Publication date : 08/23/2024

Course : Hacking and Pentesting: IoT

Practical course - 3d - 21h00 - Ref. HIO
Price : 2100 € E.T.

4,2 / 5

The Internet of Things (IoT) is evolving rapidly, and has become an integral part of our daily lives, which is why it is one of the major challenges facing IT security. We need to know about their vulnerabilities to be able to trigger the appropriate response and raise the level of security.

Teaching objectives

At the end of the training, the participant will be able to:

- Defining the impact and scope of a vulnerability
- Understand hacker techniques and counter their attacks
- Measuring the security level of a connected object
- Perform a penetration test

Intended audience

Security managers and architects. System and network technicians and administrators.

Prerequisites

Good knowledge of IS security, networks, systems (especially Linux) and programming. Or knowledge equivalent to that of the Systems and Network Security, Level 1 course (ref. FRW).

Course schedule

1 A reminder of IoTs (Connected Objects)

- The different types of IoT (Connected Objects).
- Wireless protocols (WiFi...) and their ranges (operating distance). Links with M2M.
- Architectures: ARM, MIPS, SuperH, PowerPC.

2 Hacking and security

- Forms of attack, modus operandi, players, stakes.
- Audits and penetration tests.

PARTICIPANTS

Security managers and architects. System and network technicians and administrators.

PREREQUISITES

Good knowledge of IS security, networks, systems (especially Linux) and programming. Or knowledge equivalent to that of the Systems and Network Security, Level 1 course (ref. FRW).

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

3 The IoT environment

- Network: 4G, LTE, LoRA, WiFi, MQTT, 802.11.15.4, ZigBee, Z-Wave, 6LoWPAN and BLE (Bluetooth LE).
- Application: Web App, Mobile App, Web, mobile or API (SOAP, REST).
- Firmware, the device's operating system: Windows, Linux x86/x64 bits or Raspbian.
- Encryption: protects communications and data stored on the device.
- Hardware: chip, chipset, Storagestorage, JTAG, UART ports, sensors, camera, etc.), port, sensor, camera.
- Architecture: ARM, MIPS, SuperH, PowerPC.
- System structure, components, protection and updates.

Hands-on work
Collect the information (hardware, chip, etc.) making up the connected object.

4 Vulnerabilities

- The search for vulnerabilities.
- Connected object links to a network.
- Authentication mechanisms.
- Installation search and default password.
- Intrusion testing methodology for IoTs (Connected Objects).
- Tools: logic analyzers, debuggers, disassemblers and decompilers.

Hands-on work
Measure the security level of an IoT (Connected Object).

5 The attacks

- Software (XSS, SQLi, command injection, mishandled exceptions and RCE or DoS memory corruption attacks).
- Hardware (JTAG, SWD, UART, SPI, I2C bus, etc.).
- Wireless connectivity, communication protocol. Emission analysis.

Hands-on work
Access a connected object via various attacks. Perform a penetration test.

6 The audit report

- Contents.
- Sections not to be overlooked.

Hands-on work
Complete a pre-filled report.

Dates and locations

REMOTE CLASS
2026 : 15 June, 14 Dec.

PARIS LA DÉFENSE
2026 : 15 June, 14 Dec.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.