PATCH: **P**roblem-Based Learning **A**pproach for **T**eaching **C**ybersecurity and Ethical **H**acking in Community Colleges

Sajal Bhatia
School of Computer Science and Engineering
Sacred Heart University
Fairfield, USA
bhatias@sacredheart.edu

Saaid Elhadad
School of Engineering and Technology
CT State Community College, Capital
Hartford, USA
saaid.elhadad@ctstate.edu

Irfan Ahmed
Department of Computer Science
Virginia Commonwealth University
Richmond, USA
iahmed3@vcu.edu

2024 17th International Conference on Security of Information and Networks (SIN) | 979-8-3315-0973-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/SIN63213.2024.10871628

***Abstract*—Cybersecurity education incorporates a variety of teaching methods such as traditional lectures, lectures combined with hands-on exercises, and concept maps. One of the most well-known instructional methods is the use of lectures supplemented by hands-on activities. However, often these exercises either lack a strong connect with the lecture material or invariably lead students *step-by-step* in predetermined tasks, thereby hindering critical thinking and problem-solving skills. Hence, the instructional method falls short on providing students with a comprehensive understanding of complex and often associated cybersecurity concepts as encountered in real-world security incidents. The authors propose that a problem-based learning (PBL) approach can effectively address these gaps and improve cybersecurity education learning outcomes. This paper presents an application of PBL approach for teaching cybersecurity and ethical hacking in community colleges that play a crucial role in meeting the demand for cybersecurity professionals, but often face several challenges to effectively introduce cybersecurity concepts in their curriculum. Through this research, an existing course on ethical hacking is redesigned using the PBL pedagogy and offered to community college students. The course involves several PBL modules that are developed to cover all key aspects of ethical hacking and implemented using open-source software's. Each PBL module is based on a real-world cybersecurity incident and mapped to the MITRE ATT&CK framework. An external independent evaluation is conducted to assess the effectiveness of the proposed teaching methodology. Overall, the obtained results positively impact students' critical thinking, problem-solving, and communication skills, along with facilitating their understanding of key cybersecurity concepts. 100% of students reported that they enjoyed the PBL exercises. 75% of the students believed that PBL enhanced their learning of key concepts to a great extent, and remaining 25% believed that their learning of key concepts was somewhat enhanced.**

***Index Terms*—Cybersecurity, Problem-based Learning, Education, Community College, Ethical Hacking**

I. Introduction

The cybersecurity education domain comprises of a variety of curriculum design and teaching methods such as traditional lecture-based approaches, lectures coupled with hands-on exercises, peer instruction teaching, virtual machine introspection, capture-the-flag platforms, and concept maps [1–3]. Traditional lecture-based instruction combined with hands-on exercises is often considered as the *modus operandi* in cybersecurity education. A key shortcoming of this approach is the hands-on exercises themselves. These narrowly-focused lab exercises are typically designed in a very *hand holding* fashion where students are instructed to follow a step-by-step approach to complete a series of tasks associated to the topic being covered. A key missing piece in this pedagogy is the absence of problem identification and solving skills. Hence, the approach fails short in providing students with an opportunity to develop a deeper understanding of complex and invariably intertwined cybersecurity concepts – a norm in real world cybersecurity incidents. The authors believe that problem-based learning (PBL) pedagogy holds substantial promise in addressing these shortcomings and improving student learning in cybersecurity education.

Professionals in the cybersecurity field are in high demand in industry and government. The challenges for academia include producing diverse and high-quality professionals. Unfortunately, the demand is far exceeding the supply of students. Community colleges can play a crucial role in meeting the demand for cybersecurity professionals. Unfortunately, community colleges face several challenges in introducing effective cybersecurity programs for cyberinfrastructure, namely the lack of an effective curriculum compatible with the student population, insufficient computing infrastructure to support hands-on exercises and assignments, and fewer credit hours to accommodate cybersecurity courses.

The overarching goal of this research is to target the next generation of cyberinfrastructure professionals (CIP) by proposing to integrate core literacy as well as advanced cybersecurity skills into the undergraduate curriculum of community colleges through PBL. As a pilot, an existing course on ethical hacking is redesigned using PBL and offered to students at a participating community college and an external evaluation is

979-8-3315-0973-6/24/$31.00 ©2024 IEEE

conducted to assess the effectiveness of the proposed instructional method.

II. Background and Related Work

Problem-based learning (PBL) is a student-centered pedagogy in which students are presented with complex, open-ended, real-world problems to promote learning of concepts and principles, contrary to traditional lecture-style presentations [4]. In addition to covering domain-specific concepts, the PBL approach also fosters critical thinking, develops problem-solving, writing, communication and collaboration skills, enhances motivation to learn and retention of information, and promotes self-directed and lifelong learning [5]. PBL was pioneered by Barrows and originally used for medical education [6]. Over the years, the model has been adopted in other disciplines including business administration, architecture, law, engineering and social work [7, 8].

