TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Software-Defined Radio applied to security assessments

Date of the online training: **March 22-25, 2021**

Overview

In this 4-day training, students will learn about software-defined radio applied to security and will get survival reflexes and methods to test real-world radio devices (intercoms, cars, industrial modules, mobile phones, various remote controls, as well as other IoT systems).

Compared to other courses that teach how to use public tools, this class is more about understanding how these tools work and also how to build proper tools to analyze and attack targeted systems

All techniques here will demonstrate real uses-cases encountered in pentests and Red Teams, but also techniques that aim to be applied to future systems, by teaching important steps when dealing with unknown targets.

All students will also receive a Software-Defined Radio kit to send and receive in full-duplex to continue hacking in the wild.

ERNW Enno Rey Netzwerke GmbH
Carl-Bosch-Str. 4
69115 Heidelberg
info@ernw.de

Tel. +49 – 6221 – 48 03 90
Fax +49 – 6221 – 41 90 08
BIC: GENODE61HD3
IBAN: DE43 6729 0100 0059 7891 04

Managing Directors
Florian Grunow
Michael Schaefer
VAT-ID: DE 813 376 919

What we will teach

With this class students will learn how to find interesting radio-communications and ways to attack targeted systems:

- Learn how radio works and about actual technologies using this interface
- Find and analyze a signal
- Modulate and demodulate a signal
- Encode and decode data meant to be transported over-the-air
- Capture, generate, replay and analyze a signal
- Interface with a signal using SDR devices and software
- Get primary reflexes to attack embedded and IoT systems
- Create your own tools with the GNU Radio framework and its alternatives
- Learn how to use SDR and classical attacks on mobile 2G/3G/4G, RFID/NFC, LoRa(WAN), wireless mousses/keyboards/presenters, sub-GHz remotes/alarms, and other similar or custom technologies

DAY 1 - RF PRELIMINARIES

Day 1 is an introduction to radio that will help students to learn its concepts and the techniques used today to receive and transmit signals, but also the constraints that we have to deal with in heterogeneous environments:

DAY 2 - HANDS-ON RADIO

Day 2 will put the student in the playground of the Software-Defined Radio, where every idea can be written on software to be simulated, and then concretized to realize receivers and transmitters depending on the chosen hardware limitations.

DAY 3 - ATTACKING PHYSICAL INTRUSION SYSTEMS

Day 3 will put the student in the playground of the Software-Defined Radio, where every idea can be written on software to be simulated, and then concretized to realize receivers and transmitters depending on the chosen hardware limitations.

DAY 4

Day 4 will focus on attacking custom RF devices but also devices used in industrial systems using LPWAN technologies such as the LoRa(WAN), but also other technologies like Power-Line Communications systems, and how to manage to do testbeds many current technologies. We will also introduce devices that could act like unexpected implants and ways to analyze them. Then we will finish with an introduction to hardware hacking that could be complementary to RF hacking by talking about survival and practical reflexes, as well as methods to interface with hardware.

Who should attend this training?

- Security researchers and pentesters
- Embedded developers who want to improve the security of their products

Prerequisites

- Knowledge of Linux and a programming language such as C, C++, C# or Python is necessary
- Understanding of pentesting (network and applications) or Red teaming
- Basic knowledge of radio is not mandatory but is a plus

Requirements

- All attendees will need to bring a laptop capable of running VMware virtual machine (8GB of RAM is a minimum)

About the Trainer

Sébastien Dudek is a security researcher at Trend Micro and is also the founder of the PentHertz consulting company specialized in wireless and hardware security. He has been particularly passionate about flaws in radio-communication systems, and published research on mobile security (baseband fuzzing, interception, mapping, etc.), and on data transmission systems using the power-line (Power-Line Communication, HomePlug AV) like domestic PLC plugs, as well as electric cars and charging stations. He also focuses on practical attacks with various technologies such as Wi-Fi, RFID, and other systems that involve wireless communications.

Booking

Recommended online booking of trainings through:

https://troopers.de/tickets/

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German. +49 6221 480390 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