
COURSE PROFILE:
Hacking 101
1 day | Beginner training
Version 6
101
claranet cyber security
NotSoSecure Training

Your course

This 1-day course teaches you how to apply basic security principles in your current role and can help you begin a career in cybersecurity. You'll build a strong foundation of knowledge based on key industry principles, covering where hacking began to the modern techniques used by threat actors to target organizations and individuals today. 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?

- **Network admins: understand how your environment could be attacked**
- **Developers: see how real cyber criminals might target your applications**
- **Students and graduates: improve your employability and enhance your CV**
- **Career changers: get a taste of what it's like to work as a penetration tester**

This course provides an introduction to offensive security by looking at the basic principles of application and infrastructure hacking. Sit in the seat of a pentester for the day, use the same tools and commands, and learn how cyberattacks work start to end.

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

- **A genuine interest in cybersecurity and a desire to develop your skills**
- **Basic knowledge of common command line syntax**

Top 3 takeaways

- **The 101 on how cyberattacks and security testing have evolved**
- **Exploitation techniques to target applications and different infrastructure environments**
- **Knowledge of the risks associated with different applications, systems, and technologies**

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 a real-world threat actor**
- **Fingerprint, enumerate, and exploit common Windows and Linux misconfigurations and vulnerabilities**
- **Exploit common web application security flaws**
- **Differentiate between types of wireless standards and understand the benefits and associated risks**
- **Differentiate between different network topologies and addressing schemes**

What you will be doing

You'll be learning hands on:

- **Spending most of the session (~80%) on lab-based exercises**
- **Exploiting a range of systems and environments**
- **Discussing case studies with your course leader to understand the real-world impact of the hacks covered**

Why it is relevant

Cybersecurity underpins everything. Whether you want to become a specialist or simply keep your skills relevant, now is an incredible time to do so. However, there's a right way to start. As many seasoned security professionals will tell you, the stronger your baseline knowledge, the faster and better you'll develop in the long-term. We believe the same, so our syllabus has been designed to equip you with the fundamentals needed to go on and specialize. Rather than focusing on novel and complex hacks that take years of experience and technical knowledge to master, we've selected some core themes and exercises to build your confidence and proficiency and prepare you for the next step. Delegates who go on to use these skills in the real world can return to take one of our Basic Hacking courses in around a year's time.

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
HACKING FUNDAMENTALS	• Hacking History 101 • Hacking today • The CIA Triad • Art of Hacking methodology • Introduction to Kali Linux
WINDOWS SECURITY	• Windows fundamentals • Windows password hashing • Workgroups vs Domains • Windows authentication • Windows exploitation 101 • Client-side attacks • Case study: WannaCry
HACKING CONTENT MANAGEMENT SYSTEM (CMS) SOFTWARE	• Introduction to Content Management Systems • Enumerating CMS platforms • Hacking WordPress • Joomla exploitation
NETWORK SECURITY	• Network fundamentals. • MAC addressing and network addressing. • Introduction to port addressing. • Understanding the Open Systems Interconnection (OSI) layer and transmission control protocol/internet protocol (TCP/IP) model • Domain Name System (DNS) attack surface • TCP vs user datagram protocol (UDP) • Network scanning. • Shodan

LINUX SECURITY	• Introduction to Linux • Linux filesystem hierarchy • Linux file permissions • Berkeley Remote Shell (Rsh)/ Remote Login (Rlogin) services • Network file system (NFS) security. • Missing security patches • Vulnerability identification • Case study: Shellshock • Introduction to Metasploit
WEB SECURITY	• HTTP protocol basics • Understanding web application attack surface • SQL injection (SQLi) • Case study: TalkTalk SQLi • Command injection. • Cross-Site Scripting (XSS) • Open redirect
WIRELESS SECURITY	• Wi-Fi Security 101 • Wired Equivalent Privacy (WEP) • Wi-Fi Protected Access (WPA) • WPA2 Security • Wi-Fi Protected Setup (WPS) flaws. • Rogue access points attacks

What you will get

- **Certificate of completion**
- **7 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.
- **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 behave.
- **Specialist-led training:** you'll learn from highly skilled and experienced practicing penetration testers and red teamers.
- **Course topics:** our Hacking History 101 goes on to inform how our delegates think and hack and develop their approach.

Outcomes for budget holders

This course is designed to provide entry-level security practitioners and specialists in other fields with practical industry knowledge and technical skills, helping you:

- Build security awareness across your workforce
- Nurture and retain passionate, highly skilled, and security conscious employees
- Prepare junior IT and security staff for further training

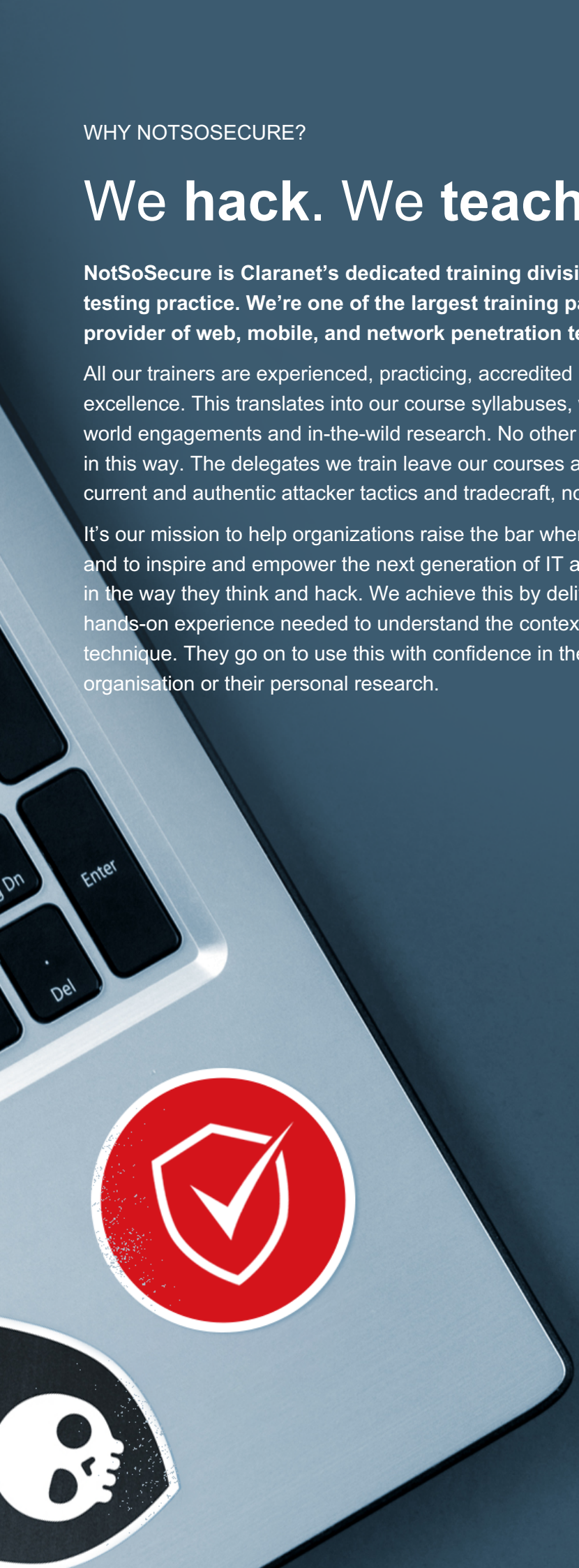
WHY NOTSOSECURE?

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®