

COURSE PROFILE:

Hacking Cloud Infrastructure



2 Day **Intermediate** training

Your course

As cloud innovation gives birth to new technologies and new threats, now is the time to modernize your cloud security skills. Join this hands-on, 2-day course to push your cloud hacking 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 it's 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

- **Exploitation techniques to gain cloud entry via exposed services**
- **Post-exploitation techniques to enumerate systems and achieve exfiltration**
- **Methods for defending different cloud environments**

What you'll 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 vulnerabilities and 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) platforms, and serverless functions**
- **Support cloud defense strategies that include patching, asset inventory management, and other security controls**

What you'll be doing

You'll be learning hands on:

- Spending most of the session (~70%) 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's 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's in the syllabus

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

INTRODUCTION TO CLOUD COMPUTING

- 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

- DNS-based enumeration
- Open-Source Intelligence Gathering (OSINT) techniques for cloud-based asset identification
- Username enumeration

ATTACKING STORAGE SERVICES (AWS, Azure, GCP)

- Exploring files storage
- Exploring shared access signatures (SAS) URLs in MS Azure
- Exploit misconfigured storage service

ATTACKING MICROSOFT AZURE AD ENVIRONMENT

- Introduction to MS Azure
- MS Azure application attacks (App Service, Function App, Enterprise Apps)
- MS Azure service exploitation (Database, Key Vault, Automation account)
- MS Azure AD attacks (manage user identities, role-based access control (MS Azure Active Directory, Subscriptions, Dynamic Group)

AWS: GAINING ENTRY VIA EXPOSED SERVICES

- Serverless-based attacks (AWS Lambda)
- PaaS attack: server-side request forgery (SSRF Exploitation over AWS ElasticBeanStalk)
- Attacking AWS Incognito misconfiguration
- Exploiting internal service using Virtual Private Cloud (VPC) misconfiguration (demo only)

AWS: IDENTITY AND ACCESS MANAGEMENT (IAM)

- AWS IAM policies and roles
- IAM policy evaluation
- Roles and permissions-based attacks
- Shadow admin attacks

GCP

- Introduction to GCP IAM (shadow admin (demo only))
- GCP service exploitation via web application vulnerability (Google Compute Engine and App Engine, Google Cloud Storage)
- Lateral movement Within GCP to access container images

POST EXPLOITATION

- Persistence in cloud
- Post-exploit enumeration
- Snapshot access

CONTAINERS AS A SERVICE (CAAS) AND KUBERNETES (K8S) EXPLOITATION

- Understanding how container technology works (namespaces, cgroup, chroot)
- From Docker to K8S
- Identifying vulnerabilities in Docker images
- Exploiting misconfigured containers
- Exploiting Docker environments and breaking out of containers
- Exploring K8S environments
- K8S exploitation and breakouts
- Pivoting to host OS

CLOUD DEFENCE USING OPEN-SOURCE AND CLOUD-NATIVE TOOLS

- Identification of cloud assets
- Inventory Extraction for AWS, Azure, and GCP
- Continuous inventory management
- Protection of cloud assets
- Principle of least privilege
- Control plane and data plane protection
- Financial protections
- Cloud-specific protections
- Metadata API protection
- Detection of security issues
- Setting up monitoring and logging of the environment
- Identifying attack patterns from logs
- Revisiting Day 1 attacks via logs
- Real-time monitoring of logs
- Monitoring in a multi-cloud environment
- Response to attacks
- Automated defence techniques
- Cloud defence utilities
- Validation of setup

CLOUD AUDITING AND BENCHMARKING

- 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'll 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, 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
- **Course topics:** our Kubernetes module is a favorite

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®

