Cloud Security Attack Vectors and Exploitation 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

In the rapidly evolving digital landscape, organizations are aggressively migrating to cloud environments, yet this adoption introduces complex and novel attack surfaces. Traditional security models fail against the unique threats posed by shared responsibility, massive scale, and cloud-native services. Cloud Security Attack Vectors and Exploitation Training Course is designed to bridge the critical cybersecurity skills gap by equipping security professionals with the hacker mindset. We move beyond compliance checklists to offer deep, technical mastery in identifying, exploiting, and effectively mitigating the most critical and trending cloud vulnerabilities.

This program provides a deeply immersive, hands-on experience. Participants will engage with live-fire labs focusing on real-world Cloud Attack Scenarios, from Identity and Access Management (IAM) privilege escalation and serverless function exploitation to container breakout and exploiting Infrastructure as Code (IaC) misconfigurations. By adopting the perspective of a skilled attacker, you will learn to uncover critical security flaws in multi-cloud and hybrid cloud environments. The ultimate goal is to enable you to design and implement Zero Trust Architecture and automated DevSecOps controls, ensuring cloud resilience and proactive defense against sophisticated Advanced Persistent Threats (APTs).

Programme Curriculum

Cloud Security Attack Vectors and Exploitation Training Course

Introduction

In the rapidly evolving digital landscape, organizations are aggressively migrating to cloud environments, yet this adoption introduces complex and novel attack surfaces. Traditional security models fail against the unique threats posed by shared responsibility, massive scale, and cloud-native services. Cloud Security Attack Vectors and Exploitation Training Course is designed to bridge the critical cybersecurity skills gap by equipping security

professionals with the hacker mindset. We move beyond compliance checklists to offer deep, technical mastery in identifying, exploiting, and effectively mitigating the most critical and trending cloud vulnerabilities.

This program provides a deeply immersive, hands-on experience. Participants will engage with live-fire labs focusing on real-world Cloud Attack Scenarios, from Identity and Access Management (IAM) privilege escalation and serverless function exploitation to container breakout and exploiting Infrastructure as Code (IaC) misconfigurations. By adopting the perspective of a skilled attacker, you will learn to uncover critical security flaws in multi-cloud and hybrid cloud environments. The ultimate goal is to enable you to design and implement Zero Trust Architecture and automated DevSecOps controls, ensuring cloud resilience and proactive defense against sophisticated Advanced Persistent Threats (APTs).

Course Duration

5 days

Course Objectives

1. Master the Cloud Shared Responsibility Model and identify the security boundaries in IaaS, PaaS, and SaaS.
2. Exploit and defend against common Cloud Misconfigurations.
3. Perform comprehensive Cloud Reconnaissance and Asset Inventory across major CSPs
4. Execute and mitigate IAM Privilege Escalation techniques and Credential Theft in cloud environments.
5. Analyze and weaponize vulnerabilities in Infrastructure as Code (IaC) templates
6. Penetrate and secure modern cloud workloads, including Container Security and Kubernetes clusters.
7. Identify and exploit flaws in Serverless and Function-as-a-Service (FaaS) architectures.
8. Analyze and secure CI/CD Pipeline vulnerabilities to prevent Supply Chain Attacks.
9. Implement Cloud Security Posture Management (CSPM) to automate the detection of misconfigurations.
10. Develop offensive strategies for targeting and exploiting Insecure APIs and microservices in the cloud.
11. Perform effective Cloud Forensics and Incident Response steps following a cloud breach.
12. Design and deploy Zero Trust Architecture principles within a Multi-Cloud setting.
13. Integrate security into the development lifecycle for continuous cloud security.

Target Audience

1. Cloud Security Engineers
2. Penetration Testers and Red Teamers
3. Security Architects
4. DevSecOps Engineers
5. Cloud Architects and Developers
6. Security Analysts
7. Cybersecurity Consultants
8. IT/Security Managers

Course Modules

Module 1: Cloud Attack Fundamentals and Reconnaissance

- Shared Responsibility Model in depth and security gaps.
- Cloud Reconnaissance and Asset Inventory techniques.
- Understanding the Cloud Control Plane and potential attack entry points.
- Identifying and Mapping the Cloud Attack Surface for AWS, Azure, and GCP.

- Case Study: Exploiting publicly exposed cloud resource metadata endpoints for initial access.

Module 2: Identity and Access Management (IAM) Hacking

- Exploiting overly permissive policies and Principle of Least Privilege violations.
- Credential Theft and compromise techniques
- Methods for Privilege Escalation via resource misconfigurations and role assumption.
- Attacking Federations, SSO, and leveraging trust relationships.
- Case Study: Lateral movement and data exfiltration using a compromised IAM Role with excessive permissions.

Module 3: Storage and Data Exploitation

- Discovering and exploiting public/misconfigured storage buckets
- Exploiting data access vulnerabilities in databases and snapshot services.
- Techniques for bypassing encryption and poor Data Loss Prevention controls.
- Securing data at rest and in transit; mastering encryption keys and services.
- Case Study: A major data breach via an unauthenticated, publicly readable Amazon S3 bucket.

Module 4: Network and Infrastructure Misconfigurations

- Exploiting insecure Virtual Private Cloud and network segmentation.
- Bypassing and hardening Cloud Firewalls and Security Groups.
- Attacking Load Balancers, WAFs, and network routing configurations.
- Identifying and exploiting unmanaged or legacy virtual machine instances
- Case Study: Gaining C2 access by exploiting a misconfigured Azure Network Security Group rule.

Module 5: Container and Kubernetes Security

- Deep dive into Docker and Kubernetes architecture and common security flaws.
- Exploiting misconfigured Pod Security Policies and insecure images.
- Executing a Container Breakout to gain access to the underlying host.
- Securing the Kubernetes Control Plane and preventing unauthorized access.
- Case Study: Compromising a Kubernetes cluster by exploiting a vulnerable application running as a privileged container.

Module 6: Serverless and API Exploitation

- Identifying and exploiting vulnerabilities in Serverless Functions.
- Injection attacks and logic flaws in API Gateways and microservices.
- Securing event-driven architectures and API backends.
- Advanced techniques for exploiting Insecure APIs.
- Case Study: Taking down a critical business function by exploiting a resource exhaustion vulnerability in a serverless application.

Module 7: DevSecOps and Supply Chain Attacks

- Exploiting vulnerable Infrastructure as Code templates.
- Attacking the CI/CD Pipeline to inject malicious code.
- Leveraging dependency confusion and repository misconfigurations.
- Integrating security tools for automated scanning and policy enforcement.

- Case Study: A Software Supply Chain Attack resulting from exploiting a vulnerable secret stored in a CI/CD variable.

Module 8: Defense, Monitoring, and Incident Response

- Implementing Cloud Security Posture Management and Cloud Workload Protection Platform.
- Advanced Cloud Logging and Threat Detection using native services.
- Developing and testing a Cloud Incident Response plan.
- Applying the Zero Trust Model to cloud security engineering.
- Case Study: Simulating a cloud breach and conducting a full Cloud Forensics investigation and recovery.

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