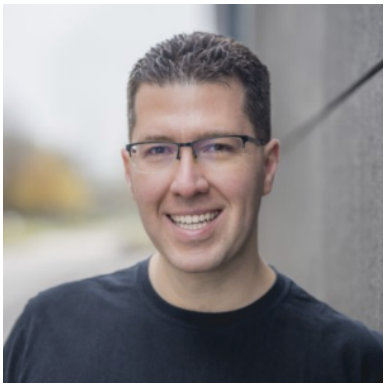
IOT SECURITY TRAINING

Pablo Endres



COURSE OBJECTIVES

This is a hands-on IoT hacking class. It covers all aspects of IoT Security, from the technologies and testing methodologies to the vulnerabilities. The main focus is offensive security: attacking and testing the devices and platforms. We first cover the basics and lay out the ground with concepts before diving into the actual hacking. This provides the understanding of what and why the things can be hacked, with a good mix of knowledge and learning-by-doing or in this case learning-by-hacking.

TRAINING OUTCOMES

After the class, the attendees will be able to evaluate the security of different IoT architectures, identify the attack surface, knowledge of security testing methodologies and how to use them, dump, extract and analyze device firmware, hack UART, SPI, I2C and JTAGs, debug and attack hardware and software, analyze protocols, attack radio and wireless communications like BLE, Zigbee, and custom protocols and much more.

WHO SHOULD ATTEND?

> All kinds of professionals with an understanding of IT or hacking
> Anyone interested in learning IoT device hacking
> Security Professionals
> IT Professionals
> Embedded Security Enthusiasts

ABOUT THE TRAINER

Pablo Endres is the founder and CEO of SevenShift GmbH, an IoT boutique security company. He is an experienced Security Consultant, Professional Hacker, Technological Solution Architect and published author. He is a computer engineer, and he holds a handful of security certifications ISC2 CISSP, CompTIA Security+, and ISECOM's OPSA + OPST. Pablo's career has taken place mostly doing security in a variety of industries, like wireless phone, VoIP solution and Cloud Service providers, Banks, contact centers and university labs. Pablo has founded multiple companies in different continents and enjoys hacking, IoT, reverse engineering, teaching, working with new technologies, startups, collaborating with Open Source projects, learning new things, teaching, networking and being challenged. In the last

couple of years, he has been working mainly in IoT security, testing dozens of devices and working with multiple platform providers to secure their solutions.

WHAT TO BRING

Laptop that meets the following requirements:

- 64-bit processor with 64-bit operating system
- VT or other 64-bit virtualization settings enabled in your BIOS to run 64-bit VMs
- At least eight (8) GB of RAM, recommended sixteen (16) GB if possible
- At least fifty (50) GB of free hard drive space
- VMware Player 12 (or later), VMware Workstation 12 (or later), or VMware Fusion 8 (or later) installed BEFORE class begins. Other virtualization software such as Parallels, VirtualBox, or earlier versions of VMware products may work if the attendee is familiar with its functionality and takes full ownership of its configuration, however non-VMware software is not officially supported and VMware should be pre-installed as a backup just in case.
- Access to an account with administrative permissions and the ability to disable all security software on their laptop such as Antivirus and/or firewalls if needed for the class.

WHAT WILL BE PROVIDED?

Students will receive a free IoT Hacking Kit (hardware with a value of +350 Euros), which contains the tools and some vulnerable devices used in class, so that they can continue sharpening their skills or hack devices after the event.

PARTICIPANT SKILL SET

Basic knowledge of Linux or UNIX (especially bash) and security is always an advantage, but not required. It is assumed that attendees will have no knowledge of the topics of the class.

CLASS SYLLABUS [1]

Wednesday, 13 September 2023 - Day 1

Lecture 1 - IoT Security Concepts

- Evaluate the security of different IoT architectures
- Identify the attack surface

Lecture 2 - IT and IoT Pentest methodologies and frameworks

Lecture 3 - Bluetooth: classic and BLE

- Concepts
- Sniffing
- MiTM attacks and proxy attacks

Thursday, 14 September 2023 - Day 2

Lecture 4 - Firmware

[1] Schedule of lectures on the specified days may be subject to changes

- > Definitions
- > Dump, extract and analyze device firmware
- > Emulate parts of and entire firmware
- > Adding a backdoor and re-building firmware

Lecture 5 - Hardware and debugging interfaces

- > Electronics 101
- > Serial interfaces: UART, SPI, I2C and JTAG
- > Extracting firmware and data from EEPROM chips
- > JTAG debugging, exploitation

Friday, 15 September 2023 - Day 3

Lecture 6 - Software defined radio

- > Concepts
- > Sniffing and reversing radio frequencies
- > Working with 433 MHz: rx, tx, decoding

Lecture 7 - Zigbee

- > Concepts
- > Working with Zigbee: rx, tx, decoding
- > Hacking Zigbee