Leveraging Gamification and Game-based Learning in Cybersecurity Education: Engaging and Inspiring Non-Cyber Students

Preprint · December 2023

CITATIONS
0

READS
153

4 authors, including:

Lowri Williams
Cardiff University
16 PUBLICATIONS **905** CITATIONS
SEE PROFILE

Eirini Anthi
Cardiff University
35 PUBLICATIONS **1,010** CITATIONS
SEE PROFILE

Amir Javed
Cardiff University
22 PUBLICATIONS **471** CITATIONS
SEE PROFILE

Leveraging Gamification and Game-based Learning in Cybersecurity Education: Engaging and Inspiring Non-Cyber Students

Lowri Williams
School of Computer Science & Informatics
Cardiff University
Cardiff, UK
WilliamsL10@cardiff.ac.uk
0000-0002-3794-6145

Eirini Anthi
School of Computer Science & Informatics
Cardiff University
Cardiff, UK
0000-0002-5274-0727

Yulia Cherdantseva
School of Computer Science & Informatics
Cardiff University
Cardiff, UK
0000-0002-3527-1121

Amir Javed
School of Computer Science & Informatics
Cardiff University
Cardiff, UK
0000-0001-9761-0945

***Abstract*—This paper investigates the use of gamification and game-based learning in the field of cybersecurity education. Due to their technical complexity and lack of coherence, traditional pedagogical methods, such as lectures, may fail to engage and inspire students, especially those from non-cyber backgrounds. To address this issue, we devised two distinct cybersecurity frameworks/games based on traditional Capture The Flag (CTF) competitions; an open-ended CTF event and a story-based CTF. Such games have demonstrated potential across multiple disciplines, including computer science, physics, mathematics, and engineering, as well as across multiple levels of study including undergraduate and postgraduate students. The positive feedback and significant increase in the interest to pursue a postgraduate course in cybersecurity, especially among non-cybersecurity students, attest to the success of this gamification strategy. As such, this paper provides valuable insights for enhancing the attractiveness and efficacy of cybersecurity education, thereby encouraging a broader spectrum of non-technical and non-cybersecurity students to pursue this crucial field.**

Keywords—Gamification, Capture The Flag (CTF), Cybersecurity, Decision Making, Education

I. INTRODUCTION

The escalating threats posed by the digital world highlight the critical need for solid cybersecurity training. This education is vital for educating professionals who can protect against advanced cyber threats [1]. As the cyber landscape continues to evolve, the task of teaching cybersecurity becomes an equally dynamic challenge. Moreover, fostering an interest in cybersecurity among students from non-technical and non-cyber backgrounds including physics, mathematics, engineering, and more, remains a substantial pedagogical obstacle [2]. This may be because the traditional lecture-based format, although foundational, often falls short in encouraging cross-disciplinary engagement and inspiration, highlighting the need for innovative, more interactive teaching strategies.

One potential solution to this challenge lies in the emerging fields of gamification and, in particular, game-based learning. Gamification refers to the incorporation of game-design elements in non-game contexts, while game-based learning involves using games explicitly for educational purposes [3], [4]. Research across a range of disciplines has demonstrated that these approaches significantly enhance student engagement, motivation, and ultimately, the efficacy of learning [5]. With their inherent emphasis on problem-solving, strategy, and active participation, these methods are particularly suited to the hands-on, practical nature of cybersecurity education.

Building on the effectiveness of gamified learning, several cybersecurity training platforms, such as Hack The Box [6] and Try Hack Me [7], have emerged. Such platforms incorporate gamification elements to stimulate user engagement and facilitate skill acquisition, with particular emphasis on Capture the Flag (CTF) events. Nevertheless, while these platforms have proven beneficial in certain aspects, they are not without their limitations. The primary concern is that such platforms often pose challenges that are extremely technical and require significant pre-existing knowledge, which can be overwhelming for many users, particularly those who are new to the field [8]. The difficulty level labelling on such platforms is often subjective by the challenge creator, with ‘easy’ challenges frequently proving to be quite complex or requiring significant prior experience and knowledge to complete them. Consequently, users may become discouraged and potentially abandon their efforts, or worse, be dissuaded from pursuing further cybersecurity education. Therefore, while the potential of gamification in cybersecurity education is apparent, it is essential to consider these challenges and strive to develop a more user-friendly and inclusive approach.

