11th LIS International Conference
Liga Ilmu Serantau 2025

ISSN: 2985-4393

Educator's Perspective on Using Capture the Flag as a Learning Platform

Mas Ayu Mohd. Ariff [1,a)], Nor Azimah Ibrahim[1,b)] and Muhammad Murshid Ramlan[1,c)]

[1]*Politeknik Mersing Johor, Jalan Nitar 86800 Mersing, Johor, Malaysia*

[a)]*Corresponding author: masayu@tvet.pmj.edu.my*
[b)]*norazimah@tvet.pmj.edu.my*
[c)]*murshid@tvet.pmj.edu.my*

Abstract. The growing demand for skilled cybersecurity professionals has prompted educational institutions to explore innovative teaching methods that connect theory with real-world practice. Capture the Flag (CTF) competitions have emerged as a gamified learning platform that simulates cybersecurity challenges, offering participants hands-on experience in cryptography, penetration testing, and digital forensics. While CTFs are widely used in universities, their use in Malaysia's Technical and Vocational Education and Training (TVET) institutions—particularly the Polytechnic and Community College (POLYCC) system—remains underexplored. This study investigates POLYCC lecturers' views on using CTF competitions as an educational tool. Guided by two research objectives (RO1: to explore lecturers' awareness and perceptions of CTF competitions; RO2: to assess the benefits and challenges of using CTFs in teaching), a mixed-methods approach was used. Quantitative data came from structured surveys, while qualitative insights were gathered through open-ended responses. Descriptive statistics and thematic analysis were used to interpret the findings. Results show that most lecturers are familiar with CTFs and support their use in academic programs. Key benefits include improved technical skills, better problem-solving abilities, and higher student engagement. However, limited time, budget, and infrastructure challenges were also identified. Thematic analysis revealed skill development as the most valued benefit, followed by teamwork, gamification, and curriculum fit. This research adds to the literature on cybersecurity education by offering evidence from Malaysia's TVET context. It provides recommendations for curriculum designers and policymakers to support CTF adoption. Future studies may examine student perspectives and long-term learning impacts.

Keywords: Capture the Flag, cybersecurity education, gamification, TVET, skill development.

1. INTRODUCTION

In today's rapidly evolving digital landscape, the demand for skilled workers in cybersecurity has never been more critical. As technology advances, the frequency and complexity of cyber threats continue to increase. Consequently, the need for highly skilled cybersecurity personnel has become essential to mitigate these risks. Malaysia, like many other countries, is experiencing a significant shortage of professionals in this field. By 2025, the Malaysian cybersecurity workforce is projected to expand from 15,248 to 27,000 skilled professionals [1], highlighting the growing demand for skilled workers. This critical shortage emphasizes the need for educational institutions to bridge the skills gap.

Public educational institutions, including Technical and Vocational Education and Training (TVET) institutions, have a pivotal role in addressing this shortage by equipping students with the necessary skills to meet industry demands. Specifically, polytechnics and community colleges (POLYCC) must adopt innovative and effective teaching methods to complement theoretical knowledge with practical skills required in the real world. Existing research at Politeknik Tuanku Syed Sirajuddin establishes a clear need for improved cybersecurity education. Ismail et al. [2] found that a commensurate level of cybersecurity knowledge does not match students' regular internet use. Furthermore, a follow-up initiative aimed at phishing awareness revealed that even practical training can suffer from

low engagement, limiting its effectiveness [3]. This evidence collectively points to the inadequacy of conventional teaching methods and argues for adopting innovative, interactive learning approaches to bridge this educational gap.

Cybersecurity education demands hands-on training to prepare students for the complexities of protecting systems from cyber threats. To address the need for practical and engaging training, Capture the Flag (CTF) competitions emerge as a salient pedagogical tool. Evidence for their applicability in educational settings is provided by frameworks like SKRCTF, which is designed to integrate real-world cybersecurity scenarios into the classroom [4]. Through CTF challenges, students actively develop competencies in key areas such as cryptography, penetration testing, and digital forensics. The efficacy of this gamified approach for building technical skills is well-documented in global contexts [5]. Despite this recognized potential, the utilization of CTFs across POLYCC institutions is not yet widespread. Consequently, expanding the deployment of CTF platforms represents a promising strategy for aligning educational outcomes with the evolving demands of the cybersecurity industry.

