Multi-Level Approach to Cybersecurity Education

1st Willi Lazarov  
Department of Telecommunications  
FEEC, Brno University of Technology  
Brno, Czechia  
lazarov@vut.cz

2nd Tomas Stodulka  
Department of Telecommunications  
FEEC, Brno University of Technology  
Brno, Czechia  
xstodu07@vut.cz

Abstract—This paper addresses challenges in building a cyber range platform and presents the design, implementation, and testing of a software platform for cybersecurity education, which scope ranges from technical universities to high schools. Our contribution is a multi-level approach to cybersecurity education, which is applied through extensive testing with students from two different technical universities and high schools.

Index Terms—BUTCA, Capture the Flag, Cyber Arena, cyber range, cybersecurity, education, testing, training

I. INTRODUCTION

From the cybersecurity perspective, information and communication technologies are facing numerous types of threats, including malware, password attacks, denial of service (DoS), spam, injection attacks, and many others. These threats have been rapidly increasing recently and are expected to continue to grow at the same or even higher rates. No one is 100% immune to cyberattacks, from government organizations to smaller family-owned businesses or ordinary internet users. Therefore, it is crucial to educate both the public and experts so that they can identify potential attacks, prepare for their consequences, and generally know how to mitigate these security threats. These requirements can be fulfilled by a cyber range (CR) [1], [2] – the platform responsible for the complete preparation of simulated scenarios where users are exposed to different challenges. Cyber ranges are innovative solutions designed to prepare security environments for effective user training against today’s cybercrimes. They can replicate thousands of scenarios for beginners and professionals alike, and offer a great opportunity in the academic sector to test theoretical information in practice.

One of the main challenges in building a cyber range is the complexity of the process. A cyber range typically involves a simulated network environment with various virtual machines, servers, and other components that are designed to emulate real-world cybersecurity scenarios. Designing and building such an environment can be a time-consuming, expensive, and technically challenging task, requiring expertise in areas such as networking, virtualization, development, and security. Additionally, maintaining and updating a cyber range can be an ongoing challenge, as new cyber threats and vulnerabilities emerge and need to be incorporated into the training scenarios. As a result, many organizations may struggle to build and maintain their cyber ranges, leading to a lack of effective cybersecurity training and educational resources [3].

A particular challenge in building a cyber range platform is providing an effective interface for administrators to control the whole platform and on the other side guide users through the prepared scenarios. This paper addresses these challenges and introduces the reader to the Brno University of Technology Cyber Arena (BUTCA) administration interface. The main function of this application is to provide administrators with an easy-to-use environment for controlling scenario creation and restoration to their original state, user management, and basic connectivity to the OpenStack virtualization platform through instances that are created when the user launches the selected scenario. Additionally, the application allows administrators to monitor and track the total cloud resources available at BUTCA. All of these functions are managed from a central application without the need to connect to other tools.

II. RELATED WORK

Currently, several analyses are available that compare the various properties and functions of different types of CRs. In literature, at least 6 quality publications have been found that address this topic in the time span between 2013 and 2021. Most of the publications are focused on general CR types [4], [5]. Papers by Holm [6] and Kucek [7] are particularly focused on CRs with the ICS (Industrial Control System) and CTF (Capture the Flag) support. The most detailed article by Chouliaras [8] presents a review of CRs and, in addition to an analysis of the available literature, includes structured interviews with agencies and academic institutions that directly own and develop their CR. Chouliaras’s article generally provides a comprehensive analysis of approximately 25 CRs and the description of 10 platforms is further expanded to include supported features and tools used. Although the number of CRs examined is the smallest compared to other research, the treatment is the most comprehensive of all. On the other hand, Yamin’s research [1] examined the largest number of CRs (about 100), but the analysis only compared the basic features of the platforms.

The features relevant to the BUTCA platform presented in this paper are the custom administration software and the type of environment built by the CR. Table I provides a summary of basic information about CR platforms, including BUTCA (last row). The overview is based on [2] and has been extended by [8]–[28]. A total of 8 CRs were excluded from the overview due to the unavailability of information.
The comparison above shows that most cyber ranges use proprietary software for administration and their environment is emulation-based. We have expanded our focus to include HCP and are the only ones listed to cover the industrial sector.

### III. PROPOSED SOLUTION

The proposed platform was created as part of an applied research project (V120192022132), whose main goal was to develop a platform for research, testing, and education in cybersecurity. In terms of education, our primary focus was to support teaching for our Information Security study program, but we also extended our scope to high schools.

Users primarily log in to the application using a Microsoft account. There is also an option to register a new account using any email address, such as for invited guests who do not have a university account. All users are further divided into groups, typically by study courses or organization, to determine which game scenarios are available to them.

All scenarios have a maximum number of players and can also be limited by time. If an administrator starts a scenario (it is disabled by default), a user can only join if there is an available slot and can only run one scenario instance until they finish or run out of time. Players complete individual tasks and take a final test to verify their knowledge. Once the test is completed, the player’s current ranking is displayed along with their total score. Players can also view a scoreboard and table of other players in the scenario during and after the game. Additionally, the administrator can remove a user instance at any time, view a log of incorrect answers for a given scenario, or view the scoreboard of all users’ scores.

