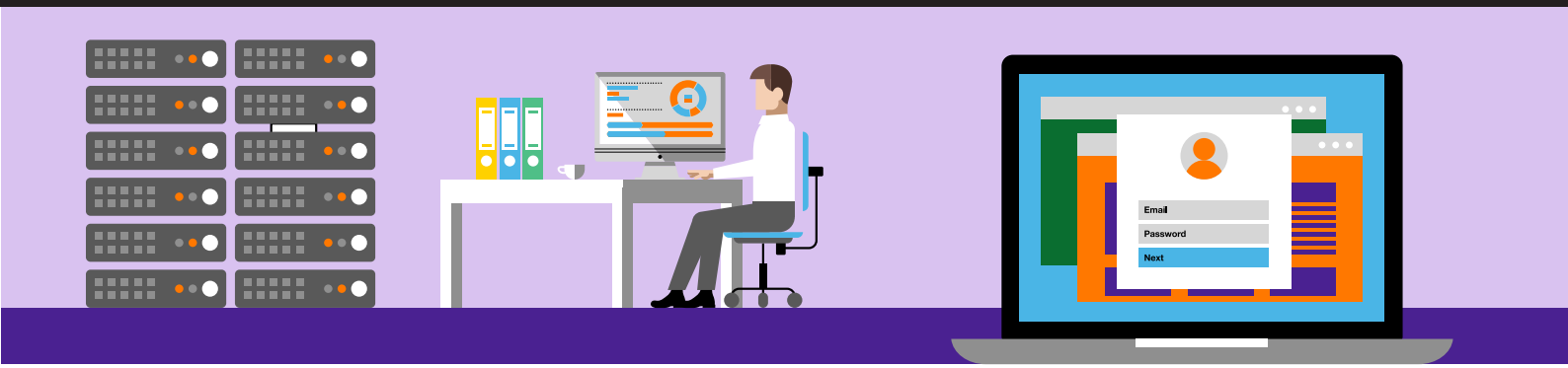
Orange Cyberdefense



SensePost training

Hands-On-Hacking fundamentals

Key benefits

Understand
How to think like a hacker.

Practical
The difference between finding known vulnerabilities and exploiting them, and finding unknown vulnerabilities and exploiting them.

Hands-on experience
How vulnerabilities can exist at different layers of the tech stack.

About the course

If you want to understand how criminals run hacking campaigns, and emulate them, this course is for you.

This is 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.

By the end of the course, you will have a good grasp of how vulnerabilities and exploits work, how attackers think about networks and systems and have compromised several of them from infrastructure to web applications to Wi-Fi.

Who is the course for

People wanting to get started with penetration testing including defenders, developers or administrators looking to better understand how attacks and attackers work to better defend their systems.

This is also very useful for managers of technical security teams looking to understand the work better.

HHF
SENSEPOST TRAINING

Why Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries.

We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Our Hacking training facility is delivered 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.

What is covered

Understanding the hacking mindset - the different ways hackers think, and hacking makes you think

- Much of hacking is looking at the world differently. By understanding the differences, both attacking and defending systems can be made easier

Setting up your environment, from getting your Kali ready to getting comfortable on the command line

- Getting your own set up going can be a daunting first task. We'll help you with what you need, how to set it up, and how to use it

Understanding vulnerabilities and exploits - how to find them and use them

- Understanding the difference between these concepts will help you find vulnerabilities and exploit them
- We start with vulnerability scanners, and move to exploitation of known vulnerabilities
- This section is focused on internal networks and related infrastructure

Finding and hacking Infrastructure over the internet

- Hacking over the Internet requires a different approach to the internal network. We'll show you how to find a target organisation's infrastructure on the Internet (the more you find the higher your chances of success)
- Technologies such as DNS and techniques such as OSINT are introduced
- Next we look at both the thinking and attacks required to penetrate the perimeter, including introductions to phishing, password spraying and network tunnelling

Hacking web applications and other custom applications

- Where prior content focused on finding and using known vulnerabilities, this section introduces bug hunting in custom applications, using web applications to teach the concept
- Attacks such as cross-site scripting and SQL injection are practised, as well as understanding the fundamentals of HTTP and intercepting proxies

Hacking wi-fi and traffic interception/analysis

- To complete our hacking overview, we move to attacking the network layer, with a focus on the physical layer in the form of Wi-Fi hacking as well as network traffic through person-in-the-middle (MitM) attacks and traffic manipulation
- Passive traffic interception, and active ARP spoofing attacks, as well as offensive traffic analysis in real applications will be discussed