Course Outline

Kubernetes and Container-based Application Security with CKS exam prep

Course Summary

Description

This 2-days long training introduces concepts, procedures, and best practices to harden Kubernetes based systems and container-based applications against security threats. It deals with the main areas of cloud-native security: Kubernetes cluster setup, Kubernetes cluster hardening, hardening the underlying operating system and networks, minimizing microservices vulnerabilities, supply chain security as well as monitoring, logging, and runtime security.

Topics

- User and Authorization Management
- Supply Chain Security
- Validating Cluster Setup and Penetration Testing
- System Hardening
- Monitoring and Logging

Audience

This course is designed for Kubernetes administrators who participated in a Kubernetes administration training or have a Certified Kubernetes Administrator (CKA) certification and want to learn about securing Kubernetes based systems and container-based applications.

Prerequisites

Linux container (e.g., Docker) and Kubernetes administration skills are required for this course.

Duration

Two Days

Course Outline

I. User and Authorization Management
- A. Users and service accounts in Kubernetes
- B. Authenticating users
- C. Managing authorizations with RBAC

II. Supply Chain Security
- A. Vulnerability checking for images
- B. Image validation in Kubernetes
- C. Reducing image footprint
- D. Secure image registries

III. Validating Cluster Setup and Penetration Testing
- A. Use CIS benchmark to review the security configuration of Kubernetes components
- B. Modify the cluster components' configuration to match the CIS
- C. Penetration testing Kubernetes for known vulnerabilities

IV. System Hardening
- A. Use kernel hardening tools
- B. Setup appropriate OS level security domains
- C. Container runtime sandboxes
- D. Limit network access

V. Monitoring and Logging
- A. Configure Kubernetes audit logs
- B. Configure Audit Policies
- C. Monitor applications behavior with Falco