Publication date : 05/13/2024

Course : Network forensics

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

This training course will give you the skills you need to identify the traces left behind when a computer system is breached, carry out investigations on different types of networks, and correctly collect the evidence required for legal proceedings.

Teaching objectives

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

- Acquire the knowledge needed to perform forensic analysis on a network
- Acquire methods for investigating wired and wireless networks
- Learn how to write a forensic audit report on penetration tests
- Identify the traces left by intrusion on a computer network

Intended audience

Systems and network engineers/administrators, security managers

Prerequisites

Good knowledge of IT security and networks/systems

Practical details

Hands-on work

Training alternating theory and practice. Everything we learn is put into practice.

Course schedule

1 Modern cybercrime

- Types of crime.
- Security incident management framework, CERT.
- Setting up labs: tools needed to investigate networks.
- Analyze and understand network attacks.
- Network intrusion detection.
- Protection tools, French legislation.

Hands-on work

Network analysis of DDOS attacks, infections and BotNet traffic to C2

PARTICIPANTS

Systems and network engineers/administrators, security managers

PREREQUISITES

Good knowledge of IT security and networks/systems

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 Digital proof

- Definition, role, types and filing rules.
- Evaluate and secure the electronic elements of a crime scene.
- Collect and preserve the integrity of electronic evidence.

Hands-on work

Duplicate data bit by bit, check integrity. Capture network data. Digital data analysis

3 Network forensic analysis

- Understand network architecture.
- Understand network attacks and vulnerabilities.
- Investigation methods for wired and wireless networks.
- Analyze frame captures.
- Identify different types of attack: ARP Storm, DHCP Starvation, ARP Spoofing, network scanning, data exfiltration...

Hands-on work

Examples of attacks on wired and wireless networks. Forensic investigation of wireless connections detected at a crime scene.

4 Audit and security

- Intrusion detection and prevention systems.
- Assimilation and execution of the intrusion test steps.
- Safety supervision.

Hands-on work

Analyze networks and intrusions with IDS/IPS. Apply investigations using the Snort tool.

5 Forensic investigation reports

- Understand the importance of investigative reports.
- Methodologies and templates for writing forensic audit reports and penetration tests.

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 : 27 May, 7 Oct.

PARIS LA DÉFENSE
2026 : 27 May, 7 Oct.