COURSE PROFILE:

Hacking Cloud Infrastructure

2 days | **Intermediate training**

Version 6

claranet cyber security

NotSoSecure Training

Your course

With the rapid adoption of cloud infrastructure and the prevalence of hybrid cloud environments among organizations, the need to address cloud misconfigurations has become paramount. This course offers a holistic approach to understanding and mitigating misconfigurations in AWS and Azure.

From building and migrating to managing and innovating in the cloud, organizations face increasing pressure to secure their cloud infrastructure effectively. To achieve this, a deep understanding of cloud attack architecture and hands-on experience with relevant tools and techniques are essential.

This comprehensive 2-day course immerses participants in the attacker's mindset, providing the opportunity to deploy over 20 novel attacks through state-of-the-art labs. The training is delivered by seasoned penetration testers with extensive experience in cloud hacking, gained through real-world engagements.

By the end of the course, participants will be well-equipped to confidently identify vulnerabilities within cloud deployments. This course is a crucial step toward enhancing cloud security in an ever-evolving threat landscape.

Who is it for?

- **Cloud administrators and architects**
- **Penetration testers and red teamers**
- **CSIRT/SOC analysts and engineers/blue teams**
- **Developers**
- **Security/IT managers and team leads**

This course is suitable for anyone with a stake or interest in cloud security, from technical practitioners to decision makers. The syllabus has been designed to cover the cloud misconfigurations and advances in hacking, as well as the skills to penetration test cloud systems and environments and remediate vulnerabilities.

Delegates must have the following to make the most of the course:

- **Basic to intermediate knowledge of cybersecurity (1.5+ years' experience)**
- **Experience with common command line syntax of cloud CLI**

Top 3 takeaways

- **Exploit labs in a kill-chain style and escalate privilege by exploiting multiple services**
- **Understand how to perform enumeration to identify different misconfiguration in the cloud environment**
- **Gain an understanding of Shadow Admin permissions and acquire skills on leveraging these permissions to elevate your privileges**

What you will learn

This course uses a Defense by Offense methodology based on real world engagements and offensive research (not theory). That means everything we teach has been tried and tested on live environments and in our labs and can be applied once the course is completed. By the end of the course, you'll know how to:

- **Think and behave like an advanced, real-world threat actor**
- **Identify and exploit complex vulnerabilities and security misconfigurations in AWS and Microsoft Azure**
- **Design your penetration tests around real-world attacker behaviors and tooling, making it relevant to the threats facing your organization**
- **Identify the attack surface exposure created by cloud-based services such as virtual machines (VMs), buckets, container as a service (CaaS) platform, and serverless functions**

What you will be doing

You'll be learning hands on:

- **Spending most of the session (~60%) on lab-based exercises**
- **Using lab-based flows to explore and hack lifelike cloud environments**
- **Exploiting, defending, and auditing different cloud environments**
- **Competing in a Capture the Flag (CTF) challenge to test your new skills**
- **Discussing case studies with your course leader to understand the real-world impact of the hacks covered**

Why it is relevant

The cybersecurity skills shortage is felt perhaps nowhere as deeply as in the cloud. With new rulebooks and standards, practitioners often find themselves playing catch up with the latest developments in technology and in the threat landscape. This course is designed to be a highly informative bootcamp to help you advance your skills in the most important and relevant areas of cloudsec. Across 2 days, you'll learn about the high-impact vulnerabilities and flaws that could be open in your organization right now and how to fix them.

Our syllabuses are revised regularly to reflect the latest in-the-wild hacks, the newest system releases, and whatever proof of concepts we've been developing in our own research. Because they remain so up to date with the threat landscape and security industry standard, **many delegates return every 1-2 years** to update their skills and get a refresh.

What is in the syllabus

Note: our syllabuses are subject to change based on new vulnerabilities found and exploits released.

