KOENIG SOLUTIONS · COURSE OUTLINE

Hacking and Securing Docker Containers v2.0

Learn to hack and secure Docker containers, from image fundamentals to container breakout and defensive hardening.

1 Day	5	30
8 HOURS A DAY	MODULES	TOPICS

COURSE OVERVIEW

This course introduces students to the security concepts associated with Docker. Docker is a popular software and it is widely used in Information Technology Industry. It's popularity also brings a larger attack surface and thus it is important to understand it's security aspects to be able to protect Docker containers.

WHO THIS COURSE IS FOR

- **Docker Administrators**
- **Security Engineers**
- **Penetration Testers**
- **DevOps Engineers**
- **System Administrators**

PREREQUISITES

- This course starts from very basics and thus no Docker experience is required

TOOLS AND REQUIREMENTS

Lab Requirement

- Koenig DC

LEARNING OBJECTIVES

- Explain differences between virtual machines and containers
- Build and run Docker images and containers
- Describe how Docker images are stored locally
- Identify the Docker attack surface and common vulnerabilities
- Apply container breakout techniques using docker.sock and privileged flags
- Access Docker secrets through exploitation techniques
- Scan Docker images and audit environments with Docker Bench Security
- Configure AppArmor, Seccomp and Docker Content Trust as defenses

COURSE SYLLABUS

5 Modules, 30 Topics

01

Introduction

02

Fundamentals of Docker

TOPICS

- What is Docker?
- Virtual Machines vs Containers
- Virtual Machine Download
- Lab setup
- Building your first Docker Image
- Running your first Docker container
- Images vs Containers
- How Docker Images are stored locally
- Control Groups
- Namespaces

03

Hacking Docker Containers

TOPICS

- Introduction
- Docker Attack Surface
- Exploiting Vulnerable Images
- Backdooring Docker Images
- Privilege Escalation
- Introduction to Container Breakout
- Introduction to docker.sock
- Container escape using docker.sock
- Introduction to –privileged flag
- Writing to Kernel Space from a container
- Writing a Kernel Space to get a reverse shell
- Accessing Docker Secrets

04

Automated Assessments

TOPICS

- Introduction
- Scanning Docker Images
- Auditing the Environment using Docker Bench Security

05

Defenses

TOPICS

Introduction · Apprarmor Profiles · Seccomp Profiles · Capabilities · Docker Content Trust

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training | Live Online Classes (ILO) | Fly-Me-A-Trainer (FMAT) | Flexi (Self-Paced) | 1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com | info@koenig-solutions.com