Interactive Environment for Effective Cybersecurity Teaching and Learning

Willi Lazarov
Brno University of Technology
Brno, Czechia
lazarov@vut.cz

Tomas Stodulka
Brno University of Technology
Brno, Czechia
tomas.stodulka@vut.cz

Tiina Schafeitel-Tähtinen
Tampere University
Tampere, Finland
tiina.schafeitel-tahtinen@tuni.fi

Marko Helenius
Tampere University
Tampere, Finland
marko.helenius@tuni.fi

Zdenek Martinasek
Brno University of Technology
Brno, Czechia
martinasek@vut.cz

ABSTRACT

Cybersecurity affects all users to some extent, and it is essential to raise awareness about potential cybersecurity risks and improve practical skills from an early stage of their education. This paper addresses these aspects and discusses the research, design, and implementation of a platform for effective cybersecurity teaching and learning. Our main contribution is the creation of an interactive environment with the easy-to-use execution and management of educational and training scenarios. Our solution is tailored for multi-level education, as well as small to medium-sized institutions, and we have validated its effectiveness through several test sessions conducted with university and high school students. In addition, the paper presents selected preliminary results from the testing performed and an overall evaluation of the environment.

CCS CONCEPTS

• **Social and professional topics** → **Computing education**; • **Applied computing** → **Interactive learning environments**.

KEYWORDS

BUTCA, CTF, Cyber Range, Cybersecurity, Education, Training

ACM Reference Format:
Willi Lazarov, Tomas Stodulka, Tiina Schafeitel-Tähtinen, Marko Helenius, and Zdenek Martinasek. 2023. Interactive Environment for Effective Cybersecurity Teaching and Learning. In *The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29–September 01, 2023, Benevento, Italy*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3600160.3605007

1 INTRODUCTION

When it comes to cybersecurity (CS), information and communication technologies (ICT) face a range of threats, such as malware, zero-day exploits, password attacks, denial of service (DoS), Man-in-the-Middle (MITM), phishing, injection attacks, and many others. These threats have been increasing rapidly and are expected to continue to grow at the same or even higher rates. No one is immune to cyberattacks, from government organizations to small-sized businesses or individual internet users. Therefore, it's crucial to educate both the public and experts to identify potential attacks, prepare for the consequences, and know how to mitigate such security threats. This is where cyber range (CR) comes into play. CR is a platform that creates simulated scenarios for users to experience different challenges. CR is particularly useful in the academic sector, where it can test theoretical knowledge in practical situations and can replicate thousands of scenarios [56].

Building a CR platform can be a complex and challenging process due to the comprehensive design and construction of the simulated or emulated environment. A typical CR includes various virtual machines, servers, and other components that emulate real-world cybersecurity scenarios, requiring expertise in networking, virtualization, development, and security. Creating and maintaining such an environment can be time-consuming, expensive, and technically demanding, leading organizations to face difficulties in building and sustaining their CRs. As new threats and vulnerabilities emerge, the ongoing challenge of updating the scenarios and training content adds to the overall complexity. As a result, many organizations struggle to provide effective cybersecurity training and educational resources to their employees [50].

To effectively manage and control the CR platform, a user-friendly interface is crucial for both the administrators and users. The paper addresses this challenge by introducing the interactive environment that was built and tested on the Brno University of Technology Cyber Arena (BUTCA) platform[1]. It provides an easy-to-use user interface for controlling the creation and restoration of Capture the Flag (CTF) scenarios, user management, and basic connectivity to the OpenStack virtualization platform. The comparison with other cybersecurity-focused educational and training platforms is detailed in Section 2.2. With this environment, administrators can efficiently manage and control the platform while guiding users through the prepared scenarios. The implemented solution and our multi-level approach to education are introduced in Section 3.

We organized several testing with high school and university students and also present preliminary effectiveness evaluation results of the interactive environment (Sections 4 and 5). We conducted pre- and post-surveys to gather detailed information about how

[1]More information about the BUTCA platform is available at https://butca.vut.cz/en/.

ARES 2023, August 29–September 01, 2023, Benevento, Italy

ACM ISBN 979-8-4007-0772-8/23/08.
https://doi.org/10.1145/3600160.3605007

students' cybersecurity knowledge, skills, self-efficacy, and interest changed after playing CTF. In addition, we collected CTF feedback in the post-survey, based on the Attention, Relevance, Confidence, Satisfaction (ARCS) model [30], and modified the survey items according to the Reduced Instructional Materials Motivation Survey (RIMMS) validated by Loorbach et al. (2015) [38].

2 BACKGROUND AND RELATED WORK

2.1 Scientific Review

Based on the Delphi Method in the article [8], five basic methods dealing with cybersecurity education have been evaluated. These methods with examples of their use are briefly listed as: **conventional** – on-site courses, classroom training and exercise, presentations and conferences; **online and software** – online courses; cloud-based training; software and materials available on the web; **game-based** – training in the form of built scenarios or CTF; **video-based** – educational videos; **simulation/virtualization** – testbeds, simulation platforms, virtual labs and exercises.

Game-based methods or simulation environments are highly recommended for cybersecurity education. They provide numerous benefits, such as enabling participants to get involved in interactive and hands-on activities and develop teamwork skills. These methods are also considered more attractive and enjoyable than traditional ones. Furthermore, user engagement and motivation are key factors for successful cybersecurity education and training in recent years [7, 36, 37]. Cyber ranges greatly meet the recommended methods of cybersecurity education mentioned earlier. By simulating real-world scenarios in a controlled environment, CRs can help individuals and organizations to better prepare for and respond to cyber threats. Depending on the technologies chosen, it may offer both simulated scenarios as well as game-based learning scenarios. CRs can be also accessed online, for example by connecting via a VPN (Virtual Private Network).

The importance of cybersecurity education at the high school level cannot be overstated in today's digital age. According to Irina (2022) [19], education at the high school level greatly influences a student's future career choice. In the case of cybersecurity education, this can lead to an increase in the number of cybersecurity experts, who are currently in high demand [2].

Many cybersecurity trainings have been conducted to cater to the diverse needs of students at different educational levels. Among these initiatives, the University of Wyoming organized three separate week-long camps (2020) [55] specifically targeting middle and high school students. Additionally, the UNITEN (Universiti Tenaga Nasional) Cyber Hunt (2021) [25] aimed to engage high school students, and a 4-week cyber security and cyberattack training was offered online (2022) [31], tailored for university students across five universities in Kazakhstan. These diverse programs were designed to introduce and enhance participants' understanding of various cybersecurity topics, interest, and motivation among students at different educational stages. The findings indicate that attending these events increased the overall interest in cybersecurity. At the same time, participants in UNITEN Cyber Hunt were less motivated to pursue opportunities to learn more about cybersecurity, likely due to more difficult challenges to solve, and also most of the students were at lower technical levels.

