TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

SensePost Unplugged; Modern WiFi Hacking

Date of the training: **March 16-17, 2020** in Heidelberg, Germany

Book now using the voucher code: **TR20_HMTS** and save an additional 5% of the current valid rate of any package!

Overview

If you want to learn how to understand and compromise Wi-Fi networks, this is your course. Learning modern Wi-Fi hacking can be a pain. There is lots of outdated material for technologies we rarely see deployed in the real world anymore.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 underlying attack is understood. Even worse, some popular attacks will rarely if ever work in the real world.

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. We've been pentesting Wi-Fi networks for nearly two decades and have built some popular Wi-Fi hacking tools such as Snoopy and Mana.

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.

Learning Objectives

- How Wi-Fi hacking fits into wider attack or defense 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, tunneled mode key derivation and how to practically attack them with downgrades, relays and manipulating state.

Prerequisites

Students should have at least a basic understanding/familiarity with the Linux command line. Some prior Wi-Fi hacking experience is required, in particular knowledge and use of monitor mode, deauthing and capturing/cracking WPA2 handshakes. The practicals are designed so that more advanced students can progress further and students new to the field can complete the base requirements.

Requirements

A device with a working web browser and comfortable keyboard is all that is required. Practicals are hosted at katacoda.com. This page[1] can be used to test compatibility and give you a feel for the practical environment.

[1] https://katacoda.com/singe/scenarios/monitor-mode

About the Trainer

SensePost has been hacking for two decades… we pride ourselves to be contributors to the industry by sharing knowledge on a regular basis.

Booking

Recommended online booking of trainings through:
https://troopers.de/tickets/

Voucher code: TR20_HMTS
Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German. +49 151 16228365 or info@troopers.de

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany
+49 6022 508200 / info@hmtrainingsolutions.com
+49 6022 5089999 / www.hmtrainingsolutions.com