AWS Pentesting and Security Auditing 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

The rapid adoption of cloud computing has made Amazon Web Services (AWS) the leading platform for mission-critical applications, simultaneously expanding the attack surface for cyber adversaries. AWS Pentesting and Security Auditing Training Course provides essential, hands-on training in Cloud Penetration Testing and AWS Security Auditing, addressing the critical demand for specialized Cloud Security Posture Management skills. Participants will master offensive and defensive techniques to identify, exploit, and remediate vulnerabilities in core AWS services like IAM, S3, EC2, and Serverless functions. By focusing on the Shared Responsibility Model and adherence to the AWS Penetration Testing Policy, this program ensures graduates can conduct compliant, high-impact security assessments, elevating the security posture of any cloud environment.

The curriculum is built around real-world scenarios, leveraging cutting-edge Offensive Security tools like Pacu and CloudGoat to provide a deep, practical understanding of modern cloud native threats. Beyond exploitation, the course emphasizes comprehensive Security Auditing, teaching participants how to implement and verify least privilege controls, enforce Zero Trust architectures, and ensure strict compliance with industry regulations like GDPR and HIPAA. This dual focus on both hacking and defense empowers security professionals to become true AWS Security Architects and Cloud Security Engineers, equipped to implement robust, automated security practices using Infrastructure as Code and DevSecOps principles to prevent data breaches and achieve continuous monitoring.

Programme Curriculum

AWS Pentesting and Security Auditing Training Course

Introduction

The rapid adoption of cloud computing has made Amazon Web Services (AWS) the leading platform for mission-critical applications, simultaneously expanding the attack surface for cyber adversaries. AWS Pentesting and Security Auditing Training Course provides essential, hands-on training in Cloud Penetration Testing and AWS Security Auditing, addressing the critical demand for specialized Cloud Security Posture Management skills. Participants will master offensive and defensive techniques to identify, exploit, and remediate vulnerabilities in core AWS services like IAM, S3, EC2, and Serverless functions. By focusing on the Shared Responsibility Model and adherence to the AWS Penetration Testing Policy, this program ensures graduates can conduct compliant, high-impact security assessments, elevating the security posture of any cloud environment.

The curriculum is built around real-world scenarios, leveraging cutting-edge Offensive Security tools like Pacu and CloudGoat to provide a deep, practical understanding of modern cloud native threats. Beyond exploitation, the course emphasizes comprehensive Security Auditing, teaching participants how to implement and verify least privilege controls, enforce Zero Trust architectures, and ensure strict compliance with industry regulations like GDPR and HIPAA. This dual focus on both hacking and defense empowers security professionals to become true AWS Security Architects and Cloud Security Engineers, equipped to implement robust, automated security practices using Infrastructure as Code and DevSecOps principles to prevent data breaches and achieve continuous monitoring.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Understand and strictly adhere to the AWS Penetration Testing Policy and legal compliance framework.
2. Perform in-depth AWS Reconnaissance and Enumeration to map the target's cloud infrastructure.
3. Identify and exploit misconfigurations in AWS IAM for effective Privilege Escalation.
4. Conduct S3 Bucket Audits and exploit vulnerable permissions, including public access and cross-account misconfigurations.
5. Assess and secure VPC and Network Security controls, including Security Groups and Network ACLs.
6. Penetrate and secure EC2 instances and related services using techniques like SSRF and metadata service exploitation.
7. Identify and remediate security flaws in Serverless architectures, focusing on Lambda and API Gateway.
8. Master the use of Cloud Pentesting Tools such as Pacu, ScoutSuite, and CloudGoat for automated assessments.
9. Implement Data Protection best practices, including KMS encryption and securing secrets with Secrets Manager.
10. Design and implement a strategy for Cloud Security Posture Management (CSPM) and Continuous Monitoring using AWS native tools like Security Hub and GuardDuty.
11. Perform a full AWS Security Audit to verify adherence to industry standards and compliance frameworks
12. Integrate DevSecOps security practices into CI/CD Pipelines to prevent the deployment of insecure Infrastructure as Code (IaC).
13. Develop practical incident response and Cloud Forensics skills for security events in the AWS environment.

