COURSE PROFILE:

The Art of Hacking

5 days | Basic training

Version 6

claranet cyber security®

NotSoSecure Training

Your course

This course introduces the attendees with a wealth of hacking tools and techniques that are crucial in getting started within the dynamic field of hacking. The most commonly exploited entry point for many breaches that are reported, comes from internet-facing applications. Due to this, our course begins by focussing on the very basics of web application security and utilises industry standard tools to build up the knowledge of various attack vectors, and how they can be exploited and used as an entry point into an internal network.

We then discuss the basic concepts of infrastructure security and gradually build up to the level where attendees not only use the tools and techniques to exploit various components involved in infrastructure hacking, but also walk away with a solid understanding of the concepts on how these tools work and are therefore ready to face real-world engagements.

Who is it for?

- **Security Enthusiasts**
- **Penetration Testers** (1 year's experience): build up your ability with the guidance of experienced pentesters and researchers
- **System Administrators:** understand how your environment could be attacked
- **Application Developers:** Get a hands-on insight to the impact of application vulnerabilities
- **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 & web hacking 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 & web application security**
- **Basic familiarity with common command line syntax**

Top 3 takeaways

- **The ability to find and exploit vulnerabilities and other weaknesses in web & 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 & web 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**
- **How to identify a list of IPs in your network all the way up to getting system level access on the domain controller**
- **How to identify and exploit various web application vulnerabilities and misconfigurations**

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

Why it is relevant

Our courses are tailored to provide delegates with in-depth knowledge to protect modern organizations. The Art of Hacking course provides a thorough understanding of how and why web applications and infrastructure are targeted by threat actors. By teaching the latest and most useful offensive testing and remediation techniques, the course empowers security and software development teams to protect these assets effectively.

With solid baseline knowledge and a consistent approach to ethical hacking, delegates can progress faster in the long term. Our syllabus is curated to comprehensively improve subject matter understanding and practical methodology by analyzing both archaic and modern techniques, which will help delegates progress into advanced topics. The speed of software development and workplace evolution makes it crucial for infrastructure security to move at an incredible pace, which our Art of Hacking course addresses perfectly. Attendees will gain up-to-date offensive testing and remediation skills that equip them to protect their organization's architecture and systems from potential attacks.

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
UNDERSTANDING THE HTTP PROTOCOL	• HTTP protocol basics • Introduction to proxy tools
INFORMATION GATHERING	• Enumeration techniques • Understanding web attack surface
ISSUES WITH SECURE SOCKETS LAYER (SSL) AND TRANSPORT LAYER SECURITY (TLS)	• SSL/TLS Misconfigurations
USERNAME ENUMERATION AND FAULTY PASSWORD RESET	• Attacking authentication and faulty password mechanisms • User enumeration • Broken authentication • Second factor authentication bypass
BROKEN ACCESS CONTROL – ROLE BASED AUTHORIZATION BYPASS	• Horizontal Privilege Escalation attack • Vertical Privilege Escalation attack • Insecure Direct Object Reference attack
SECURITY MISCONFIGURATION	• Business Logic Attacks
CROSS SITE SCRIPTING (XSS)	• Various types of XSS • Session hijacking and other attacks
SERVER SITE REQUEST FORGERY (SSRF)	• Understanding SSRF attack • Various impacts of SSRF attack
SQL INJECTION (SQLi)	• SQL injection types • Manual exploitation • Automated exploitation
XML EXTERNAL ENTITY (XXE) ATTACKS	• XXE basics • XXE exploitation
INSECURE FILE UPLOADS	• Attacking file upload functionality Executing remote code through malicious file upload
COMPONENTS WITH KNOWN VULNERABILITIES	• Understanding the risk introduced by known vulnerabilities • Known vulnerabilities leading to critical exploits • Log4J attacks

MISCELLANEOUS VULNERABILITIES	• System Path Traversal • Open Redirection • HTML5 Cross-Origin Resource Sharing
INSUFFICIENT LOGGING AND MONITORING	• Understanding importance of logging and monitoring • Evaluate the logging events • Common pitfalls in logging and monitoring
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 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 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 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®