not provide a simple and reliable way to do that, while Terraform does. The Terraform scripts can be generated by our platform as JSON files. This makes it easy to implement a user interface that allows instructors and contributors to create their own scenarios. In our platform, we have defined our exercises using Terraform templates that can be copied and adjusted. At the lowest level, this allows exercise developers to write bash scripts which modify an existing Docker image to create the desired environment. In practice, once contributors have written their desired scripts, they can just list them in JSON format to apply them and extend the Docker image. This can be contrasted with other testbeds, in which manual editing of a Dockerfile or a NS file is required in addition to prepare low level scripts. Alternatively, contributors can create their own Docker images and incorporate them by modifying a single line to reference them.

Two Terraform templates are used to configure the virtual network. One of these templates defines how the host appears to the external network. It defines the IP address and external network, allowing Docker to expose ports publicly, as well as an internal network for hosting potentially vulnerable containers. Secondly, at least a

single container Terraform file must be copied, which in the case of most our platform exercises is the file "nat.tf.json". All of this can and will be automated. This file provisions a container with a basic SSH server running. The container is connected to both the external and internal networks. Terraform will automatically add any of the students' user accounts to it, as well as any additional scripts listed in the JSON User Files.

For all the base Docker containers, SSH must be installed because Terraform uses it to install files. For most of the exercises, SSH is also used by students to interact with the container. In one of the new exercises, VNC is used for student interaction. At this point, with a new folder created and templates copied, contributors can make a choice of how to proceed based on the requirements of their scenario. If their scenario does not require the installation of new software or specialized containers beyond the capabilities of the base SSH server, then they can write bash scripts and list files in the JSON description file as their only means of customizing the scenario. On the other hand, if they need containers that are running databases, web servers, or other complex applications, then they can choose to build a Docker image that fulfills their requirements and list that image in the Terraform file instead of writing any configuration scripts. With those steps done, the scenario would be ready to be tested. In the remainder of this paper, we describe the experiences of two different authors in creating new exercises.

4.5 Developing a Ransomware Exercise

Amid ever-increasing incidents that are caused by ransomware attacks around the world, it is critical for students who are learning about cybersecurity to understand that a ransomware attack is based on asymmetric key encryption. This exercise mimics the execution of a ransomware attack. The goals are for students to learn how an adversary can weaponize public key cryptography and how that can be deployed

on a vulnerable system. The newly added ransomware exercise will introduce the foundations of ransomware and asymmetric key encryption to the students. Through this scenario, the students learn about the generation of asymmetric key pairs, how the asymmetric key pairs can be weaponized and how end users can potentially stop such an attack before it fully executes its corresponding cyber kill-chain.

4.5.1 Converting an Existing Exercise with Novel Requirements

This is an example of converting an exercise that was developed independently and then ported to our platform. The first version of the exercise was developed on Windows [41]. It consists of collection of Python scripts that installed a key pair, encrypted files, popped up some windows, and then decrypted the files if the user complied with some file modifications. The author developed this into an exercise with learning objectives and tested it on a Docker container for Windows.

The last step was to integrate the container into our platform. We made some adjustments and converted the script into a Linux compatible program to ensure that it can be deployed within our platform. We also adapted an existing Ubuntu-VNC desktop Docker container [40] to make the experience more realistic while providing the users a visual effect as the program gets executed. This was a significant extension because the previous exercises had only used the command line interface with SSH, so this involved a major change to exercise structure. The authoring process took about two weeks (part-time) starting from the Python scripts for Windows.

4.6 Results

The development of the SQL-Injection exercise was spread over 1-2 months. At the end of that time, it was used in the classroom. Developing the exercise only required about 150 lines of PHP and HTML code, and about 250 lines of Terraform templates, mostly copied. The exercise process was very flexible and iterative because Terraform keeps track of interconnected components. The development of the Ransomware

exercise was even more rapid (two weeks), but it has not yet been tested in the classroom. Most importantly, the ease of importing a unique and pre-existing exercise to our platform illustrates the potential for adding many more exercises that are not just based on the current ones. Both new exercises introduced completely novel interfaces for student interaction - a web application in the case of SQL-Injection and a VNC desktop in the case of the Ransomware. In both cases, the authors had access to our platform developers and were able to ask questions, but now this expands the range of topics that can be taught.

4.7 Conclusion and Future Work

Two new exercises were developed rapidly by people who were not familiar with the platform framework, which demonstrates that the framework has the flexibility for instructors to create new exercises. In one case, they were able to learn enough about the framework and develop an exercise in a matter of weeks. For the other case, it took about 2 months. In both cases, the authors had some specific learning objectives in mind: one is teaching SQL-Injections whereas the other is teaching how Ransomware works. They differed in terms of the starting point. In one case, there was already a script that could be used on Windows, and that had to be translated from Windows to Linux and then integrated into our platform. In the other case, everything had to be created from scratch. Potentially most cases will fall in between these two.

We expect that many instructors who teach cybersecurity have some tools that they often use and are familiar with. In that case, constructing a Docker container with those tools and targets would be fast. If they are already using Linux, then the integration with our platform could be exceptionally fast. If they are developing something new to them, and the scope is reasonable, they should still be able to develop something in less than one term and have it ready for the next one.

This process has uncovered several new features that we want to add to our platform. We plan to automate all of file copying and editing described in Section 3. Beyond that, we would create a GUI that could run those scripts. In addition, the Ransomware author has thought of a new exercise to be added. The exercise was inspired by the challenge-based learning pedagogy where an improperly configured Linux image and applications will be presented to the students. By mitigating the challenges or adjusting the configuration of the image, the student will receive flags to enter the forms within our platform for a score. This exercise will add system security and proper privilege configuration of users and the file system infrastructure to our list of topics. In addition to the image, a descriptive list of exercise objective will be provided to the students as a guiding reference so that they are properly informed of what the ideal configuration should be.

Chapter5
MOBILE CYBER-WARFARE RANGE

This was a joint collaborative effort with the WICTRA (Wisconsin Cyber Threat Response Alliance) and a team of senior design students at Marquette. Within this work, we took a few of the intentionally vulnerable system VM images and reverse engineered it onto ARM-based Raspberry Pis to increase the portability and scalability of the cyber-warfare range. This is a project that I intend to continue in the future because a portable cyber range is going to be a fantastic addition to any cybersecurity classrooms.

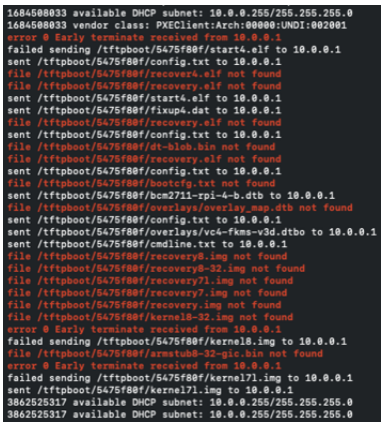
5.1 Introduction

Cybersecurity courses often include interactive exercises instantiated through virtual machines [32, 37, 55, 84]. Engaging with the exercises requires the user to install and configure images, a process that can add a learning obstacle especially to students without system administration experience, typically in the case in K-12 or early college. Providing pre-configured, portable, well-documented cybersecurity scenario containers can benefit both students and teachers.

Reverse engineering the exact source codes, library versions and binaries that demonstrate a particular walk through's combination of vulnerabilities can be painstaking work. Transporting those required combinations to another processor architecture and platform is a further technical challenge. The large body of existing x86 cyber range images and walk through justifies the attractiveness of a smaller, lower cost, more portable, and easily administered cyber range platform of comparable scalability and capability. Our research aims to support an affordable, portable, reusable, and scalable cyber warfare range based on Raspberry Pis [72] where scenario images can

be removed and reinstalled within minutes upon user request based on the scenario selected. The figure below shows the netbooting process of a Raspberry Pi in which we deployed a vulnerable box image on.

Figure 5.1: netboot



5.2 Methods and Preliminary Results

We based our mobile cyber warfare range exercises on existing community built virtual machines like BWapp (a buggy web application) [63] and Mr.Robot [52]. Our interface enables users to request access to available Raspberry Pis for specific exercises. Pi targets receive the needed images and file systems through common Linux services like NFS (Network File System) and TFTP (Trivial File Transfer Protocol) running within virtual machines in the back end. A web power switch enables us to turn off power to the Pis, if a Pi becomes unresponsive during an exercise or must be returned to the "known good" state. A single Raspberry Pi may be requested by a user at any given time, which prevents conflicting access. When a target Raspberry Pi is ready, the user is given an IP address for the vulnerable target so that they may freely engage in offensive activities in a safe sandbox.

5.3 Contribution and Future Work

The primary contribution of this work is a new set of tools and exemplar ARM-based versions of existing x86-based cyber range images that demonstrate the scal-

ability, decreased physical size, lowered cost, and increased portability of a Pi-based mobile cyber range. This type of cyber range is preferable particularly in educational contexts with limited internet connectivity or highly restrictive policies that negate the usefulness of centralized virtual cyber ranges. The Pi-based cyber range is more portable than x86-based predecessor systems and requires much less sophisticated local system administration than virtualized cyber ranges. Our current accomplishments pave the way for additional research to expand capabilities and further optimizations. Hosting TFTP and NFS services on an independent Raspberry Pi rather than a host machine can further decrease size and cost of the mobile cyber range. Slimmer operating system images, such as Raspbian lite, would further improve boot up time of the target Pis. Besides feature and architecture optimizations, we will investigate other vulnerability concepts that can be demonstrated on ARM.

Figure 5.2: Pi Request

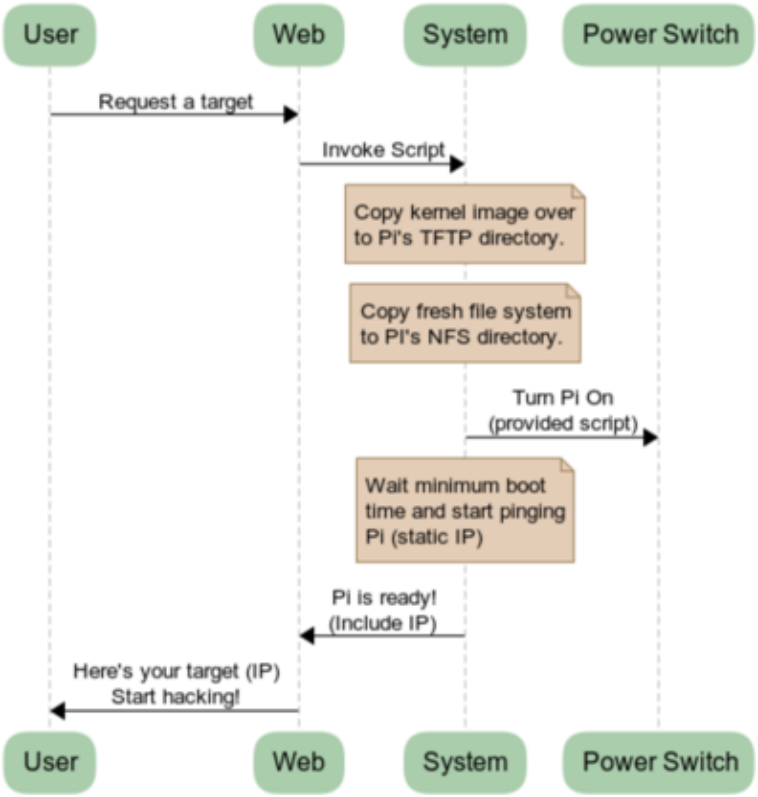
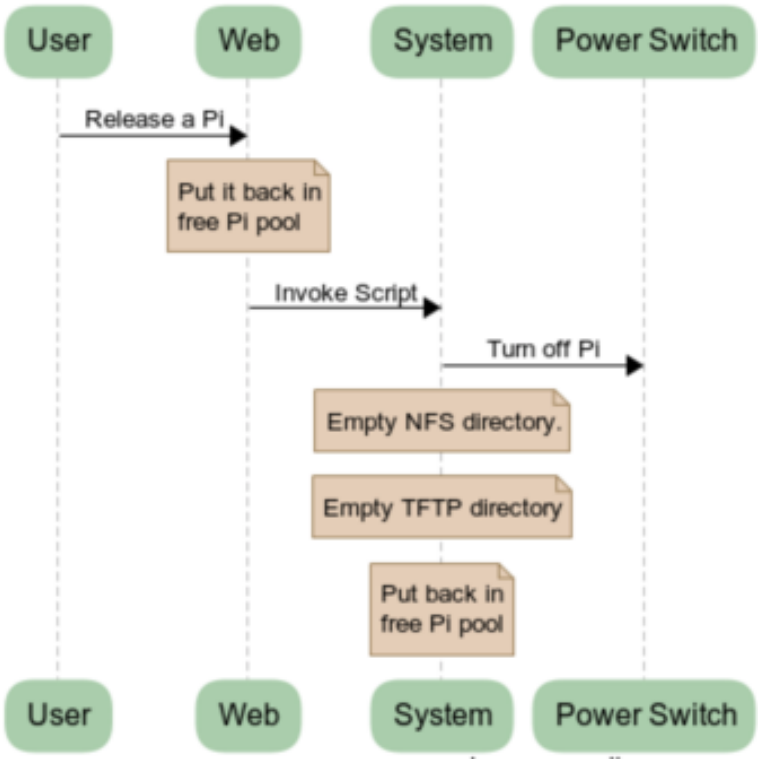


Figure 5.3: PiRelease



Figures 5.2 and 5.3 demonstrates the operation cycle of the cyber range when a user requests for that resource and after the user has finished the exercises and release that resource back into the pool. As shown in the picture, before a student can access the Raspberry Pi, it will invoke an installation script to copy the kernel image and a fresh file system over to Pi's TFTP directory. The Pi will then be turned on and an IP address will be assigned, once the Raspberry Pi become ready, the IP address of the device will be given to the student for use. Similarly, after a student release the Raspberry Pi, the NFS and TFTP directory will be emptied on the Pi, so it returns to the ready for deployment state and re-enters the available resource pool before being turned off to conserve energy. A single range may consist of any number of Raspberry Pi ranges, ideally, this portable range would be able to support the need for a mid-sized classroom to offer each individual student the opportunity to learn actively.

