Empowering Cybersecurity Education: Designing a Capture the Flag Platform Using Kubernetes

Thea U. Kjeldsmark[1], Mai S. A. Odgaard[2], Marcus Sebastian E. Holmgaard[2]

[1]University of California, Irvine, [2]IT University of Copenhagen

Motivation

The potential of Capture the Flag (CTF) platforms is often confined by the issue of accessibility and complex setup. Most platforms are either closed-sourced or complicated to configure, which can be frustrating and time-consuming for organizers.

Our project explores the feasibility of designing a CTF platform using a container orchestration tool. We propose *Haaukernetes*, an open-source CTF platform that uses Kubernetes (K8s) to improve the setup and management of users and challenges.

Haaukernetes was built to replace *Haaukins*, an open-source jeopardy-style CTF platform built by Aalborg University. While Haaukins is used for the Danish Cyber Security Championship, its manual container orchestration has led to a complex codebase and setup, making it difficult to distribute, maintain, and expand.

Challenges

- Maintaining high availability.
- Ensuring security both internally and externally.
- Allowing user access via VPN and browser VM.
- Providing easy setup for CTF organizers.

System Architecture and Methods

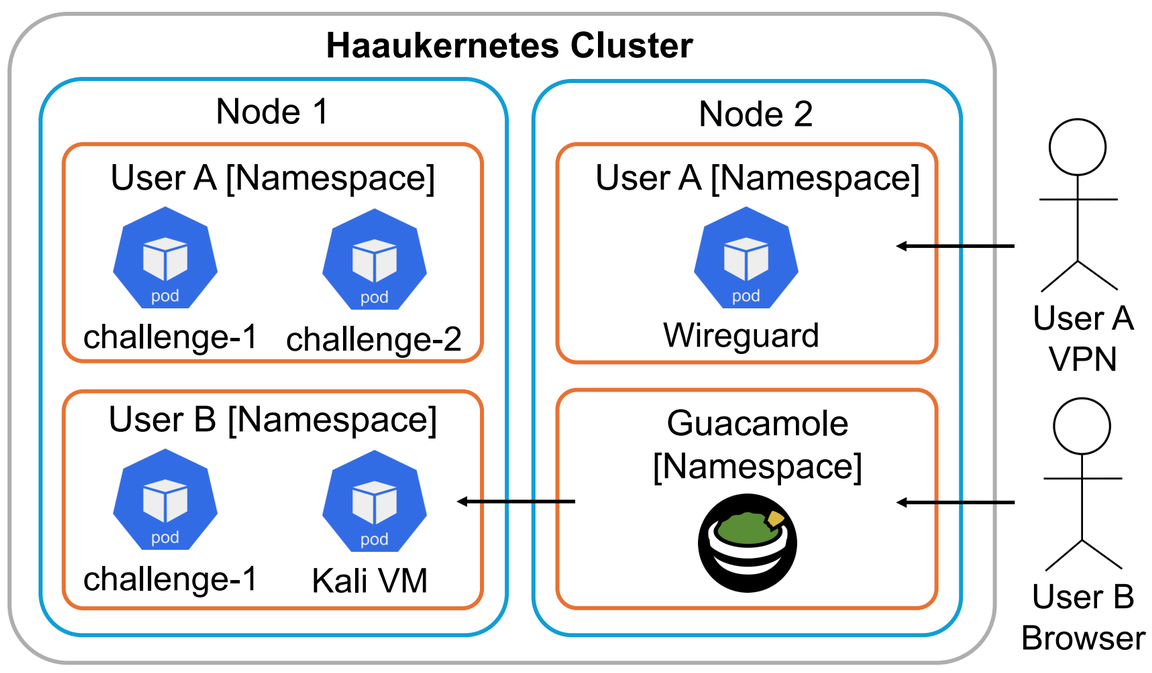

Figure 1: Simplified Haaukernetes cluster setup. Namespaces can span across nodes to take advantage of node resources.

- We first mapped CTF concepts to K8s elements. Users are assigned a namespace containing their CTF resources. Each challenge and connection is placed in separate pods with the relevant Docker containers.
- We developed Haaukernetes using Go, Wireguard for VPN, Apache Guacamole for in-browser Kali VM connections, and Prometheus for monitoring.
- Haaukernetes uses K8s network policies (ingress and egress) to isolate users both from each other and the outside internet.

Results

Benefits of K8s: Using K8s allows us to take advantage of its self-healing property for pods, automatic resource distribution, security options, and network management.

Setup and Distribution: Haaukernetes offers flexible setup via our setup script (creates the cluster from scratch), cloud providers, or ready-made distributions.

