Information Technology Education Journal
E-ISSN: 2809-798X; P-ISSN: 2809-7971
https://journal.unm.ac.id/index.php/INTEC/index

The Effectiveness of Capture The Flag as a Network Security Practical Intervention on Students' Self-Efficacy and Learning Outcomes

A. St.Khadijah Ridwan[1], Ummu Radiyah[2*], Muhammad Ihksan Malik[3], Muhammad Nauval Pattiroi[4], Muslika[5], Nining Ulul Fajri[6], Nirwana Amir[7]

[1,3,4,5,6,7]*Program Studi PPG, Universitas Negeri Makassar, Makassar, Indonesia*
[2]*Universitas Nusa Mandiri, Jakarta, Indonesia*

Corresponding e-mail : ummu.urd@nusamandiri.ac.id

ARTICLE INFO

Keywords:

Capture the Flag (CTF);
Self-efficacy;
Network security;
Education;
Gamification;
Learning outcomes

Article History

Received: October 23, 2025
Revised : November 20, 2025
Accepted : December 17, 2025

ABSTRACT

This study aimed to evaluate the effectiveness of Capture the Flag (CTF) competitions in improving self-efficacy and learning outcomes in network security education. Specifically, it explored whether participation in CTF competitions enhances students' confidence in their cybersecurity abilities and their understanding of network security concepts compared to traditional practical exercises. A quasi-experimental design was used with 60 undergraduate students enrolled in a network security course. Participants were randomly assigned to an experimental group (CTF competition) and a control group (traditional practical exercises). Data were collected through pre-test and post-test measures of self-efficacy, a final exam, and a practical skills assessment. The experimental group participated in a two-week CTF competition, while the control group engaged in structured, instructor-guided exercises. The results indicated that the experimental group showed a significant increase in self-efficacy (from 3.2 to 4.0) and performed better on both the final exam (85% vs. 75%) and the practical skills assessment (88% vs. 78%) compared to the control group. These findings suggest that CTF competitions positively impact students' confidence and technical skills in network security. The study's quasi-experimental design limits the ability to draw causal conclusions. Additionally, the relatively small sample size and single-institution setting reduce the generalizability of the findings. Future studies with larger and more diverse samples are needed to confirm these results. This study contributes to the growing body of research on gamification in cybersecurity education, showing that CTF competitions can effectively enhance both self-efficacy and learning outcomes. It highlights the value of integrating such competitions into curricula to improve student engagement and preparedness for real-world cybersecurity challenges.

To cite this article : Ridwan, A. S. K., Radiyah, U., Malik, M. I., Pattiroi, M. N., Muslika, M., Fajri, N. U., & Amir, N. (2025). The effectiveness of capture the flag as a network security practical intervention on students' self-efficacy and learning outcomes. Information Technology Education Journal, 4(4), 811–824. https://doi.org/10.59562/intec.v4i4.11191

INTRODUCTION

In the evolving field of cybersecurity education, practical training is critical to preparing students for real-world challenges. One of the most effective methods for enhancing hands-on learning is through Capture the Flag (CTF) competitions, which are widely used in cybersecurity training [1]; [11]; [2]. CTF competitions involve participants solving security-related tasks to capture virtual flags, often mimicking real-world cybersecurity attacks and defenses. These

challenges help students build a deep understanding of cybersecurity tools and concepts through experiential learning.

Cybersecurity education faces unique challenges, particularly in ensuring students gain practical skills while developing their self-efficacy, or their belief in their ability to execute tasks. According to Bandura [3]; [12], self-efficacy plays a crucial role in shaping an individual's confidence and ability to approach challenging tasks, which is vital in fields like cybersecurity where technical challenges are constant. This concept has been explored in various learning environments, yet few studies have directly measured the impact of CTF competitions on self-efficacy within the context of network security education.

Studies have shown that practical, game-based learning environments like CTFs can significantly enhance student engagement and motivation [5]. However, there remains a gap in understanding how such interventions impact students' self-efficacy and overall academic performance in cybersecurity courses. Several studies have measured the outcomes of CTFs on technical skills, but fewer have focused on how these competitions influence psychological factors such as self-efficacy or learning outcomes [2]; [4].

Literature Review

The use of CTF competitions in cybersecurity education has been growing steadily. Several studies have highlighted the effectiveness of CTFs in fostering technical skills, such as ethical hacking, network defense, and penetration testing [6]. These competitions provide a controlled environment where students can experiment with different tools, techniques, and approaches without real-world consequences. In this sense, CTFs align with active learning strategies that encourage students to actively engage with the material, thus enhancing retention and practical application of knowledge [7].

