+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 09/17/2026

Sign Up

# GIAC GCPN Certification Training

5 days (35 hours)

## Overview

The GIAC GCPN Certification Training prepares you for the official GIAC Cloud Penetration Tester certification and validates your ability to conduct cloud penetration tests on modern environments.

The GIAC Cloud Penetration Tester certification assesses the skills needed to analyze the security of cloud systems, networks, architectures, and services. It covers environment discovery, the identification of attack surfaces, and the controlled exploitation of vulnerabilities in AWS, Azure, and cloud-native contexts.

Our GIAC GCPN Certification training course helps you structure your exam preparation, master the assessed topics, and reinforce the expected reasoning methods. You'll learn how to map a cloud target, assess identities and permissions, analyze exposed configurations, and document realistic attack scenarios.

You will study attacks on cloud services, web applications, serverless functions, containers, and CI/CD pipelines. The hands-on workshops allow you to practice reconnaissance, privilege escalation, pivoting, bypass, and remediation techniques within a controlled environment.

Upon completion of the training, you will be able to approach the exam with an effective strategy, identify areas that need review, and apply the skills validated by the GIAC Cloud Penetration Tester certification in cloud penetration testing engagements.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

## Objectives

- Master the exam topics and format of the GIAC Cloud Penetration Tester exam
- Map an attack surface in AWS and Azure environments
- Assess exposed identities, permissions, configurations, and cloud services
- Analyze risks associated with cloud-native applications, containers, and CI/CD pipelines
- Apply an ethical cloud penetration testing methodology and produce remediation recommendations
- Develop an effective preparation strategy for the certification

# Target Audience

- Penetration Tester
- Cybersecurity consultant
- Vulnerability analyst
- Cloud security engineer
- DevOps Engineer

# Prerequisites

- Hands-on experience with penetration testing and network reconnaissance
- Knowledge of AWS or Azure services, identities, and permissions
- Proficiency with Linux commands and the basics of Python or Bash scripting
- Understanding of network protocols, HTTP, DNS, and TLS
- Basic understanding of Docker container security and CI/CD pipelines

# Technical Prerequisites

- Isolated AWS and Azure lab environments with accounts, IAM roles, and permissions set up for penetration testing scenarios
- Linux environment equipped with AWS and Azure CLIs and the offensive security tools used during the exercises
- Kubernetes cluster and container environment dedicated to cloud-native security exercises
- Demo Git repositories and CI/CD pipelines configured for analysis and exploitation

# GIAC GCPN® Training Program

## [Day 1 - Morning]

### Certification framework and cloud penetration testing methodology

- Overview of the GIAC Cloud Penetration Tester certification, assessed domains, and validated skills

- Understanding the exam format, time management, and the systematic use of authorized resources
- Principles of cloud penetration testing, legal framework, rules of engagement, and scope of authorization
- The lifecycle of an offensive audit, from reconnaissance to reporting results
- Modeling shared responsibilities and attack surfaces in the cloud

[Day 1 - Afternoon]

## Reconnaissance and mapping of cloud environments

- Public intelligence gathering, digital fingerprinting, and identification of exposed assets
- Discovery of domains, subdomains, IP addresses, web services, and API endpoints
- Enumeration of accessible cloud resources and analysis of metadata useful for penetration testing
- Prioritizing targets based on their exposure, criticality, and possible attack vectors
- Creating an actionable map for practical exercises and exam questions
- Hands-on workshop: mapping the attack surface of a fictional organization and producing a prioritized inventory of cloud assets

[Day 2 - Morning]

## AWS Identities, Permissions, and Attacks

- Review of AWS IAM identity models, roles, policies, and authentication mechanisms
- Searching for exposed secrets, access keys, temporary tokens, and credentials
- Analysis of configuration errors related to permissions, service roles, and approval relationships
- Enumerating AWS services and identifying privilege escalation vectors
- Best practices for remediation, the principle of least privilege, and logging of sensitive actions

[Day 2 - Afternoon]

## Storage, Networking, and Exposure of AWS Services

- Security assessment of AWS object storage, volumes, snapshots, and backups
- Analysis of security groups, network access control lists, routes, and exposed entry points
- Identifying weak configurations in compute and managed services
- Identifying risks related to instance metadata and roles associated with workloads
- Review of certification scenarios covering access paths and business impacts
- Hands-on workshop: Analyze an AWS lab environment, identify misconfigurations, and propose a prioritized remediation plan

[Day 3 - Morning]

## Azure Identities, Resources, and Attacks

- Microsoft Entra ID Identity Architecture, Roles, Applications, and Service Principals
- Mapping relationships between identities, subscriptions, resource groups, and Azure workloads
- Assessing excessive permissions, application consents, and service account secrets
- Discovery of Azure resources and analysis of common service exposures
- Identifying defense mechanisms, logging, and privilege restriction

[Day 3 - Afternoon]

## Attack scenarios and pivoting in Azure

- Analysis of attack vectors on virtual machines, storage accounts, functions, and web services
- Controlled exploitation of exposed secrets, delegated permissions, and vulnerable network configurations
  vulnerabilities
- Pivoting, relay, and obfuscation techniques tailored to an authorized cloud environment
- Correlation of technical findings with risks to data and business services
- Preparation of synthetic responses to exam-style scenarios
- Hands-on workshop: Follow an Azure attack path in the lab, from an exposed identity to access a sensitive resource

[Day 4 - Morning]

## Web applications and cloud-native services

- Specific characteristics of attacks on web applications deployed in the cloud
- Analysis of vulnerabilities related to authentication, access control, injection, and session management
- Analysis of APIs, API gateways, and serverless functions
- Understanding command redirection, proxy, bypass, and obfuscation mechanisms
- Identification of application security controls and remediation strategies

[Day 4 - Afternoon]

## Containers, orchestration, and CI/CD pipelines

- Attack surface of images, registries, containers, and orchestration platforms
- Searching for secrets, excessive privileges, and configuration errors in manifests and images
- Risks associated with service accounts, mounted volumes, and inter-service communications
- Security assessment of CI/CD pipelines, code repositories, and delivery mechanisms
- Implementation of appropriate prevention, detection, and hardening controls
- Hands-on workshop: auditing a CI/CD pipeline and a containerized deployment to identify at-risk secrets and privileges

[Day 5 - Morning]

### Skill consolidation and exam strategy

- Comprehensive review of objectives: authentication, cloud services, identities, applications, and cloud-native technologies
- Analysis of certification case studies involving AWS, Azure, web applications, and containers
- Techniques for reading questions, evaluating clues, and eliminating irrelevant answers
- Organizing a review index and quickly identifying concepts that need reinforcement
- Managing time, overcoming roadblocks, and tracking progress during the proctored exam

## [Day 5 - Afternoon]

### Certification simulation and debriefing

- Solving scenarios covering discovery, exploitation, pivoting, and remediation
- Group review of technical reasoning and clarification of sensitive concepts
- Review of common errors related to identities, storage, networks, and managed services
- Final preparation for the GIAC Cloud Penetration Tester certification exam
- Development of an individual review plan following the training
- Hands-on workshop: Conduct a simulation of a complete cloud penetration test, then justify technical choices and recommendations

# Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

# Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

# Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

# Organization

The course alternates between theoretical input from the instructor, supported by examples and

reflection sessions and group work.

## Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

## Certification

A certificate will be issued to each trainee who has completed the entire training program.