Adapting CTF Challenges into Virtual Cybersecurity Learning Environments

Stylianos Karagiannis [0000-0001-9571-4417], and Emmanouil Magkos [0000-0002-5922-4274]

Department of Informatics, Ionian University,
Plateia Tsirigoti 7, 49100, Corfu, Greece
{skaragiannis,emagos}@ionio.gr

Abstract.

Purpose - This paper aims to highlight the potential of using CTF (Capture the Flag) challenges, as part of an engaging cybersecurity learning experience for enhancing skills and knowledge acquirement of undergraduate students in academic programs.

Design/methodology/approach – Our approach involves integrating interactivity, gamification, self-directed and collaborative learning attributes using a CTF hosting platform for cybersecurity education. The proposed methodology includes the deployment of a pre-engagement survey for selecting the appropriate CTF challenges in accordance with the skills and preferences of the participants. During the learning phase, storytelling elements were presented, while a behavior rubric was constructed in order to observe the participants' behavior and responses during a 5-weeks lab. Finally, a survey was created for getting feedback from the students and for extracting quantitative results based on the ARCS model of motivational design.

Findings - Students felt more confident about their skills and were highly engaged to the learning process. The outcomes in terms of technical skills and knowledge acquisition were shown to be positive.

Research limitations – Since the number of participants was small, the results and information retrieved from applying the ARCS model only have an indicative value; however, specific challenges to overcome are highlighted which are important for our future deployments.

Practical implications – Educators could use the proposed approach for deploying an engaging cybersecurity learning experience in an academic program, emphasizing on providing hands-on practice labs and featuring topics from real-world cybersecurity cases. Using the proposed approach, an educator could also monitor the progress of the participants and get qualitative and quantitative statistics regarding the learning impact for each exercise.

Social implications – Educators could demonstrate modern cybersecurity topics in the classroom, closing further the gap between theory and practice. As a result, students from academia will benefit from the proposed approach by acquiring technical skills, knowledge and experience through hands-on practice in real-world cases.

Originality/value – This work intends to bridge the existing gap between theory and practice in the topics of cybersecurity by using CTF challenges for learning purposes and not only for testing the participants' skills. This paper offers important knowledge for enhancing cybersecurity education programs and for educators to use CTF challenges for conducting cybersecurity exercises in academia, extracting meaningful statistics regarding the learning impact.

Keywords Cybersecurity, Education, CTF, Challenge-Based Learning, Gamification

Paper type Research paper

1 Introduction

The demand for cybersecurity professionals grows fast nowadays, a fact which establishes the need for encouraging students to engage in cybersecurity education (Mahdi *et al.* 2016). Public and private sector maintain high interest in cybersecurity education and training programs, usually struggling to recruit enough workforce specialized in technical and complex topics. Arguably, a lot of companies and organizations cannot afford large-scale training programs in order to enhance the security awareness of their employees (Berger *et al.*, 2016). Most of the training programs which exist on the market are not flexible enough and usually are focused on advanced users or fail to meet the specific learning objectives of the beginners and non-IT workforce. Therefore, modern educational tools and training programs need to be extended in terms of reflecting the participants' personal needs, integrating *personalization* and *adaptiveness* (Schiaffino and Amandi, 2009; Dabolins, 2012; Liegle & Woo, 2000; Sottilare, 2017).

Maintaining high interaction levels in cybersecurity education is difficult, due to the absence of participants' skills and technical experience. Achieving high motivational rates in cybersecurity is still an

issue due to the required high background knowledge and advanced skills required for participating in cybersecurity education and training programs (Cheung *et al.*, 2011). Even nowadays there is an increasing demand for enhancing the learning process by integrating elements which provide high levels of interactivity, an important attribute for improving the learning experience (Chan *et al.*, 2019). Furthermore, the variation among participants in terms of background knowledge, skills and experience is a major issue and requires adaptiveness and personalization in order to conduct successful learning programs (Tsekeridou *et al.*, 2008). Particularly in academia, a small size of knowledge hyperspace is covered, with major difficulties in terms of skills, knowledge and experience acquirement. It is important for the learning programs to be able to extract information about the characteristics of the participants in order to improve the current approaches, and at the same time a necessity for conducting personalized exercises and amending the current educational approaches (Schiaffino and Amandi, 2009; Kirlappos *et al.*, 2014; Alvarez-Xochihua *et al.*, 2010).

During the last years, *Capture the Flag* (CTF) competitions have attracted much interest from the information security community (Chothia & Novakovic 2015). Using CTF challenges, the skills of contesters are tested in various security topics such as cryptography, steganography, Web or binary exploitation and reverse engineering among others. Previous work has shown concerns that CTF challenges are mostly used for bug hunting, usually without including real-case scenarios and without having specific learning objectives (Vigna, 2003; Eagle & Clark, 2004; Mirkovic & Peterson, 2014; Werther et al., 2011). On the other hand, CTF challenges maintain the option for customization and might offer high interactivity levels, thus enhancing the learning experience (Trickel *et al.*, 2017; Schreuders *et al.*, 2017; Schreuders *et al.*, 2018). Indeed, creating learning experiences which appeal to personalized characteristics, specific skillset and background knowledge might improve the motivation rates of the learning programs and enhance the learning outcomes (Chung & Cohen, 2014; Irvine, 2011; Irvine et al,. 2017). Towards this direction, security scenarios based on CTF challenges could be used for enhancing the educational context in cybersecurity topics.

1.1 Our Contribution

To the best of our knowledge, not much work has been done regarding the use of CTF challenges as a virtual cybersecurity learning environment for undergraduate students in academic programs. Most of the approaches present CTF challenges as an opportunity for the participants to test their skills and not as a learning tool. In this paper, a selected set of CTF challenges was adopted and presented as the main learning environment for cybersecurity topics in the official academic curriculum, using a CTF hosting platform. In our case, the CTF challenges were presented through a linear sequence while simultaneously presenting educational context for the students to engage gradually and acquire the appropriate knowledge, skills and experience. As a result, students were highly engaged to the complex topics of cybersecurity, overcoming the knowledge obstacles which usually prohibit them from engaging to hand-on practice exercises.

The theoretical value of this research concerns the integration and alignment of the ARCS model in combination with the learning theory of constructivism, in order to align each learning step accordingly, construct a methodological approach for using CTF challenges as a learning tool, and extract results regarding each deployed challenge. Towards this direction, we integrated attributes such as gamification, collaborative learning and attributes which enhanced knowledge and skills acquirement. An empirical analysis was conducted as well as a behavioral analysis using observation research to evaluate our approach. The impact of the proposed method, in terms of skills and knowledge acquirement was confirmed, as well as the potential of using CTF challenges for acquiring skills and technical experience in an academic environment. The possibility to use CTF challenges in topics other than cybersecurity was also evaluated by presenting the relevance between various topics such as technical concepts varying from operating systems, networks, databases and web infrastructure among others.

1.2 Outline

The rest of this paper is organized as follows: Section 2 discusses the related work in the area, while Section 3 presents the proposed methodology, including the main building blocks of the proposed approach. Section 4 describes the conducted experiment and the deployment of the proposed approach, while Section 5 presents evaluation results, also discussing benefits, drawbacks and challenges of the proposed approach. Section 6 concludes the paper.

2 Related Work

A number of previous works mentioned the importance of maintaining live exercises and of using CTF challenges as a necessary component of the computer security curriculum (Vigna, 2003; Antonioli *et al.*, 2017). Works such as the above outline the high difficulty and the pitfalls in the implementation and deployment of such approaches. Most researches mention the lack of familiarity of the participants in terms of skills and propose CCTFs (Classroom CTFs), as an alternative method of lecturing (Mirkovic & Peterson, 2014). Designing and embedding CTF challenges for enhancing the learning process has been mentioned as an alternative approach for skills and knowledge acquirement, in contrary to traditional educational methods (Mirkovic & Peterson, 2014; Werther *et al.*, 2011). More specifically, CTF challenges are presented as a method for enhancing the learning experience in cybersecurity, by increasing the motivation of the participants and presenting the positive outcomes in terms of skills acquirement (Dark & Mirkovic, 2015). However, no clear evidence has been given on how CTF-based approaches enhance the performance of students in the official exams and assessments (Kapp, 2012; Annetta *et al.*, 2009; Cheong, 2013). Ford *et al* (2017) introduced how high school students could engage in basic cybersecurity concepts, mentioning the negative outcomes regarding the lack of students' confidence. In their research, they highlighted the role of self-confidence and the sense of comfort on how it affects knowledge acquisition. Furthermore, Chothia & Novakovic (2015) proposed Jeopardy-style CTFs as an assessment and exercise method. The proposed method is similar to our research in terms of presenting clearly the steps and learning goals of their approach. However, in their research they do not highlight the ability to present educational context other than cybersecurity to extend their approach towards other IT topics as well. Moreover, they present CTF challenges as exercises and evaluation method only and not as a tool for the usual presentation of educational context, without providing a specific educational structure.

Leune & Petrilli (2017) and Lehrfeld & Guest, (2016) highlighted the positive effect of using CTF challenges in terms of the participants' self-confidence. More specifically, students with high self-confidence indicated high engagement levels and enjoyment, while they were able to develop practical skills. However, they mention that the participation itself has not clearly reinforced theoretical concepts, while in our approach the connection of theoretical concepts was addressed better. Last but not least, research was conducted on how to develop a randomized set of CTF challenges to create a large variety of unique challenges (Schreuders *et al.*, 2017; Burket *et al.*, 2015). Embedding gamification elements in the learning process has also been studied elsewhere (Boopathi *et al.*, 2015; Denning *et al.* 2013; Leune & Petrilli, 2017). The criteria that affect cybersecurity curriculum and particularly the impact of the users' technical skills and knowledge during cybersecurity competitions have also been mentioned (Weiss *et al.*, 2015; Haney & Lutters 2017). It has been noted that by not meeting the participants' needs, this will eventually lead to a lack of incentives for keeping the participants motivated and focused on the learning process (Vandewaetere *et al.*, 2012). By highlighting the users' interests and the main motivational criteria, some studies also categorize students' interests into short-term and long-term interests (Schiaffino & Amandi, 2009). Finally, previous research presents a major concern regarding that CTF challenges are mostly used for bug hunting, usually without including real-case scenarios and without having specific learning objectives (Chung & Cohen, 2014).

