rfhwsdr

Original file

COURSE DESCRIPTION:

In this 3-day training, students will learn about Software-Defined Radio applied against physical intrusion systems (alarms, intercoms, various remotes, etc.). This course provides basics, survival reflexes when testing real-world radio devices, and methods to go further. 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.

The training

The training will provide strong feedback and techniques when attacking radio devices in non-perfect environments and ways to succeed your pentests or red team tests. Students will also get hardware to play at home including a SDR to transmit and receive signal and RF transmitter that could be customized and continue to practice after the training.

In addition to the course, **students will receive:** a Tx/Rx full-duplex device, that could be tuned to 70 MHz to 6000 MHz with 20 MHz bandwidth, to continue to play at home.

Day 1 - RF preliminaries

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

- **Introduction to radio**
  - **History, evolution, and EU regulations**
  - **Radio waves**
  - **Digital Signal Processing**
  - **Software-Defined Radio**
  - **Antennas**
  - **Amplifiers and connectors**
- **Software-Defined Radio devices**
  - **Specifications**
  - **How to choose them**
  - **Few tips and hacks**
- **Observations**
  - **Waterfall and spectrum analyzers**
  - **Signal identification**
  - **Modulation/Demodulation**
  - **Encoding/Decoding**
- **Faraday cages and how to design a very cheap one**
- **Use of attenuators and software gain parameters**

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 a software to be simulated, and then concretized to realize receivers and transmitters depending on the chosen hardware limitations:

- **Introduction du GNU Radio**
- **Software-Defined Radio processing in the chain**
- **Practice with GNU Radio Companion**
    - **Block schemas**
    - **Parameters**
    - **Generators**
    - **Sinks and sources**
    - **Operators**
    - **Simulations**
    - **Modules**
    - **Executing a block in a real SDR device**
    - **Working with analogical and binary modulations**
    - **Transferring a simple signal**
    - **Optimizing samples processing**
    - **Features to process samples**
- **Investigation and handy tools**
- **Alternative to GNU Radio**

Day 3 - Attacking physical intrusion systems

Day 3 resumes and applies previous chapters to study physical intrusion systems and brings useful tricks for Red Team tests as well as pentests:

- **Common sub-GHz Remotes**
    - **Introduction**
    - **Capturing data**
    - **Replaying saved samples**
    - **Analyzing samples (manually and with powerful tools)**
    - **Rolling codes security**
- **Devices using the mobile network (2G/3G/4G**
    - **Introduction**
    - **Monitoring**
    - **Mobile security**
    - **Existing tools**
    - **Interception techniques**
    - **Our feedback in missions**
    - **Tooling with GNU Radio**
- **Attacking physical accesses and custom devices**
    - **Introduction**
    - **Identification (looking at device’s references, components, etc.)**
    - **Sniffing and decoding signals**
- **Introduction to hardware hacking**

WHO SHOULD ATTEND?

This course is intended for any:

- **pentesters who do not want to be limited by public radio tools**
- **developers who want to debug and test their wireless devices**
- **people curious about SDR and security**
- **security researchers.**

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**
- **All attendees will need to bring a laptop capable of running VMware virtual machine (8GB of RAM is a minimum)**
- **Basic knowledge of radio is not mandatory but is a plus.**

ABOUT THE TRAINER:

Sébastien DUDEK is a security researcher at Trend Micro and founder of the PentHertz company specialized in radiocommunication and hardware security. He has been particularly passionate about flaws in radio-communication systems, and published researches 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.