Chapter6
INSTRUCTION METHODOLOGY AND FRAMEWORK COMPONENT

The Adaptive Pedagogy Framework is my proposed solution that would help instructors to educate their students regarding risk management, incident response, and disaster recovery to increase their awareness of those topics. The framework consists of four primary components that can be used at the instructor's discretion to ensure that the modules' efficiency, usability, and flexibility are optimal to help the learners understand specific concepts and topics. The details of each component are discussed below.

6.1 Education Module

The current education module consists of three primary subjects: Risk management, Incident Response, and Disaster Recovery, each of the modules is expected to have corresponding sub-modules. For example, within risk management, a sub-module would consist of lecture material on a specific offensive security tactic such as man in the middle at the link-layer. Such sub-module demonstrate how threat actors can use the tactic and how one may exercise risk management practices at their discretion to increase their defense against such an offensive tactic.

Within each of the education module materials, mini-interaction exercises such as brainstorming challenges or a fill-in-the-blank are incorporated throughout the lecture materials. These mini-interactions enable the instructor to assess student engagement periodically, evaluate whether the learning outcome will be met as expected, and increase student interest through interaction. In addition to the built-in interactive exercises, most education modules offer a quick conceptual recap and a knowledge

check to help students master the new knowledge introduced through repetitions and content recollection. The knowledge check also serves as a small utility for instructors to assess the overall effectiveness of the lecture material and determine whether a concept flashback or additional homework assignment exercises on the covered topics may be necessary.

Table 6.1 and 6.2 below demonstrates the currently available sub-modules that correspond to each of the three primary education modules. Each educational module can be presented as presentations (traditional lectures), pre-recorded videos, delivered through peer learning, or injected into other existing curricula. As shown in the table, each educational module incorporates four sub-modules, including additional micro-modules such as mini-exercises or a deep-dive investigation into a specific topic of interest.

Moreover, the lecture materials about risk management aim to increase the cyber-security awareness of the students by introducing utilities. Specifically, we introduce intrusion detection/prevention systems, fail tolerance systems (RAID), security controls, shared best practices, defensive strategies such as defense in depth, the configuration of firewalls, and the deployment of honeypot. The material briefly introduces the utilities and offers examples of how cybersecurity engineers can implement these specific systems and security controls in real-world settings.

The currently available materials should be accessible and easily adapted by instructors to deliver lectures on realistic risk mitigation practices. However, for some of the available materials to be effective, some requirements may need to be met. Specifically, students may need prior knowledge of network structure, safe online courses, or knowledge of specific terms such as Wi-Fi or VPN to maximize the benefit this set of resources may offer to the students.

The purpose of further categorizing the education modules into sub-categories

Risk Management
Risk Response Methods
Threat Modeling
Resource Protection Management
Link-Layer Risk Management

Table 6.1: Risk Management Education Modules and Sub-Modules

Incident Response	Disaster Recovery
Incident Mgmt Phases	Disaster Recovery Process
Reporting, Recovery	Backup Strategy and versioning
Detection, Response, Mitigation	Backup Validation
Remediation and Lesson Learned	Recovery Site

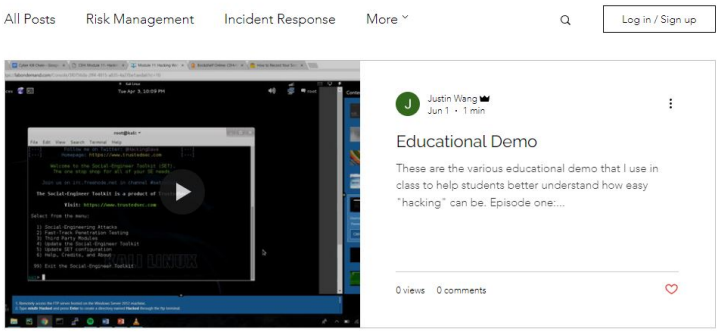
Table 6.2: IR and DR Education Modules and Sub-Modules2

serves the purpose of helping instructor to engage in preparation activities. Specifically, this prevents instructors, especially the inexperienced ones, from feeling cognitively overloaded and indirectly enable the instructors unfamiliar with specific subject content to learn and process the information gradually in a stress-free manner. In addition, the education module's sub-topics may include a smaller subset of topics (e.g., threat modeling) that may involve hands-on live demonstration of utilities to explain the concept better. For instructors to be able to demonstrate, additional prep time will be necessary. Nonetheless, many sub-modules offer instructors the flexibility to utilize different pedagogical approaches to engage their students.

6.2 Educational Resource Web Page

In addition to educational modules, I also created a resource-sharing website for supplementary use. Instructors can redirect their students to the site to obtain additional information for the students to read before engaging in peer education during classroom discussions. Additional information regarding risk management, best practices introduced in the standardized framework, and other relevant cybersecurity news will be available in the form of blog posts for those interested in learning more about cybersecurity on this resource page. The blog posts contain related attachments such

Figure 6.1: Resource Blog



as an instruction for lab exercises, corresponding lecture slides, and demonstration videos. The blogs aim to help students who may be interested in engaging in additional hands-on activities to reproduce the exercise in a semi-guided/assisted manner. The goal is to evolve this resource website into an interactive web component capable of offering short pop knowledge quizzes on the fly for users to test their knowledge and understanding.

As shown in Figure 6.1 below, the blog enables end-users to log in and comment on the specific blog posts they may be interested in. In the example, I incorporated several pre-recorded educational demo videos into the blog post.

6.3 Topic-Oriented Exercises

Topic Oriented Exercises are one of the most critical components within the educational module set as they offer the students much-needed hands-on exercise experiences. The exercises are also the component that enables the instructors to deploy active learning pedagogy within their classrooms. The activities are meant to be short in length with varying difficulties to offer students the means to engage deeply with course content and learn by doing. Small exercises can vary in their presentation formats, and the instructors will have the final discretion to decide how they would like to present the materials. However, instructors can show the material in many ways. For instance, it can be given as a pre-recorded video walk-through or

a homework assignment with key term hints where students may need to conduct additional research. Besides, it can also be adjusted to require the students to deploy a virtual machine and perform a specific task or ask students to work in small teams to generate an investigation report of a particular scenario situation.

In Table 6.3 above, I demonstrated the suitability acronyms used to describe the suitability of delivery methods. Using the acronyms shown in Table 6.3 I mapped a small subset of utilities that offers hands-on exercises for students to the previously discussed content delivery methods. The mapped result is shown in Table 6.4 below. The mapping is subjective based on personal experiences using the mentioned utilities. Still, it should offer the instructors insight into how they can incorporate some exercises into their classroom. For example, the NICE Challenge platform also has several pre-built and challenging exercise scenarios to which the instructors can grant students access. Specifically, challenges such as "incoming zero-days prepare the IDS and IPS," "Dangerous Drive," "Defense in Depth Layer," "Malicious Software," and "Malware aftermath clean-up" are a few of the scenarios that are closely related to the topic of instruction.

Besides the pre-built utilities that offer laboratory exercises, scenario challenges, and pre-built utilities for instructors to deploy and use, I also thought about a few potential exercise ideas that have the potential to become a mini exercise. For example, when covering the risk management module, a possible exercise may be for students to craft a phishing email using the social engineering toolkit on Kali Linux and see if their peers can identify the phishing email that gets sent to them. This exercise will enable students to learn how to distinguish a phishing attempt and take appropriate action when a phishing email is identified. Another example could be setting up virtual machines for students to engage in man-in-the-middle attacks through DNS spoofing or ARP poisoning to learn about the potential risks associated with access-

ing the internet through publicly available Wi-Fi networks. Furthermore, it may be worthwhile to offer students the opportunity to create a disaster recovery plan as if they were a newly appointed CIO or CISO. This project exercise will allow them to work in small teams and create a disaster recovery or plan and business continuity plan using the educational module materials and information they can obtain through careful research.

Table 6.3: Content Delivery Method Mapping

Delivery Method Suitability	Acronym
Excellent	E
Fitting/Fair	F
Not Ideal	NI
Not Applicable	NA

Table 6.4: Delivery Method and Utility Mapping

Tool/Methods	Video Walk through	research assignment	VM lab	projects
Atomic Red	E	F	NA	F
EDURange	F	F	NA	F
Nice Challenge	E	NI	NA	E
Reverse Shell	E	E	NA	NI
Kali-Linux Exercise	E	F	E	NI
SeedLabs	E	F	E	NA
TryHackMe	F	NI	NA	E
HackThisBox	NI	E	E	E

6.4 Adaptive Rubric

Like a lesson plan, a rubric is key to ensuring the students receive insight into potential improvements they can make. The adaptive rubric was designed to assure learners receive standardized and actionable learning experiences. The adaptive rubric helps to ensure that the educational framework remains applicable to assess the effectiveness of the education modules, exercises, and scenario challenge as the scope of the educational modules widens and incorporate more topics of interest. The adaptive rubric effectively determines the best advice or feedback to provide to its

students based on the combination of the answers given by the larger participation pools. When each scenario or combination of submissions is present within a single response (survey or lab reports with missed objectives), appropriate tags will be issued to such a combination. The tag will then be the indicator used to generate standardized feedback when other students submit similar responses. The standardized feedback system will reduce the potential workload on the instructor in terms of grading and providing customized input for each submission which may be extremely time-consuming. Ideally, while the adaptive rubric may offer the learners standardized and actionable feedback, the feedback provides students hints to try different approaches and engage in additional exploratory and active learning. An example of the adaptive rubric is shown in Figure 6.2, where the combination of submissions with tags will offer standardized feedback to students for those who may be meeting a specific subset of conditions.

Figure 6.2: Adaptive Rubric Example

Combination Tag	Student submitted report with two incomplete objectives
A (objective A +C)	For objective A did you try X, Y, Z? For objective C did you see this take place, and did you try options QWER after seeing a specific prompt which may lead to completing the objective?
B (Objective A + B)	For objective A did you try X, Y, Z? For objective B these actions 1,2,3 should have been done to help you achieve the objective.
C (Objective B +C)	For Objective B did you try the following steps? For objective C did you see this specific screen or prompt before proceeding with the following actions?

Combination Tag	Student submitted a report with one incomplete objective and altered a pre-defined condition leading to objective incompletion
A (Objective A +Incomplete)	For objective A did you execute the following the steps? Did you accidentally do this which caused the initial condition to fail a previously passing objective?
B (Objective B +Incomplete)	For objective B did you execute the following the steps? Did you accidentally do this which caused the initial condition to fail a previously passing objective?
C (Objective C+ Incomplete)	For objective C did you execute the following the steps? Did you accidentally do this which caused the initial condition to fail a previously passing objective?

6.5 Assessment Surveys

The assessment of knowledge for the student participants, who voluntarily participated in this research experiment was based on the responses provided. The participants provided answers to each of the eighteen questions I created on the practices of risk management practices, incident response strategies, and disaster recovery methodologies.

I evaluated the student responses following an evaluation rubric that examines the thoroughness of the reaction, the correctness of the answer, and the content coverage or utilization demonstrated through the responses on a full 15-point scale. Each focus is scored on a scale of 0-5 points. The final assessment score is the cumulative value of the scores received for each scoring criteria. Specifically, the scores are issued within each of the requirements depending on the responses' comprehensiveness, correctness, and utility. Generally, 1 point is given if the answer is irrelevant to the context, 3 points if the student offered a generalized summary response without specific details, and 5 points if the response provides a set of correct, neat, and detailed answers for each independent component and examples were given when requested or applicable. Individuals that are interested can find the scoring rubric, the assessment survey questions, and the expected response for each question in detail within the appendix of this document.

6.6 Trial Implementation Instruction Methodology

To test the framework's effectiveness, I used the available preliminary educational framework and resources, visited an upper-division Computer Science course, delivered the lecture content in three introductory programming courses and a mid-tier computer science elective course. Data samples were collected from all these class sessions. To incentivize the participation of the students, I offered extra credits to students who completed the pre-evaluation and the post-evaluation surveys.

The pre-lecture assessment surveys were made available to the participating students approximately one week before the lecture; students were allowed to use online resources to search for answers and help them respond to the survey questions. This setting was intentional as most students do not have any exposure to any of the topics on which the survey questions focus. After the students had finished the pre-lecture assessment survey, two lectures were delivered to students by me regarding the three core subject topics. At the end of the two lectures, the post-lecture survey assessment was made available to the students. I disclosed the detailed results of student performance in Chapter 7; I also offered statistical evidence to prove the materials presented helped the students to increase their knowledge regarding the practices of risk management, incident response, and disaster recovery.

While I gave no specific instructions, it is likely that the students utilized help from search engines to answer some of the questions, thus causing the response results to be potentially biased. I discussed this along with other potential design flaws in the result discussion section of the dissertation. The trial implementation helped me discover several critical issues regarding survey design and content delivery methodology. Overall, the trial implementation of the educational framework not only proved its usability and flexibility but was overall a success that offered insights into potential issues that I should address.

Table 6.5: Tools Used For Trial

Tool Name	Used
Educational Module	Y
Exercise Demo	Y
Interactive exercises	Y
Topic-Oriented Exercises	NA
Resource Web-page	NA
Adaptive Rubric	NA

6.6.1 Participant Recruitment

The participants who voluntarily agreed to participate in this study were recruited directly from the Computer Science undergraduate classrooms. With the permission and properly filed IRB protocol, I recruited the students directly within the classroom as the study's principal investigator. For the classes where I was the instructor, I directly incorporated the risk management, incident response, and disaster recovery modules into my course syllabus using the injection-based education pedagogy. I obtained permission from classes instructed by other instructors to visit their classrooms for two class periods and deliver the framework trial contents.