Although significant work has been carried on the benefits of maintaining CTF challenges as exercises for testing the participants' skills, the empirical evaluation and the usage of CTF challenges for maintaining live exercises inside a classroom for educational purposes is still open for research. More importantly, the integration of metrics that could identify the learning impact has not been sufficiently studied when maintaining such exercises. Consequently, this research paper proposes a method for maintaining live exercises for educational purposes using CTF challenges inside a classroom. Towards this direction, this research paper aspires to integrate Keller's ARCS model of motivational design (Keller, 1987) and a naturalistic observation research method for collecting the participants' behavioral events during the experiment.

3 Methodology and Building Blocks

To achieve our goals, we presented an engaging learning experience by integrating interactivity, gamification, self-directed and collaborative learning attributes, among others. Specifically, we run a teaching lab, featuring cybersecurity topics, for undergraduate students of the 7th semester of the Department of Informatics, Ionian University, Corfu, Greece and then evaluated our approach using

quantitative and observational research. Our methodology includes the creation and deployment of a pre-engagement survey, an observational research during the learning phase and a final survey for evaluating the ability to include the ARCS model to our approach. The goal of the pre-engagement survey was to identify the topics which students were mostly familiar with and to get feedback from the students. This information was used for selecting the appropriate CTF challenges in accordance with the skills of the participants and their personal preferences (pls also see Appendix B). More specifically, our methodology was created using the following building blocks:

ARCS Model of Motivational design. For designing our learning method and for extracting our results, we used metrics based on Keller's ARCS model of motivational design (Keller, 1987). This model is focused on intrinsic attributes which enhance the total motivation affecting the metrics of attention, relevance, confidence and satisfaction. Extra attributes were taken into consideration such as *perceived learning* and *self-directed learning* capabilities (Richardson *et al.*, 2003; Barzilai *et al.*, 2014; Garrison & Randy 1997).

The proposed learning method is derived from the learning theory of constructivism, meaning that the lecturer's role is to guide and facilitate the total process and help students to achieve their goals (Kim, 2001; Kalina & Powell 2009; Pittman, 2016; Cifuentes *et al.*, 2010, Jonassen & David, 1997; Pivec *et al.*, 2004). The theory of social constructivism and Vygotsky's Zone of Proximal Development was also taken into consideration (Chaiklin, 2003; Kalina & Powell 2009). Therefore, in our approach, the instructor acts like a facilitator during the learning process while supporting the learning curve of each student. Deriving from the Keller's model of motivation (Keller, 1987), the concepts of *Attention*, *Confidence*, *Relevance* and *Satisfaction* are specified and enhance the method. In order to evaluate the proposed approach, this study is focused on the topics of cybersecurity and more specifically on the investigation of the motivation levels and of perceived learning (Burley *et al.,* 2017; Namin *et al.*, 2016; Parekh *et al.,* 2017; Yasinsac, 2002).

CTF challenges as a cybersecurity learning tool. CTF challenges are proposed as the main tool in our method for enhancing the learning process, by enabling active participation and achieving high engagement levels. Before the process, user profiles were maintained to present and design new exercises. It is important to discover the main themes and elements the participants are mostly interested in. CTF challenges have been already proposed as an assessment method (Chothia & Novakovic, 2015; Leune & Petrilli, 2017) and we tried to investigate the outcomes from such an approach as well.

For the purpose of this research, we used CTF challenges from Vulnhub[1] in order to deploy our approach. CTF challenges seem to be important both to the participants and to the organizers, regarding the provision of experience and knowledge for designing better methods and learning tasks (Eagle & Clark, 2004; Antonioli *et al.*, 2017; Leune & Petrilli, 2017; Chapman *et al.,* 2014; Werther *et al.*, 2011). The positive learning outcomes of gamification in a virtual learning environment are also noted in the literature (Boopathi *et al.*, 2015; Denning *et al.*, 2013; Leune & Petrilli, 2017; Hendrix *et al.*, 2016). Nowadays, it is common for various events to include CTF competitions and workshops, presenting a large variety of security challenges (Nakaya *et al.*, 2016; Leune & Petrilli, 2017). Conducting a successful learning process requires converting and adapting CTF challenges taking into consideration the specific learning goals and skillset requirements. CTF challenges provide instant feedback, resulting in self-directed learning and self-assessment experiences which derive from the theory of constructivism, since participants are called to solve the set of tasks on their own or with collaboration (Pittman, 2016; Cifuentes *et al.*, 2010, Jonassen & David, 1997; Pivec *et al.*, 2004). We used the pre-engagement survey and extracted information regarding the participants' needs, interests as well as details about previous experience and background knowledge.

Gamification. Concerning the attribute of gamification and the impact of computer games to cybersecurity, various examples can be found in the literature, such as serious games, board games and tabletops, STEM (Science, Technology, Engineering, and Mathematics) and finally CTF challenges (Dillenbourg *et al.*, 2002; Tseng *et al.*, 2013; Boopathi *et al.*, 2015). A balance between problem solving, instructive material and assessments, together with gamification elements could result in positive learning outcomes (Cordova & Lepper, 1995; Pivec *et al.*, 2004). Gamification elements were used in our approach by providing scoreboard, using the CTFd[2] and FBCTF[3] hosting platforms. Furthermore, the challenges included step by

[1] vulnhub.com

[2] https://github.com/CTFd/CTFd

[3] https://github.com/facebook/fbCTF

step scenarios, some of them providing storytelling elements as well, and participants were encouraged to work in teams and help each other. The learning experience included goals and sub-goals, usually presented as scenarios from a computer game, including tutorials. Through scoreboards the participants were highly engaged, creating a competitive environment during the assessments. Gamification attributes presented through our approach were the following:

1. Problem solving challenges
2. Rewarding system and scoreboards
3. Trial-and-error processes
4. Storytelling elements
5. Event, Competition and Tournament deployment
6. Teamwork/Collaborative learning elements
7. Information sharing across the participants regarding their own approach

Problem Based and Challenge Based Learning. By integrating *Challenge Based Learning (CBL)* and *Problem Based Learning (PBL)*, students are usually invited to learn about a topic by exposing themselves to multiple problems and being able to construct their own understanding of each concept and set their personal solutions. These attributes are important for achieving high motivation levels and developing self-paced steps, as well as enhancing collaboration during the learning process. Designing and constructing personalized projects and presenting them to the participants, could result in active learning experiences which is more promising from just digesting course content (Bruckman, 1998; Papert & Harel, 1991; Savery *et al.*, 1995; Jonassen *et al.*, 1999; Pittman *et al.*, 2016; Dark & Mirkovic, 2015). During the challenges, it was important to maintain information about the participants' skillset, background knowledge and motivations for participating in such activities, in order to have a clearer view of the whole process (Cheung *et al.*, 2011).

PBL and CBL, are usually embedded as approaches in CTF challenges resulting in engaging learning experiences and introducing gamification elements such as rewarding systems (Larking *et al.*, 2013; Margetson, 1994; Norman, 2000; Camacho *et al.*, 2018). Designing and constructing personalized challenges, is an active learning approach which is more promising from just digesting course content (Bruckman, 1998; Papert & Harel, 1991). The students' lack of experience in terms of technical skills in academia, often reveals major issues during the learning curve (Cheung *et al.*, 2012; Tobey, 2015). The context of each course, educational material and instructional methods have to be converted and updated, depending on the topics and the background knowledge of the participants (Hendrix *et al.*, 2016). In Fig. 1, we highlight the importance of presenting challenges to students for enhancing the learning process and improving the learning outcomes.

Fig. 1. Proposed Learning Flow

Instructions were mostly supportive, to facilitate the process for the students to bypass issues that might derive from lack of background knowledge and experience. More specifically, in this paper, we used CTF challenges to introduce the educational context of the official academic curriculum. The participants were exposed to the challenges and expected to learn from practice while trying to find an appropriate solution to the presented problems. Furthermore, participants were expected to be able to execute real-world exploits and to discover vulnerabilities which match to the existing past incidents and real-world cases. The ARCS motivation model (Keller, 1987) was also included for analyzing the outcomes of our approach in terms of perceived learning and method acceptance in other courses as well.

Evaluation using observational and quantitative research: For the evaluation of our method qualitative and quantitative research was conducted. The qualitative research included a naturalistic observation research, using a rubric to collect behavior actions of the participants. An external observer recorded through pencil and paper those actions without using any personal data. The qualitative research was conducted to observe the participants' behavior and responses during a 5-weeks lab.

The students were informed and explicitly consented to the use of the in-class observations for research purposes. The observation method and the timeline were not discussed further, and the students were asked to behave naturally, informing them that specific questionnaires will be distributed afterwards without collecting any personal data. The students were informed that this lab was experimental and still under construction, highlighting that their contribution will enhance further the specific approach. The observation was focused on event sampling (Reis *et al.*, 2000; Irwin & Bushnell, 1980), meaning that specific behavior actions were recorded when occurred and nothing else before or afterwards. We specified in advance the types of behavior (events) in which we were interested in (Table 2). The data collection was proceeded using printed reports which were maintained by an external observer using detached observation (Whitehead, 2016). No personal data were collected such as names, age or gender and therefore the anonymity of the dataset was guaranteed. Regarding the classroom observations, guidelines for the research methodology were also taken into consideration (Ferguson et al., 2004; Barnard, 1998) as well as the rules related to privacy protection and data handling, such as Regulation (EU) 2016/679 (GDPR). Finally, the participation was voluntary, and students were not obligated to attend the specific lab. The quantitative research was conducted to collect responses regarding the ARCS model regarding the levels of attention, relevance, confidence and satisfaction.

Self-directed learning attributes were introduced by presenting guidelines that participants needed to follow in order to solve the challenges. In our case, through a pre-engagement survey, we collected from the participants statements and feedback regarding their personal characteristics such as background knowledge or motivational criteria. Before designing the proposed learning method, a needs analysis was conducted for identifying the participants' motives. The goal of this survey was also to increase the interest towards the proposed learning method.

