APPSECDAY
AUSTRALIA

OWASP AppSec Day
1st of Nov 2019
Melbourne, Australia
info@appsecday.io
appsecday.io

Attacking and Defending Containers and Kubernetes

Training Course

28th & 29th of October

Table of Contents

Attacking and Defending Containers and Kubernetes 1

- Course Abstract 2
- What attendees will learn? 2
- What attendees will be provided? 2
- What attendees should bring? 2
- Pre-requisites 3
- Detailed Outline 4
  - Day 1 4
  - Day 2 5
- Trainer Biography 7

All training courses are two full days of intensive, hands-on learning and include complimentary morning tea, lunch and afternoon tea. Tickets can be secured buy going to the website https://appsecday.io/.

Course Abstract

With Organizations rapidly moving towards micro-service style architecture for their applications, container technology seems to be taking over at a rapid rate. Leading container technologies like Docker have risen in popularity and have been widely used because they have helped package and deploy consistent-state applications. Orchestration technologies like Kubernetes help scale such deployments to a massive scale which can potentially increase the overall attack-surface to a massive extent, if security is not given the attention required.

Security continues to remain a key challenge that both Organizations and Security practitioners face with container orchestrated deployments. While container orchestrated deployments may be vulnerable to security threats that plague any typical application deployments, they face specific security threats related to the containerization daemon, shared kernel, shared resources, secret management, insecure configurations, role management issues and many more!

Attacking an infrastructure or Applications leveraging container technology requires specific skill-set and a deep understanding of the underlying architecture.

What attendees will learn?

This training has been created with the objective of understanding both offensive and defensive security for containers and container orchestrated deployments. It will be a 2 day program that will detail through specific theory elements with extensive hands-on exercises that are similar to real-world threat scenarios that the attendees will understand and take part in and, will also understand the ways in which containerized deployments can be attacked, made secure, yet scalable, efficient and effective.

What attendees will be provided?

- Slides for the training course.

What attendees should bring?

- A terminal program to SSH into the remote lab environments. These programs should work fine:
  - Mac OSX => ITerm2 or Terminal (no need to install)
  - Windows => Putty or Cygwin
  - Linux => Terminal (no need to install anything else)
- Working WiFi adapter with ability to connect to third party wireless networks.

Pre-requisites

- Attendees should have a basic understanding of Linux environment and know their way around the terminal
- A basic understanding of 'OWASP TOP-10 Vulnerabilities' and 'Basics of Docker' will be helpful

Detailed Outline

Day 1

Session 1: Evolution to Container Technology and Container Tech Deep-Dive:

- Introduction to Container Technology
  - Namespace
  - Cgroups
  - Mount
- Hands-on Lab: Setting up a Minimal Container with nothing but Namespaces and CGroups
- Introduction to Containerized Deployments - Understanding and getting comfortable using Docker.
- An Introduction to containers
  - LXC and Linux Containers
  - Introducing Docker Images and Containers
  - Deep-dive into Docker
  - Docker Commands and Cheatsheet
- Hands-on:
  - Docker commands
  - Dockerfile
  - Images

Session 2: Introduction to Basic Container Orchestration with Docker-Compose

- Docker Compose
  - Introduction to docker-compose
  - Hands-on:
    - Docker-compose commands
  - Docker Compose Deep-Dive
  - Application Deployment Using docker
  - Hands-on
    - Containerize an application
    - Deploying a containerized application
    - Deploy a containerized application using docker-compose
- Threat Landscape- An Introduction to possible threats and attack surface when using Containers for Deployments.
  - Threat Model for Containerized Deployments
  - Daemon-related Threats
  - Network related Threats
  - OS and Kernel Threats
  - Threats with Application Libraries
  - Threats from Containerized Applications
- Traditional Threat-Modelling for Containers with STRIDE
  - Spoofing
  - Tampering
  - Repudiation

  - Information Disclosure
  - Denial of Service
  - Elevation of privileges

Session 3

- Attacking Containers and Containerized Deployments
  - Hands-on:
    - Container Breakout
    - Exploiting Insecure Docker Configurations
    - OS and Kernel level exploits
    - Trojanized Docker images
- Securing Containers and Container Deployments
  - Container Security Deep-Dive
  - Hands-on
    - AppArmor/SecComp
    - Restricting Capabilities
    - Analysing Docker images
  - Container Security Mitigations
  - Hands-on: Container Vulnerability Assessment
    - Clair
    - Dagda
    - Anchore
    - Docker-bench

Day 2

Session 1

- Introduction to Scalable Container Orchestrators
- Introduction to Container Orchestrators
- Getting started with Kubernetes
- Understanding Kubernetes Architecture and Components
- Hands-on:
  - Exploring Kubernetes Cluster
  - Deploying application to Kubernetes

Session 2

- Attacking Kubernetes Cluster
- Kubernetes Threat Model
- Attack Surface for a Kubernetes Cluster
- Hands on:
  - Attacking application deployed on Kubernetes
  - Exploiting a Vulnerable Kubernetes cluster
  - Maintaining Persistent Access and Pivoting in the K8s Cluster
  - Dissecting the K8s Attack and identifying Security Missteps

Session 3

- Kubernetes Security Deep-Dive

- K8s Threat Model and its counterpoint in Security Practices
- Hands-on: Ideal Security Journey: Kubernetes
    - Pod Security
    - Access Control
    - Secret Management
- Hands-on: Kubernetes Vulnerability Assessment
    - Kube-sec
    - Kube-hunter
    - Kube-bench
- Hands-on: Logging and Monitoring
    - Logging and Monitoring specific Parameters within the K8s Cluster
    - Identifying anomalies (especially security) with the K8s Cluster
- Hands-on: Kubernetes Network Security Implementation
    - Network Security Policy
    - Service Mesh - Istio/Envoy

Trainer Biography

Nithin Jois

https://www.linkedin.com/in/bondijois/

Nithin Jois is a Solutions engineer at we45 - a focused Application Security company. He has helped build ‘Orchestron’ - A leading Application Vulnerability Correlation and Orchestration Framework. He is experienced in Orchestrating containerized deployments securely to Production.

Nithin and his team have extensively used Docker APIs as a cornerstone to most of we45 developed security platforms and he has also helped clients of we45 deploy their Applications securely. Nithin is a passionate Open Source enthusiast and is the co-lead-developer of ThreatPlaybook - An Open Source framework that facilitates Threat Modelling as Code married with Application Security Automation on a single Fabric. He has also written multiple libraries that complement ThreatPlaybook. Nithin is an automation junkie who has built Scalable Scanner Integrations that leverage containers to the hilt and is passionate about Security, Containers and Serverless technology.

He speaks at meetup groups, webinars and training sessions. He participates in multiple CTF events and has worked on creating Intentionally Vulnerable Applications for CTF competitions and Secure Code Training. Nithin was a trainer and speaker at events like AppSecUS, LasCon, AppSecCali, DevSecCon, CodeBlue-Japan and SANS Secure-DevOps-Summit. In his spare time, he loves reading about personal finance, leadership, fitness, cryptocurrency, and other such topics. Nithin is an avid traveller and loves sharing stories over a cup of hot coffee or a mug of cold beer