The introduction of cybersecurity education in primary or high schools opens a great opportunity to bring more cybersecurity experts, however, it raises another concern, which is the lack of teachers able to address this subject matter. This lack can be effectively compensated by the use of CRs [2], where users are guided through an engaging story, referenced to documentation, can take advantage of hints in case of a hitch, and are furthermore motivated to solve the problem thanks to the competitive mode. Teachers are still needed to provide additional explanations or help in case of unexpected problems, but they may no longer need to have a deep knowledge of the topics involved. Therefore, this type of solution can effectively support practical learning.

2.2 Platforms Overview

The relevant features of the interactive environment, as presented in this paper, have been compared to other solutions in Table 1. This comparison provides a summary of basic information about educational platforms, including BUTCA (listed in the last row). The overview is based on [44] and has been extended to include other educational or training platforms. A total of 35 solutions were analyzed, including CR platforms, software applications, and other tools for cybersecurity education and training. The analysis compared the available **cybersecurity challenges** that the platforms support such as network security, cryptography, and malware. Additionally based on scenarios, it considered **team types**[2] (red team – offensive security, blue team – defensive security, and yellow team – security design and development), **purpose** (educational, training, and research), **sector** (academic, government, military, and private), **open source availability**, and the **environment type** used to run scenarios. The choice of the environment type depends on the specific scenario being played out, the training objectives, and the level of risk that can be tolerated. In the analysis, we focused on the following 4 environment types:

- **Emulation** – a virtualized representation of the scenario topology, it mimics the behavior and functionality of the actual system, allowing users to interact with it as if it were real (e.g., emulating a DoS attack).
- **Hybrid/Cyber-physical** – the system runs on both physical and virtual topology, and is used in situations where the physical environment is an integral part of the system being tested or trained.
- **Simulation** – scenarios run on simulated real systems and are useful for testing and training in situations where it is not possible or safe to use production systems (for example, in case of attacking nuclear power plant).
- **Industrial** – scenarios can be a descendant part of emulation, hybrid, or simulation environment, but in addition, it is focused exclusively on industrial systems such as those used in manufacturing or critical infrastructure.

The properties included are not limited to those listed in Table 1, as the solutions may potentially contain other parameters that are not publicly available. Additionally, eight platforms were excluded from the comparison due to a lack of public information.

[2]We deliberately omitted the orange, purple, and green teams from the analysis due to the unavailability of public information on some of the compared solutions.

Table 1: Comparison of cyber ranges and other educational or training platforms

Platform	Cybersecurity challenges	Team types	Purpose	Sector	Open source	Environment
TryHackMe [51]	**NS, SS, SG, RE, C, E, F, M, W**	**RT, BT**	**L**	**P**	✗	**EM**
CTF365 [11]	-	**RT, BT, YT**	**T**	**P**	✗	**EM**
BTLO [4]	**NS, OS, SS, RE, F**	**BT**	**T**	**P**	✗	**EM**
Florida Cyber Range [41]	**NS, OS, F, M**	**RT, BT**	**L, T, R**	**A, G, M**	✗	**EM, S, I**
Virginia Cyber Range [9]	**NS, OS, SS, RE, C, E, F, W**	-	**L, T**	**A**	✗	**EM**
Cloud Range [46]	**NS, OS, SS, F, M, E, W**	**RT, BT**	**L, T**	**P, G**	✗	**EM, S, I**
Cyrange [17]	**NS, F**	**RT, BT**	**L, T, R**	**A, M**	✗	**EM**
CYBER RANGES [48]	**NS, OS, SS, E, F, W**	**RT, BT**	**L, T**	**P, G, M**	✗	**EM**
AIT Cyber Range [35]	**NS, M, F**	**RT, BT, YT**	**L, T, R**	**P**	✗	**EM, I**
KYPO CRP [53]	**NS, OS, SS, M, E, F, W**	**RT, BT, YT**	**L, T, R**	-	✓	**EM**
Norwegian CR [32]	**SG, DD, C, E, M, F, W**	**RT, BT**	**L, T, R**	**A, P, G**	✗	**EM, HCP, S**
JYVSECTEC [29]	**SG, DD, RE, C, E, M, F, W**	**RT, BT, YT**	**L, T, R**	**A, P, G**	✗	**EM, HCP, S**
CRATE [24]	-	**RT, BT**	**T, R**	**A, G, M**	✗	**EM, HCP, I**
CYBERIUM (Fujitsu) [26]	-	-	**T**	-	✗	**EM**
DECIDE (NUARI) [40]	-	**RT, BT**	**T**	**P, G, M**	✗	**S, I**
Hack the Box [3]	**NS, OS, SS, SG, RE, C, F, E, W**	**RT, BT**	**L, T**	**A, P**	✗	**EM**
PortSwigger WSA [43]	**W**	**RT**	**L, T**	-	✗	**EM**
Virtual Hacking Labs [34]	**NS, OS, C, E, W**	-	-	-	✗	**EM**
CTFlearn [12]	**SS, RE, C, E, F, W**	-	-	-	✗	**EM**
RingZer0 [49]	**OS, SG, RE, C, E, M, F, W**	-	**T**	-	✗	**EM**
PentesterLab [42]	**OS, E, W**	**RT**	**L, T**	**P**	✗	**EM**
Parrot CTFs [13]	**C, E, F, W**	-	**L, T**	**P**	✗	**EM**
VuCSA [52]	**SS, E, W**	**RT**	**T**	-	✓	**EM**
Root-Me [39]	**NS, OS, SS, SG, RE, C, E, F, W**	**RT, BT**	**T**	**P**	✗	**EM**
Georgia Cyber Range [6]	-	-	**L, T, R**	**A, P, G**	✓	**EM, HCP**
GACWR [23]	-	**RT**	**L, T**	**P**	✓	**EM**
Cyberbit CR [14]	-	**RT, BT**	**L, T**	**A, P, G**	✗	**EM, S**
CyberDefenders [15]	**NS, OS, SS, RE, F, M**	**BT**	**T**	**A, P**	✗	**EM**
Airbus CyberRange [18]	-	**RT, BT**	**T**	**P**	✗	**EM, HCP, S, I**
IBM X-Force C-TOC [28]	-	-	**T**	**P**	✗	**S**
PwC Cyber Arena [45]	**NS, OS, DD, M, F**	**RT, BT**	**T**	**P**	✗	**S**
CybExer [16]	-	**RT, BT**	**T, R**	**P, M**	✗	**EM, HCP, I**
CR14 NATO CR [10]	-	-	**T**	**M**	✗	**EM, HCP, I**
RangeForce [47]	**NS, OS, C, M, W**	**RT, BT, YT**	**L, T**	**P**	✗	**EM**
BUTCA	**NS, OS, SS, SG, RE, C, E, F, W**	**RT, BT**	**L, T, R**	**A, P, G**	✗	**EM, HCP, S, I**