4 A Virtual Cybersecurity Learning Environment based on CTF Challenges

The experiment was conducted on undergraduate students of the Department of Informatics, Ionian University, Corfu, Greece, with most of them not having significant experience or strong background knowledge in cybersecurity. Before starting the experiment, a pre-engagement survey was distributed. The number of the participants for the pre-engagement survey was 32 students and for the observation research during the lab experiment the number was raging from 25 to 30 students. Since the lab was optional, the number of participants differentiated each week. After completing the learning phase and the observation research, we conducted a final survey for getting feedback from the participants and used the ARCS model to verify that the model is appropriate and applicable to our approach.

4.1 Pre-engagement Survey

User profiling is important for creating personalized learning experiences, adaptive systems, intelligent tutoring systems, recommender systems, intelligent e-commerce approaches and knowledge management systems (Brusilovsky and Millan, 2007; Poo *et al.*, 2003; Schiaffino and Amandi, 2009; Wang *et al.*, 2006; Gauch *et al.*, 2007). To be effective in terms of the learning outcomes, specific directive instruction material has to be carefully organized and embedded into the learning process (Greitzer *et al.*, 2007). Virtual labs could be used as a virtual learning environment (Karlov, 2016), for the students to acquire the appropriate technical skills (Gilberg, 2006). The main goal of this questionnaire was to increase engagement and understand the needs, interests and characteristics of the participants towards a more focused learning experience.

Participants recognized the importance of adaptiveness and of the personalized learning experience and really appreciated the idea of presenting educational context through CTF challenges. Most of the pre-engagement survey answers (n=32) were mostly affiliated to students from Ionian University.

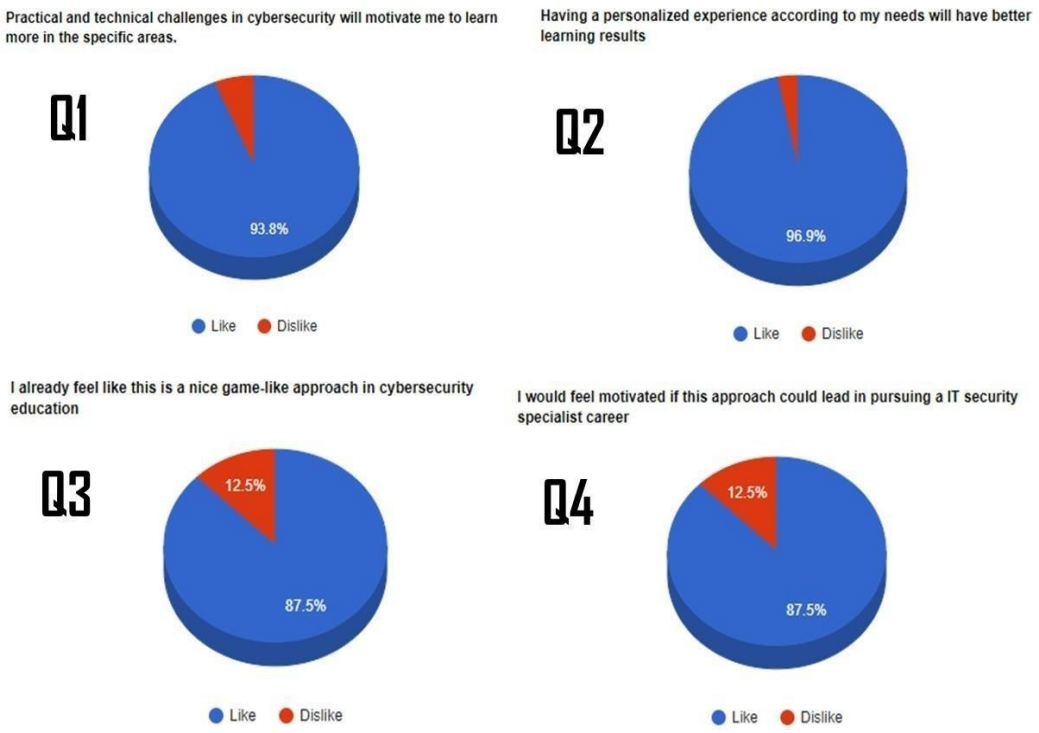

Fig. 2. Example questions from the Pre-engagement survey (32 students)

From the answers, participants found the prospect of maintaining realistic challenges very interesting. Specifically, the following statement was declared: *"Some examples of everyday life problems and a platform which will give me theoretical basic knowledge through tests and exercises"*. Positive attitude was expressed on gamification elements, although we did not present any specific details on how to achieve this. Some of the participants indicated negative feedback regarding game-based approaches and specifically the following statements were expressed: *"There is a difference between a game and educational context. I prefer an environment which will help me understand simple things even if I don't know anything about cybersecurity, but not using a game, because the context might be misleading"*. Most of the participants (n=23) seemed to be interested in actively participating in the creation of various scenarios and in contributing to the improvement of the proposed approach (Fig. 2). Some of the participants' statements were the following: *"Please contact me for further information as I'm interested in dealing with this kind of topics" / "I'm interesting in that" / "Of course I will provide any necessary help in topics related to cybersecurity" / "Cool" / "I won't be able to participate in the development during summer"*. The participants responded positively in maintaining future communication and collaboration with us, while most of the participants were positive in volunteering in every aspect of development, deployment or expanding the proposed approach to create their own CTF challenges.

4.2 Lab and Experiment

After collecting data regarding the participants' profile, we created a lab and the teaching methodology was divided into phases, depicted in Fig. 3. The figure represents our approach for adding content during the labs, steadily increasing or decreasing the instruction in contrary to the hands-on practice, homework assignments and black-box challenges. As depicted in Fig. 3, instructions were important at the beginning for the students to get familiar with fundamental concepts such as virtualization technologies and basic security topics. We decided steadily to introduce home assignments for the students to practice and included black-box challenges for testing their skills and increasing the competitiveness. The learning phase extended the training sessions using the CTF challenges, providing hands-on practice together with educative content to enhance the learning process and provide the connection to the theoretical concepts.

Phase 1: Instructions. Basic instructions were given regarding the purpose of the lab as well as basic commands and information related to the infrastructure and the CTF challenges.

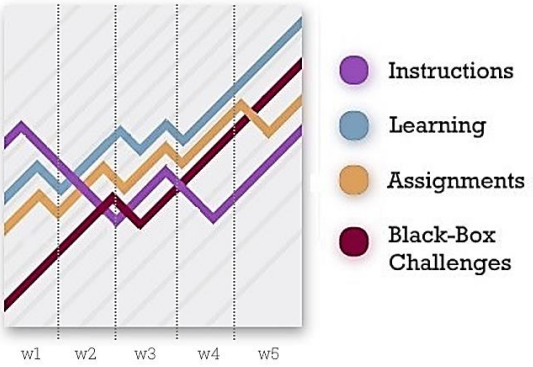

Fig. 3. Time spent for each week on each phase (Instructions, Learning, Assignment, Black-box Challenges)

The experiment was mostly focused on students' perspective for accepting this method as an engaging learning experience in cybersecurity and other IT topics as well. The instructions included directions for setting up a virtual lab, using virtualization technologies and providing the fundamental steps related to topics such as vulnerability scanning, information gathering and exploitation, among others.

Phase 2 – Learning Phase. Students followed appropriate guidelines to solve the challenges and some challenges were given for homework. During the learning process, observational research was conducted and afterwards a questionnaire was presented for the students to express their opinion regarding the approach. The selected challenges were chosen to be easy to deploy and for the students to clearly understand basic technical aspects such as networks, databases and cybersecurity topics, following specific guidelines.

In Fig. 4 the main interface of the CTF platform is presented along with the challenges of "Mr-Robot: 1" and "The Necromancer". The platform we used was CTFd[4] and we adapted the selected CTF challenges to this platform, by extending and increasing the number of flags for each challenge and by providing more details for each step.

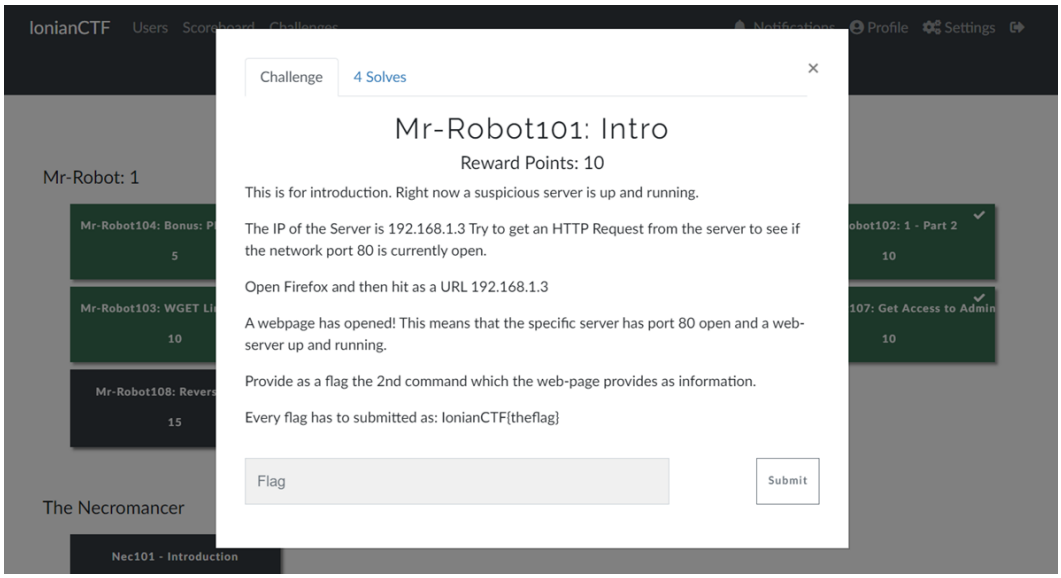

Fig. 4. The main interface of the CTFd in combination with the CTF challenges

The outcome was the usage of the CTF challenges for learning purposes, presenting step by step guidelines and integrating educational context into the platform itself. Every challenge was separated into multiple goals and sub-goals, to enhance the educational impact. For instance, the sub-challenge of "Nec101 – Introduction" needed to be completed for the participant to continue. On each step, various information and learning content was presented to the participants. While, typically, CTF challenges are used to evaluate

[4] https://github.com/CTFd/CTFd

the skills of the participants and test their abilities, in our setting, educational context was presented along with step by step guidelines to educate the participants. More importantly, educational context other than of cybersecurity was also presented, for the participants to acquire fundamental technical skills. Such skills included, among others, the familiarity with the Web infrastructure, networks, databases and operating systems. As a result, the required number of flags was increased, to enhance and stabilize the learning curve. In our setting, the instructor acted like a facilitator, while attributes such as collaborative learning and self-directed learning were starting to appear. During the learning phase, observation research was conducted, focusing on the participants' behavior.

