Publication date : 02/09/2024

Course : Active Directory compromise and security

Practical course - 4d - 28h00 - Ref. ADK
Price : 2890 CHF E.T.

★★★★☆ 4,6 / 5

Lors de cette formation, vous verrez quelles méthodologies et techniques sont utilisées par les attaquants, de l'accès anonyme jusqu'à la compromission totale de l'environnement. Vous apprendrez comment sécuriser son Active Directory (AD) et gérer une situation de crise après compromission de tout son réseau.

Teaching objectives

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

- ✓ Describe the internal mechanisms of Active Directory
- ✓ Identify safety features
- ✓ Designing a robust architecture
- ✓ Understand and implement the main attacks and exploits of an Active Directory network
- ✓ Implementing countermeasures
- ✓ Rebuilding your Active Directory in the event of a compromise

Intended audience

Windows administrators, IT support staff, CISOs, slotters.

Prerequisites

Basic knowledge of Windows, Active Directory, networks and IT security.

Practical details

Teaching methods

Méthode expositive, démonstrative et active. Alternance entre présentation, démonstration et mise en pratique.

Course schedule

PARTICIPANTS

Windows administrators, IT support staff, CISOs, slotters.

PREREQUISITES

Basic knowledge of Windows, Active Directory, networks and IT 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.

1 Active Directory security fundamentals

- Understand a typical Active Directory architecture.
- Understand Active Directory compromise methodology.
- The main attack vectors used to compromise Active Directory.
- Review of authentication/authorization.
- An overview of the different protocols.
- Understand the associated recommendations and best practices.

Tutored hands-on work

2 Understanding risks and attacks

- Overview of IS risk management methods.
- Methodology for compromising an Active Directory (on-premise).
- Understand the different stages of an attack.
- Simulate attacks and analyze countermeasures.
- Detect security vulnerabilities.
- Overview of related tools.

Hands-on work

Implement the main attacks and exploits of an Active Directory network.

3 Hardening the AD infrastructure

- Design a curing plan.
- Deploy associated directives.
- Audit an infrastructure.
- Collect events at company level.
- Implement recommended guidelines and new hardening standards (PAM, JIT/JEA, etc.).

Tutored hands-on work

Implement AD infrastructure hardening.

4 Managing a compromised Active Directory

- The main stages in AD incident management.
- Crisis management and communication.
- Rebuilding the AD.

Hands-on work

Implement countermeasures.

Dates and locations

REMOTE CLASS
2026 : 2 June, 7 July, 15 Sep., 24 Nov.

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.