Additionally, the challenges presented by existing CTFs tend to be disjointed, focusing on isolated skill sets or concepts. This fragmentation makes it challenging for learners to comprehend the interconnected nature of various cybersecurity principles and strategies. Effective learning in cybersecurity, as in many complex disciplines, requires a holistic understanding of how different components and principles interplay and affect each other [9]. This concept of ‘connected learning’ emphasises the importance of

integrative thinking, aiding learners in recognising patterns, predicting consequences, and making more informed decisions [10]. When learners can see the fluidity between tasks and understand how different parts interrelate, their ability to retain and apply the information in a practical context significantly improves [11]. Hence, while the existing gamified platforms serve as useful tools in promoting cybersecurity learning, their approach to creating largely disconnected challenges does not support the development of a broader comprehension of cybersecurity as a complex organisational and multidisciplinary problem.

To address the aforementioned limitations, this paper presents an innovative application of gamification and game-based learning in cybersecurity education. The authors have developed and tested two unique game formats inspired by traditional CTF competitions — an open-ended CTF and a story-based CTF. Such educational frameworks were purposefully crafted to cater for a diverse educational student population, encompassing a broad range of academic disciplines and spanning from undergraduate to postgraduate levels. The primary objectives of these frameworks were not only to enhance student's understanding and mastery of crucial cybersecurity skills but also to ignite interest in cybersecurity, especially among non-cybersecurity students. More specifically, this term refers to students who are enrolled in academic programs, courses, or disciplines of study other than cybersecurity. This includes students in the humanities, social sciences, natural sciences, arts, business, engineering, and even computer science who may not have been exposed to or trained in the complexities of cybersecurity. While they may have general knowledge or a basic comprehension of technology and computing, they typically lack the specialised training and knowledge that is needed in this field.

The key contribution of this paper lies in its effort to bridge the aforementioned gaps in current gamified cybersecurity learning platforms. By offering a more connected and fluid learning experience through the proposed games, it addresses the critical need for more holistic, integrated learning experiences. Through an open-ended CTF, the learner navigates a range of interrelated challenges, fostering a more comprehensive understanding of the cybersecurity landscape. Simultaneously, the story-based CTF offers a coherent narrative, ensuring continuity and context, allowing participants to see how individual challenges relate to one another within a larger plot. As they progress, participants are not only accumulating points, but they are also advancing a storyline, allowing learners to see the relevance and application of the skills they acquire, adding a layer of engagement and motivation. Furthermore, a narrative-driven structure can facilitate a deeper understanding, as participants can often remember and relate to a story more effectively than disjointed pieces of information. The unfolding plot offers context for each challenge, making the learning experience more immersive and memorable.

The ultimate aim of this paper is to showcase the potential and efficacy of gamification and game-based learning in enhancing cybersecurity education. By presenting the innovative design and successful implementation of the proposed games, this research hopes to inspire further adoption and adaptation of such pedagogical strategies, thereby making a significant contribution to the evolution of cybersecurity pedagogy. The paper is structured into sections that cover existing cybersecurity learning platforms (Section II), game development methodologies (Section III), game development and execution in academic contexts (Sections IV and V), and discussions of future research directions (Section VI).

II. RELATED WORK

The rising interest in gamified learning within the domain of cybersecurity education has led to the development of several platforms that aim to facilitate the learning process through interactive, game-based tasks. Such platforms exhibit significant variation in their methodology, structure, the target audience they cater to, and the degree of complexity inherent in their challenges. The following summarises the common issues and shortfalls in some of the most well-known cybersecurity learning platforms:

- **Technical difficulty:** Many platforms, including Hack The Box, TryHackMe, OverTheWire, and National Cyber League, present challenges that can be overwhelmingly technical. Novices and individuals without prior cybersecurity knowledge may find it difficult to access and engage with these platforms effectively.
- **Lack of accessibility:** Some platforms, such as CyberStart Game and picoCTF, target specific audiences, such as high school students or beginners, potentially leaving more advanced learners or those seeking deeper understanding underserved.
- **Isolated challenges:** Several platforms, like TryHackMe and National Cyber League, offer isolated challenges that do not provide learners with a clear understanding of how various cybersecurity concepts interrelate. This can hinder the development of a holistic cybersecurity skill set.
- **Emphasis on technical skills:** Many platforms, including OverTheWire and Sans NetWars, heavily emphasise technical skills and assume a solid foundation in cybersecurity. This can discourage beginners or individuals from non-technical fields from participating.
- **Lack of comprehensive narrative:** Some platforms, like Hack The Box, TryHackMe, and National Cyber League, lack a structured narrative that guides learners through the interconnectedness of cybersecurity aspects, resulting in a disjointed learning experience.
- **Limited audience scope:** Platforms like Secure Code Warrior are highly specialised, focusing on secure coding techniques and specific programming languages. This limited scope may not cater to

individuals interested in broader cybersecurity topics.

