SEC588: **Cloud Penetration Testing™**

GCPN
Cloud Penetration Tester
giac.org/gcpn

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Conduct end-to-end IaaS, PaaS, and SaaS Penetration Testing Scenarios
- Learn modern attack techniques in real-world ranges
- Build a methodology to assess weaknesses in Cloud Environments
- Modern attacks on Microsoft and AWS Environments
- Use Modern C2 Toolsets to move laterally in Cloud Environments

"Meticulously designed, SEC588 balances in-depth theory with practical labs, addressing today's pivotal cloud security challenges. This course is indispensable for security professionals seeking cutting-edge knowledge."

—Armin Iraqi, **Fortum**

GCPN
Cloud Penetration Tester
giac.org/gcpn

GIAC Cloud Penetration Tester

The GIAC Cloud Penetration Tester (GCPN) certification validates a practitioner's ability to conduct cloud-focused penetration testing and assess the security of systems, networks, architecture, and cloud technologies.

- Cloud Penetration Testing Fundamentals, Environment Mapping, and Service Discovery
- AWS and Azure Cloud Services and Attacks
- Cloud Native Applications with Containers and CI/CD Pipelines

SEC588 training is a specialized course that focuses on penetration testing in Cloud environments. The course itself is part of both the Offensive Operations and Cloud Curricula. It equips Penetration Testers, Red Team Operators, Cloud Practitioners, Cloud Architects, and those involved in incident response with the tools to assess and operate in various cloud environments. The course features AWS, Azure, Microsoft 365, and Kubernetes to provide students with hands-on experience across the broadest range of environments, ensuring comprehensive coverage. Apply offense and defense capabilities in the cloud immediately.

Be Ready to Test Tomorrow's IT Landscape

SEC588 training is designed around testing and assessment of environments as they move from legacy Data Centers into the more modern Cloud Infrastructure. Some of our students come from environments that utilize hybrid cloud, fully cloud-based, or purely SaaS applications. Evaluating how these systems are integrated into the business becomes increasingly important to organizations. Students will learn how to perform assessment work on both the identity layer and the infrastructure layer of cloud infrastructure.

SEC588 training prepares you to confront scenarios that we increasingly see in penetration testing, focusing on the components that are most encountered and asked about. The methodologies are flexible enough to be applied to other types of clouds, as many of their similarities are exposed.

A big focus of the class is on hands-on labs, in environments that are typically difficult to set up and expensive to operate. The students will spend 50% of the class time in their labs. Students will also be able to apply the course content to the practical applicability directly in those labs. Many multipart labs increase the learner's ability by simulating challenging operational environments.

In the SEC588 course, we only use toolsets that have a proven record and have been used in real-world engagements. This provides students with the ability to fulfill the SANS promise of being able to return to the workplace and immediately apply what was learned in the course. Whether you are a consultant looking to enhance your own skill set or are on the defensive side, seeking to build detections, we believe SEC588 Cloud Penetration Testing will make your training investment immediately valuable day one.

Author Statement

When this course was first launched in April 2020, the concept of cloud penetration testing was a known yet still emerging and specialized field, gaining significance as a key area of concern. In 2025, to address the continually evolving landscape and focus, the course underwent its fifth and most substantial update to date. My goal was to incorporate as many real-world assessment methods as possible across various cloud platforms, a commitment we will maintain until the pace of innovation in this field decelerates. Ultimately, I hope this class will continue to empower both the red and blue teams to build stronger defenses and enhance the security of these environments.

—Moses Frost

Section Descriptions

SECTION 1: Architecture, Discovery, and Recon at Scale

How do clouds work? How do the offensive teams operate in these environments? What are the limits of testing? How do we scan for vulnerabilities externally and internally in a safe manner? The first section of the course is designed to help the student begin their Cloud Assessment journey.

TOPICS: Cloud Architectures for Scoping a Test; External Network Discovery Using The Asset Discovery Pipeline; Internal Cloud Vulnerability Scanning; Cloud Authentication Overview

SECTION 2: Attacking Identity Systems

While Section 1 covered the mechanisms for starting and evaluating an environment, Section Two deals with a core component of the cloud. Identity Systems are core to most cloud environments, so we dedicate a whole section to evaluating them. This includes a comprehensive evaluation of Microsoft Entra ID and its key strengths.

TOPICS: Authentication Standards; Microsoft Cloud Services and Entra ID; Malicious App Consents; Microsoft Graph; File Storage Attacks

SECTION 3: Attacking and Abusing Cloud Services

In Section 3, students will attack the cloud infrastructure assets. Students will learn how to leverage these assets to navigate cloud environments further, elevate privileges, and persist. Cloud Infrastructures can be highly complex, and in that complexity, the students will learn how to navigate and assess the risk each attack path poses.

TOPICS: Compute Attack Scenarios; AWS IAM and Privilege Escalations; Using AWS Attack Tools and C2; Azure Compute; Code Execution in Azure

SECTION 4: Vulnerabilities in Cloud Native Applications

Section 4 will walk the students through workloads in the cloud. Applications in the cloud are one of the most common workloads in the cloud, beyond internal data center migration. One of the key features of many of these applications is their cloud-integrated nature. Learning how to assess these systems will be crucial during assessment work.

TOPICS: Infrastructure as Code and CI/CD Attacks; Web Applications and API Attacks; Common Web Attack Paths; Attacking Serverless Functions; Databases, Datalakes, and LLMs

SECTION 5: Infrastructure Attacks and Red Teaming

Section 5 provides the student with an overview of infrastructure core components that are cloud-agnostic. Containers comprise a significant portion of cloud workloads. This section provides students with a methodology for assessing container and container workloads. The section concludes with an assessment of work on Kubernetes.

TOPICS: Red Team Operations in the Cloud; Containers, Docker, and Docker Vulnerabilities; Kubernetes; Backdooring Workloads

SECTION 6: Capstone Event

In a final capstone event, we demonstrate cloud penetration testing's unique demands and the specialized expertise required to go beyond traditional security assessments. Students collaboratively bring their new knowledge to bear on a simulated end-to-end test, reinforcing theory and practice and producing an effective, readable report.

"This emerging course perfectly complements the change in the direction of red team engagement scopes."

—Kyle Spaziani, **Sanofi**

Who Should Attend

SEC588 training is recommended for:

- Penetration testers, Red Team operators, or offensive roles wanting to expand their cloud assessment knowledge
- Systems architects, engineers, and operators who want to harden their environments to the latest cloud attacks
- Systems integrators and manufacturers that are building offensive and defensive products
- People, leaders, and managers who wish to understand the current cloud-attack landscape better

NICE Framework Work Roles

- Security Control Assessor (OPM 612)
- System Testing and Evaluation Specialist (OPM 671)
- Vulnerability Assessment Analyst (OPM 541)
- Pen Tester (OPM 541)
- Cyber Ops Planner (OPM 332)

"SANS course SEC588 taught me more than I expected. With the rapid development of new technologies offered by cloud providers, SEC588 has given me an important framework for cloud pen testing."

—Jonus Gerrits, **Phillips 66**