navixia information security

sensepost

Infrastructure

Fight the hackers! This security training course will teach you about the art of offensive and defensive approaches. You will learn what tools and techniques hackers use in the wild and acquire a deep enough understanding to defend your organization against them.

Who should take this course?

This course is ideal for **those wanting to learn** how attackers are gaining access to networks, for **penetration testers** who are new to network penetration testing, and/or for **those who wish to brush up** on effective ways to own companies from the net and internally.

The course is also ideal for **administrators** who want to defend their infrastructure against these attacks.

Exploit and control common architecture and network deployments

This hands-on course looks at the methods and approaches attackers take when targeting organisations. Each student will have a fully functional network, simulating an organisation, with a target rich environment geared towards hacking with no bounds. Your aim will be to think like an attacker and map out your target, find weaknesses and fully exploit trust relationships in place. Using scenarios along with presentations, this course is a healthy mix of thinking, strategies and the methodologies you might need for every step along the way.

Owning the network

Keeping a global overview is key when targeting networks. Footprinting and fingerprinting your target is often overlooked. This module delves into the most efficient ways to enumerate targets, discover vulnerabilities and successfully exploit them.

SensePost training portal

SensePost have developed a training portal for students to interact with the trainers, keep updated on content and also download all files, slides and tools delivered during the course. This portal is made available to all students, even when the course has finished. In addition, SensePost have moved their training infrastructure into their own cloud, which means students get their own individual environments to test against, making use of VPN's and numerous targets. This gives a fully immersive experience of attacking real-world architecture and networks.

Course syllabus (2 days)

- *Perform reconnaissance against your target*
- *Footprinting and fingerprinting*
- *Technical exploitation*
- *You've found a way in, now what?*
- *Attribution*
  Hiding in the shadows
- *Post exploitation Passwords, tokens, data and more*
- *Moving Laterally - Compromising other hosts*
- *Attacking active directory*
- *Hunting down mission critical systems and key players*
- *Cracking passwords and getting into corporate emails*
- *Exfiltration techniques*

SensePost

Security specialist company SensePost is one of Black Hat Briefings' longstanding training partners. Over the years, SensePost have taught thousands of students about the art of offensive and defensive approaches. They have long been a trusted partner of Navixia.