A. Teaching Methodology

In PBL, the teacher acts as a facilitator and a mentor rather than the source of solution and presents the students with a problem instead of lectures and assignments. As the students are not handed any content, the learning becomes more active and encourages students to explore and work with the specific contents identified as important by the teacher to find a solution to the problem. A simplified problem-based learning process is composed of four key steps (See Figure 1):

- Step I: Problem presentation – the teacher introduces an "ill-structured" problem and discusses its important parts.
- Step II: Problem redefinition – the teacher helps the students redefine the problem based on their prior knowledge. The problem gets decomposed into smaller parts at this stage and relevant concepts, principles, skills, and tools – both known and unknown – are identified.
- Step III: Self-study – students engage in self-study to learn new concepts, principles, skills, and tools previously identified. In this step, students share their findings with their peers and as a group work towards all possible solutions. The teacher facilitates the problem-solving process by providing feedback and encouraging students to explore all possibilities.
- Step IV: Solution presentation – students present their solutions and engage in self, peer, and instructor review of the process and the solution.

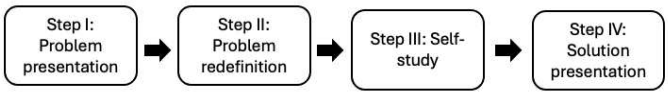

Fig. 1. Problem-Based Learning Process.

B. Effectiveness of Problem-based Learning

The effectiveness of PBL is mainly evaluated in the field of medicine [9]. For instance, it is explored in nursing education to prepare nursing professionals for a growing range of patient care services. Shin and Kim reported that problem-based learning has positive effects on student satisfaction with training, clinical education, and skills development [10]. Furthermore, Oja reported a positive impact on nursing students' critical thinking [11]. Loyens et al. [12] compared the effectiveness of three pedagogical methods: problem- based learning, traditional lecture-based, and self-study. They randomly assign students to one of the three group types and use conceptual tests immediately after the lesson and a post-test after one week. The evaluation results conclude that students in the PBL group have a higher likelihood of conceptual change. Reference [13] performed meta-analysis on problem-based learning by quantitatively synthesizing research results of previously separate but related studies, involving various statistical methods to retrieve, select, and combine effect sizes and results of the studies. They conclude that problem-based learning is an effective approach to "train competent and skilled practitioners and to promote long-term retention of knowledge and skills acquired during the learning experience."

C. Problem-based Learning in Cybersecurity

Unfortunately, the literature offers very limited studies on problem-based learning in cybersecurity education. In [14], the Higher Education Academy (HEA) assessed the effectiveness of problem-based learning in four UK universities: University of Sunderland, University of Gloucestershire, University of Warwick, and Canterbury Christ Church University. They use case studies and scenarios for the problems, and measure students' summative performance, student engagement, and confidence. They develop interventions at several levels including single lecture, week-long activity, semester, complete year, and whole program. Overall, the universities reported promising results. Importantly, this study is focused on university students, instead of community colleges, was performed in the United Kingdom (UK), and does not focus on vocational training. Our project specifically assesses problem-based learning as a better teaching method for cyberinfrastructure security in the context of community college students (in the United States), which includes many first-generation students with low-income backgrounds. Reference [15] proposed the use of PBL by mapping its working model to two security scenarios. Reference [16] presented an overview of using PBL to redesign an existing curriculum for a ethical hacking and network defense course to cover each of the required concepts as proposed by the NICE (National Institute for Cybersecurity Education) [1] framework. The authors mapped each of the developed PBL

[1] https://www.nist.gov/itl/applied-cybersecurity/nice

scenarios to the MITRE ATT&CK framework [2], however, no implementation and evaluation results were presented.

III. PBL Implementation for Ethical Hacking

As part of this project, the entire curriculum for an existing course on ethical hacking at a participating community college was redesigned using the PBL pedagogy. The redesigned course covered each of the required concepts as proposed by National Initiative for Cybersecurity Education (NICE) [3] such as reconnaissance & foot printing, network scanning, enumeration, and vulnerability analysis. Each of the 16 developed PBL scenarios is based on a real-world cybersecurity incident and is mapped to the MITRE ATT&CK framework. Each of the PBL scenarios was implemented using an experimental testbed using open-source and off-the-shelf software's.

A. PBL-based Ethical Hacking Course

The State of Connecticut (CT) is home to 12 community colleges with majority of its student population being parents, working either full-time or part-time, and replying on public transportation. As of July 1, 2023, all 12 community colleges became one single institution under the name of Connecticut State Community College [4]. In other words, this move simply created one statewide college with multiple campuses across CT thereby giving the students the freedom of movement and choice to plan their college degree around their life. Each student is registered with a "home" community college based on their preferred program of study, however, has the flexibility to take specialized courses offered by other community colleges to satisfy the degree requirements. These specialized courses are offered by a "host" college equipped with qualified faculty and resources and taken by interested students from other community colleges.

