Certified in Hacking and Defending the Cloud Training

Duration: **4 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

As cloud adoption continues to accelerate and hybrid cloud environments become increasingly common, configuration weaknesses and access-control errors have become major security concerns. **Certified in Hacking and Defending the Cloud** provides a broad, practical approach to identifying, exploiting and remediating security weaknesses across AWS, Microsoft Azure and Google Cloud Platform.

This intensive four-day course places learners in the mindset of a real-world attacker while maintaining a strong defensive focus. Participants explore more than 25 attack techniques through advanced practical environments, supported by approximately **38 hands-on labs** and **10 demonstrations**.

The program is delivered by experienced penetration testers with direct exposure to cloud security assessments and offensive security engagements. Learners gain insight into how attackers discover cloud assets, abuse misconfigurations, escalate privileges and maintain access across cloud environments.

The training also places significant emphasis on detection and response. Participants learn how to identify cloud weaknesses, validate security fixes, apply cloud-native and open-source defensive controls, monitor cloud activity and establish stronger security baselines.

Attack surfaces associated with virtual machines, storage services, serverless functions, container platforms, IAM systems and metadata services are explored across the three major cloud platforms.

By the end of the course, learners will be better prepared to assess cloud deployments, recognise complex attack paths, validate remediation activities and apply practical defensive controls across modern cloud environments.

Prerequisites

To gain the most from the course, learners should have:

- Basic to intermediate cybersecurity knowledge
- Ideally at least 1.5 years of cybersecurity experience
- Familiarity with common command-line syntax

Certified in Hacking and Defending the Cloud Training

Duration: **4 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

This course is particularly suitable for:

- Cloud administrators and architects
- Penetration testers and red teamers
- Blue teams
- CSIRT and SOC analysts
- Incident responders
- Cloud developers and engineers
- Security and IT managers
- Technical team leads

It is also suitable for professionals with a wider responsibility or interest in cloud security who want to improve their ability to assess and protect AWS, Azure and GCP environments.

What You Will Learn

By the end of the course, learners will be able to:

- Think more like an advanced real-world threat actor.
- Identify complex vulnerabilities and cloud misconfigurations across AWS, Azure and GCP.
- Design penetration tests around realistic attacker behaviour and tooling.
- Assess the attack surface created by VMs, buckets, CaaS platforms and serverless services.
- Understand exploitation techniques used to gain initial access through exposed cloud services.
- Evaluate post-exploitation techniques for enumeration and data exfiltration.
- Compare defensive approaches across different cloud platforms.
- Support cloud defence strategies using patching, asset inventory and least-privilege controls.
- Monitor cloud environments with cloud-native and open-source security tools.
- Perform cloud auditing and benchmarking activities.
- Validate remediation actions in hardened cloud environments.

Training Approach

The course follows a **Defense by Offense** methodology. Techniques are based on offensive research and realistic cloud security engagements rather than purely theoretical examples.

Approximately 60% of the course is lab based.

Participants will:

- Work through realistic cloud attack flows
- Exploit and defend AWS, Azure and GCP environments
- Audit cloud configurations
- Validate fixes and remediation actions
- Take part in a Capture the Flag challenge
- Discuss real-world attack case studies with the instructor

Certified in Hacking and Defending the Cloud Training

Duration: **4 Day**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

Training Outline

Module 1: Introduction to Cloud Computing

This module establishes the core concepts required to understand cloud security.

- Introduction to cloud computing
- Importance of cloud security
- Shared Responsibility Model
- Comparison with conventional security models
- Importance of cloud metadata APIs from an attacker perspective

Module 2: Cloud Asset Enumeration

Learners explore techniques for identifying cloud assets from an external perspective.

- Importance of DNS in cloud environments
- DNS-based enumeration
- OSINT techniques for cloud asset discovery
- Username enumeration using cloud provider APIs

Module 3: Attack Surface of Cloud Services

The attack surfaces of common cloud delivery models are examined.

- Infrastructure as a Service (IaaS) attack surface
- Function as a Service (FaaS) attack surface
- Platform as a Service (PaaS) attack surface
- Container as a Service (CaaS) attack surface

Module 4: Cloud Storage

This module explores cloud storage security across AWS, GCP and Azure.