Information from the pre-questionnaire was also taken into consideration regarding the properties and learning needs of the participants (pls also see Appendix B). For example, information was collected regarding the participants' confidence in specific topics such as programming, data structures, web infrastructure and mathematical background, among others. The purpose of the learning phase was to help students understanding the relevance between the complex theoretical concepts, and allow them to create their own knowledge interconnections. During this process, it is important for the students to correlate practical skills with theoretical concepts and get familiar with the related software tools and components.

For conducting the learning phase, a variety of implemented challenges were used (Perrone *et al.*, 2017) such as Metasploitable[5], DVWA[6] and Webgoat[7] among others. In our case we used the challenges presented in Table 1. The selected challenges are mostly focused on specific topics and usually embed storytelling elements, while maintaining fast-paced learning experiences. Fig. 5. presents the immersive context of a specific CTF challenge (Mr. Robot: 1). Through this task the participants got familiar with the Web infrastructure and with basic concepts of networking. Details regarding the total progress for each challenge are presented in Table 1, as well as limitations in terms of insufficient guidelines, limited time and other various issues which prohibited or differentiated the expected process.

Challenge	**Progress**	**Topics**	**Limitations**
JIS CTF	+++++	[1][2][3][4]	Insufficient walk-through
RickdiculouslyEasy	+++++	[1][2][3][4][8]	No serious issues
The Necromancer	++	[1][2][4][7][8][9][10][11]	Virtual machine has to be deployed independently
Web Developer	+++++	[1][2][3][5][7]	Outdated guidelines, WordPress plugin has been removed
Mr. Robot1	++++	[1][2][3][7][4][3][10]	Limited Time
Basic Penetration Testing	+++++	[1][9][11]	No serious issues

Topics: [1] Network Enumeration —[2] Directory Enumeration —[3] Web Services —[4] Reverse Shell —[5] Password Attacks —[6] Packet Analysis —[7] Privilege Escalation —[8] Network Tools —[9] Forensics —[10] Metasploit/Searchsploit —[11] Privilege enumeration —[12] Storytelling Elements

Table 1. Details and presented topics or attributes from the selected CTF challenges

The participants were using KALI Linux to find the solutions to the challenge. CTF challenges can be deployed either locally, or as a centralized service to the local network. In each case there are specific advantages and disadvantages which apply differently to each CTF challenge. In our case most CTF challenges were deployed locally on participants' computers. For example the participants, after opening a webservice using their browser, were introduced to the story, having the ability to interact with the virtual system and with the webservice (Fig. 5). The storytelling elements of this challenge derive from the TV-series "Mr. Robot[8]".

The learning process begins with the presentation of the topics, a set of directions and the upcoming learning outcomes. Afterwards, students proceeded in solving the proposed challenges following a set of guidelines in order to complete the challenges. Each challenge included specific sub-goals that must be fulfilled to reach the final goal.

[5] sourceforge.net/projects/metasploitable/
[6] dvwa.co.uk
[7] github.com/WebGoat/WebGoat
[8] https://www.imdb.com/title/tt4158110/

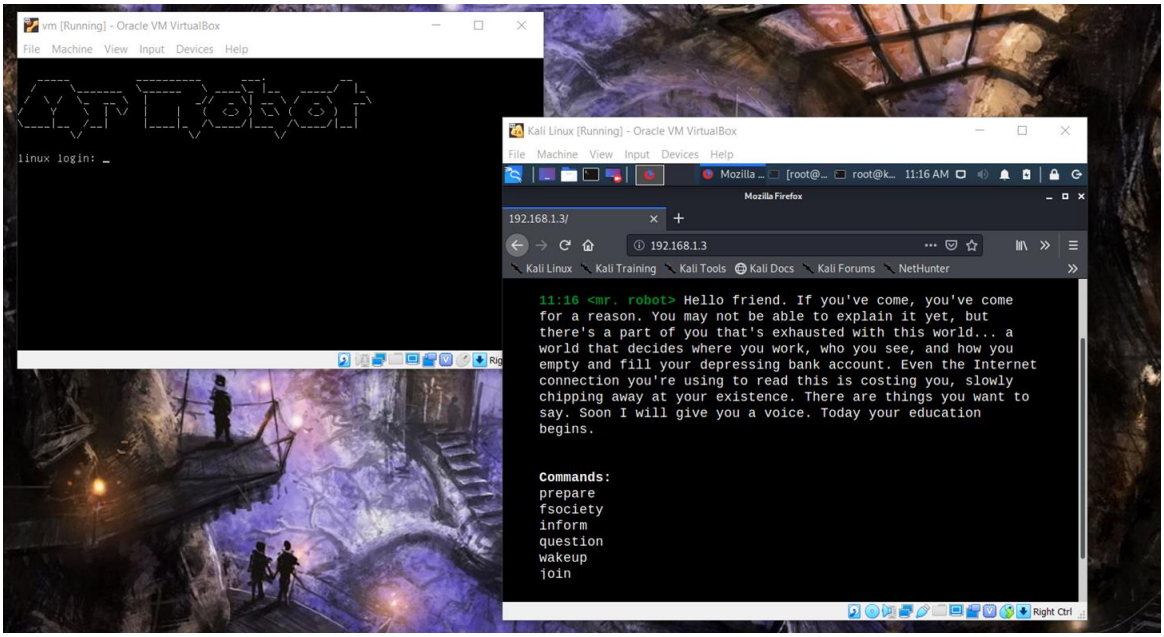

Fig. 5 Immersive content which was presented from the CTF challenge "Mr. Robot: 1[9]"

Phase 3 - Assignments. To improve the learning outcomes, assignments were distributed to the participants, since this method incorporates self-directed learning capabilities. The main purpose of this process was for the participants to have sufficient time to discover and analyze the tasks thoroughly and collaborate to find the solutions. For achieving better results, it was important to the participants to improve their searching and problem-solving skills as well as to improve their approaches through collaboration and self-discovery. As an extra task, participants were asked to create their own guidelines, explaining most of the sub-tasks and commands they executed. As a result, participants had to construct their own knowledge and provide a concrete and detailed guideline for solving the challenges as well as to present different aspects and approaches for each incident, proposing methods for enhancing the security of the systems.

Phase 4 - Black-Box Challenges/CTF Event and Assessment. After the alignment of the learning phase (duration: 5 weeks, 2 hours/week), we conducted a CTF challenge as an event/tournament. We used custom CTF challenges as an assessment tool and conducted an assessment, based on a 2-day event. The purpose of this event was to evaluate the effectiveness of the proposed learning method and learning outcomes, increasing the engagement levels. Through this approach it was possible to monitor and evaluate the progress of each student, however the scoreboard was not taken into consideration as an official assessment method. In this phase, the participants were mostly undergraduate students of the 7th semester of the Department of Informatics, Ionian University, Corfu, Greece. The scoreboard with the nine highest ranking scores is presented in Fig. 6. Four participants outside of our academic environment were participated in the final competition and expressed interest in participating in the future as well. Their participation was not included in the research; however, it is useful to mention since it indicates that people outside of academia may also be interested in such approaches. From the scoreboard it was discovered that there were 3 major groups of participants regarding their skills:

- The first group included participants who scored higher than others.
- The second group included participants who had medium scores.
- The last group included participants that scored lower than the others or had no activity.

Participants who did not have any previous experience on CTF challenges, had specific problems on how to correctly submit the flags and understand the process. For beginner-level participants it was time-consuming to effectively search for any support from Google and for further directions. It was inevitable that most of the students were confused on how to proceed, since they did not have any similar experience in the past. However, they acquired enough familiarity and started submitting flags afterwards.

[9] https://www.vulnhub.com/entry/mr-robot-1,151/

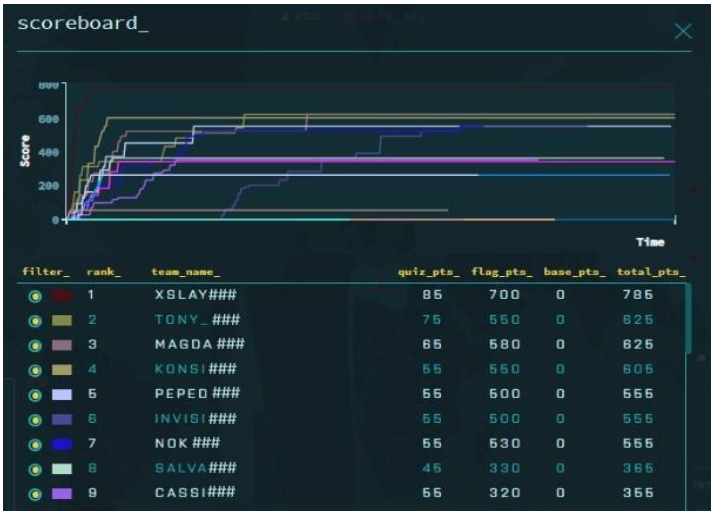

Fig. 6. Scoreboard from CTF challenge - Event-Based CTF using FBCTF

Using the scoreboard from FBCTF platform and the extracted game logs, the instructor/facilitator could monitor the progress of each participant and offer extra support when required. Details from the logs include failed and successful submissions, categories that the participant is mostly familiar with and the total progress. Such details could help the educator to manage better the learning process and extract meaningful statistics for each participant.

4.3 Qualitative Research Results - Naturalistic Observation Research

Through naturalistic observation, information was collected concerning specific behavior actions. Regarding the students' skills, the participants were separated again into 3 different groups, depending on their skills and performance. This was the result of a quick set of questions regarding their familiarity with UNIX systems, networks, coding and other fundamental IT topics. The first group included participants who did not have any specific skills in terms of IT, while the second group indicated participants with significant and basic knowledge of fundamental IT topics. The third group included participants with expert-level skills in programming, networks, databases and the IT infrastructure. The number of participants is also presented in Table 2 and the different colors indicate the participants' level of skills (Low, Medium, High). The participants' level was determined based on the pre-engagement survey as well as on observations in the classroom. The skills level for each participant was also matched with the scoreboard presented in the scoreboard (Fig. 6). It seems that in our case, the most appropriate method for extracting valuable information was probably to collect empirical data using observation research, since the collected data indicate the behavior of the participants during the learning process.