TABLE I
PBL-Based Ethical Hacking Course Data

Community College (CC)	Demographic/Race	Grade
CC-1	White	Sophomore
CC-2	Arman	Sophomore
CC-3	African American	Freshman
CC-4	Asian	Freshman
CC-3	White	Sophomore
CC-4	Hispanic or Latino	Sophomore
CC-2	African American	Sophomore
CC-2	White	Sophomore
CC-4	Not Provided	Sophomore
CC-2	Asian	Sophomore
CC-1	African American	Freshman
CC-2	African American	Sophomore
CC-1	Hispanic or Latino	Sophomore

In the current implementation of the project, the authors partnered with one community college and redesigned their existing course on ethical hacking using PBL. This course was offered in Fall 2023 and Spring 2024 semesters. All evaluation presented in this paper are for the Spring 2024 course offering which was taken by 13 students from 4 different community colleges including the host college [5]. All students were in the Networking and Cybersecurity Associate or Certificate programs of study. 77% of the students taking the course were sophomores while remaining 23% were freshmen, all across 5 different demographic/racial backgrounds (see Table I).

B. PBL Process for Ethical Hacking

PBL process as described in Figure 1 is adapted for covering various concepts in ethical hacking. The PBL process for ethical hacking comprises of four steps described below.

- Step I: Cyber-attack scenario presentation – the teacher introduces a cyber-attack scenario and discusses its important parts.
- Step II: Hypothesis definition – the teacher helps the students define a hypothesis to investigate based on the attack scenario. The hypothesis gets decomposed into smaller parts at this stage and relevant concepts, principles, skills, and tools – both known and unknown – are identified.
- Step III: Self-study – students engage in self-study to learn new concepts, principles, skills, and tools previously identified. In this step, students share their findings with their peers and as a group work towards all possible solutions. The teacher facilitates the hypothesis-testing process by providing feedback and encouraging students to explore all possibilities.
- Step IV: Solution presentation – students present their solutions that proves and disproves the hypothesis and helps figuring out the cyber-attack scenario. Students engage in self, peer, and instructor review of the process and the solution.

The class was divided into groups of 2-3 students and the aforementioned process was used for each of the PBL modules developed for the ethical hacking course.

C. PBL Modules for Ethical Hacking Course

The entire curriculum of an exisitng course on ethical hacking and penetration testing was redesigned using the PBL pedagogy. In the revised curriculum, 16 PBL modules were created covering all key aspects of ethical hacking and penetration testing. The PBL modules developed as part of this project were: (1) reconnaissance (2) social engineering (3) metasploit (4) web penetration (5) password cracking (6) SSL certificates (7) vulnerability scanning (8) enumeration (9) backdooring (10) packet crafting (11) network analysis (12) client side exploitation (13) firewall (14) SQL injection (15) buffer overflow (16) evading IDS.

[2]https://attack.mitre.org/

[3]https://www.nist.gov/itl/applied-cybersecurity/nice

[4]https://www.nbcconnecticut.com/news/local/connecticuts-12-community-colleges-merge-july-1/3055040/

[5]Names of all community colleges are anonymized and replaced with CC (community college) abbreviation to comply with the blind-review process.

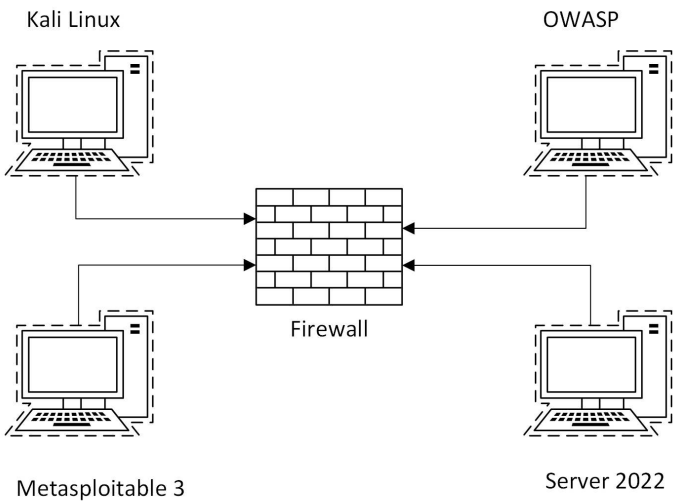

Fig. 2. Experimental Testbed for PBL Implementation

An experimental testbed using open-source and off-the-shelf software's was developed to implement all PBL modules. As shown in Figure 2, the test environment consisted of 5 virtual machines (VMs) using VirtualBox as the virtualization platform. These virtual machines were grouped into two categories, viz., attacker machine and target machines, all connected via firewall virtual machine running pfsense. For some PBL exercises, the firewall was intentionally misconfigured or disabled to emulate realistic insider attacks. Kali Linux virtual machine served as the attacker while OWASP, Metasploitable 3, and MS Windows Server 2022 served as target machines for different PBL modules.

