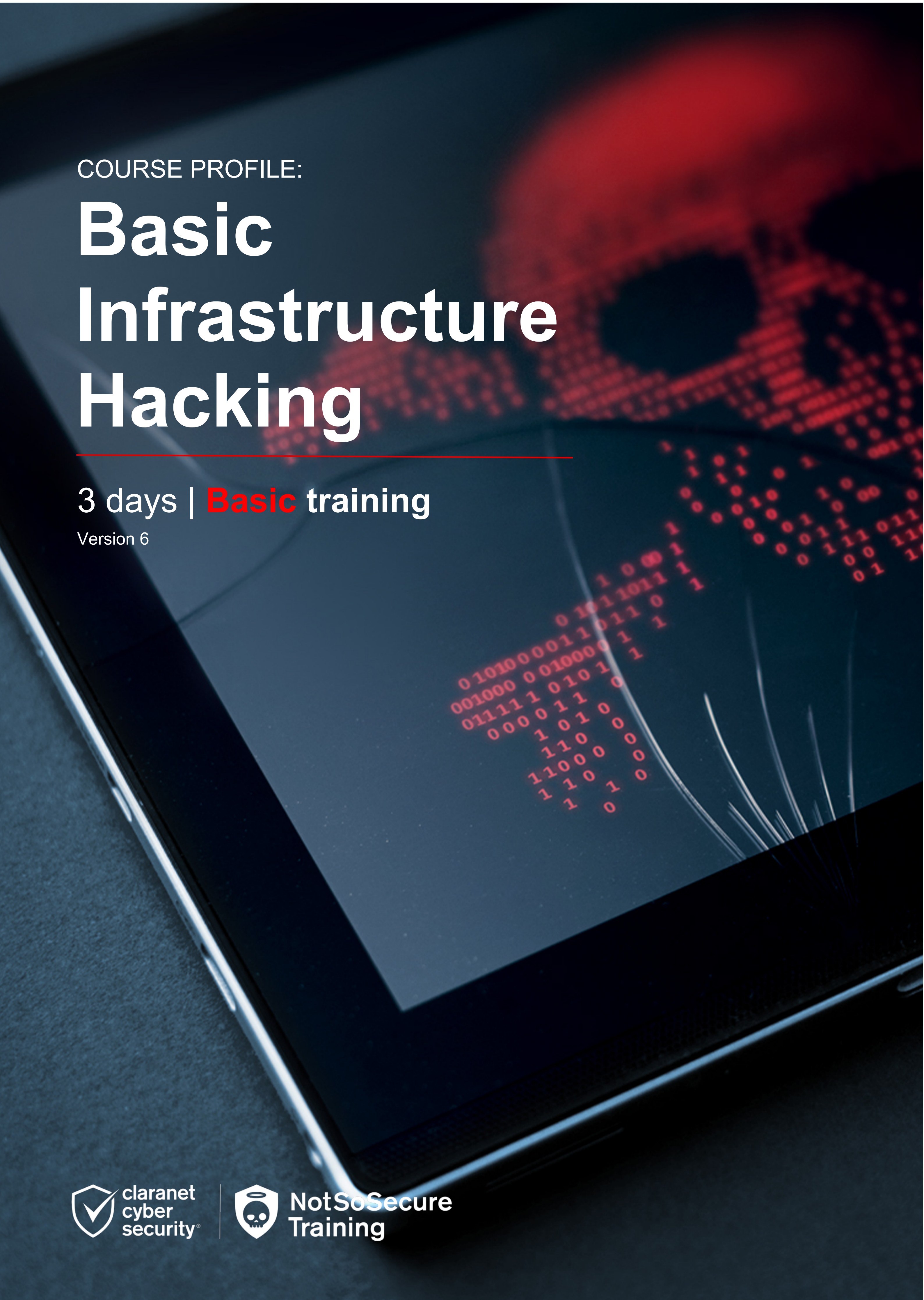

COURSE PROFILE:

Basic Infrastructure Hacking

3 days | **Basic training**

Version 6

claranet cyber security®

NotSoSecure Training

Your course

IT infrastructure is more complex and dynamic than it's ever been, demanding comprehensive, modern, and well-rehearsed security skills to match. Join this hands-on, 3-day course to develop a strong baseline in infrastructure hacking 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?

