Analytical review of interactive technologies for teaching cybersecurity skills

Svitlana Klymenko[1,*,†], Vitaliy Konko[1,†], Oleksii Klymenko[1,†], Volodymyr Hnatushenko[2,†] and Marina Bychkova[1,†]

[1] *Oles Honchar Dnipro National University, Gagarin Ave., 72, Dnipro, 49000, Ukraine*
[2] *Dnipro University of Technology, Dmytra Yavornytskoho Ave., 19, Dnipro, 49005, Ukraine*

Abstract

The article discusses issues related to the development of educational platforms, the main feature of which is the use of an interactive sandbox, on the basis of which the features of information technology, computer engineering and cybersecurity are studied. An analysis of existing educational platforms and CTF platforms was carried out. Based on the analysis, the disadvantages and advantages of existing platforms were identified and the tasks of developing a more modern interactive platform for teaching and researching problems in the field of cybersecurity were identified. The distinctive features of the new platform are presented, which will be useful to those who research cybersecurity methodology in order to develop preventive systems in the information technology industry to minimize damage to business.

Keywords

cybersecurity, education, platform, information technology, computer engineering

1. Introduction

Modern information technology growth invokes world changing. Today's business is directly connected with digital activity and virtual world incidents affect real-life activities. While computer usage gives us a lot of advantages, it also requires great responsibility, otherwise, it can lead to a high damage for companies.

Some threats can be avoided or their effect can be minimized as they are well-known. A denial-of-service attack can be a bright example. This is a powerful attacking method, but there are technologies that can handle that by analyzing a network traffic to stop DDoS before the start.

There is no absolutely safe information system, and the reason for that is not only the complexity of such systems, but also the improvement of modern information technologies, the rapid growth in the emergence of new hardware and software. This process requires new approaches to protect systems from modern attacks. To counter new types of threats, in most cases, it takes time to study and build new methods of protection against such threats. Such questions are the tasks of "ethical" hacking. While white-hat hackers use existing systems testing techniques, they do not fully cover all possible weak points however.

In order to study new hacking and threats prevention methods, there is a need to create some kind of platform for studying modern types of attacks. The platform for the safe study of various attacking types will give students more opportunities to understand existing threats and further

CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
Klymenko@ftf.dnu.edu.ua (S. Klymenko); konko@365.dnu.edu.ua (V. Konko); o.klymenko@ftf.dnu.edu.ua (O. Klymenko); vvgnat@ukr.net (V. Hnatushenko); bychkova@ftf.dnu.edu.ua (M. Bychkova)
0000-0003-2005-9993 (S. Klymenko); 0009-0006-9713-9712 (V. Konko); 0009-0009-5164-1688 (O. Klymenko); 0000-0003-3140-3788 (V. Hnatushenko); 0009-0000-0316-5968 (M. Bychkova)

study to fight against them. Thus, creating a sandbox platform is the only solution for such a problem, so that surveillance is absolutely safe.

2. Existing solutions

We will analyze existing solutions and some issues related to training and acquiring skills in cybersecurity tasks. Solutions will be classified in the following areas: modern information technology training platforms, interactive sandboxes in systems for training and obtaining cybersecurity skills, and also consider modern analytics systems (Figure 1).

CISCO Networking Academy [1] is a cybersecurity, networking and programming educational platform, owned by CISCO, US transnational company. The platform provides networking, cybersecurity, IoT, programming, infrastructure and automation and other IT-related certificated courses. Each course is interactive and theory is perfectly combined with practice.

For students, there are opportunities to get knowledge in the IT and networking industry, while for teachers it is a great study material that can be used in their job. Certificated students have an advantage during employment as companies can hire the best students.

This is a learning platform with both free and paid options.

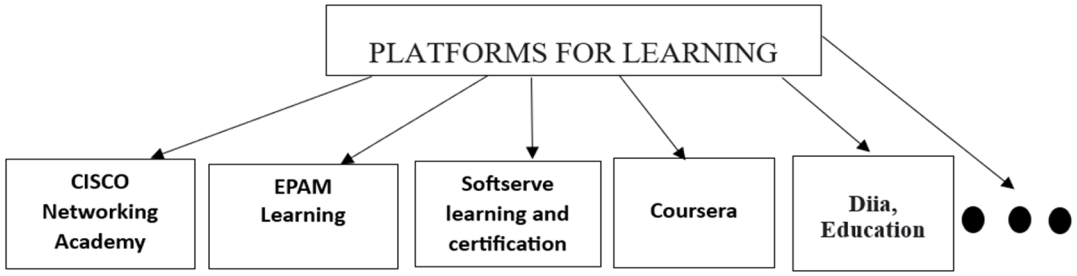

Figure 1: Classification of learning platforms.

