Orange Cyberdefense

SensePost training

Red Teaming

Key benefits

Understand
Understanding how real criminal hackers work.

Practical
A practical red teaming approach.

Hands-on experience
A significant amount of hands-on experience with tools many pentesters don't know about.

About the course

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.

Our red team experience in going after critical business systems, from cross-border financial systems to large SCADA systems and the paths and techniques to get there are distilled into this course and taught by our senior analysts.

Who is the course for

Experienced penetration testers, network administrators, red/blue teams, security professionals, and IT security enthusiasts who have a need to acquaint themselves with real-world offensive tactics, techniques and tools.

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

Exploitation via phishing

- Stalking target employees and crafting approaches and pretexts

Malware delivery vectors, loaders, FUD AV bypass including real malware samples

- Evasion techniques such as polymorphic crypter
- Using GauDox loaders and FrauDox evasion
- Advanced usage of tools like Empire, Metasploit and Cobalt Strike

Privesc and low noise persistence

- Smart privesc
- Evading EDR detections
- Persisting for repeat access over the long term
- Dealing with different architectures
- Physical device implants

Stealth lateral movement and living off the land

- Finding pivots without triggering detections
- Using the access you have and the myth of always needing administrator privileges
- Understanding tools vs detection trade offs
- Advanced Active Directory compromise

Unusual C2's and hiding in plain sight

- DNS, DNS over HTTPS, and Exchange based C2s
- Egress and exfiltration testing

Ransomware

- Deploy ransomware samples

Emulating real threats - stealing money and other stories

- Understanding segregation of duties and reconciliations
- The importance of smart targeting
- How to take your test as far as possible without breaking the law