This study aims to explore lecturers' perspectives on using CTF competitions as an educational tool within POLYCC. It will focus on the perceived benefits, challenges, and recommendations for their integration into the curriculum. Understanding these perspectives will provide valuable insights into the potential of CTF competitions to enhance cybersecurity education in TVET institutions and contribute to addressing the industry's workforce needs.

1.1 Research Objectives

i) To explore lecturers' awareness and perceptions of CTF competitions.
ii) To assess the benefits and challenges of using CTF as a teaching tool in POLYCC.
iii) To provide recommendations for integrating CTF competitions into POLYCC's curriculum.

2. LITERATURE REVIEW

CTF in cybersecurity is performed to find a hidden file or piece of information - the "flag" - in a target environment. The adaptability of CTF challenges makes them a top way to prepare for trending cyber-attacks [6]. In the competition, participants will solve a series of challenges that include cryptography, reverse engineering, web security, and digital forensics. These competitions have become effective teaching methods in cybersecurity, as the competition allows students to apply theoretical knowledge in a practical, problem-solving environment. CTFs have been integrated into many higher education institutions worldwide to foster a deeper understanding of cybersecurity concepts and enhance student engagement.

Several studies have highlighted the educational benefits of CTF competition. For example, research by [7], examines student motivation in participating in cybersecurity CTF competitions. Results also showed that interest and attainment were the elements of motivation that were most salient. This study contributes to CTF developers and educators' efforts to build CTFs that successfully engage students in cybersecurity education. [8] conducted a comprehensive survey on cyber competitions, including Capture The Flag (CTF) events, emphasizing their role in enhancing cybersecurity education. They found that such competitions effectively engage students by incorporating gamification techniques, which make learning more interactive and enjoyable. The study also highlighted that CTFs help in developing practical skills relevant to real-world cybersecurity challenges, thereby bridging the gap between theoretical knowledge and practical application. Moreover, the authors noted that these competitions can attract a diverse student body, fostering inclusivity in cybersecurity education. However, they also pointed out challenges such as the high knowledge barrier for beginners and the need for better interoperability between competition platforms.

Despite the widespread use of CTF competitions in higher education, there is a noticeable gap in research concerning their use in TVET institutions, particularly in Malaysia's POLYCC. TVET institutions often focus on practical skills, and as such, the integration of CTF competitions could be a beneficial way to enhance students' technical abilities. However, the literature on this topic is sparse, with limited studies investigating lecturers' perspectives on implementing such competitions in the context of TVET education in Malaysia. Therefore, this research aims to fill this gap by exploring the views of lecturers in POLYCC regarding the potential of CTF as an educational tool.

While numerous studies have explored the use of CTF in higher education and its potential benefits in cybersecurity training, there remains a lack of research focused on TVET institutions like POLYCC. Additionally,

most existing studies focus on student outcomes, with limited attention given to lecturers' perspectives and the challenges of implementing CTF in resource-constrained environments. This research will provide valuable insights into the effectiveness of CTF as an educational platform in POLYCC, highlighting the barriers to implementation and offering practical recommendations for educators and policymakers.

3. RESEARCH METHODOLOGY

3.1 Research Design and Participants

This study used a convergent parallel mixed-methods design [11] to evaluate lecturers' perspectives. Purposive sampling was employed to recruit 20 lecturers from 6 POLYCC institutions, selected based on their involvement in CTF activities and varied teaching experience (0-5 to 16+ years).

3.2 Data Collection

A single online survey was used for data collection. The instrument, developed based on research objectives and a literature review [6, 7, 8, 10], contained:

a) **Quantitative sections:** Likert-scale and multiple-choice questions on awareness, perceived benefits, and challenges.

b) **Qualitative section:** Open-ended questions on expectations and recommendations.

3.3 Data Analysis

a) Quantitative Analysis: Descriptive statistics (frequencies, percentages, means) were applied to the closed-ended responses using Microsoft Excel.