Number of participants with skills of: — L: Low level M: Medium level H: High level

Responses	Week 1	Week 2	Week 3	Week 4	Week 5
Fun [1]	1 2 1	4 2 3	3 3 2	5 4 5	2 1 4
Teaching [2]		1	1 2	1 1 2	3 2 3
Collaboration [3]	1 1 2	3 2 2	4 2 4	4 4 3	2 5 5
Theory [4]	2	2 1 3	1 2	1 3 4	1 5 6
New knowledge [5]	2 1 4	4 3 2	1 2 1	1 3	2 4
Participants [6]	12 10 7	8 9 6	4 8 7	9 6 7	8 7 6
Customization [7]			1	1 2	1 1 2
Questions [8]	9 7 9	14 8 4	5 7 5	7 4 4	6 4 7
Free Lab [9]	7 6 4	7 5 6	4 5 5	5 2 7	2 3 6

Table 2. Behavioral responses from 25 to 30 students during the lab (5 weeks)

The observation matrix is a sample of an evaluation rubric, maintaining much information about the potential of the proposed approach. This was a constructed observation, meaning that only specific behaviors were observed and monitored, without collecting any personal data. The observation was

conducted without using any monitoring devices, to conform to data privacy protection rules, such as Regulation (EU) 2016/679. Specific actions (Table 2) indicated the following aspects of behavior:

Fun [1]: Fun is considered as actions related to happiness and entertainment derived from social-emotional interaction process (Bisson *et al.,* 1996), such as smiling or speaking out loud or showing enthusiasm.

Teaching [2]: This action indicates the will for presenting a constructed and specific action of collaboration, in which the participant is trying to explain the method or issue to other participants (Hiebert *et al.,* 2007).

Collaboration [3]: This action indicates collaboration of participants for completing a simple task or set of tasks (Dillenbourg, 1999; Peters *et al.,* 1998).

Theory [4]: Participants mentioned the connection of specific action or a set of actions with various theoretical aspects (Wolffe *et al.,* 2014).

New Knowledge [5]: Participants are usually overconfident concerning their background knowledge and fall into simple mistakes easily. Therefore, a high level of perceived learning exists since the students are familiar to the topic and their mistakes push them to engage to the related topics (Wolffe *et al.,* 2014; Peters *et al.,* 1998).

Participants [6]: This indicator presents the number of participants for each week.

Customization [7]: This represents behavior related to the intention of the participants to set their own challenges or customize the process to their own perspective.

Questions [8]: The number of questions which have strong relation with the main topics.

Free Lab [9]: We maintained an optional lab. This represents the high engagement of the students, since it is self-driven action to participate in a lab outside the academic curriculum.

4.4 Quantitative Research Results - ARCS

Specific attributes derived from the ARCS motivation model (Keller, 1987) were used to extract results related to perceived learning. Most of the answers indicated sufficient reliability levels, as presented in the reliability check (Table 3). The results are not determined, due to the small number of the questionnaire's answers; however, in this section the applicability for the ARCS model to be aligned to our approach was tested.

Construct	*Cronbach's Alpha*
Attention	.91
Relevance	.72
Confidence	.87
Satisfaction	.95
Perceived Learning	.78
Self-Directed Learning	.76
Assessment Capabilities	.75

Table 3. Reliability check for each construct

The following statement evaluates this assumption, since perceived learning indicated high correlation: PER05 - *"I am able to learn, acquire skills and knowledge during this process"*. It is mentioned that specific attention variables indicated high and positive correlation taking into consideration the high score for perceived learning.

High rates in metrics of relevance, perceived learning and high confidence. Participants had issues in understanding the impact of the learning process in other IT topics. As a result, the constructs of satisfaction, perceived learning and the acceptance of this method concerning other courses was affected (Table 4). The construct of relevance indicated significant positive correlation with the construct of confidence (p=0.001, Pearson Correlation: 0.79). We assume that the presented challenges were able to highlight relevant topics, an important attribute for the participants to feel comfortable with the context.

Relevance	Satisfaction	Relevance	Perceived Learning
Pearson Correlation	.49	Pearson Correlation	.59
Sig.(2-tailed)	0.090	Sig.(2-tailed)	0.033

Relevance	Acceptance in other Courses
Pearson Correlation	.34
Sig.(2-tailed)	0.256

Table 4. Bi-variate correlation between Relevance and other constructs

For the participants to better follow the learning process, more attributes and sub-goals need to be integrated to further introduce other topics to them. Since the cybersecurity context is of high complexity, participants usually have issues in acquiring and understanding the required context regarding the related topics.

The importance of the confidence factor. Confidence is an important principle which enables the participants to continue and want to finish the tasks. Confidence indicates a positive correlation of 0.79 towards perceived learning (p=0.01).

High satisfaction and acceptance. Satisfaction along with the construct of attention, scored higher than any other element regarding the positive effects on perceived learning. Pearson correlation scored higher than 0.64 and p≤0.20 and attributes such as satisfaction seem to be very important for the learning process. The statement which encapsulates this aspect is the following: *"Excited (Satisfaction construct)— I can learn and gain skills and knowledge during this process (Perceived learning construct)"*. Satisfaction indicates correlation towards the acceptance of this method in other courses as well. The following statements indicate this connection: *"I would like to use similar methods in other courses / It would be nice to create scenarios like these in other courses"*.

High Scores in Perceived Learning. Participants scored perceived learning quite high 86.15%. The mean values for every variable of the perceived learning construct are presented in Fig. 7.

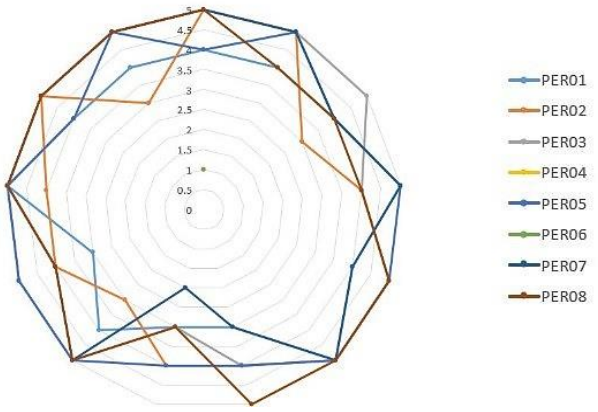

Fig. 7. Perceived learning - Mean Scores (Appendix A – Table 6)

Self-directed learning. Self-directed learning elements scored high (83%), however, sufficient correlation with other constructs were not identified. An updated version of this approach must be developed, focused on the elements of self-directed learning capabilities.

Usage of CTF challenges as an assessment method. The most difficult aspect of this approach is to correlate with the official academic curriculum. Most of the students were able to correlate this learning process with skills and knowledge acquirement. The students did not realize how and if such experience will help them achieve better grades. Many participants mentioned that the acquired skills and knowledge were very important, but most of the times the context of other courses is theoretical. Therefore, it is important during the learning process to enhance the connection to the theoretical concepts, by presenting educational context.

5 Evaluation and Discussion

This section presents some of the conclusive results and challenges or issues we experienced through the experiment. A high number of students enrolled in the course, showing a significant difference in terms of total participation, compared to last year's number of participants (Table 5). The number of total hits on the specific course during May 2019 was 3876, compared to May 2018 which was 2179. The number of the course registrations during 2019 were 69, compared to only 25 registrations in 2018. Therefore, the students were more active during the academic semester of 2019 and even if a few other reasons could have affected this result, such metrics are important indicators of the high engagement and interest towards our proposed method. Furthermore, such numbers highlight the students' preference to engage in hands-on practice and better understand technical topics.

Month/Year	**03/2018**	**03/2019**
N. of Hits	2179	3876
Duration	88.5	128.9

Month/Year	**04/2018**	**04/2019**
N. of Hits	1605	2533
Duration	65.8	119.1

Year	**2018**	**2019**
Registrations	25	69

Table 5. Number of Hits and Registrations of the course for 2018 and 2019

Many participants mentioned that they would accept CTF challenges as an official evaluation and assessment method. Bi-variate correlation indicates that the constructs of attention and satisfaction correlates highly with the construct of perceived learning (Fig. 8). More specific, the constructs of satisfaction and perceived learning indicated high correlation (8 of 11 statements indicate Pearson correlation greater than 0.70 with Sig.(2-tailed) lower than 0.08).

Correlations

		ATT01	*ATT02*	*ATT03*	*ATT04*	*ATT07*	*ATT08*	*ATT11*	*PER05*
ATT01	*Pearson Correlation*	1.00	.13	.72	.83	.44	.75	.73	.73
	Sig. (2-tailed)		.668	.006	.000	.136	.003	.005	.004
	N	13	13	13	13	13	13	13	13
ATT02	*Pearson Correlation*	.13	1.00	.22	.44	.68	.36	.47	.64
	Sig. (2-tailed)	.668		.477	.135	.010	.231	.105	.019
	N	13	13	13	13	13	13	13	13
ATT03	*Pearson Correlation*	.72	.22	1.00	.64	.31	.79	.83	.82
	Sig. (2-tailed)	.006	.477		.020	.299	.001	.000	.001
	N	13	13	13	13	13	13	13	13
ATT04	*Pearson Correlation*	.83	.44	.64	1.00	.39	.84	.74	.83
	Sig. (2-tailed)	.000	.135	.020		.190	.000	.004	.001
	N	13	13	13	13	13	13	13	13
ATT07	*Pearson Correlation*	.44	.68	.31	.39	1.00	.37	.50	.58
	Sig. (2-tailed)	.136	.010	.299	.190		.209	.079	.038
	N	13	13	13	13	13	13	13	13
ATT08	*Pearson Correlation*	.75	.36	.79	.84	.37	1.00	.77	.87
	Sig. (2-tailed)	.003	.231	.001	.000	.209		.002	.000
	N	13	13	13	13	13	13	13	13
ATT11	*Pearson Correlation*	.73	.47	.83	.74	.50	.77	1.00	.86
	Sig. (2-tailed)	.005	.105	.000	.004	.079	.002		.000
	N	13	13	13	13	13	13	13	13
PER05	*Pearson Correlation*	.73	.64	.82	.83	.58	.87	.86	1.00
	Sig. (2-tailed)	.004	.019	.001	.001	.038	.000	.000	
	N	13	13	13	13	13	13	13	13

Fig. 8. Bivariate correlation between Attention and Perceived Learning (see Appendix - Table 7)

The results highlight the importance of satisfaction towards the construct of perceived learning, meaning that it is important for the participants to feel satisfied to acquire technical skills. Participants, although confused, appreciated this method for acquiring practical skills and knowledge. Since beginner-level participants were not familiar with technical concepts and processes, they mentioned low levels of engagement. However, after 2 weeks this group of participants managed to follow quite well. The mean values for each construct are presented on Fig. 9, presenting how the attributes were expressed throughout the learning process.