III. THE CONCEPT OF GAMIFICATION AND GAME BASED LEARNING

Gamification, the incorporation of game elements into non-game contexts, has emerged as a major trend in multiple industries, including education, marketing, and health [3]. By leveraging the core elements that make games engaging and enjoyable, such as competition, achievement, and the gratification derived from overcoming obstacles, gamification offers a promising tool for stimulating user engagement and promoting specific behaviours [12].

Gamification is reshaping education through the incorporation of game elements such as points, certificates, leaderboards, levels, and achievements. These elements offer immediate feedback, boost student motivation, and foster a competitive learning atmosphere, transforming teaching and learning into interactive, rewarding, and engaging experiences. Empirical research indicates that gamification in education leads to increased learner engagement, active participation, improved academic performance, and enhanced learning outcomes [13]. Game-based learning, a subset of gamification, goes beyond memorisation-based teaching methods, emphasizing active learning where students learn by doing, interacting with content, and reflecting on their actions. In this immersive environment, students apply theoretical knowledge, make strategic decisions, and face the consequences of their actions, resulting in higher retention rates and intrinsic motivation for an engaging educational journey [14].

Therefore, CTF competitions, simulated cyber attack and defence scenarios, and puzzle-solving games involving deciphering codes and securing networks are all viable formats for the application of game-based learning in cybersecurity education. These activities can be adapted to various skill levels and learning objectives, accommodating beginners who are still learning cybersecurity fundamentals as well as advanced learners who wish to enhance their expertise and improve their problem-solving abilities [15].

However, the journey of implementing gamification and game-based learning in cybersecurity education often faces obstacles. Designing effective educational games necessitates a delicate balance between educational content and gameplay, something that is not easily achieved. Additionally, educators face the challenge of creating tasks that cater to a diverse group of learners with varying degrees of knowledge and skills. If the tasks are too difficult, students may feel overwhelmed; too easy, and they might not feel adequately challenged. This highlights the importance of Vygotsky's concept of the Zone of Proximal Development [16], which recommends aligning task difficulty with the learner's current ability and potential growth with appropriate guidance.

Subsequently, as technology continues to advance and digitalisation becomes increasingly prominent, the utility of gamification and game-based learning in cybersecurity education is undeniable. These pedagogical tools provide engaging, immersive, and practical learning experiences that inspire passion, drive engagement, and deepen understanding, in a manner that traditional approaches often struggle to achieve. Although challenges persist, continued research and innovation in this field promise to yield more effective strategies for game-based cybersecurity education, leading to a more robust cybersecurity workforce and a safer digital world.

IV. CAPTURE THE FLAG (CTF) GAMES

CTF competitions are a popular form of gamified learning in the field of cybersecurity education. Originating from traditional outdoor games, CTF competitions in the context of cybersecurity involve participants working in teams to solve a variety of security-related challenges to find 'flags' [17]. Flags often take the form of secret pieces of information or tokens that are hidden within the system, which participants need to discover and retrieve. The process of finding flags usually involves exploiting a vulnerability in the system, cracking a password, or solving a puzzle, hence incorporating various aspects of cybersecurity such as ethical hacking, digital forensics, cryptography, and network security [17].

Such competitions offer participants practical experience in dealing with real-world security issues through a variety of flags, ranging from simple tasks for beginners to highly complex challenges for advanced participants. These challenges cater to a wide range of skill levels, enabling all participants to learn and enhance their cybersecurity skills. Teams earn points by completing specific tasks represented by each flag, with the team accumulating the most points declared as the winner. CTF competitions come in two main types: Jeopardy-style and Attack-Defense. In Jeopardy-style CTFs, teams select and solve challenges from different categories to earn points, while in Attack-Defense CTFs, teams must defend their network while exploiting vulnerabilities in opponents' networks. The scoring system in CTFs is tied to the difficulty level of flags, motivating participants to tackle more complex tasks and creating a competitive and engaging learning environment [18].

