Container Escape and Hacking Kubernetes Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Container Escape and Hacking Kubernetes Training Course offers an offensive and defensive deep-dive into the cutting-edge field of Cloud-Native Security. As organizations rapidly migrate critical workloads to containerized environments orchestrated by Kubernetes, the attack surface expands, making expertise in this domain a non-negotiable requirement for modern security professionals. This training moves beyond theoretical concepts, providing participants with the practical, hands-on hacking skills needed to proactively identify, exploit, and meticulously defend against the most severe cloud-native threats.

This program specifically targets the critical and frequently-exploited vulnerability of Container Escape, where an attacker breaks out of the confined container environment to gain access to the underlying Host System or Kubernetes Cluster. Through real-world Red Team TTPs Tactics, Techniques, and Procedures, attendees will learn how to weaponize common misconfigurations such as insecure Role-Based Access Control, exposed Docker Sockets, and kernel vulnerabilities to achieve Privilege Escalation and Lateral Movement. By adopting a purple team mindset, the course ensures that the offensive knowledge gained is immediately translated into actionable Security Best Practices and robust Runtime Defense strategies, ultimately building a truly Resilient Cloud Infrastructure.

Programme Curriculum

Container Escape and Hacking Kubernetes Training Course

Introduction

Container Escape and Hacking Kubernetes Training Course offers an offensive and defensive deep-dive into the cutting-edge field of Cloud-Native Security. As organizations rapidly migrate critical workloads to containerized environments orchestrated by Kubernetes, the attack surface expands, making expertise in this domain a non-negotiable requirement for modern security professionals. This training moves beyond theoretical

concepts, providing participants with the practical, hands-on hacking skills needed to proactively identify, exploit, and meticulously defend against the most severe cloud-native threats.

This program specifically targets the critical and frequently-exploited vulnerability of Container Escape, where an attacker breaks out of the confined container environment to gain access to the underlying Host System or Kubernetes Cluster. Through real-world Red Team TTPs Tactics, Techniques, and Procedures, attendees will learn how to weaponize common misconfigurations such as insecure Role-Based Access Control, exposed Docker Sockets, and kernel vulnerabilities to achieve Privilege Escalation and Lateral Movement. By adopting a purple team mindset, the course ensures that the offensive knowledge gained is immediately translated into actionable Security Best Practices and robust Runtime Defense strategies, ultimately building a truly Resilient Cloud Infrastructure.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Master Container Breakout techniques, including exploiting vulnerable Cgroups and User-Mode Helpers.
2. Identify and exploit dangerous Kubernetes Misconfigurations and insecure defaults.
3. Perform comprehensive Cluster Reconnaissance and Threat Modeling for cloud-native environments.
4. Weaponize insecure Role-Based Access Control (RBAC) to achieve Privilege Escalation to Cluster Admin.
5. Exploit common HostPath and Volume Mount exposures for data exfiltration and persistence.
6. Understand and defend against Supply Chain Attacks involving malicious or vulnerable container images.
7. Implement Network Segmentation using Kubernetes Network Policies for defense-in-depth.
8. Utilize open-source tools like Falco and Kube-Hunter for Threat Detection and Vulnerability Assessment.
9. Secure Container Runtime environments using technologies like AppArmor and SELinux.
10. Harden the CI/CD Pipeline to enforce Immutable Infrastructure and Security Gates.
11. Securely manage sensitive data using Kubernetes Secrets and Vault Integration.
12. Apply Open Policy Agent (OPA) Gatekeeper to enforce declarative security policies.
13. Formulate and execute a robust Incident Response plan for a Kubernetes cluster breach.

Target Audience

1. Penetration Testers / Ethical Hackers
2. DevSecOps Engineers / Security Engineers
3. Cloud Security Architects
4. SRE (Site Reliability Engineers)
5. Developers working with containers and Kubernetes
6. Red Team and Blue Team members
7. Vulnerability Analysts
8. Security Auditors / Compliance Officers

Course Modules

Module 1: Cloud-Native Foundations & Attack Surface

- Linux Container Primitives.

- Docker/Containerd Deep Dive.
- Kubernetes Architecture Review.
- Threat Modeling.
- Case Study: Analysis of the TeamTNT crypto-mining campaign exploiting insecure Docker/Kube APIs.

Module 2: Initial Access and Container Exploitation

- Identifying and exploiting insecure container configurations.
- Secret Management Hacking
- Remote Code Execution in microservices to gain a shell.
- Leveraging misconfigured health checks or web-shells.
- Case Study: Exploiting a vulnerable application with a mounted Service Account Token.

Module 3: Advanced Container Escape Techniques

- Escaping via exposed Docker.sock or other runtime sockets.
- Breaking out using kernel vulnerabilities and user-mode helper exploits.
- Exploiting dangerous HostPath and device volume mounts.
- Abusing SUID binaries and other privilege escalation methods within the container.
- Case Study: Walkthrough of the CVE-2019-5736 vulnerability and host compromise.

Module 4: Hacking the Kubernetes Cluster: Reconnaissance & Lateral Movement

- In-depth kubectl and API Server reconnaissance for internal information.
- Kubelet API and Kubeconfig exploitation.
- Targeting the etcd data store for sensitive configuration and secrets.
- Techniques for Lateral Movement between namespaces and nodes.
- Case Study: Compromising a Kubelet using an anonymous binding for node access.

Module 5: Privilege Escalation via RBAC and Admission Controllers

- Understanding and enumerating Role-Based Access Control permissions.
- Exploiting weak ClusterRoles and RoleBindings to gain higher privileges.
- Chaining exploits to achieve Cluster Admin status.
- Bypassing and exploiting misconfigured Admission Controllers.
- Case Study: Exploiting a Service Account with 'get' and 'create' permissions to pivot to full cluster access.

Module 6: Defensive Strategies and Hardening

- Implementing Pod Security Standards and Security Contexts.
- Enforcing the Principle of Least Privilege for Service Accounts and users.
- Secure base images, vulnerability scanning, and supply chain defense.
- Kubernetes Hardening Benchmarks and secure configuration management.
- Case Study: Hardening a deployment by removing the CAP_NET_RAW capability to block network sniffing.

Module 7: Policy Enforcement and Runtime Defense

- Implementing declarative security with Open Policy Agent Gatekeeper.
- Network Segmentation and micro-segmentation using Network Policies.
- Runtime Security Monitoring with tools like Falco for event-based threat detection.

- Auditing and monitoring API Server Logs and Audit Policies.
- Case Study: Writing a Falco rule to detect a container spawning a shell or mounting the host filesystem.

Module 8: Incident Response and Advanced Defense

- Best practices for securing the CI/CD Pipeline.
- Developing an Incident Response playbook for a container escape event.
- Container forensics.
- Advanced isolation with gVisor or Kata Containers.
- Case Study: Post-mortem analysis of the CVE-2022-0811 incident and mitigation steps.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com