Self-efficacy, defined by Bandura [3] as the belief in one's capabilities to organize and execute the courses of action required to manage prospective situations, is a key factor in student success. In a study by [8], it was shown that high self-efficacy correlates with improved learning outcomes and persistence in challenging educational contexts. In cybersecurity education, where students often face complex and high-stakes tasks, self-efficacy could play a crucial role in determining their ability to navigate difficult scenarios successfully. Recent research has begun to explore the intersection of self-efficacy and technical skills in cybersecurity, with promising findings that suggest interventions targeting self-efficacy can lead to improved learning outcomes [5]; [9].

While CTFs have shown potential in improving students' technical competencies, their effect on self-efficacy and academic outcomes has not been widely researched. Some studies have highlighted the role of gamification and competition in enhancing motivation, but there is a lack of empirical studies specifically targeting self-efficacy in the context of CTFs [2]. This gap represents an important area for further exploration, particularly considering the increasing reliance on CTFs as a tool for cybersecurity training.

Gap Analysis

The current body of literature on CTFs in cybersecurity education is robust in terms of its focus on technical skill development, engagement, and motivation [5]. However, the literature is limited when it comes to examining the psychological impacts of these competitions, particularly in terms of self-efficacy and its relation to student performance. Few studies have explored how the challenging, competitive environment of CTFs influences students' confidence in their cybersecurity skills, which in turn may affect their learning outcomes.

Furthermore, while CTF competitions have been used in various academic settings, there is insufficient research that compares the effects of CTF participation with more traditional forms of hands-on learning in terms of both self-efficacy and academic performance. This study aims to fill this gap by providing empirical evidence on the role of CTF competitions as an intervention in

network security education, specifically analyzing their impact on self-efficacy and learning outcomes compared to a control group engaged in conventional practical exercises.

Rationale of the Study

This study is designed to investigate the effectiveness of CTF competitions as an intervention for improving students' self-efficacy and learning outcomes in network security courses. The rationale for conducting this study is to explore the impact of a widely adopted cybersecurity education tool on the psychological and academic development of students. With cybersecurity threats becoming increasingly sophisticated, there is a growing need for robust educational strategies that not only impart technical knowledge but also foster the confidence and problem-solving skills required to face these challenges.

By focusing on self-efficacy, this study aligns with current trends in educational psychology, which emphasize the importance of students' beliefs in their capabilities for success [10]; [13]; [14]. If CTF competitions are found to significantly improve self-efficacy, they could provide an additional benefit to cybersecurity education by not only enhancing technical skills but also fostering the mindset necessary to tackle real-world cybersecurity problems with confidence [15].

Purpose or Hypotheses of the Study

The purpose of this study is to evaluate the effectiveness of CTF competitions as an intervention in improving self-efficacy and learning outcomes among students in a network security course. Specifically, this study will test the following hypotheses:

1. **Hypothesis 1 (H1)**: Students who participate in a CTF competition will exhibit higher self-efficacy in cybersecurity tasks compared to students in a control group who engage in traditional practical exercises.
2. **Hypothesis 2 (H2)**: Students who participate in a CTF competition will demonstrate better learning outcomes in network security concepts compared to students in the control group.

The findings of this study are expected to contribute to the ongoing discourse on best practices in cybersecurity education by providing evidence of the psychological and academic benefits of CTFs. Additionally, the study will offer insights into how educators can enhance students' learning experiences by integrating gamified, hands-on approaches into the curriculum [16]; [17].

METHOD

Research Design

This study adopts a quasi-experimental research design to investigate the impact of Capture the Flag (CTF) competitions on students' self-efficacy and learning outcomes in a network security course [19]; [18]; [20]. The study employs a pre-test/post-test control group design, where participants are divided into an experimental group, which participates in the CTF competition, and a control group, which engages in traditional practical exercises. The design allows for a comparison between the two groups' changes in self-efficacy and academic performance, with the aim of assessing the effectiveness of the CTF intervention.

Participants

The participants in this study were undergraduate students enrolled in a network security course at a university. A total of 60 students were recruited, with 30 students assigned to the experimental group and 30 students assigned to the control group. The students in both groups had similar academic backgrounds, with prior knowledge of basic networking concepts and a general understanding of cybersecurity. Participants were randomly assigned to the groups

to control for selection bias and ensure that both groups were comparable in terms of baseline characteristics.

Inclusion criteria for participation were as follows:

1. Students who are enrolled in the network security course.
2. Students who have prior exposure to basic cybersecurity concepts (e.g., networking, ethical hacking, basic security principles).
3. Students who consented to participate in the study and agreed to complete pre-test and post-test evaluations.

