SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

SEC588: **Cloud Penetration Testing**

GCPN
Cloud Penetration Tester
giac.org/gcpn

6	36	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Conduct cloud based penetration tests
- Assess cloud environments and bring value back to the business by locating vulnerabilities
- Understand first-hand how cloud environments are constructed and how to scale factors into the gathering of evidence
- Assess security risks in Amazon and Microsoft Azure environments, the two largest cloud platforms in the market today

GCPN
Cloud Penetration Tester
giac.org/gcpn

GIAC Cloud Penetration Tester

“The GIAC Cloud Penetration Testing (GCPN) certification provides our industry with a first focused exam on both cloud technologies and penetration testing disciplines. This certification will require a mastery in assessing the security of systems, networks, web applications, web architecture, cloud technologies, and cloud design. Those that hold the GCPN have been able to cross these distinct discipline areas and simulate the ways that attackers are breaching modern enterprises.”
— Moses Frost, Course Author SEC588: Cloud Penetration Testing

- 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

Aim Your Arrows To The Sky And Penetrate The Cloud

You have been asked to perform a Red Team penetration test assessment. The assets are located mainly in the cloud. What if you have to assess Azure Active Directory, Amazon Web Services (AWS) workloads, serverless functions, or Kubernetes? In this course, you will learn the latest penetration testing techniques focused on the cloud and how to assess cloud environments.

Computing workloads have been moving to the cloud for years. Analysts predict that most if not all companies will have workloads in public and other cloud environments very soon. While organizations that start in a cloud-first environment may eventually move to a hybrid cloud and local data center solution, cloud usage will not decrease significantly. So when assessing organizations’ risks going forward, we need to be prepared to evaluate the security of cloud-delivered services.

The most commonly asked questions regarding cloud security are “Do I need training for cloud-specific penetration testing?” and “Can I accomplish my objectives with other pen test training and apply it to the cloud?” The answer to both questions is yes, but to understand why, we need to address the explicit importance of conducting cloud-focused penetration testing. In cloud-service-provider environments, penetration testers will not encounter a traditional data center design. Specifically, what we rely on to be true in a formal setting such as who owns the Operating System and the infrastructure, and how the applications are running will likely be very different. Applications, services, and data will be hosted on a shared hosting environment unique to each cloud provider.

SEC588: Cloud Penetration Testing draws from many skill sets that are required to properly assess a cloud environment. If you are a penetration tester, the course will provide a pathway to understanding how to take your skills into cloud environments. If you are a cloud-security-focused defender or architect, the course will show you how the attackers are abusing cloud infrastructure to gain a foothold in your environments.

The course dives into topics of classic cloud Virtual Machines, buckets, and other new issues that appear in cloud-like microservices, in-memory data stores, files in the cloud, serverless functions, Kubernetes meshes, and containers. The course also covers Azure and AWS penetration testing, which is particularly important given that AWS and Microsoft account for more than half of the market. The goal is not to demonstrate these technologies but rather to teach you how to assess and report on the actual risk that the organization could face if these services are left insecure.

> **“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**

> **“This emerging course perfectly complements the change in the direction of red team engagement scopes.”**
>
> —Kyle Spaziani, **Sanofi**

sans.org/sec588

- **Watch a preview of this course**
- **Discover how to take this course: Online, In-Person**

Section Descriptions

SECTION 1: Architecture, Discovery, and Recon at Scale

In this initial course section you will conduct the first phases of a cloud-focused penetration testing assessment. We'll get familiar with how the terms of service, demarcation points, and limits imposed by cloud service providers function. The section features labs on how to perform scans and discovery jobs at Internet scale that can be used in near real-time and through historical searches to uncover target infrastructure and vulnerabilities. We'll also describe how web-scale affects reconnaissance and how to best address it. The exercises are designed to walk you through how to discover valuable artifacts a virtual hacker treasure hunt!