Each PBL module is comprised of 5 parts, viz., scenario, objectives, network topology, deliverables, and resources and background material. A sample PBL module on vulnerability scanning is described below.

- **PBL Scenario:** You work as a cybersecurity analyst for a consulting firm that has been hired by a client (Harvey's Bureau of Investigation – HBI) to perform a security assessment of their network as there are concerns following some recent suspicious activity. HBI has provided you with the access of their critical system suspected to be vulnerable to cyber-attacks. The head of IT at HBI would like you to perform a security assessment of their network to identify potential vulnerabilities and provide recommendations to improve the security posture. Your task should include the following key parts:
  - Identify and prioritize vulnerabilities: Use vulnerability assessment tools such as Nmap, Nessus, OpenVAS, or any other well-known tool to scan the network for live hosts, open ports, operating systems, and potential vulnerabilities. Analyze the obtained results and identify the most critical vulnerabilities based on their severity and potential impact.
  - Develop a plan to remediate vulnerabilities: Based on the discovered vulnerabilities, develop a remediation plan, prioritizing vulnerabilities based on their severity and potential impact, and including steps to mitigate or eliminate them, such as patch management and security controls.
  - Present findings and recommendations: Prepare a report that outlines the identified vulnerabilities, potential impact of each vulnerability, and a plan to remediate them. The technical should include recommendations for improving the network security posture of the organization.
- **Network Topology:** For this PBL scenario, you will be using two VMs - Kali Linux as the attacker VM and OWASP VM as the target.
- **Objectives:** By completing this project, you will:
  - Understand the importance of network vulnerability assessments in ensuring the security of an organization's network.
  - Gain experience using network vulnerability scanners to identify potential vulnerabilities.
  - Learn how to analyze the results of a network vulnerability assessment to determine the potential risks associated with each vulnerability.
  - Develop skills in report writing and communication, specifically for presenting technical information to a non-technical audience.
  - Learn how to provide recommendations for mitigating the risks associated with vulnerabilities.
- **Resources and Background Material:** For this PBL scenario, the following resources are provided to facilitate learning and problem solving.
  - Importing a VM into VirtualBox [6]
  - Related real world cyber-attack scenario [7]
  - Kali tools documentation [8]
- **Deliverables:** At the end of the project, each group is required to submit a report including the following:
  - Executive Summary: A summary of the findings and recommendations.
  - Methodology: A brief overview of the methodology and tools used for the vulnerability assessment.
  - Vulnerability Assessment Results: A summary of the vulnerabilities found and their severity levels.
  - Risk Analysis: An analysis of the potential risks associated with each vulnerability.
  - Recommendations: Suggestions for mitigating the risks associated with vulnerabilities.

[6]https://docs.oracle.com/cd/E26217_01/E26796/html/qs-import-vm.html
[7]https://www.wired.com/story/cam4-adult-cam-data-leak-7tb/
[8]https://www.kali.org/tools/

IV. PBL Evaluation Methods, Instruments and Procedures for Ethical Hacking

An external independent evaluation was conducted to assess the effectiveness of the PBL pedagogy used in the Spring 2024 Ethical Hacking and Pen Testing course at the participating community college [17]. This section provides details of the evaluation methods, instruments and procedures, and results.

A. Evaluation Methods

The evaluation work was led by the director of Program Evaluation and Educational Research (PEER), a service center located in the College of Community Innovation and Education at the University of Central Florida (UCF). A feedback questionaire was designed and administered for all students registered in the course. This evaluation method was designed to assess and improve the PBL implementation processes and outcomes, and how well academic and other-type support activities are carried out for the duration of the course. Evaluation support was provided according to well established program evaluation standards [18] and the Guiding Principles for Evaluators established by the American Evaluation Association [9]. UCF's IRB reviewed PEER's CyberTraining Evaluation Study and determined that the proposed activities are not research involving human subjects.

B. Evaluation Instruments and Procedures

The evaluation data was collected using web-based questionnaire, and semi structured telephone interviews with community college instructor. All students enrolled in the course, elected to complete the questionnaire. The external evaluator also held regular meetings with project investigators.