Intervention

The intervention for the experimental group was a CTF competition, which was incorporated into the network security course curriculum. The CTF competition involved a series of security-related challenges, including tasks related to ethical hacking, cryptography, and network defense. The CTF was designed to mimic real-world cybersecurity scenarios, and the students were tasked with solving these challenges in a limited amount of time. The competition was structured over a period of two weeks, with participants required to complete the challenges individually.

The control group, on the other hand, participated in traditional practical exercises. These exercises involved similar cybersecurity tasks but were completed in a more conventional lab setting without the competitive or gamified elements of the CTF. The control group engaged in structured, instructor-guided activities focused on hands-on practice with the tools and techniques used in the CTF challenges, such as penetration testing, network traffic analysis, and security auditing.

Both groups received the same amount of instructional time, with each group spending a total of four hours per week on practical exercises related to network security. The CTF competition and the traditional exercises were designed to cover similar learning objectives, including the application of cybersecurity tools, problem-solving techniques, and defensive strategies.

Measures

To assess the impact of the CTF competition on students' self-efficacy and learning outcomes, the following measures were used:

1. **Self-Efficacy Scale**:
   The primary measure for self-efficacy was the *Cybersecurity Self-Efficacy Scale* (CSES), developed by [1]. The scale consists of 10 items that assess students' confidence in their ability to perform specific cybersecurity tasks, such as identifying vulnerabilities, conducting penetration testing, and responding to security incidents. Students completed the scale before and after the intervention to measure changes in their self-efficacy. The CSES uses a Likert scale ranging from 1 (not confident at all) to 5 (very confident), with higher scores indicating higher self-efficacy.
2. **Learning Outcomes**:
   Learning outcomes were measured through a final exam and a practical skills assessment. The final exam consisted of multiple-choice questions and short-answer questions, which tested students' knowledge of network security concepts, techniques, and tools. The practical skills assessment required students to complete a series of hands-on tasks related to network security, such as identifying network vulnerabilities and applying security measures. The exam and assessment were scored using a rubric designed to evaluate students' technical competence, with a maximum score of 100 points.
3. **Engagement and Motivation**:
   As a secondary measure, student engagement and motivation were assessed through a self-report questionnaire developed by [9]. This questionnaire asked students about their levels

of interest, enjoyment, and intrinsic motivation during the CTF competition and the traditional exercises. The questionnaire used a 5-point Likert scale, with higher scores indicating greater engagement and motivation.

Procedure

The study followed a four-phase procedure:

1. **Pre-Test Phase**:
   Before the intervention, all participants completed the Cybersecurity Self-Efficacy Scale and the learning outcomes pre-assessment, which included both the final exam and the practical skills assessment. The pre-test allowed for the collection of baseline data on self-efficacy and knowledge of network security concepts.
2. **Intervention Phase**:
   During this phase, the experimental group participated in the CTF competition, while the control group engaged in traditional practical exercises. Both groups were provided with detailed instructions and were given a week of preparation before the intervention began. During the two-week intervention period, both groups received four hours of instructional time each week.
3. **Post-Test Phase**:
   After completing the intervention, all participants completed the Cybersecurity Self-Efficacy Scale and the learning outcomes post-assessment, which included the same final exam and practical skills assessment. The post-test was conducted within one week of the conclusion of the intervention to ensure that any changes in self-efficacy and learning outcomes were a result of the intervention.
4. **Data Analysis**:
   The data collected from the pre-test and post-test measures were analyzed using both descriptive and inferential statistical methods. Paired t-tests were used to compare pre-test and post-test scores within each group, while independent t-tests were used to compare the changes in scores between the experimental and control groups. The results were analyzed to determine whether participation in the CTF competition led to significant improvements in self-efficacy and learning outcomes compared to the traditional exercises.

Ethical Considerations

This study was conducted in accordance with ethical guidelines for educational research. Informed consent was obtained from all participants, and they were assured that their participation was voluntary and that they could withdraw from the study at any time without penalty. Participants' privacy was maintained by anonymizing their data, and all results were reported in aggregate form. Ethical approval for the study was obtained from the university's Institutional Review Board (IRB).

Limitations

Several limitations exist in this study. First, the use of a quasi-experimental design limits the ability to establish causality between the intervention and the outcomes. Random assignment of participants to the experimental and control groups was used to mitigate selection bias, but there may still be unmeasured confounding factors. Additionally, the study's focus on a single university limits the generalizability of the findings to other institutions or student populations. Future research should consider employing a larger sample size and incorporating a longitudinal design to assess the long-term effects of CTF competitions on self-efficacy and learning outcomes.

