Publication date : 02/16/2024

Course : Hacking and Pentesting: embedded architectures

Practical course - 4d - 28h00 - Ref. HAE
Price : 2890 CHF E.T.

The basic architecture is usually made up of a central processing unit (CPU), an operating system (or specific software) and its connectivity: these are all components vulnerable to attack, which need to be assessed and protected, not forgetting the countermeasures to be deployed.

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 an embedded architecture
- 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 the course "System and network security, level 1" (ref. FRW).

Course schedule

1 Embedded architectures

- Ordinary and embedded computer systems.
- The different types of embedded architectures.
- The various constraints linked to the embedded solution.

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 the course "System and network security, level 1" (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 embedded environment

- Network: 4G, LTE, LoRA, WiFi, MQTT, 802.11.15.4, ZigBee, Z-Wave, 6LoWPAN and BLE (Bluetooth LE).
- 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.

4 Embedded architecture vulnerabilities

- The search for vulnerabilities.
- Authentication mechanisms.
- Connections between an embedded system and its environment (connectivity): network, sensor and peripheral.
- Identify and use applications and programs hosted on an embedded system.
- Intrusion testing methodology.
- Tools: analyzers, debuggers, disassemblers and decompilers.

Hands-on work

Measure the security level of an embedded architecture.

5 The attacks

- Physical attacks.
- Hardware: access to various components.
- Wireless connectivity, communication protocol. Emission analysis.
- Software: file system structure, vulnerability of hosted applications, access to services via applications.
- Testing exception handling with a program, exhaustion attacks.
- System reprogramming.
- Introduction of falsified information.

Hands-on work

Access an embedded system 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.

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.