Practical Cybersecurity Education: A Course Model Using Experiential Learning Theory

Sashank Narain
sashank_narain@uml.edu
University of Massachusetts Lowell
Lowell, MA, USA

Pranathi Rayavaram
nagapranathi_rayavaram@uml.edu
University of Massachusetts Lowell
Lowell, MA, USA

Christopher Morales-Gonzalez
christopher_moralesgonzalez@uml.edu
University of Massachusetts Lowell
Lowell, MA, USA

Matthew Harper
matthew_harper@uml.edu
University of Massachusetts Lowell
Lowell, MA, USA

Maryam Abbasalizadeh
maryam_abbasalizadeh@uml.edu
University of Massachusetts Lowell
Lowell, MA, USA

Krishna Vellamchety
krishnaa_vellamchety@uml.edu
University of Massachusetts Lowell
Lowell, MA, USA

Xinwen Fu
xinwen_fu@uml.edu
University of Massachusetts Lowell
Lowell, MA, USA

Abstract

The increasing sophistication of cybersecurity threats necessitates an educational approach that blends theoretical knowledge with practical experience. Many courses focus primarily on theoretical concepts, leaving students with limited hands-on experience with real-world challenges. This paper introduces a cybersecurity course model that integrates Experiential Learning Theory to provide a comprehensive hands-on learning environment. The course covers important cybersecurity topics, including SSH, VPNs, TLS, MFA, OpenID Connect, OAuth2, web server security, high availability, replication, distributed file systems, and orchestration with Docker and Kubernetes. These topics are explored through a mix of lectures, peer presentations, and weekly hands-on team practices. Over three years, the course has been offered at our large public university with 72 students enrolled, consistently receiving high course ratings between 4.8 and 5.0. This paper discusses the course design, methodology, and outcomes, offering insights for educators to replicate and adapt the model for their own institutions.

CCS Concepts

• **Applied computing** → **Collaborative learning**; • **Security and privacy** → **Security services**; **Systems security**.

Keywords

Cybersecurity Education, Cyber Defense, Hands-on Learning, Experiential Learning Theory

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

SIGCSE TS 2025, February 26-March 1, 2025, Pittsburgh, PA, USA

© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM ISBN 979-8-4007-0531-1/25/02
https://doi.org/10.1145/3641554.3701922

ACM Reference Format:
Sashank Narain, Pranathi Rayavaram, Christopher Morales-Gonzalez, Matthew Harper, Maryam Abbasalizadeh, Krishna Vellamchety, and Xinwen Fu. 2025. Practical Cybersecurity Education: A Course Model Using Experiential Learning Theory. In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE TS 2025), February 26-March 1, 2025, Pittsburgh, PA, USA*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3641554.3701922

1 Introduction

The rapid evolution of cybersecurity threats necessitates a dynamic, practical approach to education. As threats become more sophisticated, students need hands-on experience alongside conceptual knowledge to understand real-world scenarios, develop problem-solving skills, and apply security measures effectively [19, 25]. Without experiential learning, students may be less prepared for the complex challenges they will encounter in the field [33, 37].

Despite the importance of practical skills, a significant gap exists in the cybersecurity education domain. Many cybersecurity courses emphasize theoretical concepts, providing a strong foundation but limited practical application [31]. Current practical experiences, such as take-home labs and assignments, are often limited in scope and do not fully address real-world cybersecurity demands [21]. This theory-over-practice approach can leave students knowledgeable but less equipped to handle real-world threats [17]. Consequently, graduates may struggle with practical aspects like configuring security protocols, responding to incidents, and implementing robust defenses in real-time environments [37].

Previous studies have highlighted the need for more hands-on approaches in cybersecurity education. Sharevski et al. emphasized the importance of incorporating hands-on experimentation and experiential learning to train future cybersecurity professionals [31]. Kim and Beuran discussed the effectiveness of comprehensive cybersecurity educational programs at the higher education level [21]. Holley et al. recommended hands-on strategies such as threat modeling and human-centered authentication to enhance early security

awareness [17]. Triplett found that game-based strategies significantly increase students' awareness and interest in cybersecurity careers [37]. However, many of these approaches still lack comprehensive integration of experiential learning principles in a structured curriculum, which is necessary to prepare students effectively for the modern cybersecurity industry.

To address this gap, we developed an innovative cybersecurity course model integrating Experiential Learning Theory (ELT) [23] principles. ELT is well-suited for cybersecurity education as it emphasizes learning through experience, allowing students to apply theoretical knowledge to real-world problems [31]. This course offers hands-on experience by simulating real-world cybersecurity environments using modern technologies. The curriculum covers essential topics such as Secure Shell (SSH) [40], Transport Layer Security (TLS) [2], Virtual Private Networks (VPN) [7], Multi-Factor Authentication (MFA) [18], OpenID Connect (OID) [30], OAuth2 [16], web server security, high availability (HA), replication, distributed file systems, Docker containerization [26], and Docker Swarm/Kubernetes orchestration [13]. These topics are introduced through lectures and peer presentations for foundational knowledge, followed by weekly team practices to transform learning into practical solutions. Take-home tasks further reinforce learning, requiring students to independently secure modern technologies, thus ensuring mastery of cybersecurity skills.