TOPICS: Cloud Assessment Methodology; Infrastructure Cloud Components; Terms of Service and Demarcation Points; Recon at Cloud Scale; IP Addressing and Hosts in Cloud Service Providers; Mapping URLs to Services; Commonspeak2 and Wordlists; Visualizations Aids; Asset Discovery Frameworks

SECTION 2: Attacking Identity Sessions

This course section will have students work on identity and access management systems that include AWS IAM, Azure Active Directory, and standards-based protocols that underpin these technologies. Students will discover their target range environments and use the technologies to start finding entry points into systems. We'll also walk through standard identity systems for federated SSO, including Azure Active Directory and the underlying Oauth and SAML protocols. Students will learn how to perform username harvesting, look for authentication and unauthenticated file shares, and use standard tooling to automate discovery. We'll also dive into using developer tools such as Postman against systems.

TOPICS: The Mapping Process; Authentications and Key Material; AWS Command Line Interface (CLI) Introduction; Azure CLI Introduction; Username Harvesting; Unauthenticated Fileshares; Microsoft Identity Systems and Azure Active Directory; Authentication Standards in the Web; SAML and Golden SAML; Introduction to Postman

Who Should Attend

- Both attack and defense-focused security practitioners will benefit greatly from this course by gaining a deep understanding of vulnerabilities, insecure configurations, and associated business risk to their organizations
- Penetration testers
- Vulnerability analysts
- Risk assessment officers
- DevOps engineers
- Site reliability engineers

SECTION 3: Attacking and Abusing Cloud Services

Cloud infrastructure lends itself to the potential for priviledge escalation through mechanisms that are afforded to systems administrators and developers. We can abuse these features to move laterally, escalate priviledges, or change our permission sets. This course section walks students through several Compute automation structures in which we are able to perform attacks on cloud targets to show each use case. This course section is very heavy on labs to enforce the concepts of how these attacks operate with or without attacker tools.

TOPICS: Mimikatz and PRT; Microsoft Graph for Data Exfiltration; AWS IAM Privilege Escalation Paths; AWS Compute; Amazon KMS and Keys; PACU for AWS Attack Automation; Azure Virtual Machines; Code Execution on Azure VMs

SECTION 4: Vulnerabilities in Cloud Native Applications

This course section focuses on what are referred to as cloud-native applications. While we look in particular at web applications themselves, the section is designed to show how cloud-native applications operate and how we can assess them. Applications in the wild are increasingly container-packaged and microservice-oriented. These applications will have their nuances. They will typically be deployed in a service mesh that at times could indicate a system like Kubernetes is being used. We will be exploring many questions in this section, including:

- Which application vulnerabilities are very critical in my environments?
- How does Serverless and Lambda change my approach?
- What is the continuous integration/continuous delivery (CI/CD) pipeline, and how can it be abused?
- How do microservice applications operate?

TOPICS: TravisCI and Git Actions; Deployment Pipelines; Web Application Injections; Server Side Request Forgeries and Their Impacts; Command Line Injections; Serverless Functions in AWS; Serverless Functions in Azure; Exposed Databases and Ports; SQL Injections in Cloud Applications

SECTION 5: Infrastructure Attacks and Red Teaming

This course section explores the world of Kubernetes and infrastructures, then dives into exploitation and red teaming in the cloud. By this point in the course you have a base understanding of our target environments. From that vantage point, we will explore how to exploit what we have found, advance further into the environments, and finally move around laterally. This section will focus on breaking out of containers, understanding service meshes, and exfiltrating data in various ways to show the real business impact of these types of attacks.

TOPICS: Kubernetes and Kubernetes Clusters; Leveraging Backdoors in Clusters; Red Team and Methodologies; Heavy and Lite Shells; Data Smuggling; Domain Fronting; Avoiding Detections

SECTION 6: Capstone Event

On your final course day, be prepared to work as a team and complete an end-to-end assessment in a new cloud environment. The applications and settings are all newly designed to imitate real-world environments. This course section is designed to allow students to put together the week's worth of knowledge, reinforce theory and practice, and simulate an end-to-end test. It is also a capstone event, as we will be asking students to write a report using a method that is easy to read for both developers and administrative staff. We will provide students with a few rubrics and ways to work through the scenarios. There are always new and novel solutions, and we like students to share what they have learned and how they did what they did with one another.