Publication date : 05/22/2024

# Course : System and network security basics

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

4,1 / 5

This highly practical course will teach you how to implement the main means of securing systems and networks. You'll learn about the threats to your information system and how to deal with them.

## Teaching objectives

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

- Understand information system vulnerabilities and threats
- Understand the role of various safety devices
- Implement the main network security measures

## Intended audience

Systems and network technicians and administrators.

## Prerequisites

Good knowledge of networks and security. Familiarity with the ANSSI security hygiene guide. Completion of the introductory cybersecurity course.

## Course schedule

### 1 The safety integrator's job

- What does a security integrator do?
- What are its skills?
- Participate in maintaining OS in optimal safety conditions.
- Integrate, deploy and maintain security solutions.
- Essential safety solutions.

**PARTICIPANTS**

Systems and network technicians and administrators.

**PREREQUISITES**

Good knowledge of networks and security. Familiarity with the ANSSI security hygiene guide. Completion of the introductory cybersecurity course.

**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 Risks and threats

- Introduction to safety.
- TCP/IP protocol strengths and weaknesses.
- Illustration of ARP and IP Spoofing attacks, TCP SYN Flood, SMURF, etc.
- Denial of service and distributed denial of service.
- HTTP, a particularly exposed protocol (SQL injection, Cross Site Scripting, etc.).
- Attacks on DNS.

### Hands-on work

Install and use the Wireshark network analyzer. Implementing an application attack.

## 3 Security architectures

- Which architectures for which needs?
- Secure architecture through virtualization.
- Firewall: the cornerstone of security.
- Technological evolution of firewalls (Appliance, VPN, IPS, UTM...).
- Firewalls and virtual environments.
- Reverse proxy, content filtering, caching and authentication.

### Hands-on work

Implementation of a Cache/Authentication proxy.

## 4 Data security

- Cryptography.
- Symmetrical and asymmetrical encryption. Hash functions.
- Cryptographic services.
- User authentication.
- X509 certificates. Electronic signature. Radius. LDAP.
- Worms, viruses, trojans, malware and keyloggers.

### Hands-on work

Deploy HTTP/FTP Antivirus proxy. Implement a server certificate.

## 5 Exchange security

- WiFi security.
- WEP's limitations. WPA and WPA2 protocol.
- Attack Man in the Middle with the AP rogue.
- The IPSec protocol.
- Tunnel and transport modes. ESP and AH.
- Analysis of protocol and associated technologies (SA, IKE, ISAKMP, ESP, AH, etc.).
- SSL/TLS protocols.
- The SSH protocol. Overview and features.

### Hands-on work

Perform a Man in the Middle attack on an SSL session. Implement IPSec transport/PSK mode.

**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.

### 6 Securing a system, the "Hardening"

- Evaluation criteria (TCSEC, ITSEC and common criteria).
- Securing Windows.
- Account and authorization management.
- Service control.
- Network configuration and auditing.
- Securing Linux.

**Hands-on work**
Example of securing a Windows and Linux system.

## Dates and locations

**REMOTE CLASS**
2026 : 18 Mar., 3 June, 16 Sep., 16 Nov.