Abstract

The popularity of cloud deployments for applications has made Kubernetes the largest container orchestration system. Given the many benefits and functionalities it features, its growth is not showing any signs of stopping.

This en masse adoption, however, has put Kubernetes' security flaws on the spotlight, as most of its industrial deployments have suffered from security issues, ranging from architectural vulnerabilities and insecure default configurations native to Kubernetes, to user misconfigurations. As a consequence, multimillion dollar losses and several Gigabytes of sensitive user data were stolen as a result of attacks.

Unfortunately, there is a lack of precise, comprehensive and up to date documentation pertaining to Kubernetes security, compiling risks associated with vulnerabilities, how to exploit them, how to configure a cluster to be as secure as possible and security best practices. This deficit has led to a lack of skills on how to design secure Kubernetes architectures. Furthermore, there are very few open-source monitoring tools, capable of detecting attacks and educating users on attack vectors. The combination of both would help users understand in detail how a secure Kubernetes cluster is constructed, from development to deployment, while allowing them to explore and visualize simulated or real attacks.

This dissertation's aims are twofold. First, to describe in detail the most crucial configuration pitfalls, the best practices to follow and the common attacks that can be conducted against a Kubernetes cluster. Second, to develop a near real time, scalable and fault-tolerant monitoring tool, that serves as a baseline for industrial Kubernetes deployments. This tool features concepts such as Stream processing, fast indexing and representation using Kafka, Elasticsearch and Kibana.

Both of these goals were achieved in this dissertation, nonetheless, there are improvements (TLS implementation, Kafka topic/broker replication or Firewalling), studied in the future work section of this dissertation, that should be made to transform the monitoring tool from a prototype to a fully functional industrial design.