Running the CTF: Organizers can limit the number of challenges users can turn on, helping save resources and not hitting the K8s 110 pods per node limit. Users can also switch between the VPN and browser VM access.

Performance: Our performance tests indicate that CPUs and memory scale linearly with users (without challenge interaction), demonstrating the platform's ability to handle increasing user loads efficiently.

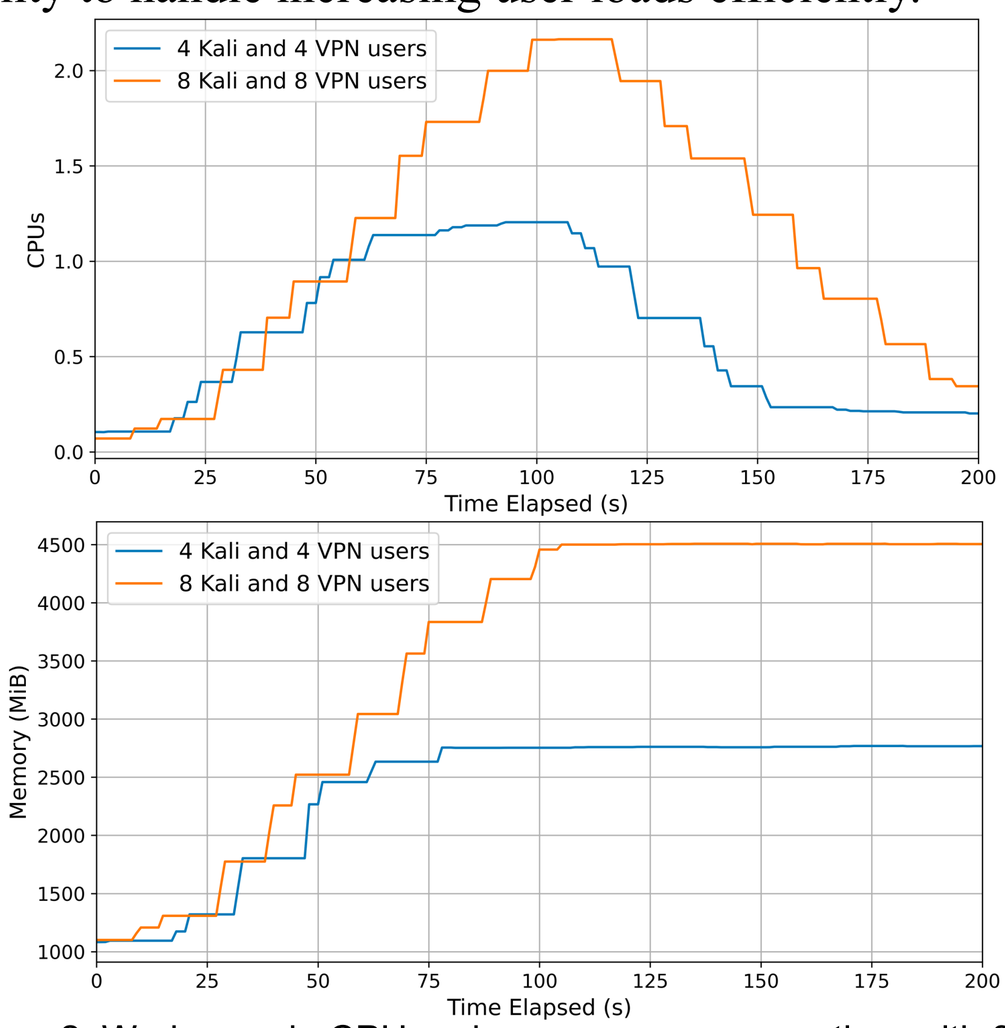

Figure 2: Worker-node CPU and memory usage over time with 8 versus 16 users each with 5 challenges (but no interaction).

Conclusions and Future Work

Haaukernetes is open-source, has flexible setup, and allows both VPN and browser connections, increasing accessibility compared to other CTF platforms.

Compared to Haaukins, using K8s allows us to significantly reduce setup time and code complexity while still handling increasing load, which can empower more organizers to hold CTF events.

The next steps include connecting Haaukernetes to a CTF frontend and carrying out performance tests with user interactions to understand needed resources better.

References

[1] Kubernetes, https://kubernetes.io/ (accessed Mar. 15, 2024).
[2] T. K. Panum, K. Hageman, J. M. Pedersen and R. R. Hansen, "Haaukins: A Highly Accessible and Automated Virtualization Platform for Security Education," 2019.