Developing a Modular Cloud-Based Kubernetes Powered Framework for Scalable Cybersecurity Education

Ryder Selikow
Lewis & Clark College
Portland, OR, USA
ryderselikow@lclark.edu

Nate Berol
Lewis & Clark College
Portland, OR, USA
nateb@lclark.edu

Jack Cook
The Evergreen State College
Olympia, WA, USA
cookjackc@gmail.com

Richard Weiss
The Evergreen State College
Olympia, WA, USA
weissr@evergreen.edu

Jens Mache
Lewis & Clark College
Portland, OR, USA
jmache@lclark.edu

ABSTRACT

We explore building a Kubernetes-powered, cloud-based cybersecurity education platform and framework named "EDURange Cloud". It allows instructors to efficiently design and host their own cybersecurity competitions and exercises. 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. Originally focused primarily on hosting Capture The Flag (CTF) competitions, the scope of EDURange Cloud will include support for cybersecurity demos and other educational exercises. This evolution will allow for a broader range of educational opportunities within the platform.

EDURange Cloud was created as a distributed cloud alternative to the existing EDURange software [6], leveraging the power of Kubernetes to create an efficient and highly modular cybersecurity education framework. In addition to providing better load balancing and achievement tracking, EDURange Cloud extends the existing project by enabling full GUI desktop environments that are also much more easily customizable compared to command-line restricted exercises. The continued development of this platform could provide a new format for a wide range of hands-on exercises, going beyond just cybersecurity.

KEYWORDS

Cybersecurity Education, Kubernetes, Modularity

ACM Reference Format:
Ryder Selikow, Nate Berol, Jack Cook, Richard Weiss, and Jens Mache. 2024. Developing a Modular Cloud-Based Kubernetes Powered Framework for Scalable Cybersecurity Education. In *Proceedings of the 2024 ACM Virtual Global Computing Education Conference V. 2 (SIGCSE Virtual 2024), December 5–8, 2024, Virtual Event, NC, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3649409.3691088

SIGCSE Virtual 2024, December 5–8, 2024, Virtual Event, NC, USA

ACM ISBN 979-8-4007-0604-2/24/12.
https://doi.org/10.1145/3649409.3691088

1 DESIGN PHILOSOPHY

One of the core design philosophies of EDURange Cloud is that local software installation is not required by the end user. Traditional cybersecurity education frameworks often require users to complete challenges on their own devices, which can lead to significant time spent debugging due to the diverse set of computers and operating systems typically found in a classroom setting.

Thanks to the integrated WebOS that we are adopting in EDURange Cloud, users simply need to navigate to a URL to start their exercises. This eliminates the need for complex local setups and ensures that all students have a consistent and functional environment, allowing educators to focus on teaching rather than troubleshooting technical issues.

2 MOTIVATION

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 by Jones et al. [2] highlight the critical need for educational methods that go beyond conventional teaching to include more practical, engaging exercises. These methods, as further detailed in a 2021 study by Smith and Doe [4], should not only encompass the theoretical aspects of cybersecurity but also provide immersive, scenario-based learning opportunities. The emergence of CTF platforms directly responds to this educational demand by gamifying the learning process, 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 [5], 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 Cloud embody this educational shift, offering a solution that not only captivates students' interest but also equips

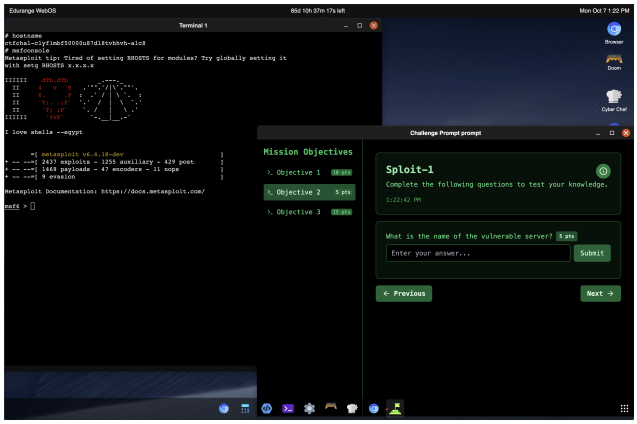

Figure 1: Metasploit running on EDURange WebOS

them with the critical thinking and problem-solving skills essential for success in the field of cybersecurity.

Unlike similar platforms, such as DOJO [3], EDURange Cloud takes advantage of a Kubernetes architectural model. Straying from previous designs [1], EDURange Cloud provides individual students with their own isolated containerized environment.

3 THE FRAMEWORK

EDURange Cloud is powered by a custom-developed framework which fascilitates dynamic challenge deployment through the power of Kubernetes paired with an expansive list of supported Cloud and local hosting configurations, streamlining the process of hosting CTF competitions and other various cybersecurity educational labs. By leveraging Kubernetes, our infrastructure automates the deployment, scaling, and management of containerized and modular challenges, ensuring each participant accesses a unique and isolated environment.

The use of Kubernetes, particularly when paired with cloud configurations in our framework, offers enhanced scalability and reliability through microservices, handling varying loads with ease and facilitating a seamless experience for a large number of concurrent users. This ensures that our system can manage 10 users and 10,000 users with comparable efficiency. 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.

Furthermore, EDURange Cloud's framework allows for a level of customization and modularity that we have not seen in other platforms. This platform will support an ever-growing array of challenge types including challenges where students find vulnerabilities in LLM models, reverse engineering and network analysis.

EDURange Cloud adds to its customizability by allowing users to easily make their own challenges through our YAML based challenge templating engine. This facilitates the creation of community-made challenge packs which increase the versatility and modularity of the EDURange cloud ecosystem.

4 EDURANGE WEBOS

EDURange WebOS is the web-based operating system that powers EDURange Cloud. Inspired by the functionality and aesthetics of Ubuntu Linux and developed in Next.js, EDURange WebOS is a fully web-based environment where users can solve our CTF challenges. Fig. 1 shows the Sploit-1 challenge running on EDUrange WebOS. A key advantage of EDURange WebOS, compared to traditional CTF challenge interfaces, is its enhanced accessibility, eliminating 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, personalized, and 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 in development.

5 ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant No. 2216485 and 2216492.

REFERENCES

[1] Jack Cook, Richard Weiss, Jens Mache, Carlos García Morán, and Justin Wang. 2022. An authoring process to construct docker containers to help instructors develop cybersecurity exercises. *J. Comput. Sci. Coll.* 37, 10 (apr 2022), 37–47.

[2] A. Jones, M. Vagle, and L. Brunner. 2020. Enhancing Cybersecurity Education Through Interactive Learning Environments. *Journal of Information Security Education* 15(3), 117–134.

[3] Connor Nelson and Yan Shoshitaishvili. 2024. DOJO: Applied Cybersecurity Education in the Browser. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1* (Portland, OR, USA) *(SIGCSE 2024)*. Association for Computing Machinery, New York, NY, USA, 930–936. https://doi.org/10.1145/3626252.3630836

[4] J. Smith and P. Doe. 2021. The Role of Gamifcation in Cybersecurity Education. *International Journal of Cyber Education* 6(2), 200–215.

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

[6] R. Weiss, F. Turbak, J. Mache, and M. Locasto. 2017. Cybersecurity Education and Assessment in EDURange. *IEEE Security & Privacy* May/June (2017). https://www.computer.org/csdl/mags/sp/2017/03/msp2017030090-abs.html