EPAM Learning [2] promotes the accumulated company's working experience in the IT field to everyone. They have university programs in a wide range of qualifications, such as Java, .NET and JavaScript development, automated testing, development and operations, embedded systems, business analysis and more. EPAM is a Ukrainian IT company, focused on media business, finance services, medicine and other fields [3].

SoftServe learning and certification is a Ukrainian IT-company engaged in software development and consulting [4]. Company has its own learning platform with a large number of courses in development, project management, business and technology [5].

Coursera is a huge online-courses provider founded in the United States. Similar to CISCO's Networking Academy, there are options for students, companies and teachers [6].

In the cybersecurity course, we will analyze the psychology and techniques of online fraudsters, the nature of fakes and viruses, and understand how to counteract them effectively.

Diia, Education [7] is the most popular and accessible training platform for the basics of information hygiene. The educational series was created on the initiative of the Ministry of Digital Transformation for the Diia.Education platform with the support of the USAID Project "Cybersecurity of Critically Important Infrastructure of Ukraine" and was developed by experts of the Kyiv-Mohyla Academy.

There are more and more distance learning platforms every year: Skillbox, Skillfactory, ProductStar, GeekBrains, OTUS and others. Of course, not all learning platforms are listed, but only the most commonly used platforms for learning in higher education institutions.

Let's take a look at existing sandboxes to control the operation of various programs and increase the level of security, including online ones. Sandbox or playground - is an isolated environment for

running programs to search for errors or vulnerabilities and prevent their further spread. Sandboxing allows you to protect critical network systems by emulating a working environment with a dedicated set of resources and running a suspicious program or code inside it.

Sandbox - IT-Dialog can be used as a tool to detect malware attacks and block them before they reach the network. The system allows IT professionals to inspect the code and understand exactly how it works before it makes its way onto the end device, introducing malware or viruses.

OWASP Juice Shop is a vulnerable web application designed for security education purposes, written in JavaScript. It is literally crammed with problems of varying levels of complexity, designed to be exploited by the user.

PentesterLab is a platform that provides both online and offline labs designed to teach the art of web application pentesting and web security. The site offers a number of free exercises and a PRO subscription package that gives access to over 200 private exercises.

CISCO Packet Tracer is a cross-platform powerful network simulator [7]. It allows users to design and simulate networks, practice with IoT, device configuration and cybersecurity. This software is perfect either for students who learns networking, engineers and researchers. CISCO Network Academy courses have laboratory works that use Packet Tracer to practice.

This tool is free and available for Windows, Linux, Android, iOS and MacOS.

Graphical Network Simulator-3 (GNS3) is a free, open-source software networking simulator first released in 2008 [8]. This tool allows to combine virtual and physical devices to simulate complex networks. CISCO Networking Academy courses can also be done there.

Network Simulator (NetSim) is an advanced network simulator designed for CISCO certification training by US company, Boson [9]. Based on the web platform, this solution is cross-platform. Can be used to design, profile and verify performance of simulated networks. This software is paid, however a free trial is available.

It should also be noted that the most popular introduction into the learning process today is computer games, the so-called gamification. Gamification is a technology for using methods to teach practical skills [10]. The modern generation of young people is interested in computer games from a very early age, and for them the competitive process in learning looks quite natural and interesting. Completing tasks at various levels, from simplest to more complex, solving problems and puzzles, various types of digital rewards - all this makes the learning process interesting and informative. The first network computer online game to date is “CaptureTheFlag” (CTF) [11].

CTF is a competitive game mode in which participants try to capture the “flags” of their opponents and defend their own. In CTF competitions, a flag is usually understood as a digital sequence of arbitrary symbols obtained in the course of solving a problem. The information security CTF has changed over time, and today not all stages of the competition involve capturing and holding the flag. Students of the Oles Honchar Dnipro National University of the Department of Cybersecurity and Computer-Integrated Technologies took part in CTF competitions in Ukraine in 2023. Thanks to participation in such competitions, we were able to identify the strengths and weaknesses of the theoretical training of students in our department. It also made it possible to improve approaches to theoretical training in some disciplines and identify students’ interest in such gaming competitions. Therefore, we can safely talk about the relevance of using gaming platforms in the learning process.

