Publication date : 06/10/2024

Course : Securing a Linux/Unix system

Practical course - 3d - 21h00 - Ref. SRX
Price : 2110 CHF E.T.

4,6 / 5

This highly practical course will show you how to define a security strategy, secure Linux servers and maintain security levels. Among other things, the course covers securing the isolated system, securing the corporate network and what you need to know to carry out a security audit.

Teaching objectives

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

- Measure the security level of your Linux/Unix system
- System security solutions
- Setting up security for a Linux/Unix application
- Establish network security

Intended audience

Systems and network technicians and administrators.

Prerequisites

Good knowledge of systems and network administration.

Practical details

Hands-on work

Numerous exercises will be carried out on a network of Unix and Linux servers.

Course schedule

1 Introduction

- Why secure a system?
- Define a secure authentication strategy.
- Different encryption algorithms. Password encryption. Password verification.
- Examples of dictionary attacks.

PARTICIPANTS

Systems and network technicians and administrators.

PREREQUISITES

Good knowledge of systems and network administration.

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 Security and Open Source

- Corrections are made quickly, and bugs are made public.
- A hacker's approach: know the loopholes, know how to attack.
- Example of a vulnerability and security solution. Which solution?

3 Too complete an installation: the Linux example

- Debian, RedHat and other distributions.
- Avoid the trap of easy installation.
- Lighter kernel. Device drivers.

Hands-on work
Optimizing installations for safety management.

4 Local system security

- Examples of malice and inadvertence.
- Low permissiveness by default. File rights checking, efficient scripting and command diagnostics.
- Read-only FS: file attributes, availability and benefits. Tripwire tools.
- How long do you keep logs?
- The log analysis tool: logwatch. Reacting in real time: sample script. Using RPM as a HIDS.
- Setting up PAM in different contexts.
- Process execution containment. Terminology DAC, MAC, RBAC, context, model...

Hands-on work
Work on rights, logs and processes.

5 Network security

- Use a firewall? Use wrappers?
- Set up service access filters.
- Configure a firewall securely.
- Diagnostic commands. Setting up a NetFilter firewall under Linux.
- iptables philosophy and syntax.
- The xinetd super-server. Wrapper access restrictions, trace files.
- Audit active services. The ssh.

Hands-on work
Configure a firewall. Audit functional services.

6 Security audit utilities

- Proprietary products and free alternatives.
- Crack, John the Ripper, Qcrack.
- HIDS and NIDS intrusion detection systems.
- Test vulnerability with Nessus.
- Implementing a safety tool.

Hands-on work
Use of a few tools.

Dates and locations

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.

REMOTE CLASS
2026 : 25 Mar., 4 May, 24 June, 7 Oct., 16 Dec.