orange™ Business Services

Arm yourself with cybersecurity tools

A critical part of our business is our **Hacking Training Facility**, which we deliver via **SensePost**, the specialist pentesting arm of Orange Cyberdefense.

SensePost have trained thousands of students on the art of network and application exploitation for the past decade. It's safe to say we enjoy teaching others how to own networks and applications. Our courses are developed from the work we perform for clients, so that you get a better understanding of how to exploit real-world scenarios. As one of BlackHat briefings longstanding training partners, our courses have taught thousands of students about the art of offensive and defensive approaches.

Our introductory course for those starting the journey into penetration testing or those working in environments where understanding how hackers think and the tools, tactics and techniques they use. The course presents the background information, technical skills and basic concepts required to those desiring a foundation in the world of information security.

Available training courses

Hands on fundamentals

Our introductory course for those starting the journey into hacking

Web application hacking

Understand the fundamentals of how web applications are built and controlled

Infrastructure hacking

Aimed at beginner penetration testers wanting to understand infrastructure

Black ops

Intended for existing penetration testers with technical understanding

Modern Wi-Fi hacking

If you want to learn how to understand and compromise modern Wi-Fi networks, this is your course

Offensive cyber warfare

A 4-week intensive application of offensive cyber capabilities

Teaching students/teams to conduct integrated electronic warfare in authorised, directed operations in a controlled, classroom environment and under operationally-representative conditions. The course culminates in a three-day exercise where the student/team are tested through actively discovering and proactively hunting malicious actors planning on executing an attack

Hands on hacking fundamentals

This course mimics attackers

Our introductory course for those starting the journey into penetration testing or those working in environments where understanding how hackers think and the tools, tactics and techniques they use. The course presents the background information, technical skills and basic concepts required to those desiring a foundation in the world of information security.

Internal networks are attractive to attackers as they are often the least secure component of a company's infrastructure. This hands-on course mimics what attackers and criminals are doing – compromising networks, hunting down key accounts and business-critical information. The student will be trained in the methods and approaches taken when performing internal and external network penetration tests in a fully functional lab.

- How to think like a hacker
- The difference between finding known vulnerabilities and exploiting them
- How vulnerabilities can exist at different layers of the tech stack

Web application hacking

Designed for those new to penetration testing

This hands-on course teaches the student the fundamentals of how applications are built and where vulnerabilities are introduced in the development process. Designed for those new to penetration testing, network administrators or who want to understand more about offensive testing by breaking into various networks and applications, this course follows both the OWASP Top 10 and the OWASP Application Security Verification Standard (ASVS).

This hands-on course teaches the student the fundamentals of how applications are built and where vulnerabilities are introduced in the development process. Designed for those new to penetration testing, network administrators or who want to understand more about offensive testing by breaking into various networks and applications, this course follows both the OWASP Top 10 and the OWASP Application Security Verification Standard.

- A general approach and methodology for hacking web applications
- A good understanding of the tools and techniques for examining web application
- Practical and practiced skills (there are a lot of pracs in this course)

Master black ops

Solid and technical understanding

Master/black ops: Intended for existing penetration testers with a solid and technical understanding of penetration testing tools and techniques, this course teaches students how to hack like criminal network operatives. With a strong offensive focus drawing on the techniques employed in recent industry hacks, the student is taught about new vulnerabilities (current year – 3 years) and how to use them to their full potential.

Intended for existing penetration testers with a solid and technical understanding of penetration testing tools and techniques, this course teaches students how to hack like criminal network operatives. With a strong offensive focus drawing on the techniques employed in recent industry hacks, the student is taught about new vulnerabilities (current year – 3 years) and how to use them to their full potential.

- Understanding how real criminal hackers work
- A practical red teaming approach
- A significant amount of hands on experience with tools many pentesters don't know about

Infrastructure hacking

Aimed at beginner penetration testers

This also technically included people wanting to understand how to go about compromising their companies through their infrastructure and how to defend it. It will take you on a journey from learning about an organisation right through to stealthy exploitation of their critical infrastructure. This is a follow on from our 'Hands on Hacking Fundamentals' course.

Internal networks are attractive to attackers as they are often the least secure component of a company's infrastructure. This hands-on course mimics what attackers and criminals are doing – compromising networks, hunting down key accounts and business-critical information. The student will be trained in the methods and approaches taken when performing internal and external network penetration tests in a fully functional lab.

- How to hack corporate networks
- Methodologies for repeat success
- How the blue team could detect you

Unplugged: Modern Wi-Fi hacking

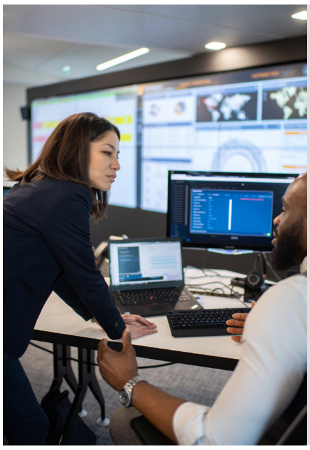
Intermediate level

Learning modern Wi-Fi hacking can be a pain. Several new advances in Wi-Fi security have been released, along with some new attacks. But public literature still has lots of outdated material for technologies we rarely see deployed in the real world anymore. Numerous tools overly rely on automation, and leave you wondering when they don't work, because neither the fundamentals nor underlying attack is understood. Even worse, some popular attacks will rarely if ever work in the real world.

If you want to really understand what's going on and master the attacks in such a way that you can vary them when you encounter real world complexities, this course will teach you what you need to know.

- Modern Wi-Fi hacking
- How to think about and adjust approaches when facing obstacles
- New approaches and tooling

Who the course is for:
This course is for anyone who wants to understand how to attack and defend Wi-Fi networks. It's an offensive course and has obvious benefits for pentesters and red teamers, however it's also essential for dis-abusing defenders of false notions of security as well as what defences have a meaningful impact.



SensePost

Want to know about us?

SENSEPOST
PART OF ORANGE CYBERDEFENSE

SensePost is the specialist pentesting arm of Orange Cyberdefense, renowned for its expertise, 19 year track-record and innovation on the frontlines of cybersecurity.

With team members that include some of the world's most preeminent cybersecurity experts, SensePost has helped governments, military organisations, and blue-chip companies both review and protect their information security and stay ahead of evolving threats.

SensePost is also a prolific publisher of leading research articles and tools on cybersecurity which are widely recognised and used throughout the industry and featured regularly at industry conferences including BlackHat and DefCon.