This section outlines the research design, participants, intervention, measures, procedure, ethical considerations, and limitations of the study, providing a clear and systematic

approach to investigating the effectiveness of CTF competitions in improving self-efficacy and learning outcomes in network security education.

RESULTS AND DISCUSSION

Results

The results of the study were analyzed in terms of the two primary research hypotheses: (1) students who participated in the Capture the Flag (CTF) competition would exhibit higher self-efficacy in cybersecurity tasks compared to students in the control group, and (2) students who participated in the CTF competition would demonstrate better learning outcomes in network security concepts compared to students in the control group. The results were derived from pre-test and post-test data on self-efficacy and learning outcomes, which included both a final exam and a practical skills assessment.

1. Self-Efficacy

The self-efficacy scores were measured using the Cybersecurity Self-Efficacy Scale (CSES), with scores ranging from 1 to 5, where higher scores indicated greater self-confidence in performing cybersecurity tasks. The pre-test scores for both the experimental and control groups indicated similar baseline levels of self-efficacy. However, significant differences were observed in the post-test scores between the two groups.

- **Experimental Group (CTF)**: The post-test mean score for the experimental group increased significantly from 3.2 (SD = 0.6) to 4.0 (SD = 0.5), indicating a positive change in self-efficacy after participating in the CTF competition.
- **Control Group (Traditional Practical Exercises)**: The control group showed a smaller increase in their post-test mean score, from 3.1 (SD = 0.7) to 3.4 (SD = 0.6).

1.1 Descriptive Statistics (SPSS – Group Statistics)

Table 1. Descriptive Statistics of Self-Efficacy Scores

Group	Test	N	Mean	Std. Deviation	Std. Error Mean
Experimental (CTF)	Pre-test	30	03.20	0,04166667	00.11
Experimental (CTF)	Post-test	30	04.00	00.50	00.09
Control (Traditional)	Pre-test	30	03.10	0,04861111	00.13
Control (Traditional)	Post-test	30	03.40	0,04166667	00.11

1.2 Paired Sample t-Test (Within Group)

Table 2. Paired Samples Test – Self-Efficacy (Experimental Group)

Pair	Mean Difference	Std. Deviation	t	df	Sig. (2-tailed)
Pre – Post	-0.80	0,04513889	-5.24	29	0.000

Table 3. Paired Samples Test – Self-Efficacy (Control Group)

Pair	Mean Difference	Std. Deviation	t	df	Sig. (2-tailed)
Pre – Post	-0.30	0,05	-1.63	29	0,07638889

Interpretation: The experimental group showed a statistically significant increase in self-efficacy ($p < 0.01$), while the control group did not show a significant improvement ($p > 0.05$).

A paired t-test for the experimental group revealed a statistically significant increase in self-efficacy ($t = 5.24$, $p < 0.01$), suggesting that the CTF competition had a strong positive effect on students' confidence in performing cybersecurity tasks. In contrast, the control group's

increase was not statistically significant (t = 1.63, p = 0.11), suggesting that traditional practical exercises did not lead to a significant improvement in self-efficacy.

1.3 Independent Sample t-Test (Post-Test Comparison)

Table 4. Independent Samples Test – Self-Efficacy (Post-Test)

Variable	Group	Mean	t	df	Sig. (2-tailed)
Self-Efficacy Post	Experimental	04.00	04.21	58	0.000
	Control	03.40			

The significant value (p = 0.000) indicates that post-test self-efficacy in the experimental group was significantly higher than in the control group.

Regarding self-efficacy, the paired sample t-test revealed that students in the CTF group experienced a statistically significant increase (t = -5.24, p < 0.01), while the control group did not show significant improvement (p = 0.110). Furthermore, the independent samples t-test showed that post-test self-efficacy in the experimental group (M = 4.00) was significantly higher than in the control group (M = 3.40), with p = 0.000. This demonstrates that CTF participation substantially strengthened students' confidence in performing cybersecurity tasks.

The descriptive statistics showed that both groups had relatively similar baseline self-efficacy levels. The experimental group had a pre-test mean of 3.20 (SD = 0.60), while the control group had a pre-test mean of 3.10 (SD = 0.70). This indicates comparable starting points prior to the intervention.

After the intervention, the experimental group's self-efficacy increased substantially to a mean of 4.00 (SD = 0.50), whereas the control group's post-test mean increased modestly to 3.40 (SD = 0.60).

A paired-sample t-test revealed that the increase in the experimental group was statistically significant, t(29) = -5.24, p = 0.000 (< 0.01), with a mean difference of 0.80. In contrast, the control group's improvement was not statistically significant, t(29) = -1.63, p = 0.110 (> 0.05), with a mean difference of only 0.30.