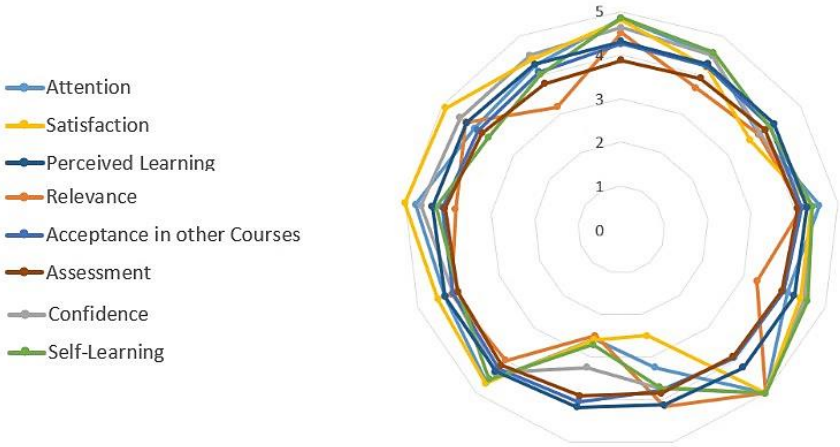

Fig. 9. All constructs - Mean Scores

The indicators regarding the constructs of perceived learning and attention were quite good. Minor issues reflected to the constructs of relevance, satisfaction (in some cases), self-directed learning and confidence. The participants highlighted the potential of this approach in terms of skills and knowledge acquirement. However, for some of the students it was difficult to follow due to lack of technical skills and insufficient background knowledge. Therefore, attributes such as self-directed learning elements could be improved and the ability for us to present relevant IT topics or to enhance the connection to the theoretical concepts. The findings were distilled based on both our observations and feedback of a total number of 32 enrolled students from the ARCS model and 25-30 students during the observation research. Information was collected using a final questionnaire as well as using the observation research that was conducted during the labs.

Our conclusions deriving from the questionnaire are currently restrained from the small number of participants; however, the proposed approach is considered to be appropriate and we intend to improve it and extract more results. Our purpose for using the ARCS model was to test if it is applicable in our case and to use it recursively for extracting quantitative metrics. On the other hand, we used the observation research to extract more information and behavioral statistic. Overall, our method succeeded in, or challenged the following attributes:

1. **Motivation and Engagement.** The results we got regarding the attention, relevance, confidence and satisfaction indicated the high motivation rates of our approach. Course subscriptions were increased (Table 5) and more students were physically participated in the learning process. At least half of the students were highly engaged in the whole process and participated in out-of-the-classroom events.
2. **Teamwork and Collaborative Learning.** During the learning process, students indicated the following:
   - They frequently collaborated and helped each other.
   - Participants were also tried to improve the current approaches conducting useful comments inside the classroom.
   - It was difficult for most of the students to collaborate, however they managed to share knowledge afterwards and solve challenges as teams.
3. **Self-Directed Learning.** Some participants did not maintain basic technical skills, however, following the guidelines and sufficient directions they eventually managed to understand the process. Attributes such as collaborative learning were also helpful to succeed in completing the tasks.
4. **Technical Skills and the Extent on other IT Topics.** Through the learning process, participants managed to understand technical aspects related to networks, databases, programming and operating systems. Therefore, not only cybersecurity skills were improved, but students were also able to understand other topics as well, filling the gap between theory and practice, while maintaining high information retention rates.
5. **Fun.** Most of the students were happy during this process, indicating emotions of excitement and satisfaction. Most of the comments were quite positive for maintaining such a more practical and technical approach. Furthermore, participants mentioned the entertaining aspects of the challenges, regarding elements such as storytelling and the theme-based context.

6. **Active Participation.** Participants indicated actions of active participation being critical, asking questions and interacting each other. Class discussions, short-written exercises, student debates and learning by teaching actions were present in the learning process.
7. **Security Awareness.** Students were able to understand most of the cybersecurity concepts. They demonstrated the attack vectors, vulnerabilities and mentioned ways for increasing security. Some of the cases included weak passwords, outdated software, lack of intrusion detection processes, phishing methods, inappropriate network topology and code flaws. The process of exploiting these concepts increased students' security awareness, not only as simple users but also as future engineers.

The following issues and specific challenges were discovered during and after the learning process:

1. **Official Curriculum.** The main challenge continues to exist regarding the usage of CTF in relation to the official curriculum. In order to incorporate our CTF–based methodology in the official educational process, the learning goals need to be well specified and mapped to the appropriate topics of the official curriculum.
2. **Learning Goals.** Every CTF challenge must indicate specific learning outcomes and learning goals.
3. **The balance between what students can do and cannot do -** *Zone of Proximal Development (ZKP)***.** Maintaining balance between the effort and what students could accomplish is difficult. Some tasks were very demanding, however the students succeeded in following the learning process. However, more work is needed to maintain the sufficient balance and settle to the ZKP accordingly. A solution could be the enhancement of self-directed learning attributes.
4. **Relevance.** Relevant IT topics were presented and discussed using our approach. However, it was difficult to reflect positive learning outcomes in every IT topic. A solution is to create sub-tasks or sub-challenges to embed appropriate guidelines.
5. **Competitiveness.** Our approach did not include attack and defense scenarios. The selected CTFs were mostly focused on Jeopardy-style CTFs. Furthermore, the CTF event increased the competence and engagement. We conclude that attack and defense scenarios might be difficult to maintain, but through competence the engagement levels would probably reach high scores. We came to this assumption by observing the behavior of the participants through the 2-day event.
6. **Real-World Cases.** The cases must be as real as possible for the participants to engage more in the learning process and acquire knowledge related to real incidents. The best way is to create or replicate existing infrastructures and to include exploitable services in order to introduce students to existing security incidents that took place in the past.

6 Conclusions

In this paper, a selected set of CTF challenges was adopted and presented as the main environment for skills and knowledge acquirement of undergraduate students in an academic class. Our approach involved integrating interactivity, gamification, self-directed and collaborative learning attributes, using a CTF hosting platform. The CTF challenges were presented through a linear sequence while simultaneously presenting educational context for the students to engage gradually and acquire the appropriate knowledge and skills. Our methodology included the deployment of a pre-engagement survey for selecting the appropriate CTF challenges in accordance with the skills and preferences of the participants. During the learning phase, storytelling elements were presented, and participants were encouraged to work in teams and help each other, while a behavior rubric was constructed in order to observe the participants' behavior and responses during a 5-weeks lab. Finally, a survey was created, for getting feedback from the students and extracting quantitative results based on the ARCS model of motivational design. Educators could use the proposed approach to systematically deploy an engaging cybersecurity learning experience in an academic program, emphasizing on providing hands-on practice labs for learning purposes, monitoring the progress of the participants and getting qualitative and quantitative statistics regarding the learning impact or each exercise, closing more the gap between theory and practice in cybersecurity.

Using a behavioral analysis, we extracted information regarding the participants' opinion and method acceptance. The results of this research presented specific important factors such as the impact of perceived learning, meaning that most of the students recognized that they learned and acquired various skills through this process. The fact that a small number of participants answered the final post-research survey might affect the quantitative results. Therefore, our conclusions deriving from the ARCS model are restrained as the main goals was to test the possibility for ARCS to be integrated to the proposed approach.

In terms of relevance and method acceptance the results indicate that the proposed method could be applied in other courses as well, but specific customization is required. More specifically, most of the participants indicated a positive attitude towards using this method in other IT topics as well and as an official assessment method.

Future work on the academic environment includes the improvement of the connection between theoretical concepts and hands-on practice and to create CTF challenges which focus on specific learning objectives. For example, we consider creating custom CTF challenges which will include learning objectives related to cryptography, networking and operating systems by identifying the specific skills which are required or can be acquired from each exercise scenario. The main challenge is to fully-integrate the attributes of this method to the CTF challenges in a better way. Explicit learning objectives and the relation to other IT topics need to be improved as well. Guidelines and the educational content could also be improved, to provide a complete and sufficient educational package. More work is also required for the integration of the attributes such as self-directed learning for embedding enhanced gamification elements. Finally, attack-defense scenarios could be included and tested, using our methodology, to improve the participants' engagement through teamwork and competitiveness. To address the above aspects, we consider creating a tool for creating and designing security scenarios according to the proposed methodology.

For applying this method to non-academic environments, it would be important to clarify the learning goals and understand the special characteristics of the participants. More specifically, for this method to successfully address the learning perspectives of such environment, the selected CTF challenges must be aligned to address the participants' skillset. Using for example the (NICE) Cybersecurity Workforce Framework provided by NIST (SP 800-181), the CTF challenges could be aligned to a fundamental reference for the workforce to meet cybersecurity needs accordingly. Matching the official guidelines to the requirements regarding the knowledge, skills and abilities acquirement, our approach could be revised accordingly. This process remains a challenge since not all the workforce has the same experience, knowledge and technical skills. Therefore, we consider creating specific CTF challenges or revising the existing ones to align to such aspects and extend our approach to be applicable to non-academic environments as well.

