COURSE PROFILE:

Hacking and Securing Cloud Infrastructure

4 days | **Intermediate training**

Version 6

claranet cyber security® | NotSoSecure Training

Your course

As cloud innovation gives birth to new technologies and new threats, now is the time to modernize your cloud security skills and bring them up to the industry standard. Join this hands-on, 4-day course to push your cloud hacking and vulnerability remediation skills to the next level and widen your career prospects. Get your hands dirty with our popular virtual labs and learn from experienced, practicing penetration testers with a legacy of training at Black Hat.

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 latest vulnerabilities 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

Top 3 takeaways

- **Gained understanding of identifying and exploiting misconfigured IAM policies**
- **Learned strategies for using IAM permissions effectively to prevent data leakage**
- **Acquired skills in correcting cloud misconfigurations through practical, lab-based demonstrations**

What you will learn

This course uses a Defense by Offense methodology based on real world 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 over. By the end, you'll know how to:

- **Think and behave like an advanced, real-world threat actor**
- **Identify and exploit complex security misconfigurations in AWS, Microsoft Azure, and Google Cloud Platform (GCP)**
- **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**
- **Support cloud defense strategies that include patching, asset inventory management, and other security controls**

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 and container 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 four 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 and why cloud security matters • Comparison with conventional security models • Shared responsibility model • Legalities around cloud pentesting • Attacking cloud services
ENUMERATION OF CLOUD ENVIRONMENTS	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. • DNS-based enumeration • Open-Source Intelligence Gathering (OSINT) techniques for cloud-based asset identification. • Username enumeration
ATTACK SURFACE OF CLOUD SERVICES	This module delves into the attack surfaces of key cloud service models: Infrastructure as a Service (IaaS), Function as a Service (FaaS), Platform as a Service (PaaS), and Container as a Service (CaaS). It provides an in-depth understanding of the vulnerabilities and security challenges associated with each model. The module kicks off with an examination of the "IaaS Attack Surface," followed by the "FaaS Attack Surface," "PaaS Attack Surface," and "CaaS Attack Surface." • Understanding Infrastructure as a Service (IaaS) Attack Surface • Understanding Function as a Service (FaaS) Attack Surface • Understanding Platform as a Service (PaaS) Attack Surface • Understanding Container as a Service (CaaS) Attack Surface

ATTACKING CLOUD STORAGE	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
ATTACKING MICROSOFT AZURE AD ENVIRONMENT	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 • Azure Identity Protection to Monitor User Behaviour

ATTACKING AWS ENVIRONMENT	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 within AWS infrastructures. • Introduction to the AWS IAM Policies and Shadow Admin Permissions. • Understand AWS Policy Evaluation Logic • IAM Misconfiguration (Identity Based Policy, and Resource Based Policy) • Enumerate Roles using PACU • Gaining Access to EC2 Instance by Abusing Instance Attribute • PaaS Service exploitation and understand the pitfall of default permissions. • Attacking AWS Cognito misconfiguration • Stealing sensitive information from ECR and ECS deployment. • Exploit Lambda and API Gateway. • Exploiting internal service using Virtual Private Cloud (VPC) misconfiguration (demo only) • Introduction to AWS Organisation. • Understand Delegated administrator for AWS Organisations and, it's risk.

ATTACKING GCP ENVIRONMENT	Participants will delve into essential GCP security aspects, including IAM Role and Service Account, Authentication methods using Service Account files and Access tokens. The module introduces Compute Engine, Cloud Storage, App Engine, and Identity-Aware Proxy (IAP). Furthermore, this module covers the GCP services like Cloud Function, Cloud Storage, Pub/Sub, Cloud Run and databases. Security-related topics include IAM Impersonation and Secret Manager, bolstering access control. The module concludes by introducing Container Registry, a vital component of GCP container management. • Introduction to GCP • Introduction to IAM Role, Service account • Understanding the Authentication in GCP • Introduction to Compute Engine and Cloud Storage • Understanding App Engine, IAP • Database: Firestore/Firebase • Cloud Function and Cloud Storage • Pub/Sub and Cloud Run • IAM Impersonation and Secret Manager • Container Registry
REVISITING AWS, AZURE AND GCP MISCONFIGURATIONS IN HARDENED ENVIRONMENT	This section revisits the key cloud misconfigurations discussed in the Azure, AWS, and GCP sections, focusing on comprehensive fixes in a hardened environment. The module provides insights into the practical implementation of robust security measures, ensuring that cloud environments are fortified against vulnerabilities and risks. By actively validating these fixes, participants will be better prepared to enhance cloud security and maintain a robust posture across Azure, AWS, and GCP platforms. • Microsoft Entra ID • Azure MFA Bypass • Azure Key Vault • Elastic Beanstalk • AWS IAM Misconfigurations • ECS and ECR • AWS Cognito • GCP IAM • GCP IAP