V. DESIGN AND DEVELOPMENT OF CYBERSECURITY GAMES

This section delves into the theoretical foundations of gamification and game-based learning while detailing the design and development of two cybersecurity games: an open-ended CTF game and a beginner-friendly story-based CTF. These games are tailored to seamlessly integrate with the cybersecurity curriculum and exemplify the discussed gamification and game-based learning concepts. Inclusivity is a key focus, allowing participants without prior cybersecurity knowledge to engage, as each challenge is beginner-friendly. As participants progress through the CTF, they acquire foundational cybersecurity knowledge, with challenges building upon previously acquired skills, ensuring a consistent learning curve and boosting participants' confidence, making the experience both educational and rewarding.

A. The Platform

To facilitate both forms of the CTF challenges presented in this paper, the open-source platform, Root The Box [19], is used. Once hosted, the web application provides a robust environment where administrators can craft intricate challenge questions that capture the essence of real-world cybersecurity dilemmas. The platform's flexible interface allows for the setting of scores for each challenge, based on their complexity and the skills required to solve them. More specifically:

- 'Easy' questions are designed for beginners and require basic knowledge and straightforward application of tools and concepts. Points for such questions are lower as they serve as an introduction to the concepts and typically require less time and fewer steps to solve. A question that requires participants to find hidden text in a document's metadata may be considered as being easy and worth a minimal point value.
- 'Medium difficulty' questions demand a deeper understanding and some experience in cybersecurity practices. Participants may need to employ multiple tools or methods to arrive at the solution, such as decoding base64 strings or performing basic network analysis. The points awarded for medium questions are higher, reflecting the increased complexity and the greater time investment needed to solve them.
- 'Hard' questions are tailored towards more advanced participants and assume a high level of expertise to solve potentially multi-layered questions. To solve these, participants must demonstrate proficiency in areas such as reverse engineering, exploit development, or advanced cryptography. Such questions are valued with even more points due to their complexity, often becoming the deciding factor in the competition's leaderboard standings.
- 'Very hard' questions are often the pinnacle of the CTF challenge. Such questions are akin to real-world cybersecurity problems and require advanced problem-solving skills, creativity, and persistence. The highest points are reserved for these questions, offering a significant boost to the score as a reward for the exceptional skill and effort required to solve them.

As participants successfully answer questions and input correct flags onto the platform, their scores are immediately updated on the platform's scoreboard. This dynamic feature allows teams/players to track their progress and standing among other participants in real-time. As such, it injects a layer of excitement into the learning process by creating a sense of immediacy and competition.

B. Game 1: Open-ended, non-technical CTF

The open-ended CTF introduces a non-technical perspective to cybersecurity education. This game incorporates an interactive challenge that engages students in teams, thereby promoting collaboration, to address open-ended questions relevant to the cyber-security domain.

Grounded in the principles of constructive alignment, explicit statements of the intended goals and learning outcomes of the game, such as fostering collaboration, critical thinking, and problem-solving skills, are provided at the commencement of this activity [20]. This offers students clarity and guidance about the skills and knowledge they are expected to gain during the game, thereby aligning the learning activities with the intended learning outcomes.

Recognising that cybersecurity can be a daunting field for newcomers, the game design includes structured guidance to facilitate students' research processes. Resources are provided to help students navigate the vast landscape of online information related to cybersecurity. This approach is aligned with Vygotsky's [10] educational theory, which emphasises the role of supportive guidance in learning, particularly for learners who are new to the topic.

Further enhancing the learning experience, formative feedback is integrated into the game via regular check-ins with each team. This approach, supported by Paul & Elder [21], allows students to refine their strategies and approaches to the questions in real-time, facilitating a more effective and engaging learning experience.

The open-ended CTF is a component of an MSc module, providing an innovative platform for students to review course techniques and promote critical thinking. It involves the participation of the entire class, usually comprising over 80 students, who are formed into teams of no more than six individuals to navigate challenges, fostering teamwork and collaborative problem solving [22]. Teams are created by the main facilitator of the session, who uses their understanding of the participant's skills and background based on past communication to form groups of participants from different backgrounds, knowledge, and skills. This diversity can lead to several developmental advantages, such as a broader range of ideas and solutions to the questions, enhancement of students' communication, negotiation, and conflict resolution skills, mitigation of cliques, and promotion of inclusivity and flexibility.