The course has been offered for three years at our university, with 72 students enrolled. Feedback has been consistently positive, with course ratings between 4.8 and 5.0. Students report high levels of satisfaction, engagement, and learning benefits. These ratings demonstrate the course's effectiveness in providing an immersive educational experience that equips students with the practical skills and knowledge needed for cybersecurity. The adaptable nature of this course model will enable instructors at other institutions to tailor the content and structure to their specific educational contexts and student needs. By providing a detailed framework and best practices, we aim to facilitate a broader adoption of this experiential approach in cybersecurity education.

In summary, this paper makes the following key contributions:

- We introduce an innovative course model that integrates Experiential Learning Theory to create a hands-on, experiential learning environment for practical cybersecurity education focused on modern cybersecurity topics.
- We demonstrate how the course content and activities are aligned with the current demands of the technology and cybersecurity industry, ensuring students are well-prepared for professional challenges in the domain.

The rest of this paper is structured as follows: Section 2 reviews related work in cybersecurity education. Section 3 details the course design, including the objectives, content coverage, and progressive learning approach. Section 4 explains the alignment with Experiential Learning Theory. Section 5 presents key evaluation results. Finally, Section 6 concludes the paper.

2 Related Work

Numerous studies have explored various aspects of cybersecurity education; here, we focus on a selected few for brevity.

EDURange provides a cloud-based platform that improves undergraduates' cybersecurity skills [39]. Similarly, Sharevski et al. developed an interdisciplinary course focused on secure design, allowing students from various backgrounds to apply principles of secure design through hands-on experimentation [31]. The COVID-19 pandemic necessitated innovative instruction methodologies for teaching cybersecurity online, highlighting new challenges and solutions in delivering effective education [3]. Simulation-based experiential learning has proven effective in providing non-technical workers with practical cybersecurity experience, enhancing their exposure to specific threats and opportunities for active experimentation [8]. Practical cybersecurity training exercises in controlled virtual environments improve students' understanding and problem-solving skills [38]. Gamification and virtual arenas, such as those used in CyberChallenge.IT, allow students to experiment with cybersecurity vulnerabilities and defenses in a legal and structured manner, reinforcing learning outcomes [11]. Providing hands-on experiential learning to social sciences students has significantly increased their likelihood of considering cybersecurity as a future career, demonstrating the broader applicability of these educational techniques [25]. Additionally, a project-based hands-on cybersecurity pen-testing course fosters deep learning and high levels of student satisfaction, highlighting the effectiveness of immersive, practice-oriented pedagogy [9].

These studies underscore the critical role of experiential learning in cybersecurity education, emphasizing the need for hands-on experiences to develop necessary skills. While existing courses incorporate some hands-on elements, they often focus on specific areas like secure design or online instruction. In contrast, our course comprehensively applies Experiential Learning Theory (ELT) principles across the curriculum. This ensures an immersive learning experience aligned with industry demands. By integrating iterative, real-world exercises and aligning content with industry practices, our course equips students with both theoretical knowledge and practical skills, enhancing their learning and preparation for professional cybersecurity roles.

3 Course Design

3.1 Course Objectives

The primary objectives are to develop students into proficient cybersecurity professionals capable of designing, implementing, and evaluating secure enterprise networks, security protocols, and networked services. The course also aims to equip students with advanced skills for comprehensive security and vulnerability analyses. Emphasizing teamwork, presentation skills, meeting deadlines, and working under pressure, the course ensures students are knowledgeable and possess practical expertise for complex, real-world cybersecurity environments. Integrating hands-on activities, real-world simulations, and collaborative tasks provides practical learning experiences to meet the industry's high demands.

3.2 Course Methodology

The course methodology blends conceptual knowledge with practical skills to simulate real-world cybersecurity environments, organized into two sessions each week.

Peer Presentations: Each Monday, a team of three or four students presents on a predefined cybersecurity topic detailed in Section 3.4. These presentations, about one hour long, cover security vulnerabilities, best practices, and service setup and security demonstrations. A 10-minute Q&A session follows, along with a 20-minute discussion on the topic's real-world implications. For example, a presentation on SSH includes defining the protocol, exploring alternatives, demonstrating authentication modes, identifying vulnerabilities, and suggesting mitigation strategies. Similarly, a VPN presentation covers defining VPNs, exploring alternatives, explaining operation modes, discussing tunneling modes, identifying types, and live demonstrations with tools like Wireguard [24]. Course structure, syllabus, and materials are available upon request.

