Orange Cyberdefense

SensePost training

Infrastructure Hacking

Key benefits

Understand
How to hack corporate networks.

Practical
Methodologies for repeat successes.

Hands-on experience
How the blue team could detect you.

About the course

This course is all about compromising companies through their infrastructure. Aimed at beginner penetration testers and technically included people wanting to understand how to go about compromising their companies through their infrastructure and how to defend it, this course will take you on a journey from learning about an organisation right through to stealthy exploitation of their critical infrastructure.

This year we've added a new section on Blue Teaming to help defenders learn how to defend against what's been learned, and penetration testers better understand how they could be detected.

Please be advised that this a follow on from our 'Hands on Hacking Fundamentals' course.

Who is the course for

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

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

Introduction to a hacking methodology, how to repeatably compromise organisations without merely relying on common tricks

- How learning the trade, and not just the tricks will allow you to think through a threat model to find the gaps in an organisation's defences

Intelligence - organisation OSINT, understanding the business, how that is represented by their technology and how to examine it

- How Google and investor reports can guide your attack
- Common and not so common sources of information on organisations and how to turn passwords dumps and pastebins into searchable directories

Footprinting - finding targets and understanding what you are likely to get from pursuing them. How to identify common and uncommon paths to the internal network as well as poorly secured targets the IT team may not know about

- How technologies such as DNS, Whois, BGP, and certificate transparency can be used to find an organisation's targets

Fingerprinting - discovering the technology and architecture used by the targets, and what attack approaches these require, as well as how to balance your time to optimise for compromise

- Advanced service identification and gotchas to speed up enumeration across large networks
- Methods of stealthy or passive fingerprinting

Vulnerability identification

- Common and not so common types of vulnerabilities, and how to find them
- Vulnerability scanners for different technologies and protocols
- Stealthy vulnerability identification

Exploitation - the biggest section in the course! Exploiting users, different operating systems, databases, protocols such as SMB and more

- Different exploitation frameworks such as Metasploit, Empire and Cobalt Strike
- The difference between exploits, droppers and payloads
- Physical access exploitation of different operating systems
- Hacking people and processes
- Common low hanging fruit on internal networks and how to find them quietly
- Credential abuse
- SMB Exploitations
- Fuzzybunch, Wannacry and Eternalblue
- Exploiting databases

Post-Exploitation - network tunnelling, privilege escalation, PowerShell/C# local exploits, anti-virus bypass, password cracking and more

- Privilege escalation across the network with a focus on Active Directory exploitation
- Host-based privilege escalation both on Windows and Linux systems
- Understanding and exploiting credential storage on Windows
- Understanding, exploiting/using and cracking hashes
- PowerShell and C# based post-exploitation tool kits
- Basic anti-virus/EDR evasion

Red teaming introduction - an introduction to red teaming and the differences in approach

- The differences in goal between penetration tests and red teams
- The differences in approach between penetration tests and red teams
- How blue and red teams can ensure maximum benefit to the target organisation - from scoping to operations to purple teaming

Blue teaming introduction (half day)

- An introduction to blue team theories and how it is changing approaches on both the red and blue side
- Putting together detection infrastructure using Windows Event Forwarding, Sysmon and Elastic stacks
- Detecting and alerting on the fingerprinting, exploitation and post-exploitation activities discussed in previous section