The questions included in this game require students to think like potential cyber adversaries, considering various aspects of cyber operations, such as social engineering and exploitation. This not only enhances their understanding of the multifaceted nature of cybersecurity but also strengthens their ability to anticipate and counter potential cyber threats. Examples of the questions that students might be presented with include:

1) *What method would you use to gain more information about the target before you actively start the exploitation?*
2) *Assuming as an attacker you have gained access to the organisation's network, what would you do next to gain more information about the IT infrastructure?*

3) *If you were to deploy a phishing attack, who would you target, and how would you deploy the attack?*

4) *How would you find vulnerable Industrial Control Systems around the world from your computer?*

5) *You identify that the company has machines running Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2, that have not been patched since 2016. What is a critical vulnerability that you can exploit?*

During the CTF event, when teams arrive at a potential answer, they must articulate and defend their problem-solving methods to facilitators who utilise a developed rule-based template to guide the evaluation of responses. This template is designed to ensure consistency with the synchronous class teaching setting, focusing on the logical progression and analytical depth of the answer rather than its correctness. Facilitators assess if the team's approach is methodologically sound and meets the learning objectives associated with the question before giving the teams the flags. The following is an example of how a facilitator may evaluate whether a flag is awarded for the response given to *'assuming as an attacker you have gained access to the organisation's network, what would you do next to gain more information about the IT infrastructure?'* or use the structure to prompt participants to enhance their answers to achieve the flag:

- Identification of initial steps: The response must begin with a clear identification of initial reconnaissance steps. A good example of a response may be *'I would start by conducting a network scan using tools like Nmap to identify active devices on the network.'*
- Use of appropriate tools: The team must specify at least one appropriate tool for further exploration of the network, for example, utilising Wireshark to monitor network traffic for open ports and services.
- Understanding of network topology: The response must demonstrate an understanding of how to map the network topology. An example of a good response is *'Mapping the network with a tool such as Zenmap to understand the layout and find critical nodes.'*
- Depth of the methodology: The answer must include a multi-step methodology, not just a single action. For example, after identifying active devices, the next step would be to perform vulnerability scanning to find weak points.
- Prioritisation of information gathering: The response should prioritise gathering sensitive information that could lead to escalated access or valuable data, such as seeking admin credentials or access tokens by searching through unsecured files or misconfigurations.
- Ethical consideration: The response must acknowledge the ethical implications and legal boundaries of actions taken during penetration testing.

It is important to note that the flags may not necessarily represent the concrete answer but validate the team's process and understanding and hone the students' abilities in communication and presentation, ensuring they learn to articulate cybersecurity concepts clearly and effectively. As previously noted, each flag corresponds to a predetermined number of points, and upon inputting the correct flag onto the platform, the team's score is immediately updated on a live dashboard visible to all contestants. This element of the competition fosters a keen but friendly, competitive spirit.

C. Game 2: Story-based CTF

To address the need for a more inclusive, engaging, and interactive learning experience, particularly in cybersecurity education, this paper presents a gamified approach that encompasses the development and application of story-line-based CTF challenges. These events have been carefully crafted to appeal to a broad audience and align with key pedagogical theories to enhance the overall learning experience [23], as well as adding an element of fun and excitement while increasing relevance and learner engagement [24].

The CTF themes revolve around well-known events, such as Christmas and Easter, as well as generic themes. Each of these themes serves as a storyline that guides the learners throughout the event, creating a coherent narrative that increases the perceived relevance of the tasks. This approach reflects the narrative learning theories that stress the importance of stories in shaping our understanding and interpretations of experiences [25].

These CTFs have been thematically designed to coincide with these non-teaching periods at universities in the United Kingdom, where the curriculum calendar frequently features vacations around Christmas and Easter. The use of these well-known cultural events provides learners with a sense of familiarity and an engaging narrative backdrop. By organising CTFs around these well-known occurrences, participants are guided by a coherent narrative that enhances the relevance of the tasks. Nonetheless, it is essential to recognise the larger context of exclusivity and diversity in the thematic choices. While the primary objective of these CTFs is to ensure that all participants, regardless of their prior cybersecurity knowledge, can actively participate and benefit, it is essential to keep in mind the cultural diversity of the student population.

The CTFs are designed for remote, on-campus, or hybrid play, encouraging collaboration in teams of four and independent participation. They are often launched at the end of semesters or during holiday breaks. Such events are open to all university members, irrespective of their degree levels (BSc/MSc/PhD) or roles (staff or students), promoting an inclusive learning community. A Discord channel was created where participants could ask questions during the

event. This provided a forum for instant support and collaborative problem solving, enhancing engagement and learning experience. Such challenges were also not confined to one university. Collaborations were established with several institutions around the world, promoting international cooperation and enhancing the diversity of participants and learning experiences.