Note: ***Cybersecurity challenges***: **NS** – Network security, **OS** – OS security, **SS** – SW security, **SG** – Steganography, **RE** – Reverse engineering, **DD** – (D)DoS, **C** – Cryptography, **E** – Exploitation, **M** – Malware, **F** – Forensic analysis, **W** – Web security. ***Team types***: **RT** – Red team, **BT** – Blue team, **YT** – Yellow team. ***Purpose***: **L** – Learning, **T** – Training, **R** – Research. ***Sector***: **A** – Academic, **P** – Private, **G** – Government, **M** – Military, **EM** – Emulation. ***Environment***: **HCP** – Hybrid/Cyber-physical, **S** – Simulation, **I** – Industrial.

Based on the comparison in Table 1, we can observe the distinct characteristics of each solution. The vast majority of the platforms are not distributed as open source and have been developed by private organizations or as part of research at various universities. Although the targeted sector is mostly private, some platforms focus on the academic, government, and military sectors. The comparison also indicates that most platforms focus on web security and red teaming scenarios, and their environment is emulation-based, with industrial environments being the least represented. In the case of the purpose, the ratio of learning and training platforms is fairly balanced, and academic solutions also target research.

For our research, we utilized the BUTCA cyber range platform, which targets research, training, and education in cybersecurity. In addition to the emulation environment, the BUTCA platform also includes the hybrid/cyber-physical environment and industrial sector. The interactive environment has already been integrated into cybersecurity courses at the Brno University of Technology and Tampere University. Furthermore, we have deployed the platform to support cybersecurity education at the Secondary Technical School in Třebíč. Our main goal is to continuously integrate the environment into more high schools, following our multi-level education approach, to support their cybersecurity teaching efforts.

3 IMPLEMENTED SOLUTION

3.1 Environment Architecture

The environment is composed of 3 component groups: databases, virtual machines, and services. These components are managed within the OpenStack cloud computing platform [22], utilizing shared networking and hardware resources. The virtual machines within the cloud platform consist of software applications that further communicate with both the services and databases.

The services include critical applications such as a web application that functions as the user interface, a relation database, and AWX [27] for automating complex processes. Additionally, we have implemented monitoring of hardware and cloud resource statistics through Prometheus [1] exporters. These statistics are displayed on a Grafana [33] dashboard. We also have central logging of OpenStack and system services using Fluentd [21] logs scraping, which is stored in an ElasticSearch [5] database and visualized on a Kibana [5] dashboard. The environment user interface, which provides users with access to their instances, is at the core of the platform. Most of the virtual machines are dedicated to educational and training scenarios, but the platform also contains research and development environments (e.g., mirrored and simplified components). Figure 1 displays a high-level diagram showcasing all the environment components built on the OpenStack platform.

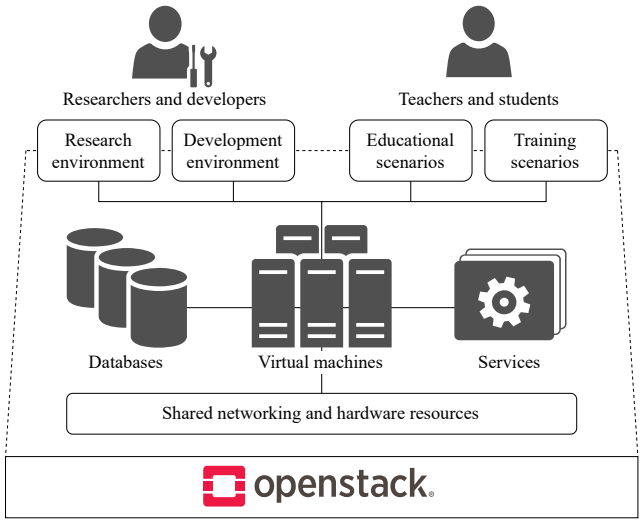

Figure 1: High-level diagram of the environment

The interactive environment is built on a user interface that visualizes all the components of a scenario to the user. Each educational or training scenario has its own template from which user instances are created. Instances can be categorized into two types: with or without a virtualized environment. If virtual machines are assigned to a scenario within its topology, users are given the opportunity to run them while performing tasks on the scenario. To enable easy portability and facilitate multi-level education, virtual machines can be controlled through a web browser using a VNC (Virtual Network Computing) console. Each instance begins with an introduction to the scenario, followed by individual hands-on training exercises. As part of the interactivity, users can use supporting documents such as manuals, presentations, and other materials, as well as attachments like files that require analysis. Instances contain hints, the use of which is penalized by deduction of points. Each scenario task always allows using the 100% hint to reveal the correct answer and continue the progress. Once the users complete the last task of the scenario, they are required to take a short final test to verify their acquired knowledge from the practical part of the scenario. A detailed example of an instance including an attachment and a virtual machine is shown in Figure 2.

3.2 Multi-Level Approach to Education

Our original objective was to support the teaching of the Information Security degree program at our university. However, during our research, we realized the need for a multi-level approach to education on cybersecurity, for the following reasons:

- Cybersecurity affects all users and should be taught from a young age, rather than only in specific majors.
- High schools often face a shortage of teachers in specialized areas such as cybersecurity.
- To obtain relevant results in our further research, we need data from various age groups, including lower grades.

To enhance learning, we prepared gamified scenarios in addition to the usual laboratory exercises (see Table 2). These scenarios incorporate a background story to enhance the learning experience while maintaining the integrity of the subject matter being taught. Despite the gamification, students interact with the tools and solve problems in a way that corresponds to the hands-on exercises. We have extended this concept to high school students, who have provided positive feedback on this approach to learning. Gamified stories are also intentionally designed to be adaptable to various scenarios with different difficulty levels. For instance, the CTF04 gamified scenario is a prime example of this design approach, as its story was also used and slightly modified for CTF05 and CTF10, with the corresponding difficulty for high schools. This variability ensures that the difficulty of the tasks aligns with the students' level of knowledge, making it a suitable challenge for them.