### A. High-Level Architecture

The BUTCA platform consists of 3 components: application server, database, and Ansible AWX. All of these components run in a virtual machine (VM) on top of the main part, which is the OpenStack cloud computing platform. The deployment and communication flow of all components are illustrated in Figure 1. Communication between the client’s web browser and the application server is based on the Model-View-Controller (MVC) architectural pattern.

![Fig. 1: High-level diagram of key components](image)

### B. Implemented Platform

We host all components of the BUTCA platform ourselves, including the web application for users and administrators, logging and monitoring, and the educational scenarios that we have created. One of the key advantages of our solution is the easy creation of scenarios and their gamification (story with prologue and epilogue, competitions, etc.). Our goal was to simplify the entire process for all users, so we developed a unified interface that allows administrators to manage all scenarios from a single application. Each game instance for connected users is composed of several tasks in a predefined linear scenario. Each task has a specific assignment that is either educational (more instructional) or part of the gamification story (more challenging). Tasks contain hints, the use of which may be penalized by the loss of points for the given task, and the last hint reveals the correct answer, but with a loss of 100% points. Furthermore, additional resources can be attached to the task, such as PDF files, multimedia files, ZIP archives, etc. The primary objective of each task is to find the flag, which represents the correct answer, similar to classic CTF (Capture the Flag) games. The user interface components described above are shown in Figure 2.

1The automation of complex processes is handled by the Virtualization Stack project in Ansible AWX, which is an open-source automation task engine with API (Application Programming Interface) developed by Red Hat.
IV. Testing and Evaluation

In total, the following 6 playtests with students were organized from Dec. 2021 to Dec. 2022:

1) 47 students, FEEC Brno University of Technology.
2) 10 students, Secondary Technical School in Třebíč.
4) 60 students, FEEC Brno University of Technology.
5) 42 students, Secondary Technical School in Třebíč.
6) 29 students, Tampere University (TAU).

During all playtests, logging and monitoring were conducted to track the following: incorrect answers, hints used, time taken to complete each task and scenario, final test points, overall scores of students, and feedback provided.

Based on the testing results, the difficulty was appropriately set and did not require any modifications in the future. Most of the students completed the tasks with at least one hint. However, one task needed a correction in the correct answer, which was a Base64 decoded string. According to the recorded incorrect answers, most of the students entered the correct result but in the wrong format, such as using lowercase instead of uppercase or subtracting spaces. The reason for these errors was that the students used different decoding tools, and some of them decoded the string differently than its original version. Therefore, the encoded string was modified to a single word consisting of only numbers and a special character to avoid such variations when using different tools.

Furthermore, we have established research cooperation with Tampere University to collect feedback based on the Attention, Relevance, Confidence, Satisfaction (ARCS) model [29]. For a better perspective of the collected feedback, we use the Reduced Instructional Materials Motivation Survey (RIMMS) version of the Keller’s original survey, validated by [30], in which we have modified the survey items to fit our context. In the post-survey, students also assess 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 assess how their general interest in cybersecurity changed due to these tasks and properties, which provides valuable feedback for teachers.

Surveys conducted during the playtesting with educational institutions investigate the interest in the BUTCA platform and cybersecurity in general, as well as the difficulty and quality of each task customized for particular scenarios. As an example, one result from a survey completed by 31 students from Secondary Technical School in Třebíč is shown in Figure 3. Charts in the figure indicate that students would welcome more playing sessions at the BUTCA, and a higher number of students would be satisfied if the playing sessions could take place on their campus without the need to commute to the Brno University of Technology.

In the future, we plan to include Czech students in research with Tampere University that focuses more on evaluating the effectiveness of cybersecurity education using cyber ranges in comparison to conventional teaching and learning, such as common lab tasks using VirtualBox or VMware.
V. RESULTS AND DISCUSSION

From a technical point of view, our solution has passed all the tests successfully. However, there were some issues related to the user interface (UI) and user experience (UX) based on feedback from the involved students. Specifically, these include the organization of the help section, multi-level user access to the platform, and more detailed description of scenarios in the main menu. We will take all of these suggestions into account in the future development and focus on improving the UI and UX of the BUTCA.

Although the originally proposed solution was focused on supporting cybersecurity teaching at FEEC BUT, the idea of expanding educational scenarios to high schools arose during the platform development. Additionally, the user interface of BUTCA has been translated into English, opening up potential international collaborations, such as the current collaboration with the Tampere University. With increasing interest from other universities and high schools, we plan to redesign the current architecture of BUTCA to meet the CRaaS (Cyber Range as a Service) model, enabling students to play CTF scenarios directly from their university or high school. Our multi-level approach to cybersecurity education does not require any significant technical changes, and its implementation involves only creating scenarios with appropriate difficulty levels for the targeted level of study.

Based on the results achieved, new questions and suggestions for improving the current state of our solution have arisen. Future research and development will require further testing. By expanding the target group to include high schools, we can carry out testing with more subjects. In addition, establishing long-term cooperation with the Tampere University can help to continuously improve BUTCA, obtain more feedback, and collect research data.

ACKNOWLEDGMENT

We would like to express our gratitude to the Tampere University for their cooperation in organizing the playtesting sessions of the educational scenarios and for given feedback, namely to Tiina Schafeitäl-Tähtinen and Marko Helenius from the NISEC research group.

REFERENCES