Output: Descriptive tables summarizing trends (e.g., Table 1, 3, 5, 6).

b) Qualitative Analysis: Thematic analysis followed Braun and Clarke's [12] framework, involving familiarization, code generation, and theme development.

Output: Key themes (e.g., Skill Development, Resource Constraints) supported by direct quotes (See Section 4.5).

The separate quantitative and qualitative results were integrated during interpretation to provide a comprehensive understanding of the research problem.

4. RESULTS

4.1 Awareness and Familiarity

Table 1: Familiarity Level by Teaching Experience
Question: *What is your level of familiarity with CTF competitions?*

Teaching Experience	Very Familiar	Somewhat Familiar	Not Familiar	Mean
0-5 years	4 (57%)	3 (43%)	-	**2.57**
6-10 years	1 (50%)	1 (50%)	-	**2.50**
11-15 years	2 (33%)	4 (67%)	-	**2.33**
16+ years	2 (40%)	2 (40%)	1 (20%)	**2.20**
Total	**9 (45%)**	**10 (50%)**	**1 (5%)**	**20**

The survey shows that 45% of lecturers are Very Familiar with CTF competitions, while 50% are Somewhat Familiar and only 5% are Not Familiar, indicating generally high awareness across teaching experience levels. Younger lecturers (0–5 years of experience) reported higher familiarity (57% Very Familiar) compared to senior lecturers, suggesting generational differences in exposure.

Table 2: Experience in Technical Preparation and Execution by Teaching Experience
Question: *Have you ever been involved in the technical preparation and execution of a CTF competition?*

Teaching Experience	Yes	No	Total
0-5 years	6 (67%)	3 (33%)	9
6-10 years	1 (50%)	1 (50%)	2
11-15 years	3 (60%)	2 (40%)	5
16+ years	2 (50%)	2 (50%)	4
Total	**12 (60%)**	**8 (40%)**	**20**

All respondents (100%) reported having participated in or organized a CTF competition, showing that lecturers had at least baseline exposure across the cohort. However, when asked about technical preparation, only 60% had been directly involved, while 40% had no such experience. This indicates a gap between general awareness and deeper technical engagement.

4.2 Benefits and Challenges

CTF Integration into Academic Programs

Table 3 : Support for CTF Integration into Academic Programs by Teaching Experience
Question: *Do you think CTF competitions should be integrated into academic programs?*

Teaching Experience	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Mean
0-5 years	6 (67%)	2 (22%)	1 (11%)	-	-	**4.56**
6-10 years	1 (50%)	1 (50%)	-	-	-	**4.00**
11-15 years	3 (60%)	1 (20%)	1 (20%)	-	-	**4.50**
16+ years	2 (50%)	2 (50%)	-	-	-	**4.50**
Total	**12 (60%)**	**6 (30%)**	**2 (10%)**	**0 (0%)**	**0 (0%)**	**20**

There was overwhelming support for integrating CTFs into academic programs, with 85% of respondents either Strongly Agreeing or Agreeing (Mean = 4.45/5), reflecting broad endorsement across all teaching experience levels.

Most lecturers (70%) preferred a mixed approach combining in-class activities with inter-POLYCC competitions, while 20% prioritized in-class activities only and 10% supported competitions exclusively. This highlights the demand for flexibility in implementing CTF.

Expectation

Table 4: Expectations for CTF Competitions as an Academic Learning Platform
Question: *What are your expectations for CTF competition as a platform designed for academic purposes?*

Theme	Response
Skill Development	**12 (63%)**
Academic Integration	**8 (42%)**

Collaboration & Access	**6 (32%)**

Educators also identified their expectations of CTF as an academic platform: the majority emphasized skill development (63%), followed by academic integration (42%) and collaboration and access (32%). These findings suggest that lecturers value CTF not only for technical training but also for curriculum enhancement and institutional collaboration.

4.3 Benefits and Challenges

Table 5: Overall Perceived Value
Question: *In your opinion, what is the value of CTF competitions for students?*

Benefit	Response
Enhances technical skills	18 (90%)
Builds problem-solving skills	20 (100%)
Develops teamwork	19 (95%)
Fostering ethical hacking practices	17 (85%)
Prepares for real-world challenges	18 (90%)

Lecturers strongly recognized the value of CTF competitions in education. All respondents (100%) agreed that CTFs improve problem-solving skills, while 95% highlighted teamwork, 90% technical skills, 90% real-world preparation, and 85% ethical hacking practices. These results confirm that lecturers perceive CTF as a comprehensive tool for developing both technical and soft skills.