Table 2: Educational and training scenarios

CTF ID	Education level	Gamified	CS challenges
01	All	✗	**C, W**
02	University	✓	**OS, C, E, W**
03	University	✓	**SG, C**
04	University	✓	**NS, C, F**
05	High school	✓	**NS, SG, C**
06	University	✓	**OS, SS, RE, W**
07	University	✗	**NS, OS ,SS**
08	University	✗	**NS, RE**
09	University	✗	**NS, DD, F**
10	High school	✓	**E, W**

Note: **NS** – Network security, **OS** – OS security, **SG** – Steganography, **RE** – Reverse engineering, **DD** – (D)DoS, **C** – Cryptography, **E** – Exploitation, **F** – Forensic analysis, **W** – Web security.

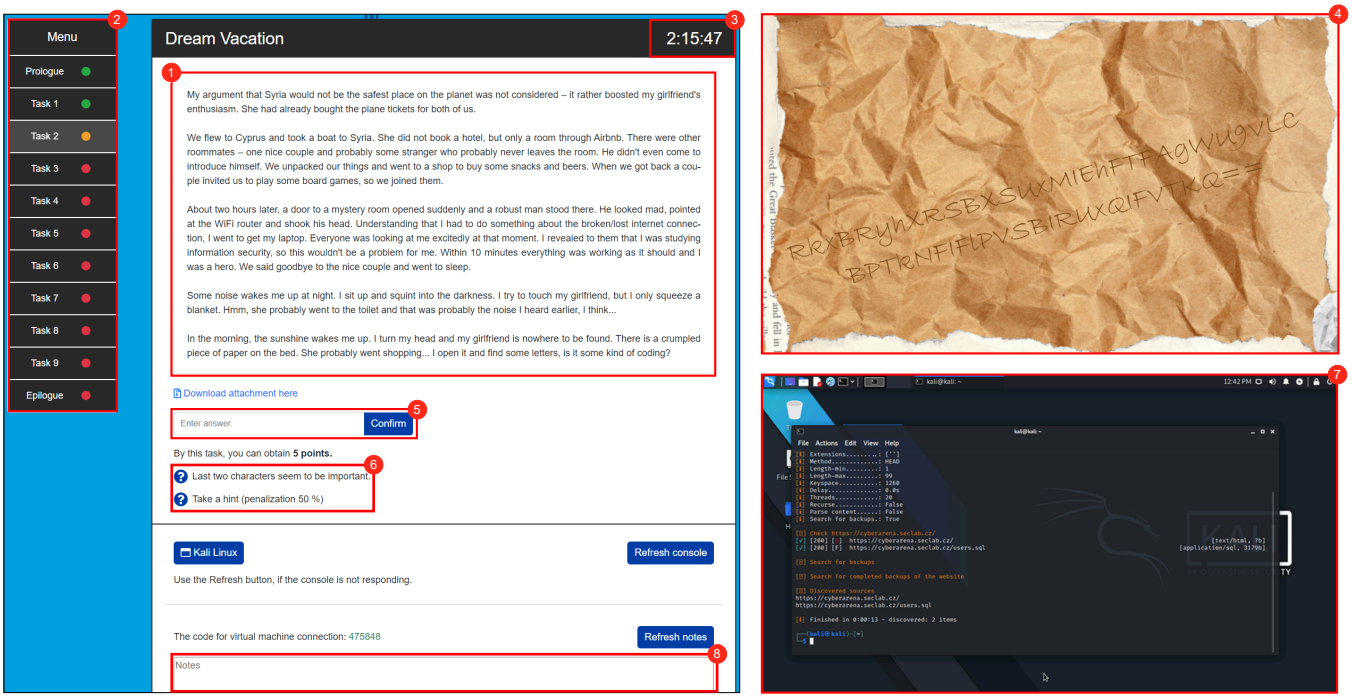

Figure 2: Detailed overview of scenario instance: ① Task description containing text relevant to the scenario, ② Progress with linear sequence, ③ Timer until the end of the scenario, ④ Attachment (e.g. PDF, video, image, etc.), ⑤ Input for entering the Flag, ⑥ Hints whose use is penalized, ⑦ Virtual machine (Kali Linux, Ubuntu, etc.), ⑧ Notes on the entire scenario.

For newcomers who haven't played any CTF in our environment, we prepared a Tutorial game (CTF01) with very simple tasks. The goal of this CTF is to introduce users to the principles of the CTF and how to navigate the user interface, including general rules and advice. For users who are unable to play the Tutorial CTF (for instance, due to missing prerequisites), we have prepared a small pocket guide that contains useful commands and guides for Kali Linux and Linux essentials, particularly for those with limited experience using the Linux operating system.

Since September 2022, Brno University of Technology (BUT) established a cooperation with Tampere University (TAU) regarding the connection of CTF games to cybersecurity education effectiveness. Initially, TAU students in two cybersecurity courses, representing beginners and advanced users, were invited to participate. However, due to a lack of participation, the promotion campaign was extended to all students at TAU. Students were able to choose from 2 prepared CTFs according to their skills, with CTF03 designated for beginners and CTF02 for advanced users. Furthermore, both CTFs were slightly modified to integrate the storyline better with the local area and the educational materials available in the local cybersecurity courses. Students who wished to take part in the research had to come to TAU's cyberlab at the Hervanta campus.

4 TESTING AND EVALUATION

In total, 9 CTF testing sessions with students were organized from December 2021 to April 2023 according to Table 3. The data collected during all play sessions could be separated into 3 groups: (**1**) data generated by the environment itself during playing, (**2**) data collected by a post-survey implemented by BUT, (**3**) more detailed data collected by pre- and post-surveys implemented by TAU.

Logging and monitoring were conducted by the environment itself to track the following personal data: incorrect answers, hints used, time taken to complete each task and scenario, final test points obtained, and overall scores of students. Furthermore, the students could provide feedback during in-person sessions according to environment visuals, functionality, and their insights.

In CTF testings organized in 05/2022, 06/2022, 12/2022, and 03/2023, we extended the collected data by a post-survey customized for each CTF. The questions covered overall satisfaction from the played game, satisfaction and difficulty for each task, and interest

Table 3: List of CTF testing sessions with students

Date range	CTF ID	Students	Age range	Data
12/2021	02	47	20–29	1
05/2022	05	10	15–19	1, 2
06/2022	05	28	15–19	1, 2
09/2022	04	28	20–29	1
11/2022	02	60	20–29	1
12/2022	05	35	15–19	1, 2
03/2023	04	23	20–29	1, 2
02–04/2023	03	30	Section 4.1.1	1, 3
02–04/2023	02	18	Section 4.1.2	1, 3

in attending future play-testing sessions either at Brno University of Technology or remotely. It is important to note that participation in filling out the post-surveys was voluntary.

