orsys TRAINING 50 YEARS

Publication date : 03/15/2024

Course : Forensic analysis

Practical course - 3d - 21h00 - Ref. AFB
Price : 2470 CHF E.T.

★★★★⯪ 4,8 / 5

Post-mortem analysis (also known as inforensic) of IT security incidents has become essential for preserving evidence. Following simulated attacks, you will learn how to collect and preserve evidence, analyze it and improve IS security after the intrusion.

Teaching objectives

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

- ✓ Master the right reflexes in the event of machine intrusion
- ✓ Collect and preserve the integrity of electronic evidence
- ✓ Analyze intrusion a posteriori

Intended audience

Systems and network engineer/administrator.

Prerequisites

Good knowledge of IT security and networks/systems. Must have taken the course "Collecting and analyzing logs, optimizing your IS security".

Course schedule

1 How do you manage an incident?

- Signs of successful IS intrusion.
- What have the hackers achieved? How far did they get?
- How do you react to a successful intrusion?
- Which servers are affected?
- Find the entry point and fill it.
- The Unix/Windows toolbox for evidence retrieval.
- Clean-up and return compromised servers to production.

2 Analyze incidents for better protection: Forensic analysis

- Computer forensics: types of computer crime, role of the computer investigator.
- Modern cybercrime.
- Digital proof.

PARTICIPANTS

Systems and network engineer/administrator.

PREREQUISITES

Good knowledge of IT security and networks/systems. Must have taken the course "Collecting and analyzing logs, optimizing your IS security".

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 Forensic analysis of a Windows operating system

- Acquisition, analysis and response.
- Understanding start-up processes.
- Collect volatile and non-volatile data.
- How the password system and Windows registry work.
- Analysis of data contained in RAM and Windows files.
- Cache analysis, cookie and browsing history, event history.

Hands-on work

User injection. Break password. Collect, analyze RAM data. Reference and hash all files. Explore browser and registry data.

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 : 18 Mar., 8 June, 16 Sep., 12 Oct., 23 Nov.