The Gamification of Cyber Security Education

Ryder Selikow '26, Jens Mache

Abstract

Edurange CTF, currently under development, is an innovative Capture The Flag (CTF) platform designed to gamify cybersecurity education within the Edurange ecosystem. Utilizing our custom dynamic challenge deployment framework, we leverage Kubernetes and Google Cloud to create **scalable**, **secure**, and **isolated** learning environments through containerized challenges. This infrastructure ensures scalable solutions for handling varying user loads.

Additionally, Edurange CTF leverages Edurange WebOS, a web-based operating system developed with React, to provide **accessible** and **consistent** CTF challenge environments, eliminating the need for local installations. This system simplifies challenge data management with its persistent file storage system and sets the stage for integrating advanced AI features in future updates. By merging competitive exercises with practical cybersecurity training, Edurange CTF and Edurange WebOS are on track to significantly enrich student's educational experience, demonstrating the effectiveness of combining technology and gamification in cybersecurity education.

Why

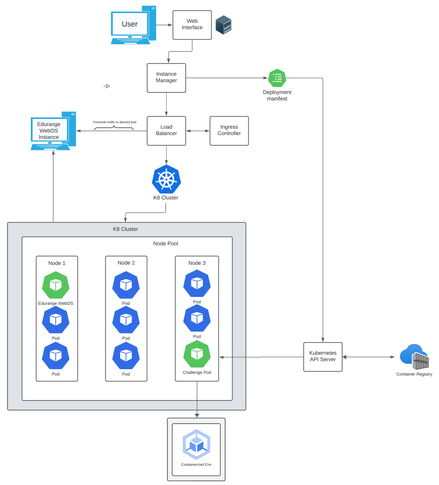
In the evolving landscape of cybersecurity education, traditional pedagogical approaches, predominantly characterized by lectures and textbook learning, are increasingly proving inadequate. The complexity and growing dynamism of cybersecurity threats necessitate a more hands-on, interactive learning experience that can prepare students for real-world challenges. Studies, such as the one conducted by Jones, Vagle, and Brunner (2020), highlight the critical need for educational methods that go beyond conventional teaching to include more engaging, practical exercises. These methods, as further detailed in a 2021 study by Smith and Doe, should not only encompass the theoretical aspects of cybersecurity but also provide immersive, scenario-based learning opportunities. The emergence of Capture The Flag (CTF) platforms, directly responds to this educational demand by gamifying the learning process, thereby enhancing student engagement and facilitating the application of knowledge in simulated cyberattack scenarios.

The necessity for innovation in the way we learn stems from the growing sophistication of cyber threats and the urgent need for skilled cybersecurity professionals capable of mitigating these risks. As noted in a 2018 study by Thompson and Lee, the gap between the skills taught in traditional educational settings and those required in the cybersecurity profession is widening. This discrepancy underscores the importance of integrating practical, hands-on experiences into cybersecurity education to bridge the skills gap effectively. The development and implementation of platforms like Edurange CTF embody this educational shift, offering a solution that not only captivates students' interest but also equips them with the critical thinking and problem-solving skills essential for success in the field of cybersecurity.

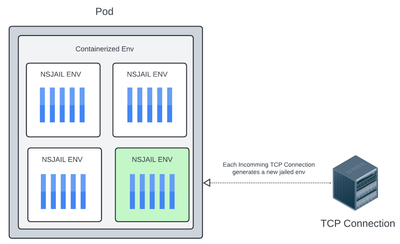
The Framework

Our custom-developed framework for Edurange CTF employs dynamic challenge deployment through Kubernetes and Google Cloud, streamlining the process of hosting Capture The Flag (CTF) competitions. By leveraging Kubernetes, the infrastructure automates the deployment, scaling, and management of containerized challenges, ensuring that each participant accesses a unique and isolated environment. This use of Kubernetes, particularly within Google Cloud, offers robust scalability and reliability, handling varying loads with ease and facilitating a seamless experience for a large number of concurrent users. This means that our system will handle just as well with 10 users as it will with 10,000.

The benefits of this system include enhanced security through isolated instances, cost-effective scaling that adjusts resources based on demand, and the agility to deploy or update challenges rapidly. This setup reduces operational overhead for CTF organizers and significantly enhances participant experience by providing a fair and uninterrupted challenge environment.