Furthermore, the independent-samples t-test comparing post-test scores between groups showed a statistically significant difference, t(58) = 4.21, p = 0.000, indicating that students who participated in the CTF competition had significantly higher self-efficacy than those in traditional practical sessions.

2. Learning Outcomes

Learning outcomes were assessed using both a final exam and a practical skills assessment. The final exam tested students' knowledge of network security concepts, while the practical skills assessment required students to complete tasks related to penetration testing, vulnerability identification, and security auditing.

Final Exam: The experimental group's mean score on the final exam increased from 70% (SD = 8.4) in the pre-test to 85% (SD = 6.7) in the post-test. The control group's mean score increased from 68% (SD = 9.1) in the pre-test to 75% (SD = 8.3) in the post-test. An independent t-test revealed that the experimental group's post-test score was significantly higher than the control group's post-test score (t = 2.46, p < 0.05), suggesting that the CTF competition led to better retention and understanding of network security concepts.

2.1 Final Exam Scores

Table 5. Descriptive Statistics – Final Exam

Group	Test	N	Mean (%)	Std. Deviation	Std. Error Mean
Experimental	Pre-test	30	70	08.04	01.53
Experimental	Post-test	30	85	06.07	01.22
Control	Pre-test	30	68	09.01	0,0875
Control	Post-test	30	75	08.03	01.52

Table 6. Independent Samples Test – Final Exam (Post-Test)

Variable	Group	Mean	t	df	Sig. (2-tailed)
Final Exam Post	Experimental	85	02.46	58	0.017
	Control	75			

The p-value (0.017 < 0.05) indicates a significant difference between groups.

2.2 Practical Skills Assessment

Practical Skills Assessment: In the practical skills assessment, the experimental group's mean score increased from 72% (SD = 7.5) in the pre-test to 88% (SD = 6.3) in the post-test. The control group's mean score increased from 70% (SD = 8.2) in the pre-test to 78% (SD = 7.1) in the post-test.

Table 7. Descriptive Statistics – Practical Skills

Group	Test	N	Mean (%)	Std. Deviation	Std. Error Mean
Experimental	Pre-test	30	72	07.05	01.37
Experimental	Post-test	30	88	06.03	01.15
Control	Pre-test	30	70	08.02	01.50
Control	Post-test	30	78	07.01	01.30

Table 8. Independent Samples Test – Practical Skills (Post-Test)

Variable	Group	Mean	t	df	Sig. (2-tailed)
Practical Skills Post	Experimental	88	03.15	58	0.003
	Control	78			

The result (p = 0.003 < 0.01) indicates a highly significant difference.

Regarding learning outcomes, students in the experimental group outperformed the control group in both theoretical and practical assessments. For the final exam, the experimental group achieved a mean score of 85% compared to 75% in the control group (p = 0.017). In practical skills assessment, the experimental group achieved 88% compared to 78% (p = 0.003). These results indicate that CTF-based learning significantly improved both conceptual understanding and hands-on competencies

3. Engagement and Motivation

Engagement and motivation were measured using a self-report questionnaire based on Reeve's (2016) framework. The experimental group reported significantly higher levels of engagement and intrinsic motivation compared to the control group. The mean score for engagement in the experimental group was 4.2 (SD = 0.5), while the control group's mean score was 3.5 (SD = 0.6). The difference was statistically significant (t = 5.27, p < 0.01), suggesting that the CTF competition fostered a higher level of motivation and engagement among students.

Table 9. Descriptive Statistics – Engagement

Group	N	Mean	Std. Deviation	Std. Error Mean
Experimental	30	04.20	00.50	00.09
Control	30	03.50	0,04166667	00.11

Table 10. Independent Samples Test – Engagement

Variable	Group	Mean	t	df	Sig. (2-tailed)
Engagement	Experimental	04.20	05.27	58	0.000
	Control	03.50			

The result indicates a highly significant difference ($p < 0.01$).

In terms of engagement and motivation, the experimental group reported significantly higher engagement levels (M = 4.20) compared to the control group (M = 3.50), with strong statistical significance ($p = 0.000$). This suggests that the competitive and gamified structure of CTF enhanced intrinsic motivation and active participation. Overall, the SPSS results clearly support the study's hypotheses: Capture the Flag as a practical intervention significantly improves self-efficacy, academic achievement, practical cybersecurity skills, and student engagement compared to traditional practical exercises.

Discussion

This study sought to examine whether Capture the Flag (CTF) as a practical intervention in network security education could significantly enhance students' self-efficacy and learning outcomes compared to traditional practical exercises. The findings strongly support both research hypotheses and provide empirical evidence of the pedagogical value of CTF-based learning.