Appendix A

Questions for Perceived Learning
PER01 – The topics were very useful and more interesting than expected
PER02 - I feel I slightly improve my skills during the participation
PER03 - The content of this course is valuable and worth learning
PER04 - The presented learning activities in this course were very helpful to me
PER05 - I Feel like that the presented content is similar to Real-World events and cases
PER06 - I can acquire skills, knowledge and experience from this process
PER07 - Through this process not only real systems could be deployed but a whole real-word scenario
PER08 - Through this process I acquire skills and knowledge which will be important for my future on the IT

Table 6. Example questions for Perceived Learning

Questions for Attention
ATT01 - The themes (storytelling elements, scenarios, types of challenges) of the lab drew my attention
ATT02 - I was motivated to get more information related to security and privacy after participating
ATT03 – This process captured my attention
ATT04 - The way the learning goals and the skills are presented catch my attention and help me focus
PER05 - I Feel like those are Real World challenges. It is good representation of real systems
ATT07 - I learned some things that were surprising or positively unexpected
ATT08 - I wanted to explore all the options available to me. Complete all the sub-tasks
ATT11 - I enjoyed this lesson so much that I would like to know more about this topic

Table 7. Example questions for Attention

Appendix B

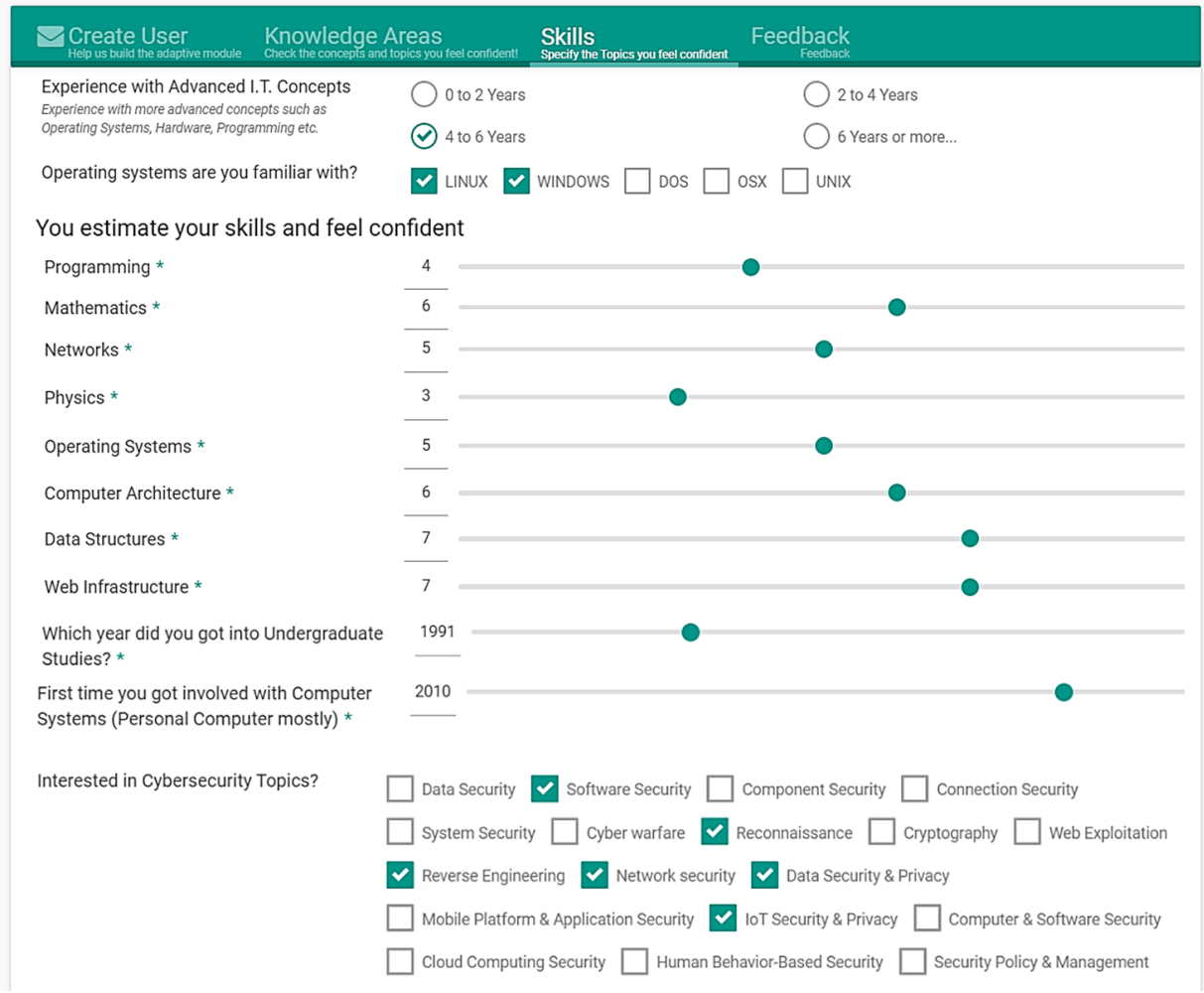

Fig. 10. Example from the pre-engagement questionnaire

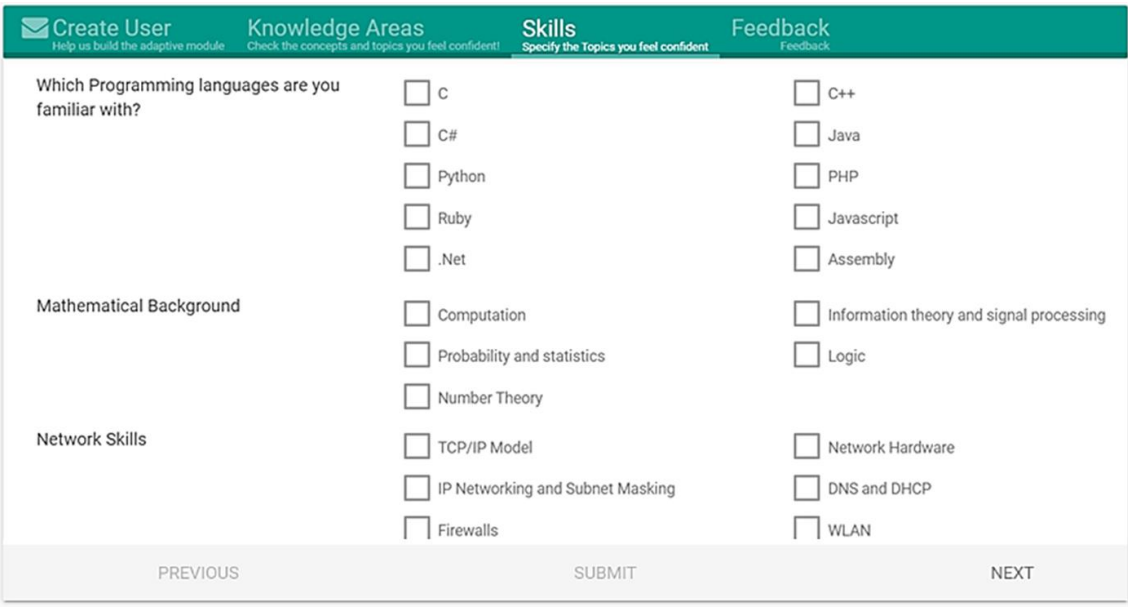

Fig. 11. Example from the pre-engagement questionnaire

References

Alvarez-Xochihua[1], O., Bettati[1], R., & Cifuentes, L. (2010). Mixed-initiative intelligent tutoring addressing case-based problem solving (Vol. 2). Technical Report TAMU-CS-TR-2010-7.

Annetta, L. A., Minogue, J., Holmes, S. Y., & Cheng, M. T. (2009). Investigating the impact of video games on high school students' engagement and learning about genetics. Computers & Education, 53(1), 74-85.

Antonioli, D., Ghaeini, H. R., Adepu, S., Ochoa, M., & Tippenhauer, N. O. (2017, November). Gamifying ICS security training and research: Design, implementation, and results of S3. In Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy (pp. 93-102). ACM.

Barnard, R. (1998). Classroom observation: Some ethical implications.

Barzilai, S., & Blau, I. (2014). Scaffolding game-based learning: Impact on learning achievements, perceived learning, and game experiences. Computers & Education, 70, 65-79.

Berger, H., & Jones, A. (2016, July). Cyber Security & Ethical Hacking for SMEs. In Proceedings of the 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society (p. 12). ACM.

Bisson, C., & Luckner, J. (1996). Fun in learning: The pedagogical role of fun in adventure education. Journal of Experiential Education, 19(2), 108-112.

Boopathi, K., Sreejith, S., & Bithin, A. (2015). Learning cyber security through gamification. Indian Journal of Science and Technology, 8(7), 642-649.

Bruckman, A. (1998). Community support for constructionist learning. Computer Supported Cooperative Work (CSCW), 7(1-2), 47-86.

Brusilovsky, P., & Millán, E. (2007). User models for adaptive hypermedia and adaptive educational systems. In The adaptive web (pp. 3-53). Springer, Berlin, Heidelberg.

Burket, J., Chapman, P., Becker, T., Ganas, C., & Brumley, D. (2015). Automatic Problem Generation for Capture-the-Flag Competitions. In 2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15).

Camacho, H., & Christiansen, E. (2018). Teaching Critical Thinking within an Institutionalized Problem Based Learning Paradigm--Quite a Challenge. Journal of Problem Based Learning in Higher Education, 6(2), 91-109.

Chaiklin, S. (2003). The zone of proximal development in Vygotsky's analysis of learning and instruction. Vygotsky's educational theory in cultural context, 1, 39-64.

Chan, S. C., Wan, J. C., & Ko, S. (2019). Interactivity, active collaborative learning, and learning performance: The moderating role of perceived fun by using personal response systems. The International Journal of Management Education, 17(1), 94-102.

Cheong, C., Cheong, F., & Filippou, J. (2013, June). Quick Quiz: A Gamified Approach for Enhancing Learning. In PACIS (p. 206).

Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge based learning in cybersecurity education. In Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F., & Carrillo-Marquez, V. (2012). Effectiveness of cybersecurity competitions. In Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Chothia, T., & Novakovic, C. (2015). An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education. In 2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15).

Chung, K., & Cohen, J. (2014). Learning obstacles in the capture the flag model. In 2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14).

Cifuentes, L., Mercer, R., Alverez, O., & Bettati, R. (2010). An architecture for case-based learning. TechTrends, 54(6), 44-50.