In addition to the logging and monitoring conducted during the play sessions (1st data group collection), we have implemented pre- and post-surveys to gather much more detailed information about the students who played during 02–04/2023. These surveys are intended to replace the post-survey from the 2nd group of data collection. The students had to fill in surveys before and after playing, and we measured how their knowledge, skills, self-efficacy, and interest in CTF topics changed due to CTF playing. Using pre- and post-surveys, we also measured if CTF influenced students' cybersecurity-specific self-efficacy or cybersecurity attitude in general, and whether playing influenced students' interest in further studying cybersecurity, pursuing a cybersecurity career at a company, or a cybersecurity research career.

In the post-survey, we also collected CTF-feedback based on the ARCS model. We used also the RIMMS version of the Keller's original survey, modifying the survey items to fit our CTF-context. Students also assessed how various CTF properties and CTF tasks affected their satisfaction, and how meaningful these properties and tasks were for their learning. In addition, they also assessed how their general interest in cybersecurity changed due to these tasks and properties. Evaluation and feedback results can be used for further development. It should be noted that participation in CTF events and surveys was voluntary. Thus results are influenced by self-selection bias. This affects the generalization of the results. More details are presented in the following Subsection 4.1.

4.1 Preliminary Research Evaluation

CTF playing sessions in the period 02–04/2023 were evaluated using pre-post CTF surveys. The surveys consist of Likert-5 subscales. Some are identical for both CTFs and some are tailored CTF-specific to match CTF content. The subscales that we used for this preliminary analysis are listed in Tables 4 and 5.

Table 4: CTF-specific subscales in the preliminary analysis

CTF-specific subscales	CTF03		CTF02	
	Items	α	Items	α
CTF topic knowledge	8	.721	7	.848
CTF skills	4	.771	7	.858
CTF skill-related self-efficacy	5	.880	8	.858
Interest in CTF topics	12	.972	15	.967

4.1.1 CTF03 02–04/2023. A total of 30 students (16 males, 14 females) participated in a post-survey. Specifically, 20 students were aged 20–29, 7 were 30–39, 2 were 40–49, and 1 was under 20. Regarding the specialization: 2 students had cybersecurity as a major, 16 were other ICT students, and 12 were from other study programs.

A total of 28 students (16 males, 12 females) participated in both pre- and post-surveys. Specifically, 18 students were aged 20–29, 7 were 30–39, 2 were 40–49, and 1 was under 20. Regarding the specialization: 2 students had cybersecurity as a major, 16 were other ICT students, and 10 were from other study programs.

Table 5: Identical subscales in the preliminary analysis

Identical subscales	Items	α
Cybersecurity-specific self-efficacy[1]	20	.950
Cybersecurity attitude[2]	6	.840
Interest in further studying cybersecurity	5	.800
Interest in a cybersecurity career at a company	4	.944
Interest in a cybersecurity research career	3	.922

[1]Scale adapted from Wee et al. (2016) [54].
[2]Scale adapted from Faklaris et al. (2019) [20].

4.1.2 CTF02 02–04/2023. A total of 18 students (11 males, 7 females) participated in a post-survey. Specifically, 15 students were aged 20–29, 2 were 30–39, and 1 was 40–49. Regarding the specialization: 11 students had cybersecurity as a major, 5 were other ICT students, and 2 were from other study programs.

A total of 7 students (3 males, 4 females) participated in both pre- and post-surveys. Specifically, 4 students were aged 20–29, 2 were 30–39 and 1 was 40–49. Regarding the specialization: 3 students had cybersecurity as a major, 3 were other ICT students, and 1 was from other study programs.

5 RESULTS AND DISCUSSION

The interactive multi-level learning environment, which was designed to effectively support cybersecurity learning and teaching, was successfully validated through 9 testings with a total of 279 students (73 from high school and 206 from university).

The data group 1 collected during the playing helped to improve our environment and led to the handling of so far undiscovered bugs, either in the platform or in the played CTF scenario. The data are also very helpful in the case of testing newly developed CTF scenarios, as there can usually occur some problems. For instance, during CTF02, some students submitted flags in the wrong format because they used a different tool than the one we used in the pilot testing of the scenario. As a result, the flags were decoded incorrectly. Additionally, we made changes to the task descriptions and hints in CTF03 based on feedback, as they were not very clear. Apart from these modifications, we have also improved the user interface to enhance the overall experience.

The results from data group 2 testing showed that the difficulty level of the tasks was appropriate, and any necessary adjustments were made to ensure that the points obtained for each task corresponded to its difficulty. As a result, scenarios CTF01–CTF05 require no further modifications. The feedback we received from participants indicates a positive interest in playing in the BUTCA environment in the future. Particularly, we received:

- 8 responds from testing in 05/2022 with 100% interest,
- 10 responds from testing in 06/2022 with 100% interest,
- 6 responds from testing in 03/2023 with 100% interest,

and 31 responds from testing in 12/2022 (Secondary Technical School in Třebíč), where their interest is shown in Figure 3. The pie graphs in the figure indicate that while students desire more play-testing sessions at our university, a high number of students would prefer play-testing sessions on their campus without the need to commute to the Brno University of Technology.

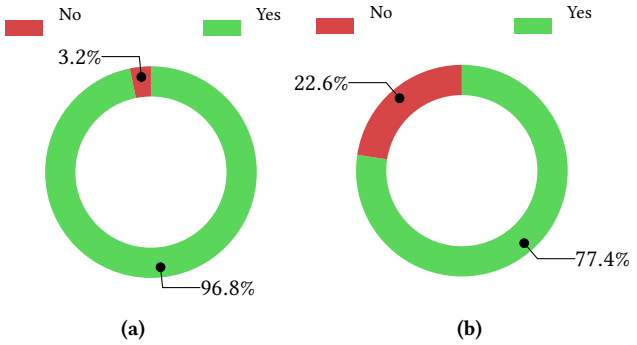

Figure 3: Would you be interested in taking part in further testing at (a) Secondary Technical School in Třebíč / (b) Brno University of Technology in the future?