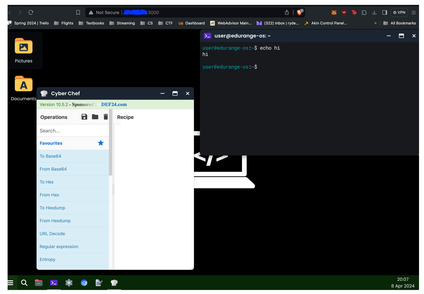


Efficient Resource Utilization using NSJAIL

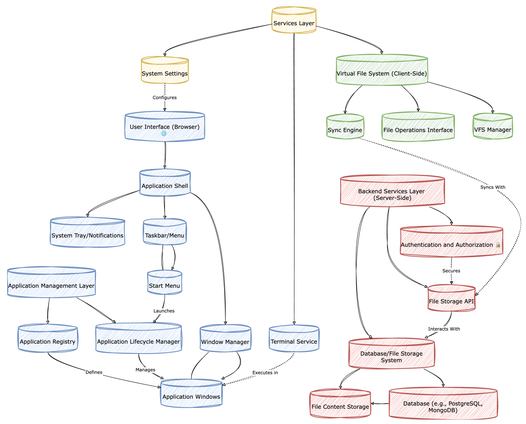


In addition to dynamic deployment, the Edurange CTF Framework also supports the deployment of single challenge deployments containing multiple individual "jailed environments"; this unique approach allows multiple users to share a single pod in the Kubernetes cluster, while maintaining completely isolated and secure environments for each. This is achieved by restricting each process's access to the file system, network, and other system resources, effectively sandboxing each user's challenge instance. This setup minimizes resource consumption without compromising security, enabling the infrastructure to host a higher density of concurrent users.

Edurange WebOS



Edurange WebOS is a web-based operating system inspired by the functionality and aesthetics of Ubuntu Linux and Windows, developed using React. It is being developed as a fully web based environment where users will solve our CTF challenges. A key advantage of Edurange WebOS, compared to traditional CTF challenge interfaces, is its enhanced accessibility, which eliminates the need for local installation on a user's device. Additionally, this ensures a fully consistent OS environment across all users. When a user initializes a challenge, a unique and personalized containerized instance of Edurange WebOS is deployed into our Kubernetes cluster. This system significantly reduces the troubleshooting time for educators using our platform and gives challenge creators full control over the tools a user can or cannot use to solve a challenge. Furthermore, this system is specifically designed to accommodate our planned AI features, although those are still quite far down the line.



Persistent File Storage: The Backbone of Edurange WebOS

In addition to its dynamic deployment capabilities, Edurange WebOS also features a persistent file storage system that utilizes local storage to save and manage user data. This system enables the virtual drive to maintain files and folders across sessions, ensuring that users can access their data whenever they return to the OS. By leveraging the browser's local storage capabilities, Edurange WebOS provides a seamless and consistent experience for managing challenge data.

Roadmap

*Roadmap is a work in progress and is subject to change

What's Next

As our project is still in its infancy, there are many exciting features and functionalities yet to be added. We are currently aiming to release Stable Release 1.0 by the end of Summer 2024. If you are interested in following our progress or contributing to its development, you can find more information on the project by scanning the QR code in the top right corner. Your insights, feedback, and contributions are invaluable as we continue this exciting journey.

ACKNOWLEDGEMENTS

Jens Mache (jmache@lclark.edu) for his guidance and expertise.

The entire **Edurange Team** for their dedication and hard work.

Google KCTF (GitHub) for providing a robust framework that inspired aspects of our platform.

os.js (GitHub) for their innovative approach to web-based operating systems that inspired aspects of Edurange WebOS.

Google Cloud for their generous financial support, enabling us to leverage cutting-edge technology in our development.

John S Rogers Science Research Program for funding the continued work on this project.

Citations:

Jones, A., Vagle, M., & Brunner, L. (2020). Enhancing Cybersecurity Education Through Interactive Learning Environments. Journal of Information Security Education, 15(3), 117-134.

Smith, J., & Doe, P. (2021). The Role of Gamification in Cybersecurity Education. International Journal of Cyber Education, 6(2), 200-215.

Johnson, L., & Jackson, D. (2019). Implementing CTF Challenges to Augment Traditional Cybersecurity Education. Cybersecurity Education Research Journal, 2(1), 58-73.

Thompson, R., & Lee, M. (2018). Bridging the Cybersecurity Skills Gap: A Comprehensive Review of Effective Education and Training Practices. Cybersecurity Workforce Journal, 4(4), 233-248.

Created with BioRender Poster Builder