COURSE PROFILE:

Hacking Azure: From Recon to Domination

2 days | **Intermediate** training

Version 1

claranet cyber security | NotSoSecure Training

Your Course

As organizations rapidly adopt Microsoft Azure, the risk of misconfigurations and security gaps grows, making cloud environments a prime target for attackers. Understanding offensive security techniques in Azure is critical for penetration testers, security professionals, and cloud engineers aiming to assess and fortify cloud security.

This intensive 2-day hands-on training is designed to teach real-world attack techniques used against Azure environments. Participants will explore the entire attack chain, from reconnaissance and initial access to lateral movement, token theft, cloud-to-on-prem pivoting, and privilege escalation. The training also includes bypassing conditional access policies, abusing misconfigured identities, and leveraging automation services for persistence.

With 18+ hands-on labs, attendees will step into the attacker's mindset, executing live exploitation scenarios while gaining expertise in offensive tooling, enumeration methods, and security bypasses. This training, led by seasoned cloud security professionals, provides an in-depth understanding of Azure hacking techniques while covering mitigation strategies to help organizations secure their cloud infrastructure effectively.

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 Azure cloud security, from technical practitioners to decision-makers. The syllabus is designed to cover Azure cloud misconfigurations and advanced hacking techniques while equipping participants with the skills to conduct penetration tests on cloud environments and identify security gaps effectively.

Additionally, this course provides a practical, hands-on approach to cloud penetration testing, allowing participants to apply the acquired skills directly in their day-to-day pen-testing activities. By following a structured pen-testing methodology, attendees will gain real-world experience in assessing, exploiting, and understanding Azure security risks.

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 Azure Cloud CLI

Top 3 Takeaways

- Execute exploit labs in a kill-chain sequence, escalating privileges by compromising multiple Azure services.
- Learn effective enumeration techniques to identify misconfigurations within the cloud environment
- Understand Microsoft Entra ID misconfigurations and master techniques to bypass Conditional Access Policies for privilege escalation.

What You Will Learn

This course uses a Defence 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 misconfigurations in Microsoft Azure.
- Design your penetration tests around real-world attacker behaviours and tooling, making them 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.

What You Will 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 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 boot camp to help you advance your skills in the most important and relevant areas of cloud security. Across 2 days, you'll learn about the high-impact misconfigurations 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 AZURE AND 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 • Importance of Cloud Metadata API from an Attacker's perspective • Introduction to the Azure
CLOUD ASSET ENUMERATION FOCUSING AZURE ENVIRONMENT	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," and Leaked database 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 and Leaked Database
AZURE STORAGES	This module 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 Azure Storage • Azure: Shared Access Signature (SAS) URL Misconfiguration
ATTACKING MICROSOFT AZURE RESORUCE MANAGER SERVICES	The module extensively covers "Azure Resource Manager Attacks" across critical components such as App Service, Function App, Database, Automation Account, Key Vault and Logic Apps. • Azure Application Attacks on App Service, Function App and Storages • Azure Database • Automation Account • Hybrid Automation Account Abuse • Azure Key Vault • Azure Logic Apps

