Orange Cyberdefense

SensePost training

Unplugged: Modern Wi-Fi Hacking

Key benefits

Understand
How to think like a hacker.

Practical
The difference between finding known vulnerabilities and exploiting them, and finding unknown vulnerabilities and exploiting them.

Hands-on experience
How vulnerabilities can exist at different layers of the tech stack.

Our Expertise
We 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 Black Hat briefings longstanding training partners, our courses have taught thousands of students about the art of offensive and defensive approaches.

About the course

If you want to learn how to understand and compromise Wi-Fi networks, this is your course.

If you want to really understand what's going on and master the attacks in such a way that you can vary them when you encounter real world complexities, this course will teach you what you need to know.

This course is highly practical, with concepts taught through theory delivered while your hands are on the keyboard, and semi-self-directed practicals at the end of each section to reinforce the learning. The course is hosted in a "Wi-Fi in the cloud" environment we invented several years ago, which means no more fiddling with faulty hardware or turning the classroom into a microwave.

Who is the course for

This course is for anyone who wants to understand how to attack and defend Wi-Fi networks. It's an offensive course and has obvious benefits for pentesters and red teamers, however it's also essential for disabusing defenders of false notions of security as well as what defences have a meaningful impact.

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.

What is covered:

How Wi-Fi hacking fits into wider attack or defence objectives.

Important physical and low level RF concepts and how to reason through/debug strange situations.

Understanding how monitor mode works, when to use or not use it, and practical examples of what to do with collected frames or data.

Grokking the WPA2 4-way handshake and the numerous ways of recovering PSKs and what do with them.

First looks at attacking WPA3's Dragonfly handshake with downgrades.

Grokking EAP & EAP vulnerabilities relating to certificate validation, tunnelled mode key derivation and how to practically attack them with downgrades, relays and manipulating state.

Online training environment

We've setup the whole course with Katakoda to host our "WiFi in the cloud" environment we invented several years ago. This ensures students can interact with the labs and content online during the course. This means no more fiddling with faulty hardware or turning the classroom into a microwave.

Also, we strive to make the theory as practical as possible and break away from death by slides, we want students to walk away with a strong understanding of the topics and demonstrative practical experience.

Who should take this course

This course is for anyone who wants to understand how to attack and defend Wi-Fi networks. It's an offensive course and has obvious benefits for pentesters and redteamers,however it's also essential for disabusing defenders of security, aswell as what defences have a meaningful impact.

Why should you take this course?

Take this course if you want to learn WiFi fundamentals well enough to adjust approaches when the basics aren't working. Take this course to learn about new WiFi security protocols like WPA3 and OWE. Take this course to learn about newer WiFi attacks like EAP tunnelling (sycophant), LootyBooty (EAP-GTC downgrade), PMKID cracking and more.

Top 3 takeaways:

Modern WiFi hacking
How to think about and adjust approaches when facing obstacles
New approaches and tooling

Student requirements

Students should have at least a basic understanding/familiarity with the Linux command line. Prior Wi-Fi hacking experience will help but is not required. The practicals are designed so that more advanced students can progress further and students new to the field can complete the base requirements.