Hands-on Activities: Wednesdays are dedicated to hands-on activities, where students work in teams of three or four to solve security problems based on Monday's presentations. These sessions aim to foster teamwork, meet deadlines, and solve complex challenges. Teamwork develops essential collaborative skills, while time constraints teach students to work efficiently under pressure, reflecting real-world cybersecurity environments. The sessions emphasize critical problem-solving and the practical application of security measures discussed earlier in the week. Additional details and examples of these activities are provided in Section 3.5.

Weekly Take-home Tasks: To reinforce learning, students are assigned weekly take-home tasks to replicate concepts and demonstrations presented during the week. These tasks ensure continuous engagement and provide additional practice in configuring and securing technologies independently. Recordings of presentations and demonstrations are available, allowing students to follow along and understand concepts at their own pace. By working on these tasks, students can deepen their understanding and refine their skills in a controlled, step-by-step manner.

Grading Criteria: The grading system emphasizes hands-on learning and practical application, evaluating students on their active engagement and effective application of material. Presentations, accounting for 20% of the grade, are graded rigorously to ensure thorough understanding and effective communication. The grading is strict because the instructor emphasizes the importance of these presentations for the entire class's learning experience. Hands-on activities, making up 30% of the grade, are graded leniently to encourage learning and collaboration without stress. Take-home tasks, due 14 days after the presentation, comprise the remaining 50% and are graded based on accuracy and professionalism, ensuring factual and well-documented submissions.

3.3 Course Infrastructure

The course infrastructure supports both individual and team-based learning. Each student has a personal virtual machine (VM), and each team shares a set of VMs, as illustrated in Figure 1.

Individual VMs: Each student is allocated their own VM, accessible remotely via VPN certificates to our cybersecurity lab. This setup allows students to connect from home or dorm and access their VM through SSH, enabling independent work on tasks and hands-on experience in configuring and securing systems. No UI access is provided, encouraging familiarity with shell environments and operating systems common in technology companies.

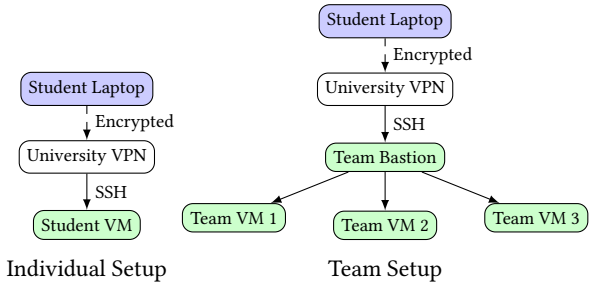

Figure 1: Course infrastructure setup.

Team VMs: Each team is provided with three VMs to facilitate collaboration. These VMs are accessed via a bastion host through the VPN using SSH. This setup mimics a real-world cloud environment, like AWS, where organizations use Virtual Private Clouds (VPCs) [20] accessed via a bastion host or VPN. These VMs simulate a multi-server environment, allowing teams to distribute workloads, implement network security measures, and practice complex configurations. This setup also promotes designing proxies, distributed file systems, and private services controlled through the bastion host. By working in a simulated cloud environment, students gain valuable, industry-relevant experience.

VM Specifications: Each VM runs an Ubuntu server with 1 vCPU, 2GB RAM, and a 10GB disk. Initially, only password-based SSH is set up, providing a clean slate for students to configure and secure their environments. This setup can be replicated using VirtualBox or VMware. Over the past three years, this infrastructure has proven efficient and reliable. For a class of up to 50 students, approximately 70 vCPUs and 140GB RAM are needed, which can be achieved with 5-10 desktop computers. The maximum enrollment so far has been 32 students, with no performance bottlenecks observed at this level. This allocation is feasible for many educational environments.

3.4 Cybersecurity Topics

The course covers a wide range of cybersecurity topics, providing a comprehensive understanding of modern enterprises and networks. These topics address current cybersecurity challenges, ensuring students gain familiarity with both foundational and cutting-edge technologies. The primary emphasis is on defensive security, aligned with industry demands, while also incorporating essential offensive techniques for a well-rounded education. Topics are categorized into different domains, each building on the previous to create a cohesive learning experience. This structure is illustrated in Figure 2. Detailed topics and materials will be available to instructors and researchers upon request.

Secure Access to Remote Systems and Networks: This domain ensures secure remote administrative access and protects data transmission across insecure networks. Tasks on SSH hardening involve defining the protocol, exploring alternatives, demonstrating authentication modes, and implementing security measures on OpenSSH [28]. Similarly, the course covers VPNs, addressing modes, tunneling methods, and implementation using tools like Wireguard. In the real world, SSH and VPNs are critical for securing remote environments and protecting sensitive data during transmission.