Another feedback we received with the same amount of responses indicates high overall satisfaction with the scenarios, in particular, we obtained median scores (1 – lowest, 10 – highest):

- testing in 05/2022 (CTF05) – 9.0,
- testing in 06/2022 (CTF05) – 9.0,
- testing in 12/2022 (CTF05) – 9.0,
- testing in 03/2023 (CTF04) – 9.5.

These results show that the scenarios were well-received by the participants and that they found them enjoyable and engaging.

As part of the data collection for the 02–04/2023 CTF playing events, we evaluated the preliminary post-survey results of 30 students for CTF03 and 18 students for CTF02, and preliminary pre-post-survey results of 28 students for CTF03 and 7 students for CTF02. Survey participants are presented in more detail in Sections 4.1.1 and 4.1.2. The collected data are processed according to Post-survey feedback (see Subsection 5.1) and Pre-post CTF analysis (see Subsection 5.2).

5.1 Post-survey feedback

Overall satisfaction was high for both scenarios (Figure 4). For CTF03, 20 students (67%) were very or extremely satisfied. For CTF02, 12 students (67%) were very or extremely satisfied.

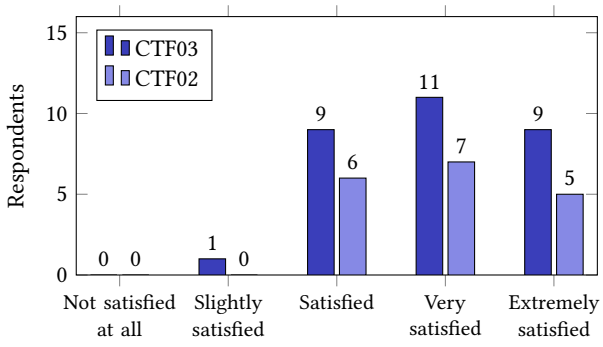

Figure 4: Overall satisfaction from experiences of the CTFs

Overall meaningfulness for learning was also high (Figure 5). For CTF03, 17 students (57%) rated the scenario as very or extremely meaningful for learning. For CTF02, 13 students (72%) rated the scenario as very or extremely meaningful for learning.

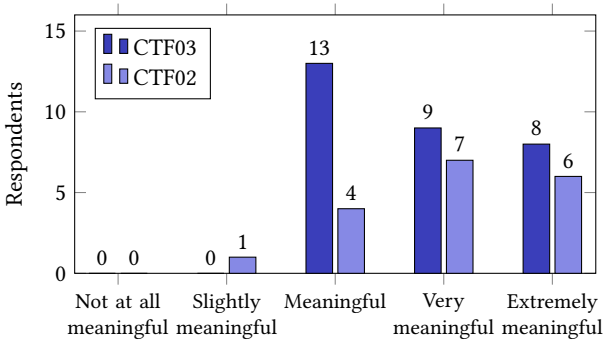

Figure 5: Overall meaningfulness for learning when played the CTF scenarios

Students also estimated how their interest in learning cybersecurity topics, in general, changed due to the scenarios (Figure 6). For CTF03, 13 students (43%) reported a slight increase, and 14 students (47%) a lot of increase in interest in learning cybersecurity topics in general. For CTF02, 11 students (61%) reported a slight increase, and 5 students (28%) a lot of increase in interest in learning cybersecurity topics in general.

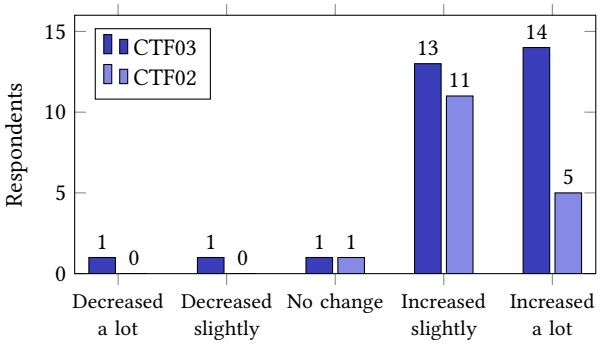

Figure 6: Overall interest in learning cybersecurity topics changed due to the CTF scenarios

5.2 Pre-post CTF analysis

In pre-post analysis, we evaluated whether there were changes after playing CTFs in measured variables. We measured the same variables with the same group of students before and after playing the CTF. As the collected data had non-normally distributed differences in pre-post scores, a Wilcoxon signed ranks test was conducted to evaluate whether students' CTF-related knowledge, CTF-related skills, CTF skill-related self-efficacy, and interest towards CTF topics had changed after playing the CTF. In addition, we evaluated whether students' cybersecurity-specific self-efficacy and cybersecurity attitude had changed after playing the CTF scenario. We also evaluated whether their interest in further study of cybersecurity, cybersecurity career at some company, or cybersecurity research career had changed after playing the CTF scenario.

5.2.1 CTF03. A total of 28 students participated in both pre- and post-surveys. The mean ranks for higher pre-score vs. higher post-score were as follows: 2.50/13.44 for knowledge, 9.00/12.65 for skills, 10.00/11.65 for CTF skill-related self-efficacy, and 8.71/10.00 for interest in CTF topics. The results indicate a statistically significant increase in rank for knowledge ($z = -4.344$, $p < .001$), skills ($z = -4.068$, $p < .001$), and CTF skill-related self-efficacy ($z = -3.751$, $p < .001$). For interest in CTF topics, the increase was not statistically significant ($z = -1.161$, $p = .269$). Mean ranks for higher pre-score vs. higher post-score were 7.00/6.33 for cybersecurity-specific self-efficacy, 11.30/8.81 for cybersecurity attitude, 7.00/7.00 for interest in further studying cybersecurity, 5.33/6.80 for cybersecurity career interest, and 3.33/4.50 for cybersecurity research career interest. However, none of these changes were statistically significant.

5.2.2 CTF02. A total of 7 students participated in both pre- and post-surveys. The mean ranks for higher pre-score vs. higher post-score were 0.00/3.50 for knowledge, 0.00/3.50 for skills, 0.00/3.00 for CTF skill-related self-efficacy, and 3.25/2.00 for interest in CTF topics. The results indicate a statistically significant increase in knowledge ($z = -2.251$, $p = .024$), skills ($z = -2.271$, $p = .023$), and CTF skill-related self-efficacy ($z = -2.032$, $p = .042$). For interest in CTF topics, the decrease was not statistically significant ($z = -1.518$, $p = .129$). Mean ranks for higher pre-score vs. higher post-score were 0.00/1.50 for cybersecurity-specific self-efficacy, 0.00/2.00 for cybersecurity attitude, 0.00/1.00 for interest in further studying cybersecurity, 2.75/3.17 for cybersecurity career interest, and 3.00/1.50 for cybersecurity research career interest. However, none of these changes were statistically significant.

