Publication date : 01/20/2025

Course : Active Directory offensive security, level 1

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

This training course will teach you the essential techniques for measuring the security level of your Active Directory. Following these attacks, you will acquire the skills needed to carry out an Active Directory penetration test, as well as the methodology and techniques used during an intrusion.

Teaching objectives

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

- Understand the architecture and operating principles of Active Directory (AD)
- Master techniques for attacking and analyzing an AD environment
- Identify and remedy common vulnerabilities
- Implement preventive measures to secure AD infrastructures

Intended audience

Pentesters, system administrators, security managers and cybersecurity professionals.

Prerequisites

Good knowledge of Windows environments and network concepts.

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

- Understanding of administration mechanisms (RPC, SMB, WMI, etc.).
- Identity and access management (NTLM, Kerberos).

PARTICIPANTS

Pentesters, system administrators, security managers and cybersecurity professionals.

PREREQUISITES

Good knowledge of Windows environments and network concepts.

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 Recognition

- OSINT techniques and tools (images, emails, identifiers, websites, etc.).
- Recognition from anonymous and authenticated access.
- Advanced network recognition and operation techniques.

3 Lateral movements

- ADIDNS, WinRM and JEA poisoning, LAPS secret extraction, gMSA/sMSA,
- Abuse of MS-SQL trust links, NTLM relaying, authentication coercing.
- Kerberos relay, inter-forest pivots, pivots to Azure (PHS, PTA, ADFS), pivots from Azure (Intune).

4 Elevation of privileges

- Local elevation of privileges: access token and impersonation, study of potato vulnerabilities.
- Bypass software restrictions (AppLocker, restricted environments such as Citrix).
- Elevation of domain privileges: study and abuse of ACLs, advanced exploitation of Kerberos delegation, ADCS, abuse of privileged groups.
- Public vulnerability scanning, authentication replay, kerberoasting, control path abuse.

5 Active Directory secret extraction and persistence techniques

- Extraction and manipulation of critical secrets: LSASS, DPAPI, Kerberoasting.
- Persistence: ADCS (certificates), Kerberos tickets (golden, diamond, sapphire), DSRM, golden gMSA, AdminSDHolder abuse.
- Skeleton key creation, Kerberos delegation, GPO poisoning.
- Extending compromise: studies of inter-domain/inter-forest trust relationships.
- Abuse of Kerberos delegation.

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 : 7 Apr., 30 June, 6 Oct., 8 Dec.

PARIS LA DÉFENSE
2026 : 23 June, 29 Sep., 1 Dec.