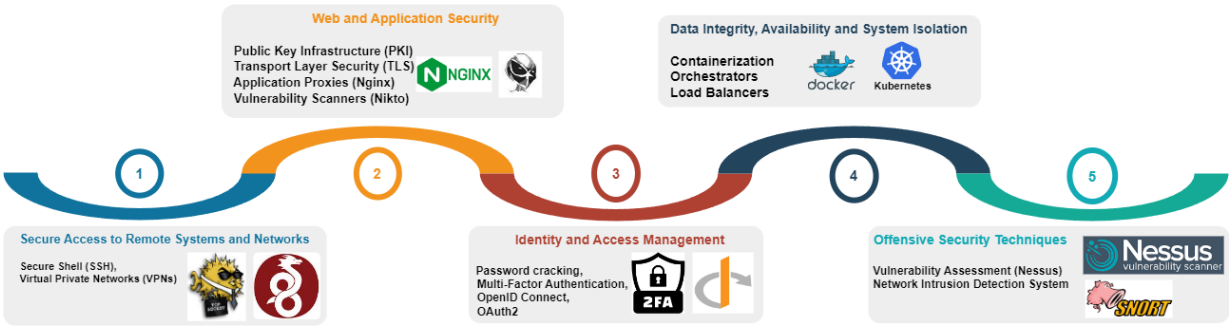

Figure 2: Structure of course topics, highlighting the breadth of the real-world and practical cybersecurity exposure for students.

Web and Application Security: This domain addresses securing web applications and services, frequent targets of cyberattacks. It includes Public Key Infrastructure (PKI) [4] and Transport Layer Security (TLS), essential for protecting web communications. A PKI task involves setting up a Certificate Authority (CA) [1] with easy-rsa [10], managing digital certificates, and understanding PKI's role in securing communications. Another task focuses on configuring application proxies like Nginx [35], setting up TLS, and enforcing strong TLS versions. The course also covers common web application attacks and mitigation strategies. A web server hardening task involves setting up an application like Nextcloud [27], a file-sharing web service, scanning for vulnerabilities with tools like Nikto [34], and implementing measures against attacks like SQL injection [14] and cross-site scripting (XSS) [6].

Identity and Access Management: This domain emphasizes secure user authentication and authorization, starting with password security. Students learn about different types of password cracking attacks—online, offline, dictionary, and brute-force—and demonstrate prevention methods. The course then covers Multi-Factor Authentication (MFA), exploring implementation methods like hardware tokens and software solutions, with students implementing MFA on Linux systems to enhance authentication. Finally, the domain covers OpenID Connect (OID) and OAuth2 protocols, focusing on implementation, security services, and real-world applications. For OID and OAuth2, students set up these protocols on a web application such as Nextcloud to explore their benefits and vulnerabilities. These tasks are crucial for preventing unauthorized access and ensuring secure user authentication in modern applications.

Data Integrity, Availability, and System Isolation: This domain ensures the reliability, integrity, and isolation of data and services, crucial for maintaining the trustworthiness and functionality of enterprise systems. Students use Docker containers for isolation, ease of deployment, and sandboxing different services. To ensure high availability and resilience, they employ orchestration technologies like Docker Swarm and Kubernetes for automated deployment, scaling, and management of containerized applications. Additionally, proxies are used to provide secure external access to web services and load balancing across multiple service replicas. By integrating these techniques into hands-on activities, students learn to build robust, scalable, and secure infrastructures, preparing them to design and manage enterprise systems requiring high availability, data integrity, and effective service isolation.

Offensive Security Techniques: The course emphasizes identifying and mitigating vulnerabilities using best practices, crucial for cybersecurity professionals. A hands-on task involves setting up a Nessus [36] vulnerability scanner to identify security weaknesses in their VMs. Key components include an introduction to vulnerability scanning, its role in enhancing system security, and its differentiation from tools like nmap [15] and Snort [32]. Students learn to interpret scan results, prioritize vulnerabilities, and implement remediation steps. This practical exercise ensures proficiency in using vulnerability scanners and prepares students to identify and mitigate security risks proactively.

3.5 Hands-on Activities

The hands-on activities offer practical, real-world cybersecurity experience by simulating real-world cybersecurity challenges. Each session begins with a 10-minute instructor overview of the day's objectives, during which high-level requirements for the activity are presented, and effort and participation are emphasized. Students are encouraged to give their best, as full points can be earned through sincere effort even if the activity is incomplete. For the remainder of the session, students work in teams on the activities, with the instructor and TA available for questions and troubleshooting. Each activity has a minimum requirement achievable by all skill levels, ensuring everyone benefits from the exercise.

We illustrate the structure of an activity with an example focusing on deploying NextCloud and configuring TLS over three Wednesday sessions. Students start by researching deployment options, selecting a database, and considering Docker usage. They deploy and secure the database, configure NextCloud, and plan proxy use for controlled access, gaining experience in deploying and securing a web application. Next, students set up an Nginx proxy to redirect traffic to the NextCloud instance. In subsequent sessions, they establish a Certificate Authority (CA) and configure TLS with CA-signed certificates to secure the proxy and web application, ensuring all communication is encrypted, resulting in a secure and well-configured system.