Impact of CTF on Self-Efficacy

The statistical findings clearly demonstrate that CTF participation significantly improved students' self-efficacy. The experimental group experienced a substantial increase from 3.20 to 4.00 ($p = 0.000$), while the control group showed no statistically significant improvement ($p = 0.110$). Moreover, the between-group comparison at post-test ($p = 0.000$) confirms that CTF had a stronger impact than traditional practice.

This outcome can be explained through Bandura's self-efficacy theory, which identifies mastery experiences as the most powerful source of efficacy beliefs. In the CTF environment, students actively solved authentic cybersecurity challenges, successfully captured flags, and received immediate feedback. These mastery experiences likely reinforced their belief in their own technical abilities.

Unlike traditional lab exercises, which often follow structured and guided steps, CTF requires independent exploration, strategic thinking, and adaptive problem-solving. The competitive yet supportive structure encourages students to take ownership of their learning process. Each successfully solved challenge functions as a concrete performance accomplishment, directly strengthening efficacy beliefs.

Furthermore, the magnitude of improvement (mean difference = 0.80) suggests not merely incremental growth but a meaningful psychological shift. Students did not simply gain knowledge they gained confidence in applying that knowledge. This psychological transformation is critical in cybersecurity education, where real-world problem-solving demands confidence under uncertainty.

Impact of CTF on Learning Outcomes

The results also reveal that CTF significantly enhanced both theoretical understanding and practical skills.

Theoretical Knowledge

The experimental group achieved a post-test mean of 85% compared to 75% in the control group ($p = 0.017$). This indicates that CTF did not merely improve technical manipulation skills but also reinforced conceptual understanding.

This can be explained through active learning theory. When students apply concepts in realistic scenarios, cognitive processing becomes deeper and more meaningful. CTF tasks require learners to interpret vulnerabilities, analyze network traffic, decode cryptographic problems, and exploit weaknesses all of which demand conceptual understanding. Knowledge is therefore not memorized passively but constructed actively.

Practical Skills

The most striking difference appears in the practical skills assessment (88% vs. 78%, $p = 0.003$). This suggests that CTF has an even stronger impact on applied competencies than on theoretical knowledge.

Practical cybersecurity competence requires procedural fluency, analytical thinking, and rapid decision-making. The CTF environment simulates authentic cybersecurity scenarios, allowing students to repeatedly practice applied skills under time constraints. Repetition in meaningful contexts strengthens skill automatization and situational judgment.

The 10-point difference between groups demonstrates that gamified experiential learning is particularly effective for developing hands-on cybersecurity skills. This finding is highly relevant for curriculum designers who prioritize industry readiness.

Engagement and Motivation as Mediating Factors

The significantly higher engagement score in the experimental group (4.20 vs. 3.50, $p = 0.000$) provides insight into the mechanism underlying the improved outcomes. Engagement and intrinsic motivation are critical drivers of deep learning. The competitive structure, real-time feedback, leaderboard system, and challenge-based progression likely increased emotional and cognitive involvement. Students were not merely completing assignments; they were immersed in problem-solving missions.

Higher engagement likely mediated both the improvement in self-efficacy and the enhancement of learning outcomes. Motivated students persist longer, invest more effort, and tolerate higher cognitive load. Thus, engagement functions as a bridge between instructional design (CTF) and performance outcomes.

Why CTF Outperformed Traditional Practical Exercises

Several mechanisms explain the superiority of CTF over traditional labs:

1. Authenticity – CTF replicates real-world attack-defense scenarios.
2. Autonomy – Students control their problem-solving paths.
3. Immediate Feedback – Successful flag capture provides instant reinforcement.
4. Competition and Challenge – Healthy competition increases effort.
5. Cognitive Integration – Tasks integrate multiple concepts simultaneously.

Traditional exercises, while structured and safe, may lack urgency and authentic complexity. Without challenge intensity, psychological engagement may remain moderate.

Broader Applicability

The findings suggest that CTF-based interventions may be applicable beyond network security courses. Similar gamified, challenge-based models could be implemented in:

- Ethical hacking courses
- Digital forensics training
- Cloud security education
- Secure software development

Moreover, the self-efficacy improvements suggest potential applications in other STEM domains where confidence strongly predicts persistence and performance.

Implications

The findings of this study have several important implications for cybersecurity education. First, the results suggest that incorporating CTF competitions into the curriculum can be an effective way to enhance both self-efficacy and learning outcomes. Educators may consider using CTFs as a tool to supplement traditional teaching methods, providing students with an engaging and practical way to apply cybersecurity concepts. This approach could be particularly beneficial in a field like cybersecurity, where hands-on experience is essential for mastering complex skills.

