



# Learn Hard. Hack Harder!

Offensive Security Course Brochure

# Introduction.

## We are SensePost Training.

A team within Orange Cyberdefense focused on ethical hacking specialised in offensive tactics, learnings and research.

Our team has been delivering security related trainings all over the planet for the last two decades; teaching real-world adversarial and industry leading techniques, tactics, procedures and methodologies to thousands of delegates at world renowned conferences and events.

Our trainings are developed from the work we perform as penetration testers and red team members further supplemented by in-depth research. This allows our trainings to be relevant, real-world centric and effective.

We are proud to say our trainings are delivered by active security analysts, researchers and penetration testers and are aimed at teaching through hands-on practice.

Explore our training courses and packages and find the solutions that could benefit yourself, team or organisation.

Have fun, hack hard and make a difference.

## SensePost Training

# Hands-On Hacking Fundamentals

BEGINNER LEVEL



### Overview

Our introductory hacking course is focused on the fundamentals of the security landscape, 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 from an offensive perspective. Understanding the approaches attacker take will greatly enhance the defensive requirements and understanding required to defend against these attacks.

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 an infrastructure, web application and Wi-Fi perspective.

### Who should attend

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

This is also very useful for managers of technical teams looking to upskill in security.

### Skills you'll learn



Hacker Mindset



Vulnerability discovery



Web Application Hacking



Wi-Fi Targeting

### Training in a glance

**4** core training modules

**21** sub-modules and learning objectives

**12** hands-on practicals

**16** hours of training

### Why our training is great

- ✓ Our training is provided by active penetration testers and security analyst
- ✓ Our training is hands-on with a course split of 40% theory and 60% practical
- ✓ We teach offensive methodologies to proactively enhance defensive thinking
- ✓ Each student gets their own lab environment during the course to practice real-world attacks

## SensePost Training

# Hands-On Hacking Fundamentals (Continued)

BEGINNER LEVEL



## Course Modules

1. Introduction To Hacking
  - Hacker mindset
  - Linux command line and usage
  - Risk and business related security
  - History and threat landscape
2. Understanding the Attack
  - Vulnerabilities VS Exploits
  - Attacker methodology
  - Target identification
  - Information gathering
  - Footprinting and fingerprinting
  - Vulnerability discovery
  - Exploits and payloads
3. Web Application Hacking
  - Web and HTTP fundamentals
  - Web application risks
  - Cookies / Hashes / Encoding
  - Person-in-the-Middle Proxies
  - OWASP Top 10
4. Wi-Fi Hacking
  - Wi-Fi fundamentals
  - Risks associated with Wi-Fi networks
  - Traffic monitoring and gathering
  - Capture and crack Wi-Fi password
  - Intercepting traffic

All modules contains several practical exercises and sub-objectives

## Key take-aways

How to execute attacks based on an attacker methodology and hacker mindset

A sound technical understanding of the security landscape, vulnerabilities and exploits

Fundamentals required to attack common Web Application and Wi-Fi vulnerabilities

## Prerequisites

No security or hacking experience is required. Basic exposure to the IT field is.

## What you'll need

A laptop with a modern browser (Chrome or Firefox)

Zoom and/or Microsoft Teams installed

A Discord account

## What you'll get

Access to our online class portal with lifetime access to the course resources and practical answer guides

Access to our realistic lab environment during the training to practice your newly taught skills

## Value for your organisation

A greater understanding of the potential threat landscape and what to expect from attackers

Increased security mindset that can actively be applied to everyday the everyday work environment and tasks at hand.

# Contact.

## Reach out to train with us!

Contact our training team for more information or to setup a detailed discussion to learn more about our trainings.

Training packages are available on request.

SensePost Training:

[training@orangecyberdefense.com](mailto:training@orangecyberdefense.com)