SEC588: **Cloud Penetration Testing**

6 Day Program	36 CPEs	Laptop 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

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 in the very near future. 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 it comes to assessing risk to organizations, we need to be prepared to assess the security of cloud-delivered services. In this course you will learn the latest in penetration testing techniques focused on the cloud and how to assess cloud environments.

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 having 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 traditional setting - such as who owns the Operating System, who owns 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 that is potentially unique to each cloud provider.

What makes cloud native different? The Cloud Native Computing Foundation, which was chartered to provide guidance on what is a cloud-first and cloud-native application, states that the application and environment will be composed of containers, service meshes, microservices, immutable infrastructure, and declarative APIs.

While some of these items are available in a non-cloud environment, in the cloud these features are further decomposed into services that are made available by cloud providers. In this environment, an example of complexity is a microservices architecture in which there may be a virtual machine, a container, or even what is considered a “serverless” hosting area. We must therefore deal with additional complexity in order to appropriately assess this environment, stay within the legal bounds, and learn new and different ways to perform what we would consider legacy attacks.

SEC588 dives into these topics as well as other new topics that appear in the cloud like microservices, in-memory data stores, files in the cloud, serverless functions, Kubernetes meshes, and containers. The course also specifically covers Azure and AWS penetration testing, which is particularly important given that Amazon Web Services 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 true risk that the organization could face if these services are left insecure.

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Section Descriptions

SECTION 1: Discovery, Recon, and Architecture at Scale

In this course section you will be conducting 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. There are labs on how open databases and Internet-level scans can be used in near real time as well as historically to uncover target infrastructure and vulnerabilities. In this course section we'll describe how web scale affects reconnaissance and how we can best address it. The exercises are designed to walk through the discovery of useful artifacts and the labs themselves throughout the course – a virtual hacker treasure hunt!

TOPICS: Cloud Assessment Methodology; Infrastructure Cloud Components; Terms of Service and Demarcation Points; Domains and Certificates for Enumeration; Host Discovery with MassCAN and Nmap; Git Mirroring; Services and Databases in the Cloud; Recon and Discovery through Visual Tracking

SECTION 2: Discovery, Authentication, and Cloud Services

In this course section we'll show the differences between mapping at the port level, application-level, and infrastructure mapping through cloud-service-provider APIs. The section features labs designed to show how we can go from outer to inner reconnaissance and discovery. We'll then shift to three very important and interrelated topics: authentication and authorization in APIs, identifying undisclosed APIs and how they can be used, and how to abuse privilege and identity management. Amazon Web Services and other cloud providers have adopted an RBAC system to which many of their services can turn to for authorization checking. The last part of this section will cover privileges in RBAC and how we can abuse them to elevate privileges. Our labs will show how a low-privilege user can run lambda functions, enumerate s3 buckets, execute ec2 instances, and even decrypt sensitive data.

TOPICS: APIs; Cloud SDKs; AWS IAM and Privileges; Building and Using Powerful Wordlists; Turning Tokens into Access; Persistence through AWS IAM

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: Windows in the Cloud with Azure

While Amazon Web Services holds the largest share of the market, many large enterprises are moving their on-premise workloads into the cloud. Microsoft Azure, while being equivalent to many other cloud providers, also has some unique services that are used. Azure Active Directory and other user services such as Office365, Exchange, and even Microsoft Graph are unique in their services. This section will introduce you to an Azure Environment in which we have provided Windows machines, containers, and services. As during the previous course sections, the environments are live and running, and each has its own set of artifacts to run through. We will leverage similar CLI tooling to take over Azure services in a controlled manner.

TOPICS: Azure Active Directory; VHD and Volume Shadow Copies; SAML and Microsoft ADFS; Windows Containers; Azure Roles; Microsoft Graph API; Office365

SECTION 4: Vulnerabilities and Exploitation of Cloud Native Applications

The fourth section of this course focuses on what are referred to as cloud native applications. While the instruction particularly examines web applications themselves, it is designed to show how cloud native applications operate and how we can assess them. More and more, what we see being created in the wild are applications that are container-packaged and microservice-oriented. These applications will have their nuances. They will typically be deployed in a service mesh at times that could indicate a system like Kubernetes is 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?
- How does managed and unmanaged Kubernetes change my testing?
- How do microservice applications operate?
- What is the CI/CD pipeline and how can it be abused?

TOPICS: AWS IAM Metadata Discovery; Kubernetes and Escapes; TravisCI and Git Actions; Moving Laterally Across Containers; Privileged and Unprivileged Containers

SECTION 5: Red Team in the Cloud

The final section of this course explores the world of exploitation and red teaming in the cloud. By this time we have a very good understanding of our target environments, and as such we will explore how we can exploit what we have found, advance further into the environments, and finally how to move around laterally. This includes breaking out of containers and service meshes and exfiltrating data in various ways to show the real business impact of these types of attacks.

TOPICS: Red Team and Methodologies; Heavy and Lite Shells; Data Smuggling; Avoiding Detections

SECTION 6: Capstone

Be prepared on your last day to work as a team and complete an end-to-end assessment in a new cloud environment. The applications and environments are all newly designed to imitate real-world environments. This day is designed to allow students to put together the week's worth of knowledge, reinforcing theory and practice, and simulating 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 each other.