1) Feedback Questionnaires: The evaluator worked with the project's principal investigators to develop web-based questionnaires housed in the evaluator's Qualtrics account, consisting of a combination of 27 Likert-type, multiple choice, and open-ended questions designed to collect student perspectives for each of the following:

- Difficulty level of the module
- Length of time to complete the module
- Effectiveness of problem-based learning exercises
- Enhancement of their understating of digital forensic tools and techniques
- Retrospective pre-post measures knowledge and skills based on module learning objectives
- What they plan to do differently because of the new knowledge/skills gained
- Their biggest takeaway
- What they liked the most and what should be improved

Community college instructor was provided with a link to the web-based questionnaire with instructions for how to embed it into a web-course quiz assignment, inviting their students to access and complete the feedback questionnaire. Instructors were asked to award extra-credit points for answering either "Yes" or "No" for whether they completed the questionnaire.

2) Instructor Interviews: PEER developed an interview protocol to collect data on community college instructor perceptions of the PBL module content. Questions were designed to extract information about whether they believed the content helped them to better prepare to serve their students, what they thought worked well, and what suggestions they had for improvement. Semi-structured interviews were conducted over the phone, lasting 20–30 minutes. The instructor interviewed gave permission to be recorded and were made aware that their feedback would help document and improve the effectiveness of the PBL content and delivery.

[9]https://www.eval.org/About/Guiding-Principles

V. PBL Evaluation Results and Discussion for Ethical Hacking

Findings for the effectiveness of PBL experiences and support provided at the participating community college was almost all positive. Students liked the hands-on practice, the structure, and how it improved their understanding. When asked, a few of the students provided recommendations for what could be improved. These results and results from the instructor interviews are described in detail in this section.

The evaluation results are obtained from the PBL feedback questionnaire, administered to students enrolled in the Spring 2024 Ethical Hacking and Pen Testing course at the participating community college at the conclusion of the semester. All students were in the Networking and Cybersecurity Associate or Certificate programs of study. For those enrolled in the course, 8 elected to complete the questionnaire. Not every respondent answered every question. Findings described below are mostly positive. For example, 100% of students reported that they enjoyed the problem-based learning exercises. These and other results are described below.

A. PBL Module Design and Content

Students were asked to give feedback on the design and content of the module.

1) Difficulty Level: When asked to rate their perception of the difficulty level of the module, seven (88%) of the students thought the difficulty was about right and one (13%) thought it was too easy. See Figure 3

2) Length: When asked their perception of the length of the module, seven (88%) felt it was about right and one (13%) thought it was too long. See Figure 4.

Below are some of the students' comments received on module's length or difficulty:

- "It was good."
- "Exercises were helpful, more exercises [for] more understanding."
- "Great time."

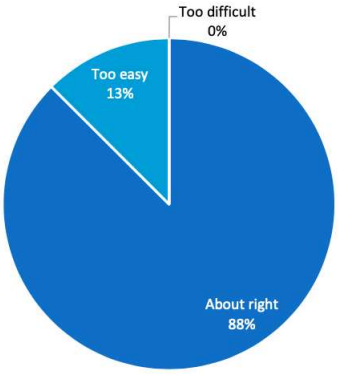

Fig. 3. Student Perceptions on Difficulty Level of PBL Modules

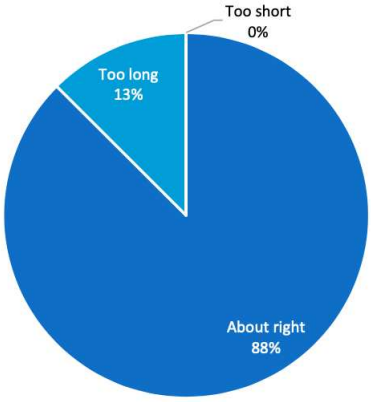

Fig. 4. Student Perceptions on Length of PBL Modules

3) PBL Experience: 75% of the students believed that the PBL exercises enhanced their learning of key concepts to a great extent, and 25% believed that their learning of key concepts was somewhat enhanced (See Figure 5).

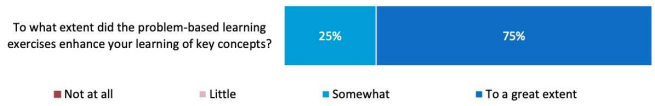

Fig. 5. Student Perspectives on Enhancement of Learning Key Concepts

Students rated their agreement with several statements evaluating the PBL experience (See Figure 6). All (100%) agreed exercises were appropriate for this course and supported the states learning outcomes. 63% of the participating students "strongly agreed" and 38% "agreed" that the contents presented in the exercises effectively prepared them for the learning experiences. All (100%) enjoyed the PBL exercises.

Below are some of the comments received on students' overall PBL experience in the course:

- "[I] wish the lesson learned in the course could continue by leaving the virtual lessons active to have more opportunity to practice."
- "[Problem]-based learning exercises were very helpful."
- "The teacher was great."
- "I enjoyed learning new things with this problem-based learning exercises."