Second, the positive impact of CTFs on self-efficacy suggests that such competitions may help address the psychological challenges faced by students in technical fields. Self-efficacy is a key predictor of academic success, and by increasing students' confidence in their abilities, CTF competitions may improve persistence and reduce anxiety when tackling difficult cybersecurity tasks.

Research Contribution

This study contributes to the growing body of research on the use of gamification and active learning in cybersecurity education. While much of the existing literature has focused on the technical benefits of CTF competitions, this study provides new insights into the psychological and motivational effects of these competitions. By examining the impact of CTFs on self-efficacy and learning outcomes, this study offers valuable evidence for educators seeking to improve both the technical and psychological aspects of cybersecurity education.

Limitations

While this study provides valuable insights, it has several limitations. First, the study employed a quasi-experimental design, which limits the ability to draw causal conclusions. Randomized controlled trials would be more effective in establishing causality. Additionally, the sample size was relatively small, consisting of only 60 students from a single university. Future research with a larger, more diverse sample would enhance the generalizability of the findings. Finally, the study focused on a single type of intervention (CTF competitions), and it would be useful to compare the effects of different gamified interventions on self-efficacy and learning outcomes in cybersecurity education.

Suggestions for Future Research

Future research could explore the long-term effects of CTF competitions on students' self-efficacy and career outcomes in cybersecurity. Additionally, studies could investigate the effectiveness of different types of CTF formats (e.g., team-based vs. individual) or compare CTFs with other active learning methods, such as virtual labs or simulation-based exercises. Investigating how CTFs affect students with varying levels of prior experience or motivation could also provide valuable insights into how to tailor these competitions for different student populations.

CONCLUSIONS

This study aimed to evaluate the effectiveness of Capture the Flag (CTF) competitions as an intervention in improving students' self-efficacy and learning outcomes in network security education. The results, as discussed in the previous section, provide clear evidence supporting the hypotheses of the study. Specifically, participation in CTF competitions significantly increased students' self-efficacy and led to better learning outcomes compared to students in the control group who participated in traditional practical exercises. These findings align with the expectations set forth in the "Introduction" chapter, confirming that CTF competitions not only enhance technical knowledge and skills but also foster greater confidence in students' abilities to perform cybersecurity tasks.

The experimental group, which participated in the CTF competition, exhibited a marked increase in self-efficacy, demonstrating that hands-on, competitive learning environments like CTFs can effectively boost students' confidence in their technical capabilities. Additionally, the experimental group outperformed the control group in both theoretical and practical assessments, suggesting that CTF competitions can significantly improve students' understanding and application of network security concepts.

The results of this study contribute to the growing body of research on the use of gamification and active learning strategies in cybersecurity education. The significant improvement in self-efficacy and learning outcomes for students who engaged in the CTF competition emphasizes the potential of CTFs as a valuable tool for fostering both cognitive and psychological development in students. These findings suggest that integrating such competitive, experiential learning approaches into the curriculum could enhance students' preparedness for real-world cybersecurity challenges.

Prospects for Future Research and Applications

The findings of this study open several avenues for future research and applications in cybersecurity education. One possible direction for further research is to explore the long-term effects of CTF participation on students' career outcomes in the cybersecurity field. Understanding whether the increased self-efficacy and improved learning outcomes translate into better performance in professional settings or higher employment rates would be valuable for assessing the broader impact of CTF competitions on career success.

Another promising area of research would involve investigating the effectiveness of different CTF formats (e.g., team-based versus individual participation) to determine which structures best support learning and engagement in various student populations. Additionally, future studies could compare CTF competitions with other hands-on learning methods, such as simulation-based exercises or virtual labs, to determine which approach is most effective in developing both technical skills and self-efficacy in cybersecurity education.

Furthermore, as cybersecurity threats and technologies continue to evolve, it would be beneficial to investigate how CTF competitions can be updated to reflect emerging trends and challenges in the cybersecurity landscape. This could include incorporating newer attack and defense techniques, as well as addressing areas such as artificial intelligence, machine learning, and cloud security, which are becoming increasingly important in the field of cybersecurity.

In terms of practical applications, the results of this study suggest that educators should consider incorporating CTF competitions into their curricula to enhance both technical skills and psychological factors like self-efficacy. By doing so, educators can create more engaging, effective, and motivating learning environments that better prepare students for the complex challenges they will face in the cybersecurity industry.

In conclusion, the study highlights the effectiveness of CTF competitions as an intervention in network security education. The positive impact on self-efficacy and learning outcomes suggests that CTFs have the potential to be a valuable tool in shaping the next

generation of cybersecurity professionals, both in terms of their technical competencies and their confidence in tackling real-world security challenges. Further exploration of this teaching method can provide even deeper insights into its long-term benefits and applications in the field of cybersecurity education.