6.6.2 Data Collection Procedure

Before obtaining any data for the experiment, I requested the instructors to ask the students for their consent to participate. The consent form is also included as part of the experiment survey. If they selected "NO, I do not provide consent to participate," the survey would terminate on the spot, and the survey would collect no data. After obtaining the students' consent, I collected the pre-lecture knowledge assessment survey responses before the agreed-upon lecture dates. In contrast, I collected the post-assessment survey data one week after the lecture.

6.6.3 Participant Demographics

Across the nine sections of classes that I taught or visited, there were a total of 125 students. I collected 85 valid student responses by offering the students of various classes the incentive of some course extra credits. Among the 85 good data samples, 21 were completed by female undergraduate students, while male undergraduate students completed 64 samples. The 85 samples contain data from 20 juniors and seniors, a few sophomores, and the rest were first-year students. Given the distribution of students in terms of age, their observed behavior will slightly differ. I discussed the study limitation and other observations in Chapter 8 of this documentation.

Chapter7
FRAMEWORK IMPLEMENTATION RESULTS

7.1 Inferential Statistics Using T-Tests

Before the student performances are discussed, we briefly discuss the inferential statistical analysis method that we used to determine whether the responses offered by the students demonstrate statistically significant improvements in this section. We performed the paired samples T-tests using JASP [8] to evaluate the statistical significance between the student's pre-and post-lecture assessment ratings. Specifically, for the test option, we used the student's t-test with a confidence level of 95 percent with the descriptive statistics option selected. For the 1-tailed T-test, the alternative hypothesis is set to Measure 1 > Measure 2 (post-assessment rating > Pre-assessment rating). In contrast, in the 2-tailed T-test, we set the alternative hypothesis to Measure 1 $\neq$ Measure 2 (Post-assessment rating $\neq$ Pre-assessment rating). When we performed the T-tests against various student categorization samples, the sample sizes fluctuated depending on how the test samples were categorized. However, the other test configurations set using JASP remained consistent throughout all T-tests.

7.2 Full Sample Descriptive Statistics

The preliminary data analysis involves 85 completed student samples across nine sections of classes. The project's data collection phase lasted for eight months across two academic semesters at Marquette University. The preliminary data analysis begins with assessing whether the framework-driven lectures benefited students.

To achieve the objective, we evaluated the pre-survey performance average per question and compared that to the post-survey score average. Figures 7.1 and 7.2

Figure 7.1: The Mean Response Rating by Question Based on the Pre-Survey

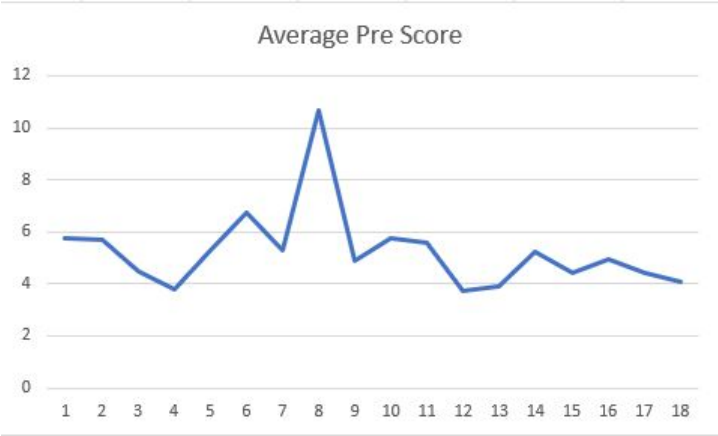


Figure 7.2: The Mean Response Rating by Question Based on the Post-Survey

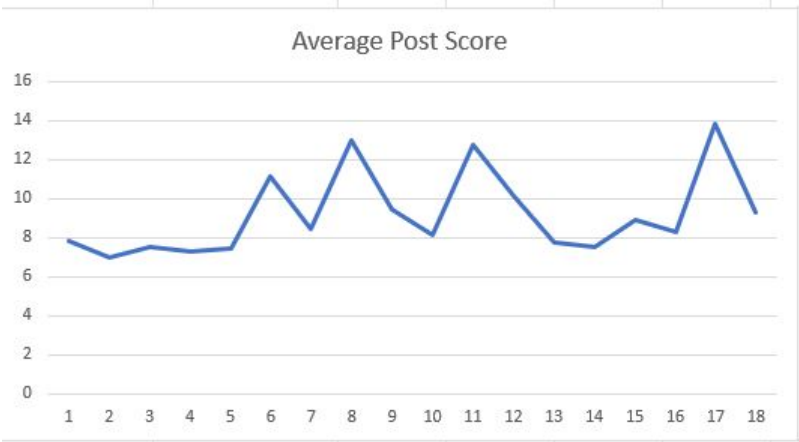
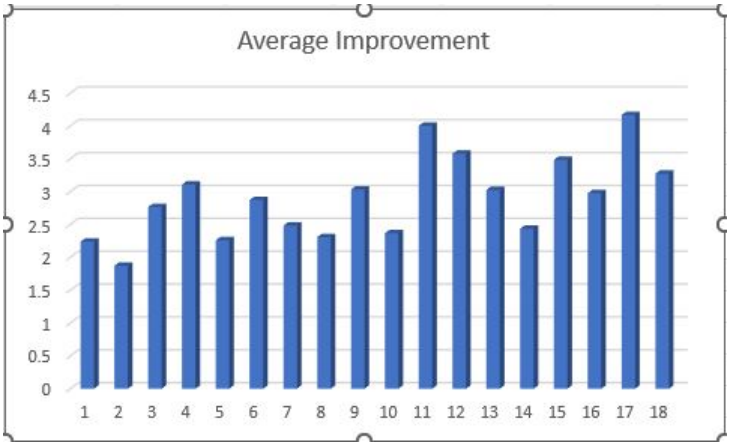


Figure 7.3: The Performance Improvement Mean by Question



show the average performance for each knowledge assessment question in the pre-and post-lecture assessment surveys. We obtained the average improvement by subtracting the average score on the pre-survey from the average score of the post-survey for each question. Figure 7.3 demonstrates the average score improvement for each question. The average score for Questions 11,12, and 17 increased by more than three points, while the remaining nine questions also demonstrated a gain of two or more points. In contrast, the score for Question 2 only increased by 1.871 points. We also validated the statistical significance of these demonstrated improvements using two (1-tail and 2 Tails T-Test) T-tests. The 85 participants who received exposure to the educational framework content demonstrated significantly better scores, t values for the full sample were ranging from 3.468 to 16.321, with a p-value for all questions being < 0.001. The detailed descriptive statistics of the full sample are demonstrated through Table 7.1 below.

7.2.1 Student improvement by question categories

After the initial analysis, we investigated the performance improvement by the question categories. The knowledge assessment survey consists of 18 questions that classify into five categories: current understanding, CIA triad, threat, and vulnerability, defensive strategy, incident response, and disaster recovery. Amongst these categories, the demonstrated improvement for the self-assessment questions was the lowest, and the scores fluctuated significantly. The potential cause of the fluctuation may be that the student's perceived personal knowledge may have changed after the lectures. Some students have expressed self-doubt about whether they understood the materials well while completing the post-lecture assessments.

In addition to identifying the categories which depicted the slightest improvement, we also recognized that questions about the incident response and disaster recovery topics demonstrated the most improvement. On average, the rating for each question

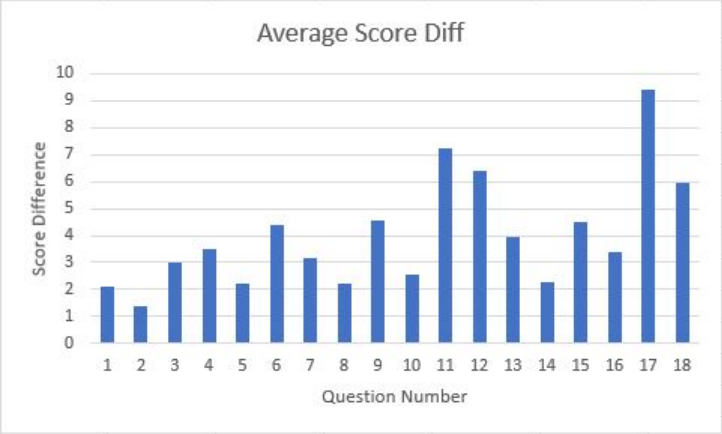
Table 7.1: Mean, SD, and T-Test Statistics for 18 Educational Framework Content of the Full Sample (N=85)

content	Post		Pre		T-Test	1-Tailed	2-Tailed
N=85	Mean	SD	Mean	SD	t value	p value	p value
1	7.847	1.384	5.753	1.969	9.664	$< .001$	$< .001$
2	7.000	1.669	5.671	2.190	6.176	$< .001$	$< .001$
3	7.506	1.517	4.471	1.968	14.10	$< .001$	$< .001$
4	7.259	1.807	3.765	2.125	16.321	$< .001$	$< .001$
5	7.471	4.654	5.271	3.130	3.967	$< .001$	$< .001$
6	11.129	5.237	6.753	4.921	6.418	$< .001$	$< .001$
7	8.424	5.441	5.306	4.175	5.319	$< .001$	$< .001$
8	12.965	3.246	10.682	4.190	4.856	$< .001$	$< .001$
9	9.447	5.065	4.894	3.546	8.537	$< .001$	$< .001$
10	8.012	5.286	5.765	4.431	3.468	$< .001$	$< .001$
11	12.765	3.355	5.576	4.255	12.982	$< .001$	$< .001$
12	10.129	5.099	3.753	2.430	11.031	$< .001$	$< .001$
13	7.788	4.57	3.894	4.896	7.897	$< .001$	$< .001$
14	7.541	3.571	5.259	2.386	5.749	$< .001$	$< .001$
15	8.894	3.719	4.400	2.274	11.402	$< .001$	$< .001$
16	8.306	3.32	4.929	2.219	9.105	$< .001$	$< .001$
17	13.871	3.525	4.412	3.889	17.682	$< .001$	$< .001$
18	9.329	4.691	4.094	2.789	10.082	$< .001$	$< .001$

within that category increased by 3.12 points. We were surprised by that result for two reasons: first, our department does not offer any content associated with incident response and disaster recovery at the undergraduate level. Secondly, the questions within that category were the toughest based on student input. The questions within that category were scenario-driven, testing the students on how they would respond if they were the victim of a cybersecurity incident.

The average improvement of the entire sample for the remaining categories is as follows: on average, the CIA triad questions improved by 2.53 points, vulnerability and threat questions improved by 2.66 points, and defensive strategies questions improved by 3.51 points based on a 15-point scale. The score improvements translate to 16.5 to 23 percent of knowledge improvement, respectively. The Figure 7.4 demon-

Figure 7.4: The Score Difference Mean by Question



strates the clear score difference for each question. The preliminary investigation suggests that offering students exposure to the framework component results in the students being more knowledgeable about risk management, incident response, and disaster recovery concepts.

7.3 Advanced Data Analysis

While the preliminary analysis offers satisfying results, we wanted to take a step further to investigate the student performances and identify potential influencing factors that may impact the student's performance on the knowledge assessment surveys. Specifically, we focused on the following factors: the classes in which the students enroll, their previous knowledge, the question difficulty, student maturity, course offering times, and student behaviors in class. To further examine the impact of these factors on student performance and obtain additional insights on student improvement, we organized the test samples into three categories based on the question responses offered during the knowledge assessment surveys. Particularly, students are categorized as high performers if their knowledge assessment rating averaged greater than 12 points in the post-survey or 5.5 points in the pre-survey. At the same time, students whose rating average is between 4.4 and 5.5 points on the pre-survey or between 9-12 points on the post-survey fall into the intermediate performer category.

I then classified all remaining test samples as poor performers. The performance of the test subjects in each of these student categories are evaluated using the T-Test to ensure the improvements demonstrated by the students were statistically significant.

7.3.1 Test Sample Categorization

Based on a 15-point scale, there were 16 classified as high performers, 39 classified as intermediate performers, and 30 classified as poor performers. When attempting to categorize the students into the same three categories using their pre-survey scores, the separating score line had to be adjusted because the average score for pre-surveys was significantly lower when compared to the post-survey scores. As a result, when categorizing students using the pre-survey assessment rating, there were 30 classified as high performers, 27 classified as intermediate performers, and 28 classified as poor performers. In the end, Table 7.2 shows the student distribution by count and categories.

Table 7.2: Student Distribution Count By Sample Categorization

Student Category	Pre-Count	Post-Count
High Performer	30	16
intermediate Performer	27	39
Poor Performer	28	30

7.3.2 Question Categorization by Topic

We examined their performance ratings based on the previously disclosed five question categories to examine student performances better. Specifically, Table 7.3 describes the question distribution by each corresponding category of the survey. As shown in the Table, four questions in the survey asked the students to measure their current understanding of risk management, incident response, and disaster recovery. Three of the questions tests to see if the participants can define the CIA triad and describe the purpose of those triad members using examples. Threat and vulnerability questions primarily functioned as a knowledge check for the assessment. The

Table 7.3: The Question Pool Distribution by Question Categories

Question Category	Question Count
Current Understanding	4
CIA Triad	3
Threat and Vulnerability	2
Defensive Strategy	3
Incident Response and Disaster Recovery	6

participants were required to list and describe the objective of each of the six threat actor groups introduced within the lecture. Three questions test their understanding of the two most common risk management defense strategies in defense in depth and honeypot. The survey closes with six questions that ask students to respond to potential cybersecurity incident scenarios to examine whether they can apply the knowledge regarding incident response and disaster recovery by following the corresponding standardized operational procedures.

