Publication date : 03/12/2024

Course : VPN security, wireless and mobility, overview

Seminar - 2d - 14h00 - Ref. VPN
Price : 2170 CHF E.T.

★★★★★ 5 / 5

Today, wireless communication technologies and mobile terminals greatly facilitate access to corporate applications. This seminar provides a comprehensive overview of threats and vulnerabilities, as well as practical solutions to protect against them.

Teaching objectives

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

- Assessing safety risks in a mobile context
- Know the types of attack
- Understanding the VPN solution
- Securing wireless networks and smartphones

Intended audience

CIOs, CISOs, security managers, project managers, consultants, administrators.

Prerequisites

Basic computer skills.

Practical details

Example

Theoretical and practical approach with demonstrations, advantages and disadvantages of solutions, feedback.

Course schedule

1 Threats and vulnerabilities

- Developments in cybercrime in France.
- Statistics and evolution of attacks.
- Risk assessment in a mobile context.

PARTICIPANTS

CIOs, CISOs, security managers, project managers, consultants, administrators.

PREREQUISITES

Basic computer skills.

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 Attacks on the user

- User-oriented attack techniques.
- Social engineering techniques.
- Malicious code and social networks.
- The specific dangers of Web 2.0.
- Attack on passwords.
- Attack "Man in the Middle".

3 Attacks on client workstations

- Risks specific to client workstations (worms, viruses, etc.).
- The safest browser.
- Rootkit browser and user station.
- How effective is antivirus software?
- Risks associated with removable devices.
- The role of the personal firewall.
- USB key security.
- Client workstations and virtualization.

4 Virtual private network (VPN) security

- Tunneling techniques. Remote access via the Internet: an overview of what's available.
- PPT, LTP, L2F protocols for VPNs.
- The IPsec standard and the AH, ESP and IKE protocols.
- VPN solutions for 3G access.
- Solutions for Blackberry, iPhone... ?
- SSL VPN: the technology and its limits.
- Overview of SSL VPN solutions. Selection criteria.
- IPsec or SSL VPN: what's the right choice for mobile workstations?

5 Wireless network security

- Access Point security (SSID, MAC filtering, etc.).
- Why is WEP dangerous? What are the benefits of WPA, WPA2 and 802.11i?
- Authentication in corporate Wi-Fi networks.
- VPN (IPsec) technologies for Wi-Fi networks.
- How is Wi-Fi hotspot security ensured?
- WPA and WPA2 attack techniques.
- Rogue AP.
- Specific attacks on Bluetooth.

6 Smartphone security

- Cell phone security (Edge, 3G, 3G+...).
- The specific risks of Smartphones.
- Security breaches: the top ten by platform.
- Viruses and malicious code: what's the real risk?
- Protect your data in the event of loss or theft.

Demonstration

Implementation of highly secure Wi-Fi access with IPsec and EAP-TLS. Man in the Middle" attack on an HTTPS Web application via a Smartphone (sslsnif and sslstrip).

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 : 9 June, 24 Sep., 15 Dec.