The challenges included in these CTFs are intentionally set at a beginner-friendly level, enabling participants with no prior cybersecurity knowledge to solve them using common tools like a web browser. These challenges, such as analysing image meta-data for hidden information, promote self-directed exploration aligned with constructivist learning theory, emphasising learners' active knowledge creation through problem-solving and exploration [10].

Flags often serve as keys to subsequent challenges, adding an element of coherence and continuity to the CTF. This is coupled with carefully crafted hints to guide the players, without depriving them of critical thinking and problem-solving experience. The alignment of the flags with the broader storyline further underscores the relevance and practical applicability of the tasks [26].

Real-world cybersecurity scenarios are embedded within the tasks, adding authenticity and relevance to the challenges, and promoting the application of skills to practical situations [27]. For instance, participants might be required to find an employee's Instagram account using specific hashtags and then decipher information from a QR code on a photo of a work badge. This example illustrates common privacy compromises that occur daily, educating participants about such vulnerabilities while they navigate the challenge. On this note, it is important to highlight that the creation of these Instagram accounts was approached with rigorous ethical considerations. The accounts used for these challenges were fictional, created explicitly for the game, and no real individual's data or likeness was used. Additionally, the content, such as the work badge, was artificially fabricated, ensuring that there was no association with real-world organisations or personnel. This methodology ensured that the learning experience was as realistic as possible, in a safe and ethical environment by developing controlled, fictional scenarios.

Several challenges incorporate components of network forensics and digital forensics at a level that participants can manage with some Internet-guided research. These tasks might include inspecting a packet capture (pcap) file or using a tool like Volatility, thus exposing students to essential cybersecurity practices.

To conclude, these story-line-based CTFs provide an immersive, interactive, and educative platform for participants to learn and apply cybersecurity concepts. Through careful design and development that align with pedagogical theories, these events can be effective in promoting learner engagement, critical thinking, collaboration, and problem-solving, and raise awareness of cybersecurity risks among participants. One might compare the appeal and intrigue of these challenges to an Easter egg hunt, where the reward is not just the thrill of discovery, but an enhanced understanding of cybersecurity.

VI. ASSESSMENT FRAMEWORK

Evaluating the effectiveness of the CTF's challenges as teaching tools is crucial for determining their educational value. Feedback for such challenges is often gathered informally through tools such as Mentimeter and Google Forms, offering firsthand insights into the immediate reception and impact of the games. For example, the feedback on the open-ended CTF was very positive, further endorsing its successful implementation. Comments such as *"we need more of these!"*, *"the CTF was one of the best things I did this semester"*, and *"what a fun way to revise everything we learned"* are indicative of its effectiveness and the enjoyable learning environment it creates.

However, such feedback does not fully adhere to structured research assessment methodologies. To address this, and to work towards future work, in this section, a framework of assessment metrics is proposed. By incorporating this framework as part of future research, the aim is to shed light on the potential benefits of using CTF challenges as teaching tools and how they compare to conventional methods in enhancing learning outcomes and student engagement. Collecting quantitative data is essential to provide empirical evidence of the findings and contribute to the ongoing discussion surrounding innovative educational practices.

Quantitative Data Collection

- Participation Rate: To gauge the level of student engagement with CTF challenges, the percentage of participants who initiate and complete these challenges could be measured. This metric allows the assessment to which extent students actively participate.
- Completion Time: Measuring the time taken by students to complete each challenge may provide insights into the challenges' engagement and difficulty levels. Longer completion times may suggest more challenging and educational experiences.
- Correct Answers: Collect data on the number of correct answers or solutions submitted by participants. This metric may directly reflect participants' understanding and problem-solving capabilities.
- Frequency of Attempts: Monitoring how often participants attempt challenges may reveal their level of commitment and motivation to learn through CTFs.
- Feedback and Surveys: Participants' feedback and survey responses may offer qualitative insights into their perceptions of the challenges, including difficulty, educational value, and overall satisfaction.

