Publication date : 07/30/2024

Course : Cybersecurity, testing environments

attack, detect, collect and analyze

Practical course - 3d - 21h00 - Ref. CTE

Price : 2100 € E.T.

3,8 / 5

This advanced training course will teach you the techniques you need to measure the security level of your Information System. Following these attacks, you will learn how to trigger the appropriate response and raise the security level of your network.

Teaching objectives

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

- Understand hacker techniques and counter their attacks
- Measure the security level of your Information System
- Perform a penetration test

Intended audience

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

Prerequisites

Good knowledge of IS security, networks and systems (especially Linux).

Course schedule

PARTICIPANTS

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

PREREQUISITES

Good knowledge of IS security, networks and systems (especially Linux).

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.

1 Web attacks

- OWASP: organization, chapters, Top10, manuals, tools.
- Discover the infrastructure and associated technologies, strengths and weaknesses.
- Client side: clickjacking, CSRF, cookie theft, XSS, components (Flash, Java). New vectors.
- Server side: authentication, session theft, injections (SQL, LDAP, files, commands).
- Inclusion of local and remote files, cryptographic attacks and vectors.
- Evasion and bypassing protection: WAF bypass techniques, for example.
- Burp Suite tools, ZAP, Sqlmap, BeEF.

Role-playing

Presentation and familiarization with environments and tools. Implementation of various Web attacks in real-life conditions on the server and client sides.

2 Detecting intrusions

- Operating principles and detection methods.
- Market players, overview of systems and applications.
- Network (Nmap) and application (Web applications) scanners.
- IDS (Intrusion Detection System).
- The advantages of these technologies, and their limitations.
- How do you place them in your enterprise architecture?
- Market overview, detailed SNORT study.

Role-playing

Presentation and familiarization with environments and tools. Installation, configuration and implementation of SNORT, writing attack signatures.

3 Information gathering

- Heterogeneous sources. What is a safety event?
- Security Event Information Management (SIEM). Events collected from the IS.
- Equipment system logs (firewalls, routers, servers, databases, etc.).
- Passive collection in listening mode and active collection.

Role-playing

Log analysis procedure. Geolocating an address. Correlating logs from different sources, visualizing, sorting and searching for rules.

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 : 24 June, 7 Oct., 9 Dec.

PARIS LA DÉFENSE
2026 : 24 June, 7 Oct., 9 Dec.