7.3.3 Question Difficulty

To investigate what factors may be influencing the student participant's performance, we categorized the question by difficulty based on the student performance. We then evaluated each question personally to determine the corresponding difficulty of each question. In Figure 7.5 below, questions are color coded. Question numbers marked red are challenging questions, questions marked yellow are considered difficult but manageable, and questions marked green are considered easy questions.

From the student response, we were able to conclude that the self-assessment questions, the incident response questions, and the disaster recovery questions were more difficult when compared to other questions related to defensive strategies and CIA triads. This finding on the question difficulty is understandable because we created the self-assessment question to gauge their current knowledge. Most student participants scored low as these topics are mostly new. Besides, the questions related to incident response and disaster recovery were scenario questions asking the students

to apply what they learned without having access to the lecture materials. Therefore, we expected the assessment scores to range from low to intermediate, considering that the difficulty of the questions influenced the student's performance.

When we evaluated the questions, we reflected upon the lecture content delivered to the students during the trial implementation. We believe the self-assessment questions were challenging, considering they were new to the subject. For Questions 9, 12, 13, and 15, we classified them as challenging but manageable questions because they asked the students to recall the incident response procedures and disaster recovery phases. Considering that we did not provide them with the lecture slides to review and the information they could obtain online was different than our materials, it was

Figure 7.5: The Student's perceived Difficulty of the Questions V.S the Instructor's Perceived Difficulty of the Questions

Question Difficulty Based on Response	Instructor Question Difficulty
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10
11	11
12	12
13	13
14	14
15	15
16	16
17	17
18	18

relatively complex for them to fully recall the content and offer a comprehensive and correct response. As a result, the scores were within the intermediate ranges. The easy questions examine students' knowledge of the definition of terms, and we incorporated these questions to function as knowledge checks. Anyone can quickly obtain the answers to these questions through search engines with the correct keywords.

When comparing the question difficulties based on the score response and our subjective opinion, there were a few questions within the survey that were rated slightly differently. Question 6 asked the participants for the definition of each of the CIA triad members. Many left this question blank because Question 7 asked them to describe each of the CIA triad members using an example. Some students combined the members' definition with an example and used that to answer Question 7 instead. As a result, the students rated Question 6 as challenging but manageable, even though we thought the question was easy. Students thought Questions 9 and 12, where we asked the participants about the threat actors, the primary objectives of the mentioned actors, and the phases of incident management were relatively easy. Still, due to the expectation of correctness and comprehensiveness, we rated the questions challenging but manageable. Overall, the difficulty rating that we assigned to each of the remaining questions on the assessment survey aligns with the difficulty level reflected by the student's survey responses.

7.3.4 Student Performance by Post Survey Categorization

When we grouped the students by their average post-assessment survey ratings, the improvement for each question and question category differed across the three performance groups.

Figures 7.7 and 7.6 demonstrate the student's average performance by performance groups and question topic categories. As shown in the figure, the responses associated with questions on defensive strategies demonstrated the most improvement across

all students when we grouped them by their post-assessment survey ratings. To better analyze the performance improvements of the students in different categories, their corresponding behavior and improvement trends are discussed separately in the subsections below.

7.3.5 High-Performance Student by Post-Assessment Rating

Students classified as high performing demonstrated a steady trend in knowledge improvement across both the pre-and post-lecture knowledge assessment survey ratings. Remarkably, if we list the student performance improvement of the various question categories in descending order, it will rank as follows: defensive strategy >

Figure 7.6: The Mean Value of Students Performance By Performance Categorization using Post Survey Ratings and Question Categories

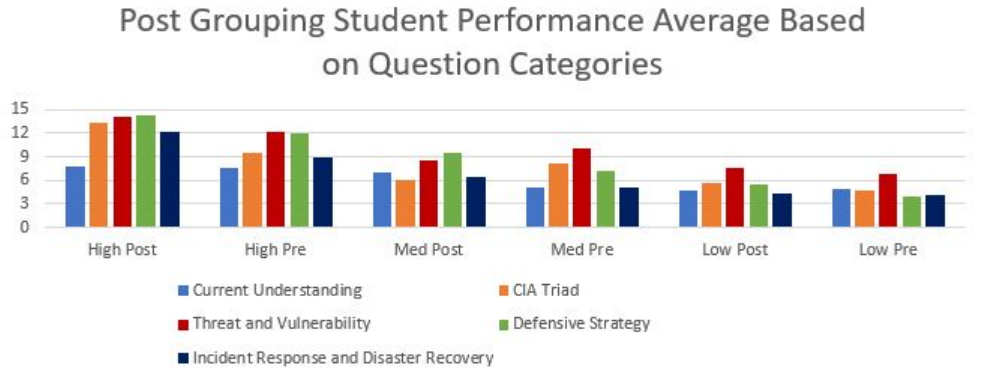
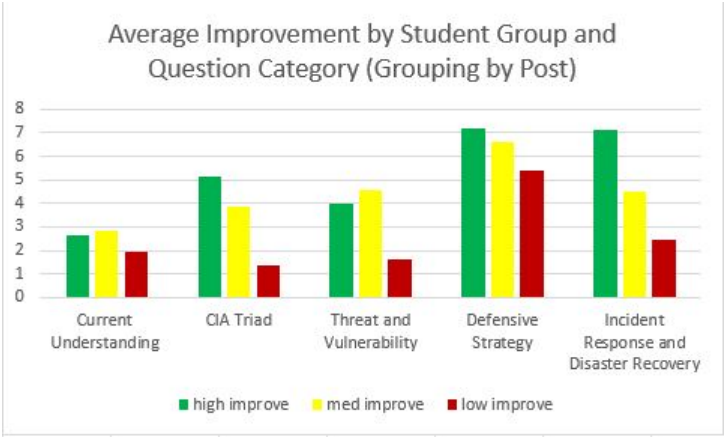


Figure 7.7: The Mean Value of Students Performance by Post-Survey Categorization and question Categories



threat and vulnerability > the CIA triad > incident response and disaster recovery > current understanding assessments. To further examine the credibility of the results depicted through the response rating analysis, we also executed 2 T-tests to ensure the statistically significant improvement in the student's performance rating on the knowledge assessment surveys.

Table 7.4: Mean, SD, and T-Test Statistics for 18 Educational Framework Content of the High-Performance Students Categorized by Post-Rating (N=16)

content	Post		Pre		T-Test	1-Tailed	2-Tailed
N=16	Mean	SD	Mean	SD	t value	p value	p value
1	8.063	1.389	6.063	2.144	3.554	< .001	<.001
2	7.438	1.896	6.000	2.477	3.286	0.003	0.003
3	8.063	1.237	4.563	2.097	7.668	< .001	0.005
4	7.313	1.852	3.625	1.928	8.668	< .001	< .001
5	10.688	4.644	7.500	4.243	2.043	0.030	< .001
6	14.625	1.500	8.688	4.729	4.549	< .001	0.059
7	14.625	1.500	8.375	5.005	5.213	< .001	< .001
8	14.438	1.632	14.125	1.746	0.892	0.193	< .001
9	13.75	3.256	6.063	3.907	6.602	< .001	0.386
10	13.313	3.459	9.250	5.310	2.297	0.018	< .001
11	14.813	0.750	7.000	4.719	6.173	< .001	0.036
12	14.438	1.632	4.875	4.225	8.951	< .001	< .001
13	12.000	3.464	4.875	2.419	6.530	< .001	< .001
14	10.750	3.130	5.250	2.569	6.149	< .001	< .001
15	12.000	2.191	5.063	2.620	8.126	< .001	< .001
16	11.063	3.043	5.625	2.872	5.928	< .001	< .001
17	15.000	0.000	5.250	4.837	NaN		
18	13.313	2.676	5.188	4.355	7.608	< .001	< .001

Following the T-Test configurations described at the beginning of this chapter, we conducted both T-tests to verify the validity of the results. Given that our sample size for this category was 16, the degree of freedom is 15, and the T-value we need to reject the null successfully is 1.753(one tail) and 2.131 (two tails), respectively. We would fail to reject the null hypothesis if the T-values were less than the threshold or the p-values were more significant than 0.05. Table 7.4 shows the detailed statistics of

the T-tests. We failed to reject the null for Questions 8, 17, and 5,8,17 for the one and two tail T-tests. Question 17 did not yield a valid t or p-value because the variance in the post-assessment rating for Question 17 was equal to 0. The remaining questions demonstrated a statistically significant effect, indicating that the participants exposed to the education framework content scored significantly higher in all questions except Questions 5,8, and 17.

7.3.6 Intermediate Performance Student by Post-Assessment Rating

In contrast to the high-performing students, the students labeled intermediate performers demonstrated a different performance improvement across the various question subjects. For example, we can describe the average improvements by question category when sorted in a descending order as follows: defensive strategies > threat and vulnerability > incident response and disaster recovery > CIA triad > current understanding. To further examine the credibility of the observed improvement by the students, we repeated both T-tests against this group of student samples.

Following the T-Test configurations described at the beginning of this chapter, we conducted both T-tests to verify the validity of the results. Given that our sample size for this category was 39, the degree of freedom is 38, and the T-value we need to reject the null successfully is 1.684(one tail) and 2.021 (two tails), respectively. We would fail to reject the null hypothesis if the T-values were less than the threshold or the p-values were more significant than 0.05. In this student subject category, the participants who have exposed to the educational framework content scored significantly higher in all content areas. The only question with a T value close to the T-test threshold is Question 10, where we asked the students about the definition of defense in depth and testing to see if they could offer an example that comprehensively describes the concept of defense in depth and correctly. Table 7.5 shows the detailed statistics of the T-tests.

Table 7.5: Mean, SD, and T-Test Statistics for 18 Educational Framework Content of the Intermediate-Performance Students Categorized by Post-Rating (N=39)

content	Post		Pre		T-Test	1-Tailed	2-Tailed
N=39	Mean	SD	Mean	SD	t value	p value	p value
1	8.103	1.252	5.667	2.030	7.423	$< .001$	$<.001$
2	7.308	1.524	5.692	2.214	4.725	$< .001$	$< .001$
3	7.615	1.388	4.282	2.089	9.443	$< .001$	$< .001$
4	7.487	1.775	3.538	2.075	12.416	$< .001$	$< .001$
5	7.795	4.680	5.026	2.767	3.276	$< .001$	0.002
6	12.769	4.170	7.718	5.605	4.401	0.001	$< .001$
7	8.051	5.140	4.231	3.133	4.772	$< .001$	$< .001$
8	13.923	2.120	10.154	4.165	5.004	$< .001$	$< .001$
9	10.333	4.954	4.949	3.727	6.658	$< .001$	$< .001$
10	7.769	5.137	5.538	4.328	2.358	$< .001$	0.024
11	13.846	2.242	6.436	4.866	8.699	0.012	$< .001$
12	10.923	4.858	3.795	2.215	8.250	$< .001$	$< .001$
13	7.974	4.545	3.641	1.709	5.596	$< .001$	$< .001$
14	7.462	3.307	5.359	1.828	3.826	$< .001$	$< .001$
15	9.128	3.443	4.513	2.427	8.383	$< .001$	$< .001$
16	8.615	2.988	4.974	2.019	6.897	$< .001$	$< .001$
17	14.385	2.681	4.231	3.688	14.457	$< .001$	$< .001$
18	9.026	4.804	3.795	1.949	6.537	$< .001$	$< .001$

7.3.7 Poor Performance Student by Post-Assessment Rating

We analyzed the performance improvement of the student samples that demonstrated the slightest improvement. We concluded that the most significant improvement was when they responded to defensive strategies, incident response and disaster recovery questions. The gain was minimal, where the average improvements were less than 2 points. After the conclusion on performance improvement, we repeated the T-tests on the scores of this group of students.

In this group, the sample size was 30, the degree of freedom was 29, and the T-value we need to reject the null successfully is 1.699(one tail) and 2.045 (two tails), respectively. We would fail to reject the null hypothesis if the T-values were less than the threshold or the p-values were more significant than 0.05. Table 7.6 shows the

detailed descriptive statistic for the scores of this subject group. From the table, we failed to reject the null for Questions 5,7,10,14 and 5,7,8,10,14 for the one and two tail T-tests, respectively. The potential reason we failed to reject the null for Question 8 is worth noting. Question 8 asks the student about the difference in terms of definition between the term vulnerability and threat. A potential reason that may contribute to why the performance rating for Question 8 was not statistically significant was that students could quickly obtain the answer to this question through any search engine as the question was trivial. Many students submitted identical answers that they retrieved online across the two surveys. While the rating differences for these identified questions were not statistically significant, the responses they offered for the other questions still demonstrated knowledge improvements to some extent.