Cordova, D., & Lepper, M. (1995). Intrinsic Motivation and the Process of Learning: Beneficial Effects of Contextualization. Personalization, and Choice.

Dabolins, J. (2012). Trends of the usage of adaptive learning in intelligent tutoring systems. Databases and Information Systems BalticDB&IS '2012, 191.

Dark, M., & Mirkovic, J. (2015). Evaluation theory and practice applied to cybersecurity education. IEEE Security & Privacy, 13(2), 75-80.

Denning, T., Lerner, A., Shostack, A., & Kohno, T. (2013, November). Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (pp. 915-928).

Dillenbourg, P. (1999). What do you mean by collaborative learning?

Dillenbourg, P., Schneider, D., & Synteta, P. (2002). Virtual learning environments. In 3rd Hellenic Conference" Information & Communication Technologies in Education" (pp. 3-18). Kastaniotis Editions, Greece.

Eagle, C., & Clark, J. L. (2004). Capture-the-flag: Learning computer security under fire. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

Ferguson, L. M., Yonge, O., & Myrick, F. (2004). Students' involvement in faculty research: Ethical and methodological issues. International Journal of Qualitative Methods, 3(4), 56-68.

Ford, V., Siraj, A., Haynes, A., & Brown, E. (2017, March). Capture the flag unplugged: an offline cyber competition. In Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education (pp. 225-230). ACM.

Gauch, S., Speretta, M., Chandramouli, A., & Micarelli, A. (2007). User profiles for personalized information access. In The adaptive web (pp. 54-89). Springer, Berlin, Heidelberg.

Garrison, D. R. (1997). Self-directed learning: Toward a comprehensive model. Adult education quarterly, 48(1), 18-33.

Gilberg, F. (2006). Using Games to Improve Network Security Decisions.

Greitzer, F. L., Kuchar, O. A., & Huston, K. (2007). Cognitive science implications for enhancing training effectiveness in a serious gaming context. Journal on Educational Resources in Computing (JERIC), 7(3), 2.

Haney, J. M., & Lutters, W. G. (2017). Skills and Characteristics of Successful Cybersecurity Advocates. In SOUPS.

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game based cyber security training: are serious games suitable for cyber security training? International Journal of Serious Games, 3(1).

Hiebert, J., Morris, A. K., Berk, D., & Jansen, A. (2007). Preparing teachers to learn from teaching. Journal of teacher education, 58(1), 47-61.

Irvine, C. (2011). The Value of Capture-the-Flag Exercises in Education: An Interview with Chris Eagle. IEEE Security & Privacy, 9(6), 58-60.

Irvine, C. E., Thompson, M. F., McCarrin, M., & Khosalim, J. (2017, August). Labtainers: a Docker-based framework for cybersecurity labs. In Proc. 2017 USENIX Workshop on Advances in Security Education.

Irwin, D. M., & Bushnell, M. M. (1980). Observational strategies for child study. Holt, Rinehart, and Winston.

Jonassen, D. H. (1997). Instructional design models for well-structured and III-structured problem-solving learning outcomes. Educational technology research and development, 45(1), 65-94.

Jonassen, D. H., & Rohrer-Murphy, L. (1999). Activity theory as a framework for designing constructivist learning environments. Educational technology research and development, 47(1), 61-79.

Kalina, C., & Powell, K. C. (2009). Cognitive and social constructivism: Developing tools for an effective classroom. Education, 130(2), 241-250.

Kapp, K. M. (2012). The gamification of learning and instruction (p. 93). San Francisco: Wiley.

Karlov, A. A. (2016). Virtualization in education: Information Security lab in your hands. Physics of Particles and Nuclei Letters, 13(5), 640-643.

Keller, J. M. (1987). Development and use of the ARCS model of instructional design. Journal of instructional development, 10(3), 2.

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security.

Kim, B. (2001). Social constructivism. Emerging perspectives on learning, teaching, and technology, 1(1), 16.

Larkin, H., & Richardson, B. (2013). Creating high challenge/high support academic environments through constructive alignment: student outcomes. Teaching in higher education, 18(2), 192-204.

Lehrfeld, M., & Guest, P. (2016, March). Building an ethical hacking site for learning and student engagement. In SoutheastCon 2016 (pp. 1-6). IEEE.

Leune, K., & Petrilli Jr, S. J. (2017, September). Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. In Proceedings of the 18th Annual Conference on Information Technology Education (pp. 47-52). ACM.

Liegle, J. O., & Woo, H. G. (2000). Developing adaptive intelligent tutoring systems: a general framework and its implementations. Proceedings of the ISECON Philadelphia, PA, USA.

Mahdi, A. O., Alhabbash, M. I., & Naser, S. S. A. (2016). An intelligent tutoring system for teaching advanced topics in information security.

Margetson, D. (1994). Current educational reform and the significance of problem-based learning. Studies in Higher Education, 19(1), 5-19.

Mirkovic, J., & Peterson, P. A. (2014). Class capture-the-flag exercises. In 2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14).

Nakaya, M., Akagi, S., & Tominaga, H. (2016, November). Implementation and Trial Practices for Hacking Competition CTF as Introductory Educational Experience for Information Literacy and Security Learning. In Proceedings of ICIA 2016 (Vol. 5, pp. 57-62).

Namin, A. S., Aguirre-Muñoz, Z., & Jones, K. S. (2016). Teaching cybersecurity through competition. In Annual International Conference On Computer Science Education: Innovation & Technology (pp. 98-104).

Norman, G. R., & Schmidt, H. G. (2000). Effectiveness of problem-based learning curricula: Theory, practice and paper darts. Medical education, 34(9), 721-728.

Papert, S., & Harel, I. (1991). Situating constructionism. Constructionism, 36(2), 1-11.

Perrone, G., & Romano, S. P. (2017, September). The Docker Security Playground: A hands-on approach to the study of network security. In 2017 Principles, Systems and Applications of IP Telecommunications (IPTComm) (pp. 1-8). IEEE.

Peters, J. M., & Armstrong, J. L. (1998). Collaborative learning: People laboring together to construct knowledge. New directions for adult and continuing education, 1998(79), 75-85.

Pittman, J. M., & Pike, R. (2016). An Observational Study of Peer Learning for High School Students at a Cybersecurity Camp. Information Systems Education Journal, 14(3), 4.

Pivec, M., Dziabenko, O., & Schinnerl, I. (2004). Game-based learning in universities and lifelong learning: "UniGame: social skills and knowledge training" game concept. Journal of Universal Computer Science, 10(1), 14-26.

Poo, D., Chng, B., & Goh, J. M. (2003, January). A hybrid approach for user profiling. In 36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the (pp. 9-pp). IEEE.

Reis, H. T., & Gable, S. L. (2000). Event-sampling and other methods for studying everyday experience. Handbook of research methods in social and personality psychology, 196.

Richardson, J., & Swan, K. (2003). Examining social presence in online courses in relation to students' perceived learning and satisfaction.

Savery, J. R., & Duffy, T. M. (1995). Problem based learning: An instructional model and its constructivist framework. Educational technology, 35(5), 31-38.

Schiaffino, S., & Amandi, A. (2009). Intelligent user profiling. In Artificial Intelligence an International Perspective (pp. 193-216). Springer, Berlin, Heidelberg.

Schreuders, Z. C., Shaw, T., Shan-A-Khuda, M., Ravichandran, G., Keighley, J., & Ordean, M. (2017). Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting {CTF} Events. In 2017 {USENIX} Workshop on Advances in Security Education ({ASE} 17).

Schreuders, Z. C., Shaw, T., Mac Muireadhaigh, A., & Staniforth, P. (2018). Hackerbot: Attacker Chatbots for Randomised and Interactive Security Labs, Using SecGen and oVirt. In 2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18).

Sottilare, R. A., Brawner, K. W., Sinatra, A. M., & Johnston, J. H. (2017). An updated concept for a Generalized Intelligent Framework for Tutoring (GIFT). GIFTtutoring. org.

Tobey, D. H. (2015, June). A vignette-based method for improving cybersecurity talent management through cyber defense competition design. In Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (pp. 31-39). ACM.

Trickel, E., Disperati, F., Gustafson, E., Kalantari, F., Mabey, M., Tiwari, N., ... & Vigna, G. (2017). Shell We Play A Game? CTF-as-a-service for Security Education. In 2017 {USENIX} Workshop on Advances in Security Education ({ASE} 17).

Tseng, K. H., Chang, C. C., Lou, S. J., & Chen, W. P. (2013). Attitudes towards science, technology, engineering and mathematics (STEM) in a project-based learning (PjBL) environment. International Journal of Technology and Design Education, 23(1), 87-102.

Tsekeridou, S., Tiropanis, T., Christou, I., & Vakilzadeh, H. (2008). Toward virtual campuses: collaborative virtual labs & personalized learning services in a real-life context.

Vandewaetere, M., Vandercruysse, S., & Clarebout, G. (2012). Learners' perceptions and illusions of adaptivity in computer-based learning environments. Educational Technology Research and Development, 60(2), 307-324.

Vigna, G. (2003). Teaching network security through live exercises. In Security education and critical infrastructures (pp. 3-18). Springer, Boston, MA.

Wang, J., Li, Z., Yao, J., Sun, Z., Li, M., & Ma, W. Y. (2006, January). Adaptive user profile model and collaborative filtering for personalized news. In Asia-Pacific Web Conference (pp. 474-485). Springer, Berlin, Heidelberg.

Weiss, R. S., Boesen, S., Sullivan, J. F., Locasto, M. E., Mache, J., & Nilsen, E. (2015, February). Teaching cybersecurity analysis skills in the cloud. In Proceedings of the 46th ACM Technical Symposium on Computer Science Education (pp. 332-337). ACM.

Werther, J., Zhivich, M., Leek, T., & Zeldovich, N. (2011, August). Experiences in cyber security education: The MIT Lincoln laboratory capture-the-flag exercise. In CSET.

Whitehead, D., & Whitehead, L. (2016). Sampling data and data collection in qualitative research.

Wolffe, R. J., & McMullen, D. W. (1995). The constructivist connection: Linking theory, best practice, and technology. Journal of computing in teacher education, 12(2), 25-28.

Yasinsac, A. (2002). Information security curricula in computer science departments: Theory and practice. The George Washington University Journal of Information Security, 1(2), 1-9.