

TRAINING | Bootcamp



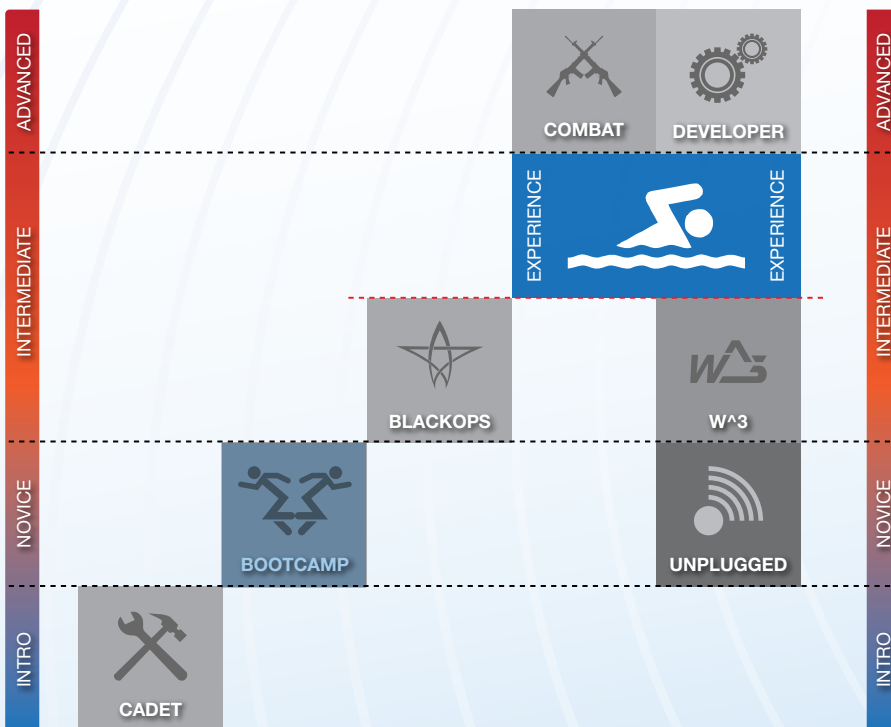
**Bootcamp Edition**

This course is the “How-did-they-do-that”? of modern hacking attacks.

From start to finish we will lead students through the full compromise of a company’s IT systems, explaining the tools and technologies but especially the thinking, strategies and the methodologies for every step along the way.

“Bootcamp Edition” will give students a complete and practical window into the methods and thinking of hackers. “Bootcamp” is SensePost’s “introduction-to-hacking” course. It is strongly method-based and emphasizes structure, approach and thinking relating to tools and tricks. The course is popular with beginners, who gain their first view into the world of hacking, and experts, who appreciate the structured approach.

**Training Overview**



**SensePost Information Security**

**Information Security**

As trusted advisors we deliver insight, information and systems to enable our customers to make informed decisions about Information Security that support their business performance.

SensePost is an independent and objective organisation specialising in Information Security Consulting, Training, Security Assessment Services and IT Vulnerability Management.

SensePost is about security. Specifically - Information Security. Even more specifically - measuring Information Security.

We’ve made it our mission to develop a set of competencies and services that deliver our customers with insight into the security posture of their information and information systems.

**Training Overview**

- Cadet Edition
- Cadet Online Edition
- Bootcamp Edition
- BlackOps Edition
- Combat Edition
- Unplugged Edition
- W^3 Edition
- Developer Edition

**What People Say**

*“The training from SensePost was one of the best I have ever attended! The SensePost courses are of a high standard and merit the highest recommendation.”*

## TRAINING | Bootcamp

### Content

“Bootcamp” Edition follows a strict method-based approach to teach the fundamental technical and thinking skills used for hacking over the network. The content of this course mirrors the methodology step-by-step:

#### 1. Introduction

- An introduction to method-based hacking
- A quick review of key concepts and technologies
- A method for hacking into computers over the network

#### 2. A Review of Reconnaissance

- Intelligence
- Footprinting
- Verification
- Vitality

#### 3. A Review of FingerPrinting

- Advanced Portscanning
- OS and Service Identification

#### 4. Vulnerability Discovery

- Reviewing basic vulnerability types
- Understanding vulnerability scanners
- Using vulnerability scanners
  - Nessus
  - Wikto

#### 5. Exploiting Vulnerabilities

- Understanding the link between exploits and vulnerabilities

- Exploiting known vulnerabilities
- The Metasploit Framework
  - Exploits without code
- Discovering and Exploiting new vulnerabilities

#### 6. Finding and Exploiting Vulnerabilities in Web Applications

- The issue with web applications
- Tools for attacking web applications
- The common web application vulnerability categories
- Hacking other custom applications
  - Web Services
  - Java
  - C#

#### 7. Owning the target

- The difference between exploiting and owning a system
- Building a channel
- Privilege Escalation
- Ensuring Repeat Access
- Hiding your tracks
- A strategy for phase 2

All of the areas above are illustrated with real-life technical labs capture-the-flag exercises.

### Context

This course follows directly on from “Cadet Edition” and serves as a prerequisite for the “BlackOps Edition”.

As always, the course can also be taken without any of the others. “Bootcamp Edition” can be taken back-to-back with either “Cadet Edition” (for beginners) or “BlackOps Edition” for more advanced students.

### Prerequisites

SensePost will provide fully configured laptop computers as well as CDs with all the tools and materials used on the course. Students need to ensure they have the necessary level of skill. No hacking experience is required for this course, but a solid technical grounding is an absolute must. Students are expected to be versed in basic programming or scripting, networking and Internet technologies, ‘nix and Windows operating systems, basic SQL and database technologies. No advanced skills are required, but students without a good, practical knowledge of these areas will fall behind in this fast-paced class. Students without the requisite technical skills are encouraged to consider “Cadet Edition”.

### Who Should Attend

Information Security Officers, System and Network Administrators, Security Consultants and Government Agencies will all benefit from the valuable insights provided by this class.

***“The “Bootcamp Edition” is SensePost’s “introduction-to-hacking” course.”***