The SOC is a team of primarily security analysts tasked with detecting, analyzing, responding to, preventing, and reporting cybersecurity incidents. The tasks of the SOC:

- Monitor, search and analyze intrusions in real time.
- Prevent cyber threats by being proactive: continuously scan computer networks for vulnerabilities and analyze security incidents.
- Quickly respond to confirmed incidents and eliminate false alarms.
- Generate reports on the state of security, cyber incidents and enemy behavior patterns.

The most time-consuming part of running a SOC is constantly analyzing large volumes of data. The Security Operations Center collects, stores, and analyzes tens to hundreds of millions of security

events daily. Do not forget that all this is controlled by experts: they get involved when you need to decide what to do with a detected threat.

Analysis and research in information systems is the most important task. These skills come with experience, if we consider the most well-known and common vulnerabilities in computer systems and networks. It is necessary to prevent cyber threats prematurely; only then can we talk about security.

If we consider, from the point of view of a higher school graduate, as a future specialist in the field of SOC, then he should:

- Full cycle of processing suspected incidents: answering the customer's questions when analyzing a suspected incident, providing downloads at the customer's request;
- Creating requests to exclude False-Positives (false positives, when the detection system reports the presence of malicious software or an attack, but in fact there is none);
- Processing requests for unavailability of the information system;
- Solving personal tasks assigned by the group leader when working outside of shifts.

Thus, the development of modern interactive technology in which all three basic aspects of learning (theoretical knowledge, gaming components and data analysis) will be presented will give a higher education student a more complete opportunity to delve into cyberspace on the basis of one platform, which in turn will provide better training for cybersecurity specialists.

3. Review of CTF gaming platforms

Let's look at the five most famous CTF platforms: WebGoat and Security Shepherd from OWASP, CTFd, FBCTF, RootTheBox from third parties. The last three CTF platforms in JuiceShop from OWASP are used as a demonstrably vulnerable application. All platforms are open source and available on GitHub.

Table 1
Understanding Platform Development

Platform title	developer	year of release	Interactivity/ ease of configuration/ condition monitoring
WebGoat	Bruce Mayhew, OWASP	2002	No/ No / No
Security Shepherd	Mark Denihan, Sean Duggan, OWASP	2014	No/ No / No
CTFd	KevinChung	2017	No/ Yes / Yes
FBCTF	FaceBook Inc.	2017	No/ Yes / Yes
RootTheBox	Joe D. (Alias: Moloch)	2016	No/ Yes / Yes

Coming back to the described task, the problem consists of three parts. Our solution also has three modules: learning platform, interactive sandbox and analysis tool.

4. Proposal for the development of an interactive learning platform illusion

4.1. Learning platform illusion

This section is required to provide essential study material. Very important to develop course sources in a unified form so they can be represented in different formats according to the user's preferences. Teachers would rather prefer learning material as a book, while students may choose a more interactive format.

By completing these courses users will get new skills in information technology, cybersecurity, IoT, data theory and more related topics. Existing online learning platforms can be a great source of inspiration. Combining theory with practice would be an excellent combination.

User-end of this software can be implemented using a web engine to achieve cross-platform capabilities, or using native user interface for each platform to target execution speed. Course materials will be stored in a database with user-end caching ability to provide offline access.

This module can be used by students during studying in university or college.

4.2. Interactive sandbox of the platform illusion

The most exciting part of the project, a virtual networking container that allows users to develop, test and profile networks and systems. Key features are low-level hardware virtualization and networking technologies.

Implementing this module in the form of computer video games would have maximum effect. If so, users can choose from online and offline playgrounds. Offline playground can be used for personal projects or to master networking and engineering skills, learned in the first section of this software.

Online playground can be hosted both by local and dedicated servers. Local hosting model allows a small group of users to build a virtual network using shared virtual space. Dedicated server usage allows users to connect from around the world.

The sandbox – is a virtual reality with no limits or rules. This is important to give players maximum liberty in their in-game activities. While they can design their own networks and computing systems, they are also able to perform sabotage and other IT threats to other players.

4.3. Analytics system of the platform illusion

All user-related data will be collected for further analysis.

The first module will provide student’s success, learning threads and courses popularity. This data can be used to improve the course’s materials and to grade students.

The second module will provide even more important data. All in-game events and actions will be recorded. These records will include detailed information about virtual network packages, in-game user interactions and other activities. Logged data will be used to increase the non-game world’s cybersecurity and IT infrastructure as a result of analysis.

5. Possible implementation

The platform requires high execution speed to complete given tasks, so the user-end core must be implemented using native code base to achieve best performance.

Virtualization technologies can be redistributed from existing open-source solutions, like q-emu virtualization and Kathara.

