Publication date : 01/20/2025

Course : Active Directory offensive security, level 2

Practical course - 4d - 28h00 - Ref. SDC
Price : 2410 € E.T.

Cette formation vous apprendra les techniques indispensables pour mesurer le niveau de sécurité de votre Active Directory. A la suite de ces attaques, vous acquerrez les compétences nécessaires à la réalisation d'un test d'intrusion Active Directory, la méthodologie et les techniques utilisées lors d'une intrusion.

Teaching objectives

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

- Master advanced operating techniques in Active Directory environments
- Identify and exploit complex configurations and vulnerabilities
- Work on realistic scenarios in simulated corporate environments

Intended audience

Pentesters, system administrators, security managers and cybersecurity professionals.

Prerequisites

Bonne connaissance des environnements Windows et des concepts réseau. Ou connaissances équivalentes à celles apportées par le cours "Sécurité offensive de l'Active Directory, niveau 1" (réf. SDB).

Practical details

Hands-on work

Expositive, demonstrative and active method. Alternating presentations, demonstrations and practical exercises.

Course schedule

1 Fundamental theories and initial attack techniques

- Initial attack techniques.
- Understanding of administration mechanisms (RPC, SMB, WMI, etc.).

PARTICIPANTS

Pentesters, system administrators, security managers and cybersecurity professionals.

PREREQUISITES

Bonne connaissance des environnements Windows et des concepts réseau. Ou connaissances équivalentes à celles apportées par le cours "Sécurité offensive de l'Active Directory, niveau 1" (réf. SDB).

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 Techniques for bypassing safety equipment

- Anti-virus bypass techniques.
- AMSI bypass techniques.
- EDR bypass techniques.

3 Azure and the compromise of Azure environments

- Fundamental concepts of Azure and integration with Active Directory.
- Recognition and compromise techniques in hybrid environments.

4 Active Directory and red-teaming

- Gathering information for a Red Team operation.
- Hiding his attacks.
- Offensive tools for the red team.
- Compromise of SCCM-type equipment.

5 Development of offensive tools

- Introduction to the development of offensive tools in C# for Windows.
- The main C# frameworks and libraries useful for developing offensive tools (.NET, WinAPI, P/Invoke).
- Creation of C# projects for the development of offensive tools.
- Use debugging tools to create and maintain tools.
- Overview of the main Active Directory services (e.g. DNS, LDAP, Kerberos, etc.).
- Attacks against the Kerberos protocol in Active Directory.
- Development of tools for attacking and defending Active Directory.

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 : 23 June, 29 Sep., 1 Dec.

PARIS LA DÉFENSE
2026 : 16 June, 22 Sep., 24 Nov.