These activities simulate real-world scenarios, equipping students with essential skills in deploying secure web applications, managing infrastructure, and implementing best practices. Detailed descriptions of these activities will be made available to interested instructors and researchers upon request.

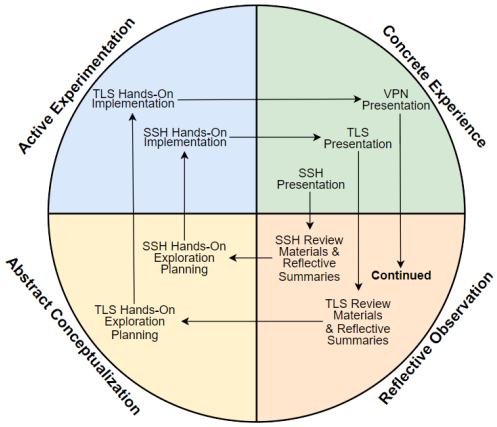

Figure 3: Illustrating the alignment of the course structure with Experiential Learning Theory (ELT).

4 ELT Alignment

Experiential Learning Theory (ELT) posits that knowledge is created through transforming experience via a cycle of concrete experience, reflective observation, abstract conceptualization, and active experimentation. Research highlights ELT's benefits in enhancing engagement, retention, and problem-solving [5, 22, 29]. ELT fosters a deeper understanding and practical application of knowledge by engaging students in active learning and reflection.

Each stage of the ELT cycle is integrated into the course structure, ensuring a comprehensive and practical understanding of cybersecurity. Each topic implements the full ELT cycle, creating a spiral effect where students continuously build on their experiences. As they progress, they revisit and deepen their understanding of core concepts, enhancing critical thinking and problem-solving abilities. This iterative process, illustrated in Figure 3, ensures students grasp individual technologies and improve their overall competence and adaptability in cybersecurity.

Concrete Experience: Students experience a topic in two forms during peer presentations. When presenting, they gain a deep understanding by researching, preparing, and teaching it to peers, internalizing the material for a stronger grasp [12]. When listening to peers' presentations, they observe, interact, engage in discussions, ask questions, and see demonstrations, reinforcing their understanding. This dual exposure ensures that students are both teaching and learning, solidifying their comprehension of the topics.

Reflective Observation: Reflection occurs post-presentation when students review the recordings. This phase involves understanding the technology's importance, assessing demonstrations, and contemplating real-world applications. By critically analyzing their presentations or observations, students identify key insights and areas for improvement. Revisiting the material deepens their understanding, prompting them to question methods and explore alternatives. This analysis helps internalize information and prepares them for hands-on application. Writing reflective summaries for weekly tasks further enhances their ability to synthesize and apply knowledge effectively.

Abstract Conceptualization: Abstract conceptualization is fostered during the hands-on activities, designed to be open-ended as detailed in Section 3.5. These activities require students to explore multiple approaches to solving security challenges. Given time constraints, student teams evaluate solutions, consider their effectiveness, and anticipate potential issues. This critical evaluation and strategic planning help students develop abstract conceptualizations of cybersecurity concepts. By analyzing methodologies, weighing pros and cons, and hypothesizing outcomes, students enhance their strategic thinking and problem-solving skills.

Active Experimentation: After selecting the most appropriate solution, students implement and test it for security, efficiency, and accuracy, configuring technologies and running security checks to ensure requirements are met. This phase consolidates their learning and exposes them to practical challenges in real-world scenarios, refining their skills and building confidence in addressing cybersecurity issues effectively.

5 Evaluation

The course evaluation was conducted over three years (Fall 2021, Fall 2022, Fall 2023) with feedback from 45 students via university-administered surveys. A total of 72 students were enrolled during this period (21 in 2021, 19 in 2022, and 32 in 2023). The voluntary, anonymized surveys assessed aspects such as student engagement, course challenge, learning outcomes, participation, assignment effectiveness, and overall course rating. Evaluations used a Likert scale from 1 (most negative) to 5 (most positive). These insights provide a comprehensive understanding of the course's strengths and areas for improvement.

5.1 Demographics

The course included students from diverse backgrounds, primarily undergraduates. Of the 45 students surveyed, 33 were undergraduates and 12 were graduates. Among undergraduates, 6 had completed up to 30 credit hours, 3 had completed 31-60 credit hours, 2 had completed 61-90 credit hours, and 22 had completed more than 90 credit hours. Graduate students did not provide their completed credit hours. This diversity in academic standing provided a broad perspective on the course's impact. Feedback from both undergraduate and graduate students highlights the course's accessibility and benefits across varying levels of experience and knowledge.

5.2 Course Evaluation

The course evaluation highlights key aspects of student engagement, challenge, participation, task effectiveness, and overall course effectiveness. The following sections detail these results and the overall results are illustrated in Figure 4.

