|  |  |  |
| --- | --- | --- |
| **Day** | **Time Schedule** | **Topics Covered** |
| 1 | 9:30 Am – 11:30 Am | **Managing Cluster**   * **Managing the Kubernetes Cluster** * **Upgrading the Kubernetes Cluster** * **Backing Up and Restoring a Kubernetes Cluster** * **Lab: Upgrading Kubernetes Cluster** * **Troubleshooting** |
|  | 11:30 Am – 11:40 am | Tea Break |
|  | 11:40 am – 1pm | * **Cluster Setup Node Metadata Protection** * **Cluster Setup CIS BenchMark** |
|  | 1pm – 1:40 pm | Lunch break |
|  | 1:40 pm – 4:00 pm | * **Cluster Setup Verify Platform Binary** * **Cluster Hasrdening Exercise caution in using Service Account** * **Cluster hardening: Restrict APi Access** * **Cluster Hardening Upgrade K8s** |
|  | 4:00 pm – 4:10 pm | Tea Break |
|  | 4:10 pm – 6:30 pm | * **Micro service vulnerability Manager Secret**. * **Micro service vulnerability -container runtime sandbox** * **Micro service vulnerability** -OS level * **Microservice vulnerability-Mtls** * **Open Policy Agent** * **Supply Chain Security Image Footprint**. * **Supply Chain Security Image Vulnerability** |

**1. Managing Cluster**

* Managing the Kubernetes Cluster
* Upgrading the Kubernetes Cluster
* Backing Up and Restoring a Kubernetes Cluster

**Lab:** Upgrading Kubernetes Cluster

**2.** **Troubleshooting**

* Control Plane Failures
* Node Failure
* Application Failure
* Components manifests and errors
* Scenarios and Solutions

**Lab:** Troubleshooting in Kubernetes

**3.** **Cluster Setup Node Metadata Protection**

Introduction

Practice: Access Node Metadata

Practice: Protect Node Metadata via NetworkPolicy

TEST - NetworkPolicy Metadata Protection

**4. Cluster Setup CIS BenchMark**

introduction

Practice - CIS in Action

Practice - kube-bench

Recap

TEST - Apply CIS rules for Controlplane

**5. Cluster Setup Verify Platform Binary**

Introduction

Practice - Download and verify K8s release

Practice - Verify apiserver binary running in our cluster

TEST - Verify Kubelet Binary

**5. Cluster Hasrdening Exercise caution in using Service Account**

Introduction

Practice - Pod uses custom ServiceAccount

Practice - Disable ServiceAccount mounting

Practice - Limit ServiceAccounts using RBAC

Recap

TEST - ServiceAccount Token Mounting

**6. Cluster hardening: Restrict APi Access**

Introduction

Practice - Anonymous Access

Practice - Insecure Access

Practice - Manual API Request

Practice - External Apiserver Access

NodeRestriction AdmissionController

Practice - Verify NodeRestriction

Recap

TEST - Crash that Apiserver

TEST - Apiserver Manifest Misconfigured

TEST - NodeRestriction

**7. Cluster Hardening Upgrade K8s**

Introduction

Ubuntu 20.04 Update

Practice - Create outdated cluster

Practice - Upgrade controlplane node

Practice - Upgrade node

**8. Micro service vulnerability Manager Secret**

Introduction

Practice - Create Simple Secret Scenario

Practice - Hack Secrets in Container Runtime

Practice - Hack Secrets in ETCD

ETCD Encryption

Practice - Encrypt ETCD

Recap

TEST - Access Secrets in Pods

TEST - Read Secret Values

TEST - Secrets Pods and ServiceAccount

TEST - ETCD Encryption

**9. Micro service vulnerability -container runtime sandbox**

practice - Container calls Linux Kernel

Open Container Initiative OCI

Sandbox Runtime Katacontainers

Sandbox Runtime gVisor

Practice - Create and use RuntimeClasses

Practice - Install and use gVisor

Recap

TEST - gVisor and RuntimeClass

**10. Micro service vulnerability** -OS level

intro and Security Contexts

Practice - Set Container User and Group

Practice - Force Container Non-Root

Privileged Containers

Practice - Create Privileged Containers

PrivilegeEscalation

Practice - Disable PrivilegeEscalation

TEST - Privileged Containers

TEST - Privilege Escalation Containers

**11. Microservice vulnerability-Mtls**

Intro

Practice - Create sidecar proxy

**12. Open Policy Agent**

Cluster Reset

Introduction

Practice - Install OPA

Practice - Deny All Policy

Practice - Enforce Namespace Labels

Practice - Enforce Deployment replica count

Practice - The Rego Playground and more examples

**13. Supply Chain Security Image Footprint**

introduction

Practice - Reduce Image Footprint with Multi-Stage

Practice - Secure and harden Images

TEST - Image Footprint User

TEST - Image Container Hardening

**14. Supply Chain Security Image Vulnerability**

Introduction

Clair and Trivy

Practice - Use Trivy to scan images

Recap

TEST - Scan images using Trivy