4.4 Key Challenges

Table 6: Barriers in CTF Competition Implementation
Question : *What challenges might you face in implement CTF competition at your institution?*

Implementation Barriers	Response
Lack of technical expertise	12 (60%)
Limited time for preparation	17 (85%)
Budget constraints	17 (85%)
Limited infrastructure or resources	17 (85%)
Student engagement issues	4 (20%)

At the same time, several challenges were highlighted. The most common barriers were limited preparation time, budget constraints, and inadequate infrastructure (85% each). A further 60% reported a lack of technical expertise, while only 20% mentioned student engagement issues. This indicates that systemic and resource-related barriers are more pressing than motivational ones.

4.5 Thematic Analysis of Open-Ended Responses

Thematic analysis of lecturers' open-ended responses revealed four key themes:

i) Skill Development: Most lecturers emphasized that CTFs strengthen technical skills and bridge the gap between theory and practice.
"CTF provides real-world practice that textbooks cannot offer."
ii) Teamwork and Collaboration: Respondents highlighted the role of CTF in promoting peer learning and cooperation.

iii) Gamification and Engagement: The competitive element was seen as effective in motivating students and sustaining interest in cybersecurity topics.
iv) Curriculum Fit and Sustainability: Lecturers stressed the importance of integrating CTF within existing courses for long-term adoption.

Summary

Overall, the results demonstrate that POLYCC educators are familiar with CTF competitions and strongly support their integration into academic programs. They value CTF primarily for skill development, problem-solving, and real-world preparation, while also recognizing its potential for teamwork and ethical practices. However, widespread adoption faces challenges, particularly resource limitations and technical expertise gaps. These findings directly address the research objectives by highlighting both the benefits and barriers of CTF as a learning platform, while also shaping recommendations for future curriculum integration.

5. DISCUSSION

The findings demonstrate that educators in POLYCC have a positive orientation toward the adoption of CTF competitions in academic settings. In addressing RO1, awareness and familiarity were relatively high, with nearly all lecturers having prior experience participating in or organizing CTF activities. This aligns with studies by Balon and Baggili (2023) and Beauchamp et al. (2024), which highlight CTF as a globally recognized tool in cybersecurity education. However, senior lecturers were found to be less familiar with CTF, suggesting the importance of peer-led workshops or structured professional training to close this exposure gap.

For RO2, lecturers consistently emphasized the benefits of CTFs for POLYCC students, particularly in developing problem-solving abilities, technical competency, teamwork, and ethical practice. These outcomes align with global findings on gamified learning; the high value placed on engagement supports the work of Marciano et al. [9], who identified gamification as a key property for effective and motivating cybersecurity training. Furthermore, the recognition of CTFs as a tool for real-world preparation resonates with the comprehensive ENISA report [10], which positions CTF events as a vital platform for developing practical skills relevant to the industry. However, despite this strong endorsement and the established efficacy of CTFs, their adoption within the POLYCC system faces significant systemic challenges. Our findings identify that limited preparation time, budget constraints, and inadequate infrastructure are the most pressing barriers, alongside a need for greater technical expertise among educators. This indicates that the primary obstacles to implementation within the Malaysian TVET context are not pedagogical hesitancy but rather resource-related limitations that must be addressed to unlock the potential of CTFs, as recognized in global best practices [10].

Finally, in relation to RO3, the study highlights that lecturers expect CTFs to serve not only as a tool for skill development but also as an integrated component of academic programs. The strong preference for both in-class activities and inter-POLYCC competitions suggests that a hybrid approach would best support sustainability. A practical recommendation is to embed CTFs within project-based courses or as elective modules, while also fostering inter-institutional competitions to encourage collaboration and benchmarking across POLYCC. Partnering with industry stakeholders could further strengthen these initiatives by ensuring that CTF challenges reflect real-world cybersecurity problems, thereby bridging academic learning and workforce needs.

