Publication date : 01/31/2024

Course : Intrusion testing, organizing your audit

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

4,6 / 5

Intrusion testing, or Pentesting, is a technical procedure used to determine the real potential for intrusion and destruction of an IS infrastructure by a hacker. This course presents the approach and tools needed to carry out this type of test, and to write the final audit report in a professional manner.

Teaching objectives

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

- Acquire a methodology for organizing a penetration test-type security audit of your IS
- Write a final report following an intrusion test
- Formulate safety recommendations

Intended audience

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

Prerequisites

Good knowledge of IT security (hardware, network architectures, application architectures). Experience required.

Practical details

Teaching methods

After a first day dedicated to reminders and preparation of the environment, the following days will be devoted to carrying out intrusion tests in real-life situations.

Course schedule

1 The threats

- Developments in IS security.
- The current state of IT security.
- The hacker mindset and culture.
- What are the risks and threats?

PARTICIPANTS

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

PREREQUISITES

Good knowledge of IT security (hardware, network architectures, application architectures). Experience required.

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.

2 Audit methodology

- The regulatory context.
- The benefits of performing a penetration test, a Pentest, the different types of Pentest.
- How to integrate penetration testing into an overall security process.
- Learn how to define a security management policy and an iterative Pentest.
- Organize and plan the intervention. How to prepare the repository?
- The technical scope of the audit. Performing the Pentest.

Hands-on work
Perform an audit.

3 Pentest tools

- What tools should you use? Are they really essential?
- Information acquisition. Access acquisition.
- Elevation of privileges. Maintaining access to the system.
- Scan and network tools.
- System and Web analysis tools.
- Tools for attacking employees.
- What tools can be used to maintain access?
- Operating frameworks.

Hands-on work
Handling Pentest tools. Use of scanning tools.

4 Report writing

- Collect information.
- Document preparation and report writing.
- Overall system security analysis.
- Describe the vulnerabilities found.
- Formulate safety recommendations.

Group discussion
Production of a report following an intrusion test.

5 Case studies

- Interception of insecure HTTP or HTTPS flows.
- Intrusion test on an IP address.
- Intrusion testing of client-server applications: FTP , DNS , SMTP.
- Web application penetration testing (SQL Injection, XSS, PHP module and CMS vulnerabilities).
- Internal penetration tests: compromise via a booby-trapped USB key and a malicious PDF.

Hands-on work
Participants will audit a corporate network based on a real-life scenario.

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.

Dates and locations

REMOTE CLASS
2026 : 2 June, 22 Sep.