Table 7.6: Mean, SD, and T-Test Statistics for 18 Educational Framework Content of the Poor-Performance Students Categorized by Post-Rating (N=30)

content	Post		Pre		T-Test	1-Tailed	2-Tailed
N=30	Mean	SD	Mean	SD	t value	p value	p value
1	7.400	1.476	5.700	1.841	5.277	$< .001$	$<.001$
2	6.367	1.586	5.467	2.047	2.619	0.007	0.014
3	7.067	1.721	4.667	1.768	8.057	$< .001$	$< .001$
4	6.933	1.837	4.133	2.300	7.846	$< .001$	$< .001$
5	5.333	3.507	4.400	2.328	1.262	0.109	0.217
6	7.133	5.348	4.467	2.945	2.756	0.005	0.01
7	5.600	4.507	5.067	4.226	0.563	0.289	0.578
8	10.933	4.068	9.533	4.273	1.785	0.042	0.085
9	6.000	3.620	4.200	3.010	2.946	0.003	0.006
10	5.500	4.249	4.200	2.905	1.323	0.098	0.196
11	10.267	3.921	3.700	2.037	7.272	$< .001$	$< .001$
12	6.800	4.521	3.100	0.548	4.432	$< .001$	$< .001$
13	5.300	3.313	3.700	1.705	3.117	0.002	0.004
14	5.933	3.028	5.133	2.945	1.484	0.074	0.149
15	6.933	3.562	3.900	1.788	4.963	$< .001$	$< .001$
16	6.433	2.738	4.500	2.047	3.729	$< .001$	$< .001$
17	12.60	4.882	4.200	3.662	8.226	$< .001$	$< .001$
18	7.600	4.223	3.900	2.631	4.889	$< .001$	$< .001$

7.3.8 Student Performance by Pre-Survey Categorization

In addition to grouping the students by their post-survey scores, we also grouped them by their average performance in the pre-survey responses and classified them into three similar groups. However, because the pre-survey scores were significantly lower, it was difficult to determine the line of separation between performance groups since the score differences were much narrower compared to the post-survey assessment ratings.

Figure 7.8: The Mean Value of Students Performance By Performance Categorization using Pre Survey Ratings and Question Categories

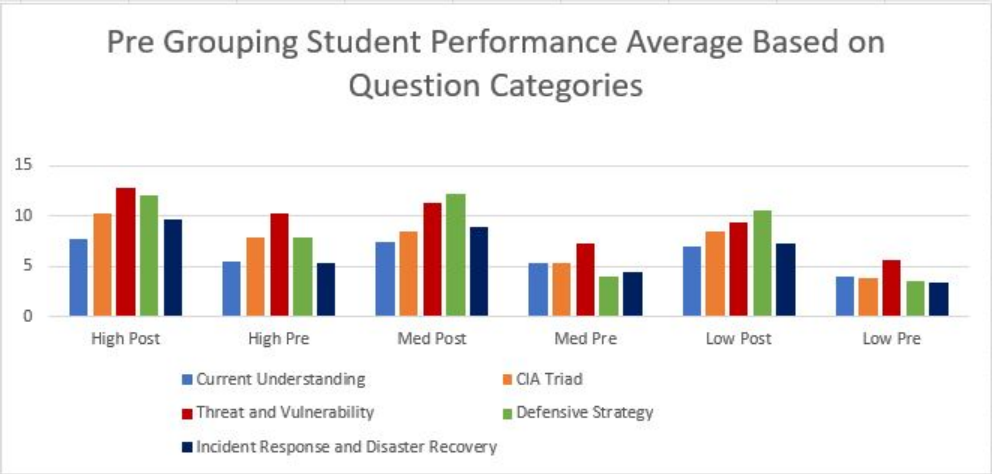
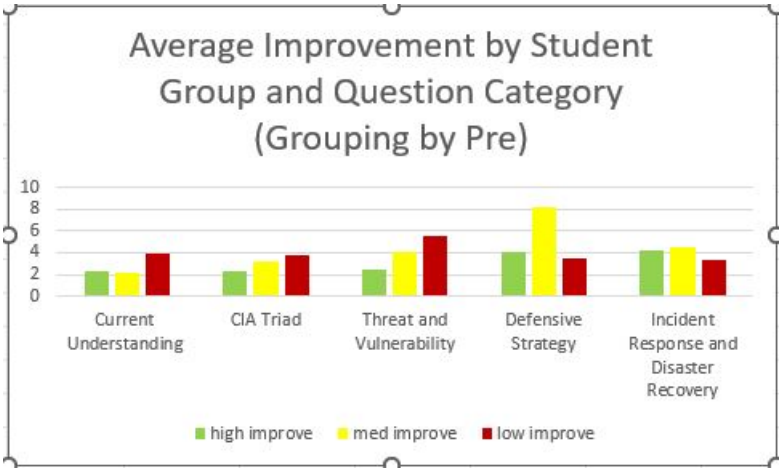


Figure 7.9: The Mean Value of Students Performance by Pre-Survey Categorization and Question Categories



As a result, there were 30, 27, and 28 students in each of the groups, respectively, when we classified the student using the following cutoff thresholds (poor if the average rating is less than 4, intermediate if between 4 and 5.5, and high if their average rating was higher than 5). Since the scores differences were very narrow for the pre-assessment grouping, the sample sizes for each corresponding group were significantly different compared to that of the post-assessment categorization. We could not identify a clear trend across the knowledge improvements for each group of student samples. To further investigate the performance improvements, we repeated the T-tests against each grouping to determine the net influence the materials had on the student performance. The results of the T-tests for each group will be presented below in their respective discussion sections.

7.3.9 High performance by Pre Assessment

Following the T-Test configurations described at the beginning of this chapter, we conducted both T-tests to verify the validity of the results. Given that our sample size for this category was 30, the degree of freedom is 29, and the T-value we need to reject the null successfully is 1.699(one tail) and 2.045 (two tails), respectively. We would fail to reject the null hypothesis if the T-values were less than the threshold or the p-values were more significant than 0.05. The detailed statistics of the category sample are presented in Table 7.7. According to the results in the table, we failed to reject the null hypothesis for Questions 7,8, and 10, and 6,7,8,10 for the one and two tail T-tests, respectively. Since the t and p values for the other questions were statistically significant, the result suggests that the students within this specific category demonstrated knowledge improvements for the remainder of the questions through their responses.

Table 7.7: Mean, SD, and T-Test Statistics for 18 Educational Framework Content of the High-Performance Students Categorized by Pre-Rating (N=30)

content	Post		Pre		T-Test	1-Tailed	2-Tailed
N=30	Mean	SD	Mean	SD	t value	p value	p value
1	8.133	1.358	6.267	1.76	5.466	$< .001$	$<.001$
2	7.400	1.714	6.067	1.856	4.085	$< .001$	$< .001$
3	8.167	1.289	5.233	2.029	7.651	$< .001$	$< .001$
4	7.633	1.921	4.500	2.080	8.676	$< .001$	$< .001$
5	8.900	5.195	6.233	3.830	2.675	0.006	0.012
6	11.90	4.950	9.933	5.037	1.789	0.042	0.084
7	9.533	5.686	8.067	5.388	1.449	0.079	0.158
8	13.50	2.583	13.03	2.526	0.842	0.203	0.407
9	12.267	3.947	7.667	4.229	5.109	$< .001$	$< .001$
10	8.800	5.455	9.433	4.904	-0.595	0.722	0.556
11	13.10	3.387	8.500	5.131	4.349	$< .001$	$< .001$
12	10.267	5.369	4.700	3.583	5.627	$< .001$	$< .001$
13	8.667	4.436	4.833	2.422	4.348	$< .001$	$< .001$
14	9.200	4.055	5.900	2.857	4.157	$< .001$	$< .001$
15	10.50	3.589	5.467	2.921	6.798	$< .001$	$< .001$
16	9.000	3.582	6.067	2.477	4.523	$< .001$	$< .001$
17	14.20	3.044	6.200	5.397	7.616	$< .001$	$< .001$
18	11.00	3.806	5.467	3.730	6.611	$< .001$	$< .001$

7.3.10 Med performance by Pre Assessment

The sample size of the intermediate performers was 27, and the degree of freedom was 26, the T-value needed to reject the null hypothesis was 1.706 (one tail) and 2.056 (two tails), respectively. The detailed statistics of the intermediate performer category are presented in Table 7.8. According to the results in the table, we failed to reject the null hypothesis for Questions 5 and Questions 2 and 5 for the one and two tail T-tests, respectively. The participants within this group who have exposed to the educational framework content scored significantly higher in all questions except Questions 2 and 5.

Table 7.8: Mean, SD, and T-Test Statistics for 18 Educational Framework Content of the Intermediate-Performance Students Categorized by Pre-Rating (N=27)

content	Post		Pre		T-Test	1-Tailed	2-Tailed
N=27	Mean	SD	Mean	SD	t value	p value	p value
1	7.815	1.241	6.111	1.826	5.410	$< .001$	$<.001$
2	7.111	1.625	6.481	2.137	4.885	0.035	0.071
3	7.407	1.421	4.704	1.636	9.277	$< .001$	$< .001$
4	7.333	1.494	3.852	1.812	12.702	$< .001$	$< .001$
5	6.852	4.176	5.444	3.004	1.382	0.089	0.179
6	10.15	5.223	6.333	4.506	3.329	0.001	0.003
7	8.296	5.210	4.185	2.167	4.103	$< .001$	$< .001$
8	13.11	3.130	10.667	3.752	3.114	0.002	0.004
9	9.556	5.184	3.778	2.577	5.587	$< .001$	$< .001$
10	8.667	5.015	4.333	3.363	3.976	$< .001$	$< .001$
11	13.556	2.407	4.222	3.030	13.256	$< .001$	$< .001$
12	10.333	5.152	3.481	1.740	6.222	$< .001$	$< .001$
13	8.444	4.995	3.667	1.732	5.337	$< .001$	$< .001$
14	7.370	3.027	5.667	2.094	2.729	0.006	0.011
15	8.778	3.816	4.333	1.922	6.183	$< .001$	$< .001$
16	8.778	2.991	5.222	1.968	5.228	$< .001$	$< .001$
17	14.11	3.203	3.444	2.309	14.422	$< .001$	$< .001$
18	9.481	4.586	3.704	2.447	6.288	$< .001$	$< .001$

7.3.11 Low performance by Pre Assessment

Lastly, the sample size of the poor performers was 28, and the degree of freedom was 27, the T-value needed to reject the null hypothesis was 1.701 and 2.052, respectively. We could not obtain a valid p and t value for Questions 9, 12, and 18 due to the variance in the pre-assessment response being equal to 0. Therefore, we could not determine whether the difference demonstrated were statistically significant. However, the participants exposed to the educational framework content scored significantly higher in all content areas other than those three questions. The detailed statistics of this subject sample are presented in Table 7.9.

Table 7.9: Mean, SD, and T-Test Statistics for 18 Educational Framework Content of the Poor-Performance Students Categorized by Pre-Rating (N=28

content	Post		Pre		T-Test	1-Tailed	2-Tailed
N=28	Mean	SD	Mean	SD	t value	p value	p value
1	7.571	1.526	4.857	2.068	6.141	$< .001$	$<.001$
2	6.464	1.575	4.464	2.117	4.750	$< .001$	$< .001$
3	6.893	1.595	3.429	1.794	8.199	$< .001$	$< .001$
4	6.786	1.912	2.893	2.200	8.662	$< .001$	$< .001$
5	6.536	4.247	4.071	1.864	2.821	0.004	0.009
6	11.250	5.575	3.750	2.784	6.908	$< .001$	$< .001$
7	7.357	5.356	3.429	2.268	3.998	$< .001$	$< .001$
8	12.250	3.912	8.179	4.643	4.268	$< .001$	$< .001$
9	6.321	4.269	3.000	0.000	NaN		
10	6.536	5.232	3.214	0.787	3.270	0.001	0.003
11	11.643	3.880	3.750	2.102	9.438	$< .001$	$< .001$
12	9.786	4.917	3.000	0.000	NaN		
13	6.214	3.994	3.107	0.567	3.989	$< .001$	$< .001$
14	5.929	2.721	4.179	1.701	3.0112	0.003	0.006
15	7.286	3.101	3.321	0.945	6.853	$< .001$	$< .001$
16	7.107	3.107	3.429	1.069	6.022	$< .001$	$< .001$
17	13.286	4.276	3.429	2.268	11.145	$< .001$	$< .001$
18	7.393	5.065	3.000	0.000	NaN		

7.4 Results Summary

When observing the mean scores differences in pre-post assessment surveys of the full sample, we noticed a significant performance improvement for all questions. That finding suggests that the materials offered to the students benefitted the students in terms of increased awareness of risk management, incident response and disaster recovery practices. The T-test results shown in 7.1 offers support for the finding. However, when we examine the student performance based on different categorization configurations based on their average performance rating, the findings differed slightly. Specifically, across the distinct groups of T-tests, it became apparent that we routinely failed to reject the null hypothesis for Questions 5, 7, 8, and 10. We intend to investigate potential ways to optimize those questions through the change

of wording or other forms of modifications before any future framework adaptation takes place. Nevertheless, the results of the various T-tests suggests that all other remaining questions influenced students' knowledge about risk management practices, incident response, and disaster recovery. Overall, the data analysis results demonstrated within this chapter offered supportive evidence to validate the proposed thesis statement of this dissertation document.

Chapter8
IMPLEMENTATION RESULT DISCUSSION

In this chapter, we would like to discuss potential factors that may have influenced student performance. In addition, we also briefly discussed some of the design flaws and the future work associated with this framework before it can be fully ready for classroom implementation.

8.1 Influencing Factors

Throughout the process of experiment sample collection, we noticed that several factors might influence students' behavior and performance. These factors may directly impact their performance on the assessment surveys. Therefore, we decided to investigate further. The specific elements are the maturity of students, instruction delivery methods, how students responded to lectures, and behavioral observations.