6. CONCLUSION

This study confirms that POLYCC educators view Capture the Flag competitions as an effective learning platform that enhances technical skills, problem-solving, and teamwork. Despite strong support, challenges such as time, budget, and infrastructure constraints, along with limited technical expertise, remain key barriers to implementation. Embedding CTF into courses, providing institutional support, and building lecturer capacity are essential steps to ensure sustainability.

For future research, studies could explore students' perspectives on CTF-based learning, examine the long-term impact of CTF integration on skill development, and investigate scalable models for curriculum adoption across

POLYCC. Collaboration with industry stakeholders could also be studied to ensure that CTF challenges reflect real-world cybersecurity demands.

REFERENCES

[1] L. Fourrage, "Malaysia Cybersecurity Job Market: Trends and Growth Areas for 2025," *Nucamp*, 2025. [Online]. Available: https://www.nucamp.co/blog/coding-bootcamp-malaysia-mys-malaysia-cybersecurity-job-market-trends-and-growth-areas-for-2025

[2] N. N. S. Ismail, T. K. Tunku Norizan, and N. L. Hashim, "Internet Usage and Cybersecurity Awareness among Students at Politeknik Tuanku Syed Sirajuddin," Politeknik & Kolej Komuniti Journal of Social Science and Humanities, vol. 9, no. 1, pp. 46–59, 2024. [Online]. Available: https://app.mypolycc.edu.my/journal/PMJSSH/article/download/646/374/2228

[3] N. N. S. Ismail, T. K. Tunku Norizan, and N. L. Hashim, "Enhancing Information Security Awareness on Phishing Among IT Students: A Pilot Test Case Study at Politeknik Tuanku Syed Sirajuddin," Journal of Digital System Development, vol. 4, no. 2, pp. 58–71, Oct. 2023. [Online]. Available: https://e-journal.uum.edu.my/index.php/jdsd/article/view/21390

[4] M. S. S. M. Rasid, M. F. I. Othman, A. Z. Jamin, et al., "SKRCTF: A Capture The Flag (CTF) Framework for Cybersecurity Classroom Teaching," Bulletin of Electrical Engineering and Informatics, vol. 11, no. 4, pp. 2123–2133, Aug. 2022.

[5] D. Tidmarsh, "Why Is Capture the Flag (CTF) Important in Cyber Security?," *EC-Council*, Sep. 27, 2023. [Online]. Available: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/capture-the-flag-ctf-cybersecurity

[6] J. Goglio, "A Beginner's Guide to Capture the Flag Cybersecurity Challenges," *Tec-Refresh*, 2024. [Online]. Available: https://tec-refresh.com/blog/capture-the-flag-cybersecurity

[7] C. Beauchamp and H. Matusovich, "A Mixed-Method Study Exploring Student Motivation Participating in Cybersecurity CTF Competitions," *Cybersecurity Pedagogy and Practice Journal*, vol. 3, no. 1, pp. 4–26, 2024. [Online]. Available: https://cppj.info/2024-3/n1/CPPJv3n1p4.html

[8] T. Balon and I. Baggili, "Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education," *Education and Information Technologies*, vol. 28, pp. 1–33, 2023. [Online]. Available: https://doi.org/10.1007/s10639-022-11451-4

[9] V. Marciano, J. du Toit, and R. Maluleka, "Gamification in Cybersecurity Training: High-Level Properties of Cybersecurity Games," in *Human Aspects of Information Security and Assurance (HAISA 2024)*, IFIP Advances in Information and Communication Technology, vol. 722, pp. 74–87, Springer, Nov. 2024. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-72563-0_6

[10] European Union Agency for Cybersecurity (ENISA), *CTF Events: Contemporary Practices and State-of-the-Art in Capture-the-Flag Competitions*, May 2021. [Online]. Available: https://www.enisa.europa.eu/publications/ctf-events/@@download/fullReport

[11] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qual. Res. Psychol*., vol. 3, no. 2, pp. 77–101, 2006.

[12] J. W. Creswell and V. L. Plano Clark, Designing and Conducting Mixed Methods Research, 3rd ed. Thousand Oaks, CA, USA: Sage Publications, 2017.