Practical DevSecOps

Container Security Expert

COURSE

www.practical-devsecops.com

Container Security Expert

Practical DevSecOps

Practical approach to Offensive And Defensive techniques in Container technology.

Abstract

Linux containers allow both developers and IT operations to create a portable, lightweight, and self-sufficient environment for every application.

However, securing containerized environments is a significant concern for Dev/Sec/Ops teams. The Container Security Expert course provides the tools, techniques, and tactics to audit, secure, and monitor containers in production environments.

Container Security Expert is the training program for professionals tasked with securing the container environment. The course allows you to get hands-on experience as you work with live containers in our lab, gaining significant insights that will arm you to attack and secure a containerized infrastructure in any environment.

Who should take this course?

This course is aimed at professionals interested in securing the container environment as part of agile/cloud/DevOps environments like Security Professionals, Penetration Testers, IT managers, Developers, and DevOps Engineers.

Course Prerequisites

Course participants should know basic Linux commands like ls, cd, mkdir, etc.

Learning Objectives

The following are the course's objectives.

1. Building solid foundations that are required to understand the container security landscape.
2. Embedding security while creating, building container images, and securing running containers.
3. Gaining knowledge in limiting the blast radius in case of a container compromise.
4. Gaining expert skills in analyzing container weaknesses, attacking containers, and defending containers through various tools and tactics
5. Learning to monitor containers for detecting anomalies and responding to threats.
6. Gaining abilities to apply practical container security skills in real-world container deployments.

Software and Hardware Requirements

Our state-of-the-art DevSecOps Training Platform works within your browser. You can even do the labs from your mobile devices like iPad and Android phones. All you need is a modern browser on a laptop or desktop.

Container Security Expert

Practical DevSecOps

Practical approach to Offensive And Defensive techniques in Container technology.

Course Syllabus

The CCSE course takes you through the container basics, core components of container technology, and ways to interact with the container. Once you learn the fundamentals, you will gain hands-on experience with realistic attack scenarios like privilege escalation, container breakouts, and security misconfigurations. We will finish the course by hardening the container environment and monitoring the container workloads.

The following topics are covered as part of the course.

1. Introduction to Containers
2. Container Reconnaissance
3. Attacking Containers and Containerized Apps
4. Defending Containers and Containerized Apps on Scale
5. Security Monitoring of Containers

Training Duration

The participant can complete the course in 20 hours. That includes 5 hours of video lectures and 15 hours of hands-on practice. However, a participant has lifetime access to the on-demand course with 30 days of online lab access.

What Will Students be Provided?

Resources for your Container Security Learning:

1. Course Videos and Checklists
2. Course Manual
3. 30 days Online Lab Access
4. 40+ Guided Exercises
5. Access to a dedicated Mattermost channel
6. One exam attempt for Certified Container Security Expert Certification

Learn more

To learn more about our courses, certifications and pricing, please visit **our courses** or **contact us**

Container Security Expert

Practical DevSecOps

Detailed Syllabus

DAY 1

1 Introduction to Containers

1. What is a container?
2. Basics of a container and its challenges
3. Container vs. Virtualization
    a. Container Advantages
    b. Container Disadvantages
4. Container fundamentals
    a. Namespaces
    b. Cgroup
    c. Capabilities
5. Docker architecture and its components
    a. Docker CLI
    b. Docker Engine (Daemon, API)
    c. Docker Runtime (containerd, shim, runc)
6. Interacting with container ecosystem
    a. Docker images and image layers
    b. Build Container images using Dockerfile
    c. Docker image repository
    d. Running a container
7. Managing / Orchestrating multiple containers
    a. Using CLI/API to manage multiple containers
    b. Docker Compose
    c. Docker Swarm
    d. Kubernetes
8. Docker alternatives
    a. Podman
    b. CRI-O

Container Security Expert

Practical DevSecOps

Detailed Syllabus

9. **Hands-on Exercises**:
    a. Learn Docker commands
    b. Create Docker Image using Dockerfile
    c. How to use container registry
    d. Interact with Docker API using API/SDK
    e. How to run multiple containers using CLI/API
    f. Learn Docker Compose

2 Container Reconnaissance

1. Overview of Container Security
2. Attack surface of the container ecosystem
3. Identifying the components and their security state
    a. Get an inventory of containers
        i. Docker Images
        ii. Dockerfile and Environment variables
        iii. Docker volumes
        iv. Docker Networking
        v. Ports used/Port forwarding
        vi. Docker Registries
    b. Exhaustive review of Namespaces, cgroups and capabilities
4. Analysis of the attack surface
    a. Using native tools
    b. Using third-party tools
5. **Hands-on Exercises**:
    a. Writing the Dockerfile
    b. Learn how to work with data in a container
    c. Networking in Docker
    d. Scanning the remote host for unauthenticated Docker API access
    e. Identify a container and extract sensitive information
    f. Identify misconfigurations in namespace, capabilities, and networking
    g. Create and restore a snapshot (tar) of the container for further analysis