6 CONCLUSIONS AND FUTURE WORK

Based on the presented preliminary results, gamified CTFs appear to be an effective way to increase students' knowledge, skills, and self-efficacy for skills related to cybersecurity topics that CTF consists of. Post-surveys suggest that CTFs also raise general interest in learning cybersecurity topics. However, a statistically significant increase in CTF topic interest was not observed. Pre-post measurements also show an increase and also decrease in other measured variable medians, however, these were not statistically significant and could just represent the uncertainty of the measurement method with small sample sizes. Therefore, more measurements are needed to confirm these preliminary results. In addition, measurements with randomly selected students should be conducted to check whether the results can be generalized.

The research findings indicate that the surveys collected prior to December 2022 and in March 2023 were not comprehensive enough to draw consistent conclusions. In contrast to Tampere University's approach, Czech high schools and Brno University of Technology did not have actual pre- and post-surveys in place, and our study design only allowed for the collection of feedback on the satisfaction and difficulty levels of each task within the CTF scenario. As a result, we were only able to fully assess the differences in the overall interest in learning through CTFs between different education levels, which were consistently high across all testing sessions. Comparing the data from Czech secondary schools, Brno University of Technology, and Tampere University, it is evident that the interest in cybersecurity education is high across both educational levels. In the future, we plan to extend the pre-post surveys to Czech high schools and Brno University of Technology. We also plan to extend the research to Finnish high schools. This would allow us to compare effectiveness in different education levels and also in different countries.

After conducting all presented tests with students, we have confirmed the necessity of utilizing our solution across various levels of education. Based on feedback received from students, several suggestions emerged to enhance the BUTCA interactive environment and improve the user interface (UI) and user experience (UX). These planned changes are intended to address the issues raised by students and make the platform more intuitive, user-friendly, and efficient. By implementing these suggestions, we hope to create a more engaging and enjoyable experience for students. In addition, we are exploring ways to expand the platform's services for improved data collection, particularly for research purposes.

ACKNOWLEDGMENTS

The research described in this paper was financially supported by the Ministry of the Interior of the Czech Republic, Security Research Programme (BV III / 1 VS), project No. VI20192022132.

REFERENCES

[1] Prometheus Authors. [n. d.]. Prometheus Introduction – Overview. Retrieved June 21, 2023 from https://prometheus.io/docs/introduction/overview
[2] Borka Jerman Blažič. 2021. The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. *Technology in Society* 67 (2021), 101769. https://doi.org/10.1016/j.techsoc.2021.101769
[3] Hack The Box. [n. d.]. Level Up Your Hacking Skills. Retrieved March 20, 2023 from https://www.hackthebox.com/hacker/hacking-labs
[4] BTLO. [n. d.]. Blue Team Labs Online. Retrieved March 17, 2023 from https://blueteamlabs.online/
[5] Elasticsearch B.V. [n. d.]. Learn about the Elastic Stack. Retrieved June 21, 2023 from https://www.elastic.co/guide/index.html
[6] Georgia Cyber Innovation & Training Center. [n. d.]. Cyber Range. Retrieved March 25, 2023 from https://www.gacybercenter.org/services/cyber-range/
[7] Tom Chothia and Chris Novakovic. 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)*. USENIX Association, Washington, D.C. https://www.usenix.org/conference/3gse15/summit-program/presentation/chothia
[8] Nabin Chowdhury, Sokratis Katsikas, and Vasileios Gkioulos. 2022. Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security* 113 (2022), 102551. https://doi.org/10.1016/j.cose.2021.102551
[9] Virginia CR. [n. d.]. Courseware. Retrieved March 17, 2023 from https://www.virginiacyberrange.org/courseware?cat=exercise
[10] CR14. [n. d.]. CR14 Ranges. Retrieved March 30, 2023 from https://www.cr14.ee/
[11] CTF365. [n. d.]. Security Training Platform. Retrieved March 17, 2023 from https://ctf365.com/
[12] CTFlearn. [n. d.]. CTF Challenges. Retrieved March 23, 2023 from https://ctflearn.com/challenge/1/browse
[13] Parrot CTFs. [n. d.]. Realistic Capture The Flags & Practical Penetration Testing Labs Featuring Authentic Hacking Situations. Retrieved March 23, 2023 from https://parrot-ctfs.com/
[14] Cyberbit. [n. d.]. Cyber Labs. Retrieved March 25, 2023 from https://www.cyberbit.com/platform/cyber-labs/
[15] CyberDefenders. [n. d.]. Blue Team Training Platform. Retrieved March 25, 2023 from https://cyberdefenders.org/
[16] CybExer. [n. d.]. Cyber Range as a Service – CybExer Technologies. Retrieved March 30, 2023 from https://cybexer.com/solutions/cyber-range-as-a-service/
[17] Cylab.be. [n. d.]. Cyber Defence Lab. Retrieved March 19, 2023 from https://cylab.be
[18] Airbus Defence and Space Cyber. [n. d.]. CyberRange. Retrieved March 25, 2023 from https://www.cyber.airbus.com/cyberrange/
[19] Irina E. Kulikovskaya and Evgeniya N. Mironova. 2022. Factors of Shaping the Image of the Professions of the Future among High School Students. *ARPHA Proceedings* 5 (2022), 975–991. https://doi.org/10.3897/ap.5.e0975

[20] Cori Faklaris, Laura Dabbish, and Jason I Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*. 61–77.

[21] Fluentd. [n. d.]. Fluentd Introduction. Retrieved June 21, 2023 from https://docs.fluentd.org/

[22] OpenInfra Foundation. [n. d.]. Software Overview – What is OpenStack? Retrieved June 21, 2023 from https://www.openstack.org/software

[23] GACWR. [n. d.]. Georgia Cyber Warfare Range. Retrieved March 25, 2023 from https://gacwr.org/

[24] Tommy Gustafsson and Jonas Almroth. 2021. Cyber Range Automation Overview with a Case Study of CRATE. In *Secure IT Systems*, Mikael Asplund and Simin Nadjm-Tehrani (Eds.). Springer International Publishing, Cham, 192–209.

[25] Ahmad Haziq Ashrofie Hanafi, Haikal Rokman, Ahmad Dahaqin Ibrahim, Zul-Azri Ibrahim, Md Nabil Ahmad Zawawi, and Fiza Abdul Rahim. 2021. A CTF-Based Approach in Cyber Security Education for Secondary School Students. *electronic Journal of Computer Science and Information Technology* (2021).

