Training:

Kubernetes Security Masterclass

Date of the online training: **March 15-16, 2021**

Overview

Kubernetes is the world’s leading Container Management and Orchestration Platform. However, Kubernetes is often deployed without understanding some of its security features, limitations, available tools or security-oriented design. This has caused many an organization to run extremely critical infrastructure, very insecurely on Kubernetes. In addition, organizations incorrectly assume that Kubernetes in cloud-native environments and managed cloud environments is automatically secure, which is also far from the truth. While certain configuration parameters are abstracted away from the operators, Kubernetes clusters can still be subject to a plethora of misconfigurations and application security lapses.

This Masterclass is meant to prepare practitioners and operators alike, on the depths of Kubernetes Security. We start off with participants setting up and running their own Kubernetes clusters on a simulated “on-prem” environment. This ensures that they understand the intrinsic aspects of the cluster and underlying technology without blindly depending on managed cloud providers to secure them.

Subsequently, the class takes a firm toward the “Red-Team” by delving deep into Kubernetes attacks. The participants use a variety of known exploits, vulnerable apps and container escape techniques to attack and privilege-escalate on Kubernetes clusters, including some of the latest DNS Spoofing attack possibilities against Kubernetes. This segment is meant to train participants on “security through insecurity”. By understanding techniques from the attacker’s playbook, participants have a deep understanding of not only the cluster, but some of the ways these misconfigurations can impact the cluster, in terms of security.

The training then takes a "Blue Team" turn where we dive deep into Kubernetes defenses. Here we explore in depth, a variety of areas, tools and strategies to define a more secure Kubernetes cluster. The participants, through hands-on, cookbook-style sessions, learn how they can audit and secure Kubernetes clusters. In addition, they are exposed to a smorgasbord of useful OSS tools to help them assess, audit and defend against attackers looking to leverage vulnerable Kubernetes clusters. This segment focuses on, not limited to:

- Kubernetes Security Maturity Model
- Authentication, Authorization and Admission Control
- Secrets Management for Kubernetes deployments
- Vulnerability Assessment for Kubernetes Deployments
- Runtime Container Protections for Kubernetes Security
- Introduction to Service Mesh Security concepts, with Istio
- Introduction to Security Policy Management with Kubernetes with Open Policy Agent
- Kubernetes Logging API and Monitoring Practices
- CI/CD Pipelines for Kubernetes with Security

At the end of the training, we (trainers) are of the opinion that participants will walk away with a comprehensive and practical view of Kubernetes security. We believe that they will be equipped to address these and many other security concerns with Kubernetes within their own organizations, with a great deal of assurance.

The labs are highly advanced and per-student environments on the cloud that the students can access throughout the length of the training.

In addition, we will be giving students a useful repository of OSS Kubernetes Security Tools and access to our online training portal to learn more about Container Security, AppSec, Managing Secrets on the cloud and Kubernetes Security concepts.

Who should attend this training?

- AppSec Engineers and Professionals
- DevOps Professionals
- Senior Security Managers overseeing cloud and DevSecOps initiatives
- Penetration Testers
- Cloud Engineers

Prerequisites

- Working knowledge of Linux command line
- Basic knowledge of some (any) programming language
- Working knowledge of Docker or any container run time
- Working knowledge of Kubernetes will be useful

Requirements

Our entire lab environment is delivered over the cloud and accessible via the browser. No need for any VM to be set up. All that is needed is a laptop or a tablet (with keyboard) with a browser installed.

About the Trainers

Abhay Bhargav is the Founder of we45, a focused Application Security Company. Abhay is a builder and breaker of applications. He is the Chief Architect of “Orchestron", a leading Application Vulnerability Correlation and Orchestration Framework.

He has created some pioneering works in the area of DevSecOps and AppSec Automation, including the world’s first hands-on training program on DevSecOps, focused on Application Security Automation. In addition to this, Abhay is active in his research of new technologies and their impact on Application Security, namely Containers, Orchestration and Serverless Architectures.

Abhay is a speaker and trainer at major industry events including DEF CON, BlackHat, OWASP AppSecUSA, EU and AppSecCali. His trainings have been sold-out events at conferences like AppSecUSA, EU, AppSecDay Melbourne, CodeBlue (Japan), BlackHat USA, SHACK and so on.

Booking

Recommended online booking of trainings through:

https://troopers.de/tickets/

Contact

Need assistance? Don’t hesitate to call us. We are fluent in English and German. +49 6221 480390 or info@troopers.de

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / info@hmtrainingsolutions.com

+49 6022 5089999 / www.hmtrainingsolutions.com