8.1.1 Responses to Lectures and Observed Behaviors

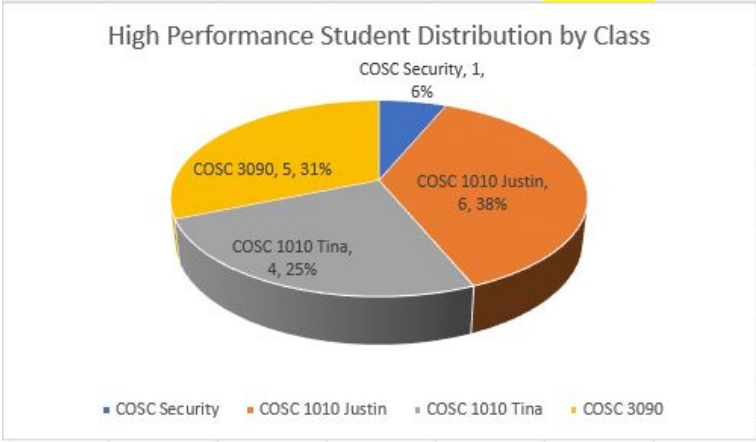
Learning from prior instruction experiences, we knew that classroom experiments such as the trial implementation would result in students responding differently. Students may react passively or offer minimal to no responses if they are not interested in the topic. They may react semi-actively because the subject materials appear exciting, and they are eager to learn more. They may also react proactively by asking questions and volunteering to participate when we offer students brainstorming challenges or in-class mini-interactive exercises. Even though we only had 85 completed samples of survey submission, we observed how students responded to lecture materials. They reacted differently depending on how we delivered the lecture, the time of course offering, and their maturity as students.

For example, when we delivered the contents to the morning sections of the first-

year students, most appeared disinterested, with a few being semi-active, but not many were taking notes. In this scenario, we had to incorporate impromptu interactions with the students to receive responses from them. Most students in the morning sections performed relatively worse than others. However, when we delivered the materials to the afternoon sections of the first-year students, most were taking notes. Even though a few clearly expressed disinterest in the topic. We still got a significantly more active audience to respond to questions, and many asked for additional examples and clarifications on specific concepts associated with defensive strategies and disaster recovery.

We believe how the students respond to lecture materials is related to the scheduled time for class, the instruction method used by the instructor, and whether they are interested in the subject. The student distribution by Class can be found in Figures 8.1, 8.2, 8.3, respectively. The COSC-1010 Tina was the class section with a scheduled class time in the morning whereas COSC-1010 Justin was scheduled to take place in the early afternoon. COSC-3090 and COSC-4360 took place in the early evening.

Figure 8.1: High Performance Student Distribution



8.1.2 Instruction Pedagogy and Deliver Method

In addition to the scheduled class time, we thought another factor that significantly influenced student response and their corresponding performance on the assessment surveys was the instruction pedagogy and the lecture delivery method. While we kept the pedagogical approach consistent, using traditional lectures with a few injected interactive exercises. Some data samples came from a classroom where Marquette offered hybrid instruction (Spring 2021). Even though we classified most of the students in the computer security course as intermediate performers, a few things

Figure 8.2: Intermediate Performing Student Distribution

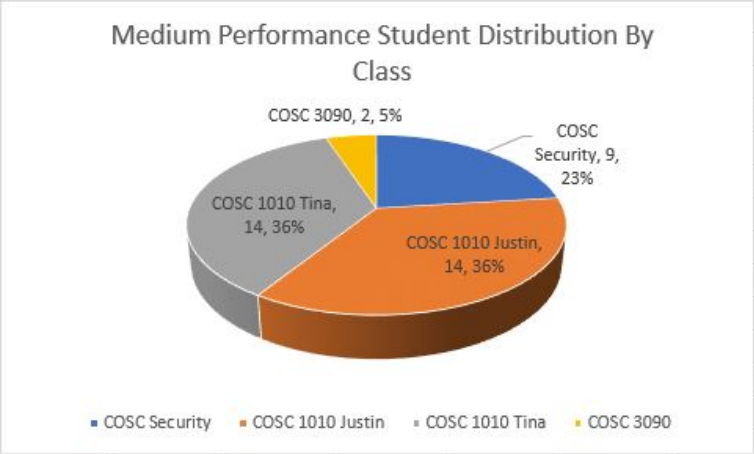
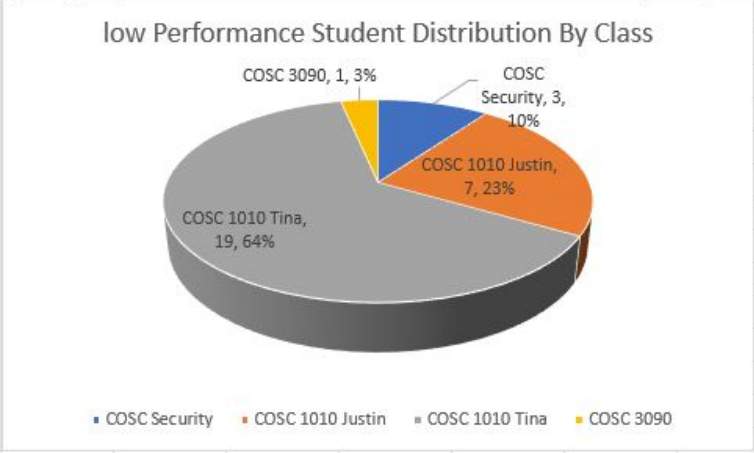


Figure 8.3: Low Performing Student Distribution



in terms of environmental differences compared to other class sections where we offered this material are worth noting. Specifically, in this section, where we collected a portion of the data sample (13 samples), half of the students attended the lecture synchronously, preventing them from interacting with us effectively. Also, on the day of lecture delivery, the audio system in the room was inconsistent, causing the audio reception to be problematic, and directly impacting the lecture quality for those attending class synchronously. Besides the factors mentioned above, our inexperience in instructing the material may also contribute to the relatively inferior performance of the students.

8.1.3 Student Maturity

Since we collected the data samples from various classes, the student population was diverse. COSC-1010 consisted of first-year students, while COSC 3090 was primarily of sophomores and juniors, and COSC-4360 consisted of mostly juniors and seniors. The student's behavior and maturity drastically differed from observing their behavior in class. As a result, we thought this might also contribute to their performance on the assessment surveys. Specifically, when informed students that the lecture materials would not be available after the lectures concluded, most upper-class students immediately took out notebooks and started taking notes. Also, most upper-class students actively sought clarifications and additional examples to help them better understand the materials. Besides, judging from their assessment responses, they most clearly leveraged the help of internet resources when encountering problems to which they did not know the answers. In contrast, most first-year students would skip the question or offer irrelevant responses like I don't know, N/A, or no clue. This observation is a potential concern for instructors who may be offering the materials in a different course setting. The lecture delivery method and lesson plans may have to be slightly adjusted to fit the audience behavior better and

maximize the potential benefit this framework offers.

8.2 Future Work and Potential Optimization

This project will be ongoing. It is in decent shape in terms of usability. Still, it can be further optimized to incorporate more topics and exercises and add adaptive rubrics for every exercise or activity in which instructors may expect students to participate. We will work with other subject matter experts to make this framework a valuable educational resource for other instructors. We identified several items that can be optimized before instructors adapt the framework in their classroom. Specifically, some of the survey questions in terms of wording will need to be updated. For example, we should structure the questions on the redundant array of independent disks in an open-ended manner and ask students to offer elaboration in terms of definition and configurations instead of merely asking whether they know what RAID is. Besides that, in terms of the experiment environment, we believe a monitored session of survey response collection may work better than hosting the assessment through online links. Collecting the student's knowledge assessment survey in a monitored setting is more beneficial. Especially when we know that most students will opt to use online resources when responding to the knowledge assessment questions, making their existing knowledge challenging to measure. If the current knowledge assessment is biased, then the absolute improvement of knowledge derived from the data analysis could also be potentially misleading, defeating the study's purpose.

8.3 Concluding Remarks

Overall, through the trial implementation of the framework, we were able to identify numerous factors that could bias the student's performance, which instructors would need to consider controlling. Given that our sample size was small, and we rated the assessment surveys very subjectively as the content developer, we think many other alternative explanations exist. we consider these as potential limita-

tions that may hinder the usability of this educational resource. We would like other instructors interested in adapting this framework to know this potential limitation. Nonetheless, when fully developed and completed, we believe these materials will be a valuable educational resource that would help instructors with minimal experience in risk management, incident response, and disaster recovery to instruct their students effectively.

Chapter9
CONCLUSION

In this dissertation, we offered an alternative approach to instructing complex topics about cybersecurity in incident response and disaster recovery. During the past decade, many institutions have begun to incorporate additional course offerings about cybersecurity topics. Still, to our knowledge, few institutions offer courses around the three topics of interest: risk management, incident response, and disaster recovery within a single program track. In addition, from surveying the available cybersecurity educational resources and utilities, it was apparent that educational resources teaching proper risk management practices, incident response, and disaster recovery on a personal level are lacking. Not many of the existing non-commercial utilities offer incident response and disaster recovery contents.

To achieve the goal of contributing educational resources to the field of cybersecurity education, we developed an educational framework that instructors can use to instruct their students using a flexible variety of pedagogical approaches. Precisely, the content consists of four primary components. One of the contents is several educational modules for lecture, The other was an educational resource on relevant cybersecurity framework, news, and best practices. Thirdly, a pool of topic-oriented exercises that offer students the opportunity to engage in hands-on activities both independently and in small groups. Lastly, an adaptive rubric that offers students standardized, actionable feedback in the format of hints on the failed objective to motivate students to engage in active learning and re-attempt the tasks assigned. We currently host all of these on one of the development team member's website in the format of published blog posts, located at: `https://hsiaoanwang.wixsite.com/jwhome`. We

anticipate migrating the resources over to Clark Center for complete access when the framework is closer to being mature and complete.

Our approach to building an adaptive framework enables instructors to deliver education content using various educational pedagogy as deemed appropriate. Based on the trial implementation of 85 experiment samples from multiple classrooms, we obtained T-test results demonstrating that the increase in the student's performance on the knowledge assessments were mostly statistically significant.

In the future, this framework will continue to be developed to optimize survey assessments and potentially incorporate additional assessment questions to understand student knowledge better. In addition to the survey re-design and optimization, we may include other topic-oriented exercises as new educational resources become available. Furthermore, additional adaptive rubrics must be created or fine-tuned to target each exercise. The optimized rubrics will be helpful to enable students to receive standardized feedback and then engage in active learning if they would like to utilize the actionable comments to explore the assignment further. In addition, we will continue to develop and incorporate more educational resources onto the website. The additional contents on the resource web page can offer students other supplementary utilities to help facilitate their learning.

Overall, the implementation of the framework yielded beneficial results for students of all classes regardless of their existing knowledge, which offered supportive evidence suggesting that the framework is a long-term project with potential. Given more work and additional contributions, this framework will eventually become a worthwhile contribution to cybersecurity education research.

AppendixA

Adjacency Matrices of Test Cases

This section of the document contains the assessment survey evaluation rubric, the assessment survey questions, and the corresponding answer expectations that I, as the instructor, was looking for when I tasked the students to respond to those questions after the lecture.

A.1 Knowledge Assessment Rubric

The assessment has three primary evaluation criteria that I will describe them in their corresponding table below. Figure A.1 describes the rating requirements for response correctness. A.2 describes the rating requirements for each response based on response comprehensiveness. Figure A.3 describes the rating requirement for each response based on content coverage and utilization demonstrated by students.

A.2 Knowledge Assessment Survey Questions

In this section, I will categorize each question into their independent subsections and present the questions I created to test the students' knowledge and the answers I was looking for, which would warrant the student a 15-point rating. The title of each

Figure A.1: Response Correctness

Feature/Category	Correctness of response
1	The response was irrelevant or incorrect.
2	A blur definition of the terms in question are mentioned but not necessarily correctly corresponding to the context presented in the lecture.
3	A generalized definition was given, the response to some extend describes the definition of terms or summarized definition of the term and answers a small portion of the question in context
4	A specific clear definition was given for the terms, the response covers most of the question components in detail. Example were not clearly identified.
5	A specific clear definition was given for the terms, the response covers all the question components in detail. Examples were provided when requested

Figure A.2: Response Thoroughness

Feature/Categories	Thoroughness of Response
1	The response was irrelevant to what was being asked on the survey questions or any response in the lines of I don't know, or no idea fits into this category,
2	The response briefly touches on cybersecurity in general but did not answer the questions asked in the survey
3	The response offers generalized summary of definition for specific vocabularies and answers a small portion of the questions
4	The response offers neat and detailed summary of the vocabulary definitions and answer most of the sub questions included in the question
5	The response offers neat and detailed answers for each independent component of the questions being asked and examples were attached when requested by the questions

Figure A.3: Content Coverage and Utilization

Feature/Category	Content Coverage/Utilization
1	A response that was irrelevant to the context.
2	A response that answers some question components incompletely or incorrectly.
3	A response that answers some question components while omitted portions of the question. Answers were merely a list of items without definition or clarification.
4	A response that answers all components of the questions, examples were given based on the content of the lecture.
5	A response that answers all components of questions, referencing external sources to provide example application of specific knowledge

sub-section represents the questions they see, and the contents within each sub-section present my expected response.

A.2.1 The role of CIA triad within the cyber space

Confidentiality helps ensure that information is comprehensively protected and safe for communication and other applicable usages. Integrity ensures that data within cyberspace are accurate and true without malicious modifications and that the data entry is trustworthy for analysis or other usages. Availability ensures that information is made available to the authorized users when the demand for such information arises. Availability is also applicable to applications and services where the authorized users should have access to the needed application and services when they demand such services or access.

A.2.2 Do you know the definition of each of the triad members?

Confidentiality: Information or data should remain confidential to all except the intended recipient. Integrity: Information should be accurate and true without malicious modifications and trustworthy. Availability: Information should be available to the authorized users upon request.

A.2.3 Can you provide an example of each of the three terms?

Confidentiality: Any key encryption algorithms such as SHA256, Advanced Encryption Standards, Diffie-Hellman, and hashing. Integrity: MD5, digital signatures. Availability: Any authentication measure and availability of server or applications.

A.2.4 What is the difference between threats and vulnerabilities?

Threat: The potential for something harmful to take place that results in financial damage or harm to the targeted system or client. Vulnerability: Known weaknesses that can be potentially leveraged/exploited to cause harm and obtain data of value.

A.2.5 Can you identify each threat actor in a list indicating their names and primary objective?