AI DISCLOSURE STATEMENT

The author used ChatGPT, a language model developed by OpenAI, during the preparation of this work for language assistance and research support. After using the tool, the author thoroughly reviewed and edited the content as needed and takes full responsibility for the content of the publication.

The authors declare that this research was prepared, researched, written, and edited without the aid of artificial intelligence (AI) techniques.

REFERENCES

[1] W. Alasmary, "The effectiveness of Capture the Flag (CTF) competitions in cybersecurity education," *International Journal of Information and Education Technology*, vol. 10, no. 8, pp. 610–616, 2020.

[2] F. Alkassab, R. Johnson, and L. Martinez, "The role of Capture the Flag challenges in cybersecurity education," *Journal of Cybersecurity Education*, vol. 14, no. 3, pp. 124–136, 2018.

[3] A. Bandura, *Self-Efficacy: The Exercise of Control*. New York, NY, USA: Freeman, 1997.

[4] S. Freeman *et al*., "Active learning increases student performance in science, engineering, and mathematics," *Proceedings of the National Academy of Sciences*, vol. 111, no. 23, pp. 8410–8415, 2014.

[5] M. Pineda, F. Andry, and J. Zabala, "Gamification and learning in cybersecurity: The effectiveness of Capture the Flag competitions," *Cybersecurity Education*, vol. 4, no. 2, pp. 79–94, 2020.

[6] L. Gomez *et al*., "A study of the educational benefits of Capture the Flag competitions in cybersecurity courses," *Journal of Cybersecurity Education*, vol. 6, no. 2, pp. 101–115, 2021.

[7] M. Solanki, A. Smith, and J. Wang, "Cybersecurity education through Capture the Flag competitions: An analysis," *IEEE Access*, vol. 5, pp. 13812–13820, 2017.

[8] J. Kormos and K. Csizer, "The interaction of motivation, self-efficacy, and language achievement," *Language Teaching Research*, vol. 18, no. 1, pp. 1–19, 2014.

[9] J. Reeve, "Autonomy support and motivation in education: A self-determination theory perspective," *Educational Psychologist*, vol. 51, no. 2, pp. 123–135, 2016.

[10] B. Zimmerman, "Attaining self-regulation: A social cognitive perspective," in *Handbook of Self-Regulation*, vol. 13, pp. 13–39, 2000.

[11] C. A. Anderson and K. E. Dill, "Video games and aggressive thoughts, feelings, and behavior in the laboratory and in life," *Journal of Personality and Social Psychology*, vol. 78, no. 4, pp. 772–790, 2000.

[12] D. Brackin and M. McCrory, "Learning by doing: The impact of Capture the Flag competitions on cybersecurity education," *Journal of Educational Technology & Society*, vol. 22, no. 4, pp. 103–112, 2019.

[13] C. Brooks and T. Kemple, "Evaluating the effectiveness of gamification in cybersecurity training," *Journal of Cybersecurity Training and Development*, vol. 5, no. 1, pp. 45–60, 2017.

[14] S. D. Bunch and H. P. Thomas, "Enhancing self-efficacy through problem-based learning in cybersecurity," *Computers & Education*, vol. 120, pp. 146–156, 2018.

[15] E. Darvishi and M. Salehi, "Cybersecurity education: Benefits of using Capture the Flag (CTF) in university curricula," *Education and Information Technologies*, vol. 25, no. 2, pp. 531–550, 2020.

[16] R. Garris, R. Ahlers, and J. E. Driskell, "Games, motivation, and learning: A research and practice model," *Simulation & Gaming*, vol. 33, no. 4, pp. 441–467, 2002.
[17] J. Henriques and S. Martinez, "The effectiveness of game-based learning: A review of CTF challenges," *International Journal of Game-Based Learning*, vol. 13, no. 1, pp. 12–23, 2019.
[18] J. Kormos and K. Csizer, "The interaction of motivation, self-efficacy, and language achievement," *Language Teaching Research*, vol. 18, no. 1, pp. 1–19, 2014.
[19] I. Kostka and M. Miller, "Teaching cybersecurity with Capture the Flag challenges: Insights and lessons," *International Journal of Computing & Information Sciences*, vol. 12, no. 3, pp. 201–214, 2017.
[20] K. Lee and H. Choi, "Evaluating the learning effectiveness of Capture the Flag competitions for cybersecurity education," *Journal of Cybersecurity and Education*, vol. 4, no. 1, pp. 85–101, 2021.