MODULES	WHAT YOU WILL LEARN
INTRODUCTION TO CLOUD COMPUTING	This module introduces the core concepts of cloud computing, emphasizing the importance of security. It explores the shared responsibility model, comparing cloud security with traditional models. Additionally, it sheds light on the significance of cloud metadata APIs from an attacker's perspective. This module lays the groundwork for a deeper understanding of cloud security and its unique challenges • Introduction to the Cloud • Importance of Cloud Security • Shared Responsibility Model in the Cloud • Comparison with Conventional Security Model • Importance of Cloud Metadata API from an Attacker's perspective
CLOUD ASSET ENUMERATION	This module will explore DNS-based Enumeration techniques, gaining insights into identifying cloud assets through DNS records. The module then delves into "OSINT Techniques for Cloud Asset Enumeration," equipping participants with open-source intelligence methods to uncover valuable information. Additionally, it covers "Username Enumeration using Cloud Provider APIs," empowering attendees to utilize cloud provider APIs to enumerate usernames effectively. • Importance of DNS in the Cloud • DNS-based Enumeration • Open-Source Intelligence Gathering (OSINT) techniques for Cloud Asset Enumeration • Username enumeration using Cloud provider APIs
CLOUD STORAGES	This module covers cloud storage security in AWS, GCP and Azure. It starts with an introduction to AWS S3, followed by addressing AWS S3 misconfigurations. The module then explores GCP and Azure storage solutions. It culminates with a focus on securing Azure's Shared Access Signature (SAS) URLs. Attendees will gain the knowledge and skills to secure their cloud storage effectively, avoiding common pitfalls and optimizing data protection in these cloud environments. • Introduction to AWS S3 • AWS S3 misconfigurations • Introduction to GCP Storage • Introduction to Azure Storage • Azure: Shared Access Signature (SAS) URL Misconfiguration

INTRODUCTION TO AZURE AND ATTACKING MICROSOFT AZURE AD

This Module commences with an "Introduction to Azure and Microsoft Entra ID," setting the foundation for understanding Azure security.
The module extensively covers "Azure Application Attacks" across critical components such as App Service, Function App, and Storages. Participants will also delve into the intricacies of securing Azure Databases and the significance of the Automation Account, Azure Key Vault, a pivotal component in safeguarding sensitive data, is thoroughly explored.
Additionally, this module introduces "Microsoft Entra ID" and elaborates on its authentication methods and associated risks. Participants will gain insights into potential attacks on Microsoft Entra ID, particularly concerning Managed User Identities. The training provides advanced techniques for bypassing Multi-Factor Authentication (MFA) security and navigating Conditional Access Policies effectively.
Participants will also learn how to exploit Dynamic Membership Policies and harness Azure Identity Protection to monitor user behaviour, enhancing the overall security posture

- Introduction to Azure and Microsoft Entra ID
- Azure Application Attacks on App Service, Function App and Storages
- Azure Database
- Automation Account
- Azure Key Vault
- Introduction to Microsoft Entra ID authentication methods and risks
- Microsoft Entra ID Attacks (Managed User Identities)
- Bypassing MFA Security and Conditional Access Policy
- Abusing Dynamic Membership Policy

INTRODUCTION TO AWS

This module offers an in-depth exploration of advanced Amazon Web Services (AWS) security topics. Beginning with an Introduction to AWS Identity and Access Management (IAM) and Policies, the module explores policy evaluation and AWS Cognito Service, with a focus on potential IAM misconfigurations.

The training delves into various aspects of AWS security, including Elastic Beanstalk, AWS Cross-Account misconfigurations, and the enumeration of roles using Pacu. Participants will gain insights into gaining access to EC2 instances by exploiting instance attributes and addressing resource-based policy misconfigurations.

Additionally, the module covers Lambda and API Gateway exploitation, AWS Elastic Container Registry (ECR), and Elastic Container Service (ECS). It educates participants on protecting sensitive data within Docker images and introduces AWS Organizations and IAM Access Analyzer.