Nation State-Geopolitical, or causing interruption. Cyber Criminals - profit and cause damages. Hacktivists - ideal expression. Terrorist Groups - violence or discontent. Thrill Seekers - satisfaction. Insiders - revenge.

A.2.6 What do you know about defense in depth?

The deployment of a variety of physical, administrative, and technical controls to deter malicious actors from taking actions that could be harmful and malicious. It is a critical risk management strategy that includes DMZ, honeypot, intrusion detection/prevention, data leak protection, and firewalls.

A.2.6.1 Can you provide an example or analogy that describes the concept of defense in depth?

A Castle with multiple lines of defense or an organization that has actively deployed fences, cameras, security guards, badge scanners, firewall, intrusion detection system, intrusion prevention system.

A.2.7 Do you know what a Honeypot is in the scope of cybersecurity?

Honey pot is an asset that looks like something of value and an active production component, but does not carry production data.

A.2.7.1 Can you briefly describe the purpose of incorporating a honeypot?

The purpose of the honeypot is to track and monitor attacker behavior and distract the threat actor from the treasure and gold. Honeypots are typically placed outside the perimeter of the intranet as bait such that the malicious attacker will treat it as the crown jewel and try to ex-filtrate data from that fake target. However, one can not use a honey pot to bait an attacker and then turn around and prosecute them for malicious intrusion.

A.2.8 Do you know the incident management phases typically involved in security operations? If so, can you briefly describe each phase?

The phases of incident response involve preparation, detection, reporting, containment and eradication, and recovery. During the preparation phase, a company typically prepares for a potential threat by setting up defensive strategies. Detection software is then used to detect a breach, hack, or virus. The problem is reported to stakeholders in the company, then the root cause is determined, and the threat is contained and eradicated. Next, recovery is used to recover the system to its state before the incident. Preparation is the phase that the security team works diligently to ensure that everyone is prepared for an attack and security measures

are in place. Identification corresponds to the ability of an individual to identify the breach. Mitigation describes the idea that actions are taken to minimize or contain harm. Reporting consists of filing a report to law enforcement. Recovery is the process that gets you back to the last known good operational state. Remediation is the phase where you figure out why and how. Lessons learned is where the security team documents what happened, take notes of potential issues, and mitigate those issues. Detection is being able to detect a potential security risk. The response is the investigation to determine the next step and how to respond to the risk. Mitigation is how to contain the harm from the risk. Reporting is reporting the information to the shareholder and whoever is concerned about the risk. Recovery is the process of getting back to an operational state—remediation, which is figuring out how not to become a victim again. Finally, the lessons learned are learning from the experience and using that information to prepare for next time.

A.2.9 What elements should be included in a typical disaster recovery procedure?

Know the objective of recovery, how you will recover, document it, and regularly test that procedure. Companies should have backups in place for their data and computers. The security team members should eradicate the threat, and then the incident response team can recover the data. Usually, data is backed up in a cloud, secondary storage, or offsite storage.

A.2.10 If someone stole your social media or other personal account credential and performed detrimental conduct or actions as you, how would you respond?

The students are expected to utilize part of if not the incident response and disaster recovery procedure to respond to this incident, determine the magnitude of influence, pick a mitigation strategy then begin the processes of recovery: Below are

a few responses in which I rated 15. Once I realized my social media was stolen, I would respond by doing damage control, contacting everyone I could to let them know what had happened. I would then try to delete my social media accounts and report that they have been stolen to the app or whoever else could help. To ensure it does not happen again, I would not click on random links to enter my password and make a highly complex password. I would report the incident to the proper people or organization, learn all the information that was compromised, and call all the right people to change my passwords. I would also consider closing any accounts that need to be closed, and issue a public social media apology for my account being compromised.

A.2.11 How would you react if your computer's data were compromised and encrypted (impacted by ransomware)?

The critical point I am looking for in this question is whether they utilize the incident response or disaster recovery procedure. Specifically, students should note that they will assess the situation, attempt to decrypt, report to law enforcement, and then fall back to back up files if possible. A sample answer from the student to which I gave 15 is demonstrated below. I would first understand my situation if I could decrypt myself using free tools. Otherwise, I will have to restore the files from the backup or pay the ransom. I would then lock it down by taking everything offline to identify the source of the infection. I would work to eliminate the infection, implement my backups after backup validation, and pay the ransom. Either try to recover or restore the impacted information, assuming I created a backup. If not, once again present all evidence with calculated damage to law enforcement and prosecute the attacker.

A.2.12 Suppose you own a customized online store or personal website that contains your guests' information. If the data of your company gets compromised and disclosed, what would you do?

This question aims to test their understanding of complete incident response and disaster recovery procedures and see how much of it they used or partially used. Also, they need to be more specific regarding the actions that they will take because this could potentially be a severe concern for users. While I do not expect perfect answers, I want to see at least that they mention the use of investigation, some restoration, and reporting of such issues. I would first respond and verify if the threat occurred, then mitigate the damage and minimize what happened. I would report it to the business shareholders and law enforcement. Then, I would recover to the last good operational state. I would remediate it and figure out why and how it happened. I would perform a risk assessment. I need to figure out how much this will cost me, what my asset value, exposure factors, and single loss expectancy are, how I can prevent this in the future, and how to apologize to my customers for losing their information. I would have to be prepared to lose a lot of business. I would disclose the information to shareholders and customers so they know what happened. I would then try to find the source of the leak. Depending on the severity of the leak, I would also inform the authorities.

A.2.13 Do you know what a Redundant array of independent disks is?

This question was initially intended to ask them to briefly describe what RAID is to me and how the different configurations of RAID can differ. Still, since I worded the question incorrectly, the responses were mostly YES, so I had to award full points.

A.2.14 Do you know any appropriate recovery strategies?

This question is to check on their memory of all the recovery procedures discussed throughout the lecture. We discussed backup methods such as full, differential, and

incremental each with corresponding pros and cons. We talked about RAID and spoke about recovery sites (hot, warm, cold).

A.2.14.1 Can you provide any examples?

Recovery strategies include recovering lost data. Data recovery can be made using a RAID method. These are ways to store and backup data securely. For example, I could have my data backed up on multiple drives and afterward piece them together. Process of restoring backups. Types of backup strategies are complete (duplicate of every element), differential (only capturing the data that users changed since the last full backup), and incremental (only taking data that altered since the latest differential backup). A full backup saves the document. A differential backup saves the edits you make to the document, like in Google Docs. A downside backup saves everything with the modifications. The incremental backup saves any changes since the last download of edits.

A.3 IRB Consent Information Sheer

MARQUETTE UNIVERSITY RESEARCH INFORMATION SHEET Adaptive Pedagogy Framework for Risk Management, Incident Response, and Disaster Recovery Education Dr. Debbie Perouli Computer Science

You have been asked to participate in a research study. You must be age 18 or older to participate. This study aims to evaluate the effectiveness of the incorporated educational modules that teach students risk management, incident response, and disaster recovery. The study involves the completion of two surveys, a pre-survey that takes place before lectures are given and a post-survey that needs to be completed after the lecture and will take about 30 minutes(15 minutes each) to complete. You will be asked questions about risk management, incident response, and disaster recovery. Your name and other identifying information, including your IP address, will be collected. Your responses will be kept confidential. The risks associated with

this project are minimal, and you have no direct benefits except for some extra credits. Collection of data and survey responses using the internet involves the same risks that a person would encounter in everyday use of the internet, such as hacking or information unintentionally being seen by others. Participation is entirely voluntary, and you may withdraw from the study anytime. You can skip any questions you do not wish to answer. Your decision to participate will not impact your relationship with Marquette University or your instructors/employers.

If you have any questions about this study, you can contact Dr. Debbie Perouli at despoina.perouli@marquette.edu. If you have questions or concerns about your rights as a research participant, contact Marquette University's Office of Research Compliance at (414) 288-7570.

Thank you for your participation.

A.4 IRB Procedural Details

MARQUETTE UNIVERSITY AGREEMENT OF CONSENT FOR RESEARCH PARTICIPANTS Adaptive Pedagogy Framework for Risk Management, Incident Response and Disaster Recovery Education Dr. Debbie Perouli Computer Science Department

You have been invited to participate in this research study. Before you agree to participate, it is important that you read and understand the following information. Participation is completely voluntary. Please ask questions about anything you do not understand before deciding whether or not to participate.

A.4.1 PURPOSE

The purpose of this research study is to measure and evaluate the effectiveness of instruction materials created to educate students regarding the concept of risk management, incident response and disaster recovery. You will be one of approximately 200 participants in this research study.

A.4.2 PROCEDURES

You will review the consent form and provide consent. You may opt out as this study is completely voluntary. You will fill out a pre-survey asking you questions related to risk management, incident response and disaster recovery to assess your current knowledge during lecture time. Lectures and exercises regarding risk management, incident response and disaster recovery will then be given to increase or deepen your existing knowledge. After the lecture module concludes, you will be asked to complete the post survey that asks similar questions to evaluate your current knowledge during lecture time. Your survey responses will be evaluated by the principal investigator and student investigator.

A.4.3 DURATION

Your participation will consist of approximately 3 hours of learning activities (2 hours of lecture, 1 hour of survey.)

A.4.4 RISKS

The risks associated with participation in this study are no greater than you would experience in everyday life. Collection of data and survey responses using the internet involves the same risks that a person would encounter in everyday use of the internet, such as hacking, or information being unintentionally seen by others. BENEFITS: "There are no direct benefits to you for participating in this study. This research may benefit society by providing the society an educational framework that would help to educate more students and increase cybersecurity risk awareness in the general population."

A.4.5 CONFIDENTIALITY

Data collected in this study will be kept confidential, only the principal investigator and the student research investigator will have access to the collected data for result analysis purposes. The data will not be shared or distributed by any means

to anyone. “All your data will be assigned an arbitrary code number rather than using your name or other information that could identify you as an individual.” The key linking names to ID numbers will be stored as a protected excel sheet file that only the principal investigator and the student research investigator will have access to. Once the data collection phase is complete, the data set will be downloaded and protected with password, a copy of the protected file will be uploaded into Microsoft teams in the dissertation group where only the principal investigator and the student researcher will have access.

Another copy will be protected by password and stored locally on the student research investigator’s computer. When the results of the study are published, you will not be identified by name. Direct quotes from the responses collected from students will not be used in publication, the responses will be paraphrased. The data will be destroyed by shredding paper documents and deleting electronic files 2 years after the completion of the study. Although your responses will be deleted from the survey provider website (2 years after the completion of the study), your data may exist on backups or server logs beyond the time frame of this research project. Your research records may be inspected by the Marquette University Institutional Review Board or its designees, and (as allowable by law) state and federal agencies.

A.4.6 COMPENSATION

Students who choose to participate will be compensated through the form of a course assignment grade and extra credits given towards the corresponding course that are listed in the eligibility table (Computer Security, Introduction to Information System, Cybersecurity Seminar, Introduction to Cybersecurity).

A.4.7 VOLUNTARY NATURE OF PARTICIPATION

Participating in this study is completely voluntary and you may withdraw from the study and stop participating at any time without penalty or loss of benefits to

which you are otherwise entitled. If you choose to withdraw from the study, the data you have previously provided will be deleted. You may skip any questions you do not wish to answer. Your decision to participant or not will not impact your relationship with the investigators or Marquette University. Your decision to participate or not will not impact your grades in a negative manner, as the compensation for study completion is awarded through extra credits.

A.4.8 ALTERNATVES TO PARTICIPATION

There are no known alternatives other than to not participate in this study. If you do not wish to participate in this study you can choose to engage in alternative hands-on exercises that relates to the topics of risk management, disaster recovery and incident response. The non-research alternative will be for students to finish exercises from the labtainer virtualization environment, specifically the back up laboratory and the CyberCiege laboratory.

A.4.9 CONTACT INFORMATION

If you have any questions about this research project, you can contact Dr. Debbie Perouli at despoina.perouli@marquette.edu or Justin Wang at hsiaoan.wang@marquette.edu If you have questions or concerns about your rights as a research participant, you can contact Marquette University's Office of Research Compliance at (414) 288-7570.

I HAVE HAD THE OPPORTUNITY TO READ THIS CONSENT FORM, ASK QUESTIONS ABOUT THE RESEARCH PROJECT AND AM PREPARED TO PARTICIPATE IN THIS PROJECT.

Bibliography

[1] Abet accredits 54 additional programs in 2021, including first associate cybersecurity programsoct 13, 2021. https://www.abet.org/abet-accredits-54-new-programs-in-2021-including-first-associate-cybersecurity Accessed:2021-6-10.

[2] Build cyber skills, beat cyber threats. https://www.cybrary.it/. Accessed:2022-7-13.

[3] Cyber education wisconsin. https://cyberedu.wi.gov/Home/CyberResources. Accessed:2019-1-25.

[4] Cyber patriot. http://www.uscyberpatriot.org. Accessed: 2019-1-10.

[5] Cybersecuriy library: Clark. https://www.clark.center/home. Accessed: 2019-3-15.

[6] Gencyber. https://www.gen-cyber.com/about/. Accessed: 2019-1-21.

[7] Infosec institute. www.infosecinstitute.com/company. Accessed: 2019-3-15.

[8] Jasp: A fresh way to do statistics. https://jasp-stats.org/. Accessed:2021-7-17.

[9] Open cyber challenge platform. https://opencyberchallenge.net. Accessed: 2019-4-11.

[10] Open web application security project. http://www.owasp.org. Accessed:2018-11-30.

[11] SANs CyberStart. https://www.sans.org/CyberStartUS. Accessed:2018-11-13.

[12] Teach cyber. `http://teachcyber.org/about`. Accessed: 2019-3-10.

[13] Thousands of courses authored by our network of industry experts. `https://www.pluralsight.com/browse`. Accessed:2022-7-13.