Target Audience

1. Security Analysts/Engineers.

2. Penetration Testers.
3. Cloud Architects.
4. Security Auditors/Compliance Officers.
5. DevSecOps Engineers.
6. Red Team/Blue Team Members.
7. IT/System Administrators.
8. CISO/Security Managers.

Course Modules

Module 1: Cloud Pentesting Fundamentals and IAM Exploitation

- Deep dive into the AWS Shared Responsibility Model and the AWS Penetration Testing Policy.
- Mastering AWS CLI and advanced Enumeration techniques for target discovery.
- Identifying and abusing overly permissive IAM Policies and Roles.
- IAM Privilege Escalation using misconfigured iam:PassRole permissions.
- Case Study: Simulating a breach resulting from an exposed IAM access key leading to lateral movement.

Module 2: Storage and Data Service Security Auditing

- Comprehensive security review of Amazon S3 Buckets, including ACLs and Bucket Policies.
- Exploiting S3 public access, unauthorized cross-account access, and data leakage.
- Securing data at rest and in transit with AWS KMS and AWS Secrets Manager.
- Auditing security of other storage services like EBS and EFS volumes.
- Case Study: Replicating the Capital One breach scenario to demonstrate S3 and WAF vulnerabilities.

Module 3: EC2 and Compute Exploitation Techniques

- Attacking the EC2 Metadata Service for credential and token theft.
- Exploiting misconfigured Security Groups to gain unauthorized network access.
- Techniques for post-exploitation persistence and lateral movement within the VPC.
- Auditing AMI and Container Security for weak configurations.
- Case Study: Exploiting an SSRF vulnerability on an EC2 instance to steal temporary credentials and pivot within the environment.

Module 4: Network and Application Security Hacking

- Assessing VPC configurations, Subnets, Route Tables, and Internet Gateways.
- Penetration testing and auditing AWS WAF and CloudFront security configurations.
- Exploiting API Gateway and Load Balancer misconfigurations.
- Advanced tactics for bypassing network segmentation and filtering controls.
- Case Study: Discovering and exploiting an unauthenticated API endpoint in API Gateway to gain initial access to an application environment.

Module 5: Serverless and Application Services Pentesting

- Security assessment of AWS Lambda functions, including code injection and execution environment attacks.
- Identifying vulnerabilities in serverless access and permissions, often leading to function chaining attacks.
- Auditing SQS and SNS for unauthorized message handling and eavesdropping.

- Securing CloudFormation and Terraform templates using IaC Scanning tools.
- Case Study: Exploiting a vulnerable Lambda function's environment variables to retrieve a database connection string and exfiltrate data.

Module 6: Cloud Security Posture Management and Monitoring

- Implementing and tuning Amazon GuardDuty for intelligent threat detection.
- Using AWS Security Hub to centralize and prioritize security alerts and compliance checks.
- Configuring AWS Config and CloudTrail for comprehensive logging and change auditing.
- Automating security checks and remediation using AWS Lambda and EventBridge.
- Case Study: Setting up continuous monitoring and automated response to a root user login event using CloudTrail and Lambda.

Module 7: Advanced Compliance and Security Auditing

- Deep dive into Compliance frameworks.
- Performing a holistic AWS Security Audit using best-practice checklists and open-source tools
- Reviewing the security of AWS Organizations and multi-account strategies.
- Utilizing AWS Audit Manager to simplify compliance evidence collection.
- Case Study: Conducting a mock SOC 2 audit of a company?ÇÖs AWS environment, focusing on logging, monitoring, and access controls.

Module 8: Incident Response and Offensive Tools

- Introduction to Cloud Forensics and preserving evidence in a dynamic AWS environment.
- Mastering the Pacu Framework for automated AWS reconnaissance and exploitation.
- Hands-on with CloudGoat scenarios to practice end-to-end attack paths.
- Developing and deploying custom scripts for targeted security assessment
- Case Study: Utilizing forensic readiness to capture a snapshot of a compromised EC2 instance and analyze CloudTrail logs to determine the attacker's initial vector.

Training Methodology

Our training employs a highly practical, hands-on methodology, ensuring participants can immediately apply learned skills.

- Instructor-Led Sessions.
- Live Lab Environment
- Attack-Defend Scenarios.
- Case Study Analysis.
- Assessment.
- Role-Playing.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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