Student Engagement and Effort: Students consistently reported significant effort in the course, with a mean rating of 4.55 out of 5 from undergraduates and 4.83 out of 5 from graduates, indicating higher effort than in other courses. This high level of commitment suggests the course effectively motivated both groups to invest time and energy into their learning. The integration of practical hands-on activities with theoretical knowledge likely inspired dedication and serious involvement, fostering an environment where students were encouraged to give their best.

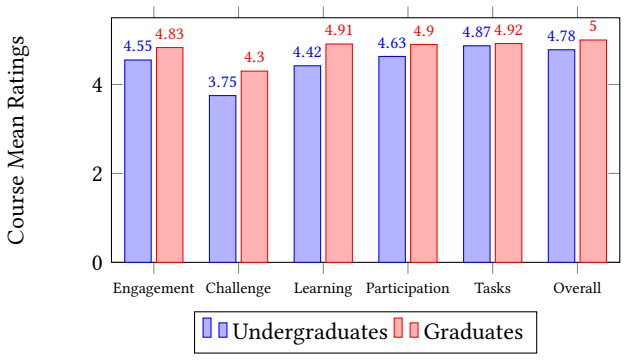

Figure 4: Summary of student feedback and evaluation.

Course Challenge and Learning Outcomes: Students found the course challenging, with mean ratings of 3.75 out of 5 for undergraduates and 4.3 out of 5 for graduates, where 5 indicates a higher challenge. This challenge appeared to motivate deeper engagement with the material. Students reported learning more in this course compared to others, with mean ratings of 4.42 out of 5 for undergraduates and 4.91 out of 5 for graduates. This feedback underscores the course's significant educational impact, indicating that the practical, hands-on approach effectively facilitated deep learning and comprehension. The data suggests that students valued the challenge, which encouraged greater effort and resulted in a higher learning experience.

Encouragement and Participation: Students felt highly encouraged to participate, with undergraduates giving a mean rating of 4.63 out of 5 and graduates 4.9 out of 5. These scores indicate the course's success in fostering an inclusive and participatory classroom environment. Active participation is essential for deep engagement and learning, showing that the course effectively promoted student involvement across different academic levels.

Effectiveness of Take-home Tasks: Tasks were rated highly effective in enhancing understanding, with undergraduates giving a mean rating of 4.87 out of 5 and graduates 4.92 out of 5. This feedback suggests that students perceived the tasks as well-designed to bridge theory and practice, focusing on real-world cybersecurity practices. Effective tasks are key to experiential learning, reinforcing concepts through practical application and integrating relevant technologies like SSH, VPNs, PKI, TLS, Docker, and Kubernetes to ensure students are well-versed in current industry practices.

Overall Effectiveness: The course structure played a pivotal role in delivering cybersecurity concepts effectively. Emphasizing hands-on, practical experiences, the course engaged students deeply and conveyed complex topics clearly. This methodical approach achieved high mean ratings: 4.87 out of 5 for teaching effectiveness among undergraduates and a perfect 5.0 among graduates. Overall course ratings were also high, with undergraduates giving 4.78 out of 5 and graduates 5.0 out of 5. These ratings underscore the course's success in meeting student expectations and learning objectives. The well-structured, experiential learning environment proved critical for teaching cybersecurity effectively, with positive feedback indicating that the course exceeded educational needs and enhanced learning outcomes.

5.3 Student Experiences

The student surveys provided valuable insights into the strengths and areas for improvement of the course.

Positive Aspects: Many students highlighted in their survey comments that the hands-on nature of the course was a significant positive. They appreciated the real-world and practical experience. One student mentioned, "The practices, because it was hands-on and got to take what we learned and actually implement it,". Another noted, "The hands-on work assigned helped understand the material." The combination of peer presentations and hands-on activities was also well-received, with comments such as, "I love how the hands-on practice allows us to set up our own infrastructure. The class presentations were a good idea too."

Students valued the course's structure and organization. Feedback included comments like, "I really enjoyed the group presentation... and the hands-on assignments," and "The way the course is designed makes the students learn more than any other course." The course's student-driven nature, with active engagement and peer teaching, was highly complimented. One student remarked, "This course was largely student-driven with a lot of team involvement," highlighting the collaborative and interactive learning environment. Another student appreciated the flexibility and freedom, stating, "I like the structure and freedom given to the students to learn the subjects effectively."

The real-world relevance of the content was another significant positive. Students felt the skills and knowledge were directly applicable to their careers. Comments like, "Real-world applications of programs being used that we might actually encounter in the future," and "Learning about tools that are actively being used in the industry," emphasize the practical benefits and career readiness fostered by the course.

Areas for Improvement: While overall feedback was positive, some students suggested areas for improvement. About five students mentioned the need for more structure and clearer instructions for hands-on activities. One student commented,"More structure for practices would be helpful," and another noted, "I think being a bit more clear/specific with some of the hands-on activities would have been helpful." A couple of students felt the weekly tasks were overwhelming, with remarks like, "Having weekly tasks with write-ups feels like a lot." Overall, the feedback indicates that while the course is highly effective and well-received, there are opportunities to enhance the structure and clarity of the hands-on activities. Addressing these areas will further improve the student experience and continue to provide an exceptional learning environment for the challenges of the cybersecurity field.