- Introduction to AWS S3
- AWS S3 misconfigurations
- Introduction to GCP Storage
- Introduction to Azure Storage
- Azure Shared Access Signature (SAS) URL misconfigurations

Module 5: Azure and Microsoft Entra ID Attacks

Azure services and identity infrastructure are examined in detail.

- Introduction to Azure and Microsoft Entra ID
- Attacks against App Service, Function App and Storage
- Azure Database
- Automation Account
- Azure Key Vault
- Microsoft Entra ID authentication methods
- Authentication risks
- Managed User Identity attacks

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- MFA and Conditional Access bypass scenarios
- Abuse of Dynamic Membership Policies
- Azure Identity Protection for monitoring user behaviour

Module 6: Introduction to AWS Security

This module covers advanced AWS security concepts and common attack paths.

- AWS IAM and policies
- AWS policy evaluation
- AWS Cognito
- IAM misconfigurations
- Elastic Beanstalk
- AWS cross-account misconfigurations
- Role enumeration using Pacu
- EC2 access through instance attribute abuse
- Resource-based policy misconfigurations
- Lambda and API Gateway exploitation
- AWS ECR and ECS
- Extracting sensitive information from Docker images
- AWS Organizations
- IAM Access Analyzer

Module 7: Introduction to GCP Security

Learners examine GCP identity, compute, storage and application security.

- Introduction to GCP
- IAM roles and service accounts
- Service Account file authentication
- Access token authentication
- Compute Engine
- Cloud Storage
- App Engine
- Identity-Aware Proxy (IAP)
- Firestore and Firebase
- Cloud Functions
- Pub/Sub
- Cloud Run
- IAM impersonation
- Secret Manager
- Container Registry

Module 8: Revisiting AWS, Azure and GCP Misconfigurations in a Hardened Environment

This module revisits major cloud weaknesses and focuses on validating remediation.

Fixes are tested across:

- Microsoft Entra ID
- Azure MFA
- Azure Key Vault

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Elastic Beanstalk
- AWS IAM
- ECS and ECR
- AWS Cognito
- GCP IAM
- GCP IAP

Module 9: Backdooring and Maintaining Access

This module explores persistence techniques within cloud environments and considers how defenders can recognise and respond to attempts to maintain unauthorised access.

Module 10: Differences Between AWS, Azure and GCP IAM

The identity and access management models of the three main cloud providers are compared.

- AWS IAM
- Azure and Microsoft Entra ID
- GCP IAM
- Key architectural differences
- Common IAM pitfalls
- Access-control risks

Module 11: Cloud Defence Using Open-Source and Cloud-Native Tools

Cloud defence is considered through four primary stages: identification, protection, detection and response.

- Identifying cloud assets
- Hybrid account asset inventory
- AWS multi-account inventory using open-source tools
- Protecting cloud assets
- Principle of Least Privilege
- Least-privilege examples across EC2, IAM and RDS
- Financial protection through cloud budgets
- Metadata API protection
- Metadata API protection using Linux firewall rules
- Monitoring cloud activity with cloud-native tools
- Hybrid cloud monitoring strategies
- Automated response to malicious cloud activity
- Responding to attacks using AWS Config and AWS Step

Module 12: Cloud Auditing and Benchmarking

The final module examines structured auditing and security baselines.

- Preparing for an audit
- Automated auditing with tools
- Practical auditing exercise
- Golden Image audits
- Docker Image audits
- Practical image auditing exercises

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Relevant cloud benchmarks
- CIS benchmark concepts

Top Three Takeaways

The course places particular emphasis on:

1. Exploitation techniques used to gain cloud access through exposed services
2. Post-exploitation techniques for enumeration and exfiltration
3. Defensive methods suitable for different cloud environments

Exam and Assessment

The examination is delivered through the APMG proctored examination platform.

Exam Format

- 60 questions
- Four multiple-choice answers per question
- One correct answer
- Four syllabus categories:
  - Azure
  - AWS
  - GCP
  - General cloud security
- 60-minute duration
- Closed book
- 50% pass mark