Open-source game engines, such as Godot or Defold, can be used to develop a second module. Otherwise, our own graphical engine implementation can be used instead to avoid licensing conflicts and redundant functionality.

Third module's analytics would become impossible during the usage scaling process. To leave this feature possible fog computing will be used. So, personal user data will not be collected directly, instead, post-processed abstract data will be sent for further summary generation. Public API can be developed for this module to provide useful data for third-party services.

Let's consider a number of requirements that an interactive platform must satisfy:

1. Ease of installation: The interactive platform should be easy to install without causing any confusion.
2. Cross-platform: the ability to install on different operating systems.
3. Ease of configuration: the interactive platform should be easily customizable and have a user-friendly interface, a sufficient set of functionality for conducting various types of competitions, training sessions, and research.
4. Status Monitoring: The interactive platform must be able to track activities users and display the results on a special display in real time.
5. Extensibility: the interactive platform should provide the ability to easily change topics for theoretical training, practical tasks, modify them, add new tasks and delete old ones.
6. Interactivity: the possibility of interaction between participants who use the platform, attacking and defending sides during the competition.

Installation methods interactive platform illusion and access to research:

- Placing platforms using host services.
- Local installation. Participation in the competition in the place where it will be held.
- Possibility of holding online competitions in real time.
- Possibility of online training.

It should be noted that today not all platforms support this functionality, which means the question of the relevance of developing an interactive platform illusion is very high.

6. Conclusions

As a result of a comparative analysis of existing interactive platforms, a number of advantages of the CTFd platform can be identified. It has a more friendly interface, is easy to customize, allows you to quickly adapt to new conditions for training or competitions, and also does not require the organizer to have special programming knowledge for management, editing and configuration. In addition, the ability to integrate the platform with the OWASP JuiceShop project allows you to diversify the game-based learning process using real examples of vulnerable web applications.

Game mechanics are fully present, and the most popular type of CTF competition "Jeopardy" is used. The RootTheBox and FaceBookCTF platforms also allow you to interact with the JuiceShop project. Both platforms have excellent elements of a computer game, be it status, incentives and discoveries, rewards, etc. Moreover, they have their own plot that allows you to involve participants in the gameplay. Among the disadvantages of the FaceBookCTF platform, it can be noted that at the moment the developers have placed the project's source code on GitHub in an archive, thereby ending its support from the community.

Among the disadvantages of the RootTheBox platform are difficult interface settings and controls. There is no ready-to-use user database, which makes only the administration mode available. However, in this mode it is not possible to complete tasks. The WebGoat and Security Shepherd platforms are easy to install and run, have a fairly friendly interface, but are difficult to configure, as they require practical web programming skills in Java. The WebGoat platform is closest to the Quiz type of competition, which makes it less attractive from the point of view of work goals.

It should be noted the excellent game mechanics embedded in the Security Shepherd platform. Based on the totality of features, among the available modern platforms, we can highlight the CTFd

platform, which allows you to easily and quickly launch training or a cybersecurity competition in the Jeopardy format, edit, add and change tasks at your discretion, organize team tournaments and test the skills of participants, but there is no opportunity to conduct research.

Therefore, the development of a new interactive platform with the possibility of obtaining a more complete opportunity from teaching to research is relevant.

Acknowledgements

We thank mentors of the Noosphere Engineering School of Dnipro for their help for material support and the opportunity to implement the interactive platform Illusion, as well as conduct research.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] CISCO Networking Academy, 2024. URL: https://netacad.com.
[2] Learning with EPAM, 2024. URL: https://careers.epam.ua/learning.
[3] About EPAM Ukraine, 2024. URL: https://careers.epam.ua/company.
[4] Softserve homepage, 2024. URL: https://www.softserveinc.com/en-us.
[5] Softserve learning and certification – online IT courses, 2024. URL: https://career.softserveinc.com/en-us/learning-and-certification.
[6] Coursera – learn without limits, 2024. URL: https://www.coursera.org/.
[7] Packet Tracer, 2024. URL: https://www.netacad.com/courses/packet-tracer.
[8] The software that empowers network professionals, 2024. URL: https://www.gns3.com/.
[9] NetSim Network Simulator – Most Advanced Network Simulator Designed for CISCO Certification Training, 2024. URL: https://netsim.boson.com/.
[10] D. Berube, Motivate player for better engagement and retention, 2022. URL: https://thinkgamedesign.com/player-retention-engagement.
[11] S. Kucek, M. Leitner, An empirical survey of functions and configurations of open-source capture the flag (CTF) environments, Journal of Network and Computer Applications 151 (2020) 102470. doi: 10.1016/j.jnca.2019.102470.