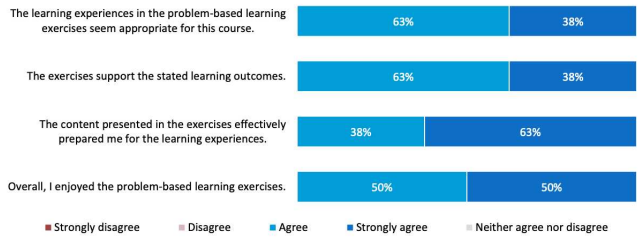

Fig. 6. Student Perspectives on PBL Modules and Learning Experiences

B. Participant Perception of Knowledge and Abilities

A part of the feedback questionnaire was geared to gauge students' perception of the acquired knowledge and abilities while being taught using the PBL method. This section presents the obtained results.

1) Understanding of Tools and Techniques: Four (50%) students agreed or strongly agreed that they have a better understanding of ethical hacking tools and techniques after the problem-based learning experiences. Two (25%) respondents strongly disagreed. See Figure 7

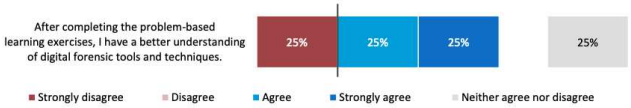

Fig. 7. Student Perspectives on Understanding of Ethical Hacking Tools and Techniques

2) Gains in Skills: Students rated their knowledge skills for each of the learning objectives shown in Figure 8, for BEFORE and AFTER completing the PBL module. After the ratings, one student wrote in the open comment box, "All these tools and skills are crucial and very important for a system security professional and continued practice is the key to fully master them."

C. Other Perceptions

1) What They Plan To Do Differently: When asked if they plan to do things differently because of the new knowledge they have gained from the module, four (57%) answered Yes, and three (43%) answered No. One did not respond. See Figure 9.

Respondents were given the opportunity to provide comments regarding what they will do differently in the future. Below are some of the comments received:

- "Practicing more to keep what I have learned."

Item	Before		After		Mean Change
	Mean	SD	Mean	SD	
Performing social engineering attacks using SET (Social-Engineer Toolkit).	0.88	1.13	**2.25**	0.89	
Performing basic reconnaissance and vulnerability scanning using Nmap and OpenVAS.	0.88	1.13	**2.25**	0.89	
Utilizing basic Linux command line tools such a grep, nano and vi.	1.13	0.83	**2.25**	0.89	
Setting up and configuring a simple computer network, assign IP address, default gateway, and perform basic network troubleshooting.	1.13	1.13	**2.25**	0.89	
Analyzing network traffic using Wireshark and tcpdump.	**0.88**	**1.36**	**1.88**	**1.13**	
Utilizing sqlmap tool for discovering SQL injection vulnerabilities in web applications.	0.50	1.07	**1.63**	1.06	
Utilizing Nikto to perform vulnerability scanning against web servers.	0.50	1.07	**1.63**	1.06	
Utilizing John the Ripper tool to perform password cracking.	0.88	1.13	**1.63**	1.06	

Notes. N = 8. Self-rated scaled for knowledge and skills: 0 = None; 1 = Minimal; 2 = Moderate; 3 = Advanced.

Fig. 8. Retrospective Pre-Post Measures for the Module: Student Self-Assessment for Knowledge and Skills

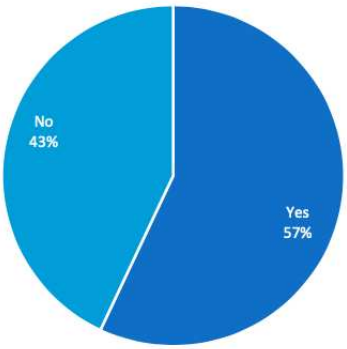

Fig. 9. Student Perspectives on Plan to Do Things Differently with New Knowledge

- "I would adjust my approach in future interactions by incorporating more visual aids when explaining programming concepts like conditional statements."
- "For now, I don't have plan, but maybe in the future."
- "I believe that participating in such exercises would greatly improve my capacity to understanding the needs of the user."

2) Biggest Takeaway: Students were asked to share their biggest takeaway from the problem-based learning exercises. Five (63%) respondents shared their thoughts. Most responses fell along the themes of the importance of adaptability, expanding on skills, and groupwork.

- Importance of Adaptability
  - "One of my biggest takeaways from problem-based learning exercises is the importance of adaptability and personalized learning approaches."
  - "I think the biggest take away would be to adapt and learn from certain events and use that knowledge and understanding for similar situations in the future."
- Expand Skills
  - "I need to continue to expand the skills learned in the course."
  - "[I] need to learn more."
- Groupwork
  - "Working in groups to solve an open-ended problem is very creative work. Critical thinking skills, problem-solving abilities, and communication skills [are important]."