Performance Metrics

- Accuracy: The percentage of correct answers submitted by participants may serve as a key performance metric in measuring the participants' proficiency in solving CTF challenges accurately.
- Completion Rate: Calculating the percentage of participants who complete challenges would allow the assessment of the challenges' accessibility and overall appeal.
- Time Efficiency: Analysing the average time taken by participants to complete challenges may provide insights into the efficiency of the challenges in promoting learning within reasonable time frames.
- Skill Progression: By examining how participants' performance evolves, it can be determined whether they improve their accuracy and completion time as they progress through the challenges.

Performance Variations Under Different Conditions

- Skill Levels: Administer pre-tests and post-tests to participants to measure their knowledge and skills before and after engaging with CTF challenges and traditional methods.
- Group vs. Individual: Comparing the performance of students who work individually with those who collaborate in groups would provide an understanding of the impact of collaboration on their CTF experience.
- Time Constraints: Introducing time constraints would allow for the evaluation of how participants maintain accuracy and completion rates under pressure, simulating real-world scenarios.

Comparison with Conventional CTF Methods

- Learning Outcomes: Assessing the effectiveness of CTF challenges in achieving specific learning outcomes compared to traditional methods such as lectures and textbooks.
- Retention: Measuring the long-term retention of knowledge acquired through CTF challenges versus traditional resources.
- Engagement: Evaluating student engagement levels in CTF challenges compared to traditional teaching methods to determine whether CTFs are more motivating and active learning tools.
- Resource Utilisation: Analysing the cost-effectiveness of implementing CTF challenges as part of the curriculum compared to traditional educational resources. To measure this metric, as well as the aforementioned ones, participants may be divided into groups, with one group using CTF challenges and the other using traditional methods. Their learning outcomes, such as test scores, skill development, or project performance may then be compared.
- Feedback and Surveys: Utilising participant feedback to identify strengths and weaknesses in CTF challenges relative to traditional teaching methods.

VII. CONCLUSION

Such gamified events foster a range of skills beyond mere domain-specific knowledge, such as collaboration, research abilities, critical thinking, and problem-solving capabilities, all of which are considered foundational skills for any discipline. As a result, the gamified learning approach embodied by the open-ended CTF can be adapted to various modules and subjects, thereby diversifying and enriching the traditional academic curriculum.

For instance, a similar open-ended CTF model can be deployed in business or economics courses to explore various market scenarios or economic theories. Participants can engage in solving complex business scenarios, strategising under different market conditions, or making financial predictions based on available data. The successful implementation of such events can not only augment the learning experience but also develop critical business acumen and strategic thinking among participants.

The utility of such gamified learning approaches also extends to interdisciplinary modules, enabling students to navigate the complexities and interconnectedness of different subjects. In addition, the integration of cultural diversity, as seen in the international collaboration during the CTF events, promotes cultural inclusivity and broadens students' perspectives.

Finally, even though the preliminary findings of this study, which were enriched by informal student feedback and anecdotal accounts, are promising, additional structured research is still required. It is essential to quantify the effects of these gamified methods on the academic performance of students and investigate their adaptability across diverse disciplines. This spontaneous feedback disclosed participants' genuine enthusiasm, highlighting the potential and significance of such educational approaches. However, while this paper represents a promising beginning in the effort to more broadly integrate gamification in educational contexts, it also highlights the enormous untapped potential awaiting future exploration and application.

The games are not publicly available online to preserve their integrity and challenge, but educators or institutions can contact the corresponding author for arrangements to use them in their courses or events.

REFERENCES

[1] K. Cabaj, D. Domingos, Z. Kotulski, and A. Respício, "Cybersecurity education: Evolution of the discipline and analysis of master programs," *Computers & Security*, vol. 75, pp. 24–35, 2018. [Online]. Available: https://doi.org/10.1016/j.cose.2018.01.015

[1] L. Tsado, "Cybersecurity education: The need for a top-driven, multidisciplinary, school-wide approach," *Journal of Cybersecurity Education, Research and Practice*, vol. 2019, no. 1, p. 4, 2019.

[2] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, "From game design elements to gamefulness: defining "gamification"," in *Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments*, 2011, pp. 9–15. [Online]. Available: https://doi.org/10.1145/2181037.2181040

[3] M. J. Habgood and S. E. Ainsworth, "Motivating children to learn effectively: Exploring the value of intrinsic integration in educational games," *The Journal of the Learning Sciences*, vol. 20, no. 2, pp. 169–206, 2011. [Online]. Available: https://doi.org/10.1080/10508406.2010.508029

[4] T. M. Connolly, E. A. Boyle, E. MacArthur, T. Hainey, and J. M. Boyle, "A systematic literature review of empirical evidence on computer games and serious games," *Computers & education*, vol. 59, no. 2, pp. 661–686, 2012. [Online]. Available: https://doi.org/10.1016/j.compedu.2012.03.004

[5] "Hack the box: Hacking training for the best — individuals & companies," https://www.hackthebox.com/, (Accessed on 08/01/2023).