Container Security Expert

Practical DevSecOps

Detailed Syllabus

Please note
Every topic/subtopic has an exercise in this module

3 Attacking Containers and Containerized Apps

1. Containers Attack Matrix
2. Image-based attacks
    a. Malicious Images
    b. Extracting passwords, tokens, TLS certs, etc.
    c. Exploiting vulnerable components
3. Registry-based attacks
    a. Insecure Docker registries
    b. Open Docker registries
    c. Lack of authorization (RBAC)
4. Container-based attacks
    a. Manipulating the Privileged mode containers
    b. Attacking mounted docker volumes
    c. Abusing SetUID/SetGID binaries
    d. Exploiting shared namespaces
    e. Attacking Linux capabilities
5. Docker host (Daemon) / kernel attacks
    a. Exploiting unauthenticated Docker API
    b. Insecure Docker endpoint
    c. Lack of network segregation
    d. Denial of service attacks
    e. Kernel exploits
6. Privilege escalation methods in Docker
7. Security misconfigurations
    a. Attacking management tools (Portainer)
    b. Exploiting OWASP Top 10 issues in containerized apps

Container Security Expert

Practical DevSecOps

Detailed Syllabus

DAY 2

4 Defending Containers and Containerized Apps on Scale

1. Container image security
    a. Building secure container images
        i. Choosing base images
        ii. Distroless images
        iii. Scratch images
    b. Security Linting of Dockerfiles
    c. Static Analysis(SCA) of container images
    d. Scan for vulnerabilities in container
        i. Choosing the right container scanner tool for your needs
2. Docker Daemon security configurations
    a. Docker user remapping
    b. Docker runtime security (gVisor, Kata)
    c. Docker socket configuration
        i. fd
        ii. TCP socket
        iii. TLS authentication
    d. Dynamic Analysis of the container hosts and daemons
3. Docker host security configurations
    a. Kernel Hardening using Seccomp and AppArmor
    b. Custom policy creation using Seccomp and AppArmor
4. Network Security in containers
    a. Segregating networks
5. Misc Docker Security Configurations
    a. Content Trust and Integrity checks

Container Security Expert

Detailed Syllabus

6. Docker Registry security configurations
    a. Private vs. Public Registries
    b. Authentication and Authorization (RBAC)
    c. Built-in Image scanning capabilities
    d. Policy enforcement
    e. DevOps CI/CD Integration
7. Docker Tools, Techniques and Tactics
    a. Tools
        i. Dive (Forensic)
        ii. Dockle
    b. Techniques
    c. Tactics
8. **Hands-on Exercises**:
    a. Minimize security misconfigurations in Docker with CIS
    b. Build a secure & most miniature image to minimize the footprint
    c. Build a distro less image to reduce the footprint
    d. Docker Content Trust with Notary
    e. Securing the container by default using Harbor
    f. Scanning Docker for vulnerabilities with Trivy

5 Security Monitoring of Containers

1. Monitoring Docker events, logs
2. Incident response in containers
3. Docker runtime prevention
4. Policy creation, enforcement, and management
5. Docker security monitoring using Wazuh
6. **Hands-on Exercises**:
    a. Anchore Engine - Policy creation and enforcement
    b. Sysdig Falco - Runtime protection and monitoring
    c. Tracee - Runtime security

Container Security Expert

Practical DevSecOps

Certification Process

Exam and certification process

Our certifications are well recognized in the industry as we ensure our students gain practical skills to implement DevSecOps. To ensure we deliver on our promise, we have a rigorous certification program.

CCSE exam is an online, task-oriented exam where you attempt to solve **5 challenges** (tasks) in a span of **6 hours**. The exam is based on the content covered in the course but might require further research to pass the exam. After the exam, you have **24 hours** to send us the exam report.

Please note
it's not an MCQ or tests your memory type of exam but practical applicability of the content covered in the course.

Exam Pass percentage

The student needs to achieve at least 80 points (80%) to achieve the CCSE certification.

Exam Challenges/tasks

The exam has 5 challenges for the exam, each of these challenges provides you points based on how complete or partial your solution was. You would need to score 80 points out of 100 (80%) to achieve the CCSE certification.

Exam documentation

After the exam, you have about 24 hours to send us the exam report via email.

Steps Involved

A typical certification flow involves 5 steps.

1. The student schedules the exam.
2. The student will receive an exam guide that includes challenges via email. Our instructors will be there to assist you if you face any difficulty while connecting to the exam lab.
3. The student will connect to the exam lab using details from the exam guide and will attempt the practical exam.
4. After the exam, the student will have 24 hours to send us the exam report.
5. Practical DevSecOps team will evaluate the report and share the result (pass/fail) with the student.

Practical DevSecOps

About us

Practical DevSecOps (a Hysn Technologies Inc company) offers vendor-neutral, practical, and hands-on DevSecOps training and certification programs for IT Professionals. Our online training and certifications are focused on modern areas of information security, including DevOps Security, Cloud-Native Security, Cloud Security & Container security. The certifications are achieved after rigorous tests (12-24 hour exams) of skill and are considered the most valuable in the information security field.

@pdevsecops

@pdevsecops

Practical DevSecOps

USA

+1 (415) 800 4768
trainings@practical-devsecops.com
201 Spear St #1100, San Francisco, CA 94105

India

+91 81216 77008
apac@practical-devsecops.com
Hyderabad, India

Singapore

+65 85042132
apac@practical-devsecops.com
531A Upper Cross Street #04-95
Hong Lim Complex Singapore 051531