3) What They Liked The Most: Responses fell into three themes, for what they liked the most about the problem-based learning experience, including: the hands-on experience, the facilitated learning, and how it developed their skills.

- Hands-on Practice
  - "Addressing the issues and interacting with the real-world situations."
  - "What I like most about problem-based learning exercises is the opportunity they provide to apply knowledge in a practical context."
  - "It is hands-on skills training for those who have no experience in the field of study."
- Facilitated Learning
  - "[The experiences] increased motivation and engagement. PBL facilitates effective content mastery because we attach emotion to the learning, rather than passively hearing a lecture."
- Skill Development
  - "[The experiences] promoted the development of critical thinking skills, problem-solving abilities, and communication skills."

4) Suggestions for Improvement: Four (50%) of the students provided suggestions for what could be improved.

- More Interaction
  - "Incorporating more interactive elements, such as simulations or interactive simulations, could further enhance the engagement and effectiveness of problem-based learning exercises."
- More Support
  - "Providing more guidance and support for users who may struggle with certain concepts or problems could be beneficial."
- Less Repetition
  - "Sometimes, it may be time-consuming, detracting from time available for other subjects yet resulting in less content learned. So, eliminating repetition is good."

5) Anything Else?: When asked if they had anything else to share about the PBL experiences or support provided throughout the module, five (63%) responded.

- Appreciation
  - "I've enjoyed the classes and this semester. Thank you for creating such a positive and engaging learning environment."

  - "I think it's a great platform to learn."
- Continued Practice
  - "The problems connect to previous courses or knowledge."
  - "Wish I could keep account active after the course over, so I could practice and continue to improve."

D. Results from Community College Instructor Interviews

The instructor reported that the courses were successful overall, and few changes were needed for the PBL components, for the next offering. The instructor had previously taught the course where the new PBL content was implemented. The instructor had taught the same course three times.

1) Student Levels and Programs of Study: The instructor taught a mix of associate-level networking & technology students, and students pursuing certificate in the field of cybersecurity. When asked about the student levels & programs of study, the instructor reported "It's an associate degree in networking and cybersecurity. Those that already have a bachelor's degree get their certificates instead. They may be interested only in the certificate, not the entire degree."

2) Module Structure: The course was conducted in a flexible format. The classes were held online, however, the instructor provided in-person meetings for students but some students remained virtual/stayed at a distance. When asked about the module structure and modality, the instructor reported "Fully online. I do assign lab and homework, but also meet weekly with students and [hold] office hours monthly. I am always available to those that need me. When we started, the grant was face-to-face. But during that process, the state has approved this consolidation. Now you have 12 colleges become one bigger college and the student can take classes from anywhere in the state. So, it's become almost infeasible to have them in one single physical location." The instructor conducted the PBL exercises by dividing the students into different teams and facilitating the problem-solving process. The instructor also assisted the teams in setting-up the required lab environment for the PBL modules.

3) Module Content: The instructor was asked to share his thoughts on the module content and the PBL experience. He rated the relevance of the topics in the problem-based learning exercises as *extremely relevant* for his course, on a scale of 1 to 5 with one being *not at all relevant* and 5 being *extremely relevant*. The instructor believed the difficulty level was appropriate for his students. He also indicated that he had provided more guidance to his students, leading to the difficulty level being appropriate.

4) Challenges and Lessons Learned: The instructor indicated that the biggest challenge was having students come together to collaborate on their work, especially with the online course modality. Additionally, he would have preferred to have multiple different images to reference for some of the PBL activities. The instructor also shared the some alterations made to the PBL exercises by including a relevant demonstration wherever necessary to assist students who felt overwhelmed with open-endedness of this teaching method. The instructor suggested adding small projects of the same topic to build upon the students' skills and acknowledged to start giving these PBL exercises early in the semester. Despite of all these challenges, the instructor strongly believed that his students enjoyed the PBL modules and he enjoyed seeing his students gain a deeper understanding of the content.

VI. Conclusion and Future Work

Several teaching methods are used in cybersecurity education such as conventional lectures, lectures coupled with hands-on exercises, peer-instruction, and concept maps. An instructional *de facto* in cybersecurity education domain is lectures supplemented with practical hands-on activities. These activities often provide students with step-by-step instructions to perform some predefined tasks, in-turn hindering their problem-solving and critical thinking skills. Through this work, the authors propose the use of problem-based learning (PBL), a student centric approach, for teaching cybersecurity and ethical hacking to community college students, thereby addressing the shortcomings of existing instructional methods. An existing course on ethical hacking was redesigned using PBL and implemented using open-source software's. An independent external evaluation was conducted to assess the effectiveness of the proposed approach. Overall, the obtained results positively impacted students' critical thinking and problem-solving skills, and facilitated comprehensive understanding of key cybersecurity concepts. 100% of students reported that they enjoyed the PBL exercises. 75% of the students believed that PBL enhanced their learning of key concepts to a great extent, and remaining 25% believed that their learning of key concepts was somewhat enhanced.