- **Students and graduates:** improve your employability and enhance your CV
- **Infrastructure penetration testers** (1-2 years' experience): build up your ability with the guidance of experienced pentesters and researchers
- **Penetration testers in other fields** (e.g., web, mobile): develop your infrastructure hacking skills and knowledge
- **Network admins:** understand how your environment could be attacked
- **SOC analysts and engineers:** develop your awareness of potential indicators of compromise (IoCs) and more complex malicious behaviors
- **Security/IT managers and team leads:** update your knowledge of the threat landscape

This course is designed to help individuals bring their proficiency in infrastructure hacking and defense up to the industry baseline. It's a foundation course that can lead on to our Advanced courses after a year or more spent using your new skills out in the wild.

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

- **Basic knowledge of infrastructure application security (at least 1 year experience)**
- **Basic familiarity with common command line syntax**

Top 3 takeaways

- **The ability to find and exploit vulnerabilities and other weaknesses in different infrastructure environments**
- **Knowledge of how to apply the leading industry infrastructure security standards and approaches**
- **Time spent with experienced, practicing penetration testers who can answer your questions**

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:

- **Everything you need to about the risks associated with various infrastructure-based vulnerabilities**
- **How to think and behave like a real threat actor**
- **How to exploit vulnerabilities seen recently in the wild, as well as older but still prevalent vulnerabilities**
- **The fundamental principles of infrastructure hacking**
- **How to identify a list of IPs in your network all the way up to getting system level access on the domain controller**

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 environments.**
- **Trying out different hacking techniques to exploit common infrastructure misconfigurations**
- **Discussing the real-world impact of hacks covered with the course trainer**

Why it is relevant

Infrastructure security must move at the incredible speed of software development, cloud innovation, and workplace evolution to remain relevant and useful. 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 Basic Infrastructure Hacking course provides delegates with this knowledge and more, by providing them with an up-to-date arsenal of basic offensive testing and remediation skills.

Delegates with solid baseline knowledge and a consistent approach to ethical hacking tend to develop faster in the long-term, so we've created a syllabus designed to comprehensively improve your subject matter understanding and practical methodology. It does this by analyzing both archaic and modern techniques, which once mastered, will help you progress further into advanced topics.

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
THE ART OF PORT SCANNING	• Methodology: basic concepts of hacking • Enumeration techniques and port scanning
THE ART OF ONLINE PASSWORD ATTACKS	• Configure online password attack • Exploiting network service misconfiguration
THE ART OF HACKING DATABASES	• MySQL and PostgreSQL • Attack chaining techniques
METASPLOIT BASICS	• Exploitation concepts: manual exploitation methodology • Metasploit framework
PASSWORD CRACKING	• Basic cryptography concepts • Design an offline brute force attack
HACKING UNIX	• Linux vulnerabilities and misconfigurations • Privilege escalation techniques
HACKING APPLICATION SERVERS ON UNIX	• Web server misconfiguration • Multiple exploitation techniques
HACKING THIRD PARTY CONTENT MANAGEMENT SYSTEM (CMS) SOFTWARE	• CMS software overview • Vulnerability scanning and exploitation
WINDOWS ENUMERATION	• Windows enumeration techniques and configuration issues • Attack chaining
CLIENT-SIDE ATTACKS	• Various Windows client-side attack techniques
HACKING APPLICATION SERVERS ON WINDOWS	• Web server misconfiguration • Exploiting application servers
POST EXPLOITATION	• Metasploit post-exploitation techniques • Window 10 security features and bypass techniques

PRIVILEGE ESCALATION ON WINDOWS	• Post-exploitation techniques • Windows privilege escalation techniques
HACKING WINDOWS DOMAINS	• Understanding Windows authentication • Gaining access to a domain controller

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:

- **Intensive format:** three days of focused learning to give you a crash course you won't forget.
- **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 get 30+ days access to practice your new skills afterwards.
- **Dedicated Kali instance:** you'll have your own infrastructure to play with, enabling you to hack at your own speed.
- **Real-world learning:** where many of the leading cybersecurity training courses are based on theory, our scenario-led, research-based approach ensures you learn how real threat actors think and behave.
- **Specialist-led training:** you'll learn from highly skilled and experienced practicing penetration testers and red teamers.

Outcomes for budget holders

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

- **Respond to the security skills shortage in your organization from the ground up**
- **Take the first steps towards building a team of advanced infrastructure security testers**
- **Create a stronger case for securing your organization's software development and procurement practices**
- **Build a closer relationship between network admin and security teams**
- **Nurture and retrain 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 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®