CLOUD DEFENCE USING OPEN-SOURCE AND CLOUD-NATIVE TOOLS	This module focuses on an all-encompassing approach to cloud defense, encompassing four fundamental pillars: identification, protection, detection, and response. Participants will gain insights into how to proactively identify vulnerabilities and potential threats within their cloud infrastructure. They will also explore strategies for safeguarding cloud assets and data. The module delves into the critical aspect of real-time threat detection, equipping individuals with the skills to recognize and respond to security incidents effectively. By the end of this module, participants will be well-prepared to establish robust cloud defense mechanisms, ensuring the security and resilience of their cloud environments. • Identification of Cloud Assets • Hybrid Account Asset Inventory • AWS Multi-Account Asset Inventory using Open Source Tools • Protection of Cloud Assets • Principle of Least Privilege (with examples like EC2, IAM, RDS, etc.) • Financial Protections by Enabling Budgets • Metadata API Protection • Demo of Metadata API Protection using Linux Firewall Rules • Monitoring Cloud Activities using Cloud Native Tools • Hybrid Cloud Account Monitoring Strategy • Automated Response in Cloud Against Malicious Activities • Response to Attacks Using AWS Config.
CLOUD AUDITING AND BENCHMARKING	This module delves into the comprehensive CIS benchmark, and essential cloud security best practices designed to establish a baseline security posture within cloud infrastructures. Participants will gain profound insights into industry standards and proven methodologies for enhancing cloud security, ultimately fortifying their cloud environments against vulnerabilities and threats. • Preparing for the audit • Automated auditing via tools • Golden image/Docker image audits • Windows Infrastructure as a Service (IaaS) auditing • Linux IaaS auditing • Relevant benchmarks for cloud
CAPTURE THE FLAG	• A timed competition to test your new skills and reinforce everything you've learnt

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 hackat 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 practicingpenetration testers and red teamers
- **Up-to-date content:** our syllabus remains so relevant, delegates come back year afteryear 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.
- 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.

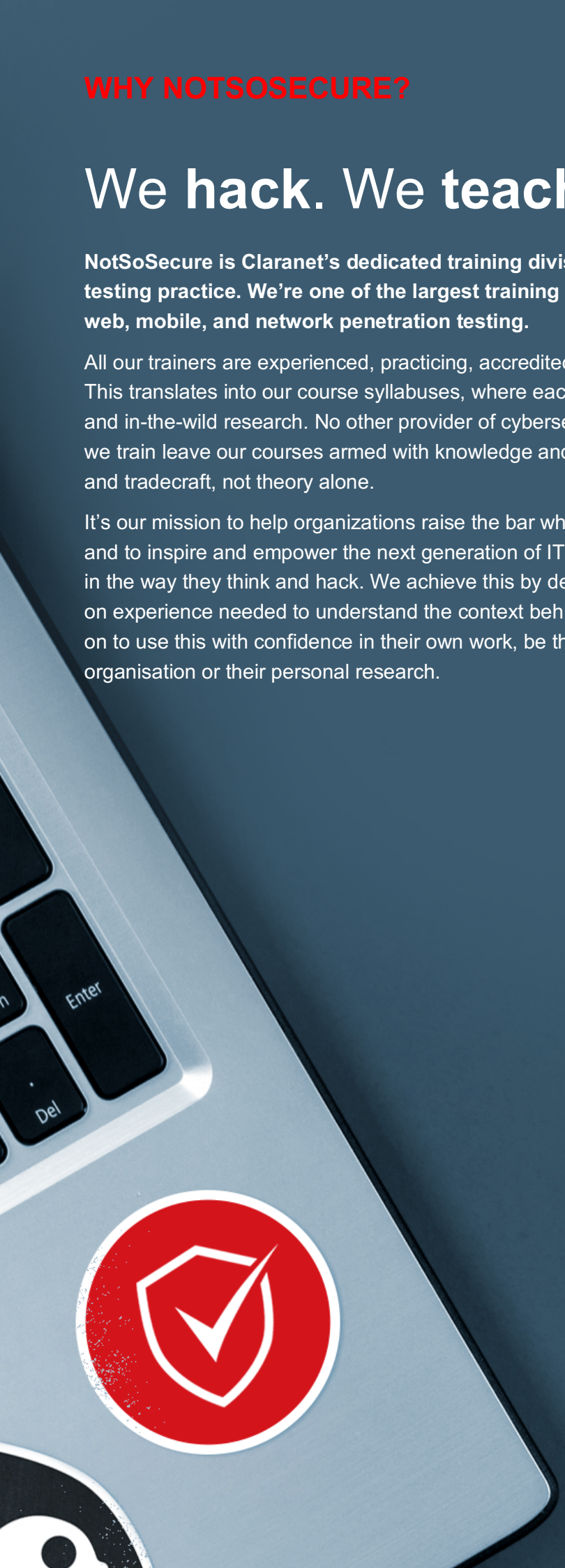
WHY NOTSOSECURE?

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