[6] "Tryhackme — cyber security training," https://tryhackme.com/, (Accessed on 08/01/2023).

[7] M. Coenraad, A. Pellicone, D. J. Ketelhut, M. Cukier, J. Plane, and D. Weintrop, "Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games," *Simulation & Gaming*, vol. 51, no. 5, pp. 586–611, 2020. [Online]. Available: https://doi.org/10.1177/1046878120933312

[8] J. B. Biggs and C. S. Tang, "Society for research into higher education," *Teaching for quality learning at university: what the student does*, 2011.

[9] L. S. Vygotsky and M. Cole, *Mind in society: Development of higher psychological processes*. Harvard university press, 1978.

[10] R. Paul and L. Elder, "A miniature guide for students on how to study & learn a discipline: Using critical thinking concepts & tools," *Rohnet Park, Calif: Foundation for Critical Thinking*, 2001.

[11] G. Zichermann and C. Cunningham, *Gamification by design: Implementing game mechanics in web and mobile apps*. O'Reilly Media, Inc., 2011.

[12] J. Hamari, J. Koivisto, and H. Sarsa, "Does gamification work? a literature review of empirical studies on gamification," in *2014 47th Hawaii international conference on system sciences*. IEEE, 2014, pp. 3025–3034. [Online]. Available: https://doi.org/10.1109/HICSS.2014.377

[13] M. Prensky and S. Thiagarajan, "Digital game-based learning," St. Paul, MN: *Paragon House*, 2007.

[14] L. McDaniel, E. Talvi, and B. Hay, "Capture the flag as cyber security introduction," in *2016 49th hawaii international conference on system sciences (hicss)*. IEEE, 2016, pp. 5479–5486. [Online]. Available: https://doi.org/10.1109/HICSS.2016.677

[15] S. Chaiklin, "The zone of proximal development in vygotsky's analysis of learning and instruction," *Vygotsky's educational theory in cultural context*, vol. 1, no. 2, pp. 39–64, 2003. [Online]. Available: https://doi.org/10.1017/CBO9780511840975.004

[16] J. Mirkovic and P. A. Peterson, "Class capture-the-flag exercises," in 2014 *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, 2014.

[17] E. Russo, G. Costa, and A. Armando, "Building next generation cyber ranges with crack," *Computers & Security*, vol. 95, p. 101837, 2020. [Online]. Available: https://doi.org/10.1016/j.cose.2020.101837

[18] "Github - moloch–/rootthebox: A game of hackers (ctf scoreboard & game manager)," https://github.com/moloch--/RootTheBox, (Accessed on 08/01/2023).

[19] J. Biggs and C. Tang, "Train-the-trainers: Implementing outcomes-based teaching and learning in malaysian higher education," *Malaysian Journal of Learning and Instruction*, vol. 8, pp. 1–19, 2011.

[20] L. Elder and R. Paul, "Critical thinking: Thinking to some purpose," *Journal of Developmental Education*, vol. 25, no. 1, p. 40, 2001.

[21] D. W. Johnson and R. T. Johnson, "An educational psychology success story: Social interdependence theory and cooperative learning," *Educational researcher*, vol. 38, no. 5, pp. 365–379, 2009. [Online]. Available: https://doi.org/10.3102/0013189X09339057

[22] K. M. Kapp, *The gamification of learning and instruction: game-based methods and strategies for training and education*. John Wiley & Sons, 2012.

[23] J. P. Gee, "What video games have to teach us about learning and literacy," *Computers in entertainment (CIE)*, vol. 1, no. 1, pp. 20–20, 2003. [Online]. Available: https://doi.org/10.1145/950566.950595

[24] J. Bruner, "The narrative construction of reality," *Critical inquiry*, vol. 18, no. 1, pp. 1–21, 1991.

[25] G. P. Wiggins and J. McTighe, *Understanding by design*. Ascd, 2005.

[26] J. Herrington and R. Oliver, "An instructional design framework for authentic learning environments," *Educational technology research and development*, vol. 48, no. 3, pp. 23–48, 2000.