6 Conclusion

This paper presents an innovative cybersecurity course model that bridges the gap between theory and practice by integrating Experiential Learning Theory. Through a structured curriculum of lectures, peer presentations, and extensive hands-on activities, the course ensures students gain a robust understanding of foundational and advanced cybersecurity topics. Consistently high ratings from 45 students over three years underscore its effectiveness in preparing students for real-world cybersecurity challenges.

References

[1] SF Al-Janabi and AK Obaid. 2012. Development of certificate authority services for web applications. In *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*. IEEE.

[2] Ghada Arfaoui, Xavier Bultel, Pierre-Alain Fouque, Adina Nedelcu, and Cristina Onete. 2019. The privacy of the TLS 1.3 protocol. *Proceedings on Privacy Enhancing Technologies* 2019, 3 (2019). https://doi.org/10.2478/popets-2019-0065

[3] Yan Bai, Chunming Gao, and B Goda. 2020. Lessons Learned from Teaching Cybersecurity Courses During Covid-19. *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (2020). https://doi.org/10.1145/3368308.3415394

[4] Fruzsina Bene and A. Kiss. 2023. Public Key Infrastructure in the Post-Quantum Era. In *Proceedings of the 2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. https://doi.org/10.1109/SACI58269.2023.10158562

[5] Anita Boggu. 2016. THE IMPACT OF EXPERIENTIAL LEARNING CYCLE ON LANGUAGE LEARNING STRATEGIES. *International Journal of English Language Teaching* 4 (12 2016).

[6] Richard Braganza. 2006. Cross-site scripting - an alternative view. *Network Security* 2006, 9 (2006). https://doi.org/10.1016/S1353-4858(06)70425-1

[7] Setiyo Budiyanto and Dadang Gunawan. 2023. Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol. *IEEE Access* 11 (2023). https://doi.org/10.1109/ACCESS.2023.3286032

[8] John W Burris, Wesley Deneke, and Brandon Maulding. 2018. Activity Simulation for Experiential Learning in Cybersecurity Workforce Development. In *Advances in Human Factors in Cybersecurity*. Springer. https://doi.org/10.1007/978-3-319-91716-0_2

[9] Chola Chhetri. 2023. "It was a one of a kind experience:" Student Experiences and Pedagogical Design of a Project-based Hands-on Cybersecurity Pen-testing Course. In *Proceedings of the 24th Annual Conference on Information Technology Education* (Marietta, GA, USA) *(SIGITE '23)*. https://doi.org/10.1145/3585059.3611402

[10] Easy-RSA Team. 2024. *Easy-RSA Documentation*. https://easy-rsa.readthedocs.io/en/latest/ Accessed: 2024-07-12.

[11] Gaspare Ferraro, Giovanni Lagorio, and Marina Ribaudo. 2020. CyberChallenge.IT@Unige: Ethical Hacking for Young Talents. In *Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization* (Genoa, Italy) *(UMAP '20 Adjunct)*. https://doi.org/10.1145/3386392.3399311

[12] Logan Fiorella and Richard Mayer. 2013. The relative benefits of learning by teaching and teaching expectancy. *Contemporary Educational Psychology* 38, 2 (2013), 281–288. https://doi.org/10.1016/j.cedpsych.2013.06.001

[13] Avinash Ganne. 2022. CLOUD DATA SECURITY METHODS: KUBERNETES VS DOCKER SWARM. *International Research Journal of Modernization in Engineering Technology and Science* 4, 12 (2022). https://doi.org/10.56726/irjmets32176

[14] Mario Garcia. 2006. Sql Injection Attacks And Prevention Techniques. In *ASEE Annual Conference and Exposition*. https://doi.org/10.18260/1-2--195

[15] Gordon Lyon. 2024. *Nmap Network Scanning*. https://nmap.org/ Accessed: 2024-07-12.

[16] D. Hardt. 2012. The OAuth 2.0 Authorization Framework. *RFC 6749* (2012). https://doi.org/10.17487/RFC6749

[17] Buffie Holley, Dan Garcia, and Julia Bernd. 2023. Teaching Cybersecurity: Introducing the Security Mindset. In *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 2 (SIGCSE 2023)*. https://doi.org/10.1145/3545947.3569637

[18] Sanjar Ibrokhimov, Kueh Lee Hui, Ahmed Abdulhakim Al-Absi, hoon jae lee, and Mangal Sain. 2019. Multi-Factor Authentication in Cyber Physical System: A State of Art Survey. In *2019 21st International Conference on Advanced Communication Technology (ICACT)*. https://doi.org/10.23919/ICACT.2019.8701960