[14] Trend micro, the fugle company: An educational game, 2015. `http://targetedattacks.trendmicro.com`, Accessed: 2012-06-22.

[15] Ahmed, I., and Roussev, V. Peer instruction teaching methodology for cybersecurity education. *IEEE Security Privacy 16*, 4 (2018), 88–91.

[16] Akinsanya, C., and Williams, M. Concept mapping for meaningful learning. *Nurse Education Today 24*, 1 (2004), 41 – 46.

[17] ATT&CK, M. `https://attack.mitre.org/`.

[18] Bellovin, S. Security by checklist. *IEEE Security Privacy 6*, 2 (Mar. 2008), 88–88.

[19] Bhatt, M., Ahmed, I., and Lin, Z. Using virtual machine introspection for operating systems security education. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (New York, NY, USA, 2018), SIGCSE '18, Association for Computing Machinery, p. 396–401.

[20] Bombal, D. Youtube channel of david bombal. `https://www.youtube.com/c/DavidBombal/`. Accessed:2022-7-13.

[21] Bort, H., and Brylow, D. Cs4impact: Measuring computational thinking concepts present in cs4hs participant lesson plans. In *Proceeding of the 44th ACM Technical Symposium on Computer Science Education* (New York, NY, USA, 2013), SIGCSE '13, ACM, pp. 427–432.

[22] Bouquet, R., Condon, D., Daniel, A., Lyon, L., Thompson, J., and Veramo, G. https://www.pbs.org/wgbh/nova/labs/lab/cyber/.

[23] Box, H. T. A massive hacking playground. https://www.hackthebox.com/.

[24] Burd, S. D., Gaillard, G., Rooney, E., and Seazzu, A. F. Virtual computing laboratories using vmware lab manager. In *2011 44th Hawaii International Conference on System Sciences* (2011), pp. 1–9.

[25] Business, V. 2017 The Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/dbir/. Accessed: 2019-04-15.

[26] Cañas, A. J., Bunch, L., Novak, J. D., and Reiska, P. Cmapanalysis: an extensible concept map analysis tool. *Journal for Educators, Teachers and Trainers 4*, 1 (2013), 36–46.

[27] Chen, P. M., and Noble, B. D. When virtual is better than real [operating system relocation to virtual machines]. In *Proceedings Eighth Workshop on Hot Topics in Operating Systems* (2001), pp. 133–138.

[28] Cheung, R. S., Cohen, J. P., Lo, H. Z., and Elia, F. Challenge based learning in cybersecurity education. In *Proceedings of the International Conference on Security and Management (SAM)* (2011), The Steering Committee of The World Congress in Computer Science, p. 1.

[29] Code.org. Computer science discoveries. https://code.org/educate/curriculum/middle-school, Accessed: 2019-04-15.

[30] Code.org. Computer science fundamentals. https://code.org/educate/curriculum/elementary-school, Accessed: 2019-04-15.

[31] Code.org. Computer science principles. https://code.org/educate/csp, Accessed: 2019-04-15.

[32] Cook, J. Edu range installation. https://github.com/edurange/edurange-flask-docs/blob/master/installation.md.

[33] Crowley, E. Experiential learning and security lab design. In *Proceedings of the 5th Conference on Information Technology Education* (New York, NY, USA, 2004), CITC5 '04, Association for Computing Machinery, p. 169–176.

[34] Deshpande, P., and Ahmed, I. Topological scoring of concept maps for cybersecurity education. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education* (New York, NY, USA, 2019), SIGCSE '19, Association for Computing Machinery, p. 731–737.

[35] Docker. Docker. https://www.docker.com/, Accessed: 2012-06-23.

[36] Du, W. Hands-on labs for security education. http://www.cis.syr.edu/~wedu/seed/. Accessed: 2019-04-15.

[37] Du, W., and Wang, R. Seed: A suite of instructional laboratories for computer security education. *J. Educ. Resour. Comput. 8*, 1 (Mar. 2008).

[38] EC-Council. Ec-council-hackers are here. where are you? www.eccouncil.org/, 2003.

[39] Fischer, E. A. Cybersecurity issues and challenges: in brief. Congressional Research Service Report prepared for Members and Committees of Congress, 2014.

[40] github.com/fcwu. Docker-ubuntu-vnc-desktop. https://github.com/fcwu/docker-ubuntu-vnc-desktop, 2021.

[41] GITHUB.COM/NCORBUK. Python-ransomware. https://github.com/ncorbuk/Python-Ransomware, 2021.

[42] GOODE, J., AND CHAPMAN, G. Exploring computer science. http://www.exploringcs.org/. Accessed: 2019-2-05.

[43] HAMMOND, J. Youtube channel of john hammond. https://www.youtube.com/c/JohnHammond010/. Accessed:2022-7-13.

[44] HU, J., MEINEL, C., AND SCHMITT, M. Tele-lab it security: An architecture for interactive lessons for security education. In *Proceedings of the 35th SIGCSE Technical Symposium on Computer Science Education* (New York, NY, USA, 2004), SIGCSE '04, Association for Computing Machinery, p. 412–416.

[45] HU, J., MEINEL, C., AND SCHMITT, M. Tele-lab it security: An architecture for interactive lessons for security education. *SIGCSE Bull. 36*, 1 (Mar. 2004), 412–416.

[46] INSTITUTE, S. Sans-the most trusted source for cyber security training, certification, and research. https://www.sans.org/, 1989.

[47] INSTITUTE, S. F. Project GUTS: Growing up thinking scientifically. http://www.projectguts.org/, Accessed: 2019-04-15.

[48] IRVINE, C. E., THOMPSON, M. F., MCCARRIN, M., AND KHOSALIM, J. Live lesson: Labtainers: A docker-based framework for cybersecurity labs. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)* (Vancouver, BC, Aug. 2017), USENIX Association.

[49] ISACA. Isaca cybersecurity, advancing the best talent and learning in technology. https://www.isaca.org/training-and-events/cybersecurity.

[50] ISC2. Cybersecurity and it security certifications and training. https://www.isc2.org/.

[51] Jens Mache, R. W., and Cook, J. Edurange a cyber-security playground. http://www.edurange.org/.

[52] Johnson, L. https://www.vulnhub.com/entry/mr-robot-1,151/, Accessed: 2012-06-23.

[53] Jones, J., Yuan, X., Carr, E., and Yu, H. A comparative study of cyber-ciege game and department of defense information assurance awareness video. In *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)* (2010), pp. 176–180.

[54] Kaza, B. T. S. Cyber4all. https://cisserv1.towson.edu/~cyber4all/, Accessed: 2012-06-23.

[55] Kimminich, B. Owasp juiceshop. https://owasp.org/www-project-juice-shop/, Accessed: 2019-04-15.

[56] Kolb, D. A. *Experiential learning: Experience as the source of learning and development*. FT press, 2014.

[57] Kuhn, K. Northwestern Mutual Encourages Students to Explore Careers in IT. www.unitedwaygmwc.org/Speak-United-Blog/Northwestern-Mutual-Encourages-Students-to-Explore-Careers-in-IT. Accessed: 2019-3-23.

[58] McLeod, S. Kolb's learning styles and experiential learning cycle. *Simply psychology* (2017).

[59] Meng, X., Perrone, L., and Aburdene, M. Approaches to undergraduate instruction in computer security. In *2005 Annual Conference*

(Portland, Oregon, June 2005), no. 10.18260/1-2–14575, ASEE Conferences. https://peer.asee.org/14575.

[60] Micco, M., and Rossman, H. Building a cyberwar lab: Lessons learned: Teaching cybersecurity principles to undergraduates. *SIGCSE Bull. 34*, 1 (Feb. 2002), 23–27.

[61] Mirkovic, J., and Benzel, T. Teaching cybersecurity with deterlab. *IEEE Security Privacy 10*, 1 (2012), 73–76.

[62] Mirkovic, J., and Benzel, T. Teaching cybersecurity with DeterLab. *IEEE Security & Privacy 10*, 1 (2012), 73–76.

[63] mmesellem. An extremely buggy web app! `https://sourceforge.net/projects/bwapp/`, Accessed: 2012-06-23.

[64] Nance, K., Hay, B., Dodge, R., Wrubel, J., Burd, S., and Seazzu, A. Replicating and sharing computer security laboratory environments. In *2009 42nd Hawaii International Conference on System Sciences* (2009), pp. 1–10.

[65] Nestler, V., Ashley, J., and Coulson, T. `https://nice-challenge.com/`, Accessed: 2012-06-23.

[66] Nestler, V., and Bose, D. Leveraging advances in remote virtualization to improve online instruction of information assurance. In *2011 44th Hawaii International Conference on System Sciences* (2011), pp. 1–8.

[67] NetworkChuck. Coffee, hacking, tech. `https://www.youtube.com/c/NetworkChuck`. Accessed:2022-7-13.

[68] of Standards, N. I., and Technology, N. I. f. C. E. https://www.nist.gov/system/files/documents/2021/12/03/NICE\%20FactSheet_Workforce\%20Demand_Final_20211202.pdf.

[69] Owens, K., Fulton, A., Jones, L., and Carlisle, M. pico-boo!: How to avoid scaring students away in a ctf competition.

[70] Padman, V., and Memon, N. Design of a virtual laboratory for information assurance education and research. 17–19.

[71] P.E., N. S. A multi-tier approach to cyber security education, training, and awareness in the undergraduate curriculum (cseta). In *2014 ASEE Annual Conference & Exposition* (Indianapolis, Indiana, June 2014), no. 10.18260/1-2–19964, ASEE Conferences. https://peer.asee.org/19964.

[72] Pi, R. Raspbeery pi 4. https://www.raspberrypi.com/products/raspberry-pi-4-model-b/, Accessed: 2012-06-23.

[73] Piazza. The incredibly easy, incredibly engaging q and a platform. https://piazza.com/, Accessed: 2012-06-23.

[74] Powell, V. J. H., Davis, C. T., Johnson, R. S., Wu, P. Y., Turchek, J. C., and Parker, I. W. Vlabnet: The integrated design of hands-on learning in information security and networking. In *Proceedings of the 4th Annual Conference on Information Security Curriculum Development* (New York, NY, USA, 2007), InfoSecCD '07, Association for Computing Machinery.

[75] PUMP-CS. Preparing the upper midwest for principles of computer science. http://pumpcs.mu.edu/, Accessed: 2019-04-15.

[76] Silver-Greenberg, J., Goldstein, M., and Perlroth, N. JP Morgan Chase hack affects 76 million households. https://dealbook.nytimes.com/

2014/10/02/jpmorgan-discovers-further-cyber-security-issues/. Accessed: 2018-11-1.

[77] Siraj, A., Ghafoor, S., Eberle, W., Rogers, M., and Haynes, A. Security knitting kit. https://www.tntech.edu/ceroc/research/sec_knit_kit_integrating_security_overview.php, Accessed: 2012-07-01.

[78] Taylor, B., and Kaza, S. Security injections: Modules to help students remember, understand, and apply secure coding techniques. In *Proceedings of the 16th Annual Joint Conference on Innovation and Technology in Computer Science Education* (New York, NY, USA, 2011), ITiCSE '11, Association for Computing Machinery, p. 3–7.

[79] Taylor, B., and Kaza, S. Security injections@towson: Integrating secure coding into introductory computer science courses. *ACM Trans. Comput. Educ. 16*, 4 (June 2016).

[80] Technologies, U. Unity technologies. https://unity.com/, Accessed: 2012-06-23.

[81] Thompson, M., and Irvine, C. Active learning with the cyberciege video game.

[82] Thompson, M., and Irvine, D. C. Active learning with the cyberciege video game. In *In Proceedings of the 4th conference on Cyber security experimentation and test* (2011).

[83] Thompson, M. F., and Irvine, C. E. Cyberciege scenario design and implementation. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)* (San Diego, CA, Aug. 2014), USENIX Association.

[84] Thompson, M. F., and Irvine, C. E. Individualizing cybersecurity lab exercises with labtainers. *IEEE Security Privacy 16*, 2 (2018), 91–95.

[85] TryHAckMe. A fun way to learn cybersecurity. `https://tryhackme.com/`.

[86] Vykopal, J., Ošlejšek, R., Čeleda, P., Vizváry, M., and Tovarňák, D. Kypo cyber range: Design and use cases. In *Proceedings of the 12th International Conference on Software Technologies - Volume 1: ICSOFT* (Madrid, Spain, 2017), C. J., C. J., M. L., M. L., van Sinderen M., and C. E., Eds., SciTePress, pp. 310–321.

[87] Weiss, R., Turbak, F., Mache, J., and Locasto, M. E. Cybersecurity education and assessment in EDURange. *IEEE Security & Privacy 15*, 03 (May 2017), 90–95.

[88] Weiss, R., Turbak, F., Mache, J., and Locasto, M. E. Cybersecurity education and assessment in edurange. *IEEE Security & Privacy*, 3 (2017), 90–95.

[89] Wharton, C., Rieman, J., Lewis, C., and Polson, P. *The Cognitive Walkthrough Method: A Practitioner's Guide*. John Wiley & Sons, Inc., USA, 1994, p. 105–140.

[90] Wiggins, G., and McTighe, J. What is backward design. *Understanding by design 1* (1998), 7–19.

[91] Wisconsin Department of Public Instruction. Wisconsin standards for computer science. `https://dpi.wi.gov/sites/default/files/imce/computer-science/ComputerScienceStandardsFINALADOPTED.pdf`. Accessed:2019-2-7.

[92] Zhang, K., Dong, S., Zhu, G., Corporon, D., McMullan, T., and Barrera, S. picoctf 2013 - toaster wars: When interactive storytelling game meets the largest computer security competition. In *2013 IEEE International Games Innovation Conference (IGIC)* (2013), pp. 293–299.