ATTACKING AZURE DEVOPS	This module provides an in-depth analysis of the security implications of Azure DevOps, focusing on potential privilege escalation scenarios within a DevOps environment. Participants will also learn how to enumerate other key DevOps services, such as Azure Repos and Azure Container Registry, which are closely integrated with Azure DevOps for daily operations. • Introduction to Azure DevOps • Understanding Azure DevOps Service Connection and potential abuse. • Exploiting Azure repository and Azure container registry for sensitive information.
AZURE ARC SERVICE	This module provides an in-depth analysis of the security implications of Azure Arc, focusing on potential privilege escalation scenarios in a hybrid cloud environment. Participants will learn how Azure Arc integrates with on-premises and multi-cloud environments, enabling the management of resources across different infrastructures.
ABUSING ENTRA ID MISCONFIGURATIONS	This module provides an in-depth analysis of **Microsoft Entra ID**, focusing on its **authentication methods, security risks, and attack scenarios** in cloud environments. Participants will learn about **potential attacks on Entra ID**, along with advanced techniques for **bypassing Multi-Factor Authentication (MFA)** and evading **Conditional Access Policies**. Additionally, the module explores **Dynamic Membership Policy abuse**, and how **refresh tokens can be exploited to gain access to Office 365 and SharePoint Drive** of compromised users. • Introduction to Microsoft Entra ID authentication methods and associated risks • Attacking Microsoft Entra ID, focusing on Managed User Identities • Bypassing MFA security and evading Conditional Access Policies • Exploiting Dynamic Membership Policies for privilege escalation • Leveraging Azure Identity Protection to detect and respond to threats • Using Refresh Tokens to Maintain Persistent Access to Office 365 and SharePoint Drive
BACKDOORING AZURE ENVIRONMENTS: PERSISTENCE TECHNIQUES	This module explores techniques attackers use to backdoor Azure environments, ensuring persistent access while remaining unnoticed. Participants will learn how to manipulate Azure configurations, exploit identity and access management (IAM) flaws, and abuse legitimate services to maintain unauthorized access. The session also covers defensive measures to detect and mitigate such threats.
AZURE AD IDENTITY PROTECTION	This module provides an in-depth understanding of Azure AD Identity Protection, focusing on its security mechanisms, risk detection, and potential attack vectors. Participants will learn how Microsoft Entra ID analyzes sign-in behavior, detects threats, and enforces security policies.

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 Q&A 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 of 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 that delegates come back year after year.
- 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 industry standard, helping you to:

- 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.

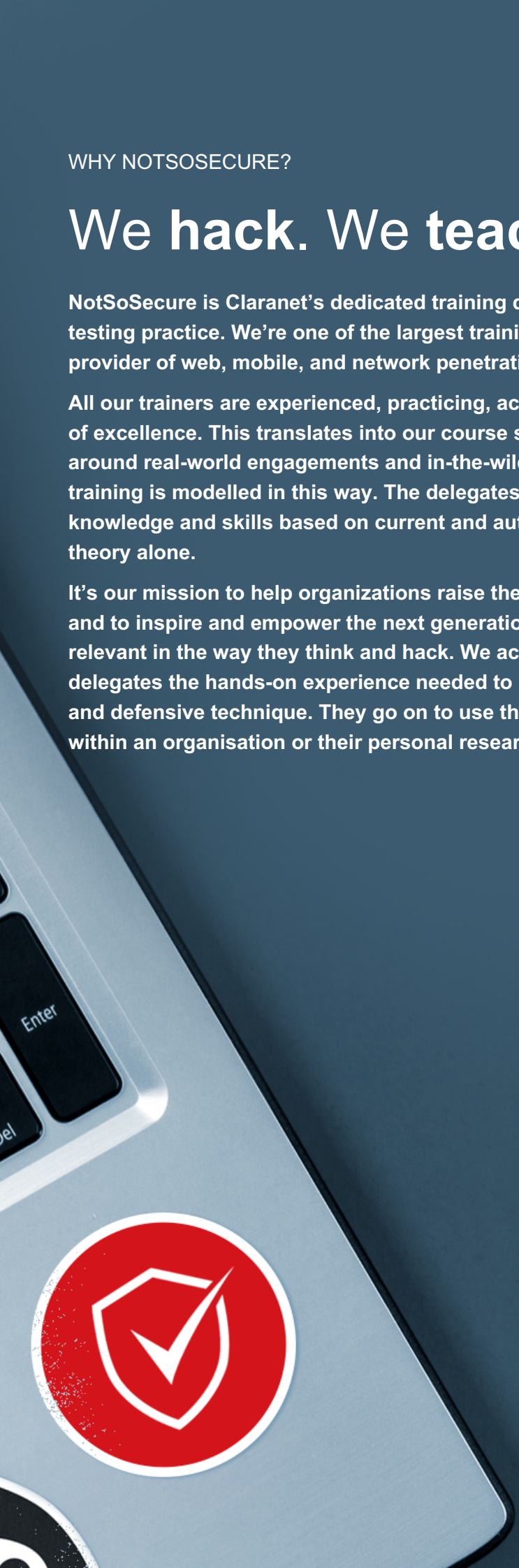
WHY NOTSOSECURE?

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