COURSE PROFILE:

Advanced Infrastructure Hacking

5 day | **Advanced training – 2024 Edition**

Version 6

claranet cyber security

NotSoSecure Training

Your course

IT infrastructure is more complex and dynamic than it's ever been demanding comprehensive, up-to-date, and well-rehearsed security skills to match. Join this hands-on, 2-day course to push your infrastructure hacking 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?

- **Penetration testers and red teamers**
- **Security consultants and architects**
- **Network admins with security experience**
- **CSIRT/SOC teams/blue teamers**
- **Security/IT managers and team leads**

This course is suitable for in-house security teams from intermediate to pro-level. It's also relevant to other security and IT practitioners and managers who want to understand the current threat landscape and defend their organization.

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

- **Intermediate knowledge of infrastructure application security (at least 2 years' experience)**
- **Common command line syntax competency**
- **Experience using virtual labs for pentesting and/or offensive research**

Top 3 takeaways

- **Many of the latest and most complex infrastructure testing techniques**
- **Hacks to use against your organization's own products**
- **Knowledge of how to remediate as well as attack weaknesses in infrastructure**

What you will learn

This course uses a Defence by Offence 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, so you can put it into practice as soon as the training is over. By the end of the course, you'll know:

- **How to think and behave like an advanced, real world threat actor**
- **How to identify commonly used vulnerabilities known to have recently caused damage and disruption**
- **How to deploy the latest and most common network infrastructure and cloud hacks, (including many novel techniques that can't be detected by scanners)**
- **How to analyze vulnerabilities within your own organization and customize your hacking techniques in response**
- **A huge menu of hacks for Windows, Linux, Microsoft Azure, AWS, Google Cloud Platform (GCP), software development systems, and more...**

What you will be doing

You'll be learning hands on:

- **Spending most of the session (~80%) on lab-based exercises**
- **Using lab-based flows to explore and hack lifelike web application environments**
- **Discussing the impact of the hacks covered with your course trainer**

Why it is relevant

As different on-premises and cloud environments shapeshift and converge, the practice of infrastructure security is becoming more complex. Organisations and their security teams can no longer afford to understand the overarching attack surface at a high level. Nor can they rely on the same security practices that worked in the past. What's needed is a thorough, contextual understanding of how and why your architecture and systems get targeted by threat actors, which are at risk, and what happens when those attacks succeed. Our Advanced Infrastructure Hacking course provides delegates with this knowledge and more, by giving them an up-to-date arsenal of advanced offensive testing and remediation skills.

Our syllabuses are revised regularly to reflect the latest in-the-wild hacks and whatever proof of concepts we've been developing through 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
IPV4/IPV6 BASICS	• IPv6 service discovery and enumeration • MiTM attacks • Exploiting systems/services over IPv6 • Host discovery and enumeration. • Advanced OSINT and asset discovery • Exploiting DVCS and CI-CD server (updated flow)
HACKING DATABASES	• PostgreSQL / MySQL • Oracle • NoSQL
WINDOWS EXPLOITATION	• Windows enumeration and configuration Issues • Windows desktop breakout and AppLocker bypass techniques (Win 10) • Local privilege escalation • Offensive PowerShell /Offsec Development • AMSI bypass Techniques • AV Evasion Techniques • Post-exploitation Tips, Tools, and Methodology
ACTIVE DIRECTORY (AD) ATTACKS	• Active Directory delegation reviews and pwnage (Win 2019 Server) • Pass the hash/ticket (Updated) • ADCS Misconfiguration • Resource-based constrained delegation • Cross domain and forest attacks • Pivoting, port forwarding, and lateral movement techniques • Persistence and backdooring techniques (Golden and Diamond Ticket) • Command and Control (C2) frameworks (Updated)

LINUX EXPLOITATION	• Linux vulnerabilities and configuration issues • Treasure hunting via enumeration • Kerberos authentication • File share/SSH Hacks • Restricted shells breakouts • Breaking hardened web servers • Local privilege escalation • MongoDB exploitation • TTY “Teletype” hacks and pivoting • Gaining root access via misconfigurations • Kernel exploitation • Post exploitation • Persistence techniques (Linux capabilities)
CONTAINER BREAKOUT	• Breaking and abusing Docker (updated) • Exploiting Kubernetes vulnerabilities • Breaking out of Kubernetes containers
CLOUD HACKING	• AWS, MS Azure, and GCP specific attacks • Storage misconfigurations • Credentials, APIs, and token abuse • Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Container as a Service (CaaS), and serverless exploitation • Azure AD attacks • Exploiting insecure VPN configuration • VLAN hopping attacks

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.
- **Course topics:** cryptography, SQL injection, and RCE often come out on top.

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: question & answer sheets, setup documents, and command cheat sheets**

Outcomes for budget holders

This course is designed to bring your organisation's infrastructure security testing competency up to an advanced industry standard, helping you:

- Harden your organisation's infrastructure and lower the likelihood of security incidents by identifying high impact vulnerabilities across your infrastructure.
- Improve your understanding of the organization's risk posture based on the frequency and severity of vulnerabilities identified.
- Create a stronger case for securing your organization's network admin and architecture practices.
- Build a closer relationship between network and security teams.
- Internally pentest new tools and systems before making an investment.
- Nurture and retain passionate, highly skilled, and security conscious employees.
- Keep your own infrastructure security knowledge up to date.
- Demonstrate commitment to security through training, compliance, and change management.
- Develop the organisation'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®