[26] Kazuhiro Hara. 2019. Cyber range CYBERIUM for training security meisters to deal with cyber attacks. *Fujitsu Sci. Tech. J* 55 (2019), 59–63.

[27] Red Hat. [n. d.]. Red Hat Ansible Automation Platform. Retrieved June 21, 2023 from https://www.ansible.com/products/automation-platform

[28] IBM. [n. d.]. IBM Security X-Force Cyber Range. Retrieved March 25, 2023 from https://www.ibm.com/services/security-operations-center

[29] JYVSECTEC. [n. d.]. Secure exercise environment. Retrieved March 20, 2023 from https://jyvsectec.fi/cyber-range/overview/

[30] John M. Keller. 2010. *Motivational Design for Learning and Performance*. Springer US, Boston, MA. https://doi.org/10.1007/978-1-4419-1250-3

[31] Botagoz Khamzina, Nabuova Roza, Gulsara Zhussupbekova, Karlygash Shaizhanova, Aiganym Aten, and Baikulova Aigerim Meirkhanovna. 2022. Determination of Cyber Security Issues and Awareness Training for University Students. *International journal of emerging technologies in learning* 17, 18 (2022), 177–190.

[32] Mazaher Kianpour, Stewart Kowalski, Erjon Zoto, Christopher Frantz, and Harald Øverby. 2019. Designing Serious Games for Cyber Ranges: A Socio-technical Approach. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 85–93. https://doi.org/10.1109/EuroSPW.2019.00016

[33] Grafana labs. [n. d.]. Introduction to Grafana. Retrieved June 21, 2023 from https://grafana.com/docs/grafana/latest/introduction

[34] Virtual Hacking Labs. [n. d.]. Penetration testing course. Retrieved March 23, 2023 from https://www.virtualhackinglabs.com/pro-lab

[35] Maria Leitner, Maximilian Frank, Wolfgang Hotwagner, Gregor Langner, Oliver Maurhart, Timea Pahi, Lenhard Reuter, Florian Skopik, Paul Smith, and Manuel Warum. 2021. AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research. In *Proceedings of the European Interdisciplinary Cybersecurity Conference*. Association for Computing Machinery, New York, NY, USA, Article 2, 6 pages. https://doi.org/10.1145/3424954.3424959

[36] Kees Leune and Salvatore J. Petrilli. 2017. Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. In *Proceedings of the 18th Annual Conference on Information Technology Education*. Association for Computing Machinery, New York, NY, USA, 47–52. https://doi.org/10.1145/3125659.3125686

[37] Chengcheng Li and Rucha Kulkarni. 2016. Survey of Cybersecurity Education through Gamification. In *2016 ASEE Annual Conference & Exposition*. ASEE Conferences, New Orleans, Louisiana. https://doi.org/10.18260/p.25981 https://peer.asee.org/25981.

[38] Nicole Loorbach, Oscar Peters, Joyce Karreman, and Michaël Steehouder. 2015. Validation of the Instructional Materials Motivation Survey (IMMS) in a Self-Directed Instructional Setting Aimed at Working with Technology: Validation of the IMMS. *Br J Educ Technol* 46, 1 (Jan. 2015), 204–218. https://doi.org/10.1111/bjet.12138

[39] Root Me. [n. d.]. Root Me: Hacking and Information Security learning platform. Retrieved March 25, 2023 from https://www.root-me.org/?lang=en

[40] NUARI. [n. d.]. Cyber Security Live Exercises. Retrieved March 20, 2023 from https://nuari.org/decide

[41] University of West Florida. [n. d.]. Center for Cybersecurity. Retrieved March 17, 2023 from https://uwf.edu/centers/center-for-cybersecurity/

[42] PentesterLab. [n. d.]. PentesterLab: Our exercises. Retrieved March 23, 2023 from https://pentesterlab.com/exercises

[43] PortSwigger. [n. d.]. Web Security Academy. Retrieved March 23, 2023 from https://portswigger.net/web-security

[44] Ishaani Priyadarshini. 2018. *Features and architecture of the modern cyber range: a qualitative analysis and survey*. University of Delaware.

[45] PwC. [n. d.]. Cyber Resilienc. Retrieved March 25, 2023 from https://www.pwc.com/cz/en/sluzby/cyberandprivacy/cyber-resilience.html

[46] Cloud Range. [n. d.]. Cyber Range Simulation Solutions. Retrieved March 17, 2023 from https://www.cloudrangecyber.com

[47] RangeForce. [n. d.]. Free Cybersecurity Training from RangeForce. Retrieved March 30, 2023 from https://www.rangeforce.com/cyber-skills-training

[48] CYBER RANGES. [n. d.]. Scenarios. Retrieved March 19, 2023 from https://www.cyberranges.com/cyber-range-security-training

[49] RingZer0. [n. d.]. Challenges. Retrieved March 23, 2023 from https://ringzer0ctf.com/challenges

[50] Tomas Stodulka and Radek Fujdiak. 2022. *Building the Cyber Range platform with cloud computing technology*. Brno University of Technology, Brno, Czechia.

[51] TryHackMe. [n. d.]. Hacktivities. Retrieved March 17, 2023 from https://tryhackme.com/hacktivities

[52] VuCSA. [n. d.]. Vulnerable Client-Server Application. Retrieved March 23, 2023 from https://vucsa.warxim.com

[53] Jan Vykopal, Pavel Čeleda, Pavel Seda, Valdemar Švábenský, and Daniel Tovarňák. 2021. Scalable Learning Environments for Teaching Cybersecurity Hands-on. In *2021 IEEE Frontiers in Education Conference (FIE)*. 1–9. https://doi.org/10.1109/FIE49875.2021.9637180

[54] Jian Ming Colin Wee, Masooda Bashir, and Nasir Memon. 2016. Self-Efficacy in Cybersecurity Tasks and Its Relationship with Cybersecurity Competition and Work-related Outcomes. In *2016 USENIX Workshop on Advances in Security Education*. 8.

[55] Shaya Wolf, Andrea Carneal Burrows, Mike Borowczak, Mason Johnson, Rafer Cooley, and Kyle Mogenson. 2020. Integrated outreach: Increasing engagement in computer science and cybersecurity. *Education sciences* 10, 12 (2020), 1–23.

[56] Muhammad Mudassar Yamin, Basel Katt, and Vasileios Gkioulos. 2020. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security* 88 (2020), 101636. https://doi.org/10.1016/j.cose.2019.101636