[19] Hwee-Joo Kam and Pairin Katerattanakul. 2019. Enhancing Student Learning in Cybersecurity Education using an Out-of-class Learning Approach. *Journal of Information Technology Education: Innovations in Practice* 18 (2019). https://doi.org/10.28945/4200

[20] Neha Kewate, Amruta Raut, Mohit Dubekar, Yuvraj Raut, and Ankush Patil. 2022. A Review on AWS - Cloud Computing Technology. *International Journal for Research in Applied Science and Engineering Technology* 10, 1 (2022). https://doi.org/10.22214/ijraset.2022.39802

[21] Eunyoung Kim and Razvan Beuran. 2018. On designing a cybersecurity educational program for higher education. In *Proceedings of the 10th International Conference on Education Technology and Computers* (Tokyo, Japan) *(ICETC '18)*. https://doi.org/10.1145/3290511.3290524

[22] Alice Y. Kolb and David A. Kolb. 2006. Learning styles and learning spaces: A review of the multidisciplinary application of experiential learning theory in higher education. *Learning styles and learning: A key to meeting the accountability demands in education* (2006).

[23] David A Kolb. 1984. *Experiential Learning: Experience as the Source of Learning and Development*. Prentice Hall.

[24] Steven Mackey, Ivan Mihov, Alex Nosenko, Francisco Vega, and Yuan Cheng. 2020. A Performance Comparison of WireGuard and OpenVPN. In *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy* (New Orleans, LA, USA) *(CODASPY '20)*. https://doi.org/10.1145/3374664.3379532

[25] Aleksandras Melnikovas, R Lugo, Kaie Maennel, A Brilingaité, Stefan Sütterlin, and A Juozapavičius. 2023. Teaching pentesting to social sciences students using experiential learning techniques to improve attitudes towards possible cybersecurity careers. *Proceedings of the European Conference on Cyber Warfare and Security* (2023). https://doi.org/10.34190/eccws.22.1.1145

[26] Dirk Merkel. 2014. Docker: lightweight Linux containers for consistent development and deployment. *Linux Journal* 2014, 239, Article 2 (mar 2014).

[27] Nextcloud. 2024. Nextcloud - Open source content collaboration platform. https://nextcloud.com/about/ Accessed: 2024-07-12.

[28] OpenSSH. 2024. OpenSSH. https://www.openssh.com/. Accessed: 2024-07-12.

[29] Steven J. Phillips, Kayleanna Giesinger, Rania Al-Hammoud, Scott Walbridge, and Chris Carroll. 2018. Enhancing student learning by providing a failure risk-free environment and experiential learning opportunities. In *2018 ASEE Annual Conference & Exposition*. https://scholar.archive.org/work/v3n2zy4hovffvpc2ctf4ycgpim/access/wayback/https://cms.jee.org/30429.pdf

[30] David Recordon and Drummond Reed. 2006. OpenID 2.0: a platform for user-centric identity management. *Proceedings of the Second ACM Workshop on Digital Identity Management* (2006). https://doi.org/10.1145/1179529.1179532

[31] Filipo Sharevski, Adam Trowbridge, and Jessica Westbrook. 2018. Novel approach for cybersecurity workforce development: A course in secure design. In *2018 IEEE Integrated STEM Education Conference (ISEC)*. https://doi.org/10.1109/ISECon.2018.8340471

[32] Snort. 2024. Snort: The Open Source Network Intrusion Detection System. https://www.snort.org/ Accessed: 2024-07-12.

[33] J. Straub. 2020. Assessment of Cybersecurity Competition Teams as Experiential Education Exercises. In *ASEE Annual Conference & Exposition*. https://doi.org/10.18260/1-2--34187

[34] Chris Sullo and David Lodge. 2024. *Nikto Web Scanner*. https://cirt.net/Nikto2 Version 2.5.

[35] Igor Sysoev. 2024. NGINX. https://nginx.org/en/ Accessed: 2024-07-12.

[36] Tenable. 2024. *Nessus Vulnerability Scanner*. https://www.tenable.com/products/nessus Accessed: 2024-07-12.

[37] Will Triplett. 2023. Addressing Cybersecurity Challenges in Education. *International Journal of STEM Education for Sustainability* 3 (01 2023). https://doi.org/10.53889/ijses.v3i1.132

[38] Luay A Wahsheh and B Mekonnen. 2019. Practical Cyber Security Training Exercises. *2019 International Conference on Computational Science and Computational Intelligence (CSCI)* (2019). https://doi.org/10.1109/CSCI49370.2019.00015

[39] Richard Weiss, Franklyn Turbak, Jens Mache, and Michael E. Locasto. 2017. Cybersecurity Education and Assessment in EDURange. *IEEE Security & Privacy* 15, 3 (2017). https://doi.org/10.1109/MSP.2017.54

[40] Tatu Ylonen and Chris Lonvick. 2006. The Secure Shell (SSH) Protocol Architecture. RFC 4251. https://www.rfc-editor.org/rfc/rfc4251.