In order to accommodate students from various community colleges, the pilot PBL-based course was offered online. This flexibility, however, also presented inherent challenges in getting the students to work collaboratively, especially for outside the classroom activities, critical to PBL-based learning. The authors are exploring ways to address this challenge. Some of the students also indicated on enhancing the overall engagement and receiving additional support particularly for the first few PBL modules to further improve the effectiveness of the proposed instructional method. Additionally, the existing analysis is based on relatively low data points. As part of the future work, the authors plan to address this concern by offering multiple iterations of the proposed PBL-based course at multiple community colleges.

Acknowledgment

This work is supported by the National Science Foundation (NSF) under Award No. 2017371.

REFERENCES

[1] D. Mouheb, S. Abbas, and M. Merabti, "Cybersecurity curriculum design: A survey," in *Transactions on Edutainment XV*. Springer, 2019, pp. 93–107.

[2] I. Ahmed and V. Roussev, "Peer Instruction Teaching Methodology for Cybersecurity Education," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 88–91, 2018.

[3] S. Bhatia, S. Bhatia, and I. Ahmed, "Automated Waterloo Rubric for Concept Map Grading," *IEEE Access*, vol. 9, pp. 148 590–148 598, 2021.

[4] J. F. Barell, *Problem-based learning: An inquiry approach*. Corwin Press, 2006.

[5] B. J. Duch, S. E. Groh, and D. E. Allen, "The power of problem-based learning: a practical" how to" for teaching undergraduate courses in any discipline," *(No Title)*, 2001.

[6] H. S. Barrows, *How to design a problem-based curriculum for the preclinical years*. Springer Publishing Company, 1985, vol. 8.

[7] W. H. Gijselaers, D. T. Tempelaar, P. K. Keizer, J. M. Blommaert, E. M. Bernard, and H. Kasper, *Educational Innovation in Economics and Business Administration:: The Case of Problem-Based Learning*. Springer Science & Business Media, 2013, vol. 1.

[8] D. Boud and G. I. Feletti, "Changing problem-based learning," in *The Challenge of Problem-based Learning*. Routledge, 2013, pp. 9–22.

[9] E. H. Yew and K. Goh, "Problem-based learning: An overview of its process and impact on learning," *Health professions education*, vol. 2, no. 2, pp. 75–79, 2016.

[10] I.-S. Shin and J.-H. Kim, "The effect of problem-based learning in nursing education: a meta-analysis," *Advances in Health Sciences Education*, vol. 18, pp. 1103–1120, 2013.

[11] K. J. Oja, "Using problem-based learning in the clinical setting to improve nursing students' critical thinking: an evidence review," *Journal of Nursing Education*, vol. 50, no. 3, pp. 145–151, 2011.

[12] S. M. Loyens, S. H. Jones, J. Mikkers, and T. van Gog, "Problem-based learning as a facilitator of conceptual change," *Learning and Instruction*, vol. 38, pp. 34–42, 2015.

[13] J. Strobel and A. Van Barneveld, "When is pbl more effective? a meta-synthesis of meta-analyses comparing pbl to conventional classrooms," *Interdisciplinary journal of problem-based learning*, vol. 3, no. 1, pp. 44–58, 2009.

[14] A. Irons, H. Lallie, P. Thomas, and P. Stephens, "Application of problem based learning–cybersecurity," in *HEA Annual Conference 2017*, 2017.

[15] M. Shivapurkar, S. Bhatia, and I. Ahmed, "Problem-based learning for cybersecurity education," in *Journal of The Colloquium for Information Systems Security Education*, vol. 7, no. 1, 2020, pp. 6–6.

[16] S. Bhatia, S. Elhadad, A. Deshmukh, M. K. Yellela, and O. S. R. Vangala, "Hack the problem: A problem-based learning approach for ethical hacking and network defense curriculum," in *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 2*, 2022, pp. 1346–1346.

[17] B. Swan and I. Musengwa, "Cybertraining: Implementation: Small: Using problem-based learning for vocational training in cyberinfrastructure security at community colleges year 4 summative evaluation report (rep. no. 100shunsfcyber2024)," Program Evaluation and Educational Research Group (PEER), University of Central Florida, Orlando, FL, Tech. Rep., 2024.

[18] D. B. Yarbrough, L. M. Shulha, R. K. Hopson, and F. A. Caruthers, *The program evaluation standards: A guide for evaluators and evaluation users*. Sage Publications, 2010.