Upon completion of this Module, attendees will emerge with a deep understanding of advanced AWS security practices and the practical skills required to secure cloud environments effectively. This module is designed to empower individuals to proactively address security challenges with AWS infrastructures.

	• Introduction to AWS IAM and Policies • Understanding AWS Policy Evaluation • AWS Cognito Service • IAM: Misconfigurations • Elastic Beanstalk • AWS Cross-Account Misconfigurations • Enumerate roles using Pacu • Gaining access to EC2 instance by abusing instance attribute • Resource based policy misconfiguration • Lambda and API Gateway exploitation • IAM Access Analyzer
DIFFERENCE BETWEEN AWS, AZURE & GCP IAM AND PITALLS	This module offers a concise comparison of Identity and Access Management (IAM) in AWS, Azure, and GCP. It illuminates the key differences and potential pitfalls associated with IAM in these cloud platforms. Participants will gain insights into the nuanced IAM features and challenges specific to each provider, equipping them with a solid understanding to navigate and secure access control effectively.

What you will get

- **Certificate of completion**
- **30 days lab access post-course completion (with the opportunity to extend)**
- **8 Continuing Professional Education (CPE) credits awarded per day of training fulfilled**
- **Learning pack, including question & answer sheets, setup documents, and command cheat sheets**

Course highlights

What delegates love:

- **Our labs:** probably the biggest selling point for our courses. Not only will you spend most of the course hacking hands-on in a lifelike web environment, but you'll also have 30+ days access to practice your new skills afterwards.
- **Individual access:** you'll have your own infrastructure to play with, enabling you to hack at your own speed.
- **Real-world learning:** where many leading cybersecurity training courses are based on theory, our scenario-led, research-based approach ensures you learn how real threat actors think and act.
- **Specialist-led training:** you'll learn from highly skilled and experienced practicing penetration testers and red teamers.
- **Up-to-date content:** our syllabus remains so relevant, delegates come back year after year for more.
- **Remediations included:** you'll learn how to fix as well as find vulnerabilities.

Outcomes for budget holders

This course is designed to bring your in-house cloud security testing competency up to the industry standard, helping you:

- **Lower the likelihood of security incidents by identifying weaknesses in your cloud infrastructure**
- **Improve your understanding of the organization's risk posture based on the frequency and severity of weaknesses identified**
- **Improve the organization's approach to access control management**
- **Create a stronger case for securing software development, cloud deployment, and governance practices**
- **Develop a secure cloud roadmap that balances growth and risk**
- **Implement cloud-based attack detection and response tactics**
- **Build a closer relationship between development and security teams**
- **Internally pentest new tools and systems before making an investment**
- **Nurture and retain passionate, highly skilled, and security conscious employees**
- **Demonstrate commitment to security through training, compliance, and change management**
- **Develop the organization's competitive advantage for security-conscious customers**

WHY NOTSOSECURE?

We **hack**. We **teach**.

NotSoSecure is Claranet's dedicated training division and part of its global penetration testing practice. We're one of the largest training partners at Black Hat and a respected provider of web, mobile, and network penetration testing.

All our trainers are experienced, practicing, accredited penetration testers with their own field of excellence. This translates into our course syllabuses, where each module is designed around real-world engagements and in-the-wild research. No other provider of cybersecurity training is modelled in this way. The delegates we train leave our courses armed with knowledge and skills based on current and authentic attacker tactics and tradecraft, not theory alone.

It's our mission to help organizations raise the bar when it comes to their cybersecurity, and to inspire and empower the next generation of IT and security professionals to remain relevant in the way they think and hack. We achieve this by delivering practical content, giving delegates the hands-on experience needed to understand the context behind each offensive and defensive technique. They go on to use this with confidence in their own work, be that within an organisation or their personal research.

**WE HACK.
WE TEACH.**

claranet cyber security®