Building a Secure, Scalable Capture The Flag Platform for Cybersecurity Education

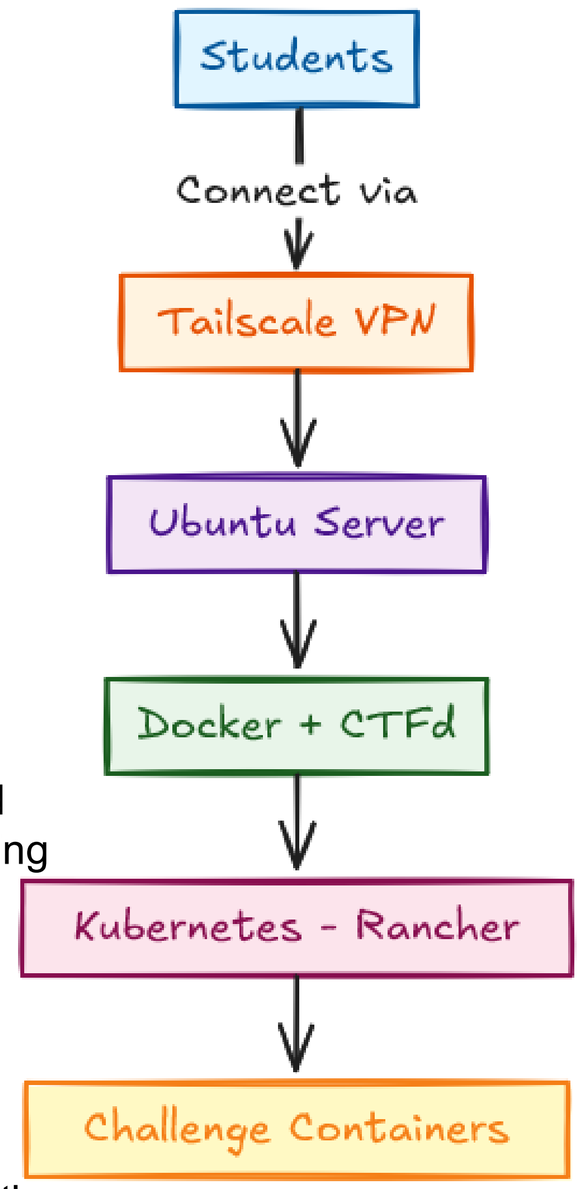
Giovanni Braun
University of Southern Maine

Results

Platform Reliability
The CTF environment operated without major technical issues throughout the event. Containerized services remained stable while supporting multiple simultaneous users.

Secure Access
Tailscale provided controlled, encrypted access to the platform, preventing unauthorized connections while allowing remote participation.

User Engagement
Students actively attempted challenges across all categories, with most completing multiple beginner and intermediate tasks.



Skill Development
Participants demonstrated improved understanding of cryptography, networking, and OSINT techniques through successful challenge completion.

Challenge Difficulty
Reverse engineering tasks were the most difficult, requiring advanced analysis of compiled programs.

Instructional Insight
Results highlight the need for additional instructional support in reverse engineering concepts for future events.

Introduction

Hands-on learning is essential for preparing students for real-world cybersecurity challenges. This project designed a custom Capture The Flag (CTF) environment that allows students to practice technical skills in a realistic and controlled setting. The goal was to create a secure, scalable, and reusable platform that instructors could easily deploy for future training.

Materials and methods

The CTF platform was built using CTFd, containerized with Docker, and orchestrated with Kubernetes via Rancher on an Ubuntu Server host. Secure access was provided through Tailscale to limit exposure to the public internet. Custom challenges were developed across multiple cybersecurity domains, including cryptography, networking, OSINT, password cracking, and reverse engineering.

Conclusions

This project demonstrates that a secure and scalable CTF environment can be built using open-source tools.

The hands-on challenges improved student engagement, technical skills, and problem-solving ability.

Future versions will expand reverse engineering instruction to better support advanced learners.

Literature cited

CTFd. (n.d.). CTFd: Open source capture the flag platform.

Docker, Inc. (n.d.). Docker documentation.

Kubernetes. (n.d.). Kubernetes documentation.

Tailscale. (n.d.). Secure networking for teams.

NIST. (2023). Cybersecurity Workforce Framework (NICE).

Acknowledgments

Special thanks to PATHS students and the University of Southern Maine for supporting this project.

Further information

For more details on this project or access to the deployment guide, please contact:

Giovanni Braun -- University of Southern Maine
Giovanni.Braun@maine.edu