Orange Cyberdefense

SensePost Training

Unplugged: Modern Wi-Fi Hacking

INTERMEDIATE TO ADVANCED LEVEL

Overview

Wireless networks are the backbone of our day-to-day life. We all rely on them to provide us access but rarely ever think about the access we could achieve through compromising them.

Learning about modern Wi-Fi hacking can be a pain. Several new advances in Wi-Fi security have been released, along with some new attacks. But public literature still has lots of outdated material for technologies we rarely see deployed in the real world anymore. Numerous tools overly rely on automation, and leave you wondering when they don't work, because neither the fundamentals nor the underlying attacks are understood. Even worse, some popular attacks will rarely work in the real world.

Our course will change that and expose you to the fundamentals and the techniques used to approach and attack wireless networks to achieve real world compromise and overcome complexities.

Who should attend

This is aimed at intermediate penetration testers or technically minded people wanting to understand how to go about compromising their organisation to better defend it.

This course is also helpful for network defenders, architects and administrators.

Skills you'll learn

- Wireless Fundamentals
- Exploiting Wi-Fi
- Attacking Enterprise Networks
- Monitoring Traffic

Training in a glance

7 core training modules

18 sub-modules and learning objectives

18 hands-on practicals

32 hours of training

Why our training is great

- Our training is provided by active penetration testers and security analyst
- Our training is hands-on with a course spilt of 40% theory and 60% practical
- We teach offensive methodologies to proactively enhance defensive thinking
- Each student gets their own lab environment during the course to practice real-world attacks

training@orangecyberdefense.com

orangecyberdefense.com

Orange Cyberdefense

SensePost Training

Unplugged: Modern Wi-Fi Hacking

INTERMEDIATE TO ADVANCED LEVEL

Course Modules

1. Introduction To Wi-Fi Fundamentals
2. Monitor Mode
3. Probing, Tracking & Deanonymisation
4. WPA/2/3 PSK
5. EAP
6. EAP-TLS
7. Tunnelled EAP Relays

All modules contains several sub-modules and practical exercises.

The above provides a summarised course outline, full course outline available on request.

Key take-aways

Greater understanding of the risks associated with wireless networks

A good understanding of the tools and techniques for attacking Wi-Fi solutions

Practical skills to exploit a wide variety of Wi-Fi flaws and vulnerabilities

Prerequisites

A strong familiarity with Linux command line usage and basic security concepts.

A solid understanding of networks are a must.

What you'll need

A laptop with a modern browser (Chrome or Firefox)

Zoom and/or Microsoft Teams installed

A Discord account

What you'll get

Access to our online class portal with lifetime access to the course resources and practical answer guides

Access to our realistic lab environment and attack network during the training

Value for your organisation

Understanding the potential risks associated to wireless networks and the threats your organization may be susceptible to from a perimeter perspective.

Practical exposure to exploitation of Wi-Fi related issues leading to better defensive approach to be developed..

training@orangecyberdefense.com

orangecyberdefense.com